Informationssikkerhedshåndbog

Version 2.2

Team Byråd og Direktion

Næstved Kommune
Sagsbehandler: llinn
Tlf. 5588 5300

www.naestved.dk

17. januar 2020

Indhold

1. Indledning

Næstved kommunes informationssikkerhedshåndbog er en samlet beskrivelse af kommunens implementering af informationssikkerhedspolitikken.

Informationssikkerhedshåndbogen er udarbejdet af Team Byråd og Direktion og kvalitetssikret af informationssikkerhedsudvalget.

Ændringer i informationssikkerhedshåndbogen godkendes af direktionen.

Ændringer i operationelle procedurer kan foretages i de ansvarlige centre, afdelinger eller virksomheder.

Informationssikkerhedshåndbogen er behandlet og godkendt af Informationssikkerhedsudvalget 27. januar 2020.

2. Omfang

Næstved kommune har valgt at indarbejde kapitler udarbejdet af Digitaliseringsforening Sjælland (DIGIT) for at sikre overensstemmelse på tværs af kommunerne.
Nogle afsnit indeholder lokale tilføjelser, som er markeret med *. Teksten indeholder desuden specifikke referencer til bilag og henvisninger til kommunens intranet.

Informationssikkerhedshåndbogen er suppleret en bilagssektion med lokale retningslinjer. Retningslinjerne er tilgængelige fra kommunens intranet og er henvendt til to målgrupper. Bilag 1-9 henvender sig til alle medarbejdere, mens bilag A-K henvender sig til systemejere, it-medarbejdere, leverandører og eksterne brugere.

3. Normative referencer

Informationssikkerhedshåndbogen følger den internationale standard for informationssikkerhed ISO 27002, der supplerer ISO 27001 med en uddybning af sikkerhedsforanstaltninger og tilhørende implementeringsvejledning.

ISO 27001/2 er en international ledelsesstandard for informationssikkerhed. Standarden er et styringsværktøj, der hjælper kommunen til at beskytte værdifuld information - herunder persondata - på en sikker og troværdig måde. ISO 27001/2 opstiller blandt andet krav til risikostyring, dokumentation af processer samt fordeling af roller og ansvar for informationssikkerhed.

Alle offentlige virksomheder er i dag underlagt at følge principperne i standarden ISO 27001. Standarden er desuden et godt afsæt til at håndtere kravene i EU Databeskyttelsesforordning (2016/679), og Databeskyttelsesloven (2018/502).

Formålet med ISO 27001 er at opnå effektiv informationssikkerhedsledelse, der passer til en virksomheds særlige behov samt sikre, at denne effektivitet fastholdes gennem en proces for løbende forbedring. Det betyder, at informationssikkerheden løbende opdateres, så virksomheden er i stand til at håndtere udfordringerne i en forretningsverden under konstant forandring.

4. Begreber og definitioner

Ord	Forklaring
Aktivejer	Ejer af et eller flere af kommunens aktiver. Omfatter systemejere, dataejere og IT-Teamlederen
Aktiver	It-udstyr (fx pc'er, tablets, mobiltelefoner) Infrastruktur (fx servere, routere, firewalls, netværk) Systemer (fx fagsystemer, egenudviklede programmer, standard programmer) Data (fx dokumenter i elektronisk, papir, billede eller lydformat samt databaser)
Almindelige personoplysninger	De personoplysninger, der ikke falder ind under kategorien "følsomme personoplysninger", kan kaldes "almindelige personoplysninger". Almindelige personoplysninger kan f.eks. være identifikationsoplysninger som f.eks. navn og adresse, oplysninger om økonomiske forhold, kundeforhold, andre lignende ikke-følsomme oplysninger.
Anneks A	Anneks A er en del af ISO27001 og indeholder 114 sikkerhedskontroller, der kan bruges som inspiration eller anvendes som tjekliste, for at sikre at relevante sikkerhedskrav er taget med i betragtning. Anneks A omtales ofte som SoA-dokumentet.
Brugerautentifikation	Fastlæggelse af autenticitet kaldes autentifikation. Brugerautentifikation betyder, at man sikrer sig, at brugeren er den, han giver sig ud for at være. Dette kan sikres ved fx personligt kodeord og/eller biometri.
CPR-nummer	Nationalt identifikationsnummer.
Databehandler	Typisk en virksomhed, offentlig myndighed eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne og efter instruks fra den dataansvarlige.
Dataejer (dataansvarlig)	En chef/leder som har dispositionsret til data og ansvar for behandling af data. Dataejer kan også være systemejer. Se desuden "En rejsefortælling om funktioner, roller og ledelse" hvor roller og opgaver for en data/systemejer er beskrevet.
DIGIT	Digitaliseringsforeningen Sjælland
DMZ	DMZ (Demilitarized zone) er en zone, der fungerer som en bindeled mellem eksterne og interne netværk. På den måde er der aldrig åbent for trafik direkte fra Internettet og ind til det interne net.
Eksekverbare filer	En eksekverbar fil eller eksekverbar applikation er et udtryk, der anvendes i informationsteknologien. Det er en fil, der får en computeren til at udføre angivne opgaver i henhold til de krypterede instruktioner. Dette i modsætning til en datafil, som skal læses af et computerprogram for at være meningsfuldt. Eksekverbare filer er fx .exe, .com, .scr, .pif, .bat, .cmd, .vbs.
Firewall	En firewall eller på dansk brandmur er et stykke netudstyr eller software, der udvælger hvilke netværkspakker som skal have adgang fra den ene side af firewall til den anden side efter et regelsæt.
FIT	Der bør altid gennemføres en konsekvensvurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed (FIT). Med fortrolighed menes, at uvedkommende får adgang til data, som de ikke burde have adgang til. Med integritet menes, at data, f.eks. i et system, er de rigtige, og at man kan træffe beslutninger på baggrund af dette. Med tilgængelighed menes, at man i organisationen kan tilgå nødvendige data.

Ord	Forklaring
Fortrolige oplysninger	Fortrolige personoplysninger er oplysninger, som hvis de videregives uden bemyndigelse vil kunne skade den pågældende persons rettigheder, omdømme, interesser, økonomiske forhold eller andre personlige forhold. Fortrolige oplysninger (ikke personoplysninger) defineres som enhver form for information, som hvis videregivelse uden bemyndigelse, vil kunne skade kommunens omdømme, sagsbehandling, økonomiske interesser, medarbejdere eller andet af kommunens arbejdsområder.
Fællesfortegnelser	Som et led i arbejdet med databeskyttelsesforordningen har KL påtaget sig opgaven med at udarbejde fællesfortegnelser, der er dækkende for alle kommunale behandlingsaktiviteter.
Følsomme personoplysninger	Oplysninger om race eller etnisk oprindelse Politisk, religiøs eller filosofisk overbevisning Fagforeningsmæssigt tilhørsforhold Behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person Helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
Informationssystemer	Et informationssystem er et system bestående af personer, data og aktiviteter, der behandler data og informationer en organisation
IoT	Internet of Thing, forkortet IOT eller IoT, defineres slet og ret som ”et netværk af alle elektroniske enheder, i stand til at indsamle og dele data via sensorer”. Eller med andre ord ”at alt elektronik kan forbindes”.
ISAE 3000	En 3000-erklæring er som regel en kortere erklæring, der dækker en konkret arbejdshandling, f.eks. persondataloven, outsourcing-bekendtgørelsen, eller forpligtelser over for en bestemt kunde. I erklæringen gennemgås udvalgte område samt relateret dokumentation, hvorefter der givers en samlet vurdering af, hvor betryggende området håndteres hos virksomheden. Samtidig gives der en vurdering for hvert delområde, så virksomheden præcist kan se, hvad der fungerer som det skal, og hvad der eventuelt skal arbejdes med. Denne type erklæring kan afgives enten som et øjebliksbillede eller for en bestemt periode – fx et år.
ISAE 3402	3402 er en lidt længere erklæring, hvor en lang række af kontrolområder gennemgås, og den må betragtes som den klassiske it-revisionserklæring. 3402 forholder sig til alle forretningsgange omkring it-funktionen, som kan have indflydelse på den finansielle rapportering: Udvikling, drift, beredskab, dokumentation mv. Den forholder sig også til det helt lavpraktiske, som fx de fysiske forhold, såsom hvordan er servere/datacenter placeret.
ISMS	Information Security Management System – ledelsessystem for informationssikkerhed I DIGIT-regi anvendes Neuparts system SecureISMS
ISO27001	ISO27001 standarden er udarbejdet med det formål at opstille krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS).
Konsekvens	En del af risikoanalysen er en identifikation af de konsekvenser, som et tab af fortrolighed, integritet og/eller tilgængelighed vil medføre for et aktiv. Der kan være direkte økonomiske tab, tab af omdømme, indflydelse på serviceniveau mv.
Kontrahent	Person som indgår en kontrakt eller aftale

Ord	Forklaring
Kontrahenter	Person eller firma, som indgår en kontrakt med anden person eller firma, om at udføre en specificeret opgave.
Kryptografi	Kunsten at hemmeligholde information (typisk en besked), så den bliver ulæselig for tredjepart.
Licenseret	At kommunen har (det nødvendige antal) tilladelse(r) til at udnytte et program, et produkt, en patentret el.lign. som led i en licensaftale
Mitigere	Forebygge eller mindske
Mobile enheder	It-udstyr som fx mobiltelefoner/smartphones/iPhone, tablets/iPad, bærbar PC, memory-stick, ekstern harddisk, kamera og mobile IoT generelt
NDA	NDA står for "Non Disclosure Agreement'' En NDA er et juridisk dokument der sikrer at den der underskriver den, ikke misbruger den viden han/hun får ved et møde eller ved udlevering af fortroligt materiale. Hemmeligholdelsesaftalen skal beskytte en eller begge parters fortrolige oplysninger.
NDA	En NDA er et juridisk dokument der sikrer at den der underskriver den, ikke bruger den viden han/hun får ved et møde eller ved udlevering af fortroligt materiale. Hemmeligholdelsesaftalen skal beskytte en eller begge parters fortrolige oplysninger.
NTP	Med NTP (Network Time Protocol) kan en computer synkronisere sit indbyggede ur med serverens ur, så tidspunkterne er ens.
Personoplysninger	Personoplysninger er enhver form for information, der kan henføres til bestemte personer, også selv om dette forudsætter kendskab til et personnummer, registreringsnummer eller lignende. Også oplysninger i form af f.eks. et billede eller et fingeraftryk er personoplysninger. Forordningen sondrer mellem følsomme og almindelige personoplysninger.
Phishing	Phishing er et internetfænomen, hvor svindlere forsøger at franarre internetbrugere deres brugernavn, adgangskode, kreditkort eller netbank oplysninger. Det sker typisk ved at brugeren får tilsendt en e-mail eller SMS, hvis indhold forsøger at få brugeren til at dele sine oplysninger pr. e-mail eller logge ind på en falsk internetside. Mailen kan fremstå, som om den er afsendt fra et sted brugeren har tillid til eller en person fra modtagerens adressekartotek.
Revisionserklæring	Revisionserklæring giver systemejeren mulighed for at få en fagkyndig person til at se leverandøren i kortene, og dertil besvaret spørgsmålet, om leverandøren overholder sine forpligtigelser.
Risiko	En risiko kan opstå, hvis en trussel udnytter en sårbarhed, f.eks. en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb.
Risikoejer	Risikoejer vil ofte være den, der har det økonomiske ansvar for risikoen. Kan f.eks. være systemejer eller kontraktansvarlig.
Risikologgen	I risikologgen kan relevante trusler, sårbarheder, deres indvirkning samt konsekvenser ved et sikkerhedsbrud beskrives. Ligeledes beskrives hvordan risikoen håndteres/kontrolleres, hvis risikoniveauet er højere end den grænse der er fastlagt. *Alle DIGIT-kommuner benytter primært Secure ISMS til risikostyring. Risikologgen er KL's alternativ.*
Risikoprofil	Det fastlagte niveau for hvornår risici er acceptable. Niveauet i accept af risici kan hos informationssikkerhedsudvalget lægges forskelligt for f.eks. økonomiske risici i

Ord	Forklaring
	forhold til risici på liv/ære/velfærd området. Det samlede billede af risikovillighed udgør organisationens risikoprofil.
Risikovurdering	Risikovurdering handler om at identificere og analysere mulige trusler, sårbarheder overfor truslerne og sandsynligheden for de kan opstå samt tilhørende konsekvenser i forhold til risikoen for tab af fortrolighed, integritet og tilgængelighed.
Sandsynlighed	Når en trussel vurderes, vurderes sandsynligheden for at truslen udnytter en sårbarhed og dermed giver brud på fortrolighed, integritet og/eller tilgængelighed.
SIEM	Security Information and Event Management (SIEM), log-håndteringssystem til sikkerhedsanalyse og overvågning af aktiviteter.
SoA	SoA står for 'Statement of Applicability'. SoA-dokumentet er en formel beskrivelse af udvalgte sikkerhedstiltag der udføres som et led i håndteringen af risici. SoA'en kaldes også beslutningsdokumentet og består konkret af en liste med kontroller.
Social Engineering	Kunsten at aflure fortrolige informationer uden at blive opdaget. F.eks. kan denne form for bedrag udføres via e-mail, telefon og/eller messenger-programmer.
Statisk medie	Eks. bånd, DVD eller andet, oftest billigere, lagringsmedie til langtidslagring. Ofte med højere accesstid.
Systemadministrator	Systemadministrator arbejder med driften af et it-system og har typisk udvidet rettigheder til systemet. Systemadministrator kan være intern eller ekstern.
Systemejer	En chef/leder, der er ansvarlig for et eller flere systemer.
Sårbarhed	En trussel kræver en sårbarhed for at kunne resultere i en risiko og omvendt. Sårbarheder kan være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb.
Trusler	Identifikationen af relevante trusler er afgørende for, at man ikke overser risici. Derfor bør trusselsvurderingen ske på en systematisk måde. Der findes meget omfattende trusselskataloger, som indeholder enhver tænkelig situation, men man kan også anvende mere generiske kataloger. Ifølge National strategi for cyber- og informationssikkerhed er det et krav, at cyber trusler også indgår i myndighedernes risikovurderinger og risikoledelse. Eksempler på trusler kan være hackerangreb, oversvømmelse, menneskelige fejl eks. deling af fortrolige oplysninger via mail, servernedbrud, spionage etc.
Type-I eller type-II erklæringer for ISAE 3000 og ISAE 3402	En type-I erklæring viser et øjebliksbillede, hvor en type-II dækker en periode, typisk et år. ISAE-erklæringerne er nærmere forklaret nedenfor. Det er systemejeren der skal træffe beslutning om, hvorvidt it-systemet skal være omfattet af en revisionserklæring. Indledningsvist skal Systemejeren dog først afdække, hvorvidt der er lovmæssige krav om, at leverandøren skal være omfattet af revisionspligt. Dette er f.eks. tilfældet for studieadministrative it-systemer for almene voksenuddannelser, erhvervsuddannelser, de gymnasiale uddannelser m.fl. – hvor leverandøren årligt skal kunne stille med en ISAE 3402 type-II erklæring.
Uklassificerede oplysninger	Uklassificerede oplysninger er oplysninger, som ikke ved en offentliggørelse på nogen måde vil skade kommunens interesser.
Værdidata	Data som udgør en særlig værdi for kommunen eller kommunens interessenter. Kan fx være fortrolige oplysninger i form kontraktbestemmelser, patentoplysninger, økonomiske forhold)

5. Informationssikkerhedspolitik

5.1. Formål

Næstved Kommunes (herefter ”Kommunen") informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i Kommunen og fastlægger vores ambitionsniveau herfor. Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af Kommunens informationssikkerhedshåndbog, der forstås som fællesbetegnelsen af informationssikkerhedspolitikken med de underliggende retningslinjer og forretningsgange.

Informationssikkerhedspolitikken er en vigtig del af Kommunens informationssikkerhedshåndbog og beskriver det ledelsesgodkendte niveau for informationssikkerhed og beskyttelse af persondata. Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i Kommunens organisation og virke. De retningslinjer, der udformes for at understøtte informationssikkerhedspolitikkens hovedmålssætninger, skal sikre, at alle, der arbejder med Kommunens informationer, forholder sig til informationssikkerhed i det daglige arbejde.

Kommunen ser ikke kun et tilstrækkeligt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement for at kunne tilbyde en sikker service for borgerne og virksomheder. Informationssikkerhed er derfor en nøgleværdi hos Kommunen, og den vil være en naturlig del af vores aktiviteter.

Informationssikkerhedshåndbogen følger principperne i den internationale standard for informationssikkerhed, ISO 27001:2013, og er udarbejdet i et samarbejde mellem kommunerne i Digitaliseringsforening Sjælland. Målet med samarbejdet er en udstrakt harmonisering af medlemskommunernes ledelse og styring af informationssikkerheden med henblik på et tæt samarbejde for at opnå effektiviseringer og øget kvalitet på informationssikkerhedsområdet.

Herudover skal Informationssikkerhedshåndbogen og kommunens Informationssikkerhedspolitik også udgøre de overordnede rammer for kommunens efterlevelse af databeskyttelsesreglerne. Det vil navnlig sige EU’s databeskyttelsesforordning (GDPR) og den supplerende danske databeskyttelseslov (lov nr. 502 af 23. maj 2018). *

Informationssikkerhedspolitikken er gældende for alle uden undtagelse med en fysisk eller logisk adgang til Kommunens systemer, data og informationer.

Informationssikkerhedspolitikken omfatter alle typer af informationer herunder lyd, billede og tekst og uanset, hvordan informationerne anvendes og opbevares.

5.2. Gennemgang af politikker for informationssikkerhed

De informationssikkerhedspolitikker og retningslinjer mv., der indgår i denne Informationssikkerhedshåndbog, revurderes og godkendes mindst én gang hvert år, eller i forbindelse med eventuelle situationer, der tilsiger det. Ændringer af Informationssikkerhedshåndbogen skal koordineres med Digitaliseringsforening Sjælland.

Gennemgangen bør omfatte en vurdering af mulighederne for at forbedre organisationens politikker og metode til styring af informationssikkerhed som følge af ændringer i organisationen, forretningsforhold, juridiske forhold eller det tekniske miljø.
Gennemgangen bør tage højde for resultaterne af udført revision, tilsyn eller gennemførte audit.

5.3. Hovedmålsætninger og sikkerhedsniveau

Sikkerhedsmålsætning:
"Vi vil have et tilstrækkeligt informationssikkerhedsniveau for alle med relation til Kommunen og for anvendelsen af informationsaktiver."

Et tilstrækkeligt informationssikkerhedsniveau opnås igennem sikringsforanstaltninger, der sikrer:

1. Fortrolighed, integritet- og tilgængelighed af Kommunens systemer og data i forhold til den risikovurdering, der er fastsat for det enkelte system/data.
2. Beskyttelse af Kommunens informationsaktiver, organisationens image og informationer/data i Kommunens varetægt.
3. Sikring af databeskyttelse for fysiske personer, herunder ved efterlevelse af databeskyttelseslovgivningen.

For at fastholde det tilstrækkelige sikkerhedsniveau i Kommunen skal følgende overholdes:

- Der skal være implementeret retningslinjer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af Kommunens drift og daglige arbejde.
- Kommunen skal gennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke udhuler Kommunens informationssikkerhedsniveau.
- Kommunen skal sikre en struktureret og kontinuerlig forbedringsproces af arbejdet med informationssikkerhed.

5.4. Organisation og ansvar

Sikkerhedsmålsætning:
"Alle har ansvar for informationssikkerheden. De er bekendte med og efterlever vores informationssikkerhedspolitik, informationssikkerhedshåndbog, retningslinjer og forretningsgange i Kommunen."

Planlægning, implementering og kontrol af informationssikkerhed er defineret af Kommunens ledelse. Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet i Kommunen og er ansvarlig for opfølgning på sikkerhedshændelser.

Kommunaldirektøren er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, så informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Den nødvendige viden og kompetence om informationssikkerhed kommunikeres til alle, der arbejder med Kommunens informationer, og der bliver løbende arbejdet med holdninger og viden om informationssikkerhed. Ledelsen på alle niveauer er ansvarlig for, at informationssikkerheden overholdes.

5.5. Informationssikkerhedshåndbogen

Informationssikkerhedspolitikken uddybes i retningslinjer og forretningsgange. Tilsammen udgør politikken, retningslinjer, beredskabsplanen og forretningsgange informationssikkerhedshåndbogen.

5.6. Risikovurdering og klassifikation

Risikovurdering

Informationssikkerheden i Kommunen er på et niveau, der tilgodeser lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser overfor de aktører, der skal anvende Kommunens informationsaktiver. Kommunen ønsker ikke at sikre sig for enhver pris, men ønsker at være bevidst om enhver risiko, og forholde sig tilfredsstillende til disse, hvormed et tilstrækkeligt sikkerhedsniveau etableres.

Ledelsen deltager aktivt i risikovurderingen og er ansvarlige for at vurdere trusler, konsekvenser og risici af informationssystemer og andre relevante områder.

Risikovurderingen opdateres mindst én gang årligt, samt ved eventuelle større ændringer i opgaver, leverandører, informationssystemer eller anvendelsen deraf.

Risikovurderingen skal ikke kun have fokus på risici for organisationens aktiver/værdier. Der skal også udføres risikovurdering med fokus på risici for fysiske personers rettigheder og frihedsrettigheder.

Klassifikation

Kommunens informationer skal klassificeres efter lovmæssige krav, værdi og efter, hvor kritisk og følsom informationen er i forhold til uautoriseret offentliggørelse eller ændring.

Baseret på klassifikationen samt risikovurderingen etableres relevante sikkerhedsforanstaltninger.

5.7. Overtrædelse af informationssikkerhedspolitikken

Alle i Kommunen er forpligtet til at efterleve den til enhver tid gældende informationssikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag. En overtrædelse kan, efter omstændighederne, medføre sanktioner.

Hvis en medarbejder er vidende om, at Kommunens informationssikkerhed overtrædes, skal det meddeles til ledelsen.

5.8. Afvigelser

Hvis der opstår situationer, hvor kravene i informationssikkerhedshåndbogen ikke kan efterleves, skal der skriftligt anmodes om dispensation hos Kommunens formand for informationssikkerhedsudvalget. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger og en udløbsdato.

5.9. Udarbejdelse og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: Godkendes af byrådet/direktionen.
- Informationssikkerhedshåndbogen samt bilag og retningslinjer: Godkendes af Informationssikkerhedsudvalget.
- Operationelle procedurer: Kan foretages af den lokale ledelse.

6. Organisering af informationssikkerhed

6.1. Intern organisering

6.1.1. Roller og ansvarsområder for informationssikkerhed

I nedenstående skema er vist rollefordelingen i Næstved kommune. Oversigten revideres ved relevante organisationsændringer og minimum én gang om året.

Rollefordelingen i Næstved kommune:

Rolle	Navn	Funktion
Formand for Informationssikkerhedsudvalget	Rie Perry	Kommunaldirektør
Medlem af Informationssikkerhedsudvalget	Steen Andersen	Centerchef, CKO
Medlem af Informationssikkerhedsudvalget	Thomas Carlsen	Centerchef, CBU
Medlem af Informationssikkerhedsudvalget	Gitte Nonbo	Teamleder, TBD
Medlem af Informationssikkerhedsudvalget	Lars Borg	Teamleder, TSI
Medlem af Informationssikkerhedsudvalget	Bo Hauge Laursen	Skoleleder
DPO, rådgiver for Informationssikkerhedsudvalget	Bech-Bruun Advokatfirma	DPO
Informationssikkerhedskoordinator og sekretær for Informationssikkerhedsudvalget	Lars Linnemann	Informationssikkerhedskoordinator
Sidst opdateret 16. december 2019		

Informationssikkerhedsudvalget

Organisering

- Informationssikkerhedsudvalget er en tværfaglig gruppe med et direktionsmedlem som formand, der sætter mål for informationssikkerhed i kommunen
- Informationssikkerhedskoordinatoren er sekretær for gruppen
- DPO rådgiver og støtter Informationssikkerhedsudvalget i spørgsmål om beskyttelse af personoplysninger (databeskyttelse)
- Informationssikkerhedsudvalget kan efter behov besættes med yderligere medlemmer
- Udvalget står til ansvar over for Økonomiudvalget og Byrådet*

Roller og ansvar

- Informationssikkerhedsudvalget sætter mål for sikkerheden og sørger for, at informationssikkerheden realiseres og efterleves i organisationen. Udvalget har således det daglige ansvar for styring af informationssikkerheden
- Udvalget udformer og beskriver retningslinjer, organisatoriske rammer, ansvarsfordeling, retningslinjer for kontrol og beredskab mv. vedrørende informationssikkerhed

- Udvalget har ejerskabet til Informationssikkerhedshåndbogen, herunder ansvaret for, at der regelmæssigt sker gennemgang af de informationssikkerhedspolitikker og retningslinjer mv., der indgår i håndbogen
- Endelig er det udvalget, der sikrer, at sikkerhedsarbejdet har ledelsens opbakning
- Formanden for informationssikkerhedsudvalget godkender oplæg til procedurer, retningslinjer, mv. udarbejdet af informationssikkerhedsudvalget (jf. informationssikkerhedsudvalgets opgaver)

Opgaver
Informationssikkerhedsudvalget skal bl.a.:

- Sikre, at udvalget har den nødvendige viden om reglerne om databeskyttelse samt ISO27001, da medlemmernes indsigt i disse regler og standardens indhold og dækningsområde er væsentligt for informationssikkerhedsudvalgets arbejde og succes
- Fastlægge organisationens styringsmodel for informationssikkerheden ud fra ISO-principperne
- Sikre, at beslutninger bygger på et afvejet helhedssyn – en balance mellem informationssikkerhed, brugervenlighed og økonomi
- Revidere og ajourføre de overordnede retningslinjer for informationssikkerhed med udgangspunkt i den aktuelle risikovurdering for organisationen
- Godkende ændringer til Informationssikkerhedshåndbogen
- Initiere den årlige risikovurderingsproces og på baggrund heraf indstille SoA-dokument eller lignende til godkendelse i Direktionen
  SoA (Statement of Applicability) indeholder de nødvendige kontroller i ISO27001, anneks A, og begrundelse for, hvorfor nogle kontroller er medtaget, hvad enten de er implementeret eller ej, samt begrundelse for hvorfor andre er udeladt.
- Formidle de trufne beslutninger til organisationen

Informationssikkerhedskoordinator

Rolle

- Informationssikkerhedskoordinatoren er organisationens daglige informationssikkerhedsleder og sekretær for informationssikkerhedsudvalget
- Ideelt set bør informationssikkerhedskoordinatoren referere direkte til direktionen, men uanset den organisatoriske placering er det vigtigt, at koordinatoren har direkte adgang til direktionen
- Informationssikkerhedskoordinatorens ansvar og beføjelser præciseres af direktionen
- Er bindeled til Digitaliseringsforening Sjælland vedr. informationssikkerhed

Opgaver
Informationssikkerhedskoordinatoren skal:

- Lede risikovurderinger og komme med forslag til opdatering af overordnede retningslinjer for informationssikkerhed
- Registrere og rapportere kritiske hændelser
- Evaluere og benchmarke organisationens informationssikkerhed
- Mindst en gang årligt gennemgå Informationssikkerhedshåndbogen samt efter koordinering med Digitaliseringsforening Sjælland udforme forslag til opdateringer, når der er behov herfor
- Skabe opmærksomhed om informationssikkerhed blandt organisationens medarbejdere

- Indkalde til møder og være sekretær for Informationssikkerhedsudvalget
- Afklare grænsesnit med øvrige politikker i organisationen og vurdere behovet for drøftelse af de overordnede retningslinjer for informationssikkerhed i fx teknologi-, samarbejds- og sikkerhedsudvalg
- Koordinere informationssikkerhedsindsatsen med de øvrige kommuner i Digitaliseringsforening Sjælland

Databeskyttelsesrådgiver (DPO)

Rolle

- Databeskyttelsesrådgiveren ("Data Protection Officer"/DPO) er udpeget af organisationen som led i efterlevelse af databeskyttelseslovgivningen herunder GDPR
- DPO'en skal involveres tilstrækkeligt og rettidigt i alle spørgsmål vedrørende databeskyttelse
- DPO'en fungerer desuden som kontaktperson for registrerede og databeskyttelsesmyndighederne
- DPO'en må ikke modtage instruktioner om opgaver og skal rapportere direkte til højeste ledelsesniveau.

Opgaver
DPO'en skal bl.a.:

- rådgive organisationen om beskyttelse af personoplysninger, herunder om databeskyttelseslovgivningen
- Assistere organisationen i forbindelse med håndtering af sikkerhedsbrud
- Rådgive i forbindelse med kontrolbesøg og skriftlige tilsyn fra Datatilsynet
- Undervise medarbejdere i kommunen
- Overvåge, at organisationen overholder både lovgivningen og interne retningslinjer ift. beskyttelse af personoplysninger
- Rådgive i alle aspekter vedrørende udarbejdelse af konsekvensanalyser
- Indgå og støtte Informationssikkerhedsudvalget i forvaltningen af interne retningslinjer ift. beskyttelse af personoplysninger (databeskyttelse)
- Rådgive om udvikling og vedligeholdelse af intern dokumentation om beskyttelse af personlige oplysninger
- Fungere som kontaktperson for registrerede og databeskyttelsesmyndighederne om både brud på datasikkerheden samt andre spørgsmål, som fx generel information omkring rettigheder, herunder at modtage telefoniske og skriftlige henvendelser, som videreformidles til håndtering i den relevante enhed i organisationen

*Tværgående koordination – Center arbejdsgrupper **

Ledelsen på alle niveauer er ansvarlig for, at informationssikkerheden overholdes. Hvert center udpeger en arbejdsgruppe, der har ansvaret for at

- udarbejdelse af procedurer og retningslinjer vedrørende informationssikkerhed på centerspecifikke områder
- vedligeholdelse af centrets fortegnelser, systemoversigt og databehandleraftaler
- deltagelse i risiko- og konsekvensvurderinger og beredskabsplanlægning på centrets fagområde

- opfølgning på sikkerhedsinitiativer og awareness kampagner, der når ud til alle medarbejdere i centret og tilhørende virksomheder
- opfølgning på sikkerhedshændelser, persondatabrud og anmodning om indsigt i personoplysninger på centrets fagområde
- centrets nøglepersoner deltager i koordinationsmøder med Informationssikkerhedskoordinatoren hvert kvartal.

*Digitalisering – Centeragenter **

Centeragenterne i Team Kommunikation, Udvikling og HR understøtter dialog om udvikling af digitale løsninger mellem centrene og it. Samarbejdet med Informationssikkerhedskoordinatoren omfatter

- gensidig orientering om digitale udviklingsprojekter og sikkerhedsforanstaltninger,
- udveksling af viden om forretningsområderne, deres it-systemer m.m. og
- ajourføring af KITOS systemlisten i dialog med forretningsområderne.

*Støttefunktioner – Ressourcepersoner **

I tæt samarbejde med Informationssikkerhedskoordinatoren varetager ressourcepersoner inden for jura, kommunikation, digitalisering og it-service en række støttefunktioner vedrørende databeskyttelse og informationssikkerhed. Ressourcepersonerne udgør ikke en samlet gruppe, men bistår Informationssikkerhedskoordinatoren med specifikke kompetencer til løsning af konkrete opgaver.

- Jura
    - Varetager juridisk rådgivning af Informationssikkerhedskoordinatoren og indkøbsfunkton i særlige tilfælde, hvor tolkning af lovgivning anses for påkrævet
- Kommunikation
    - Grafisk design af informationsmateriale
    - Webredaktionsopgaver
    - Ansvarlig for vedligeholdelse af side på kommunens intranet om systemejerskaber og systemoversigter
    - Deltagelse i tilrettelæggelse af Awareness kampagner
- Servicedesk og IT
    - Gennemgang og forbedring af sikkerhedsarkitektur og –løsninger
    - Bistand ved sikkerhedshændelser
    - Deltagelse i risikovurderinger
    - Beredskabsplanlægning og -test
    - Opdatering af sikkerhedsprocedurer

Systemejer

Roller og ansvar

- Systemejer har ansvar for informationssikkerheden, for det/de systemer de ”ejer”, herunder ansvaret for at der bliver udarbejdet (detaljerede) procedurer, instrukser og tjeklister inden for rammerne af de sikkerhedsniveauer direktionen har fastlagt
- Det er ligeledes systemejers ansvar at føre løbende kontrol med overholdelsen af retningslinjer og procedurer og at sikre vedligeholdelse af overblik af system, herunder processer, interessenter, aktiver, kontrakter etc.

- Systemejer har ansvar for at indkøb og implementering af it-systemer er koordineret med Team Servicedesk og IT *

Opgaver
Skabe sig et overblik over, hvilke forretningsprocesser systemet understøtter. Overblikket bruges til at sikre, at der stilles relevante sikkerhedsmæssige krav med udgangspunkt i organisationens sikkerhedsniveauer. Arbejdet inkluderer at

- Klassificere aktiver og specificere sikkerhedsmæssige krav samt godkende anskaffelser og installation af hvert aktiv
- Give adgang til systemet
- Godkende placering af kritiske aktiver samt udviklings- og hjælpemiljøer
- Godkende beredskabsplaner og følge op på sikkerhedshændelser
- Systemejer kan delegere rutinemæssige opgaver til en person (entitet), der dagligt holder øje med aktiverne, men systemejeren har stadig det endelige ansvar for systemets informationssikkerhed i hele systemets levetid

Systemejers ansvar og opgaver er yderligere beskrevet i bilag A.*

Dataejer

Roller og ansvar
Dataejer har dispositionsret til data og ansvar for behandling af data, herunder at retningslinjer og instrukser for et systems anvendelse overholdes af brugerne.

Opgaver
Dataejer skal skabe sig et overblik over, hvilke forretningsprocesser data understøtter og indgår i. Overblikket bruges til at sikre, at der stilles relevante sikkerhedsmæssige krav med udgangspunkt i organisationens sikkerhedsniveauer. Arbejdet inkluderer at:

- Klassificere data
- Give adgang til data
- Godkende beredskabsplaner og følge op på sikkerhedshændelser
- Føre tilsyn og kontrol med, at retningslinjer og instrukser følges*

*IT-Teamleder **

Rolle og ansvar

- Sikring af principper for design og udvikling af kommunens it-systemer og for deres indbyrdes sammenhæng
- Varetage sikker og stabil driftsafvikling af it-systemer

Opgaver

- Beskrive og etablere forretningsgange og procedurer, som støtter overholdelsen af Informationssikkerhedspolitik og -håndbog
- Etablering af sikkerhedsarkitektur og valg af sikkerhedsløsninger, herunder løsninger til monitorering, logning og rapportering
- Vedligeholde og teste beredskabsplan for kommunens it-infrastruktur
- Sikre, at der løbende følges op på kommunens trusselsvurdering og tekniske cyberforsvar

- Sikre sikkerhedsmæssig monitorering af kommunen overordnede infrastruktur
- Deltage i incidentprocessen og i afdækningen af brud på it-sikkerheden

*Systemadministrator **

Roller og ansvar

- Teamleder eller medarbejder med særligt kendskab til et system, som har ansvaret for at udføre opgaver uddelegeret af systemejer vedrørende kontrakt, budget, autorisation, teknik, sikkerhed og kontroller.

Opgaver

- Udarbejdelse af instrukser for de enkelte systemer
- Udarbejdelse af uddybende systemdokumentation
- Beskrivelse af relaterede interne kontroller

Direktionen

Rolle

- Direktionen har det overordnede ansvar for informationssikkerheden i organisationen, herunder at fastlægge sikkerhedsniveauet gennem den årlige godkendelse af SoA dokumentet.
- Ansvaret inkluderer ansvaret for, at medarbejderne er kvalificerede til at arbejde sikkert og lovligt med organisationens informationer
- Direktionen træffer de overordnede beslutninger vedrørende informationssikkerhed og forholder sig til økonomiske, ressourcemæssige og organisatoriske konsekvenser

Opgaver

- Sikre, at arbejdet med informationssikkerhed har ledernes opbakning
- Holde sig ajour med det aktuelle risikobillede ved at samarbejde med sikkerhedskoordinatoren og de personer (entiteter), der har ansvar for informationsaktiver eller behandling af personoplysninger
- Etablere et Information Security Management System (ISMS)/ledelsessystem for de retningslinjer, procedurer, processer, organisatoriske beslutningsgange og aktiviteter, som udgør komponenterne i organisationens styring af informationssikkerhed
- Vurdere, om der er behov for ekstern rådgivning og bistand til sikkerhedsarbejdet

Mellemleder

Rolle

- Mellemledere (centerchefer, teamledere og virksomhedsledere)* er ansvarlige for operativ implementering og løbende kontrol med overholdelsen af retningslinjer, procedurer, budget mv.
- De bidrager i øvrigt til at højne opmærksomheden omkring informationssikkerhed, og fungerer som daglig sparringspartner for medarbejderne i forhold til efterlevelse af sikkerhedsforanstaltningerne

Opgaver

- Påtage sig ansvaret for at sikre udarbejdelser af de detaljerede procedurer, instrukser og tjeklister inden for rammerne af de sikkerhedsniveauer organisationens topledelse har fastlagt
- Sikre, at organisationens arbejde planlægges på en måde, så informationssikkerheden understøttes
- Følge op på sikkerhedsinitiativer i forhold til medarbejdernes daglige arbejde, herunder sikre høj awareness om informationssikkerhed
- Rapportere risici og hændelser

Medarbejder

Rolle

- Medarbejderne har den vigtigste rolle i forhold til informationssikkerhed, hvor medarbejderne sikrer, at de uddelegerede opgaver udføres på en måde, så organisationen efterlever lovgivningen og interne retningslinjer
- Medarbejdergrupper har naturligvis meget forskellig berøring med data, information og fysisk sikkerhed. Dermed har medarbejdere forskellige roller i sikkerhedsarbejdet

Opgaver
Medarbejdernes opgaver i sikkerhedsarbejdet afhænger i høj grad af, hvor meget data mv. de er i berøring med i deres daglige arbejde. Generelt kan det dog siges, at de skal:

- Overholde gældende lovgivning og kommunens retningslinjer
- Udpege mangler i gældende retningslinjer og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde

6.1.2. Funktionsadskillelse

Det bør sikres, at ingen enkeltpersoner kan få adgang til, ændre eller bruge aktiver uden autorisation, og uden at det opdages.

Autorisationer til it-systemer beskrives nærmere i Bilag B, samt i Kasse og regnskabsregulativets afsnit 10 og bilag 9.3.*

6.1.3. Kontakt med myndighederne

Samarbejde med tilsynsmyndigheden for personoplysninger.

Kommunen samarbejder med tilsynsmyndigheden i forbindelse med tilsynsmyndighedens udførelse af dens opgaver. Kommunen skal svare tilsynsmyndigheden inden for en rimelig frist, som fastsættes af tilsynsmyndigheden. Generelt skal svaret omfatte en redegørelse for de iværksatte foranstaltninger og de opnåede resultater som reaktion på bemærkningerne fra tilsynsmyndigheden.

Særlige forhold vedrørende Databeskyttelsesforordningen er beskrevet i bilag 9.*

Håndtering af sikkerhedsbrud

Der er etableret en procedure for håndtering af sikkerhedsbrud og eventuelt kontakt med relevante myndigheder. Brud på persondatasikkerheden skal anmeldes til Datatilsynet, medmindre

det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at kommunen er blevet bekendt med bruddet.

Er der sandsynlighed for, at sikkerhedsbruddet indebærer en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underrettes personen ligeledes om bruddet uden unødig forsinkelse.

Hvis personoplysninger behandles på kommunens vegne hos en tredjepart (databehandler), underretter denne kommune om ethvert brud uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Kommunen skal dokumentere alle brud på persondatasikkerheden sammen med oplysninger om de faktiske omstændigheder ved bruddet, dets virkning samt de trufne afhjælpende foranstaltninger.

Se administrationsgrundlag for Håndtering af brud på persondatasikkerhed i Bilag 9. *

6.1.4. Kontakt med særlige interessegrupper

Information om nye trusler, virus og sårbarheder

It-afdelingen skal holde sig orienteret inden for de benyttede platforme.
It-afdelingen skal informere relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder.
It-afdelingen er ansvarlig for eksternt samarbejde med de nødvendige informationskanaler, herunder samarbejde omkring it-sikkerhed med relevante eksterne interessegrupper og sikkerhedsorganisationer.

Kontakt med interessegrupper og fora

Der skal opretholdes passende kontakt med Digitaliseringsforeningen Sjælland, særlige interessegrupper, andre faglige sikkerhedsfora og faglige organisationer.
Dette som middel til at:

- forbedre viden om bedste praksis og være ajour med relevant sikkerhedsinformation
- sikre et bredt og opdateret kendskab til informationssikkerhedsmiljøet
- modtage tidlige varsler om alarm, meldinger og patches vedrørende angreb og sårbarheder
- få adgang til ekspertrådgivning om informationssikkerhed
- dele og udveksle information om nye teknologier, produkter, trusler og sårbarheder
- skabe passende kontaktpunkter ved håndtering af informationssikkerhedsbrud

6.1.5. Informationssikkerhed ved projektstyring

Projektmodellen skal indeholde følgende overvejelser omkring informationssikkerhed:

- Der skal være fokus på informationssikkerheden ved projektstyring, uanset projekttype.
- Projektmodellen skal indeholde overvejelser omkring informationssikkerhed, som skal dokumenteres i projektet.

- Identifikation af nødvendige sikringstiltag skal blandt andet ske ved hjælp af risikovurderinger, og der skal foreligge en afklaring af, om der skal udformes en konsekvensanalyse.

Retningslinjer samt værktøjer, der anvendes i forbindelse med projekter, fremgår på NORA. *
Projekthåndbogen:
https://noraapp.naestved.dk/ProjektTools
Digitaliseringsforum:
https://noraapp.naestved.dk/Organisation?item=4581

Overordnede retningslinjer ifm. anskaffelse fremgår desuden af bilag A afsnit 5.*

6.2. Mobilt udstyr og fjernarbejdspladser *

6.2.1. Politik for mobilt udstyr

Når der anvendes mobilt udstyr, bør det sikres, at kommunens informationer ikke bringes i fare. Der bør udvises forsigtighed, når mobilt udstyr anvendes på offentlige steder, møderum andre ubeskyttede områder. Mobilt udstyr bør også være fysisk beskyttet mod tyveri, især hvis udstyr efterlades f.eks. i bil andre transportmidler, hotelværelse, konferencecentre og mødesteder. Udstyr som indeholder vigtig følsom eller kritisk information, bør ikke være uden opsyn og bør om muligt, låses fysisk inde, eller der bør anvendes speciallås til at sikre udstyret.

Retningslinjer for anvendelse af bærbare og mobile enheder er beskrevet i Bilag 5.

6.2.2. Fjernarbejdspladser

Brug af fjernadgang uden for kommunens bygninger stiller særlige krav til anvendelse og sikring af det anvendte udstyr. Der skal være særlig opmærksomhed på lagring af data og håndtering af udskrifter fra kommunens systemer. Alle brugere af fjernadgang skal være bekendt med de særlige forhold.

Retningslinjer for fjernadgang til kommunens netværk er beskrevet i Bilag 4.

7. Medarbejdersikkerhed

Medarbejderne skal sikre sig, at deres håndtering af data, færden logisk (på pc-arbejdspladserne) såvel som fysisk (fysisk behandling af it-udstyr) er i overensstemmelse med kommunens informationssikkerhedspolitik, -regler og -procedurer.

Lederne har ansvar for, at alle deres medarbejdere er bekendt med og overholder kommunens informationssikkerhedspolitik, -regler og –procedurer og har opdaterede rettigheder til og færdigheder i at anvende relevante systemer.

Informationssikkerheden i kommunen afhænger af de medarbejdere, der behandler kommunens data. Det er derfor nødvendigt, at kommunen gennemfører den nødvendige efteruddannelse af både nuværende og nye medarbejdere.

7.1. Før ansættelsen

7.1.1. Screening

Medarbejdere

I forbindelse med en ansættelse skal den ansættende chef/leder vurdere kandidaten i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante informationssikkerhedsrisici. Med det udgangspunkt bør følgende baggrundsverifikation gennemføres:

- Tilfredsstillende referencer indhentes – fx en erhvervsmæssig eller en personlig reference.
- Stikprøvevis verifikation af ansøgerens CV (for fuldstændigheden og nøjagtigheden)
- Bekræftelse på uddannelse og faglige kvalifikationer
- Straffeattest

Der kan ved andre roller efter den enkelte chef/leders vurdering og/eller lovgivning være behov for indhentning af yderligere informationer inden en ansættelse – fx børneattest eller kreditvurdering.

Ved indgåelse af kontrakt med eksterne konsulenter skal den ansvarlige chef/leder tilse, at der sker et tilsvarende forsvarligt baggrundscheck.

Kontrahenter

I forbindelse med indgåelse af kontrakter med fx eksterne leverandører skal kontrahenten have gennemført tilsvarende baggrundsverifikation for det personale, som skal udføre arbejde for kommunen.

7.1.2. Ansættelsesvilkår og –betingelser

Medarbejdere

Alle medarbejdere skal ved ansættelse gøres bekendt med kommunens informationssikkerhedspolitik og de forpligtigelser der følger med ansættelsesforholdet.

Alle medarbejdere i kommunen har tavshedspligt efter straffelovens § 152 og forvaltningslovens § 27. Det følger heraf, at medarbejderne ikke uberettiget må videregive eller udnytte de fortrolige oplysninger, som de får kendskab til igennem arbejdet. Tavshedspligten gælder også efter ophør af ansættelsen i kommunen.

Inden medarbejderen må behandle kommunens informationer, skal den enkelte chef/leder sikre, at medarbejderen:

- Bliver introduceret til kommunens informationssikkerhedspolitik, -regler og procedurer – herunder sanktionsforhold (se pkt. 7.2.3).
- Bliver introduceret til forhold vedrørende sikkerhedshændelser.
- Bliver orienteret om databehandlingsskik – herunder om forvaltningslovens § 32 om ikke at må skaffe sig adgang til fortrolige oplysninger, som ikke er af betydning for udførelse af den pågældendes opgave, samt at der gennemføres logning i systemerne.
- Er bekendt med, at adgang til kommunens data under alle forhold skal være arbejdsmæssigt begrundet.
- Er bekendt med, at tavshedspligten også gælder efter ansættelsesforholdets ophør.
- Bliver orienteret om, at det ikke er tilladt at forsøge at omgå sikkerhedsmekanismer eller at foretage uautoriseret afprøvning af sikkerheden.

Det skal dokumenteres at ovenstående informationer er givet. Dette kan ske ved, at informationerne gives i forbindelse med ansættelseskontrakten som et bilag (Fortrolighedserklæring), eller ved at medarbejderen i kontrakten forpligtes til at gøre sig bekendt med materialet, som f.eks. kan indgå i en personalehåndbog eller lign.

Ovenstående regler gælder også personer, der ikke er ansatte - fx praktikanter og frivillige.

Kontrahenter

For at sikre, at kommunens informationssikkerhed ikke kompromitteres, skal ethvert formaliseret samarbejde være baseret på en skriftlig samarbejdsaftale/kontrakt.

Kontrahenten eller kontrahentens medarbejdere, som får adgang til eller muligvis kan komme i kontakt med klassificeret information, skal underskrive en fortrolighedserklæring. Det er den enkelte medarbejder, der skal underskrive denne – ikke leverandøren på medarbejdernes vegne.
Fortrolighedserklæringen skal være indarbejdet i den aftale, der er indgået med kommunen om leverandørforholdet.

Kontrahenten skal sikre, at tredjepart, der kan få adgang til kommunens data via samarbejdsaftalen, opfylder tilsvarende krav om fortrolighedspligt.

Hvis kontrahenten skal behandle personoplysninger for kommunen, skal systemejeren sikre udarbejdelse af en databehandleraftale.

7.2. Under ansættelsen

7.2.1. Ledelsesansvar

Det er chefens/lederens ansvar, at alle, som har adgang til kommunens data, it-systemer og netværk:

- holdes opdateret om kommunens informationssikkerhedsorganisation.
- er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med informationssikkerhed.
- holdes opdateret om informationssikkerhedsregler og -procedurer, så de kan leve op til koncernens informationssikkerhedspolitik.
- følger de retningslinjer og bestemmelser, der er for ansættelsen, inkl. kommunens informationssikkerhedspolitik.
- løbende bibringes en sikkerhedsforståelse således, at der opretholdes et højt bevidsthedsniveau om informationssikkerhed.
- fortsat har de nødvendige færdigheder og kvalifikationer og undervises med jævne mellemrum.

Hvis der er tale om en ekstern leverandør, som har adgang til kommunens data, it-systemer og netværk, er det chefens/lederens ansvar, at alle ovenstående forhold ligeledes gør sig gældende i forhold til leverandøren.

7.2.2. Bevidsthed om, uddannelse og træning i informationssikkerhed

Alle medarbejdere har ansvar for at kende og overholde informationssikkerhedspolitikken, -regler og –procedurer, samt påpege eventuelle risici, mangler eller uhensigtsmæssigheder.

Uddannelse i sikker omgang med data

Det skal sikres, at alle medarbejdere, og hvor det er relevant leverandører, er bekendt med og overholder kommunens informationssikkerhedsregler og –procedurer og i øvrigt har opdaterede færdigheder i at anvende relevante systemer, herunder anvendelse af sikker e-mail.

Alle medarbejdere skal undervises i, hvordan kommunens informationer klassificeres og hvordan informationerne - såvel elektroniske som fysiske - skal behandles og opbevares.

Alle medarbejdere skal undervises i, hvordan mundtlig kommunikation kan udgøre en sikkerhedstrussel.

Det er den enkelte ansattes nærmeste leder, som er ansvarlig for, at ovennævnte uddannelse og efteruddannelse finder sted og dokumenteres. Der kan foretages test af medarbejderens viden efter endt uddannelsesforløb med henblik på at vurdere såvel medarbejderens færdigheder på de behandlede områder som effekten af undervisningen.

Sikkerhedsuddannelse for it-medarbejdere

Alle it-medarbejdere eller medarbejdere med udvidede rettigheder skal uddannes i sikkerhedsaspekterne i deres job bl.a. for at mindske risiko for hændelser i forbindelse med deres særlige adgang til kommunens systemer.

Uddannelse og awareness

Der skal etableres og udbydes en informationssikkerhedsuddannelse for kommunens medarbejdere samt en for chefer og ledere, som relaterer til deres særlige ansvarsområder.

Informationssikkerhedsudvalget sikrer at der gennemføres periodiske awareness-kampagner, der skal sikre et højt bevidsthedsniveau om informationssikkerhed. Kampagnerne bør sammensættes således, at de er målrettet de forskellige målgrupper – fx chef/ledergruppen, alle medarbejdere, et center, virksomhed eller lignende.

Informationssikkerhedsudvalget sikrer sig indblik i de uddannelses- og awareness-aktiviteter, der foregår i kommunen.

7.2.3. Sanktioner

En overtrædelse af den gældende informationssikkerhedspolitik med tilhørende regler og procedurer kan, efter omstændighederne, medføre sanktioner, herunder ansættelsesretslige konsekvenser.

Hvis en medarbejder er vidende om, at kommunens informationssikkerhedspolitik overtrædes eller kompromitteres, skal dette håndteres, som beskrevet for sikkerhedshændelser og -brud.

7.3. Ansættelsesforholdets ophør eller ændring

Følgende forhold skal indgå i kommunens procedurer for ændring i ansættelsesforholdet samt for ansættelsesforholdets ophør i overensstemmelse med efterfølgende punkter.

7.3.1. Ændring af ansættelsesforhold

Ved ændring i ansættelses-/organisatoriske forhold, skal den personaleansvarlige sikre at adgange og rettigheder henholdsvis fjernes og tildeles.

7.3.2. Ansvar ved ansættelsens ophør

Den personaleansvarlige for den fratrædende medarbejder skal sikre, at medarbejderen ved fratrædelse informeres om sine pligter bl.a. med reference til fortrolighedserklæring.

Ved ophør af ansættelsesforholdet skal den personaleansvarlige sikre, at adgange og rettigheder fjernes.

Det skal i forbindelse med en opsigelse af et ansættelsesforhold vurderes, om den fratrædende medarbejder i sin arbejdsfunktion kan udgøre en risiko med hensyn til misbrug af tildelte rettigheder.

Hvis det er tilfældet, skal den personaleansvarlige overveje, hvordan risikoen kan nedbringes. F.eks. om der er rettigheder, der skal fratages den opsagte øjeblikkeligt, om arbejdsopgaver skal omlægges, eller om der skal ske fritstilling.

7.3.3. Returnering af aktiver ved fratrædelse

Den personaleansvarlige for den fratrædende medarbejder har ansvaret for at denne overdrager og returnerer alle kommunens aktiver.

7.3.4. Eksterne konsulenter

For eksterne konsulenter gælder tilsvarende, som beskrevet i afsnit 7.3.3.

8. Styring af aktiver

8.1. Ansvar for aktiver

8.1.1. Fortegnelse over aktiver

Formålet med fortegnelsen over aktiver med relation til information og informationsbehandlingsfaciliteter er at sikre, at kommunens aktiver er effektivt beskyttet. Fortegnelsen skal indeholde de aktiver, der er relevante i informationers livscyklus.

Formanden for Informationssikkerhedsudvalget er ejer af fortegnelser over aktiver og ansvarlig for, at fortegnelsen er fyldestgørende og vedligeholdt. Informationssikkerhedsudvalget bør revidere fortegnelsen minimum en gang årligt eller ved større organisatoriske ændringer.

Registrering af it-udstyr

Det er chefens ansvar, at relevant it-udstyr er registreret med ejer, bruger, serienummer og placering. Der skal vedligeholdes en fortegnelse over samtlige relevante enheder, som er forbundet til virksomhedens it-infrastruktur.

Registrering af infrastruktur

Det er chefens ansvar, at infrastrukturen er registreret med placering, navn, samt fabrikationsdata. For netværk gælder, at der skal være opdaterede netværksdiagrammer samt informationer om ip-adresser og scopes.

Registrering af systemer

Systemejeren (se rolle- og ansvarsbeskrivelse for systemejer i kapitel 6.1.1) har ansvar for, at registrering af fagsystemer og egenudviklede systemer sker i Kitos. Registreringen skal som minimum omfatte navn, version, kontrakt, databehandleraftale hvis påkrævet, navn på systemejer, arkivforpligtigelse, systemets klassifikation samt eventuelt indhold af persondata.
I forhold til egenudviklede systemer er det projektlederen, som i udviklingsfasen har ansvar for registrering af ovennævnte data. Efter idriftsættelse overgår ansvaret til systemejer.

Registrering af data

Det er dataejerens ansvar (se rolle- og ansvarsbeskrivelse for dataejer i kapitel 6.1.1), at data er klassificeret og registreret i henhold til klassificeringen i relevant fagsystem.

8.1.2. Ejerskab af aktiver

Ejerskab af aktiver er defineret i kapitel 8.1.1.
For et hvert registreret aktiv i organisationen skal udpeges en ejer, som har ansvar for aktivets livscyklus, og som er kvalificeret til at blive udpeget som aktivejer. Jf. kapitel 8.1.1 omfatter aktivejere: systemejer og dataejer.
Aktivejerens opgave er at:

1. Sikre, at aktiverne opføres i en fortegnelse jf. kapitel 8.1.1
2. Sikre, at aktiverne klassificeres og beskyttes på behørig vis jf. kapitel 8.2

3. Definere og regelmæssigt gennemgå adgangsbegrænsninger og klassifikationer for vigtige aktiver under hensyntagen til gældende regler for adgangsstyring
4. Sikre korrekt håndtering, når aktivet slettes og destrueres
5. Sikre, at der udarbejdes instruks for anvendelse af aktivet

8.1.3. Accepteret brug af aktiver

Der skal – hvor det er relevant – udarbejdes en politik/procedure for accepteret brug af aktiver jf. de aktiv-kategorier, som er nævnt i kapitel 8.1.1.
Det tilladte brug skal afspejle kommunens valgte sikkerhedsniveau.

8.1.4. Tilbagelevering af aktiver

Returnering af aktiver ved aftrædelse

Der skal udarbejdes en procedure som sikrer, at alle, som har haft adgang til kommunens informationsaktiver, returnerer disse ved forholdets ophør. Det skal fremgå af proceduren, hvem der har ansvar for at sikre dette.

Proceduren skal dække alle typer af tilknytningsforhold til kommunen fx medarbejdere, folkevalgte, frivillige, praktikanter, eksterne samarbejdspartnere

Informationer på privat udstyr ved forholdets ophør mv.

Medarbejderen har pligt til at slette eventuelle data tilhørende kommunen på privat udstyr ved forholdets ophør eller i tilfælde af, at medarbejderen bortgiver, sælger eller kasserer udstyr, som har været anvendt til håndtering af persondata på kommunens vegne.

Medarbejderen skal være indforstået med, at private enheder der har været anvendt til kommunens data, kan nulstilles (wipes) hvis det er nødvendigt af hensyn til datasikkerheden.

Andet

Hvis en medarbejder, en folkevalgt eller andre køber kommunens udstyr, skal procedurer følges for at sikre, at al relevant information overføres til kommunen og slettes fra udstyret.

Hvis en medarbejder eller kontrahent har viden, som er vigtig for den videre drift, skal sådan information dokumenteres og overføres til kommunen.

I opsigelsesperioden skal kommunen sikre, at opsagte medarbejdere og kontrahenter ikke foretager uautoriseret kopiering af relevante data. Ligeledes skal det sikres, at medarbejdere og kontrahenter ikke foretager skadevoldende handlinger på data og udstyr.

8.2. Klassifikation af information

8.2.1. Klassifikation af information

Kommunens informationer skal klassificeres efter lovmæssige krav, værdi og efter, hvor kritisk og følsom informationen er i forhold til uautoriseret offentliggørelse eller ændring.

Klassifikationen skal give personer, som behandler kommunens informationer og data, en kortfattet indikation af, hvordan informationen skal håndteres og beskyttes.

Ansvar for klassifikation

Ejere af aktivet, er ansvarlige for klassifikationen af aktivet.

Revurdering af klassifikation

Informationer kan i deres livscyklus ændre klassifikation og skal derfor revurderes regelmæssigt.

Klassifikationssystem

Klassifikation af informationer og data
Informationer og data skal indplaceres i følgende klassifikationssystem.

Personoplysninger	Andre oplysninger
Følsomme personoplysninger	Fortrolige oplysninger
Fortrolige personoplysninger	Interne oplysninger
Almindelige personoplysninger	Uklassificerede

- Personoplysninger omfatter enhver form for information om en identificeret eller identificerbar fysisk person, og opdeles i de kategorier, der anvendes i Databeskyttelsesforordningen (2016/679 af 27. april 2016) og Databeskyttelsesloven (Lov nr. 502 af 23. maj 2018): Almindelige personoplysninger og følsomme personoplysninger. De mest private af de almindelige personoplysninger er fortrolige (i henhold til bl.a. forvaltningsloven), og skal beskyttes på linje med følsomme personoplysninger (som altid også er fortrolige).
- Andre oplysninger omfatter alle oplysninger, som ikke er personoplysninger
- Ved interne oplysninger forstås oplysninger, som er tilgængelige for alle internt i kommunen
- Ved fortrolige oplysninger forstås oplysninger, som kun en mindre og nærmere defineret gruppe personer må få adgang til
- Ved uklassificerede oplysninger forstås oplysninger, som må videregives til den brede offentlighed

Klassifikation af systemer

Efterfølgende vurderes systemerne på baggrund af integritet, fortrolighed og tilgængelighed, hvorefter risikoreducerende foranstaltninger kan iværksættes.
Systemerne klassificeres efter det hovedprincip, at det er systemets data, som afgør systemets klassifikation. Dette sker ved, at data tildeles en score for konsekvenserne af brud på hvert af de tre områder fortrolighed, integritet og tilgængelighed. Denne score lægges sammen, og summen angiver systemets kritikalitet og dermed også dets klassificering.

Klassifikationen udgør sammen med risikovurderingen grundlaget for om og i givet fald hvordan, kompenserende foranstaltninger skal iværksættes.

Uddannelse i klassificering af informationer

Alle med en fysisk eller logisk adgang til kommunens systemer, data og informationer skal modtage instruktioner om, hvordan data er klassificeret og skal håndteres. Instruktionen skal tilpasses den enkeltes jobfunktion/opgaver.

8.2.2. Mærkning af information

Der skal udarbejdes og implementeres et passende sæt af procedurer til mærkning af information i overensstemmelse med klassifikationssystemet jf. kapitel 8.2.1.

8.2.3. Håndtering af aktiver

Der skal udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med klassifikationssystemet jf. kapitel 8.2.1
Proceduren skal indeholde regler for håndtering, lagring, behandling og kommunikation.

8.3. Mediehåndtering*

8.3.1. Styring af bærbare medier

Brug af bærbare medier til fortrolige data

Alle databærende medier skal beskyttes mod uautoriseret adgang. Der er derfor etableret forretningsgange for autorisation til data og systemer, ligesom fysiske datamedier skal være beskyttet. (Fysiske datamedier kan f.eks. være pc'er, mobiltelefoner og eksterne lagringsenheder).

Desuden skal udskrifter med personoplysninger håndteres på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med fortrolige personoplysninger.

Retningslinjer for bærbare medier er beskrevet i bilag 5.

Når fortrolige eller følsomme personoplysninger lagres på bærbare digitale medier, herunder på bærbare computere, mobiltelefoner eller tablets, skal der anvendes kryptografi til at beskytte oplysningerne, se også kapitel 10.1.1.

Den enkelte it-bruger skal identificere sig over for systemerne inden adgangen kan etableres. Sammen med identificeringen skal der ligeledes angives et personligt password eller tilsvarende autentifikationsløsning.

Retningslinjer for anvendelse af adgangskoder samt beskyttelse af dataadgang er beskrevet i bilag 1.

Opbevaring og registrering af datamedier

Data på medier skal behandles med samme omhu som data på centrale systemer.
Retningslinjer for bærbare medier er beskrevet i bilag 5.

8.3.2. Bortskaffelse af medier

Bortskaffelse og genbrug af medier

Udskrifter med fortrolige eller følsomme personoplysninger må ikke bortskaffes som almindeligt affald, men skal lægges i beholdere, der er beregnet til papirmateriale til destruktion. Beholdere med papirmateriale til destruktion skal holdes aflåste. Alle datamedier skal slettes inden genbrug.

Hvis en ekstern leverandør benyttes til destruktion af kommunens datamedier, skal det sikres at leverandøren efterlever de aftalte sikkerhedskrav. Alle datamedier, f.eks. harddiske, disketter, cd'er, dvd'er, bånd og hukommelsesenheder skal sikkerhedsslettes eller destrueres inden bortskaffelse.

8.3.3. Fysiske medier under transport

Instruks for intern og ekstern post behandling

Al post er som udgangspunkt tjenestepost, dvs. post modtaget i arbejdsmæssig sammenhæng. Arbejdsgange i forbindelse med håndtering, skanning og fordeling af posten er opdelt i 2 arbejdsfunktioner.

- Postfunktionen: Modtagelse, sortering og åbning.
- Skanningsfunktionen: Klargøring, skanning og arkivering.

Ved inddatering af papirpost og lignende til kommunens digitale løsninger, skal oplysningerne gemmes på den rigtige sag. Under og efter inddatering skal materialet håndteres på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med fortrolige personoplysninger.

Der er udarbejdet retningslinjer for modtagelse og scanning af post. Retningslinjerne er tilgængelige i postfunktionen.

Forsendelse af fysiske breve bør så vidt muligt undgås og sendes i stedet vha. doc2mail. Retningslinjer for afsendelse fremgår på NORA.

Brug af datamedier

Udstyr eller medier, der indeholder fortrolig information må kun forsendes med sikker kurer, eller via en præcis sporbar leveringsmetode.

Benyttelse af bærbare datamedier skal være forretningsmæssigt begrundet.

Der skal føres en log over medier med fortrolige informationer, som er blevet flyttet fra sikre områder. Loggen skal opbevares og være tilgængelig for revision.

Udskrifter med fortrolige eller følsomme personoplysninger må som udgangspunkt ikke komme uden for kommunens bygninger. Er det undtagelsesvist nødvendigt at tage udskrifter med sådanne oplysninger med uden for arbejdspladsen, skal der udvises den yderste påpasselighed, herunder i forbindelse med transporten til og fra arbejdspladsen.

Bærbare medier med personoplysninger eller fortrolig information skal krypteres. Vejledning i kryptering af usb medier findes på NORA.

8.4. Risikovurdering af informationsaktiver

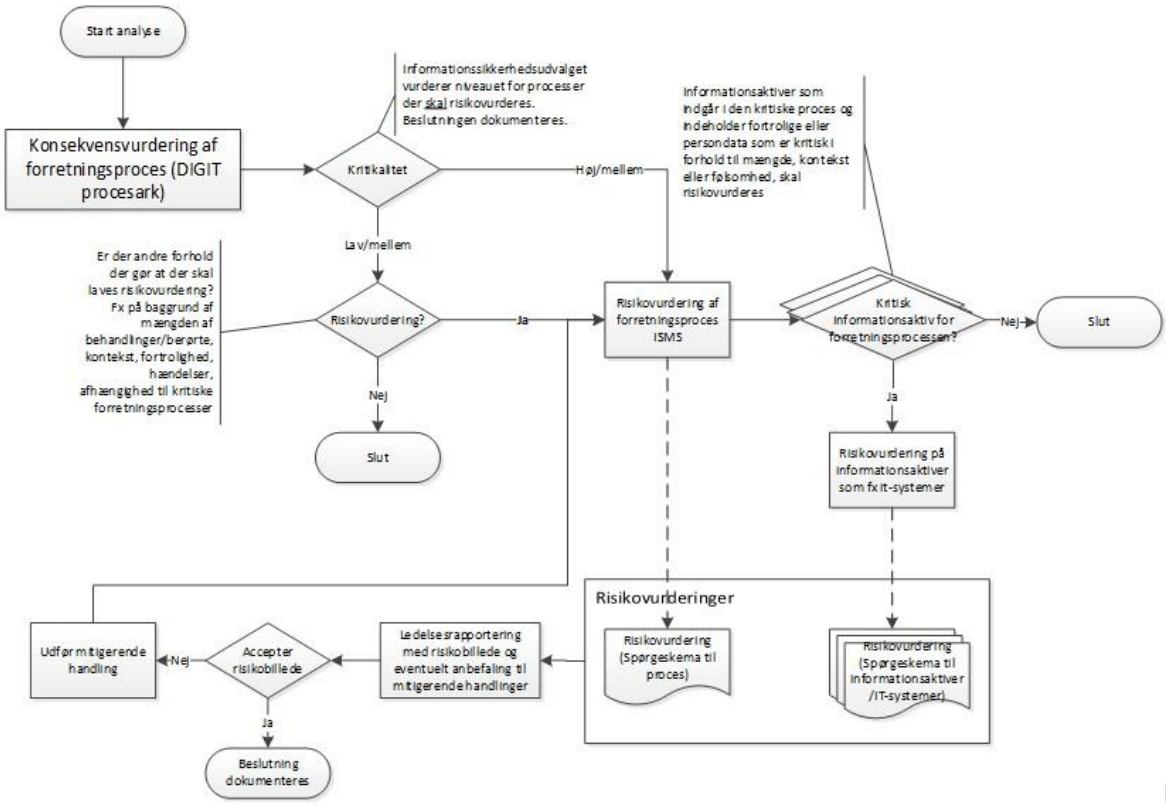
Risikovurderingen i Kommunen skal understøtte en effektiv afdækning, håndtering og imødegåelse af risici relateret til beskyttelse af Kommunens kritiske informationsaktiver. Kritiske informationsaktiver omfatter informationsaktiver, der ved brud på tilgængeligheden, fortroligheden og/eller integriteten vil kunne få væsentlige konsekvenser for Kommunen.

Risikovurderingen skal sikre, at system- og dataejere er bevidste om alle kendte risici for egne informationsaktiver, har taget aktivt stilling til den mulige konsekvens heraf for kommunen og har truffet beslutning om igangsættelse af nødvendige imødegående handlinger.

Én gang årligt skal der gennemføres en risikovurderingsproces for alle eksisterende, kritiske informationsaktiver. Desuden skal risikovurderingsprocessen anvendes ved hændelser, ændringer i trusselsbilledet, it-anskaffelser og systemændringer.

Informationssikkerhedsudvalget har ansvar for at igangsætte den årlige risikovurderingsproces samt at beslutte, hvilke processer der skal risikovurderes. Informationssikkerhedskoordinatoren har ansvar for at drive processen og præsentere et samlet risikobillede for informationssikkerhedsudvalget med tilhørende anbefalinger til en handlingsplan.

For konsekvensvurdering af forretningsprocesser og dokumentation af risikovurdering af processer og informationsaktiver henvises til proceduren Risikovurdering af informationsaktiver.



9. Adgangsstyring

Formål

Adgangen til at udføre handlinger på kommunes it-systemer skal beskyttes af autorisationssystemer. Systemerne har til formål at sikre mod uautoriserede ændringer, ordrer, fejl og svindel. Kommunens medarbejdere er medvirkende til beskyttelse af informationsaktiverne gennem korrekt brug af autorisationssystemerne. Reglerne skal omsættes til konkrete procedurer.

9.1. Forretningsmæssige krav til adgangsstyring

9.1.1. Politik for adgangsstyring

Adgangen til kommunens informationer skal beskyttes af autorisationssystemer og/eller fysiske adgangskontrol foranstaltninger. Det skal sikres, at der kun gives adgang til informationer til personer, der er beskæftiget med de formål, hvortil informationerne skal behandles. Den enkelte bruger må efter "Need-to-know-princippet" ikke autoriseres til anvendelse af flere informationer, end de har behov for til løsning af deres opgaver. Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til informationer og anvendelser, som de er autoriserede til.

For privilegerede rettigheder skal tildelingen af adgang ske ud fra "Need-to-use-princippet" baseret på minimumskrav for deres funktioner.

Der bør være en opdeling af de funktioner, der søger om adgang til informationer, de der autoriserer adgang, og de der administrerer adgang, og der skal etableres en formel procedure for denne proces.

Det skal løbende sikres, at de autoriserede personer fortsat opfylder betingelserne for adgang til informationer. Kontrol heraf skal ske regelmæssigt, eventuelt som stikprøver.

Når en bruger ikke længere har behov for adgang til bestemte informationer eller vurderes at udgøre en risiko, skal der ske en lukning af adgange.

Al adgang til data skal være tjenstligt begrundet. Ingen må tilgå data, som ikke er relevante for den tjenstlig opgaveløsning – uanset de givne adgangsrettigheder.

Politik for adgangsstyring er uddybet i bilag B. *

9.1.2. Adgang til netværk og netværkstjenester

Adgangsstyringen skal ske via en unik bruger-id og en adgangskode. Adgangen til services og applikationer bør ske gennem den rolletildeling, der autoriseres i den enkeltes brugerprofil. Ved særligt kritiske systemer kan der stilles krav om yderligere identificering af den enkelte bruger ved en "two-factor-identification".

Adgangen til det interne netværk fra andre lokationer end kommunens skal være adgangskodebeskyttet samt ske via en krypteret datakommunikation (fx VPN).

Adgang, sletning og ændring af adgang gives af nærmeste leder eller på instruks fra nærmeste leder.

Team Servicedesk og It skal ved styring af brugernes netværksadgang sikre imod uautoriseret anvendelse af fælles netværk og hertil knyttede tjenester

Retningslinjer for autorisation, herunder tildeling, ændring og sletning af autorisationer, er beskrevet i bilag B. *

Retningslinjer for anvendelse af digitale signaturer fremgår af bilag 6. *

9.2. Administration af brugeradgang

9.2.1. Brugerregistrering og -afmelding

Personer, som er ansat, byrådsmedlemmer eller de som har konsulent/leverandøraftale, kan oprettes som brugere. Andre personer kan oprettes som brugere (fx forskere), men dette kræver særskilt dispensation fra IT-Teamlederen.

Brugere skal have unikt bruger-id og adgangskode, der gør det muligt at identificere den person, som er ansvarlig for en given aktivitet. Adgangsrettigheder skal afstemmes med arbejdsopgavernes behov. Tilgang, afgang og ændringer af rettigheder skal godkendes af nærmeste chef/leder og arkiveres. Det er den enkelte chef/leders ansvar at verificere brugerens identitet.

Fælles brugerprofiler må kun ske som en undtagelse, der skal begrundes i et forretningsmæssigt behov. Oprettelse af en sådan bruger skal godkendes af systemejer samt IT-Teamlederen og dokumenteres.

Autorisationerne skal som minimum angive i hvilket omfang den enkelte bruger må forespørge, inddatere eller slette informationer. Herudover kan der være behov for styring af transaktionsrettigheder, hvorfor der skal anvendes en rollebaseret adgangsstyring.

Brugere må som udgangspunkt ikke have administratorrettigheder på kommunens enheder eller systemer. Der kan dispenseres midlertidigt i særlige tilfælde.

Adgangsrettigheder til fysiske arkiver/medier (dokumenter, lyd- videooptagelser mm) med klassificerede informationer skal dokumenteres.

Retningslinjer ved autorisation fremgår af bilag B. *

9.2.2. Tildeling af brugeradgang

Det er systemejers ansvar at tildele brugeradgang til dennes it-systemer. Det er brugerens nærmeste leder, der anmoder systemejer om adgang.

Ved brugeroprettelse eller nulstilling af adgangskode skal brugere tildeles en, midlertidig unik adgangskode, som skal ændres umiddelbart efter første anvendelse.

Adgang til fysiske arkiver/medier med klassificerede informationer skal ligeledes tildeles i forhold til brugerens behov for at kunne løse sine opgaver. Brugeradgang gives af den enkelte chef/leder, og kun de brugere, der har behov må gives adgang.

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 en officielt godkendt elektronisk autorisationsblanket. *

Retningslinjer fremgår af bilag B. *

9.2.3. Styring af privilegerede adgangsrettigheder

De privilegerede adgangsrettigheder skal registreres for de enkelte systemer og it-platforme.

Der skal foreligge en procedure for at sikre, at privilegerede rettigheder ikke misbruges.

Antallet af brugerkonti med domæne- eller lokaladministratorrettigheder skal begrænses mest muligt.

Et bruger-id med privilegerede rettigheder må ikke anvendes til kommunens almindelige forretningsaktiviteter.

Det er systemejers ansvar at adgangskoder ændres i henhold til gældende procedure, samt hvis udenforstående får kendskab til disse.

Systemejer har ansvar for at standardadgangskoder ændres efter installation af et nyt system, og generiske administrator-id skal fjernes/inaktiveres, hvis der er muligt i forhold til systemets konfigurationsegenskaber.

Hvis en person med privilegerede rettigheder fratræder, er det systemejers ansvar at disse privileger ændres med det samme.

Når en person med privilegerede rettigheder ikke længere har behov for adgang til disse privileger, eller hvis vedkommende vurderes at udgøre en risiko, skal der straks ske en lukning af adgangsrettigheder.

Systemejer skal løbende sikre, at bruger(-profiler) med privilegerede rettigheder fortsat opfylder betingelserne for adgang samt, at de besidder de nødvendige kompetencer til at varetage deres opgave. Ligeledes skal identificeres inaktive profiler eller tilsvarende, der skal fjernes eller ændres. Kontrol heraf skal ske en gang hvert kvartal.

9.2.4. Styring af hemmelig autentifikationsinformation om brugere

Brugerne skal, inden adgang gives, erklære, at de vil behandle personlig adgangskode fortroligt. Det kan ske i form af et selvstændigt dokument eller være indeholdt i ansættelsesvilkår og –betingelser.

Adgangskoden må ikke oplyses til andre, og må kun oplyses til brugeren selv, hvis der kan etableres en entydig identifikation. Systemejer etablerer og vedligeholder en procedure for, hvordan en brugers identitet fastslås, før en ny midlertidig adgangskode må udleveres.

Ved ny oprettelse eller nulstilling af adgangskode skal brugere tildeles en, unik midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse.

Krav til adgangskode

Adgangskoder til kommunens netværk bør overholde bedste praksis på området og skal være beskrevet i en procedure.

Adgangskoden skal skiftes regelmæssigt afhængigt af kodeordets kompleksitet i henhold til gældende procedure, samt hvis udenforstående får kendskab til dette. Procedure skal udarbejdes af Team Servicedesk og It.

En bruger må ikke kunne vælge en adgangskode, der er identisk med de senest 10 benyttede adgangskoder.

Kun systemer der er autoriseret af kommunen, må anvende automatisk login eller løsninger, hvor adgangskoder gemmes i genveje eller på funktionstaster.

Ved brugeroprettelse (information via e-Boks) eller nulstilling af adgangskode skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse. Kode må ikke udleveres gennem telefonen. Der skal oprettes en ”sag” og midlertidig kode udleveres til slutbruger (en anden end medarbejderen) på sagen. *

Retningslinjer for kodeord fremgår i bilag 1. *

Brug af adgangskodebeskyttet pauseskærm

Hvis at arbejdsstationen forlades, skal brugeren selv aktivere adgangskodebeskyttet pauseskærm (Ctrl–Alt–Del eller WIN–L). Som supplement skal adgangskodebeskyttet pauseskærm aktiveres automatisk på pc-arbejdspladser efter 15 minutters inaktivitet.

Ved adgang via mobile løsninger skal der implementeres automatisk sign-off efter kort tids inaktivitet. Se evt., nærmere retningslinjer herfor i afsnit 6.2. *

Fysiske arkiver/medier

Adgang til fysiske arkiver/medier med klassificerede informationer skal sikres med autentifikationsinformation i form af nøgler, nøglekort eller lignende.

9.2.5. Gennemgang af brugeradgangsrettigheder

Brugere med administratorrettigheder skal gennemgås hver 3. måned (oftere end normale brugere).

Systemejer skal løbende sikre, at de autoriserede brugerprofiler fortsat opfylder betingelserne for adgang til informationer. Ligeledes skal identificeres inaktive profiler eller tilsvarende, der skal fjernes eller ændres. Desuden skal der ske en løbende kontrol af, at der ikke sker misbrug af tildelte rettigheder. Kontrol heraf skal ske en gang hvert kvartal. *

Der skal udarbejdes og iværksættes procedurer for hver måned at sammenholde oversigter fra kommunens lønsystem over fratrådte medarbejdere med aktive brugere i Active Directory for at identificere brugere, som er fratrådt. Findes der fratrådte medarbejderes, hvis adgang fortsat er aktiv, skal disse deaktiveres og/eller slettes. *

Systemejernes opgaver er uddybende beskrevet i bilag A.*

9.2.6. Inddragelse eller justering af adgangsrettigheder

Når en bruger ikke længere har behov for adgang til bestemte informationer, skal der ske en lukning af adgangsrettigheder.

Hvis en bruger vurderes at udgøre en risiko, skal der ske en umiddelbar lukning af adgangsrettigheder.

Ved ændring af en medarbejders rolle skal rettigheder og privileger revurderes af nærmeste chef/leder – både så vidt angår tildeling som sletning af rettigheder.

Ved fratrædelse skal nærmeste chef/leder iværksætte en sletning af brugerens id mm. Alle profiler og adgange til kommunens netværk og systemer skal slettes.

Autoriserede brugere, som ikke har været aktive på kommunens netværk, skal automatisk deaktiveres efter 3 måneder.

9.3. Brugernes ansvar

Uanset tildelte autorisationer må en bruger i sit virke ikke skaffe sig adgang til klassificerede informationer, som ikke er af betydning for udførelsen af den pågældendes opgaver.

9.3.1. Brug af hemmelig autentifikationsinformation

Adgangskode må ikke oplyses til andre, og må kun oplyses til brugeren selv, hvis der kan etableres entydig identifikation.

Adgangskoder er strengt personlige og må ikke deles med andre. Valg af adgangskode skal ske i overensstemmelse med pkt. 9.2.4.1 Ved mistanke om kompromittering skal adgangskoden straks ændres, og der skal rapporteres til nærmeste leder.

Brugere må kun opbevare kopier af adgangskoder til systemer i en kodeordsdatabase der er godkendt i kommunen.

Der må ikke anvendes samme adgangskode til private og arbejdsmæssige formål. Kodeord der bruges på kommunens interne systemer bør ikke samtidig anvendes til eksterne tjenester, uagtet at det er til arbejdsmæssige formål.

Hvis at arbejdsstationen forlades, skal brugeren selv aktivere adgangskodebeskyttet pause-skærm.

Retningslinjer for adgangskoder er beskrevet i bilag 1. *

9.4. Styring af system- og applikationsadgang

9.4.1. Begrænset adgang til informationer

Der må i systemer, hvor der behandles fortrolige oplysninger samt almindelige og følsomme personoplysninger, kun gives adgang til autoriserede brugere, og der skal ske en maskinel log-ning af alle transaktioner.

Den enkelte brugers profil skal altid være i overensstemmelse med den rolle, som brugeren skal udføre.

For så vidt angår personoplysninger skal logningen mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Ved eventuelle sikkerhedsmæssige hændelser kan loggen opbevares i op til 5 år.

Politikken for adgangskontrol på de enkelte systemer er vedtaget og fremgår i bilag 1. *

9.4.2. Procedurer for sikker log-on

Systemadgang skal beskyttes af en sikker log-on procedure – her ved anvendelse af unikt bru-ger-id og adgangskode.
Ved vurderet behov kan der stilles krav om yderligere identificering af den enkelte bruger ved en "two-factor-identification".

I systemer der indeholder persondata, skal der foretages logning af alle afviste adgangsforsøg. Afviste adgangsforsøg skal gennemgås regelmæssigt.
Logningen skal som minimum omfatte følgende:

- Dato og tidspunkt for seneste log-on.
- Oplysninger om fejlslagne log-on forsøg siden sidst gennemførte log-on forsøg.

Brugerprofil skal låses efter tre fejlslagne log-on forsøg.

Der skal oprettes en sikkerhedshændelse ved tilbagevendende eller mistænkelig fejlslagne log-on forsøg.

Log-on må ikke vise den indtastede adgangskode, og den må ikke transmitteres i klar tekst over netværket.

Retningslinjer for fjernadgang findes i bilag 4.*

Retningslinjer for generelt log-on og anvendelse af adgangskoder fremgår i bilag 1.*

9.4.3. System for administration af adgangskoder

Der må kun benyttes it-systemer, der automatisk kan styre de krav, der findes til adgangskoder.

Anvendelsen af adgangskoder skal ske i overensstemmelse med pkt. 9.2.4.

9.4.4. Brug af privilegerede systemprogrammer

Team Servicedesk og It begrænser og styrer adgangen til programmer, f.eks. utilities, der kan påvirke eller omgå systemers eller enheders sikkerhed.

Team Servicedesk og It forebygger, at unødige privilegerede systemprogrammer ikke er installeret eller tilgængelige på brugeres pc'er.

Anvendelsen af privilegerede systemprogrammer skal reduceres til et minimum af betroede og autoriserede brugere.

9.4.5. Styring af adgang til kildekoder til programmer

Der skal være procedurer for sikker håndtering af Kommunens kildekode for egenudviklede programmer, software robotter, installationsscript mv.

10. Kryptografi

10.1. Kryptografiske kontroller

10.1.1. Anvendelse af kryptografi

Kryptografi anvendes på data efter en konkret risikovurdering. Kryptografi anvendes til at opfylde målsætninger om fortrolighed, integritet, uafviselighed og autenticitet.

Når fortrolige og/eller følsomme personoplysninger transporteres, sendes eller opbevares via netværk, skal der foretages en risikovurdering med henblik på at fastlægge krypteringsbehovet.

Kodeord skal opbevares krypteret i henhold til foretaget risikovurdering med særlig fokus på administrative konti til essentielle infrastruktursystemer

Som udgangspunkt anvendes en tidssvarende og tilstrækkelig kryptostandard til kryptering af data.

Retningslinjer for kryptering fremgår i bilag 9 – Beskyttelse af persondata og i bilag 6 – Retningslinjer for anvendelse af digital signatur. *

Ved forsendelse via e-mail fremgår retningslinjerne i bilag 2. *

10.1.2. Administration af nøgler

Autenticiteten af offentlige nøgler skal sikres ved brug af godkendte certifikater, som kan valideres af uvildig tredje part.

For at sikre at kommunen altid har adgang til data ved nøglemedarbejderes fratrædelse eller ved bortkomst af nøgle, skal der udarbejdes en procedure, som sikrer at krypteringsløsninger har et "master" kodeord eller lignende mulighed, hvorved det er muligt for kommunen at dekryptere alle data, som kommunen er dataansvarlig for.

Der skal ligeledes udarbejdes særlige beskyttelsesforanstaltninger til denne "master-key"/løsning. Beskyttelsesforanstaltningerne godkendes af It-Teamleder, inden master-key løsningen etableres.

For at øge sikkerheden i forbindelse med krypteringsnøgler skal kommunen beskrive, hvordan systemet administreres, herunder procedurer og metoder til eks.:

- Generering af nøgler.
- Ændring og opdatering af nøgler.
- Håndtering af kompromitterede- og udløbne nøgler.
- Retablering af mistede nøgler.
- Logning og auditering af nøgleadministrationen.

I forhold til adgang til systemer med digital signatur, skal der udarbejdes konkrete procedurer, som beskriver tildeling af adgang, fjernelse af adgang samt adgang til konkrete systemer. Der

skal i kommunen udpeges en medarbejder, som har ansvaret for opfølgning og kontrol med adgang til systemer via digital signatur, herunder skærpet opmærksomhed på den digitale signatur som en juridisk bindende underskrift.

Beskrivelse af VPN og PKI-infrastrukturen skal fremgå i en driftshåndbog (Team Servicedesk og It's fællesdokumentationen). Se retningslinjer for It-medarbejdere i Bilag E. *

11. Fysisk sikring og miljøsikring*

11.1. Sikre områder

11.1.1. Fysisk perimetersikring

Sikre områder

Den fysiske sikkerhed skal stå i et naturligt forhold til de værdier, som skal beskyttes. Kravene til sikring af centralt udstyr er således højere, end kravene til sikring af udstyr i kontormiljø-erne.

Den fysiske sikkerhed er tilrettelagt ud fra en konkret risikovurdering og skal som minimum overholde retningslinjerne, som de er beskrevet i bilag I. Den fysiske sikkerhed skal i relevant omfang være dokumenteret således, at kommunens ledelse - som en del af den generelle it-risikostyring - kan planlægge sikkerhedsprocedurer i forhold til den fysiske sikkerhed.

Den fysiske sikkerhed skal afvejes 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'er, printere og tilsvarende periferiudstyr.

Sikkerhedsniveau 3: Omfatter decentrale arbejdspladser og bærbare pc'er uden for kommu-nens lokaler, herunder bærbare enheder som USB-nøgler, Smartphones, IPads og lignende.

Adgang til serverrum og (it-klargøringsrum, krydsfelter mv.)

Adgangen skal beskyttes med adgangskort (adgangskontrolsystem). Kort må kun udstedes til godkendte medarbejdere med et arbejdsbetinget behov.
Retningslinjer fremgår af bilag E – Retningslinjer for it-medarbejdere.

Gæsters adgang

Adgangskort til serverrum må ikke udleveres til eksterne leverandører.
Retningslinjer fremgår af bilag J – Retningslinjer for eksterne leverandører.

Indbrudsalarmer

Kommunen skal anvende passende alarmsystemer på samtlige bygninger og lokaler.
Retningslinjer for sikkerhedsniveau 1 fremgår af bilag I.

11.1.2. Fysisk adgangskontrol

Registrering af gæster

Der foretages ikke registrering af gæster.

Adgangskort til håndværkere og andet midlertidigt personale

Håndværkere, reparatører, teknikere og andre gæster, kan få udleveret midlertidige adgangskort, hvor et arbejdsbetinget behov gør dette relevant.

Adgangskort

Adgangskontrolkort er personlige. De skal opbevares forsvarligt og må ikke overdrages til andre.

11.1.3. Sikring af kontorer, lokaler og faciliteter

Oplysninger om sikre områder
Oplysninger om sikre områder og deres funktion, fx dokumentation af installationer, må alene videregives ud fra et arbejdsbetinget behov.

11.1.4. Beskyttelse mod eksterne og miljømæssige trusler

Miljømæssig sikring af serverrum

Serverrum, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger.
Foranstaltningerne er nærmere beskrevet i bilag I.

Forsyningssikkerhed

Alle forsyninger som elektricitet, vand, kloak, varme, og ventilation har den nødvendige kapacitet, og løbende inspiceres for at forebygge uheld, der kan have indflydelse på informationsaktiverne.

Data-og telekommunikationsforbindelser skal etableres via minimum to adgangsveje for forretningskritiske systemer.

Foranstaltningerne er nærmere beskrevet i bilag I.

Brandsikring

Serverrum må ikke benyttes som lager for brændbare materialer. Serverrum skal sikres med veldimensioneret automatisk brandslukningsudstyr.
Foranstaltningerne er nærmere beskrevet i bilag I.

11.1.5. Arbejde i sikre områder

Aflåsning af lokaler og bygninger

Alle døre og vinduer skal kunne låses forsvarligt.

Ubenyttede lokaler i sikre områder

Når serverrum og krydsfelter mv. forlades, også for en kort periode, skal lokalet/bygningen være aflåst.

11.1.6. Områder til af- og pålæsning

Af- og pålæsningsområder til it-centerets lager skal indrettes, så risiko for uautoriseret adgang til kommunens øvrige områder mindskes.

Adgang til af- og pålæsningsområder må kun gives til identificerede og autoriserede personer.
Retningslinjer fremgår af bilag I.

11.2. Udstyr

11.2.1. Placering og beskyttelse af udstyr

Adgang til serverrum og hovedkrydsfelter

Adgang til serverrum og hovedkrydsfelter tillades kun efter godkendt autorisation eller ved overvåget adgang af autoriserede medarbejdere fra Team Servicedesk og IT.
Retningslinjer fremgår af bilag E og bilag I.

Spisning og rygning i nærheden af udstyr

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

Distribueret it-udstyr

Alle decentrale serverrum og lignende faciliteter med kritisk it-udstyr skal aflåses for at hindre uautoriseret adgang til disse.

Retningslinjer fremgår af bilag E

Aflåsning af hovedkrydsfelter og lignende teknikrum

Alle krydsfelter og andre teknikrum skal være aflåste.
Retningslinjer fremgår af bilag E.

11.2.2. Understøttende forsyninger (forsyningssikkerhed)

Køling

Serverrum skal sikres med veldimensionerede airconditionanlæg.
Retningslinjer fremgår af bilag I.

Nødstrømsanlæg

Alle server-systemer skal beskyttes med nødstrømsanlæg til at sikre fortsat drift i tilfælde af strømudfald.

Retningslinjer fremgår af bilag I.

11.2.3. Sikring af kabler

Kabler til datakommunikation skal beskyttes mod uautoriserede indgreb og skader.

Faste kabler og udstyr skal mærkes klart og entydigt. Beskrevet i driftsprocedure (hvidbog) dokumentation ligger på NK SharePoint.

11.2.4. Vedligeholdelse af udstyr

Team Servicedesk og IT er ansvarlig for, at der føres log over alle fejl og mangler samt reparationer og forbyggende vedligeholdelse.
Kun godkendte leverandører må udføre reparationer og vedligeholdelse.

11.2.5. Fjernelse af aktiver

Udstyr må kun fjernes fra kommunen, hvis der foreligger en underskrevet kvittering på det udleverede.

11.2.6. Sikring af udstyr og aktiver uden for organisationen

Fortrolige informationer i offentlige rum

Der skal udvises forsigtighed ved omtale af fortrolige informationer i offentlige rum. Fortrolige informationer må ikke efterlades uden opsyn i offentligt tilgængelige rum, fx driftsdokumentation og netværksdiagrammer mv.

11.2.7. Sikker bortskaffelse eller genbrug af udstyr

Næstved Kommunes data må ikke blive tilgængelige for uvedkommende ved kassation eller genbrug af udstyr.

Der udarbejdet retningslinjer for destruktion af databærende medier – bilag 8. Derudover er der skitseret retningslinjer for håndtering af data ved reparation og service samt sletning af data jf. Databeskyttelseslovgivningen – bilag 9.

11.2.8. Brugerudstyr uden opsyn

Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyr, der benyttes til at behandle kritiske/følsomme informationer, skal placeres så informationerne ikke kan ses af uvedkommende. Det er brugerens ansvar at uovervåget udstyr enten er slukket eller beskyttet mod uautoriseret adgang ved at låse udstyret, så adgangskode skal anvendes. Mobilt udstyr der forlades kortvarigt, skal låses med pauseskærm med adgangskode. Ved inaktivitet skal enheden automatisk låses efter en kortere periode, som ikke bør overstige 5 minutter. Derudover skal uovervåget udstyr i videst muligt omfang opbevares under lås, så det er fysisk beskyttet mod tyveri.

Retningslinjer er uddybet i bilag 1.

11.2.9. Politik for ryddeligt skrivebord og blank skærm

Brug af adgangskodebeskyttet pauseskærm

Adgangskodebeskyttet skærmlås skal aktiveres på pc-arbejdspladser efter 15 minutters inaktivitet.

Retningslinjer fremgår af bilag 1

Opbevaring af fysiske dokumenter

Skriveborde skal ryddes for fortrolige dokumenter senest ved arbejdsdagens afslutning. Dokumenter med personhenførbare oplysninger må ikke ligge med forsiden opad, når skrivebordet forlades. Dokumenter med personhenførbare oplysninger skal opbevares i aflåst skab eller skuffe efter arbejdstid.

Fortrolige dokumenter skal opbevares i aflåst skab eller skuffe.

12. Driftssikkerhed

12.1. Driftsprocedurer og ansvarsområder*

12.1.1. Dokumenterede driftsprocedurer

Sikring af arbejdsstationer inden ibrugtagning

Alle arbejdsstationer skal installeres ved brug af den, af Team Servicedesk og IT, valgte værktøj til installation der skal sikre ensartet opsætning af arbejdsstationer. Alle arbejdsstationer skal sikres inden brug. Minimum sikring inkluderer installation af seneste sikkerhedsrettelser for operativsystemet og antivirusprogram.

Retningslinjer og dokumentation fremgår i Team Servicedesk og It's driftsdokumentation.

Driftsansvar

Team Servicedesk og IT har ansvaret for, at systemer og relaterede data, altid er tilgængelige for kommunens medarbejdere.
Retningslinjer fremgår af bilag E.

Sikkerhed i systemplanlægning

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 test og idriftsættelse finder sted på betryggende vis.
Retningslinjer fremgår af bilag E.

Driftsafviklingsprocedurer

For at opnå stabil og sikker drift af systemerne og samtidig sikre uafhængighed af enkelte IT-medarbejdere, skal der udarbejdes driftsplaner for netværk, servere og øvrigt udstyr, herunder printere, pc'er og tilsvarende.
Retningslinjer fremgår af bilag E.

Sikring af serversystemer

Næstved Kommune benytter et basisimage til installation af servere, der efterfølgende tilpasses individuelt efter funktion.

Registrering af driftsstatus

Der skal føres logbog over uregelmæssigheder i IT-driften således, at historikken kan komme Næstved Kommune til gavn, hvis eventuelle uregelmæssigheder gentager sig.
Retningslinjer fremgår af bilag E.

12.1.2. Ændringsstyring

Planlægning, test og godkendelse af ændringer

Ændringer skal igennem en formaliseret godkendelsesprocedure inden drift. Ændringer skal planlægges og afprøves inden de sættes i drift.
Ændringernes konsekvenser skal vurderes inden drift.

Ændringsstyring

Der skal vedligeholdes en versionsstyring for alle systemændringer.

Der skal indhentes en formel godkendelse af ændringen, før arbejdet går i gang. Godkendelsen foretages af Change Board.

Change Board skal 1 gang ugentligt vurdere indkomne RFC (request for change).

Der skal vedligeholdes et kontrolspor for alle ændringer.

Driftsdokumentation og forretningsgange for brugerne skal holdes opdateret, så de stadig er gældende efter ændringen.

Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.

Der skal foretages test af driftsfunktionaliteten før ændringer gennemføres.

Team Servicedesk og IT skal oprette og vedligeholde procedurer for ændringsstyring for alle software- og systemkonfigurationsændringer (inklusiv netværksudstyr).

Der skal foretages test af ændringer i netværk, firewall og routere.

Team Servicedesk og IT har udarbejdet et procesdiagram for ændringsstyring.

12.1.3. Kapacitetsstyring

It-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges således, at opgradering og tilpasning kan finde sted løbende. Dette gælder især for kritiske systemer. Team Servicedesk og IT skal have procedurer, der minimerer risikoen for driftsstop som følge af manglende kapacitet.

Der skal opsættes grænseværdier for diskforbrug på overvågningssystemet, alarmer skal sendes til udvalgte it-medarbejdere, herunder it-vagten.

Procedure for genoprettelse fremgår i Team Servicedesk og It's driftsdokumentation.

12.1.4. Adskillelse af udviklings test- og driftsmiljøer

Udvikling af applikationer sker kun internt i Team Servicedesk og It og kun til driftsautomatisering. Funktionsadskillelse anses i dette tilfælde ikke relevant.

12.2. Beskyttelse mod malware*

Malware, 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.

12.2.1. Kontroller mod malware

Antivirus-produkter på systemer

Kommunen råder over forskellige værktøjer, som beskytter it-systemer og netværk imod virusangreb.

Ud over anvendelse af opdaterede værktøjer, opfordres it-brugerne til at praktisere god it-skik som er beskrevet i bilag 1 - Retningslinjer for it-brugere.

Uddybende retningslinjer for tilrettelæggelse af virusberedskab er beskrevet i bilag H mens betryggende adfærd til imødegåelse af virus, fremgår i bilag 1.

Kontrol af antivirus på arbejdsstationer

Medarbejdere kan antage, at antivirus fungerer. Det er alene Team Servicedesk og It's ansvar at kontrollere korrekt funktion.
Brugerne må ikke påvirke sikkerhedsindstillingerne gennem stop af service eller afinstallation.

12.3. Backup*

12.3.1. Backup af information

Opbevaring af sikkerhedskopier på ekstern lokation

Backupudstyr samt datamedier med sikkerhedskopier skal opbevares i sikker afstand fra driftsdata for at undgå skadevirkninger fra et uheld på det centrale serverrum.

Backup af systemer og data

Der tages sikkerhedskopi af alle systemer og data. For hvert enkelt system skal der tages stilling til frekvensen i forbindelse med sikkerhedskopiering, og hvordan sikkerhedskopier skal opbevares. Der skal foretages en teknisk afprøvning af kopieringsrutinerne, mindst en gang om året, eller i forbindelse med omlægning af rutinerne.

Procedurer for sikkerhedskopiering og reetablering skal være beskrevet således, at procedurerne til enhver tid kan udføres af udvalgte it-medarbejdere i kommunen. Sikkerhedskopier opbevares på en forsvarlig måde.

Uddybende retningslinjer for sikkerhedskopiering er beskrevet i bilag G.

Sikkerhedskopiering af data på andre systemer

Der foretages ikke sikkerhedskopiering af pc'er. Sikkerhedskopiering er yderligere beskrevet i bilag 1.

Sikkerhedskopiering af udstyr, hvor indholdet kun sjældent ændrer sig tages der kun sikkerhedskopier efter behov.

Overvågning af procedurer for sikkerhedskopiering

Muligheden for at retablere data fra backup-systemer skal regelmæssigt aftestes i et testmiljø. Desuden skal retablering testes efter system- eller procesændringer, der kan påvirke backuprutiner.

12.4. Logning og overvågning

12.4.1. Hændelseslogning

Formål

Der foretages logning og overvågning som forebyggende foranstaltning mod uretmæssig adgang. Som led i loggens forebyggende funktion informeres alle brugere om, at der sker logning af deres brug af systemerne, herunder læsning og anvendelse af fortrolige og følsomme personoplysninger, og at loggen bl.a. kan bruges i forbindelse med efterforskning af hændelser eller ved kontrol af, om anvendelse af personoplysninger har været berettiget. Hændelser registreres og dokumentation tilvejebringes til brug for opklaring og evt. sanktionering i forbindelse med uregelmæssige og/eller ulovlige handlinger og til brug for eventuel kontrol.

Se også Bilag C Retningslinjer for logning. *

Logning

Systemejeren skal sikre, at der foretages logning på egne systemer. Risikovurdering og konkret lovgivning afgør hvilke, herunder logning af adgang, brugeraktiviteter, undtagelser, fejl og sikkerhedshændelser.

Logningen skal sikre at hændelser og sikkerhedsbrud kan opdages og som sådant skal disse indeholde følgende data: Bruger-id, systemaktiviteter, dato, tidspunkt. Denne liste er ikke udtømmende idet logningen skal afspejle den konkrete anvendelse og/eller lovkrav.

Ligeledes skal en log indeholde oprettelse og sletning af objekter på systemniveau for systemkomponenter eks. netværksudstyr og servere. Der skal for denne log være mulighed for at identificere hvem, som har udført handlingen samt hvornår.

For alle systemer, som behandler personoplysninger eller fortrolige oplysninger, skal information om adgang og forsøg på adgang logges, for at kunne spore uautoriseret aktivitet.

Da loggen ofte anvendes i forbindelse med SIEM systemer, bør denne indsamles i et anerkendt format således, at der nemt og hurtigt kan dannes et overblik visende de ønskede aktiviteter.

Opbevaring af log

Systemejer skal sikre at logs opbevares i seks måneder, hvorefter den skal slettes. Ved særligt behov kan logs opbevares i op til fem år.

12.4.2. Beskyttelse af logoplysninger

Det må ikke være muligt for systemadministrator at slette eller deaktivere loggene for egne aktiviteter.

Log-faciliteter og log-oplysninger skal beskyttes mod manipulation og tekniske fejl, herunder må det heller ikke være muligt for systemadministratorer at slette eller deaktivere loggene for egne aktiviteter.

Loggen kan indeholde følsomme data og personoplysninger. Der bør træffes passende foranstaltninger til beskyttelse af privatlivets fred (se 18.1.4.)

12.4.3. Administrator- og operatørlog

Log-gennemgang

På baggrund af kommunens risikovurdering og –villighed, som er fastlagt af Informationssikkerhedsudvalget har systemejeren ansvar for, at konkrete planer udarbejdes for logning og efterfølgende gennemgang.

Systemejeren har ansvaret for, at den vedtagne logning opsættes.

Systemejeren har ansvaret for, at logning foretages, og at der foreligger en procedure, der angiver frekvensen for gennemgang og opfølgning på hændelser.

Da betroede konti, herunder administratorkonti udgør en særlig risiko, bør handlinger udført af disse logges separat og have en særskilt procedure for gennemgang, som sikrer at aktiviteter registreres og gennemgås.

Logregistreringer fra servere, som udfører sikkerhedsfunktioner, skal have en særskilt procedure, der angiver frekvensen for gennemgang og opfølgning på hændelser.

Overvågning af serviceleverandøren

Systemejeren skal sikre regelmæssig overvågning af serviceleverandørerne, og gennemgang af de aftalte rapporter og logninger.

Desuden skal systemejeren sikre, at sikkerhedshændelser håndteres og rapporteres til informationssikkerhedskoordinatoren.

12.4.4. Tidssynkronisering

Tidssynkronisering

Urene i alle relevante systemer (hardware såvel som software) i organisationen skal være synkroniseret til én referencetidsangivelseskilde, så tidsstempler er ens på tværs af systemer. Dette kan f.eks. ske ved anvendelse af NTP mod én kilde. Herefter synkroniseres hele organisationen imod denne ene tidsmaster.

12.7 Overvejelser i forbindelse med audit af informationssystemer

Auditkrav og –aktiviteter, der indebærer verifikation af informationssystemer, skal planlægges og aftales omhyggeligt for at minimere risikoen for afbrydelse af forretningsprocesserne.

Auditkrav vedrørende adgang til systemer og data skal aftales med den relevante ledelse. *

Audittest må kun omfatte læseadgang til software og data. *

Hvis det er nødvendigt at tildele andet end læseadgang, må dette kun ske til isolerede kopier af systemfiler, som skal slettes, når auditten er afsluttet, eller beskyttes på behørig vis, hvis der er pligt til at bevare sådanne filer i henhold til auditdokumentationskravene. *

Audittest, som kan påvirke systemets tilgængelighed, skal afvikles uden for arbejdstid. *

Al adgang bør overvåges og logges med henblik på at frembringe et referencespor. *

Informationssikkerhedskoordinatoren udarbejder en oversigt, der viser hvilke informationssystemer, der er udtaget til audit, og Informationssikkerhedsudvalget godkender oversigten. Dette arbejde skal ligeledes afspejles i et evt. årshjul for opgaver i forbindelse med informationssikkerhed.

I oversigten skal det fremgå, hvorfor et informationssystem er udtaget, og med hvilken frekvens dette foregår. I forbindelse med gennemførelse af audit, vil denne ofte være baseret på en stikprøve eller en defineret delmængde, i disse tilfælde skal det ligeledes fremgå af oversigten, hvilke kriterier der ligger til grund for evt. stikprøve eller delmængde.

Når der gennemføres audit, skal der efterfølgende være dokumentation der tjener følgende formål:

- Udvælgelse og gennemførelse af auditprogram
- Registrering af konstaterede afvigelser
- opfølgning på registrerede afvigelser og informationssikkerhedshændelser

13. Kommunikationssikkerhed

13.1. Styring af netværkssikkerhed

13.1.1. Netværksstyring

Krav til firewall

Det skal ikke være muligt at etablere forbindelser direkte fra internettet til interne systemer.

Regelsættet på firewallen giver adgang til ressourcer eller forhindrer adgangen til samme. Som udgangspunkt opbygges regelsættet efter princippet om "alt er forbudt", hvis det ikke eksplicit er tilladt, samt at rettigheder tildeles på lavest mulige niveau.

Ligeledes vil definitionen af de enkelte regler tage udgangspunkt i de konkrete arbejdsmæssige opgaver ("need to have" princippet) som skal løses.

Der bør i firewallen være opsat logning på alle regler, så såvel accepterede som droppede pakker registreres, og logfilen sendes til en central log-enhed, som matcher hændelser i firewallen og på nettet med øvrige hændelser på centrale systemer. *

Adgangen fra eksterne netværk - herunder internet - til Næstved Kommunes netværk, er sikret således, at det kun er autoriserede it-brugere, som kan opnå adgang. *

Team Servicedesk og IT er ansvarlig for, at adgangen til netværket er beskyttet med en firewall, herunder betryggende administration af firewall samt vedligeholdelse af firewallsoftware, overvågning af firewall, logning af trafikken samt test af funktionaliteten. *

Retningslinjer for administration og håndtering af firewall er uddybet i bilag F. *

*Sikring af netværk**

Team Servicedesk og IT har det overordnede ansvar for at beskytte Næstved Kommunes it-infrastruktur samt lokalnet på alle kommunens lokationer.

Alle eksterne kommunikationsforbindelser skal godkendes af Team Servicedesk og IT, som vedligeholder oversigter over netværk og datakommunikation.

Retningslinjer for it-medarbejdere fremgår i bilag E.

Tilslutning af udstyr til netværk

Medarbejderne må koble kommunens godkendte udstyr på det interne netværk. Medarbejdere og eksterne kan anvende gæstenetværket til internetadgang for andet udstyr.

Personlige firewalls

Der skal benyttes firewalls på alle pc-arbejdspladser, som tillades adgang til kommunes netværk. Reglerne i denne firewall administreres af Team Servicedesk og It uden det er muligt for brugerne at ændre disse.

Adgang til netværket

Adgangen til kommunes netværk må kun ske gennem sikkerhedsgodkendte løsninger.

Retningslinjer for autorisation til netværket er beskrevet i bilag B. *

Retningslinjer for fjernadgang er beskrevet i bilag 4. *

Installation af netværksudstyr

Det er ikke tilladt at installere netværksudstyr uden forudgående sikkerhedsgodkendelse. Team Servicedesk og It er ansvarlig for konfiguration og dokumentation af enheden.

Standardværdier, f.eks. administrator-logins og andre fabriksindstillinger der kan kompromittere sikkerheden, skal ændres, før et system installeres på netværket. Dette gælder alt netværksforbundet udstyr f.eks. også printere.

Retningslinjer fremgår i bilag E. *

Placering af trådløse netværk

Kun Team Servicedesk og IT har ansvaret for opsætning, konfiguration og dokumentation af trådløst udstyr.

Adgang til aktive netværksstik

Den logiske adgang til aktive netværksstik skal styres af Team Servicedesk og IT.

Ved tilslutning af udstyr til netværksstik i offentligt tilgængelige områder, skal det sikres at der kun er adgang til et servicenet med begrænset adgang. Der skal ikke være adgang til det administrative net. Der må ej heller tildeles DHCP adresser i en range som anvendes i det øvrige administrative net.

Rutekontrol

Team Servicedesk og IT skal vedligeholde konfigurationsstandarder for routere.

Team Servicedesk og IT skal sikre tilstrækkelig filtrering på afsender- og modtager-adresser på relevante protokoller imellem alle relevante netværkssegmenter.

Team Servicedesk og IT skal begrænse rutning imellem forskellige netværkssegmenter således at kun nødvendig trafik videresendes.

Dokumentationen fremgår i Team Servicedesk og It's driftsdokumentation.*

Begrænset netværkstid

Brugersystemer med særlig høj risiko bør kræve fornyet autentifikation med fastlagte intervaller. Dette interval bør være fastlagt til 4 timer.

Public netværk har begrænset netværkstid 6 timer. Ellers anvendes begrænset netværkstid ikke. *

Fysisk sikring af netværk

Der bør etableres dubleret internetforbindelse samt firewalls som terminerer på 2 forskellige fysiske steder i kommunen. Team Servicedesk og IT bør regelmæssigt kontrollere om uautoriseret udstyr er blevet tilkoblet netværket.

Krydsfelter og aktivt udstyr skal være placeret så fysisk adgang begrænses. For krydsfelter og udstyr som transmittere personhenførbare data gælder, at skal dette udstyr være låst inde i et skab eller tilsvarende.

Netværksdokumentation

Team Servicedesk og IT skal vedligeholde et opdateret netværksdiagram. Netværksdiagrammet skal omfatte samtlige netværksforbindelser (trådløse og fysiske net med tilhørende netværksudstyr skal indgå). Diagrammet skal revideres som minimum 1 gang halvårligt eller ved større ændringer

Netværksdokumentationen skal ligeledes indeholde en beskrivelse af den logiske administration, samt en beskrivelse af implementerede sikkerhedsforanstaltninger mod potentielt usikre protokoller. Denne dokumentation skal ligeledes revideres halvårligt eller ved større ændringer.

Retningslinjer fremgår i bilag E. *

Firewall-funktioner på servere

Alle servere med indbygget firewall-funktionalitet skal benytte denne til at sikre, at der kun gives adgang til nødvendige (og godkendte) services og porte. Hvis en server ikke har mulighed for at anvende en indbygget firewall, skal der etableres en tilsvarende funktionalitet.

Brug af trådløse lokalnetværk

Sikkerhedssystemerne WPA2 skal som minimum anvendes i alt trådløst netværksudstyr.

Der kan desuden anvendes preshared keys og eller certifikatløsning: Hvis der anvendes en preshared key løsning skal den implementeres på en sådan måde at brugeren ikke får kendskab til nøglen.

Domain pc'er eller mobile devices skal, når de går på fremmede trådløse netværk, anvende sikrede forbindelser så al kommunikation sker via Kommunes centrale firewall.

13.1.2. Sikring af netværkstjenester

Fjernstyring og administration

Forbindelser til fjernadgang til brug for leverandører og support, skal overvåges, mens de benyttes.

Det er tilladt at benytte værktøjer til fjernadministration, hvis der foreligger sikkerhedsgodkendelse af produktet fra IT-Teamlederen.

Adgang til administrations- og konfigurationsporte til trådløse netværk skal begrænses til netværksadministratorer.

Værktøjer til fjernadministration tillades, hvis adgangen er krypteret ved hjælp af teknologier som f.eks. SSH, VPN, eller SSL/TLS.

Retningslinjer for fjernovertagelse fremgår i bilag E. *

Afvikling af programmer i forbindelse med internetsurfing

Det er tilladt at afvikle browserbaserede programmer, f.eks. netbank-programmer, forudsat at sikkerhedspolitikken i øvrigt overholdes.

Retningslinjer for anvendelse af internet fremgår i bilag 3. *

Internetbaserede tjenester

IT-Teamlederen kan begrænse adgangen til applikationer og services efter en konkret vurdering. Der må ikke etableres forbindelser til services eller applikationer på internettet som resultere i en lavere sikkerhedsniveau end det vedtagne eller vanskeliggør compliance i forhold til databeskyttelsesforordningen.

Det er informationssikkerhedsudvalget som på baggrund af en konkret risikovurdering fastlægger en positiv eller negativ liste.

Retningslinjer for anvendelse af internet fremgår i bilag 3. *

Brug af kryptering i forbindelse med dataudveksling

Det kræves, at e-mail og data, der indeholder fortrolige informationer, herunder data som skal beskyttes efter gældende lov om persondata, altid er krypteret under transmission.

Man må aldrig sende fortrolige personoplysninger ukrypteret over internettet eller andre åbne net.

Når logininformationer sendes over internettet eller andre åbne netværk, skal der benyttes løbende opdaterede og stærke krypteringer samt sikkerhedsprotokoller.

13.1.3. Opdeling af netværk

Netværket

Den logiske adgang til kommunens data og it-ressourcer kan kun ske via kommunens administrative it-netværk. Dette netværk er adskilt fra de øvrige netværk, der anvendes i kommunen, herunder den offentligt tilgængelige del af skolenetværket, tekniknetværket og andre eksterne net, som f.eks. internettet. Der er desuden oprettet sikre zoner (DMZ) baseret på systemers risikoprofil.

Segmentering

Kommunikationsadskillelsen mellem de enkelte netværk sker med udgangspunkt i, at intet er tilladt, medmindre der specifikt foreligger en begrundet godkendelse af den specifikke kommunikationssammenkobling. Forud for en godkendelse skal der udføres en konkret risikovurdering af hvordan ændringer i netværket påvirker IT-sikkerheden, IT-Teamlederen foretager den endelige godkendelse af ændringen. I tvivlstilfælde er det Informationssikkerhedsudvalget, som tager stilling til de sikkerhedsmæssige aspekter i netværksopsætningen.

13.2. Informationsoverførsel

13.2.1. Politikker og procedurer for informationsoverførsel

Opbevaring og bortskaffelse af data

Der skal foreligge en procedure for håndtering af opbevaringstiden for data. For opbevaringstiden gælder at data kun må opbevares i det tidsrum, som er nødvendigt i henhold til gældende lovgivning og forretningsmæssige formål.

Det er data- og systemejer der har ansvaret for at opbevaringstiden defineres i forhold til gældende lovgivning, samt at der foreligger en bortskaffelsesprocedure, som sikrer at både elektroniske såvel som papirbårne data destrueres så de ikke kommer til uvedkommendes kendskab.

Uddybende retningslinjer for destruktion af data fremgår af bilag 8.*

Elektroniske dokumenter

Elektroniske kopier af dokumenter, f.eks. indscannede dokumenter og faxer, med fortrolige informationer eller data som skal beskyttes i forhold til gældende lov om persondata, må kun behandles og lagres på kommunens it-udstyr.

13.2.2. Aftaler om informationsoverførsel

Fortrolige informationer og oplysninger må udleveres, hvis der foreligger underskrevne fortrolighedsaftaler.

Fortrolig information må ikke udleveres uden forudgående aftale med dataejer.

For data som skal beskyttes i henhold til gældende lov om persondata, kan disse ikke udleveres uden den registreredes samtykke samt efter reglerne, som findes i afsnittet om videregivelse.

Hvis der i forbindelse med driftsopgaver eller tilsvarende er brug for at store mængder af oplysninger som skal beskyttes i henhold til gældende lov om persondata skal udleveres, skal der altid udarbejdes en databehandleraftale. Databehandler aftalen skal leve op til de krav som er i Kommunens sikkerhedspolitik. Det er dataejers ansvar at der er udarbejdet en aftale.

13.2.3. Elektroniske meddelelser

Ejerskab

Alle e-mails er som udgangspunkt kommunens ejendom. Dog er medarbejderes private mails ikke omfattet af kommunes generelle ejerskab af mail. Medarbejdere skal opfordres til tydeligt at markere private mails.

Se retningslinjer for anvendelse af e-mail og internet i bilag 2 og bilag 3.*

Filudveksling

Der må ikke udveksles filer eller internet-links via messenger-programmer eller tilsvarende tjenester.

Brug af messenger-programmer

Det er kun tilladt at bruge messenger- og chatprogrammer, som er godkendt af IT-Teamlederen.

Kommunens informationer på sociale netværk

Bortset fra offentlige 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, hvorvidt kommunen bevarer sin ophavsret til informationerne.

Retningslinjer for anvendelse af internet fremgår af bilag 3.*

Opbevaring og sletning af e-mail

E-mail, der indeholder personoplysninger, skal behandles i overensstemmelse med gældende lovgivning om databeskyttelse. Hvis en e-mail indgår i en sagsbehandling, skal den på linje med breve journaliseres.

Retningslinjer for anvendelse af e-mail er beskrevet i bilag 2.*

Elektronisk udveksling af post og dokumenter

Hvis e-mail bruges til bindende aftaler, skal de underskrives med en digital signatur. Dokumenter og e-mails, som indeholder fortrolige oplysninger, skal altid sendes i krypteret form.

Retningslinjer for anvendelse af digital signatur fremgår i bilag 6 og brug af e-mail af bilag 2.*

Social Engineering

Medarbejdere skal, især når de behandler fortrolige oplysninger, være passende opmærksomme på begrebet "Social Engineering".

Retningslinjer for e-mail fremgår af bilag 2.*

Vedhæftede filer

Det er tilladt at benytte vedhæftede filer ved brug af e-mail systemet.

Team Servicedesk og It blokerer for filtyper som vurderes som farlige eller uhensigtsmæssige i forhold til driften. Som udgangspunkt kan eksekverbare file ikke vedhæftes og åbnes.

Alle filer virus tjekkes af kommunes antivirus system før de åbnes – og før de afsendes.

Phishing og bedrageri

Uanset at kommunen udfører indholdsscanning af alle e-mails, skal brugere skal være opmærksomme på "phishing" og "Social Engineering".

Retningslinjer for e-mail fremgår i bilag 2. Se også informationsvideoerne på NORA.*

Sagsbehandling og journalisering af e-mail

Sendte og modtagne e-mails skal håndteres på samme måde som traditionel post og fax. E-mails med vigtig information skal arkiveres systematisk for at sikre lagring.

Modtaget og afsendt e-mail skal journaliseres og behandles efter samme principper, som gælder for almindelig brevpost og fax.

Næstved Kommune anvender funktionspostkasser, der bestyres efter særlige regler. *

Retningslinjer for anvendelse af e-mail er beskrevet i bilag 2.*

13.2.4. Fortroligheds- og hemmeligholdelsesaftaler

Når der indgås en fortrolighedsaftale mellem kommunen og en ekstern samarbejdspartner skal aftalen som minimum indeholde følgende punkter:

- Betingelser for returnering eller destruktion af informationsaktiver ved aftalens ophør.
- Underskriverens ansvar for at undgå brud på den aftalte fortrolighed.
- Definition af de informationer, der er omfattet.
- Kommunens ret til overvågning af og opfølgning på overholdelse af fortrolighedspligten.

- Sanktioner ved brud på fortrolighedspligten.
- En fastlagt løbetid.
- Procedure for advisering og rapportering af brud på fortroligheden.

Næstved kommune benytter sig af databehandleraftaler, der sikrer at data alene behandles efter instruks, herunder betingelser for returnering eller destruktion af informationsaktiver ved aftalens ophør. *

Kommunens har pligt til overvågning af, og opfølgning på, overholdelse af databehandleraftalerne. *

Se vejledning om tilsyn med databehandleraftaler på NORA.*

14. Anskaffelse, udvikling og vedligeholdelse af systemer

14.1. Sikkerhedskrav til informationssystemer

14.1.1. Analyse og specifikation af informations-sikkerhedskrav

Formål

Formålet er at sikre at informationssikkerheden håndteres som en integreret del af anvendelsen af det enkelte informationssystem gennem hele dets livscyklus. Altså lige fra kravspecifikation, udbud, installation, test, drift og til sidst afinstallation og arkivering. Dette omfatter også informationssystemer, som leverer tjenester over offentlige netværk.

Anskaffelsesprocedurer

Informationssikkerhedskrav afdækkes/klarlægges/identificeres i forbindelse med anskaffelse og udvikling af systemer. De identificerede krav må ikke give anledning til konflikt med eksisterende krav i sikkerhedspolitikken.

Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser uden forudgående risikovurdering og eventuel detaljeret risikoanalyse.

Der skal foreligge en standardiseret godkendelses- og anskaffelsesprocedure, som sikrer at anskaffelsen lever op til funktionelle såvel som sikkerhedsmæssige krav.

Informationssikkerhedskravene omfatter:

a. Hvor stor en sikkerhed man vil have for, at brugeren er den, han giver sig ud for at være (brugerautentifikation)
b. Processer for tildeling og autorisation af adgang for eksterne leverandører samt privilegerede eller tekniske brugere
c. Information til brugere, systemadministratorer om deres opgaver og ansvar
d. Det nødvendige beskyttelsesbehov for de pågældende aktiver, særligt i relation til tilgængelighed, fortrolighed og integritet
e. Krav udledt af forretningsprocesser, såsom transaktionslogning og –overvågning, uafviselighedskrav
f. Krav afledt af andre sikkerhedskontroller, eks. grænseflader til logning og overvågning eller systemer til detektering af datalækager.

For behandlingsaktiviteter, som indebærer høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal der som nærmere beskrevet i databeskyttelsesforordningens artikel 35 udformes en konsekvensanalyse vedrørende databeskyttelse (DPIA). Styregruppe, procesejer eller projektleder træffer beslutningen om, hvorvidt der skal udføres en konsekvensanalyse.*

Den i DIGIT-regi udformede skabelon for DPIA-screening kan anvendes som hjælpeværktøj, når det skal afklares, om en DPIA skal gennemføres. Denne skabelon anvendes også til at dokumentere kommunens overvejelser og beslutning.*

Når der skal gennemføres en DPIA, udpeger kommunen en DPIA-tovholder, som styrer processen. Ved gennemførelsen af DPIA tages der afsæt i DIGIT skabelonen til DPIA-rapport. Der

indhentes rådgivning fra kommunens databeskyttelsesrådgiver/DPO (jf. databeskyttelsesforordningens artikel 35, stk. 2).*

Retningslinjer for systemejere fremgår af bilag A.*

14.1.2. Sikring af applikationstjenester på offentlige netværk

Der skal benyttes sikre autentifikations- og autorisationsprocesser for at sikre services, transaktioner og applikationer over offentlige netværk.

Datas integritet og fortrolighed skal sikres, når der benyttes applikations-services over offentlige netværk

I forbindelse med 3. parts samarbejder anvendes databehandleraftale/kontrakt til at regulere kommunens krav til behandlingen.

Webtjenester og services, som tilbydes via hjemmesider, skal som minimum anvende https og evt. autentifikation bør være NemID.

14.1.3. Beskyttelse af handelsapplikationer og –tjenester

Online transaktioner

Informationer i forbindelse med handelsapplikationer og –tjenester bør beskyttes for at forhindre ufuldstændig transmission, fejleforsendelser, uautoriseret ændring af meddelelser, uautoriseret offentliggørelse, uautoriseret kopiering og/eller retransmission af meddelelser.

Der skal anvendes markedsstandarder for signaturer (kryptografiske løsninger) af alle involverede parter i transaktionerne.

Kommunens medarbejdere, der anvender e-handelsapplikationer, er omfattet af de generelle retningslinjer i bilag 3 - Retningslinjer for anvendelse af Internet.*

14.2. Sikkerhed i udviklings- og hjælpeprocesser

14.2.1. Sikker udviklingspolitik

Udviklingsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Data skal sikres efter følsomhedsniveau.

Krav til sikkerhed herunder databeskyttelse gennem design og standardindstillinger, ved anskaffelse af applikationer skal beskrives i kravspecifikationer til kommunens systemleverandører.

14.2.2. Procedurer for styring af systemændringer

Systemejere har ansvaret for, at der bliver indgået en aftale med Team Servicedesk og IT vedrørende sikkerheden i applikationer. De indgåede aftaler skal sikre, at der bliver etableret systemteknisk sikkerhed, herunder adgangskontrol og centralt opdateret sikkerhedskopiering

samt, at test og idriftsættelse finder sted på betryggende vis og lever op til kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Systemejere har selv ansvaret for den tilpasse forretningsgange og procedurer, herunder forretningsgang vedrørende autorisation og logning. Desuden har Systemejere ansvaret for udarbejdelse af præcis dokumentation.

Retningslinjer fremgår i bilag A.*

14.2.3. Teknisk gennemgang af applikationer efter ændring af driftsplatforme

Det skal vurderes om beredskabsplanerne skal ajourføres i overensstemmelse med ændringer.

Ændringer i driftsmiljøerne skal tilrettelægges således, at der er god tid til gennemgang og test inden implementeringen.

Når driftsmiljøerne ændres, skal kritiske forretningssystemer gennemgås og testes for at sikre, at det ikke har utilsigtede afledte virkninger på kommunens daglige drift.

14.2.4. Begrænsning af ændringer af softwarepakker

Ændringer i eksternt leverede systemer bør begrænses til nødvendige ændringer, og sådanne ændringer skal styres.

Indbyggede sikringstiltag, f.eks. logning samt adgangs- og integritetskontrol, bør gennemgås for at sikre, at de fortsat er i overensstemmelse med kravene til systemet.

Eventuelle kompatibilitetsproblemer med anden software, der anvendes i kommunen skal afdækkes.

Generel procedure for ændringshåndtering skal følges (Jf. kapitel 12.1). Proceduren fremgår af Team Servicedesk og It's driftsdokumentation.*

14.2.5. Principper for udvikling af sikre systemer

Sikkerhedskrav til informationsbehandlingssystemer

Kommunen ønsker at nye såvel som bestående systemer skal indeholde krav til sikkerheden med udgangspunkt i en risikovurdering jf. databeskyttelsesforordningens artikel 5.

Ved anskaffelse og implementering af nye it-systemer skal Kommunens procedure for it-anskaffelser følges, så det sikres at sikkerheds- og arkitekturbetragtninger bliver afdækket og dokumenteret.

Center for Politik og Udvikling, Team Byråd og Direktion er ansvarlige for implementering af fælleskommunale digitaliseringshandlingsplaner.*

Digitaliseringsforum fastlægger arkitekturprincipper og standarder.*

Specifikation af sikkerhedskrav

Hvis en overordnet risikovurdering retfærdiggør aktiviteten, skal sikkerhedskrav dokumenteres i forbindelse med enhver nyanskaffelse eller opgradering af systemer. Dette gælder både for kundetilpassede- og standardsystemer.

Uddybende retningslinjer og information om projekter fremgår på NORA.*

14.2.6. Sikkert udviklingsmiljø

Kommunen udvikler ikke selv applikationer.

14.2.7. Outsourcet udvikling

Systemudvikling udført af ekstern leverandør

Kommunen kræver at der løbende sker dokumenteret kvalitetssikring.

Der skal, som en del af leverancer, aftales testscenarier for kvalitet, nøjagtighed og sikkerhed inden leverancen kan godkendes.

Kommunen kan, hvor dette skønnes relevant, kræve revisionserklæring fra uafhængig revisor om systemets applikationskontroller.

Retningslinjer fremgår af bilag A.*

Ejerskab af data, cloudløsninger

Kommunen skal sikre, at ejerskab, herunder regler for ophavsret, kildekode mm. er klart defineret mellem kommunen og cloududbyder.

Ekstern revision af outsourcing-partnere

Outsourcing-partnere skal få foretaget en ekstern revision mindst en gang om året. Kommunen kan i forbindelse med implementeringen anmode leverandøren om dokumentation, f.eks. ved uafhængig revisorerklæring.

Retningslinjer fremgår af bilag J.*

14.2.8. Systemsikkerhedstest

Kommunen udvikler ikke selv IT-systemer, men skal sikre, at der ikke introduceres sårbarheder i forbindelse med implementering af nye systemer.

14.2.9. Systemgodkendelsestest

Kommunens godkendelsesprocedure skal gennemføres for nye systemer, for nye versioner og for opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.

Godkendelsesproceduren skal sikre, at sårbarheder mitigeres, før et system installeres i infrastrukturen.

14.3. Testdata

14.3.1. Sikring af testdata

Formål: at sikre beskyttelse af data, som anvendes til test.

Udvælgelse af testdata

Data til test skal udvælges, kontrolleres og beskyttes i henhold til klassifikation.

Testdatasæt skal i videst mulige omfang bestå af fiktive data, alternativt bør personoplysninger anonymiseres. Benyttes personoplysninger eller fortrolige data alligevel som testdata, skal disse håndteres efter samme regler, som gælder i det tilsvarende driftssystem, og anvendelsen skal godkendes af systemejer.

Det skal sikres, at behandlingen af testdata er indeholdt i databehandleraftalen.

Sletning af testdata

Testdata skal fjernes inden systemer sættes i endelig drift.
Særlige applikationskonti, brugernavne og adgangskoder, anvendt i forbindelse med udvikling og test, skal slettes før en applikation sættes i drift.

Sikring af testdata

Kopiering og brug af data fra driftsmiljøet til test skal logges for at sikre kontrolsporet. Loggen skal gemmes efter samme regler som er gældende for driftsmiljøet.

Formelle adgangskontrolprocedurer skal også omfatte testapplikationssystemer, hvor der anvendes personoplysninger eller fortrolige data.

15. Leverandørforhold

15.1. Informationssikkerhed i leverandørforhold

Formålet med kravene til informationssikkerhed i leverandørforhold er at minimere risici forbundet med leverandørers adgang til Kommunens aktiver og informationer.

15.1.1. Informationssikkerhedspolitik for leverandørforhold

Team Servicedesk og IT skal deltage i vurdering og godkendelse af outsourcingleverandører.*

Kommunen skal aftale omfanget af leverandørers adgang til Kommunens aktiver med leverandøren og sikre dokumentation af det aftalte, samt overholdelse heraf.

Kommunen skal identificere de informationssikkerhedskontroller, som er relevante for leverandørers specifikke behandling af og adgang til Kommunens informationer. Kontrollerne skal nedskrives og dokumenteres.

Kontrollerne skal omfatte hhv. processer og procedurer, der implementeres i Kommunen, samt processer og procedurer, som Kommunen kræver, at leverandøren implementerer. Kontrollerne skal sikre nogle mindstekrav af beskyttelse af Kommunens og leverandørens oplysninger, herunder blandt andet i forhold til Kommunens forpligtelser om tavshedspligt og beskyttelse af persondata.

Hvis det er nødvendigt, skal Kommunen ligeledes identificere behovet for særlig sikring. Det kan være i relation til anvendelse af hemmeligholdelsesaftaler/fortrolighedsaftaler, hvis der er et særligt behov for fortrolighed eller databehandleraftaler, hvis leverandøren får overdraget personoplysninger til behandling på vegne af Kommunen.

Databehandleraftaler skal leve op til artikel 28, stk. 3, i databeskyttelsesforordningen

Aftalerne skal dække informationerne 'fra vugge til grav' samt i alle led af en eventuel forsyningskæde, f.eks. ved cloud tjenester.

Processer og procedurer skal omhandle følgende afhængigt af behov:

- Identifikation og dokumentation af typer af leverandører. Leverandørerne skal opdeles ud fra en vurdering af, hvilke informationer, leverandøren må få adgang til og hvilken form for behandling af informationer og oplysninger, leverandøren foretager. Her er det blandt andet relevant at se på, hvilken ydelse, leverandøren udfører, f.eks. levering af it-systemer, varer eller tjenesteydelser, rådgivnings- og konsulentydelser, ydelser det udliciteres af Kommunen og ydelser, Kommunen ikke selv har mulighed for at udføre.
- En standardiseret proces og livscyklus til håndtering af leverandørforhold afhængigt at den leverede ydelse.
- Fastlæggelse af omfanget af adgang til informationer, forskellige leverandører får tildelt samt overvågning og styring af adgangen.
- Minimumskrav til sikkerhedsniveau og -foranstaltninger for alle typer af informationer, der behandles af leverandøren. Disse baseres på Kommunens behov og risikovurdering.

- Processer og procedurer for kontrol af, at de fastlagte sikkerhedskrav for alle typer leverandører overholdes, samt at den fastsatte adgangsstyring og -begrænsning efterleves.
- Kontroller til sikring af information og oplysningers integritet.
- Typer af forpligtelser for leverandøren til sikring af tilstrækkelig beskyttelse af Kommunens informationer.
- Håndtering af sikkerhedsbrud og -hændelser.
- Robusthed af leverandørens udstyr til sikring af tilgængelighed samt eventuelt aftaler om retablering og nødordninger i forbindelse med nedbrud.
- Bevidstgørelse af de medarbejdere i Kommunen, der varetager sikringsarbejdet, om de gældende kontroller, processer og procedurer.
- Krav om indgåelse af aftaler om informationssikkerhedskrav med leverandøren afhængigt af, hvilken ydelse, der leveres. Herunder databehandleraftaler, fortroligheds-/hemmeligholdelsesaftaler eller andre aftaleretlige forpligtelser.
- Håndtering af nødvendige forandringer i henhold til informationssikkerhed, for konstant at sikre et højt sikkerhedsniveau for informationer. Dette både når informationerne opbevares samt når de flyttes.

15.1.2. Håndtering af sikkerhed i leverandøraftaler

Behov og niveau for beskyttelse af informationer skal fastlægges for hver enkelt leverandør, der kan få adgang til, behandle, opbevare, kommunikere eller levere informationer eller it-systemer til Kommunen. Når behov og niveau er afdækket, skal der udarbejdes leverandøraftaler til sikring af, at forpligtelserne mellem parterne er helt klare så der ikke sker misforståelser og risiko for tab af informationer.

Aftalerne, der indgås med leverandørerne, skal tilpasses den ydelse, leverandøren udfører for Kommunen. Informationssikkerhedskravene i aftalen skal derfor også tilpasses den enkelte ydelse og dermed også den risiko, der er ved at leverandøren behandler eller har adgang til Kommunens informationer.

Kommunen skal overveje at inkludere følgende betingelser i aftalerne:

- Beskrivelse af den information, der skal gives eller gøres tilgængelig, samt metoder for oversendelse og tilgængeliggørelse.
- Klassifikation af informationen.
- Lov- og myndighedskrav, herunder blandt andet databeskyttelse, tavshedspligt og immaterielle rettigheder, samt en beskrivelse af, hvordan kravene opfyldes.
- Parternes forpligtelser til at udføre kontroller, f.eks. i forhold til adgangsstyring, resultatgennemgang, overvågning, rapportering og audit.
- Regler for accepteret anvendelse af informationer samt ikke-accepteret anvendelse, hvis nødvendigt.
- Betingelser for autorisations af medarbejdere eller oplistning af medarbejdere med autorisation, som må tilgå eller modtage Kommunens informationer.
- Informationssikkerhedspolitikker, som er relevante for den enkelte kontrakt.
- Krav til procedure for styring af informationssikkerhedsbrud, herunder underretning og samarbejde under håndtering af sikkerhedsbrud.
- Krav til træning og bevidsthed om specifikke procedure og informationssikkerhedskrav.
- Kontaktoplysninger på kontaktperson til informationssikkerhedsmæssige spørgsmål.

- Eventuelle screeningsprocedurer for leverandørens medarbejdere til sikring af, at et tilstrækkeligt sikkerhedsniveau kan garanteres.
- Ret til at auditere leverandørens processer og kontroller relateret til aftalen.
- Fejl- og konfliktløsningsprocesser.
- Leverandørens forpligtelse til regelmæssigt at udarbejde en rapport om efterlevelse af aftalen, herunder om effektiviteten af kontrollerne, samt aftale om rettidig afhjælpning af relevante problemer nævnt i rapporten.
- Leverandørens eventuelle forpligtelser i forbindelse med efterlevelse af Kommunens sikkerhedskrav.

I overvejelserne af, hvilke krav, Kommunen skal stille til de enkelte leverandører, skal Kommunen være opmærksom på at tilpasse kravene til leverandøren. Indholdet af aftalerne samt kravene heri kan variere betydeligt alt efter hvilken del af Kommunen, aftalen tilhører, og hvilken leverandør, der er tale om. Det er derfor nødvendigt at tage aktivt stilling til sikkerhedsbehovet i hver enkelt aftale. Derudover skal der tages højde for, om aftalen også skal involvere andre parter, f.eks. underleverandører.

Ud over sikkerhedsniveau skal der i aftalerne tages stilling til procedurerne for, hvordan driften fortsættes i tilfælde af, at leverandøren ikke er i stand til at levere som aftalt, så forsinkelser og lignende undgås.

Vejledning i håndtering af databehandleraftaler kan findes på NORA.*

15.1.3. Forsyningskæde for informations- og kommunikationsteknologi *

Leverandøren skal sikre en hensigtsmæssig opbygning af netværk, firewall, segmentering, kryptering mm. Kommunen skal sikre at leverandørens opbygning af netværk og netværkssikkerhed har et passende sikkerhedsniveau. Vurdering kan ske på baggrund af, it-revisorerklæringer eller ved egen inspektion.

Netværksleverandøren skal kunne levere:

- De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen.
- Det nødvendige sikkerhedsniveau i hele leverandør-forsyningskæden

15.2. Styring af leverandørydelser

Formålet med at foretage styring af leverandørydelser er at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

15.2.1. Overvågning og gennemgang af leverandørydelser

Kommunen skal regelmæssigt overvåge, gennemgå og auditere leverandørydelser. Det gøres for at sikre, at de informationssikkerhedsrelaterede betingelser i aftalerne overholdes, samt at informationssikkerhedsbrud og -problemer håndteres korrekt.

Kommunerne bør fastlægge en serviceledelsesproces mellem den enkelte leverandør og Kommunen på baggrund af de krav, der er fastsat i aftalen. Afhængigt af behov kan processen omfatte f.eks.:

- Overvågning af serviceniveauer fastsat i aftalen.
- Gennemgang af servicerapporter og deltagelse på statusmøder.
- Foretage auditering af leverandørens forhold samt følge op på tidligere identificerede problemer.
- Informering om informationssikkerhedsbrud.
- Gennemgang af leverandørens auditspor og registreringer af informationssikkerhedshændelser, driftsproblemer, nedbrud, lokalisering af fejl og driftsforstyrrelser i relation til den leverede ydelse.
- Løsning og håndtering de identificerede problemer.
- Gennemgang informationssikkerhedsforpligtelser mellem leverandøren og dennes underleverandører.
- Sikring af, at leverandøren fastholder tilstrækkelig kapacitet til sikring af, at det aftalte serviceniveau opretholdes efter nedbrud mv.

Overvågning, gennemgang og auditering af leverandørens forhold skal foretages af medarbejdere hos Kommunen med særlige kompetencer inden for informationssikkerhed. Kommunen bør iværksætte passende tiltag, hvis der observeres mangler i serviceleverancen.

Kommunen bør bevare tilstrækkelig overordnet styring og indsigt i alle sikkerhedsaspekter, når information gøres tilgængelig for, behandles af eller administreres af en leverandør. Dette er særligt vigtigt ved følsomme eller kritiske informationer.

15.2.2. Styring af ændringer af leverandørydelser

Ændringer af leverandørydelser skal styres og vurderes under hensyntagen til, hvor kritiske de involverede informationer, systemer og processer er. Giver ændringerne anledning til, at der sker en revurdering af risici, skal det gøres straks, og gerne inden ændringens ikrafttræden.

Også ændringer hos Kommunen kan give anledning til en revurdering af risici.

Kommunen skal særligt være opmærksom på ændringer i selve aftalen med en leverandør, ændringer i Kommunen med henblik på implementering af forskellige tiltag, f.eks. nye serviceydelser eller applikationer, eller ændringer i leverandørens ydelser med f.eks. henblik på at implementere nye teknologier, udviklingsværktøjer og -miljøer, leverandørskift og lokation for servicefaciliteter. *

16. Styring af informationssikkerhedsbrud

16.1. Styring af informationssikkerhedsbrud og forbedringer

16.1.1. Ansvar og procedurer

Det er Informationssikkerhedsudvalgets ansvar, at der udarbejdes procedurer, der sikrer en ensartet og effektiv metode til styring af informationssikkerhedsbrud og brud på persondata-sikkerheden (herefter omtalt som sikkerhedsbrud).

Informationssikkerhedskoordinator er ansvarlig for udarbejdelse af procedurer for håndtering af informationssikkerhedshændelser og –brud, herunder procedure for rapportering af hændelser og brud samt rapporteringsskemaer. Proceduren skal samtidig sikre et passende svar til de personer, som rapporterer om mulige sikkerhedshændelser.

Informationssikkerhedskoordinator er ansvarlig for at dokumentere og registrere alle informationssikkerhedshændelser og -brud og deres håndtering, samt at Informationssikkerhedsudvalget løbende orienteres om disse.

Systemejer er ansvarlig for, at hændelser, der har indflydelse på tilgængelighed, bliver afklaret i henhold til gældende procesvurdering (KLE-ark). Driftshændelser, der ikke kan afklares inden for de aftalte rammer, skal håndteres som en sikkerhedshændelse. De ramte brugere og systemejere skal informeres hurtigst muligt.

Alle medarbejdere er ansvarlige for at være opmærksom på informationssikkerhedshændelser og –brud, samt at indberette disse efter gældende procedurer for håndtering af informations-sikkerhedshændelser og -brud.

Alle it-brugere i kommunen skal hurtigst muligt rapportere informationssikkerhedshændelser til nærmeste leder. Nærmeste leder skal altid underrette Informationssikkerhedskoordinator på databeskyttelse@naestved.dk i sådanne tilfælde. Her vil det blive vurderet, om der er tale om en reel informationssikkerhedshændelse og hvilke foranstaltninger, der skal iværksættes.*

Administrationsgrundlag for håndtering af brud på persondatasikkerhed findes på NORA.

16.1.2. Rapportering af informationssikkerhedshændelser

Informationssikkerhedsudvalget skal sikre, at der etableres en rapporteringsmulighed i forbindelse med informationssikkerhedshændelser og -brud.

Informationssikkerhedsudvalget skal sikre, at der gennemføres informationskampagner og lignende for at gøre alle medarbejdere bekendt med, hvad sikkerhedsbrud er, og at de har pligt til omgående at indberette alle sikkerhedsbrud og mistanke om sikkerhedsbrud.

Ved informationssikkerhedshændelser eller -brud skal dette straks rapporteres – også hvor omfanget endnu ikke er fuldt afdækket. Hurtigheden er vigtigere end at formelle formularer bliver udfyldt korrekt.

For sikkerhedsbrud, som omhandler data, der skal beskyttes i forhold til Databeskyttelsesforordningen, gælder det, at der anmeldelsespligt i forhold til Datatilsynet indenfor 72 timer.

Situationer, der skal rapporteres som brud på persondatasikkerheden, omfatter bl.a.:

- Uautoriseret videregivelse af eller adgang til personoplysninger
- Hændelig eller ulovlig tilintetgørelse, tab eller ændring af personoplysninger

Situationer, der skal rapporteres som informationssikkerhedshændelser eller -brud, omfatter bl.a.:

- Ineffektiv sikkerhedsstyring
- Brud på integritet, fortrolighed eller tilgængelighed
- Overtrædelse af politikker eller retningslinjer som vedrører informationssikkerhed
- Brud på fysisk sikkerhed
- Ukontrollerede systemændringer
- Fejl i software eller hardware
- Brud på adgangskontrollerne

Fejl og andre situationer, hvor systemer opfører sig unormalt, kan være en indikator for et sikkerhedsangreb, eller at et sikkerhedsbrud har fundet sted, og skal derfor altid indrapporteres.

Informationssikkerhedskoordinatoren skal sikre en periodisk rapportering til Informationssikkerhedsudvalget over konstaterede informationssikkerhedshændelser og -brud.

16.1.3. Rapportering af informationssikkerhedssvagheder

Informationssikkerhedsudvalget skal sikre, at der etableres en rapporteringsmulighed, så alle ledere, medarbejdere og leverandører mv. så enkelt som muligt kan indrapportere observerede svagheder eller mistanke om svagheder i systemerne (elektroniske såvel som fysiske).

Informationssikkerhedsudvalget skal sikre, at der gennemføres informationskampagner og lignende for at gøre alle medarbejdere bekendt med, at de har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester.

Det er alene Informationssikkerhedsudvalget eller en person, som udvalget bemyndiger til dette, der kan give tilladelse til at ledere, medarbejdere og leverandører mv. tester for svagheder eller sikkerhedsbrister. Hvis en person foretager opslag som en test uden at have tilladelse, kan det blive anset for misbrug af adgangen til personoplysninger, hvilket kan udløse sanktioner.

Team Servicedesk og IT skal registrere it-sikkerhedsbrud i servicedesk-systemet. Disse oplysninger skal bruges til at identificere og afbøde tilbagevendende sikkerhedshændelser eller disses konsekvenser.*

16.1.4. Vurdering af og beslutning om informationssikkerhedshændelser

Informationssikkerhedsudvalget skal sikre, at der i forbindelse med modtagelse af indrapporteringer, er en proces for vurdering af hændelsens omfang og kritikalitet, og om hvorvidt der er tale om et informationssikkerhedsbrud og/eller et brud på persondatasikkerheden. Processen

skal desuden indeholde beskrivelse af, hvordan prioriteringen og eskalering af hændelsen skal foregå, samt hvordan dokumentationen skal udformes.

De procedurer, som Informationssikkerhedsudvalget fastlægger, jf. afsnit 16.1.1., skal på baggrund af Datatilsynets retningslinjer omfatte en konkret procedure for indberetning til Datatilsynet og for registrering af den lovpligtige interne dokumentation omkring hændelser og brud.

16.1.5. Håndtering af informationssikkerhedsbrud

Alle informationssikkerhedsbrud og brud på persondatasikkerheden skal håndteres i overensstemmelse med de procedurer, som Informationssikkerhedsudvalget har fastsat, jf. afsnit 16.1.1.

Det første mål ved håndteringen er at genoprette det normale sikkerhedsniveau og herefter påbegynde den nødvendige retablering.

16.1.6. Erfaringer fra informationssikkerhedsbrud

Opfølgning på rapporterede sikkerhedshændelser

Informationssikkerhedskoordinator er ansvarlig for at indsamle og analysere rapporterede sikkerhedshændelser og -brud.

Vurdering af tidligere hændelser

Mindst en gang om året skal Informationssikkerhedskoordinatoren gennemgå den forgangne periodes hændelser og brud og på denne baggrund udforme en vurdering af, hvorvidt sikkerhedsforanstaltningerne kan forbedres eller præciseres. Dette kan udmunde i forslag om opdaterede regler, procedurer eller opdateret risikovurdering. Rapporteringen skal forelægges for Informationssikkerhedsudvalget til beslutning af eventuelle videre skridt samt evt. for direktionen til orientering.

16.1.7. Indsamling af beviser

Hvis et sikkerhedsbrud forventes at afstedkomme et retsligt efterspil - uanset om sikkerhedsbruddet er foretaget af en person eller en virksomhed - skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale.

Medarbejdere eller eksterne konsulenter, der skal sikre indsamling af beviser, skal være certificeret eller på anden måde være kvalificeret til opgaven, samt benytte værktøjer, som er i stand til at styrke værdien af bevismaterialet.

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Kommunes opgaveløsning og varetagelse af samfundsmæssige forpligtelser er i vid udstrækning it-understøttet. Det betyder, at it-nedbrud kan have alvorlige konsekvenser for kommunens opgaveløsning og serviceringen af borgere og virksomheder.

Det er således af afgørende betydning, at kommunen har et it-beredskab og nødplaner, der kan sikre, at hændelser med alvorlige og omfattede it-nedbrud, kan håndteres ansvarligt og på betryggende vis.

Risikostyring og katastrofeplanlægning har til formål at mindske risikoen for og effekten af uforudsete hændelser. Nødprocedurer skal være med til at opretholde den pågældende service således, at skaderne for kommunen, borgerne og virksomhederne minimeres.

17.1. Informationssikkerhedskontinuitet

17.1.1. Planlægning af informationssikkerhedskontinuitet

Identifikation af kritiske systemer

Planlægning for kontinuitet skal som minimum ske for alle forretningskritiske systemer. Herudover kan der være tale om særligt udvalgte systemer.

Den øverste sikkerhedsansvarlige har ansvaret for, at alle forretningskritiske og udvalgte systemer er identificeret og dokumenteret med ejerskab.

Prioriteringsliste for hændelser fremgår i Team Servicedesk og It's driftsdokumentation.*

Generel it-beredskabsstyringsproces

It-beredskabet skal:

- Formaliseres i it-beredskabsplanen med organisatorisk tilrettelæggelse af krisehåndtering i forbindelse med kritiske sikkerhedshændelser.
- Fastlægge ansvarsfordeling, og beskrive procedurer for information og kommunikation til den øverste ledelse samt medarbejdere og samarbejdspartnere og eventuelt borgere i forbindelse med alvorlige it-nedbrud.
- Overordnet sikre, at vitale it-nedbrud kan håndteres effektivt, kan reetableres og bringes tilbage til normal drift indenfor en acceptabel tidsramme.
- Fastlægge ledelsesansvar, koordination og kommunikation mhp. at kommunen er i stand til at videreføre og/eller reetablere vitale it-funktioner inden for accepterede tidsfrister.
- Skal sikre, at der i relevant omfang findes nødplaner for opretholdelse af kritiske kommunale opgaver under omfattende it-nedbrud.

Informationssikkerhedsudvalget er ansvarlig for, at der er udarbejdet og til stadighed er vedligeholdt en generel it-beredskabsstyringsproces, som skal omhandle de krav til it-sikkerhed, der er nødvendige for kommunens fortsatte it-drift.

Team Servicedesk og IT skal udarbejde og vedligeholde en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for kommunens fortsatte drift. Processen fremgår af bilag D It-beredskabsplan. Desuden er der udarbejdet en kanal og kommunikationsstrategi for Team Servicedesk og IT.*

It-beredskabsplanen

It-beredskabsplanen indgår som en del af det overordnede beredskab for kommunen.

Som udgangspunkt omfatter planen it-beredskabet for kommunens it-infrastruktur og de it-systemer, som anvendes af kommunen.

It-beredskabsplanen skal være grundlaget for at kunne opretholde eller genetablere vitale it-funktioner i forbindelse med katastrofesituationer og andre alvorlige krisesituationer.

Der skal udarbejdes en kontaktliste fx som et bilag til beredskabsplanen.

Informationssikkerhedsudvalget er ansvarlig for, at der bliver udarbejdet en it-beredskabsplan.

It-beredskabsplanen skal være tilgængelig i elektronisk form og herudover altid forefindes i to papirkopier, som skal opbevares i Team Servicedesk og It samt en anden geografisk lokation. It-beredskabsplanen skal være underlagt versionsstyring.

Det skal være klart defineret, hvem der har ansvaret for aktivering af it-beredskabsplanen. Medarbejdere, der udgør en del af it-beredskabsplanen, skal være informeret om dette ansvar.

Organisering

Det skal udpeges en kriseledelse med kompetence til at træffe nødvendige beslutninger og til at informere i den aktuelle situation på baggrund af instruks i kommunens samlede beredskabsplan og nødberedskab.

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

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.*

Kommunikation i den generelle beredskabsplan for Næstved Kommune fremgår af:
https://nstvedkommune1.saas.neupart.com/authenticate?redirectto=/main/security/redirect *

Der skal for alle funktioner være udpeget suppleanter.

Nødplaner

Systemejer er ansvarlig for at der, for alle kritiske og udvalgte forretningssystemer, forefindes en opdateret nødplan, der kan aktiveres ved behov.

En særskilt beredskabsplan for reaktion på malwareudbrud og lignende fremgår i bilag H. *

17.1.2. Implementering af informationssikkerhedskontinuitet

Risikovurdering

Der skal foreligge en risikovurdering for alle kritiske it-systemer (jf. kapitel 8 om risikostyring).

På baggrund af risikovurderingen fra systemejere samt en forretningsmæssig vurdering fra ledelsen skal alle systemer prioriteres ud fra deres væsentlighed for kommunens fortsatte drift. I prioriteringen tages højde for indbyrdes afhængighed, så alle systemer, som kræves for driftsafvikling af kritiske systemer, som udgangspunkt også betegnes som kritiske.

Konsekvensvurdering

Konsekvenser af hændelser i forbindelse med it-systemerne skal jævnligt vurderes og danne grundlag for justering af beredskabsplanen.

Indkaldelse af medarbejdere i vagtordning og ekstra personale

I tilfælde af behov for ekstraordinær drift, ved sikkerhedshændelser og lignende, skal der forefindes retningslinjer for tilkaldelse af relevant personale.

Uddannelse i nødprocedurer

Systemejer har ansvaret for, at der foregår tilstrækkelig uddannelse af medarbejdere i de aftalte nødprocedurer.

Hver systemejer skal sikre, at alle medarbejdere er bekendt med procedurer for etablering og anvendelse af nødberedskabet, og hvilke opgaver de har i denne forbindelse.

Det skal løbende sikres, at de nødvendige kompetencer til løsning af opgaverne forbundet med beredskabet er til stede i kommunen eller kan skaffes inden for fastsatte tidsfrister, f.eks. ved brug af eksterne leverandører.

17.1.3. Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten

Afprøvning og vedligeholdelse af it-beredskabsplanen

It-beredskabsplanen skal ved større ændringer og mindst en gang årligt afprøves og opdateres for at sikre, at den er tidssvarende og effektiv.

Den anvendte afprøvning kan være:

- Skrivebordstest af forskellige scenarier (diskussioner af beredskabsplanerne ved brug af eksempler på nedbrud)
- Simuleringer (med henblik på at træne deltagerne i håndtering af deres roller efter episoden)
- Teknisk retablering (sikring af at tekniske systemer kan retableres effektivt)
- Afprøvning af retablering fra andre lokaler end de oprindelige (sikre uafhængighed fra driftspersonalets arbejdspladser)
- Afprøvning af retablering af systemer der placeres andetsteds end det oprindelige (serverrum)

- Afprøvning af leverandørers faciliteter og ydelser (sikre at eksterne ydelser og produkter lever op til betingelserne i kontrakten)
- Total afprøvning (afprøve at virksomheden, personalet, udstyret, faciliteterne og nødprocedurerne kan håndtere katastrofer).

Informationssikkerhedsudvalget træffer afgørelse om afprøvningens omfang.

Resultatet af afprøvningen skal dokumenteres, og opdatering af it-beredskabsplanerne skal foretages, hvor det er nødvendigt.

Afprøvning af reetableringsprocesser

It-beredskabet lægges an på, at der kan reetableres data, operativsystemer og applikationer fra backup. Derfor skal det løbende og mindst en gang om året kontrolleres, at reetablering fra backupdata kan gennemføres og er korrekt.

Retningslinjer for sikkerhedskopiering fremgår af bilag G Backup.*

Evaluering af beredskabet og nødprocedurer

Senest 14 dage efter afslutning af et aktiveret beredskab, skal der ske en evaluering af forløbet mhp. eventuel opdatering af beredskabs- og nødplaner.

17.2. Redundans

Tilgængelighed af informationsbehandlingsfaciliteter

Hvis der inden for kommunen identificeres et forretningskrav om tilgængelighed, som ikke kan garanteres af den almindelige systemarkitektur, bør der for de identificerede systemer være etableret fuld redundans. Ved fuld redundans forstås, at der ved nedbrud umiddelbart kan skiftes over til det sekundære system mhp. fortsat drift.

Redundante funktionaliteter bør opfylde samme sikkerhedskrav som det primære system, og bør testes ved større ændringer. Det anbefales at gennemføre test to gange om året.

18. Overensstemmelse

Formål

For at overholde gældende lov og kontraktkrav skal kommunen identificere alle relevante lov-, myndigheds- og kontraktkrav med relevans for den enkelte fagforvaltning.

18.1. Overensstemmelse med lov- og kontraktkrav

18.1.1. Identifikation af gældende lovgivning og kontraktkrav

Ansvar

Systemejer har ansvaret for at sikre, at der er overensstemmelse mellem lov- og kontraktkrav, samt at der udarbejdes underliggende procedurer, hvor der er behov.

Relevant lov-, myndigheds- og kontraktkrav

Når det skal klarlægges, hvilke relevante krav der findes på et område, tages der udgangspunkt i de konkrete arbejdsopgaver. Herunder tages stilling til, hvilke krav der er til håndtering af informationer i lovgivning, eventuelle forpligtelser og krav pålagt i medfør af kontrakter samt overordnede myndighedskrav.

Metoden til at sikre, at alle krav overholdes, er en formalisering af retningslinjer, der sikrer overholdelse af de krav, der er inde for dit arbejdsområde. Det skal altid være muligt at dokumentere, at kravene overholdes.

18.1.2. Immaterielle rettigheder

Kommunen skal sikre, at immaterielle rettigheder ikke krænkes. Dette gælder både for immaterielle rettigheder ejet af Kommunen, samt for immaterielle rettigheder ejet af tredjeparter, herunder Kommunens leverandører. Ved behov skal der fastsættes procedurer for sikring af heraf.

Kommunen skal sikre overblik og overholdelse af immaterielle forpligtelser. Forpligter Kommunen sig til at overholde visse immaterielle rettigheder samt eventuelle udvidelser af disse fastsat ved indgåelse af kontrakter, skal det sikres, at de enkelte forpligtelser er beskrevet og formidlet til brugerne af leverandørens ydelse(r). Er der behov for at fastsætte særlige procedurer for sikring af overholdelse af immaterielle rettigheder fastsat af leverandøren, skal det sikres, at disse udarbejdes og kommunikeres til de relevante medarbejdere.

Kommunen skal løbende sikre, at der kun er installeret autoriserede systemer med autoriserede licenser i Kommunen.

Systemejer skal sikre sig, at software-licensaftaler overholdes, f.eks. at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.

Retningslinjer for programanvendelse og licenser fremgår af bilag 1.*

Team Servicedesk og IT har som opgave, at forhandle og administrere licensaftaler for programmer, som anvendes af hele kommunen. Team Servicedesk og IT skal være i stand til at dokumentere, at licensforholdene til standard kontorprogrammer er i orden.*

Licensforhold og programanvendelse af de enkelte fagsystemer påhviler systemejeren.*

Retningslinjer for systemejere fremgår af bilag A.*

18.1.3. Beskyttelse af registreringer

Oplysninger, som tilgår kommunen, skal sikres mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overensstemmelse med lov-, myndigheds-og kontraktkrav samt forretningsmæssige krav. Det betyder, at oplysningerne skal sikres både teknisk og organisatorisk, så der ikke opstår situationer, hvor oplysninger anvendes på en utilsigtet måde, eller Kommunen mister kontrollen med oplysningerne. Derudover skal der sikres en høj kvalitet af oplysningerne.

18.1.4. Privatlivets fred og beskyttelse af personoplysninger

Privatlivets fred og personoplysninger skal beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter for de enkelte arbejdsområder.

Der skal gennemføres sikkerhedsforanstaltninger med henblik på, at der kun behandles de personoplysninger, der er nødvendige til at opfylde behandlingens specifikke formål.

Kommunen skal sikre, at der fastsættes procedurer til sikring af overholdelse af lovfæstede krav til behandling af personoplysninger. Procedurerne skal klarlægge og strukturere kravene til de enkelte behandlinger, herunder tage højde for blandt andet formålsbegrænsning, oplysningspligt, risikovurdering, sikkerhedsniveau, databehandleraftaler, dataminimering og slettefrister.

Alle personoplysninger skal behandles på baggrund af et gyldigt grundlag, i henhold til lov.

Når personoplysninger sendes mellem medarbejdere eller personoplysninger bliver brugt i kommunikation, skal der sikres et tilstrækkeligt niveau af beskyttelse, herunder kryptering, sikre mailtjenester, mv.

Fortegnelse

Den ansvarlige leder skal sikre at nye behandlinger indføres i fortegnelsesoversigten og denne ajourføres ved ændringer.

Gennemsigtige oplysninger og meddelelser for personoplysninger

Det skal sikres, at der er fastsat gennemsigtige og lettilgængelige regler for behandlingen af personoplysninger og udøvelsen af registreredes rettigheder.

Uddybende detaljer findes i kapitel 18.3.

Databeskyttelsesrådgiver (DPO)

Kommunen skal sikre at der til enhver tid er en fungerende databeskyttelsesrådgiver.

18.1.5. Regulering af kryptografi

Systemejer skal sikre at kryptografi anvendes i overensstemmelse med alle relevante aftaler, love og forskrifter. Systemejer er ansvarlige for at informere medarbejdere om de regler og retningslinjer, der er gældende for kryptografi.

18.2. Gennemgang af informationssikkerhed

18.2.1. Uafhængig gennemgang af informationssikkerhed

Informationssikkerhedsudvalget skal mindst en gang årligt kontrollere, at informationssikkerhedspolitikken er implementeret i organisationen, og at den overholdes. Kontrollen skal foretages af uafhængig part fx DPO, revisionen, intern auditgruppe.

18.2.2. Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

Alle systemejere skal mindst en gang om året i henhold til den risikobaserede tilsynsplan, kontrollere de kontraktlige forhold, herunder databehandleraftaler og revisionserklæringer, som er knyttet til de systemer, den enkelte systemejer er ansvarlig for. Derudover skal systemejer påse, at forretningsprocesser, risikovurdering og beredskabsplaner/nødplaner, samt brugerstyring og logning er i overensstemmelse med kommunens vedtagne niveau og databeskyttelseslovgivningen.

Systemejerne skal dokumentere resultaterne af deres kontrol og de eventuelle korrigerende handlinger, den har givet anledning til.

18.2.3. Undersøgelse af teknisk overensstemmelse

IT-Teamleder skal løbende og mindst en gang årligt vurdere om informationssystemer, herunder eksternt og internt netværksudstyr og servere er i overensstemmelse med kommunens vedtagne sikkerhedsniveau. Der skal i den forbindelse gennemføres penetrationstest eller sårbarhedsvurdering på netværksudstyr og servere.

IT-Teamleder skal dokumentere resultaterne sine af vurderinger, penetrationstest mv.

18.3. Registreredes rettigheder *

Kommunen skal til enhver tid overholde sin oplysningspligt.

Oplysninger om behandlingen skal gøres tilgængelige for den registrerede inden behandlingen påbegyndes og skal til enhver tid kunne gøres tilgængelig for den registrerede under behandlingen.

Dataejer skal sikre, at det er muligt at kunne udlevere alle oplysninger og meddelelser vedrørende behandlingen til den registrerede i en letforståelig form og i et klart og forståeligt sprog, som er tilpasset den registrerede.

Det skal sikres, at borgeren bliver givet alle lovpligtige oplysninger, omkring behandlingen, ved behandlingens start. Det omfatter bl.a. formålet, retsgrundlaget, klagemuligheder, hvilket oplysninger der ønskes behandles m.v. I ansøgningssager, der sker på borgerens initiativ, skal alle lovpligtige oplysninger være givet på forhånd.

Der sondres mellem, hvorvidt personoplysningerne indhentes hos borgeren selv, eller om de bliver indhentet fra andre end borgeren.

1. Oplysningspligt ved indsamling af personoplysninger hos den registrerede

F.eks. ansøgningssager eller anden bevilling, der sker på borgerens initiativ

Det skal sikres, at borgeren bliver givet alle lovpligtige oplysninger, omkring processen, ved behandlingens start. Kommunens Oplysningspligt omfatter bl.a., at borgeren er klar over, hvad oplysningerne skal bruges til, hvilket retsgrundlag vi behandler oplysningerne på baggrund af, klagemulighede osv.

Disse oplysninger skal fremgå af alle relevante ansøgningsskemaerne m.v.

2. Oplysningspligt, når personoplysningerne bliver indhentet hos andre end borgeren selv

F.eks. indsamling fra en anden forvaltningsenhed eller myndighed.

Det skal sikres, at borgeren bliver givet alle lovpligtige oplysninger, omkring behandlingen, inden for fastsatte tidsfrister.

Efter samme principper, som under punkt 1 har borgeren ret til at få oplysninger om, når der sker behandling af vedkommendes personoplysninger, uden dennes viden. Det stiller derfor krav til, at man skal have gjort sig overvejelser om formålet med behandlingen og ikke mindst vurderet retsgrundlaget, da det, ud over en række andre oplysninger, skal meddeles borgeren. Borgeren har bl.a. ret til at gøre indsigelser mod eller klage over behandlingen.

Forudgående godkendelse og høring for behandling af personoplysninger

Kommunen (den dataansvarlige) og leverandøren (databehandleren) skal, vedligeholde en fortegnelse over databehandlinger. For særligt kritiske typer behandlinger, skal der udarbejdes en konsekvensvurdering (Data Protection Impact Assessment) DPIA inden behandlingen af personoplysninger påbegyndes.

Gennemsigtige oplysninger og meddelelser for personoplysninger

Kommunen skal sikre, at der er fastsat gennemsigtige og lettilgængelige regler for behandlingen af personoplysninger og udøvelsen af registreredes rettigheder.
Kommunen skal sikre, at det er muligt at kunne udlevere alle oplysninger og meddelelser vedrørende behandlingen til den registrerede i en letforståelig form og i et klart og forståeligt sprog, som er tilpasset den registrerede.

Begrænsning i behandlingen af personoplysninger

Kommunen skal implementere mekanismer med henblik på at sikre, at kun de personoplysninger, der er nødvendige til det specifikke formål med behandlingen, behandles.

Ret til indsigt i personoplysninger

Den registrerede har til enhver tid ret til at anmode kommunen om at få indsigt i hvilke personoplysninger der behandles om vedkommende.
Retningslinjer fremgår af bilag 9 Persondata.

Berigtigelse af behandlede personoplysninger

Kommunen skal sikre, at oplysningerne er korrekte. Der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles straks slettes eller berigtiges.

Udpegning af databeskyttelsesrådgiver for personoplysninger

Kommunen har udpeget en databeskyttelsesrådgiver i henhold til databeskyttelsesforordningen. Databeskyttelsesrådgiverens stilling og opgaver fremgår af databeskyttelsesforordningens artikel 37-39.

19. Bilag

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. Destruktion
9. Beskyttelse af persondata
10. Brug af foto-, video- og lydoptagelser

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