DS 484:2005

Standard for informationssikkerhed

-Korte uddrag fra DS484

Informationssikkerhedsstrategi

- Ledelsen skal godkende en skriftlig informationssikkerhedspolitik, som skal offentliggøres og kommunikeres til alle relevante interessenter, herunder alle virksomhedens medarbejdere.
- Politikken skal indeholde følgende punkter:
  - En definition af virksomhedens informationssikkerhed, dennes formål, omfang
  - En understregning af ledelsens støtte og engagement
  - Ledelsens overordnede sikkerhedskrav
  - En kort beskrivelse af de generelle krav til:
    - overholdelse af udefrakommende forpligtelser og krav, herunder relevant lovgivning
    - uddannelse, træning og bevidstgørelse
    - beredskabsplaner, herunder den maksimalt acceptable utilgængelighed for kritiske forretningssystemer
    - konsekvenser ved overtrædelse af politikken
  - En beskrivelse af ansvarsplaceringen
  - Referencer til øvrig sikkerhedsdokumentation

Informationssikkerhedsstrategi(cont)

- Løbende vedligeholdelse
  - Informationssikkerhedsstrategien skal revurderes med planlagte intervaller
  - Baset på tilbagemeldinger fra interessenter
  - Resultat af uafhængige gennemgange
  - Ændringer i trussels landskabet
  - Nye anbefalinger

- Implementeringsretningslinjer
  - Informationssikkerhedsstrategien skal have udpeget en ejer, som er ansvarlig for udviklingen, vedligeholdelsen og revurderingen af sikkerhedsstrategien

Organisering af informationssikkerhed

- Ansvarsplacering
  - Der skal udpeges en ansvarlig “ejer”, og ejerskabet skal dokumenteres.
  - Den ansvarlige skal verificere at opgaven bliver udført korrekt.

Organisering af informationssikkerhed

- Godkendelsesprocedure ved anskaffelser
  - Der skal være en godkendelsesprocedure for anskaffelse og installation.
  - Ved større eller forretningskritiske nyanskaffelser skal det verificeres, at de ikke kompromitterer det fastlagte sikkerhedsniveau.
  - Brugen af personligt Informationsbehandlingsudstyr

Organisering af informationssikkerhed

- Tavshedserklæringer
  - Definition af de informationer, tavshedserklæringen omfatter
  - den fastlagte løbetid
  - underskriverens adgangs- og brugsrettigheder
  - virksomhedens ret til overvågning af og opfølgning på overholdelse af tavshedspligten
  - sanktioner ved brud på tavshedspligten.

Eksterne samarbejdspartnere

- Eksternts samarbejde
  - Adgang(fysisk, logisk)
- Kunder
  - Beskyttelsesprocedurer
  - begrænsninger vedrørende kopiering og videregivelse af oplysninger
  - brugerautorisation og rettighedstildeling
  - præcisering af at enhver uautoriseret adgang er forbudt

Eksterne samarbejdspartnere

- Samarbejdsaftaler
  - Adgang(fysisk, logisk)
  - procedurer for konstatering af eventuelle sikkerhedsbrud
  - restriktioner vedrørende kopiering og videregivelse
  - rapporteringsomfang, -struktur og –format
  - beredskabsplaner, herunder krav til maksimal retableringstid

Styring af informationsrelaterede aktive

- Alle informationsaktiver skal identificeres, og der skal etableres en ajourført fortegnelse over alle væsentlige aktiver.
- Hvert informationsrelateret aktiv skal have udpeget en ejer.

- Accepteret brug af aktiver
  - Der skal foreligge retningslinjer for accepteret brug af virksomhedens informationsaktiver.
    - brugen af elektronisk post og internet
    - brugen af mobilt udstyr, specielt uden for virksomheden.

Styring af informationsrelaterede aktive

- Mærkning og håndtering af informationer og data
  - Der skal være en procedure for mærkning og håndtering af virksomhedens informationer og data.(Fysisk & elektronisk)
  - Ved samarbejde med andre virksomheder skal begge parters mærkningsregler være aftalt
  - Hvis det ikke er muligt at anvende fysisk mærkning, må andre mærkningsteknikker anvendes, fx via brugervejled-ninger eller som en tekst på et skærmbillede.

Medarbejdersikkerhed

- Sikkerhedsprocedure før ansættelse
  - At sikre at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle
  - Sikkerhedsansvar skal være fastlagt før ansættelsen igennem stillingsbeskrivelse og i ansættelseskontrakten.
  - Der skal udføres en efterprøvning af ansøgere, før en aftale indgås
    - CV
    - Identitetskontrol
    - (Straffeattest)

Medarbejdersikkerhed

- Ansættelsesforholdet
  - Virksomhedens medarbejdere skal løbende uddannes i virksomhedens sikkerhedspolitik
  - ansvar ifølge dansk lovgivning
  - virksomhedens regler om sanktioner

Medarbejdersikkerhed

- Ansættelsens ophør
  - Ansvaret for fratrædelsesproceduren skal være klart defineret og placeret
  - Medarbejderen skal aflevere alle udleverede virksomhedsaktiver
  - I de tilfælde, hvor medarbejderen er i besiddelse af viden, der er vigtig for virksomheden, skal det sikres, at denne vi-den dokumenteres og overføres til virksomheden.

Fysisk sikkerhed

- Fysisk afgrænsning
- Fysisk adgangskontrol
- Beskyttelse mod eksterne trusler
- Områder til af- og pålæsning med offentlig adgang
  - Placering af udstyr
  - Forsyningssikkerhed
  - Sikring af kabler
  - Udstyrs og anlægs vedligeholdelse

Medarbejdersikkerhed

- Ansættelsens ophør
  - Ansvaret for fratrædelsesproceduren skal være klart defineret og placeret
  - Medarbejderen skal aflevere alle udleverede virksomhedsaktiver
  - I de tilfælde, hvor medarbejderen er i besiddelse af viden, der er vigtig for virksomheden, skal det sikres, at denne vi-den dokumenteres og overføres til virksomheden.

Styring af netværk og drift

- Ændringsstyring
  - entydig identifikation og registrering af væsentlige ændringer
  - krav til planlægning og afprøvning af ændringer
  - vurdering af ændringens konsekvenser
  - en informationsformidlingsprocedure
  - nødprocedure ved fejlslagne ændringer
  - logningsprocedure

Styring af netværk og drift

- Funktionsadskillelse
  - Adskillelse mellem udvikling, test og drift
  - Retningslinjer for overførsel af forretningskritiske systemer fra udviklings- og testmiljøet til driftsmiljøet
  - Følsomme/fortrolige data må ikke benyttes i udviklings- og testmiljøet, medmindre adgangskontrolforanstaltnin-gerne er lige så restriktive som i driftsmiljøet

Styring af netværk og drift

- Styring af driftsmiljøet
  - Ressourceforbruget skal overvåges og tilpasses
  - Godkendelse af nye eller ændrede systemer
  - Skadevoldende programmer og mobil kode
  - Et formelt forbud mod anvendelse af uautoriserede systemer

Styring af netværk og drift

- Sikkerhedskopiering
  - Der skal tages sikkerhedskopier af alle virksomhedens væsentlige informationsaktiver
  - Behovet for sikkerhedskopiering skal være fastlagt
  - Omfanget og hyppigheden skal afspejle de forretningsmæssige behov
  - Sikkerhedskopier skal afprøves regelmæssig
  - Gendannelsesprocedurer skal ligeledes afprøves regelmæssigt

Netværkssikkerhed

- Netværket
  - Funktionsadskillelse
  - de fornødne lognings- og overvågningsprocedurer skal være etableret
  - Netværkstjenester
    - Adgangskontrol
    - AAA

Informationsudveksling

- retningslinjer og procedurer
- Fysiske datamediers sikkerhed under transport
- Elektronisk post og dokumentudveksling
  - beskyttelse mod uautoriseret adgang
  - forholdsregler mod ukorrekt adressering og fejlrutning
  - tilstrækkelig kapacitet
  - Retningslinjer for medarbejdernes brug af elektronisk post
  - elektronisk post, der anvendes til at indgå bindende aftaler, skal have beskyttelsesforanstaltninger

Logning og overvågning

- Informationsbehandlingssystemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres med:
  - Brugeridentifikation
  - dato og klokkeslæt
  - arbejdsstationens identitet
  - registrering af systemadgange og forsøg herpå
  - ændringer i systemkonfigurationen
  - benyttede netværk og protokoller
  - alarmer fra adgangskontrolsystemet
  - aktivering og deaktivering af beskyttelsessystemer, fx antivirus og indbrudsalarmer.

Logning og overvågning

- Overvågning af systemanvendelse
  - Brugeridentifikation
  - dato og klokkeslæt
  - Hendelsestype
  - uautoriserede adgangsforsøg
- Beskyttelse af log-oplysninger mod:
  - enhver form for ændringer af indholdet
  - sletninger og ændringer af logfiler
  - tekniske fejl, eksempelvis overskrivninger

Adgangsstyring

- Der skal være udarbejdet retningslinier for adgangstyring.
- Udviklet forretningsgange til styring af adgangsrettigheder(tildeling/ændring)
- Adgangskode politik
- Opdeling af netværk
  - i store netværk kan det være nødvendigt at opdele dem efter adskilte tjenester
- Automatiske afbrydelser

Styring af sikkerhedshændelser

- Sikkerhedshændelser skal rapporteres til ledelsen hurtigst muligt.
- Håndtering af sikkerhedsbrud og forbedringer

Opgave

- Opbygge et netværk for Birksund kommune
  - Udarbejde design plan
  - Opgaveløser, ansvar
  - Godkedelse
  - Tidsplan
  - Sikkerheds Aspekter