INFORMATIONSSIKKERHEDS-POLITIK

DAHMLOS
SECURITY

Indhold

1 Formål

Dahmlos Security (i det følgende benævnt "**Dahmlos**"). ønsker at opretholde og løbende udbygge et IT sikkerhedsniveau på højde med de krav, som skitseres i 'Den fællesstatslige standard for informationssikkerhed' (DS 484 basale krav). Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretslige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Dahmlos fremstår troværdig både nationalt og internationalt.

For at fastholde Dahmlos´s troværdighed skal det sikres, at information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som Dahmlos´s mest kritiske ressource. Der lægges derfor vægt på drift sikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at Dahmlos image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

2 Omfang

2.1 Sikkerhedskonceptet omfatter følgende:

- En informationssikkerhedspolitik, der godkendes af direktionen på baggrund af indstilling fra Udvalget for informationssikkerhed.
- En informationssikkerhedshåndbog, der uddyber informationssikkerhedspolitikken, fastlægges af Udvalget for informationssikkerhed.
- Sikkerhedsinstrukser og –procedurer, som formuleres af respektive ejere og linjechefer ud fra krav og retningslinjer i informationssikkerhedshåndbogen
- En 12-trins styringsmodel opbygget efter Plan, Do, Check, Act principperne i BS 7799 Del 2: 2002.

Politikken er gældende for alle Dahmlos informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i Dahmlos eller af samarbejdspartnere. Politikken gælder desuden ved arbejde uden for Dahmlos´s bedriftsområde herunder ved arbejde i udlandet m.v., når dette arbejde foregår under Dahmlos´s ledelsesansvar

Dette inkluderer f.eks. alle data om personale, data om finansielle forhold, alle data som bidrager til administrationen af virksomheden, produktionsdata og anlægsdata samt informationer som er overladt til Dahmlos af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller anden information, som kun er til intern brug.

Informationssikkerhedspolitikken har gyldighed for alle ansatte i Dahmlos og al anvendelse af Dahmlos informationsaktiver.

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 Dahmlos."

Et tilstrækkeligt informationssikkerhedsniveau opnås igennem sikringsforanstaltninger, der sikrer at:

- opnå høj driftsikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

For at fastholde det tilstrækkelige sikkerhedsniveau i Dahmlos skal følgende overholdes:

- Der skal forefindes retningslinjer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af Dahmlos´s drift og daglige arbejde.
- Dahmlos skal igennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke udhuler <organisationens> informationssikkerhedsniveau.
- Dahmlos skal følge op på informationssikkerheden ved fortsat at optimere Dahmlos´s

  ledelsessystem igennem løbende vedligehold og optimering af informationssikkerhedsstrategien, informationssikkerhedspolitikken og de dertilhørende retningslinjer og forretningsgange. Målet er, at sikre en struktureret og kontinuerlig forbedringsproces.

Ovenstående mål skal konkretiseres i Service Level Agreements (SLAs) og kontrakter overfor samarbejdspartnere. Regler og retningslinjer fra informationssikkerhedspolitikken skal løbende indarbejdes i de relevante gældende regler på personalepolitikkens område.

Direktionen ønsker derfor, at Dahmlos´s enheder sammen og aktivt bidrager til at opfylde målene i informationspolitikken, så chefer og medarbejdere har en fast ramme med kendte roller og procedurer i forbindelse med anvendelse af informationer og informationssystemer.

4 Organisationens ansvar

Det delegerede sikkerhedsrelaterede ansvar og den tilhørende myndighed er generisk beskrevet/rollefordelt i Bilag 1 til denne politik.

Sikkerhedsmålsætning:
"Alle medarbejdere har ansvar for informationssikkerheden. De er bekendte med og efterlever vores informationssikkerhedspolitik, informationssikkerhedshåndbog, retningslinjer og forretningsgange i Dahmlos."

Planlægning, implementering og kontrol af informationssikkerhed er defineret af Dahmlos´s edelse. Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet i Dahmlos 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

6.1 Risikovurdering

Informationssikkerheden i Dahmlos er på et niveau, der tilgodeser lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser overfor de aktører, der er forpligtigede til at anvende Dahmlos.

Dahmlos 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.

6.2 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:

A. Korte systemafbrud (timer) vil medføre katastrofale følgevirkninger for forretningen som følge af væsentlige og uoprettelige svigt i målopfyldelse eller brud på love eller aftaler.
B. Langvarige afbrud (dage) vil medføre katastrofale følgevirkninger for forretningen som følge af væsentlige og uoprettelige svigt i målopfyldelse eller brud på love og aftaler.
C. Afbrud vil medføre væsentlig ulempe, men vil ikke i væsentlig grad hindre målopfyldelse eller føre til brud på love eller aftaler.
D. Afbrud medfører mindre ulemper og begrænsede tab eller omkostninger.

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.

Fortrolighed af data inddeles i følgende kategorier:

- **"OFFENTLIG" (OFF)** - Denne klassifikationsgrad anvendes om informationer, der må offentliggøres eller komme til alles kendskab. Omfatter alt hvad der ikke er omfattet af ovenstående som f.eks. alle oplysninger, der er egnet til almen offentliggørelse, åbne dagsordner, kunde og erhvervsinformation.
- **"TIL TJENESTEBRUG" (TTJ)** - Denne klassifikationsgrad anvendes om informationer, der ikke må offentliggøres eller komme til uvedkommendes kendskab. Omfatter oplysninger, som ikke indeholder følsomme eller særlig følsomme personoplysninger eller fortrolige informationer, men kun er tiltænkt internt brug og hvor offentliggørelse kun vil forårsage ubetydelig skade på Dahmlos's image eller økonomi, som f.eks. vagtplaner og interne notater.
- **"FORTROLIGT" (FTR)** - Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse vil kunne forvolde Dahmlos skade. Omfatter oplysninger, som indeholder følsomme eller særlig følsomme personoplysninger eller fortrolige informationer, men kun er tiltænkt internt brug og hvor offentliggørelse kun vil forårsage ubetydelig skade på Dahmlos's image eller økonomi,
- **"HEMMELIGT" (HEM)** - Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse vil kunne forvolde Dahmlos alvorlig skade Omfatter oplysninger, som indeholder følsomme eller særlig følsomme personoplysninger eller fortrolige informationer, men kun er tiltænkt internt brug og hvor offentliggørelse kun vil forårsage ubetydelig skade på Dahmlos's image eller økonomi,

7 Overtrædelse af informationssikkerhedspolitikken

Alle medarbejdere i Dahmlos er forpligtet til at efterleve den til enhver tid gældende informationssikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag. En overtrædelse kan, efter omstændighederne, medfører sanktioner. Hvis en medarbejder er vidende om, at Dahmlos's informationssikkerhed overtrædes, skal det meddeles til informationssikkerhedskoordinatoren eller direktøren hurtigst muligt.

8 Bilag

8.1 Bilag 1 Organisation og ansvar

Organisationen overholder alle lovkrav, og hvor det er muligt og relevant, løfter vi anvendelse af informationer og informationssystemer til et højere niveau end lovens krav.

Udvalget for informationssikkerhed

Udvalget består af:

- Administrationschefen (formand for udvalget)
- Dahmlos´s IT-sikkerhedskoordinator (sekretær for udvalget),
- samt repræsentanter fra relevante aktører/interessenter i Dahmlos
- Kontorchefen for ***
- En repræsentant for *** på ledelsesniveau
- En – eller flere – repræsentanter for brugerfunktionerne

Udvalget er normgivende og fastsætter på grundlag af den vedtagne informationssikkerhedspolitik de principper/retningslinjer, der skal sikre målopfyldelsen. Udvalget behandler alle sikkerheds-spørgsmål af principiel karakter.

Udvalget foretager en årlig vurdering af informationssikkerhedspolitikken og de tilknyttede sikker-hedsretningslinjer – herunder at disse lever op til de eksterne forpligtelser udtrykt i lovgivning og kontrakter/aftaler. Udvalget vurderer samtidigt, om der er behov for fornyet risikovurdering/ kon-sekvensanalyse.

Udvalget kan ad hoc lade sig supplere med faglig assistance fra IT-Sikkerhedsfunktionen

8.2 IT Sikkerhedsfunktionen

På grund af Dahmlos store grad af outsourcing af drift og support til Koncern-IT og derigennem ofte til større, professionelle samarbejdspartnere er det ikke hensigtsmæssigt at operere med en større særskilt/funktionsadskilt IT Sikkerhedsafdeling/-funktion. I stedet løses opgaverne primært ved:

- at tage hensyn hertil i aftalegrundlag med samarbejdspartnere, f.eks. ved at pålægge samar-bejdspartnere at foretage forskellige former for kontrol og opfølgning og rapportere herom til Udvalget for informationssikkerhed
- at iværksætte egne revisionsopgaver og/eller sikkerhedsundersøgelser i det omfang Udvalget for informationssikkerhed finder det fornødent.

8.2.1 Funktionen har ansvar for:

- At udarbejde og vedligeholde sikkerhedshåndbogen indeholdende sikkerhedsprincipper for informationsanvendelsen – evt. med ekstern assistance
- At udarbejde relevante sikkerhedskrav, der operationaliserer informationssikkerhedspolitik-ken – evt. med ekstern assistance

- At foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende
- At behandle dispensationsansøgninger for begrundede afvigelser i forhold til retningslinjerne og rapportere disse til Udvalget for informationssikkerhed
- At holde sig ajour med den generelle udvikling på det sikkerhedsmæssige område
- At koordinere relevante initiativer med de øvrige aktører i koncernsamarbejdet

8.3 Linieledelsen

Den enkelte chef i linjen – herunder direktionen - har ansvar for:

- At informationssikkerhedspolitikken og de regler, der er relevante for hans/hendes ansvarsområde, er kendte og efterleves
- At medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer og at disse efterleves
- At der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for Dahmlos´s/kontorets område
- At der ved installation af nye systemer gennemføres en forudgående sikkerheds-/risikovurdering
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Resultatet rapporteres til IT Sikkerhedsfunktionen
- At retningslinjerne for ansættelse, introduktion, løbende vurdering, funktionsskift og afvikling af medarbejdere overholde

8.4 Systemejere

8.4.1 System ejere har ansvar for:

- at der udarbejdes en kravspecifikation som tager eksplicit hensyn til sikkerhedsmæssige forhold forud for enhver systemudvikling/ –ændring/-anskaffelse /-opdatering – evt. med ekstern assistance
- at der udarbejdes en risikovurdering i h.t. kravene hertil
- at Change Management retningslinjerne følges ved enhver ændring af systemet
- at der ved idriftsætning af systemet foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- at autorisere adgangen til systemet i h.t. retningslinjerne herfor
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinjerne og konkret i regler og procedurer for systemadministrationen.

8.5 Dataejere

8.5.1 Dataejeren har ansvar for:

- at der udarbejdes en risikovurdering i h.t. kravene hertil – for systemtilknyttede data i samarbejde med systemejeren
- at der inden indrapportering af data i systemer foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- at autorisere adgangen til data i h.t. retningslinjerne herfor samt at sikre, at enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, som har udført aktiviteten
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinjerne og konkret i regler og procedurer for dataadministrationen.

8.6 Ejere af fysiske aktiver

Alle fysiske aktiver får udpeget/ tildelt en ejer.

Såfremt aktivet er omfattet af en aftale om Holsting, tages der hensyn hertil i aftalegrundlaget med samarbejdspartneren, f.eks. ved at pålægge samarbejdspartneren at foretage forskellige former for kontrol og opfølgning og rapportere herom.

8.6.1 Ejeren af det fysiske aktiv har ansvar for:

- at der udarbejdes en kravspecifikation ved placering, indretning, forandring m.v. som tager eksplicit hensyn til sikkerhedsmæssige forhold – evt. med ekstern assistance
- at der udarbejdes en risikovurdering i h.t. kravene hertil
- at der ved ibrugtagning af lokaler/udstyr foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- at autorisere adgangen til lokalerne/ udstyret i h.t. retningslinjerne herfor
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinjerne og konkret i regler og procedurer for fysisk sikkerhed og adgangsadministrationen.

8.7 Medarbejdere

Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisationsplaner. Hvor dette ikke er praktisk eller økonomisk hensigtsmæssigt, skal kompenserende kontroller indføres.

8.7.1 Den enkelte medarbejder har ansvar for:

- At overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver
- At rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste chef og til IT-Sikkerhedsfunktionen

8.8 Samarbejdspartnere

Samarbejdspartnere – herunder KIT - bærer pga. det valgte koncept en meget væsentlig del af ansvaret for at det valgte sikkerhedsniveau etableres og opretholdes.

8.8.1 Samarbejdspartnerne har ansvar for:

- At Dahmlos informationssikkerhedspolitik og de regler, der er relevante for deres ansvarsområde, er kendte og efterleves – mest hensigtsmæssigt ved at egne sikkerhedspolitikker og regler til enhver tid afspejler krav fra Dahmlos
- At medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer, herunder tiltrædelseserklæringen
- At der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for samarbejdspartnerens område
- At der ved installation af nye og modifikation af eksisterende interne systemer og komponenter med påvirkningsmulighed til Dahmlos informationsaktiver gennemføres en forudgående risiko-/sikkerhedsvurdering
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Hændelsen og resultatet rapporteres via egen sikkerhedsorganisation til Dahmlos IT Sikkerhedsfunktion

8.9 Afvigelser

Hvis der opstår situationer, hvor kravene i informationssikkerhedspolitikken ikke kan efterleves, skal der skriftligt anmodes om dispensation af Dahmlos´s 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 1. december 2017., og træder i kraft den 1. januar 2018.

10 Dokumentinformation

Dokumenthistorik/version:

Revision	Ændringsbeskrivelse	Dato/Forfatter