IT-sikkerhedspolitik

for

Gladsaxe Kommune

2. Del
(RETNINGSLINIER)

INDHOLDSFORTEGNELSE

1. Organisation og ansvar

1.1. Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring organisation og ansvar:

"Byrådet har udpeget vicekommunaldirektøren som den øverste ansvarlige for kommunens IT-sikkerhed.

Der er etableret en sikkerhedsorganisation, der under ansvar overfor vicekommunaldirektøren skal varetage de daglige opgaver i relation til IT-sikkerheden.

Arbejdet i sikkerhedsorganisationen skal sikre, at IT-sikkerhedspolitikken og tilhørende retningslinier implementeres effektivt i Gladsaxe Kommune. Organisationen skal sikre, at IT-sikkerhedsniveauet altid er i overensstemmelse med IT-sikkerhedspolitikken, og skal derfor etablere og vedligeholde rutiner der overvåger, hvor effektivt IT-sikkerheden er implementeret i kommunen.

Sikkerhedsorganisationen skal specifikt sikre, at der mindst en gang årligt foretages en gennemgang af IT-sikkerhedspolitikken og den tekniske og faktiske implementering.

Forvaltningscheferne er overfor vicekommunaldirektøren ansvarlig for de enkelte forvaltningers håndtering af informationer, herunder overholdelse af Gladsaxe Kommunes IT-sikkerhedsregler.

Forvaltningscheferne kan overlade nærmere afgrænsede dele af deres funktioner til områdeansvarlige, der derefter varetager disse funktioner under ansvar overfor den pågældende forvaltningschef."

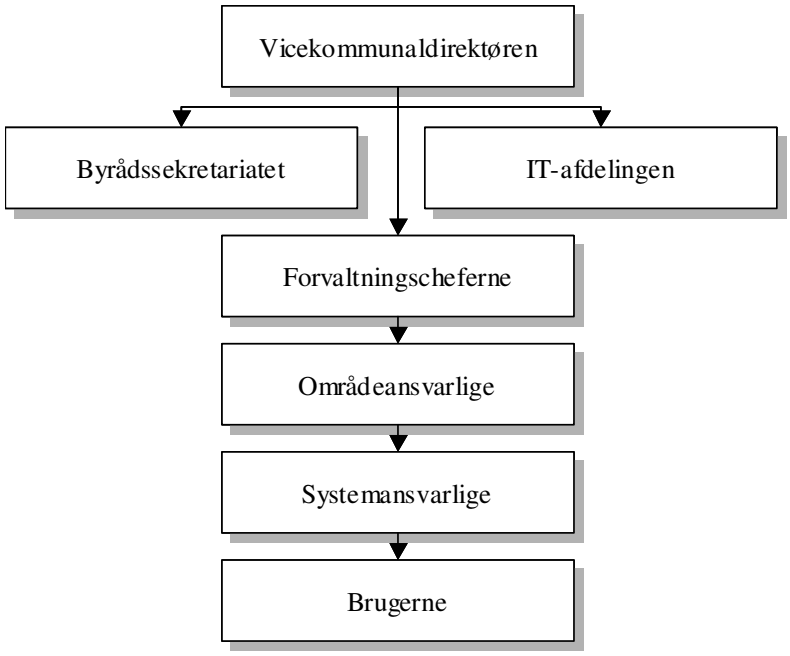
1.2 Retningslinier

1.2.1 Sikkerhedsorganisationen

Behandlingen af elektronisk information, herunder persondata i henhold til persondataloven, sker under den dataansvarliges ansvar. Når en medarbejder i Gladsaxe Kommune behandler disse informationer på den dataansvarliges vegne (Gladsaxe Kommune), skal medarbejderen følge kommunes sikkerhedsregler. Disse sikkerhedsregler er beskrevet i nærværende retningslinier for IT-sikkerhed.

Byrådet vedtager politikker på de områder, der har betydning for Gladsaxe Kommunes sikkerhed, herunder bl.a. IT-sikkerhedspolitikken. Byrådet modtager årligt en redegørelse om IT-sikkerhedsarbejdet i kommunen.

Gladsaxe Kommune har etableret en sikkerhedsorganisation, som har det overordnede ansvar for IT-sikkerheden i kommunen. Organisationen er delt op i en administrativ enhed og en teknisk enhed, der hver især har ansvaret for, at henholdsvis de administrative procedurer og den implementerede teknik understøtter det ønskede IT-sikkerhedsniveau. Sikkerhedsorganisationen ser således ud:



1.2.2 IT-sikkerhedsudvalget

Øverste IT-sikkerhedsmyndighed er IT-sikkerhedsudvalget, som består af vicekommunaldirektøren, lederen af byrådssekretariatet og IT-chefen. Det er IT-sikkerhedsudvalgets overordnede ansvar og opgave at overvåge, at IT-sikkerhedspolitik og tilhørende retningslinier er tilstrækkelige i relation til det ønskede IT-sikkerhedsniveau, og at disse efterleves i Gladsaxe Kommune. IT-sikkerhedsudvalget skal overfor Byrådet rapportere årligt omkring IT-sikkerhedsniveauet i Gladsaxe Kommune.

Det er endvidere IT-sikkerhedsudvalgets opgave at vurdere de sikkerhedsmæssige aspekter i forbindelse med større IT-investeringer, ændringer i den anvendte teknologi eller andre forhold, som har stor indflydelse på IT-sikkerheden i kommunen.

Der pålægges sikkerhedsorganisationen følgende ansvar:

Vicekommunaldirektøren

Vicekommunaldirektøren er den øverste sikkerhedsansvarlige med lederen af byrådssekretariatet som stedfortræder. Vicekommunaldirektøren skal godkende alle retningslinier til IT-

sikkerhedspolitikken, alle systemer og sikkerhedsmæssige aspekter i væsentlige ændringer til IT-anvendelsen i Gladsaxe Kommune.

Vicekommunaldirektøren har ansvaret for synliggørelse af kommunens IT-sikkerhedspolitik og for at fastsætte et ensartet sikkerhedsniveau i kommunen, der giver et tilfredsstillende sikkerhedsniveau ved anvendelse af få ressourcer. Vicekommunaldirektøren har også ansvar for organiseringen af sikkerhedsorganisationen, herunder sikre udpegning af systemansvarlige for de enkelte systemer.

Vicekommunaldirektøren skal sikre, at IT-sikkerhedspolitik og tilhørende retningslinier gennemgås mindst en gang årligt med henblik på at kontrollere, at de er fyldestgørende, tilstrækkelige og afspejler de faktiske sikkerhedsforhold i Gladsaxe Kommune.

Byrådssekretariatet

Byrådssekretariatet har det organisatoriske ansvar for de retningslinier, som omhandler de administrative områder, jf. IT-sikkerhedspolitikkens punkt 3.2. I byrådssekretariatet varetager 2 sikkerhedsmedarbejdere sikkerhedsarbejdet under ansvar overfor den øverste sikkerhedsansvarlige. Dette arbejde omfatter blandt andet:

- Koordinering af anmeldelser til datatilsynet,
- Tilslutning til fællesanmeldelser,
- Vejledning af forvaltningerne vedrørende persondatalovens bestemmelser,
- Håndtering af forespørgsler om udtræk eller sammenkørsler af systemer m.m.
- Informering af de system- og områdeansvarlige for kommunens systemer.
- Udarbejdelse af oversigter over de system- og områdeansvarlige for kommunes systemer.
- Vedligeholdelse af fortegnelse over foretagne anmeldelser af systemer til DatatilsynetVaretagelse af funktioner vedrørende anmodning om indsigtsret.
- Adgangs- og autorisationsordninger på KMD-NET og ØS, herunder kontrol af, at anmodningen indeholder den fornødne godkendelse fra den relevante afdelingschefautorisationer

IT-afdelingen

IT-afdelingen har ansvaret for de retningslinier, som omhandler de tekniske områder, jf. IT-sikkerhedspolitikkens punkt 3.2. Som følge af IT-afdelingens begrænsede størrelse er der ikke en egentlig funktionsadskillelse i IT-afdelingen i forhold til de opgaver, som IT-medarbejderne varetager. Dette skal ligeledes medvirke til at personafhængighed undgås i IT-afdelingen.

IT-afdelingens primære opgave er at håndtere driften og sikre, at systemer er tilgængelige i henhold til brugernes krav. Herudover er det IT-afdelingens opgave at foretage teknisk kvalitetssikring af nye systemer, konfigurationsændringer og andre ændringer til den eksisterende

IT-anvendelse for at sikre, at disse ikke påvirker sikkerhedsniveauet i negativ retning. Ved anvendelse af ny teknologi eller særligt sikkerhedskrævende systemer/aktiver, skal anvendelsen og sikkerheden på forhånd godkendes af vicekommunaldirektøren.

1.2.3 Øvrige implicerede parter

Alle medarbejdere og eksterne parter, som har adgang til Gladsaxe Kommunes administrative netværk skal følge reglerne der er specificeret i retningslinien for medarbejdere. Herudover er der følgende særlige forhold for visse medarbejdere:

Forvaltningscheferne

Forvaltningscheferne er overfor vicekommunaldirektøren ansvarlige for de enkelte forvaltningers behandling af informationer, herunder overholdelse af Gladsaxe Kommunes sikkerhedsregler inden for den pågældende forvaltnings område og overholdelsen af lovgivningen. Det påhviler forvaltningscheferne at påse, at:

- systemer, der behandler fortrolige og følsomme personoplysninger, ikke oprettes eller tilsluttes uden vicekommunaldirektørens godkendelse. Systemer uden fortrolige og følsomme personoplysninger kan oprettes uden vicekommunaldirektørens godkendelse. Når der er givet tilladelse til oprettelse eller tilslutning skal der ske en anmeldelse af systemet til Datatilsynet. Forvaltningen er ansvarlig for udformning af anmeldelsen. Byrådssekretariatet koordinerer og rådgiver i forbindelse med anmeldelse til Datatilsynet,
- alle systemer, uanset om de behandler fortrolige og følsomme personoplysninger eller ej, skal anmeldes til byrådssekretariatet af hensyn til opfyldelse af indsigtsretten samt ajourføring af oversigter over kommunens systemer, og
- kommunes retningslinier for medarbejdere overholdes, herunder medarbejdere med hjemmearbejdspladser, bærbare computere mv.

Forvaltningschefens stedfortræder varetager disse forpligtelser under fravær eller efter aftale, dog stadig under forvaltningschefens ansvar.

Områdeansvarlige

Forvaltningscheferne kan overlade nærmere afgrænsede dele af deres funktioner til områdeansvarlige, der derefter varetager disse funktioner under ansvar overfor den pågældende forvaltningschef. En områdeansvarlig skal varetage en ledelsesmæssig funktion, og vil således typisk være en afdelingschef, kontorchef, vicekontorchef eller institutionsleder.

Ved overdragelse af forvaltningschefernes funktioner påhviler det således de områdeansvarlige at sikre at:

- systemer, der behandler fortrolige og følsomme personoplysninger, ikke oprettes eller tilsluttes uden vicekommunaldirektørens godkendelse. Systemer uden fortrolige og føl-

somme personoplysninger kan oprettes uden vicekommunaldirektørens godkendelse. Når der er givet tilladelse til oprettelse eller tilslutning skal der ske en anmeldelse af systemet til Datatilsynet. Forvaltningen er ansvarlig for udformning af anmeldelsen. Byrådssekretariatet koordinerer og rådgiver i forbindelse med anmeldelse til Datatilsynet,

- systemer uden fortrolige og følsomme personoplysninger anmeldes til byrådssekretariatet af hensyn til opfyldelse af indsigtsretten samt ajourføring af oversigter over kommunens systemer,
- fagsystemer indeholder de funktionaliteter, som er påkrævet af forvaltningen og brugerne, og som er relevant for det arbejde, som skal udføres,
- de vedtagne retningslinier for brugeradministration, herunder regler omkring anmodning om adgangs- og autorisationsordninger, afmelding af fratrådte medarbejdere, organisationsændringer mv. overholdes,
- kommunes retningslinier for elektronisk kommunikation overholdes,
- medarbejdere med hjemmearbejdspladser overholder kommunens retningslinier for anvendelse af hjemmearbejdspladser, og
- anmodninger om indsigtsret efterkommes.

Ovennævnte opgaver skal tilrettelægges i samarbejde med den systemansvarlige, jævnfør afsnit 1.3.6. samt procedurerne 01.A og 01.B, som omhandler sikkerhedslogning og autorisationer.

Et fagsystem har som hovedregel alene én områdeansvarlig, således at hovedansvaret er placeret ét sted. Anderledes er det dog på de decentrale enheder, f.eks. skoler. Her kan samme fagsystem have flere områdeansvarlige (en fra hver skole).

Systemansvarlige

Den systemansvarlige er den person, som har den faglige indsigt i det enkelte system. Den systemansvarlige er ansvarlig for den praktiske udførsel af sikkerhedsopgaverne under ledelse af den områdeansvarlige.

For hvert IT-system udpeger vicekommunaldirektøren en systemansvarlig. For tværgående systemer, som benyttes af flere forvaltninger, sikrer vicekommunaldirektøren, at der bliver udpeget en systemansvarlig.

Den systemansvarlige er for sit område ansvarlig for:

- At der i kommunen er det nødvendige kendskab til systemets funktionsmåde,
- At der sker anmeldelse af systemet til Byrådssekretariatet og til Datatilsynet, hvis systemet håndterer fortrolige data,
- Med jævne mellemrum at revurdere systemet og eventuelt stille forslag til udvikling og forbedringer,

- Udarbejdelse af forslag til en hensigtsmæssig og økonomisk forsvarlig benyttelse af systemet,
- Organisering af den nødvendige uddannelse af brugerne,
- Udarbejdelse af forslag til hensigtsmæssig organisering af brugerprofiler med udgangspunkt i en klassifikation af data,
- At Gladsaxe Kommune har de fornødne licenser/tilladelser til at anvende det pågældende system, og at brugerne gøres bekendt med, hvordan systemerne efter disse tilladelser må anvendes, og
- Fastsætte logningsniveauet for systemet samt betryggende opfølgning på registreringerne.

Brugernes ansvar

Ansvaret for sikkerheden ligger ikke alene i byrådssekretariatet og hos forvaltningschefen, de områdeansvarlige og systemansvarlige, men i høj grad også hos de enkelte brugere af systemerne.

Det er således brugernes ansvar at være bekendt med retningslinier for medarbejdere, herunder særligt at:

- brugerens personlige password, som knytter sig til den enkelte autorisation, ikke videregives til andre. Passwordet er personligt og må kun benyttes af brugeren selv. Passwordet skal udskiftes jævnligt og må aldrig skrives ned,
- skærmen ikke står unødig åben når den ikke bruges, ved f.eks. deltagelse i møder. Du skal have sikkerhedslås med password på pauseskærmen,
- autorisationer og adgange, herunder e-mail og internet-adgang primært bruges tjenstligt,
- indberette IT-sikkerhedsrelaterede problemer eller uhensigtsmæssigheder til IT-sikkerhedsorganisationen,
- gøre afdelingschefen/områdeansvarlig eller systemansvarlige opmærksom på tilfælde af unødvendige adgange og autorisationer ved for eksempel jobskifte med henblik på annullering af autorisationen, og
- lokale (eller egne) systemer ikke oprettes uden godkendelse eller anmeldelse i byrådssekretariatet og evt. Datatilsynet.

Listen her er ikke udtømmende, men der henvises til særskilte retningslinier for brugerne.

2 Krav til eksterne parter og leverandører

2.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring krav til eksterne parter og leverandører:

> *"Samarbejdspartnere med adgang til systemer skal være underlagt de samme krav, som beskrives i IT-sikkerhedspolitikken og tilhørende retningslinier. Andre eksterne parter og leverandører skal ligeledes leve op til de IT-sikkerhedskrav, som Gladsaxe Kommune stiller.*
>
> *Det skal som udgangspunkt sikres, at:*
>
> - *samarbejdspartnere, som har adgang til Gladsaxe Kommunes systemer, er underlagt sikkerhedskrav svarende til mindst sikkerhedsniveauet hos Gladsaxe Kommune, og*
> - *sikkerheden i leverancer fra outsourcing partnere/leverandører er på et niveau mindst svarende til sikkerhedsniveauet hos Gladsaxe Kommune."*

2.2 Retningslinier

Leverandører, konsulenter, revisorer og andre eksterne parter kan have behov for fysisk og/eller logisk adgang til kommunens centrale servere, systemer og data i forbindelse med konsulentarbejde, revision, implementering, vedligeholdelse, support og servicering af systemer, basisprogrammel og IT-ressourcer. Nærværende retningslinie vedrører autoriseringen og administrationen af sådanne adgange.

Enhver ekstern part, som ønsker logisk adgang til Gladsaxe Kommunes systemer og data, skal godkendes af IT-sikkerhedsudvalget. Godkendelsen skal foretages på baggrund af en beskrivelse af den ydelse, som den eksterne part skal levere, samt omfanget af adgangen, risici forbundet hermed og IT-afdelingens tekniske vurdering af problemstillingen.

Inden en ekstern part eller leverandør kan få adgang til Gladsaxe Kommunes interne IT-ressourcer, skal de underskrive en fortroligheds- og sikkerhedserklæring, der sikrer, at den eksterne part/leverandør er indforstået med at overholde Gladsaxe Kommunes IT-sikkerhedspolitik. Erklæringen findes på intranettet, hvorfra den skrives ud, underskrives og sendes til byrådssekretariatet.

Ingen ekstern part/leverandør må få fysisk og/eller logisk adgang til Gladsaxe Kommunes interne IT-ressourcer uden forudgående aftale med IT-afdelingen. Der gives kun fysisk adgang til serverrummet i de situationer, hvor arbejdets karakter kræver dette, som f.eks. i for-

bindelse med service/inspektion af køleanlæg, el-installationer mv. i serverrummet. Det er IT-afdelingen, der til en hver tid vurderer om adgangen er relevant.

Enhver logisk adgang må kun ske inden for normal arbejdstid og må kun ske på en af følgende to måder:

- Adgang via pc-arbejdsplads i IT-afdelingen (uden for serverrummet), hvor leverandøren kan udføre de aftalte opgaver. Der vil ikke blive udleveret et bruger-id/password til operativsystemet, men IT-afdelingen vil sikre, at pc-arbejdspladsen er koblet op til de relevante systemer med de nødvendige rettigheder,
- Adgang via dial-up forbindelse til relevante systemer. Opkoblingen må kun ske på anfordring, og kun til en terminalserver hvorfra arbejdet kan udføres. Der vil ved opkoblingen ikke blive stillet bruger-id/password til rådighed for leverandøren. Leverandøren må kun kunne anvende en etableret session mod de relevante systemer. Når arbejdet er afsluttet informeres IT-afdelingen, der herefter vil lukke for adgangen til systemerne. Eventuelle eksterne sessioner der stadig er etableret ved arbejdstids ophør, vil blive lukket med kort eller ingen varsel.

Hvor der er givet logisk adgang til eksterne parter til Gladsaxe Kommunes servere, systemer mv. på superbrugerniveau, skal dette logges med angivelse af formål, navn og varighed. Loggen opbevares af byrådssekretariatet, og skal primært anvendes i forbindelse med opklaring af mistænkelige forhold.

Det er den systemansvarlige, der har ansvaret for at kontakte IT-afdelingen med henblik på at informere om arbejdets karakter, omfang, og tidspunkt mv. IT-chefen skal godkende beslutningen om gennemførelsen af systemændringer i henhold til retningslinien om konfigurationsændringer.

Outsourcing

Outsourcing partnere er omfattet af kravene til eksterne leverandører. Outsourcing partnere skal således godkendes af IT-sikkerhedsudvalget efter samme metode som med andre leverandører. IT-sikkerhedsudvalget kan vælge at supplere beslutningsgrundlaget med en udtalelse eller erklæring om IT-sikkerheden fra 3. mand. Outsourcing partnere skal således også afkræves en fortroligheds- og sikkerhedserklæring, hvor partneren erklærer at holde oplysninger fortrolige og at opretholde et sikkerhedsniveau, som mindst svarer til Gladsaxe Kommunes.

I tilfælde af, at driften af et givet system er outsourced til en ekstern part, skal byrådssekretariatet afkræve outsourcing partneren en revisionserklæring, hvis den pågældende outsourcing partner leverer drift af systemer, som er indberettet til Datatilsynet. Revisionserklærin-

gen skal sikre, at den eksterne part varetager sikkerheden omkring driften af Gladsaxe Kommunes system på betryggende vis og i overensstemmelse med persondatalovgivningen.

3 Klassifikation af data

3.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring klassifikation af data:

"For at kunne opretholde et ønsket sikkerhedsniveau, er det væsentligt at kunne identificere og klassificere de data, som skal beskyttes. I forbindelse med ændringer der påvirker IT-miljøet skal det sikres, at berørte systemer og data fortsat kan beskyttes i overensstemmelse med gældende krav.

For at få overblik over eksisterende data og deres anvendelse, skal disse data registreres og klassificeres, og der skal tilknyttes en systemansvarlig, som har ansvaret for vedligeholdelse af databeskrivelsen og en områdeansvarlig, som har ansvar for tildelingen af adgang til data.

Dataklassifikationen skal stille krav til håndteringen og opbevaringen for de pågældende data. Eksempelvis skal det ved introduktion af et nyt system sikres, at sikkerheden i systemet er i stand til at beskytte de data, som systemet anvender i overensstemmelse med datas sikkerhedsklassifikation.

Det skal sikres, at:

- *alle data grupperes og klassificeres i forhold til ønsket sikkerhedsniveau,*
- *alle data registreres og tildeles et ejerskab på en hensigtsmæssig og overskuelig måde, og*
- *krav efter persondataloven eksplicit fremgår af klassificeringen."*

3.2 Retningslinier

Alle systemer skal registreres og tilknyttes en områdeansvarlig, der er ansvarlig for såvel system som tilhørende data. For hvert system skal de tilknyttede data klassificeres i henhold til de fastlagte klassifikationer. Den områdeansvarlige har ansvaret for, at system og data klassificeres, og hvis det er påkrævet, har denne ansvaret for, at der sker anmeldelse til Datatilsynet. Systemejeren har endvidere ansvaret for, at det pågældende system lever op til de krav til sikring og behandling af data, som klassifikationen foreskriver.

Dataklassifikation

Dataklassifikationerne er fastlagt med udgangspunkt i "Lov om behandling af Personoplysninger", og kravene er tilsvarende fastlagt ud fra kravene i loven samt de sikkerhedskrav, som er fastlagt i "Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige Forvaltning" (bekg. nr. 528 af 15. juni 2000) og Datatilsynets "Vejledning om anmeldelse i henhold til kapitel 12 i lov om behandling af personoplysninger" (vejl. nr. 125 af 10. juli 2000).

Dataklassifikationen er opdelt i følgende kategorier:

- offentlige data - data, som ikke indeholder personhenførbare informationer eller andre informationer, som den enkelte borger uden videre kan begære indsigt i,
- fortrolige data – data, som ikke indeholder personhenførbare informationer, men 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, konfiguration af firewalls mv.,
- personrelaterede data – data, som direkte kan henføres til fysiske personer, men som ikke indeholder fortrolige informationer i persondatalovens forstand,
- følsomme data – data, som dels er direkte personhenførbare og som dels indeholder fortrolig information efter persondatalovens definitioner.

Følsomme personhenførbare informationer omfatter:

- oplysninger om racemæssig eller etnisk baggrund,
- politisk, religiøs eller filosofisk overbevisning,
- fagforeningsmæssige tilhørsforhold,
- oplysninger om helbredsforhold og seksuelle forhold,
- oplysninger om strafbare forhold og væsentlige sociale problemer,
- interne familieforhold, herunder stridigheder og oplysninger om selvmordsforsøg, ulykkestilfælde og misbrugsforhold.

Herudover kan oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold efter omstændighederne også være følsomme.

Forskellen på offentlige og fortrolige data er alene, at offentligheden kan begære indsigt i de offentlige data, men ikke de fortrolige data. For de personhenførbare informationer gælder det, at alene den registrerede person kan begære indsigt i disse data.

Følgende er en oversigt over sikkerhedskrav til registreringen af data:

	Alle data	**Følsomme data**
Autorisation	Den områdeansvarlige skal autorisere alle brugeres ad-	Den områdeansvarlige skal autorisere brugeres adgang til data samt

	Alle data	Følsomme data
	gang til data. Rettigheder gennemgås årligt.	deres rettigheder til at læse, opdatere og slette data. Rettigheder og adgange gennemgås hvert år.
Adgangsforhold	Systemet skal adgangsbegrænses med bruger-ID og password.	Systemet skal adgangsbegrænses med bruger-ID og password.
Datakommunikation	Kommunikation af fortrolige og personrelaterede data over offentlige net skal krypteres.	Der må ikke foregå kommunikation af følsomme data over offentlige net.
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 i mellem ½ og 5 år (gælder ikke dokumenter under udarbejdelse). Loggen skal indeholde tidspunkt, bruger, anvendelse og personen, som anvendelsen vedrører.
Opbevaring	Alle data skal være omfattet af backup. Fysiske papirer med personhenførbare og fortrolige informationer skal opbevares i aflåste skabe.	Alle data skal være omfattet af backup. Fysiske papirer skal opbevares i aflåste skabe.
Anmeldelse	Alle systemer skal anmeldes til Byrådssekretariatet.	Systemer med følsomme data skal anmeldes til Byrådssekretariatet og til Datatilsynet.

Alle data og systemer er underlagt de øvrige krav i nærværende retningslinier omkring IT-sikkerheden.

Anmeldelse

Alle systemer i Gladsaxe Kommune skal anmeldes til byrådssekretariatet, der er ansvarlig for registreringen af systemejerskab og dataklassifikation. Dette gælder ikke kun købte fagsystemer, men også egenudviklede Access-databaser eller lignende systemer. Samkøringer mellem eksisterende separate systemer betragtes som nye systemer, og skal derfor anmeldes til byrådssekretariatet, som var det et nyt system.

Systemejerne vurderer i samråd med byrådssekretariatet dataklassifikationen og niveauet for den påkrævede sikkerhed IT-sikkerhedspolitikken og retningslinier tillader det. Førend et givet system kan tages i brug skal de fastlagte sikkerhedskrav være opfyldt. Væsentlige ændringer til eksisterende systemer skal forelægges byrådssekretariatet for at vurdere, om sikkerhedskravene er opfyldt og om dataklassifikationen skal ændres.

Såfremt et givet system indeholder følsomme data, skal dette anmeldes til Datatilsynet. Anmeldelse til Datatilsynet er den områdeansvarliges ansvar, men byrådssekretariatet står til rådighed, hvis der er behov for rådgivning. byrådssekretariatet vedligeholder løbende en oversigt over systemer, der er anmeldt til Datatilsynet.

Halvårligt skal byrådssekretariatet foretage en gennemgang af de registrerede systemer for at slette de systemer på listen, som ikke længere er i anvendelse, og tilføje evt. nye systemer, som ikke er blevet anmeldt til byrådssekretariatet.

4 Medarbejdere

4.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring medarbejdere:

> *"Medarbejdere i Gladsaxe Kommune skal på baggrund af deres kendskab til - og deres ansvar for sikkerhed - motiveres til at bidrage til en opretholdelse af sikkerheden i Gladsaxe Kommune.*
>
> *Det skal sikres, at:*
>
> - *medarbejderne har kendskab til Gladsaxe Kommunes IT-sikkerhedspolitik,*
> - *medarbejderne forelægges begrundelse for opretholdelse af gældende sikkerhedsniveau,*
> - *medarbejderne uddannes i nødvendigt omfang til at kunne anvende Gladsaxe Kommunes IT-systemer i overensstemmelse med gældende sikkerhedspraksis,*
> - *medarbejdere motiveres til at bidrage til den samlede sikkerhed i Gladsaxe Kommune,*
> - *medarbejderne er bekendt med potentielle personlige og kommunale konsekvenser for bevidst og ubevist brud på sikkerheden."*

4.2 Retningslinier

Medarbejdere i Gladsaxe kommune skal informeres om gældende IT-sikkerhedsregler. Det er op til den enkelte afdelingsleder at sikre, at dette sker eksempelvis i forbindelse med medarbejders ansættelse.

Fra centralt hold vil Gladsaxe Kommunes sikkerhedsorganisation løbende informere medarbejderne om IT-sikkerhed via intranettet og eventuelt via e-post. Kommunen forventer derfor, at medarbejderne, der er i direkte kontakt med Gladsaxe Kommunes IT-ressourcer (systemer og data), holder sig løbende orienteret via ovennævnte informationskanaler.

Konsekvenserne for overtrædelse eller misbrug af de gældende IT-sikkerhedsregler følger helt de i IT-sikkerhedspolitikken gældende retningslinier, og Gladsaxe Kommunes almindelige procedurer for overtrædelse af kommunens regler og normer.

I relation til udvalgte IT-anvendelsesområder har Gladsaxe Kommune defineret konkrete retningslinier, som fremgår af de efterfølgende afsnit.

4.2.1 E-post anvendelse

Anvendelsen af e-post i Gladsaxe Kommune skal opfattes som et kommunikationshjælpemiddel på lige fod med for eksempel telefonen, og Gladsaxe Kommune ser gerne at medarbejderne anvender e-post i deres daglige arbejde. Samtidig tillader Gladsaxe Kommune at medarbejdere anvender e-post til private formål så længe dette ikke påvirker det daglige arbejde for kommunen.

Som overordnet hovedregel gælder at fortrolige data ikke må sendes via e-post til personer, virksomheder eller anden myndighed uden for Gladsaxe Kommune.

I forbindelse med ekstern kommunikation skal medarbejdere i Gladsaxe Kommune endvidere være opmærksom på at kommunen understøtter e-post kommunikation med digital signatur i 10 af kommunens fællespostkasser. Det er derfor tilladt at anvende e-post til ekstern korrespondance med virksomheder, borgere eller anden myndighed, hvor der kræves en underskrift fra afsender, hvis korrespondancen foregår via en fællespostkasser med digital signatur installeret.

Andre henvendelser, som anmodninger om information, beskeder, bestillinger o.l. kan modtages. Disse henvendelser kan med fordel besvares elektronisk.

Det vil ikke være hensigtsmæssigt, at borgere henvises til at skrive til den enkelte medarbejder. Der er derfor oprettet et antal officielle Gladsaxe Kommune-adresser, som f.eks. ”Kommunen”. Herudover er der oprettet en række lokale postkasser.

Af hensyn til gældende regler om sagsbehandling, aktindsigt og arkivering skal relevante indgående og udgående e-mails printes ud og lægges på den relevante sag. Eventuelt skal der af hensyn til de interne forretningsgange tages/sendes kopi til orientering af andre (chefer, andre forvaltninger etc.).

Eventuel e-post med følsomme personoplysninger må ikke opbevares i medarbejderens elektroniske indbakke, personlige foldere mv. af hensyn til persondataloven. Oplysninger af

denne karakter skal umiddelbart overføres til relevante sikre systemer, hvor adgangskontrol, logning m.v. sker i henhold til registerforskrifterne.

Af medarbejderhåndbogen fremgår følgende: ”Da alle breve åbnes, bedes du sørge for, at private breve adresseres til din bopæl”. Da de ansatte må modtager og sender privat e-mailpost, er der fastsat regler for hvorledes hensynet til kommunens sagsbehandling af alle borgerhenvendelser kan tilgodeses, samtidig med den nødvendige fortrolighed med hensyn til de ansattes private mails opretholdes.

Udgangspunktet er at al information på den enkelte pc-arbejdsplads er ”kommunens”. Det må derfor sikres, at der til enhver tid er adgang hertil, også ved ferie og sygefravær. Det er derfor tilladt, at enten den nærmeste chef eller en kollega er autoriseret til at læse og videresende mails og dokumenter ved fravær. Når denne adgang benyttes vil mails, der fremtræder som private, selvsagt ikke blive åbnet og bearbejdet. Endvidere vil det være naturligt at orientere den fraværende medarbejder, når denne er tilbage. Endelig kan der i helt særlige situationer, hvor ingen andre er autoriseret til at få adgang til maskinen, være behov for bistand fra IT-afdelingen. I så fald skal chefen for området rette henvendelse til den, øverste sikkerhedsansvarlige og forklare hvad der er baggrunden for ønsket. Denne chef vil hvis tilladelsen gives, være forpligtet til at underrette medarbejderen om det skete, når medarbejderen på ny er på arbejde.

Hvis medarbejdere ønsker helt at eliminere risikoen for at andre ansatte ved en fejl læser en privat e-mail, henvises der til de muligheder der er for at få oprettet e-mail adresser gratis på andre servere (f.eks. hot-mail).

4.2.2 Internet

Det er en del af Gladsaxe Kommunes personalepolitik, at alle medarbejdere løbende skal have mulighed for at dygtiggøre sig, herunder mulighed for at tilegne sig den nye edb teknik.

I løbet af de næste år vil kommunen tilbyde stadig flere Internet-baserede serviceløsninger for kommunens borgere og virksomheder. Internettet bliver derfor en mere integreret del af alle medarbejders hverdag.

Kommunen vil derfor sikre, at alle administrative arbejdspladser er tilkoblet Internettet, hvorved alle har mulighed for i hverdagen at anvende de nye teknologier.

For de medarbejdere, der har ønske om derudover at anvende Internettets søgemuligheder, til eget brug, børn/børnebørns projektarbejder mv., stiller kommunens sig meget positiv.

Kommunen tilbyder derfor, at alle medarbejdere frit må anvende Internettets søgefaciliteter til eget formål, når dette sker uden for normal arbejdstid.

4.2.3 Anvendelse af hjemme-pc.

I den udstrækning af en medarbejder har fået stillet en alternativ pc-arbejdsplads til rådighed i form af en hjemme-pc, er der en række forhold som medarbejderen skal være opmærksom på.

Hjemme-pc'er skal sikkerhedsmæssigt opfattes som en fuld traditionel kommunal pc-arbejdsplads, der dog ikke er underlagt retningslinierne for fysisk beskyttelse af kommunale IT-ressourcer. Det er derfor ikke tilladt uden specifik accept fra IT-afdelingen at installere privat anskaffede programmer m.v. Samtidig er det medarbejderens ansvar, at ingen uvedkommende misbruger pc'en til formål, der ikke er forenelig med Gladsaxe Kommunes IT-sikkerhedspolitik.

5 Håndtering af konfigurationsændringer

5.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring håndtering af konfigurationsændringer:

> *"Ændringer i konfigurationen af hardware og software kan have konsekvenser for sikkerheden i IT-anvendelsen. Derfor bør sådanne ændringer kun implementeres, hvis der er tilstrækkelig sikkerhed for, at disse ikke medfører svagheder i IT-sikkerheden. Derfor skal der være en klar formel retningslinie for håndtering af konfigurationsændringer for at forhindre fejl.*
>
> *Det skal sikres, at:*
>
> - *konfigurationsændringer planlægges, kvalitetssikres og godkendes."*

5.2 Retningslinier

Tekniske konfigurationsændringer

Ansvaret for ændringer i konfigurationen af netværk, servere, platforme, operativsystemer, databasesystemer mv. påhviler IT-afdelingens medarbejder. Dette gælder alt fra centrale servere og netværksudstyr til brugernes pc'er og PDA'er, og hjemme-pc'er.

Alle konfigurationsændringer skal testes af IT-afdelingen inden implementering. Test medfører teknisk review af ændringerne samt afprøvning på testmaskiner. Særlige ændringer som eksempelvis opgradering af Notes-servere eller installation af service packs skal endvidere

planlægges inden implementering, således at væsentlige fejl undgås, og der skal så vidt muligt foretages pilottests i produktionsmiljøet hos udvalgte brugere.

Gladsaxe Kommune har valgt generelt at følge alle opdateringsanbefalinger fra Microsoft og øvrige leverandører. Alle opdateringsanbefalinger gennemgår en kritisk vurdering af bl.a. væsentlighed for brugeren før de implementeres.

Fagsystemer
De systemansvarlige har ansvaret for opgradering/patchning mv. af fagsystemerne. Som udgangspunkt skal alle ændringer til fagsystemerne foretages af leverandøren. Dette skal af den systemansvarlige varsles til IT-afdelingen i god tid, og IT-afdelingen 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 byrådssekretariatet og IT-afdelingen, som hvis der var tale om et nyt system.

Inden der gives logisk adgang til servere og systemer på superbrugerniveau, skal IT-afdelingen sørge for, at IT-sikkerhedsudvalget har godkendt den pågældende leverandør, og at byrådssekretariatet har et underskrevet eksemplar af fortroligheds- og sikkerhedserklæringen fra leverandøren.

Implementeringer på netværk
I forbindelse med implementering af servere, pc'er, netværkskomponenter, printer eller andet IT-udstyr på netværket, skal IT-afdelingen vurdere risiciene i forbindelse hermed.

For implementering af IT-udstyr og programmer, der er omfattet af IT-afdelingens positivliste, er tests ikke påkrævet, da dette allerede er foretaget tidligere. Ved implementering af øvrigt IT-udstyr og programmer, er test påkrævet.

Hardware og systemsoftware, som tilføjes netværket, skal være konfigureret efter en standardkonfiguration, som er testet af IT-afdelingen og fundet i overensstemmelse med det IT-sikkerhedsniveau, som Gladsaxe Kommune ønsker.

Varsling
IT-afdelingen skal sørge for, at alle berørte brugere varsles i god tid inden implementering af konfigurationsændringer, som kan påvirke brugernes anvendelse af IT. Hvis der er berettigede indvendinger fra brugeres eller andres side, skal IT-afdelingen tage hensyn hertil i forbindelse med planlægningen af ændringerne.

6 Brugeradministration

6.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring brugeradministration:

> *"For at kunne fastholde IT-sikkerheden omkring systemer og data, skal det sikres, gennem en hensigtsmæssig administration af brugerne, at brugere kun kan få adgang til de specifikke data og systemer, som de er autoriseret til, og som deres arbejdsfunktion kræver for at kunne levere den rigtige ydelse til f.eks. borgerne i Gladsaxe Kommune.*

Det skal sikres, at:

- *den overordnede adgangspolitik skal udstikke rammerne for kontrol af logisk adgang til systemer og data, og*
- *der er implementeret en hensigtsmæssig brugeradministration, hvor system/områdeansvarlig autoriserer adgang til data."*

6.2 Retningslinier

Al autorisation af adgange skal gives af den pågældende områdeansvarlige. Al adgang til såvel netværk som systemer skal være personlig, således at alle medarbejdere har et personligt bruger-id, og al adgang skal bekræftes ved hjælp af et personligt password. Adgang kan gives i to niveauer, hvor det første er adgang til det administrative netværk, og det andet niveau er adgang til de enkelte fagsystemer.

I særlige tilfælde kan der ses bort fra kravet omkring personligt bruger-id, hvor situationen kræver det. Eksempelvis på børneinstitutioner er det acceptabelt, at der opereres med fælles bruger-id, dog under den forudsætning, at der ikke gives adgang til opdatering af regnskabsoplysninger eller fortrolige eller følsomme personhenførbare data, jf. dataklassifikationen. Adgang til disse data skal altid være med personligt bruger-id og password.

Ansvaret for autorisation af brugeradgang til Gladsaxe Kommunes IT-ressourcer er organisatorisk opdelt på følgende måde:

- IT-afdelingen varetager brugeradministrationen af adgang til Gladsaxe Kommunes interne netværk og kontorsystemerne (e-post, journalisering, filserver mv.),
- Byrådssekretariatet varetager administrationen af adgangen til de fælleskommunale systemer hos KMD samt ØS,
- De systemansvarlige varetager opgaven med adgang til de konkrete funktioner/data i fagsystemerne, der hører under de systemansvarliges forvaltningsmæssige område.

I forbindelse med ansættelse af en medarbejder sender afdelingslederen for den pågældende medarbejder et skema for oprettelse af en ny bruger til IT-afdelingen. Skemaet findes på intranettet, og udfyldes online og sendes via e-post til IT-afdelingen. På baggrund heraf opretter IT-afdelingen medarbejderen som bruger og tildeler e-postboks, personlige og afdelingsspecifikke netværksdrev og adgang til netværksservices.

Oprettelsesskemaet videresendes til byrådssekretariatet, der foretager den nødvendige brugeroprettelse til KMD-systemerne. De systemansvarlige er herefter ansvarlig for tildeling af rettigheder i det pågældende fagsystem i henhold til oprettelsesskemaet. Byrådssekretariatet har ansvaret for arkivering af skemaer vedrørende brugeroprettelser.

Det er afdelingslederens ansvar at informere byrådssekretariatet når en medarbejderes ansættelsesforhold ophører eller ændres, således at byrådssekretariatet kan sikre sletning af brugeren eller de nødvendige ændringer i autorisationsforholdene. Byrådssekretariatet giver besked til de systemansvarlige og IT-afdelingen med henblik på den konkrete tilretning i adgangskontrolsystemerne.

IT-afdelingen skal i forbindelse med fratrædelser om nødvendig sørge for at den fratrådte persons netværksdrev og e-postboks er tilgængelig for afdelingslederen. I modsat fald skal netværksdrev og e-postboks slettes. Såfremt der er behov for en forlænget tilgængelighedsperiode, skal dette aftales særskilt.

De områdeansvarlige skal årligt foranledige, at der foretage en gennemgang af de i systemerne oprettede brugere med henblik på at identificere bruger-id'er, der ikke længere anvendes, og som evt. bør inaktiveres eller slettes. For systemer, der behandler følsomme, personhenførbare data, skal denne gennemgang foretages halvårligt og skal tillige omfatte en revurdering af de tildelte rettigheder, som den enkelte bruger har. Resultatet af gennemgangen skal rapporteres til byrådssekretariatet.

7 Udvikling og anskaffelse af hard- og software

7.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring udvikling og anskaffelse af hard- og software:

> *"IT-systemerne og netværk indgår som et væsentlig element i det daglige arbejde i Gladsaxe Kommune. Det er derfor af vital betydning, at nyanskaffelser og opdateringer af hardware og software lever fuldt op til den eksisterende kvalitets- og*

sikkerhedsstandard. Da Gladsaxe Kommune samtidig har valgt ikke at påtage sig udvikling af eget programmel i nævneværdig omfang, vil det være nødvendigt at sikre, at Gladsaxe Kommune udelukkende anvender pålidelige og kompetente leverandører, samt at der anvendes standardprodukter fra pålidelige leverandører i størst muligt omfang.

Der opereres med en målsætning om at tilstræbe ensartethed i IT-anvendelsen, hvilket betyder, at Gladsaxe Kommune i forbindelse med anskaffelse af hardware og software foretrækker kendt hardware og software fra kendte leverandører.

Det skal sikres, at:

- *der indarbejdes en tilstrækkelig IT-sikkerhed og kontrol i alle systemer såvel standardsystemer som specialudviklede eller tilrettede systemer,*
- *al IT-udstyr godkendes af IT-afdelingen,*
- *alle applikationer, der behandler personhenførbare data, vurderes af byrådssekretariatet, med henblik på en afgørelse om, hvorvidt applikationerne skal anmeldes til Datatilsynet,*
- *krav til nye systemer eller ændring af eksisterende systemer omfatter krav om kontrol- og transaktionsspor, automatiske kontroller, samt den generelle IT-sikkerhed, og*
- *der er sikkerhed og kontrol i udviklings- og vedligeholdelsesprocessen."*
- *IT-afdelingen skal involveres i den indledende fase for ethvert IT-relateret projekt.*

7.2 Retningslinier

Positivliste for anskaffelser

IT-chefen vedligeholder en "positivliste" over al hardware og software, som er godkendte anskaffelser i Kommunen. Listen ajourføres efter behov med udstyr og software, som er afprøvet og godkendt af IT-chefen. Listen omfatter al databehandlingsudstyr som netværkskomponenter, servere, computere, printere, PDA'er, skærme mv. Herudover omfatter listen også operativsystemer, kontorsystemer og andet software. Grundelementet i positivlisten er ensartethed og standardisering i IT-anvendelsen, således at kendte leverandører og kendte produkter foretrækkes.

Det er ikke tilladt at anskaffe IT-udstyr uden IT-afdelingens godkendelse. IT-afdelingens godkendelse tager udgangspunkt i positivlisten, og udstyr anskaffet uden IT-afdelingens godkendelse må ikke tilsluttes Gladsaxe Kommunes administrative netværk eller andet udstyr, der er tilsluttet Gladsaxe Kommunes administrative netværk. Der er dog enkelte undtagelser fra denne regel:

- hvis en institution opnår forhåndsgodkendelse fra IT-afdelingen i forbindelse med nyanskaffelse af IT-udstyr, må dette godt tilsluttes det administrative netværk,
- hvis en udliciteringspartner skal tilknyttes det administrative netværk, kræves det ikke, at denne skal udskifte IT-udstyr,
- hvis en institution, der allerede har anskaffet IT-udstyr, tilknyttes Kommunens administrative netværk, vil det ikke blive påkrævet, at institutionen udskifter sit udstyr medmindre det vurderes, at udstyret udgør en IT-sikkerhedsmæssig risiko.

Kun hardware og software, der er afprøvet af IT-afdelingen, og vurderes at overholde kommunens ønskede sikkerhedsniveau og er kompatibelt med det øvrige IT-udstyr, kan godkendes af IT-chefen og sættes på positivlisten. Testmetoderne kan variere fra produkt til produkt, men omfatter som udgangspunkt et teknisk review kombineret med test i produktionsmiljøet.. Der foretrækkes velafprøvede standardsystemer frem for nyudvikling af systemer.

Fagsystemer

De systemansvarlige er hovedansvarlige for de fagsystemer, som er implementeret i den pågældende forvaltning. I forbindelse med anskaffelse af nye fagsystemer er de systemansvarlige også ansvarlige for, at funktionaliteterne i nyanskaffelserne stemmer overens med de krav, som brugerne stiller. Det er også den systemansvarliges ansvar, at fagsystemet indeholder tilstrækkelige indbyggede kontroller i forbindelse med bearbejdning af data inkl. kontrol- og transaktionsspor, samt at fagsystemet overholder krav vedrørende lovgivning og dataklassifikation. Det er endvidere den systemansvarliges ansvar, at fagsystemer anmeldes til byrådssekretariatet og Datatilsynet.

Intet fagsystem må implementeres uden byrådssekretariatets og IT-afdelingens godkendelse. Byrådssekretariatet skal registrere systemet og godkende dataklassifikationen af de data, som systemet behandler. Byrådssekretariatet bistår de systemansvarlige i en eventuel anmeldelse til Datatilsynet.

IT-afdelingen skal foretage teknisk review af installationen af fagsystemet inden implementering for at påse, at dette lever op til det ønskede sikkerhedsniveau i Kommunen, og ikke kompromitterer andre systemers sikkerhed, samt at systemet kan administreres på en hensigtsmæssig måde. Dette omfatter en gennemgang af den tekniske platform og integration med øvrige systemer, samt en gennemgang af adgangskontrolmekanismerne.

Selve installationen af serversoftware og klienter foretages af leverandøren selv. IT-afdelingen leverer den nødvendige platform bestående af hardware, operativsystem og eventuelle databasesystemer, som leverandøren kan installere på. Leverandøren må på ingen måde kunne ændre konfigurationen af platformen, hvilket overvåges af IT-medarbejdere. Hvis et givet fagsystem kræver, at der foretages ændringer i konfigurationen, skal dette først gennemgås, godkendes og foretages af IT-afdelingen.

Når leverandøren har leveret den nødvendige dokumentation, vil IT-afdelingen normalt foretage fremtidige installationer af klienter, såfremt leverandøren har demonstreret installationen på ca. 5 klienter.

Systemudvikling
Det er som hovedregel ikke tilladt at foretage nyudvikling af systemer i Gladsaxe Kommune. Der skal i videst muligt omfang anskaffes systemer, som er standardiserede, selvom dette sker på bekostning af funktionalitet. Udvikling i form af Access-databaser, Excel-regneark mv. må kun foretages i det omfang systemerne ikke indeholder forvaltningsmæssigt kritiske/fortrolige data eller personhenførbare data.

Det er ikke tilladt at udvikle systemer, som indeholder personhenførbare data. Det er Gladsaxe Kommunes krav, at alle personhenførbare data håndteres i professionelle fagsystemer, som er udviklet til formålet, og som lever op til kommunens sikkerhedskrav. Dette krav er fastsat dels for at beskytte kommunens data og forvaltningen som helhed, og dels for at kommunen kan overholde persondataloven og forvaltningsloven.

Al implementering af såvel systemer som platforme er omfattet af retningslinie for konfigurationsændringer, og såfremt der er en leverandør eller anden ekstern part involveret, skal kravene i retningslinie for eksterne parter og leverandører være opfyldt.

8 Beredskabsplanlægning

8.1 Målsætning
IT-sikkerhedspolitikken indeholder følgende mål omkring beredskabsplanlægning:

> *"Der skal etableres et beredskab, som skal sikre, at Gladsaxe Kommune i tilfælde af større driftsnedbrud eller egentlige katastrofer er i stand til at genoptage kritiske forvaltningsmæssige aktiviteter inden for en acceptabel tidshorisont. De større driftsnedbrud eller katastrofer betyder tab af tilgængelighed af væsentlige systemer, udstyr og/eller faciliteter, hvorfor retablering af tilgængeligheden af disse er et centralt område i beredskabsplanlægningen.*
>
> *Det skal sikres, at:*
>
> - *kritiske forvaltningsmæssige aktiviteter kan fortsætte inden for rimelig tidshorisont i tilfælde af større driftsforstyrrelser, nedbrud, større sikkerhedsbrud eller større katastrofer, og*

- *beredskabet altid er ajourført og testet*

8.2 Retningslinier

Organisering

IT-sikkerhedsudvalget udgør tillige katastrofeledelsen. Det er katastrofeledelsens opgave at beslutte, hvorvidt der foreligger en katastrofe, samt i givet fald at igangsætte beredskabet og efterfølgende foretage overordnet ledelse af den daglige nøddrift frem til en normalisering af driftssituationen. Beredskabet koordineres med det øvrige beredskab i kommunen, hvilket er vicekommunaldirektørens ansvar.

Beredskabsplanen skal revideres årligt. Ansvaret herfor er pålagt vicekommunaldirektøren som øverste IT-sikkerhedsansvarlige, men ansvaret kan delegeres til lederen af byrådssekretariatet. Der skal desuden ske opdatering af beredskabsplanen i tilfælde af:

- væsentlige/afgørende ændringer i IT-installationer og datakommunikation,
- væsentlige/afgørende ændringer i vital information og dokumentation,
- ændringer i katastrofeledelsens sammensætning,
- ændringer i andre forhold, der øver væsentlig indflydelse på beredskabet såsom f.eks. lovgivning, kontraktlige og aftalemæssige forhold.

Beredskabsplanen skal oplyse versionsnummer og datering. Udover distribution til IT-sikkerhedsudvalget, skal beredskabsplanen opbevares på samme sted som eksternt opbevarede sikkerhedskopier af data til brug for retableringer.

Risikoanalyse

Beredskabsplanen skal være baseret på en vurdering af konsekvenser relateret til manglende tilgængelighed af kommunens IT-miljø. Det skal herunder vurderes, hvor lang tid de enkelte systemer kan tåle at være "nede" uden at det har kritiske konsekvenser for kommunen, herunder for økonomi og image. Deltagere i risikovurderingen er bl.a. ejerne af fagsystemerne. Analysen skal klarlægge tidsrummet for hvornår beredskabsplanen senest skal igangsættes efter at en katastrofe er indtrådt.

Beredskabsplanens indhold

Beredskabsplanen skal indeholde følgende:

- beredskabsorganisation,
- aktivering af beredskabsplanen (trinvis skitsering af forløbet) - Beredskabsplanen skal klart redegøre for betingelserne for aktivering af beredskabsplanen og hermed tilkald/aktivering af medarbejdere,
- aktivitetsliste for katastrofeledelse - Katastrofeledelsen skal have defineret en aktivitetsliste, som sikrer et effektivt og kontrolleret forløb i den indledende fase af en katastrofesi-

tuation. Der skal tilrettelægges et hensigtsmæssigt informationsberedskab vedrørende borgere, leverandører, medarbejdere, offentligheden, myndigheder og andre interessenter,

- alarmering - Det skal sikres, at alarmering af katastrofeledelsen kan ske hurtigt via tilkaldelister, som er integreret med eksisterende alarmeringsprocedurer vedr. indbrud og brand, således at tilkald fungerer effektivt også udenfor normal arbejdstid,
- IT-installation – Netværkskonfiguration og dokumentation af hardware, software, applikationer, kommunikationslinier samt inventarliste,
- procedurer for reetablering af IT-miljø – herunder leverandører af nødhardware, afhentning og indlæsning af backups, etablering af nødarbejdspladser mv.,
- kontraktlige forhold,
- procedurer for vedligeholdelse, test og distribution af beredskabsplanen.

Der skal endvidere være udpeget et alternativt mødested for katastrofeledelsen, såfremt kommunens normale adresse er utilgængelig.

Test og vedligeholdelse
Beredskabsplanen skal testes minimum 1 gang årligt. Målsætningen er ikke en fuld test, men et praktisk gennemløb af beredskabet. Det skal forud for enhver test sikres, at alle relevante medarbejdere og andre involverede har kendskab til beredskabsplanen. Ansvaret for gennemførsel af test ligger hos lederen af byrådssekretariatet. Testresultater skal gennemgås i IT-sikkerhedsudvalget med henblik på evt. at korrigere og opdatere beredskabsplanen.

Ved test af beredskabsplanen skal der fokuseres på:

- skrivebordstests (gennemløb/diskussion af forskellige beredskabsscenarier),
- test af alarmeringsprocedurer, herunder indkaldelse af beredskabsledelsen mv.,
- delvis test af reetablering på lokal eller alternativ lokation.

Test skal desuden gennemføres når der er foretaget væsentlige ændringer i beredskabsplanen. Vurderingen af behovet herfor foretages af IT-sikkerhedsudvalget.

9 Lovgivning

9.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring organisation og ansvar:

> *"IT-anvendelsen i kommunen skal til enhver tid være i overensstemmelse med gældende lovgivning.*

Det skal sikres, at:

- *IT-anvendelsen er i overensstemmelse med lovgivningskrav,*
- *Gladsaxe Kommune til enhver tid har de fornødne licenser til kommunens aktuelle IT-anvendelse."*

9.2 Retningslinier

Det er forvaltningschefernes ansvar, at anvendelsen af IT i Gladsaxe Kommune ikke strider med lovgivningen, og det er den enkelte systemejers ansvar at sikre, at deres respektive systemer overholder gældende lovgivning.

Som eksempel på relevante love kan blandt andet nævnes:

- Straffeloven
- Forvaltningsloven
- Arbejdsretlige love
- Persondataloven
- Offentlighedsloven
- EUs udbudsdirektiver
- Lov om digital signatur
- Ophavsretsloven

Byrådssekretariatet bistår de enkelte forvaltninger i fremfinding af relevant materiale og vurdering af, om lovgivningen er overholdt. Byrådssekretariatet er ansvarlig for dataklassifikationernes krav, således at disse er i overensstemmelse med persondataloven.

Det skal specifikt sikres, at ophavsretsloven overholdes i relation til anvendelsen af licensbelagt programmel. De områdeansvarlige skal vedligeholde et register, hvori det fremgår, hvor mange licenser der anvendes for hvert system og hvem der har disse. De områdeansvarlige skal endvidere opretholde dokumentation for erhvervede licenser.
IT-afdelingen skal sikre, at der til enhver tid opretholdes det fornødne antal licenser til det programmel, som stilles til rådighed fra centralt hold, herunder kontorautomatiseringssystemer, e-postsystemer, operativsystemer og serversoftware mv.

I forbindelse med den årlige/halvårlige gennemgang af brugeradgange og –rettigheder, skal det endvidere vurderes, om der er erhvervet licenser i tilstrækkeligt omfang.

10 Håndtering af IT-problemer

10.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring håndtering af IT-problemer:

> *"Opståede IT-problemer skal håndteres på en måde, så det pågældende problem umiddelbart korrigeres alt efter graden af alvor i problemet. Alvorlige problemer skal endvidere være genstand for en analyse med henblik på at korrigere eventuelle årsager og uhensigtsmæssigheder, og dermed bidrage til den løbende forbedring af IT-sikkerheden. Alvorlige problemer kan for eksempel være uautoriseret netværksadgang eller gentagne servernedbrud.*

Det skal sikres, at:

- *IT-problemer håndteres efter en vurdering af væsentligheden af problemet, således at såvel problem og eventuelle dybere liggende årsager og evt. sikkerhedsbrister korrigeres,*
- *medarbejdere og brugere deltager aktivt i rettelse af fejl, løsning af problemer og forbedring af IT-sikkerheden, og*
- *IT-afdelingen fører log over alvorlige hændelser med henblik på at opretholde dokumentation af hændelsesforløb."*

10.2 Retningslinier

For at sikre en korrekt og effektiv håndtering af IT-relaterede problemer, som medarbejderne i Gladsaxe Kommune oplever i deres daglige arbejde, skal der etableres en hotline- og en superbruger-funktion. Hotline-funktionen er en del af den centrale IT-afdeling, og superbrugerfunktionen er erfarne brugere i de enkelte forvaltninger, som kan afhjælpe de mest almindelige problemer, eller videresende problemet til hotline.

Samtidig skal der etableres en erfaringsdatabase, hvori almindeligt forekomne IT-problemer dokumenteres, herunder også hvorledes problemerne normalt kan løses/afhjælpes. Databasen skal som minimum være tilgængelig for medarbejderne i IT-afdelingen og superbrugerne.

For at supportfunktionen kan fungere effektivt skal brugerne normalt rette henvendelse til superbrugerne angående IT-relaterede problemer. Det er så op til superbrugerne at vurdere, hvorvidt hotline-funktionen skal involveres eller ej. Samtidig er det vigtigt, at superbrugerne

dokumenterer opståede problemer, således at der evt. kan iværksættes en forebyggende indsats.

11 Fysisk sikkerhed

11.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring organisation og ansvar:

> *"Der skal etableres en fysisk sikkerhed i og omkring Gladsaxe Kommunes IT-systemer, som reducerer risikoen for ekstern påvirkning af systemer og data samt uautoriseret fysisk adgang til Gladsaxe Kommunes IT-udstyr.*

Det skal sikres, at:

- *centralt IT-udstyr og –netværkskomponenter er sikret mod uautoriseret fysisk adgang og fysisk skade."*

11.2 Retningslinier

Den fysiske sikkerhed i relation til Gladsaxe Kommunes IT-ressourcer skal differentieres i en række forskellige sikkerhedszoner, således at det er muligt at operere med forskellige sikkerhedsniveauer afhængig af hvilken zone der er tale om. Der opereres med 3 forskellige sikkerhedszoner.

Zone 1 (omfatter maskinstuen)

Den fysiske adgang til IT-ressourcer i zone 1 skal sikres 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 medarbejder fra IT-afdelingen, rådhusbetjente og elektrikere have adgang til denne zone.

Lister over udstedte nøgler, nøglekort, adgangskoder mv. til zone 1 skal årligt gennemgås med henblik på at revurdere hvilke medarbejdere i Gladsaxe Kommune der har adgang til zonen. Pinkoder til låsen udskiftes årligt.

IT-ressourcer i denne zone skal endvidere være overvåget og beskyttet mod:

- uautoriseret indtrængning f.eks. ved anvendelse af bevægelsesdetektorer,
- strømudfald således at udstyret kan lukkes behørigt ned ved længerevarende strømsvigt,
- brand ved anvendelse af godkendt branddetekterende og brandbekæmpende udstyr,
- overophedning ved anvendelse af aktiv køling (aircondition),

- vand som følge af brud på vandførende rør eller indtrængende vand fra kloakker mv., f.eks. ved forebyggende placering og indretning af lokalerne samt evt. ved anvendelse af fugtfølere

Alarmer viderestilles til rådhusbetjentene eller Falck afhængig af den aktuelle alarm. Overvågnings- og beskyttelsesudstyr skal årligt gennemses og evt. testes af en tekniker fra en autoriseret leverandør.

Zone 2 (omfatter serveradministrationsrummet)
Den fysiske adgang til denne zone skal sikres med et fysisk eller elektronisk låsesystem, således at kun autoriserede personer har adgang til zonen. Grundlæggende vil det kun være medarbejder fra IT-afdelingen, rådhusbetjente, elektrikere samt rengøringspersonale, der har adgang til denne zone. Teknikere fra leverandører mv., der har et godkendt behov for at få logisk adgang til servere kan inden for normal arbejdstid få stillet en pc-arbejdsplads til rådighed i denne zone. Medarbejdere i IT-afdelingen lukker disse personer ind.

Lokaler under zone 2 skal endvidere sikres og overvåges i relation til uautoriseret indtrængen.

Lister over udstedte nøgler, nøglekort, adgangskoder mv. til zone 2 skal årligt gennemgås med henblik på at revurdere hvilke medarbejdere i Gladsaxe Kommune, der har adgang til zonen.

Zone 3 (omfatter Hotlinerum, Backuprum, krydsfeltsrum mv.)
Den fysiske adgang til denne zone skal sikres ved anvendelse af specifikke låse, der sikrer, at kun autoriserede personer har adgang til zonen. På rådhuset vil det være medarbejdere fra IT-afdelingen, rådhusbetjentene, elektrikere og rengøringspersonale, der adgang til denne zone. På andre lokaliteter vil adgangen være baseret på autorisation fra den lokale leder i samråd med IT-afdelingen.

Autorisation
Det er IT-chefen, der kan autorisere medarbejdere til at få adgangskort og nøgler til de sikrede lokaler. Det er også IT-chefen, der skal godkende, at tredjemand, herunder leverandører og andre samarbejdspartnere, får adgang til de sikrede lokaler. Tredjemands adgang til de sikrede lokaler skal overvåges af en IT-medarbejder fra Gladsaxe Kommune. IT-chefen skal årligt gennemgå tildelte autorisationer til de sikrede lokaler.

Kassation af IT-udstyr
I forbindelse med kassation af udstyr, skal det sikres, at udstyr, der potentielt kan indeholde fortrolig information som eksempelvis pc'er, kun kasseres via en godkendt aftager af edb-

udstyr, hvor der er behørig sikkerhed for, at ingen uvedkommende har mulighed for at fjerne udstyr eller dele heraf inden det destrueres. Ved videresalg (kun relevant i forbindelse med serverudstyr) skal det sikres, at intet udstyr forlader kommunen, før det er sikret, at samtlige informationer er fjernet eller slettet fuldstændig (afmagnetisering eller fuld formatering af diske).

12 Driftsafvikling og overvågning

12.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring driftsafvikling og overvågning:

"Gladsaxe Kommune anser det for væsentligt, at kommunen kan levere en god service og kvalitet over for brugerne af IT-systemerne og dermed de borgere, som er afhængige af kommunens service. Det er derfor vigtigt, at driftsafviklingen foretages på en stabil, kvalificeret og sikker måde, således at tilgængeligheden og pålideligheden af systemerne sikres.

Dette nødvendiggør en formalisering omkring procedurer og instrukser for driftsafvikling og planlægning. Endvidere bør det tilstræbes, at der er en klar funktionsadskillelse for at forhindre tilsigtede fejl og misbrug.

Det skal sikres, at:

- *IT-systemerne som minimum er tilgængelige for brugerne inden for normal arbejdstid,*
- *procedurer for driftsafvikling dokumenteres og godkendes,*
- *datamedier håndteres og opbevares på en sikker og forsvarlig måde."*

12.2 Retningslinier

Driftsprocedurer

IT-afdelingen varetager procedurer omkring driften af kommunens netværk og IT-udstyr, og har også ansvaret for de sikkerhedsmæssige aspekter i denne forbindelse. Driftsopgaver omfatter backup, overvågning af servere og netværk, kontrol med automatiske overførsler og andre automatiske kørsler, samt gennemgang af registreringer i diverse logs, herunder registreringer vedrørende adgangsforhold.

IT-afdelingen skal sikre, at der tages en tilstrækkelig daglig backup i henhold til retningslinier omkring sikkerhedskopiering.

IT-afdelingen skal sikre, at automatiske kørsler og overførsler foregår korrekt, herunder dataudveksling af ejendomsoplysninger og replikering af hjemmeside. Herudover skal væsentlige procedurer dokumenteres og beskrives, således at kommunens IT-medarbejdere kan foretage de kontrolhandlinger, som proceduren påkræver. Væsentligheden afgøres af systemejerens vurdering af konsekvensen ved tab af integritet af de pågældende overførsler.

IT-afdelingen skal foretage overvågning af centrale servere, netværkskomponenter og andet IT-udstyr, herunder den fysiske sikring af zone 1 områder (maskinstuen). Dette skal som udgangspunkt foretages som en teknisk overvågning, hvor en IT-medarbejder dagligt gennemgår logs fra den automatiserede overvågning.

Alle mislykkede forsøg på logisk adgang til netværk og fagsystemer skal logges. Systemejeren skal gennemgå disse logs i henhold til retningslinier omkring logisk adgang til IT-ressourcer. Det er den enkelte systemejer, der vurderer hvilke kritiske hændelser i loggen, som der bør følges op på, og som skal rapporteres til IT-sikkerhedsudvalget.

IT-afdelingen skal sikre, at kommunens netværk er opdelt i et administrativt netværk og et offentligt netværk. IT-afdelingen skal herunder sikre, at disse to netværk ikke sammenknyttes så der er risiko for uautoriseret adgang til fortrolige og følsomme personhenførbare data på det administrative netværk.

IT-afdelingen skal sikre, at operativsystemfiler og andre systemrettede filer på servere og netværkskomponenter er beskyttet mod uautoriseret adgang. Kun brugere med administratorrettigheder må få adgang til systemfilerne. Brugere med administratorrettigheder skal være ansat i IT-afdelingen, og der skal også her anvendes personlige bruger-id'er og password. Al ændring i konfigurationen af operativsystemer og andet systemsoftware er omfattet af retningslinier for håndtering af konfigurationsændringer.

Som følge af IT-afdelingens begrænsede størrelse har Gladsaxe Kommune valgt ikke at implementere funktionsadskillelse mellem de enkelte arbejdsfunktioner i driften. Dette er valgt ud fra den betragtning, at risikoen ved personafhængighed er større end risikoen forbundet med manglende funktionsadskillelse.

Opståede driftsfejl og identificerede fejl i forbindelse med gennemgang af logs skal rapporteres til IT-chefen. Det skal i samråd med IT-chefen vurderes, hvilken handling, der tages på baggrund af den opståede fejl, samt om beskrivelsen skal indgå i fejldatabasen og eventuelt rapporteres til IT-sikkerhedsudvalget.

Elektronisk udveksling af data

Al datakommunikation fra Gladsaxe Kommunes administrative netværk til samarbejdspartnere eller den omvendte vej skal forhåndsgodkendes af IT-chefen. Al datakommunikation af

fortroligt eller følsomt personhenførbart datamateriale skal krypteres eller på anden måde sikres imod uautoriseret læseadgang.

Det er som udgangspunkt ikke tilladt at anvende uautoriserede og usikre datamedier til udveksling af data eller arkivering af data, herunder særligt fortrolige eller følsomme personhenførbare data. Det er op til den enkelte medarbejder at sikre datamedier, herunder eksempelvis disketter, CD'er, USB-flash-RAM mv. Hvor det i særlige tilfælde er påkrævet at opbevare systemsoftware på datamedier (eksempelvis BIOS-opdateringer mv.), skal disse opbevares i zone 2-lokaler sammen med datamedier indeholdende installationssoftware af operativsystemer, databaser, fagsystemer mv.

13 Logisk adgangskontrol til IT-ressourcer

13.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring organisation og ansvar:

"Det er Gladsaxe Kommunes IT-politik, at samtlige IT-ressourcer og kritiske data, skal beskyttes mod uautoriseret logisk adgang. Det gælder såvel de dele, der udgør Gladsaxe Kommunes IT-netværk, men også centrale og decentrale servere, applikationer og tilhørende data. Adgangskontrol til pc-arbejdspladser skal sikre beskyttelse i det omfang det måtte være muligt. Målet med at etablere logisk adgangskontrol er således at mindske risikoen for tab af integritet og fortrolighed af data, samt tilgængelighed af Gladsaxe Kommunes IT-systemer. Krav til logisk adgangskontrol skal stemme overens med de IT-sikkerhedsmæssige krav, som de involverede data og systemerne som helhed måtte stille.

Det skal sikres, at:

- *adgangen til informationer styres ved logisk adgangskontrol på baggrund af informationernes sikkerhedsklassifikation,*
- *der er tilstrækkelig logisk adgangskontrol på bærbare enheder og fjernarbejdspladser,*
- *alle adgangsmuligheder til komponenter koblet til Gladsaxe Kommunes IT-netværk er kendte og kontrolleret af IT-afdelingen,*
- *al trådløs kommunikation godkendes af IT-afdelingen inden etablering,*
- *udvekslingen af information og systemer mellem medarbejdere eller organisationer foretages på en måde, der sikkerhedsmæssigt lever op til de krav, som de berørte data måtte kræve,*

- *uautoriseret adgang og forsøg på adgang til netværk, systemer og data logges og undersøges."*

13.2 Retningslinier

Adgang til Gladsaxe Kommunes IT-ressourcer

Den logiske adgang til Gladsaxe Kommunes data og IT-ressourcer kan kun ske via Gladsaxe Kommunes administrative netværk. Dette netværk er logisk adskilt fra Kommunens øvrige netværk (det offentlig skolenetværk og biblioteksnetværket) og fra andre eksterne net som f.eks. internettet. Kommunikationsadskillelsen mellem netværk skal ske med udgangspunkt i, at intet er tilladt med mindre der specifikt foreligger en begrundet godkendelse af den specifikke kommunikationssammenkobling. IT-afdelingen har det sikkerhedsmæssige ansvar herfor, og IT-chefen foretager godkendelse heraf. IT-chefen kan i øvrigt bemyndige en ekstern og uafhængig part til at foretage en sikkerhedstest af kommunens perimetersikring (firewall, routere m.v.).

Adgangen til det administrative netværk må kun ske via autoriserede pc-arbejdspladser i Kommunen alternativt via autoriserede eksterne tilslutningsforbindelser som eksempelvis låste VPN-opkoblinger fra hjemme-pc'er, dedikerede leverandørforbindelser eller MPLS-forbindelser, der blandt andet anvendes af kommunens politikere. Enhver etablering af forbindelser eksempelvis ved anvendelse af modem eller trådløs teknologi er ikke tilladt, med mindre IT-sikkerhedsudvalget har godkendt dette. Dette gælder også hjemmearbejdspladser.

Gladsaxe Kommune anvender som udgangspunkt ikke trådløst netværk, men IT-sikkerhedsudvalget kan godkende afvigelser i forhold til denne regel. Al trådløs kommunikation skal krypteres behørigt for at undgå forsøg på aflytning og uautoriseret adgang.

Kommunikation af fortrolige eller følsomme personhenførbare data over offentlige netværk mellem Gladsaxe Kommune og driftsleverandører, hjemmearbejdspladser mv. skal krypteres i henhold til dataklassifikationen.

Autentificering

I forbindelse med adgang til Gladsaxe Kommunes administrative netværk, skal enhver brugers tilgang forinden autentificeres med et for brugeren personligt bruger-id og password. Tildeling af bruger-id til en medarbejder foretages af IT-afdelingen. Tildelingen må kun ske efter modtagelse af en elektronisk anmodning, jf. retningslinier for brugeradministration. Brugeren tildeles samtidig et standardpassword. Dette password skal af brugeren udskiftes i forbindelse med første logon på netværket.

Til det privilegerede bruger-id for systemadministrator, der giver adgang til de administrative funktioner på samtlige servere, skal der kun anvendes ét fælles password. Dette password skal nedskrives og opbevares på betryggende vis i et pengeskab, hvortil kun autoriserede

personer har adgang. IT-sikkerhedsudvalget afgør hvem, der er autoriseret til at bryde forseglingen og få adgang til dette password. I dagligdagen skal IT-medarbejdere anvende egne personlige bruger-id'er, der kun er tildelt de nødvendige rettigheder.

Passwordkvalitet

Der er opsat følgende generelle krav til password for netværks- og system-adgang for samtlige brugere:

- password skal minimum være 8 tegn langt,
- password må tidligst kunne udskiftes efter 1 dag og skal senest udskiftes efter 90 dage,
- det anvendte password skal være unikt i forhold til 24 tidligere anvendte password for samme bruger,
- efter 5 på hinanden følgende gange, hvor brugeren ikke har indtastet korrekt password vil adgangen blive blokeret og kan kun låses op systemadministratoren.

Adgang til fagsystemer

Ovennævnte bruger-id og password giver kun adgang til netværket og de basale kontorfunktioner som f.eks. e-post, kalender, fileserver og print. Adgang til fagsystemerne kræver særskilt autorisation via de fagsystemansvarlige. Se retningslinier for brugeradministration. Såvel brugeradministrationsprocedurer og logningsprocedurer skal følge de krav, som dataklassifikationen stiller.

Logning af adgangsforsøg

Ethvert uautoriseret eller fejlagtigt adgangsforsøg til det administrative netværk skal registreres og logges, i såvel netværksserver som perimeterudstyr (firewall, VPN-kontrolenhed mv). Loggen gennemses periodisk af IT-medarbejdere. Det er op til IT-medarbejderen at vurdere, om der har været tale om sikkerhedsbrister eller problemer, som skal registreres og eventuelt behandles af IT-sikkerhedsudvalget.

Anvendelse af mobilt udstyr

Anvendelsen af mobilt udstyr kræver yderligere sikring. Det skal således sikres, at der anvendes specielt password når udstyret tændes (f.eks. power-on-password). Det gælder såvel bærbare pc'er, som de såkaldte PDA'er eller mobiltelefoner, hvorpå det er muligt at lagre fortrolige oplysninger som eksempelvis intern e-post. Det er ikke tilladt at anvende trådløs kommunikation i forbindelse med mobilt udstyr med mindre, der foreligger en specifik godkendelse fra IT-afdelingen.

14 Sikkerhedskopiering

14.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring sikkerhedskopiering:

"Det er væsentligt, at Gladsaxe Kommune til en hver tid kan fremfinde de informationer, som anvendes i forbindelse med kommunens aktiviteter. Derfor skal der etableres procedurer for sikkerhedskopiering og backup, som sikrer, at data og systemer kan retableres i tilfælde af tab af systemer og data.

Det skal sikres, at:

- *data sikkerhedskopieres i overensstemmelse med dataklassifikationen, lovgivningskrav og beredskabsplanlægningen,*
- *der foretages tilstrækkelig verifikation af, at sikkerhedskopier kan genindlæses, når der er behov herfor,*
- *sikkerhedskopier opbevares sikkert og udenfor Gladsaxe Kommunes lokaliteter, således at disse altid kan fremfindes ved igangsættelse af nødplaner eller i forbindelse med andet behov."*

Retningslinier

Med henblik på at minimere konsekvenserne i forbindelse med fejl eller nedbrud, ønsker Gladsaxe Kommune, at der dagligt skal tages backup af alle relevante nye eller ændrede filer på serverne. Der tages ikke backup af filer på pc-arbejdspladser.

Der skal til hver en tid kunne foretages genetablering af data på en given server. Reetablering af en given server skal foregå ved at installere operativsystemet først, dernæst backupklienten, der sørger for genetablering af filerne fra backuppen. Der skal endvidere tages backup at den database, der styrer backupmaskinen, således at denne kan genetableres i tilfælde af integritetsfejl eller lignende.

Det skal sikres, at backupfunktionen ikke kompromitterer sikkerheden af de data, der tages backup af, således at uautoriserede personer kan få adgang til oplysninger via arkiverede filer. Backupbånd skal derfor opbevares i sikrede lokaler og/eller betryggende dataskabe, og eventuelle backupmaskiner skal være beskyttet mod uautoriseret logisk adgang, således at kun autoriserede personer kan genetablere data.

I forbindelse med backup, skal der udarbejdes en log, der dokumenterer hvilke filer, der er blevet arkiveret. Denne log skal gennemgås for fejl og mangler når backupprocessen er tilendebragt, og loggen skal gemmes som dokumentation for arkiveringen.

Det skal som minimum verificeres årligt, at backupfunktionen fungerer efter hensigten. Verifikationen skal gennemføres ved genindlæsning af en eller flere enkelt filer, samt samtlige filer fra udvalgte servere.

Opbevaringen af backupbånd, som ikke er placeret fysisk i backupstationen, skal ske på en sted, der er sikkerhedsmæssigt adskilt fra maskinstuen i aflåst skab/rum eller i bankboks.

Kun særligt autoriserede medarbejdere må have adgang til de fysiske backupbånd, og adgangen må kun ske efter autorisation fra IT-chefen, alternativt en dertil bemyndiget person uden for IT-afdelingen.

15 Beskyttelse mod ondsindet programmel

15.1 Målsætning

IT-sikkerhedspolitikken indeholder følgende mål omkring beskyttelse mod ondsindet programmel:

> *"Ondsindet programmel udgør en stor trussel mod tilgængelighed af systemer og integriteten af data. Der skal derfor på samtlige relevante punkter være etableret en veldefineret og effektiv beskyttelse mod ondsindede programmer.*

Det skal sikres, at:

- *der etableres og vedligeholdes foranstaltninger mod skadelige programmer."*

15.2 Retningslinier

Det er Gladsaxe Kommunes vurdering, at samtlige servere og pc-arbejdspladser med adgang til det administrative netværk skal beskyttes mod ondsindet programmel som eksempelvis virus og orme. Herudover skal al ind og udgående e-post skannes for ondsindet software før videresendelse til den interne eller den eksterne modtager. På serverne skal der foretages en fuld skanning af samtlige filer hver weekend.

På pc-arbejdspladserne skal beskyttelsen etableres, således at potentielt kritiske filer skannes i forbindelse med åbningen på pc'en. Denne beskyttelse må ikke kunne deaktiveres eller afinstalleres af brugerne. Herudover skal der periodisk foretages en fuld skanning af pc-arbejdspladserne for installation af uautoriseret software. Udvælgelsen af hvilke filer, der kan være potentielt kritiske, skal ske på baggrund af anbefalinger fra leverandøren af beskyttelsesværktøjet.

Opdateringen af beskyttelsesværktøjet i relation til virusmønstre mv. skal ske efter behov, dog minimum hver arbejdsdag. Opdateringen skal tilrettelægges, således at det sikres, at denne ikke fejlagtigt ødelægger beskyttelsesfunktionen på servere og pc'er. Dette kan eksempelvis ske ved at sikre, at ingen systemer opdateres før der er foretaget en manuel kontrol af opdateringen i IT-afdelingen.

Beskyttelsesværktøjet skal konfigureres, således at IT-afdelingen informeres i tilfælde af, at der er identificeret en virus eller lignende på en af Gladsaxe Kommunes servere eller pc-arbejdspladser. Potentielle filer og e-post, der identificeres som indeholdende vira mv. skal isoleres, med henblik på en nærmere manuel verifikation, der kun må foretages af medarbejdere fra IT-afdelingen.