Skabelon for IT/OT-leverandør sikkerhedsprocedure

Følgende dokument er en skabelon til udarbejdelse af en leverandør sikkerhedsprocedure, til rammesætning af regler, krav og inddragelse af de af jeres leverandører der understøtter jeres interne IT-sikkerhedsarbejde og kriseberedskab. Dokumentet er én af flere skabelon-dokumenter, som indgår i det IT-sikkerhedsmateriale, som alle organisationer bør have ift. overholdelse 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.

* IT-sikkerhedspolitik
* IT-sikkerhedshåndbogen
* Nærværende IT/OT-leverandør sikkerhedsprocedure, og leverandør tjekliste
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsproces 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.

Versionshistorik for skabelon:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 1.0 | 13.12.2024 | MTH | Oprettet første version |
| 1.1 | 03.04.2025 | MTH | Præciseret tekst i afsnit 6 og 7 patch og change management. Tilføjet afsnit 7.1 om håndtering af nyt software/hardware og 7.2 om dokumentation |

|  |  |  |  |
| --- | --- | --- | --- |
| 1.2 | 22.06.2025 | MTH | Omdøbt til Leverandørprocedure |

Dato | Version x.x

IT/OT-leverandør-sikkerhedsprocedure

termer

|  |  |
| --- | --- |
| Begreb eller forkortelse i teksten | Beskrivelse |
| FAT | Factory Acceptance Test (FAT) verificerer, at systemet og dets komponenter fungerer korrekt og at al produktion og konfiguration af fremstillingssammensætningerne er udført korrekt. Samtidig testes det, at systemets ydeevne er i overensstemmelse med den aftalte kravspecifikation. |
| 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. |
| PLC | Programmable Logic Controller' (PLC) er en programmerbar computer til kontrol af produktionsprocesser. |
| VPN | Virtuelt Privat Netværk (VPN). En VPN benyttes til at skabe en sikker krypteret forbindelse, der muliggør fjernadgang til IT- eller OT-netværket. Da forbindelsen er end-to-end krypteret, kan forbindelse bruges på sikre, såvel usikre netværk.  Forbindelsen bør altid sikres med brugernavn og kodeord og 2-faktor autentifikation. |
| SAT | Site Acceptance Test (SAT) finder sted efter installationen, og den endelige konfiguration har fundet sted. Denne test gentager FAT, eller en acceptabel delmængde af FAT, for at kontrollere, at der ikke er opstået skade under forsendelse eller installation. |
| SLA | Service Level Agreement (SLA) er en aftale mellem kunde og serviceudbydere, der definerer nødvendige tjenester og det forventede serviceniveau. |

VERsions- og Godkendelseshistorik

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

Kontaktpersoner

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)  Skriv din titel her, fx konsulent  Tlf.: +45 xxxx xxxx  [xxx@domæne.dk](mailto:xxx@domæne.dk)  <Organisation> | Fornavn Efternavn (initialer)  Skriv din titel her, fx konsulent  Tlf.: +45 xxxx xxxx  [xxx@domæne.dk](mailto:xxx@domæne.dk)  <Organisation> |

Indholdsfortegnelse

[1 Genstand for politikken 4](#_Toc194409775)

[1.1 Omfang 4](#_Toc194409776)

[1.2 Konsekvenser ved manglende overholdelse 4](#_Toc194409777)

[2 Leverandørens Medarbejderes roller & ansvar 5](#_Toc194409778)

[3 Netværksadgang 5](#_Toc194409779)

[4 Fjernadgange 5](#_Toc194409780)

[5 Bærbare medier 6](#_Toc194409781)

[6 Patch management 6](#_Toc194409782)

[7 Change management 6](#_Toc194409783)

[7.1 Installation af nyt 7](#_Toc194409784)

[7.2 Dokumentation 7](#_Toc194409785)

[8 Backup og restore 7](#_Toc194409786)

[9 Hændelseshåndtering 8](#_Toc194409787)

# Formål for proceduren

Denne IT/OT-Leverandørsikkerhedprocedure er udarbejdet af med henblik på s overholdelse af gældende regler om styrket beredskab for energisektoren og modstandsdygtighed og beredskab i energisektoren. Reglerne foreskriver, at skal udarbejde politikker og procedurer for deres respektive leverandører for at sikre forsyningskædesikkerheden og derved forsyningssikkerheden af tjenester.

s IT/OT-Leverandørsikkerhedprocedure har til formål at rammesætte og understøtte selskabets overordnede krav og retningslinjer for sikkerhed i det omfang s leverandører har en indvirkning herpå.

har med udgangspunkt i s overordnede it-sikkerhedspolitik, risikostyringspolitik og risikovurdering fastsat bestemmelserne i denne procedure.

I anvendes leverandører som kompetence og ressourcestøtte til understøttelse af s administration og drift. Leverandører er en vigtig del af s forsvar og kriseberedskab. Procedurerne indeholder alle områder og aktiviteter, som der skal tages højde for og som kan have en indvirkning på opnåelsen af organisationens forretningsmæssige mål og opretholdelse af det fornødne sikkerhedsniveau.

IT/OT-Leverandørsikkerhedsproceduren skal til enhver tid understøtte s værdigrundlag og tilstræbe at opgaver der er overlagt til Leverandøren udføres på en måde som overholder s politikker og retningslinjer, og samtidig er driftssikker og at adgange (både fysiske og virtuelle) er målrettet de konkrete opgaver.

Afvigelser fra proceduren kan godkendes men kun i samarbejde med . Dette skal afspejles i s risikovurdering af den enkelte leverandør, samt fremgå af leverandøraftalen.

## Omfang

Denne procedure omfatter følgende typer leverandører:

* OT-leverandører som understøtter <Organisation>s produktion. Dvs. alle komponenter (generatorer, pumper, motorer, PLC’er, målere etc.), som indgår i produktionen af fjernvarme.
* IT-leverandører som understøtter <Organisation>s lokale IT-services og komponenter.
* Netværksleverandører som leverer og supporterer <Organisation>s IT/OT-netværk (routere, switches, firewalls etc.)

Herefter kaldt Leverandører.

Politikken dækker ikke SaaS leverandører.

# <Organisation>s ansvar

Det er s ansvar at der for hver Leverandør indgås der en aftale om den pågældende Leverandørs medarbejdere og ansvar, således at aftalen afspejler s krav og forventninger til den pågældende leverandør.

Det er s ansvar at der for hver Leverandør udarbejdes en risikovurdering for de services som den pågældende Leverandør leverer til Det er . Det er s ansvar at aftalen med Leverandøren afspejler denne risikovurdering.

For alle IT/OT-leverandører skal der indgås ente en databehandleraftale eller en fortrolighedsaftale, som tillæg til leverandøraftalen.

Ve ændringer i denne procedure er det s ansvar at gennemgå eksisterende aftaler og sikre overholdelse.

# Uddannelse af medarbejdere

Det skal via aftale med leverandøren skriftligt sikres, at det er Leverandørens ansvar at alle deres medarbejdere, med adgang til s netværk, systemer eller data, gennem uddannelse og udvikling, skal opnå sikkerhedsbevidsthed om nødvendigheden af at overholde s sikkerhedsmæssige retningslinjer.

# Adgangsstyring

For Leverandører, for hvem der er behov for adgang til s netværk, systemer eller data, skal det fremgå af aftalen at:

* alle deres medarbejderes adgange til s netværk, systemer eller data tilpasses det arbejdsmæssige behov for den enkelte medarbejder, og overholder s adgangsstyringsprocedurer og -retningslinjer
* der er påkrævet sanering af deres medarbejderes adgange som minimum kvartalsvis, og at skal orienteres om ændringer
* det er påkrævet svar indenfor 5 arbejdsdage, når foretager forespørgel på Leverandørens medarbejderes adgange og rettigheder til s netværk, systemer eller data.

## Netværksadgang

Det skal fremgå af alle aftaler at alle eksterne kommunikationsforbindelser skal forud godkendes af og af evt. understøttende netværksleverandør, og at enheder og bærbare medier med adgang til OT-netværket, skal være hærdet[[1]](#footnote-2) og ikke må benyttes til privat brug.

Enheder og bærbare medier må kun tilkobles netværket jf. den specifikke aftale med den enkelte Leverandør.

## Fjernadgange

For Leverandører med behov for fjernadgang til s netværk, skal der indgås aftale om, at disse skal benytte den etablerede procedure for fjernadgang. Der må ikke opsættes komponenter på s netværk til omgåelse af den etablerede procedure.

Den etablerede procedurer sikrer at adgang til netværket kræver VPN og MFA, samt at fjernadgange er tidsbegrænsede og opgavebestemt; hvilket betyder at den oprettede brugeradgang ikke er aktiv med mindre opgave og tidsperiode for udførelsen af opgaven er aftalt med <Organisation>.

# Patch management

For Leverandører, som enten har installeret eget hardware eller software på s netværk, eller som har leveret hardware eller software til , og som har indgået en vedligeholdelsesaftale, skal det via aftalen sikres er det deres ansvar at sikre patch management procedurer og forberede en patch management plan for de relaterede komponenter.

Der skal af aftalen fremgå at Leverandøren er ansvarlig for at holde sig orienteret om evt. sårbarheder og sikkerhedsopdateringer relateret til det omfattede software og hardware, samt at foreslå mitigerende handlinger til .

SLA-aftaler for patch management skal indgå i aftalen med den pågældende Leverandør.

# Change management

For Leverandører, som enten har installeret eget hardware eller software på s netværk, eller som har leveret hardware eller software til , og som har indgået en vedligeholdelsesaftale, skal det via aftalen sikres, at der føres en log over ændringer, og at ændringer inkl. deres omfang og konsekvens afrapporteres til , samt at større ændringer skal aftales og godkendes af *.*

Der skal indgås aftale om at Leverandøren skal sikre, at der ved installation af nye, og modifikation af eksisterende, interne systemer og komponenter med påvirkningsmulighed til s produktion gennemføres en forudgående risiko- og sikkerhedsvurdering.

## Installation af nyt

I leverandøraftalen skal det fremgå at Leverandøren skal sikre at nye komponenter leveres med det nyeste operativsystem (OS) og patch niveau, samt at de er hærdet jf. producentens anbefalinger inkl. men ikke udtømmende:

* Ingen brug af producentens standard indstillinger for adgangskontrol. Leverandøren skal give en liste over relevante brugernavne og adgangskoder, og det skal være muligt for at skifte brugernavne og adgangskoder evt. i samarbejde med Leverandøren.
* Alle unødvendige kommunikationsporte og -services lukkes, både virtuelle og fysiske porte.

Desuden skal det fremgå at Leverandøren skal sikre at nye komponenter kan patches og ikke har en ”end-of-life” indenfor X år fra datoen for indgået kontrakt.

## Dokumentation

I leverandøraftalen skal det fremgå at Leverandøren, ved installering af hardware og/eller software på s netværk eller enheder, skal levere dokumentation af samme inkl. produktnummer pr. system og enhed, ”end-of-life” og ”end-of-support”, samt evt. kritiske reservedele og en aftale om fremskaffelse af disse reservedele i en aftalt periode på minimum X år.

I aftalen skal det fremgå, at Leverandøren skal sikre, at har den nødvendige information til at opdatere s netværksdokumentation og fortegnelser, samt at der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for leverandørens område.

Desuden skal det fremgå at Leverandøren skal dokumentere at der udføres test inden of efter levering inkl. sikring mod indbyggede kendte sårbarheder (FAT og SAT).

I aftalen skal der stå at al dokumentation skal leveres i digital form.

# Backup og restore

For Leverandører, med hvem der er indgået en vedligeholdelsesaftale, skal der indgås en aftale om backup og reetableringsprocedurer (restore) for de relaterede komponenter ift. sourcekode og konfiguration.

For Leverandører, med hvem der er indgået en aftale om backup af data, skal der indgås en aftale om backup og reetableringsprocedurer for de aftalte data.

SLA-aftaler for backup og genskabelse skal indgå i aftalen med den pågældende leverandør. Der skal være krav om at Leverandøren udarbejder en vejledning til reetablering i en nødsituation (nødprocedure).

# Hændelseshåndtering

For Leverandører, med hvem der er indgået en aftale om service og vedligehold af komponenter, skal der indgås aftale om et kontaktpunkt og tidsrum ift. support, samt hvordan disse indgår i s hændelseshåndteringsprocedurer, kriseberedskabsplaner, beredskabsøvelser og risikovurderingsarbejdet for .

Aftalen skal sikre at Leverandøren indgår i opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Dvs. at Leverandøren skal bistå med at undersøge årsagen til hændelsen, herunder ved at tilvejebringe relevante informationer o.l. til brug for undersøgelsesarbejdet og til brug for rapportering af hændelsen, samt i rimeligt omfang bistå med dennes rapporteringsforpligtelser overfor myndighederne.

Der skal aftales et kontaktpunkt, hvor igennem Leverandøren skal rapportere hændelsen og resultatet til uden unødigt ophold.

# kontrol

For Leverandører, hvor dette er relevant, skal det fremgå af aftalen, hvordan Leverandøren understøtter s egenkontrol jf. s århjul, fx ift. opfølgning på logs, konfiguration, adgangskontrol etc.

# Tilsyn

For alle Leverandører skal der indgås aftale om s tilsyn med Leverandøren pba. s risikovurdering af leverandørforholdet. Tilsyn og kontrol kan fx udføres som:

* Leverandøren får udarbejdet relevant revisionserklæring eller certificering og orienterer om resultatet
* fører selv tilsyn
* indgår aftale med en tredjepart til kontrol af sikkerhedsforanstaltninger

For udvalgte Leverandører skal der indgås aftale om Leverandørens understøttelse af i forbindelse med Energistyrelsens tilsyn af .

1. Via sikker konfiguration, anti-virus og firewalls etc. minimeres risiko for infiltration af malware. [↑](#footnote-ref-2)