

ENVO IT A/S

Uafhængig revisors ISAE 3402 type I
erklæring med sikkerhed om levering af
IT-løsninger og service

pr. 07/05 2025

The logo for ENVO IT, featuring the word "ENVO" in a bold, italicized, green sans-serif font, followed by "IT" in a similar but smaller font.

Indhold

1	Serviceleverandørens udtalelse	2
2	Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres design	4
3	Systembeskrivelse	6
	3.1 Beskrivelse af serviceorganisationen	6
	3.2 Beskrivelse af services	9
	3.3 Risikovurdering	10
	3.4 Kontrolforanstaltninger	11
4	Tests udført af EY	15
	4.1 Formål og omfang	15
	4.2 Kontrolmål, kontrolaktivitet, test og resultat heraf	16

1 Serviceleverandørens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for de kunder, der har anvendt IT-services tilpasset til den enkelte kunde fra ENVO IT, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som underleverandører udfører og kunderne selv har udført, når de opnår en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

ENVO IT anvender Microsoft som cloudplatform til levering af Operations & Cybersikkerhedsydelser til kunderne. Yderligere anvendes Sentia til hosting. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos ENVO IT og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Microsoft og Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af vores kontroller, er passende designet og implementeret. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af ENVO IT's kontroller, er passende designet og implementeret sammen med relaterede kontroller hos ENVO IT. Beskrivelsen omfatter ikke kontrolaktiviteter udført af kunder.

ENVO IT bekræfter, at:

- (a) Den medfølgende beskrivelse, i sektion 3, giver en retvisende beskrivelse af de tilpassede IT-services der leveres til den enkelte kunde pr. 07/05-2025. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:
 - (i) redegør for, hvordan systemet var designet og implementeret for at kunne levere tilpassede IT-services til den enkelte kunde, herunder redegør for:
 - de typer af ydelser, der er leveret
 - de processer i både it- og manuelle systemer
 - hvordan systemet behandlede andre betydelige begivenheder og forhold
 - ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.
 - relevante kontrolmål og kontroller designet til at nå disse mål
 - kontroller, som vi med henvisning til systemets design har forudsat ville være implementeret af brugervirksomhederne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
 - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante
 - (ii) ikke udelader eller forvansker information, der er relevant for omfanget af det beskrevne system, 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 systemet, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

- (b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet pr. 07/05-2025, hvis relevante kontroller hos underleverandører var hensigtsmæssigt designet og implementeret, og kunder har designet og implementeret de komplementerende kontroller som forudsættes i designet af ENVO IT's kontroller pr. 07/05-2025. Kriterierne for denne udtalelse var, at
- (i) de risici, som truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret, og
 - (ii) de identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer opnåelsen af de anførte kontrolmål.

København, den 19. juni 2025
ENVO IT A/S

Johan Frantz Dhin
Partner

2 Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres design

Til: ENVO IT A/S

Omfang

Vi har fået som opgave at afgive erklæring om ENVO IT's beskrivelse i sektion 3 vedrørende levering af IT- og serviceløsninger tilpasset kundernes specifikke behov pr. 07/05-2025 (beskrivelsen) og om design af de kontroller, der knytter sig de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af ENVO IT's kontroller, er passende designet og implementeret sammen med relaterede kontroller hos ENVO IT. Vores handlinger har ikke omfattet kontrolaktiviteter udført af kunderne, og vi har ikke vurderet egnetheden af design eller implementeringen af kontrolaktiviteter hos kunderne.

ENVO IT anvender Microsoft som cloudplatform til levering af Operations & Cybersikkerhedsydelser til kunderne. Yderligere anvendes Sentia til hosting. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos ENVO IT og medtager således ikke kontrolmål og relaterede kontroller hos Microsoft og Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af ENVO IT's kontroller, er passende designet og implementeret sammen med de relaterede kontroller hos ENVO IT. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Microsoft og Sentia, og vi har ikke vurderet egnetheden af design eller implementeringen af kontrolaktiviteter hos underleverandører.

ENVO IT's ansvar

ENVO IT er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene; identifikation af de risici der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier der er præsenteret i ledelsens udtalelse; samt for designet, implementeringen og operationelt effektive kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

EY Godkendt Revisionspartnerselskab anvender International Standard on Quality Management 1, 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.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om ENVO IT's beskrivelse samt om design af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB og yderligere krav ifølge dansk revisorlovgivning. 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 designet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og designet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i



serviceleverandørens beskrivelse af sit system samt for kontrollernes design. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentationen af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål og hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i sektion 1.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Begrænsning i kontroller hos en serviceleverandør

ENVO IT's 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 forhindre eller opdage fejl eller udeladelser ved ENVO IT's levering af IT- og serviceløsninger tilpasset kundernes specifikke behov.

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 sektion 1. Det er vores opfattelse:

- (a) at beskrivelsen af ENVO IT's levering af IT- og serviceløsninger tilpasset kundernes specifikke behov, således som det var designet og implementeret pr. 07/05-2025, i alle væsentlige henseender er retvisende, og
- (b) at kontrollerne, der knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet pr. 07/05-2025, hvis kontroller hos underleverandører og komplementerende kontroller hos kunder var hensigtsmæssigt designet og implementeret pr. 07/05-2025 som forudsat i designet af ENVO IT's kontroller.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4, er udelukkende tiltænkt de kunder, der har anvendt ENVO IT's levering af IT- og serviceløsninger, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundens egne kontroller, ved opnåelsen af en forståelse af kundernes informationssystemer, der er relevante for regnskabsafleggelsen.

København, 19. juni 2025

EY

Godkendt Revisionspartnerselskab

CVR no.: 30 70 02 28

Jesper Due Sørensen
Partner

Nils B. Christiansen
statsaut. revisor
mne34106

3 Systembeskrivelse

Denne beskrivelse er udarbejdet for at informere ENVO IT A/S' kunder og disses revisorer om de leverede services og det tilhørende kontrolmiljø. Formålet er at opfylde informationskravene i henhold til ISAE 3402, "Erklæringsopgaver med sikkerhed om kontroller hos en serviceleverandør".

Beskrivelsen giver indsigt i de kontroller, ENVO IT A/S har implementeret for at understøtte en sikker og stabil drift af de omfattede IT-services, som kan have betydning for brugerorganisationernes processer, herunder potentielt den finansielle rapportering. ENVO IT's ledelsessystem for informationssikkerhed (ISMS) er designet med udgangspunkt i de anerkendte principper og kontrolforanstaltninger beskrevet i ISO/IEC 27001:2022 og ISO/IEC 27002:2022 for at sikre en struktureret tilgang til risikostyring og beskyttelse af information.

3.1 Beskrivelse af serviceorganisationen

ENVO IT A/S, grundlagt i 2019, er en IT-servicevirksomhed drevet af partnere, der specialiserer sig i at levere IT-løsninger tilpasset kundernes specifikke behov. Virksomheden har oplevet vækst siden etableringen og beskæftiger pr. 1. april 2025 39 medarbejdere.

Med kontor centralt i København tilbyder ENVO IT A/S en portefølje af ydelser, der dækker:

- ▶ Cloud Operations & Cybersikkerhed
- ▶ Device Management
- ▶ Drift af netværk og Infrastruktur
- ▶ IT-rådgivning og konsulentytelser
- ▶ IT-support

ENVO IT A/S er certificeret Microsoft Modern Workplace Partner og Apple Authorized Reseller, hvilket understøtter levering af løsninger baseret på disse teknologiplatforme. Partnerskaberne giver adgang til opdateret teknologi og supportmuligheder for kunder, der anvender Microsoft-, Apple- eller hybride miljøer.

For at levere et komplet og robust serviceudbud, benytter ENVO IT A/S sig af nøje udvalgte underleverandører til specifikke, kritiske funktioner. Blandt disse er Microsoft centrale, idet deres cloud-platforme (f.eks. Microsoft Azure og Microsoft 365) danner grundlag for en væsentlig del af de Cloud Operations & Cybersikkerhedsytelser, ENVO IT A/S tilbyder, som beskrevet i afsnit 3.2.2. En anden kritisk underleverandør er Sentia A/S, som leverer data center ydelser for specifik infrastruktur. Disse relationer til centrale underleverandører styres og evalueres løbende gennem ENVO IT A/S's procedurer for leverandørstyring, som nærmere beskrevet i afsnit 3.4.9, for at sikre overholdelse af ENVO IT A/S's kvalitets- og sikkerhedsstandarder.

Virksomhedens målsætning er at fungere som en samlet leverandør af IT-løsninger, der understøtter kundernes drift og udvikling. Dette opnås gennem teknisk ekspertise og en serviceorienteret tilgang, hvor ydelser tilpasses den enkelte kundes behov.

ENVO IT A/S prioriterer levering af stabile IT-løsninger og et højt serviceniveau. Et internt mål er at løse en høj andel af alle supporthenvendelser ved første kontakt, som led i bestræbelserne på effektiv sagsbehandling.

Organisation og ansvar:

Organisationen er struktureret omkring de enkelte partners ekspertiseområder med klare ansvarsområder for at sikre effektiv servicelevering og overholdelse af sikkerhedspolitikker.

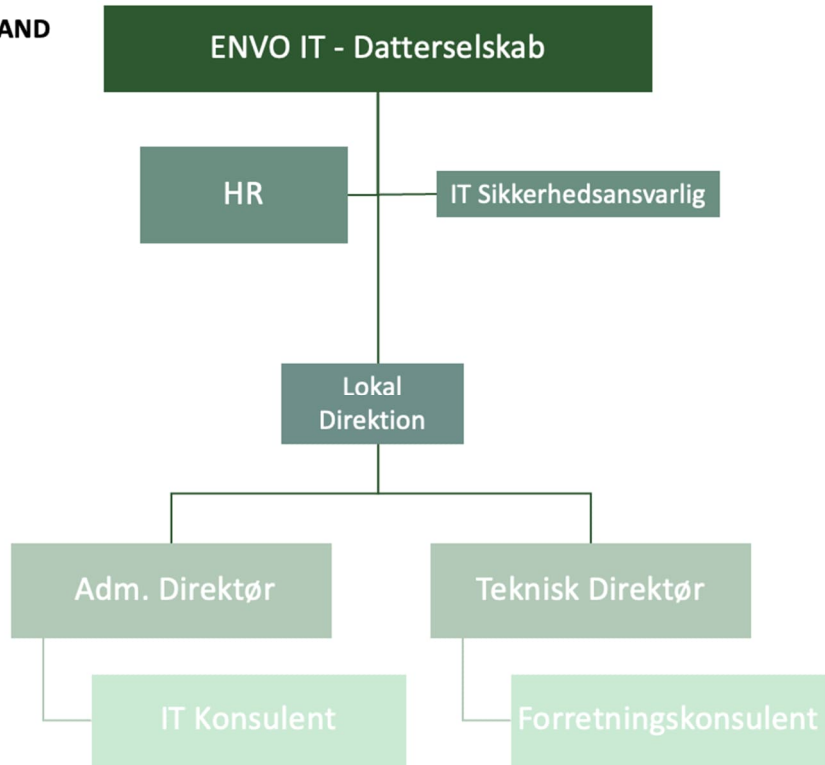
ENVO IT - KØBENHAVN



ENVO IT - KØBENHAVN

ENVO IT - KØBENHAVN
Ejerledende partnerkreds
<ul style="list-style-type: none"> • Karl-Emil Pedersen, Administration og HR • Torkel Fredly, Partner, Infrastruktur Teamet • Christian Carlsen, Partner, IT Konsulent teamet • Mark Lajer, Partner, Apple Specialist Teamet • Frantz Dhin, Partner, Cybersikkerhed Teamet
Direktionen
<ul style="list-style-type: none"> • Karl-Emil Pedersen • Signe Gry Bangsgaard Høybye
Ledelsen
<ul style="list-style-type: none"> • Karl-Emil Pedersen • Torkel Fredly • Christian Carlsen • Mark Lajer • Frantz Dhin • Signe Gry Bangsgaard Høybye • Kristine Redberga
Organisationen
<ul style="list-style-type: none"> • IT-Konsulent teamet • Device Management teamet • Infrastruktur teamet • Cloud Operations & Cybersikkerhed teamet • Elev teamet
IT Sikkerhedsansvarlig
<ul style="list-style-type: none"> • Frantz Dhin
Salg
<ul style="list-style-type: none"> • Karl-Emil
Stabsfunktion - HR, Administration & Marketing
<ul style="list-style-type: none"> • Karl-Emil Pedersen • Signe Gry Bangsgaard Høybye

ENVO IT – JYLLAND



ENVO IT – JYLLAND



3.2 Beskrivelse af services

ENVO IT A/S leverer IT-services til en bred kundegruppe, fra mindre virksomheder til større organisationer. For mange kunder varetager ENVO IT A/S væsentlige dele af IT-funktionen og håndterer opgaver, der understøtter kundernes daglige drift. Fokus er på at levere IT-løsninger, der er tilpasset kundernes forretningsmæssige behov og processer.

For at sikre kvaliteten og pålideligheden af ydelserne har ENVO IT A/S etableret interne kontroller, procedurer og politikker, som er relevante for ISAE 3402 rapportens kontrolmålsætninger. Ansvar for vedligeholdelse og overholdelse af disse er forankret hos relevante ledere og medarbejdere i organisationen.

Serviceporteføljen omfatter følgende hovedtyper:

3.2.1 Device Management

ENVO IT's Device Management service omfatter administration og overvågning af brugerorganisationens IT-enheder (computere, tablets, smartphones). Formålet er at understøtte enhedernes ydeevne, sikkerhed og compliance.

- ▶ Centraliseret administration: Udrulning og håndtering af opdateringer, sikkerhedspatches og konfigurationer via centraliserede administrationsværktøjer så som Intune og JAMF Pro. Dette bidrager til at reducere sårbarheder.
- ▶ Overvågning og rapportering: Løbende overvågning af enheders status og generering af rapporter til brug for compliance og sikkerhedsoverblik.
- ▶ Politikthåndhævelse: Implementering og håndhævelse af sikkerhedspolitikker på enheder (f.eks. krav til adgangskode, kryptering), herunder via Mobile Device Management (MDM) funktionalitet.
- ▶ Incident Response: Procedurer for at identificere, isolere og håndtere kompromitterede enheder for at begrænse potentielle sikkerhedsbrud og understøtte overholdelse af databeskyttelsesregler (GDPR).

3.2.2 Cloud Operations & Cybersikkerhed

ENVO IT A/S designer, implementerer og administrerer cloud-løsninger, primært baseret på Microsofts public cloud-platforme. Ydelsen omfatter:

- ▶ Skalbarhed og Flexibilitet: Levering af cloud-infrastruktur, der kan tilpasses brugerorganisationens skiftende behov.
- ▶ Cybersikkerhedsforanstaltninger: Implementering og drift af sikkerhedskontroller til beskyttelse af cloud-miljøet og data, herunder:
 - Datakryptering: Anvendelse af kryptering for data i transit og data i hvile, hvor relevant.
 - Adgangskontrol: Administration af brugeradgange, roller og rettigheder, herunder håndhævelse af multifaktorautentifikation (MFA) for at sikre, at kun autoriserede brugere har adgang.
 - Sikkerhedsovervågning: Kontinuerlig overvågning af cloud-miljøet for potentielle sikkerhedstrusler og uregelmæssigheder, med henblik på hurtig detektion og respons.
 - Compliance: Understøttelse af brugerorganisationernes overholdelse af relevante regulativer (f.eks. GDPR) gennem tekniske og organisatoriske foranstaltninger.
 - Leverandørstyring: Samarbejde med udvalgte cloud-leverandører, der lever op til anerkendte sikkerhedsstandarder. Processer for vurdering af underleverandører er etableret.
 - Backup og Disaster Recovery: Etablering og test af backup- og gendannelsesprocedurer for data og systemer i cloud-miljøet for at sikre forretningskontinuitet.

3.2.3 Netværk og infrastruktur

ENVO IT A/S leverer og administrerer netværks- og infrastrukturløsninger, der danner fundamentet for kundernes IT-miljø.

- ▶ Design og Implementering: Rådgivning om og implementering af netværksarkitektur (LAN, WAN, Wi-Fi) og serverinfrastruktur (on-premise eller hybrid).
- ▶ Drift og Vedligeholdelse: Overvågning, patching og vedligeholdelse af netværkskomponenter og servere for at sikre stabilitet og ydeevne.
- ▶ Sikkerhed: Implementering af sikkerhedsforanstaltninger som firewalls, VPN og netværkssegmentering for at beskytte mod uautoriseret adgang og cyberangreb.
- ▶ Skalbarhed: Design af løsninger, der kan skaleres i takt med brugerorganisationens behov.

3.2.4 IT-konsulentytelser & IT-Support

ENVO IT's konsulenter leverer strategisk og taktisk rådgivning om IT-infrastruktur, sikkerhed, cloud-strategi og digitalisering. Rådgivningen sigter mod at optimere kundernes IT-miljø og understøtte deres forretningsmål.

Konsulentafdelingen yder desuden teknisk assistance til brugerorganisationernes medarbejdere ved IT-relaterede problemer. Support leveres via telefon, e-mail, fjernsupport, on-site inden for aftalte service-niveauer (SLA'er). Formålet er at sikre hurtig og effektiv problemløsning for at minimere driftsforstyrrelser hos kunden.

3.3 Risikovurdering

Risikostyring er en integreret og fundamental del af ENVO IT A/S' ledelsessystem for informationssikkerhed (ISMS). Processen udføres systematisk for at identificere, analysere, vurdere og håndtere risici relateret til leverancen af vores Managed Services og beskyttelsen af den information, herunder kundeinformation og personoplysninger, som ENVO IT A/S behandler. Processen inkluderer en kortlægning af risici specifikt relateret til de enkelte typer af services, som ENVO IT A/S leverer til kunder, for at sikre relevans i risikobilledet og adressere trusler mod de specifikke databehandlingsaktiviteter, der udføres på vegne af kunder.

Der gennemføres en årlig, overordnet risiko- og trusselvurdering, som dækker interne systemer, processer og eksterne faktorer (f.eks. leverandørkæden), der kan påvirke serviceleverancen og informationssikkerheden. Derudover udføres specifikke risikovurderinger i forbindelse med væsentlige ændringer i IT-miljøet, implementering af nye services eller opstart af større projekter.

Risici vurderes baseret på en fastlagt metode, der kombinerer sandsynligheden for en hændelse med den potentielle konsekvens for fortrolighed, integritet og tilgængelighed (CIA) for både ENVO IT A/S og vores kunder. Vurderingen resulterer i et risikoniveau (f.eks. Høj, Mellem, Lav), som dokumenteres sammen med en beskrivelse af selve risikoen.

For identificerede risici vurderes og udvælges passende tekniske og organisatoriske foranstaltninger (TOMs) til risikobehandling. Denne vurdering sikrer, at foranstaltningerne ikke alene er effektive til at reducere risikoen til et acceptabelt niveau, men også at de lever op til relevante krav i gældende lovgivning (herunder kravene til behandlingssikkerhed i GDPR Artikel 32) samt kontraktuelle forpligtelser over for kunder. Valget, implementeringen og den løbende drift af TOMs dokumenteres for at understøtte eftervisning af compliance og kontrolmiljøets effektivitet.

Resultaterne af risikovurderingen, inklusive vurderingen af TOMs, samt forslag til risikohåndteringsplan (mitigering, accept, overførsel, undgåelse) forelægges ledelsen til gennemgang og godkendelse. Godkendelsen indebærer en dokumenteret afvejning af de identificerede risici i forhold til effekten og omkostningerne ved de foreslåede risikohåndterings tiltag.

Arbejdet med risikostyring og informationssikkerhed tager udgangspunkt i anerkendte standarder, herunder principperne i ISO 27001/27002:2022, for at sikre en struktureret og bedste praksis-tilgang.

Risikostyring er en løbende aktivitet, der involverer relevante interessenter i organisationen for at sikre, at risikobilledet og kontrolmiljøet forbliver relevant og effektivt i takt med ændringer internt og eksternt. Resultaterne af risikostyringen anvendes til løbende at prioritere og forbedre sikkerhedsforanstaltninger og interne kontroller inden for rammerne af vores ISMS.

3.4 Kontrolforanstaltninger

ENVO IT A/S har implementeret et omfattende sæt af kontrolforanstaltninger for at imødekomme de identificerede risici og opnå de fastsatte kontrolmål. Disse foranstaltninger er baseret på principperne i ISO 27001/27002:2022 og er integreret i virksomhedens ledelsessystem for informationssikkerhed (ISMS). Nedenfor beskrives de centrale kontrolforanstaltninger, grupperet efter de 11 kontrolmål anvendt i denne erklæring:

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

3.4.1 Kontrolmål 1: Ledelse

Ledelsen i ENVO IT A/S demonstrerer engagement i informationssikkerhed gennem etablering og vedligeholdelse af et ISMS. Der er defineret en overordnet "Politik for Informationssikkerhed og Dataetik", som er godkendt af bestyrelsen og minimum årligt gennemgås af direktionen. Denne politik fastlægger rammerne, sikkerhedsmålene (CIA), de ledende principper, og forpligtelsen til at overholde relevante krav samt til løbende forbedring. Politikken understøttes af en række emnespecifikke politikker (f.eks. for leverandørstyring, brugerenheder, acceptabel brug, malware-beskyttelse, netværkssikkerhed, distancearbejde m.fl.), som godkendes af direktionen. Ansvar for informationssikkerhed er placeret hos direktionen, med specifikke opgaver uddelegeret til relevante funktioner, herunder en udpeget IT Sikkerhedsansvarlig. Der er etableret en proces for håndtering af dispensationer og undtagelser, som kræver ledelsesgodkendelse og dokumenteret risikovurdering. Risikostyringsprocessen (beskrevet i afsnit 3.3) er en integreret del af ledelsessystemet. Processer for planlægning og forberedelse af håndtering af informationssikkerhedshændelser er etableret, inklusive definition af roller og ansvar (jf. Kontrolmål 10).

3.4.2 Kontrolmål 2: Styring af aktiver

ENVO IT A/S sikrer, at IT-aktiver, især brugerenheder (endpoints), håndteres og beskyttes forsvarligt gennem hele deres livscyklus. Alt arbejde for ENVO IT A/S skal udføres på udstyr udleveret og administreret centralt af virksomheden; brug af private enheder (BYOD) er ikke tilladt. Brugerenheder klagøres med en standardiseret, sikker konfiguration, der inkluderer operativsystemshærdning, automatisk distribution af system- og sikkerhedsopdateringer, fuld disk kryptering og installation af avanceret endpoint protection (EDR/XDR). Adgang til enheder sikres via krav om adgangskode, PIN eller biometri samt automatisk skærmlås. Brug af flytbare USB-lagermedier er teknisk blokeret. Der er sikret mulighed for backup af arbejdsrelaterede data via centralt administrerede løsninger (f.eks. synkronisering til OneDrive). Ved distancearbejde stilles der specifikke krav til sikker opbevaring og transport af udstyr. Processer for sikker returnering, datasletning og bortskaffelse af udstyr er etableret. Medarbejderne informeres om deres ansvar for korrekt og sikker brug af aktiver via "Vejledning i sikker brug af IT".

3.4.3 Kontrolmål 3: Beskyttelse af information

Beskyttelse af information opnås gennem en kombination af tekniske og organisatoriske foranstaltninger. Data lagret lokalt på brugerenheder er beskyttet af fuld disk kryptering. Der er implementeret omfattende beskyttelse mod malware på endpoints og i centrale systemer (e-mail, samarbejdsplatforme) via en integreret XDR-plattform (jf. Kontrolmål 6). Regler for acceptabel brug af information er defineret i "Vejledning i sikker brug af IT", som medarbejderne gøres bekendt med. Der stilles krav om fortrolighed i ansættelseskontrakter og eventuelle separate fortrolighedsaftaler. Ved distancearbejde sikres informationsbeskyttelse gennem krav om brug af firmaudstyr, sikre forbindelser (VPN), MFA og vejledning om fysisk sikring af arbejdspladsen og forebyggelse af visuel hacking (f.eks. brug af privacy screens). Der findes processer for sikker håndtering af data gennem livscyklussen, herunder sikker bortskaffelse.

3.4.4 Kontrolmål 4: Medarbejdersikkerhed

ENVO IT A/S har implementeret kontroller for at reducere risici relateret til medarbejdere. Før ansættelse gennemføres en screeningproces, der omfatter verifikation af referencer, identitet, uddannelse, indhentning af straffeattest og test af teknisk viden, hvor det er relevant og tilladt. Ansættelsesvilkår indeholder klausuler om tavshedspligt, fortrolighed og ansvar for informationssikkerhed. Alle medarbejdere gennemgår obligatorisk onboarding og løbende awareness-træning om informationssikkerhed, GDPR og relevante politikker, herunder "Vejledning i sikker brug af IT". Der udføres periodiske phishing-simuleringer. En formaliseret disciplinær proces er etableret for at håndtere overtrædelser af

sikkerhedspolitikker. Ved fratrædelse sikrer processer returnering af aktiver, tilbagekaldelse af adgange og påmindelse om fortsat tavshedspligt.

3.4.5 **Kontrolmål 5: Fysisk sikring**

ENVO IT A/S' kontorfaciliteter er sikret mod uautoriseret fysisk adgang. Adgang til kontoret kræver brug af personlig nøglebrik og pinkode eller en fysisk nøgle. Besøgende skal registreres og ledsages i overensstemmelse med gældende procedure. Særligt følsomt udstyr er placeret i sikrede områder med passende adgangskontrol. Medarbejdere er instrueret i at følge en "clean desk policy" for at beskytte information mod uautoriseret indsigt og er pålagt at låse deres skærm ved fravær. Der er også fastlagt retningslinjer for fysisk sikring af udstyr under distancearbejde, herunder sikker opbevaring og transport.

3.4.6 **Kontrolmål 6: System og netværkssikkerhed**

Netværksinfrastrukturen hos ENVO IT A/S administreres med fokus på sikkerhed. Netværket er segmenteret i sikkerhedszoner (f.eks. Sikker, Usikker, Administration) med adgangskontrol via firewalls efter "least privilege"-princippet. Administration af netværksudstyr er begrænset til autoriseret personale med sikker autentifikation (MFA hvor muligt) fra godkendte netværk. Relevant trafik inspiceres via NGFW (Next-Generation Firewalls) med passende sikkerhedsprofiler (inkl. IPS, DNS/web-filtrering, applikationskontrol). Sikker fjernadgang etableres via VPN med MFA, og trådløs adgang til sikre segmenter kræver 802.1x-autentificering. Malware-beskyttelse dækker netværksniveauet via NGFW og XDR-plattformen. Netværkstrafik, sikkerhedshændelser og konfigurationsændringer logges centralt. Sårbarheder i netværksudstyr håndteres via en defineret patch management proces med tidslinjer for kritiske opdateringer.

3.4.7 **Kontrolmål 7: Sikker konfiguration**

ENVO IT A/S sikrer, at IT-systemer og -komponenter konfigureres sikkert fra starten og vedligeholdes i en sikker tilstand. Brugerenheder klargøres ud fra en standardiseret, sikkerhedsoptimeret baseline (OS-hærdning, kryptering, sikkerhedssoftware, adgangskontrol, deaktivering af unødvendige tjenester/porte, blokering af USB-lagring). Tilsvarende etableres og vedligeholdes sikre konfigurationsbaselines for serveroperativsystemer og netværksudstyr (firewalls, routere, switche). Standardadgangskoder ændres altid ved implementering. System- og sikkerhedsopdateringer distribueres og installeres automatisk eller via en kontrolleret patch management proces på tværs af infrastruktur og brugerenheder for at adressere kendte sårbarheder. For cloudtjenester sikres det, at de konfigureres sikkert inden for ENVO IT's ansvarsområde (IAM, netværksregler, logning etc.).

3.4.8 **Kontrolmål 8: Identitetsstyring og adgangsstyring**

Adgang til ENVO IT A/S' systemer og information styres baseret på principperne om "least privilege" og "need-to-know". Brugeridentiteter oprettes, ændres og deaktiveres gennem en formaliseret proces (User Access Management), der sikrer korrekt autorisation og rettidig fjernelse af adgang ved ændringer i ansættelsesforhold. Adgang til systemer kræver som minimum unik brugeridentifikation og stærk adgangskode, og for al fjernadgang samt adgang til kritiske systemer håndhæves multifaktorautentifikation (MFA). Adgang til brugerenheder sikres via adgangskode, PIN eller biometri. Tildeling af specifikke rettigheder baseres på brugerens rolle og arbejdsopgaver og kræver godkendelse. Der gennemføres periodiske gennemgange af tildelte adgangsrettigheder for at sikre fortsat relevans. Adgang for leverandørpersonale styres særskilt og restriktivt.

3.4.9 **Kontrolmål 9: Sikring af leverandørforhold**

ENVO IT A/S har implementeret et omfattende system for leverandørstyring baseret på en dedikeret politik, der dækker hele livscyklussen. Processen starter med identifikation og risikoklassificering af leverandører og ydelser. Før kontraktindgåelse gennemføres en risikobaseret due diligence, der vurderer leverandørens sikkerhedsmodenhed og produkters/ tjenesters sikkerhed, herunder IKT-forsyningskædeaspekter som softwarekomponenter (SBOM) og integritetsvalidering for kritiske leverancer. Relevante informationssikkerhedskrav (ift. databehandling, adgang, incident response, audit, BCM, ændringer, underleverandører, sikker afslutning etc.) indarbejdes i leverandøraftaler. Leverandørers performance og compliance overvåges løbende gennem reviews, rapporter og audits. Adgangsstyring for leverandører håndteres restriktivt. Der er processer for håndtering af leverandør-relaterede incidents og for sikker

afslutning af leverandørforholdet. Cloudtjenester håndteres specifikt under denne ramme med fokus på bl.a. vurdering af standardaftaler, ansvarsfordeling (shared responsibility) og exit-strategier.

3.4.10 Kontrolmål 10: Styring af informationssikkerhedshændelser

ENVO IT A/S har etableret en formaliseret Incident Response Plan (IRP) og proces for at sikre en hurtig, effektiv og koordineret håndtering af informationssikkerhedshændelser og -incidents. Processen omfatter:

- ▶ **Forberedelse:** Definition af roller (Incidentkoordinator, beredskabsteam), ansvar og kommunikationsveje. Sikring af nødvendige kompetencer.
- ▶ **Detektion og Analyse:** Overvågning af systemer (logning, EDR/XDR, SIEM) for at opdage hændelser. Analyse for at fastslå omfang, årsag og impact. Klassificering af incidents baseret på alvorlighed.
- ▶ **Inddæmning, Udryddelse og Genopretning:** Iværksættelse af tiltag for at begrænse skaden (f.eks. isolering af systemer), fjerne årsagen til incidenten og genoprette normal drift sikkert. Eskalering til kriseledelse eller BCP aktiveres ved behov. Korrekt bevissikring prioriteres.
- ▶ **Post-Incident Aktiviteter:** Gennemførelse af rodårsagsanalyse (RCA) og "lessons learned" for at identificere forbedringsmuligheder til processer, kontroller og awareness. Udarbejdelse af incidentrapport til ledelsen. Systematisk opsamling af incident-data for trendanalyse.
- ▶ **Rapportering:** Klare kanaler for medarbejdere til at rapportere mistænkte hændelser. Procedurer for lovpligtig rapportering (f.eks. GDPR-brud) og kommunikation til relevante interne/eksterne parter (inkl. kunder hvis relevant).

3.4.11 Kontrolmål 11: Sikring af informationssikkerhed

ENVO IT A/S sikrer løbende overensstemmelse med og effektivitet af informationssikkerhedsforanstaltningerne gennem en række assurance-aktiviteter. Dette inkluderer den løbende overvågning af systemer og netværk (loganalyse, SIEM, EDR-alarmer), som beskrevet under relevante kontrolmål. ISMS'ets effektivitet og overholdelse af politikker vurderes løbende gennem de beskrevne overvågningsaktiviteter, ledelsens årlige gennemgang og resultaterne af eksterne erklæringer som denne. Resultaterne af risikovurderinger (jf. Kontrolmål 1) og incident-analyser (jf. Kontrolmål 10) bruges aktivt til at identificere svagheder og drive forbedringer. Der følges op på leverandørers compliance (jf. Kontrolmål 9) gennem overvågningsaktiviteter. En proces for sårbarhedsstyring, herunder scanning og prioritering af patching (jf. Kontrolmål 6 og 7), er etableret for at adressere tekniske svagheder proaktivt. Overholdelse af politikken for acceptabel brug overvåges, og afvigelser håndteres (jf. Kontrolmål 2). Ledelsen gennemgår regelmæssigt ISMS'ets performance og effektivitet.

3.5 Komplementerende kontroller hos kunder

For at opnå de i denne erklæring beskrevne kontrolmål fuldt ud, er det afgørende, at brugerorganisationen (kunden) selv implementerer og vedligeholder visse komplementære kontroller. Brugerorganisationens ledelse og revisorer bør vurdere tilstrækkeligheden af disse komplementerende kontroller i relation til deres egen risikoprofil og regnskabsaflæggelse.

- ▶ **Forretningskontinuitet og Disaster Recovery:** At udvikle, vedligeholde og teste egne overordnede BCP/DRP-planer, der tager højde for de gendannelsesmål (RTO/RPO), som ENVO IT A/S' ydelser understøtter via aftalte backup-services.
- ▶ **Administration af Brugeradgange:** At definere og kommunikere klare instruktioner til ENVO IT A/S for, samt godkende anmodninger om, oprettelse, ændring og deaktivering af brugeradgange til systemer administreret af ENVO IT A/S.
- ▶ **Validering af Brugerrettigheder:** At sikre, at tildelte rettigheder er passende i forhold til medarbejderroller og princippet om mindst nødvendige rettigheder ("need-to-know"), samt periodisk (f.eks. halvårligt eller årligt) at gennemgå og validere alle tildelte brugeradgange og rettigheder for fortsat korrekthed og relevans.
- ▶ **Funktionsadskillelse (Segregation of Duties):** At sikre tilstrækkelig funktionsadskillelse i egne processer og i de brugerrettigheder, der anmodes om tildeling af via ENVO IT A/S.

- ▶ **Sikkerhed i Egne Miljøer:** At etablere og vedligeholde passende tekniske og organisatoriske sikkerhedsforanstaltninger (herunder patching, malware-beskyttelse, adgangskontrol) på brugerorganisationens egne lokale netværk, systemer og brugerenheder, der interagerer med ENVO IT A/S' services, men som ikke administreres direkte af ENVO IT A/S.
- ▶ **Test af Ændringer (User Acceptance Testing):** At udføre relevante tests for at vurdere og acceptere, hvordan væsentlige ændringer i ENVO IT A/S' leverede services potentielt påvirker brugerorganisationens egne integrerede systemer, data eller forretningsprocesser.
- ▶ **Rapportering af Sikkerhedshændelser:** At underrette ENVO IT A/S uden unødigt forsinkelse ved opdagelse af eller mistanke om sikkerhedshændelser i brugerorganisationens eget miljø, der kan have relevans for eller påvirke de services, ENVO IT A/S leverer.
- ▶ **Overholdelse af Lovgivning:** At sikre, at brugerorganisationens anvendelse af ENVO IT A/S' services, samt de data der behandles heri (især personoplysninger hvor kunden er dataansvarlig), overholder al for brugerorganisationen relevant lovgivning og regulering.



4 Tests udført af EY

4.1 Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontrol hos en serviceleverandør.

Vores test af kontrollers design og implementering har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af afsnit 3. Eventuelle andre kontrolmål, tilknyttede kontroller og komplementære kontroller hos kunder, der anvender løsningen, beskrevet i afsnit 3, er ikke omfattet af vores test.

Test af design og implementering har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået pr. 07/05-2025.

Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og implementering er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er designet pr. 07/05-2025.
Forespørgsler	Forespørgsel af passende personale hos ENVO IT. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

4.2 Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål 1: Ledelse			
Procedurer og kontroller sikrer, at ledelsens retning og support til informationssikkerhed bliver leveret i overensstemmelse med forretningskrav, relevante love og regler, herunder en ledelsesramme til at igangsætte og kontrollere implementeringen og driften af informationssikkerhed i organisationen.			
<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
5.01	<p>Politikker for informationssikkerhed Informationssikkerhedspolitik er defineret, godkendt af ledelsen, meddelt og anerkendt af relevant personale og gennemgås med planlagte intervaller, og hvis der sker væsentlige ændringer.</p> <p>Emnespecifikke politikker er defineret, meddelt og anerkendt af relevant personale og gennemgås med planlagte intervaller, og hvis der sker væsentlige ændringer.</p>	<p>Inspiceret at informationssikkerhedspolitikken er gennemgået og godkendt af ledelsen årligt, samt er tilgængelig for alle medarbejdere.</p> <p>Inspiceret at emnespecifikke politikker er gennemgået og opdateret årligt, samt er tilgængelig for relevante medarbejdere.</p>	Ingen afvigelser konstateret.
5.02	<p>Roller og ansvarsområder for informationssikkerhed Informationssikkerhedsroller og ansvar er defineret og fordelt.</p>	<p>Inspiceret informationssikkerhedspolitikken indeholder beskrivelse af ansvarsfordeling.</p> <p>Inspiceret organisationsdiagrammer for kontoret i København og Silkeborg, hvor roller er fordelt.</p>	Ingen afvigelser konstateret.
5.24	<p>Forretningsgange for informationssikkerhedshændelser Organisationen har planlagt og forberedt sig på håndtering af informationssikkerhedshændelser ved at definere, etablere og kommunikere processer, roller og ansvarsområder for håndtering af informationssikkerhedshændelser.</p>	<p>Inspiceret procedure for håndtering af informationssikkerhedshændelser er gennemgået og godkendt af ledelsen årligt, samt tilgængelig for alle medarbejdere.</p>	Ingen afvigelser konstateret.

Kontrolmål 2: Styring af aktiver			
Procedurer og kontroller sikrer, at fysiske aktiver og oplysninger beskyttes både uden for og på ENVO IT's lokationer, samt mens oplysninger er under transport.			
<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
5.10	Accepteret brug af information og aktiver Regler for acceptabel brug og procedurer for håndtering af oplysninger og andre tilknyttede aktiver identificeres, dokumenteres og gennemføres.	Inspiceret politik for accepteret brug af information og understøttende aktiver, hvori ansvar for opdatering og vedligeholdelse af proceduren er defineret. Inspiceret procedure for håndtering af information og aktiver, samt at denne er tilgængelig for alle medarbejdere.	Ingen afvigelser konstateret.
6.05	Ansvar og forpligtelser efter ophør af ansættelse Informationssikkerhedsansvar og -opgaver, der forbliver gyldige efter ophør eller ansættelsesskift, er defineret, håndhæves og meddeles relevant personale.	Inspiceret flow for fratrædelse i HR-systemet. Inspiceret dokumentation for seneste fratrådte medarbejder har fulgt flowet og er informeret om den fortsatte tavshedspligt.	Ingen afvigelser konstateret.
6.07	Distancearbejde Sikkerhedsforanstaltninger er implementeret, når personalet arbejder udenfor kontoret for at beskytte oplysninger, der tilgås, behandles eller opbevares uden for organisationens lokaler.	Inspiceret procedure for distancearbejde. Inspiceret at distancearbejde kræver VPN forbindelse med multifaktor login. Inspiceret at et begrænset antal medarbejdere har adgang til VPN.	Ingen afvigelser konstateret.
8.01	User endpoint devices Oplysninger der lagres på, behandles af eller er tilgængelige via endpoint devices er beskyttet.	Inspiceret opsætning af beskyttelse på Windows og Mac PC'er. Inspiceret at Windows og Mac PC'er er beskyttet med kryptering.	Ingen afvigelser konstateret.

Kontrolmål 3: Beskyttelse af information

Procedurer og kontroller sikrer, at oplysninger klassificeres og beskyttes i overensstemmelse med deres klassifikation og slettes, når oplysningerne ikke længere er nødvendige.

Nr.	Serviceleverandørens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
5.10	Accepteret brug af information og aktiver Regler for acceptabel brug og procedurer for håndtering af oplysninger og andre tilknyttede aktiver identificeres, dokumenteres og gennemføres.	Inspiceret politik for accepteret brug af information og understøttende aktiver, hvori ansvar for opdatering og vedligeholdelse af proceduren er defineret. Inspiceret procedure for håndtering af information og aktiver, samt at denne er tilgængelig for alle medarbejdere.	Ingen afvigelser konstateret.
6.06	Fortrolighedsaftaler Fortroligheds- eller hemmeligholdelsesaftaler, der afspejler organisationens behov for beskyttelse af oplysninger, er identificeret, dokumenteret, regelmæssigt gennemgået og underskrevet af personale.	Inspiceret kontraktskabelon der indeholder afsnit om tavshedspligt. Inspiceret senest ansatte medarbejder har underskrevet kontrakt og tavshedspligt.	Ingen afvigelser konstateret.
6.07	Distancearbejde Sikkerhedsforanstaltninger er implementeret, når personale arbejder udenfor kontoret for at beskytte oplysninger, der tilgås, behandles eller opbevares uden for organisationens lokaler.	Inspiceret procedure for distancearbejde. Inspiceret at distancearbejde kræver VPN forbindelse med multifaktor login. Inspiceret at et begrænset antal medarbejdere har adgang til VPN.	Ingen afvigelser konstateret.

Kontrolmål 3: Beskyttelse af information

Procedurer og kontroller sikrer, at oplysninger klassificeres og beskyttes i overensstemmelse med deres klassifikation og slettes, når oplysningerne ikke længere er nødvendige.

<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
8.01	User endpoint devices Oplysninger der lagres på, behandles af eller er tilgængelige via endpoint devices er beskyttet.	Inspiceret opsætning af beskyttelse på Windows og Mac PC'er. Inspiceret at Windows og Mac PC'er er beskyttet med kryptering.	Ingen afvigelser konstateret.
8.07	Beskyttelse mod malware Beskyttelse mod malware er implementeret og understøttes af passende brugerbevidsthed.	Inspiceret procedure for beskyttelse mod malware. Inspiceret opsætning af beskyttelse mod malware for Windows og Mac PC'er. Inspiceret at alle Windows og Mac PC'er er beskyttet.	Ingen afvigelser konstateret.

Kontrolmål 4: Medarbejdersikkerhed			
Procedurer og kontroller sikrer, at medarbejdersikkerhed implementeres og fungerer effektivt før, under og efter ansættelsen.			
<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
6.01	Screening Baggrundskontrol af alle kandidater før ansættelse, er udført inden de tiltræder organisationen under hensyntagen til gældende love, regler og etik, og er proportional med forretningskravene, klassificeringen af de oplysninger, der skal tilgås, og de opfattede risici.	Inspiceret procedure for screening af medarbejdere. Inspiceret dokumentation for screening af seneste ansatte medarbejder.	Ingen afvigelser konstateret.
6.02	Ansættelsesvilkår og – betingelser Ansættelseskontrakterne angiver personalets og organisationens ansvar for informationsikkerhed.	Inspiceret skabelon for ansættelseskontrakt der indeholder krav til informationsikkerhed. Inspiceret seneste ansættelseskontrakt.	Ingen afvigelser konstateret.
6.03	Awareness, uddannelse og træning vedrørende informationsikkerhed Organisationens personale og relevante interesserede parter har modtaget passende viden omkring informationsikkerhed, uddannelse og træning, samt regelmæssige opdateringer af organisationens informationsikkerhedspolitik, emnespecifikke politikker og procedurer, som er relevante for deres jobfunktion.	Inspiceret procedure for awareness, uddannelse og træning vedr. informationsikkerhed. Inspiceret årshjul for træning af medarbejdere vedr. informationsikkerhed. Observeret at der gennemføres awarenesstræning.	Ingen afvigelser konstateret.
6.04	Sanktioner En disciplinær proces er formaliseret og kommunikeret for at træffe foranstaltninger mod personale, der har overtrådt informationsikkerhedspolitikken.	Inspiceret procedure og matrix for sanktioner ved overtrædelse af informationsikkerhedspolitikken. Observeret at procedure for sanktioner er tilgængelig for alle medarbejdere.	ENVO IT har oplyst, at der ikke har været tilfælde af sanktioner. Ingen afvigelser konstateret.

Kontrolmål 4: Medarbejdersikkerhed
Procedurer og kontroller sikrer, at medarbejdersikkerhed implementeres og fungerer effektivt før, under og efter ansættelsen.

Nr.	Serviceleverandørens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
		Forespurgt om dokumentation for seneste håndtering af sanktioner for overtrædelse af informationssikkerhedspolitikken.	
6.05	Ansvar og forpligtelser efter ophør af ansættelse Informationssikkerhedsansvar og -opgaver, der forbliver gyldige efter ophør eller ansættelseskift, er defineret, håndhævet og meddelt relevant personale.	Inspiceret flow for fratrædelse i HR-systemet. Inspiceret dokumentation for seneste fratrædte medarbejder har fulgt flowet og er informeret om den fortsatte tavshedspligt.	Ingen afvigelser konstateret.
6.06	Fortrolighedsaftaler Fortroligheds- eller hemmeligholdelsesaftaler, der afspejler organisationens behov for beskyttelse af oplysninger, er identificeret, dokumenteret, regelmæssigt gennemgået og underskrevet af personalet.	Inspiceret kontraktskabelon der indeholder afsnit om tavshedspligt. Inspiceret senest ansatte medarbejder har underskrevet kontrakt og tavshedspligt.	Ingen afvigelser konstateret.

Kontrolmål 5: Fysisk sikring			
Procedurer og kontroller sikrer, at fysisk sikkerhed er implementeret og fungerer effektivt.			
<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
6.07	Distancearbejde Sikkerhedsforanstaltninger er implementeret, når personale arbejder udenfor kontoret for at beskytte oplysninger, der tilgås, behandles eller opbevares uden for organisationens lokaler.	Inspiceret procedure for distancearbejde. Inspiceret at distancearbejde kræver VPN forbindelse med multifaktor login. Inspiceret at et begrænset antal medarbejdere har adgang til VPN.	Ingen afvigelser konstateret.
7.02	Fysisk Adgangskontrol Sikre områder er beskyttet af passende adgangskontrol og adgangspunkter.	Inspiceret procedure for fysisk adgangskontrol. Inspiceret specifikke lokale regler for fysisk adgang for kontoret i København og Silkeborg. Observeret at clean desk policy overholdes i København, samt at nøglebrik med kode er nødvendig for adgang til sikre områder.	Ingen afvigelser konstateret.

Kontrolmål 6: System- og netværkssikkerhed Procedurer og kontroller sikrer, at system- og netværkssikkerhed er implementeret og fungerer effektivt.			
Nr.	Serviceleverandørens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
6.07	Distancearbejde Sikkerhedsforanstaltninger er implementeret, når personale arbejder udenfor kontoret for at beskytte oplysninger, der tilgås, behandles eller opbevares uden for organisationens lokaler.	Inspiceret procedure for distancearbejde. Inspiceret at distancearbejde kræver VPN forbindelse med multifaktor login. Inspiceret at et begrænset antal medarbejdere har adgang til VPN.	Ingen afvigelser konstateret.
8.07	Beskyttelse mod malware Beskyttelse mod malware er implementeret og understøttes af passende brugerbevidsthed.	Inspiceret procedure for beskyttelse mod malware. Inspiceret opsætning af beskyttelse mod malware for Windows og Mac PC'er. Inspiceret at alle Windows og Mac PC'er er beskyttet.	Ingen afvigelser konstateret.
8.20	Netværkssikkerhed Netværk og netværksenheder er sikret, administreres og kontrolleres for at beskytte oplysninger i systemer og applikationer.	Inspiceret procedure for netværkssikkerhed. Inspiceret konfiguration for opdateret firewall. Inspiceret at opsætning af liste over lande der er blokeret adgang til netværket.	Ingen afvigelser konstateret.
8.22	Adskillelse af netværk Grupper af informationstjenester, brugere og informationssystemer er adskilt i organisationens netværk.	Inspiceret procedure for adskillelse af netværk. Inspiceret dokumentation for netværksadskillelse.	Ingen afvigelser konstateret.

Kontrolmål 7: Sikker konfiguration			
Procedurer og kontroller sikrer, at konfiguration af hardware, software, tjenester og netværk er sikker.			
<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
7.02	Fysisk Adgangskontrol Sikre områder er beskyttet af passende adgangskontrol og adgangspunkter.	Inspiceret procedure for fysisk adgangskontrol. Inspiceret specifikke lokale regler for fysisk adgang for kontoret i København og Silkeborg. Observeret at clean desk policy overholdes i København, samt at nøglebrik med kode er nødvendig for adgang til sikre områder.	Ingen afvigelser konstateret.

Kontrolmål 8: Identitet og adgangsstyring
Procedurer og kontroller sikrer, at autentificering og registrering af brugere og tildeling af adgangsrettigheder kontrolleres og fungerer effektivt.

Nr.	Serviceleverandørens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
7.02	Fysisk Adgangskontrol Sikre områder er beskyttet af passende adgangskontrol og adgangspunkter.	Inspiceret procedure for fysisk adgangskontrol. Inspiceret specifikke lokale regler for fysisk adgang for kontoret i København og Silkeborg. Observeret at clean desk policy overholdes i København, samt at nøglebrik med kode er nødvendig for adgang til sikre områder.	Ingen afvigelser konstateret.

Kontrolmål 9: Sikkerhed i leverandørrelationer
Procedurer og kontroller sikrer, at organisationens aktiver, der er tilgængelige for leverandører, er beskyttet, og at leverandørerne opretholder et aftalt niveau af informationssikkerhed og servicelevering i overensstemmelse med leverandøraftaler.

Nr.	Serviceleverandørens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
5.19	Informationssikkerhed i leverandørforhold Processer og procedurer er defineret og implementeret for at styre de informationssikkerhedsrisici, der er forbundet med brugen af leverandørens produkter eller tjenester.	Inspiceret politik for informationssikkerhed i leverandøraftaler indeholder beskrivelse af sikkerhedskrav til leverandører, samt krav om årlig risikovurdering af den enkelte leverandør og den leverede service. Inspiceret procedure for overvågning af leverandører, som inkluderer årlig gennemgang af erklæringer fra kritiske leverandører.	ENVO IT har oplyst, at der endnu ikke er indgået leverandøraftaler på den nye kontrakt, da proceduren er nyimplementeret. Ingen afvigelser konstateret.
5.20	Håndtering af sikkerhed i leverandøraftaler Relevante informationssikkerhedskrav er fastlagt og aftalt med hver leverandør baseret på typen af leverandørforhold.	Inspiceret politik for informationssikkerhed i leverandøraftaler indeholder beskrivelse af sikkerhedskrav til leverandører. Inspiceret register over ENVO IT's leverandørforhold. Forespurgt om seneste underskrevne leverandørkontrakt.	ENVO IT har oplyst, at der endnu ikke er indgået leverandøraftaler på den nye kontrakt, da proceduren er nyimplementeret. Ingen afvigelser konstateret.
5.21	Håndtering af informationssikkerhed i IKT-forsyningskæden Der er defineret og gennemført processer og procedurer for at styre de informationssikkerhedsrisici, der er forbundet med forsyningskæden for IKT-produkter og -tjenester.	Inspiceret politik for informationssikkerhed i IKT forsyningskæde indeholder beskrivelse af sikkerhedskrav til styring af informationssikkerhedsrisici i IKT-forsyningskæden, samt krav om årlig risikovurdering af disse.	ENVO IT har oplyst, at der endnu ikke er indgået aftaler om IKT-produkter og -tjenester på den nye kontrakt, da proceduren er nyimplementeret. Ingen afvigelser konstateret.

Kontrolmål 9: Sikkerhed i leverandørrelationer

Procedurer og kontroller sikrer, at organisationens aktiver, der er tilgængelige for leverandører, er beskyttet, og at leverandørerne opretholder et aftalt niveau af informationssikkerhed og servicelevering i overensstemmelse med leverandøraftaler.

<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
5.22	Overvågning af leverandører Organisationen foretager regelmæssig overvågning, gennemgang, evaluering og styring af ændringer i leverandørernes informationssikkerhedspraksis og servicelevering.	Inspiceret procedure for overvågning af leverandører, som inkluderer årlig gennemgang af erklæringer fra kritiske leverandører. Inspiceret dokumentation for opfølgning og gennemgang af kritiske leverandører.	Ingen afvigelser konstateret.
5.23	Informationssikkerhed ved brug af cloud services Processer for anskaffelse, brugerstyring og udgang fra cloud-tjenester er etableret i overensstemmelse med organisationens krav til informationssikkerhed.	Inspiceret politik for krav til anskaffelse, anvendelse og udgang af cloud tjenester. Inspiceret dokumentation for opfølgning og gennemgang af kritisk cloud leverandør.	Ingen afvigelser konstateret.
6.06	Fortrolighedsaftaler Fortroligheds- eller hemmeligholdelsesaftaler, der afspejler organisationens behov for beskyttelse af oplysninger, er identificeret, dokumenteret, regelmæssigt gennemgået og underskrevet af personalet.	Inspiceret kontraktskabelon der indeholder afsnit om tavshedspligt. Inspiceret senest ansatte medarbejder har underskrevet kontrakt og tavshedspligt.	Ingen afvigelser konstateret.

Kontrolmål 10: Administration af informationssikkerhedshændelser
Procedurer og kontroller sikrer, at informationssikkerhedshændelser identificeres og håndteres, samt at der træffes korrigerende foranstaltninger for at reducere sandsynligheden for fremtidige hændelser.

Nr.	Serviceleverandørens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
5.24	Forretningsgange for informationssikkerhedshændelser Organisationen planlægger og forbereder sig på håndtering af informationssikkerhedshændelser ved at definere, etablere og kommunikere processer, roller og ansvarsområder for håndtering af informationssikkerhedshændelser.	Inspiceret procedure for håndtering af informationssikkerhedshændelser er gennemgået og godkendt af ledelsen årligt, samt tilgængelig for alle medarbejdere.	Ingen afvigelser konstateret.
5.26	Håndtering af informationssikkerhedsbrud Informationssikkerhedshændelser er håndteret i overensstemmelse med de dokumenterede procedurer.	Inspiceret procedure for håndtering af informationssikkerhedshændelser. Forespurgt om liste og seneste håndtering af informationssikkerhedshændelser.	ENVO IT har oplyst, at der ikke er sket informationssikkerhedshændelser. Ingen afvigelser konstateret.
5.27	Erfaring fra informationssikkerhedsbrud Viden fra informationssikkerhedshændelser bruges til at styrke og forbedre informationssikkerhedskontrollen.	Inspiceret procedure for erfaring fra informationssikkerhedshændelser. Forespurgt om dokumentation for erfaring fra seneste informationssikkerhedshændelse.	ENVO IT har oplyst, at der ikke er sket informationssikkerhedshændelser. Ingen afvigelser konstateret.
6.08	Rapportering af informationssikkerhedshændelser Organisationen sørger for en mekanisme, der gør det muligt for personalet at rapportere observerede eller formodede informationssikkerhedshændelser gennem passende kanaler og rettidigt.	Inspiceret procedure for rapportering af informationssikkerhedshændelser. Forespurgt om dokumentation for rapportering af seneste informationssikkerhedshændelse.	ENVO IT har oplyst, at der ikke er sket informationssikkerhedshændelser. Ingen afvigelser konstateret.

Kontrolmål 11: Sikring af informationssikkerhed
Procedurer og kontroller sikrer, at informationssikkerhed implementeres og drives i overensstemmelse med organisationens politikker og procedurer.

<i>Nr.</i>	<i>Serviceleverandørens kontrolaktivitet</i>	<i>Revisors udførte test</i>	<i>Resultat af revisors test</i>
5.22	Overvågning af leverandører Organisationen foretager regelmæssig overvågning, gennemgang, evaluering og styring af ændringer i leverandørernes informationssikkerhedspraksis og servicelevering.	Inspiceret procedure for overvågning af leverandører, som inkluderer årlig gennemgang af erklæringer fra kritiske leverandører. Inspiceret dokumentation for opfølgning og gennemgang af kritiske leverandører.	Ingen afvigelser konstateret.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

“Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument.”

Johan Frantz Dhin

Partner - Cybersecurity

På vegne af: ENVO IT A/S

Serienummer: 15e76098-b682-4883-b67e-4db66af9d793

IP: 77.33.xxx.xxx

2025-06-19 13:20:35 UTC



Nils Bonde Christiansen

EY Godkendt Revisionspartnerselskab CVR: 30700228

Statsaut. revisor

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1

IP: 147.161.xxx.xxx

2025-06-19 13:25:08 UTC



Jesper Due Sørensen

EY Godkendt Revisionspartnerselskab CVR: 30700228

Partner

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3

IP: 46.193.xxx.xxx

2025-06-19 15:56:21 UTC



Dette dokument er underskrevet digitalt via [Penneo.com](https://penneo.com). De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.