It-sikkerhedspolitik for Uhre Windpower 3 I/S

Introduktion

Denne it-sikkerhedspolitik, som er besluttet af bestyrelsen, udgør den overordnede ramme for at opretholde it-sikkerheden hos Uhre Windpower 3 I/S. Hermed ønsker Vindmøllelauget 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, idet der bliver fokuseret på de vigtigste krav i EU's generelle persondataforordning.

Formål

Idet brugen af it anses for at være en vigtig forudsætning for vindmøllelaugets eksistens, vil det være nødvendigt at sikre vindmøllelaugets 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.

Bestyrelsens udmelding om de overordnede mål og principper

Uhre Vindmøllelaug I/S 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

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

Vigtige grundprincipper for sikkerhedsarbejdet

Funktionsadskillelse

Bestyrelsen beslutter hvem, der skal have adgang til hvilke ressourcer og hvornår. En udpeget it-ansvarlige, der kan være et bestyrelsesmedlem med it- eller it-sikkerhedsviden – eller en ekstern it-konsulent, installerer herefter rettigheder/begrænsninger i overensstemmelse med bestyrelsens. Når installationen er afsluttet, sender den it-ansvarlige en mail til bestyrelsen, om hvad han har

foretaget sig og hvad formålet med den gennemførte ændring var. Ændringen og begrundelsen tages med i referatet til næste bestyrelsesmøde.

Sikkerhedsforanstaltninger

Bestyrelsen beslutter omfang og styrke af de sikkerhedsforanstaltninger, som det findes nødvendigt at installere. Den it-ansvarlige installerer de tekniske foranstaltninger (antivirus, firewall, beskyttelse mod malware etc.), mens bestyrelsen 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 vindmøllelauget eller til at koble sig op på vindmøllelaugets 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.

Dokumentation

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

Hovedpunkterne i regelsættet/retningslinjerne er:

1. Overordnede retningslinjer (informationssikkerhedspolitikker)

Vindmøllelauget har brug for et sikkerhedsniveau afstemt efter omkostningerne og vindmøllelaugets beskedne brug af it.

2. Organisering af sikkerhedsarbejdet

Den daglige leder er ansvarlig for den overordnede it-sikkerhed samt for implementering af den af bestyrelsen vedtagne it-sikkerhedspolitik. Det er bestyrelsen, 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.

3. Styring af aktiver

Vindmøllelaugets 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 vindmøllelauget.

Hertil er det nødvendigt at udpege en ansvarlig 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.

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

4. Adgangsstyring

Der skal gennemføres styring af den generelle adgang til vindmøllelaugets systemer og informationer med udgangspunkt i de lovgivningsbetingede krav.

Der skal gøres brug af sikre adgangskoder/passwords samt sikker log-on. Password skal skiftes for hver 3 måned.

5. Fysisk sikring

Fysiske medier med persondata skal være anbragt i aflåste skabe. Vores it-udstyr er låst inde på et kontor med kodelås på.

6. Driftssikkerhed

Driftssikkerhed drejer sig om at opnå korrekt og sikker drift i relation til behandling af persondata. For at sikre at al væsentlig information kan genskabes efter et nedbrud/sikkerhedsbrud, skal der foreligge en backupplan, som følges i praksis.

7. 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, opsamling af erfaring fra sikkerhedsbrud, samt indsamling af beviser (der i givet fald kan bruges i en retslig tvist).

8. 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	Dato	Redigeret af
V1.2	It-sikkerhedspolitik	29. marts 20202	Per Bjerke Hansen