**Miljøstyrelsens DCIS**



**Skabelon for IT-sikkerhedspolitik**

# *Indledning*

Indledningen skal slettes og er kun inkluderet for at give en vejledning til skabelonen.

## *Læsevejledning*

Tekst der er markeret i *rød kursiv* er vejledende tekst, der forklarer, hvad afsnittet skal indeholde. Dette skal fjernes i udmøntningen af politikken.

Tekst der er markeret *grøn kursiv* skal erstattes med relevant information, fx navn på forsyningsselskabet, it-system, specifik rolle mv.

Yderligere tekst er teksteksempler på, hvordan en it-sikkerhedspolitik kan se ud i form af specifikke krav, beskrivelser og specificeringer. Denne tekst er ment som eksempel på indhold. Det er vigtigt, at teksten redigeres, så teksten reflekterer forsyningsselskabets kontekst, organisering, strategi, it-setup, sikkerhedskrav mv.

# *Miljøstyrelsens DCIS-strategi: Initiativ 1 – IT-sikkerhedspolitik*

En nedskrevet it-sikkerhedspolitik er et vigtigt element i arbejdet med at styrke cyber- og informationssikkerheden og derved forebygge cyberangreb. En it-sikkerhedspolitik sikrer, at forsyningsselskabets ledelse og medarbejdere har mulighed for at forstå, hvordan forsyningsselskabet forholder sig til it-sikkerhed.

It-sikkerhedspolitikken sætter rammerne for forsyningsselskabet på et overordnet niveau. It-sikkerhedspolitikken indeholder overordnede målsætninger og placerer det overordnede ansvar for cyber- og informationssikkerheden i forsyningsselskabet. It-sikkerhedspolitikken udgør fundamentet for, at forsyningsselskabet kan udarbejde underliggende politikker, retningslinjer og procedurer for it-anvendelsen, der er konkrete, implementerbare og i overensstemmelse med It-sikkerhedspolitikken.

Indholdsfortegnelse

[*Indledning* 2](#_Toc147748516)

[*Læsevejledning* 2](#_Toc147748517)

[*Miljøstyrelsens DCIS-strategi: Initiativ 1 – IT-sikkerhedspolitik* 2](#_Toc147748518)

[1. Introduktion 4](#_Toc147748519)

[1.1. Formål 4](#_Toc147748520)

[1.2 Målsætninger 4](#_Toc147748521)

[2. Gyldighedsområdet 5](#_Toc147748522)

[3. Roller og ansvar 5](#_Toc147748523)

[4. Underliggende politikker, retningslinjer og procedurer 7](#_Toc147748524)

[ Organisering af informationssikkerhed 7](#_Toc147748525)

[ Sikkerhedsbevidsthed (awareness) 7](#_Toc147748526)

[ Medarbejdersikkerhed 8](#_Toc147748527)

[ Risikostyring 8](#_Toc147748528)

[ Sikkerhedshændelser: 8](#_Toc147748529)

[ It-beredskab: 8](#_Toc147748530)

[ Fysisk sikring og miljøsikring: 8](#_Toc147748531)

[ Driftssikkerhed 8](#_Toc147748532)

[ Adgangsstyring: 8](#_Toc147748533)

[ Ændringshåndtering 8](#_Toc147748534)

[ Styring af aktiver: 9](#_Toc147748535)

[ Leverandørstyring og outsourcing 9](#_Toc147748536)

[ Klassifikationspolitik: 9](#_Toc147748537)

[ Kommunikationssikkerhed: 9](#_Toc147748538)

[5. Formaliteter ved politikken 9](#_Toc147748539)

[5.1. Undtagelser fra politikken 9](#_Toc147748540)

[5.2. Internt tilsyn og evaluering 9](#_Toc147748541)

[5.3. Manglende overholdelse 10](#_Toc147748542)

[5.4. Godkendelse og opdatering af politik 10](#_Toc147748543)

[6. Implementering af politikken 10](#_Toc147748544)

[7. Versionshistorik 11](#_Toc147748545)

# 1. Introduktion

*Beskriv forsyningsselskabets samfundsvigtige funktion med at sikre drikkevands- og/eller spildevandsforsyningen. Introducér it-sikkerhedspolitikken. Skriv gerne en sætning eller to om organisationens kontekst og strategi.*

## 1.1. Formål

*Beskriv formålet med it-sikkerhedspolitikken.*

It-sikkerhedspolitikken er [*FORSYNINGSSELSKAB*]s overordnede politik for it-sikkerhed, der definerer og kommunikerer ledelsens strategi for og krav til it-sikkerheden.

 [*FORSYNINGSSELSKAB*]s it-sikkerhedspolitik fastsætter den strategiske ramme, der understøtter forsyningssikkerheden og forretningskontinuitet, samt beskyttelse af [*FORSYNINGSSELSKAB*]s forretningskritiske aktiver.

Underliggende politikker, procedurer og retningslinjer udmønter it-sikkerhedspolitikken og konkretiserer, hvordan kravene og processerne for implementering, adfærd og handlingsaktiviteter vedrørende specifikke emner skal udføres.

## 1.2 Målsætninger

*Beskriv de overordnede målsætninger for it-sikkerhedspolitikken – disse bør ses i lyset af forsyningsselskabets målsætninger og strategi for risikovurdering, beredskab og sikkerhed.*

Det er [*FORSYNINGSSELSKAB*]s mål at sikre en stabil og sikker it-drift, der understøtter [*FORSYNINGSSELSKAB*]s forsyningssikkerhed, herunder også kritisk it-infrastruktur som forsyningernes OT-systemer.

Samtidig skal politikken sikre bestyrelsen og [*FORSYNINGSSELSKAB*]s forpligtelse til at organisere og vedligeholde it-sikkerheden i overensstemmelse med lovkrav og andre eksterne krav (fx GDPR, ISO 27001 og NIS2).

[*FORSYNINGSSELSKAB*]s målsætning er, at data og systemers fortrolighed, tilgængelighed og integritet sikres tilstrækkeligt i forhold til relevante sikkerhedsrisici og krav – herunder lovkrav, men at sikkerhedsniveauet ligeledes afbalanceres over for omkostningerne, kapacitet og de forretningsmæssige behov.

På denne baggrund gennemfører [*FORSYNINGSSELSKAB*] alle nødvendige aktiviteter for at sikre:

* **Tilgængelighed:** At opnå en høj tilgængelighed med høje oppetider, sikker forsyning og minimeret risiko for nedbrud.
* **Integritet:** At opnå en pålidelig og korrekt funktion af informationssystemerne med minimeret risiko for ukorrekt datagrundlag, fx som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.
* **Fortrolighed:** At etablere mulighed for fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede og autentificerede brugere har adgang.

**For at opnå dette vil** [*FORSYNINGSSELSKAB*]: *[indsæt delmålsætninger / aktiviteter for at opnå mål*]: fx:

*Her skal indsættes delmålsætninger og aktiviteter for at opnå delmålsætningerne. Eksempler på delmålsætninger og aktiviteter er vist nedenfor.*

[*FORSYNINGSSELSKAB*]’s har den nødvendige viden om systemer, trusler og sårbarheder

* Identificere og registrere it-aktiver og systemer, så det er muligt at definere, hvilke der er kritiske for forsyningen og forretningskontinuitet.
* Risikovurdere kritiske systemer, kendte risici og sikkerhedshuller for at kunne prioritere sikkerhedsforanstaltninger og beredskabsarbejdet efter en risikobaseret tilgang.

[*FORSYNINGSSELSKAB*]’s har gennemført nødvendige foranstaltninger

* Sikre at it-sikkerhedskrav og politikker er udarbejdet, varetaget, og håndhævet.
* Udarbejde, teste og videreudvikle beredskabsplaner, der beskriver retningslinjer og procedurer, der skal mobiliseres og aktiveres i forbindelse med it-sikkerhedshændelser.
* Gennemføre nødvendige aktiviteter mht. sikkerhedsbevidsthed og uddannelse for at alle medarbejdere kender deres ansvar i relation til it-sikkerhed.

[*FORSYNINGSSELSKAB*]’s følger og handler på udviklingen på området

* Kontinuerligt holde sig orienteret om trusselsbillede og risici f.eks. via SektorCERT’s og Center for Cybersikkerheds løbende vurderinger. Vurderingerne kan læses på <https://sektorcert.dk/publikationer/> og <https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/>.
* Kontinuerligt holde sig orienteret om ændringer i lovkrav, for at sikre at it-sikkerhedspolitikken og underliggende politikker, retningslinjer og procedurer opdateres til at være relevante og tilstrækkelige.

# 2. Gyldighedsområdet

*Beskriv gyldighedsområdet eller omfanget for it-sikkerhedspolitikken, herunder hvilke personer, systemer mv., der er omfattet af politikken. Hvis der er noget centralt, der er uden for gyldighedsområdet, bør dette også nævnes. Omfanget vil variere baseret på forsyningsselskabets størrelse, systemer og forretningsprocesser.*

*Denne politik omfatter al* it-anvendelse, der understøtter informationer, systemer og forretningsprocesser i [*FORSYNINGSSELSKAB*].

*It-sikkerhedspolitikken er gyldig for:*

* Alle [*FORSYNINGSSELSKAB*]s medarbejdere, midlertidigt ansatte og bestyrelsen.
* Alle eksterne leverandører, konsulenter og/eller andre tredjeparter der har arbejdsmæssig tilknytning til [*FORSYNINGSSELSKAB*] og/eller adgang til informationer, systemer eller kritiske forretningsprocesser, der tilhører, udbydes og anvendes af [*FORSYNINGSSELSKAB*]

Alle medarbejdere, midlertidigt ansatte, bestyrelsen, eksterne leverandører, konsulenter og eller andre tredjeparter, der har arbejdsmæssig tilknytning til [*FORSYNINGSSELSKAB*] gøres bekendt med politikken.

Se dog ”5.1. Undtagelser fra politikken”.

It-sikkerhedspolitikken træder i kraft fra udstedelsesdatoen, og udløber ikke, medmindre den erstattes af en anden politik. Se også afsnit ”5.4 Godkendelse og opdatering”.

# 3. Roller og ansvar

*Beskriv roller og tilhørende ansvarsområder/opgaver i relation til forsyningsselskabets it-sikkerhed. Roller og tilhørende ansvarsområder/opgaver i denne skabelon er ikke udtømmende. Ved udmøntning af politikken, tilpas da roller og ansvar til jeres egen organisation og organisering af it-sikkerhed. (Roller og ansvarsområder kan også formaliseres og detaljeres i større grad i en separat underliggende politik/retningslinje, som er et supplement til it-sikkerhedspolitikken)*

Cyber- og informationssikkerhed er alles ansvar og kræver, at alle medarbejdere, konsulenter, leverandører mv., bidrager til øget sikkerhedsbevidsthed og daglig varetagelse af it-sikkerheden.

Derfor er alle, der arbejder med eller for [*FORSYNINGSSELSKAB*] pålagt at efterleve regler og krav, der er fremlagt i denne it-sikkerhedspolitik, samt handlingsaktiviteter der fremkommer i underliggende politikker/retningslinjer/procedurer.

Hvis en medarbejder opdager, eller får mistanke om, trusler mod eller brud på it-sikkerheden, skal vedkommende straks underrette [*indsæt ønsket rolle*] om dette.

For at understøtte it-sikkerheden i [*FORSYNINGSSELSKAB*] er følgende organisering af it-sikkerheden defineret:

*Nedenstående kan være et separat dokument i stedet for at være inkluderet i it-sikkerhedspolitikken. Tilpas roller og ansvarsområder efter forsyningsselskabets organisering.*

|  |  |
| --- | --- |
| **Rolle**  | **Tilhørende ansvarsområder/opgaver**  |
| Bestyrelsen | * Det overordnede ansvar for it-sikkerheden i [*FORSYNINGSSELSKAB*], samt ansvar for at gennemgå og godkende denne politik, herunder at fastlægge strategiske målsætninger for it-sikkerheden.
* At evaluere [*FORSYNINGSSELSKAB*]s it-sikkerhed – fx tilsynsresultater eller evalueringsrapport efter en sikkerhedshændelse.
 |
| IT-sikkerhedschef | * Implementeringen af denne politik og underliggende politikker, retningslinjer og procedurer.
* At vedligeholde, gennemgå og udvikle denne politik, herunder fastlægge målsætninger og sikkerhedsniveauet for it-sikkerhed.
* At systemer lever op til det fastlagte sikkerhedsniveau, herunder at der er udarbejdet de nødvendige retningslinjer, procedurer mv., for brugen af systemer.
 |
| Driftsansvarlig | * At systemer lever op til det fastlagte sikkerhedsniveau, herunder at der er udarbejdet de nødvendige retningslinjer, procedurer mv., for brugen af systemer.
* At vedligeholde, gennemgå og udvikle denne politik, herunder fastlægge målsætninger og sikkerhedsniveauet for it-sikkerhed.
 |
| IT-sikkerhedsansvarlig | * Assistere med at vedligeholde, implementere og udvikle denne politik, herunder fastlægge målsætninger og sikkerhedsniveauet for it-sikkerhed.
* At løbende føre interne tilsyn med medarbejderes efterlevelse af it-sikkerhedspolitikken og underliggende politikker, retningslinjer og procedurer.
 |
| Medarbejdere | * Efterleve it-sikkerhedspolitikken samt underliggende retningslinjer, politikker og procedurer.
 |
| *[tilføj og rediger relevante roller]* | * *Tilføj og rediger yderlige ansvarsområder*
 |

# 4. Underliggende politikker, retningslinjer og procedurer

*Beskriv kort de implementerede underliggende dokumenter. Det er ikke et krav at alle underliggende dokumenter på listen inddrages. Omvendt kan der også medtages underliggende dokumenter, der ikke fremgår af listen. Der skal tages udgangspunkt i forsyningsselskabets egen risikoanalyse, egne ressourcer og eget sikkerhedsniveau/modenhedsniveau, når det fastlægges hvilke dokumenter, der skal indgå. Formålet er at få hævet forsyningsselskabets sikkerhedsniveau/modenhedsniveau, men samtidig skal arbejdet med it-sikkerhedspolitikken være overkommeligt. Det gælder derfor om at udvælge de underliggende dokumenter, der skaber størst værdi for forsyningsselskabet. Forslag til underliggende politikker, retningslinjer og procedurer er herunder gruppereret i tre grupper, hvoraf forsyningerne med fordel kan starte med at udarbejde og implementere dokumenterne i gruppe 1, derefter gruppe 2 og til sidst gruppe 3.*

De underliggende dokumenter, der fremkommer i dette kapitel, er eksempler på konkrete politikker, retningslinjer og procedurer, der er nødvendige for [*FORSYNINGSSELSKAB*]s it-sikkerhed, og udmønter it-sikkerhedspolitikken.

[*FORSYNINGSSELSKAB*] vil:

1. Sikre ledelsesforankring. Ledelsen skal fastsætte en metode for at etablere, implementere, operere, monitorere, evaluere og forbedre it-sikkerheden for [*FORSYNINGSSELSKAB*]. Endvidere skal ledelsen fastlægge [*FORSYNINGSSELSKAB*]s metodik og tilgang for risikostyring inkl. identifikation, håndtering og evaluering af risici.
2. Baseret på identifikation af kritiske aktiver og it-systemer samt risikovurdering af disse og relevante trusler, vil [*FORSYNINGSSELSKAB*] gennemgå målsætningerne i denne it-sikkerhedspolitik, samt evaluere implementerede sikkerhedskontroller og tiltag for at sikre, at sikkerhedsniveauet er tilstrækkeligt med hensyn til resultater af risikovurderinger, trusselsbillede og de forretningsmæssige behov.
3. Udarbejde og varetage politikker, retningslinjer, procedurer og tilhørende kontroller for tilstrækkeligt at beskytte aktiver, data og systemers fortrolighed, tilgængelighed og integritet i forhold til trusler og sårbarheder. Dertil hører at opretholde et sikkerhedsniveau, der er tilstrækkeligt for de forretningsmæssige behov og for at efterleve lovkrav. Dette inkluderer at udarbejde politikker, retningslinjer og procedurer for it-sikkerhed inden for de følgende områder:

*Gruppe 1*

* Organisering af informationssikkerhed:Formålet er at definere organiseringen af [*FORSYNINGSSELSKAB*]s it-sikkerhed, herunder roller og ansvarsfordeling. Retningslinjen vil fastlægge behovet for kompetencer og ressourcer for at varetage driftssikkerhed og forretningskontinuitet med et tilstrækkeligt sikkerhedsniveau. *Roller og ansvar kan defineres i it-sikkerhedspolitikken (kap. 3 i denne skabelon).*
* Sikkerhedsbevidsthed (awareness): Formålet med initiativet er*,* at etablere retningslinjer for at øge sikkerhedsbevidsthed vedr. it-sikkerhed – fx uddannelse og awareness træning. Det vil sige at sikre at alle [*FORSYNINGSSELSKAB*]s medarbejdere og relevante tredjeparter er indforstået med deres ansvarsområder og roller med hensyn til it-sikkerhed; at medarbejdere efterlever regler og krav fastsat i denne it-sikkerhedspolitik og underliggende politikker, retningslinjer og procedurer; samt uddanne medarbejdere vedr. ”god adfærd” og for at minimere risiko for menneskelige fejl.

*Eksempler kunne være uddannelse, oplæg og deltagelse i netværk.*

* Medarbejdersikkerhed: Formålet er at sikre, at alle medarbejdere har kendskab til og efterlever alle retningsliner og procedurer for it-sikkerhed både før, under og ved afsluttet ansættelse. [*FORSYNINGSSELSKAB*] er ansvarlig for at definere passende sikkerhedskrav og retningslinjer, samt kommunikere disse til medarbejdere og eventuelle tredjeparter.

*Fx sikkerhedskrav forbundet med it-udstyr, tilkobling til VPN, ikke tilladte applikationer og software, sikkerhedskrav forbundet med fjernarbejde, regler mht. anvendelse af privat udstyr, krav for kodeord osv.*

* Sikkerhedshændelser: Formålet er at etablere en formaliseret og effektiv tilgang til at håndtere sikkerhedshændelser*. Proceduren skal bl.a. omfatte hvordan man opdager en sikkerhedshændelse, hvordan man indmelder sikkerhedshændelser samt hvordan det vurderes og håndteres*
* It-beredskab: Formålet er at have en formaliseret og effektiv tilgang til at håndtere alvorlige it-sikkerhedshændelser, der udløser behov for krisehåndtering og beredskab, for at styrke og sikre [*FORSYNINGSSELSKAB*]s kapacitet for genoprettelse af forretningskritiske systemer og for at sikre rettidig reetablering af forsyningen og at varetage forretningskontinuiteten. *Der skal etableres beredskabsplan for it-beredskab, som indeholder krav for, hvornår planen skal aktiveres, identificerede risici og modtiltag/handlinger for at håndtere en alvorlig hændelse, roller og ansvarsområder, kommunikationsplan (intern, ekstern – fx med driftsleverandør og/eller DCIS), samt (systemspecifikke) plan(er) for genoprettelse af forretningskritiske systemer for at sikre rettidig reetablering af forsyningen.*

*Gruppe 2*

* Styring af aktiver: Formålet er at identificere, registrere og styre aktiver (software, hardware, data eller andre fysiske enheder). Dette er for at definere hvilke aktiver, der er kritiske for forretningen, definere tilstrækkelige sikkerhedsforanstaltninger og ansvarsområder samt modvirke uautoriseret adgang, modificering eller bortskaffelse af information og medier. *Proceduren bør endvidere indeholde vejledning for bortskaffelse og transport af aktiver (hvordan lagres, bortskaffes og evt. ødelægges aktiver, der indeholder fortrolig information).*
* Risikostyring**:** Formålet er, at [*FORSYNINGSSELSKAB*]s tilgang til it-sikkerhed og beredskab følger en risikobaseret tilgang, som prioriterer de største forretningsrisici, og beskyttelse af forretningskritiske systemer og aktiver for at sikre en strategisk tilgang til it-sikkerhed og forretningskontinuitet. *Der skal udarbejdes dokumenter som berører en metode for risikovurdering, risikovillighed samt risikohåndtering.*
* Fysisk sikring og miljøsikring: Formålet er at modvirke uautoriseret fysisk adgang, skade, uheld eller påvirkning på [*FORSYNINGSSELSKAB*]s systemer, information, aktiver, fysiske faciliteter og/eller operationer/drift. *Eksempelvis vejledninger, der fastsætter, at kritisk it- og evt. OT udstyr (hardware, software) skal være i sikre områder, beskyttet af fysiske barrierer, adgangskontroller, overvågning og alarmer mv.*
* Leverandørstyring og outsourcing: Formålet er at beskytte aktiver, systemer og operationer der er tilgængelige for eller varetages af tredjeparter, samt sikre et tilstrækkeligt niveau af it-sikkerhed, beredskab og tryg leverance. *Der skal udarbejdes en procedure som skal fastlægge krav for niveauet af it-sikkerhed, som leverandører/tredjeparter skal overholde (fx sikrings-foranstaltninger) eller processer de skal igennem. Proceduren for leverandørstyring skal også berøre udarbejdelse af databehandleraftale samt evt. årlige tilsyn.*
* Klassifikationspolitik: Formåleter at behandle information og data korrekt, herunder med tilstrækkelige tekniske og organisatoriske foranstaltninger, for at sikre beskyttelse af tilgængeligheden, integriteten og fortroligheden til informationsaktiver. *Der bør udarbejdes en klassifikationspolitik, der kortlægger forskellige niveauer af klassifikation af informationer (fx offentlig, intern og fortrolig) og passende sikkerhedsforanstaltninger (fx kryptering).*

*Gruppe 3*

* Driftssikkerhed: Formålet er at facilitere og varetage tryg, korrekt og sikker operation af driftsaktiviteter, herunder drift af systemer mht. teknisk drift. *Dokumenterne skal beskrive sikkerhedsforanstaltninger mod uautoriseret adgang, løbende back-up, samt logning og overvågning af brugeraktivitet.*
* Adgangsstyring: Formålet er at minimere adgang til information og faciliteter til personer med arbejdsbetinget behov. *Der skal defineres procedurer for at styre adgang og brugerrettigheder (og begrænsninger) til specifikke systemer og data, ved at definere brugerroller og tildele privilegerede adgangsrettigheder.*
* Ændringshåndtering: Formålet er at varetage it-sikkerheden ved anskaffelse af nyt eller ændring (udvikling, opdatering og varetagelse) af eksisterende systemer. *Ændringshåndteringsproceduren skal fastlægge processer for udvælgelse af nyt og/eller opdatering af eksisterende systemer, test af ændring, samt implementeringsprocedurer (inkl. backup og fallback procedurer)*
* Kommunikationssikkerhed: Formålet er at sikre at information, der kommunikeres over netværk (internt og eksternt), sker sikkert og har tilstrækkelige sikkerhedsforanstaltninger. *Proceduren vil beskrive, hvordan forsyningsselskabets interne netværk styres og overvåges, hvilke foranstaltninger der er på plads, adskillelse af brugere samt sikkerhedsniveau for overførsel af informationer (internt og eksternt, fx mht. fortrolighedsniveau og anvendelse af kryptering).*

# 5. Formaliteter ved politikken

## 5.1. Undtagelser fra politikken

*Beskriv undtagelser fra it-sikkerhedspolitikken samt hvordan dette dokumenteres.*

Alle undtagelser fra it-sikkerhedspolitikken samt underliggende politikker/retningslinjer/procedurer skal dokumenteres skriftligt og følge [*FORSYNINGSSELSKAB*]s formaliserede og fastsatte procedurer.

Forespørgsler om undtagelse fra it-sikkerhedspolitikken skal tydeligt beskrive hvad/hvordan henvendelsen er en undtagelse, en begrundelse for nødvendighed samt mulige risici forbundet med undtagelsen.

[*Evt. indsæt link til relevant procedure eller proces, evt. til SOA-dokumenter hvor undtagelser registreres*]

[*Alternativt, indsæt rolle og kontaktinformation på hvem man skal kontakte ved anmodninger om undtagelse fra it-sikkerhedspolitikken eller andre underliggende politikker, retningslinjer eller procedurer*]

## 5.2. Internt tilsyn og evaluering

*Beskriv krav for audit (tilsyn) eller eventuelle andre evalueringskrav der er gældende*

Det skal føres interne tilsyn med [*FORSYNINGSSELSKAB*]s it-sikkerhed. Tilsyn kan med fordel have en risikobaseret tilgang og afgrænsning. Resultater skal dokumenteres og gennemgås af bestyrelsen.

Alle [*FORSYNINGSSELSKAB*]s medarbejdere skal, såfremt det er muligt, assistere tilsynet ved at give tilgang til relevante dokumenter, systemer, procedurer, politikker mv. for at muliggøre [*FORSYNINGSSELSKAB*] (eller en uafhængig tredjepart) i at føre tilsyn og evaluering af overholdelse af it-sikkerhedspolitikken og underliggende politikker/retningslinjer/procedurer.

Alle kontrakter med eksterne leverandører skal inkludere en klausul vedrørende tilsyn med leverandørens overholdelse af kontrakten og [*FORSYNINGSSELSKAB*]s fastsatte it-sikkerhedskrav.

[*Evt. indsæt yderlige eksterne krav for tilsyn eller evaluering*]

[*Evt. tilføj link til aktuel leverandørstyringspolitik eller relevant retningslinje*]

## 5.3. Manglende overholdelse

*Beskriv regler og procedure for manglende overholdelse af it-sikkerhedspolitikken*

Hvis en af [*FORSYNINGSSELSKAB*]s ansatte eller en relevant tredjepart (fx leverandør eller konsulent) bliver opmærksom vedrørende et brud eller muligt brud på politikkens bestemmelser, skal vedkommende straks indrapportere dette til [*indsæt relevant rolle og kontaktinformation*].

For [*FORSYNINGSSELSKAB*]s medarbejdere kan manglende overholdelse af it-sikkerhedspolitikken samt underliggende politikker, retningslinjer og procedurer medføre [*indsæt ønsket handling jf. aktuel kontrakt*].

For tredjeparter, som fx leverandører og konsulenter, skal manglende overholdelse af it-sikkerhedspolitikken rapporteres til [*indsæt relevant rolle fx kontraktejer eller bestyrelsen], og kan medføre [indsæt ønsket handling jf. aktuel kontrakt*].

## 5.4. Godkendelse og opdatering af politik

*Beskriv hvor ofte og i hvilke tilfælde it-sikkerhedspolitikken skal opdateres (inkl. årlig gennemgang, revision og vedligeholdelse af politik (fx ved lovændringer)), samt hvem der er ansvarlig for revision og godkendelse.*

It-sikkerhedspolitikken gennemgås og godkendes minimum en gang årligt af [*indsæt navn på ansvarlig*].

Derudover revideres politikken, hvis der er fastsat et specifikt behov for det for at sikre politikkens fortsatte relevans med hensyn til [*FORSYNINGSSELSKAB*]s strategi og målsætninger, risikobillede og eksterne krav.

Alle revisioner skal godkendes af [*indsæt navn på rolle fx ‘bestyrelsen’ eller ‘bestyrelsesformand’*], og ajourføres i revisionshistorikken.

[*Evt. tilføj et årshjul/aktivitetstabel der anviser hvornår it-sikkerhedspolitikken, samt underliggende politiker/retningslinjer/procedurer mv. gennemgås*]

# 6. Implementering af politikken

Alle ansatte ved [*FORSYNINGSSELSKAB*] opfordres til at kontakte [*indsæt navn på relevant it-sikkerhedsansvarlig/eller anden rolle*] vedrørende spørgsmål til denne politik eller generelle henvendelser vedrørende overholdelse af politikker, retningslinjer og procedurer for it-sikkerhed.

[*FORSYNINGSSELSKAB*] skal sikre, at denne og alle underliggende politikker/retningslinjer/procedurer er tilgængelige for alle ansatte.

Det er [*indsæt relevant rolle*]s ansvar at kommunikere denne politik og underliggende politikker, retningslinjer og procedurer til alle ansatte ved [*FORSYNINGSSELSKAB*], og hvor det er relevant, leverandører eller andre tredjeparter, for at sikre kendskab og efterlevelse af it-sikkerhedspolitikken og underliggende dokumenter.

# 7. Versionshistorik

*Specificer og rediger versionshistorik inklusiv beskrivelse af gennemførte ændringer.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Dato** | **Revideret af** | **Godkendt af** | **Sammenfatning af ændringer** |
| ***[DD.MM.ÅÅ]*** | ***[indsæt navn]*** | ***[indsæt navn]*** | ***[beskriv hvad der er revideret]*** |

Godkendt den [*DD.MM.ÅÅÅÅ*], af, [*indsæt rolle, fx ‘bestyrelsesformand’*] af [*FORSYNINGSSELSKAB*].

Denne it-sikkerhedspolitik blev sidst gennemgået af [*indsæt rolle, fx ‘bestyrelsen’*] den [*DD.MM.ÅÅÅÅ*], på vegne af [*FORSYNINGSSELSKAB*].

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[*Indsæt navn*]

[*Indsæt rolle, fx ‘bestyrelsesformand’*]