INFORMATIONSSIKKERHEDSPOLITIK FOR HOVEDSTADENS BEREDSKAB (version 2.1)

25. oktober 2022

Journalnummer 33369/22

IT, Digitalisering & Shared Services, Informationssikkerhed

Bag Rådhuset 3, 1550 København V

E-Mail: informationssikkerhed@hbr.dk

www.hbr.dk

Indhold

1. INDLEDNING 2

1.1 FORMÅL 2

1.2 MÅL 2

1.3 ANVENDELSESOMRÅDE 2

1.4 OMFANG 2

2. RISIKOVURDERINGER 3

3. IT-BEREDSKAB 3

4. DATAETIK 3

4.1. GENNEMSIGTIGHED OG ÅBENHED 3

4.2. VÆRDIGHED 3

4.3. LIGHED, SAGLIGHED OG RETFÆRDIGHED 4

4.4. FAGLIG INTEGRITET 4

5. AWARENESS 4

6. ANSVAR OG ORGANISERING 4

7. OVERENSSTEMMELSE MED LOVBESTEMTE KRAV 4

8. VEDTAGELSE 5

9. ÆNDRINGER 5

1. Indledning

1.1 Formål

Hovedstadens Beredskabs informationssikkerhedspolitik er vores sikkerhedsgrundlag og vores fælles forståelse af, hvad informationssikkerhed er.

1.2 Mål

Hovedstadens Beredskab har som mål at sikre:

- **Fortrolighed**
  Målet er at etablere en fortrolig databehandling, herunder transmission og opbevaring af person- og forretningsoplysninger, hvor kun autoriserede og autentificerede brugere har adgang, og hvor brugernes adgang er begrænset til det nødvendige. Hensyn til effektivitet og fleksibilitet i opgaveløsningen skal altid afvejes mod hensynet til borgernes personlige integritet og risici i øvrigt.
- **Integritet**
  Målet er at opnå en pålidelig og korrekt funktion i beredskabets it-løsninger med minimeret risiko for ukorrekt datagrundlag og datatab, for eksempel som følge af menneskelige eller systemmæssige fejl, forsøg på svindel eller bedrageri samt udefrakommende hændelser.
- **Tilgængelighed**
  Målet er en høj tilgængelighed således, at beredskabets it-løsninger er tilgængelige for brugerne, når de har behov for det. Det er endvidere målet at minimere risikoen for it-nedbrud. It-løsningernes tilgængelighed og kapacitet skal afspejle Hovedstadens Beredskabs behov for adgang til de oplysninger, der er nødvendige for en effektiv opgaveløsning, som udføres til tiden.

1.3 Anvendelsesområde

Informationssikkerhedspolitikken gælder for al databehandling i Hovedstadens Beredskab. Det vil sige, hvor vi behandler:

- Registrerede personer og personhenførbare oplysninger (personoplysninger)
- Oplysninger af økonomisk eller forvaltningsmæssig betydning (forretningsoplysninger)

Hovedstadens Beredskabs manuelle behandlinger (i papirform) af person- og forretningsoplysninger er også inkluderet i informationssikkerhedspolitikken.

1.4 Omfang

- Informationssikkerhedspolitikken gælder for alle medarbejdere i Hovedstadens Beredskab uanset ansættelsesform, herunder også frivillige og eksterne konsulenter.
- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til Hovedstadens Beredskabs it-løsninger og data, skal ligeledes have kendskab til og følge informationssikkerhedspolitikken.

- Informationssikkerhedspolitikken gælder for alle it-løsninger og alle data i Hovedstadens Beredskabs besiddelse.

2. Risikovurderinger

Informationssikkerhedsarbejdet baseres på risikovurderinger af aktiver i Hovedstadens Beredskab. Aktiver er fortrinsvis data og forretningsprocesser, men det er også systemer, hardware, netværk, infrastruktur m.v., der indeholder eller understøtter data og forretningsprocesser. Det er Hovedstadens Beredskabs mål, at risikovurderingerne viser en stadig faldende tendens, hvis der har været påvist uacceptable risici tidligere. Dette skal blandt andet opnås gennem en løbende styrkelse af ledelsessystemet for informationssikkerhed.

3. It-beredskab

Som understøttelse for målopfyldelsen skal it-løsninger og infrastruktur, der er kritiske for Hovedstadens Beredskabs betjening af borgere og virksomheder, identificeres, og der skal fastsættes maksimalt acceptable tider for utilgængelighed. Der skal endvidere udarbejdes, vedligeholdes og afprøves it-beredskabsplaner, der sikrer nøddrift, eskalering, retablering og genoptagelse af normal drift i tilfælde af større nedbrud, ulykker eller katastrofer i forhold til kritiske it-løsninger og infrastruktur.

4. Dataetik

Dataetik handler om god praksis, når vi indsamler, bruger og deler data. Dataetik er særlig relevant, når behandlingen af data kan påvirke mennesker og samfund, direkte eller indirekte. Det er ikke bare et spørgsmål om at overholde lovgivningen, men også at behandle andres data med respekt. Individet skal sikres mod unødvendig registrering og anvendelse af personoplysninger. Selvbestemmelse over egen situation er en grundrettighed, mennesket har forrang for systemet, og den menneskelige relation vægtes højt.

I Hovedstadens Beredskab tænker vi en række centrale værdier og principper ind, når vi behandler data. De tager udgangspunkt i Dataetisk Råds anbefalinger:

4.1. Gennemsigtighed og åbenhed

I Hovedstadens Beredskab ønsker vi fuld gennemsigtighed i brugen af data. Det skal være gennemskueligt for de registrerede personer, hvordan deres data anvendes, og i hvilke sammenhænge data indgår. Det er vigtigt for Hovedstadens Beredskab, at data bearbejdes på en forsvarlig, sikker og hensigtsmæssig måde.

4.2. Værdighed

I Hovedstadens Beredskab vægtes de registrerede personers værdighed højt; det gælder også, når data indgår i vores behandling. Der arbejdes kun med løsninger, hvor privatliv respekteres, og når der tages nye

teknologiske løsninger i brug, foretages en konkret afvejning af værdien, ulempen eller risikoen for de registrerede personer set i forhold til den administrative eller operative gevinst.

4.3. Lighed, saglighed og retfærdighed

I Hovedstadens Beredskab ønsker vi ikke at bruge data på en måde, der kan påvirke de registrerede personers adfærd eller anden skævhed (bias). Metoder, der indebærer risiko for skævheder eller diskrimination, vil ikke blive anvendt.

Når der udvikles nye teknologiske løsninger, fokuseres der på inddragelse af forskellige faglige baggrunde, kompetencer og forskellige indsigter for at sikre, at der er opmærksomhed på, om resultaterne kan diskriminere særlige grupperinger, f.eks. køn, alder, etnicitet eller lignende.

4.4. Faglig integritet

I Hovedstadens Beredskab går det faglige arbejde forud for de teknologiske muligheder. Data skal anvendes til at understøtte, udvikle og kvalificere opgaver, så der kan leveres bedre indsatser til gavn for dig som borger.

5. Awareness

Awareness om informationssikkerhed er blandt de vigtigste sikkerhedsforanstaltninger. Derfor skal informationssikkerhedspolitikken kommunikeres til alle relevante personer (se afsnit 1.4). Medarbejderne m.fl. skal ved ansættelse og i løbet af ansættelsesforholdet uddannes og bevidstgøres om forhold, der relaterer sig til informationssikkerhed.

6. Ansvar og organisering

Informationssikkerhedsfunktionen i Hovedstadens Beredskab er ansvarlig for vedligeholdelse af politikken. Den skal gennemgås årligt og behandles af den øverste ledelse i Hovedstadens Beredskab. Ved større ændringer skal bestyrelsen for Hovedstadens Beredskab godkende politikken. Yderligere ansvar og organisering i øvrigt er beskrevet i underliggende retningslinjer mv.

7. Overensstemmelse med lovbestemte krav

Informationssikkerhedsniveauet skal som minimum leve op til gældende lovgivning og andre relevante krav og være i overensstemmelse med den aktuelle praksis i Danmark for offentlige myndigheder inden for dette område. Informationssikkerhedsarbejdet skal derfor baseres på ISO 27001-standarden eller tilsvarende.

8. Vedtagelse

Informationssikkerhedspolitikken er godkendt af bestyrelsen for Hovedstadens Beredskab 8. juni 2016, og blev da benævnt It-sikkerhedspolitik.

9. Ændringer

Version	Dato	Ændringer
1.0	08-06-2016	-
2.0	04-10-2022	Dokumentet er omdøbt fra ”It-sikkerhedspolitik” til ”Informationssikkerhedspolitik”. Alle afsnit er gennemgået og opdateret, så de er ajourført. Afsnit om dataetik er tilføjet. Politikken behandles i chefgruppen 10-10-2022. Efterfølgende behandling forventes at ske i hhv. Arbejdsudvalget 09-11-2022 og bestyrelsen 30-11-2022.
2.1	25-10-2022	Dokumentet er behandlet i chefgruppen 10-10-2022, hvorefter følgende ændringer er sket: - Afsnit 4 om dataetik er omskrevet, så tiltaleform nu er 3. person og ikke 2. person. Hertil imødekommes et ønske om at uddybe forskellene mellem dokumentets version 1.0 og 2.0: Generelt: - Begrebet ”it-sikkerhed” er ændret til ”informationssikkerhed”, da det er et bredere og hermed mere dækkende begreb. - ”It-systemer” omdøbt til ”it-løsninger”, da det er et bredere og hermed mere dækkende begreb. - Afsnit 1.1. Nyt: Formål tydeliggjort. - Afsnit 1.2. Intet nyt, findes også i version 1.0. - Afsnit 1.3. Intet nyt, findes også i version 1.0. Dog lettere omskrivning af kommunikative grunde. - Afsnit 1.4. Delvist nyt: Politik gælder for alle medarbejdere er tydeliggjort. Politik gælder

		også leverandører og samarbejdspartnere er tilføjet. Politik gælder alle it-løsninger og data er tydeliggjort. - Afsnit 2. Intet nyt, findes også i version 1.0. Dog er begrebet ”aktiver” tilføjet. Begrebet stammer fra ISO 27001-standarden. - Afsnit 3. Intet nyt, findes også i version 1.0. Dog er infrastruktur tilføjet. - Afsnit 4. Nyt: Afsnit 4 om dataetik er tilføjet. Teksten er inspireret af principper og værdier fra Dataetisk Råd. Disse har hidtil været uskrevne regler i Hovedstadens Beredskab, hvor vi kun behandler de data, der er nødvendige for at udføre vores opgaver. Hertil skal ingen registrerede personer føle sig udstillet, udnyttet eller krænket i vores dataregistrering, det gælder f.eks. i billeddata fra operative indsatser. - Afsnit 5. Intet nyt, findes også i version 1.0. Dog lettere omskrivning af kommunikative grunde. Afsnit i version 1.0 hed ”bevidsthed om it-sikkerhed”. - Afsnit 6. Delvist nyt: At politikken skal gennemgås årligt af den øverste ledelse, og bestyrelsen skal godkende større ændringer er tilføjet. - Afsnit 7. Intet nyt. Tilsvarende afsnit i version 1.0 hed ”minimumskrav”. - Afsnit 8. Intet nyt. Tekst lå tidligere i afsnit ”ansvar og organisering” i version 1.0. - Afsnit 9. Nyt: Således at versionering og historik fremgår.