Informationssikkerhedspolitik for <organisation>

1. Formål

<Organisationens> informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i <organisationen> og fastlægger vores ambitionsniveau herfor. Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af <organisationens> informationssikkerhedshåndbog, der forstås som fællesbetegnelsen af informationssikkerhedspolitikken med de underliggende retningslinjer og forretningsgange.

Begreber og definitioner findes i bilag 1.

Informationssikkerhedspolitikken er en vigtig del af <organisationens> sikkerhedshåndbog og beskriver det ledelsesgodkendte niveau for sikkerhed. Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i <organisationens> organisation og virke. De retningslinjer, der udformes for at understøtte informationssikkerhedspolitikkens hovedmålssætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til informationssikkerhed i det daglige arbejde.

<Organisationen> ser ikke kun et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement for at kunne tilbyde en sikker service for borgerne og behandlerne. Informationssikkerhed er derfor en nøgleværdi hos <organisationen>, og den vil være en naturlig del af vores it-aktiviteter.

2. Omfang

Informationssikkerhedspolitikken er gældende for alle medarbejdere i <organisationen>.

Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til <organisationens> systemer, data og informationer skal gøres bekendt med politikken og følge den.

Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af <organisationens> it-systemer.

3. Hovedmålsætninger og sikkerhedsniveau

Sikkerhedsmålsætning:

"Vi vil have et tilstrækkeligt informationssikkerhedsniveau for alle ansatte, samarbejdspartnere og for anvendelsen af it-ressourcer, såsom it-systemer, hardware samt elektroniske datamedier i <organisationen>."

Der henvises til informationssikkerhedsstrategien, for en nærmere beskrivelse at det niveau af sikkerhed, som er tilstrækkeligt for <organisationen> i overensstemmelse med den funktion, vi har.

Et tilstrækkeligt informationssikkerhedsniveau opnås igennem sikringsforanstaltninger, der sikrer:

1. Fortrolighed, integritet, autenticitet (uafviselighed) og tilgængelighed af <organisationens> systemer og data i forhold til den it-risikovurdering, der er fastsat for det enkelte system/data.
2. Beskyttelse af <organisationens> it-aktiver, medarbejdernes kompetencer, organisationens image og informationer/data i <organisationens> varetægt.

For at fastholde det tilstrækkelige sikkerhedsniveau i <organisationen> skal følgende overholdes:

- Der skal forefindes retningslinjer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af <organisationens> drift og daglige arbejde.
- <Organisationen> skal igennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke udhuler <organisationens> informationssikkerhedsniveau.
- <Organisationen> skal følge op på informationssikkerheden ved fortsat at optimere <organisationens> ledelsessystem igennem løbende vedligehold og optimering af informationssikkerhedsstrategien, informationssikkerhedspolitikken og de dertilhørende retningslinjer og forretningsgange. Målet er, at sikre en struktureret og kontinuerlig forbedringsproces.

4. Organisation og ansvar

Sikkerhedsmålsætning:

"Alle medarbejdere har ansvar for informationssikkerheden. De er bekendte med og efterlever vores informationssikkerhedspolitik, informationssikkerhedshåndbog, retningslinjer og forretningsgange i <organisationen>."

Planlægning, implementering og kontrol af informationssikkerhed er defineret af <organisationens> ledelse. Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet i <organisationen> og er ansvarlig for opfølgning på sikkerhedshændelser. Informationssikkerhedspolitikken revurderes og godkendes mindst én gang årligt, eller i forbindelse med eventuelle situationer, der tilsiger det.

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

Den nødvendige viden og kompetence omkring informationssikkerhed kommunikeres til alle medarbejdere, og der bliver løbende arbejdet med holdninger og viden omkring informationssikkerhed. Ledelsen er ansvarlig for, at informationssikkerheden overholdes.

5. Informationssikkerhedshåndbogen

Informationssikkerhedspolitikken uddybes i retningslinjer og forretningsgange. Tilsammen udgør politikken, retningslinjer, beredskabspolitik og forretningsgange informationssikkerhedshåndbogen, der inddeles i følgende hovedområder:

1. Retningslinje for medarbejdersikkerhed.
2. Retningslinje for styring af leverandører.
3. Retningslinje for styring af sikkerhedshændelser.
4. Retningslinje for adgangsstyring.

6. Risikovurdering og klassifikation

Risikovurdering

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

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

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

Klassifikation
For at sikre, at vores systemer og data har det rigtige sikkerhedsniveau, skal disse klassificeres. Data og systemer skal klassificeres efter både tilgængelighed, pålidelighed og fortrolighed.

I tilgængelighedskriteriet ligger, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

Tilgængelighed af data og systemer prioriteres indbyrdes i følgende kategorier:

- **Høj** – tilgængelighed er forretningskritisk og kan ikke erstattes af manuelle procedurer.
- **Medium** – tilgængelighed er vigtigt, men funktionerne kan udføres manuelt i en begrænset tidsperiode f.eks. adgang til journaliseringssystem.
- **Lav** – tilgængelighed er ikke kritisk og funktionerne kan afbrydes i en længere tidsperiode f.eks. adgang til fysiske arkiver.

Med pålidelighed menes, at data er pålidelige, når de er komplette, korrekte og opdaterede.

Pålidelighed af data klassificeres efter følgende kategorier:

- **Høj** – Forretningskritiske beslutninger bliver taget på grundlag af data.
- **Medium** – data danner grundlag for beslutninger, men de er ikke kritiske - f.eks. data med økonomisk overblik i journaliseringssystem.
- **Lav** – data danner aldrig eller kun sjældent grundlag for beslutninger - f.eks. data på intranet omkring kantineforhold m.v.

Med fortrolighed menes der, at kun autoriserede personer har ret til at tilgå informationerne, og informationerne skal kun være tilgængelige for autoriserede personer. <Organisationen> opdeler oplysningerne i kategorierne fortrolige, interne og uklassificerede.

Fortrolighed af data inddeles i følgende kategorier:

- **Uklassificeret –** Der er ingen fortrolighed og ingen begrænsninger for hvem, der må få adgang til data.
- **Internt brug** – Materiale, der er tilgængeligt for alle internt i organisationen.
- **Fortroligt** – Data der kun må være tilgængeligt for en begrænset gruppe af personer, f.eks. lukkede punkter fra bestyrelsesmøder.

Baseret på klassifikationen samt risikovurderingen etableres relevante sikkerhedsforanstaltninger.

7. Overtrædelse af informationssikkerhedspolitikken

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

Hvis en medarbejder er vidende om, at <organisationens> informationssikkerhed overtrædes, skal det meddeles til informationssikkerhedskoordinatoren eller direktøren hurtigst muligt.

8. Afvigelser

Hvis der opstår situationer, hvor kravene i informationssikkerhedspolitikken ikke kan efterleves, skal der skriftligt anmodes om dispensation af <organisationens> direktør. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger.

9. Udarbejdelse og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: Godkendes af ledelsen.
- Informationssikkerhedshåndbogen samt bilag og retningslinjer: Godkendes af informationssikkerhedsforummet.
- Operationelle procedurer: Kan foretages af de ansvarlige medarbejdere.

Informationssikkerhedspolitikken er godkendt den XX., og træder i kraft den XX.

Dokumentinformation

Dokumenthistorik/version:

Revision	Ændringsbeskrivelse	Dato/Forfatter
01.01		
01.02		
01.03		

Bilag 1: Begreber og definitioner

Begreb	Definition
Fortrolighed	Kun autoriserede personer har ret til at tilgå informationerne, og informationerne skal kun være tilgængelige for autoriserede personer. <Organisationen> opdeler oplysninger i kategorierne fortrolige, interne og uklassificerede.
Pålidelighed	Data er pålidelige, når de er komplette, korrekte og opdaterede.
Tilgængelighed	I tilgængelighedskriteriet ligger, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.
Informationssikkerhedspolitik	Sikkerhedspolitikken indgår i en dokumentstruktur, hvor politikken er det overordnede dokument, som underskrives af ledelsen, og som udstikker de overordnede krav og målsætninger, som skal opfyldes igennem specifikke retningslinjer, forretningsgange og instrukser.
Retningslinjer	I retningslinjerne udfyldes de målsætninger, der er fastlagt i politikken i konkrete beskrivelser af, hvordan sikkerhedspolitikken implementeres. Retningslinjerne fungerer på et overordnet niveau og indeholder ikke tekniske og systemrelaterede beskrivelser.
Forretningsgange og instrukser	Forretningsgange og instrukser udgør specifikke vejledninger til, hvordan retningslinjerne på detaljeret niveau overholdes og implementeres i den enkelte afdeling.
Sikringsforanstaltninger	De kontroller som indføres i form af administrative procedurer eller tekniske opsætninger for at undgå, at der indtræffer sikkerhedshændelser.
Sikkerhedsforhold	Med sikkerhedsforhold menes alle de forhold, som kan påvirke informationers sikkerhed i forhold til fortrolighed, pålidelighed og tilgængelighed.
Sikkerhedshændelser	Begrebet forstås bredt som alle de hændelser, der påvirker informationssikkerheden.