Morsø Kommune

It-sikkerhedspolitik

MORSØ KOMMUNE

Indholdsfortegnelse

1. Introduktion til it-sikkerhedspolitikken

1.1. Baggrund

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

Kommunen vil som et naturligt led i den generelle udbygning af den tekniske it- anvendelse samle og præcisere eksisterende it-sikkerhedsmæssige retningslinjer, som er gældende for it-brugere i hele Morsø Kommune. Denne it-sikkerhedspolitik skal med andre ord ses som et it-opslagsværk.

Målgruppen for IT-sikkerhedspolitikken er primært revisionen og IT-afdelingens medarbejdere. Der vil på et lidt senere tidspunkt bliver udarbejdet en pixi-udgave, som er målrettet de forhold medarbejdere og ledere skal forholde sig til i forbindelse med IT-sikkerhed.

1.2. Formål

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

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

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

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

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

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

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

1.3. Gyldighed og omfang

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

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

2. Organisation og ansvar

2.1. Generelt

Rollerne og deres medfølgende ansvar, som nævnes i it-sikkerhedspolitikken, er kun beskrevet i forhold til it-sikkerheden i Morsø Kommune. Det betyder at yderligere ansvar tildelt disse roller, er beskrevet andet steds.

2.2. Kommunalbestyrelsen og direktionen

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

Kommunalbestyrelsen har delegeret ansvaret for den daglige ledelse og kontrol af it-sikkerheden til kommunaldirektøren. Kommunaldirektøren skal i samarbejde med It- sikkerhedsudvalget eller ved uddelegering til samme eller It afdelingen præcisere it-sikkerhedsniveauet samt sikre overholdelse af it-sikkerhedsreglerne i kommunen. IT sikkerhedsniveauet er defineret ved hjælp at beskrivelse af anvendt sikkerhedsprogrammel, samt procedurer.

2.3. It-sikkerhedsudvalget

It-sikkerhedsudvalget består af chefen for Direktionssekretariatet, leder af IT-Afdelingen, 1 servicechef og en medarbejder fra It-afdelingen med kendskab til it-sikkerheden.

Arbejdet i It-sikkerhedsudvalget sikrer, at it-sikkerhedspolitikken implementeres effektivt i Morsø Kommune. Organisationen i Morsø Kommune skal sikre, at it- sikkerhedsniveauet altid er i overensstemmelse med it-sikkerhedspolitikken. En medarbejder fra It-afdelingen etablerer og vedligeholder kontroller og procedurer til at overvåge, hvor effektivt it-sikkerheden er implementeret i kommunen. It-sikkerhedsudvalget rapporterer, når det er påkrævet, om det faktiske it-sikkerhedsniveau i kommunen til kommunaldirektøren og kommunalbestyrelse.

It-afdelingen vejleder og rådgiver systemejere om aspekter vedrørende lovgivning og anmeldelser af databehandlinger på baggrund af it-registre til datatilsynet og sikrer samtidig, at eventuelle ændringer i relevante love videreformidles til systemejerne. Det er systemejerne som skal indberette personfølsomme oplysninger til datatilsynet.

It-afdelingen er med til at vurdere de sikkerhedsmæssige og evt. kommunikative aspekter i forbindelse med it-investeringer, ændringer i den anvendte teknologi eller andre forhold, som har indflydelse på it-sikkerheden i kommunen.

2.4. Afdelingsleder IT

Afdelingsleder i IT har ansvaret for:

- Den tekniske it-sikkerhed, herunder netværkssikkerhed, virusbeskyttelse, driftsstabilitet mv.
- Den administrative sikkerhed, herunder brugeradministration, dataklassifikation, systemejerskab mv.
- at netværket er korrekt dokumenteret samt at driften og udviklingen af det enkelte netværk sker i overensstemmelse med de vedtagne procedurer, sikkerhedsforskrifter og kontroller. Afdelingslederen i IT- afdelingen er desuden ansvarlig for at rapportere fejl og afvigelser til It-sikkerhedsudvalget.

2.5. Servicechefer

Servicecheferne er ansvarlige for:

- opgaverne i centre + institutioner udføres efter de gældende regler og instrukser
- medvirke til dokumentation af behovet for it-sikkerhed inden for egen organisation
- sikre medarbejdernes kendskab til gældende regler og instrukser samt føre tilsyn med at regler og instrukser overholdes
- samarbejde med It-sikkerhedsudvalget og afdelingslederen i IT-afdelingen

2.6. Systemejere

Cheferne udpeges som systemejere og har systemejerskabet for it-systemerne i deres område og derved det nævnte ansvar for dokumentation og vedligeholdelse. Systemejeren er desuden ansvarlig for:

- at data i systemet er korrekt klassificerede, og at systemet overholder kravene til denne klassifikation (jf. afsnit 4),
- at brugerne har det nødvendige kendskab til systemets funktionsmåde,
- at der sker anmeldelse af systemet til It-afdelingen, samt om nødvendigt til Datatilsynet, hvis systemet håndterer følsomme 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,
- udarbejdelse af forslag til hensigtsmæssig organisering af brugerprofiler og tildeling af rettigheder med udgangspunkt i en klassifikation af data,
- at Morsø 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,
- at sikre at logningsniveauet er i overensstemmelse med lovgivningen, at rapportere fejl og afvigelser til lederen af IT-afdelingen.
- at oversigter med kontaktpersoner på de enkelte it-systemer udarbejdes og vedligeholdes.
- At årligt vurdere brugeres adgange til systemerne.

2.7. Afdelings/Institutionsledere

Afdelingsleder/Institutionsleder er relationen mellem dennes afdeling/institution og It-afdelingen.

Som leder er man ansvarlig for, at nye medarbejdere bliver oprettet på Morsø Kommunes netværk med de rettigheder som er nødvendige for deres jobfunktion. Og ligeledes at nedlægge medarbejdernes it-profiler hvis de forlader Morsø Kommune eller ændre dem hvis der sker ændringer i deres jobfunktioner. På intranettet findes en blanket som anvendes i forbindelse med oprettelse af nye brugere, som lederen udfylder og afleverer til IT-afdelingen med henblik på tildeling af adgange til relevante systemer.

2.8. It-vejledere

It-vejlederen er relationen mellem vedkommendes skole og It-afdelingen. Som it-vejleder er man ansvarlig for, at nye medarbejdere og elever bliver oprettet på skolenetværket med de rettigheder som er nødvendige for deres jobfunktion. Og ligeledes at nedlægge medarbejdernes it-profiler hvis de forlader skolen eller ændre dem hvis der sker ændringer i deres jobfunktioner.

3. Medarbejdersikkerhed

3.1. Generelt

IT afdelingen har udstukket nogle retningslinjer for at sikre at Morsø Kommunes It-ressourcer ikke udsættes for risici i forbindelse med brugen af disse. Retningslinjerne at med til at sikre at medarbejdernes færden både logisk (på pc-arbejdspladserne) såvel som fysisk (fysiske behandling af IT-udstyret) sker i henhold til retningslinjerne.

3.2. Før ansættelse

Medarbejdere i Morsø Kommune bliver før ansættelse oprettet som bruger på Morsø Kommunes it-ressourcer på foranledning af en leder fra det område, medarbejderen skal starte i. Lederen henviser til pixiudgaven af IT-sikkerhedspolitikken, som findes på intranettet.

3.3. Under ansættelse

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

Det er kommunens politik, at eventuelle overtrædelser af gældende it- sikkerhedspolitik bør håndteres af den daglige leder, for eksempel i form af kontakt til de involverede medarbejdere med henblik på en nærmere afdækning af hændelsesforløb, baggrund og karakteren af overtrædelsen. I alvorlige eller gentagelsestilfælde kan sagen bringes op i direktionen. Overtrædelse af it- sikkerhedspolitikken kan få ansættelsesmæssige konsekvenser.

Brugere på Morsø Kommunes it-netværk skal du derfor være specielt opmærksom på følgende:

- Det skal understreges, at dit brugernavn og din kode er personlig, og derfor ikke må deles med andre.

- Forlader du pc´en, skal du huske at låse den (tryk **Ctrl**, **Alt**, **Del** og **Enter** for at låse), så uvedkommende ikke kan få adgang til dine data. Det samme gør sig gældende ved hjemmearbejde.

- Vær opmærksom på hvem der har adgang/udsyn til din skærm når du behandler personfølsomme data, ligesom du også skal være opmærksom på at udskrifter med personfølsomme data ikke bør ligge offentligt tilgængeligt.

- Pc´en er et arbejdsredskab, og skal derfor primært bruges til fagligt relevante ting. Vær opmærksom på hvad du foretager dig, når du er logget på Morsø Kommunes netværk, da du repræsenterer Morsø Kommune og dennes værdier.

- Er du i tvivl om en handling er tilladt eller udgør en sikkerhedsrisiko, skal du henvende dig til din superbruger eller til It-afdelingens ServiceDesk for vejledning. Husk at slukke din pc og skærm, når du går hjem.

- Endelig forventer Morsø Kommune, at den enkelte medarbejder reagerer aktivt på eventuelle it-sikkerhedsmæssige problemer eller fejl, og at medarbejderen i givet fald videregiver sine observationer til en superbruger eller It-afdelingen.

3.4. Fratrædelse

Ved fratrædelse skal lederen i det enkelte områder gøre It-afdelingen opmærksom, så det sikres at den tidligere medarbejders adgange til Morsø Kommune it-ressourcer fjernes helt. Ydermere skal forvaltningen/institutionen sørge for, at få tilbageleveret alle de it-ressourcer den pågældende medarbejder har haft til rådighed under ansættelsen. På intranettet findes en blanket som anvendes i forbindelse med fratrædelse.

4. Styring af it-aktiver

4.1. Generelt

It-afdelingen følger en strategi for styring af it-aktiver, som sikrer at der er kontrol over it-aktiver fra de registreres i Morsø Kommune til de kasseres.

IT-afdelingen står for løbende vedligeholdelse og udskiftning af it-aktiver i Morsø Kommune finansieret af en anlægsbevilling. Udskiftning sker kun i forbindelse med enheder, som ifølge IT-afdelingens planlægning står til udskiftning.

Morsø Kommunes it-aktiver vurderes alle i IT-afdelingens change-proces inden implementering, så det sikres at it-netværket ikke belastes af uautoriseret og ukompatibelt hardware eller software. Al indkøb af enten hardware eller software som skal bruges på Morsø Kommunes it-netværk, skal gå igennem IT-afdelingens ServiceDesk i en sag. Det er ikke tilladt at benytte udstyr købt uden IT-afdelingens samtykke på Morsø Kommunes it-netværk ligesom der heller ikke ydes support af dette udstyr. Rent undtagelsesvist kan det lade sig gøre at blive koblet på kommunes netværk med privat udstyr. Dette kræver dog særskilt godkendelse af afdelingslederen i IT-afdelingen.

4.2. Klassifikation af it-aktiver

Klassifikationen stiller krav til håndteringen og opbevaringen af de pågældende data. Eksempelvis sikres det ved introduktion af et nyt system og tilhørende hardware, at sikkerheden i systemet er i stand til at beskytte de data, som systemet anvender i overensstemmelse med data-sikkerhedsklassifikationen.

Dataklassificeringsniveauer
Dataklassifikationen er opdelt i følgende kategorier:

- Offentlige data – data, som kan offentliggøres til befolkningen på f.eks. kommunens hjemmeside, og som den enkelte borger uden videre kan begære indsigt i.
- Ikke offentligt tilgængelige data – data, som er af en sådan beskaffenhed, at den enkelte borger ikke kan få indsigt i disse data. Eksempler på sådanne data er informationer om opbygningen af sikkerhed i kommunens administration, konfiguration af firewalls mv.
- Fortrolige oplysninger - oplysninger omfattet af persondatalovens § 6.
- Følsomme oplysninger – oplysninger omfattet af persondatalovens § 7 og 8.

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

	Fortrolige oplysninger	**Følsomme oplysninger**
Autorisation	Systemejeren skal autorisere alle brugeres adgang til data. Rettigheder gennemgås årligt.	Systemejer skal autorisere brugeres adgang til data samt deres rettigheder til at læse, opdatere og slette data. Rettigheder og adgange gennemgås hvert halve år.
Adgangsforhold	Systemet skal adgangsbegrænses med bruger-ID og password.	Systemet skal adgangsbegrænses med bruger-ID og password.
Datakommunikation	Kommunikation af fortrolige oplysninger over offentlige net skal krypteres ved "Send sikkert"-funktionen i Outlook, KMD SAG EDH, Doc2mail så de sendes til brugerens "Digital post"	Kommunikation af fortrolige oplysninger over offentlige net skal krypteres ved "Send sikkert"-funktionen i Outlook, KMD SAG EDH, Doc2mail så de sendes til brugerens "Digital post"
Logning af adgang	Mislykkede adgangsforsøg logges og registreringerne herom gennemgås periodisk. Gentagne mislykkede forsøg skal medføre lukning	Mislykkede adgangsforsøg logges og registreringerne herom gennemgås periodisk. Gentagne mislykkede forsøg skal medføre lukning
Logning af anvendelse	Alle anvendelser af data vedrørende enkeltpersoner logges og gemmes i ½ og ved særlige behov op til 5 år (gælder ikke dokumenter under udarbejdelse). Loggen skal indeholde tidspunkt, bruger, anvendelse og personen, som anvendelsen vedrører.	Alle anvendelser af data vedrørende enkeltpersoner logges og gemmes i ½ og ved særlige behov op til 5 år (gælder ikke dokumenter under udarbejdelse). Loggen skal indeholde tidspunkt, bruger, anvendelse og personen, som anvendelsen vedrører.
Opbevaring	Dataene skal opbevares således at kun autoriserede brugere har adgang til dem. Alle data skal være omfattet af backup. Fysiske papirer skal opbevares i aflåste og brandsikre skabe.	Dataene skal opbevares således at kun autoriserede brugere har adgang til dem. Alle data skal være omfattet af backup. Fysiske papirer skal opbevares i aflåste og brandsikre skabe.
Anmeldelse	Behandling af personoplysninger skal anmeldes til Datatilsynet.	Behandling af personoplysninger skal anmeldes til Datatilsynet.

4.3. Registrering af it-aktiver

IT-afdelingen registrerer alle nye it-aktiver indenfor rækkevidden af strategien i et asset management system, regneark eller lignende.

Denne registrering indeholder bl.a. klassificering, ejerskab og et unikt id. Ejeren af et it-aktiv er ansvarlig for brugen af det.

4.4. Tyverisikring

Mange udsatte enheder på skoler er markeret med tyverisikring. Institutionen/skolen vurderer sammen med IT afdelingen om der er behov for tyverisikring. Ved tyverisikring, bortfalder mulighedes for brug af visse garanti og reparationsformer.

4.5. Licenser

IT-afdelingen har ansvaret for at antallet af licenser på alle standard installerede pc-arbejdspladser er registreret. Programmer som afviger fra standard installationer og som kræver licens, skal afholdes af forvaltningen/institutionen selv. IT-Afdelingen sørger kun for indkøb af software og licenser.

4.6. Vedligeholdelse af it-aktiver

Alle it-aktiver er underlagt løbende vedligeholdelse for at sikre driftsikkerhed på it- netværket og integriteten i dataene.

4.7. Kassation af it-aktiver

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

5. Risikovurdering og håndtering

5.1. Generelt

Risikovurdering og håndtering sikrer i samspil med ITIL lignende processer og Change management, at alle risici i Morsø Kommune behandles hensigtsmæssigt, så deres påvirkning på Morsø Kommunes digitaliseringsstrategi mindskes mest muligt.

5.2. Risikovurdering

IT-afdelingen identificerer, vurderer og dokumenterer risici på baggrund af inputs fra organisationen, ekstern revision og andre eksterne faktorer.

5.3. Risikohåndtering

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

6. Fysisk sikkerhed

6.1. Generelt

Fysisk sikkerhed fokuserer på sikkerheden omkring de fysiske lokationer og beskyttelse af it-aktiver hos Morsø Kommune.

6.2. Zoner

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

Beredskabet, har adgang til en nøgle, som ligger i en elektronisk spærret boks, som kun betroede beredskabsmedarbejdere har adgang til. Systemet logger hvis denne boks bliver åbnet, og af hvem.

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

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

Alarmer viderestilles til IT-afdelingens medarbejdere, beredskabsafdelingen og G4S, alt efter karakter af den aktuelle alarm.

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

Den fysiske adgang til denne zone er aflåst, således at kun autoriserede personer har adgang til zonen. Grundlæggende er det kun medarbejdere fra IT-afdelingen og pedelfunktionen der har adgang til denne zone. Teknikere og håndværkere fra huskendte firmaer, der har et godkendt behov, kan inden for normal arbejdstid eller i forbindelse med krisesituationer få uledsaget fysisk adgang til it-lager og -værksted.

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

Zone 3 (Kontorer i IT-afdelingen, krydsfelter, serverrum på eksterne lokationer mv.)
Den fysiske adgang til denne zone er sikret med specifikke låse, som kun autoriserede personer har nøgler til. På rådhuset vil det være medarbejdere fra It-afdelingen, navngivne teknikere og håndværkere fra huskendte firmaer med et godkendt behov, der har adgang til denne zone.

På andre lokaliteter vil adgangen være baseret på autorisation fra den lokale leder i samråd med IT-afdelingen.

7. Logisk adgangsstyring

7.1. Generelt

Den logiske adgang til Morsø Kommunes data og it-ressourcer kan kun ske via Morsø Kommunes administrative it-netværk. Dette netværk er adskilt fra de øvrige netværk, der anvendes i kommunen, herunder det offentlige skolenetværk, biblioteksnetværket og andre eksterne net, som f.eks. Internettet.

Logisk adgangsstyring i Morsø Kommune er organiseret således, at en stor del af ansvaret er placeret i de enkelte centre. IT-afdelingen står for at være den koordinerende faktor i forbindelse med adgangsstyring, daglige retningslinjer for og vejledning i brug af de logiske it ressourcer.

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

7.2. Brugeradministration

Standard brugeradministration
Der er udpeget ansvarlige i IT-afdelingen, som sørger for oprettelser, ændringer og sletninger af brugerprofiler på it-netværket. Derudover er ansvaret for anmodninger i forbindelse med brugeradministration lagt ud til superbrugerne i de enkelte centre. I forbindelse med ansættelse, ændring eller sletning af en medarbejder sender en brugerinstruktør et skema med brugeradministrationsønsket til IT-afdelingen. Skemaet findes på Intranettet under IT → skemaer, udfyldes og sendes via e-mail IT-afdelingen. På baggrund heraf sørger IT-afdelingen for det ønskede adgangsniveau. Skemaet journaliseres I KMD SAG EDH så den kan bruges til dokumentation.

IT-afdelingen sørger i forbindelse med fratrædelser for, at den fratrådte persons netværksdrev kan gøres tilgængelig i op til 6 måneder efter fratrædelsen. Herefter slettes netværksdrevet. E-postbokse slettes umiddelbart. I tilfælde af at man skal have adgang til en tidligere medarbejders e-postboks, kan dette ske i op til 60 dage efter sletning af brugerprofilen.

Dette må dog kun finde sted efter, at der er indhentet en autorisation fra den implicerede chef fra området eller ansvarshavende direktør. Det samme gør sig gældende i forbindelse med en fratrådt medarbejders netværksdrev. I begge tilfælde bør det undlades at mapper benævnt private undersøges uden samtykke fra ejeren af e-postkassen medmindre der er tale om tilfælde med mistanke om kriminelle forhold.

Administrator brugere
Udvalgte medarbejdere samt brugere fra IT-afdelingen er autoriseret til at have administratorrettigheder. Disse personer er dokumenteret og autoriseret af lederen af IT-afdelingen.

Adgang til fagsystemer
Adgang til fagsystemerne kræver særskilt autorisation. IT afdelingen sørger for at oprette adgang til fagsystemerne, på foranledning af en superbruger eller en leder.

Fagsystemer tilhørende decentrale enheder bliver brugeradgang administreret af lederen af på den pågældende enhed

Elektronisk udveksling af data
Det er som udgangspunkt ikke tilladt at anvende uautoriserede og usikre datamedier til udveksling af data eller arkivering af data, herunder særligt data med fortrolige eller følsomme oplysninger. Usikre datamedier er eksempelvis ukrypterede, cd-rommer eller DVD'er.

Data med fortrolige og følsomme oplysninger
Kommunikation af data med fortrolige eller følsomme oplysninger over offentlige netværk mellem Morsø Kommune og driftsleverandører, hjemmearbejdspladser mv. skal krypteres i henhold til data-klassifikationen. Som bruger skal man derfor altid sende data via "Send sikkert"-funktionen i Outlook, hvis dataene skal sendes udenfor Morsø Kommunes it-netværk. Anvendelsen af "send sikkert" funktionen i Outlook kan læses i vejledning på intranettet. Ydermere er det ikke tilladt at opbevare fortrolige eller følsomme data på eksterne medier såsom f.eks. usb-nøgler og cd-rom.

7.3. Adgangskode politik

Tildeling af adgangskode
Som Morsø Kommunes brugeradministrationsproceduren foreskriver, kan en medarbejder kun få en adgangskode/blive oprettet på Morsø Kommunes it-ressourcer på foranledning af en leder.

Brug af adgangskoder
Alle nye medarbejdere skal ændre adgangskode ved første logon, og adgangskode politikken i Morsø Kommune kræver at en adgangskode:

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

Dit ansvar som bruger
Som bruger på Morsø Kommunes it-netværk skal du være opmærksom på følgende:

- Din adgangskode er personlig og må derfor ikke deles med andre eller skrives ned således, at den risikerer at blive offentliggjort.
- Du skal skifte din adgangskode, hvis du er det mindste i tvivl om den er blevet kompromitteret.
- Din adgangskode bliver spærret hvis du taster den forkert 5 gange. ServiceDesk kan låse op så du kan forsøge den samme adgangskode igen, men har du glemt din adgangskode og skal have den nulstillet, skal du henvende dig til din superbruger eller IT-afdelingen alt efter hvilken type kode det drejer sig om.

7.4. Anvendelse af mobilt udstyr

Anvendelsen af mobilt udstyr på it-netværket er underlagt yderligere sikring, idet der anvendes et specielt password, når udstyret tændes (f.eks. power-on-password). Det gælder såvel bærbare pc'er med standard Morsø Kommune installation, PDA'er eller mobiltelefoner, hvorpå det er muligt at lagre fortrolige oplysninger som eksempelvis intern e-post. IT-afdelingen er behjælpelig med opsætningen af power-on passwords.

Disse enheder kan ligeledes være underlagt kryptering. Bærbare pc´ere med
Mobility installation kræver ikke power-on-password, da sikkerheden opstår i det øjeblik brugeren vil have adgang til XEN-Desktop løsningen (VDI).

7.5. Adgang til Morsø Kommunes it-ressourcer

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

8. Driftsafviklingsprocedurer

8.1. Generelt

IT-afdelingen har ansvaret for driften af kommunens netværk og it-udstyr, og herunder de sikkerhedsmæssige aspekter i denne forbindelse. Procedurer for driftsafvikling er dokumenteret og godkendt. Målsætningen er, at levere en god service og kvalitet over for brugerne af it-ressourcerne og dermed de borgere og virksomheder, som er afhængige af kommunens service. IT-afdelingen arbejder derfor på, at driftsafviklingen foretages på en stabil, kvalificeret og sikker måde således, at fortroligheden, pålideligheden, integriteten og tilgængeligheden af it-ressourcerne og deres data sikres. Det indebærer, at it-ressourcerne som udgangspunkt er tilgængelige for medarbejderne, borgerne og virksomhederne døgnet rundt, dog vil eventuelle driftsnedbrud primært blive udbedret inden for normal arbejdstid. Længerevarende nedlukninger af it-ressourcer så vidt muligt uden for normal arbejdstid. Ved kritiske systemnedbrud træder it-beredskabsplanen i kraft.

Varetagelse af opgaverne i forbindelse med driften kan eventuelt helt eller delvist overdrages til en ekstern leverandør i henhold til retningslinjer for samarbejdspartnere og leverandører.

8.2. Backup og genetablering

For, til enhver tid, at kunne fremfinde informationer i forbindelse med kommunens aktiviteter, sørger IT-afdelingen for, at der tages dagligt backup. Backup foretages i overensstemmelse med dataklassifikation, forretnings-/lovgivningskrav og it-beredskabsplanlægningen i kommunen.

For at sikre at data kan genindlæses ved nedbrud, foretager IT-afdelingen verifikation af sikkerhedskopier ved hjælp af løbende genetableringstests.

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

Alle data gemt i mere end en version

- Databasefiler - 2 versioner 30 dage tilbage
- Brugerfiler - 5 versioner 90 dage tilbage, slettede filer 2 versioner 180 dage tilbage
- System- og applikationsfiler i øvrigt - 2 versioner 90 dage tilbage, slettede filer 2 versioner 180 dage tilbage

For at backupfunktionen ikke kompromitterer sikkerheden af de data, der tages backup af, er der opsat adgangskontrol således at uautoriserede personer ikke kan få adgang til oplysninger via arkiverede filer. Backup er outsourcet til 3. Part og filer krypteres ved transmittering over offentlige net.

Alle i IT-afdelingen er autoriseret til at reetablere filer. Al reetablering foregår struktureret i ITIL lignede processerne, der bl.a. sikrer, at man ved genindlæsning af filer ikke ændrer på ejer og adgangsrettigheder, således at sikkerheden omkring de berørte informationer kompromitteres.

I forbindelse med backup og reetablering udarbejdes en log, der dokumenterer, hvilke filer der er blevet arkiveret og reetableret. Loggen gennemgås og gemmes som dokumentation for arkiveringen og reetableringen.

Sletning af data fra backuparkivet foregår via change processen (change processen bestemmer blandt andet hvor lang tid vi skal gemme data, hvad vi skal gemme osv.)

8.3. Driftsafvikling og planlægning

IT-afdelingen sikrer, at samtlige ikke trivielle manuelle og automatiske rutiner inklusiv automatiske jobs er dokumenteret, og at de afvikles som planlagt. Væsentligheden afgøres af systemejeren. Dette er formaliseret ved procedurer og instrukser for driftsafvikling og planlægning. Endvidere tilstræbes det, at der er en klar funktionsadskillelse for at forhindre tilsigtede fejl og misbrug.

8.4. Logning i forbindelse med it-ressourcer

IT-afdelingen sikrer, at der foretages overvågning af centrale servere, netværkskomponenter og andet it-udstyr, herunder den fysiske sikring af zone 3 - serverrummet. Dette bliver foretaget via en automatisk overvågning, hvor det sikres, at der følges op på eventuelle fejl, problemer eller sikkerhedsmæssige hændelser, der måtte kræve nærmere undersøgelse eller opfølgning. Hændelserne registreres automatisk i ServiceDesk i IT-afdelingen.

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

9. Netværket

9.1. Generelt

Morsø Kommunes it-netværk er segmenteret med henblik på at sikre de transmitterede data, samt den underliggende infrastruktur.

9.2. Segmentering

Kommunikationsadskillelsen mellem netværk sker 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 afdelingslederen i IT-afdelingen foretager godkendelse heraf. I tvivlstilfælde er det It- sikkerhedsudvalget, som tager stilling til de sikkerhedsmæssige aspekter i netværksopsætningen.

9.3. Netværksudstyr på hjemmearbejdspladser og eksterne institutioner

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

9.4. Trådløse netværk

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

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

10. Problemhåndtering

10.1. Generelt

IT-afdelingen vurderer alle indkomne fejl efter ITIL lignende principperne incident og problem håndtering, hvilket sikrer, at alle it relaterede fejl umiddelbart korrigeres efter graden af alvor i fejlen. Med problem håndtering sikres det at årsagen til gentagne fejl identificeres, afhjælpes permanent og dokumenteres.

10.2. Risikovurdering

IT-afdelingen arbejder i det daglige efter ITIL lignende principper, som sørger for at alle fejlmeldinger bliver vurderet efter effekt og konsekvens for forretningen Morsø Kommune. Alle fejl går over ServiceDesk, IT-afdelingens Single Point of Contact – SPOC – og primære indgangsvinkel for alle brugere på it-netværket. På skriverbordet findes et ikon som giver adgang IT-afdelingens helpdesk. Via af helpdesk kan brugere indberette fejl til ServiceDesk. ServiceDesk vurderer, kategoriserer og tildeler alle indkomne sager alt efter behov.

10.3. Risikohåndtering

Opståede it relaterede problemer bliver håndteret i ServiceDesk (i ITIL lignende processerne) på en måde, så det pågældende problem umiddelbart korrigeres alt efter graden af alvor. Alvorlige it problemer bliver endvidere genstand for en analyse med henblik på at korrigere eventuelle årsager og uhensigtsmæssigheder og vil dermed bidrage til den løbende forbedring af it-sikkerheden. Alvorlige problemer kan for eksempel være uautoriseret netværksadgangsforsøg eller gentagne servernedbrud.

ServiceDesks brug af ITIL lignende processer sikrer:

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

10.4. Fejlhåndtering

IT-afdelingen sikrer med fejlhåndtering, at medarbejderne hurtigst muligt kommer videre med deres arbejde når fejl (incidents) opstår. Det foregår på den måde, at alle indkomne incidents til It-afdelingen vurderes af

ServiceDesk, hvor vagten forsøger at finde en løsning eller som minimum en midlertidig løsning, en såkaldt workaround, på det pågældende incident således, at medarbejderen kan fortsætte sit arbejde med mindst mulig gene.

10.5. Problemhåndtering

Problem håndtering tager over, når den samme type incident er opstået gentagne gange og det ikke længere er tids- eller sikkerhedsmæssigt forsvarligt at fortsætte med en workaround. Incidentet ophæves derfor til status af et problem.

Problemer analyseres med henblik på at korrigere eventuelle årsager og uhensigtsmæssigheder og dermed bidrage til den løbende forbedring af it-sikkerheden og afviklingen af den daglige drift.

11. Beskyttelse mod ondsindet programmel

11.1. Generelt

Ondsindet programmel udgør en stor trussel mod tilgængelighed af systemer samt fortrolighed og integritet af data. IT-afdelingen har derfor på samtlige områder etableret en veldefineret og effektiv beskyttelse mod ondsindede programmer.

11.2. Antivirus

Samtlige servere i Morsø Kommune og pc-arbejdspladser med adgang til Morsø Kommunes administrative netværk er derfor beskyttet mod ondsindet programmel, som eksempelvis virus og orme.

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

Opdateringen af beskyttelsesværktøjet i relation til virusmønstre mv. sker via central server i kommunen. Servere og pc-arbejdspladser opdateres automatisk når det er påkrævet.

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

11.3. Antispam

E-mailserveren er der ud over beskyttet med et Antispam filter, som scanner alt ind- og udgående post for sikkerhedstrusler, og skadelig kode. Alt indgående post spam kontrolleres, og sorteres fra centralt, for ikke at forstyrre brugerne med spampost.

Spamfiltrene fungerer på den måde, at de kontrollerer afsender serverens "reputation", for et se om det er en server som er noteret på et af de offentlige spærringslister. Hvis en server er spærret på en af disse lister, er det postserverens ejers ansvar at få serverens problem identificeret og fjernet fra listen igen.

Spam filteret, gennemgår også selve e-mailen for mønstre og kendte ord og sammensætninger ud fra forskellige algoritmer og kendte systemer. Spam, som serveren er i tvivl om, kommer på en liste, som sendes hverdag til IT-afdelingen, som gennemlæses, og eventuelle forkerte spærringer, åbnes og sendes til brugeren.

Store mailservere, så som Hotmail og yahoo, kan være spærret i perioder, pga. netop deres servere tit bruges til spamudsendelser. Udbyderne holder selv øje med disse spærringer, og udfører de nødvendige rettelser, og får deres server slettet igen spærringslisterne.

Derfor er det meget vigtig at man ved e-mail kommunikation, gør afsenderne opmærksomme på at Morsø Kommune først har modtaget e-mailen, når afsenderen har fået en bekræftelse på modtagelsen fra Morsø Kommune. Dette skal f.eks. ske ved jobansøgninger, her skal huskes det at skrive i annoncens tekst, at modtagelsen først er gyldig når ansøgeren har fået en bekræftelse på modtagelsen fra Morsø Kommune.

12. Anskaffelse og vedligeholdelse af fagsystemer

12.1. Generelt

Fagsystemerne indgår som et væsentligt element i det daglige arbejde i Morsø Kommune. Det er derfor af vital betydning, at nyanskaffelser og opdateringer af disse lever fuldt op til den eksisterende kvalitets- og sikkerhedsstandard, herunder krav til systemdokumentation. Da Morsø Kommune samtidig har valgt ikke at påtage sig udvikling af eget programmel i nævneværdigt omfang, anvender kommunen udelukkende pålidelige og kompetente leverandører.

12.2. Fagsystemer

IT-afdelingen skal involveres i enhver anskaffelse af nye fagsystemer. Involveringen skal ske på et så tidligt tidspunkt, at IT-afdelingens krav og råd kan inddrages i vurderingen og forhandlingen om det nye system.

IT-afdelingen sørger ved indkøb af et nyt fagsystem for, at foretage en teknisk gennemgang af installationen af fagsystemet for at påse, at dette lever op til det ønskede sikkerhedsniveau i Kommunen, og at det ikke kompromitterer andre systemers sikkerhed. Dette omfatter en gennemgang af den tekniske platform og integration med øvrige systemer, samt en gennemgang af adgangskontrolmekanismerne.

Systemejerne er hovedansvarlige for deres fagsystemer. I forbindelse med nyanskaffelse af et fagsystem er systemejeren også ansvarlig for, at:

- funktionaliteten i fagsystemet stemmer overens med de krav, som medarbejderne stiller,
- fagsystemet indeholder tilstrækkelige indbyggede kontroller i forbindelse med bearbejdning af data, herunder sporbarhed,
- fagsystemet overholder krav vedrørende lovgivning og dataklassifikation,
- fagsystemet inden underskrift af aftale anmeldes til IT-afdelingen,
- fagsystemet anmeldes af systemejeren, hvis nødvendig, til Datatilsynet
- fagsystemet ligger på en platform, som er godkendt af IT-afdelingen.

Selve installationen af serversoftware og klienter foretages af leverandøren selv i samarbejde med IT-afdelingen. IT-afdelingen leverer den nødvendige platform bestående af hardware, operativsystem og eventuelle databasesystemer, som leverandøren kan installere på. Hvis et givet fagsystem kræver, at der foretages ændringer i standardkonfigurationen, gennemgås, godkendes og foretages dette af IT-afdelingen. Ny anskaffelser af hardware eller software i forbindelse med afviklingen af fagsystemet, skal medregnes I anskaffelses- eller oprettelsespris. Dette kan også gøre sig gældende ved større opdateringer af et fagsystem, hvor kravene til hard- og software ændres betydelig.

13. Ændringshåndtering (Change Management)

13.1. Generelt

It-afdelingen håndterer alle ændringer i Change management. Change management-processen sørger for at alle konfigurationsændringer planlægges, kvalitetssikres og godkendes inden implementering. Derved sikres det, at ændringer i konfigurationen af hardware og software skaber færrest mulige konsekvenser for sikkerheden på it-netværket.

13.2. Standard ændringer

IT-afdelingen har i forbindelse med udviklingen af Change management- processen defineret en rækkevidde for standard ændringer, som kan godkendes og implementeres uden testforløb og risikovurderinger. Standard ændringer er bl.a. tilføjelse af allerede godkendte pc´ere på it-netværket, automatisk opdatering af antivirus på pc-arbejdspladserne eller brugeradministration.

13.3. Fagsystemer

Systemejerne har ansvaret for opgradering/patching mv. af fagsystemerne (se afsnit2 "Organisation og ansvar"). Alle ændringer til fagsystemerne foretages så vidt muligt af leverandøren. Dette skal af systemejerne 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 IT-afdelingen, som hvis der var tale om et nyt system.

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

13.4. Implementeringer på netværk

I forbindelse med implementering af servere, pc'er, netværkskomponenter, printer eller andet it-udstyr på netværket vurderer It-afdelingen risiciene i forbindelse hermed igennem Change management-processen.

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

Alle større konfigurationsændringer og ændringer af væsentlige systemer planlægges ud fra Change management-processen, således at væsentlige fejl undgås. Der bliver om nødvendigt foretaget pilottests i produktionsmiljøet hos udvalgte medarbejdere, testet af IT-afdelingen inden implementering. Disse tests medfører tekniske reviews af ændringerne samt afprøvning på testmaskiner.

IT-afdelingen har valgt ikke at følge alle opdateringsanbefalinger fra Microsoft og øvrige leverandører. It-afdelingen gennemgår alle opdateringsanbefalinger med henblik på en kritisk vurdering af bl.a. væsentlighed for brugeren, før de implementeres.

13.5. Varsling

IT-afdelingen skal sørge for, at alle berørte brugere varsles i god tid inden implementering af større eller væsentlige konfigurationsændringer, som kan påvirke brugernes anvendelse af it. Samtidig informeres superbrugere og ledere om eventuelle konsekvenser ved ændringen.

14. Samarbejdspartnere og leverandører

14.1. Generelt

Det er hensigten, at It-afdelingen på sigt får indgået service level agreements (SLA) med alle interne såvel som eksterne samarbejdspartnere og leverandører med hjælp fra ITIL lignende process Service Level Management således, at forventninger bliver afstemt og samarbejdet derved understøtter Morsø Kommune på den bedst mulige måde. Der bliver primært indgået service level agreements på hardware mv.

14.2. Før samarbejde

Før et samarbejde indgås og kontrakten underskrives, aftales it-leverancen så den er målbar og kan vurderes ud fra forventningerne afstemt i service level agreements'ne. Således sikres det, at forventninger til samarbejdet er formaliseret inden start. Derudover sikrer It-afdelingen, at samarbejdet er sikkerhedsmæssigt forsvarligt ved hjælp af bl.a. tro og love erklæringer og i forhold til Morsø Kommunes retningslinjer i indeværende politik.

14.3. Under samarbejde

IT-afdelingen foretager sammen med samarbejdspartneren eller leverandøren løbende vurderinger af samarbejdet og indholdet i service level agreements'ne, så forventninger løbende bliver afstemt.

14.4. Afslutning af samarbejde

Ved afslutning af samarbejdet sørger IT-afdelingen for arkivering af relevant dokumentation samt nedlæggelse af brugerprofiler og forbindelser til Morsø Kommunes it-netværk.

15. Beredskabsplanlægning

15.1. Generelt

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

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