REVISIONSHUSET
TAL & TANKER

PROCESS FACTORY ApS

Vesterbrogade 149, 1620 København V

CVR: 30 90 59 70

ISAE 3402 TYPE II erklæring om ydelser i forbindelse med levering af Connector Plus Platformen samt generelle it-kontroller relateret hertil

1. juni 2025 - 31. maj 2026

This document has esignatur Agreement-ID: a58898u703352019639680

Indholdsfortegnelse

This document has esignatur Agreement-ID: a58898u703352019639680

Afsnit 1: PROCESS FACTORY ApS' udtalelse

Beskrivelsen i afsnit 2 er udarbejdet til brug for kunder, der anvender Process Factorys Connector Plus Platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller som kunden selv har anvendt, ved vurdering af risiciene.

Process Factory anvender itm8 A/S som underleverandør til hosting af Connector Plus Platformen.

Denne erklæring er udarbejdet med fokus på Connector Plus Platformen og de tilhørende kundeintegrationslag, der driftes og administreres i samme miljø og infrastruktur som Connector Plus Platformen. Ældre legacy platforme samt kundeintegrationslag, som driftes andetsteds, falder uden for denne erklærings anvendelsesområde.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 2, kan kun nås, hvis de komplementære kontroller hos kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Process Factory anvender itm8 A/S som underleverandør til hosting af Connector Plus Platformen.

Process Factory bekræfter, at:

(a) Den medfølgende beskrivelse giver en retvisende beskrivelse af Process Factory ApS' generelle it-kontroller med relevans for Process Factorys Connector Plus Platform. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været udformet og implementeret, herunder redegør for:

- De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
- Relevante kontrolmål, og kontroller udformet til at nå disse mål, herunder kontroller til sikring af fortrolighed, integritet og tilgængelighed af systemer og data, samt opfyldelse af kravene i den internationale ledelsesstandard for informationssikkerhed ISO/IEC 27001/2.
- Andre relevante aspekter ved Process Factorys kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, der har været relevante for de generelle it-kontroller.

(ii) Ikke udelader og forvansker oplysninger, der er relevante for omfanget af den beskrevne Connector Plus Platform, under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer, og derfor ikke kan omfatte ethvert aspekt ved Connector Plus Platformen, som den enkelte kunde måtte anse for vigtigt efter dennes særlige forhold.

This document has esignatur Agreement-ID: a58898u70335201963968O

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i den medfølgende beskrivelse, var hensigtsmæssigt udformet. Kriterierne for denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

(ii) De identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetencer og beføjelse.

København, den 10. juni 2026

_____

Susanne Møllegaard
CEO
PROCESS FACTORY ApS

This document has esignatur Agreement-ID: a5889Bu703352019639680

Afsnit 2: Beskrivelse af Process Factory ApS' ydelser i forbindelse med levering af Connector Plus Platformen samt generelle it-kontroller relateret hertil.

Introduktion og beskrivelse af Process Factory ApS' ydelser
I det følgende beskrives Process Factorys ydelser til kunder, som er omfattet af de generelle it-kontroller, som erklæringen omhandler.

Denne uafhængige revisorerklæring fokuserer på Process Factorys Connector Plus Platform, herunder de tilhørende kundeintegrationslag, der driftes og administreres i samme miljø og infrastruktur som Connector Plus Platformen. Aktiviteter relateret til disse er ligeledes inkluderet. Ældre legacy platforme samt kundeintegrationslag, som driftes andetsteds, falder uden for denne erklærings anvendelsesområde.

Hvem er Process Factory ApS
Process Factory er en innovativ dansk it-virksomhed med ekspertise i it og forretning, der blev stiftet tilbage i 2007 i København. Virksomheden fungerer som strategisk it-partner for kunder i forsikringsbranchen og leverer integrations as a service via Connector Plus Platformen.

Process Factory ApS´ grundlag
Process Factory har siden 2007 specialiseret sig i at digitalisere og understøtte aktører i branchen med it-løsninger og digitaliseringsstrategier. Virksomheden har dermed 19 års erfaring med udvikling, implementering og drift af integrationsløsninger målrettet forsikringsmarkedet.

Kompetencer og ydelser
Teamet bag Process Factory består af forretningskonsulenter, erfarne it-arkitekter, softwareudviklere, kompetente projektledere og forsikringseksperter.

Virksomhedens konsulenter har indgående erfaring med blandt andet integrationsarkitektur, API-baserede løsninger og understøttelse af samarbejde på tværs af komplekse systemlandskaber. Process Factory rådgiver desuden om risikovurdering samt planlægning og implementering af nye initiativer til automatisering af forretnings- og it-processer.

Virksomheden leverer specialiserede løsninger og kvalificeret rådgivning til den nordiske forsikringsbranche med fokus på kvalitet og værdiskabende løsninger.

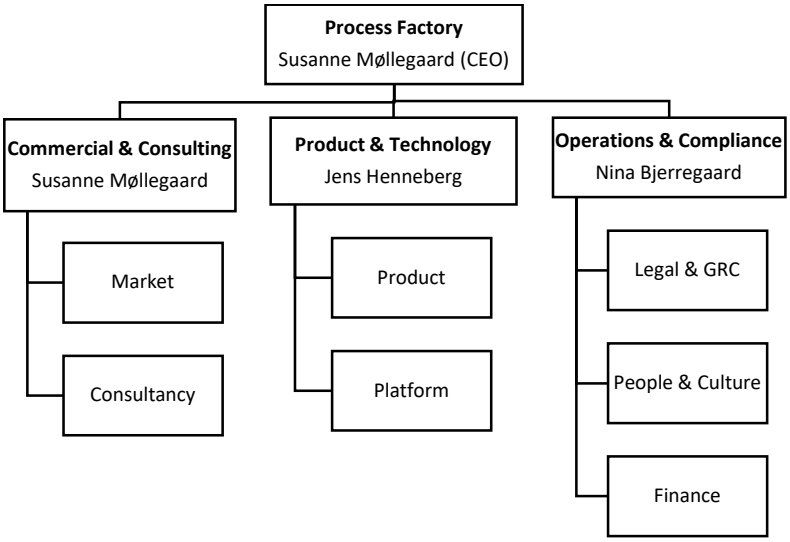
Kunder og marked
Process Factorys kunder er hovedsageligt placeret i de skandinaviske lande. Virksomhedens ambition er at være markedsledende, og dermed forsikringsbranchens foretrukne samarbejdspartner inden for integrationsløsninger.

Overordnet beskrivelse af Process Factory ApS' organisation
Process Factory har sit fysiske kontor i København. Virksomheden er organiseret med klare ledelses- og funktionsområder, der understøtter drift og videreudvikling af Connector Plus Platformen.

This document has esignatur Agreement-ID: a58898u703352019639680

Organiseringen er tilrettelagt for at sikre stabil leverance, klare ansvarsforhold og effektiv understøttelse af virksomhedens kunder og løsninger.

Organisationsdiagrammet nedenfor viser virksomhedens strukturelle opbygning pr. 1. marts 2026:



Organisatorisk kontekst
Process Factorys ISMS er tilpasset vores kontekst og tager højde for strategiske mål, eksterne og interne udfordringer samt interessenters behov og forventninger.

Process Factorys topledelse har defineret og godkendt informationssikkerhedspolitikken, der fastlægger organisationens mål for sikkerhed og sikrer sammenhæng med de overordnede forretningsmål.

Connector Plus
Connector Plus er en brancheløsning, der samler tredjepartsintegrationer på én samlet platform.

Platformens moduler og funktioner tilgås via ét enkelt login, og håndterer kald til og fra eksterne services og databehandling, så virksomhedens kunder kan fokusere på deres kerneforretning.

Process Factory håndterer med Connector Plus Platformen den løbende drift, hosting, videreudvikling og funktionsberigelse af virksomhedens kunders integrationer. Derudover understøtter Process Factory de omkringliggende forretningsprocesser, og sender data direkte ind i virksomhedens kunders forretningsapplikationer.

Generelle it-kontroller hos Process Factory
I det følgende beskrives de generelle it-kontroller, der relaterer sig til Process Factorys drift af Connector Plus Platformen.

Anvendelse af underleverandører
Process Factory anvender itm8 A/S som hostingpartner i forbindelse med leverancen af Connector Plus Platformen.

This document has esignatur Agreement-ID: a5889bu703352019639680

Risikostyring

Process Factory har udarbejdet faste procedurer for løbende risikovurderinger af forretningen, herunder for Connector Plus Platformen. Formålet med virksomhedens risikobaserede tilgang er at sikre, at alle risici identificeres og minimeres til et acceptabelt niveau. Som led heri gennemføres der mindst én gang årligt en ledelsesgodkendt risikovurdering af alle aktiver med relation til Connector Plus Platformen. Derudover risikovurderes aktiver forud for deres introduktion til Connector Plus Platformen.

Derudover udarbejder og vedligeholder Process Factory en beredskabsplan, der fastlægger roller og ansvar samt dokumenterer de processer og foranstaltninger, der aktiveres i tilfælde af hændelser, som ikke kan håndteres via den daglige drift.

Process Factory håndterer risici med udgangspunkt i det aktuelle trusselsbillede, og virksomheden har tegnet erhvervs- og produktansvarsforsikring.

Organisatoriske foranstaltninger

Organiseringen af it-sikkerhed sker med udgangspunkt i Process Factorys it-sikkerhedspolitikker, der tager udgangspunkt i ISO/IEC 27001-kontroller.

Nærværende ISAE 3402 erklæring kontrollerer følgende hovedområder:

- Risikostyringsforanstaltninger
- Organisatoriske foranstaltninger
- Personrelaterede foranstaltninger
- Fysiske foranstaltninger
- Teknologiske foranstaltninger

Process Factorys organisering af it-sikkerhed er beskrevet nedenfor.
Kontrolmål og kontroller, som Process Factory har udvalgt, fremgår af oversigten i afsnit 4.

Informationssikkerhedspolitikker

Process Factorys informationssikkerhedspolitikker sikrer, at medarbejdere overholder de fastlagte krav og rammer for it-sikkerhed. Alle politikker med relation til it-sikkerhed revideres som minimum én gang årligt. Medarbejdere trænes i virksomhedens politikker som led i ansættelses- og onboardingprocessen, og eksisterende medarbejdere informeres ved ændringer heraf.

It-udstyr

Der udføres løbende kontroller, der sikrer at alle enheder overholder de gældende politikker, og der foretages løbende overvågning af udstyr med henblik på at sikring af, at der ikke installeres uautoriseret software.

Informationssikkerhed under driftsforstyrrelse

Process Factory har udarbejdet en it-beredskabsplan, og denne opdateres i nødvendigt omfang. It-beredskabsplanen er udarbejdet med henblik på at opretholde eller genskabe drift og sikre adgang til data på det aftalte niveau.

This document has esignatur Agreement-ID: a58898u703352019639680

Process Factory gennemfører løbende risikovurderinger med henblik på at udarbejde planer for at imødekomme relevante trusler, og it-beredskabsplanen afprøves minimum én gang om året – enten som *skrivebordstest* eller *full interruption test*.

Overensstemmelse med politikker, regler og standarder for informationssikkerhed
Process Factory er meget bevidste om virksomhedens rolle som leverandør til en branche, som rammes af den strengeste regulering i forhold til it-sikkerhed.

Process Factory har organiseret arbejdet med it-sikkerhed som en integreret del af virksomhedens complianceindsats. Ansvar og opgaver vedrørende informationssikkerhed fordeles på tværs af relevante funktioner for at sikre, at virksomheden lever op til gældende krav og standarder. Dermed understøttes en struktureret og løbende opfølgning på virksomhedens forpligtelser som it-leverandør til forsikringsbranchen. Eksterne eksperter inddrages i det omfang, at dette er relevant.

Process Factorys direktion og bestyrelse er ligeledes forpligtet til at holde sig ajour med reglerne på området for it-sikkerhed, og have tilstrækkelig viden herom til at varetage deres funktioner.

Gennemgang af informationssikkerhed
Process Factory benytter et årshjul til sikring af regelmæssig gennemgang af relevante systemer, for at sikre overensstemmelse med Process Factorys sikkerhedspolitikker, -procedurer og -standarder. Ligeledes rapporterer virksomhedens compliancefunktion løbende til Process Factorys direktion.

Informationssikkerhed i leverandørforhold
Forud for indgåelse af aftaler med underdatabehandlere, foretages der en due diligence proces, hvor der udarbejdes risikovurderinger.

Derudover foretages der løbende tilsyn med underleverandører til at sikre, at relevante kontroller identificeres og implementeres.

Brug af underleverandører sker via gensidige aftaler, der løbende gennemgås med henblik på at sikre, at aftalte foranstaltninger, serviceydelser og servicemål bliver etableret, leveret og opretholdt.

Styring af leverandørydelser
Tilsyn med Process Factorys underdatabehandlere håndteres i praksis via Process Factorys årshjul, der sikrer at tilsyn udføres og dokumenteres løbende af Process Factorys compliancefunktion med inddragelse af relevant teknisk personale og ledelsen, hvor dette er nødvendigt.

Generelt er Process Factory i løbende dialog med relevante underleverandører om it-sikkerhed for at sikre, at kravene til behandlingssikkerhed efterleves.

Process Factory fører løbende, og minimum én gang årligt, et større tilsyn med virksomhedens hostingpartner, itm8. Ved disse tilsyn inddrages hele Process Factorys it-sikkerhedsteam. Derudover gennemgås itm8's ISAE 3402-erklæring årligt. Identificerede forhold vurderes af relevante funktioner i Process Factory, og ledelsen inddrages efter behov.

Administration af brugeradgang
Alle brugere har et unikt brugernavn og bruger-id, som tildeles via en formaliseret proces. Alle adgange til systemer i Process Factory, tildeles, hvor det er teknisk muligt, via brugerens *single sign-on* adgang, der er underlagt regler om passwordkompleksitet, og hvor *to-factor authentication* er påkrævet.

This document has esignatur Agreement-ID: a58898u703352019639680

Process Factorys ledelse godkender oprettelse og ændring af brugeradgange efter særlige procedurer minimum én gang årligt.

Brugernes ansvar
Process Factorys retningslinjer for længde, kompleksitet og levetid af adgangskoder er baseret på anerkendte best practices og gældende anbefalinger, som løbende revurderes og opdateres i takt med udviklingen inden for informationssikkerhed.

Styring af aktiver
Process Factory udarbejder og vedligeholder en fortegnelse over informations- og informationsbehandlingsaktiver, og der er opsat regler for acceptabel anvendelse heraf. Der bruges et Asset Management system til at føre fortegnelse over alle aktiver, der er forbundet med Connector Plus Platformen.

Forretningsmæssige krav til adgangsstyring
For at sikre styring af adgang til Process Factorys systemer, informationer og netværk, er der etableret adgangsregler og -rettigheder til alle væsentlige it-aktiver.

Process Factory vedligeholder fortegnelser over tildelte rettigheder, og tildeling af rettigheder sker med afsæt i least privilege princippet.

Alle aktiver skal have en attribut tilknyttet kaldet *Access policy* og skal indeholde en henvisning til retningslinjer omkring adgangsstyring. Aktiver skal programmatisk filtreres i Asset Management systemet for at fremfinde alle aktiver uden en tildelt *Access* policy. Dette gøres periodisk, og er indskrevet som en fast opgave i Process Factorys årshjul.

Der benyttes VPN og firewalls til at begrænse adgangen til nettjenester på Process Factorys netværk. Hvis en tjeneste anses som kritisk, oprettes der firewallregler, der kun tillader trafik fra Process Factorys interne netværk til det specifikke netværk, hvorpå tjenester er tilgængelige.

Hvis en medarbejder har behov for at tilgå en tjeneste uden for Process Factorys interne netværk, benyttes der en VPN-service (hvor dette er relevant), som er opsat med *multi-factor authentication* for yderligere sikring af tjenesterne.

Ydermere er alle services, hvor det er teknisk muligt, underlagt authentication enten i form af *single-sign on, PKI* eller i enkelte tilfælde *password authentication.* Alle adgange tildeles efter *Principle of Least Privilege.* Dette sikrer, at medarbejdere kun har adgang til det, som er nødvendigt for arbejdets udførelse.

Personrelaterede foranstaltninger

Kontrol af egnethed og hæderlighed
Process Factory har etableret procedurer der sikrer, at ansatte er kvalificerede samt bevidste om deres opgaver i relation til informationssikkerhed.

Dette sker gennem systematisk kontrol af nyansatte interne medarbejdere, såvel som eksterne konsulenters egnethed og hæderlighed, herunder via indhentelse af straffeattester, hvor dette er nødvendigt og har betydning for behandlingsaktiviteten.

This document has esignatur Agreement-ID: a58898u703352019639680

Ansattes ansvar og forpligtelser vedrørende it-sikkerhed
Ved ansættelse underskriver alle medarbejdere en ansættelseskontrakt, der beskriver medarbejderens og Process Factorys ansvar og forpligtelser vedrørende informationssikkerhed, herunder at medarbejderen er underlagt tavshedspligt.

Den enkelte medarbejder forpligtes til at overholde virksomhedens politikker vedrørende it-sikkerhed, herunder virksomhedens sikkerhedsinstruks for it-anvendelse, samt at rapportere eventuelle brud og sårbarheder til Process Factorys it-sikkerhedsteam.

Awareness og uddannelse af medarbejdere i it-sikkerhed
Alle ansatte i Process Factory introduceres i umiddelbar forlængelse af deres ansættelse til virksomhedens politikker og instrukser vedrørende it-sikkerhed, herunder Process Factorys it-sikkerhedspolitik, sikkerhedsinstruks for sikker it-anvendelse samt politik for brug af AI og Open Source. Ligeledes underskriver alle ansatte, som led i underskrivelsen af ansættelseskontrakten, virksomhedens mest centrale politikker og instrukser vedrørende it-sikkerhed.

Alle medarbejdere har adgang til virksomhedens it-sikkerhedspolitikker og instrukser, mens mere detaljeret materiale kun er tilgængeligt for udvalgte medarbejdere med behov herfor. Medarbejdere informeres løbende om væsentlige ændringer i de materialer, der er relevante for deres funktion.

Interne såvel som eksterne medarbejdere med adgang til virksomhedens data, modtager løbende uddannelse, træning og oplysninger om informationssikkerhed af Process Factorys it-sikkerhedsteam og virksomhedens ledelse.

Styring af informationssikkerhedshændelser og forbedringer
Process Factory har etableret kontroller der sikrer, at sikkerhedshændelser og forbedringer håndteres rettidigt, samt at der sikres løbende opfølgning.

En sikkerhedshændelse refererer til enhver hændelse, der potentielt kan have indvirkning på fortrolighed, integritet eller tilgængelighed for Process Factorys systemer, netværk eller data der er opbevaret i et system.

Hændelser håndteres i henhold til en indarbejdet incident management proces. Dele af overvågning, detektion og indledende vurdering af sikkerhedshændelser er outsourcet til virksomhedens SOC-leverandør, itm8. Afhængig af sikkerhedshændelsens karakter, udarbejder virksomhedens compliancefunktion i samarbejde med it-sikkerhedsteamet og ledelsen, en plan for håndtering med henblik på at sikre minimering af skaden, samt at genoprettelse af sikkerheden sker så hurtigt som muligt, og at alle relevante parter informeres herom.

Alle medarbejdere, samarbejdspartnere og andre brugere af systemer og tjenester forpligtes til at notere og rapportere observerede svagheder eller mistanke om svagheder.

Process Factorys medarbejdere informeres om svagheder, og uddannes løbende i vigtigheden af, at enhver svaghed rapporteres.

This document has esignatur Agreement-ID: a58898u703352019639680

Fysiske foranstaltninger

Sikre områder og adgangskontrol

Process Factory samt virksomhedens underleverandør, itm8, har etableret kontroller, som understøtter at it-udstyr er behørigt beskyttet mod uautoriseret adgang samt miljømæssige hændelser.

Adgang til Process Factorys lokaler sker via adgangsbrikker, og indgangen til Process Factorys kontorbygning videoovervåges til sikring af, at kun autoriserede har adgang til virksomhedens kontorfaciliteter. Der er etableret faste procedurer for tildeling og nedlægning af adgangsbrikker til virksomhedens kontorlokaler.

Process Factorys hostingpartner, itm8's lokaler og udstyr, er forsynet med adgangskontrol, afspærring og videoovervågning, der sikrer at kun autoriserede medarbejdere har adgang.

Adgangen til det datacenter, hvor Process Factorys data er lagret hos itm8, er sikret med HVAC (Heating, Ventilating, and Air Conditioning) teknologi, der overvåges løbende, og som testes minimum én gang årligt.

Udstyr

Process Factorys hostingpartner, itm8, har implementeret procedurer for at sikre, at det fysiske produktionsudstyr vedligeholdes, og at procedurerne herfor efterleves.

Til sikring af forsyningssvigt i overensstemmelse med udstyrets betydning for kritiske forretningssystemer, har Process Factorys hostingpartner, itm8, installeret UPS samt nødgeneratorer, som løbende vedligeholdes via serviceaftaler og eftersyn.

Der er hos Process Factory samt hos virksomhedens hostingpartner, itm8, etableret procedurer der sikrer, at alle enheder der indeholder lagringsmedier, bliver renset for data før enhedens bortskaffelse, hvor dette er teknisk muligt.

Det følger af Process Factorys sikkerhedsinstruks for it-anvendelse, at udstyr uden opsyn har passende beskyttelse. Alle medarbejdere hos Process Factory er via sikkerhedsinstruks for it-anvendelse forpligtet til at sikre, at alle unødvendige data fjernes efter brug, herunder også papirer og andre flytbare lagringsmedier, ligesom der stilles krav om ryddet skærm for informationsbehandlingsfaciliteter.

Teknologiske foranstaltninger

Styring af system- og applikationsadgang

Systemadgange beskyttes med en sikker log-on-procedure, som beskrevet ovenfor. Systemer som af tekniske årsager ikke kan integreres med *single-sign on,* og som vurderes at indeholde informationer eller funktioner med behov for særlig beskyttelse, bliver afdækket via sekundær OAuth2-baseret server, eller via adgang gennem en SSH-bruger. SSH-brugere, som benyttes til disse adgange, bliver konfigureret med PKI godkendelse, og almindelig passwordgodkendelse vil blive slået fra på brugeren.

Process Factorys sikkerhedsinstruks for it-anvendelse forbyder lagring af adgangskoder uden for godkendte passwordmanager løsninger.

Process Factory benytter et *Privileged Access Management* værktøj til at begrænse og kontrollere hjælpeprogrammer, der kan tilsidesætte system- og applikationskontroller.

Kryptografi

Process Factory har etableret en politik, der sikrer at anvendelse af kryptografiske kontroller udføres

This document has esignatur Agreement-ID: a58898u703352019639680

systematisk og forsvarligt, til beskyttelse af følsomme forretningsdata.

Kryptografi in transit
Process Factorys transmission af personoplysninger i Connector Plus Platformen, er krypteret med industristandarder for stærk kryptering.

Kryptografi at rest
Process Factorys lagring af fortrolige og følsomme personoplysninger, udføres udelukkende på krypterede filsystemer og databaser efter industristandarder for stærk kryptering.

Driftsprocedurer og ansvarsområder
Process Factory har etableret kontroller, som understøtter at drift af servere og væsentlige systemer foregår på en struktureret og sikker måde.

Der er etableret dokumentation for driftsprocedurer i et omfang, som sikrer effektiv driftsafvikling, samt hurtig og effektiv afhjælpning af eventuelle driftsforstyrrelser og -problemer.

Driften i Process Factorys datacenter dokumenteres efter gældende interne standarder. Relevante Process Factory medarbejdere har adgang til teknisk dokumentation på alle kritiske driftssystemer, som er samlet på Process Factorys intranet. Viden akkumuleret i det daglige arbejde dokumenteres i en fælles *Knowledge-database.*

Process Factory benytter et Service Management system til at håndtere driften. Ændringer til produktionsmiljøet styres gennem en indarbejdet *change management proces*, der bl.a. sikrer risikovurdering og test af funktionalitet og sikkerhed. Systemer, der er overgået til drift, overvåges i dagligdagen af Process Factorys Platform team. Håndtering af driftsforstyrrelser sker via en formaliseret incident management proces.

Overvågning og analyse af systemlogs, hændelser og ændringer i filsystemer understøttes gennem SOC-ydelser leveret af itm8. Løbende monitorering, analyse og eskalation af alarmer varetages af itm8, mens Process Factory har ansvaret for vurdering af hændelsernes forretningsmæssige betydning samt beslutning om og opfølgning på afhjælpende tiltag.

Overvågning af systemressourcer foretages af både itm8 og Process Factory. Overvågning af applikationslogs som stammer fra Process Factorys egenudviklede løsninger, varetages af Process Factory.

Der er opsat et separat dedikeret testmiljø, som sikrer adskillelse mellem udvikling, test og produktion.

Malwarebeskyttelse
Process Factory har installeret opdateret antivirus software på relevante servere samt i relevante firewalls.

Al netværkstrafik overvåges af itm8 via SOC-ydelser. I visse tilfælde scannes servere direkte. Såfremt data er virusbehæftet, forbeholder Process Factory sig retten til at forsøge rensning af disse data. Hvis rensning af data ikke er tilstrækkeligt, forbeholder Process Factory sig retten til at slette de inficerede data.

Backup
Der tages backup af alle væsentlige informationsaktiver, herunder parameteropsætninger og anden driftskritisk dokumentation, i henhold til retningslinjer fastsat af Process Factory - og der foretages løbende tests af gendannelsesprocessen for datafiler.

This document has esignatur Agreement-ID: a58898u703352019639680

Process Factory benytter et værktøj til at sikre, at data som tidligere er slettet fra produktionsmiljøet, ikke genintroduceres ved genindlæsning af backup, hvor dette er teknisk muligt.

Applikationer og aktiver, der varetager behandling af personoplysninger, sikkerhedspatches løbende og hurtigst muligt efter frigivelse af patchen.

Logning og overvågning
Process Factory har opsat kontroller til at sikre, at logoplysninger ikke kan forfalskes eller korrumperes. Dette sker via et værktøj der sikrer, at datahistorik for logoplysninger bibeholdes, samt at dataintegritet overholdes for logoplysninger over tid.

Styring af driftssoftware
Process Factory har etableret faste, automatiserede og reproducerbare procedurer for installation og vedligehold af installationer på Process Factorys driftssystemer, samt oversigter over installeret programmel på driftssystemerne.

Sårbarhedsstyring
Process Factory driftsmiljøer og systemer evalueres løbende for sårbarheder, og der forefindes faste procedurer for udbedring af fundne sårbarheder.

Ved hjælp af scanningsværktøjer overvåges systemer løbende for sårbarheder. Ved identifikation af en sårbarhed, adviseres den sikkerhedsansvarlige, som herefter er ansvarlig for at udbedre sårbarheden og rapportere denne til ledelsen og compliancefunktionen.

Sårbarheder og eventuelle trends evalueres løbende, og passende foranstaltninger implementeres for at modvirke nye risici.

Som led i virksomhedens strategi for at sikre robust- og modstandsdygtighed i Connector Plus Platformen, udføres der minimum én gang årligt en penetrationstest med det formål at identificere potentielle sårbarheder og sikkerhedsrisici. Penetrationstesten foretages af en uafhængig, kvalificeret tredjepart, og resultaterne af testen gennemgås og valideres, hvorefter nødvendige foranstaltninger implementeres for at afhjælpe opdagede sårbarheder.

Process Factorys hostingpartner, itm8, overvåger og vedligeholder alle af Process Factorys anvendte Windows-systemer og MacOS-enheder samt netværksenheder.

Der er etableret fastlagte politikker for installation af programmel på brugernes arbejdsmaskiner, og al programmel på medarbejderes maskiner udleveret af Process Factory scannes og holdes i katalog i værktøjer til formålet.

Styring af netværkssikkerhed
Det af Process Factory benyttede netværk er beskyttet mod trusler via en firewall.

Der er opsat port-regler på firewalls til sikring af, at kun tilladt trafik får adgang til Process Factorys netværk.

Informationsoverførsel
Process Factory har opsat formelle overførselspolitikker, -procedurer og -kontroller til at sikre, at digital transmission af oplysninger udføres forsvarligt.

This document has esignatur Agreement-ID: a5889bu703352019639680

Transmission af følsomme oplysninger sker udelukkende ved brug af kryptering, mens al kommunikation til og fra driftsmiljøer passerer gennem en firewall.

Manuel overførsel af følsomme data sker ved brug af kryptering, og kun i tilfælde hvor det vurderes at være strengt nødvendigt.

Sikkerhedskrav til informationssystemer
Process Factory har kontroller der sikrer, at digital transmission over offentligt net er tilpas beskyttet imod uautoriseret videregivelse og ændring.

Security by Design og Privacy by Design
Process Factory har procedurer der sikrer, at kravene til informationssikkerhed og privatlivsbeskyttelse indtænkes og analyseres systematisk, når der introducerer nye it-funktioner til Connector Plus Platformen, jævnfør principperne om *Security by Design* og *Privacy by Design*.

Sikkerhed i udviklings- og supportprocesser
Hos Process Factory er der fastlagt formaliserede regler og procedurer for udvikling og vedligehold af software og systemer.

Udvikling af software i Process Factory udføres ud fra fastlagte processer, som en del af virksomhedens officielle *Software Development Life Cycle* (SDLC). SDLC' en indeholder *Definition of Ready* (DoR), *Definition of Done* (DoD), samt definitioner på projekttyper, hvori typen af et givent projekt er med til at fastlægge, hvilke processer der skal udføres i projektets levetid, samt hvilke kriterier der skal opfyldes for at udvikling er klar til påbegyndelse, samt hvornår udviklingen kan anses som værende færdig.

Dokumentet indeholder regler for prioritering i organisationens projekter og opgaver, samt beskrivelser af hvordan kvalitet, sikkerhed og stabilitet sikres i alle udviklingsfaser.

This document has esignatur Agreement-ID: a5889bu703352019639680

Afsnit 3: Uafhængig revisors ISAE 3402 TYPE II erklæring om generelle IT-kontroller relateret til PROCESS FACTORY ApS' ydelser vedrørende Connector Plus Platformen

Til ledelsen hos Process Factory ApS, Process Factory ApS' kunder og deres revisorer

Omfang
Vi har fået til opgave at afgive erklæring om Process Factory ApS' beskrivelse i afsnit 2 af ydelser i forbindelse med levering af Connector Plus Platformen for perioden 1. juni 2025 – 31. maj 2026 og om udformningen af kontroller og funktionen, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Erklæringen omfatter de generelle IT-kontroller, som varetages af Process Factory ApS i forbindelse med levering af Connector Plus Platformen samt generelle it-kontroller relateret hertil.

Enkelte af de kontrolmål, der er anført i Process Factory ApS' beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Process Factory ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

Process Factory ApS' ansvar
Process Factory ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i afsnit 1, "PROCESS FACTORY ApS' udtalelse", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for levering af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring
Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA' Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Vi anvender International Standard on Quality Management (ISQM) 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Serviceleverandørens revisors ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Process Factory ApS' beskrivelse og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402 om erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og

This document has esignatur Agreement-ID: a58898u703352019639680

funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 1, " PROCESS FACTORY ApS' udtalelse".

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør
Process Factory ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i afsnit 1. Det er vores opfattelse,

a) at beskrivelsen af Process Factory ApS' ydelser og kontrolmiljø, således som det var udformet og implementeret for perioden fra 1. juni 2025 – 31. maj 2026, i alle væsentlige henseender er tilfredsstillende præsenteret, og
b) at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet for perioden fra 1. juni 2025 – 31. maj 2026.
c) at de testede kontroller som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. juni 2025 – 31. maj 2026.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af afsnit 4.

This document has esignatur Agreement-ID: a58898u703352019639680

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er tiltænkt kunder, der anvender Process Factorys Connector Plus Platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller som kunden selv har anvendt, ved vurdering af risiciene, når de vurderer risiciene for væsentlig fejlinformation i deres regnskaber.

Silkeborg, den 10. juni 2026

Revisionshuset Tal & Tanker
Statsautoriseret revisionspartnerselskab
Cvr-nr. 37 31 56 64

Per Jensen
International Partner, Statsautoriseret revisor
mne34087

This document has esignatur Agreement-ID: a58898u703352019639680

Tests af kontroller udført af den uafhængige revisor

Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med International Auditing and Assurance Standards Board' International Standard on Assurance Engagements ISAE 3402 TYPE II, Erklæring med sikkerhed om kontroller hos en serviceleverandør.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen og som fremgår af efterfølgende sider.

Evt. andre kontrolmål, tilknyttede kontroller og kontroller hos Process Factory ApS' kunder er ikke omfattet af vores gennemgang / revision.

Vores test af funktionaliteten har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden fra 1. juni 2025 – 31. maj 2026.

Udførte test

De udførte tests i forbindelse med fastlæggelsen af kontrollers funktionalitet er beskrevet nedenfor:

Test metode	Hvordan udføres testen
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen.
Forespørgsler	Forespørgsel af passende personale hos Process Factory ApS. Forespørgsler har omfattet hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentag den relevante kontrol. Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

This document has esignatur Agreement-ID: a58898u703352019639680

Afsnit 4: Revisors beskrivelse af test af kontroller

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
1. Risikostyring foranstaltninger (ISO27005)				
	N/A	Process Factorys risikostyring omfatter følgende: · Identifikation af potentielle risici · Vurdering af de identificerede potentielle risici, herunder deres væsentlighed, sandsynlighed og konsekvenser på Hosting- miljøerne · Implementering af tiltag for at reducere sandsynligheden for, at risici indtræder, efter en omkostningseffektiv måde.	Vi har inspiceret, at der er udarbejdet en ajourført og ledelsesgodkendt risikovurdering.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at potentielle risici er identificeret og at de kategoriseret efter sandsynlighed og konsekvens.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at bestyrelsen har godkendt risikoprofilen.	Ingen væsentlige bemærkninger
	N/A	Der foretages en gang årligt eller ved større organisatoriske og/eller tekniske ændringer en overordnet risikovurdering.	Vi har inspiceret, at risikovurderingen opdateres en gang om året og ved væsentlige ændringer.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at bestyrelsen en gang om året vurderer og godkender risikoprofilen.	Ingen væsentlige bemærkninger
	N/A	Process Factory håndterer risici med udgangspunkt i det øjeblikkelige trusselsbillede med opgørelse af konsekvens og sandsynlighed for at hændelser indtræffer.	Vi har forespurgt hvorledes risikohåndteringen udføres.	Ingen væsentlige bemærkninger
	N/A	Process Factory har tegnet har en erhvervs- og produktansvarsforsikring med en dækningssum på 10 mio kr. samt professionel ansvarsforsikring med en dækningssum på 1 mio. d.kr.	Vi har observeret, at præmie for de to forsikringer er betalt for 2025 samt, at forsikringerne er tegnet for 2026.	Ingen væsentlige bemærkninger

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
2. Organisatoriske foranstaltninger (ISO27002:2022 Afsnit 5)				
	5.1	Ledelsen godkender en skriftlig informationssikkerhedspolitik, som offentliggøres og kommunikeres til virksomhedens medarbejdere og relevante eksterne parter.	Vi har inspiceret, at der foreligger en opdateret og ledelsesgodkendt IT sikkerhedspolitik, der er tilgængelig for Process Factorys medarbejdere.	Ingen væsentlige bemærkninger
			Vi har forespurgt udvalgte medarbejdere om de er bekendt med IT-sikkerhedspolitikken.	Ingen væsentlige bemærkninger
	5.1	IT-sikkerhedspolitikken fastlægger det overordnede sikkerhedsniveau og de nødvendige organisatoriske rammer samt de overordnede retningslinjer for udformning af kontroller, procedurer og sikringsforanstaltninger.	Vi har inspiceret IT sikkerhedspolitikken og påset, at sikkerhedsniveauet fastlægges	Ingen væsentlige bemærkninger
	5.1	På baggrund af den af ledelsen godkendte IT sikkerhedspolitik udarbejdes en IT-sikkerhedsinstruks, der indeholder procedurer og retningslinjer for IT-sikkerheden.	Vi har inspiceret, at der foreligger en opdateret og ledelsesgodkendt IT sikkerhedsinstruks udarbejdet med udgangspunkt I IT-sikkerhedspolitikken, samt at den er tilgængelig for Process Factorys medarbejdere.	Ingen væsentlige bemærkninger
			Vi har forespurgt udvalgte medarbejdere om de er bekendt med IT-sikkerhedsinstruks.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u703352019639680

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
2. Organisatoriske foranstaltninger (ISO27002:2022 Afsnit 5)				
	5.1	Informationssikkerhedspolitikker og understøttende retningslinjer revurderes en gang om året samt ved væsentlige tekniske eller organisatoriske ændringer.	Vi har forespurgt om IT- sikkerhedspolitikken opdateres regelmæssigt og ved væsentlige ændringer.	Ingen væsentlige bemærkninger
			Vi har observeret, at bestyrelsen en gang om året tager informationsstrategien og -politikken til efterretning.	Ingen væsentlige bemærkninger
	5.4	Ledelsen skal sikre sig, at alle medarbejdere implementerer og fastholder informationssikkerhed i overensstemmelse med Process Factorys sikkerhedspolitik, retningslinjer og procedurer.	Vi har forespurgt hvorledes Direktionen og den sikkerheds- ansvarlige sikrer sig at medarbejderne overholder sikkerhedspolitikken.	Ingen væsentlige bemærkninger
	5.8	De informationssikkerhedsrelaterede krav skal indgå i kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer. Process Factory sikrer, at kravene til informationssikkerhed og privatlivsbeskyttelse analyseres systematisk i de opgave- og projektforløb, der introducerer nye IT-funktioner/features i løsningen, jf. principperne om security-by-design og privacy-by-design, samt at de valgte designvalg dokumenteres.	Vi har forespurgt hvordan det sikres at sikkerhedsrelaterede krav indgår i kravene til nye løsninger, samt forbedring/ændring af eksisterende løsninger.	Ingen væsentlige bemærkninger
	5.9	Aktiver i forbindelse med informations- og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.	Vi har inspiceret, at der findes en vedligeholdt fortegnelse over informationsikkerheds-aktiver.	Ingen væsentlige bemærkninger
	5.9	Aktiver, der opbevares i fortegnelsen, er ejet af Process Factory.	Vi har inspiceret, at fortegnelsen over informationsikkerheds-aktiver kun indeholder aktiver ejet af Process Factory.	Ingen væsentlige bemærkninger
	5.10	Regler for acceptabel anvendelse af oplysninger og aktiver i forbindelse med informations- og informationsbehandlingsfaciliteter skal identificeres, dokumenteres og gennemføres.	Vi har inspiceret, at der findes et regelsæt for acceptabel anvendelse af informationsikkerheds-aktiver.	Ingen væsentlige bemærkninger
	5.14	Der skal være indført formelle overførselspolitikker, -procedurer og -kontroller for at beskytte overførslen af oplysninger ved hjælp af alle typer kommunikationsfaciliteter.	Vi har inspiceret politikker og procedurer for overførsel af information til/fra Process Factorys systemer til/fra eksterne systemer.	Ingen væsentlige bemærkninger
	5.14	Oplysninger, der indgår i elektroniske meddelelser, skal beskyttes på passende vis. Process Factory sikrer, at al digital transmission af personoplysninger til og fra Process Factorys IT-miljø sker gennem en firewall med opdaterede sikkerhedspolitikker, at transmissionen sker krypteret, og at der er sikkerhed for afsender og modtagers identitet.	Vi har forespurgt hvordan det sikres at personoplysninger altid er sikret med stærk kryptering, samt at der opnås sikkerhed for afsender og modtagers identitet.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
2. Organisatoriske foranstaltninger (ISO27002:2022 Afsnit 5)				
	5.15	Der foreligger dokumenterede og ajourførte retningslinjer for adgangsstyring til alle væsentlige IT-aktiver. Den Tekniske Direktør giver medarbejder de nødvendige rettigheder for at kunne udføre deres opgaver.	Vi har forespurgt udvalgte medarbejdere, hvordan tildeling af adgangsrettigheder sker.	Ingen væsentlige bemærkninger
	5.15	Brugerne må kun have adgang til de net- og nettjenester, som de specifikt har fået tilladelse til at bruge.	Vi har forespurgt hvordan det sikres at brugere kun har adgang til de tildelte net- og nettjenester.	Ingen væsentlige bemærkninger
	5.16	Brugere modtager en skriftlig bekræftelse af de tildelte rettigheder. Process Factory vedligeholder fortegnelser over, hvordan bruger-ID eller rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion. Tildeling sker med afsæt i medarbejderens rolle-tilhørsforhold og med afsæt i least-privilegde-princippet samt efter en formel procedure for opretholdelse, rokering og fratrædelse af brugere samt for tildeling af adgange, autorisationer og kodeord. Der anvendes en rollebaseret minimums tildeling at rettigheder til applikationers funktioner. Der udarbejdes og vedligeholdes oversigter over, hvilke medarbejdere hos Process Factory, der har adgang til Process Factorys kunders personoplysninger.	Vi har forespurgt udvalgte medarbejdere, om de har modtaget skriftlig bekræftelse på tildeling/ændring af deres adgangsrettigheder.	Ingen væsentlige bemærkninger
			Vi har inspiceret oversigter over, hvilke medarbejdere hos Process Factory, der har adgang til Process Factorys kunders personoplysninger.	Ingen væsentlige bemærkninger
	5.16	Brugere har unikt brugernavn og bruger-id. Ledelsen skal godkende oprettelse og ændring af brugeradgang.	Vi har for et udvalg af servere observeret oprettede brugere og vurderet om der er en unik identitet.	Ingen væsentlige bemærkninger
	5.17	Tildeling af adgangskoder styres ved en formaliseret proces.	Vi har inspiceret, hvorledes adgangskoder tildeles.	Ingen væsentlige bemærkninger
	5.17	Virksomhedens retningslinjer for brugernes valg og anvendelse af adgangskoder er i overensstemmelse med god skik og brug.	Vi har inspiceret retningslinjer for brugernes valg og anvendelse af adgangskoder.	Ingen væsentlige bemærkninger
	5.17	Systemer til styring af adgangskoder er interaktive og sikrer, at der kun benyttes adgangskoder med den fastlagte kvalitet. Process Factory anvender systemer til administration, transmission og lagring af adgangskoder, der bl.a. beskytter mod forsøg på at hacke adgangskoderne (høj kompleksitet), logger fejlslagne og gennemførte log-on forsøg samt sikrer, at der ikke transmitteres adgangskoder i klar tekst over åbne netværk.	Vi har forespurgt udvalgte medarbejdere hvordan reglerne er for administration af adgangskoder.	Ingen væsentlige bemærkninger
			Vi har observeret at kravene til brug af adgangskoder på udvalgte servere overholdes.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
2. Organisatoriske foranstaltninger (ISO27002:2022 Afsnit 5)				
	5.18	Brugernes adgangsrettigheder gennemgås regelmæssigt (min. 1 gang årligt).	Vi har inspiceret proceduren for gennemgang af adgangsrettigheder er udført indenfor seneste år.	Ingen væsentlige bemærkninger
			Vi har for et udvalg af medarbejdere observeret om adgangsrettigheder svarer til deres arbejdsområder.	Ingen væsentlige bemærkninger
	5.18	Medarbejderen er forpligtet til at overdrage alt materiale og alle rettigheder ved fratrædelsen eller afskedigelsen.	Vi har fået en oversigt over fratrådte medarbejdere 1. juni 2025 - 31. maj 2026 og observeret om adgangsrettigheder for fratrådte medarbejdere er inddraget.	Ingen væsentlige bemærkninger
	5.19	Ved samarbejde med andre parter, der har adgang til virksomhedens informationsaktiver, gennemføres en risikovurdering, og relevante kontroller identificeres og implementeres. Process Factory sikrer før indgåelse af underdatabehandleraftaler med tredjeparter, at der gennemføres en dokumenteret due dilligence proces, med henblik på at vurdere underdatabehandlerens organisatoriske og tekniske sikkerhedsforanstaltninger.	Vi har forespurgt hvordan det sikres at der for underdatabehandlere (f.eks. itm8) udarbejdes risikovurdering samt implementeres relevante kontroller.	Ingen væsentlige bemærkninger
	5.20	Ved serviceleverance, bliver der udarbejdet en gensidig aftale omkring det ønskede serviceniveau, eksempelvis gennem formelle SLA (Service Level Agreements) som en del af den indgåede driftsaftale. Process Factory sikrer sig, at aftalte sikrings- og kontrolforanstaltninger, serviceydelser og servicemål bliver etableret, leveret og opretholdt.	Vi har observeret, at der er indgået hostingaftale med itm8 indeholdende aftale omkring SLA.	Ingen væsentlige bemærkninger
			Vi har inspiceret itm8 løsningsbeskrivelse, samt itm8 SLA-beskrivelse.	Ingen væsentlige bemærkninger
	5.22	Process Factory overvåger regelmæssigt serviceleverandøren. Dette sker ved gennemgang af aftalte rapporter og logninger samt udførelse af egentlige revisioner, for at sikre at aftalen overholdes, og at sikkerhedshændelser og - problemer håndteres betryggende. Process Factory dokumentere, at der løbende følges op på, at de benyttede Underdatabehandlere efterlever kravene til behandlingssikkerhed.	Vi har observeret, at der er indgået hostingaftale med itm8, og at der løbende følges op på denne ift. aftalte serviceniveauer.	Ingen væsentlige bemærkninger
			Vi har inspiceret itm8´s ISAE3402 erklæring for perioden 1. januar – 31. december 2025 for itm8 med henblik på at indhente tilstrækkelig information og bevis for implementering og funktionalitet af kontroller hos itm8.	PwC har i forbindelse med revisionen af itm8 identificeret afvigelser i kontrollerne (5.18, 8.19 og 8.32). Process Factory følger op på dette via etablerede tilsynsprocesser.
			Vi har forespurgt om Process Factory er i dialog med itm8 om IT-sikkerhed.	Ingen væsentlige bemærkninger
	5.24	Der skal fastlægges ledelsesansvar og -procedurer for at sikre en hurtig, effektiv og velordnet reaktion på informationssikkerhedshændelser. Process Factory dokumentere, at hændelser håndteres i henhold til en indarbejdet incident management-proces.	Vi har inspiceret Process Factory procedurer for håndtering af sikkerhedshændelser.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
2. Organisatoriske foranstaltninger (ISO27002:2022 Afsnit 5)				
	5.29	Der udarbejdes og vedligeholdes en beredskabsstyringsproces, som behandler de krav til informationssikkerhed, der er nødvendige for Process Factorys fortsatte drift.	Vi har forespurgt udvalgte medarbejdere om beredskabsstyring.	Ingen væsentlige bemærkninger
	5.29	Process Factory udarbejder og vedligeholder en beredskabsplan, der fastlægger roller og ansvar og dokumenterer de processer og foranstaltninger, der skal aktiveres i tilfælde af en nødsituation, som ikke kan håndteres med de normale daglige driftsprocedurer.	Vi har inspiceret, at der er udarbejdet en beredskabsplan.	Ingen væsentlige bemærkninger
	5.29	Process Factory udfører en gang årligt verificering af beredskabsplanen for at sikre reetablering kan ske inden for 3 dage. Process Factory sikrer, at der udføres beredskabsafprøvninger for at sikre, at de etablerede tekniske og organisatoriske foranstaltninger til håndteringen af et større nedbrud, fungerer efter hensigten.	Vi har forespurgt hvornår og hvordan der sidst er foretaget verificering/afprøvning af beredskabsplanen .	Ingen væsentlige bemærkninger
	5.34	Privatlivets fred og beskyttelse af personligt identificerbare oplysninger skal sikres som krævet i relevant lovgivning og regulering, hvor det er relevant.	Vi har forespurgt hvordan det sikres at håndtering af personinformationer altid følger relevante regler og lovgivning.	Ingen væsentlige bemærkninger
	5.36	Informationssystemer skal regelmæssigt gennemgås for at sikre overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder.	Vi har forespurgt hvordan det sikres at der sker en regelmæssig gennemgang af relevante systemer for at sikre overensstemmelse med Process Factorys sikkerhedspolitikker, -procedurer og -regler.	Ingen væsentlige bemærkninger
	5.37	Driftsafviklingsprocedurer for forretningskritiske systemer skal dokumenteres, føres ajour og være tilgængelige for server/drift og andre med arbejdsrelateret behov. Process Factory sikrer, at alle anvendte driftsprocedurer er dokumenteret.	Vi har observeret relevant Process Factorys dokumentation placeret i Process Factorys Knowledgebase.	Ingen væsentlige bemærkninger
			Vi har inspiceret en stikprøve af driftsprocedurer i Process Factorys Knowledgebase.	Ingen væsentlige bemærkninger
	5.37	Driften i Process Factorys datacenter dokumenteres efter gældende interne standarder. Relevante Process Factory-medarbejdere har adgang til teknisk dokumentation på alle kritiske driftssystemer, som er samlet på Process Factorys intranet. Viden akkumuleret i det daglige arbejde dokumenteres også i en fælles Knowledge-database til brug i effektivisering/løsning af lignende problemer i fremtiden. Process Factory sikrer, at ændringer til produktionsmiljøet styres gennem en indarbejdet change management-proces, der blandt andet omfatter risikovurdering samt test af funktionalitet og sikkerhed.	Vi har observeret relevant Process Factorys dokumentation placeret i Process Factorys Knowledgebase.	Ingen væsentlige bemærkninger
			Vi har inspiceret procedurer for ændringer i forretningskritisk infrastruktur.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
3. Personrelaterede foranstaltninger (ISO27002:2022 Afsnit 6)				
	6.1	Det er den ansættelsesansvarlige Process Factory-medarbejders ansvar at foretage forsvarligt baggrundstjek af kandidaten, hvis dette er relevant for stillingen.	Vi har forespurgt om der har været nyansættelser.	Ingen væsentlige bemærkninger
			Vi har forespurgt hvordan Process Factory sikrer rette kompetencer for kandidaten.	Ingen væsentlige bemærkninger
	6.1	Process Factory sikrer, at der som led i ansættelses/onboarding-proceduren gennemføres systematisk kontrol af nyansatte/eksterne konsulenters egnethed og hæderlighed, herunder at de ansatte ikke har strafbare forhold noteret på straffeattesten, som har betydning for Process Factorys behandlingsaktiviteter.	Vi har forespurgt hvordan Process Factory sikrer nyansatte/eksterne konsulenters egnethed, herunder hvordan straffeattester vurderes.	Ingen væsentlige bemærkninger
	6.2	Medarbejderen skal underskrive en aftale om ansættelse, som beskriver medarbejderens og Process Factorys ansvar og forpligtelser vedrørende informationssikkerhed.	Vi har forespurgt om forretningsgangen for afgivelse af tavsheds-klausuler med den HR-ansvarlige.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at der i medarbejdernes ansættelsesaftaler fremgår, at medarbejdere har tavshedspligt.	Ingen væsentlige bemærkninger
			Vi har inspiceret, at forhold om medarbejdernes ansvar og forpligtelser vedrørende informationssikkerhed er omtalt i IT sikkerhedspolitikken og i personalehåndbogen.	Ingen væsentlige bemærkninger
-	**6.3**	Process Factory sikrer, at der jævnligt gennemføres oplysningskampagner og uddannelse i informationssikkerhed og privatlivsbeskyttelse for Process Factorys medarbejdere.	Vi har forespurgt hvorledes og hvor ofte der gennemføres oplysning/uddannelse i informationssikkerhed for alle medarbejdere.	Ingen væsentlige bemærkninger
	6.5	Informationssikkerhedsansvar og -pligter, der forbliver gyldige efter opsigelse eller ændring af ansættelse, skal defineres, meddeles medarbejderen eller underleverandøren, og håndhæves.	Vi har forespurgt hvorledes informationssikkerhed håndhæves for opsagte/fratrådte medarbejdere/eksterne konsulenter.	Ingen væsentlige bemærkninger
	6.8	Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt. Process Factory udarbejder én gang årligt en samlet oversigt over hændelser, der har medført tab af tilgængelighed, fortrolighed eller integritet af de personoplysninger, som er omfattet af Databehandleraftalerne.	Vi har forespurgt udvalgte medarbejdere om, hvordan de rapporterer sikkerhedshændelser.	Ingen væsentlige bemærkninger
			Vi har forespurgt hvordan der systematisk indsamles information om sikkerhedshændelser, samt hvordan disse rapporteres til ledelsen.	Ingen væsentlige bemærkninger
			Vi har inspiceret log over sikkerhedshændelser.	Ingen væsentlige bemærkninger
	6.8	Alle medarbejdere, samarbejdspartnere og andre brugere af systemer og tjenester har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i systemer og tjenester.	Vi har forespurgt udvalgte medarbejdere om, hvordan de rapporterer sikkerhedssvagheder.	Ingen væsentlige bemærkninger
			Vi har forespurgt hvordan der systematisk indsamles information om sikkerhedssvagheder, samt hvordan disse rapporteres til ledelsen.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u7033520196396680

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
4. Fysiske foranstaltninger (ISO27002:2022 Afsnit 7)				
	7.2	Sikre områder beskyttes af adgangskontrol, så kun autoriserede personer kan få adgang, herunder eksterne itm8 kunder. Databehandleren skal sikre, at adgangen til Databehandlerens fysiske produktionsfaciliteter er beskyttet med et passende adgangskontrolsystem.	Vi har inspiceret ISAE3402 erklæring for perioden 1. januar – 31. december 2025 for itm8 for de områder, hvor Process Factory har itm8 udstyr placeret hos itm8 for at påse: · at der kræves adgangsbrik/id-kort og personlig kode for at få adgang til driftslokaler · at kun autoriserede personer har adgang til datacenteret.	Ingen væsentlige bemærkninger
	7.2	Af- og pålæsningsområder samt andre områder, hvor offentligheden kan få adgang, er overvåget.	Vi har inspiceret, at der ikke er offentlig adgang til områder, hvor Process Factory udstyr er placeret, samt at der er overvågning.	Ingen væsentlige bemærkninger
	7.3	Fysisk sikkerhed for kontorer, lokaler og faciliteter skal udformes og anvendes.	Vi har forespurgt hvordan fysisk sikkerhed for Proces Factorys lokaler er implementeret og anvendes.	Ingen væsentlige bemærkninger
	7.4	For at sikre mod tyveri er datacenter sikret med nyeste alarmteknologi. Både internt og eksternt bliver hele bygningen overvåget via bevægelsesdetektorer. Databehandleren skal sikre, at der er etableret sikring af perimeteren af de områder, hvor behandlingen af personoplysningerne foregår, fx gennem videoovervågning, alarmer, receptioner samt div. former for afspærringer.	Vi har inspiceret ISAE3402 erklæring for perioden 1. januar – 31. december 2025 for itm8 for de områder, hvor Process Factory har itm8 udstyr placeret hos itm8 for at påse, at der er videoovervågning.	Ingen væsentlige bemærkninger
	7.5	Virksomheden har tilrettelagt den fysiske sikkerhed, så skadevirkninger fra brand, oversvømmelser, jordskælv, eksplosioner, civile optøjer og andre former for natur- eller menneskeskabte trusler minimeres. Databehandleren skal sikre, at der er etableret nødstrømsforsyning, der kan overtage elforsyningen til produktionsfaciliteterne i tilfælde af nedbrud/fejl i hoved-elforsyningen. Databehandleren skal have etableret passende, tekniske foranstaltninger til at detektere og imødegå røgudvikling og brand.	Vi har inspiceret ISAE3402 erklæring for perioden 1. januar – 31. december 2025 for itm8 for de områder, hvor Process Factory har itm8 udstyr placeret hos itm8 for at påse, at der er sikkerhedsforanstaltninger i og omkring datacenteret.	Ingen væsentlige bemærkninger
	7.6	Procedurer for arbejde i sikre områder skal udformes og anvendes.	Vi har inspiceret proceduren for arbejde i sikrede områder.	Ingen væsentlige bemærkninger
	7.7	Der vedtages en ryddet skrivebordspolitik for papirer og flytbare lagringsmedier og en politik for ryddet skærm for informationsbehandlingsfaciliteter.	Vi har inspiceret politikken for ryddet skrivebord..	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
4. Fysiske foranstaltninger (ISO27002:2022 Afsnit 7)				
	7.8	Udstyr er placeret og beskyttet, så risikoen for skader og uautoriseret adgang minimeres. Databehandleren skal have implementeret procedurer for at håndtere det løbende vedligehold af det fysiske produktionsudstyr og sikre, at disse procedurer efterleves.	Vi har inspiceret ISAE3402 erklæring for perioden 1. januar – 31. december 2025 for itm8 for de områder, hvor Process Factory har itm8 udstyr for at påse, at der er udført beskyttelse af kritisk udstyr.	Ingen væsentlige bemærkninger
	7.11	Udstyr er sikret mod forsyningssvigt i overensstemmelse med udstyrets betydning for kritiske forretningssystemer.	Vi har inspiceret ISAE3402 erklæring for perioden 1. januar – 31. december 2025 for itm8 for de områder, hvor Process Factory har itm8 udstyr for at påse, at der er etableret en fuldt redundant infrastruktur med særskilt backup.	Ingen væsentlige bemærkninger
	7.13	Udstyr vedligeholdes efter forskrifterne for at sikre dets tilgængelighed og integritet. Databehandleren skal sikre, at uvedkommende ikke får adgang til personoplysninger omfattet af Databehandleraftalerne i forbindelse med reparation, service eller destruktion af fysisk udstyr. Såfremt adgangen til personoplysningerne ikke kan undgås, skal Databehandleren sikre, at der anvendes erklæringer om tavshedspligt eller lignende.	Vi har inspiceret ISAE3402 erklæring for perioden 1. januar – 31. december 2025 for itm8 for de områder, hvor Process Factory har itm8 udstyr for at påse, at der forligger retningslinjer for, hvordan udstyr vedligeholdes korrekt.	Ingen væsentlige bemærkninger
	7.14	Alt udstyr, der indeholder lagringsmedier, skal verificeres for at sikre, at følsomme data og licenseret software er blevet fjernet eller sikkert overskrevet inden bortskaffelse eller genbrug. Process Factory sikrer, at bortskaffelse af fysiske lagringsmedier og anden hardware sker på en sikkerheds- og miljømæssig forsvarlig måde.	Vi har forespurgt hvordan det sikres at bortskaffelse af fysiske lagringsmedier (harddisk, usb o.a.) sker på en sikkerheds- og miljømæssig forsvarlig måde.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
5. Teknologiske foranstaltninger (ISO27002:2022 Afsnit 8)				
	8.1	Der vedtages en politik og understøttende sikkerhedsforanstaltninger for at styre de risici, der opstår ved brug af mobilt udstyr, og til sikring af, at der ikke opbevares personoplysninger udenfor Process Factorys miljøer.	Vi har inspiceret, at der foreligger en opdateret instruks for anvendelse af hjemmearbejdsplads samt mobilt udstyr.	Ingen væsentlige bemærkninger
	8.1	Brugerne skal sikre, at udstyr uden opsyn har passende beskyttelse.	Vi har forespurgt hvordan det sikres at udstyr uden opsyn har passende beskyttelse.	Ingen væsentlige bemærkninger
	8.2	Udvidede adgangsrettigheder tildeles i begrænset omfang og kun hvis den ansatte har behov for dette til at udføre sit arbejde. Udvidede rettigheder knyttes til særlige brugeridentiteter der entydigt identificerer brugeren. Process Factory sikrer, at systemadministrative/privilegerede adgange til de personoplysninger, der er omfattet af Databehandleraftalerne, sker med 2-faktor autentificering (hvor det er teknisk muligt) og efter særlige procedurer for håndtering, herunder oprettelse, anvendelse, logning og opfølgning.	Vi har forespurgt udvalgte medarbejdere, hvordan tildeling af udvidede adgangsrettigheder sker.	Ingen væsentlige bemærkninger
			Vi har observeret brugere med udvidede beføjelser håndteres efter særlige procedurer.	Ingen væsentlige bemærkninger
	8.5	Systemadgang beskyttes af en sikker log-on-procedure (min. single sign-on (SSO) eller PKI).	Vi har inspiceret proceduren for log-on.	Ingen væsentlige bemærkninger
	8.6	Ressourceforbruget overvåges og tilpasses Process Factory sikrer, at kapacitetsudnyttelsen (fx CPU og båndbredde) på de tekniske komponenter, der indgår i behandlingen af personoplysninger, overvåges og analyseres løbende og tilpasses med henblik på opretholdelse af den aftalte tilgængelighed. Process Factory har etableret overvågning af IT-miljøet, herunder sikre, at der sker alarmering ved fejl på de tekniske komponenter, der indgår i den samlede løsning (servere, databaser, netværksudstyr mv).	Vi har observeret driftsprocesser for verificering af passende ressourcekapacitet mod anvendt ressourceforbrug.	Ingen væsentlige bemærkninger
			Vi har forespurgt hvilke tiltag der iværksættes når der er stor belastning på systemkapacitet [CPU, Storage, osv.].	Ingen væsentlige bemærkninger
	8.7	Process Factory scanner alt netværkstrafik for virus via såkaldt parameter-scanning. I visse tilfælde scannes servere direkte. Såfremt data er virusbehæftet, opretholder Process Factory sig retten til at forsøge rensning af disse data. Såfremt dette ikke er tilstrækkeligt, forholder Process Factory sig retten til at slette de inficerede data.	Vi har observeret, at der er installeret opdateret antivirus software på et udvalg af servere, samt i relevante firewalls.	Ingen væsentlige bemærkninger
	8.7	Process Factory sikrer, at klienter og servere hos Process Factory er beskyttet med antivirus/-malware-programmel, som løbende opdateres.	Vi har forespurgt hvordan antivirus og -malware programmer holdes løbende opdateret.	Ingen væsentlige bemærkninger
	8.8	Process Factory indhenter løbende informationer om eventuelle sårbarheder i de anvendte systemer. Sårbarhederne evalueres, og passende foranstaltninger skal implementeres for at modvirke de nye risici.	Vi har forespurgt hvordan information om sårbarheder indsamles, evalueres og tilhørende foranstaltninger implementeres. Evt. ifbm. sikkerhedshændelser.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
5. Teknologiske foranstaltninger (ISO27002:2022 Afsnit 8)				
	8.8	Process Factory sikrer, at de applikationer/aktiver, der varetager behandlingen af personoplysninger, sikkerhedspatches hurtigst muligt efter frigivelsen af patch'en.	Vi har forespurgt hvordan det sikres at systemer involveret ved behandling af personoplysninger, løbende sikkerhedspatches hurtigst muligt.	Ingen væsentlige bemærkninger
	8.8	Process Factory sikrer, at software på klienter, servere, netværksudstyr mv. sikkerhedsopdateres i henhold til formelle politikker og procedurer for patch management.	Vi har forespurgt om software på klienter, servere, netværksudstyr mv. sikkerhedsopdateres i henhold til formelle politikker og procedurer.	Ingen væsentlige bemærkninger
	8.8	Windows opdateringer udføres via Microsofts værktøj Intune. Windows opdateringer implementeres ugentligt efter beskreven procedure.	Vi har inspiceret procedurer for opdateringer.	Ingen væsentlige bemærkninger
			Vi har observeret, at der sker automatisk opdatering for kritiske og sikkerhedsmæssige opdateringer for Windows servere.	Ingen væsentlige bemærkninger
	8.8	Process Factory sikrer, at de etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests. Resultatet af disse afprøvninger stilles til rådighed for den Process Factorys kunder, når de anmoder herom.	Vi har inspiceret at der løbende foretages sårbarhedsscanninger og penetrationstests, samt resultaterne af disse afprøvninger.	Ingen væsentlige bemærkninger
	8.13	Der tages sikkerhedskopier af Process Factorys væsentlige informationsaktiver, herunder parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har inspiceret retningslinierne for sikkerhedskopiering.	Ingen væsentlige bemærkninger
	8.13	Process Factory sørger for, at der tages backup af de data, herunder personoplysninger, som Process Factory behandler på vegne af Process Factorys kunder, samt af alle de komponenter/aktiver/ applikationer, som understøtter behandlingen af data. Process Factory afprøver restore af datafiler samt det samlede understøttende it-miljø fra backup med jævne mellemrum.	Vi har observeret, at der er afprøvet restore fra backup med jævne mellemrum af datafiler, samt det samlede understøttende it-miljø.	Ingen væsentlige bemærkninger
	8.13	Process Factory sikrer, at personoplysninger, som tidligere er slettet, fx i forlængelse af en henvendelse fra en registreret, ikke genintroduceres i produktionsmiljøet efter genindlæsning af backup.	Vi har forespurgt hvordan det sikres at tidligere slettede personoplysninger, ikke genskabes ved restore fra backup.	Ingen væsentlige bemærkninger
	8.15	Brugen af virksomhedens informationsbehandlingssystemer overvåges og følges op løbende.	Vi har observeret, at brugen af virksomhedens informationsbehandlingssystemer overvåges og følges op løbende.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u7033520196396680

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
5. Teknologiske foranstaltninger (ISO27002:2022 Afsnit 8)				
	8.15	Fejl logges og analyseres, og nødvendige udbedringer og modforholdsregler gennemføres. Process Factory sikrer, at der er etableret logning af følgende aktiviteter på de tekniske komponenter, der indgår i løsningen (servere, databaser, netværksudstyr mv.): 1. Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder 2. Sikkerhedsændringer/-hændelser omfattende: i. Ændringer i logopsætninger, herunder deaktivering af logning ii. Ændringer i systemrettigheder til brugere iii. Fejlede forsøg på log-on til systemer, databaser og netværk. Process Factory overvåger og logger applikationsmæssig aktivitet herunder brugeraktivitet, afvigelser og fejl, informationssikkerhedsmæssige hændelser samt behandlinger, hvori Personoplysningerne indgår. Loggen indeholder som minimum oplysninger om tidspunkt, bruger, anvendelsestype og søgekriterium/resultat.	Vi har observeret, at der er etableret logning af aktiviteter på de tekniske komponenter, samt overvågning og logning af applikationsmæssig aktiviteter, herunder informationssikkerhedshændelser.	Ingen væsentlige bemærkninger
	8.15	Logningsfaciliteter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang. Process Factory sikrer, at logoplysningerne er beskyttet mod manipulation og tekniske fejl samt at loggen gennemgås løbende.	Vi har forespurgt hvordan det sikres at logningssystemer og -data beskyttes imod senere ændringer, samt hvor ofte logs gennemgås.	Ingen væsentlige bemærkninger
	8.15	Der er, så vidt der er muligt, etableret logning af alle aktiviteter, der kræver systemadministrator rettigheder, eller andre særlige rettigheder. Hvor det ikke er muligt at etablere denne logning, er der etableret kompenserende forebyggende manuelle procedurer og registreringer, så revisionssporet til stadighed er intakt.	Vi har inspiceret metoden for logning af aktiviteter der kræver systemadministrator rettigheder, samt evt. manuelle registreringer.	Ingen væsentlige bemærkninger
	8.17	Urene i alle relevante informationsbehandlingssystemer, inden for en organisation eller et sikkerhedsdomæne, skal synkroniseres med en enkelt referencetidskilde.	Vi har forespurgt hvordan det sikres at tiden i alle Process Factorys systemer er synkroniseret til en enkelt reference.	Ingen væsentlige bemærkninger
	8.18	Anvendelsen af hjælpeprogrammer, der kan være i stand til at tilsidesætte system- og applikationskontrol, skal begrænses og kontrolleres nøje.	Vi har forespurgt hvordan anvendelsen af hjælpeprogrammer, der potentielt kan omgå sikkerhedsfunktioner, begrænses/kontrolleres.	Ingen væsentlige bemærkninger
	8.19	Der skal gennemføres procedurer til kontrol af installationen af software på driftssystemer.	Vi har inspiceret procedurer for installation af software på driftssystemer.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
5. Teknologiske foranstaltninger (ISO27002:2022 Afsnit 8)				
	8.19	Der skal fastsættes og gennemføres regler for brugernes installation af software.	Vi har inspiceret reglerne for brugernes installation af software.	Ingen væsentlige bemærkninger
	8.20	Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og de transmitterede data. Den netværksansvarlige skal sikre, at der er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder logning og overvågning. Process Factory sikrer, at designet af det benyttede netværk, fx gennem anvendelse af logisk segmentering, understøtter en høj grad af beskyttelse af de behandlede personoplysninger.	Vi har inspiceret netværksstegning og påset, at der er installeret firewall.	Ingen væsentlige bemærkninger
	8.20	Fysisk og logisk adgang til diagnose- og konfigurationsporte kontrolleres.	Vi har forespurgt om der på firewalls er port-regler, der skal sikre kun tilladt trafik får adgang til netværket.	Ingen væsentlige bemærkninger
	8.24	Der skal udvikles og gennemføres en politik for anvendelse af kryptografiske kontroller til beskyttelse af oplysninger.	Vi har inspiceret politikken for anvendelse af kryptografi.	Ingen væsentlige bemærkninger
	8.24	Process Factory sikrer, at transmission af personoplysninger er krypteret med industristandarder for stærk kryptering (encryption in transit).	Vi har forespurgt hvordan det sikres at personoplysninger altid er sikret med stærk kryptering.	Ingen væsentlige bemærkninger
	8.24	Process Factory sikrer, at de filsystemer og databaser, der anvendes til registrering og opbevaring af fortrolige og følsomme personoplysninger, er krypteret med industristandarder for stærk kryptering (encryption at rest).	Vi har forespurgt hvordan det sikres at filsystemer og databaser, der anvendes til personoplysninger, altid er sikret med stærk kryptering.	Ingen væsentlige bemærkninger
	8.24	Der skal udvikles og gennemføres en politik for brug, beskyttelse og levetid for kryptografiske nøgler i hele deres livscyklus.	Vi har inspiceret politikken for brug, beskyttelse og levetid for kryptografiske nøgler.	Ingen væsentlige bemærkninger
	8.25	Regler for udvikling af software og systemer skal fastlægges og anvendes på udviklingen i organisationen.	Vi har inspiceret Process Factory regler for udvikling af software og systemer.	Ingen væsentlige bemærkninger
	8.26	Oplysninger, der er involveret i applikationstjenester, der passerer over offentlige net, skal beskyttes mod svigagtig aktivitet, kontrakttvister og uautoriseret videregivelse og ændring. Process Factory sikrer, at funktionalitet/services, som eksponeres via internettet, er beskyttet mod almindeligt kendte typer af cyber-trusler, fx som de optræder på OWASP-Top-10.	Vi har forespurgt hvordan det sikres at information som passere over offentlige net, altid er sikret med stærk kryptering, samt at der opnås sikkerhed for afsender og modtagers identitet.	Ingen væsentlige bemærkninger
	8.27	Principper for konstruktion af sikre systemer skal etableres, dokumenteres, vedligeholdes og anvendes på alle bestræbelser på at gennemføre informationssystemer.	Vi har inspiceret at principper for konstruktion af sikre systemer er etableret, vedligeholdes samt anvendes.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

	2022 Ref.	ISO27002 Kontrol	Test af kontrol Juni 2025 - Maj 2026	Bemærkning 2026
5. Teknologiske foranstaltninger (ISO27002:2022 Afsnit 8)				
	8.31	Der er et separat dedikeret testmiljø. Testmiljøet er så identisk med driftsmiljøet som muligt. Process Factory har implementeret adskillelse (logisk og evt. fysisk) af de IT-miljøer, der understøtter henholdsvis udvikling, test og produktion af de databehandlingsaktiviteter, som Process Factory udfører for Process Factorys kunder.	Vi har observeret, at der er et separat dedikeret testmiljø.	Ingen væsentlige bemærkninger
			Vi har forespurgt om testmiljøet er adskilt helt fra driftsmiljøet.	Ingen væsentlige bemærkninger
	8.32	Ændringer til forretningskritisk informationsbehandlingsudstyr, -systemer og -procedurer styres gennem en formaliseret procedure. Process Factory sikrer, at ændringer til produktionsmiljøet implementeres gennem en indarbejdet release- og deployment proces, der blandt andet omfatte risikovurdering samt test af funktionalitet og sikkerhed.	Vi har observeret change management procedurer.	Ingen væsentlige bemærkninger
			Vi har forespurgt udvalgte medarbejdere, hvordan ændringshåndtering udføres.	Ingen væsentlige bemærkninger
			Vi har inspiceret en stikprøve på en konkret change/release.	Ingen væsentlige bemærkninger

This document has esignatur Agreement-ID: a58898u70335201963968O

Dette dokument er underskrevet af nedenstående parter, der med deres underskrift har bekræftet dokumentets indhold samt alle datoer i dokumentet.

Susanne Møllegaard

Navn returneret af MitId: NAVNE & ADRESSEBESKYTTET
Direktør
ID: 0cbf9c4e-69ba-4f00-956e-a533de2c507b
IP-adresse: 87.50.166.68:54291:54291
Dato for underskrift: 11-06-2026 19:46:46 CEST (+02:00)
Underskrevet med MitID

Per Jensen

Navn returneret af MitId: Per Jensen
Statsautoriseret revisor
ID: 5f9acb21-b1bd-4ad5-ae5c-fddc50c2da58
IP-adresse: 77.241.128.162:18204:18204
Dato for underskrift: 11-06-2026 19:57:04 CEST (+02:00)
Underskrevet med MitID

This document has esignatur Agreement-ID: a58898u70335201963968O

This document is signed with esignatur. Embedded in the document is the original agreement document and a signed data object for each signatory. The signed data object contains a mathematical hash value calculated from the original agreement document, which secures that the signatures is related to precisely this document only. Prove for the originality and validity of signatures can always be lifted as legal evidence.

The document is locked for changes and all cryptographic signature certificates are embedded in this PDF. The signatures therefore comply with all public recommendations and laws for digital signatures. With esignatur's solution, it is ensured that all European laws are respected in relation to sensitive information and valid digital signatures. If you would like more information about digital documents signed with esignatur, please visit our website at www.esignatur.dk.

Secured by esignatur