Skabelon for IT/OT-leverandør sikkerhedspolitik

Følgende dokument er en skabelon til udarbejdelse af en IT/OT-leverandør sikkerhedspolitik, 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 sikkerhedspolitik, 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.

Dato | Version x.x

IT/OT-leverandør sikkerhedspolitik

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. |
| PLC | PLC står for 'programmable logic controller' og er en programmerbar computer til kontrol af produktionsprocesser. |
| VPN | VPN står for Virtuelt Privat Netværk. 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. |
| SLA | Service Level Agreement (SLA) er en aftale mellem kunde og serviceudbydere, der definerer nødvendige tjenester og det forventede serviceniveau. |

Revisions- og Godkendelseshistorik

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

Kontaktpersoner

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)Skriv din titel her, fx konsulentTlf.: +45 xxxx xxxxxxx@domæne.dk<Organisation> | Fornavn Efternavn (initialer)Skriv din titel her, fx konsulentTlf.: +45 xxxx xxxxxxx@domæne.dk<Organisation> |

Indholdsfortegnelse

[1 Genstand for politikken 4](#_Toc184154077)

[1.1 Konsekvenser ved manglende overholdelse 4](#_Toc184154078)

[2 Leverandørens Medarbejdres roller & ansvar 5](#_Toc184154079)

[3 Netværksadgang 5](#_Toc184154080)

[4 Fjernadgange 5](#_Toc184154081)

[5 Bærbare medier 6](#_Toc184154082)

[6 Patch management 6](#_Toc184154083)

[7 Change management 6](#_Toc184154084)

[8 Backup og restore 6](#_Toc184154085)

[9 Hændelseshåndtering 7](#_Toc184154086)

# Genstand for politikken

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

I anvendes IT/OT-leverandører som kompetence og ressourcestøtte til understøttelse af s administration og drift. Leverandøren er en vigtig del af s forsvar og kriseberedskab. IT/OT-leverandør sikkerhedspolitikken 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 IT-sikkerhedsniveau.

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

## Omfang

Denne politik 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.

Herefter kaldt Leverandører.

Politikken dækker ikke SaaS leverandører.

## Konsekvenser ved manglende overholdelse

Brud på denne politik vil ses som et brud på kontrakten med Leverandøren, og kontraktens misvedligeholdelsesaftaler vil træde i kraft.

# Leverandørens Medarbejderes roller & ansvar

For hver Leverandør indgås der en aftale om den pågældende Leverandørs medarbejdere og ansvar, således at:

* alle deres medarbejderes adgange tilpasses det arbejdsmæssige behov for den enkelte medarbejder
* alle deres medarbejdere, med adgang til s systemer, netværk eller data, gennem uddannelse og udvikling, skal opnå sikkerhedsbevidsthed om nødvendigheden af at overholde s sikkerhedsmæssige retningslinjer
* at udskiftning af medarbejdere meddeles med rettidig omhu, således at adgange lukkes ikke senere end 10 arbejdsdage efter medarbejderens arbejdsskifte og nye adgang tildeles mindst 1 arbejdsdag før denne skal bruges
* at der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for leverandørens område
* at leve op til punkterne i databehandler- / fortrolighedsaftalen.

# Netværksadgang

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

# Fjernadgange

Fjernadgang til s netværk skal gå via den etablerede procedure for fjernadgang. Der må som udgangspunkt ikke opsættes komponenter til omgåelse af den etablerede procedure.

Tildeling og fjernelse af adgang fås ved henvendelse til kontaktpunkt.

Adgang til netværket kræver VPN, som også opsættes via henvendelse til kontaktpunkt.

# Bærbare medier

Bærbare medier må tilkobles netværket jf. den specifikke aftale med den enkelte Leverandør.

Bærbare medier skal sikres således at risiko for infiltration af malware minimeres. Dvs. at i det omfang det er muligt, skal det bærbare medie være: holdt opdateret sikkerhedsmæssigt, anti-virus og firewalls etc.

# Patch management

For de Leverandører, hvor der er indgået aftale herom, er det deres ansvar at sikre patch management procedurer for de relaterede komponenter. SLA-aftaler for patch management indgår i aftalen med den pågældende Leverandør.

# Change management

Ved ændringer i komponenter skal det sikres, at der føres en log over ændringer, og at ændringer inkl. deres omfang og konsekvens afrapporteres til . Ved større ændringer skal disse aftales og godkendes af *.*

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-/sikkerhedsvurdering

# Backup og restore

For de Leverandører, hvor der er indgået aftale herom, er det deres ansvar at sikre backup og genskabelsesprocedurer (restore) for de relaterede komponenter. SLA-aftaler for backup og genskabelse indgår i aftalen med den pågældende leverandør.

# Hændelseshåndtering

For de IT- og/eller OT-leverandører, hvor der er indgået aftale om service og vedligehold af komponenter, er der indgået aftale om et kontaktpunkt og tidsrum ift. support, samt hvordan disse indgår i s hændelseshåndteringsprocedurer og kriseberedskabsplaner.

Leverandøren skal indgå i opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud.

Leverandøren skal rapportere hændelsen og resultatet til via kontaktpunkt.