STRUER KOMMUNE

IT-SIKKERHEDSPOLITIK STRUER KOMMUNE 2018

STRUER KOMMUNE

INDHOLDSFORTEGNELSE:

Side

KAPITEL 1: IT-SIKKERHEDSPOLITIK – HVORFOR OG HVORDAN

Nærværende revision af Struer Kommunes IT-sikkerhedspolitik er sidste revision i sin nuværende form. Den vil være gældende indtil en ny baseret på ISO27001 er på plads. Arbejdet med dette vil være i etaper, hvor hver etape vil erstatte dele af denne politik. Dette vil blive kommunikeret på komin.struer.dk og direkte til centerledere.
Det afløsende rammeværk vil skulle være færdig og godkendt senest 25. maj 2018, hvor EU's Persondata forordning træder i kraft.

En IT-sikkerhedspolitik for en arbejdsplads som Struer Kommune er en meget vidtforgrenet og kompliceret affære. Kompleksiteten og kravene til sikkerheden bliver ikke mindre af, at der er tale om en offentlig arbejdsplads med høj grad af myndighedsudøvelse.

Hertil kommer organisationens forgrening fra det centrale niveau med Rådhuset i centrum over afdelingerne fysisk placeret andetsteds til de enkelte institutioner. Alle disse enheder er forbundet i et samlet netværk. Disse forhold stiller ligeledes krav til IT-sikkerheden.

Udviklingen indenfor IT-teknologien er voldsom ekspansiv, hvorfor en IT-sikkerhedspolitik selvsagt ikke er statisk, men derimod en stadig fortløbende proces, der tilpasses organisationens aktuelle niveau og muligheder på IT-området.

Det er Byrådets primære hensigt med IT-sikkerheden at optimere borgernes sikkerhed i forhold til anonymitet, diskretion og integritet omkring enhver form for personrelaterede data, der behandles af Struer Kommune, både i sin egenskab af myndighed og serviceudbyder. Gældende lovgivning fastsætter en række normer og standarder herfor.

Samtidig med at IT-sikkerheden skal være i højsædet, har Byrådet også en forpligtigelse til at sikre Struer Kommune som en effektiv, rationel og velfungerende arbejdsplads. Bureaukratiske og omstændelige regler og arbejdsgange skal derfor så vidt muligt elimineres.

Disse betragtninger er således altid medgået i forbindelse med de udstukne regler i IT-sikkerhedspolitikken.

Der må dog aldrig herske tvivl om, at IT-sikkerheden i denne sammenhæng altid har højeste prioritet. Hensynet til økonomiske gevinster og lignende vil altid skulle vige for IT-sikkerheden.

Denne IT-sikkerhedspolitik er gældende for hele Struer Kommune, d.v.s. for alle ansatte som har adgang og autorisation til en pc.

Regelsættet gælder for alt hardware og software, som ejes af Struer Kommune, uanset materiellets fysiske placering.

IT-sikkerhedspolitikken er også gældende for hardware og software, fysisk placeret i institutioner, som Struer Kommune har IT-driftsaftale med. Dette selvom Struer Kommune ikke er indehaver af materiellet.

IT-sikkerhedspolitikken skal også tjene som et informationsredskab til afdelinger/institutioner og medarbejderne. Stort set alle administrative medarbejdere – uanset fysisk placering - kommer daglig i kontakt med IT-systemet og skal dermed også forholde sig til sikkerhedsbestemmelserne. Det er helt afgørende for funktionaliteten, at samtlige medarbejdere respekterer IT-sikkerhedspolitikken. En given forudsætning herfor er, at alle kender og forstår den. Samtlige medarbejdere har derfor en forpligtigelse til som minimum at læse instruks for IT-brugere, som sendes til nye brugere, når de oprettes i systemet.

IT-sikkerhedspolitikken er af overordnet karakter og har derfor et generelt præg. Det betyder, at de sikkerhedsregler, normer og standarder der her angives er minimumsstandarder for IT-sikkerheden. Der er tale om de mindstekrav, der stilles fra såvel politisk som administrativ ledelse. Det kan således i mange tilfælde være hensigtsmæssigt, at der rundt om i afdelinger/institutioner gennemføres skærpede krav til hele eller dele af IT-sikkerheden.

IT-sikkerhedspolitikken er opbygget i 2 hovedafsnit, idet kapitlerne 2-4 omhandler fysisk, teknisk og administrativ sikkerhed. Altså et mere generelt niveau. Kapitlerne 5-6 er mere specifikke, idet der her listes sikkerhedsregler op for brug af elektronisk post og Internettet.

Alle efterfølgende afsnit er gældende, ikke kun for kommende løsninger men også for eksisterende. Det påhviler løsningsejere og IT-sikkerhedsledere at tilse at disse efterkommes.

KAPITEL 2: FYSISK SIKKERHED

Fundamentet for en solid og velfungerende IT-sikkerhed er, at de grundlæggende fysiske rammer er til stede. Uden disse basale ting, er det ikke muligt at udvikle og opretholde en forsvarlig IT-sikkerhed.

I forhold til brugerne af Struer Kommunes netværk, er der nogle få og enkle forhold omkring de fysiske rammer, der skal iagttages og overholdes af hensyn til IT-sikkerheden.

2.1 Definition af fysisk sikkerhed

Med fysisk sikkerhed menes i denne sammenhæng enhver handling eller operation omkring fysiske forhold, af betydning for eller med indvirkning på Struer Kommunes IT-ejendom.

2.2 Målgruppe

Reglerne for IT-sikkerheden nævnt i dette kapitel omfatter enhver person, der i kommunens tjeneste har autoriseret adgang til en pc-arbejdsplads eller en hjemme-pc tilhørende Struer Kommune. Personkredsen er samtidig ansvarlig for, at eventuelle 3. personer overholder de fysiske sikkerhedsregler i forbindelse med brug af nævnte pc'er.

2.3 Fysisk sikkerhed omkring servere

Livsnerven i ethvert netværk er serverne. I Struer Kommune er der fysisk placeret dels en række servere på Rådhuset dels en række eksterne servere.

De eksterne servere er fysisk placeret under vidt forskellige omstændigheder.

For at opnå forsvarlig fysisk sikkerhed omkring serverne, er der for Rådhusets serverrum fastsat følgende sikkerhedskrav:

1. brandsikre og solide indervægge, med rimelig grad af beskyttelse mod indbrud samt solid og brandsikker adgangsdør
2. energen-anlæg (brandbekæmpelsesanlæg, som opsluger ilten i rummet). Anlægget aktiveres automatisk, enten ved røg- eller varmeudvikling
3. adgangskontrol til serverrum i form af elektronisk lås. Den elektroniske lås forsynes med en personlig PIN-kode. Kun medarbejdere med relevant arbejdsmæssigt formål tildeles kort og PIN-kode
4. tyverialarm
5. køleanlæg som er i stand til at fastholde en fuld acceptabel temperatur i serverrummet
6. serverne skal være hævet over gulvhøjde til imødegåelse af eventuel oversvømmelse
7. der er alarm for varme, fugtighed og støj.

De eksterne servere skal principielt sikres som beskrevet ovenfor. I praksis er dette selvsagt ikke muligt, men flest mulige af ovenstående sikkerhedskrav bør nyde fremme.

Som minimum skal eksterne servere opbevares i brandsikre, ventilerede (nedkølede) og aflåselige skabe. Adgangen til skabene skal begrænses til så få personer som muligt, f.eks. institutionslederen, servicelederen og IT-afdelingen. Lokalerne hvor serverne befinder sig, skal desuden i perioder hvor lokalerne ikke er i brug, være forsvarligt aflåsede.

2.4 Kabling (ledningsnet)

Kabling er de ledninger, kabler og stik, der er sat op og monteret i tilknytning til netværket og fjernarbejdspladserne, fysisk placeret ved hver pc-arbejdsplads.

Al kabling (opsætning/nedtagning og ændringer) i forbindelse med kommunens netværk sker via IT-afdelingen. Ansvaret for kablingen hører ligeledes under IT-afdelingen. Opsætning af net-udstyr, må kun foregå med IT-afdelingens mellemkomst.

2.5 Bortskaffelse af data

Brugte og kassable datamedier (CD'er, disketter, mikrofilm mm.) skal indleveres til 'Hotline', som sørger for den endelige bortskaffelse.

Brugte og eventuelt kassable harddiske og USB memory-STIK skal afleveres til 'Hotline', som sørger for den endelige bortskaffelse.

Såfremt en brugt harddisk skal anvendes i anden sammenhæng, skal den ligeledes afleveres til IT-afdelingen, som sørger for sletning af data, eventuel ny-opsætning og videre distribution.

Brugt og kasseret udstyr, der bærer data, bortskaffes af IT-afdelingen. Dette sker ved fysisk destruktion eller afhændelse til ekstern partner med speciale i datasletning af enheder.

Den enkelte afdelingsleder/institutionsleder eller IT-sikkerhedsleder er ansvarlige herfor.

2.6 Mærkning og distribution af udstyr

IT-afdelingen forestår mærkning og registrering af al hardware ejet af Struer Kommune. Alle enheder registreres med serienummer og alle pc-arbejdspladser mærkes med en bestandig mærkning.

Al distribution, installation og opsætning af hardware foregår enten direkte via IT-afdelingen eller med IT-afdelingens mellemkomst.

2.7 Forsikringsforhold

Alt IT-udstyr tilhørende Struer Kommune skal være fuldt og tilstrækkeligt forsikret mod tyveri og hærværk.

2.8 Placering af skærme og printere

Skærme skal for så vidt angår de netværksbaserede pc'ere placeres på en måde, hvor publikum og andre uvedkommende ikke har umiddelbar adgang til at kunne læse tekst og andet på disse. Som led i god borgerservice vil det naturligvis i mange sammenhænge være hensigtsmæssigt at kunne dreje skærmen, så borgeren kan følge med i dispositionerne ved sagsgennemgang o.lign. Dette skal naturligvis fortsat være muligt.

Printere skal som udgangspunkt placeres i afsnit, hvor der ikke er adgang for publikum, så muligheden for at kunne se eller fjerne udskrifter elimineres. I tilfælde hvor dette ikke er fuldt ud muligt, er det den enkelte medarbejder, som forestår udskriften af følsomme eller fortrolige oplysninger, der er ansvarlig for, at udskriften ikke læses eller fjernes af uvedkommende.

Hvis funktionen "sikker udskrift" findes på kopimaskinen anvendes denne.

Alle centrale printere, der understøtter Follow-You-Print opsættes med dette og de, der ikke understøtter en sikker teknologisk løsning udfases.

Når det gælder fjernarbejdspladser kan/skal der ikke opsættes eksplicitte krav til fysisk placering af skærm eller printer. Det vil dog altid være den autoriserede bruger af fjernarbejdspladsen, der er ansvarlig for iagttagelse af gældende sikkerhedskrav.

2.9 TV-overvågning

Med henblik på at forebygge bl.a. vold og chikane mod medarbejderne (præventive formål) samt til brug for eventuel dokumentation og/eller bevismateriale i forbindelse med eventuelle straffelovsovertrædelser, benytter Struer Kommune i visse dele af administrationen TV-overvågning.

Dette afsnit er afløst af ” Retningslinjer for anvendelse og indkøb af TV-overvågning” som findes på komin.struer.dk

2.10 Øvrige forhold

Personalet skal til enhver tid være opmærksomme på sikkerhedsmæssige forhold af betydning for IT-sikkerheden. Her tænkes specielt på forskriftsmæssig låsning af lokaler og kontorer, hvor der opbevares eller findes pc-arbejdspladser.

Det er vigtigt at låse sin PC/terminal når den forlades, også hvis det er et kort ærinde.

Personalet skal desuden være opmærksom på både uhensigtsmæssigheder i eller deciderede overtrædelser af IT-sikkerhedspolitikken. Bliver man opmærksom herpå, skal dette enten påtales direkte til den enkelte bruger, meddeles til nærmeste foresatte, IT-sikkerhedsleder eller til den øverste IT-sikkerhedsansvarlige, alt afhængig af sagens karakter.

KAPITEL 3: TEKNISK SIKKERHED

Dette kapitel omhandler den tekniske del af IT-sikkerheden i Struer Kommune.

Netop tekniske forhold kan for den almindelige bruger fremstå temmelig abstrakte og vanskeligt tilgængelige. I det følgende er fagudtryk og tekniske beskrivelser begrænset til et absolut nødvendigt minimum, idet indhold og præcision i de angivne retningslinier ikke må fortabes.

3.1 Definition af teknisk sikkerhed

Med teknisk sikkerhed menes i denne sammenhæng enhver handling eller operation omkring tekniske forhold, af betydning for eller med indvirkning på Struer Kommunes IT-ejendom.

3.2 Målgruppe

Reglerne for IT-sikkerheden nævnt i dette kapitel omfatter enhver person, der i kommunens tjeneste har autoriseret adgang til en pc-arbejdsplads eller en hjemme-pc tilhørende Struer Kommune. Personkredsen er samtidig ansvarlig for, at eventuelle 3. personer overholder de tekniske sikkerhedsregler i forbindelse med brug af nævnte pc'er.

3.3 Datatransmission

Ved datatransmission forstås her dataoverførsel på det offentlige datanet og privat drevne linier.

Nettet forvaltes af teleselskaberne. Struer Kommune har derfor formelt ingen indflydelse på sikkerhedsniveauet.

3.4 Almindelige tekniske sikkerhedsforskrifter

Al hardware tilsluttet det administrative netværk købes og tilsluttes i samarbejde med IT-afdelingen.

Eksterne institutioner kobles op mod kommunens netværk af IT-afdelingen. Alle kommunens lokationer er bundet sammen af et lejet MPLS-fibernet. Ved eksterne opkoblinger er det IT-afdelingen, der står for og råder over forbindelsen. Dvs. der må ikke tilsluttes andet udstyr til Ændringer af linier sker i samarbejde med IT-afdelingen.

Fagsystemer og andre software løsninger skal i vid udstrækning baseres på standardkomponenter, (f.eks. Office-pakken, SQL database og lignende). Systemer må ikke baseres på proprietære komponenter[1], uden behandling i og med udtrykkelig tilladelse fra Direktionen.

Kommunens netværk skal til enhver tid være baseret på standard protokoller[2]. Valg af protokol foretages af IT-afdelingen. Ved skift af protokol skal ekstern rådgiver give anvisninger på faldgrupper, fejlkilder m.v.

Infrastrukturen skal til enhver tid være tidssvarende og sikres af IT-afdelingen eventuelt via medvirken fra ekstern rådgiver.

3.4.1 Strømsvigt

Elforsyningen kan svigte og blive afbrudt.

[1] Speciel lavet software, som ikke nødvendigvis bygger på standardprodukter. Kan som regel ikke vedligeholdes af andre firmaer ved konkurs eller tvistligheder.
[2] En del af den teknologi som medfører, at maskinerne kan kommunikere med hinanden.

Alle centrale og vitale servere samt andet vitalt aktivt udstyr skal sikres med no-break anlæg, der automatisk sikrer en holdbar kontrolleret nedlukning.

De enkelte pc-arbejdspladser kan ikke anvendes ved strømsvigt. Ikke lagrede data går tabt ved strømsvigt.

3.5 Leverandører, service og reparation

Der skal tegnes servicekontrakt på centrale/vitale servere med de respektive leverandører. Servicekontrakterne dækker 4 timers tilkaldeservice for udbedring af hardwarefejl.

IT-afdelingen er ansvarlig for udarbejdelse og vedligeholdelse af samtlige servicekontrakter.

Servere og pc'er skal, hvis ikke der er vægtige grunde for andet, installeres med standard basissoftware, som kan serviceres af andre eksterne leverandører ved tvistligheder.

For at sikre en hurtig løsning af eventuelle fejl, skal antallet af leverandører begrænses. Ved valg af kommende leverandører skal firmaets størrelse og økonomi afvejes.

I forbindelse med reparation af pc'er og servere, såvel internt på institutionerne som eksternt hos reparatør, iagttager reparatørerne kommunens IT-sikkerhedsregler herunder tavshedspligt.

3.6 Virus og hacking

Alle Struer Kommunes servere er sikret med antivirusprogrammel. Endvidere anvendes ekstern leverandør for skanning af post og spam. Der scannes for alle de vira, som er kendt af programmet på alle relevante filer. Programmet opdateres løbende af IT-afdelingen.

Som udgangspunkt er det umuligt at komme med uddybende retningslinier for virus og virusangreb. Har man som bruger mistanke om, at pc'en har fået virus, skal alle operationer stoppes straks. Undlad at forsøge nedlukning af maskinen eller af enkelte programmer, men kontakt omgående IT-afdelingen.

Samtlige pc'ere, med opkobling på netværket har antivirusprogram installeret.

Brugeren skal mindst én gang dagligt logge sin pc af netværket, idet antivirusprogrammet bliver aktiveret ved login.

Kommunens interne net er beskyttet mod uvedkommende indtrængen af en firewall[3]. Der foretages mindst 4 gange årligt sikkerhedsskanninger af firewall af en uafhængig sikkerhedsrådgiver.

Enhver bruger, der får den mindste mistanke om, at nogen uvedkommende (hackere) forsøger at skaffe sig adgang til Struer Kommunes netværk, har pligt til omgående at underrette den øverste IT-sikkerhedsansvarlige eller IT-afdelingen.

IT-afdelingen varsler om kendte usikre elementer i det omfang det er muligt. Varslingen sker på komin.struer.dk, alle er forpligtet på at udbrede disse varsler til kolleger i nærområdet.

3.7 Lagring af data og sikkerhedskopiering (backup)

Alle kommunens administrative netværksbaserede pc'er har en opsætning, som gør, at data som hovedregel gemmes på server, hvorved også sikkerhedskopiering af data sikres. Data er herved også sikret mod uautoriseret adgang. Den enkelte bruger er forpligtiget til at sikre, at data ikke lagres lokalt (på pc'ens egen harddisk), dels af hensyn til sikring mod datatab, dels til sikring mod uautoriseret adgang. Personrelaterede data skal altid lagres på serveren.

[3] En sikring mellem kommunens net og den øvrige verden. Ind- og udgang, hvor der sorteres på, hvad der må slippe igennem.

IT-afdelingen forestår og er ansvarlig for opsætning og vedligeholdelse af alle backup-rutiner på samtlige servere. Det er IT-afdelingens ansvar at påse, at de daglige backup-kørsler er foretaget korrekt, og i tilfælde af det modsatte foranledige at tingene bliver rettet, så de daglige backup-kørsler foregår så korrekt som muligt. Backup foretages til dedikeret backupserver og replikeres til sekundær server placeret udenfor serverrummet. Løsningen giver en høj sikkerhed for opbevaring af data, idet disse ikke findes på samme lokation som det øvrige it-udstyr.

3.7.1 Håndholdte enheder

Håndholdte enheder tablets og smartphones må ikke tilsluttes netværket på det administrative ben uden CISO'ens godkendelse og IT-afdelingens mellemkomst. Smartphones og tablets udgør en sikkerhedsrisiko, og skal hvis de skal benytte netadgang kobles på et til formålet oprettet trådløst net.

Ved mistanke om misbrug/datalækage vil enheden blive slettet fra central side.

Håndholdte enheder må som udgangspunkt ikke opbevare følsomme eller fortrolige informationer. Disse skal tilgås via en til formålet installeret applikation, der indeholder en særskilt verifikation af brugeren. Løsninger, der indbefatter følsomme og/eller fortrolige oplysninger på håndholdte enheder skal udover digitaliseringsforum også være forelagt styregruppen for IT-sikkerhed.

3.7.2 Synkronisering af post og kalender på eksterne enheder

Post- og kalenderoplysninger kan indeholde følsomme eller fortrolige oplysninger, hvorfor det med henvisning til Dataloven må fremhæves, at disse oplysninger kun synkroniseres til eksterne enheder via sikre løsninger.

Med eksterne enheder menes der såvel håndholdte enheder som mere eller mindre intelligente mobiltelefoner.

Simlås på mobiltelefoner og 4-cifret pin-kode til enhederne kan ikke betragtes som tilstrækkelig sikker.

Synkronisering af post- og kalenderoplysninger kræver, at der er installeret en klient til den sikre løsning. Denne klient kan distribueres via IT-afdelingen. Alle udgifter i den forbindelse afholdes af brugeren. Klienten bliver kun distribueret til de enheder, der er understøttet af IT-afdelingen og ellers ligger indenfor Direktionens retningslinjer for dette.

3.7.3 Fjernarbejdspladser

Ved anvendelse af bærbare pc'er og hjemme-pc'er gælder principielt de samme retningslinier som for Struer Kommunes almindelige IT-arbejdspladser: Den enkelte bruger skal sikre, at der opretholdes en sikkerhed, der er på højde med den sikkerhed, som gælder terminaler og pc'er i kommunens vante rammer. Al behandling af data, der kan klassificeres som følsomt eller fortroligt bør foregå på arbejdspladsen, men i særlige tilfælde kan det forekomme nødvendigt andre steder. I disse tilfælde må det ikke ske i det offentlige rum (tog, lufthavne o.lign.). Arbejdet skal i givet fald ske i diskrette rammer og altid via kommunens VDi-løsning (Citrix).

Udskrivning af følsomt og/eller fortroligt materiale skal ske indenfor kommunens rammer.

3.7.4 Bærbare pc'er.

Ved anvendelse af bærbare pc'er gælder principielt de samme retningslinier som for Struer Kommunes øvrige IT-arbejdspladser. Du skal som bruger således sikre, at der så vidt muligt opretholdes en sikkerhed,

der er på højde med den sikkerhed, som gælder for terminaler tilkoblet netværket. Det ligger udenfor kommunens kompetence at stille krav til indretning af boligen med mere.

Det skal understreges, at uhensigtsmæssig adfærd (jf. 3.7.3) kan resultere i, at hele Struer Kommunes sikkerhed kan blive svækket.

Følgende forhold er således specielt vigtige ved anvendelse af en bærbar pc:

Generelt skal der altid ageres efter almindelig sund fornuft

- pc'en skal altid opbevares forsvarligt. Det vil blandt andet sige, at bærbare pc'er ikke efterlades i køretøjer eller uden opsyn
- der må ikke ændres på pc'ens sikkerhedsindstillinger. Pc'en er forsynet med antivirussoftware, som opdateres løbende ved opkobling til Struer Kommunes netværk
- når pc'en forlades, skal den sikres mod uautoriseret adgang. Log altid af eller aktivér skærmlås som er password-beskyttet
- du skal være opmærksom på, hvilke data du har liggende på pc'en. Opbevar kun data på pc'en, såfremt det er nødvendigt. Anvend altid netværket til opbevaring af data hvis muligt. Opbevaring af følsomme personoplysninger på mobilt udstyr skal som udgangspunkt lagres på servere og tilgås med klientsoftware. Hvis den bærbare pc ikke er koblet til nettet lagres data på en af IT-afdelingen udleveret RAM-STIK der gemmer indhold i krypteret form. Den enkelte bruger er ansvarlig for at kontakte IT-afdelingen for udlevering af RAM-STIK, idet den ved udlevering skal beskyttes med et af brugeren valgt kodeord. Ved først given lejlighed den bærbare pc er på netværket, overføres data fra RAM-STIK til netværket. Brugeren er ansvarlig for korrekt lagring af personfølsomme data
- der må aldrig tilsluttes enheder til netværksudstyret, som ikke er godkendt af IT-afdelingen.

3.7.5 Trådløst netværk

Kommunens bygninger er i vid udstrækning dækket med trådløst netværk. Dette opsættes og styres af IT-afdelingen og kun af IT-afdelingen eller af dem bestilte leverandører.

Tilslutning til trådløst netværk på kommunens adresser sker enten ved hjælp fra IT-afdelingen eller ved at følge den guide, der er tilgængelig på komin.struer.dk

IT-afdelingen følger løbende med i udviklingen af sikre standarder i forbindelse med trådløse netværk og vil agere herefter.

Der må aldrig tilsluttes et trådløst tilslutningspunkt til netværket uden IT-afdelingens godkendelse.

3.8 Registrering af licenser og nye projekter

IT-afdelingen skal have registrering af licenser til alt software, som indehaves af Struer Kommune, og som anvendes på det administrative netværk.

Alle nye softwareløsninger skal projektbeskrives. Disse forelægges IT-afdelingen til udtalelse, og efterfølgende digitaliseringsforum.

KAPITEL 4: ADMINISTRATIV SIKKERHED

Foranstaltninger af administrativ karakter der foretages med henblik på at sikre en forsvarlig, tilstrækkelig og betryggende IT-sikkerhed er meget omfattende. Den administrative sikkerhed omhandler to hovedgrupper

1. selve IT-sikkerhedsorganisationen
2. den almindelige adfærd brugerne udviser i det daglige arbejde med pc'erne.

4.1 Definition af bruger

For at blive oprettet som bruger i Struer Kommunes netværk skal man i forbindelse med ansættelsen og jobfunktionen være pålagt arbejdsopgaver af administrativ karakter, som kun kan udføres via adgang til netværket og dermed en brugerregistrering.

Byrådets medlemmer er undtaget herfra.

Endvidere kan som bruger oprettes personer, for hvem en autorisation er nødvendig, som led i udførelsen af deres hverv i tilknytning til funktioner indenfor Struer Kommunes myndighedsområde.

Oprettelse som bruger sker i henhold til bestemmelserne angivet i afsnit 4.6.

Såfremt der opstår tvivl om relevansen i brugeroprettelsen, kan IT-afdelingen – forinden oprettelsen finder sted – rette henvendelse til den respektive direktør eller øverste IT-sikkerhedsansvarlige afhængig af den konkrete sags karakter.

Direktøren/øverste IT-sikkerhedsansvarlige træffer i så fald afgørelse på forespørgslen, som meddeles IT-afdelingen skriftlig.

4.2 Definition af administrativ sikkerhed

Med administrativ sikkerhed menes i denne sammenhæng enhver handling eller operation omkring administrative forhold, af betydning for eller med indvirkning på Struer Kommunes IT-ejendom.

4.3 Målgruppe

Reglerne for IT-sikkerheden nævnt i dette kapitel omfatter enhver person, der i kommunens tjeneste har autoriseret adgang til en pc-arbejdsplads, en hjemme-pc, en bærbar pc, en håndholdt enhed (PDA) eller en mobiltelefon, der understøtter post og kalender, tilhørende Struer Kommune. Personkredsen er samtidig ansvarlig for, at eventuelle 3. personer overholder de administrative sikkerhedsregler i forbindelse med brug af nævnte pc'er.

4.4 IT-sikkerhedsorganisationen

Borgmesteren varetager formelt den overordnede ledelse og koordination af IT-sikkerheden.

Kommunaldirektøren skal - som den øverste IT-sikkerhedsansvarlige – i samarbejde med styregruppen for IT-sikkerhed forestå IT-sikkerheden, og er herunder ansvarlig for administrationen af de enkelte anmeldelser, som er godkendt af Datatilsynet.

Stedfortræder for øverste IT-sikkerhedsansvarlige (CISO, udpeges blandt styregruppen for IT-sikkerheds medlemmer) varetager opgaverne ved fravær.

Styregruppen for IT-sikkerhed består af kommunens DPO, CISO, digitaliseringskonsulenten med ansvar for IT-strategi, projektleder samt kommunaldirektøren, der er født formand for styregruppen.

DPO''en er en den juridisk kompetente person, der skal sikre at Struer Kommune til enhver tid arbejder for at efterkomme såvel Persondataloven som EU's Persondataforordning. DPO'en har retten og pligten til at intervenere når og hvis, der er tiltag der kan kompromittere borgernes data.
CISO'en udfører det daglige administrative arbejde med styring autorisationskoder, benyttelseskontrol, rettigheder m.v. CISO'en opbygger og vedligeholder strukturer, løsninger og kompetencer, der sætter Struer Kommune i stand til at sikre borgernes data og medarbejdernes integritet.

Digitaliseringskonsulenten sikrer at nye systemer og strategier er i tråd med såvel kommunens strategier på området som det lovgivningsmæssige der fordres i Persondataloven som EU's Persondataforordning.

Projektlederen er organisatorisk tovholder for gruppen, som sikrer fremdrift og kontinuitet i arbejdet.

En komplet organisatorisk fortegnelse over IT-sikkerhedsorganisationen kan ses på intranettet under IT-sikkerhed.

4.4.1 IT-sikkerhedsledere

Den enkelte centerchefer IT-sikkerhedsleder for eget område. Denne uddelegerer ansvaret til afdelings-/team-/institutionsledere der hører under sig.

IT-sikkerhedslederne er overfor den øverste IT-sikkerhedsansvarlige ansvarlig for, at IT-sikkerhedsbestemmelserne indenfor pågældendes afdeling/institution overholdes, herunder de af Datatilsynet godkendte anmeldelser.

IT-sikkerhedsledernes opgaver i forhold til IT-sikkerheden er:

- anmodning om oprettelse/sletning af brugere og autorisationskoder
- gennemgang af brugerstatistikken med henblik på at begrænse antallet af brugere og autorisationskoder
- gennemgang af benyttelseskontrol (kontrol af at systemerne ikke misbruges)
- fysisk sikkerhed, herunder opbevaring af materiale og opsyn med at ingen uvedkommende får adgang til pc'erne, jf. kapitel 2 i IT-sikkerhedspolitikken
- behandling af ind- og uddata (sikre at modtagne oplysninger kun anvendes til det formål, de er indhentet til, og at uddata ikke kommer i forkerte hænder)
- sikre destruktion af materiale, i henhold til reglerne i kapitel 2 og 3
- sikre at reglerne for indsigt følges, herunder overholdelse af Datalovens regler for videregivelse af oplysninger til private og andre offentlige myndigheder
- forestå at nye løsninger i eget områder forelægges IT-styregruppen, og som følge heraf overholder retningslinjer for backup, adgangskontrol, logning, benyttelseskontrol mv.

Souschef eller anden af lederen udpeget medarbejder udfører funktionerne i lederens fravær.

4.5 Administrativ sikkerhed for brugerne - brugernavn og adgangskode

Enhver anvendelse af kommunens IT-anlæg skal ske ved et login bestående af brugernavn og adgangskode.

Enhver bruger af Struer Kommunes netværksbaserede IT-system tildeles et brugernavn. Brugernavnet er entydigt og tildeles af IT-afdelingen.

Den enkelte bruger tildeler sig selv en adgangskode (password). Adgangskoden skal som minimum bestå af 8 tegn (en kombination af bogstaver og tal) og skal udskiftes mindst 4 gange årligt. Tidligere benyttede adgangskoder kan ikke genanvendes. Systemet giver meddelelse, når der skal skiftes adgangskode.

Adgangskoden er strengt personligt, og må under ingen omstændigheder videregives til nogen som helst anden person. Det er ikke tilladt at have papirlapper o. lign. liggende på og i umiddelbar nærhed af skrivebord/arbejdsplads, som muliggør identificering af adgangskoden.

Adgangskoden kan helt undtagelsesvis – i forbindelse med aftestning eller fejlsøgning – udleveres til en for brugeren udtrykkelig kendt medarbejder fra IT-afdelingen. I så fald skal adgangskoden straks skiftes efterfølgende.

Den enkelte bruger er personligt ansvarlig for, at uautoriserede personer ikke kan få adgang til brugerens pc og data.

4.5.1 Administrativ sikkerhed for systemet

Alle servere sikres med password. Liste med alle administrative passwords gemmes i en forseglet kuvert i et brandsikret skab eller på RAM-STIK.

4.6 Tildeling af rettigheder og autorisationer

IT-sikkerhedslederne i de enkelte afdelinger/institutioner er ansvarlig for

- oprettelse/sletning af en ny bruger
- tildeling, ændring eller sletning af den enkelte brugers rettigheder (adgang til programmer, mapper og kataloger i netværket)
- transaktionskoder og profiler til KMD og andre eksterne leverandører.

Tildelingen af rettigheder/autorisationer sker via en blanket til IT-afdelingen med angivelse af hvilke dataområder, programmer og transaktionskoder brugeren skal have adgang til.

- blanketten ligger på komin.struer.dk – IT-sikkerhed - Autorisationsskema
- blanketten skal være IT-afdelingen i hænde senest 10 dage inden ændringerne træder i kraft
- blanketten skal også anvendes, hvis en medarbejder flyttes til en anden funktion
- blanketten underskrives af IT-sikkerhedslederen eller stedfortræderen

Brugerne må i henhold til Dataloven ikke autoriseres til mere end de har behov for.

IT-sikkerhedslederen er ansvarlig for, at tildelingen sker på baggrund af en individuel vurdering, så den enkelte medarbejder kun tildeles de rettigheder/autorisationer, som er nødvendige for at kunne løse de pålagte arbejdsopgaver. Rettigheder/autorisationer må derfor kun gives, når formålet hermed er klart og sagligt, og når anvendelsen sker til et klart defineret formål, der er naturligt og nødvendigt. IT-afdelingen kan ikke vurdere om de bestilte autorisationer er korrekte.

Ved ansøgt afsked eller orlov, udfylder sikkerhedslederen - senest 14 dage før medarbejderen fratræder - ovennævnte blanket (autorisationsskema) og følger ovennævnte procedure. Den enkelte afdeling skal – evt. med IT-afdelingens mellemkomst – og så vidt muligt i samarbejde med den afgående medarbejder sikre sig gennemgang af den afgående medarbejders databibliotek, (hvori ingen dokumenter må være låst med kodeord), postkasse og kalender, inden data slettes. Data slettes uden yderligere varsel ved arbejdstids ophør på fratrædelsesdagen.

Ved uansøgt afsked, bortvisning eller fritstillelse meddeler IT-sikkerhedslederen til IT-afdelingen, at brugerens netværksadgang straks lukkes.

Sletning af adgang til KMD meddeles efterfølgende IT-afdelingen af pågældende centerchef, direktør eller øverste IT-sikkerhedsansvarlige. Førnævnte blanket (autorisationsskema) skal benyttes.

Adgang til brugernes data finder ligeledes om nødvendigt kun sted i forbindelse med længerevarende sygdom (over én uge), medmindre der udtrykkeligt er indhentet personlig tilladelse til adgang til P-drev fra den sygemeldte medarbejder. Adgangen skal konfirmeres af den øverste IT-sikkerhedsansvarlige eller CISO'en og pågældendes fagdirektør.

Efter behov eller på IT-afdelingens foranledning gennemgår IT-sikkerhedslederen i den enkelte afdeling/institution samtlige tildelte rettigheder med henblik på en revision af, om disse fortsat er relevante i forhold til den enkelte brugers behov i opgaveløsningen. Eventuelle korrektioner i tildelingen af rettigheder finder sted i henhold til ovenstående procedure.

Resultatet af gennemgangen sendes til den øverste IT-sikkerhedsansvarlige.

4.8 Brugerstatistik, benyttelseskontrol, logning og sikkerhedsrapport

4.8.1. Brugerstatistik

Efter behov udskriver IT-afdelingen en brugerstatistik over anvendte behandlinger, for hvilke der er foretaget anmeldelser. Statistikken angiver for hver enkelt bruger, hvilke transaktionstyper vedkommende har anvendt eller forsøgt at anvende, samt antallet af gange, det har fundet sted.

IT-afdelingen sender brugerstatistikken til IT-sikkerhedslederne.

IT-sikkerhedslederen gennemgår statistikken med baggrund i:

- at vurdere behovet for de tildelte autorisationer med henblik på eventuel tilbagekaldelse eller ændringer af autorisationerne
- at opdage misbrug, for eksempel et usædvanligt transaktionsbrug
- at undersøge årsagen til forsøg på at anvende skærmbilleder/transaktionsblanketter, som vedkommende ikke er autoriseret til
- at afdække andre former for uregelmæssigheder.

IT-sikkerhedslederne udfylder og sender autorisationsblanketter til IT-afdelingen, hvis gennemgangen har givet anledning til at foretage ændringer i de enkelte autorisationer. IT-sikkerhedslederne holder fagdirektørerne underrettet.

4.8.2 Benyttelseskontrol

Øverste IT-sikkerhedsansvarlige foretager stikprøvevis en kontrol af anvendelsen. Resultatet af denne kontrol bliver forelagt den enkelte bruger, der redegør for brugen af systemet. Redegørelsen returneres til øverste IT-sikkerhedsansvarlige med påtegning af IT-sikkerhedslederen.

4.8.3 Logning

For systemer, som indeholder personlige oplysninger, skal der foretages en logning (sker automatisk) af alle transaktioner. Registreringen (logningen) skal mindst indeholde oplysninger om tidspunkt, pc-operatør, transaktionstype og den/de personer, transaktionen vedrører/de anvendte søgekriterier.

Øverste IT-sikkerhedsansvarlige foretager periodisk og ved mistanke om misbrug, kontrol af log. Resultatet af logningen kan om nødvendigt forelægges den enkelte bruger, der redegør for brugen af systemet.

Statistikker og logninger opbevares i 6 måneder, hvorefter de destrueres. Er materialet udskrevet på papir makuleres disse.

4.9 Behandling af persondata og oprettelse af registre

Som udgangspunkt skal enhver behandling af personoplysninger, der foretages i kommunen, anmeldes til Datatilsynet.

Personoplysninger kan indtil 25. maj 2018 opdeles i nedenstående 3 typer eller niveauer:

Niveau 1: følsomme oplysninger om rent private forhold. F.eks. race, etnisk baggrund, politisk eller religiøs overbevisning, fagforeningsmæssigt tilhørsforhold, helbredsmæssige forhold

Niveau 2: andre følsomme oplysninger - om rent private forhold. F.eks. interne familierelationer, sociale problemer, strafbare forhold. (Niveau 1 og 2 skal ses i sammenhæng)

Niveau 3: almindelige personoplysninger, (ikke følsomme). F.eks. identifikationsoplysninger, økonomiske forhold og kundeforhold. Flere af disse oplysninger kan godt være fortrolige.

Behandling af persondata, der ikke indeholder andre fortrolige oplysninger end almindelige personoplysninger godkendes af IT-sikkerhedslederen. Disse behandlinger skal ikke anmeldes til Datatilsynet.

Første gang behandlingen finder sted, eller når der sker ændringer i indholdet, retter IT-sikkerhedslederen henvendelse til brugeren og vurderer databehandlingens følsomhed.

IT-sikkerhedslederen sørger - om nødvendigt - for den fornødne anmeldelse til Datatilsynet. Anmeldelsen skal forinden forelægges og godkendes af fagdirektøren. Anmeldelsen skal efterfølgende altid forelægges Direktionen og Økonomiudvalget til orientering.

Endelig sørger IT-sikkerhedslederen for, at medarbejdere, som arbejder med personoplysninger, får den fornødne instruktion i relation til Datalovens bestemmelser.

4.9.1 Fælleskommunale registre

Kommunedata og andre dataleverandører opretter og fører fælleskommunale registre for flere kommuner. Oprettelsen af registret og behandlingen godkendes af Datatilsynet. Meddelelse om tilslutning til en fællesanmeldelse underskrives af fagdirektøren i den pågældende forvaltning eller af kommunaldirektøren. Datatilsynets svar forelægges efterfølgende til orientering for Direktionen og Økonomiudvalget.

4.9.2 Indsigt

For at oversigten over registre, borgere kan få indsigt i, altid kan være ajourført, har samtlige afdelinger/institutioner pligt til straks at give styregruppen for IT-sikkerhed v/ digitaliseringskonsulenten besked ved oprettelse/nedlæggelse af samtlige registre, uanset om de er omfattet af Dataloven eller ej.

4.9.3 Databehandleraftaler

IT-sikkerhedslederen har ansvaret for, at de løsninger med følsomme data, der benyttes i dennes område har indgået en databehandleraftale med eksterne leverandører. Skabelon til dette vil kunne findes på komin.struer.dk under IT-sikkerhed. Aftalen sendes i underskrevet stand til styregruppen for IT-sikkerhed /DPO'en. Foreligger der ikke en databehandleraftale er det DPO'ens pligt at stoppe benyttelsen af systemet indtil dette er afklaret.

4.10 Øvrige retningslinjer for den administrative IT-sikkerhed

Enhver pc'er skal – via tastaturet - låses når den forlades, også når fraværet blot er af kort varighed.

KAPITEL 5: ELEKTRONISK POST (E-MAIL)

Håndteringen af elektronisk post og dokumenter benævnes i denne politik som e-mail. Stort set alle medarbejdergrupper, som i dag har med almindelig posthåndtering at gøre, vil også skulle håndtere e-mail og skal derfor iagttage og efterleve de sikkerhedsmæssige krav i tilknytning hertil.

Med indførelsen af elektronisk dokumenthåndtering og digital signatur vil retsvirkningerne af elektroniske dokumenter blive sidestillet med almindelige håndunderskrevne papirdokumenter.

5.1 Definition af e-mail

Med e-mail menes i denne sammenhæng: Ethvert fremsendt/afsendt dokument eller besked i elektronisk form fra eller til en administrativ pc-arbejdsplads tilhørende Struer Kommune.

Det følger i sagens natur, at sikkerhedsniveauerne i håndteringen heraf, vil variere afhængig af dokumentets karakter. F.eks. er der forskel på en almindelig mødeindkaldelse og overførsel af stærkt følsomme personoplysninger.

5.2 Målgruppe

Reglerne for IT-sikkerheden nævnt i dette kapitel omfatter enhver person, der i kommunens tjeneste eller på anden vis har autoriseret adgang til en pc-arbejdsplads eller en hjemme-pc tilhørende Struer Kommune. Personkredsen er samtidig ansvarlig for, at eventuelle 3. personer overholder de sikkerhedsregler der gælder for e-mail i forbindelse med brug af nævnte pc'er.

5.3 Sikker post

Anvendelsen af e-mail giver ikke anledning til juridiske problemer, når der er tale om uformel kommunikation.

Struer Kommune opfylder kravene til E-dag2 om modtagelse og afsendelse af sikker post, Der er etableret en løsning hos ekstern leverandør, der sikrer, at der kan modtages og afsendes signeret og krypteret post. Alle der har en digital signatur kan sende sikker post til adressen sikkerpost@struer.dk. Postkassen tømmes af Sekretariatet, der videresender posten til rette afdeling. E-mails, der indeholder fortrolige oplysninger, skal altid sendes som sikker post, hvilket kræver, at modtageren har en digital signatur.

Intranettet indeholder en adressebog over postadresse, der kan modtage sikker post.

Borgere, der ikke har en e-mail konto, kan sende sikker post fra kommunens hjemmeside.

Se www.struer.dk:

http://671intra2/webtop/webedit/images/common-doc/20050308123343.pdf

En quickvejledning ligger på intranettet.

Struer Kommune har et virksomhedscertifikat, der anvendes til formålet, og som dækker hele kommunen.

I ethvert tvivlstilfælde om gyldigheden, retsvirkningerne eller øvrige lovgivningsmæssige rammer, skal e-mail ikke benyttes.

5.4 Håndtering af modtaget post

Som udgangspunkt skal enhver borger, virksomhed eller anden myndighed kunne rette elektronisk henvendelse til Struer Kommune og følgelig modtage et elektronisk svar.

Behandlingen af modtaget e-post adskiller sig ikke fra modtagelsen af almindelig papirbaseret post, telefax eller telefon.

Ved modtagelse af ikke-sikker post indeholdende fortrolige og følsomme oplysninger er det vigtigt, at den enkelte sagsbehandler gør sig en række sikkerhedsmæssige overvejelser. Her tænkes specielt på sikring af meddelelsens autenticitet, altså om afsenderen også rent faktisk er dén, pågældende giver sig ud for at være. Man skal endvidere være opmærksom på integriteten, dvs. der skal være sikkerhed for, at meddelelsen modtages i uforvansket form. Endelig skal man sikre sig meddelelsens uafviselighed, hvormed menes, at dokumentet rent faktisk er afsendt/modtaget på det afgivne tidspunkt.
Den enkelte sagsbehandler er principielt selv ansvarlig for at nødvendige og passende kontrolforanstaltninger gennemføres. I tvivlstilfælde konsulteres nærmeste foresatte.
Det vil herudover være op til den enkelte afdeling, at udarbejde specifikke retningslinjer omkring sikkerheden i forbindelse med modtagelse af elektronisk post.

E-mail kan ofte have karakter af telefonisk henvendelse, men alle henvendelser af betydning for en sagsbehandling er omfattet af forvaltningslovens regler om notatpligt.

Modtageren af ekstern e-mail – efter den er omdelt til rette sagsbehandler, jf. afsnit 5.3. – har ansvaret for, at den bliver journaliseret. E-mail indgår som enhver anden akt i sagen og kan således gøres til genstand efter reglerne om aktindsigt i henhold til offentlighedslovens og forvaltningslovens bestemmelser.

Arkiverings- og kassationsregler er identiske med reglerne for almindelige papirbaserede dokumenter.

Modtaget e-mail føres på kommunens postlister efter samme regler som papirbaseret post.

Når modtagne e-mail kan betragtes som skriftlig kommunikation (altså kan sidestilles med papirbrev eller telefax), skal kommunen (sagsbehandleren) kvittere for modtagelsen og evt. anføre sagsbehandlingstid, svarfrister m.v. i henhold til informationshåndbogens retningslinjer. Dette uanset om afsenderen eventuelt benytter funktionen om automatisk kvittering.

Kvitteringen kan sendes elektronisk.

5.5 Håndtering af afsendt post

Ved enhver borgerrelateret afsendelse eller besvarelse af e-mail, angives kommunenavn, adresse, afdeling/institution, afdelingspostkasse, telefonnummer og navn på sagsbehandler. De angivne retningslinjer i informationshåndbogen skal følges. Ikke alle e-mail systemer er lige pålidelige når det gælder medsendelse eller gengivelse af identifikation. Det er derfor vigtigt, præcist at anføre afsender- og modtageradresse fuldt ud i selve meddelelsen.

Enhver korrespondance indeholdende følsomme eller personlige oplysninger, herunder f.eks. personnumre, skal sendes som sikker post.

Behandlingen af afsendt post i elektronisk form adskiller sig ikke fra afsendelsen af almindelig papirbaseret post, telefax eller telefon. De angivne regler om notatpligt, aktindsigt, journalisering, arkivering og kassation i afsnit 5.4. følges.

5.6 Postkasser

Al officiel elektronisk korrespondance til Struer Kommune stiles som udgangspunkt enten til kommunens officielle e-mailadresse struer@struer.dk, til sikkerpost@struer.dk eller til afdelings- og institutionspostkasserne. Kommunens officielle postkasser administreres af Sekretariatet.

Enhver borger, virksomhed eller anden myndighed, som via e-mail ønsker at rette henvendelse til Struer Kommune, skal således som udgangspunkt benytte en af disse postkasser. Det vil også være adresserne på disse postkasser, der fremgår af alt informationsmateriale om kommunen - telefonbøger, vejviser, brevpapir, officielle skrivelser m.v. En komplet oversigt over afdelings- og institutionspostkasser ligger på Struer Kommunes hjemmeside.

Medarbejdernes private postkasser offentliggøres ikke overfor borgere, virksomheder eller andre myndigheder. Der henvises i stedet til de officielle adresser.

Postkasserne skal som minimum tømmes én gang dagligt, og den modtagne post distribueres til de respektive sagsbehandlere, som herefter er ansvarlige for det videre forløb i henhold til afsnit 5.3.

De enkelte afdelinger fastsætter selv nærmere retningslinjer herfor.

Den enkelte medarbejder må benytte sin private postkasse, som led i det daglige arbejde i forbindelse med udsendelse og modtagelse af meddelelser/dokumenter. Undtaget herfra vil være borgerrelateret e-post, som skal afsendes fra afdelingspostkassen. Man skal endvidere være opmærksom på, at meddelelser og dokumenter, som indgår i kollektiv sagsbehandling, (f.eks. sager til politisk behandling), ikke gemmes i den private postkasse, idet der hermed kan opstå problemer i forbindelse med ikke planlagt fravær, jf. nedenfor.

I forbindelse med planlagt fravær (ferie eller afspadsering) udover én arbejdsdag, skal den enkelte medarbejder sikre, at e-mail, som tilgår den private postkasse, omadresseres til en kollega(er) eller afdelingspostkassen. Der kan også indgås aftale med kollega om adgang til den private postkasse. Medarbejderen skal endvidere altid sørge for tilkobling af ”ikke til stede assistenten” i forbindelse med planlagt fravær udover én arbejdsdag.

I forbindelse med ikke planlagt fravær udover én arbejdsdag, har medarbejderens nærmeste foresatte, med hjælp fra systemadministrator, ret til at skaffe sig adgang til den private postkasse, såfremt det måtte formodes, at meddelelser af interesse for kommunen er tilgået den private postkasse. I sådanne tilfælde skal åbning/læsning af privat post så vidt mulig undgås.

Forinden der tages skridt til åbning af privat postkasse, skal medarbejderen så vidt muligt orienteres. Er dette ikke muligt skal IT-afdelingen have skriftlig anmodning herom fra den respektive fagdirektør eller fra kommunaldirektøren.

Åbning af privat postkasse vil også kunne finde sted under planlagt fravær. I så fald finder ovennævnte procedure ligeledes anvendelse

Ved uansøgt afsked finder reglerne i IT-sikkerhedspolitikkens afsnit 4.6. anvendelse.

IT-afdelingen sørger for oprettelse/nedlæggelse samt tildeling af rettigheder til samtlige afdelings- og institutionspostkasser.

Den enkelte afdelings- og institutionsleder er ansvarlig for, at IT-afdelingen orienteres om hvilke ansatte, der skal have sende- og modtageret m.v. til postkasserne. Det er i særdeleshed vigtigt, at IT-afdelingen ligeledes straks orienteres når en medarbejder fratræder.

5.7 Private e-mails

Det er tilladt at afsende og modtage private e-mails. Hver medarbejder med adgang til en administrativ pc-arbejdsplads har sin egen e-mailadresse. Struer Kommune anser medarbejdernes egne e-mailadresser og tilhørende postkasser som værende helt private. Ingen andre har som udgangspunkt adgang hertil. Det påhviler den enkelte medarbejder at åbne sin post mindst én gang dagligt, og for så vidt angår arbejdsrelateret post, at agere i henhold hertil, jfr. afsnit. 5.6.

Medarbejderne kan under særlige omstændigheder risikere, at meddelelserne læses af nærmeste foresatte og systemadministratoren, jf. forholdene nævnt i afsnit 5.6.

5.8. Sikkerhedskontroller

Struer Kommune foretager ikke løbende og rutinemæssige sikkerhedskontroller af medarbejdernes brug af e-mail. Opmærksomheden henledes dog på, at der opbevares log og at al e-mail sendt som sikker post registreres automatisk hos ekstern leverandør. I tilfælde af mistanke om misbrug, kan loggen tages i anvendelse.

5.9 Sikkerhed mod virus og hacking

Der var normalt ingen virusrisiko ved modtagelse af e-mails uden vedhæftede dokumenter. Virusrisikoen eksisterer først når vedhæftede dokumenter eller programfiler åbnes. Man skulle derfor være varsom når vedhæftede dokumenter med ukendte ikoner og programfiler modtages fra ukendte afsendere. I dag er såvel e-mail som SMS den største risikofaktor. De, der vil forårsage skade er blevet meget sofistikerede og benytter mange forskellige metoder i forskellige kombinationer. Det stiller store krav til modtageren om, at være sikker på at det er validt indhold. Ved den mindste tvivl kontaktes hotline!

Det er i øvrigt ikke muligt at komme med fyldestgørende sikkerhedsforskrifter vedrørende virus og hacking. Der henvises til IT-afdelingens løbende anvisninger, som enhver bruger af systemet er forpligtiget til at følge.

IT-afdelingen følger konstant udviklingen og tilstræber kontinuerligt at opstille nye og tidssvarende værn mod såvel virus som hacking.

KAPITEL 6: INTERNETTET

Internettet er et stadigt mere anvendt værktøj i opgaveløsningen. Internettet er unikt når det gælder hurtig informationssøgning og formidling, ligesom mediet rummer fine muligheder for kompetenceudvikling. Mange informationer fra ministerier, styrelser m.v. samt indberetninger af diverse oplysninger er allerede i dag kun mulige via Internettet. Samtidig er borgerbetjening via kommunens Internetside blevet et stadig vigtigere element for at give en bedre borgerservice.

6.1 Definition vedr. brug af Internettet

Med brug af Internettet menes enhver bevægelse på Internettet, foretaget af en person ansat ved Struer Kommune med adgang til en pc-arbejdsplads (inkl. fjernarbejdspladser) tilhørende Struer Kommune. Personer med autorisation til brug af en pc-arbejdsplads tilhørende Struer Kommune er samtidig ansvarlig for eventuelle 3. personers brug af Internettet på den pågældende pc. Sidstnævnte gælder også for fjernarbejdspladser.

6.3 Oplysningernes validitet4

Som antydet ovenfor er informationsmængden på Internettet nærmest uudtømmelig. Informationernes validitet kan derfor være meget svingende. Normalt har informationer hentet fra officielle myndigheders hjemmesider en meget høj validitet, mens informationer fra andre hjemmesider kan være mere usikre.

I det omfang informationerne hentet fra Internettet indgår i den almindelige sagsbehandling og dermed danner grundlag for en forvaltningsafgørelse, er det vigtigt at have ovennævnte betragtninger in mente. Igen skal de sædvanlige sikkerhedsmæssige overvejelser vedr. autenticitet, integritet, fortrolighed og uafviselighed iagttages, jf. kap. 5. Normalt vil kun oplysninger, der stammer fra andre offentlige myndigheders Internetsider, blive anvendt i sagsbehandling og lagt til grund for afgørelser.

Den enkelte sagsbehandler er ansvarlig for at nødvendige og passende kontrolforanstaltninger gennemføres. I tvivlstilfælde konsulteres nærmeste foresatte.

6.4 Personalets brug af Internettet

I forbindelse med sikkerheden omkring personalets brug af Internet, er det nødvendigt at sondre mellem to brugergrupper. Dels gruppen, der betjener sig af de netværksbaserede pc'ere og dels medarbejdere med adgang til en fjernarbejdsplads, herunder byrådsmedlemmer. Årsagen hertil er teknisk bestemt, idet fjernarbejdspladserne opererer med en åben platform, mens de netværksbaserede pc'ere som hovedregel arbejder ud fra en lukket platform, (restriktiv opsætning). Sidstnævnte nødvendiggør af hensyn til netværkssikkerheden en lidt mere restriktiv sikkerhedspolitik.

6.4.1 Netværksbaserede pc'ere

Internettet er som udgangspunkt at betragte som et arbejdsværktøj, der anvendes til opgaveløsning af ansatte ved Struer Kommune med autorisation hertil.

Privat brug af Internet i arbejdstiden skal begrænses til et absolut minimum.

Udenfor arbejdstiden er det tilladt at benytte kommunens Internet til private formål.

Aktiviteter som kræver installation af software er ikke tilladt.

[4] Nøjagtighed, retsgyldighed, gyldighed, pålidelighed.

Uanset om der er tale om brug i arbejdsmæssig eller privat sammenhæng, er det ikke tilladt at benytte Struer Kommunes udstyr, programmel eller netværk til at sende, søge efter, downloade eller opbevare filer indeholdende musik, video og obskønt materiale.

Endelig er det ikke tilladt ved benyttelse af udstyret at krænke andres ophavsret eller overtræde anden lovgivning.

Der eksisterer altid en vis virusrisiko, også ved almindelig trafik på eller brug af Internettet. Virusrisikoen eksisterer specielt, når man begynder at downloade filer m.v. Man skal derfor være yderst påpasselig når man downloader filer, specielt fra ukendte udbydere.

Det er ikke tilladt at downloade eller distribuere software. Såfremt det viser sig, at downloading af software er nødvendig af arbejdsmæssige årsager, skal dette altid foregå i samarbejde med IT-afdelingen.

Al installation af software og drivere skal ske i samarbejde med IT-afdelingen.

Det er i øvrigt ikke muligt at komme med fyldestgørende sikkerhedsforskrifter vedrørende virus og hacking. Der henvises til IT-afdelingens løbende anvisninger, som enhver bruger af systemet er forpligtiget til at følge.

6.4.2 Fjernarbejdspladser

Brug af IT-løsninger henover åbne datalinjer skal ske via kommunens VDi-løsning som beskrevet i pkt. 3.7.3

6.5 GENERELT OM SIKKERHED OG SIKKERHEDSKONTROLLER

IT-afdelingen er ansvarlig for administrationen og vedligeholdelsen af sikkerheden i kommunens Internet-forbindelse.

Internettet er et åbent netværk med de risici for hacking m.v. dette indebærer. Dette forhold skal tages i betragtning når man søger eller videregiver informationer via Internettet. Specielt i forbindelse med videregivelse af informationer skal der ske en afvejning af disses følsomhed og fortrolighed vægtet op imod Internettets almene sikkerhedsniveau.

Struer Kommune foretager løbende og rutinemæssige sikkerhedskontroller af medarbejdernes brug af Internet. Al færden af arbejdspladsen på Internettet bliver logget. Logningen indgår i såvel proaktive som reaktive sikkerhedstiltag.

Adgangen til logdata er stærkt begrænset til teamet der forestår drift af IT-sikkerhedsløsninger.

KAPITEL 7 IT-SIKKERHEDSHÆNDELSER

IT-sikkerhedshændelser er et begreb, som har fået fornyet og stort fokus i forbindelse med introduktionen af EU-parlamentets arbejde med forordning for sikring af borgernes persondata. Persondataforordningen giver alle organisationen private såvel som offentlige i medlemslandene 72 timer til at reagere korrekt på en hændelse, der ligger indenfor forordningens virkefelt.

7.1 Definition af IT-sikkerhedshændelser

IT-sikkerhedshændelser er mange mulige scenarier. Det vil typisk være en mail med følsomme og/eller fortrolige oplysninger, som enten sendes ukrypteret eller sendes til en eller flere uvedkommende parter. Desuden kan nævnes sagsakter hjemmeside der identificerer en person; udtalelser til pressen af følsom eller personlig karakter der kan identificere en person; deling af følsomme eller fortrolige oplysninger om en person med uvedkommende part; aktivering af virus/malware; utilsigtet sletning af data; adgang til sager i ESDH, som ikke er en del af en aktuel sagsbehandling...

7.2 Håndtering af IT-sikkerhedshændelser

Alle IT-sikkerhedshændelser skal registreres og vurderes. Hændelserne skal scores efter om det er tilsigtet eller utilsigtet, om det er brud på IT-sikkerhedspolitikken eller Persondataloven/EU's Persondataforordning, om det skal afføde disciplinære handlinger.

Hændelser vil forekomme, derfor er det vigtigt at alle parter reagerer hensigtsmæssigt på disse. Den ansatte, der kommer til at forårsage en hændelse som vedkommende bliver opmærksom på laver en registrering selv og indberetter den til IT-sikkerhedslederen.

Ikke alle hændelser vil komme til overfladen af sig selv, de kan også komme frem ved stikprøvekontroller, indberetning fra andre eller som følge af en klage. I de tilfælde er det IT-sikkerhedslederen der udreder hændelsen.

Endelig kan hændelser komme op ved centrale kontroller og/eller alarmer, der genereres pga. mønstre der matcher uheldig adfærd.

I tilfælde af grelle IT-sikkerhedshændelser vil det afstedkomme automatisk deaktivering af brugerens adgang til IT-systemerne. Udredning af hændelserne vil i nogle tilfælde føre til indledning af om der skal foretages yderligt disciplinært og/eller i forhold til den(e) forudrettede.

KAPITEL 8 AWARENESS (FORSTÅELSE OG OPMÆRKSOMHED)

Awareness er ligeledes et fokusområde og et udtalt krav fra EU. Awareness skal sikre at alle klædes bedst muligt på til at overholde såvel love og forordninger som interne politikker og retningslinjer.

Alle ansatte, der benytter Struer Kommunes IT-systemer eller behandler følsomme og/eller fortrolige oplysninger på vegne af Struer Kommune er forpligtet på at holde sig ajour med disse. Struer Kommune sikrer dette bl.a. ved at sikre tilgængeligheden til såvel politikker og vejledninger som love og forordninger. Interne politikker og vejledninger er at finde på komin.struer.dk og dér vil der også være links til gældende love og forordninger for området.

8.1 Links til forordninger, love eksterne og interne forskrifter

EU's forordning her

Håndbog om europæisk databeskyttelseslovgivning her

Persondataloven her

Retningslinjer for anvendelse og indkøb af TV-overvågning her

Versioner:
Godkendt af Sammenlægningsudvalget, den 5. december 2006 (Version 1)

Godkendt af direktionen, den xx. august 2017