Informationssikkerhedspolitik
for
<organisation>

Indholdsfortegnelse

1. Indledning

1.1 Formål med informationssikkerhedspolitikken

<Organisationens> informationssikkerhedspolitik er vores sikkerhedsgrundlag og vores fælles forståelse af, hvad informationssikkerhed er. Informationssikkerhedsstrategien og informationssikkerhedspolitikken fastlægger vores ambitionsniveau og opstiller rammerne for de sikkerhedstiltag, som er nødvendige at følge, når vi som en organisation med stor samfundsmæssig betydning skal leve op til lovgivningskrav og best practices.

<Organisationen> ser ikke kun et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement i forhold til at kunne tilbyde en sikker service over for samarbejdspartnere, myndigheder og professionelle, og private kunder i det hele taget.

Med informationssikkerhed forstår vi den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til <organisationens> behandling og kommunikation af data elektronisk, i papirform mm. – herunder også teknologi og organisatoriske processer.

1.2 Hovedmålsætninger i informationssikkerhedspolitikken

Informationssikkerhed og troværdighed

Informationssikkerheden skal understøtte <organisationens> virksomhed i forhold til at sikre stabilitet i tilgangen til data, fortrolighed i forhold til følsomme data samt pålidelighed i datas indhold. Det sikres ved, at <organisationen> i vores daglige virksomhed lever op til almindeligt anerkendte principper for informationssikkerhed. Herved understøtter informationssikkerheden, at <organisationen> fortsat vil kunne leve op til ejerkredsens og kundernes forventning om troværdighed.

<Organisationens> opgaver består bl.a. i

- Samarbejde med myndigheder
- Borgerservice
- Administration
- Behandling af persondata
- Information til myndigheder, samarbejdspartnere og kunder

Informationssikkerhedspolitikken skal være med til at sikre, at de data og informationer, som <organisationen> kommunikerer til borgere, samarbejdspartnere og offentlige myndigheder, er tilgængelige, forbliver fortrolige, når de er af fortrolig karakter, og fremstår med et korrekt indhold.

Målet for informationssikkerheden er at:

- Understøtte bevidstheden om informationssikkerhed i organisationen
- Opnå høj driftssikkerhed og minimeret risiko for store nedbrud og tab af data
- Opnå korrekt funktion af it-systemerne med minimeret risiko for manipulation af data og systemer og fejl i disse
- Opnå mulighed for fortrolig behandling, transmission og opbevaring af data. Dvs. at faciliteter hertil skal være til stede og benyttes efter konkret behov
- Sikre mod forsøg på tilsidesættelse af sikkerhedsforanstaltninger

Afbalanceret informationssikkerhed

<Organisationen> er afhængig af et godt omdømme og fortsat politisk tillid. Derfor skal informationssikkerhedspolitikken være med til at sikre, at data og informationer behandles i overensstemmelse med de krav, der stilles til organi-

sationer med stor samfundsmæssig betydning. Sikkerhedsniveauet skal dog afbalanceres, således at fleksibiliteten og dynamikken i vores dagligdag ikke mistes. Derfor er det en målsætning i sikkerhedspolitikken, at data og systemer sikres ud fra en vurdering af, hvad der er nødvendigt at gøre under hensyntagen til de økonomiske rammer. Krav til informationssikkerhed skal vurderes i forhold til deres relevans for <organisationen> - dermed holdes fokus på et informationssikkerhedsniveau, hvor god sund fornuft er en afgørende faktor.

1.3 Omfang

Informationssikkerhedspolitikken er det dokument, der angiver de beslutninger, som ledelsen i <organisationen> har truffet med henblik på nærmere at fastlægge det tilstrækkelige sikkerhedsniveau samt definere de krav, der skal stilles, for at sikkerhedsniveauet opretholdes. Derfor fastlægges omfanget af informationssikkerhedspolitikken således:

- Informationssikkerhedspolitikken gælder for alle ansatte i <organisationen> uanset ansættelsesform, herunder også eksterne konsulenter og servicemedarbejdere. Det forventes, at informationssikkerhedspolitikken overholdes.
- Informationssikkerhedspolitikken gælder for alle systemer og alle data i <organisationens> besiddelse.
- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til organisationens systemer og data, skal ligeledes have kendskab til og følge informationssikkerhedspolitikken.
- Informationssikkerhedspolitikken udgør en præcisering af <organisationens> informationssikkerhedsstrategi.
- Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af <organisationens> it-systemer og papirarkiver.
- Informationssikkerhedspolitikken godkendes af bestyrelsen og revurderes en gang årligt for at sikre, at den er i overensstemmelse med de sikkerhedsmålsætninger, som <organisationen> arbejder efter.

2. Risikovurdering og risikoanalyse

Risikovurdering

Det sikkerhedsniveau, denne politik repræsenterer, er fastsat på baggrund af <organisationens> vurdering af de forretningsmæssige it-risici, som vi ønsker at imødegå.

It-risikovurderingen opdateres årligt og ved eventuelle større ændringer i it-systemerne, ændringer i anvendelse af systemerne eller ved større organisatoriske ændringer med efterfølgende tilretning af informationssikkerhedspolitikken, retningslinjer mm.

Sikkerhedsniveau

<Organisationens> sikkerhedsniveau skal først og fremmest indfri de forventninger til troværdighed og stabilitet, der er til behandling af forretningskritiske data i en organisation med samfundsmæssig betydning. <Organisationen> ønsker at fremstå med et højt sikkerhedsniveau, der tilgodeser:

- Lovgivningsmæssige krav samt EU-direktiver, inden de er omsat i national lovgivning
- De anerkendte standarder for informationssikkerhed i form af ISO 27001

3. Organisering og ansvar

3.1 Interne organisatoriske forhold

Organisering af informationssikkerhed i <organisationen> er defineret i informationssikkerhedsstrategien. Bestyrelsen har det overordnede ansvar for at sikre, at <organisationens> ledelse har defineret en informationssikkerhedsstrategi.

Ledelsen beslutter overordnede strategiske projekter af informationssikkerhedsmæssig karakter, men har i praksis delegeret det daglige ansvar for informationssikkerheden til økonomidirektøren og it-chefen. Almindelige problemstillinger af informationssikkerhedsmæssig karakter behandles i Chefgruppen, og Chefgruppen vil som helhed dele det generelle ansvar for informationssikkerheden. Ledelsen vil uddelegere ansvar og opgaver vedrørende de enkelte funktionsområder, herunder også for vejledning og instruktion af medarbejdere.

3.2 Styringsprincipper

Informationssikkerhed er et fælles anliggende for hele organisationen og vil blive ledet af it-chefen, herunder it-afdelingen, ifølge de regler og procedurer, der indgår i informationssikkerhedsstyringssystemet.

It-afdelingen vejleder ledelse og medarbejdere i informationssikkerhedsspørgsmål, og koordinerer og følger op på informationssikkerheds-relaterede aktiviteter.

3.3 Eksterne samarbejdspartnere

Der skal indgås skriftlige aftaler med eksterne samarbejdspartnere, og de sikkerhedskrav, der stilles, skal defineres ud fra den danske persondatalov, samt ISO 27001. Kravene skal fremgå af de skriftlige aftaler.

For at sikre klarhed over de sikkerhedskrav, der skal stilles, skal der ske en konkret identifikation af risici i forbindelse med brug af eksterne leverandører.

Eksterne samarbejdspartnere, der har adgang til data, skal efterleve samme retningslinjer som gælder internt i organisationen.

4. Klassifikation af systemer og data

For at sikre at vores systemer og data har det rigtige sikkerhedsniveau, skal disse identificeres og klassificeres. Der udarbejdes en fortegnelse over alle væsentlige it-aktiver, både hardware og software.

Der skal angives ansvarlige ejere for alle kritiske it-aktiver.

Data og systemer skal klassificeres i forhold til tilgængelighed og til sikkerhed (fortrolighed og datas pålidelighed).

Tilgængelighed af data og systemer prioriteres indbyrdes i følgende kategorier:

- **A** – tilgængelighed er forretningskritisk, og kan ikke erstattes af manuelle procedurer
- **B** – tilgængelighed er vigtigt, men funktionerne kan udføres manuelt i en begrænset tidsperiode
- **C** – tilgængelighed er ikke kritisk, og funktionerne kan afbrydes i en længere tidsperiode

Informationssikkerhed af data klassificeres efter følgende kategorier:

- **1** – forretningskritiske beslutninger bliver taget på grundlag af data – data med høj grad af fortrolighed
- **2**– data danner grundlag for beslutninger, men de er ikke kritiske – data er interne og eksponeres ikke udadtil
- **3** – data danner aldrig eller kun sjældent grundlag for beslutninger – data er offentlige

5. Brugeradfærd

Opretholdelse af det ønskede sikkerhedsniveau er afhængig af, at vi alle tager ansvar for informationssikkerheden.

Alle ansatte skal være bekendt med sikkerhedspolitikken og gældende retningslinjer for ønsket adfærd.

Anvendelse af it og behandling af data er selvfølgelige redskaber i varetagelsen af de daglige arbejdsopgaver. Håndteringen af vore redskaber kræver ikke specielle forudsætninger, men bør ske med omtanke og almindelig sund fornuft. Det er således tilstrækkeligt, men vigtigt, at følge disse få retningsgivere:

- 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 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 It-afdelingen.
- Hvis man oplever, at der sker brud på informationssikkerheden, er det vigtigt at informere sin nærmeste leder eller It-afdelingen.

5.1 Ansættelsesforholdet

Alle medarbejdere har et medansvar for at opretholde det ønskede sikkerhedsniveau i <organisationen>. For at kunne leve op til medansvaret, er det den enkelte afdelingsleders 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 udarbejdes deltaljerede retningslinjer for ønsket brugeradfærd på udvalgte områder som f. eks. e-mail og internet, password, og rapportering af sikkerhedshændelser. Retningslinjer for brugeradfærd godkendes af Chefgruppen efter behandling i samarbejdsforum. Som afhjælpningsforanstaltninger til at minimere vurderede risici, skal retningslinjerne jævnligt revurderes og opdateres. Overtrædelser af informationssikkerhedspolitikken vil efter omstændighederne kunne medføre disciplinære sanktioner.

5.2 Funktionsadskillelse

Der er etableret regler for funktionsadskillelse. Dette princip er en grundlæggende forudsætning for forebyggelse og begrænsning af konsekvenser, som stammer fra fejl, uheld og bevidst negative handlinger forårsaget af enkeltpersoner

eller grupper af enkeltpersoner. I de tilfælde, hvor det ikke er muligt at etablere funktionsadskillelse, kompenseres så vidt muligt med andre sikkerhedskontroller.

5.3 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.

5.4 Sikkerhedsprocedurer før ansættelse

Der skal være procedurer, der sikrer ansættelse af kompetente og sikkerhedsmæssigt egnede medarbejdere. Medarbejdere, der skal arbejde med fortrolige oplysninger, skal fremlægge straffeattest inden ansættelse.

Det skal sikres, at der foreligger ansættelseskontrakter på alle ansatte, hvor ansvar for informationssikkerheden er beskrevet, og der skal tages stilling til behovet for brug af tavshedserklæringer.

5.5 Ansættelsens ophør

Der er procedurer, der sikrer, at it-aktiver returneres, og at adgange og rettigheder ophører ved ansættelsesforholdets ophør. Brugerkonti deaktiveres efter 90 dage og lægges på en watch-liste.

6. Fysisk sikkerhed

Adgangen til alle fysiske lokaliteter er sikret mod uvedkommendes adgang.

6.1 Sikre områder

Lokaler er opdelt i sikkerhedsområder. Lokaler, hvor der opbevares fortrolige dokumenter eller medarbejderdata, skal være aflåst, når ingen er til stede. Serverrummet, hvor data lagres elektronisk er videoovervåget, og optagelserne opbevares i 30 dage.

6.2 Fysisk adgangskontrol

Adgang til lokationer tildeles på baggrund af autorisationer og beskyttes med et hensigtsmæssigt adgangskontrolsystem, udvalgt på baggrund af en risikovurdering. Gæster registreres og skal bære synligt gæstekort under besøget.

6.3 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.

Kritisk it-udstyr skal 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, så de ikke kan gendannes.

7. Styring af netværk og drift

Driftsforstyrrelser skal imødegås gennem:

- Forebyggende foranstaltninger såsom kvalitetssikring, ændringshåndtering og dokumentationsvedligeholdelse

- Problemhåndtering, der sikrer skadeudbedring, og som sikrer, at omgåelse, opkobling eller tilsvarende ikke er muligt

Sikkerhedshændelser rapporteres til it-chefen, ligesom planlagte forbedringstiltag.

Som en forudsætning for hurtig imødegåelse af driftsforstyrrelser, er der etableret procedurer for daglig sikkerhedskopiering (backup). Backup opbevares eksternt på en anden geografisk og sikker lokation, hvor sikkerheden jævnligt kontrolleres.

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

Procedure for vurdering af leverandører anvendes, når der skal stilles krav over for de leverandører, der leverer drift og udvikling til <organisationen>. De overordnede krav i dette afsnit anvendes til at stille krav over for leverandørerne, som skal overholde <organisationens> informationssikkerhedspolitik.

7.1 Operationelle procedurer og ansvarsområder

For at sikre stabiliteten i driften er der etableret funktionsadskillelse, 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. Procedurer, ansvarsområder og anvendt teknologi skal understøtte den nødvendige funktionsadskillelse.

7.2 Eksterne serviceleverandører

Der er procedurer til at overvåge, at eksterne serviceleverandører varetager kontroller, som udføres på vegne af <organisationen>, hensigtsmæssigt og i overensstemmelse med det aftalte.

7.3 Styring af driftsmiljø

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, f. eks. "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 programmer kan sætte hele organisationen ud af drift, og det kan være meget dyrt at rense it-systemerne, hvis de er blevet ramt af et hackerangreb eller en virus. Alt godkendt it-udstyr, der er tilsluttet <organisationens> netværk har, hvor det er muligt, installeret et aktivt og opdateret antivirusprogrammel, der kan opdage, rense og beskytte mod forskellige former for skadevoldende programmer. Det gælder også eksterne brugere, der tilsluttes netværket via fjernopkobling. Det overvåges, at antivirusprogrammerne hele tiden er opdaterede.

Det kontrolleres løbende, at anti-virus er aktivt på arbejdsstationerne, og at signatur-filerne ikke er ældre end én uge. Arbejdsstationer, der ikke har opdateret anti-virus kan ikke tilgå netværket, før den er opdateret. Opdatering finder automatisk sted, når brugeren aktiverer arbejdsstationen igen, men kræver ingen særlige interaktion af brugeren. Opdateringen kan medføre, at netværket i kort tid ikke er tilgængeligt.

Det er ikke tilladt at installere egne programmer på <organisationens> maskiner. Ved installation af programmer skal de procedurer, der findes i <organisationens> egne retningslinjer følges.

7.5 Sikkerhedskopiering

For at vigtige informationer altid kan fremfindes, og for at undgå tabt arbejde, foretages der sikkerhedskopiering og backup med faste intervaller. De nærmere regler herfor findes i retningslinjen for backup. Aftaler med eksterne leverandører skal indeholde krav til samme procedure, som gælder internt i <organisationen>.

Det skal ved regelmæssige test sikres, at sikkerhedskopierne kan genindlæses. Sikkerhedskopierne opbevares på en anden lokation adskilt fra produktionsdata, så de kan fremfindes ved igangsættelse af nødplaner eller i forbindelse med andre behov.

7.6 Netværkssikkerhed

For at undgå uautoriseret adgang, skal vores netværk sikres. Sikring af vores netværk imod uautoriseret adgang styres af it-afdelingen. Det sker f. eks. via adgangskontrol og adskillelse af netværkstjenester, hvor dette er hensigtsmæssigt. Der må ikke installeres netværksudstyr som f. eks. trådløse modems uden it-afdelingens godkendelse.

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

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

Det skal sikres, at it-afdelingen vedblivende har den nødvendige viden samt redskaber til overvågning af <organisationens> for at kunne opdage og spore sikkerhedsbrister samt til fejlretning. Netværket overvåges løbende med henblik på at opdage og udbedre brud på sikkerheden. Bærbare medier med adgang til netværket skal styres og beskyttes.

7.6.1 Trådløse netværk

Der er etableret trådløst netværk på alle <organisationens> lokationer. Der må kun etableres trådløst lokalnet efter it-afdelingens godkendelse. 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.

7.7 Informationsudveksling

Regler i forbindelse med informationsudveksling af fortrolig information via e-mail og andre elektroniske medier findes i retningslinjen for e-mail.

I forbindelse med ekstern opkobling til <organisationens> systemer må fortrolige data ikke kopieres, flyttes eller lagres på bærbare medier.

Derudover har alle medarbejdere et ansvar for at beskytte uovervåget it-udstyr og bærbare datamedier.

7.8 Logning og overvågning

It-afdelingen står for logning af vore kritiske systemer. Overvågning og opfølgning sker via alerts fra 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.

Som en del af logningen skal sikkerhedsrelaterede hændelser registreres.

Logfaciliteter og logoplysninger skal beskyttes mod manipulation og tekniske fejl.

Alle ure synkroniseres, så hændelser kan identificeres entydigt.

8. Adgangsstyring

8.1 De forretningsmæssige krav til adgangsstyring

Alle informationsaktiver (programmel, udstyr, data, informationer og databærende medier) skal i nærmere specificeret omfang være beskyttet mod uautoriseret adgang.

Ud over den nødvendige adgangskontrol til bygninger og lokaler, anvendes der elektroniske/-programmelbaserede adgangskontrolsystemer. Disse skal ud over adgangskontrol i nødvendigt omfang kunne alarmere og via logning danne grundlag for efterfølgende kontrol.

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

8.2 Administration af brugeradgang

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

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 være begrænset til tekniske systemer, hvor dette ikke kan undgås.

8.3 Brugerens ansvar

Alle medarbejdere er ansvarlige for deres personlige adgangskoder, og for at følge vedtagne retningslinjer for password:

- Første password – f. eks. i forbindelse med ansættelse – ændres efter it-afdelingens anvisninger
- Password indeholder mindst 8 tegn. Anvend bogstaver samt tal
- Undgå passwords, som er lette at gætte for andre
- Udskift passwordet med et nyt, når systemet giver melding om det
- Efter 5 mislykkede adgangsforsøg lukkes brugerkonto i en begrænset periode.
- Ændring af bruger ID imødekommes kun rent undtagelsesvis.

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 herover. 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

Informationssikkerhedspolitikken gælder for alt it-udstyr tilhørende <organisationen>. I retningslinjen for medarbejdere fastlægges de regler, som skal overholdes ved brug af mobilt udstyr og hjemmearbejdspladser.

9. Anskaffelse, udvikling og vedligeholdelse af it-systemer

9.1 Sikkerhedskrav til informationsbehandlingssystemer

De sikkerhedskrav, der stilles til systemers behandling af data, skal indgå i vurderingen, som foretages ved indkøb og test af eksternt udviklede systemer. Det enkelte system skal have implementeret sikringsforanstaltninger, som er tilstrækkelige i forhold til klassifikation af de data, systemet behandler, samt de forretningsmæssige funktioner, som systemet varetager.

9.2 Korrekt informationsbehandling

Vurderingen af, hvilke sikringsforanstaltninger, der er nødvendige i det enkelte system, foretages ud fra, hvilke data systemet indeholder, og hvilke forretningsmæssige funktioner systemet varetager. Som en del af sikring af data, tages der stilling til behovet for ind- og uddatavalidering.

9.3 Kryptering

Behovet for brug af kryptering skal identificeres ud fra en vurdering af, hvor kryptering som sikringsforanstaltning kan imødegå behovet for sikring af datas fortrolighed og/eller integritet. Det sker på grundlag af datas klassifikation, se afsnit 4. For at leve op til best practice for efterlevelse af persondataloven, bør kommunikation af persondata med identitetsangivelse, der kan misbruges, ske i krypteret form.

Ved anvendelse af kryptering skal der tages højde for nøglehåndtering.

9.4 Styring af driftsmiljøet

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

Data, der anvendes til test, skal udvælges omhyggeligt, kontrolleres nøje og beskyttes i henhold til deres klassifikation.

<Organisationen> besidder kildekode til webudvikling. Kildekode opbevares internt.

9.5 Sikkerhed i udviklings- og hjælpeprocesser

Vi udvikler 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 hvert kvartal, ved hjælp af servicevinduer uden for almindelig arbejdstid.

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 Sårbarhedsstyring

Der skal løbende indhentes informationer om sårbarheder i de anvendte systemer. Der foretages eksterne sårbarhedstest hver 6. måned, mens der testes internt hver nat. Sårbarhederne skal evalueres, og passende foranstaltninger implementeres.

10. Styring af sikkerhedshændelser på it-området

10.1 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 systemejeren og/eller it-chefen, så sikkerhedshændelserne kan imødegås, inden de udvikler sig. Rapportering af sikkerhedshændelser er beskrevet i retningslinje herfor. Økonomidirektøren orienteres om indtrufne hændelser.

10.2 Håndtering af sikkerhedsbrud og forbedringer

Målet og ansvaret for håndtering af sikkerhedsbrud er fastlagt af ledelsen.

Sikkerhedshændelser, fejlhændelser og væsentlige brugeraktiviteter i forhold til 1 og 2 klassificerede systemer skal logges, og uønskede hændelser skal så vidt muligt kunne spores tilbage til en enkeltperson.

Opståede problemer skal håndteres og korrigeres med udgangspunkt i en vurdering af alvoren i problemet. Alvorlige problemer skal analyseres med henblik på løbende forbedringer i informationssikkerheden. Hændelser der har indflydelse på tilgængelighed, skal afklares i overensstemmelse med gældende driftsaftaler (SLA). Driftshændelser, der ikke kan afklares inden for aftalt tid, skal håndteres i overensstemmelse med procedurer for hændelseshåndtering, og de ramte brugere og systemejere informeres.

Hvor der kan komme et retsligt efterspil, skal beviser indsamles, opbevares og præsenteres, så vi kan sikre, at de udgør et fyldestgørende og pålideligt bevismateriale.

11. It-beredskabsstyring

<Organisationen> har udarbejdet en it-beredskabsplan med en praktisk strategi for, hvordan <organisationen> organisatorisk skal håndtere en beredskabssituation. Beredskabets arbejde består i at begrænse konsekvenserne af tab af data og systemer forårsaget af katastrofer og sikkerhedsbrister.

It-beredskabet indgår i <organisationens> overordnede kriseberedskab.

I forbindelse med it-risikoanalysen har <organisationen> identificeret kritiske data og systemer. It-beredskabsstrategien bygger på it-risikoanalysen og de forretningsaktiviteter, som er vigtige for organisationen. For-

målet med beredskabskravene for informationssikkerheden er at få defineret og integreret de krav, der stilles til leverandører og til os selv i forhold til drift, personale, anlæg og øvrige faciliteter.

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.

For at beredskabsplanerne skal kunne fungere efter hensigten, skal følgende forudsætninger være opfyldt:

- Beredskabsplanerne skal ajourføres og testes som skrivebordstest 1 gang årligt, og med fuld test en gang hvert 3. år
- Sikkerhedskopier og reserveudstyr skal opbevares i en anden bygning end den, hvor originalmaterialet og driftsudstyret befinder sig

Der henvises i øvrigt til <organisationens> overordnede beredskabsplan.

12. Overensstemmelse med lovbestemte krav

Da der er flere lovgivninger, der påvirker vores daglige administration, skal der tages højde for disse i vores informationssikkerhedspolitik og de dertilhørende retningslinjer. <Organisationens> retningslinjer og procedurer skal være i overensstemmelse med alle sikkerhedskrav i lovgivning og med indgåede kontrakter.

Der er procedurer, der sikrer, at relevante sikkerhedskrav i lovgivning, bekendtgørelser samt i indgåede kontraktlige forpligtelser styres og overholdes for de enkelte systemer såvel som for <organisationen> som helhed.

Den fornødne juridiske ekspertise skal inddrages i vurderingen af disse krav.

13. Godkendelse

Informationssikkerhedspolitikken er godkendt af ……

Dato: _____- _____

Underskrift:

_____