Arcedi Biotech

Informationssikkerhedspolitik

1. Indholdsfortegnelse

2. Formål

Formålet med denne politik er at sætte rammen for arbejdet med informationssikkerhed i Arcedi Biotech.

3. Gyldighedsområde

Denne politik er gældende for Arcedi Biotech A/S.

4. Princip

Informationssikkerhed styres baseret på principperne i ISO 27001, juridiske og regulatoriske krav samt forretningsbehov.

5. Forpligtigelse

Som virksomhed er behandling af information afgørende for vores succes, og beskyttelsen og sikkerheden af disse oplysninger er en prioritet på ledelsesniveau. Uanset om det er forretningsinformation, medarbejderinformation, information om kunder eller andre eksterne parter, tager vi vores forpligtelser under GDPR, NIS2 og øvrig relevant lovgivning alvorligt.
Vi forpligtiger os på at engagere os i arbejdet med informationssikkerhed, samt afsætte de nødvendige ressourcer til at udvikle, implementere og kontinuerligt forbedre informationssikkerhedsstyringen passende for vores forretning.

6. Informationssikkerhed

6.1. Formålet med informationssikkerhed

God informationssikkerhed er forudsætningen for beskyttelse af de oplysninger, der er betroet os.
Mangelfuld informationssikkerhed kan have betydelige negative konsekvenser for vores medarbejdere, vores kunder, vores omdømme, vores økonomi og i yderste konsekvens for samfundet.

Ved at have et effektivt ledelsessystem for informationssikkerhed kan vi:

- Sikre at de rigtige personer, har den rigtige adgang (fortrolighed) til de rigtige data (integritet) på det rigtige tidspunkt (tilgængelighed), og derved opretholde en høj grad af tillid mellem Arcedi Biotech og vores samarbejdspartnere, samt medarbejdere.
- Sikre en effektiv og stabil forretningsdrift.
- Sikre at vi overholder vores juridiske, lovgivningsmæssige og kontraktlige forpligtelser.

6.2. Risikoappetit

Samlet set har Arcedi Biotech en **moderat** risikoappetit, hvilket betyder, at vi:

- Balancerer mellem sikkerhed og innovation.
- Investerer i informationssikkerhed i et omfang, der understøtter vores moderate risikoappetit. Dvs. at anvendte ressourcer skal balanceres ift. den besluttede risikoappetit.
- Implementerer solide sikkerhedsforanstaltninger, men også er villig til at prøve nye teknologier efter forudgående risikovurdering.
- Har politikker og procedurer, der ved behov kan tilpasses nye trusler og muligheder.
- Er opmærksom på risici, men er villig til at acceptere moderate risici for at opnå forretningsfordele.

Grundet naturen af vores forretningsaktiviteter vægtes FORTROLIGHED og INTEGRITET af information generelt over TILGÆNGELIGHED af information.
Risikoappetitten beskrives i flere detaljer af informationssikkerhedsudvalget.

6.3. Mål for informationssikkerhed

1. At sikre fortroligheden, integriteten og sekundært tilgængeligheden af virksomhedens oplysninger, herunder personoplysninger baseret på god risikostyring, juridiske, lovgivningsmæssige og kontraktlige forpligtelser og forretningsbehov.
2. At tilvejebringe og anvende effektivt de ressourcer, der kræves for at udvikle, implementere og løbende forbedre informationssikkerhedsstyringssystemet.
3. At implementere en god informationssikkerhedskultur gennem effektiv uddannelse og træning.
4. Opnå D-mærkning[1] af virksomheden inden udgangen af 2026.

Ovenstående mål nedbrydes til delmål af informationssikkerhedsudvalget.

6.4. Informationssikkerhedsramme

Denne politik udgør sammen med en række emnespecifikke politikker, processer og procedurer rammen for informationssikkerhedsstyring i Arcedi Biotech.

Behovet for emnespecifikke politikker afgøres af informationssikkerhedsudvalget, dog skal følgende områder, som minimum være dækket:

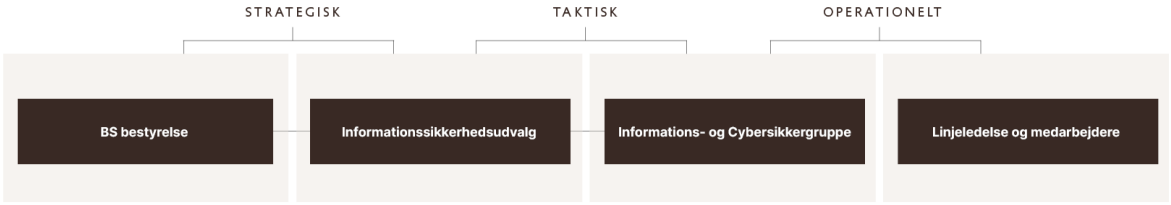
- Styring af informationsaktiver og risici.
- Håndtering af sikkerhedshændelser.
- Driftskontinuitet og krisestyring.
- Forsyningskædesikkerhed.
- Adgangskontrol – både fysisk og digitalt.
- Sikkerhedstræning og uddannelse.
- Regler for informationssikkerhed (acceptabelt brug).
- Personalesikkerhed.
- Systemsikkerhed (tekniske krav).
- Persondatasikkerhed.
- Dataetik
- Evaluering og vurdering af effektiviteten af informationssikkerhed.

[1] D-mærket er en dansk ordning, der kombinerer it-sikkerhed og ansvarlig dataanvendelse i ét mærke, og dermed skaber basis for overholdelse af både NIS2 og GDPR.
Hvad er D-mærket?

6.5. Organisering af informationssikkerhed

Informationssikkerhed er alles ansvar, herunder at forstå og overholde politikkerne, følge, behandle og rapportere formodede eller faktiske overtrædelser.

Desuden er arbejdet med informationssikkerhed i Arcedi Biotech organiseret som følger.



6.5.1. Arcedi ledelsesteam

- Godkender informationssikkerhedspolitikken, herunder mål for informationssikkerhed og risikoappetit, samt sikrer kompatibilitet med organisationens strategiske retning.
- Fører tilsyn med informationssikkerhed gennem årlig rapportering.
- Deltager i relevante kurser eller uddannelse om styring af informations- og cybersikkerhedsrisici og tilskynder til at tilsvarende kurser tilbydes til enhedens øvrige ansatte i det omfang, at det er relevant.

6.5.2. Informationssikkerhedsudvalg

Består af CEO, CFO, COO, CIO (IT-direktøren) og Cyber- og informationssikkerhedskonsulenten for BS & Co, samt CEO for selskaber, der er omfattet jf. punkt 3 “Gyldighedsområde”.

- Godkender og aftaler ressourcer og delmål for informationssikkerhed.
- Godkender emnespecifikke politikker relateret til informationssikkerhed.
- Overordnet ansvarlig for implementeringen af politikker og kontinuerlige forbedringer af informationssikkerhedsstyringssystemet.
- Ansvarlig for krisestyring.

6.5.3. Informations- og Cybersikkerhedsgruppe

En gruppe af personer med faglig ekspertise og ansvar indenfor forskellige discipliner (f.eks.: Compliance, IT, Fysisk sikkerhed & HR).

Arbejdet i gruppen ledes af CIO for Arcedi.

- Daglig drift af informationssikkerhedsstyringssystemet, herunder:

    - Identificerer og styrer risici forbundet med informationsaktiver i samarbejde med relevante systemejere og procesejere.
    - Vedligeholder og gennemgår sikkerhedskontroller af informationsaktiver i samarbejde med relevante systemejere og procesejere.
    - Udvikler processer, procedurer, vejledninger eller lignende, der skal sikre en ensartet og effektiv overholdelse af de emnespecifikke politikker. Dette sker i samarbejde med linjeledelse og med iagttagelse af at indsatser sker med effektivitet og produktivitet in mente.
    - Kommunikerer informationssikkerhed til organisationen.
    - Tilbyder træning og rådgivning til alle medarbejdere om informationssikkerhed.
    - Håndterer informationssikkerhedsrelaterede hændelser.
    - Sikrer effektiv tredjepartsstyring af leverandører og tredjeparter.
    - Sikrer, at passende driftskontinuitetsplaner er dokumenteret, på plads og testet periodisk.
- Leder den kontinuerlige forbedringsproces, herunder:
    - Udvikler og forbedrer løbende dokumentationen for informationssikkerhedsstyringssystemet.
    - Gennemfører et struktureret revisions-/auditprogram af alle områder af informationssikkerhedsstyringssystemet baseret på risiko over en periode på maksimalt 3 år.
    - For produktionsrelevante processer, gennemføre et struktureret auditprogram minimum en gang årligt.
- Rapporterer til informationssikkerhedsudvalget f.s.v.a. revisionsresultater, hændelser, risikostyring og løbende forbedringer.

6.5.4. Linjeledelse

Enhver leder med personaleansvar.

- Promoverer overholdelse af informationssikkerhedskrav, samt kontinuerlig forbedring af informationssikkerheden.
- Allokerer ressourcer for at sikre integrationen af informationssikkerhedskrav i organisationens processer.
- Rapporterer om projekter eller interne og eksterne faktorer, der kan påvirke informationssikkerhedstiltag.

7. Overholdelse af politik

7.1. Måling og rapportering

Overholdelse af denne politik verificeres gennem forskellige metoder, herunder, men ikke begrænset til, interne og eksterne revisioner/audits.
Status rapporteres til Arcedi ledelsesteam minimum årligt.

7.2. Undtagelser

Enhver undtagelse fra politikken skal godkendes og registreres af informationssikkerhedsudvalget. Væsentlige undtagelser eller afvigelser rapporteres til Arcedi ledelsesteam løbende.

7.3. Manglende overholdelse

Gentagen eller bevidst væsentlig overtrædelse af denne politik, kan medføre disciplinære foranstaltninger, op til og inklusive opsigelse af ansættelsen og bortvisning.

7.4. Revision

Politikken revideres og godkendes på ny af Arcedi ledelsesteam ved behov, dog minimum en gang årligt.

8. Dokumentstyring

Version	Ændret	Ændret af	Ændringer
0.1	27-05-2025	Mathias Kølvraa	Første udkast
0.2	11-06-2025	Mathias Kølvraa	Anden udkast

Version	Godkendt	Godkendt af	Bemærkninger
1.0	18-06-2025	Arcedi Ledelsesteam	Forankring ændret fra bestyrelse til Arcedi ledelsesteam