Informationssikkerhedshåndbog Bilag

Version 2.1

Team Strategi og Digitalisering

Næstved Kommune
Sagsbehandler: Ilinn
Tlf. 5588 5300

www.naestved.dk

19. april 2018

Retningslinjer for brugere

1. It-brugere
2. E-mail
3. Internet
4. Fjernadgang
5. Bærbare og mobile enheder
6. Digital signatur
7. Trådløst netværk
8. Sletning af data
9. Beskyttelse af persondata

Retningslinjer for systemejere og it-medarbejdere

A. Systemejere
B. Autorisation
C. Logning
D. It-beredskab
E. It-medarbejdere
F. Firewall
G. Backup
H. Virusberedskab
I. Fysisk sikkerhed
J. Eksterne leverandører
K. Eksterne brugere

Bilag 1	Retningslinjer for it-brugere

Er du medarbejder i Næstved Kommune, og anvender du en af kommunens it-arbejdspladser, så skal du have kendskab til disse retningslinjer for it-brugere.

Retningslinjerne er en del af kommunens informationssikkerhedspolitik, som består af de overordnede informationssikkerhedspolitiske regler, informationssikkerhedshåndbogen samt en række bilag, der indeholder retningslinjer på konkrete områder.

Retningslinjerne er tilgængelige i Næstved Kommunes informationssikkerhedsportal Secure ISMS, som du kan få adgang til via kommunens intranet. Retningslinjerne bliver årligt ajourført af kommunens Informationssikkerhedskoordinator. Det er derfor nødvendigt, at du løbende sikre dig, at du kender til de seneste retningslinjer.

Center-, afdelings- og virksomhedsledelserne har ansvaret for, at alle it-brugere er orienteret om retningslinjer for it-brugere, som de er beskrevet her og i de øvrige retningslinjer.

> Som it-bruger i Næstved Kommune er det dit personlige ansvar at overholde retningslinjerne. Gå derfor jævnligt ind på informationssikkerhedsportalen for at holde dig ajour.

1 Den enkeltes ansvar som it-bruger

Som it-bruger i Næstved Kommune er du personligt ansvarlig for det, der foregår på din pc og de systemer og drev, som denne giver adgang til. Det gælder fra du logger dig på, til du logger dig af igen. Hvis pc'en overlades til en kollega, skal du først logge dig af, hvorefter kollegaen kan logge sig på. Du må ikke overlade din pc til en person, som ikke er oprettet som bruger i Næstved Kommunes it-miljø.

> Det er som it-bruger i Næstved Kommune ikke tilladt at anvende eller tilgå systemer eller sager som brugeren ikke er autoriseret til at tilgå. Overtrædelse af dette medfører en tjenestelig påtale og ultimativt kan det medføre en afskedigelse fra jobbet i Næstved Kommune

2 Adgangskode - sikkerhed

Når du som it-bruger får adgang til kommunens netværk og fælles it-systemer, får du samtidig adgang til en række ressourcer og oplysninger, som kan være fortrolige og strengt personlige. Derfor får alle it-brugere et personligt brugernavn, der er udstyret med en hemmelig og personlig adgangskode.

> Du må ikke videregive din personlige adgangskode til andre, heller ikke dine nærmeste kolleger eller it-medarbejdere.
>
> Når du får en ny adgangskode, skal den altid ændres første gang du logger på.

2.1 Gode adgangskoder

For at adgangskoden skal have den ønskede effekt er det nødvendigt, at definere en række minimumskrav til opbygning og hvor tit, den skal ændres.

> En god adgangskode er en bogstav- og talkombination, som er nem at huske, men til gengæld er svær at gætte for andre.

Adgangskoder til kommunens netværk og systemer, skal opfylde følgende betingelser:

- Skal som minimum bestå af 8 karakterer.
- Må ikke indeholde dit eget navn
- Skal indeholde mindst 3 typer af følgende karakterer: Store bogstaver, små bogstaver, tal eller specielle karakterer.
- Må ikke være en adgangskode der har været brugt de sidste 10 gange
- Adgangskoden til netværk og systemer gælder i 90 dage. Du vil automatisk blive bedt om at ændre.

I dagligdagen skal du undgå, at andre får kendskab til din personlige adgangskode, da det ved et misbrug, er dig som indehavere, der bliver gjort ansvarlig. Undlad derfor at skrive adgangskoden ned på huskesedler. Forsøg på uautoriseret adgang til systemerne, bliver registreret af systemerne.

Hvis du får kendskab til forsøg på uautoriseret adgang til kommunens it-systemer eller andre uregelmæssigheder, har du pligt til at meddele dette til din nærmeste leder, der efterfølgende er forpligtiget til at informere Informationssikkerhedskoordinatoren hurtigst muligt

Overtrædelse af Informationssikkerhedspolitikken og relaterede bilag, kan medføre sanktioner, alt efter omstændighederne.

3 Pauseskærm med adgangskode

Den almindelige udvikling samt lovgivning om effektivisering af den offentlige forvaltning, betyder en stadig større digitalisering af kommunens forretningsgange. Det har medført, at en række sikkerhedshandlinger og kontroller, som tidligere blev foretaget manuelt, nu finder sted som en integreret del af den elektroniske databehandling.

> Det har derfor stor betydning, at brugerrettigheder til de enkelte systemer, ikke bliver tilgængelige for andre end den oprettede bruger.

For at sikre dig imod uautoriseret adgang til systemer og data, skal pc'er og skærmbilleder gøres utilgængelige for uvedkommende ved anvendelse af pauseskærm med adgangskode.

3.1 Aktivering af pauseskærm

For at undgå, at uautoriserede brugere opnår adgang til data- og systemadgange, skal du enten lukke programmer og logge dig af alle systemer og netværk, eller du skal aktivere en pauseskærm med adgangskode. Uanset at der eventuelt er kolleger til stede, som du arbejder sammen med - og har tillid til - skal du lukke af for adgang til data og programmer, også selvom pc'en kun forlades i en kort periode. Dette vil både beskytte dig selv og dine kollegaer.

> Du kan aktivere pauseskærmen ved at taste *Windows Start tasten* + *L*. Når du igen skal anvende pc'en, skal du igen taste *Ctrl Alt Delete* og derefter indtaste din adgangskode til netværket.

Aktivering af pauseskærm med adgangskode skal sikre Næstved Kommune - og dig som it-bruger - mod, at andre får adgang til personlige rettigheder og data.

Husk altid at slukke pc og skærm helt ved arbejdstids ophør. Ud over at spare på strømmen vil du også sikre dig at eventuelle opdateringer automatisk bliver installeret på din pc. Lad altid eventuelle opdateringer køre færdig.

4 Beskyttelse imod virus

Et virusangreb kan medføre store konsekvenser. En destruktiv virus kan målrettet ødelægge kommunens data og forårsage tab – såvel tidsmæssige som økonomiske.

De værste vira kan slette oplysningerne på harddisken, mens andre vira er mere eller mindre humoristiske indslag eller politiske eller ideologiske tilkendegivelser. Ligeledes kan oplysninger og data ufrivilligt blive videreformidlet til borgere og samarbejdspartnere og dermed blive læst af "udenforstående".

En pc kan blive smittet via disketter, cd'er, USB-nøgler, modem, kommunens netværk eller via internet og e-mail.

For at undgå virus råder kommunen over et antivirusprogram, som er installeret på alle pc'ere. For at kunne følge med udviklingen i vira og orme, bliver programmet løbende opdateret således, at man altid kan fjerne nyeste vira.

Som et supplement til det almindelige virusberedskab, sker der endvidere filtrering af uønsket og masseudsendt e-mail, også betegnet spam.

Selvom der således er etableret effektive værktøjer til at fjerne virus, orme og spam, er det vigtigt, at den generelle anvendelse af eksterne datamedier som disketter, cd'er, USB-nøgler og internet, foregår under hensyntagen til sund fornuft og god *it-skik*.

For at minimere risikoen for at din pc bliver inficeret med virus, gælder følgende regler:

- Hvis der er vedhæftet filer til en e-mail, skal du altid skanne filerne for virus, inden du åbner, aktiverer eller gemmer filen. Dette sker normalt automatisk.
- Af sikkerhedsmæssige grunde må du ikke installere egne programmer på kommunens pc'er.
- Kør altid et virusscan på datamedier, som har været uden for kommunens netværk eller på anden måde har været i kontakt med andre pc'er.
- Benyt aldrig datamedier, hvor du ikke kender oprindelsen.
- Slet beskeder fra mistænkelige afsendere.

Virusadvarsler via e-mail er oftest kædebeskeder, som reelt ikke betyder noget.

Videresend derfor ikke virusadvarsler til andre. Du kan eventuelt kontakte Team Servicedesk og IT, som vil foretage en konkret trusselsvurdering.

> Hvis du har mistanke om, at pc'en har fået virus, skal du fysisk afbryde forbindelsen til netværket, for at undgå at virus spredes. Endvidere skal du omgående orientere Team Servicedesk og IT.

Hvis der er tale om en kendt virus, vil kommunens antivirusprogram automatisk stoppe den pågældende virus og samtidig orientere Team Servicedesk og IT om, at du har været ramt af virus. Hvis afsenderen kan lokaliseres, vil pågældende blive orienteret om, at der er fundet virus.

Du bør herefter overveje, hvordan virus er kommet ind i systemet, for på den måde at undgå fremtidige forekomster.

5 Beskyttelse mod billeder af seksuel udnyttelse af børn.

I samarbejde med Næstved Kommunes internetudbyder er der opsat filtre der sikrer, der fra Næstved Kommunes it-udstyr ikke er adgang til internet adresser med billeder af seksuel udnyttelse af børn. Denne adgangsbegrænsning svarer til den danske blokeringsordning.

Der kan i yderst sjældne tilfælde åbnes for adgang til specifikke adresser. Dette kan kun ske i en begrænset periode og efter en grundig faglig vurdering, samt under personligt ansvar i henhold til gældende lovgivning.

Adgangen til disse adresser spærres igen når den faglige anvendelse er afsluttet og det påhviler den ansvarlige for åbningsanmodningen at sikre lukningen umiddelbart efter anvendelsens afslutning.

Nedenstående figurer viser hvad en leder eller en it-bruger/it-medarbejder skal foretage sig hvis der observeres billeder med seksuel udnyttelse af børn.

Hvad skal en bruger gøre hvis brugeren uforvarende bliver udsat for billeder af seksuel udnyttelse af børn mens de er på internettet.

- Brugeren kontakter nærmeste leder.
- Nærmeste leder kontakter center for personale og HR
- De hjemmesideadresser som indeholder ulovlige eller mistænkelige billeder skal indberettes til red barnets internet hotline på www.redbarnet.dk. Indberetningen foretages af en udpeget medarbejder fra center for personale og HR.
- Der fremsendes alle hjemmesideadresser og ikke kopier af de pågældende billeder.
- Næstved Kommune sikrer at de pågældende adresser bliver blokeret i firewallen.
- Der vil ikke være strafferetslige eller ansættelsesretslige konsekvenser.

Hvad skal en bruger eller it medarbejder gøre hvis brugeren finder billeder af seksuel udnyttelse af børn på fælles drev eller andre delte digitale enheder.

- Brugeren kontakter nærmeste leder.
- Nærmeste leder kontakter Center for personale og HR
- Center for personale og HR kontakter Team Servicedesk og It for at finde ud af hvordan materialet er havnet på den fælles digitale enhed og for at bevissikre materialet. Det vurderes, i hvilket omfang der skal søges efter yderligere potentielt kriminelt materiale på Næstved kommunes IT-udstyr.
- Hvis Center for personale og HR er i tvivl om, hvorvidt billederne er kriminelle, kontaktes politiet med henblik på at afgøre om billederne er kriminelle eller ej. Center for personale og HR kan vælge at kontakte det lokale politi eller gå ind via www.politi.dk/da/hjaelppolitiet/itkriminalitet/ og anmelde forholdet til rigspolitiets IT-efterforskningscenter NITEC.
- Materialet krypteres og indberettes til politiet jævnfør ovenstående.
- Indberetningen foretages af en udpeget medarbejder fra Center for personale og HR.
- Det videre forløb aftales mellem Center for personale og HR, Center for IT og digitalisering og politiet.

6 Dokumentdeling og anvendelse af "drev"

På Næstved Kommunes netværk er der adgang til en række centrale servere og systemer, som flere brugere samtidig kan anvende og dele data fra.

Serverne er struktureret med en række fællesdrev, som er områder på servernes datalager, hvor du kan gemme filer/dokumenter. Som it-bruger har du som hovedregel adgang til følgende drev:

Det personlige drev, som du kan benytte til egne arbejdsmæssige data. Dette drev må ikke benyttes til borger relaterede sager/dokumenter eller andet sagsrelevant materiale. Det er kun dig som bruger, der har adgang til disse data.

Centrets drev, som benyttes til at gemme data fra det enkelte centers produktion.

For hver organisatorisk enhed bliver der stillet en mappe til rådighed. Du vil have adgang til de organisatoriske enheder, som du er ansat i.

Generelt er det disse mapper, du skal benytte til data, med mindre du kan arkivere data i det kommunale ESDH-system.

Det fælles kommunale drev benyttes til udveksling af data på tværs af centrerne.

Der bliver automatisk taget backup af ovenstående drev på alle hverdage. Bemærk, at hvis du gemmer data lokalt på din pc, vil der ikke blive taget backup af disse.

Som hovedregel skal alle dokumenter gemmes i kommunens ESDH-system eller et fagsystem, der er godkendt til formålet, og ikke på de enkelte drev.

Husk - at du ikke må gemme personfølsomme data, hverken direkte på kommunens fællesdrev, dit personlige drev eller lokalt på din pc. Personfølsomme data må kun gemmes i særligt indrettede systemer. Jf. Persondataloven må personfølsomme data undtagelsesvis gemmes på fællesdrev så længe sagsbehandlingen finder sted - dog højst 30 dage.

Der er stillet en begrænset mængde diskplads til rådighed på de enkelte drev. Dette vil være nærmere specificeret i Team Servicedesk og ITs ydelseskatalog, ligesom muligheden for udvidelse fremgår af dette.

Du må ikke gemme borgerrelaterede sager/dokumenter eller andet sagsrelevant materiale på din private pc, Lokalt på kommunens pc'ere, på distance-pc'ere eller andre flytbare datamedier.

Næstved Kommune anvender Microsoft OneDrive som cloudbaseret drev. Denne mulighed er tilgængelig for brugerne.
Anvendelse af andre former for cloudbaserede løsninger, dropbox, Icloud, G-drive m.v. må kun anvendes med yderste varsomhed, **og må under ingen omstændigheder indeholde personhenførbare data.**
Anvendelsen af andre cloudbaserede løsninger må ikke ske uden forudgående aftale og tilladelse fra Centerchef eller afdelings leder.

7 Fysisk sikkerhed

Den fysiske sikkerhed er vurderet i forhold til mulige driftsforstyrrelser og driftstab. I praksis betyder det, at kravene til den fysiske sikkerhed er opdelt i tre sikkerhedsniveauer:

- Sikkerhedsniveau 1: Omfatter centralt udstyr, herunder udstyr i centrale serverrum - servere og kommunikationsudstyr samt krydsfelter.
- Sikkerhedsniveau 2: Omfatter almindeligt IT-udstyr i kommunens lokaler, herunder primært pc'ere, printere og tilsvarende periferiudstyr.
- Sikkerhedsniveau 3: Omfatter decentrale arbejdspladser og bærbare pc'ere uden for kommunens lokaler, herunder bærbare enheder som USB-nøgler, PDA'er og lignende.

I retningslinjen her omhandler den fysiske sikkerhed specielt sikkerhedsniveau 2, hvilket er almindeligt IT-udstyr i kommunens lokaler.

Retningslinjer for fysisk sikkerhed i øvrigt er medtaget under de relevante retningslinjer.

Udstyr som er reguleret af sikkerhedsniveau 2, må ikke indeholde personfølsomme oplysninger eller andre sagsakter.

Dette gælder i øvrigt også for sikkerhedsniveau 3, der er beskrevet retningslinjerne for distance pc'er og bærbare enheder.

Bygningsindretning og placering af udstyr
Pc'er, printere og øvrige komponenter skal være opbevaret i beskyttede og sikrede omgivelser således, at der ikke er direkte offentlig adgang og muligheden for uautoriseret adgang minimeres.

Skærm til pc skal - så vidt det er muligt – være placeret sådan, at uvedkommende ikke kan se oplysningerne på skærmen - vær i den forbindelse også opmærksom på vinduer og lignende. Printere, som bliver anvendt til udskrivning af personoplysninger - eller andre data, som ikke må blive tilgængelige for uvedkommende - må ikke være placeret i gangarealer eller andre områder, hvor publikum har adgang.

Der kan efter behov blive etableret fysiske foranstaltninger, som fysisk fastgørelse og lignende.

Der må kun opsættes IT-udstyr, der er godkendt af Næstved Kommunes IT-center.

Adgangskontrol
Det er kun Næstved Kommunes ansatte, som må have fysisk adgang til pc'ere, printere og andet af kommunens IT-udstyr. På områder hvor det vanskeligt kan håndhæves, eksempelvis på kommunale virksomheder, skal udstyret være under konstant opsyn eller i aflåst ved aktivering af pauseskærm.

Ovenstående gælder også for eksterne brugere, der arbejder/optræder for Næstved Kommune. Se bilag K Retningslinjer for eksterne brugere.

Udenfor normal arbejdstid skal IT-udstyret være låst forsvarligt inde.

8 Backup

Back-up-funktionen er ikke en arkiv-funktion, men en funktion, der skal sikre reetablering af vores IT-miljø, hvis vi kommer ud for systemnedbrud.

I den daglige IT-anvendelse forventer man, at have en mængde data til sin rådighed. Sådan er det også normalt, men det kan gå galt!

Trods back-up-procedurer er det ikke altid muligt at genetablere tabte data, da der gælder helt specielle back-up-procedure omhandlende typer, tidspunkter og hyppighed.

En mulig genetablering kan endvidere være forbundet med et uforholdsmæssigt stort tidsforbrug. Det er derfor kun i helt særlige tilfælde, at Team Servicedesk og IT kan tilbyde at genfinde et specifikt mistet dokument – hvis det overhovedet er muligt.

De daglige back-up-procedurer omhandler ikke data, der eventuelt er gemt lokalt på din pc.

9 Udskrivning

Som it-bruger udskriver du ofte dokumenter og notater - enten egne - eller andres. Disse dokumenter kan være fortrolige, og skal behandles med rette omhu.

Dokumenter, som indeholder personfølsomme eller andre fortrolige oplysninger, skal du opbevare på en sådan måde, at uvedkommende ikke kan få adgang, alternativt skal du sørge for at makulere dokumenterne.

Du skal derfor altid, straks efter udskrivning har fundet sted, hente dokumenter, som er udskrevet på centrale printere.

Dokumenter med fortrolige og personfølsomme oplysninger, må kun behandles af medarbejdere, der er autoriseret til behandlingen af den type

oplysninger, og som har en tjenestelig adkomst, samt af personer, der til brug for revision eller drift- og systemtekniske opgaver, har et konkret arbejdsbegrundet behov.

Hvis du får udskrevet et forkert dokument med fortrolige og personfølsomme oplysninger, er det dit ansvar at dokumentet bliver makuleret efter de gældende regler.

10 Programanvendelse og licenser

Du må kun anvende programmer på Næstved kommunes IT-udstyr, som kommunen har licens til.

Næstved Kommune råder over en række generelle licensaftaler, som gælder for alle kommunens standard pc arbejdspladser.

Information om kommunens standardprogrammer kan findes på intranettet.

Det er systemejer, der er ansvarlig for, at licensforholdene er i orden. Originale licensbeviser og tilhørende installationsmedier skal afleveres til Team Servicedesk og IT fysisk eller pr. mail, da det er Team Servicedesk og ITs ansvar, at opbevare disse.

Hvis enkelte medarbejdere har yderligere behov, anbefales det, at installation af særlige programmer og applikationer aftales med Team Servicedesk og IT.

Brugere der selv installerer programmer skal udvise forsigtighed og sikre programmet ikke overtræder licensregler. Overtrædelse af licensregler kan medføre sanktioner.

Installation af programmer kan medføre skader på brugerens pc.

Eventuel geninstallation af en pc udføres af Team Servicedesk og IT medfører at alle gemte data og filer slettes.

11 Hold dig ajour om Informationssikkerhed

For at sikre, at IT-installationen er forbundet med optimal sikkerhed er det vigtigt, at du som it-bruger altid holder dig ajour om nye tiltag og forhold, der har betydning for IT-anvendelsen og dermed Informationssikkerheden i Næstved Kommune.

Du kan holde dig ajour ved at besøge Næstved kommunens Informationssikkerhedsportal. Skriv ikke retningslinjerne ud – men tilgå dem online, så du altid er sikker på at læse de senest opdaterede.

Ajourføringshistorik (tidligere bilag B1)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i IT-centret, herunder også generel omskrivning m.h.p. lettere tilgang for it-brugerne.	14-09-2009 01-10-2009 30-10-2009 02-11-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	17-04-2014
Version 1.4	Opdateret af PBA/BDO	23-11-2017
Version 1.5	Opdateret af LLINN	14-05-2018

Bilag 2	Retningslinjer for anvendelse af e-mail

En stadig større mængde korrespondance modtages via elektronisk post (e-mail). For at sikre at anvendelsen af e-mail bliver indarbejdet i de eksisterende rutiner for sagsbehandling, journalisering og arkivering, er der i dette bilag fastsat retningslinjer for anvendelse af e-mail.

> Anvendelse af e-mail er et af midlerne til at skabe bedre service og fleksibilitet.

Retningslinjer for anvendelse af e-mail gælder alle, der har en e-mailadresse i Næstved Kommunes e-mail-system.

> Det er dit ansvar at indsætte de korrekte e-mailadresser og kun sende til relevante modtagere, vælg derfor dine e-mail-modtagere med omhu.
>
> Det er hurtigt at sætte mange modtagere på som CC, men det tager tid for alle modtagerne at forholde sig til en modtaget e-mail.
>
> Ved masseudsendelse af e-mail (f.eks. nyhedsbrev, orientering, høring, invitation) skal modtagerne tilføjes skjult (BCC).

1 Opdeling af e-mailadresser

Næstved Kommune anvender sikker digital post på en række områder. Loven kræver, at offentlige myndigheder beskytter de informationer, der sendes digitalt, hvis de indeholder såkaldte fortrolige "personfølsomme" oplysninger

I Næstved kommune findes en fælles hovedpostkasse og en række funktionspostkasser for virksomheder/centre/afdelinger som borgere og virksomheder kan benytte til sikker post via digital postkasse på borger.dk eller via e-Boks.

Derudover har kommunens medarbejdere en e-mail-postkasse, som ikke kan benyttes til mail med personoplysninger. Den officielle korrespondance mellem kommunens centre, afdelinger og virksomheder skal normalt foregå via de respektive officielle e-mail-postkasser.

For hovedpostkassen og funktionspostkasserne gælder, at der altid skal være én overordnet ansvarlig for hver funktionspostkasse.

Denne person har ansvaret for:

- At postkassen bliver tømt på alle hverdage – også i ferier og ved sygdom
- At tildele rettigheder til alle de personer, der skal have adgang til postkassen
- At give besked til Team Servicedesk og IT, hvis ansvarlig for postkassen skal ændres
- At give Team Servicedesk og IT besked, hvis postkassen skal nedlægges.

Hovedpostkassen

Næstved Kommunes hovedpostkasse er kommunens overordnede og officielle e-mailadresse og dermed den elektroniske hovedindgang til Næstved Kommune. Denne postkasse er en sikker postkasse, således at både modtagelse og afsendelse af sikker post kan håndteres. Læs mere om sikker post på kommunens intranet.

Funktionspostkasser

Kommunens sikre funktionspostkasser dækker Næstved Kommunes forskellige områder, hvor følgende retningslinjer er gældende:

Alle børneinstitutioner og skoler skal have en funktionspostkasse. For øvrige virksomheder er det valgfrit. Alle funktionspostkasser til institutioner og virksomheder bliver i hovedreglen offentlige postkasser, som man kan skrive til udefra. Dvs. borgere, leverandører m.v. kan skrive til disse funktionspostkasser.

Ved særlige behov kan en funktionspostkasse blive oprettet som en intern postkasse.

Funktionspostkasserne er den direkte adgang til det pågældende center, afdeling eller virksomhed.

Medarbejder postkasse

E-mail-postkasser oprettes til de medarbejdere, der har et arbejdsrelateret behov for at kunne kommunikere via elektronisk post. (Herefter kaldet den personlige e-mail-postkasse).

Den enkelte medarbejder, der har ansvaret for åbning, tømning og behandling af e-mail i sin personlige e-mail-postkasse.

Det er medarbejderens ansvar, at e-mail-postkassen bliver tømt dagligt, og at den ved fravær enten bliver tømt af en kollega eller at der er sat autosvar på postkassen, så afsenderen får besked om, at e-mail-postkassen ikke bliver tømt med det samme.

2 Adgangskode

Adgang til e-mail-postkasserne finder sted via den normale netværksadgang. Du skal derfor ikke indtaste et særligt password for at få adgang til e-mail-systemet.

Hvis du forlader din pc skal du altid enten logge af eller aktivere din pauseskærm med password, da andre ellers vil få direkte adgang til e-mails herunder have mulighed for at afsende e-mails i dit navn.

3 Adgang til e-mail-postkasserne

E-mail-systemet er oprettet med henblik på arbejdsrelateret anvendelse og Næstved Kommune opfatter derfor e-mail, sendt via kommunens systemer, som tilhørende Næstved Kommune, herunder også de e-mails, du modtager i din personlige e-mail-postkasse.

Du kan som medarbejder i Næstved Kommune anvende din personlige e-mail-postkasse til private beskeder i begrænset omfang.

Det er dig som medarbejder, der har den daglige adgang til den personlige e-mail-postkasse og dermed adgangen til at læse de indgåede e-mails. Du er dermed også ansvarlig for, at vurdere, hvorvidt en kollega skal tømme din e-mail-postkasse ved dit fravær. Du kan også aktivere et autosvar, hvor der bliver oplyst, hvornår du forventes at læse dine mails. Håndteringen af dette kan være meget forskellig alt efter dit arbejdsområde. Aftal derfor en procedure for håndteringen af din e-mail-postkasse ved fravær, med din nærmeste leder.

Som udgangspunkt bliver dine private e-mails ikke læst af andre, og Næstved Kommune foretager ingen løbende overvågning af dine ind- og udgående e-mails. Trafikken logges dog løbende for at sikre vores Næstved Kommunes it-miljø mod virus og spam. I den forbindelse vil virus- og spam-behæftede mails bliver frasorteret.

Et begrænset antal teknikere, med systemadministrator rettigheder har adgang til alle e-mail-postkasser og deres indhold. Dette er nødvendigt med henblik på at have mulighed for at udbedre driftsproblemer og servicere systemerne. Alle teknikere med denne adgang er godkendt af It-chefen. E-mails og mapper i postsystemet mærket med ”privat” må under ingen omstændigheder åbnes af andre end brugeren selv uden forudgående tilladelse.

Der bliver taget daglig backup af kommunens systemer for at sikre, at alle nødvendige data kan genskabes efter et eventuelt nedbrud af systemerne.

Du skal være opmærksom på, at e-mail systemet er indrettet sådan, at private e-mails kan blive læst af andre i kommunen, eksempelvis teknikere, systemejere eller under visse omstændigheder andre medarbejdere.

Dette vil dog kun undtagelsesvis finde sted, og du vil blive underrettet, såfremt e-mail postkassen er blevet åbnet.

For at undgå, at private e-mails utilsigtet bliver åbnet, bør du sørge for, at det af overskriften klart fremgår, at e-mail meddelelsen er privat.

4 Den daglige håndtering

Tømning af de officielle e-mail-postkasser skal ske dagligt af de udpegede medarbejdere, jf. ovenfor.

Du har som medarbejder ansvaret for, at din personlige e-mail-postkasse bliver tømt mindst én gang dagligt, og at e-mails bliver viderebehandlet og journaliseret jf. Centrets-/institutionens almindelige procedurer.

Du har som medarbejder ansvaret for, at din egen e-mail-postkasse bliver tømt dagligt.

Hvis du er fraværende, er det dit ansvar at sikre, at dine e-mails enten bliver omdirigeret, eller at en stedfortræder får adgang til din e-mail-postkasse.

Du kan sætte e-mail-systemet op til at give et automatisk svar. Dette bør indeholde en besked om, hvornår du kan træffes igen, samt henvisning til en kollega/funktionspostkasse, hvor afsenderen kan få hjælp, hvis sagen er af hastende karakter.

Automatisk videresendelse af e-mail må kun finde sted til e-mail-postkasser i kommunens interne netværk.

I forbindelse med en medarbejders fratræden eller orlov er det nødvendigt, at sikre en god service over for de borgere, firmaer eller kollegaer, der henvender sig til den pågældende.

Direktøren, afdelingschefen, virksomhedslederen eller medarbejderen skal derfor iværksætte følgende: (også ved længerevarende sygdom):

- Udsend information til hyppige kontakter med henvisning til ny medarbejder.
- Afmeld nyhedsgrupper.
- Tøm e-mail-postkassen og sikrer at den bliver tømt i den periode hvor E-mail adressen stadig er aktiv.
- Sæt e-mail postkasse op med automatisk svar og henvis til ny e-mail adresse.
- Ved fratrædelse: Orienter Team Servicedesk og IT ved brug af Servicedesk-systemet. E-mail-adressen vil herefter blive deaktiveret, hvilket betyder, at e-mailadressen ikke længere er synlig i adresselister og lignende. Derimod vil det opsatte autosvar fortsat blive returneret til de eventuelle personer, der skriver til e-mailadressen i en begrænset periode. I Næstved Kommune holdes E-mail kontoen som hovedregel tilgængelig i 3 måneder, men kan i særlige tilfælde holdes aktiv i op til 12 måneder.
- Ved fratrædelse skal oplysninger om E-mail adresse hurtigst muligt fjernes fra hjemmesider og andre offentligt tilgængelige informationssteder, Team Servicedesk og IT skal underrettes ved oprettelse af en sag i Ihelp.
- Ved både fratrædelse eller længevarende sygdom et det ledelsens ansvar at sikre Autosvar er aktiveret med henvisning til ny E-mail adresse samt anden relevant information.

Næstved Kommune anvender funktionspostkasser, der er særlige regler for funktionspostkasseansvarlige.

Det indebærer følgende at være ansvarlig for en funktionspostkasse:

- Postkassen skal tømmes på alle hverdage – også i ferier og ved sygdom, så tjek altid, at der er dækning i disse situationer.
- Du kan tildele rettigheder til de medarbejdere, der skal have adgang til postkassen.

- Mail fra en borger eller virksomhed bliver betragtet som et brev, og skal have samme forvaltningsmæssige behandling.

Du skal give Servicedesk besked, hvis ansvarlig for postkassen skal ændres, eller hvis postkassen skal nedlægges.

5 Besvarelse af e-mails fra borgerne

Afsendere af en e-mail kan have en forventning om, at modtage et hurtigt svar. Din besvarelse af e-mails skal - trods dette - ikke have anden tidsmæssig prioritet end post modtaget på papir. Ved modtagelse af e-mails direkte fra borgere, bør du dog kvittere for modtagelsen og eventuel supplere med en oplysning om den forventede sagsbehandlingstid.

BEMÆRK! Hvis dit svar indeholder personfølsom information må svaret som udgangspunkt ikke sendes som e-mail. Sendes det som e-mail skal du sikre dig, at de krav til mailforsendelsen som er nævnt nedenfor i afsnit 8 "Fortrolige data og personoplysninger" er overholdt. Ved borgerrettet kommunikation er det derfor en forudsætning, at borgeren selv har startet dialogen med at sende en sikker mail. Myndigheden kan kun sende sikre mails til borgere, der selv har sendt en digitalt signeret e-mail. Alle andre henvendelser uden digital signatur fra borgerne skal behandles manuelt.

6 Formalia og sprog

E-mails skal have tydelig afsender.

Når du afsender en e-mail fra Næstved Kommunes e-mail-system vil din signatur automatisk blive tilføjet. Denne indeholder logoet for Næstved Kommune, Center, afdeling, dit navn og titel, adresse, telefon- og faxnumre, e-mailadresse og henvisning til www.naestved.dk

E-mails skal have en præcis overskrift, der dækker indholdet. I forhold til eksterne modtagere kan overskriften være en hjælp til at få meddelelsen placeret hos rette vedkommende. Hvis meddelelsen skal journaliseres, er det også vigtigt, at overskriften er entydig.

E-mails er sidestillet med telefonsamtaler og papirbreve. Det er dog vigtigt, at du skelner mellem interne e-mails til kollegaer eller samarbejdspartnere og eksterne e-mails til borgere, andre myndigheder og lignende. Du bør som udgangspunkt skrive eksterne e-mails i samme stil som et papirbrev.

7 Vedhæftede filer

Du kan vedhæfte filer til en e-mail. Det kan være alle typer filer med betydelige datamængder, herunder tekst, regneark, data, fotos med videre.

> Undgå at sende store filer som billede-filer og videoklip til mange brugere ad gangen. Det gør e-mail-systemet langsomt og generer kollegaerne. Du kan samtidig risikere, at modtager ikke kan/må modtage så store datamængder.
>
> Som udgangspunkt skal du sende vedhæftede dokumenter i PDF-format.
>
> Alternativt kan meddelelser til store grupper eller hele kommunen formidles via intranet. Her sker oprydning automatisk.

8 Fortrolige data og personoplysninger

Ved behandling af fortrolige data og personoplysninger skal du sikre, at uvedkommende ikke kan få adgang til oplysningerne. Ved fremsendelse af e-mails med fortrolige eller personfølsomme oplysninger skal mailen krypteres og signeres. Du skal derfor sikre dig at:

- Modtager e-mail adressen er en sikker postkasse. Kun hvis den er det vil indholdet af mailen kunne krypteres og signeret.
- At der ikke står personoplysninger i emne linjen på e-mailen, da denne ikke krypteres.

- At e-mailen er opmærket, så mailsystemet ved at der er tale om forsendelse af en sikker e-mail. Vejledningen "Sikker post i Næstved Kommune" til hvordan du gør dette, finder du på intranettet Sikker post i Næstved kommune

Retningslinjer for anvendelse af digitale signaturer er beskrevet i bilag 6 Retningslinjer for anvendelse af digitale signaturer. Vejledning til borgere fremgår på kommunens hjemmeside. Du kan også finde mere information om sikker post på kommunens intranet.

Fortrolige data og personoplysninger vil på nuværende tidspunkt kunne afsendes sikkert i kommunens egne lukkede netværk. Det betyder, at du kan sende beskeder og filer med fortrolige eller personfølsomme oplysninger, som intern e-mail indenfor - og mellem - kommunens lokationer uden anvendelse af digital signatur.

Elektronisk behandling af personoplysninger er som udgangspunkt omfattet af Persondataforordningens regler. Det betyder, at såfremt du modtager eller sender fortrolige og personfølsomme oplysninger via e-mail, så skal du sørger for at slette disse fra e-mail-postkassen og journalisere disse e-mails inden 30 dage. Hvis du ikke gør dette vil du overtræde Persondataforordningens krav om behandling og sikkerhed.

Næstved Kommune følger persondataforordningen. Du må derfor ikke opbevare e-mails med fortrolige eller personfølsomme oplysninger i mere end 30 dage. Arkiver den aktuelle e-mail i ESDH-systemet eller i et fagspecifikt system, der er godkendt til formålet. Slet derefter den aktuelle e-mail fra din indbakke.

Læs mere i bilag 9 Persondata.

9 Journalisering

For journalisering af e-mails, både indgående og udgående, gælder de samme retningslinjer, som ved almindelig brevpost og faxmeddelelser.

Forretningsgangene vil normalt ske automatisk ved anvendelse af kommunens ESDH system.

Du bør derfor journalisere og gemme e-mails i ESDH systemet, hvis du vil have dem opbevaret i længere tid. For at undgå unødig lagring i e-mail systemet bør du med jævne mellemrum gennemgå og tømme din personlige e-mail-postkasse.

10 Virus og SPAM

Der er mange trusler mod kommunens it-systemer. De fleste trusler kan dog reduceres eller fjernes ved en kombination af sund fornuft, klare regler og praktiske foranstaltninger.

Der er ingen virusrisiko forbundet med at modtage almindelige beskeder uden vedhæftede filer. Virusrisikoen opstår, når du modtager vedhæftede filer, som du importerer og/eller udfører.

God it-skik med henblik på at undgå virusangreb, er beskrevet i bilag 1 Retningslinjer for it-brugere.

Hvis du bliver i tvivl kan du kontakte Team Servicedesk og IT. Her vil man altid vide besked om aktuelle virus-trusler.

I Næstved Kommune bliver eksterne e-mails og vedlagte filer kontrolleret for kendte vira. Virusprogrammet bliver jævnligt opdateret således, at det kan håndtere alle vira. Dog kan virus spredes så hurtigt, at man ikke kan være 100% sikker.

Mængden af SPAM, som er "uønsket masseudsendte e-mails", er stigende. Modtager du reklame og lignende e-mails, som du ikke selv har tilmeldt sig, bør du ikke besvare beskeden.

Kommunens SPAM filter sørger også for at fange den største del af den SPAM, som kommunen modtager. Af hensyn til sikkerheden bliver SPAM-mails og mails, der minder om SPAM-mails, automatisk fjernet fra mail-systemet.

11 Postgrupper

En postgruppe er en samling af en række e-mailadresser, der har noget til fælles.

Næstved Kommune stiller en række organisatoriske postgrupper til rådighed. Disse postgrupper bliver dannet automatisk ud fra organisationen og de medarbejdere, der er tilknyttet i de enkelte afdelinger.

Du vil altid kunne se, at en postgruppe er automatisk genereret ved, at der står (auto) sidst i navnet.

Derudover findes der en række ikke-organisatoriske postgrupper.

Alle postgrupper er foranstillet "postgruppe" i navngivningen. F.eks. "Postgruppe – Jobcenteret (auto)". Dette er for at gøre dig specielt opmærksom på, at du er ved at sende en e-mail til en større gruppe personer. I eksemplets tilfælde over 100 personer.

Det er dit ansvar at sikre, at modtagerne er de rette.

> Det er helt generelt dit ansvar at sikre, at modtagerne er de rette.
>
> Vær derfor ekstra opmærksom, når du benytter en eller flere af kommunens postgrupper. En fejlsendt e-mail forstyrrer dine kollegaer unødigt.

Benyt funktionspostkassen for de enkelte afdelinger, hvis du er i tvivl om, hvem i afdelingen, der skal modtage din e-mail. F.eks. "Jobcenteret (funktionspostkasse). Den person, der tømmer e-mail-postkassen vil så sørge for, at din e-mail ender hos rette modtager. På den måde undgår du at forstyrre flere end højst nødvendigt.

En funktionspostkasse kan kendes ved at der efter postkassenavnet er angivet (funktionspostkasse)

12 Nyhedsgrupper

Du kan som medarbejder tilmelde dig eventuelle arbejdsrelevante nyhedslister, som du skønner nødvendige. Du skal selv afmelde disse, når behovet ikke længere er til stede eller, hvis du fratræder.

13 Misbrug

Næstved kommune tolererer ikke, at medarbejderne misbruger kommunens postsystem, såvel indenfor som uden for normal arbejdstid. Misbrug kan dreje sig om kriminel adfærd, systemtruende adfærd, eller f.eks. at en medarbejder driver privat virksomhed fra arbejdspladsen.

Ajourføringshistorik (tidligere bilag B2)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune	02-11-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Opdateret 1.3	Yderligere præcisering af vigtigheden af overholdelse af persondataloven ifm.	09-02-2011
1.4	Opdateret AMS/Næstved Kommune	16-04-2014
1.5	Opdateret af PBA/BDO	19.12.2017
1.6	Opdateret af LLINN	13-06-2018

Bilag 3	Retningslinjer for anvendelse af internet

Retningslinjer for anvendelse af internet gælder alle medarbejdere, der anvender internet via kommunens administrative netværk - både fra pc'er på Næstved Kommunes lokationer og fra distance - og politiker pc'er samt andre bærbare enheder, der er koblet til det administrative netværk.

> Som medarbejder i Næstved Kommune kan du frit anvende internet til arbejdsmæssige formål. Endvidere har du mulighed for, at anvende internet til private formål i begrænset omfang, hvis arbejdet tillader det.

Når du anvender internet, skal du være særlig opmærksom og nøje overveje, hvilke sider du besøger, og hvad du evt. svarer ja/nej til. Dette gælder i øvrigt alle de steder, hvor du benytter it i Næstved Kommune.

Generelt skal du altid bruge din sunde fornuft og følge god it-skik. Det betyder blandt andet, at du under ingen omstændigheder må foretage ændringer i de anvendte programmer.

Du skal også være opmærksom på, at der af hensyn til drift, sikkerhed, genetablering og dokumentation bliver taget daglig sikkerhedskopiering af kommunens it-systemer, herunder også registrering af internetbrugernes ID samt de enkelte transaktioner.

1 Anvendelsen af internet

Internet er en vigtig kilde til viden og informationer. Validiteten (troværdigheden) af informationerne er dog afgørende for, om de kan anvendes.

Det er dit ansvar at være kritisk over for de informationer, som du finder på internettet.

Du skal være opmærksom på følgende forhold:

- Når du er på internettet, afsætter du spor, som kan føres til Næstved Kommune. Du skal derfor altid opfatte dig selv som en ambassadør, og kun anvende internet i kommunens interesse. Næstved Kommune ønsker ikke at blive identificeret med private diskussionsfora, porno, racisme og lignende. Eventuelle indlæg i diskussionsfora og lignende, er udelukkende et udtryk for en individuel holdning og er ikke nødvendigvis i overensstemmelse med Næstved Kommunes officielle politik.
- Søgning kan være tidskrævende. Du bør derfor målrette din søgning og overveje, hvor muligheden for at få informationen er størst.
- Det er forbudt, at søge efter - eller anvende - web-steder, som indeholder ulovligt materiale som f.eks. hacking, terrororganisationer, børneporno samt andre beslægtede steder. Dette må kun ske i embeds medfør mod skriftlig godkendelse fra Kommunaldirektøren, der er øverste sikkerhedsansvarlig.
- Du må kun downloade materiale (musik, film, spil), som du har brugsret/licens til. Du skal som bruger selv kunne dokumentere, at du har brugsret/licens til det aktuelle materiale.

2 Sociale netværk, Nyhedsgrupper mv.

Deltagelse på sociale netværk er tilladt under hensyntagen til de generelle forhold omkring anvendelse af internet (nævnt i afsnit 1).

De sociale netværk, som du bruger, kan registrere og gemme oplysninger om dig og hvilke informationer du søger og bruger.

Informationer som du har lagt ud på et socialt netværk, kan kun meget vanskeligt, måske aldrig, trækkes tilbage. Du vil med stor sandsynlighed opleve at nogen forsøger at franarre dig dine bruger-id''er og/eller dine adgangskoder (phishing).

Persondata må aldrig deles på sociale netværk

Bortset fra offentlige eller uklassificerede informationer, må kommunens informationer aldrig deles på et socialt netværk.

Kommunens informationer, f.eks. præsentationer, billeder og film, må ikke offentliggøres på sociale netværk, hvor der kan være tvivl om det strider mod Persondataloven eller om, hvorvidt kommunen bevarer sin ophavsret til informationerne.

Brugen af nyhedsgrupper mv. giver dig mulighed for at blive tilmeldt et interesseområde for derefter at få tilsendt e-mail med nyheder. Dette område er voksende og kan belaste kommunens servere unødigt. Det må derfor kun foregå med omtanke og hvis det er arbejdsrelevant.

Du skal altid afmelde en nyhedsgruppe, når du ikke længere har behov for at modtage nyhedsbrevet.

Team Servicedesk og IT kan til enhver tid spærre for sociale netværk og nyhedsgrupper mv., såfremt disse truer informationssikkerheden i Næstved Kommune eller på anden måde belaster kommunens it-miljø.

3 Distance- og politiker pc'er

Som udgangspunkt gælder de samme regler, når du anvender internettet fra distance- og politiker pc'er.

4 Handel og aftaleindgåelse på internet

De dispositionsregler, der i øvrigt er fastsat i Næstved Kommune for handel og indgåelse af aftaler, er også gældende for e-handel og indgåelse af aftaler på internet.

På nogle områder er der etableret fælles indkøbsaftaler. Disse aftaler vil også omfatte handel på internet.

Ved spørgsmål i forbindelse med indkøbsaftaler og lignende kan du kontakte indkøbskontoret.

5 Sikkerhed

Alle pc'ere, der er koblet på kommunens administrative netværk, er omfattet af et fælles antivirusprogram, som bliver opdateret af Team Servicedesk og IT. Programmet må ikke afinstalleres og vil automatisk blive geninstalleret ved næste logon på netværket. Antivirusprogrammet kontrollerer alt, hvad der hentes fra internettet til kommunens administrative netværk og frasorterer alle filer med kendte vira.

Du må ikke downloade programmer fra internettet.

I samarbejde med Næstved Kommunes internetudbyder er der opsat filtre som sikrer der fra Næstved Kommunes it-udstyr ikke er adgang til internet adresser med billeder af seksuel udnyttelse af børn. Denne adgangsbegrænsning svarer til den danske blokeringsordning.
Se Bilag 1 Retningslinjer for it-brugere, hvis du uforvarende bliver udsat for billeder af seksuel udnyttelse af børn mens du er på internettet.

Det er ikke tilladt, at ansatte kobler udstyr til netværket uden forudgående aftale med Team Servicedesk og IT. Det er dog tilladt, at tilslutte mobile enheder og bærbare pc'er til det trådløse gæstenetværk uden forudgående tilladelse.

Du må ikke tage nye web-baserede systemer i brug uden at disse er forhåndsgodkendt af Team Servicedesk og IT.

Næstved Kommune følger datatilsynets anbefalinger og det er derfor ikke tilladt at anvende Cloud baserede drev, såsom Dropbox, ICloud, Google drive eller skydrive fra udstyr stillet til rådighed af Næstved Kommune til opbevaring af personhenførbare data.

6 Logning

Trafikken til og fra internettet er omfattet af logning.

Logningsværktøjet er et statistisk værktøj i forbindelse med kommunens firewall, der registrerer unormale trafikmønstre, og det logger endvidere anvendelsen af internettet.

Der foretages en daglig backup af kommunens it-systemer, herunder også registrering af log-ID og de enkelte transaktioner.

Udgangspunktet er, at loggen gemmes minimum en uge. Det er udelukkende Team Servicedesk og ITs netværksmedarbejdere, der forestår logningsprocedurerne, og procedurerne må kun anvendes som foranstaltning mod misbrug o. lign.

Som udgangspunktet bliver den enkelte medarbejders anvendelse af internet ikke kontrolleret.

> Hvis der imidlertid opstår mistanke om misbrug af kommunens udstyr, forbeholder Næstved Kommune sig dog ret til at overvåge og gennemgå den enkelte medarbejders aktiviteter og lagrede data på it-udstyret.

Hvis en sådan gennemgang vurderes at være nødvendig, vil den blive foretaget af en it-medarbejder efter aftale med kommunaldirektøren eller dennes stedfortræder og under fuld fortrolighed.

Retningslinjerne er lavet i overensstemmelse med lov om behandling af personoplysninger.

Ajourføringshistorik (tidligere bilag B3)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i IT-centret, herunder også generel omskrivning m.h.p. lettere tilgang for it-brugerne.	18-09-2009 05-10-2009 02-11-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune på foranledning af Informationssikkerhedsudvalget	18-04-2014
Version 1.4	Opdateret af PBA/BDO	23-11-2017
Version 1.5	Opdateret af LLINN	14-05-2018

Bilag 4	Retningslinjer for fjernadgang til kommunens netværk

Retningslinjer for fjernadgang til kommunens netværk vedrører anvendelse af pc og mobile enheder med adgang til kommunens netværk uden for kommunens lokationer.

Brug af fjernadgang uden for kommunens bygninger stiller særlige krav til anvendelse og sikring af det anvendte udstyr. Du skal derfor være særlig opmærksom på lagring af data og håndteringen af udskrifter fra centrale systemer. Som bruger af fjernadgang skal du være bekendt med de særlige sikkerhedsforhold.

1 Generelle forhold

1.1 Backup

Team Servicedesk og IT sørger for, at der dagligt bliver taget backup af alle data på centrale servere på Næstved Kommunes netværk. Du skal være opmærksom på, at der ikke bliver taget backup af dokumenter, du har gemt lokalt på din pc.

1.2 Udskrivning

Når du udskriver på printere, der er placeret andre steder end på Næstved Kommunes fysiske lokationer, skal du være ekstra opmærksom på, at papir, der indeholder fortrolige data, aldrig må bortskaffes med det almindelige husholdningsaffald eller afleveres til genbrug.

Udskrivning er således underlagt de samme regler om opbevaring og kassation, som andet fortroligt papirmateriale. Udskrifterne skal afleveres i de dertil indrettede sække/aflåste containere i Næstved Kommune med henblik på makulering.

2 Udstyr

Indledningsvis skal det præciseres, at pc og udstyr tilhører Næstved Kommune. Du skal derfor tilbagelevere udstyret ved ophør af ansættelsesforholdet eller ved udtrædelse af byrådet. Hvis der sker bevidst misbrug, kan udstyret blive krævet tilbageleveret og linjen nedlagt

Udstyret må ikke anvendes til erhvervsmæssige formål uden for Næstved Kommunes regi.

Ved anvendelse af fjernadgang gælder principielt de samme retningslinjer som for Næstved Kommunes øvrige pc-arbejdspladser. Du skal derfor sikre, at der opretholdes en sikkerhed, som er på højde med den sikkerhed, som gælder pc'er, som er placeret i kommunens bygninger, og som er koblet på det administrative netværk. Det ligger dog uden for kommunens kompetence, at stille krav til indretning af boligen.

Det skal dog understreges, at uhensigtsmæssig adfærd kan resultere i, at hele Næstved Kommunes informationssikkerhed bliver svækket.

Følgende regler skal overholdes:

- Du skal altid opbevare pc'en forsvarligt.
- Du må ikke ændre på pc'ens sikkerhedsindstillinger.
- Pc'en er forsynet med antivirussoftware, som løbende opdateres. Virusskan skal være aktiveret.
- Du skal være opmærksom på hvilke data, du gemmer på pc'en. Opbevar kun data på pc'en, såfremt det er nødvendigt og vær specielt opmærksom på Persondatalovens regler vedrørende opbevaring af personhenførbare data. Anvend i stedet kommunens centrale servere eller kommunens ESDH-system til opbevaring af data.

2.1 Adgang til netværk og data

Den tekniske opsætning af fjernadgang til kommunens netværk er opsat og konfigureret af Team Servicedesk og IT. Der anvendes sikre adgangsformer med to-faktorvalidering.

Som udgangspunkt vil du som bruger af fjernadgang få tildelt samme rettigheder til netværket, som du har på arbejdspladsen i kommunen. Når du forlader pc'en, skal du derfor sikre den mod uautoriseret adgang. Dette indebærer, at pc'en enten skal slukkes helt eller, at du som minimum logger af Næstved Kommunes netværk.

En VPN-forbindelse er en direkte opkobling til Næstved Kommunes Netværk. Du skal derfor være ekstra opmærksom på sikkerheden, når du arbejder på en pc med VPN-forbindelse.

Fjernadgang må ikke anvendes af andre end den autoriserede medarbejder. I stedet er der mulighed for at tilslutte en privat pc til routeren, således at der kan opnås forbindelse til internettet uden om kommunens netværk. Opsætning skal ske efter vejledning fra den konkrete teleudbyder.

2.2 Fysisk sikkerhed

Ved anvendelse af fjernadgang skal opbevaring finde sted på forsvarlig vis. Der er ingen særlige krav til indretning, opbevaring og placering af udstyr ud over, hvad forsikringsselskaberne normalt kræver for at yde forsikringsdækning. Lokationer hvor kommunens udstyr opbevares, skal kunne aflåses.

2.3 Forsikring

Kommunens it-udstyr er dækket af kommunens interne forsikring. Det skal dog pointeres, at du selv er ansvarlig for, at data bliver sikret på betryggende vis, jf. kapitel 1 ovenfor.

3 Citrix-adgang og VPN-forbindelse

Adgang til kommunens netværk med Citrix-adgang finder sted med to faktorvalidering, hvorimod VPN-forbindelsen er en direkte forbindelse.

Når pc'en er koblet på kommunens netværk, gælder principielt de samme retningslinjer som for almindelige administrative pc'er, herunder retningslinjer for anvendelse af e-mail, internet og øvrige retningslinjer for IT-brugere. Vær specielt opmærksom på følgende forhold:

- Det er ikke tilladt at overlade pc'en til andre, når den er koblet på kommunens systemer.
- Det er ikke tilladt at overdrage brugernavn og kodeord til andre.
- Kommunale data og dokumenter må ikke gemmes lokalt på pc'er med fjernadgang.

4 Anti-virus

Der skal altid være installeret et anti-virus-program på pc'en. Det er brugerens ansvar, at programmet løbende opdateres.

Ajourføringshistorik (tidligere bilag B4)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune	02-12-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
1.3	Opdateret af LLINN	15-05-2018

Bilag 5	Retningslinjer for anvendelse af bærbare og mobile enheder

I forbindelse med opgaveløsningen i Næstved Kommune, bliver der i stigende omfang anvendt mobilt udstyr, herunder bærbare pc'er, Tablets, iPads, USB-lagre, smartphones og mobiltelefoner og lignende.

Der er derfor udarbejdet retningslinjer for anvendelsen af den type udstyr.

Retningslinjer for anvendelse af bærbare og mobile enheder vedrører anvendelsen af bærbart og mobilt udstyr, hvor kommunens administrative data opbevares og behandles, herunder

- bærbare pc'er, netbooks etc., beskrevet i kapitel 2,
- Tablets, iPads, Smartphones og mobiltelefoner, beskrevet i kapitel 3,
- øvrige bærbare enheder, herunder USB-lagre (eksempelvis USB-nøgler og USB-drev) og andet udstyr, der kan opbevare data, beskrevet i kapitel 4.

Da bærbare enheder ofte bliver anvendt uden for kommunens bygninger, og dermed opbevaret i et ureguleret område, stilles der særlige krav til anvendelse og sikring af den type enheder. Endvidere gør størrelsen af udstyret det ofte nemmere, at miste den pågældende enhed.

Du skal derfor være særlig opmærksom på sikkerheden, når du anvender bærbare enheder. Endvidere skal du være bekendt med de særlige sikkerhedsforhold, der gælder for denne type.

Retningslinjen her beskriver disse særlige forhold og opstiller en række kriterier, som skal være opfyldt ved anvendelse af bærbare og mobile enheder, uanset om udstyret anvendes i - eller udenfor - kommunens bygninger.

1 Generelle forhold

For alle typer bærbare og mobile enheder er der særlige retningslinjer for fysisk sikkerhed og udskrivning.

1.1 Fysisk sikkerhed

Opbevaring af bærbare og mobile enheder skal finde sted på forsvarlig vis.

> Opbevaring af bærbare og mobile enheder skal finde sted på forsvarlig.

Uanset om du anvender udstyret i - eller udenfor - kommunens bygninger, skal du opbevare de bærbare og mobile enheder sådan, at udstyr og data ikke kan blive tilgængelige for uvedkommende.

Det gør du ved, at opbevare udstyret på steder der ikke er synlige udefra, herunder

- i skabe og skuffer, der eventuelt kan aflåses,
- i afstand fra vinduer,
- i bilen - hvis den forlades skal udstyret opbevares i bagagerummet.

Generelt skal du opbevare den type udstyr i aflåste og tyverisikrede omgivelser, hvis det er muligt. Endvidere må du ikke overlade udstyret til andre.

1.2 Destruktion af data

Hvis udstyret skal overdrages til en anden medarbejder eller udgår, skal du sikre, at alle data bliver fjernet på betryggende vis.

1.3 Udskrivning

Hvis udskrivning sker andre steder end på Næstved Kommunes lokationer, skal du være opmærksom på, at papir, der indeholder fortrolige data, aldrig må bortskaffes med det almindelige husholdningsaffald eller afleveres til genbrug.

Udskrivning er således underlagt de samme regler om opbevaring og kassation, som andet fortroligt papirmateriale. Udskrifterne skal afleveres i de dertil indrettede sække/aflåste containere i Næstved Kommune mhp. makulering.

1.4 Forsikring

Bærbare og mobile enheder er - som kommunens øvrige IT-udstyr - dækket af kommunens interne forsikring. Det skal dog pointeres, at man selv er ansvarlig for, at data sikres på betryggende vis.

2 Retningslinjer for bærbare pc'er

> Ved anvendelse af bærbare pc'er, gælder principielt de samme retningslinjer som for Næstved Kommunes øvrige pc arbejdspladser, som de er beskrevet i IT-sikkerhedspolitikken, IT-sikkerhedshåndbogen.

Du skal således som bruger tilstræbe, at opretholde en sikkerhed, som er på højde med den sikkerhed, som gælder for stationære pc'er, der er placeret i kommunens bygninger og som er koblet på Næstved Kommunes netværk.

Du skal altid overholde følgende regler:

- Du skal altid opbevare pc'en forsvarligt. Det vil blandt andet sige, at du ikke må efterlade bærbare pc'er uden opsyn, med mindre de er i aflåste og betryggende omgivelser.
- Bærbare pc'er skal være opsat med opstartspassword.
- Bærbare pc'er skal altid være permanent mærket.
- Du må ikke ændre på pc'ens sikkerhedsindstillinger.
- Pc'er skal være forsynet med opdateret antivirussoftware, som altid er aktiveret.
- Pc'er må ikke benyttes af andre end autoriserede brugere i Næstved Kommune.

2.1 Adgang til netværk og data

- **Adgang til data:** Det er kun autoriserede medarbejdere i Næstved Kommune, der må anvende udstyret. Når du forlader pc'en skal du sikre den mod uautoriseret adgang. Det er dermed dit ansvar - som minimum - at låse pc'en, så der skal indtastes opstartspassword, for at få adgang til pc'en igen.
- **Personfølsomme data:** Du skal være opmærksom på, hvilke data du gemmer på pc'en. Opbevar kun data på pc'en, såfremt det er nødvendigt. Du må ikke gemme personhenførbare data på bærbare pc'er
- **Netværksadgang:** Bærbare pc'er har som udgangspunkt adgang til Næstved Kommunes netværk. Det er dit ansvar at pc'en jævnligt bliver tilsluttet Næstved Kommunes netværk. Dette skal ske for at sikre, at pc'en bliver opdateret med nyeste software-opdateringer herunder specielt antivirus-software.

2.2 Backup

Det er dit ansvar som bruger, at overføre data til centrale servere og dermed sikre, at der bliver taget sikkerhedskopi af de aktuelle data.

3 Retningslinjer for tablets, iPads mv.

> Ved anvendelse af Tablets, iPads og mobiltelefoner, gælder principielt de samme retningslinjer som for Næstved Kommunes bærbare pc'er

Du skal anvende password eller opstartskode for at aktivere udstyret.

Følgende regler skal overholdes:

- Du skal altid opbevare udstyret forsvarligt. Det vil blandt andet sige, at du ikke må efterlade Tablets, iPads, mobiltelefoner etc. uden opsyn med mindre de er i betryggende omgivelser.
- Udstyrets opsætning bliver foretaget af Team Servicedesk og IT eller tilknyttet underleverandør, og du eller andre må ikke efterfølgende ændre på sikkerhedsindstillingerne.
- Såfremt udstyret understøtter det skal antivirusprogrammet altid være aktiveret og opdateret.
- Opbevar kun data på udstyret, som er nødvendige.
- På mobile enheder anvendes låsekoder, der automatisk aktiveres efter 10 minutters inaktivitet.
- Enhederne skal være tilmeldt Telenor MDM for adgang til e-mail og kalender.

Det er kun de autoriserede medarbejdere i Næstved Kommune, der må anvende udstyret. Når du efterlader udstyret, skal du sikre det mod uautoriseret adgang således, at der som minimum skal indtastes opstartskode/password igen for at få adgang til data.

3.1 Sikkerhedskopiering

I de tilfælde, hvor udstyret understøtter det, skal du sørge for at data med passende intervaller, bliver overført fra Tablets, iPads, mobiltelefoner etc. til centrale servere eller andre opsamlingsenheder.
Det er under alle omstændigheder dit eget ansvar som bruger, at overføre data til centrale servere, når det er muligt, eller at sikkerhedskopiere data efter behov.

4 Retningslinjer for øvrige bærbare enheder

Ved anvendelse af øvrige bærbare enheder, herunder USB-lagre (eksempelvis USB-nøgler, USB-drev etc.) og andet bærbart udstyr, der kan opbevare data, gælder principielt de samme retningslinjer som for Næstved Kommunes bærbare pc'er.

Da udstyret ikke altid kan sikres logisk med passwordsikkerhed og lignende, kan sikkerheden i stedet planlægges på det fysiske niveau. Hvis det er muligt skal adgangen altid være spærret med password eller anden adgangskode.

Følgende regler skal overholdes:

- Du skal altid opbevare udstyret forsvarligt. Det vil blandt andet sige, at du ikke må efterlade USB-lagre og lignende uden for kommunens lokationer uden opsyn, med mindre de er i betryggende omgivelser.
- USB-lagre betragtes som midlertidige datalagre til datatransport og lignende. Du skal slette data, når data er transporteret til rette sted eller, når behovet for et midlertidigt datalager - i øvrigt - er ophørt. Opbevar kun data på udstyret, som er nødvendige.
  Det skal endvidere understreges, at det jf. Persondataloven ikke er tilladt at opbevare personhenførbare data på øvrige bærbare enheder med mindre der anvendes kryptering og personligt logon, og at dette kun må ske undtagelsesvis.

4.1 Backup

I det omfang det er muligt, skal du sørge for, at data med passende intervaller, bliver overført fra bærbare enheder til centrale servere eller andre opsamlingsenheder og efterfølgende slettes fra den bærbare enhed.

Det er under alle omstændigheder dit eget ansvar som bruger, at overfører data til centrale servere, når det er muligt, eller at sikkerhedskopiere data efter behov.

Ajourføringshistorik

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i IT-centret, herunder også generel omskrivning m.h.p. lettere tilgang for IT-brugerne.	21-09-2009 05-10-2009 02-12-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	23-04-2014
Version 1.4	Opdateret af PBA/BDO	23-11-2017
Version 1.5	Opdateret af LLINN	15-05-2018

Bilag 6	Retningslinjer for anvendelse af digitale signaturer

Digitale signaturer bliver anvendt:

- som adgangskontrol - logon - til en række offentlige tjenester,
- i forbindelse med afsendelse og modtagelse af elektroniske meddelelser, hvor sikkerhed for identitet, sikkerhed for indholdets autenticitet (troværdighed) og fortrolighed (kryptering) kan være ønsket eller påkrævet.

Næstved Kommune kan håndtere digitale signaturer, herunder udveksle signerede og krypterede elektroniske meddelelser med virksomheder, borgere og andre offentlige myndigheder.

Til det formål, anvender Næstved Kommune følgende certifikater:

- *Virksomhedscertifikater* – der bliver anvendt ved kommunens sikrede kommunikation med eksterne parter, virksomheder, andre offentlige institutioner såvel som private borgere.
- *Medarbejdercertifikater* – der bliver anvendt af ansatte med behov for logon til eksterne tjenester.

Du skal behandle digitale signaturer med samme omhu som øvrige passwords, hvilket vil sige, at du skal hemmeligholde din personlige kode til aktivering af signaturen for andre.

Team Servicedesk og IT har det overordnede ansvar for anskaffelse og drift af udstyr og faciliteter til signaturhåndtering, herunder administration og vedligeholdelse af udstedte certifikater.

Nedenfor kan du læse mere om de helt specielle og formelle retningsliner der gælder for digitale signaturer.

1 Ansvar og kompetence

Følgende roller har betydning i organiseringen af digitale signaturanvendelser:

- Øverste sikkerhedsansvarlig (kommunaldirektøren) eller den person til hvem opgaven er delegeret
- Direktører, centerchefer, teamledere, afdelingsledere og virksomhedsledere
- IT-chefen
- LRA-funktionen (Lokal Registrerings Autoritet)
- Postkasseadministrator
- Journalførere
- Medarbejdere med certifikat
- Medarbejdere uden certifikat

1.1 Certifikattyper

Kommunaldirektøren er øverste sikkerhedsansvarlige i Næstved Kommune.

IT-chefen beslutter, hvilke certifikattyper Næstved Kommune skal anvende i forbindelse med borgerrettede web-løsninger.

Direktører, centerchefer, teamledere, afdelingsledere og virksomhedsledere beslutter, hvilke medarbejdere der skal have tildelt medarbejdercertifikater til anvendelse ved logon med adgang til eksterne services etc. Det er endvidere direktørers, centerchefers, teamlederes, afdelingslederes og virksomhedslederes ansvar at sikre, at medarbejderne er orienteret om krav til - og begrænsninger - i anvendelsen af denne mulighed.

Den almindelige autorisationsprocedure følges i forbindelse med medarbejdercertifikater.

1.2 LRA - funktionen

Der er oprettet en LRA-funktion, der varetager administrationen af tildeling, vedligeholdelse og tilbagekaldelse af certifikater. LRA-funktionen er placeret i Team Servicedesk og IT.

Denne funktion har en hierarkisk opbygning, hvor det overordnede ansvar, samt muligheden for at oprette andre LRA'er, er placeret.

Der skal være mindst 2 medarbejdere, der er oprettet som LRA.

LRA kan bestille adgang til Virk.dk efter de generelle retningslinjer som beskrevet i bilag B Retningslinjer for autorisation, hvor der anvendes medarbejdercertifikater skal bestilles lokalt i de enkelte centre.

1.3 Postkasseadministratorer

Til postkasser i centre, afdelinger og virksomheder skal der være udpeget administratorer, som har til ansvar at sikre dokumentation og fordeling af indgåede (digitalt signerede/krypterede) dokumenter og de valgte bevismidler.

1.4 Journalførere

I forbindelse med ind- og udgående elektroniske meddelelser skal den enkelte, eller de udpegede medarbejdere, drage omsorg for at den valgte journalisering bliver foretaget.

1.5 Medarbejder uden certifikat

Som modtager, skal du sikre dig at underskriftsformalia er opfyldt.

Som afsender skal du anvende centerets, afdelingens eller virksomhedens centrale postkasses virksomhedscertifikat, når du afgiver svar med retsvirkning til borgere.

> Virksomhedscertifikater har ikke retsgyldighed som - de personlige - medarbejdercertifikater; men praksis er, at en skrivelse fra kommunen med en afgørelse, står ved magt, og det er normalt ikke op til borgeren at sikre sig, at der er tale om en bemyndiget underskriver.

Kravene om fortrolighed skal overholdes - blandt andet ved - at meddelelser, der indeholder personoplysninger, skal krypteres.

1.6 Medarbejdere med certifikat

Medarbejdercertifikatet er personligt.

Som modtager, skal du sikre dig at underskriftsformalia er opfyldt. Det vil sige, at hvis du modtager en krypteret e-mail i din personlig e-mail postkasse, så skal du afvise den og henvise til en fællespostkasse.

Hvis ikke bevisligheden er sikret på anden vis, skal du efter anvisning sikre, at der til enhver tid kan føres bevis for underskrifters gyldighed og for meddelelsesindholdets autenticitet og eventuelle registreringer af tidspunkt for modtagelse.

Som afsender skal du anvende afdelingspostkassens (virksomheds)certifikat (en af kommunens sikre postkasser), når du afgiver svar med retsvirkning til borgere med mindre, der er særligt behov for at afgive en bindende underskrift. Se endvidere ovenfor vedrørende bevislighed.

Medarbejdercertifikater kan ofte anvendes til flere services og på flere områder end den enkelte er bemyndiget til. Ved anvendelse af certifikatet til logon, må du kun foretage de handlinger, som du er bemyndiget til.

2 Bevislighed

Definition: Sikring af vished for certifikaters gyldighed, herunder identifikation og meddelelsesintegritet samt historik og uafviselighed.

Der opereres her med to typer bevisførelse, *systembeviset* og *signaturbeviset*, hvor *systembeviset* relaterer til sikkerheden i IT-systemerne, mens *signaturbeviset* alene relaterer til et givet dokument eller en given dokumentkæde.

3 Virus- og spamkontrol

Krypterede meddelelser skal som øvrige e-mails kontrolleres for virus og spam inden de modtages og anvendes i kommunen. Dette sker automatisk, når e-mailen modtages i Næstved Kommunes IT-miljø.

Ajourføringshistorik (tidligere bilag B6)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	02-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i IT-centret, herunder også generel omskrivning m.h.p. lettere tilgang for IT-brugerne.	21-10- 2009 05-10-2009 02-12-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	24-04-21014
Version 1.4	Opdateret af PBA/BDO	19.12.2017
Version 1.5	Opdateret af LLINN	13-06-2018

Bilag 7	Retningslinjer for trådløs kommunikation

Etablering af trådløst netværk skal altid ske i samarbejde med Team Servicedesk og IT.

1 Etablering af sikre WLAN

WLAN - Wireless Local Area Network – trådløst lokal netværk.

WLAN er baseret på radiobølger, kan kommunikationen foregå lige så godt uden for bygningerne som indenfor. Dermed kan alle og enhver i princippet få adgang til netværket.

I forbindelse med etablering af WLAN er det vigtigt, at man tager højde for sikkerheden. Næstved Kommune anvender derfor altid en kryptering, der lever op til de gældende standarder på området.

Etablering af WLAN i forbindelse med Næstved Kommunes netværk skal af samme grund altid ske i samarbejde med IT-centret.
På ERNA findes oversigten over etablerede WLANs i Næstved Kommune Klik her

Kommunale virksomheder, som har til hensigt at benytte denne type netværk, skal kontakte Team Servicedesk og IT, som herefter foretager opsætning og etablerer den fornødne kryptering.

2 WLAN og generel sikkerhed i netværket

Datasikkerheden i kommunens netværk er opbygget af flere elementer. Et af de væsentlige elementer er den fysiske sikkerhed.
Den fysiske sikkerhed består i, at lokalnet i kommunens bygninger kun er tilgængelige for kommunens ansatte. Netværksstik må derfor kun være monteret i områder, der er aflåst eller overvåget.

Kommunens lokalnet er indbyrdes forbundet med sikrede dataforbindelser, efter normer fastsat af IT-centret. Denne sikkerhed risikerer at blive brudt, hvis der eksempelvis tilsluttes et telefonmodem til et netværksstik. Fra et sådant modem kan man komme ind bag kommunens firewall og forvolde væsentlig skade. Dette gælder også, hvis du har din trådløse forbindelse tændt samtidig med, at pc'en er på det kablede netværk. (f.eks. når du har din bærbare pc stående i sin docking-station). Du skal derfor altid slukke for din trådløse forbindelse, hvis du er tilsluttet netværket direkte.

Et sikkerhedshul af den type, kan blive benyttet af hackere overalt i verden. Et tilsluttet telefonmodem er derfor et brud på datasikkerheden.

Ved etablering af trådløse netværk uden den fornødne sikkerhed, opstår der tilsvarende brud på datasikkerheden, dog med den undtagelse, at man skal være fysisk til stede i nærheden af den pågældende bygning, for at kunne opnå forbindelse til det trådløse netværk.

Det er derfor alene Team Servicedesk og IT, som må etablere trådløse netværk.

Opkobling til eksterne trådløse netværk fra kommunens bærbare pc'er og øvrige bærbare enheder er det tilladt (hoteller, konferencer, private trådløse netværk o. lign) Du skal dog altid være ekstra opmærksom og altid have dit antivirus-program opdateret og aktiveret.

Ajourføringshistorik (tidligere bilag A6-B7)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i IT-centret, herunder også generel omskrivning m.h.p. lettere tilgang for IT-brugerne.	05-10-2009 02-12-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	23-04-2014
Version 1.4	Opdateret af LLINN	16-05-2018

Bilag 8	Retningslinjer for sletning af data

For at sikre, at Næstved Kommunes data ikke bliver tilgængelige for uvedkommende, er der udarbejdet retningslinjer for sletning af databærende medier. Derudover er der skitseret retningslinjer for håndtering af data ved reparation og service samt sletning af data jf. Persondataloven.

1 Bortskaffelse generelt

Hvis der er behov for at bortskaffe databærende medier, herunder cd'er, USB-nøgler eller harddiske, skal man følge en række forholdsregler for at sikre, at data ikke bliver tilgængelige for uvedkommende.

1.1 Når IT-udstyr skal kasseres – herunder harddiske

> Hvis du har forældet IT-udstyr, eller IT-udstyr som ikke længere skal anvendes, skal du altid indlevere dette til Team Servicedesk og IT. IT-centret sørger for, at data og programmer bliver slettet, så disse ikke kan blive genskabt og dermed blive tilgængelige for uvedkommende.

Ved kassation af IT-udstyr skal du altid sikre, at fortroligt eller personhenførbart datamateriale bliver slettet effektivt, således at gendannelse af data ikke er mulig. Eventuelt kan fjernelse af data foregå som egentlig destruktion af lagringsmediet eller ved afmagnetisering. Team Servicedesk og IT sørger for dette.

Fjernelsen af data må aldrig overlades til eventuelle opkøbere af IT-udstyret, da der skal være sikkerhed for, at sletning af data er betryggende og overholder kommunens retningslinjer på området.

1.2 Når andre databærende medier skal kasseres

> Har du andre databærende medier som f.eks. cd'er, USB-nøgler, diske o.lign., som du skal have kasseret, skal du altid aflevere disse til IT-centret.

Ved anvendelse af cd'er, USB-nøgler, diske eller andre datamedier til korrespondance eller anden fil- og dataoverførsel, skal du være opmærksom på, at data som formidles, kan være fortrolige og kan blive tilgængelige for uvedkommende.

Hvis der er tale om fil-formidling til eksterne parter, skal du altid sikre, at det kun er relevante data, som befinder sig på cd'en, USB-nøglen eller disken. Samtidig må formidling kun finde sted til samarbejdspartnere, hvor der er en kendt, navngivet modtager.

> Er data personhenførbare, skal de være krypteret. Hvis dette ikke er muligt skal det altid overleveres personligt.

1.3 Når backupmedier skal kasseres

Forældede sikkerhedskopier og backupmedier bliver destrueret fysisk i Team Servicedesk og IT.

2 Reparation og service

I forbindelse med reparation og service af databærende udstyr skal der træffes foranstaltninger til sikring af data i forhold til adgangen for servicepersonalet.

Hvis IT-udstyr bliver sendt til reparation, skal du sørge for, at fortroligt og personhenførbart datamateriale bliver fjernet først. Hvis dette ikke er muligt, skal Team Servicedesk og IT sikre sig, at de oplysninger, som servicepersonalet kan blive bekendt med under reparationen, vil blive behandlet fortroligt. Du skal derfor altid gøre Team Servicedesk og IT opmærksom på, hvis der findes fortroligt og personhenførbart materiale, der ikke umiddelbart kan fjernes.

Retningslinjer for eksterne leverandører er beskrevet i bilag J.

3 Sletning af data jf. Databeskyttelsesforordningen

Ved behandling - herunder sletning - af personhenførbare data henvises i øvrigt til retningslinjen 9 ”Særlige forhold vedrørende Persondata”

I forbindelse med påbegyndelse af behandling af personoplysninger skal du altid tage stilling til, hvor længe der er behov for at opbevare oplysningerne, så du i den forbindelse kan fastsætte en frist for sletning af personoplysningerne.

Ved tilintetgørelse af både ind- og uddatamateriale, der indeholder fortrolige og personhenførbare oplysninger, skal du sikre, at materialet ikke kan blive misbrugt eller komme til uvedkommendes kendskab. Du skal derfor lægge papirmaterialet i de aflåste containere, som kommunen har til netop dette formål. Disse er tydeligt mærket med information om, at de indeholder fortroligt materiale til makulering. Det samlede materiale skal herefter makuleres, så materialets fortrolighed fortsat er sikret.

Ajourføringshistorik (tidligere bilag A7-B8)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2010
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i IT-centret, herunder også generel omskrivning m.h.p. lettere tilgang for IT-brugerne.	01-10-2009 03-12-2009
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Udarbejdet af AMS/Næstved Kommune	23—01-2018
Version 1.4	Opdateret af LLINN	14-05-2018

Bilag 9	Beskyttelse af persondata

1 Behandling af personoplysninger

EU's Databeskyttelsesforordning og Databeskyttelsesloven har til formål at sikre at persondata ikke misbruges.

Lovgrundlaget giver den enkelte borger nogle rettigheder, når kommunen behandler oplysninger om vedkommende. Formålet er i den forbindelse, at borgeren får kendskab til den måde kommunen håndterer oplysninger om den enkelte på. På denne måde styrkes den enkelte borgers retsstilling.

Direktører, centerchefer, afdelingschefer og ledere af kommunale virksomheder har ansvaret for, at kravene i Databeskyttelsesforordningen overholdes. Informationssikkerhedskoordinator og Kommunens jurister yder bistand i forbindelse med spørgsmål om Databeskyttelsesforordningen.

Næstved Kommune skal efterleve principperne om

- lovlighed, rimelighed og gennemsigtighed
- formålsbegrænsning
- dataminimering
- rigtighed
- opbevaringsbegrænsning
- integritet og fortrolighed
- ansvarlighed

som defineret i databeskyttelsesforordningen.

Informationssikkerhedskoordinatoren har den koordinerende rolle ved behandling af henvendelser fra borgere, brugere og myndigheder i forbindelse med registreredes rettigheder og brud på persondatasikkerhed.

2 Oplysningspligt

Kommunen har som udgangspunkt oplysningspligt. Det betyder, at kommunen skal oplyse borgeren om kommunens behandling af indsamlede oplysninger. Det betyder, at det skal fremgå af kommunens kommunikation med borgeren hvorfor- og til hvilken brug oplysninger indsamles, hvordan oplysninger efterfølgende håndteres, om de videregives, opbevares eller kasseres, om det er frivilligt eller obligatorisk at afgive oplysninger og borgeren skal orienteres om reglerne om indsigtsret og retten til at gøre indsigelser.

Kommunen skal være opmærksom på om der skal indhentes samtykke fra borgeren inden behandling af oplysninger må finde sted.

3 Indsigtsret

Indsigtsret omhandler i modsætning til aktindsigt efter offentlighedsloven og forvaltningsloven, en ret til at få oplysninger fra kommunen om, hvilke oplysninger kommunen behandler om en borger, og til hvilken brug oplysninger behandles. Derfor føres fortegnelser over alle systematiserede behandlingsaktiviteter, der indeholder personoplysninger.

3.1 Fortegnelser

For at forenkle og smidiggøre administrationen af indsigtsretten, bliver information om alle kommunens aktive systemer og anmeldelser stillet til rådighed for alle ansatte i Næstved Kommune. Næstved Kommune skal vedligeholde fortegnelser over behandling af persondata. Fortegnelserne vedligeholdes af de respektive centre og kvalitetssikres af Team Strategi & Digitalisering (TSD).

I de enkelte centre og virksomheder, skal der være fortegnelser over, hvad der bliver foretaget af elektroniske og eventuelle manuelle behandlinger og registreringer af personoplysninger. Ansvaret for denne registrering påhviler centerchefen.

Fortegnelsen indeholder følgende oplysninger:

- Kontaktoplysninger på dataansvarlig og databeskyttelsesrådgiver (DPO)
- Formålet med behandlingen, herunder delformål (KLE)
- Kategorier af registrerede og personoplysninger
- Kategorier af modtagere ved videregivelse af oplysninger
- Overførsel til tredjelande og internationale organisationer
- Frist for sletning af oplysningerne
- Tekniske og organisatoriske foranstaltninger

For særligt kritiske typer behandlinger, skal der udarbejdes en konsekvensvurdering (Data Protection Impact Assessment) DPIA.

3.2 Fremgangsmåde ved begæring om indsigt

Borgere, der retter henvendelse om indsigt, bliver henvist til BorgerService, som er ansvarlig for, at den pågældende legitimerer sig og angiver, hvilke data borgeren ønsker oplysning om. Borgerservice orienterer Informationssikkerhedskoordinatoren, og varetager indsamling af oplysninger fra forvaltninger, som har ansvaret for de relevante datasamlinger.

Indsigtssager skal altid journaliseres og registreres i kommunens ESDH-system.

Blanketten "Anmodning om indsigt i personoplysninger", der er tilgængelig på Næstved Kommunes hjemmeside kan benyttes til formålet.

I tilfælde hvor der forekommer fortrolige og personfølsomme oplysninger om den registrerede sendes disse enten i lukket kuvert, eller via kommunens lukkede systemer, til BorgerService.

Begæringen om indsigt skal jf. Databeskyttelsesforordningen imødekommes inden 4 uger efter modtagelsen. Er begæringen ikke besvaret inden for de 4 uger, skal den pågældende underrettes om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge.

BorgerService varetager en samlet tilbagemelding til rekvirenten. Tilbagemeldingen skal fremgå i et klart og forståeligt sprog, og eventuelle printudtræk fra fagsystemer med koder skal altid være efterfulgt af en vejledende tekst.

Som udgangspunkt skal kommunen give oplysningerne skriftligt. I særlige tilfælde kan hensynet til den registrerede tale for at indsigten i stedet for bliver givet mundtligt af en medarbejder.

Hvis informationerne bliver sendt til borgeren via e-mail, skal disse være krypteret. Retningslinjer for anvendelse af digital signatur er beskrevet i informationssikkerhåndbogens bilag 6 "Retningslinjer for anvendelse af digitale signaturer".

4 Videregivelse

Kriterier for videregivelse af personoplysninger fremgår af Databeskyttelsesforordningen. Som udgangspunkt kræves specifik lovhjemmel eller samtykke for en videregivelse af oplysninger.

Ved elektronisk fremsendelse af fortrolige og personfølsomme oplysninger, skal oplysningerne krypteres ved anvendelse af digital signatur. Dette gøres ved at sende besvarelsen via en af kommunens sikre postkasser.

Personoplysninger *kan* sendes og modtages inden for Næstved Kommunes netværk uden anvendelse af digital signatur. Dette er ensbetydende med, at e-mail og filer med fortrolige eller personfølsomme oplysninger, kan sendes som intern e-mail uden at anvende digital signatur. Dette gælder alene for sags-relevante data.

Mails indeholdende personoplysninger skal journaliseres og registreres i sags- og dokumenthåndteringssystemet, og må ikke figurere i mail-systemet i længere tid end der administrativt er brug for indholdet.

Der henvises i øvrigt til lovgivningens bestemmelser om videregivelse.

5. Registreredes øvrige rettigheder

Kommunen er forpligtiget til at behandle og træffe afgørelse i sager om indsigelser fra borger mod at oplysninger om vedkommende gøres til genstand for behandling.

Det samme gælder henvendelser om berigtigelse, sletning eller blokering af oplysninger, som borger mener er urigtige eller vildledende eller på anden måde er behandlet i strid med lovgivningen.

Afgørelser om indsigelser i henhold til Databeskyttelsesforordningen skal træffes af det center, som har behandlet oplysninger om borgeren. Borgeren har et retskrav på, at kommunen berigtiger eller blokerer oplysninger, som viser sig vildledende eller urigtige.

Grundet kommunens pligt til overholdelse af arkivlovgivning, offentlighedslovens regler om aktindsigt, principper om gennemsigtighed med videre, kan kommunen ikke berigtige eller blokere oplysninger ved sletning. Berigtigelse af vildledende og forkerte oplysninger skal derfor ske i notatform på sagen. Af notatet skal fremgå, at tidligere noterede oplysninger af den og den karakter hermed berigtiges til et nyt indhold.

Borgeren har jf. Databeskyttelsesforordningen ret til at klage til Datatilsynet over kommunens behandling af personoplysninger vedrørende pågældende.

6. Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden

Medarbejdere skal ved konstatering af brud på persondatasikkerhed kontakte kommunens informationssikkerhedskoordinator på persondataforordning@naestved.dk.

Eksempler på brud er:

- Uautoriseret adgang til persondata
- Personoplysninger slettes eller ændres ved et uheld eller tilsigtet
- Personoplysninger videregives til uvedkommende personer

Informationssikkerhedskoordinator skal senest 72 timer efter et brud på persondatasikkerheden, foretage anmeldelse til Datatilsynet, medmindre at det er usandsynligt at bruddet på persondatasikkerheden indebærer en risiko for borgerens rettigheder.

Anmeldelsen skal begrundes, hvis den ikke er indgivet inden for 72 timer.

Anmeldelse skal blandt andet beskrive bruddets art, karakteren af bruddet på persondatasikkerheden, konsekvenser og afhjælpende foranstaltninger.

Anmeldelsen skal desuden indeholde navn og kontaktoplysninger på databeskyttelsesrådgiveren.

Næstved Kommune (Informationssikkerhedskoordinatoren) skal dokumentere alle brud på persondatasikkerhed, herunder de faktiske omstændigheder, dets virkninger og de trufne afhjælpende foranstaltninger. Dokumentationen skal kunne sætte datatilsynet i stand til at kontrollere at retningslinjerne efterleves.

Se Administrationsgrundlag for Håndtering af brud på persondatasikkerhed og skabelon for redegørelse om brud på sagen 85.13.00-P20-11-18.

Ajourføringshistorik (tidligere bilag B12-C5)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune	28-10-2009

	Tilrettet jf. kommentarer fra Datatilsynet.	
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af PBA/BDO / AMS	15-03-2018
Version 1.4	Opdateret af LLINN	13-06-2018

Bilag A Retningslinjer for systemejere

Alle systemer i Næstved Kommune tilhører en systemejer, som med udgangspunkt i et fagligt ansvar anskaffer et IT-system til at understøtte opgavevaretagelsen.

Systemejer er øverste ansvarlig for en selvforvaltende enhed eller virksomhed inden for kommunens hierarkiske struktur. Systemejerskabet vil ofte falde sammen med det økonomiske budgetansvar for enheden.

Hierarkisk er systemejeren en centerchef eller en virksomhedsleder. Systemejeren kan også være en direktør.

Systemejerskabet kræver ikke særlig teknisk indsigt, ud over den en typisk slutbruger af it-systemer har.

Systemejerskabet forudsætter til gengæld den faglige indsigt på det område, hvor systemerne udgør en del af arbejdsprocesserne. Det er denne viden, som gør det muligt for systemejeren at stille de relevante krav til, hvordan systemet skal understøtte forretningsprocesserne og at følge effektivt op på dem.

Mere konkret har systemejeren ansvaret for, at der foreligger retningsliner og instrukser for det pågældende system og at de bliver overholdt. I de tilfælde, hvor et system bliver anvendt i et andet center eller afdeling end systemejerens, er det chefen for det center eller afdeling, hvor systemet anvendes, der har ansvaret for, at retningslinjerne og instrukserne bliver overholdt.

Systemejer kan uddelegere hele opgaven eller dele af opgaven til en systemadministrator. Specielt i forbindelse med godkendelse af autorisationer kan systemejer uddelegere opgaven til den aktuelle brugeres nærmeste leder med personaleansvar. Ansvaret som systemejer kan ikke uddelegeres.

Oversigt over systemejere og systemadministratorer er tilgængelig på Næstved Kommunes intranet og bliver vedligeholdt af Team Strategi og Digitalisering i KITOS.

1 Generelle opgaver

Systemejer har ansvaret for

- et systems anskaffelse og implementering, herunder betryggende opsætning og fastlæggelse af systemsikkerheden i samråd med informationssikkerhedskoordinatoren / Informationssikkerhedsudvalget.
- at der foreligger retningslinjer og instrukser for et systems anvendelse, og for, at forretningsgange og instrukser bliver overholdt.
- at der er beskrevet relaterede interne kontroller
- at der er etableret systemsupport og administration af leverandøradgang
- at indgå databehandleraftaler med it-leverandører
- at der er taget stilling til nødprocedurer.
- en række supplerende opgaver i forbindelse med systemanvendelsen. Opgaverne er beskrevet i de enkelte kapitler nedenfor.

2 Autorisation

Helt generelt skal alle brugere af it-systemer og data i Næstved Kommune, have de nødvendige rettigheder, for at kunne løse opgaverne. Samtidig må ingen brugere have rettigheder til systemer og data, som ikke er arbejds- og opgavemæssigt begrundet.

Med henblik på at sikre ovenstående, er der udarbejdet retningslinjer for autorisation og brugeroprettelse til systemer og data, som beskrevet i bilag B "Retningslinjer for autorisation og brugeroprettelser".

Systemejere skal føre tilsyn med, at retningslinjerne for egne systemer og data, bliver overholdt.

Det er systemejer eller den til hvem systemejer deleger opgaven der skal godkende samtlige autorisationer til it-systemet. Godkendelsen skal være entydig og sporbar.

Systemejere eller delegerede skal i forbindelse med godkendelse af adgange forholde sig til, om adgangen er arbejdsmæssigt begrundet. De skal vurdere på relevansen af den ønskede adgang, herunder skelne mellem rettigheder til at læse, rette, oprette og slette. Endvidere skal de vurdere, om tildelingen af adgang medfører, at der samtidig bliver tildelt yderligere adgang, som kan indebære en forøget risiko.

Af hensyn til varetagelse af en hensigtsmæssig funktionsadskillelse, skal godkendelse og oprettelse være fordelt på forskellige personer. Den der godkender, må ikke samtidig have mulighed for at foretage selve autorisationen i systemet.

Systemejere har ansvaret for etablering af en kontrolprocedure, der skal sikre, at der med faste intervaller føres tilsyn med omfanget af autorisationer.

Alle elektroniske autorisationsblanketter skal af hensyn til senere opfølgning arkiveres så længe, brugeren er ansat i kommunen, og tillige 1 år efter fratrædelsen. Autorisationsblanketten opbevares i kommunens HelpDesk-system.

Ud over autorisation af kommunens it-brugere, skal systemejere - i samråd med øverste sikkerhedsansvarlig, informationssikkerhedskoordinatoren og Team Servicedesk og IT - planlægge i hvilket omfang borgere kan opnå adgang til kommunens data.

3 Logning

Systemejere har ansvaret for definition af logningsniveau og gennemgang af logs i de pågældende systemer. Det er Team Servicedesk og IT eller leverandøren af produktet, der skal foretage den tekniske opsætning af loggen.

Niveauet for logning skal generelt defineres ud fra en vurdering af de enkelte systemer og datas væsentlighed for opgaveløsningen i kommunen. Derudover skal man ved vurderingen forholde sig til risikoen for uhensigtsmæssig anvendelse af systemer og data.

Logning af anvendelsen af systemer og applikationer, der bliver driftsafviklet på Næstved Kommunes eget udstyr eller databehandler/systemleverandør, skal ske via de indbyggede logningsfaciliteter. I tilfælde, hvor der ikke er et sikkerhedssystem til rådighed, skal logningen ske via netværksoperativsystemet.

Afhængig af det enkelte systems væsentlighed, kan der være behov for logning af hændelser direkte i databaserne, hvor ændringer i væsentlige tabeller eller felter skal være underlagt konstant logning og overvågning.

Desuden skal lovgivningens krav til logning af personhenførbare oplysninger overholdes.
Der skal jævnligt, i det omfang det pågældende system giver mulighed for det, ske en gennemgang af samtlige bevægelser vedrørende it-medarbejdernes rettigheder til systemerne. Kontrollen foretages af systemejere, med udgangspunkt i autorisations- og benyttelsesinformation fra systemerne sammenholdt med autorisationsblanketterne. Øverste sikkerhedsansvarlige eller dennes repræsentant orienteres løbende om kontrollens resultat.
Retningslinjer for logning er uddybende beskrevet i bilag B11/C4 "Retningsliner for logning".

4 Interne kontroller

Systemejer er ansvarlig for, at der for det enkelte system er taget stilling til, hvilke interne kontroller, der skal foretages ved behandlingen af data.
Formålet er at sikre systemets og forretningsgangens sikkerhed og integritet, og hvem der er ansvarlig. Systemejer skal sikre, at procedurerne iværksættes.

Der skal som minimum være etableret interne kontroller for de systemer, der leverer data til kommunens økonomistyring. Det gælder både kommunens overordnede økonomisystem og øvrige systemer, der har med snitflade til økonomisystemet, herunder opkrævnings- og udbetalingssystemer, som fremgår i bilag til kommunens Kasse- og Regnskabsregulativ.
Derudover skal der for systemer, der behandler personfølsomme eller personhenførbare informationer, etableres interne kontroller.
Systemejere har ansvaret for, at interne kontroller bliver planlagt og implementeret.

5 Udvikling og anskaffelse

Det er normalt systemejere, der har ansvaret for anskaffelse af et systemkompleks til løsning af en konkret opgave.

Hvis der ikke er tale om et standardsystem - eller hvis et standardsystem eventuelt skal tilrettes den konkrete opgaveløsning - har systemejere tilsynet med denne udviklingsopgave.

Systemejer kan uddelegere opgaven.

Team Servicedesk og IT skal i samarbejde med systemejere sikre, at anskaffede systemer og driftsmiljøer bliver etableret på en sådan måde, at retningslinjerne i informationssikkerhedshåndbogen og bilagene bliver efterlevet.

Systemejere har ansvaret for, at udviklede applikationer bliver sikret i et tilfredsstillende omfang, dels via centralt opdaterede sikkerhedskopier dels ved udarbejdelse af præcis dokumentation af programmeringsgrundlaget.

Man må ikke tage systemer i brug, før de er blevet testet. Omfanget af testen er afhængig af væsentlighed og risiko. Efterfølgende ændringer af systemet skal også altid testes inden de bliver sat i drift.

Af hensyn til kontraktlige forhold, test og drift med mere, skal Team Servicedesk og IT **altid** inddrages i processen, inden installation af nyt software på kommunens administrative netværk.

6 Nødberedskab

Nødberedskabet for IT-anvendelsen skal skabe sikkerhed for, at Næstved Kommune kan genskabe en normal driftssituation hurtigt og sikkert.

Derudover skal IT-brugerne være informeret om relevante dele af nødberedskabet, så der er et generelt kendskab til det informationssikkerhedsniveau, der er etableret.

Det tekniske nødberedskab er forankret i Team Servicedesk og IT. Derudover skal der for alle systemer/områder været taget stilling til behovet for nødprocedurer. En nødprocedure kan være en beskrivelse af, hvilke manuelle forretningsgange man som bruger skal følge, hvis et IT-system ikke er tilgængeligt i en kortere eller længere periode.

Hvis systemet har den højeste prioritet, skal der være beskrevet manuelle forretningsgange, som kan medvirke til at minimere konsekvenserne ved et egentligt katastrofescenario eller et mere begrænset systemnedbrud.
Nødberedskab for IT-anvendelsen er uddybende beskrevet i bilag A8/B9/C2.

Ajourføringshistorik (tidligere bilag C1)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune	13-11-2009 25-01-2010
Endelig Version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret AMS/Næstved kommune	17-04-2014
Version 1.4	Opdateret AMS/ Næstved Kommune	22-03-2018
Version 1.5	Opdateret af LLINN	14-05-2018

Bilag B	Retningslinjer for autorisation og brugeroprettelse

Retningslinjer for autorisation har til formål at sikre, at alle brugere af Næstved Kommunes it-systemer og data har de nødvendige rettigheder, som er krævet til løsning af opgaverne. Modsat skal retningslinjen også sikre, at ingen brugere har rettigheder til systemerne, som ikke er arbejds- og opgavemæssigt begrundet.

Nedenstående forretningsgange gælder samtlige systemer og data, som bliver anvendt til opgaveløsningen i Næstved Kommune.

1 Generelt

Alle autorisationer skal være dokumenteret, så man efterfølgende kan genfinde anmodningen om adgange til diverse IT-systemer.

Alle henvendelser vedrørende brugeres rettigheder til Næstved Kommunes systemer og data skal således ske via HelpDesk-systemet IHLP. Vejledning i oprettelse af brugerautorisationer ligger på ERNA.
http://erna/Praktisk/It_og_telefoni/Brugeradministration.aspx

Der skal her være angivet, om der er tale om en oprettelse, ændring, sletning eller flytning. Systemejer - eller en af denne udpeget person til varetagelse af denne opgave - skal godkende samtlige autorisationer. Godkendelsen skal være entydig og sporbar.

Den særligt udpegede person vil som hovedregel være brugerens nærmeste leder med personaleansvar, da denne er den nærmeste til at kende brugerens specifikke behov for systemadgange. I den efterfølgende beskrivelse benævnes personen, der godkender autorisationen alene som "systemejer".

Systemejer skal i forbindelse med godkendelse af adgange forholde sig til, om adgangen er arbejdsmæssigt begrundet. Systemejer skal vurdere, om den ønskede adgang er relevant, herunder skelne mellem rettigheder til at læse, rette, oprette og slette. Endvidere skal de vurdere, om tildelingen af adgang medfører, at der samtidig bliver tildelt yderligere adgange, som ikke er hensigtsmæssig og som indebærer en risiko.

Af hensyn til varetagelse af en hensigtsmæssig funktionsadskillelse, skal minimum godkendelse og oprettelse være fordelt på forskellige personer. Den, der godkender, må ikke samtidig have mulighed for at foretage selve autorisationen i systemet.

Alt dokumentation for autorisationer, oprettelse, ændringer og nedlæggelse skal af hensyn til senere opfølgning arkiveres så længe, brugeren er ansat i kommunen, og tillige 1 år efter fratrædelsen. Dokumentationen opbevares i kommunens HelpDesk-system.

2 Oprettelse af brugere

Grundoprettelse af brugere foregår efter forretningsgangbeskrivelsen, jf vejledningen i brugeroprettelse: http://erna/Praktisk/It_og_telefoni/Brugeradministration.aspx

Derudover kan brugerne tildeles specifikke rettigheder til relevante fagsystemer.
For samtlige fagsystemer skal oprettelsen følge forretningsgangsbeskrivelsen for det enkelte system. Forretningsgangen skal som minimum følge nedenstående overordnede procedure.
Den til opgaven udpegede medarbejder udarbejder anmodning om autorisation.

I HelpDesk-systemet skal angives, det/de systemer, som brugeren skal have adgang til. Man skal også angive hvilke profiler eller rettigheder, brugeren skal have tildelt.

Autorisationsanmodningen sendes til godkendelse hos systemejer i de tilfælde hvor der er tvivl om autorisationens arbejdsbetingede berettigelse, for eksempel meget brede eller systemadministrative adgange.

I forbindelse med ekstern revision og analyse af it-systemer, servere og netværk må der ikke gives rettigheder ud over læseadgang.

Hvis revisionen, eller analysen, nødvendiggør mere end læseadgang, må dette kun tillades på kopier af de berørte filer og data, der skal slettes efter brug.

Autorisationsanmodningen skal arkiveres i HelpDesk-systemet så længe medarbejderen er ansat i kommunen plus 1 år. Team Servicedesk og IT Eventuel videre behandling er afhængig af, hvilken forretningsgang der findes for det enkelte område/system.

Ved implementering af nye IT-systemer, hvor en større mængde brugere skal oprettes m.h.p. en samlet opstart, skal Team Servicedesk og IT altid kontaktes, så fremgangsmåden kan aftales i det specifikke tilfælde.

3 Ændring af brugere

Når en medarbejder skal have ændret rettighederne til et eller flere systemer, som medarbejderen allerede har adgang til, skal man fremsende en ny anmodning.

For samtlige fagsystemer skal ændringen følge forretningsgangsbeskrivelsen for det enkelte system. Forretningsgangen skal som minimum følge nedenstående overordnede procedure. Den til opgaven udpegede medarbejder udarbejder ændring om autorisation.

I HelpDesk-systemet skal den ansvarlige angive, at der er tale om en ændring. Marker eller tilføj de pågældende system og angiv profiler eller rettigheder, brugeren skal have ændret.

Autorisationsanmodningen sendes til godkendelse hos systemejer i de tilfælde hvor der er tvivl om autorisationens arbejdsbetingede berettigelse, for eksempel meget brede eller systemadministrative adgange.

Autorisationsanmodningen skal arkiveres i HelpDesk-systemet så længe medarbejderen er ansat i kommunen plus 1 år. Eventuel videre behandling er afhængig af, hvilken forretningsgang der findes for det enkelte område/system.Team Servicedesk og IT

3.1 Særlige forhold ved ændring

Der kan være tale om en generel ændring i adgangen til et system, som berører flere brugere. I disse tilfælde godkender systemejer en gang alle for ændringerne, hvorefter de iværksættes for alle berørte brugere.

Ved ændring af en medarbejders ansættelsesforhold eller jobindhold, skal der altid ske en vurdering af autorisationerne. Hvis en medarbejder skal have ændret sine autorisationer på grund af ændring af jobfunktion eller jobindhold, skal man også følge forretningsgangen vedrørende ændring. Her skal man altid sikre, at ændringen findes sted i fuld udstrækning på netop det tidspunkt, hvor rokeringen finder sted således, at det interne kontrolniveau ikke bliver svækket.
Den leder der er ansvarlig for ændringen er også ansvarlig for, at de systemmæssige adgange bliver vurderet.

4 Sletning af brugere

Når en fratrædelse bliver kendt, skal den fratrådte medarbejders adgang til systemer og netværk straks vurderes. Ud fra en konkret vurdering af systemejer, kan adgangen enten lukkes, reduceres eller forblive åben, indtil endelig fratrædelse finder sted.

For at sikre gennemførelse af forretningsgangen, skal **nærmeste chef** altid orientere Team Servicedesk og IT, når en opsigelse fra en it-bruger er modtaget eller en afskedigelse effektueret. Til formålet benyttes samme standard-autorisationsblanket, som ved oprettelse. Team Servicedesk og IT underrettes ved oprettelse af en sag i Ihelp.

5 Opfølgning på autorisationer

Alle ledere har pligt til at følge op på om deres medarbejdere fortsat har et arbejdsbetinget behov for adgang til de enkelte systemer. For systemer der behandler persondata gælder særligt skærpede regler.

De særlige kontroller af brugerrettigheder i systemer der behandler persondata henhold til Persondataloven fremgår af bilag 9.

Team Servicedesk og IT
Til sikring af, at brugere nedlægges rettidigt er der etableret en automatisk proces der dagligt udsøger brugere der ikke har anvendt sit logon. Processen fritager ikke den enkelte leder, at indberette fratrædelser og interne flytninger til Servicedesk.

6 Specielt om Team Servicedesk og ITs medarbejdere

Team Servicedesk og ITs medarbejdere kan på grund af deres arbejde være tildelt administratoradgange, der giver dem flere adgange end de almindelige brugere. Dette sker via en speciel konto.

Der skal derfor tages særlige forholdsregler, så det bliver sikret, at disse medarbejdere til stadighed udelukkende har adgang til systemer og data, som er arbejdsmæssigt begrundet.

Hvor it-medarbejdere har adgang til systemer med personfølsomme data skal der udtages stikprøver på medarbejderens opslag i disse systemer. Kontrollen skal udføres mindst halvårligt og dokumenteres.

Ajourføringshistorik (tidligere bilag B10-C3)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i Team Servicedesk og IT, herunder også generel omskrivning m.h.p. lettere tilgang for it-brugerne. Opbevaring af autorisationsblanket ændret.	13-11-2009 25.-01- 2010 14-06- 2010
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune på foranledning af IT-sikkerhedsudvalget	16-4-2014
Version 1.4	Opdateret af PBA/BDO	24-10-2017
Version 1.5	Opdateret af LLINN	13-06-2018

Bemærk: Et projekt vedr. brugerstyring er i analysefase i fællesskab med de øvrige kommuner i samarbejdet. Pilotprojektet skal være klar sommeren 2018. dataflow bestilles 1 sted og sættes i omløb hos de brugeransvarlige. Projektet er en delmængde af "Sammenhængende administrative opgaver". Projektnavn: Optimering af processer for brugerstyring. Projekt skal bla. Sørge for compliance til GDPR.

Bilag C	Retningslinjer for logning

Retningslinjer for logning har til formål at sikre, at der sker:

- Registrering af anvendelsen af systemer og data af hensyn til sporbarhed,
- Registrering af den systemmæssige drift af hensyn til driftsstabiliteten.
- Opfyldelse af gældende lovgivning

> Logning skal medvirke til at sikre en hensigtsmæssig og betryggende anvendelse af kommunens IT-systemer. Blandt andet opdages hændelige fejl, medarbejderne beskyttes mod uberettiget mistanke, uregelmæssigheder i system- og dataanvendelsen registreres og der defineres en entydig ansvarsplacering.

Bilaget beskriver dels rammerne for definition af et konkret logningsniveau for de enkelte systemer, dels rammerne for gennemgang af logningsmateriale samt afrapportering af resultatet.
Systemejerne har ansvaret for udarbejdelse af uddybende instrukser med henblik på fastsættelse af forretningsgang for registrering og kontrol i de enkelte systemer.

1 Logningsniveau

Niveauet for logning skal generelt defineres ud fra en vurdering af de enkelte systemer og datas væsentlighed for opgaveløsningen i kommunen. Desuden skal man ved vurderingen forholde sig til risikoen for uhensigtsmæssig anvendelse af systemer og data.

> I henhold til Persondataloven skal der foretages logning af alle handlinger, som vedrører fortrolige og personhenførbare oplysninger.

Da logning kun kan foretages i systemer, der driftsafvikles på kommunens servere eller systemer, der afvikles hos databehandler/systemleverandør, må pc'er ikke anvendes til arkivering af fortrolige og personhenførbare oplysninger. Personhenførbare oplysninger må dog gemmes på fællesdrev og bærbare enheder i sagsbehandlingsperioden, plus løbende 30 dage.

Af hensyn til dokumentation og eventuel efterforskning skal alle systemer, servere, arbejdsstationer og netværksudstyr tidssynkronisere med en fælles kilde.

For alle systemer, der indeholder et sikkerhedssystem, skal samtlige tilgængelige muligheder og faciliteter vurderes og som udgangspunkt implementeres. Der skal dog tages hensyn til omfanget af logningen samt systemernes driftssikkerhed, væsentlighed og performance.
Logningsmaterialet skal – hvis systemet muliggør dette – omfatte oplysninger om,

- hvem, der har foretaget en bestemt handling (brugerens ID),
- hvornår handlingen er foretaget (tidspunkt),
- hvad, der er foretaget (læst eller skrevet i en biblioteksti og/eller fil og/eller kartotek),
- hvilken person handlingen har vedrørt.

> Der skal foretages registrering af alle uautoriserede forsøg på adgang til fortrolige og personhenførbare oplysninger.

1.1 Systemer og applikationer

Logning af anvendelsen af systemer og applikationer, der driftsafvikles på Næstved Kommunes *eget udstyr* eller hos databehandler/systemleverandør skal ske via de indbyggede sikkerhedsmoduler.

> Fokus skal være på nægtet adgang, hvor brugeren har forsøgt adgang til systemer og data, som den pågældende ikke er autoriseret til.

I tilfælde, hvor der ikke er et sikkerhedssystem til rådighed, skal logningen ske via netværksoperativsystemet.

Afhængig af det enkelte systems væsentlighed, kan der være behov for logning af hændelser direkte i databaserne, hvor ændringer i væsentlige tabeller eller felter skal være underlagt konstant logning og overvågning.

Desuden skal lovgivningens krav til logning af personhenførbare oplysninger overholdes. Systemejerne har ansvaret for definition af logningsniveau samt gennemgang af logs, mens den tekniske opsætning foretages af Team Servicedesk og IT eller finder sted hos databehandler/systemleverandør.

1.2 Netværksoperativsystem

Der skal via netværksoperativsystemet og IT-systemernes fælles indbyggede sikkerhedsmoduler, føres kontrol med brugernes adgang eller forsøg på adgang til filer og data.

Fokus skal være på nægtet adgang, hvor brugeren har forsøgt adgang til filer og data, som brugeren ikke er autoriseret til.

.

Logningen opdeles administrativt i to dele:

- Del 1 omfatter kontrol med IT-driften, hvor der fokuseres på den centrale sikkerhed og performance i systemet. Denne del defineres af Team Servicedesk og IT.
- Del 2 omfatter kontrol med anvendelsen af systemer og data. Denne del defineres af systemejerne.

Særlige aftaler om logning i netværksoperativsystemerne skal fremgå af en eventuel indgået Service Level Agreement (SLA).

1.3 Logning af eksterne leverandører

Der kan være behov for, at eksterne leverandører eller andre samarbejdspartnere skal have adgang til Næstved Kommunes IT-systemer. Der kan blandt andet være tale om online-support fra en ekstern lokation.
Der skal føres kontrol med leverandørers adgang til, samt handlinger i, de pågældende systemer. Ved anvendelse af online-support, skal der tillige foretages logning via det anvendte kommunikationsudstyr.

Ansvaret for definition, opsætning og gennemgang følger afsnit 1.1 – 1.2 ovenfor. Vedrørende kommunikationsudstyr har Team Servicedesk og IT det fulde ansvar.

Systemtekniske sikkerhedsforanstaltninger for eksterne leverandører er også behandlet i systemtekniske bilag A-J.

2 Gennemgang af logs samt afrapportering

2.1 Gennemgang

Ansvaret for gennemgang af logningsmateriale følger ansvaret for definition af logningsniveau.

Der kan optræde registreringer i logningsmaterialet, som kræver nærmere undersøgelse. I nødvendigt omfang tages kontakt til brugeren eller andre interessenter for en afklaring.
IT-medarbejderne kan have adgang til manipulation med logningsmateriale. Der skal således i nødvendigt omfang ske begrænsning af denne mulighed. Hvor it-medarbejdere har adgang til

systemer med personfølsomme data skal der udtages stikprøver på medarbejderens opslag i disse systemer. Kontrollen skal udføres mindst halvårligt og dokumenteres.

2.2 Afrapportering

For systemer med personhenførbare oplysninger, skal der genereres en benyttelsesstatistik, som efter behov kan udskrives på papir eller til elektronisk medie. Denne skal indeholde information om den enkelte bruger, herunder

- hvilke transaktioner brugeren har anvendt eller forsøgt at anvende,
- antallet af gange den enkelte transaktion er anvendt eller forsøgt anvendt.

Det er systemejerne der beslutter forretningsgang for håndtering af benyttelsesstatistik, herunder eventuelle kontrolhandlinger. Forretningsgangen har udgangspunkt i systemernes væsentlighed og er beskrevet i uddybende instrukser for de enkelte systemer.

2.3 Arkivering

Logningsmateriale skal normalt gemmes ½ år således, at der blandt andet er mulighed for at følge tendenser og mønstre samt foretage opfølgning.
For særlige systemer kan lovgivningen kræve, at logningsmateriale gemmes i kortere eller længere perioder.
Dokumentation for gennemgang og afrapportering, skal gemmes i mindst 5 år.
Hvis der er særlige krav til arkivering af logningsmateriale og dokumentation for gennemgang, er det beskrevet i uddybende instrukser for de enkelte systemer.

Ajourføringshistorik (tidligere bilag B11-C4)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02- 2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilføjelse i afsnit 2.1 om at kontrollen skal dokumenteres.	25-01- 2010 14-06- 2010
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af: PBA/BDO	23-11-2017
Version 1.4	Opdateret af LLINN	13-06-2018

Bilag D	IT-beredskabsplan

IT-beredskabsplanen er underlagt både Næstved Kommunes IT-sikkerhedspolitik og Beredskabspolitik.

> Næstved Kommunes IT-beredskabsplan indeholder en overordnet beskrivelse af nødberedskabet på IT-området.

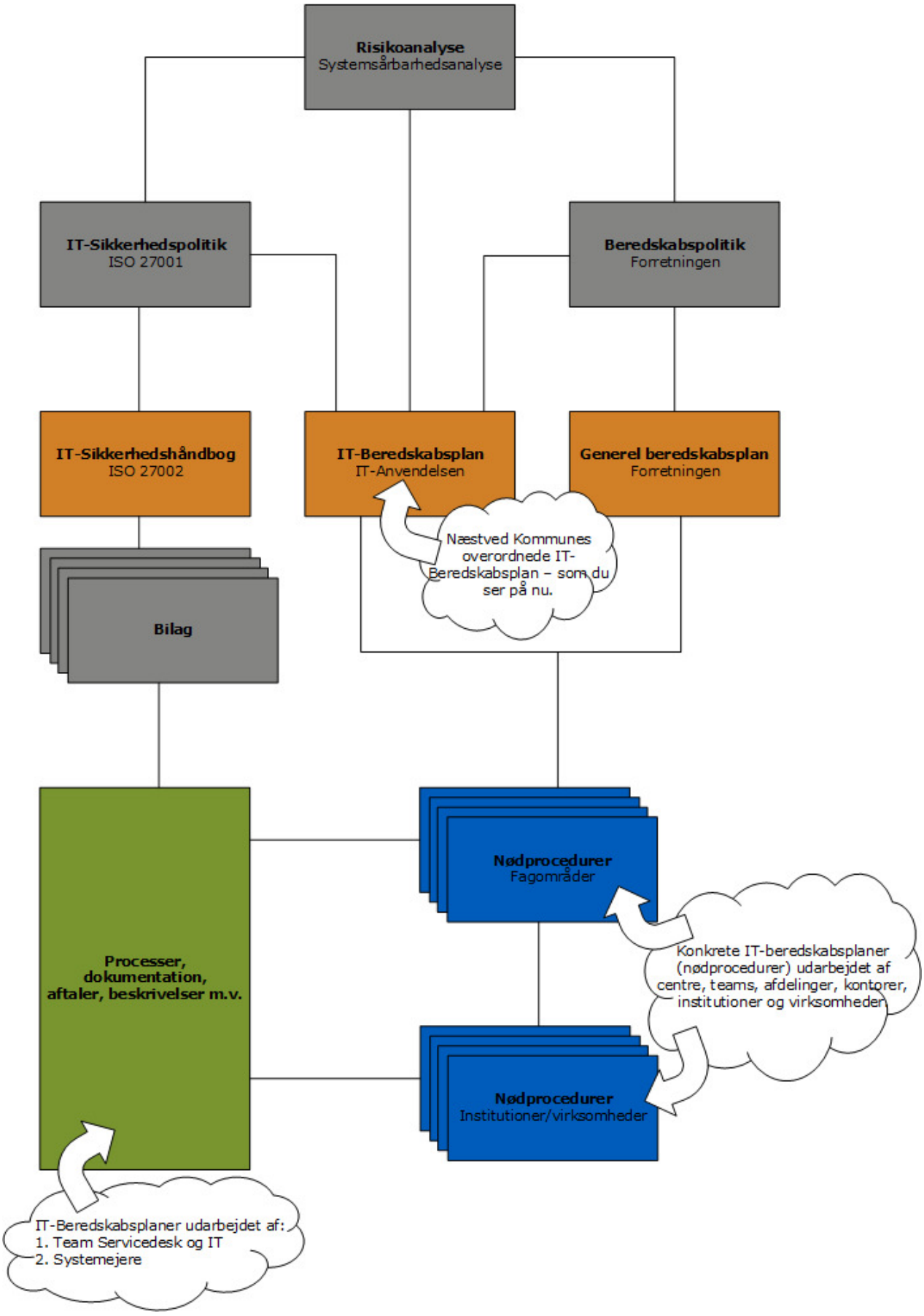
Den overordnede IT-beredskabsplan skal konkretiseres i detaljerede IT-beredskabsplaner på følgende tre områder:

1. **Team Servicedesk og IT** udarbejder og vedligeholder en beredskabsplan for driften af Næstved Kommunes IT-miljø (IT-systemer, netværk, telefoni, servere, backup o.s.v.) med fokus på de væsentligste IT-funktioner i Næstved Kommune.

2. **Systemejerne** udarbejder og vedligeholder en overordnet beredskabsplan for de(t) konkret(e) IT-system(r), som de er ansvarlige for.

3. **Centre, afdelinger, kontorer, institutioner og virksomheder** udarbejder og vedligeholder en plan for eget beredskab herunder også for deres væsentlige IT-funktioner. Beredskabsplanerne på IT-området skal indeholde konkrete instrukser for, hvordan det enkelte område vil sikre sig *før,* og hvad det skal gøre *under og efter* et eventuelt nedbrud.

På oversigtstegningen nedenfor kan du se, hvor IT-beredskabsplanen, som du sidder og læser nu, er placeret og hvor de mere konkrete IT-beredskabsplaner er placeret i den store sammenhæng.


Risikoanalyse
Systemsårbarhedsanalyse
IT-Sikkerhedspolitik
ISO 27001
Beredskabspolitik
Forretningen
IT-Sikkerhedshåndbog
ISO 27002
IT-Beredskabsplan
IT-Anvendelsen
Generel beredskabsplan
Forretningen
Næstved Kommunes overordnede IT-Beredskabsplan – som du ser på nu.
Bilag
Processer, dokumentation, aftaler, beskrivelser m.v.
Nødprocedurer
Fagområder
Konkrete IT-beredskabsplaner (nødprocedurer) udarbejdet af centre, teams, afdelinger, kontorer, institutioner og virksomheder
Nødprocedurer
Institutioner/virksomheder
IT-Beredskabsplaner udarbejdet af:
1. Team Servicedesk og IT
2. Systemejere

1 Indledning

IT-systemerne i Næstved Kommune danner baggrund for store dele af kommunens opgaveløsning og er medvirkende til, at effektivisere forretningsgange og skabe et dynamisk workflow.
Samtidig er en række forretningsgange og en stor del af kommunens opgaveløsning, afhængig af velfungerende IT-værktøjer. Selv et mindre nedbrud kan derfor have store konsekvenser.

IT-beredskabsplanen for IT-anvendelsen skal skabe sikkerhed for, at Næstved Kommune kan genskabe en normal driftssituation hurtigt, sikkert og i prioriteret rækkefølge. Endvidere skal relevante dele af nødberedskabet kommunikeres ud til kommunens IT-brugere således, at der er synlighed omkring det IT-sikkerhedsniveau, som er etableret.

Konsekvensen af ikke at have et beredskab kan være, at opgaverne ikke kan løses med deraf følgende økonomiske konsekvenser, juridiske konsekvenser, tab af omdømme med videre.

> I en politisk styret organisation vil det i sidste ende være et spørgsmål om tab af tillid. Derfor vil *risikostyring* og *damage control* være af central betydning i forbindelse med fastsættelse af et nødberedskab.

I Næstved Kommune har IT-sikkerheden høj prioritet. Det er dog ikke realistisk, at opnå 100% sikkerhed i forhold til alle de risici, der eksisterer i relation til kommunens IT-anvendelse. Der er derfor en risiko for, at det - trods forebyggende foranstaltninger - kan gå galt.

IT-beredskabet skal ses som en korrigerende foranstaltning, som skal følges, hvis det alligevel går galt. Målet med IT-beredskabet er således, at sikre rationel og effektiv handling i katastrofesituationer eller andre nødsituationer.
Hændelser kan variere fra brand, oversvømmelse eller strømsvigt, over tekniske systemnedbrud, til tilfældig hacking eller politisk motiverede angreb.

2 Formål

IT-beredskabsplanen har til formål at sikre den fortsatte varetagelse af kommunens væsentlige forretningsprocesser i en nødsituation, hvor der kræves mere end almindelig problemløsning.

> Da der aldrig kan tages højde for alle tænkelige situationer, vil kommunens nødberedskab forholde sig til en realistisk "i værste tilfælde-situation".

For at sikre at IT-beredskabsplanen har rette fokus, skal der ,som ved alle *forsikringsaftaler*, foretages en vurdering af prisen for beredskabet i forhold til skadens sandsynlighed og skadens effekt på organisationens funktionalitet og dermed kommunens ydelser.

Målet er at kunne videreføre væsentlige forretningsprocesser indenfor en given tidsperiode i kontrolleret rækkefølge.

Et katastrofeforløb kan skitseres ved 7 faser:

1) Mulighed for katastrofescenarie, forhøjet beredskab.
2) Katastrofen opstår, identifikation.
3) Katastrofeberedskabet initieres.
4) Katastrofen håndteres, "gør det vigtigste først".
5) Katastrofesituationen stabiliseres.
6) Katastrofen afsluttes, normalsituation.
7) Katastrofen og beredskabet evalueres.

2.1 Afgrænsning

Reetablering af forretningsprocesser - hvor IT-systemerne indgår - er ikke omfattet af Team Servicedesk og ITs IT-beredskab, der alene består i at få netværk, IT-systemer o.s.v. tilbage til normal drift i prioriteret rækkefølge.
Systemejerne har ansvaret for, at reetablering af de generelle/overordnede processer på betryggende vis og de enkelte organisatoriske enheder har ansvaret for reetablering af deres lokale processer og at følge deres manuelle nødberedskab ved manglende adgang til IT-systemer, netværk o.s.v.

2.2 Målgruppe

IT-beredskabsplanen for IT-anvendelsen er målrettet de medarbejdere, som enten har det overordnede ansvar for, at opgaverne bliver løst eller som varetager den konkrete opgaveløsning:

- Ledelsen - direktionen, systemejere og forretningsledelser.
- IT-chefen.
- IT-sikkerhedskoordinatoren.
- IT-medarbejderne.
- Informationsmedarbejderne - i forhold til borgere og medarbejdere.
- De opgaveansvarlige - IT-medarbejdere og andre medarbejdere, som løser opgaver i forlængelse af IT-beredskabsplanen.
- Beredskabschefen - har ansvaret for opgaveløsningen i overensstemmelse med kommunens beredskabsplan.

2.3 Forudsætninger

Det er en forudsætning, at krav og procedurer defineret i kommunens IT-sikkerhedspolitik, IT-sikkerhedshåndbog og bilag samt andet relevant materiale, bliver efterlevet. Eksempelvis forudsætter reetablering af IT-driften, at procedurerne for sikkerhedskopiering til enhver tid bliver efterlevet.

3 Kommunikation jf. den generelle beredskabsplan for Næstved Kommune

Under unormale forhold vil der være behov for en hurtig og enslydende information til kommunens ansatte, borgere med flere.

Væsentlige nedbrud og uregelmæssigheder på systemer kommunikeres i det omfang det er muligt på ERNA.

Læs den fulde tekst vedrørende kommunikation i den generelle beredskabsplan for Næstved Kommune.
https://nstvedkommune1.saas.neupart.com/authenticate?redirectto=/main/security/redirect

OBS. Midlertidig URL

4 Risikoanalyse

4.1 Overordnede risici

Overordnede risici og trusselsscenarioer, der kan true kommunens IT-systemer, kan være:

- Brande og eksplosionsulykker, nedbrænding af serverrum eller nedbrænding af andre væsentlige lokationer.
- Naturkatastrofer eller andre forhold, der kan medføre vandskader eller strømsvigt.
- Sikkerhedsbrud, som virus- og hackerangreb, der skader IT-anvendelsen.
- Tyveri af vitalt IT-udstyr.
- Terrorhandlinger der direkte eller indirekte skader IT-anvendelsen.

- Strømudfald, uanset årsagen.

I forbindelse med en uheldssituation eller et katastrofescenarie, er der mange koordinerende funktioner, som skal understøttes, primært for at begrænse skadens omfang og sekundært for at genskabe det oprindelige driftsmiljø. Den i situationen nedsatte kriseledelse har kompetencen til at varetage og tage hånd om sådan en nødsituation.

4.2 Trusselsvurdering i Næstved Kommune

Isoleret set vurderes Næstved Kommune ikke at være særlig udsat for målrettede trusler som eksempelvis terrorangreb.

En umiddelbar trusselsvurdering fokuserer i højere grad på problemer i forbindelse med længerevarende strømudfald eller længerevarende brud på kommunens kommunikationslinjer.

Hardware og software, som indgår i kommunens opgaveløsning, risikovurderes med baggrund i systemejernes tilkendegivelse om afhængigheder, omkostninger ved nedbrud med videre.

Med udgangspunkt i en sårbarheds- og afhængighedsvurdering opdeles alle systemer i 3 kategorier, efter en konkret prioritering. Prioriteringen finder sted efter aftale mellem systemejerne og IT-chefen. Efterfølgende indgår systemet i IT-beredskabsplanen med deraf følgende instrukser og vejledninger.

Systemejere skal desuden meddele ændringer i risikobilledet vedrørende det enkelte system til IT-sikkerhedskoordinatoren og sørger for ajourføring af de gældende IT-beredskabsplaner.

5 Ansvar og kompetence (Kriseledelse)

Næstved kommune har en krisestyringsorganisation, som består af ledere og eksperter fra de i situationen berørte centre, afdelinger, kontorer, institutioner og virksomheder.

Kriseledelsens opgave er, at træffe beslutninger og informere i den aktuelle situation på baggrund af instruks i kommunens IT-beredskabsplan for IT-anvendelsen.

Fremgangsmåden for sammensætning af en kriseledelse følger beskrivelsen i den generelle beredskabsplan, hvorfor der henvises til denne. Team Servicedesk og IT vil dog altid være repræsenteret, når der er IT involveret.

6 Prioritering af systemer og drift

6.1 Prioritering af kommunens systemer og driftsopgaver

For at undgå tvivl om det enkelte systems væsentlighed for kommunen, skal alle systemer være indplaceret i forhold til de forskellige prioriteringer, som er beskrevet nedenfor. Indplaceringen foretages med udgangspunkt i en sårbarheds- og afhængighedsvurdering i dialog mellem systemejere og Team Servicedesk og IT.

Systemerne inddeles i grupper med prioritet Guld, sølv og bronze. Der er for de væsentligste it-systemer udarbejdet Service Level Agreements (SLA), der omfatter forventninger til oppetid, reaktion på hændelser og reetablering.

Prioritet guld systemer dækker en række kerneopgaver og forretningsgange, der ikke kan udføres uden IT – eller kun kan udføres uden IT ved anvendelse af uforholdsmæssigt store ressourcer.
For disse systemer/forretningsområder skal der udarbejdes et nødberedskab, som – så vidt muligt – sikrer fortsat drift. Samtidig skal der beskrives manuelle forretningsgange, som kan medvirke til at minimere konsekvenserne ved et egentligt katastrofescenario eller et mere begrænset systemnedbrud.

Prioritet sølv systemer dækker en række opgaver og forretningsgange, der kan udføres uden IT i en kortere periode. Til sikring af opgaveløsningen, skal der derfor etableres et nødberedskab, der dels beskriver en kortvarig manuel forretningsgang, dels sikre fortsat drift af systemet efter en kortere periode.

Prioritet bronze systemer dækker en række opgaver og forretningsgange, der kan udføres manuelt – dog med nogen ulempe. Til sikring af opgaveløsningen, skal der etableres et nødberedskab, der dels beskriver en manuel forretningsgang og samtidig sikre fortsat drift af systemet efter en periode med manglende adgang til systemet.

Det vigtigste er i alle tilfælde at tage stilling til, hvor vigtigt det enkelte IT-system er. Hvis systemet ikke er vigtigt er beredskabet måske blot at afvente til systemet er i drift igen.

Team Servicedesk og IT vedligeholder en oversigt over alle systemer og deres prioriteringer. Systemejere og centre, der benytter et specifikt system er forpligtiget til at indberette eventuelle forhold, der kan ændre i den aktuelle prioritering.

6.2 Beskrivelse af driftsfaser

Med henblik på at sikre kommunens IT-driftsafvikling, er der defineret følgende 3 driftssituationer:

Nøddrift vil blive iværksat i forbindelse med et katastrofescenario, hvor kommunens IT-driftsafvikling vil blive skadet. Der skal øjeblikkeligt foretages en vurdering af kommunens fortsatte driftsafvikling og – i fornødent omfang – skal beredskabsplaner for berørte IT-systemer iværksættes.

Som udgangspunkt vil der være fokus på prioritet guld systemer, og dette *kan* betyde at driften af øvrige systemer stoppes midlertidig.

Reservedrift kan dels forekomme i forlængelse af nøddrift, indtil systemerne er i normal drift igen, eller i forbindelse med mindre nødsituationer, hvor det kun er dele af systemet, der rammes.

Når reservedrift er som følge af nøddrift, kan der i en kortere eller længere periode, forekomme forstyrrelser i den egentlige IT-driftsafvikling ligesom udviklings- og vedligeholdelsesopgaver sættes i bero. I forbindelse med mindre nødsituationer, kan der være behov for at etablere reservedrift, hvor dele af kommunens it-beredskab træder i kraft, hvilket kan betyde begrænset funktionalitet på berørte område.

Normaldrift er når IT-driftsafviklingen afvikles som planlagt.

7 Dokumentation, test og ajourføring af IT-beredskabsplaner

Dokumentation og opbevaring af IT-beredskabsplaner følger samme fremgangsmåde som for øvrige beredskabsplaner i Næstved kommune jf. den generelle beredskabsplan.

IT-beredskabsplanerne skal løbende afprøves – som minimum som ”skrivebordstest” – hvor man gennemgår hele forløbet uden dog at udføre det i praksis. Hyppighed besluttes af IT-sikkerhedsudvalget.

De mere tekniske test vil være beskrevet i Team Servicedesk og ITs IT-beredskabsplan.

IT-sikkerhedsudvalget kan udpege specielle områder, hvor IT-beredskabsplanerne skal gennemgås ellers testes.

IT-beredskabsplanerne skal ajourføres, når der sker ændringer, der påvirker disse. Dette kan være:

- Nye IT-systemer
- Tekniske eller organisatoriske ændringer
- Ændret risiko-billede i kommunen.

8 Evaluering af nødberedskab

Senest 14 dage efter afslutning af et eskaleret nødberedskab, skal der ske en evaluering af de indsatte beredskab. Dette er nærmere beskrevet i de enkelte IT-beredskabsplaner.

IT-sikkerhedskoordinatoren er ansvarlig for at evalueringen finder sted.

9 Uddannelse/information

Der skal sikres, at den nødvendige viden kan tilvejebringes i forbindelse med aktivering af beredskabet. Dette skal sammenholdes med aftaler med leverandører i det omfang, hvor disse skal involveres.

Relevante dele af nødberedskabet skal kommunikeres ud i organisationen, så ingen er i tvivl om, hvad de skal gøre, herunder hvem de skal kontakte. Dette finder sted på kommunens intranet.

Den overordnede beredskabsorganisation skal fremgå af Næstved Kommunes overordnede beredskabsplan.

For IT-medarbejderne vil IT-beredskabet være en del af den almindelige opgavevaretagelse.

Kommunens ledelse har pligt til, at gøre sig bekendt med de overordnede beredskabsplaner, ledelsen kan endvidere involveres i afprøvninger at it-beredskabsplanen.

Ajourføringshistorik (tidligere bilag A8-B9-C2)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer i hele kvalitetssikringsforløbet i Team Servicedesk og IT, herunder også generel omskrivning m.h.p. lettere tilgang for IT-brugerne. IT-sikkerhedskoordinatoren er fjernet fra afs. 4.2 og 6.1., tegning tydeliggjort, misvisende henvisning fjernet	05-10- 2009 11-17-2009 05-02-2010 24-02-2010 14-06-2010
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	23-04-2014
Version 1.4	Opdateret af PBA/BDO	11-01-2018
Version 1.5	Opdateret af LLINN	13-06-2018

Bilag E	Retningslinjer for IT-medarbejdere

Alle IT-medarbejdere i Næstved Kommunes IT-center

er underlagt nærværende retningslinjer.

Det er den enkelte IT-medarbejders ansvar, at retningslinjerne følges, og at administration, support og drift af IT-systemerne i kommunen generelt finder sted i overensstemmelse med god IT-skik. Herudover bør IT-medarbejderne - når det gælder IT-anvendelsen - også fremover være et eksempel til efterfølgelse.

1 Fysisk sikkerhed

IT-medarbejderne skal overholde og styrke den fysiske sikkerhed på IT-området. IT-medarbejderne skal således sikre, at alle tekniske installationer, som er relevante i forbindelse med IT-anvendelsen, overvåges på behørig vis således, at driftsforstyrrelser undgås.

IT-medarbejderne skal også sikre, at adgang til serverrum og prioriterede tekniske installationer overvåges således, at uvedkommende ikke kan opnå adgang. Dette skal blandt andet sikres ved, at dørene altid holdes lukket og låst.

2 Udskrivning

Ved udskrivning og specielt ved udskrivning af filer og kommandoer, som beskriver IT-sikkerhedsrelaterede aspekter - skal IT-medarbejderne sikre, at oplysningerne ikke bliver tilgængelige for uvedkommende.
Dette kan sikres ved, at der udelukkende anvendes printere, som er placeret i lokaler hvor kun IT-medarbejderne har adgang. Hvis der alligevel anvendes en almindelig tilgængelig printer, skal print straks fjernes således, at det ikke bliver tilgængeligt for uvedkommende.

3 Programanvendelse

For IT-medarbejderne i Næstved Kommune gælder de samme retningslinjer, som for kommunens øvrige medarbejdere. IT-medarbejderne skal råde over licenser til samtlige programmer der anvendes, også programmer som anvendes på forsøgs- og testbasis.
Endvidere har Team Servicedesk og IT som opgave, at forhandle og administrere licensaftaler for programmer, som anvendes af hele kommunen:

- Team Servicedesk og IT skal altid kunne tilbyde en række standard kontorprogrammer til varetagelse af kommunens forskelligartede opgaver.
- Team Servicedesk og IT skal være i stand til at dokumentere, at licensforholdene til standard kontorprogrammer er i orden.

4 Systemudvikling

Systemejere har ansvaret for, at der bliver indgået en aftale med Team Servicedesk og IT vedrørende sikkerheden i udviklede applikationer. De indgåede aftaler skal sikre, at der bliver etableret systemteknisk sikkerhed, herunder adgangskontrol og centralt opdateret sikkerhedskopiering samt at aftestning og idriftsættelse finder sted på betryggende vis.
Systemejere har selv ansvaret for den logiske sikkerhed, herunder forretningsgang vedrørende autorisation og logning. Endvidere har Systemejere ansvaret for udarbejdelse af præcis dokumentation.

Det skal sikres, at der findes en kopi af udviklede værktøjer, version 1.0 og det skal sikres, at ændringer i værktøjerne kun finder sted på baggrund af en konkret anmodning og kravspecifikation og at ændringer dokumenteres

og gemmes i sin oprindelige form. Opbevaring skal ske i Team Servicedesk og IT eller hos leverandøren, hvis systemet driftes decentralt.

5 Virussikkerhed

IT-medarbejderne har en stor kontaktflade til eksterne parter. Derfor skal man være ekstra agtpågivende ved anvendelse af filer og programmer, som er modtaget via internet og andre eksterne opkoblinger.

IT-medarbejderne har en forpligtigelse til at være ekstra forsigtige, ved altid at virusscanne indkomne filer, også selvom de ikke umiddelbart er forbundet med en risiko.

Viruskontrol skal i øvrigt finde sted i overensstemmelse med beskrivelsen i bilag B1, Retningslinjer for IT-brugere. Kommunens virusberedskab er beskrevet i bilag A4, Retningslinjer for virusberedskab.

6 IT-drift

Team Servicedesk og IT har ansvaret for, at systemer og relaterede data, altid er tilgængelige for kommunens medarbejdere. Samtidig skal det sikres, at Næstved Kommunes data er struktureret således, at der skabes mulighed for en opdeling, som er baseret på medarbejdernes organisatoriske tilknytning eller andre specifikke ansættelsesforhold.

Det skal sikres, at data og systemer ikke er tilgængelige for uvedkommende. Dette skal iværksættes ved anvendelse adgangskontroller, som udelukker ikke autoriserede IT-brugere.

Filtrering imod internet og øvrige interne som eksterne netværk, finder sted med firewall. Retningslinjer for administration af firewall fremgår i bilag A2.

For at opnå stabil og sikker drift af systemerne og samtidig sikre uafhængighed af enkelte IT-medarbejdere, skal der udarbejdes:

- Driftsdokumentation for netværk, herunder opsætning af overvågning, konfigurationsdokumenter, adgang til systemadministration og vedligeholdelse og service på hardware og software.
- Driftsdokumentation for servere, herunder konfigurationsdokumenter, adgang til systemadministration og vedligeholdelse og service på hardware og software.
- Driftsdokumentation for øvrigt udstyr, herunder printere, pc'er og andet. Dokumentationen skal blandt andet indeholde et generelt overblik over antal, placering, brugere og konfiguration.
- Uregelmæssigheder og fejl i IT-driften skal registreres således, at historikken kan komme Næstved Kommune til gavn, hvis eventuelle uregelmæssigheder og fejl gentager sig. Det er den enkelte it-medarbejders ansvar, at registrere fejl og hændelser i sagssystemet.

Driftsdokumentationen skal ajourføres i forbindelse med ændringer i konfigurationerne som en naturlig del af Change Management proceduren.
Driftsdokumentationen skal opbevares i Team Servicedesk og ITs database for driftsdokumentation og må kun være tilgængelig for medarbejdere med et reelt arbejdsbetinget behov. IT-chefen skal påse, at der til enhver tid foreligger tilstrækkelig driftsdokumentation for alle kommunens IT-driftmiljøer.

7 IT-support

For at afvikle en tilfredsstillende IT-support, skal det som minimum altid være muligt, at træffe en IT-medarbejder på telefon indenfor Næstved Kommunes normale kontortid.

Kontaktinformation, herunder telefonnumre og e-post adresser samt supporttidspunkter, skal dels være tilgængelige på kommunens intranet samt være udmeldt til kontaktpersoner i alle Centre, afdelinger og kommunale virksomheder.

7.1 Servicedesk

Support af kommunens netværk og standard kontorprogrammer, varetages af Team Servicedesk og IT. Ansvaret for support vedrørende de enkelte systemer og applikationer, er placeret hos systemejerne. De enkelte systemejere kan herefter vælge at foretage support selv eller indgå aftale med andre, herunder Team Servicedesk og IT. Som hovedregel anbefaler Team Servicedesk og IT, at der indgås en supportaftale.
Det skal sikres, at alle henvendelser registreres og fejlrettelser dokumenteres således, at løsninger eventuelt kan anvendes på et senere tidspunkt i tilsvarende situationer.

7.2 Servicevinduer

Servicevinduer er de perioder, hvor systemtilretning normalt finder sted og systemer derfor ikke er tilgængelige.
Servicevinduer skal altid være informeret til IT-brugerne.

7.3 Fjernovertagelse af pc'er

Der kan forekomme situationer, hvor der er behov for at fjernovertage en pc. Ved fjernovertagelsen bliver den pågældende bruger adviseret. Normalt skal brugeren samtidig godkende at der sker fjernovertagelse. Afhængig af værktøjet der anvendes, kan godkendelsen enten finde sted via e-mail eller telefon, eller pop up på skærm - eller vedkommende skal selv foretage opstart af fjernovertagelsessoftware på sin pc.

8 Administratoradgang

I forbindelse med administration og support af Næstved Kommunes IT-systemer, tildeles IT-medarbejderne forskellige administratorrettigheder. Udover systemadministrator til netværksoperativsystemer samt kommunens firewalls, anvendes tillige administratorrettigheder til kommunens forskellige applikationer og systemer.
Alle administrator-brugerprofiler er personlige, og der anvendes således ikke fælles administratorbrugere.
For at undgå fejl eller uheld i forbindelse med misbrug, er der defineret følgende konkrete regler for tildeling og anvendelse af administratorrettigheder, X-konti:

Alle oprettelser af X-konti skal følge nedenstående procedure.

1. Det identificeres hvem der skal have X-konto

2. Der oprettes en opgave i opgavesystemet med angivelse af hvem der skal have adgang, til hvad og hvor længe
   Opgaven er alene til orientering og dokumentering

3. Opgaven skal oprettes med Teamchefen som opgavestiller

4. Opgaven er præautoriseret og kan derfor udføres og afsluttes

5. I ADs tekstfelt anføres det sagsnummer som oprettelsen af X-kontoen er oprettet i

8.1 Tildeling af administratoradgang

IT-medarbejderne tildeles administratoradgang i overensstemmelse med den enkeltes konkrete behov. Tildelingen af adgangen er strengt personlig og må ikke deles med andre.

- IT-chefen - eller delegeret - vurderer og godkender hvem der har administratoradgang til kommunens servere, netværk, firewall m.m.
- Systemejerne godkender, hvem der har administratoradgang til systemer og applikationer.

Da administratoradgang giver den enkelte IT-medarbejder udvidede beføjelser i forhold til kommunens IT-anvendelse, skal adgangen reguleres efter følgende kriterier:
Hvis en IT-medarbejder fratræder sin stilling, vil den pågældende medarbejder blive frataget administratoradgang, når Team Servicedesk og IT får kendskab til den pågældende fratrædelse.
Den enkelte IT-medarbejders status i opsigelsesperioden vil afhænge af en konkret vurdering. Den enkelte vil dermed have mulighed for at fortsætte beskæftigelsen i opsigelsesperioden.

Der skal mindst 1 gang årligt udsendes et autorisationsdokument til systemejerne på it-medarbejdere med systemadministratorrettigheder i fagsystemerne. Autorisationsdokumentet skal angive hvilket niveau administratorrettigheden er givet fx brugeradministration eller fuld systemadministration mv.

Når en medarbejder, som har haft administratoradgang fratræder sin stilling, skal alle system- og administratorpasswords skiftes omgående.

8.2 Anvendelse af administratoradgang

IT-medarbejderne skal sikre, at uvedkommende ikke opnår administratoradgang. Når administratoradgangen ikke anvendes, skal der altid være logget af systemet således, at risikoen for fejl og uhensigtsmæssigheder i systemerne minimeres.
Chefer og ledere bør ikke kende administratorpasswords, med mindre der er tale om systemer, som de pågældende chefer og ledere selv administrerer.
I stedet skal alle systempasswords til de centrale servere og systemer, opbevares i et password repository. Dermed kan andre IT-medarbejdere til enhver tid - hvis den daglige administrator er indisponibel - opnå administratoradgang til systemerne. Adgang til repository skal logges og adgangens berettigelse skal dokumenteres i sagsstyringssystemet.

8.3 Eksterne administratorbrugere

I forbindelse med online-support fra systemleverandører skal det tilstræbes, at systemleverandører udelukkende tildeles administratoradgang til det relevante system eller applikation.
Hvis det er netoperativsystemet, som skal serviceres, bør de anvendte passwords ændres i det pågældende tidsrum således, at udenforstående ikke opnår kendskab til Næstved Kommunes generelle passwordstruktur.
Leverandørens administratoradgang skal lukkes umiddelbart efter at leverandøren har afsluttet den opgave der krævede administratoradgang.
Der føres log over tildeling af administratoradgang til eksterne brugere. Loggen skal som minimum indeholde oversigt over tidspunkt for åbning og for lukning af administratoradgang samt hvilke system/systemer der blev givet adgang til. Endvidere skal logføres opgavens art.
Loggen administreres af Team Servicedesk og IT og kontrolleres ad-hoc af IT-sikkerhedskoordinatoren.

8.4 Distance pc'er og bærbare pc'er

Som det er beskrevet i bilag B4 og B5, Retningslinjer for distance- og politiker pc'er og Retningslinjer for bærbare enheder, gælder principielt de samme retningslinjer, som for kommunens almindelige pc-arbejdspladser.

Da IT-medarbejderne har administratorrettigheder i de forskellige systemer, skal der vises ekstra agtpågivenhed ved anvendelse af disse rettigheder fra distance pc'er samt bærbare enheder. Næstved Kommunes pc'er, som anvendes på IT-medarbejdernes private bopæl eller andre lokationer, må ikke anvendes af andre personer end IT-medarbejderne.

Ajourføringshistorik (tidligere bilag A1)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer fra IT-ledelsen. Opdateret af: JJ/Næstved Kommune Præcisering af at det er IT-medarbejdere i IT-centret og anbefaling om support-aftaler	09-11-2009 14-06-2009
Endelig Version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	22-04-2014
Version 1.4	Opdateret af PBA/BDO	18-01-2018
Version 1.5	Opdateret af LLINN	13-06-2018

Bilag F	Retningslinjer for administration af firewall

For at sikre Næstved Kommunes netværk imod uautoriseret adgang, er der etableret flere firewalls til filtrering af trafikken imellem kommunens netværk og andre netværk, herunder internet.

Kommunens firewall-administratorer varetager opsætning af firewall med henblik på sikring af stabil og sikker drift. IT-chefen har ansvaret for, at sikkerheden i kommunens firewall lever op til retningslinjerne i dette bilag.

1 Konfiguration af firewall

Ændringer og justeringer i opsætningen foretages af kommunens firewalladministratorer, som er ansvarlige overfor IT-chefen med hensyn til administration af firewall og håndtering af netværkssikkerheden. Opgaven kan løses i samarbejde med andre medarbejdere fra Team Servicedesk og IT.

Ændringer i opsætningen finder kun sted i forbindelse med en præcis kravspecifikation. Det bliver endvidere kontrolleret løbende, at firewall har den ønskede filtrering og ikke er hverken for åben eller for lukket.

> Håndteringen af firewall er restriktiv. Der åbnes kun for et minimum af porte og services og først efter, at der er foretaget en konkret risikovurdering af, hvilke konsekvenser det vil medføre.
> Alt er forbudt medmindre, det er eksplicit tilladt.

Ændringer til firewallens filtreringsregler oprettes i sagsstyringssystemet og dokumenteres ved angivelse af sagsnummer fra sagsstyringssystemet i reglens beskrivelsesfelt. Konfigurationen skal gemmes i et passende antal generationer med henblik på fallback og auditering.
IT-chefen har ansvaret for, at kommunens firewall løsning er i overensstemmelse med det aktuelle trusselsbillede.

2 Overvågning af firewall

Der foretages overvågning således, at den aktuelle drift af firewall monitoreres. Dermed sikres optimal stabilitet og optimal performance. Endvidere sikres det, at uregelmæssigheder og indbrudsforsøg håndteres straks, når de opdages.
IT-Teknisk chef har ansvaret for, at firewall overvåges med udgangspunkt i en fast plan. Uregelmæssigheder i driften skal fremgå af en driftslog, som ikke må være tilgængelig for uvedkommende.

Følgende handlinger skal sikre kommunens netværk:

- Ved driftstop lukker firewall for trafikken til Næstved Kommunes netværk - såkaldt "closed on failure" funktionalitet.
- Gentagne uregelmæssigheder informeres til IT-Tekniskchef og IT-sikkerhedskoordinatoren.
- Firewall skal konfigureres med passende alarmer, som sikrer, at firewalladministratorerne straks orienteres ved særligt kritiske hændelser. Alarm vil normalt finde sted i (firewallens management konsol) form af (e-mail til administratorerne).

Opsætning af alarmer skal dokumenteres i driftsdokumentationen.

Der træffes aftale med ekstern leverandør vedrørende afprøvning af firewallfunktionalitet. Denne afprøvning skal finde sted i et aftalt servicevindue mindst en gang om året i juli måned.

3 Logning af anvendelsen

Udover den aktuelle overvågning, skal kommunens firewall generere et logmateriale. Loggen skal sikre et overblik over de handlinger, der er sket på firewall i løbet af en længere periode.

Indsamling og behandling af information fra loggen skal være systematisk og finde sted med passende intervaller.

For at sikre muligheden for at samle information om firewallfiltrering igennem en passende periode, skal der allokeres tilstrækkelig diskplads til, at firewall kan opbevare logoplysninger i ca. 30 dage dog mindst 1 uge. Dermed har Næstved Kommune mulighed for, at lokalisere angrebsmønstre og andre tilbagevendende uregelmæssigheder i adgangen til netværket.

Som dokumentation for firewalls filtrering og anvendelse, kan der efter behov udtrækkes logoplysninger i klar tekst.

IT-chefen har ansvaret for, at logning finder sted i overensstemmelse med retningslinjerne. Som udgangspunkt logges afviste forsøg til og fra internettet. Log på enkelte firewallfiltre kan efter behov etableres, fx ved mistanke om misbrug.

4 Dokumentation

Det skal sikres, at dokumentation vedrørende kommunens firewall ajourføres og opbevares på et sikkert sted. Der skal opbevares dokumentation for følgende forhold:

- Dokumentation for den aktuelle konfiguration.
- Dokumentation for væsentlige ændringer, jf. Change Management proceduren.
- Dokumentation for logning.
- Driftslog, herunder dokumentation for uregelmæssigheder.
- Dokumentation for test af firewallfunktionalitet.

Dokumentationen skal have en fast defineret struktur og opbygning, og følge Næstved Kommunes standard på området.
IT-chefen har ansvaret for, at dokumentation opbevares betryggende og til enhver tid er tilgængelig.

5 Eksterne forbindelser

Alle eksterne forbindelser skal ske via kommunens centrale firewall, med mindre der er særligt vigtige grunde til at etablere alternative løsninger.

Hvis der etableres eksterne forbindelser, som ikke går igennem kommunens centrale firewall, skal der være etableret funktionalitet med tilsvarende høj sikkerhed.

Det er således ikke tilladt at installere analoge modems eller ADSL forbindelser, uden at Team Servicedesk og IT har risikovurderet og godkendt sikkerheden i løsningen. Installation af dataforbindelser skal følge Team Servicedesk og IT's formelle ændringsstyringsprocedure.

Team Servicedesk og IT skal godkende alle eksterne forbindelser skriftligt.

Der skal vedligeholdes en central oversigt over alle eksterne forbindelser og kommunikationslinjer.

Ajourføringshistorik (tidligere bilag A2)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer IT-ledelsen.	09-11-2009 04-02-2010

Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af: PBA/BDO	11-01-2018
Version 1.4	Opdateret af LLINN	13-06-2018

Bilag G	Retningslinjer for backup

For at sikre, at medarbejdere i Næstved Kommune, til enhver tid, har adgang til centralt lagrede data, er der udarbejdet retningslinjer for backup.

Bilag G beskriver Team Servicedesk og ITs opgaver og ansvar i forbindelse med backup.

1 Team Servicedesk og ITs opgaver og ansvar

Team Servicedesk og IT skal sikre, at der dagligt foretages backup af alle databærende servere i Næstved Kommune. For servere, hvor indholdet ikke tilføres daglige ændringer, herunder gateways, printservere og andet dedikeret udstyr, kan der tages backup længere intervaller.

> Det er Team Servicedesk og ITs ansvar, at der på ethvert givet tidspunkt er foretaget backup af servere i Næstved Kommunes således, at der højst kan mistes en dags arbejde.

Team Servicedesk og IT skal vedligeholde oversigter over eksisterende backups således, at der indenfor et fastlagt tidsrum, til enhver tid, kan reetableres data fra en backup.

Team Servicedesk og IT skal sikre, at alle nye servere får etableret backup. Omfanget af backup skal fremgå af kravspecifikationen eller af Change Management dokumentationen.

Backup af data fra kommunens servere er outsourcet til en it-serviceleverandør. Team Servicedesk og IT skal gennem stikprøver overvåge, at serviceleverandøren yder den aftalte service. Endvidere skal den årlige revisorerklæring fra serviceleverandøren indhentes og vurderes.

2 Procedure for backup

Backup skal finde sted i et ubrudt forløb således, at data kan reetableres mindst 90 dage tilbage for almindelige filer og 15 dage for databasefiler. Dette kan enten være tilrettelagt efter princippet om dag, uge og månedskopier eller det kan tilrettelægges efter et princip, hvor der gemmes et nærmere defineret antal versioner af filer og databaser.

Logmateriale skal gemmes i overensstemmelse med lovkravene indenfor de respektive systemer. For anvendelseslog og transaktionslog i systemer der behandler personoplysninger gælder reglen, at disse ikke må gemmes i mere end 6 måneder.

Kommunen skal råde over beskrivelse af forretningsgang for backup.

Brugere af distance- og politiker pc'ere, der undtagelsesvis arbejder lokalt, skal overføre dokumenter, regneark og andre filer til servernes fællesdrev på citrix, så der kan tages backup af data via netværket.

3 Opbevaring og adgang til backup

Opbevaring af backup skal imødegå, at data mistes ved brand, oversvømmelse, tyveri eller uheld. I Næstved Kommune er backup outsourcet til en it-serviceleverandør. Backup af data skal kunne gendannes i op til 90 dage.
Team Servicedesk og IT har ansvaret for, at kun medarbejdere eller andre med tjenstligt behov, har adgang til backups.

4 Reetablering af data

Team Servicedesk og IT håndterer normalt reetablering af data. Alternativt kan it-serviceleverandøren stå for gendannelse.

Reetablering skal testes for de mest kritiske systemer således, at der er sikkerhed for, at indhold på backups er i overensstemmelse med forventningerne. Samtidig sikrer test, at funktionalitet i forbindelse med restorefunktionen, er kendt af de ansvarlige medarbejdere. Test skal finde sted med passende intervaller - mindst en gang om året. For mindre kritiske systemer og filservere anses den løbende gendannelse af enkeltfiler og mapper for, at være dækkende. Team Servicedesk og IT har ansvaret for, at forretningsgang vedrørende reetablering bliver udarbejdet. Endvidere har Team Servicedesk og IT ansvaret for, at test finder sted i overensstemmelse med de fastsatte retningslinjer.

Ajourføringshistorik (tidligere bilag A3)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer fra IT-ledelsen. Sætning, der også fremgår i IT-sikkerhedspolitikken er fjernet – så det ikke er dobbelt.	09-11-2009 04-02-2010 14-06-2010
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Ajourført af: PBA/BDO	11-01-2018
Version 1.4	Opdateret af LLINN	13-06-2018

Bilag H	Retningslinjer for virusberedskab

Virus og orme er programstumper, som finder et program eller et dokument at knytte sig til, i princippet en ekstra - uheldig eller skadelig - funktion. Når programmet aktiveres eller dokumentet åbnes, aktiveres den nye "funktion" og kan samtidig smitte andre programmer og sprede sig via netværket.

De alvorligste vira kan slette oplysningerne på harddisken eller forvanske oplysninger, mens andre vira kan være humoristiske indslag. Smitten kan komme til Næstved Kommunes netværk via e-mail, via opslag på internet eller via eksterne datamedier.

Det er derfor afgørende, at virus - og beskyttelse imod virus - tages alvorligt.

Den tekniske beskyttelse via antivirusprogrammel skal være vel tilrettelagt, ligesom medarbejderne skal udvise agtpågivenhed, ved anvendelse af e-mail, internet og eksterne datamedier.

For at sikre en ensartet og hensigtsmæssig administration af kommunens virusberedskab, beskriver bilag A4 retningslinjer for it-medarbejdernes opgaver og ansvar i forbindelse med håndtering af virus og tilrettelæggelse af et betryggende virusberedskab.

Retningslinjer for virusberedskab på IT-brugerniveau er beskrevet i bilag B1, Retningslinjer for IT-brugere.

Der er beskrevet nærmere information om virus og andre skadelige programmer på intranettet.
http://erna/Praktisk/It_og_telefoni/It_sikkerhed/Antivirusforanstaltninger.aspx

1 Antivirusprogram

Som antivirusprogram anvender Næstved Kommune anbefalede og ledende antivirusprodukter.

Der er etableret virusbeskyttelse på samtlige pc'er på netværket, idet der installeres antivirusprogrammer på alle pc'er i forbindelse med basisinstallation.

På alle pc'er er der etableret automatisk opdatering af signaturfiler og sikkerhedspakker.

2 Antispyware

Udover truslen fra traditionel virus, er der opstået en øget trussel fra såkaldt spyware.
Spyware har normalt følgende karakteristika:

- Ændrer pc'ens opsætning.
- Distribuerer reklamer - sædvanligvis i stort omfang.
- Indsamler personlige informationer fra pc'er og kan distribuere dem via internet.
- Nedsætter pc'ens hastighed og forlænger svartider.

Som supplement til de traditionelle antivirusprogrammer, skal kommunen derfor altid råde over opdateret antispyware.
Håndtering af antispyware følger håndteringen af det traditionelle virusberedskab. Team Servicedesk og IT varetager denne opgave.

3 Opdagelse af virus

Opdagelse af virus kan finde sted på pc eller server.

3.1 Opdagelse af virus på pc

Hvis en bruger åbner en fil eller et program på sin pc, som er inficeret med en virus, vil antivirusprogrammet normalt opdage den pågældende virus, og enten reparere filen eller afvise at åbne den.

3.2 Opdagelse af virus på server

En virus, der spredes via internet, vil oftest blive fanget på serveren, allerede inden den når til pc'en og Team Servicedesk og IT bliver dermed orienteret om angrebet og kan foretage de fornødne handlinger.

De ansvarlige IT-medarbejdere skal i hvert enkelt tilfælde vurdere, om der skal foretages yderligere handlinger med henblik på beskyttelse af netværket og IT-systemerne mod eksterne trusler.

Yderligere handlinger kan være:

- Afbrydelse af forbindelsen til internet, hvis det vurderes, at kunne fjerne risikoen for et potentielt angreb.
- Dialog med de pågældende brugere, som har været modtagere af de inficerede filer eller programmer.
- Orientering af afsender af virus, hvis det er sporbart.
- Orientering af kommunens ledelse, som eventuelt kan foretage retlige handlinger eller politianmeldelser i forhold til afsender af virus, hvis dette er sporbart.
- Information af brugerne, hvis netværk eller systemer rammes af en virus, som man ikke er beskyttet imod.
- Logning af væsentlige observerede virusangreb og tiltag i den forbindelse.

4 Handlinger ved generelle virusalarmer

Der er mange eksempler på generelle virusalarmer, som har til formål, at forberede IT-brugere og IT-medarbejdere over hele verden på, at der er en virus på vej.

Den type alarmer er ikke altid reelle og skal vurderes kritisk.

Når der udsendes en virusalarm kan der være flere årsager:

- Virus bliver lokaliseret, og der udsendes en reel advarsel således, at der kan tages forholdsregler. Samtidig vil leverandører af antivirusprogrammer komme med en opdatering af deres værktøjer.
- Afsender af virus er interesseret i opmærksomhed og påpeger derfor huller i eksisterende programmer eller styresystemer frem for afsendelse af virus.
- Afsender af alarmen bruger dette middel som alternativ til en virus, da alarmen i sig selv allokerer store mængder båndbredde og tidsressourcer og derfor kan være et problem af samme omfang som en rigtig virus.

5 Handlinger ved inficering af virus

Hvis uheldet først er ude og systemer og/eller netværk er blevet inficeret med virus, er der flere forholdsregler som skal tages, for at minimere skadens omfang. Forholdsreglerne skal afpasses i forhold til den pågældende virus og skal finde sted efter en nærmere analyse af virustypen og eventuelt i dialog med hardware og/eller programleverandør:

- Virus skal så vidt muligt isoleres fra den øvrige del af netværket. Herefter kan udbedring af skaden finde sted.
- Hvis virus observeres på en server, vurderes om virus kan fjernes umiddelbart eller om serveren skal tages ud af produktion.
- Hvis virus observeres på en pc, skal arbejdspladsen fjernes fra netværket og - hvis det vurderes forsvarligt - slukkes.

6 Scanning af WEB-trafik

Der benyttes scanning ved http-trafik for virus, tilladelser m.v.

Ajourføringshistorik (tidligere bilag A4)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune. Tilrettet i forhold til modtagne kommentarer IT-ledelsen. Opdateret af: JJ/Næstved Kommune. Tilføjelse at, at der skal føres en log over væsentlige konstaterede virus-angreb og tiltag i den forbindelse.	09-11-2009 14-06-2010
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af: PBA/BDO	11-01-2018
Version 1.4	Opdateret af LLINN	13-06-2018

Bilag I	Retningslinjer for fysisk sikkerhed i serverrum og krydsfelter

Den fysiske sikkerhed skal etableres i forhold til det udstyr, som skal sikres. I Næstved Kommune skelnes der imellem:

- Sikkerhedsniveau 1: Centrale enheder, herunder servere og komponenter, som er relateret til kommunens netværk.
- Sikkerhedsniveau 2: Decentrale enheder på lokalnet, herunder pc'er og printere, som er placeret i kontormiljøer.
- Sikkerhedsniveau 3: Decentrale enkeltstående enheder, herunder pc'er på eksterne lokationer samt pc'er i medarbejdernes hjem - med forbindelse til netværket - og bærbare pc'er.

> I Næstved Kommune er alle servere konsolideret i det centrale serverrum.
> I det centrale serverrum har den fysiske sikkerhed den højeste prioritet.

Retningslinjerne i dette bilag beskriver kravene til den fysiske sikkerhed i det centrale serverrum. Endvidere er der beskrevet retningslinjer for fysisk sikkerhed i krydsfelter, som anvendes til Næstved Kommunes netværksforbindelser.

Retningslinjer for fysisk sikring af decentralt udstyr, herunder pc'er og printere på kommunens lokationer, er beskrevet i bilag 1. Retningslinjer for fysisk sikring af distance- og politiker pc'er er beskrevet i bilag 4, og retningslinjer for fysisk sikring af bærbare enheder er beskrevet i bilag 5.

1 Bygningsindretning

Serverrummet er udformet således, at det kun er muligt at opnå adgang via autoriserede adgangsveje.
Serverrummet er udstyret med de fornødne tekniske installationer:

- El-tilførsel i tilstrækkelige mængder - opdelt på flere grupper.
- Dedikeret batteribaseret nødstrømsanlæg samt nødstrømsgenerator.
- Køleanlæg med termostatstyring.
- Automatisk brandslukningsanlæg samt aspirationsanlæg.

Serverrummet er tyverisikret og der er etableret indbrudsalarmer. Der er enkelte vandrør, som er sikret med drypbakker samt fugtalarm. Alle tekniske installationer er endvidere sikret på samme måde som selve IT-udstyret.
Serverrummet må udelukkende indeholde udstyr og effekter, som er relevant i forhold til IT-driften.

Hylder, reoler og andet, som enten kan være brandbart eller ikke har relevans for oplag i datacenteret, skal opbevares udenfor datacenteret.

> Anvendelse af åben ild samt rygning, er ikke tilladt i serverrummet.
>
> Der må ikke spises og drikkes i serverrum.

2 Adgangskontrol

Der er etableret procedurer, som sikrer, at det kun er autoriserede medarbejdere, som har adgang til lokaliteter, der har den højeste prioritet.
Der er således særlige adgangskort og systemnøgler til serverrum samt særlige koder til alarmsystemer. Adgangskort, nøgler samt koder er kun udleveret til medarbejdere, som har et særligt behov.

De ansvarlige medarbejdere skal altid sikre, at serverrummet holdes forsvarligt aflåst.

Af og pålæsning af varer ved fragtmand mv. til it-centerets lager må kun finde sted efter aftale med en medarbejder i Team Servicedesk og IT.

3 Alarmsystemer

Der er etableret tilstrækkelige alarmforanstaltninger således, at eventuelle uregelmæssigheder alarmeres til de ansvarlige:

- Der er etableret alarm til registrering af indbrud samt indbrudsforsøg.
- Der er etableret alarm til registrering af brand og røg, baseret på aspirationsanlæg.
- Der er alarm til registrering af temperaturer over en fastsat grænseværdi.
- Der er systemalarmer ved kritiske systemmæssige grænseværdier.
- Der er fugtalarm til registrering af vandindtrængning.

Alarmer vedrørende brand og indbrud går til Beredskabet. Øvrige alarmer til Team Servicedesk og IT.

4 Krydsfelter

Krydsfelter er placeret i dedikerede rum eller skabe, som er udstyret med de fornødne tekniske installationer og er utilgængelige for uvedkommende.

Krydsfeltrum eller skabe indeholder ikke udstyr og effekter, som er uvedkommende for IT-driften.

Der er etableret procedurer, som sikrer, at det kun er autoriserede medarbejdere, som har adgang til krydsfelter. De ansvarlige medarbejdere skal altid sikre, at de nævnte rum eller skabe holdes forsvarligt aflåst.

Der er etableret tilstrækkelige alarmforanstaltninger således, at eventuelle uregelmæssigheder alarmeres til de ansvarlige. Alle alarmer går til Beredskabet.

Ajourføringshistorik (tidligere bilag A5)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune Tilrettet i forhold til modtagne kommentarer fra IT-ledelsen.	10-11-2009 04-02-2010
Endelig Version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	23-04-2014
Version 1.4	Opdateret af PBA/BDO	23-11-2017
Version 1.5	Opdateret af LLINN	13-06-2018

Bilag J	Retningslinjer for eksterne leverandører

I særlige tilfælde kan leverandører få adgang til Næstved Kommunes systemer og IT-infrastruktur i forbindelse med service og support.

Leverandører defineres som IT-virksomheder, der leverer maskinel, programmel eller service samt håndværkere, der udfører installations- eller reparationsarbejde i forbindelse med kommunens IT-installation.

Bilag J beskriver retningslinjer for leverandøradgang og er opdelt som følger:

- Fysisk adgang til kommunens IT-installation.
- Logisk adgang til kommunens systemer og netværk.

> Alle leverandører, der på den ene eller anden måde kommer i kontakt med Næstved Kommunes IT-miljø skal orienteres om it-sikkerhedspolitikken og være indforstået med eventuelle sanktioner ved brud på politikken.
> Endvidere skal leverandørens arbejde være klart definereti forhold til den specifikke opgave, som de er sat til at løse.

Tavshedspligt
Alle oplysninger, som den pågældende leverandør kommer i besiddelse af, skal behandles fortroligt og må ikke videregives til 3. mand. Kommunen accepterer en fælleserklæring fra en leverandør, der indestår for sine ansatte.

Leverandørerklæring finder sted på en særlig liste/protokol. Leverandøren er forpligtet til hurtigst muligt at give Næstved Kommune besked, når en tekniker, der har underskrevet leverandørerklæringen, ikke længere er ansat hos leverandøren. Team Servicedesk og IT skal med passende mellemrum følge op på, at leverandøren efterlever sin forpligtelse.

Der skal foreligge en ajourført liste over de eksterne leverandører, som Næstved Kommune har indgået aftale med.

Data må ikke overføres mellem leverandør og Næstved Kommune uden forudgående skriftlig aftale. Såfremt data indeholder persondata skal der indgås en formel databehandleraftale. Yderligere oplysninger om behandling af persondata findes i bilag 9.

1 Fysisk adgang

1.1 Serverrummet

Adgang til serverrummet finder sted med elektronisk adgangskort/nøglebrik.

Personlige adgangskort/nøglebrikker, må ikke udleveres til leverandører/reparatører. I stedet skal de ledsages til serverrummet, og der skal i reglen være en IT-medarbejder til stede i serverrum sammen med leverandøren, der dermed kan løse den opgave, som det er kommet for at løse. Det er dog acceptabelt, at særligt betroede leverandører kan udføre arbejde i serverrum uovervåget.

1.2 Andet udstyr

Andet udstyr, som er placeret i Næstved Kommunes lokaler, kan serviceres af eksterne leverandører efter aftale.
Hvis udstyret er særligt beskyttet/aflåst, skal reparatøren ledsages der til af en IT-medarbejder.

1.3 Udstyr sendt til reparation

Reparation eller service af IT-udstyr på en ekstern lokation kan kun finde sted på foranledning af Team Servicedesk og IT.

Overdragelse af IT-udstyr kan kun foretages af Team Servicedesk og IT. Inden overdragelse af udstyret skal det sikres, at udstyret ikke indeholder data, print eller andet, som er fortroligt. Samtidig skal det sikres, at udstyret er klargjort til transport til en ekstern lokation.

2 Logisk adgang

2.1 Generelt

Leverandøren har pligt til at sørge for, at der er installeret antivirus og antispyware på det udstyr, der anvendes under adgangen.

2.2 Netværk

Leverandøradgang til Næstved Kommunes netværk, kan kun finde sted på foranledning af Team Servicedesk og IT.
Med mindre der er tale om direkte support af net-operativsystem eller netkomponenter skal det tilstræbes, at leverandører udelukkende tildeles adgang til de relevante systemer, jf. nedenfor. Kun udvalgte leverandører har en fast, åben administratorbrugerID på Næstved Kommunes netværk. Dette kan f.eks. være i de tilfælde, hvor der foreligger en driftsaftale på et specifikt system. Det skal med passende mellemrum kontrolleres at leverandørers adgange er begrundet i et reelt arbejdsbetinget behov.

2.3 Systemer

Leverandøradgang til kommunens systemer finder normalt sted på foranledning af systemejer.

Konfiguration samt teknisk tildeling af adgangen varetages af Team Servicedesk og IT.

Det skal tilstræbes, at leverandørens adgang til systemerne begrænses mest muligt. Under alle omstændigheder skal der med passende mellemrum føres kontrol med leverandørers adgang til samt handlinger i de pågældende systemer. Der skal tillige foretages logning via det anvendte kommunikationsudstyr.

Team Servicedesk og IT har ansvaret for logning af trafikken.

3 Outsourcing

3.1 Overvågning af leverandøren

Leverandøren skal levere rapportering for, i hvilken grad aftalte servicemål er opfyldt.
Næstved Kommune skal foretage opfølgning på leverandøren, hvor leverandøren foretager behandling af persondata eller væsentlige finansielle data. Opfølgningen kan ske ved indhentning og vurdering af it-revisionsrapporter/erklæringer, årlig risikovurdering af leverandøren indgår også i overvågningen.
Periodiske service-statusmøder skal omhandle sikkerhedsrelaterede emner såsom sikkerhedshændelser og resultater af KPI'er.

Ajourføringshistorik (tidligere bilag D1)

Version 1.1	Udarbejdet af: JJ/Næstved Kommune Opdateret.	25-02-2009
Version 1.2	Opdateret af: JJ/Næstved Kommune	13-11-2009

	Opdateret jf. kommentarer fra IT-ledelsen og kommunikation	04-02-2010
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Ajourført af: PBA/BDO	11-01-2018
Version 1.4	Opdateret af LLINN	13-06-2018

Bilag K	Retningslinjer for eksterne brugere

Eksterne brugere i Næstved Kommune, der anvender et eller flere af kommunens IT-systemer, skal have kendskab til retningslinjen 1 "Retningslinjer for IT-brugere" og retningslinjen her K "Retningslinjer for eksterne brugere".

> Helt overordnet er eksterne brugere underlagt de samme retningsliner som interne brugere i Næstved Kommune.

Derudover skal eksterne brugere altid have underskrevet en tavshedserklæring.

1 Hvad er eksterne brugere?

Eksterne brugere kan f.eks. være enkelt konsulenter eller ansatte i eksterne virksomheder, der udfører opgaver for Næstved Kommune, hvor adgangen til et eller flere IT-systemer er en forudsætning for udførelse af den pågældende opgave.

2 Særlige forhold ved oprettelse af eksterne brugere

Eksterne brugere skal oprettes, så de til enhver til kan genkendes og adskilles fra interne brugere. Der er etableret en speciel procedure for sikring af dette.
Brugerid skal navngives med prefix JXEX og et fortløbende nummer. Metodikken er beskrevet nærmere i AD designdokumentet.

Der skal altid være angivet en ophørsdato for en ekstern brugerkonto.

Eksterne brugere skal umiddelbart have mulighed for samme rettigheder som interne brugere, og er til enhver tid underlagt samme regler og retningsliner i forbindelse med anvendelse af IT-funktioner i Næstved Kommune.

I forbindelse med ekstern revision og analyse af it-systemer, servere og netværk må der ikke gives rettigheder ud over læseadgang idet de personer, der udfører revision, skal være uafhængige af det reviderede område.

Hvis revisionen nødvendiggør mere end læseadgang, må dette kun tillades på kopier af de berørte filer, der skal slettes efter brug.

Al adgang i forbindelse med revision skal logges.
Revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges og aftales med de involverede for at minimere risikoen for forstyrrelser af kommunens forretningsaktiviteter.

Følgende forhold skal den nærmeste leder for den eksterne bruger være ekstra opmærksom på.

- Vurdering af hvorvidt der reelt er behov for adgang til Mail- og Kalendersystemet i kommunen.
- Vurdering af hvorvidt der reelt er behov for adgang til kommunens Intranet.
- Vurdering af hvorvidt der reelt er behov for adgang til kommunens ESDH-system.
- Vurdering af hvilke fagsystemer der skal oprettes adgang til samt specifikation af hvilke områder af fagsystemerne brugeren skal have adgang til.

Nærmeste leder med personaleansvar skal ved tildeling af adgang til Næstved Kommunes IT-miljø gøre den eksterne bruger ekstraordinært opmærksom på følgende forhold:

Du må ikke videregive din personlige adgangskode til andre, heller ikke dine nærmeste kolleger eller IT-medarbejdere.

Når du får en ny adgangskode, skal den altid ændres første gang du logger på.

Som IT-bruger i Næstved Kommune er det dit personlige ansvar

at overholde retningslinjerne.

Gå derfor jævnligt ind på IT-sikkerhedsportalen for at holde dig ajour. Hvis du ikke har adgang – så bed din nærmeste leder om dokumentationen på papir.

Som hovedregel skal alle dokumenter gemmes i kommunens ESDH-system eller et fagsystem, der er godkendt til formålet, og ikke på de enkelte drev, USB-nøgler o. lign.

Husk - at du ikke må gemme personfølsomme data, hverken direkte på kommunens fællesdrev, dit personlige drev eller lokalt på din pc. Personfølsomme data må kun gemmes i særligt indrettede systemer.

Jf. Persondataloven må personfølsomme data undtagelsesvis gemmes på fællesdrev så længe sagsbehandlingen finder sted - dog højst 30 dage.

Det er den nærmeste leder med personaleansvar, der har et specielt ansvar for, hvilke adgange den eksterne bruger får tildelt, ligesom det er dennes ansvar at den eksterne brugerkonto bliver lukket, når den eksterne bruger ikke længere arbejder for den pågældende.

Ajourføringshistorik (tidligere bilag D2)

Version 1.2	Udarbejdet af: JJ/Næstved Kommune Opdateret jf. kommentarer fra IT-ledelsen	13-11-2009 17-11-2009 04-02-2010
Endelig version 1.2	Godkendt på direktionsmøde Godkendt på MED Hovedudvalgsmøde	30-06-2010 23-09-2010
Version 1.3	Opdateret af AMS/Næstved Kommune	22-04-2014
Version 1.4	Opdateret af PBA/BDO	24-10-2017
Version 1.5	Opdateret af LLINN	13-06-2018