UDKAST

Tværgående retningslinjer for informationssikkerhed

Norddjurs Kommune

Godkendt af Norddjurs Kommunes direktion XX.XX.XXXX

Indholdsfortegnelse

1. Indledning

1.1: Formål med de tværgående retningslinjer for informationssikkerhed

Formålet med de tværgående retningslinjer for informationssikkerhed er at supplere Norddjurs Kommunes informationssikkerhedspolitik med overordnede retningslinjer for, hvordan informationssikkerheden skal udmøntes i organisationen.

Retningslinjerne henvender sig primært til Norddjurs Kommunes ledelse, og angiver hvordan kommunen arbejder med informationssikkerhed, samt hvilke procedurer der skal foreligge i aftaleenhederne. Det er desuden ledelsens ansvar at kommunikere de relevante retningslinjer og regler til deres medarbejdere.

1.2: Målsætninger med de tværgående retningslinjer for informationssikkerhed

Informationssikkerheden skal understøtte Norddjurs Kommunes forretningsgange og sikre den påkrævede fortrolighed af fortrolige og følsomme informationer, pålideligheden til de informationer der anvendes samt tilgængeligheden til vores forretningssystemer og -informationer.

De tværgående retningslinjer for informationssikkerhed skal sikre, at informationerne vi opbevarer, videregiver, træffer afgørelse på samt generelt behandler altid holdes fortrolige, når dette er påkrævet, altid er korrekte, så behandling sker på oplyst grundlag, og at de altid er tilgængelige for de autoriserede brugere.

De tværgående retningslinjer for informationssikkerhed skal understøtte informationssikkerhedspolitikken målsætninger:

- Skabe opmærksomhed og udvikle kompetencerne om informationssikkerhed og databeskyttelse i hele kommunen
- Styre kommunens arbejde med informationssikkerheden gennem en risikobaseret styringsmetode
- Sikre fortrolighed af kommunens informationer, således kun autoriserede kan tilgå oplysningerne
- Sikre integritet af kommunens informationer, så de fremstår korrekte og ikke uhensigtsmæssigt ændres eller manipuleres
- Sikre tilgængelighed til kommunens informationer, så autoriserede kan tilgå de oplysninger der kræves, for at kommunens services kan udføres
- Sikre, at kommunen udviser ansvarlighed ved dokumentation af overholdelse af relevante aftaler og lovgivning
- Sikre, at informationssikkerheden ikke nedprioriteres i kommunen på usagligt grundlag

1.2.1: Afbalanceret informationssikkerhed

Norddjurs Kommune er afhængig af et godt omdømme og fortsat politisk tillid, da vi er af stor samfundsmæssig betydning for lokalområdet og en vigtig aktør i den offentlige forvaltning i Danmark. Retningslinjerne skal derfor sikre, at kommunen efterlever de krav, der stilles af nationale myndigheder samt de aftaler vi indgår i. Sikkerhedsniveauet skal dog altid afbalanceres, så kommunens kerneopgaver ikke kompromitteres. Dette betyder, at der skal være fleksibilitet i arbejdet med informationssikkerhed. Kommunens økonomiske rammer, omdømme og kerneydelser skal altid indtænkes. Der skal ske en konkret vægtning af informationers værdi for kommunen og de borgere, der har personoplysninger registreret.

Sund fornuft er derfor et essentielt værktøj i arbejdet.

1.3: Omfang

De tværgående retningslinjer for informationssikkerhed er dokumentet, der angiver Norddjurs Kommunes direktions beslutninger om informationssikkerhedsniveauet for kommunen. Det definerer de krav, kommunen skal efterleve, for at det målsatte sikkerhedsniveau kan efterleves. Retningslinjerne dækker derfor følgende:

- De gælder for alle ansatte i Norddjurs Kommune, uanset ansættelsesform. Det forventes, at alle der beskæftiger sig med Norddjurs Kommunes informationer overholder relevante retningslinjer.
- De dækker alle systemer der behandler informationer i Norddjurs Kommune, både digitale og fysiske.
- De gælder for leverandører og samarbejdspartnere, som har enten fysisk eller logisk adgang til kommunens systemer og informationer. Det forventes, at de har kendskab til og følger informationssikkerhedspolitikken samt disse retningslinjer.
- Retningslinjerne revideres på årlig basis af informationssikkerhedsudvalget, for at sikre, at den er i overensstemmelse med Norddjurs Kommunes sikkerhedsmålsætninger. Direktionen orienteres om større ændringer i retningslinjerne.

2. Risikostyring

2.1: Risikovurdering

Norddjurs Kommune efterstræber, at det konkrete sikkerhedsniveau vurderes ud fra et afbalanceret forhold mellem forretningsmæssige informationsrisici, risici for de registreredes rettigheder og kommunens økonomiske forhold.

Sikkerhedsniveauet skal afspejle de trusler og sårbarheder der findes for Norddjurs Kommune, dog går gældende lovgivning og persondatarettighederne forud for kommunens ressourcemæssige forhold.

Der skal løbende foretages revidering af kommunens risikobillede, herunder også vurderingerne der etablerer sikkerhedsforanstaltningerne for kommunens informationer og systemer, således sikkerheden afspejler de konkrete risici. Vurderingerne og risikobilledet skal revideres årligt, eller ved større organisatoriske forandringer, der skaber nye arbejdsgange, herunder anvendelse af nye IT-systemer eller omstruktureringer.

2.2: Sikkerhedsniveau

Norddjurs Kommunes sikkerhedsniveau skal indfri de målsætninger, som der er beskrevet i dette dokument. Det vil sige, at der er tilstrækkelig fortrolighed, integritet og tilgængelighed for de kritiske og prioriterede forretningsmæssige informationer. Norddjurs Kommune ønsker at fremstå med et højt sikkerhedsniveau, der tilgodeser:

- Lovgivningsmæssige krav
- De anerkendte standarder for informationssikkerhed i form af ISO 27001-kravstandarden

3. Organisering og ansvar

3.1: Interne organisatoriske forhold

Norddjurs Kommunes kommunalbestyrelse har det politiske ansvar for kommunens informationssikkerhed, herunder at kommunens styring af databehandling er bæredygtig.

Direktionen har det strategiske ansvar for Norddjurs Kommunes informationssikkerhed, og uddelegerer ansvaret til de relevante funktionsområder. Det daglige ansvar for informationssikkerheden ligger i informations-

sikkerhedsudvalget og hos informationssikkerhedskoordinatoren. Udvalget har det overordnede og generelle ansvar for, at Norddjurs Kommune har et tilstrækkeligt sikkerhedsniveau.

Alle Norddjurs Kommunes ansatte har et medansvar i kommunens sikkerhed. Medansvaret afhænger af den ansattes rolle i kommunen, men stiller også forventning til, at den ansatte holder sig orienteret med kravene til sin rolle.

Organisering og ansvar i kommunens administration udmøntes konkret i "Norddjurs Kommunes informationssikkerhedsstrategi – strategi – organisering – ansvar", der beskriver forventninger og krav til de forskellige roller inden for informationssikkerhedsarbejdet. Udmøntningen af ansvar følger Norddjurs Kommunes principper for aftalestyring.

3.2: Styringsprincipper

Informationssikkerhed er et anliggende for hele organisationen, og bliver koordineret af informationssikkerhedsudvalget og informationssikkerhedskoordinatoren, ifølge de til en hver tid gældende politikker i Norddjurs Kommune.

Informationssikkerhedskoordinatoren vejleder ledelse og medarbejdere i informationssikkerhedsspørgsmål, og koordinerer samt følger op på informationssikkerhedsrelaterede aktiviteter.

IT-afdelingen, Staben og databeskyttelsesrådgiveren vejleder til enhver tid informationssikkerhedsudvalget og informationssikkerhedskoordinatoren om deres pågældende ressortområder.

3.3: Eksterne samarbejdspartnere

Der skal indgås skriftlige aftaler med eksterne samarbejdspartnere, der dokumenterer overholdelse af de sikkerhedskrav, som Norddjurs Kommune stiller, for bl.a. at efterleve databeskyttelsesforordningen og -loven, ISO 27001 og interne politikker.

Norddjurs Kommunes IT- og digitaliseringsafdeling samt kommunens databeskyttelsesrådgiver, skal involveres ved indgåelse af aftaler som henholdsvis vedrører IT-systemer eller persondatabehandlinger.

For at sikre klarhed over sikkerhedskrav, skal risici identificeres og vurderes, i forbindelse med brug af eksterne leverandører.

Eksterne samarbejdspartnere, der har adgang til kommunens informationer, skal efterleve samme retningslinjer, som dem der gælder internt i kommunen.

4. Klassifikation af systemer og informationer

For at sikre at vores systemer og informationer har det tilstrækkelige sikkerhedsniveau, skal disse identificeres og klassificeres i forhold til, hvor kritiske de er for kommunens forretningsgange.

Der skal angives ansvarlige ejere for alle kommunens systemer. Disse beskrives som systemejere i Norddjurs Kommune.

Systemer og informationer skal klassificeres ud fra et forretningsmæssigt- og databeskyttelsesperspektiv. ift. værdien for organisationen og de registrerede.

Systemets/informationsaktivets forretningsmæssige værdi klassificeres ud fra følgende kategorier:

Værdiskala for Norddjurs Kommune

1. Mindre kritisk - informationsaktivet/persondatabehandlingen er mindre vigtigt for kommunens forretningsgang, og mangel på tilgængelighed, korrekthed eller fortrolighed af det er tilgiveligt

2. Moderat kritisk – informationsaktivet/persondatabehandlingen er vigtigt for kommunens forretningsgang, og der vil være mærkbart tab hvis der er mangel på tilgængelighed, korrekthed eller fortrolighed

3. Kritisk – informationsaktivet/persondatabehandlingen er meget vigtigt for kommunens forretningsgang, og mangel på tilgængelighed, korrekthed eller fortrolighed vil lede til alvorlig indvirkning for kommunens virke

4. Meget kritisk – informationsaktivet/persondatabehandlingen er essentielt for kommunens forretningsgang, og skal på alle tidspunkter af døgnet være tilgængelig, korrekt eller fortroligt

Værdiskala for den registrerede

1. Offentlig viden – personoplysningerne er offentligt tilgængelige, og tab heraf har ingen indvirkning på de registreredes rettigheder

2. Ikke fortroligt eller følsomt – personoplysningerne er af almindelig karakter, og tab eller ændring heraf har kun begrænsede konsekvenser for de registreredes rettigheder

3. Fortroligt el. overvejende fortroligt, men ikke følsomt – kompromitterede personoplysninger har betydelig konsekvens for de registreredes rettigheder

4. Følsomt – kompromitterede personoplysninger kan have høje konsekvenser for de registreredes rettigheder, herunder med døden til følge eller grov diskrimination

5. Brugeradfærd

For at nå i mål med Norddjurs Kommunes målsætninger for informationssikkerhed, kræves det, at alle ansatte tager medansvar for sikkerheden.

Derfor, skal alle ansatte være bekendte med informationssikkerhedspolitikken, herunder de relevante og gældende retningslinjer for ønsket adfærd på området.

Det er vigtigt at huske, at systemer og informationer er redskaber til varetagelsen af Norddjurs Kommunes kerneopgaver. Behandling af systemer og informationer kræver sund fornuft, og bør ikke opleves som en hindring i arbejdet.

Norddjurs Kommunes ansatte skal derfor altid følge disse retningslinjer:

- Persondata behandles i alle tilfælde fortroligt
- Der anvendes personligt login og password, og password skiftes med jævne mellemrum
- Datamedier med persondata og vigtige informationer behandles og beskyttes med omhu mod at uvedkommende får adgang til dem
- Mobilt udstyr beskyttes og opbevares, så andre ikke kan få adgang til det
- Det er vigtigt at kunne anvende internettet i mange sammenhænge. Besøg på sider med racistisk, uetisk eller pornografisk indhold er ikke acceptabelt på noget tidspunkt på kommunens computere, mobiler m.m.

- Mail anvendes til kommunikation på mange niveauer – også til privat kommunikation, men bør holdes på et rimeligt niveau
- Der må kun anvendes IT-programmer, som er godkendt af IT-afdelingen
- Hvis man oplever, at der sker brud på informationssikkerheden, er det vigtigt at informere sin nærmeste leder og indberette bruddet til kommunens informationssikkerhedskoordinator og databeskyttelsesrådgiver

5.1: Ansættelsesforholdet

Alle medarbejdere har et medansvar for at opretholde det ønskede sikkerhedsniveau i Norddjurs Kommune. For at kunne leve op til medansvaret, er det den enkelte afdelingsleders ansvar at sørge for procedurer i forhold til anvendelse af systemer, og håndtering af informationer, i det daglige arbejde, samt i forhold til den ønskede adfærd for informationssikkerhed. Alle medarbejdere skal:

- Have et generelt kendskab til informationssikkerhed og databeskyttelse
- Kende deres ansvar og rolle i sikkerhedsarbejdet
- Passe på Norddjurs Kommunes systemer og informationer
- Deltage aktivt i rettelse af fejl, løsning af problemer og forbedringer af sikkerheden
- Rapportere sikkerhedshændelser og persondatabrud internt

Der udarbejdes detaljerede retningslinjer for ønsket brugeradfærd på udvalgte områder som fx e-mail, billeder, password, og rapportering af sikkerhedshændelser. Retningslinjer for brugeradfærd godkendes af informationssikkerhedsudvalget. For at minimere vurderede risici, skal retningslinjerne jævnligt revideres og opdateres.

Overtrædelser af informationssikkerhedspolitikken eller retningslinjerne vil efter omstændighederne kunne medføre disciplinære sanktioner, herunder ansættelsesretlige konsekvenser.

5.2: Funktionsadskillelse

Norddjurs Kommune har etableret funktionsadskillelse, således ansatte og eksterne partnere bliver begrænset i at lave fejl, uheld eller bevidst negative handlinger. I de tilfælde, hvor det ikke er muligt at etablere funktionsadskillelse, er der iværksat kompenserende sikkerhedsforanstaltninger. Der foreligger retningslinjer for roller og rettigheder for relevante systemer.

5.3: Uafhængighed af nøglepersoner

Det tilstræbes, at Norddjurs Kommune ikke bliver afhængig af særviden, som kun enkelte ansatte besidder. Derfor foretages videndeling og etablering af personbackup, hvor det er muligt. Hvor videndeling ikke er muligt, skal der kompenseres med andre foranstaltninger, fx detaljeret dokumentation for arbejdsgange.

5.4: Sikkerhedsprocedurer før ansættelse

Der skal være procedurer, hvor det er relevant jævnfør lovgivning, som sikrer potentielle medarbejdere, er kompetente og sikkerhedsmæssigt egnede til at varetage deres stilling.

Der skal foreligge ansættelseskontrakter for alle medarbejdere, hvori deres ansvar for informationssikkerhed bl.a. indgår, herunder eventuelle tavshedserklæringer.

5.5: Ansættelsens ophør
Der skal foreligge procedurer for ansættelsens ophør, der sikrer returnering af IT-udstyr, og begrænser adgang og rettigheder rettidigt.

6. Fysisk sikkerhed
Adgang til alle fysiske lokaliteter sikres imod uvedkommende.

6.1: Sikre områder
Lokaler er opdelt i sikkerhedsområder, hvor det er relevant. Lokaler, hvori der opbevares fortrolige og følsomme informationer skal være aflåst, når ingen ansatte er til stede. Serverrummene, hvor informationer er lagret elektronisk, skal være videoovervågede, og optagelserne opbevares i op til 30 dage.

6.2: Fysisk adgangskontrol
Adgang til lokationer, hvor borgere ikke bør tilgå, tildeles på baggrund af autorisationer, og beskyttes med hensigtsmæssige adgangskontroller.

6.3: Beskyttelse af udstyr
IT-systemer og fysiske systemer beskyttes imod ødelæggelse og skade, der følger af brand, vandskade, strømsvigt og andre skader, som udspringer af hændelser i det omkringliggende miljø.

Systemer der er vurderede kritiske skal overvåges og vedligeholdes. Såfremt systemet er leveret af en ekstern part, skal leverandørens anvisninger følges.

Der skal foreligge procedurer ved bortskaffelse, reparation eller vedligeholdelse af alle kritiske systemer.

Der skal desuden foreligge generelle procedurer for bortskaffelse, reparation eller genbrug af it-udstyr, således udstyrets informationer beskyttes eller renses.

7. Styring af netværk og drift
Driftsforstyrrelser skal imødegås gennem:

- Forebyggende foranstaltninger såsom kvalitetssikring, ændringshåndtering og dokumentvedligeholdelse.
- Problemhåndtering, der sikrer skadeudbedring, og som sikrer, at omgåelse, opkobling eller tilsvarende ikke er muligt.

Sikkerhedshændelser rapporteres til informationssikkerhedskoordinatoren, ligesom planlagte og dokumenterede forbedringstiltag.

Informationssikkerhedskoordinatoren rapporterer graverende sikkerhedshændelser til formanden for informationssikkerhedsudvalget.

Kommunen har etableret procedurer for daglig sikkerhedskopiering (backup), for at imødegå driftsforstyrrelser. Backup opbevares på anden fysisk lokation med rette sikkerhedsforanstaltninger og kontrol heraf.

IT-risikovurderingen dokumenterer, at det er vigtigt for organisationen, at IT-systemerne rummer korrekte og pålidelige data, og at systemerne er tilgængelige, når dette er nødvendigt – eller i det mindste inden for korte-

re tid. Det stiller krav til IT-afdelingen om tilstrækkelige backup-procedurer og godkendte SLA'er (Service Level Agreements).

Der foreligger procedurer for vurdering af leverandører, når disse er underlagt krav, og leverer drift eller udvikling til Norddjurs Kommune. De overordnede krav i dette afsnit anvendes til at stille krav overfor leverandørerne, som skal overholde Norddjurs Kommunes informationssikkerhedspolitik og -retningslinjer.

7.1: Operationelle procedurer og ansvarsområder

For at sikre stabiliteten i driften er der etableret funktionsadskillelse, således test og produktion holdes adskilt på forskellige segmenter. Nye systemer og ændringer til eksisterende systemer testes inden installering i driftsmiljøet, således tilgængelighed og integritet sikres. Procedurer, ansvarsområder og anvendt teknologi skal understøtte den nødvendige funktionsadskillelse.

7.2: Eksterne serviceleverandører

Der foreligger procedurer til overvågning af eksterne serviceleverandører, for at sikre de aftalte kontroller varetages hensigtsmæssigt.

7.3: Styring af driftsmiljøet

Der er procedurer, der sikrer stabilitet ved installation af systemer i driftsmiljøer. Der anvendes standardopsætninger for konfiguration af systemkomponenter, som kontrollerer kendte sårbarheder.

IT-afdelingen skal løbende vurdere tilgængelige sikkerhedsrettelser, fx "patches" og "hotfixes" til anvendte operativsystemer. Sikkerhedsrettelser installeres efter behov.

Data, der anvendes til test, skal udvælges omhyggeligt, kontrolleres nøje og beskyttes i henhold til deres klassifikation. Der er særligt fokus på beskyttelse af persondata.

Kapaciteten i forbindelse med alle servere med kritiske informationer skal løbende overvåges for at sikre pålidelig drift og tilgængelighed.

Ved implementering af nye systemer skal det sikres, at der er mulighed for reetablering og fornøden fejlhåndtering.

7.4: Skadevoldende programmer (vira, orme, spy- og malware)

Skadevoldende programmel kan have kritiske konsekvenser for Norddjurs Kommune. Derfor skal Norddjurs Kommunes IT-udstyr, der er tilsluttet kommunens netværk, hvor det er muligt have installeret antivirusprogrammel. Dette er også gældende eksterne brugere af netværket. Antivirusprogrammelets version skal overvåges, således Norddjurs Kommune anvender nyeste opdatering.

Det kontrolleres løbende, at anti-virus er aktivt på Norddjurs Kommunes arbejdsstationer. Arbejdsstationer, som ikke har det gældende antivirusprogrammel, må ikke tilgå netværket, før det opdateres. Opdateringen skal ske automatisk uden input fra brugerne. En opdatering kan medføre kort brud på tilgængelighed.

Det er ikke tilladt at installere egne programmer på Norddjurs Kommunes IT-udstyr, heller ikke at tilkoble uidentificerede datamedier (fx USB pind) til kommunens netværk. Der foreligger en procedure for begrænsning af programmer på kommunens IT-udstyr.

7.5: Sikkerhedskopiering

Der skal forekomme sikkerhedskopiering med faste intervaller, således kommunens informationer ikke går tabt. Reglerne herom skal findes i retningslinjen for backup. Eksterne leverandører skal efterleve samme kriterier.

Sikkerhedskopierne skal testes regelmæssigt, for at sikre, at disse kan indlæses. Sikkerhedskopierne skal opbevares på anden fysisk lokation end produktionsdata, så de kan fremfindes ved beredskabssituationer.

7.6: Netværkssikkerhed

Norddjurs Kommunes netværk skal sikres imod uautoriseret adgang. IT-afdelingen styrer sikringen. Sikringen kan fx bestå af adgangskontrol eller adskillelse af netværkstjenester.

Der er etableret firewall-løsninger, der beskytter mod forbindelse til upålidelige netværk.

Der etableres udelukkende forbindelser fra internettet til sikkerhedsgodkendte servere, som fx e-mail og webservere.

Det skal sikres, at IT-afdelingen altid har de fornødne kompetencer og redskaber til overvågning af Norddjurs Kommune for at kunne opdage og spore sikkerhedsbrister og fejlrette. Netværket skal overvåges løbende, for at opdage og udbedre brud på sikkerheden. Bærbare medier med adgang til netværket skal styres og beskyttes.

7.6.1: Trådløse netværk

Alle Norddjurs Kommunes fysiske lokationer har etableret trådløst netværk, som kun kan tilgås med autoriseret adgang. IT-afdelingen skal godkende trådløse netværks lokationer. Trådløse netværk betragtes som usikre, ubeskyttede netværk, og kræver gyldige legitimationsoplysninger og godkendt udstyr for adgang.

Gæster, hvis identitet er kendt, kan få udleveret kodeord til et gæstenetværk, og derigennem tilslutte eget udstyr, såfremt udstyret ikke har generende indflydelse på kommunens andre systemer. Gæstenetværket må aldrig give direkte adgang til Norddjurs Kommunes systemer.

Der foretages overvågning og logning af gæsters anvendelse af internettet i henhold til EU-reglerne om terrorbekæmpelse og fejlsøgning.

7.7: Informationsudveksling

Der skal foreligge retningslinjer for informationsudveksling af fortrolig og følsom information via e-mail eller andre elektroniske medier.

Ved ekstern opkobling til Norddjurs Kommunes systemer og netværk må fortrolige og følsomme oplysninger ikke kunne kopieres, flyttes eller lagres på bærbare medier.

Alle Norddjurs Kommunes ansatte har ansvar for at beskytte IT-udstyr og bærbare datamedier.

7.8: Logning og overvågning

IT-afdelingen står for logning af vores kritiske systemer. Overvågning og opfølgning sker via advarsler fra et Intrusion Detection System og Intrusion Prevention System. Logningerne kontrolleres med henblik på at opdage og spore uautoriserede handlinger, og at kunne føre disse tilbage til enkeltpersoner eller identificerbart netværksudstyr.

Det kontrolleres, at IT-systemer anvendes korrekt. Overvågningsniveauet fastlægges på grundlag af en risikovurdering af det enkelte system, og alle overvågningsaktiviteter skal beskrives. Alle aktiviteter på de fleste IT-systemer registreres automatisk.

Sikkerhedsrelaterede hændelser i loggen skal registreres.

Logfaciliteter og logoplysningers integritet skal beskyttes.

Alle ure synkroniseres, så hændelser kan identificeres entydigt.

8. Adgangsstyring

8.1: De forretningsmæssige krav til adgangsstyring

Alle informationsaktiver skal, i et specificeret omfang, være beskyttet imod uautoriseret adgang.

Udover den fysiske adgangskontrol skal der anvendes adgangskontrolsystemer på IT-systemer. Disse adgangskontrolsystemer skal kunne overvåge, alarmere og logge i nødvendigt omfang, således der også efterfølgende kan føres kontrol og evaluering.

Der skal mindst en gang hver 6. måned tages stilling til adgangsforhold, både til fysiske lokationer og IT-systemer. Der skal desuden foreligge procedurer for adgangsstyring af fysiske lokationer og informationsaktiver.

8.2: Administration af brugeradgang

Tildeling, ændring og sletning af brugeradgang til systemer og informationer sker ud fra arbejdsbetingede behov i overensstemmelse med informationernes klassifikation. Fysiske adgange og brugerrettigheder til netværk og systemer inddrages, når brugeren ikke længere skal have adgang.

Adgangsprocedurerne omfatter:

- Regler for udpegelse af autorisationsansvarlige
- Regler for, hvordan rettigheder tildeles ansatte, eksterne konsulenter eller elever og praktikanter
- Regler for, hvordan rettigheder ændres eller inddrages
- Regler for overvågning og logning, kontrol og opfølgning

Anvendelse af fællesbrugere er ikke tilladt.

8.3: Brugerens ansvar

Alle Norddjurs Kommunes ansatte, er ansvarlige for efterlevelsen af kommunens adgangspolitikker, herunder følger kommunens retningslinjer for password.

Retningslinjerne for password er:

- Passwordet skal være minimum 8 tegn
- Passwordet skal indeholde store og små bogstaver
- Passwordet skal indeholde både bogstaver og tal
- Passwordet bør ikke være ord, en sætning eller nemme at gætte (fx fødselsdato, familiemedlems navn eller hobby)
- Koden skal ændres minimum hver tredje måned

8.4: Styring af netværksadgang, systemadgang og adgang til brugersystemer og informationer

Styringen af brugeradgange til netværk, systemer mm. sikrer, at alle brugere og alt netværksudstyr er identificeret, og at der er opdaterede fortegnelser heraf. Der er sikringsforanstaltninger, så adgangskontroller til systemer og data ikke kan omgås.

Der er implementeret timeout i forbindelse med brugeradgange til systemer og netværk i forhold til sikkerhedsniveauet for det enkelte system, netværk mm.

8.5: Mobilt udstyr og fjernarbejdspladser

Alt Norddjurs Kommunes IT-udstyr og alle IT-systemer er dækket af informationssikkerhedspolitikken, uafhængigt af arbejdspladsens lokation.

Der foreligger regler for medarbejderes brug af mobilt udstyr og hjemmearbejdspladser, som udleveres ved nyansættelse.

9. Anskaffelse, udvikling og vedligeholdelse af IT-systemer

9.1: Sikkerhedskrav til informationsbehandlingssystemer

Ved indkøb eller test af eksternt udviklede systemer skal risikovurderingen indgå i vurderingen. Systemet skal have implementeret de sikkerhedsforanstaltninger, der er tilstrækkelige i forhold til kommunens informations- eller IT- klassifikation.

9.2: Korrekt informationsbehandling

Vurderingen af, hvilke sikkerhedsforanstaltninger der er nødvendige for det enkelte system, skal foretages ud fra systemets informationers værdi for kommunen og de registrerede. Som en del af sikringen af informationerne tages der stilling til behovet for ind- og uddatavalidering.

9.3: Kryptering

Behovet for kryptering af informationer skal vurderes, for at imødegå den rette fortrolighed og integritet af informationerne. Denne vurdering skal tage udgangspunkt i klassifikationen i afsnit 4.

For at efterleve databeskyttelsesforordningen og anden lov, bør behandling af persondata som vurderes fortrolige eller følsomme altid krypteres.

Ved anvendelse af kryptering skal der tages højde for nøglehåndtering.

9.4: Styring af driftsmiljøet

Der foreligger procedurer, der sikrer stabilitet ved installation af systemer i driftsmiljøet.

Informationer, der anvendes til test, skal udvælges omhyggeligt, kontrolleres nøje og beskyttes i henhold til deres værdi for kommunen og de registrerede.

Norddjurs Kommune besidder kildekode til webudvikling. Kildekoden skal opbevares fortroligt.

9.5: Sikkerhed i udviklings- og hjælpeprocesser

Vi udvikler som udgangspunkt ikke selv systemer, men anvender pålidelige og kompetente leverandører. Der anvendes standardprodukter i videst muligt omfang. Der er en retningslinje for styring af leverandører.

IT-afdelingen etablerer godkendelsesprocedurer for nye systemer, nye versioner og opdateringer af eksisterende systemer. Godkendelsesprocedurerne beskriver krav til dokumentation, specifikationer, test, kvalitetskontrol og en styret implementeringsproces. Der skal foretages en risikovurdering af ændringerne i forhold til eksisterende sikringsforanstaltninger og eventuelt opståede behov for nye sikringsforanstaltninger.

Vedligeholdelse af systemer finder sted en gang om måneden, og i det omfang der er behov for, ved hjælp af servicevinduer, som forekommer på tidspunkter, hvor det vil give mindst mulige gener for de ansatte.

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

9.6: Sårbarhedshåndtering

Der skal løbende indhentes informationer om sårbarheder i de anvendte systemer. Der foretages eksterne sårbarhedstest hver måned, mens der foretages driftsmæssige sårbarhedsskanninger døgnet rundt. Sårbarhederne skal evalueres, og passende foranstaltninger implementeres.

10. Styring af sikkerhedshændelser og -brud

10.1: Rapportering og registrering af sikkerhedshændelser og -brud

Informationssikkerhedsarbejdet bygger bl.a. på de sikkerhedshændelser og -brud der forekommer i Norddjurs Kommune. For at vide, hvor der skal indsættes yderligere foranstaltninger, kræver det registrering og opfølgning på de sikkerhedshændelser og -brud der sker.

Alle Norddjurs Kommunes ansatte har derfor pligt til at indberette sikkerhedshændelser og -brud, så de kan blive registreret og vurderet centralt. Der skal desuden foreligge en procedure for indberetning af sikkerhedshændelser og -brud.

Alle sikkerhedshændelser gennemgås på informationssikkerhedsudvalgsmøderne. Graverende sikkerhedshændelser rapporteres til direktionen uden unødig forsinkelse.

10.2: Håndtering og forbedring af sikkerhedshændelser og -brud

Målet og ansvaret for håndtering af sikkerhedsbrud er fastlagt af Norddjurs Kommunes direktion.

Sikkerhedshændelser og -brud, der efter klassifikationen i afsnit 4 kan klassificeres som 2, 3 eller 4 skal altid logges og kunne spores tilbage til kilden.

Hændelser skal håndteres og korrigeres med udgangspunkt i en konkret vurdering af alvoren. Nærmeste leder skal involveres straks, såfremt bruddet vurderes alvorligt.

Hændelser, der har indflydelse på tilgængelighed, skal afklares i overensstemmelse med gældende driftsaftaler. Driftshændelser, der ikke kan afklares inden for aftalt tid, skal håndteres i overensstemmelse med procedurer for hændelseshåndtering, og de ramte brugere og systemejere informeres. Informationen skal altid bestå af en beskrivelse af problemet, hvad er der sket og hvorfor, samt et skøn af tidsrum for udbedring.

Alvorlige hændelser skal efterfølgende analyseres med henblik på forbedring af Norddjurs Kommunes informationssikkerhed.

Norddjurs Kommune skal desuden sikre, at der indsamles, opbevares og præsenteres fyldestgørende og troværdige beviser, hvor der kan komme retsligt efterspil.

11. IT-beredskabsstyring

Norddjurs Kommune har udarbejdet en IT-beredskabsplan, der detaljerer håndtering af beredskabssituationer. Formålet med planen er at begrænse skade og tab af informationer, forårsaget af katastrofer eller sikkerheds-brister.

IT-beredskabsplanen indgår i Norddjurs Kommunes overordnede kriseberedskab.

Norddjurs Kommunes udarbejdelse af IT-beredskabsplanen baserer sig på risikovurderinger af kommunens mest kritiske informations- og IT-aktiver. Disse vurderinger stiller desuden skærpede krav til leverandører, personale, drift, anlæg og øvrige faciliteter.

Beredskabsplanerne skal bestå af:

- Skadesbegrænsende tiltag
- Etablering af midlertidig nødløsning
- Genetablering af permanent løsning

Beredskabsplanerne skal løbende afprøves og opdateres, således de er tidssvarende og effektive.

Afprøvningen skal ske med et årligt interval som skrivebordstest, og hvert tredje år som fuld test.

Sikkerhedskopier af beredskabsplanen og reserveudstyr, skal altid opbevares ved sekundær lokation.

12. Overensstemmelse med lovbestemte krav

Norddjurs Kommune bestræber sig på, at informationssikkerhedspolitikken og retningslinjer altid overholder gældende lovkrav inden for kommunens myndighedsudøvelse. Kommunen agerer under mange forskellige lovgivninger, og dette kræver konkrete vurderinger fra kommunens ledelse og ansatte, når der udarbejdes retningslinjer, procedurer og disse efterfølgende eksekveres.

Den fornødne juridiske ekspertise skal være til rådighed for at overholde disse krav.