Skabelon for IT-sikkerhedspolitik

Følgende dokument er en skabelon til udarbejdelse af en IT-sikkerhedspolitik. IT-sikkerhedspolitikken er den øverste rammesættende politik for IT-sikkerhedsarbejdet i organisationen. Dokumentet er én af flere skabelon-dokumenter, som indgår i det IT-sikkerhedsmateriale, som alle organisationer bør have ift. overholdelse af den danske implementering af NIS2.

Vi har i Lakeside lavet en række skabeloner, som du er velkommen til at bruge. Skabelonerne er tiltænkt SMV’er med produktion, men kan sagtens bruges af organisationer uden produktion (OT). Skabelonerne er udarbejdet med udgangspunkt i små og mellemstore forsyningsselskaber.

* Nærværende IT-sikkerhedspolitik
* IT-sikkerhedshåndbogen
* IT/OT-leverandør sikkerhedspolitik
* IT/OT-leverandør tjekliste
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsprocedure og Hændelseslog
* Kriseberedskabspolitik, -planer og -skabeloner

Skabelonerne for de øvrige dokumenterne kan findes og downloades på [www.lakeside.dk/publikationer](http://www.lakeside.dk/publikationer)

**Sådan bruger du skabelonen**

* Tekster med gråt og i firkantede klammer er vejledningstekster, som slettes ved endt redigering.
* <organisation> er en dokument-egenskab. Den kan rettes under Filer / Egenskaber / Brugerdefineret (nederste tekstboks) og derefter opdatere alle felter i hele dokumentet (vælg alt og højreklik).
* Alle tekster kan ændres efter behov og som tilpasning til din organisation. Alle tekster med gult bør du ændre eller som minimum forholde dig til.
* Kontaktinformation og organisation skal opdateres i sidehoved og sidefod. OBS! Organisation og logo på forsiden er også i en sidefod.

Versions historik for skabelon:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 1.0 | 13.12.2024 | MTH | Oprettet første version |
| 1.1 | 29.01.2025 | MTH | Opdateret ift. udkast til bekendtgørelse om modstandsdygtighed og beredskab i energisektoren. |
| 1.2 | 04.04.2025 | MTH | Opdateret ift. endelig version af bekendtgørelse |
| 1.3 | 06.06.2025 | MTH | Simplificeret og strømlinet |

Dato | Version X.X

IT-sikkerhedsPOLITIK

Indholdsfortegnelse

[1 Målsætning for IT-sikkerhedspolitikken 4](#_Toc200100579)

[1.1 Omfang 4](#_Toc200100580)

[1.2 Gyldighedsområde 4](#_Toc200100581)

[1.3 Governance 5](#_Toc200100582)

[2 Organisering 5](#_Toc200100583)

[2.1 Systemansvar 9](#_Toc200100584)

[3 IT-sikkerhed i det daglige 10](#_Toc200100585)

[3.1 Medarbejderansvar 10](#_Toc200100586)

[3.2 Leverandøraftaler 11](#_Toc200100587)

[4 Datahåndtering 11](#_Toc200100588)

[4.1 Destruktion af databærende medier 12](#_Toc200100589)

[4.2 Slet af data 12](#_Toc200100590)

[4.3 Sikring af databærende medier 12](#_Toc200100591)

[5 Sikkerhedsforskrifter 12](#_Toc200100592)

[5.1 Drift 12](#_Toc200100593)

[5.2 Netværk 13](#_Toc200100594)

[5.3 Firewall 13](#_Toc200100595)

[5.4 Adgangshåndtering 14](#_Toc200100596)

[5.5 Fysisk sikkerhed 14](#_Toc200100597)

[5.6 Mail 14](#_Toc200100598)

[5.7 Kryptering 15](#_Toc200100599)

[5.8 IT-systemer 15](#_Toc200100600)

[5.9 OT-systemer 15](#_Toc200100601)

[5.10 Logning og monitorering 16](#_Toc200100602)

[5.11 Tilsyn med og validering af IT-sikkerheden 16](#_Toc200100603)

[6 Overtrædelse af IT-sikkerhedspolitikken 17](#_Toc200100604)

termer

|  |  |
| --- | --- |
| Begreb eller forkortelse i teksten  | Beskrivelse |
| OT | Operationel teknologi (OT) refererer til hardware og software, der bruges til at overvåge og kontrollere fysiske enheder, processer og infrastruktur i forskellige industrier, herunder energisektoren. Udtrykket bruges til at skelne mellem traditionelle informationsteknologi (IT) systemer og industrielle kontrolsystemer. |
| NIS2 | NIS2 er den almindelige betegnelse for [EU-direktiv (EU) 2022/2555](https://eur-lex.europa.eu/eli/dir/2022/2555/oj), som fastlægger foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU. |
| CER | Et EU-direktiv inden for digital modstandsdygtighed, hvor kritiske enheder får et større ansvar for at beskytte sig mod hændelser i IT-systemer, der kan have negative konsekvenser for samfundet. |
| SaaS | Software som en service (Software-as-a-Service) er en softwareløsning, der er betalt efter forbrug hos en cloudtjenesteudbyder. Man lejer brugen af software, og brugere kan oprette forbindelse til den via internettet, typisk vha. en webbrowser. Al underliggende infrastruktur, middleware, appsoftware samt alle appdata findes i tjenesteudbyderens datacenter. Tjenesteudbyderen administrerer hardwaren og softwaren og vil, med den rette serviceaftale, sikre tilgængeligheden af og sikkerheden for både appen og dine data. |

visions- og Godkendelseshistorik

[Vejledning: Dokumentet skal godkendes af jeres bestyrelse. Godkendelsen bør fremgå på skrift – enten via en mail eller i et bestyrelsesreferat – det skal kunne fremfindes til dokumentation.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer | Godkendt |
| [0.0] | [dd.mm.yy] | [INT/navn] |  | [dato ] |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Kontaktpersoner

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)Skriv titel her, fx direktørTlf.: +45 xxxx xxxxxxx@domæne.dk<Organisation> | (optionel) Fornavn Efternavn (initialer) Skriv titel her, fx driftsleder/tekniskchefTlf.: +45 xxxx xxxxxxx@domæne.dk<Organisation> |

# Målsætning for IT-sikkerhedspolitikken

IT-anvendelsen i har til formål at understøtte selskabets overordnede forretnings-formål om at levere stabil og prisbillig varmeforsyning.

* arbejder aktivt med styring af it-sikkerhed med det formål at sikre driftsstabilitet, tilgængelighed, fortrolighed og integritet for s IT/OT-systemer og data.
* anvender en risikobaseret tilgang, hvor beskyttelsesniveau og omkostninger hertil skal være baseret på en forretningsmæssig risiko- og konsekvensanalyse, som foretages minimum årligt.
* tilstræber at overholde relevant lovgivning – herunder GDPR og Bekendtgørelse for modstandsdygtighed og beredskab i energisektoren.

Der udarbejdes og vedligeholdes løbende en IT-sikkerhedshåndbog og lokale procedurer, vejledninger og skabeloner, som understøtter medarbejdere og samarbejdspartnere i at følge rammerne sat i IT-sikkerhedspolitikken. IT-sikkerhedshåndbogen, samt supplerende dokumenter fra det samlede IT-sikkerhedsmateriale relevante for medarbejderens arbejdsopgaver, bliver udleveret til alle medarbejdere hos , med krav om gennemlæsning og efterlevelse.

## Omfang

IT-sikkerhedspolitikken er grundlaget for IT-sikkerhedsmaterialet som omfatter følgende:

* Nærværende IT-sikkerhedspolitik
* IT-sikkerhedshåndbogen
* Leverandørpolitik
* Risikostyringspolitik
* Kriseberedskabspolitik, -planer og -skabeloner
* Hændelseshåndterings- og nødprocedure
* Privatlivspolitikker for kunder, ansatte og jobansøgere
* Tilstandsrapport (inkl. fortegnelser)

## Gyldighedsområde

Politikken er gældende for alle s IT-relaterede aktiviteter, inkl. OT og netværk, uanset om disse udføres af ansatte i eller af samarbejdspartnere.

Politikken er gældende uanset om aktiviteten finder sted på selskabets lokationer, på forbrugeres lokationer, ved fjern- / hjemmearbejdsplads eller på andre lokationer.

Politikken er gældende for al brug af selskabets informationsrelaterede aktiviteter på enhver enhed (stationær computer, pc, tablet, smartphone o.l.) uanset om enheden er ejet af eller af medarbejderen selv.

I det omfang, selskabet lader eksterne leverandører varetage IT-driftsafvikling og IT-databehandling, skal det sikres, at pågældende leverandører overholder rammer og retningslinjer, som de er beskrevet i IT-sikkerhedsmaterialet jf. afsnit 1.1. Herunder også at Databehandleraftale er indgået hvor relevant.

## Governance

Nærværende IT-sikkerhedspolitik og relaterede politikker gennemgår review årligt og godkendes af bestyrelsen. Review og godkendelse af IT-sikkerhedspolitikken fremgår af versions- og godkendelseshistorikken først i dokumentet.

IT-sikkerhedsmaterialet i sin helhed gennemgår tillige review årligt og godkendes af direktionen.

# Organisering

[Vejledning: organiseringen skal passe til jeres organisation, så I skifter nedenstående figur med en rigtig. Når I overvejer hvem der skal have de forskellige roller, skal I måske tage in mente at der i bekendtgørelsen står der at Cyberkoordinatoren og Beredskabskoordinatoren skal have møder med bestyrelsen en gang i kvartalet. De ansvarlige roller udpeget i organisationsdiagrammet er ikke nødvendigvis de udførende – men de er ansvarlige for at opgaverne bliver udført, og dermed også ansvarlige for at følge op på om de er udført. Teksten og tabellerne under figuren skal selvfølgelig også tilpasses jeres sikkerhedsorganisering.]



Figur : IT-sikkerhedsorganisation. IT-sikkerhedsfunktionen er her angivet som en støttefunktion til direktøren.

Ansvaret for overholdelse af IT-sikkerhedspolitikken følger selskabets organisatoriske opbygning. Bestyrelsen udstikker de strategiske retningslinjer, og er dermed Øverste sikkerhedsansvarlig for virksomheden, men direktionen er øverste sikkerhedsansvarlig i daglig drift. Alle fagområdespecifikke IT-sikkerhedsansvarlige er ansvarlige for IT-sikkerheden inden for eget ansvarsområde. Sikkerhedsfunktionen er udførende ift. udarbejdelse og vedligehold af IT-sikkerhedsmateriale, samt ansvarlig for facilitering af risikostyring, opfølgning på handlingsplaner for IT-sikkerhedstiltag og planlægning af beredskab.

|  |
| --- |
| Øverste strategisk sikkerhedsansvarlig |
| Bestyrelsen |
| Ansvar |
| Ultimativt ansvar for it-sikkerhed i . Strategisk og rammesættende* godkendelse af IT-sikkerhedspolitik og andre politikker
* godkendelse af ROS-konklusionsrapport inden den sendes til Energistyrelsen
* godkendelse af risikovurdering af projekter der skal godkendes i Energistyrelsen
* at der er et fast kvartalsmæssigt dagsordenspunkt på bestyrelsesmøder om status for virksomhedens organisatoriske beredskab, fysiske sikring og cybersikkerhed, og at behandlingen af dette føres til referat
 |

|  |
| --- |
| Øverste sikkerhedsansvarlig i daglig driftCyberkoordinator & Beredskabskoordinator |
| Direktør |
| Ansvar |
| * fastlæggelse af styringsprincipper og delegering af specifikke ansvarsområder
* at der foretages opfølgning og kontrol med IT-sikkerheden inkl. interne audit og tilsyn
* at medarbejderne gennem uddannelse og udvikling opnår kvalifikationer og sikkerhedsbevidsthed til at udføre deres arbejdsopgaver sikkert og korrekt

Cyberkoordinator & Beredskabskoordinator:* at iværksætte egne revisionsopgaver og/eller sikkerhedsundersøgelser
* at holde sig ajour med den generelle udvikling på det sikkerhedsmæssige område
* deltage i beredskab
* afrapportering af status for virksomhedens organisatoriske beredskab, fysisk sikring og cybersikkerhed til bestyrelsen ved kvartalsmæssige møder.
 |

|  |
| --- |
| Sikkerhedsfunktion |
| Udpeget rolle som støtter direktøren. |
| Ansvar |
| Assisterende Cyberkoordinator:* at udarbejde og vedligeholde IT-sikkerhedspolitikken
* den daglige risikostyringsproces for IT-sikkerhed
* at udarbejde relevante sikkerhedskrav, der operationaliserer IT-sikkerhedspolitikken
* at udbrede viden om IT-sikkerhedspolitikken
* at foretage opfølgning og rapportering af sikkerhedsbrud til direktøren
* at holde sig ajour med den generelle udvikling på det sikkerhedsmæssige område
* at koordinere relevante initiativer med øvrige aktører indenfor sikkerhedsarbejdet
* at facilitere risikostyringsprocessen og opfølgning på handlingsplan på IT-sikkerhedsområdet

Assisterende Beredskabskoordinator:* at planlægge beredskab og hændelseshåndtering
* at planlægge test og afprøvning af beredskab
* at koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud
* at opsamle information om it-sikkerhedsbrud og foretage evt. indrapportering til relevante myndigheder
 |

|  |
| --- |
| Fagområdespecifik IT-sikkerheds-ansvarlig |
| Linjeledelse / udpeget rolle i team |
| Ansvar |
| * det daglige IT-sikkerhedsarbejde i det specifikke fagområde
* at IT-sikkerhedspolitikken og de regler, der er relevante for eget ansvarsområde, er kendte og efterleves i eget team/egen afdeling
* at retningslinjerne og instrukser for anvendelse af et system eller en proces overholdes i eget team/egen afdeling
* at der, for processer som udspringer fra det pågældende fagområde, udarbejdes og vedligeholdes retningslinjer og vejledninger til efterfølgelse i organisationen
* at der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for eget team/egen afdeling
* at retningslinjerne for ansættelse, introduktion, løbende vurdering, funktionsskift og afvikling af medarbejdere overholdes
* at indgå i opklarings- og afhjælpningsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud
* at deltage i risikostyringsarbejdet som repræsentant for sit ansvarsområde
* at påtage sig ansvar for mitigering af risici og implementering af aftalte handlinger i sit ansvarsområde
* at udarbejde nødprocedurer for eget fagområde, ved manglende it-understøttelse eller datatab
* at kontorindretningen understøtter placering af fortrolige data, fx via mulighed for aflåste skabe
 |

## Systemansvar

I placeres systemansvaret for alle systemer hos den fagligt ansvarlige leder for det team/den afdeling der er primær bruger af systemet.

Systemejer er den der, efter aftale med direktøren, træffer beslutning om anskaffelse og livscyklus for et IT-system til at understøtte opgavevaretagelsen.

Dataejer er den der med udgangspunkt i et fagligt ansvar, træffer beslutning om formål og livscyklus i forbindelse med behandling af en specifik type data.

Systemejeren kan udpege en System- og leverandøransvarlig med ansvar for at udarbejde retningslinjer og instrukser for brug af systemet.

|  |
| --- |
| System- og Dataejere |
| Direktør / Linjeledelse |
| Ansvar |
| * at der ved installation af nye systemer gennemføres en forudgående sikkerheds-/risikovurdering inkl. vurdering af risici for de registrerede jf. GDPR.
* at der foreligger retningslinjer og instrukser for det pågældende system og at de overholdes
* at systemet understøtter sporbarhed så enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, der har udført aktiviteten
 |

|  |
| --- |
| System- og leverandøransvarlig |
| Udpeget rolle i team som rapporterer til Systemejer. |
| Ansvar |
| * at aftalen med leverandøren er dækkende ift. organisationens behov og aftalt IT-sikkerhedsniveau
* at risikovurderingen for systemet løbende holdes opdateret
* at der ved ibrugtagning af systemet foreligger konkrete regler og procedurer for korrekt brug af systemet
* at der ved ibrugtagning af systemet foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil, afsnit 5.4
* at foretage opfølgning og rapportering af sikkerhedsbrud til IT-sikkerhedsfunktionen
* at autorisere adgangen til systemet iht. retningslinjerne herfor
* at foretage opfølgning og rapportering af sikkerhedsbrud til IT-sikkerhedsfunktionen
* at føre tilsyn med leverandørens overholdelse af aftaler om databehandling og it-sikkerhed
 |

# IT-sikkerhed i det daglige

Håndhævelse af IT-sikkerhed skal finde sted med deltagelse fra alle IT-brugere. Alle har et eget ansvar for at bidrage til en sikker og betryggende IT-anvendelse.

En effektiv formidling af IT-sikkerhedsmaterialet skal skærpe og udvikle brugernes opmærksomhed på IT-sikkerheden og understøtte deling af erfaringer med sikkerhedsbrud samt nær-ved-sikkerhedsbrud.

Systemer og data må udelukkende anvendes til udførelse af de relevante arbejdsopgaver og skal beskyttes samt benyttes i overensstemmelse med de udstukne rammer og regler i IT-sikkerhedsmaterialet.

## Medarbejderansvar

Alle medarbejdere defineres her som:

* Ansatte
* Ledelse
* Medlemmer af bestyrelsen
* Vikarer
* Ressourcestøttende konsulenter
* Studerende / praktikanter

Alle medarbejdere skal have kendskab til - og arbejde i overensstemmelse med – s IT-sikkerhedspolitik og relaterede regler.

s ledelse har ansvaret for, at alle IT-brugere har kendskab til - og arbejder i overensstemmelse med – IT-sikkerhedspolitikken samt relevante tilknyttede dokumenter ift. den enkeltes arbejdsopgaver.

Det betyder blandt andet, at alle IT-brugere skal orienteres om deres ansvar i forbindelse med IT-sikkerheden, forinden de gives adgang til systemer og data. IT-sikkerhedspolitik og privatlivspolitikker udleveres ved tiltrædelse samt efter ajourføring.

Alle medarbejdere uddannes om IT-sikkerhed og trænes i awareness[[1]](#footnote-2), hvilket skal medvirke til, at alle medarbejdere har kendskab til og er bevidste om IT-sikkerhed.

## Leverandøraftaler

Som en del af den daglige drift har flere eksterne leverandører adgang til s systemer og IT-/OT-infrastruktur.

For hver ekstern leverandør med adgang til, og instruks om behandling af persondata i, s systemer skal der foreligge en databehandleraftale (uanset varighed) samt i øvrigt generelt overholdes de udstukne retningslinjer i nærværende IT-sikkerhedspolitik samt selskabets Persondatapolitik.

For hver ekstern leverandør med adgang til s systemer (uden instruks om behandling af persondata) skal der foreligge en fortrolighedsaftale samt i øvrigt generelt overholdes de udstukne retningslinjer i nærværende IT-sikkerhedspolitik.

Se også s leverandørpolitik.

# Datahåndtering

 skal som dataansvarlig leve op til en række krav i Databeskyttelsesloven[[2]](#footnote-3). Hvorledes dette sikres er beskrevet i en række privatlivspolitikker.

Privatlivspolitikkerne udgør regelsættet, der arbejdes efter ift. kunder, medarbejdere og andre interessenter:

* Privatlivspolitik til kunder, om hvordan behandler deres data.
* Privatlivspolitik målrettet jobansøgere om hvorledes behandler de data, de sender i forbindelse med en jobansøgning.
* Cookie-politik der oplyser brugerne af hjemmesiden om hvilke data hjemmesiden registrerer om dem.
* Privatlivspolitik til medarbejdere der beskriver hvorledes behandler de data, der registreres om medarbejdere under deres ansættelse.

Eksterne privatlivspolitikker (kunder, jobansøgere, cookie-politik) er publiceret på hjemmesiden link.

Den interne privatlivspolitik (medarbejdere) udleveres sammen med ansættelseskontrakt og forefindes endvidere på fællesdrev / intranet.

## Destruktion af databærende medier

Bortskaffelse af data skal finde sted under betryggende forhold, som f.eks. makulering, fysisk destruktion af harddiske, USB-sticks og lignende elektroniske databærende medier. Hvis der er tale om personhenførbare data eller andre former for følsomme data, skal det sikres, at data ikke bliver tilgængelige for uvedkommende.

## Slet af data

Når kunde- og ansættelsesforhold eller anden tilknytning ophører, skal persondata, på den registrerede destrueres, når disse data ikke længere er absolut nødvendige eller påkrævet af myndighederne.

## Sikring af databærende medier

Hos anvendes bærbart udstyr, herunder bærbare pc’er, smartphones, iPads (tablets), USB-nøgler, eksterne datalagringsenheder og lignende.

For at sikre at lagret data på disse bærbare enheder ikke kan blive tilgængeligt for uvedkommende, skal de krypteres og beskyttes med adgangskode.

# Sikkerhedsforskrifter

For alle væsentlige dele af IT-anvendelsen, skal der være etableret driftsafviklingsprocedurer, der sikrer konsekvent og stabil drift af systemer og data.

## Drift

[Vejledning: Eksemplet er skrevet for en lille virksomhed uden intern IT afdeling, hvor alle IT-systemer indkøbes som Software-as-a-Service (SaaS). Formuleringen ”et aftalt sikkerhedsniveau med den enkelte leverandør”, er et obs til at alle aftaler bør gennemgås for at sikre at de netop omhandler sikkerhedskrav.]

 har ikke nogen intern IT-afdeling.

IT-sikkerhedsopgaverne udføres i samarbejde med eksterne IT- og OT-leverandører, på et aftalt sikkerhedsniveau med den enkelte leverandør. Disse samarbejdspartnere bærer dermed en meget væsentlig del af ansvaret for at det valgte sikkerhedsniveau etableres og opretholdes.

IT-systemer indkøbes som SaaS (Software as a Service), hvor de enkelte leverandører er ansvarlige for IT-sikkerheden og Databehandlere på vegne af i det omfang, hvor der opbevares persondata i systemerne.

 har entreret med en primær leverandør for sit OT-miljø. OT-miljøet hostes lokalt hos , og serviceres af en ekstern leverandør af OT-services. Dette er den primære OT-leverandør, som indgår i s beredskab.

OT-systemer indkøbes som systemer bestående af hardware og software, med IT-sikkerhedskrav til leverandørens systemer og medarbejdere.

## Netværk

Netværk for produktion skal adskilles sikkert fra øvrige netværk baseret på de til enhver tid gældende anbefalinger fra CFCS.

*/Leverandør* er IT-administrator med det overordnede ansvar for sektionering af routerne.

Alle eksterne kommunikationsforbindelser skal forud godkendes af IT-sikkerhedsfunktionen og udføres af de eksterne IT-administratorer, som vedligeholder oversigter over netværk og datakommunikation.

Produktionsnetværk (SRO), Administrationsnetværk og Gæstenetværk er adskilt og med adgangskode. Netværksudstyr og andre enheder må ikke tilsluttes netværket før standardpasswords er udskiftet.

## Firewall

Adgangen fra eksterne netværk - herunder internet - til s netværk, er sikret således, at det kun er autoriserede IT-brugere som kan opnå adgang.

*/Leverandør* er IT-administrator med det overordnede ansvar for s firewalls, herunder betryggende administration af firewall samt vedligeholdelse af firewallsoftware, overvågning af firewall, logning af trafikken samt aftestning af funktionaliteten.

## Adgangshåndtering

[Vejledning: Kvartalsvis gennemgang af adgange og rettigheder, samt tidsbegrænset fjernadgang. Dog er der først krav om fysisk adgangskontrol for: anlæg klasse 2, kontorfaciliteter og kontrolrum, samt ved lokationer og faciliteter hvor der står netværksudstyr.]

Det tilstræbes at alle medarbejdere har adgang til de systemer og de data, som de har behov for, så de kan udføre deres arbejdsopgaver. Hverken mere eller mindre. Rettigheder skal være personhenførbare, og inaktive bruger- og servicekonti skal fjernes.

Brug af to-faktor autentifikation benyttes ved fjernadgang og alle steder, hvor det vurderes nødvendigt. Er det ikke muligt at opnå to-faktor autentifikation, skal der findes andre foranstaltninger, hvorved opnår samme beskyttelse.

Fjernadgange tildeles i en tidsbegrænset periode, så fjernadgange kun er åbne i tidsrum med et godkendt arbejdsbetinget behov for at tilgå et system.

## Fysisk sikkerhed

[Vejledning: Dette sikrer overholdelse af krav for anlæg i klasse 2 eller over jf. bekendtgørelse for energisektoren – anlæg i denne sammenhæng er: kraftvarmeværker, fjernkølingsanlæg, spids- og reservelastanlæg, ledningsnet, pumpestationer, varmevekslerstationer, varmepumper og kontrolrum der styrer, regulerer eller overvåger varmeleverancer. samt kontorfaciliteter.]

For s anlæg, ledningsnet og kontorfaciliteter laves der løbende vurdering af klimarobusthed, og klimasikringstiltag planlægges og prioriteres som en del af risikovurderingsprocessen.

For anlæg der understøtter grundlast og distribution af fjernvarme, indgår genetablering som en beredskabsprocedure.

Der er opsat brand- og tyverialarm på alle lokationer med anlæg, kontrol- og kontorfaciliteter, samt generel perimetersikring.

Der er styret adgangskontrol til alle s lokationer med klasse 2 anlæg, kontor- og kontrolfaciliteter, således at alle medarbejdere og leverandører har adgang til de fysiske lokationer og til virksomhedens anlæg jf. arbejdsbehov. Adgange er personlige og logges.

Leverandørers medarbejdere må ikke færdes uledsaget på virksomhedens anlæg, medmindre dette er aftalt skriftligt med .

## Mail

Alle medarbejdere har adgang til en personlig arbejds e-mail, og er instrueret i retningslinjer for brugen af denne mail. I det omfang det understøtter forretningen er der etableret en række fælles/funktions postkasser, hvortil flere personer har adgang.

Sikker e-mail er en krypteret mail man sender fra Outlook via selskabets sikre postkasser.

## Kryptering

Alle databærende medier skal beskyttes mod uautoriseret adgang ved hjælp af adgangskontrol og kryptering. Dette gælder server-systemer såvel som personlige computere, tablets, USB-sticks osv.

## IT-systemer

[Vejledning: her er det antaget at IT-indkøbes som SaaS. Se afsnittet OT-systemer, hvor der er indsat et forslag til en tekst, hvis der i stedet er tale om systemer der hostes lokalt i organisationen.]

IT-systemer indkøbes som Software-as-a-Service (SaaS). Dette betyder at Leverandøren har ansvaret for IT-sikkerhedsforanstaltninger inkl. backup og genetablering af systemer og data.

Ved indgåelse af standardaftaler for SaaS skal det sikres at disse er dækkende ift. s behov for det pågældende IT-system, jf. tilstandsrapport og risikovurdering, ift. bl.a. support, backup, genetablering, kommunikation og understøttelse af s indrapportering til myndigheder, når dette er relevant.

## OT-systemer

Ved indkøb af nye OT-systemer eller komponenter skal det vurderes, hvem der fremadrettet skal være ansvarlige for service og vedligehold, og det skal sikres, at der er indgået aftaler og/eller fastlagt procedurer, som sikrer backup og genetablering i det nødvendige omfang, uanset om vedligehold er outsourcet eller ligger internt i organisationen.

Mobile enheder der kan tilgå produktions- og operationelle kontrolsystemer må ikke anvendes til privat brug.

Det sikres via aftaler at leverandøren er forpligtiget til at følge s retningslinjer ift. OT-sikkerhed samt adgang til netværk jf. s IT/OT-leverandør sikkerhedspolitik.

## Logning og monitorering

[Vejledning: Dette sikrer overholdelse af krav for virksomheder niveau 2 eller over jf. bekendtgørelse for energisektoren.]

 sikrer at der foretages tidssynkroniseret logning i fornødent omfang til at identificere hændelser og nærvedhændelser, samt understøtte myndighedernes efterforskning.

Logs beskyttes mod manipulation og uautoriseret adgang, og opbevares særskilt fra de enheder hvorfra der opsamles logs. Logs opbevares i minimum 6 måneder.

Logs overvåges automatisk, og ved alarmer notificeres driftsvagten via mail.

## Tilsyn med og validering af IT-sikkerheden

[Vejledning: Dette sikrer overholdelse af krav for virksomheder niveau 2 eller over jf. bekendtgørelse for energisektoren. Man må selvfølgelig godt gøre det oftere, hvis man synes. Men her er der taget stilling til minimum.]

 foretager:

* en kvartalsvis gennemgang af adgange og rettigheder til forsyningskritiske systemer, inkl. adgange til OT-miljøet og produktionsnetværket,
* en kvartalsvis kontrol af perimetersikring og fysisk adgangskontrol, inkl. procedurer for håndtering af alarmer,
* halvårlig opfølgning på konfiguration af fjernadgange og konfiguration af netværksudstyr,
* halvårlige kontrol med fysisk sikkerhed, herunder afprøvning af grundlast anlægs nødstrøm og gennemgang af adgang og rettigheder til lokationer og anlæg.
* årlig opfølgning på logs og monitorering ift. sikring af at logs kan anvendes til identifikation og efterforskning af hændelser.

[Vejledning: Gennemførelse af kontroller skal dokumenteres. Nogen har et system til dette, andre har et regneark eller blot et dokument.]

 plan for gennemførelse af ovenstående kontroller indgår i s årshjul og dokumenteres i en kontrollog.

For IT- og OT-leverandører, som er databehandlere, fastlægges løbende audit og tilsyn ift. Datatilsynets vejledning om tilsyn med databehandlere.

[Vejledning: I bekendtgørelsen er det ikke et krav til brug af tekniske sikkerhedsscanninger, så som fx sårbarhedsscanninger og penetrationstest, men det kan være et værktøj til at vurdere effektiviteten af jeres sikkerhedsforanstaltninger.]

<organisation> entrerer med et eksternt firma ift. sårbarhedsanalyser af netværket to (2) gange årligt.

# Overtrædelse af IT-sikkerhedspolitikken

Det er den enkelte medarbejders ansvar at efterleve sikkerheden omkring IT-anvendelsen i jævnfør nærværende IT-sikkerhedspolitik.

Bevidst brud på denne politik for IT-sikkerhed, eller understøttende IT-sikkerhedsmateriale, anses som en væsentlig overtrædelse af kontraktforholdet mellem og medarbejderen, og vil medføre disciplinære foranstaltninger, herunder også afslutning af ansættelsesforholdet.

1. Awareness er et engelsk begreb som oversat betyder ”opmærksomhed”. Det bruges i IT-sikkerhedssammenhæng om den træning, der skal hjælpe medarbejdere med at blive opmærksomme på og mistænksomme overfor dagligdagssituationer, som kan lede til sikkerhedsbrud. Fx træning i at spotte phishing mails. [↑](#footnote-ref-2)
2. Databeskyttelsesloven <https://www.retsinformation.dk/eli/lta/2024/289> [↑](#footnote-ref-3)