BIOFOS Holding A/S Refshalevej 250 DK-1432 København K
post@biofos.dk www.biofos.dk
Tlf: +45 32 57 32 32 CVR nr. 25 60 89 25

Bestyrelsesmøde 13. september 2019

5. september 2019

Pkt. 10. Informationssikkerhedspolitik

1. Indstilling
Det indstilles til bestyrelsen at godkende Informationssikkerhedspolitik for BIOFOS.

2. Baggrund
I BIOFOS er det vigtigt, at IT understøtter lovgivningen, vores overordnede strategi, værdier og kerneprocesser. BIOFOS vil leve op til vidtgående krav om forsyningssikkerhed, driftssikkerhed og kvalitet. Samtidig lægges stor vægt på overholdelse af lovgivningskrav herunder GDPR og personsikkerhed, at systemerne er brugervenlige, dvs. uden unødigt besværlige sikringsforanstaltninger, samt at fortrolighed kan opnås for de dokumenter og data, der har særligt behov herfor.

For BIOFOS drejer informationssikkerhed sig om beskyttelse af personer og driftsanlæg samt ressourcer, der indgår i eller bidrager til BIOFOS' elektroniske databehandling og kommunikation.

Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskelige trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

BIOFOS har hidtil iværksat en række tiltag til at styrke informationssikkerheden, og på nuværende tidspunkt vurderes det hensigtsmæssigt, at der defineres en egentlig informationssikkerhedspolitik. Forslag til informationssikkerhedspolitik for BIOFOS er vedlagt som bilag.

3. Implementering af politikken
Der er som sagt allerede iværksat flere opgaver og arbejdsgange, som skal sikre en kontinuerlig styring af informationssikkerheden. For at få et indblik i, hvorledes politikken enten allerede er blevet eller vil blive implementeret, gives i det nedenstående en kort status af implementering af politikkens enkelte elementer.

Elementer fra politikken	Implementering
Den skal efterleve gældende lovgivning og understøtte BIOFOS' strategi.	Retningslinjer tilpasses løbende BIOFOS' strategi og lovgivning og udmøntes i et årshjul, der følges. Er gennemført.
Økonomidirektøren er den overordnede ansvarlige for informationssikkerhed.	Den daglige drift overvåges af IT, og økonomidirektøren holdes løbende orienteret. Er allerede i drift.

Elementer fra politikken	Implementering
Beskrivelse af roller og ansvar for informationssikkerheden, herunder udpegning af systemansvarlige for alle IT-systemer.	Oversigt over systemejere og rollebeskrivelse med tilhørende ansvarsområder og rettigheder i de enkelte IT-systemer. Er gennemført.
Sikkerhedsniveauet skal være baseret på risikovurderinger og for en afvejning mellem hensynet til risiko, sikkerhed, funktionalitet, brugervenlighed og økonomi.	Den overordnede risikovurdering foretages af IT. Risikovurderinger af de enkelte systemer er systemejers ansvar. Vurderingerne tilpasses løbende efter de eksisterende forhold og generelle trusselsniveauer. Er gennemført, men bør gennemføres igen i dybden og derefter løbende.
IT-systemer til brug for henholdsvis produktions- og kerneprocesserne og de administrative processer skal være adskilte	Der er etableret to adskilte netværk, et administrativt og et teknisk, hvor al trafik mellem de to netværk sker gennem firewalls, og al data som udgangspunkt kun går fra det tekniske til det administrative net.
Inddragelse af alle medarbejdere gennem uddannelse og træning for at styrke en god IT-sikkerhedskultur	Der udarbejdes en plan for awareness-træning og uddannelse af brugere. Er ikke gennemført.
Utilsigtede hændelser forebygges gennem fysisk sikring og overvågning af bygninger, tekniske installationer og udstyr, gennem opdateringer og sikkerhedsprogrammer, herunder brug af passwords, gennem brugeradministration og gennem god medarbejderadfærd.	En række retningslinjer sikrer den nødvendige forebyggelse. Barrierer og tiltag beskrives i IT-håndbog, der publiceres på intranettet. Er igangsat, men ikke gennemført.
Utilsigtede hændelser håndteres gennem en beredskabsplan for informationssikkerhed, der har til formål at begrænse skadens omfang, etablere midlertidige løsninger samt genetablere den normale situation igen.	Beredskabsplanen udbygges og holdes løbende ajour. Er ikke gennemført tilfredsstillende endnu. Registrering af utilsigtede hændelser foregår via BIOFOS 365-processen ”Afvigelser på mål, indsatser og resultater”.
Informationssikkerheden skal eksternt evalueres hvert andet år, og resultatet heraf forelægges for bestyrelsen.	Der udarbejdes en ledelsesevaluering samt ekstern sikkerhedsanalyse. Vil blive gennemført efter godkendelse af politikken.

Bilag:
Informationssikkerhedspolitik for BIOFOS

BIOFOS A/S Refshalevej 250 DK-1432 København K
post@biofos.dk www.biofos.dk
Tlf: +45 32 57 32 32 CVR nr. 25 60 19 20

BIOFOS

Bilag 1 til pkt. 10

Informationssikkerhedspolitik

Formålet med informationssikkerheden i BIOFOS er at beskytte tilgængelighed, integritet og fortrolighed af data, informationer og informationssystemer.

Målet med informationssikkerheden er:

- **Tilgængelighed:** At opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab
- **Integritet:** At opnå korrekt funktion af systemerne med minimeret risiko for manipulation af fejl i såvel data som systemer
- **Fortrolighed:** At opnå mulighed for fortrolig behandling, transmission og opbevaring af data

Principperne for informationssikkerheden i BIOFOS er følgende:

- Den skal efterleve gældende lovgivning og understøtte BIOFOS' strategi
- Økonomidirektøren er den overordnede ansvarlige for informationssikkerhed
- Roller og ansvar for informationssikkerheden er beskrevet, herunder udpegning af systemansvarlige for alle IT-systemer
- Sikkerhedsniveauet skal være baseret på risikovurderinger og på en afvejning mellem hensynet til risiko, sikkerhed, funktionalitet, brugervenlighed og økonomi
- IT-systemer til brug for henholdsvis produktionsprocesser og de administrative processer skal være adskilte
- Inddragelse af alle medarbejdere skal ske gennem uddannelse og træning for at styrke en god IT-sikkerhedskultur
- Utilsigtede hændelser forebygges gennem fysisk sikring og overvågning af bygninger, tekniske installationer og udstyr, gennem opdateringer og sikkerhedsprogrammer, herunder brug af passwords, gennem brugeradministration og gennem god medarbejderadfærd
- Utilsigtede hændelser håndteres gennem en beredskabsplan for informationssikkerhed, der har til formål at begrænse skadens omfang, etablere midlertidige løsninger samt genetablere den normale situation igen
- Informationssikkerheden skal eksternt evalueres hvert andet år og resultatet heraf foreligges for bestyrelsen

Informationssikkerhedspolitikken er gældende for alle i BIOFOS samt alle virksomhedens leverandører og samarbejdspartnere.

Godkendt af bestyrelsen den "dato.måned" 2019