HOVEDSTADENS BEREDSKAB

REGULATIV FOR IT-SIKKERHED

Kapitel 1 - Anvendelsesområde og formål

§ 1. Styringen af informationssikkerheden i Hovedstadens Beredskab er beskrevet i en it-sikkerhedshåndbog, som indeholder:

- It-sikkerhedspolitikken: It-sikkerhedspolitikken fastlægger det overordnede niveau for it-sikkerheden i Hovedstadens Beredskab.
- It-sikkerhedsregulativ: It-sikkerhedsregulativet beskriver de organisatoriske rammer for Hovedstadens Beredskabs håndtering af it-sikkerhedsrisici.
- En række uddybende it-sikkerhedsregler: De uddybende it-sikkerhedsregler for Hovedstadens Beredskab er procedurer, instrukser og retningslinjer, der detailregulerer it-sikkerhedsforholdene. Indtil andet foreligger, er Københavns Kommunes uddybende it-sikkerhedsregler gældende i Hovedstadens Beredskab.

Stk. 2. It-sikkerhedshåndbogen baseres på ISO-standarden for ledelsessystemer for informationssikkerhed (ISO 27001) og den best practice for ledelsessystemer, der er beskrevet i ISO 27002.

Stk. 3. It-sikkerhedshåndbogen skal løbende tilpasses lovgivningen, den teknologiske udvikling samt internationale, statslige, fælleskommunale og regionale standarder.

Stk. 4. It-sikkerhedshåndbogen gælder for alle relevante interessenter - herunder samtlige af beredskabets medarbejdere.

Stk. 5. It-sikkerhedshåndbogen gælder for behandling af personoplysninger og værdioplysninger i Hovedstadens Beredskab, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk databehandling af personoplysninger, der er eller vil blive indeholdt i et manuelt register.

§ 2. It-sikkerhedsregulativet har til formål at beskrive den organisatoriske ramme for it-sikkerhedsarbejdet, så ansvaret for ledelsessystemets forskellige elementer er entydigt placeret.

§ 3. De begreber, der er anvendt i Regulativ for it-sikkerhed, er defineret i Bilag 1 bagest i dette regulativ.

Kapitel 2 – Ansvar og organisation

Bestyrelsen

§ 4. Bestyrelsen vedtager Hovedstadens Beredskabs it-sikkerhedspolitik og it-sikkerhedsregulativ efter indstilling fra direktionen.

Stk. 2. It-sikkerhedspolitikken fastlægger det overordnede niveau og mål for it-sikkerheden i Hovedstadens Beredskab.

Stk. 3. It-sikkerhedsregulativet beskriver de organisatoriske rammer for

HOVEDSTADENS BEREDSKAB

Hovedstadens Beredskabs håndtering af it-sikkerhedsrisici.

Beredskabsdirektøren og direktionen

§ 5. Beredskabsdirektøren skal sikre, at specifik lovgivning af betydning for it-sikkerheden og eksterne It-sikkerhedskrav bliver identificeret, dokumenteret og overholdt.

§ 6. Det daglige ansvar for overholdelsen af reglerne i persondataloven i forbindelse med behandling af personoplysninger påhviler beredskabsdirektøren.

§ 7. Direktionen varetager den umiddelbare forvaltning af Hovedstadens Beredskabs overordnede og tværgående it-sikkerhedsforhold.

Stk. 2. Direktionen er ansvarlig for at fastsætte de uddybende it-sikkerhedsregler for Hovedstadens Beredskab.

Stk. 3. Ændringer i de uddybende it-sikkerhedsregler, der ikke har væsentlig indflydelse på It- sikkerhedsniveauet eller ikke har økonomiske konsekvenser, delegeres til it-sikkerhedsfunktionen.

Stk. 4. It-sikkerhedsfunktionen orienterer mindst en gang i kvartalet direktionen om it-sikkerhedsbrud og status på it-sikkerhedsarbejdet i Hovedstadens Beredskab, samt afgivne dispensationer for og ændringer af de uddybende it- sikkerhedsregler.

Stk. 5. Hovedstadens Beredskabs it-sikkerhedsfunktion og den driftsansvarlige skal sikre, at der fastsættes uddybende it-sikkerhedsregler for Hovedstadens Beredskab. Ændringer i de uddybende it-sikkerhedsregler for Hovedstadens Beredskab skal godkendes af direktionen. Dispensation fra de uddybende it- sikkerhedsregler kan kun ske på baggrund af en godkendelse fra direktionen.

Direktionen har ansvar for fastlæggelse af it-sikkerhedsniveauet. Endvidere skal it-sikkerhedsfunktionen og den driftsansvarlige fastsætte retningslinjer for integration og netværkskommunikation til eksternt driftede løsninger.

It-sikkerhedsfunktionen

§ 8. It-sikkerhedsfunktionen udpeges af direktionen, som ligeledes godkender ændringer/tilpasninger i organisationen.

Stk. 2 It-sikkerhedsfunktionen fører det daglige tilsyn med overholdelsen af Hovedstadens Beredskabs It-sikkerhedsbestemmelser.

Stk. 3. It-sikkerhedsfunktionen tilrettelægger information, uddannelsesaktiviteter og materiale for medarbejdere i Hovedstadens Beredskab.

Stk. 4. It-sikkerhedsfunktionen rådgiver Hovedstadens Beredskab om it-sikkerhedsmæssige forhold.

Stk. 5. It-sikkerhedsfunktionen kan afkræve enhver medarbejder i Hovedstadens Beredskab oplysninger, som har betydning for varetagelsen af tilsynsfunktionen.

Stk. 6. It-sikkerhedsfunktionen skal sikre, at der sker kontrol af adgangsrettigheder og autorisationer, der er givet til medarbejderne.

Stk. 7. It-sikkerhedsfunktionen kan komme med påbud til alle ansatte og enheder i Hovedstadens Beredskab, om hvorledes man skal forholde sig i relation til It-sikkerhed.

Stk. 8. Som led i den almindelige revision af Hovedstadens Beredskab, skal der også foretages revision af It-sikkerheden. It-sikkerhedsfunktionen aftaler med revisor hvorledes It-sikkerhedsrevisionen skal udføres.

Den driftsansvarlige

§ 9. Den driftsansvarlige har ansvaret for, at de teknikunderstøttende applikationer som anvendes af eller driftes af Hovedstadens Beredskab, fx netværk og kommunikation, serverdrift, print, infrastruktur, pc-support, service- management m.m., er i overensstemmelse med de it-sikkerhedsmæssige krav og den til enhver tid gældende it-strategi.

Stk. 2. Den driftsansvarlige skal i samarbejde med it-sikkerhedsfunktionen, udarbejde it-sikkerhedsforskrifter eller retningslinjer for it-installationer/driftsmiljø og de benyttede netværk.

Stk. 3. Den driftsansvarlige har ansvaret for sikkerheden på it-platforme.

Stk. 4. Den driftsansvarlige skal sikre, at der bliver taget backup af oplysninger på serverudstyr som driftes af Hovedstadens Beredskab - efter behov på en ekstern lokation.

Stk. 5. Den driftsansvarlige kan dispensere, hvis ikke udviklings-, test- og uddannelsesmiljøer med person- eller værdidata, som driftes af Hovedstadens Beredskab, holdes adskilt fra produktionsmiljøet.

Direktionsområderne

§ 10. Vicedirektørerne skal inden for eget område iværksætte de foranstaltninger, der er nødvendige for at opnå en tilstrækkelig it-sikkerhed, indenfor de rammer, som er opstillet i it-sikkerhedshåndbogen.

Stk. 2. Vicedirektørerne er inden for eget område ansvarlig for, at de medarbejdere, som arbejder med it-sikkerhedsopgaver, er i besiddelse af de nødvendige kompetencer.

Stk. 3. Vicedirektørerne skal inden for eget område udpege systemejere for områdets it-systemer samt mindst én stedfortræder for hver systemejer. Hvor intet andet er besluttet, er det vicedirektøren der er stedfortræder.

Systemejer

§ 11. Systemejeren skal sikre, at systemets funktionalitet og anvendelse løbende

tilpasses, og bedst muligt understøtter it-sikkerhedskravene samt forretningens og brugernes behov. Generelt skal der gøres opmærksom på, at der er tale om en entydig ansvarsplacering. Udmøntningen af ansvar herunder udførelsen af opgaverne vil ske i tæt samarbejde med øvrige relevante parter. Der udarbejdes en tjekliste for systemejer, hvor de enkelte opgaver er nærmere beskrevet.

Stk. 2. Før anskaffelse af nye systemer skal systemejeren have godkendt anskaffelsen af systemet. Dette sker i forbindelse med registreringen i Hovedstadens Beredskabs fortegnelse over it-systemer. I forbindelse med anskaffelsen af systemet skal der foreligge en kortfattet risikoanalyse. Systemejeren har mulighed for at få separat It-sikkerhedsgodkendelse af andet end nye systemer. Det kan eksempelvis være tillægsmoduler til eksisterende It-systemer.

Stk. 3. Systemejerskabet skal varetages ud fra Hovedstadens Beredskabs forretningsmæssige behov. Systemejeren er ansvarlig for it-systemets funktionalitet, opbygning, anvendelse og sikkerhedsløsning. Det betyder, at systemejeren skal tilsikre disse elementer, og ikke nødvendigvis selv udføre dem. I praksis vil løsningen af denne opgave foregå i tæt samarbejde med den driftsansvarlige, it-sikkerhedsfunktionen og eksterne leverandører. Der kan indgås aftale med leverandøren som beskriver niveauet for service.

Stk. 4. Systemejer er ansvarlig for, at it-systemet kan anvendes mest muligt effektivt og at systemet løbende forbedres, så det bedst muligt understøtter arbejdsopgaverne og Hovedstadens Beredskabs forretningsmæssige behov, og lever op til kravene i It-sikkerhedshåndbogen. Der skal etableres processer, der sikre en stabil, effektiv og sikker drift af systemet.

Stk. 5. Systemejer er ansvarlig for, at dokumentationen af systemer og processer er ajourført og tilgængelig for relevante medarbejdere. Endvidere har systemejer ansvar for, at der indgås aftale om it-beredskab efter kriterier og retningslinjer fastlagt i it-sikkerhedshåndbogen, og systemejeren skal endvidere bidrage til Hovedstadens Beredskabs it-beredskabsplan.

Stk. 6. Ved brug af eksterne samarbejdspartnere/leverandører er systemejer ansvarlig for, at der indgås en databehandler-/it-sikkerhedsaftale, hvor sikkerhedsforanstaltninger i forbindelse med samarbejdet/leverancerne er beskrevet. Nye aftaler baseres på den standard, der er fastlagt i it-sikkerhedshåndbogen.

Stk. 7. Systemejeren skal sikre, at it-systemet kan logge behandling af data, når det er krævet i de uddybende it-sikkerhedsregler og som følge af gældende lovgivning.

Stk. 8. Hvis integration af it-systemer indebærer en øget it-sikkerhedsrisiko, skal denne risiko vurderes nærmere af systemejeren med inddragelse af den driftsansvarlige og it-sikkerhedsfunktionen

Stk. 9. Hvis vicedirektøren endnu ikke har udpeget en systemejer, varetages systemejerskabet af lederen af det område, som anskaffer systemet eller af en af denne udpeget projektejer. For mindre vigtige systemer, som ikke indeholder

væsentlige økonomioplysninger eller følsomme personoplysninger, består systemejers rolle i at være systemkontaktperson. Systemkontaktpersonens rolle, og om der skal udpeges en systemejer for fælles-offentlige systemer, som anvendes af Hovedstadens Beredskab, er beskrevet i en vejledning til de uddybende it-sikkerhedsregler for Hovedstadens Beredskab.

Funktionsadskillelse

§ 12. En medarbejder kan ikke samtidig varetage funktionen som it-sikkerhedsleder, systemejer eller driftsansvarlig.

Autorisationsansvarlige

§ 13. Den autorisationsansvarlige varetager de opgaver der er i forbindelse med bestilling af autorisationer og rettigheder til medarbejderne. Dvs. bestilling af oprettelser, flytning, ændringer og sletninger af medarbejdere; normalt hos brugeradministration. Den autorisationsansvarlige har ansvaret for, at der bestilles de rettigheder, som medarbejderne har behov for arbejdsmæssigt.

Stk. 2 It-sikkerhedsfunktionen fører en liste over hvem, der er godkendt som autorisationsansvarlige. Den lokale leder er ofte den autorisationsansvarlige. Lederen har mulighed for at uddelegere bestillingsopgaven til en bemyndiget medarbejder, som herved bliver autorisationsansvarlig.

Brugeradministration

§ 14. Brugeradministrationen modtager bestillingen fra den autorisationsvarlige og udfører selve oprettelsen på baggrund af det bestilte. Når bestillingen er udført, gives en melding til den autorisationsansvarlige samt systemejeren(e).

Ledere

§ 15. Ledere på alle niveauer skal sikre, at det er muligt for medarbejderne at efterleve deres ansvar for at beskytte Hovedstadens Beredskabs person- og værdioplysninger.

Den personaleansvarlige er ansvarlig for, at medarbejderen er informeret om sine opgaver og ansvar i forhold til it-sikkerheden, inden medarbejderen får adgang til Hovedstadens Beredskabs it-systemer og oplysninger.

Stk.2. Medarbejderens personaleansvarlige sikrer, at medarbejderen senest ved ansættelsesforholdets ophør afleverer it-udstyr og lignende, som tilhører Hovedstadens Beredskab, og at der sker inddragelse af medarbejderes adgangsrettigheder i henhold til en procedure, der er fastlagt af it-sikkerhedsfunktionen.

Stk. 3. Medarbejderens personaleansvarlige skal orientere medarbejderen om tavshedspligtens indhold, og at tavshedspligten er gældende, også efter ansættelsesforholdets ophør.

Stk. 4. En leder, som er ansvarlig for en omstrukturering, skal - i god tid - sørge for at sikre, at der etableres de nødvendige elektroniske kommunikationstiltag. Eksempelvis skal kontorpostkasser, sikre postkasser m.m. nedlukkes, hvis en enhed lukkes.

Stk.5. Den lokale ledelse har inden for eget område ansvaret for, at der etableres en tilstrækkelig fysisk sikring af lokaler m.v.

Alle ansatte

§ 16. Alle medarbejderne skal medvirke til at beskytte Hovedstadens Beredskabs person- og værdioplysninger og skal agere i henhold til dette it-sikkerhedsregulativ og de uddybende it-sikkerhedsregler som fastsættes af it- sikkerhedsfunktionen.

Kapitel 3 – Risikostyring

§ 17. It-sikkerhed skal afvejes med hensynet til effektiviteten i opgaveløsningen i direktionsområderne.

Stk.2. Risikovurderinger skal udarbejdes efter it-sikkerhedsfunktionen anvisninger. It-sikkerhedsfunktionen stiller it-værktøjer m.m. til rådighed for direktionsområderne, og rådgiver direktionsområderene om udarbejdelsen af risikovurderinger.

Stk. 3. Risikovurderinger skal udarbejdes inden udgangen af hvert ulige år og ved væsentlige ændringer i risikobilledet.

Stk. 4. It-sikkerhedsfunktionen udarbejder på baggrund af de respektive risikovurderinger en samlet risikovurdering for Hovedstadens Beredskab.

Stk. 5. Den samlede risikovurdering skal udarbejdes inden udgangen af 1. kvartal i hvert ulige år.

Stk. 6. På baggrund af den samlede risikovurdering træffer direktionen beslutning om fastlæggelse af Hovedstadens Beredskabs overordnede it-sikkerhedsniveau.

Stk. 7. Som led i risikovurderingen skal It-sikkerhedsfunktionen sikre, at der til enhver tid findes en ajourført fortegnelse over alle væsentlige informationsaktiver.

Stk. 8. Styring af it-sikkerhedshændelser: Ved konstatering af brud, eller formodning om brud på it- sikkerhedsbestemmelserne eller andre væsentlige it-sikkerhedshændelser, skal den, der konstaterer disse sikre, at It-sikkerhedsfunktionen underrettes herom. Hvis it-sikkerhedshændelsen har relation til et bestemt system, skal systemejeren også underrettes.

Stk. 9. It-beredskabsstyring: It-sikkerhedsfunktionen har ansvaret for, at der foreligger procedurer, som sikrer en tværorganisatorisk styring af It-beredskabet i tilfælde af større it-nedbrud mv. til uddybning af Hovedstadens Beredskabs beredskabsplan.

Kapitel 4 - Ikrafttrædelse og ændringer

HOVEDSTADENS BEREDSKAB

§ 18. It-sikkerhedsregulativet træder i kraft ved godkendelsen i bestyrelsen for Hovedstadens Beredskab.

Godkendt af bestyrelsen for Hovedstadens Beredskab den XX 2016

HOVEDSTADENS BEREDSKAB

Bilag 1 - Definitioner

I it-sikkerhedsregulativet anvendes definitionerne i persondatalovens § 3. Herudover anvendes der følgende - primært organisatoriske - definitioner:

Autorisationsansvarlig

Leder eller bemyndiget medarbejder, som varetager opgaver i forbindelse med bestilling af autorisationer til medarbejderne.

Beredskabet

Hovedstadens Beredskab.

Bestyrelsen

Hovedstadens Beredskabs bestyrelse.

Den driftsansvarlige

Ledende medarbejder i, der har det It-sikkerhedsmæssige ansvar for opbygning og anvendelse af It-driftsmiljø og kommunikationsforbindelser samt for de fysiske sikringsforanstaltninger inden for eget område, og i forhold til Hovedstadens Beredskabs netværk, netværksudstyr og servere m.v., som ejes af Hovedstadens Beredskab. It-sikkerhedsfunktionen kan kontrollere dette samt fastsætte regler for dette.

ISO 27001 og ISO 27002

Internationale standarder for It-sikkerhed. ISO 27001 beskriver kravene til ledelsessystemer for informationssikkerhed(ISMS) , mens ISO 27002 handler om best practice inden for ledelsessystemer til informationssikkerhed.

It-sikkerhedsfunktion

Enhed som efter delegation fra Direktionen varetager Hovedstadens Beredskabs It-sikkerhedsopgaver.

Uddybende It-sikkerhedsregler

It-sikkerhedsregler fastsat af It-sikkerhedsfunktionen til supplering af It-sikkerhedsregulativet med samme gyldighed som It-sikkerhedsregulativet.

It-sikkerhedsleder

Medarbejder i It-sikkerhedsfunktionen, som udfører opgaver af It-sikkerhedsmæssig karakter samt fører tilsyn med, at i t-sikkerhedsarbejdet bliver udført i overensstemmelse med de til enhver tid gældende It-sikkerhedsbestemmelser.

It-sikkerhedsregulativet

HOVEDSTADENS BEREDSKAB

Regulativ for it-sikkerhed i Hovedstadens Beredskab.

It-sikkerhedspolitik

Bestyrelsens vedtagne politik for Hovedstadens Beredskabs It-sikkerhed.

Medarbejdere

Medarbejdere i Hovedstadens Beredskab og virksomheder, der er brugere af Hovedstadens Beredskabs It-systemer, medarbejdere i selvejende og private institutioner og virksomheder, hvor dette er aftalt. Medarbejdere i eksterne virksomheder, der er vikarer eller udfører It-opgaver for Hovedstadens Beredskab, og hvor adgangen til Hovedstadens Beredskabs It- systemer er aftalt.

Persondataloven

Lov nr. 429 af 31. maj 2000, med senere ændringer om behandling af personoplysninger.

Projektejer

En projektejer kan være udpeget til at varetage systemejerens funktion - så længe der ikke er udpeget en systemejer.

Sikkerhedsbekendtgørelsen

Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning med senere ændringer.

System

Systemer som kræver, at direktionsområderne har udpeget en selvstændig systemejer:

- Administrative systemer er systemer, der understøtter administrative opgaver
- Operative systemer er systemer, der understøtter operative opgaver
- Fagsystemer er systemer, der understøtter direktionsoprådernes kerneopgaver

Systemer hvor direktionsområderne - afhængig af systemets placering og vigtighed - kan vælge selv at udpege en systemejer:

- Desktop applikationer er lokal installeret software som understøtter forretningen, men ikke i sig selv indeholder data
- Infrastruktur elementsystemer er systemer, der understøtter kerne It-driften
- En systemplatform er en platform til at bygge andre løsninger på, men som i sig selv ikke har noget forretningsfunktionalltet
- Apps er små applikationer til mobile enheder som smartphones og tablets
- Job- eller batchkørsler er små systemer uden brugergrænseflade, der fx

HOVEDSTADENS BEREDSKAB

trækker data ud om natten og laver beregninger og gemmer data igen
- En systemgrænseflade er et API som andre systemer kan kommunikere med via protokoller
- Et undermodul er en ekstra tilføjet komponent eller et delsystem af systemet
- En hjemmeside/websIte er en løsning der præsentere information via en browser

Systemejer

Medarbejder, der har ansvar for det pågældende It-systems sikkerhedsløsning, opbygning, anvendelse og for beskyttelse af de oplysninger, der indgår i systemet.

System-kontaktperson

Vidensperson der har en mindre systemejerrolle. Ansvar og opgaver er begrænset og afhænger af systemet.

Værdioplysninger

Oplysninger, der har en væsentlig økonomisk eller forvaltningsmæssig betydning for Hovedstadens Beredskab.

Væsentlige informationsaktiver

Aktiver, der indeholder fortrolige eller følsomme personoplysninger eller værdioplysninger.