Politik for Datasikkerhed

i Billund Vand & Energi A/S

Oktober 2015

Billund Vand & Energi A/S - Grindsted Landevej 40 - DK-7200 Grindsted
Tlf.: 76 50 27 00·Email: post@billundvand.dk·www.billundvand.dk

Indhold

Bilag

Bilag 1 Lovgivning, der er relevant for datasikkerhedspolitikken.

Bilag 2 Uddybende beskrivelse af ansvarsområder.

1 Indledning

Dette dokument beskriver Billund Vand & Energi A/S' politik om datasikkerhed. Datasikkerhedspolitikken er ligeledes gældende for Billund Vand & Energi A/S' datterselskaber; Billund Drikkevand A/S, Billund Spildevand og Billund Energi A/S,

1.1 Værdier

Billund Vand & Energi A/S bygger på følgende værdisæt:

- Vi tør gå foran
- Vi tager ansvar
- Vi er engagerede
- Vi udviser ordentlighed
- Vi yder service

1.2 Data

Datasikkerhed omfatter følgende væsentlige kategorier:

- Data skal være *tilgængelige* – alle skal have adgang til relevante data
- Data skal have den nødvendige *integritet* – indholdet af vores data skal være korrekte og fuldstændige
- Data skal være *fortrolige* – nogle data skal overholde lovmæssige minimumskrev til sikkerhed af fortrolighed

Billund Vand & Energi A/S behandler data vedr. kunder, personale, drift, anlæg, udvikling og formidling. Det er af afgørende betydning, at den nødvendige datasikkerhed opretholdes.

Nærværende datasikkerhedspolitik omfatter både data, som benyttes og lagres elektronisk og data, som benyttes og lagres manuelt (eks. på papir)

2 Formål

Formålet med Billund Vand & Energi A/S datasikkerhedspolitik er at sikre, at data er tilgængelige, korrekte og ikke kommer til uvedkommende personers kendskab.

Sikringen skal rettes imod alle former for trusler, som for eksempel:

- Tekniske fejl og nedbrud
- Menneskelige fejl og uheld herunder hændelige og uagtsomme
- Bevidst skadevoldende handlinger så som misbrug, berigelse, bedrageri osv.

Billund Vand & Energi A/S skal sikre, at konsekvenserne af et sikkerhedsbrud reduceres til et for Billund Vand & Energi A/S acceptabelt niveau:

- Billund Vand & Energi A/S skal sikre, at kunderne altid kan føle sig trygge ved at overlade deres data til virksomheden og dennes samarbejdspartnere
- Billund Vand & Energi A/S skal sikre medarbejdernes tryghed ved at behandle personfølsomme oplysninger fortroligt
- Billund Vand & Energi A/S skal sikre medarbejdernes arbejdsvilkår ved at såvel relevante værktøjer, herunder computere mv. som relevante data er tilgængelige

Datasikkerheden skal altid leve op til følgende krav:

- Billund Vand & Energi A/S skal leve op til de sikkerhedsmæssige krav, der udspringer af lovgivningen. Her har specielt persondataloven betydning som følge af Billund Vand & Energi A/S opgaver med behandling af personhenførbare/personrelaterede data, jfr. endvidere bilag 1
- Billund Vand & Energi A/S skal desuden leve op til de sikkerhedsmæssige krav, der er indgået aftale om med andre myndigheder ??
- Billund Vand og Energiskal udarbejde beredskabsplaner for datasikkerhed, der skal muliggøre genoptagelse af normal drift indenfor de aftalte tidsfrister efter et nedbrud.

3 Holdninger og principper

Datasikkerhed i Billund Vand & Energi A/S skal fastlægges som en afvejning af de ofte modstridende hensyn til ønsket om

- høj sikkerhed
- hensynet til brugervenlig it-anvendelse og
- omkostninger ved investeringer i sikkerhed.

Datasikkerheden implementeres i overensstemmelse med følgende overordnede holdninger og principper:

- Troværdighed på sikkerhedsområdet overfor omverdenen, herunder vore kunder og samarbejdspartnere, må ikke berettiget kunne drages i tvivl
- Sikkerhedsforanstaltninger skal søges tilrettelagt, så de opleves som en naturlig del af medarbejdernes daglige arbejde og ikke som en barriere
- Sikkerheden søges styret i overensstemmelse med almindelig anerkendte metoder og procedurer for datasikkerhed.
- Udgifter til at tilvejebringe sikkerhed skal afvejes mod de udgifter der er forbundet med mulige sikkerhedsbrud.

Sikkerhedsstyring og sikkerhedsløsninger skal følge standarder eller bedste produkt til opgaven.

Såfremt vore kunder berøres af sikkerhedshændelser hos Billund Vand & Energi A/S, vil virksomheden informere målrettet og arbejde for at genoprette normal drift hurtigst muligt.

4 Omfang

Politikken omfatter Billund Vand & Energi A/S data, som er:

- alle data, der tilhører virksomheden, herudover også data, som ikke tilhører virksomheden, men som virksomheden kan gøres ansvarlig for. Dette inkluderer for eksempel alle data om kunder, virksomheder, personale, data om finansielle forhold, alle data, som bidrager til administration af virksomheden samt data, som er overladt til virksomheden af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller ethvert andet datagrundlag, som kun er til intern brug
- alle data, ligegyldigt hvilken form de opbevares og formidles på, herunder også data i papirform.

Politikken er gældende for:

- alle ansatte uden undtagelse - både fastansatte og midlertidigt ansatte
- bestyrelse, ledelse og interessenter
- eksterne konsulenter, som arbejder i eller for virksomheden
- alle medarbejdere der er ansat under aftaleforhold

Disse personer betegnes herefter som medarbejderen.

Ved en eventuel udlicitering af dele af eller hele it-driften, skal det sikres i samarbejdet med serviceleverandøren, at virksomhedens sikkerhedsniveau fastholdes, således at serviceleverandøren, dennes faciliteter og medarbejdere, som har adgang til virksomhedens data, mindst lever op til virksomhedens datasikkerhedsniveau.

5 Sikkerhedsniveau

Sikkerhed for *tilgængelighed* sikres ved at alle medarbejdere gemmer data, så de er tilgængelige for andre, som skal bruge dem.

Sikkerhed for *kvalitet* sker ved, at alle medarbejdere i Billund Vand & Energi A/S overholder virksomhedens værdier (se afsnit 1.1)

Sikkerhed for *fortrolighed* sikres ved at Billund Vand & Energi A/S beskytter sine data og udelukkende tillader brug, adgang og offentliggørelse af data i overensstemmelse med virksomhedens retningslinjer og under hensyntagen til den enhver tid gældende lovgivning.

Hvor der behandles personfølsomme oplysninger eller cpr.nr. skal data sikres ekstra godt med de it-værktøjer, der er tilgængelige herunder personlig adgangskontrol, sikker mail og lign.

Hvor er benytter ekstern leverandør til databehandling, sikres vores datasikkerhed ved oprettelse af en datasikkerhedsaftale, som leverandøren skal tiltræde. Nærværende politik for datasikkerhed ligger til grund for en sådan datasikkerhedsaftale.

	Tilgængelighed	**Kvalitet**	**Fortrolighed**
Kunder	Lav (kun udvalgte)	Høj	Høj
Personale	Lav (kun udvalgte)	Høj	Høj
Drift	Høj	Høj	Mellem
Anlæg	Mellem	Høj	Mellem
Udvikling	Lav (kun udvalgte)	Høj	Høj
Formidling	Mellem	Høj	Mellem

6 Sikkerhedsbevidsthed, organisering og ansvar

Virksomhedens ledelse og bestyrelse har det overordnede ansvar for, at styringen af datasikkerheden er hensigtsmæssig og betryggende. Det er virksomhedens ledelse og bestyrelse der godkender datasikkerheds-politikken:

- Det daglige ansvar for den overordnede styring af datasikkerheds-indsatsen og gennemførelse af den fornødne kontrol varetages af direktionen. Det er direktionen, der godkender sikkerhedsregler
- Direktionen skal udpege en sikkerhedsansvarlig med ansvar for den overordnede styring af datasikkerhedsindsatsen, og sikre etablering af en organisatorisk tværgående sikkerhedsgruppe, der blandt andet skal hjælpe den sikkerhedsansvarlige med at vur-dere, hvorvidt der er behov for ændringer i den gældende data-sikkerhedspolitik og dennes operative udmøntning
- Datasikkerhedsgruppen godkender sikkerhedsprocedurer, forret-ningsgange med videre
- Den sikkerhedsansvarlige har ansvar for den overordnede styring af datasikkerheden. Den sikkerhedsansvarlige sikrer udarbejdelse og vedligeholdelse af datasikkerhedspolitikken, sikkerhedsstrate-gien, sikkerhedshåndbogen, beredskabsplaner der er omfattet af denne datasikkerhedspolitik og risikovurderingen
- Ansvaret for overholdelse af virksomhedens datasikkerhed er ud-delegeret til den sikkerhedsansvarlige. Det er således den sikker-hedsansvarlige, der har ansvaret for, at datasikkerhedspolitikkens krav og udmøntningen heraf i form af sikkerhedsbestemmelser og -procedurer med videre implementeres og forvaltes korrekt
- Den sikkerhedsansvarlige kan uddelegere det operationelle ansvar til andre medarbejdere
- Alle medarbejdere i Billund Vand & Energi A/S har et personligt ansvar for, at datasikkerhedspolitikken følges i forbindelse med vedkommendes aktuelle ansvarsområde og arbejdsopgaver
- Til hvert datasystem (dette gælder også eventuelle papirarkiver), udpeges en systemejer. Systemejeren har ansvaret for et specifikt programkompleks, herunder driftsafvikling, vedligeholdelse og ud-fasning
- Systemejeren er arkiv ansvarlig (gælder også papir arkiver), og dataansvarlig i henhold til persondatalovens bestemmelser. Sy-stemejer tager stilling til interne kontroller i systemet samt sikker-hed, jævnfør regler herom. Systemejer kan uddelegere dele af det daglige sikkerhedsarbejde i forbindelse med systemet til en sy-stemadministrator.

7 Brud på datasikkerheden

Når en medarbejder opdager trusler mod datasikkerheden eller brud på denne, skal dette straks meddeles til den sikkerhedsansvarlige.

Data gives samtidig til den sikkerhedsansvarlige, der redegør for hændelsen.

Overtrædelser af datasikkerhedspolitikkens udmøntning i form af sikkerhedsbestemmelser og -procedurer m.v. vil kunne medføre sanktioner over for medarbejdere eller samarbejdspartnere i overensstemmelse med virksomhedens generelle politikker, henholdsvis indgåede aftaler.

8 Operationalisering

Politikken skal af direktionen omsættes til operative sikkerhedsbestemmelser, det vil sige sikkerhedsregler for administrative, fysiske og tekniske sikringsforanstaltninger. Der skal udarbejdes procedurer, retningslinjer, forretningsgange og dokumenteres opfyldelse af krav. Dette dokumenteres i en sikkerhedshåndbog.

Den sikkerhedsansvarlige, sikkerhedsgruppen og ekstern revision eller sikkerhedskonsulentfirma skal rapportere status på datasikkerheden til den sikkerhedsansvarlige, som rapporterer til direktionen.

Sikkerhedshåndbogen skal indeholde en beskrivelse af de datasikkerhedsområder, der er relevante for Billund Vand & Energi A/S.

9 Opfølgning

Som et led i den overordnede sikkerhedsstyring tager den sikkerhedsansvarlige og direktionen, på grundlag af den løbende overvågning og rapportering, datasikkerhedspolitikken op til revurdering mindst en gang hvert tredje år, ellers efter behov.

Virksomheden fastlægger på baggrund af en risikovurdering et sikkerhedsniveau, som svarer til betydningen af de pågældende data. Virksomheden vil gennemføre en risiko- og konsekvensvurdering under hensyntagen til sammenhæng mellem investering i tid til risikovurdering og sikkerhedsniveauet.

Der gennemføres mindst en gang årligt en risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Der foretages ligeledes en risikovurdering ved større forandringer i organisationen eller datasystemerne.

Der gennemføres opfølgning på medarbejdernes vidensniveau på datasikkerhedsområdet.

Overholdelse af Billund Vand & Energi A/S sikkerhedsbestemmelser og -procedurer med videre vurderes af en uafhængig ekstern it-revision mindst en gang om året. Resultatet rapporteres til virksomhedens ledelse og bestyrelse.

10 Offentliggørelse

Denne politik skal offentliggøres for alle medarbejdere i virksomheden og kan udleveres til relevante samarbejdspartnere.

Øvrigt indhold i sikkerhedsstyringssystemet er intern viden forbeholdt virksomheden.

Den sikkerhedsansvarlige kan, i samarbejde med direktionen, give tilladelse til, at der udleveres og/eller offentliggøres materiale fra sikkerhedsstyringssystemet.

11 Bilag 1
Lovgivning, der er relevant for datasikkerhedspolitikken

Dette bilag indeholder en liste over den lovgivning, der er relevant for datasikkerhedspolitikken. Bemærk at listen ikke er udtømmende.

- Databeskyttelsesloven (Lov nr. 502 af 23/05/2018)
- Offentlighedsloven. Lov om offentlighed i forvaltningen. Gældende for al virksomhed der er udøvet af Offentlig forvaltning (Lov nr. 606 af 12/06/2013)
- Arkivloven. Gældende for al virksomhed der er udøvet af offentlig forvaltning og domstolene (Lbk nr. 1201 af 28/09/2016)
- Ophavsretsloven (Lbk nr. 1144 af 23/10/2014)
- Markedsføringsloven. Vedrørende beskyttelse af erhvervshemmeligheder og korrekte sammenligningsinformationer (Lov nr. 426 af 03/05/2017)
- Forvaltningsloven. §27 vedrørende tavshedspligt og §28 vedrørende videregivelse af oplysninger til anden forvaltningsmyndighed (Lbk nr. 433 af 22/04/2014)
- Vedrørende bestemmelser omkring immaterielle rettigheder henvises i øvrigt til patentloven (Lbk nr. 221 af 26/02/2017), varemærkeloven (Lbk nr. 223 af 26/02/2017)

12 Bilag 2
Uddybende beskrivelse af ansvarsområder

Dette bilag indeholder en uddybende beskrivelse af ansvarsområder

12.1 Direktionen

- Sikrer den overordnede styring af datasikkerhedsindsatsen og gennemførelse af den fornødne kontrol
- Sikrer godkendelse af sikkerhedsregler
- Udpeger en sikkerhedsansvarlig med ansvar for den overordnede styring af datasikkerhedsindsatsen
- Etablerer en organisatorisk tværgående sikkerhedsgruppe, der blandt andet skal hjælpe den sikkerhedsansvarlige med at vurdere, hvorvidt der er behov for ændringer i den gældende datasikkerhedspolitik og dennes operative udmøntning.
- Den sikkerhedsansvarlige sikrer at datasikkerhedspolitik og sikkerhedshåndbogens regler der er gældende for ansvarsområdet er kendte, forstået og efterleves
- Sikrer at medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer
- Sikrer at yderligere dokumentation laves efter behov
- Sikrer at risikovurdering gennemføres inden implementering af nye systemer
- Koordinerer opklaringsarbejde ved konstateret eller begrundet mistanke om sikkerhedsbrud. Resultatet rapporteres til den sikkerhedsansvarlige og virksomhedens ledelse
- Sikrer at ansættelse, introduktion, løbende vurdering, funktionsskift og afvikling af medarbejdere overholdes.

12.2 Medarbejderne

Medarbejdere har ansvar for:

- at overholde datasikkerhedspolitikken, regler og procedurer, der er relevante for den enkeltes arbejdsopgaver
- at rapportere om eventuel sikkerhedsbrud eller mistanke til øverste sikkerhedsansvarlige
- at sikre at man kun anvender data, systemer og lokaler, der er relevante for den enkeltes arbejdsopgaver.

12.3 Datasikkerhedsgruppen

- Vedligeholder datasikkerhedspolitikken og indstiller til direktionens og bestyrelsens godkendelse
- Vedligeholder regler i sikkerhedshåndbogen

- Sikrer at der er udpeget systemejere med videre
- Sikrer at systemejere udarbejder de nødvendige procedurer, forretningsgange, retningslinjer med videre
- Sikrer at der gennemføres stikprøvekontrol vedrørende implementering og overholdelse af procedurer, regler med videre
- Laver sikkerhedskommunikationsplan og informationskampagner
- Sikrer at sikkerhedsadfærd er beskrevet og indeholder information om relevante retningslinjer, procedurer, forretningsgange med videre
- Prioriterer indsatsområder og laver indstillinger
- Sikrer gennemførelse af risikovurderinger
- Kommenterer sikkerhedsansvarliges sikkerhedsrapportering
- Rapporterer status på sikkerheden til sikkerhedsansvarlig.

12.4 Sikkerhedsansvarlig

12.4.1 Planlægning

- Er ansvarlig for udarbejdelse af handlingsplaner
- Er formand for sikkerhedsgruppen
- Udarbejder sikkerhedskampagner
- Er ansvarlig for udarbejdelse af sikkerhedshåndbog og vedligeholde materialer.

12.4.2 Udførelse

- Er ansvarlig for gennemførelse af informations aktiviteter i relation til datasikkerheden
- Deltager i etablering af styringssystem
- Behandler dispensationsansøgninger
- Holder sig ajour med sikkerhedsområdet og lovgivning
- Samarbejder og koordinerer med andre funktioner og udvalg
- Rådgiver om sikkerhedsforhold.

12.4.3 Kontrol

- Måler organisationens kendskab/forståelse/accept med mere
- Følger op på retningslinjer og procedurer/instrukser
- Håndterer sikkerhedsbrud
- Følger op på håndtering af overvågning af logfiler
- Laver opfølgning på planer og budgetter samt rapportering til udvalg.

12.4.4 Forbedring og vedligehold

- Foretager løbende og periodevis vurdering af styringssystemet
- Indstiller forbedringsforslag til sikkerhedsgruppen og direktionen.

12.5 Systemejer

Sikrer at der laves kravspecifikationer der tager hensyn til sikkerhedsmæssige forhold forud for enhver systemudvikling og – ændringer – eventuel med ekstern assistance

Sikrer udarbejdelse af nødvendig risikovurdering, herunder også data i systemet

Sikrer at ændringsstyringen følges i forbindelse med systemændringer

Sikrer at der, når systemer sættes i drift, findes konkrete regler og procedurer for regulering og administration af adgangsforhold og at disse er i overensstemmelse med de principielle krav hertil. Herunder sikrer at disse er i overensstemmelse med gældende regler

Sikrer at der autoriseres adgange til systemet og til data i henhold til retningslinjer herfor

Foretager opfølgning og rapportering af sikkerhedsbrud til den sikkerhedsansvarlige.

For papirarkiver gælder for systemejer:

- at når lokaler tages i brug, skal der inden ibrugtagning være udarbejdet konkrete regler og procedurer for regulering og administration af adgangsforhold. Det skal desuden sikres, at disse er i overensstemmelse med de principielle krav hertil
- at der skal gives adgang til lokaler/udstyr jævnfør sikkerhedshåndbogens regler.

12.6 Systemadministrator

Systemadministrator kan udføre dele af det daglige sikkerhedsarbejde i relation til et givet system.

Arbejdet udføres under ansvar af systemejeren, og i henhold til en for systemet nærmere beskrevet procedure.