It-sikkerhedspolitik for Strømmen Vandværk

Introduktion

Denne it-sikkerhedspolitik, som er besluttet af bestyrelsen, udgør den overordnede ramme for at opretholde it-sikkerheden hos Strømmen Vandværk. Hermed ønsker vandværket at demonstrere sin seriøse holdning til at skabe sikkerhed for persondata, systemer og andre it-aktiver

Hensigten er at lægge et fundament, så kritiske og fortrolige informationer og systemer kan bevare deres fortrolighed, integritet og tilgængelighed.

Der bliver fokuseret på de vigtigste krav i EU's generelle persondataforordning samt på relevante krav i de internationale it-sikkerhedsstandarder ISO 27001 og 27002.

Formål

Idet brugen af it anses for at være en meget vigtig forudsætning for vandværkets eksistens, vil det være nødvendigt at sikre vandværkets it-ressourcer (data, software, hardware og kommunikationsforbindelser).

Derfor vil vi etablere og vedligeholde en afbalanceret it-sikkerhed, som i denne sammenhæng omfatter alle nødvendige organisatoriske, fysiske og tekniske sikkerhedsforanstaltninger.

It-ressourcerne skal med andre ord beskyttes mod misbrug, manipulation, ødelæggelse og tab, samt mod at blive fejlbehæftede. Beskyttelsen skal virke mod alle former for trusler, interne eller eksterne, hændelige eller bevidste.

Ledelsens udmelding om de overordnede mål og principper

Strømmen Vandværk ønsker at opnå:

- Fortrolighed, integritet og tilgængelighed af persondata i overensstemmelse med kravene i EU's persondataforordning
- Høj driftssikkerhed og minimeret risiko for større nedbrud og tab af data
- Opretholdelse af et image som en virksomhed, der demonstrerer kvalitet og sammenhæng i brugen af it

It-sikkerhedspolitikken skal danne grundlag for at forebygge og begrænse skader til en, for vandværket, kendt og accepteret størrelse samt sikre fortsat it-drift efter et sikkerhedsbrud – inden for en nærmere defineret tidshorisont.

Vigtige grundprincipper for sikkerhedsarbejdet

Funktionsadskillelse

Det er ofte vanskeligt at opretholde funktionsadskillelse, men et fravalg af dette princip vil være at sætte it-sikkerheden i fare. Derfor vil vi som minimum kræve (ligesom det er tilfældet ved adgang til kassen/bankbeholdningen), at en anden person (bestyrelsesmedlem, næstformand eller formand) medvirker.

Hvis dette ikke kan lade sig gøre i praksis, fordi ingen bestyrelsesmedlemmer har it-kompetencer, bruges følgende model:

Den daglige leder beslutter hvem, der skal have adgang til hvilke ressourcer og hvornår. En udpeget it-ansvarlige, der kan være en medarbejder med it- eller it-sikkerhedsviden – eller en ekstern it-konsulent, installerer herefter rettigheder/begrænsninger i overensstemmelse med den daglige leders beslutninger. Når installationen er afsluttet, sender den it-ansvarlige en mail til bestyrelsen eller et medlem af bestyrelsen om, hvad han har foretaget sig. Så kan bestyrelsen efterfølgende orientere sig hos den daglige leder om formålet med den gennemførte ændring. Ændringen og begrundelsen tages med i referatet til næste bestyrelsesmøde.

Se eksempel 1-2 i eksempelsamlingen.

Sikkerhedsforanstaltninger

Den daglige leder beslutter omfang og styrke af de sikkerhedsforanstaltninger, som det findes nødvendigt at installere. Den it-ansvarlige installerer de tekniske foranstaltninger, mens den daglige leder står for formuleringen af de administrative foranstaltninger (evt. retningslinjer og instrukser). Det er ikke acceptabelt at anvende privat it-udstyr til at udføre arbejde for vandværket eller til at koble sig op på vandværkets systemer.

Styring af sikkerhedshændelser

Vi vil løbende sikre en vurdering af eventuelle hændelser, der kan true sikkerheden, så risikobilledet kan opdateres ved gennemgang af såvel kendte som nye trusler og sårbarheder, og eventuelle nye tiltag kan indføres. Den daglige leder rapporterer overordnet til bestyrelsen om de hændelser, der måtte være sket, og informerer om det opdaterede risikobillede, når væsentlige ændringer er indtruffet.

Se eksempel 3-4 i eksempelsamlingen

Dokumentation

Der skal udarbejdes skriftlige procedurer for alle væsentlige sikkerhedsaktiviteter, og det skal kunne dokumenteres, at de har været gennemført.

Se eksempel 5 i eksempelsamling

Sikkerhed i forbindelse med outsourcing

Leverandører, der helt eller delvist står for drift af vandværkets systemer, skal overholde vandværkets krav til it-sikkerhed. De skal også sikre, at der er mulighed for løbende at kunne kontrollere og følge op på deres sikringsforanstaltninger.

I forbindelse med at der bliver indgået en kontrakt om outsourcing, skal der udarbejdes en databehandleraftale, der i detaljer beskriver de sikkerhedskrav, som leverandøren skal leve op til. Leverandører skal én gang årligt stille en revisionserklæring om, at it-sikkerheden er i orden i henhold til revisionsstandard 3411, type B.

Se eksempel 6 i eksempelsamlingen

De konkrete mål

Det regelsæt, der styres efter, er baseret på den internationale standard ISO/IEC 27000-serie. Herved opnås en direkte kobling fra sikkerhedspolitikken til de underliggende retningslinjer og instrukser, der peges på i standarderne.

Hovedpunkterne i regelsættet/retningslinjerne er:

1. Overordnede retningslinjer (informationssikkerhedspolitikker)

Vi har brug for et sikkerhedsniveau afstemt efter omkostningerne og de forretningsmæssige behov. Ledelsen vil derfor sammenfatte sine overordnede krav i en it-sikkerhedspolitik.

2. Organisering af sikkerhedsarbejdet

Den daglige leder er ansvarlig for den overordnede it-sikkerhed samt for udformning af en it-sikkerhedspolitik. Samtidig er det den daglige leder, der beslutter hvem, der skal have adgang til hvilke it-ressourcer og hvornår. En udpeget it-ansvarlig installerer rettigheder/begrænsninger i overensstemmelse med disse beslutninger

Styringen sker i en proces, hvor der gennemføres risikovurdering, målfastlæggelse, planlægning, gennemførelse, overvågning og opfølgning – i en tilbagevendende cyklus.

3. Medarbejdersikkerhed

Der skal informeres og stilles krav om it-sikkerheden til medarbejderne før og under ansættelsen samt efter ansættelsens ophør eller ændring. Specielt vil der være særlige sikkerhedskrav forbundet med arbejde i hjemmet eller ved andet arbejde uden for kontoret (på privat it-udstyr eller på firmaejet udstyr).

4. Styring af aktiver

Vandværkets it-aktiver (software, data, eller fysiske enheder) skal identificeres og registreres, så det er muligt at definere, hvilke der er kritiske, vigtige eller sensitive for vandværket.

Hertil er det nødvendigt at udpege en ejer for hvert aktiv, således at denne har ansvaret for korrekt håndtering af det enkelte aktiv.

Klassifikation skal sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.

I forhold til mediehåndtering skal det forhindres, at uautoriseret offentliggørelse, ændring, fjernelse eller ødelæggelse af information lagret på medier (inkl. papirmediet) finder sted.

Bortskaffelse af medier: Medier, som indeholder fortrolig information, skal lagres og bortskaffes forsvarligt, for eksempel ved ødelæggelse, makulering, eller sletning af data.

Transport af fysiske medier: Medier med fortrolig information skal beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport. Dette gælder også bærbare computere, tablets og mobiltelefoner.

Se eksempel 7 i eksempelsamlingen.

5. Adgangsstyring

Der skal gennemføres styring af den generelle adgang til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav.

Der skal desuden kunne gennemføres begrænsninger i adgangen til specifikke systemer og data ved at definere brugerroller og ved at tildele privilegerede adgangsrettigheder.

Procedurer for brugerregistrering og -afmelding samt for tildeling af brugeradgang.

System- og dataejere bør med jævne mellemrum gennemgå tildelte rettigheder for at konstatere, om de fortsat er gældende.

Der skal gøres brug af sikre adgangskoder/passwords samt sikker log-on; begge dele beskrives i særskilt procedure.

Se eksempel 8 i eksempelsamlingen.

6. Kryptering

Der skal tages stilling til i hvor høj grad, der skal gøres brug af kryptering af såvel lagrede data som data under transmission.

Behovet for at anvende kryptering baseres på en risikovurdering. Ansvaret for det praktiske arbejde samt for nøgleadministration vil i givet fald blive beskrevet i procedurer.

7. Fysisk sikring og miljøsikring

Kritisk it-udstyr skal være anbragt i sikre områder beskyttet af de nødvendige fysiske barrierer, adgangskontroller samt alarmer for at minimere risikoen for uheld og ulykker. Endvidere skal kritisk udstyr sikres mod forsyningssvigt (blandt andet el-, vand- og teleforbindelser).

8. Driftssikkerhed

Driftssikkerhed drejer sig om at opnå korrekt og sikker drift af faciliteterne, der behandler information.

Heri indgår dokumentering af procedurer for drift og softwareinstallation samt styring af de ændringer, der løbende forekommer og som kan påvirke informationssikkerheden.

Endvidere skal der indføres sikkerhedsforanstaltninger, der kan opdage og forhindre sikkerhedsbrud forårsaget af malware samt efterfølgende sikre genstart af driftssystemerne.

For at sikre at al væsentlig information, software og systemer kan genskabes efter et nedbrud/sikkerhedsbrud, skal der foreligge en backupplan, som følges i praksis. Endelig skal der, hvor det er muligt, gennemføres løbende logning og overvågning af brugeraktivitet med henblik på, at kunne dokumentere hændelsesforløbet i forbindelse med et sikkerhedsbrud.

Desuden skal der gennemføres en styring af tekniske sårbarheder, for at forhindre, at disse udnyttes i skadeligt øjemed.

Se eksempel 9-10 i eksempelsamlingen.

9. Kommunikationssikkerhed

Vandværkets interne netværk skal styres og overvåges samt have installeret passende sikkerhedsforanstaltninger. Forekommer der flere forskellige brugergrupper på netværket, bør dette opdeles, så grupperne af brugere bliver adskilt.

Ved overførsel af informationer til eksterne samarbejdspartnere eller forbrugere skal der gøres særlige overvejelser om hvilket sikkerhedsniveau, der skal benyttes.

Blandt andet kan der blive tale om at etablere særlige aftaler om fortrolighed og hemmeligholdelse samt brug af kryptering, når det drejer sig om data af højeste klassifikation.

10. Anskaffelse, udvikling og vedligeholdelse af systemer

Sikkerhed skal indgå som en integreret del af de systemer, der understøtter virksomhedens daglige drift. Det vil sige, at krav til sikkerhed skal specificeres i forbindelse med anskaffelse, udvikling og vedligeholdelse af systemerne. Sikkerhedskravene skal være begrundede, aftalte og dokumenterede. Formulering af sikkerhedskravene bør ske på basis af en risikovurdering.

Særlige overvejelser skal ske vedrørende brugen af persondata i forbindelse med testforløb.

11. Leverandørforhold

Outsourcing skal være baseret på en kontrakt samt en databehandleraftale, som sikrer, at virksomhedens it-sikkerhedspolitik ikke skades. Aftalen skal indeholde principielle og konkrete krav til it-sikkerheden hos leverandøren, samt til hvordan kommunikationen mellem vandværket og leverandøren skal sikres. Der skal leveres revisorerklæringer om it-sikkerheden og gives mulighed for inspektion af it-sikkerheden i særlige situationer (kontraktligt aftalt).

It-udstyr, der kobler sig på virksomhedens systemer via eksterne netværk, skal overholde virksomhedens sikkerhedspolitik og –retningslinjer. Dette gælder også medarbejderes brug af private computere, tablets og mobiler, hvis de har opnået tilladelse til opkobling.

Se eksempel 11 i eksempelsamlingen.

12. Styring af brud på informationssikkerhed

Styring af brud på informationssikkerhed betegnes også ”Information Security Incident Management”. Det skal sikre en ensartet og effektiv metode til at styre sikkerhedsbrud – herunder kommunikation om sikkerhedstruende hændelser og svagheder.

Ting, der bør beskrives, er blandt andet: ansvar og procedurer, hændelsesrapportering, rapportering af svagheder, vurdering af hændelser, håndtering af sikkerhedsbrud, opsamling af erfaring fra sikkerhedsbrud, samt indsamling af beviser (der i givet fald kan bruges i en retslig tvist).

Se eksempel 12 i eksempelsamlingen.

13. Beredskabsstyring m.m.

Beredskabsstyring handler om ”sammenhæng i informationssikkerhed”. Det skal gerne forankres i vandværkets generelle procedurer for nød-, beredskabs- og reetableringsstyring. Vandværket

skal indføre beredskabsstyring som en løbende opgave med det formål at begrænse konsekvenserne ved katastrofer, sikkerhedsbrud og mistet tilgængelighed.

Det indebærer specifikation af krav til beredskab samt af beredskabsplaner. Beredskabsstyringen skal indeholde procedurer, der identificerer og reducerer risici, begrænser konsekvenserne ved skadelige hændelser og sikrer rettidig reetablering af kritiske forretningsprocesser.

En nødplan skal sikre muligheden for hurtigst muligt at reetablere normal drift efter en større katastrofe (brandskade, vandskade, mv.)

For at omgå (mindre) tekniske problemer, kan det overvejes at have ekstra udstyr parat.

Se eksempel 13 i eksempelsamlingen

14. Overensstemmelse med lovbestemte og kontraktlige krav (herunder dataforordningen)

Vi vil forhindre, at der sker brud på relevante sikkerhedskrav i lovgivning, bekendtgørelser, cirkulærer og myndighedsforordninger i øvrigt, samt i indgåede kontraktlige forpligtelser.

Særligt skal der redegøres for, hvordan de konkrete/skærpede sikkerhedskrav, der stilles i den nye EU persondataforordning, skal håndteres.

Revisionshistorik

Version	Note Redigeret af		Dato
V1.0	Første udkast til skabelon	13. marts 2017	Per Rhein
V1.1	Skabelon tilrettet Strømmen Vandværk	5. april 2018	Hans Lyng