NORDJYLLANDS BEREDSKAB

Nordjyllands Beredskabs

INFORMATIONSSIKKERHEDSPOLITIK

(Senest opdateret den 30/8 - 2020)

INDHOLDSFORTEGNELSE

1. Baggrund og formålet med informationssikkerhedspolitikken

På foranledning af ikrafttrædelsen af EU-Databeskyttelsesforordningen ("GDPR") er det besluttet at der skal indføres et informationssikkerhedssystem.

Formålet med denne informationssikkerhedspolitik er at dokumentere, hvordan Nordjyllands Beredskab har etableret, implementeret og løbende vil vedligeholde sit informationssikkerhedssystem med henblik på at sikre fortrolighed, integritet og tilgængelighed af den information, som Nordjyllands Beredskab besidder. Det er ligeledes vigtigt for Nordjyllands Beredskab løbende at vurdere og håndtere informationssikkerhedsrisici.

Informationssikkerhedspolitikken fastlægger rammerne for de sikkerhedstiltag, som er nødvendige at følge, når vi som en organisation skal leve op til lovgivningskrav og Best Practices. Informationssikkerhedspolitikken skal være med til at sikre, at de data og informationer, som behandles (herunder registrerer, analyserer, videresender, arkiverer, sletter mv.) bliver behandlet korrekt og i overensstemmelse med gældende regler og fremstår med et korrekt indhold, uanset om behandlingen sker internt eller eksternt ved samarbejdspartnere, offentlige myndigheder m.fl.

Et højt sikkerhedsniveau er et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement, hvor Nordjyllands Beredskab kan tilbyde en sikker service over for samarbejdspartnere, myndigheder og private kunder.

Med informationssikkerhed forstås den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til behandlingen og kommunikation af både fysisk og elektronisk data, herunder også teknologi og organisatoriske processer.

Denne informationssikkerhedspolitik er tilgængelig for enhver person eller virksomhed, som i henhold til politikken forventes at forholde sig på en bestemt måde, det være sig en aktiv handling eller en bevidst undladelse.

2. Målsætninger med informationssikkerhedspolitikken

Informationssikkerheden skal understøtte og sikre stabilitet i adgangen til data, fortrolighed samt pålidelighed i forhold til de pågældende datas indhold.

Målsætningen er at have en høj grad af informationssikkerhed med henblik på at sikre driften mod unødig forstyrrelse, f.eks. i form af angreb på IT-systemer, samt sanktioner såsom bøder og erstatningskrav.

Målsætningen skal desuden sikre en høj grad af tillid til Nordjyllands Beredskab, sikre at den nødvendige information er tilgængelig for de relevante medarbejdere, kunder, samarbejdspartnere mv. og endeligt at sikre, at gældende lovgivning overholdes, herunder persondatalovgivningen. Dette sikres ved, at leve op til almindeligt anerkendte principper for informationssikkerhed. Herved understøtter informationssikkerheden, at vi fortsat vil kunne leve op til omverdenens forventning om troværdighed og fortrolighed.

Formålet med informationssikkerheden er at:

- understøtte bevidstgørelsen blandt medarbejdere om kravene til informationssikkerhed og vigtigheden heraf,
- opnå høj driftssikkerhed og minimeret risiko for nedbrud og tab af data,
- opnå korrekt funktion af it-systemerne med minimeret risiko for manipulation af data/systemer og fejl i disse,
- opnå mulighed for fortrolig behandling, transmission og opbevaring af data, og
- sikre mod forsøg på tilsidesættelse af sikkerhedsforanstaltninger.

Der lægges vægt på, at informationssikkerhedsprocedurerne skal være afbalancerede: Generelt skal data og systemer derfor sikres ud fra en vurdering af, hvad der er nødvendigt at gøre under hensyntagen til de økonomiske rammer og behovet for brugervenlighed. Krav til informationssikkerheden skal vurderes i forhold til deres relevans, og hvor god sund fornuft er en afgørende faktor.

3. Omfanget af informationssikkerhedspolitikken

Informationssikkerhedspolitikken angiver de beslutninger der er truffet med henblik på nærmere at fastlægge det tilstrækkelige sikkerhedsniveau samt definere de krav, der skal stilles, for at sikkerhedsniveauet opretholdes.

Omfanget af informationssikkerhedspolitikken fastlægges derfor således:

- Informationssikkerhedspolitikken gælder for alle ansatte uanset ansættelsesform. (fastansatte, deltidsansatte og frivillige).
- Informationssikkerhedspolitikken gælder for alle systemer og alle data i Nordjyllands Beredskab besiddelse.
- Leverandører og samarbejdspartnere, som har fysisk adgang til organisationens systemer og data, skal ligeledes have kendskab til og følge informationssikkerhedspolitikken.
- Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af it-systemer og papirarkiver.
- Informationssikkerhedspolitikken godkendes af ledelsen og revideres ved behov og mindst en gang i hver kommunal valgperiode.

Der er udnævnt en informationssikkerhedsansvarlig (stabschefen) og denne har ansvaret for at gennemføre ovennævnte revision af informationssikkerheds-politikken.

4. Risikovurdering og risikoanalyse

Sikkerhedsniveauet er fastsat på baggrund af Nordjyllands Beredskabs vurdering af de risici (herunder i relation til fysisk sikkerhed og IT-sikkerhed), som Nordjyllands Beredskab med rimelighed forventes at kunne blive mødt af og som vi derfor ønsker at imødegå.

IT-risikovurderingen opdateres minimum en gang årligt og ellers ved eventuelle større ændringer i IT-systemerne, ændringer i anvendelse af systemerne eller ved større organisatoriske ændringer med efterfølgende tilretning af informationssikkerhedspolitikken, retningslinjer mv.

5. Særligt om behandling af personoplysninger

Henvisninger i det følgende til persondataforordningen skal læses som en henvisning til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

For at realisere ovenstående målsætning er det besluttet, at informationssikkerhedspolitikken skal sikre, at persondataforordningen 1) efterleves, 2) implementeres og 3) dokumenteres. For at sikre at informationssikkerhedspolitikken efterleves, skal denne integreres i alle områder. I overensstemmelse med artikel 5, stk. 2, i persondataforordningen om den dataansvarliges ansvar for at kunne påvise overholdelsen, sker integreringen desuden ved, at implementeringen dokumenteres.

Desuden sikres, at medarbejdere, eksterne samarbejdspartnere og kunder informeres om målsætningen i forhold til håndtering af persondata ved at offentliggøre politik om informationssikkerhed på hjemmesiden.

6. Organisering og ansvar

Ledelsen beslutter overordnede strategiske projekter af informationssikkerhedsmæssig karakter, men har i praksis delegeret det daglige ansvar for informationssikkerheden til stabschefen. Almindelige dagligdags problemstillinger af informationssikkerhedsmæssig karakter behandles i daglig drift

6.1 Styringsprincipper

Informationssikkerhed er et fælles anliggende for hele organisationen og vil blive ledet af stabschefen ifølge de regler og procedurer, der indgår i informationssikkerhedsstyringssystemet. Stabschefen vejleder ledelse og medarbejdere i informationssikkerhedsspørgsmål og koordinerer og følger op på informationssikkerhedsrelaterede aktiviteter.

6.2 Eksterne samarbejdspartnere

Der skal indgås skriftlige aftaler med eksterne samarbejdspartnere, som tager højde for de sikkerhedskrav, der er defineret i persondataforordningen. Der skal foretages en identifikation og vurdering af risici i forbindelse med brugen af de eksterne leverandører. Eksterne samarbejdspartnere, der har adgang til data, skal desuden efterleve samme retningslinjer, som gælder internt hos Nordjyllands Beredskab.

7. Fortegnelse over persondata

Med henblik på at sikre et tilstrækkeligt sikkerhedsniveau i forhold til beskyttelse af persondata, er der udarbejdet en fortegnelse over alle væsentlige behandlinger af persondata, som Nordjyllands Beredskab foretager. Denne fortegnelse udgør en central del af informationssikkerhedspolitikken.

8. Brugeradfærd

Det er en naturlig del af det daglige arbejde at håndtere IT og behandling af information. En korrekt håndtering heraf kræver, at alle ansatte er bekendt med informationssikkerhedspolitikken og herunder gældende retningslinjer for håndtering af personoplysninger. Det er ligeledes vigtigt, at såvel ledelse som medarbejdere tager ansvar for informationssikkerheden.

Hos Nordjyllands Beredskab gælder følgende overordnede princippet for behandling af data:

- Persondata behandles i alle tilfælde fortroligt.
- Der anvendes personlig login og password, og passwords 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.
- Al brug af internettet skal ske med omtanke, og der må ikke foretages besøg på sider med racistisk, uetisk eller pornografisk indhold i forbindelse med de daglige arbejdsopgaver.
- 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 Nordjyllands Beredskab.
- Hvis man oplever, at der sker brud på informationssikkerheden, skal man informere sin nærmeste leder og DPO.

8.1 Ansættelsesforholdet

Alle medarbejdere har et medansvar for at opretholde det ønskede sikkerhedsniveau i. Det er ledelsens ansvar at sørge for instruktion i forhold til anvendelse af systemer i det daglige arbejde samt i forhold til den ønskede adfærd for informationssikkerhed.

Alle medarbejdere skal:

- Have et generelt kendskab til informationssikkerhed.
- Kende deres ansvar for sikkerheden.
- Sikre deres personlige adgangskoder.
- Passe på organisationens IT-udstyr.
- Deltage aktivt i rettelse af fejl, løsning af problemer og forbedringer af sikkerheden.
- Rapportere hændelser, der kan indikere brud på sikkerheden.

Der er udarbejdet retningslinjer for ønsket brugeradfærd på udvalgte områder, herunder brug af e-mail og internet, passwords, rapportering af sikkerhedshændelser. Retningslinjerne vil jævnligt blive revurderet og opdateret, og det er derfor vigtigt, at alle medarbejdere orienterer sig, når der kommer meddelelse rundt om opdaterede retningslinjer. Overtrædelser af informationssikkerhedspolitikken og/eller de vedtagne retningslinjer vil efter omstændighederne kunne medføre ansættelsesretlig sanktioner.

8.2 Uafhængighed af nøglepersoner

Der tilstræbes uafhængighed af enkeltpersoner gennem videndeling og etablering af personbackup, hvor dette er muligt. Hvor videndeling ressourcemæssigt ikke er muligt, skal der etableres relevante kompenserende kontroller, der gør det muligt at udføre opgaverne og sikre den nødvendige dokumentation herfor.

8.3 Sikkerhedsprocedurer før ansættelse

Det skal sikres, at der foreligger ansættelseskontrakter på alle ansatte, og at der udleveres samtlige af de relevante politikker/retningslinjer til medarbejderne, herunder informationssikkerhedspolitikken. Samtlige medarbejdere er endvidere pålagt tavshedspligt.

Medarbejdere ved Nordjyllands Beredskab skal fremlægge en "ren" straffeattest inden ansættelse, og gælder for alle både faste- og deltidsansatte samt frivillige der har underskreven kontrakt med Nordjyllands Beredskab.

I forhold til børneattester vil denne blive indhentet for medarbejdere (faste- deltidsansatte samt frivillige), der i deres arbejde har kontakt med børn under 15 år. (se retningslinjer om straffe- og børneattester).

8.4 Ansættelsens ophør

Ved ansættelsesophør skal alle IT-aktiver returneres. En brugerkonto/e-mail deaktiveres den dato medarbejderen stopper. Mail videresendes IKKE.

9. Fysisk sikkerhed

Adgangen til alle fysiske lokaliteter er sikret mod uvedkommendes adgang via en nøgle/brikadgang. Adgang til lokationer tildeles på baggrund af autorisationer og beskyttes med et hensigtsmæssigt adgangskontrolsystem, udvalgt på baggrund af en risikovurdering.

9.1 Beskyttelse af udstyr

IT-udstyr beskyttes mod ødelæggelse og skade, der følger af brand, vandskade, strømsvigt og andre skader, som udspringer af hændelser i det omkringliggende miljø. IT-udstyr indeholdende fortrolige data overvåges og vedligeholdes efter leverandørens anvisninger. Ved bortskaffelse, reparation eller genbrug af IT-udstyr sikres det, at udstyret er forsvarligt renset for alle data. Når IT-udstyr bortskaffes eller på anden måde udskiftes, slettes alle data på en sådan måde, at de ikke kan genskabes.

9.2 Beskyttelse af fysiske dokumenter

Fysiske dokumenter, der rummer fortrolige oplysninger eller persondata skal behandles med omtanke. Efter endt arbejdsdag, skal disse dokumenter låses inde i et dokumentskab. Sådanne dokumenter må endvidere kun fjernes fra kontoret, såfremt der er et sagligt behov herfor og dokumenterne overlades til en betroet medarbejder. Såfremt dokumenterne fjernes fra kontoret påhviler det medarbejderen at sikre opbevaringen. Fysiske dokumenter må kun bortskaffes på arbejdspladsen.

10. Styring af netværk og drift

Driftsforstyrrelser imødegås gennem forebyggende foranstaltninger såsom kvalitetssikring, ændringshåndtering og dokumentationsvedligeholdelse. Det sikres endvidere, at omgåelse, opkobling eller tilsvarende ikke er muligt uden autorisation. Sikkerhedshændelser rapporteres altid til den IT-ansvarlige.

Der er etableret procedurer for daglig sikkerhedskopiering (backup). Backup opbevares eksternt på en anden geografisk og sikker lokation, hvor sikkerheden jævnligt kontrolleres. Der henvises til den indgåede databehandleraftale med Aalborg Kommune.

Der er etableret funktionsadskillelse for at sikre stabiliteten i driften, således at test og produktion holdes adskilt på forskellige segmenter. Nye systemer og ændringer til eksisterende systemer testes inden installering i driftsmiljøet, således at tilgængelighed og integritet sikres.

10.1 Skadevoldende programmer (vira, orme, spy- og malware)

Skadevoldende programmer kan sætte hele organisationen ud af drift, og det kan være meget dyrt at genoprette IT-systemer/data, hvis de er blevet ramt af et hackerangreb eller en virus. Alt godkendt IT-udstyr, som er tilsluttet Nordjyllands Beredskabs netværk, har - hvor det er muligt - installeret et aktivt og opdateret antivirusprogram, der kan opdage, rense og beskytte mod forskellige former for skadevoldende programmer. Det gælder også eksterne brugere, der tilsluttes netværket via fjernopkobling. Sikkerheden kontrolleres løbende af Nordjyllands Beredskabs IT-leverandør, og der følges løbende op på, om antivirusprogram-merne er opdaterede og tilstrækkelige.

Det er ikke tilladt at installere egne programmer på Nordjyllands Beredskabs maskiner.

Almindelige brugere kan ikke med deres login installere programmer, dette kan kun gøres af en pc administrator.

10.2 Netværkssikkerhed

Med henblik på at sikre mod uautoriseret adgang skal Nordjyllands Beredskabs netværk sikres. Sikring af netværk imod uautoriseret adgang styres af den eksterne IT-leverandør. Det sker f. eks. via adgangskontrol og adskillelse af netværkstjenester, hvor dette er hensigtsmæssigt. Der er desuden etableret firewall-løsninger, der beskytter mod forbindelse til upålidelige netværk. Der henvises til den indgåede databehandleraftale med Aalborg Kommune.

Der er etableret trådløst netværk på alle Nordjyllands Beredskabs lokationer. Supplerende trådløse lokalnet må kun etableres efter godkendelse fra IT-afdelingen. Nettet skal konfigureres således, at uautoriseret adgang og aflytning ikke er mulig. Trådløse netværk betragtes som usikre, ubeskyttede netværk, og adgang til trådløst netværk kræver gyldigt brugernavn og kodeord samt anvendelse af godkendt udstyr.

Gæster, hvis identitet er kendt, kan få udleveret kodeord til gæstenetværket og tilslutte eget udstyr til netværket, forudsat at udstyret ikke generer andre systemer. Netværket kan og må kun anvendes til internetadgang – direkte adgang til interne systemer er ikke tilladt fra gæstenetværket. Der foretages overvågning og logning af gæsters anvendelse af internettet i henhold til EU-reglerne om terrorbekæmpelse.

10.3 Logning og overvågning

Der sker logning af brugeradfærden/aktiviteter. Logningen gennemføres af og opbevares hos Nordjyllands Beredskabs eksterne IT-leverandør,

således at logfaciliteter og logoplysninger er beskyttet mod manipulation og tekniske fejl. Logningerne kontrolleres med henblik på at opdage og spore uautoriserede handlinger, og at kunne føre disse tilbage til enkeltpersoner eller identificerbart netværksudstyr.

Nordjyllands Beredskab fører desuden løbende kontrol med, at IT-systemer anvendes korrekt. Overvågningsniveauet fastlægges på grundlag af en risikovurdering af det enkelte system. Som en del af logningen skal sikkerhedsrelaterede hændelser registreres.

11. Adgangsstyring

11.1 Krav til adgangsstyring

Alle informationsaktiver (programmel, udstyr, data, informationer og databæren-de medier) er beskyttet mod uautoriseret adgang. Ud over den nødvendige adgangskontrol til bygninger og lokaler, anvendes der elektroniske/-programmel-baserede adgangskontrolsystemer. Disse kan i væsentlig omfang - ud over adgangskontrol - danne grundlag for efterfølgende kontrol via logning.

Der skal løbende tages stilling til adgangsforhold til bygningerne og IT-systemerne, og der er under punkt 12.3 udarbejdet procedurer for tildeling af adgang til bygningernes lokaler med arbejdsstationer, arkiver, netværk og lignende ressourcer.

11.2 Autorisationer/adgange til IT-systemer

Der gives alene adgang til IT-systemer for medarbejdere, som direkte er autoriserede hertil. Dette indebærer, at der kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte

brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Ved vurderingen af, hvilke medarbejdere der skal autoriseres, lægges der vægt på, hvad den enkelte bruger har behov for at være autoriseret til. For brugere, som ikke længere har behov for de autorisationer, de har fået udstedt, inddrages autorisationerne. Det gælder f.eks. medarbejdere, som skifter arbejdsområde.

De tildelte rettigheder/autorisationer administreres af IT-afdelingen ud fra indmeldinger fra chef/ledere. Styringen af brugeradgange til netværk, systemer mv. sikrer, at alle brugere og alt netværksudstyr er identificeret, og at der er opdaterede fortegnelser herover.

Løbende foretages en gennemgang og vurdering af relevansen af de tildelte rettigheder/autorisationer. Dette indebærer bl.a., at der konkret tages stilling til, hvorvidt en bruger kun skal kunne foretage forespørgsler, eller om brugeren også skal kunne inddatere oplysninger, samt om brugeren skal kunne slette oplysninger. Hvis der er brugere, som alene autoriseres til enkelte af de nævnte funktioner, er systemerne teknisk indrettet således, at brugerne kun gives mulighed for adgang til oplysningerne i overensstemmelse med de givne autorisationer.

11.3 Administration af brugeradgang

Adgangsprocedurerne omfatter:

- Registrering af alle brugere med en unik brugeridentitet.
- Regler for, hvem der må disponere over hvilke IT-aktiver.
- Regler for, hvordan og i hvilke tilfælde adgangstilladelse tildeles og inddrages.
- Regler for sikkerhedsovervågning, logning, efterkontrol, ledelsesrapportering og opfølgning.

Anvendelsen af fællesadgang/systembruger skal kun ske i de tilfælde, hvor det ikke kan undgås.

11.4 Brug af passwords

Alle brugere bliver udstyret med passwords, og det er brugerens ansvar, at disse omgås hensigtsmæssigt. Passwordet må således ikke opbevares på skrift, så andre kan få adgang til det. I det tilfælde, at brugeren selv danner et password, skal nedenstående regler følges.

Alle medarbejdere skal behandle sit password efter følgende regler:

- Passwordet skal have en længde på mindst 8 tegn.
- Passwordet skal skiftes minimum hver 3. måned og gennemtvinges automatisk.
- Passwordet skal udformes, så det er komplekst og svært at bryde, og det skal bestå af en kombination af små bogstaver, store bogstaver og tal.

Følgende må ikke anvendes, når en medarbejder opretter et password:

- Bruge brugernavnet eller dele heraf
- Bruge eget navn eller dele heraf
- Anvende numre der kan identificeres med dig (f.eks. fødselsdag)
- Anvende logiske tastekombinationer (fx "qwerty" eller "asdfgh")

Hvis der indtastes forkert password 3 gange, låses brugerkontoen i 15 minutter, ved efterfølgende mislykkede forsøg låses kontoen, og der skal tages kontakt til IT-afdelingen for at få den åbnet igen. Hvis en medarbejder frygter, at dennes password er blevet afluret, skal vedkommende straks kontakte IT-afdelingen og samtidig ændre sit password.

Et password er personligt og må ikke overdrages til andre - heller ikke i forbindelse med ferie. Medarbejderne må endvidere ikke bruge det password, som anvendes til diverse systemer eller til private tjenester.

12. Retningslinjer til alle medarbejdere

12.1 Brug af e-mail

Den tildelte e-mailkonto er at betragte som en formel kommunikationskanal mellem medarbejdere og kunder/samarbejdspartnere eller andre - helt på linje med fysiske breve.

Alle e-mails betragtes som Nordjyllands Beredskab ejendom.

Sendte og modtagne e-mails, der er sagsrelaterede, skal journaliseres i og slettes i Outlook. Se instruks om håndtering af mails

Medarbejdere må anvende mailsystemet til personligt brug i begrænset omfang, hvis dette ikke har indflydelse på drift og sikkerhed i øvrigt. Der opfordres til, at man lægger private e-mails i en undermappe til indbakken, som man kalder "Privat".

Nordjyllands Beredskab forbeholder sig ret til at skaffe sig adgang til data og e-mail for medarbejdere, hvis dette sker af drifts- og sikkerhedshensyn.

Modtages eller sendes private meddelelser, skal man være opmærksom på, at de kan optræde i logfiler, forbrugsoversigter og backupfiler.

Alle mails scannes for kendte spam, vira og ransomware hos eksternt sikkerhedsfirma, inden de leveres til Nordjyllands Beredskab. Dette er dog ikke nogen garanti for, at der ikke passerer uønskede mails igennem sikkerheds-systemet.

Den enkelte medarbejder skal derfor selv være meget opmærksom på, hvad der åbnes/klikkes på.

Uanset at der udfører scanning af alle e-mails, skal medarbejdere være opmærksomme på begreberne "phishing" og "social engineering". Det vil sige, at nogen udefra med onde hensigter kan aflure fortrolige informationer uden at blive opdaget.

Denne form for bedrageri kan f.eks. udføres via e-mail, telefon og /eller *messenger* programmer. F.eks. kan man modtage tilsyneladende oprigtige e-mails, der forsøger at franarre personlige eller fortrolige oplysninger eller forsøger at få medarbejderen til at foretage uønskede handlinger.

12.2 Brug af Internet

Det er udelukkende godkendte personer der kan uploade via sociale medier, som f.eks. Facebook og LinkedIn.

Sikkerheden i Internet Explorer og andre browsere opsættes centralt og medarbejderne må/kan ikke ændre denne opsætning. Medarbejdere må ikke downloade og installere programmer lokalt på PC, medmindre dette sker efter aftale med IT-afdelingen.

Arbejdsrelaterede oplysninger må kun gemmes i Nordjyllands Beredskabs systemer.

12.3 Brug af PC

Alle administrative medarbejdere får stillet en stationær pc til rådighed. Pc´en må som udgangspunkt kun anvendes i arbejdsregi, og derfor skal privat brug begrænses mest muligt. Hvis en medarbejder gemmer private data på pc´en, er Nordjyllands Beredskab ikke ansvarlig i tilfælde af sletning. Nordjyllands Beredskab kan ikke tage hensyn til private data.

Adgangskodebeskyttet skærmlås skal aktiveres på pc-arbejdsplads, når denne forlades. Pc´en skal desuden slukkes, eller der skal logges ud hver dag, når man forlader arbejdspladsen.

Filer/data må ikke lagres pc'ens harddisk.

12.4 Tablets og mobiltelefon

Som standard er der adgangskode på disse enheder. Medarbejderen kan ikke slå det fra. Nogle mobile enheder understøtter Touch ID, hvilket kan benyttes i stedet for adgangskode. Ved 5 forkerte forsøg med adgangskode nulstilles enheden, og alle data er væk.

Der foretages som udgangspunkt ikke backup af mobile enheder. Medarbejderen er selv ansvarlig for at foretage backup. Der må ikke opbevares følsomme personoplysninger i form af oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, helbredsmæssige og seksuelle forhold eller strafbare forhold på tablet'en eller mobiltelefonen. Det er endvidere kun medarbejderens personlige data, der må uploades til skyen (såsom iCloud).

12.5 Brug af USB-nøgler mm.

Følsomme personoplysninger må ikke lagres på en USB-nøgle eller lignende bærbart medie.

Alle bærbare datamedier, som indeholder personoplysninger, skal uden for arbejdstid opbevares i et aflåst skab/lokale. Det relevante personale har fået udlevet nøgler hertil. Det samme gælder inden for arbejdstiden, hvis det nævnte udstyr ikke er under opsyn.

12.6 Hjemmearbejde

Ved arbejde hjemme finder anvendelsen af personoplysninger sted i et andet miljø. Medarbejderen er derfor forpligtet til altid at benytte en sikret internetlinje og sørge for, at denne ikke udfører arbejdet, hvor der er risiko for, at uvedkommende kan få adgang. I forbindelse med den eksterne opkobling, må der ikke kopieres, flyttes eller lagres følsomme personoplysninger (oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, helbredsmæssige og seksuelle eller strafbare forhold) eller andre fortrolige oplysninger.

Hjemmearbejde sker kun efter accept fra nærmeste leder og skal sikre at medarbejderen er bekendt med Informationssikkerhedspolitikken.

De øvrige punkter i nærværende persondatapolitik gælder også ved behandling af personoplysninger og brug af IT-systemer i forbindelse med hjemmearbejde.

12.7 Printning

Nordjyllands Beredskab har indført skyprint, hvilket betyder at der ikke sker tilfældig udprintning af materiale med personoplysninger.

13. Brug af databehandlere

Når der benyttes en ekstern databehandler til behandling af personoplysninger, er der indgået en forudgående skriftlig databehandleraftale, som har til formål at sikre, at persondatalovgivningens regler overholdes. Der følges løbende op på, at aftalen med eksterne serviceleverandører overholdes, og at den eksterne serviceleverandør varetager kontroller på en hensigtsmæssig måde.

14. Sikring af de registreredes rettigheder

Det skal sikre, at de registrerede ved, at der foretages behandling af vedkommendes personoplysninger. Som følge heraf er der indført procedurer for, at medarbejdere modtager oplysninger herom ved ansættelse.

15. Anskaffelse, udvikling og vedligeholdelse af IT-systemer

15.1 Sikkerhedskrav til informationsbehandlingssystemer

Ved indkøb og fornyelse af IT-systemer vurderer Nordjyllands Beredskab, om de stillede sikkerhedskrav er opfyldt. Vurderingen af, hvilke sikringsforanstaltninger der er nødvendige i det enkelte system, foretages ud fra, hvilke data systemet indeholder, og hvilke forretningsmæssige funktioner systemet varetager.

15.2 Kryptering

Ved vurderingen af, om der er behov for kryptering af informationer, skal der tages højde for, om kryptering som sikringsforanstaltning kan imødegå behovet for fortrolighed. For at leve op til persondataforordningen, bør al kommunikation indeholdende følsomme personoplysninger eller større mængder af personoplysninger med identitetsangivelse, der kan misbruges, ske i krypteret form.

Alle bærbare pc'er har krypteret harddisk.

15.3 Sikkerhed i udviklings- og hjælpeprocesser

Nordjyllands Beredskab udvikler ikke selv alle systemer, men anvender pålidelige og kompetente leverandører. Der anvendes standardprodukter i videst muligt omfang. IT-afdelingen etablerer sammen med den eksterne leverandør godkendelsesprocedurer for nye systemer, nye versioner og opdateringer af eksisterende systemer. 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.

Når der indføres nye IT-systemer, foretages der en risikovurdering af ændringerne i forhold til eksisterende sikringsforanstaltninger og eventuelt opståede behov for nye sikringsforanstaltninger. Vedligeholdelse af systemer finder sted en gang hvert kvartal, ved hjælp af servicevinduer uden for almindelig arbejdstid.

16. Styring af sikkerhedshændelser på IT-området

16.1 Rapportering af sikkerhedshændelser og svagheder

En væsentlig faktor i informationssikkerhedsarbejdet består i at reagere på hændelser af sikkerhedsmæssig karakter. Derfor skal sikkerhedsmæssige hændelser rapporteres, og der skal ske opfølgning herpå. Alle medarbejdere har pligt til at rapportere sikkerhedshændelser til IT, så sikkerhedshændelserne kan imødegås, inden de udvikler sig.

Målet og ansvaret for håndtering af sikkerhedsbrud er fastlagt af ledelsen. Sikkerhedshændelser, fejlhændelser og brugeraktiviteter i strid med denne informationssikkerhedspolitik skal så vidt muligt logges, således at der kan være mulighed for at spore uønskede hændelser. Hvis Nordjyllands Beredskab bliver angrebet af vira, ransomware eller anden trussel, har virksomheden ret til at gennemgå den enkelte medarbejders logfiler med henblik på at finde årsagen til angrebet.

Alle sikkerhedsbrud skal analyseres med henblik på løbende forbedringer i informationssikkerheden. I tilfælde af væsentlige sikkerhedsbrud, holdes der opfølgende møder med henblik på at vurdere behovet for eksempelvis ændringer i arbejdsgange/procedurer eller sikkerhedsforhold. Hvis der er risici for et retsligt efterspil, skal beviser indsamles og gemmes som bevismateriale.

Nordjyllands Beredskab sender jævnligt advarsler ud til medarbejderne om eventuelle trusler.

17. IT-beredskabsstyring

Nordjyllands Beredskab har udarbejdet en IT-beredskabsplan med en praktisk strategi for, hvordan man organisatorisk skal håndtere en beredskabssituation. Beredskabets arbejde består i at begrænse konsekvenserne af tab af data og systemer forårsaget af katastrofer og sikkerhedsbrister.

Der skal foreligge beredskabsplaner for:

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

Beredskabsplaner skal løbende afprøves og opdateres for at sikre, at de er tidssvarende og effektive. Beredskabsplanerne skal dog som minimum ajourføres og testes 1 gang årligt.

18. Overensstemmelse med lovbestemte krav

Informationssikkerhedspolitikken og de udarbejdede retningslinjer og procedurer skal være i overensstemmelse med den til en hver tid gældende lovgivning samt indgåede kontrakter. Der gøres således en indsats for hele tiden at holde sig opdaterede med relevante ændringer i lovgivning, ligesom der i et relevant omfang inddrages eksterne rådgivere i form af advokater, revisorer mv. med henblik på at sikre overholdelse af gældende regelsæt.

19. Godkendelse

Informationssikkerhedspolitikken er godkendt af ledelsen ved Nordjyllands Beredskab.

Aalborg den 15 / 9 2020

Underskrifter:

Beredskabsdirektør Diana Sørensen

Stabschef Per H. Vedsted