



TIMESYSTEM APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF TIDSREGISTRERINGSSYSTEMET MTIME OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING	2
2. TIMESYSTEM APS' UDTALELSE	4
3. TIMESYSTEM APS' BESKRIVELSE AF TIDSREGISTRERINGSSYSTEMET MTIME	6
TIMEmSYSTEM ApS.....	6
Tidsregistreringssystemet mTIME	6
Generelle it-kontroller	7
Applikationskontroller	10
Ændringer i perioden 1. januar til 31. december 2023	11
Komplementerende kontroller hos kunder	11
4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST	12
Governance	14
Personalesikkerhed.....	16
Aftaler med underleverandører	19
Change management.....	20
Sikkerhed	22
Applikationskontroller	26

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF TIDSREGISTRERINGSSYSTEMET MTIME OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

Til: Ledelsen i TIMEmSYSTEM ApS
TIMEmSYSTEM ApS' kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om den af TIMEmSYSTEM ApS (serviceleverandøren) for hele perioden fra 1. januar til 31. december 2023 udarbejdede beskrivelse i sektion 3 af tidsregistreringssystemet mTIME og de tilhørende kontroller, og om udformningen og den operationelle effektivitet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandørens ansvar

Serviceleverandøren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Serviceleverandøren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom serviceleverandøren er ansvarlig for at anføre kontrolmålene samt udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisors 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.

BDO Statsautoriseret revisionsaktieselskab 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.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om serviceleverandørens beskrivelse samt om udformningen og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed om kontroller hos en serviceorganisation. 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 den operationelle effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. 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 eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet 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 opnået. 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 sektion 2.

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

Serviceleverandørens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af virksomhedens kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af tidsregistreringssystemet mTIME, 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 alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller 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 serviceleverandørens udtalelse i sektion 2. Det er vores opfattelse:

- a. at beskrivelsen af tidsregistreringssystemet mTIME og de tilhørende kontroller, således som de var udformet og implementeret i hele perioden fra 1. januar til 31. december 2023, i alle væsentlige henseender er retvisende, og
- b. at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar til 31. december 2023, og
- 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. januar til 31. december 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt serviceleverandørens tidsregistreringssystem mTIME, 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 regnskabsaflæggelsen.

København, den 17. januar 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. TIME m SYSTEM APS' UDTALELSE

TIME m SYSTEM ApS udfører hosting i forbindelse med tidsregistreringssystemet mTIME for vores kunder.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt tidsregistreringssystemet mTIME, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, når de opnår en forståelse af kunders informationssystemer, som er relevante for regnskabsaflæggelsen.

TIME m SYSTEM ApS anvender serviceunderleverandør(e). Denne/disse serviceunderleverandør(e)s relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse.

Beskrivelsen omfatter ikke de af TIME m SYSTEM ApS' anvendte underleverandørers relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller vedrørende hosting.

TIME m SYSTEM APS bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af tidsregistreringssystemet mTIME og de tilhørende kontroller i hele perioden fra 1. januar til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for tidsregistreringssystemet mTIME, og hvordan de tilhørende kontroller var udformet og implementeret, herunder redegør for:
 - De typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant.
 - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder.
 - De tilhørende regnskabsregistreringer, underliggende information og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan informationen er overført til de rapporter, der er udarbejdet til kunder
 - Hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner.
 - Processen, der blev anvendt til at udarbejde rapporter til kunder.
 - Relevante kontrolmål og kontroller udformet til at nå disse mål.
 - Kontroller, som vi med henvisning til systemets udformning 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 for behandlingen og rapporteringen af kunders transaktioner
2. Indeholder relevante oplysninger om ændringer i serviceleverandørens tidsregistreringssystem mTIME foretaget i hele perioden fra 1. januar til 31. december 2023.
3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af tidsregistreringssystemet mTIME eller Skema- og Ressourceplanlægningssystemet TimeEdit og de tilhørende kontroller under hensyntagen til, at denne beskrivelse 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 tidsregistreringssystemet mTIME, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

TIME m SYSTEM ApS bekræfter, at de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet i hele perioden fra 1. januar til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.
2. De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.
3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar til 31. december 2023.

København, den 17. januar 2024

TIME m SYSTEM ApS

Khanh Bao Nguyen-Cong
Direktør og Partner

3. TIME SYSTEM APS' BESKRIVELSE AF TIDSREGISTRERINGSSYSTEMET MTIME

TIME SYSTEM APS

TIME SYSTEM ApS er et selskab i VISMA, som udvikler produkter, komponenter og tilbyder rådgivning til det offentlige og private marked samt uddannelsesinstitutioner landet over.

TIME SYSTEM udvikler mTIME, som er et tids- og aktivitetsregistreringssystem.

TIME SYSTEM har ca. 26 medarbejdere og er specialiserede inden for systemudvikling, support og informationsikkerhed. TIME SYSTEM er organiseret i en udviklingsafdeling, drift- og supportafdeling og en administrationsafdeling.

Visma timemsystem har kontor i Carlsbergbyen.

TIDSREGISTRERINGSSYSTEMET MTIME

mTIME er vores tidsregistreringssystem.

mTIME skaber overblik, og er et system, som kan angive de korrekte andele i forhold til en medarbejders arbejdstid. Det er en fleksibel måde at oprette og vedligeholde alle typer overenskomster, fraværshåndtering og ændringer i overenskomstregler. Der er samtidig mulighed for at trække data ud til ledelsesinformation uden ekstraudgifter.

mTIME er et system, som ikke kræver vedligeholdelse af kunden, og man behøver ikke teknisk indsigt eller lignende. Vores support er på dansk, men mTIME er sproguafhængigt og findes både på dansk og engelsk.

Funktionalitet

- Webbaseret (online) system, som er understøttet med en mTIME app
- Håndtering af alt omkring ferie (tildeling, afregning, regulering, hensættelser og rapportering)
- Alle former for fraværssaldi (omsorgsdage, særlige feriedage, afspadsring)
- Ledelsesinformation og rapporter
- Overblik (ansættelsesforhold, ressourcer, brugte timer, fraværstatistikker, projekttimer mm)
- Beregning af overarbejde, tillægssydler, afspadsring og frihedsoptjening
- Fraværshåndtering - Komme/gå-tid registrering
- Aktivitetsregistrering (opsat efter jeres behov)
- Fleksibel advisering (opbygge regler for forskellige mailadviseringer)

Integrationsmuligheder

- Åben API
- Lønssystemer (eks. SLS, Bluegarden, Lessor mfl.)
- Økonomisystemer (eks. NS, NAV, Schilling, Maconomy mfl.)
- HR systemer (eks. Oracle HR, Dossier mfl.)
- Datavarehus og BI
- Mfl.

De anførte kontroller og handlinger er indeholdt i et årshjul, der angiver, hvornår aktiviteterne skal gennemføres.

Resultaterne af de gennemførte kontroller bliver derefter indført i en logbog og andre sikkerhedshændelser indføres ligeledes i logbogen. Dette udgør virksomhedens dokumentation for, at TIME SYSTEM lever op til forordningens krav.

Styringen af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter:

Hovedområde	Område
Governance	<ul style="list-style-type: none"> • Risikovurdering • Informationssikkerhed • Organisering af informationssikkerhed
Personalesikkerhed	<ul style="list-style-type: none"> • Rekruttering af medarbejdere • Fratrædelse af medarbejdere • Uddannelse og instruktion af medarbejdere • Awareness og oplysningskampagner for medarbejdere • Træning og uddannelse (it-sikkerhedskursus) • Tavsheds- og fortrolighedsaftaler
Aftaler med underleverandører og kunder	<ul style="list-style-type: none"> • Aftaler med underleverandører • Tilsyn med underleverandør • Fortrolighedsaftale med leverandører
Change management	<ul style="list-style-type: none"> • Ændringsstyring • Hjemtagelse af kundedatabaser i forbindelse med opgaveløsning og support
Sikkerhed	<ul style="list-style-type: none"> • Brugerstyring • Kryptering • Fysisk sikkerhed • Reparation og service af udstyr • Logning og monitorering • Beredskabsplan • Egenkontrol
Applikationskontroller	<ul style="list-style-type: none"> • Kontrol af projektrapport i mTIME • Kontrol af logning i mTIME • Kontrol af godkendelsesproces i mTIME

GENERELLE IT-KONTROLLER

GOVERNANCE

Risikoanalyse

Sikkerhedsgruppen i TIME m SYSTEM er ansvarlig for, at der foretages identifikation af sikkerhedsrisici, at der sker kategorisering af sikkerhedsrisici, samt at der er etableret de nødvendige sikkerhedsforanstaltninger.

Sikkerhedsgruppen i TIME m SYSTEM sørger for en årlig gennemgang af nuværende og fremtidige sikkerhedsrisici og sikkerhedsforanstaltninger.

TIME m SYSTEM har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed.

Politikker

TIME m SYSTEM har indført politikker, processer og procedurer, der sikrer, at TIME m SYSTEM kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger.

PERSONALESIKKERHED

TIME m SYSTEM har udarbejdet og implementeret en procedure for rekruttering af nye medarbejdere, herunder screening af medarbejder før ansættelse samt en procedure for fratrædelse af medarbejdere ved ophør af ansættelse.

TIME m SYSTEM sørger for at uddanne medarbejdere samt at give instruktion i processer og procedurer. Dette sker gennem et årligt sikkerhedskursus. I øvrigt er der løbende awareness aktiviteter på TIME m SYSTEM's intranet og månedlige nyhedsmails til medarbejderne.

Træning og uddannelse (it-sikkerhedskursus)

TIME m SYSTEM sørger for at uddanne medarbejdere i retningslinjerne i TIME m SYSTEM's it-sikkerhedsforanstaltninger samt at give instruktion i processer og procedurer. Dette sker gennem et årligt sikkerhedskursus.

Alle personer, der arbejder med TIME m SYSTEM, er underlagt tavshedspligt. Ved ansættelsen underskrives en fortroligheds- og tavshedserklæring, som opbevares i medarbejderens personalemappe digitalt og i fysisk arkiv.

Underleverandører

TIME m SYSTEM benytter Cloud Factory som underleverandør. TIME m SYSTEM har med Cloud Factory indgået en underleverandøraftale, hvor det er aftalt, at Cloud Factory skal fremsende en ISAE 3402 type 2-erklæring. Der udarbejdes et referat, der samler det årlige tilsyn med Cloud Factory, som er lokaliseret i Danmark, Vestergade 4, 6800 Varde. Der føres et årligt tilsyn med underleverandøren, som fremgår af vores årshjul.

Nedenfor følger en beskrivelse af Cloud Factory's primære serviceydelser. Nærværende erklæring omfatter ikke disse serviceydelser.

Serverdrift:

- Servere: Cloud Factory kontrollerer løbende TIME m SYSTEM ApS' servere og sikrer, at de altid er opdaterede og driftssikre.
- Backup: Cloud Factory kontrollerer daglige backup-rapporter, og sikrer, at backuppen virker som den skal.
- Antivirus- og spamfilter: Cloud Factory sørger for at antivirus- og spamfilter altid er opdaterede og fungerer, som de skal.
- Patch management: Cloud Factory laver løbende kontrol med, hvilke opdateringer, der er relevante, og sørger for, at de bliver installeret og konfigureret korrekt.
- Netværksprintere: Cloud Factory håndterer eventuelle netværksprintere, og sikrer, at de svarer på netværket.
- ERP og branche applikationer: Cloud Factory sikrer, at de bagvedliggende systemer samt infrastruktur til andre it-løsninger, der ikke er leveret af Cloud Factory, virker korrekt. Cloud Factory vil således assistere andre it-leverandører hos TIME m SYSTEM ApS med eventuelle problemer.

Netværksdrift:

- Lokalt netværk: Cloud Factory foretager løbende kontrol med det lokale netværk hos TIME m SYSTEM ApS, og sikrer, at routere, switche, accesspoints og lignende virker korrekt.
- Internetforbindelser: Cloud Factory varetager dialogen med Internetleverandører, og sikrer, at TIME m SYSTEM ApS har den optimale løsning.

- Firewall: Cloud Factory sikrer, at firewallen hos TIME m SYSTEM ApS er konfigureret og opdateret korrekt, så den forhindrer uønsket og skadelig trafik på det lokale netværk.
- VPN-forbindelser: Cloud Factory administrerer og vedligeholder VPN forbindelser.

Overvågning:

- Overvågning: Cloud Factory foretager automatisk kontrol med alle kritiske enheder på servere og netværk via eget overvågningssystem.
- Storskærm og e-mail: Eventuelle fejl og uregelmæssigheder rapporteres til Cloud Factory på e-mail samt på fysiske overvågnings-monitorer på Cloud Factory kontorer.
- Proaktiv fejludbedring: På baggrund af rapporter fra overvågningssystemet minimerer Cloud Factory driftsforstyrrelser hos TIME m SYSTEM ApS, idet potentielle problemer opdages, inden de opstår.
- Hurtig reaktion: Cloud Factory reagerer på alle hændelser, og kan ofte løse problemerne, inden TIME m SYSTEM ApS opdager dem.

CHANGE MANAGEMENT

Opdatering og vedligeholdelse

Pc'er, der kommer på TIME m SYSTEM's interne netværk - gælder også RDS klienter - har up-to-date operativsystem og applikationer.

Security updates bliver prioriteret frem for funktionelle patches. Dette håndterer CLOUD FACTORY for os.

Udvikling og vedligeholdelse applikationer

TIME m SYSTEM har et workflow, der indeholder en procesbeskrivelse i tilfælde af fejl, som er fundet i produktionsmiljøet, eller ved ændringsønsker, der kommer fra en kunde, og som kræver koderettelse. Den beskriver flowet mellem supportafdelingen, udviklingsafdelingen og testafdelingen.

SIKKERHED

Brugeradministration

TIME m SYSTEM vedligeholder en liste over medarbejdernes adgang og autorisation til at tilgå kundens systemer, og TIME m SYSTEM følger op på disse mindst en gang årligt for vurdering af, om der fortsat er behov for adgang, herunder opfylder kravene i indgået aftale om brugeradministration.

Password og adgangsstyring

TIME m SYSTEM har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Logning i systemer, databaser og netværk

TIME m SYSTEM har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Logdata er sikret mod tab og sletning.

Der foretages følgende logning i mTIME:

- Registrering: Hvem har registreret oplysningen og tidspunkt for registreringen.
- Medarbejdersgodkendelse: Hvem har foretaget egen godkendelse og tidspunkt for godkendelsen.
- Ledergodkendelse: Hvem har foretaget ledergodkendelse og tidspunkt for godkendelsen.
- Fraværsgodkendelse: Hvem har godkendt fraværet og tidspunkt for godkendelsen.

Fysisk sikkerhed

TIME m SYSTEM har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne, og særlige sikkerhedsmæssige foranstaltninger er indført for områder, hvor der foretages behandling af personoplysninger. Kunder, leverandører og andre besøgende ledsages.

Reparation og service samt bortskaffelse af it-udstyr

TIME m SYSTEM har indført procedurer, der sikrer, at udstyr, som udleveres til tredjemand for service, reparation eller bortskaffelse, udleveres uden datadiske, og at brugte og kasserede datamedier wibes inden destruktion.

It-beredskabsplan

Der er udarbejdet en it-beredskabsplan for TIME m SYSTEM, som bliver opdateret hvert år, som det fremgår af vores Årshjul.

Egenkontrol

TIME m SYSTEM har udarbejdet et årshjul, som benyttes til at udføre egenkontrol.

TIME m SYSTEM har indført procedurer, der sikrer, at der sker løbende overvågning af indførte tekniske sikkerhedsforanstaltninger. Der foretages løbende opfølgning af medarbejdernes brugeradgange til kunders miljøer.

APPLIKATIONSKONTROLLER

TIME m SYSTEM foretager en række kontroller af mTIME, som en del af regressionstesten af mTIME. Nedenstående kontroller sikrer, at der bliver rapporteret en valid timeregistrering på EU-projekter ved anvendelse af mTIME.

Projektrapport i mTIME (Projektrapporten viser timeregistreringer på de medarbejdere, som har registreret timer på et EU-projekt)

- TIME m SYSTEM tester, at statistikken tager højde for, at det kun er data, som er personaleledergodkendt, som bliver vist i projektrapporten.
- TIME m SYSTEM tester, at det er de korrekte timer, som bliver vist i projektrapporten.
- TIME m SYSTEM tester, at rapporten udvælger de korrekte data, når rapporten afgrænses til kun at vise specifikmedarbejder, som har indtastet timer på flere projekter.

Godkendelsesproces i mTIME

- TIME m SYSTEM tester, at en medarbejder ikke kan rette i registreringerne, når en opgørelse er blevet brugergodkendt.
- TIME m SYSTEM tester, at en almindelig medarbejder uden særlige rettigheder ikke kan personaleledergodkende sin egen opgørelse.
- TIME m SYSTEM tester, at det ikke er muligt at genåbne opgørelse som personaleleder, når systemindstillingen 'MaaPersonalledeGenaabne' er sat til nej.

Logning i mTIME

- TIME mSYSTEM tester, at det bliver logget, når en opgørelse bliver genåbnet.
- TIME mSYSTEM tester, at det er det korrekte, som bliver skrevet i "Vis log", når en opgørelse bliver brugergodkendt, og at det ikke er muligt at manipulere med loggen.
- TIME mSYSTEM tester, at det er det korrekte, som bliver skrevet i "Vis log", når en opgørelse bliver personaleledergodkendt, og at det ikke er muligt at manipulere med loggen.
- TIME mSYSTEM tester, at der bliver vist de korrekte brugerinitialer i "Vis log", når der bliver logget på som en anden, og bruger godkender opgørelse.

ÆNDRINGER I PERIODEN 1. JANUAR TIL 31. DECEMBER 2023

TIME mSYSTEM skiftede lokation fra Glostrup til Carlsbergbyen i slutningen af december 2022/starten af januar 2023.

TIME mSYSTEM skiftede den 1/5-2023 serviceleverandør fra IT-Relation til Cloud Factory. Endvidere har vi i perioden taget et nyt egenudviklet kundecenter i brug, hvor komponenten Mailjet anvendes.

KOMPLEMENTERENDE KONTROLLER HOS KUNDER

Kunden er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene:

- Kunden styrer brugerrettighederne (roller og rettigheder) i mTIME, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeler de enkelte brugere, når der bliver oprettet brugere.
- Kunden skal altid igennem en brugeracceptttest, før de accepterer at tage mTIME i brug i forbindelse med fejlrettelser og opdateringer.
- Kunden har ansvaret for, at logning for den enkelte medarbejder i mTIME gennemgås og slettes.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3402 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i TIMEmSYSTEM ApS' beskrivelse af tidsregistreringssystemet mTIME samt for udformningen og den operationelle effektivitet af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af TIMEmSYSTEM ApS, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden fra 1. januar til 31. december 2023.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion, observation og genudførelse.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos TIMEmSYSTEM ApS' passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, data-transmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som IT Relation leverer inden for hosting af TIMEmSYSTEMS kundecenter, har vi modtaget en ISAE 3402 type 2-erklæring om de generelle it-kontroller for perioden 1. januar til 31. december 2022.

For de ydelser, som Cloud Factory leverer inden for Hosting af mTIMEs kundecenter, har vi modtaget en ISAE 3402 type 2-erklæring om de generelle it-kontroller for perioden 1. januar til 31. december 2022.

Disse underleverandørers relevante kontrolmål og tilknyttede kontroller indgår ikke i TIMEmSYSTEM ApS' beskrivelse af tidsregistreringssystemet mTIME og de tilhørende kontroller. Vi har således alene inspiceret

den modtagne dokumentation og testet de kontroller hos TIMEmSYSTEM ApS, der sikrer overvågning af serviceunderleverandørens opfyldelse af den mellem underleverandøren og TIMEmSYSTEM ApS indgåede aftale.

Resultat af test

Resultatet af de udførte test af t kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet og implementeret eller ikke har fungeret effektivt i perioden.

Governance		
Kontrolmål ▶ At sikre, at serviceleverandøren har implementeret en løbende gennemgang og ajourføring af risikovurdering. ▶ At sikre, at serviceleverandøren har fastlagte it-politikker.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▶ TIMEsYSTEM har indført procedure for udførelse af risikovurderinger, herunder principper og metoder for risikovurdering, opdateringsfrekvens og versionsstyring. ▶ TIMEsYSTEM har gennemført passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de identificerede risici.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af TIMEsYSTEM's procedure for risikovurdering og udarbejdet risikovurdering. Vi har observeret, at TIMEsYSTEM har gennemført passende tekniske og organisatoriske foranstaltninger, baseret på risikovurderingen. Vi har observeret, at risikovurderingen vedligeholdes og opdateres løbende og mindst en gang årligt.	Ingen afvigelser konstateret.
Informationssikkerhed ▶ TIMEsYSTEM har udarbejdet og implementeret en IT-sikkerhedspolitik, som bliver opdateret minimum en gang årligt	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af TIMEsYSTEM's IT-sikkerhedspolitik og observeret, at denne er implementeret hos TIMEsYSTEM. Vi har observeret, at IT-sikkerhedspolitikken kommunikeres til medarbejdere i forbindelse med ansættelsen og ved løbende awareness-kampanjer. Vi har på forespørgsel blevet oplyst, at IT-sikkerhedspolitikken fra 2022 har været gældende i hele 2023 og vil blive opdateret igen i 2024.	Ingen afvigelser konstateret.

Governance		
Kontrolmål ▶ <i>At sikre, at serviceleverandøren har implementeret en løbende gennemgang og ajourføring af risikovurdering.</i> ▶ <i>At sikre, at serviceleverandøren har fastlagte it-politikker.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Organisering af informationssikkerhed ▶ TIMEsYSTEM har dokumenteret og etableret ledelsesstyring af informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af TIMEsYSTEM's IT-sikkerhedspolitik. Vi har observeret, at TIMEsYSTEM har etableret ledelsesstyring af informationssikkerhed gennem politikker, der ajourføres af IT-sikkerhedsgruppen.	Ingen afvigelser konstateret.

Personalesikkerhed		
Kontrolmål <ul style="list-style-type: none"> ▶ <i>At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.</i> ▶ <i>At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informations sikkerhedsansvar.</i> ▶ <i>At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.</i> ▶ <i>At sikre, at relevante medarbejdere har forpligtet sig til fortrolighed eller er underlagt en passende tavshedspligt.</i> 		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Rekruttering af medarbejdere <ul style="list-style-type: none"> ▶ TIMEsYSTEM har udarbejdet og implementeret en procedure for rekruttering af nye medarbejdere, herunder screening af medarbejdere før ansættelse. 	<p>Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM.</p> <p>Vi har foretaget inspektion af TIMEsYSTEM's procedure for rekruttering af nye medarbejdere. Vi har observeret, at denne indeholder procedure for rekruttering og ansættelse af medarbejdere, herunder screening af potentielle medarbejdere.</p> <p>Vi har ved en stikprøve af nyansatte inspiceret dokumentation for, at serviceleverandøren har foretaget screening af medarbejdere før ansættelse.</p>	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere <ul style="list-style-type: none"> ▶ TIMEsYSTEM har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende. 	<p>Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM.</p> <p>Vi har foretaget inspektion af TIMEsYSTEM's procedure for fratrædelse af medarbejdere.</p> <p>Vi har ved en stikprøve af fratrådte medarbejdere inspiceret dokumentation for, at systemadgange er slettet i henhold til proceduren.</p> <p>Vi har ved en stikprøve af fratrådte medarbejdere observeret, at medarbejderen ved fratrædelse er blevet orienteret om, at den underskrevne fortrolighedsaftale fortsat er gældende efter fratrædelse.</p>	Ingen afvigelser konstateret.

Personalesikkerhed		
Kontrolmål ▶ At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt. ▶ At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar. ▶ At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør. ▶ At sikre, at relevante medarbejdere har forpligtet sig til fortrolighed eller er underlagt en passende tavshedspligt.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Uddannelse og instruktion af medarbejdere ▶ Der afholdes introduktionskursus for nye medarbejdere. ▶ TIMEsYSTEM foretager løbende uddannelse af medarbejdere i henhold til informationssikkerhed samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har på forespørgsel fået oplyst, at der afholdes introduktionskursus for nye medarbejdere om systemer og adgang til disse. Vi har foretaget inspektion af TIMEsYSTEM's kursusmateriale. Vi har foretaget inspektion og observeret, at TIMEsYSTEM via sikkerhedskurset og teamopfølgingsmøder løbende uddanner medarbejdere i informationssikkerhed samt håndtering heraf.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere ▶ TIMEsYSTEM udfører løbende awareness-kampagner i form af, opslag og team-opfølgingsmøder. ▶ TIMEsYSTEM udfører oplysningskampagner for medarbejdere om informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har observeret, at TIMEsYSTEM løbende udfører awareness-kampagner i form af, opslag, team-opfølgingsmøder i henhold til informationssikkerhed samt håndtering heraf.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftaler ▶ TIMEsYSTEM har indgået tavsheds- og fortrolighedsaftale med medarbejdere.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af TIMEsYSTEM's procedure for håndtering af tavsheds- og fortrolighedsaftaler med medarbejdere.	Ingen afvigelser konstateret.

Personalesikkerhed		
Kontrolmål ▶ At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt. ▶ At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar. ▶ At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør. ▶ At sikre, at relevante medarbejdere har forpligtet sig til fortrolighed eller er underlagt en passende tavshedspligt.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har ved udtagelse af en stikprøve observeret, at de pågældende medarbejdere har underskrevet en tavsheds- og fortrolighedsaftale.	

Aftaler med underleverandører		
Kontrolmål ▶ At sikre, at der foreligger skriftlige aftaler, der sikrer, at der opretholdes et aftalt niveau af Informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne. ▶ At sikre, at relevante leverandører har forpligtet sig til fortrolighed eller er underlagt en passende tavshedspligt.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Aftaler med underleverandører ▶ TIMEsYSTEM har indgået aftaler med underleverandøren Cloud Factory.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af indgåede aftaler mellem TIMEsYSTEM og deres underleverandører og observeret, at de er i overensstemmelse med de ydelser, som underleverandører leverer. Yderligere har vi observeret, at underleverandøraftalerne er underskrevet af begge parter og opbevaret elektronisk.	Ingen afvigelser konstateret.
Tilsyn med underleverandør ▶ TIMEsYSTEM udfører og dokumenterer sit tilsyn med underleverandører, herunder at den sikkerhed, der i underleverandøraftalen er stillet krav om, lever op til de krav, som kunden har stillet i sin aftale med TIMEsYSTEM.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har observeret, at TIMEsYSTEM årligt fører tilsyn med samtlige underleverandører, ved indhentelse af en ISAE 3402 type 2-erklæring. Vi har foretaget inspektion af den af IT Relation og Cloud Factory udarbejdede ISAE 3402 type 2-erklæringer om generelle it-kontroller i relation til hosting services for perioden fra 1. januar til 31. december 2022.	Ingen afvigelser konstateret.
Fortrolighedsaftale med leverandører ▶ TIMEsYSTEM har indgået fortrolighedsaftale med eventuelle leverandører.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af TIMEsYSTEM's leverandører og observeret, at TIMEsYSTEM har sikret, at leverandører er underlagt tavshedspligt i overensstemmelse med indgået aftale.	Ingen afvigelser konstateret.

Change management		
Kontrolmål ▶ At sikre, at kun ændringer, der er risikovurderede, testede og godkendte, implementeres i mTime. ▶ At sikre, at sikkerhedshændelser og svagheder registreres, håndteres og rapporteres korrekt.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Ændringsstyring ▶ TIMEsYSTEM foretager en betryggende ændringsstyring, herunder at sikre identifikation, planlægning og test af ændringer, vurdering af konsekvenser, godkendelse, verifikation af konsekvenser for informationsikkerhed, kommunikation til kunden og procedurer for tilbagerulning ved mislykkede ændringer.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af TIMEsYSTEM's procedurer for "mTime-styring af fejlrapport", "Løsning af supportsg" og "Opdatering af mTime". Vi har ved en stikprøve inspiceret dokumentation for processen for håndtering af ændringsstyring, udvikling, tests og idriftsættelse, herunder godkendelse af releases. Vi har observeret, at der er implementeret den nødvendige funktionsadskillelse mellem udvikling, test og idriftsættelse for såvel platforme som for medarbejdere. Vi har observeret, at TIMEsYSTEM kan tilbagerulle en version, hvis denne er fejlbehæftet. Vi har observeret, at TIMEsYSTEM kan udføre nødændringer (hotfixes) for at imødegå brud på datasikkerheden.	Ingen afvigelser konstateret.
Hjemtagelse af kundedatabaser i forbindelse med opgaveløsning og support ▶ TIMEsYSTEM har passende procedurer og kontroller i forhold til at hjemtage kundedatabaser i forbindelse med test, fejlrrettelser og lignende.	Vi har udført forespørgsel hos passende personale hos TIMEsYSTEM. Vi har foretaget inspektion af TIMEsYSTEM's procedure for hjemtagning af databaser via styringsværktøjet Manage Optimize Processes og for manuel hjemtagning. Vi har observeret hjemtagning af database, herunder at data er anonymiseret før hjemtagningen sker.	Ingen afvigelser konstateret.

Change management		
Kontrolmål <ul style="list-style-type: none">▶ <i>At sikre, at kun ændringer, der er risikovurderede, testede og godkendte, implementeres i mTime.</i>▶ <i>At sikre, at sikkerhedshændelser og svagheder registreres, håndteres og rapporteres korrekt.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har observeret, at hjemtagne databaser slettes efter 30 dage ved en automatisk kørsel.	

Sikkerhed		
Kontrolmål ▶ <i>At sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.</i> ▶ <i>At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger.</i> ▶ <i>At sikre, at der er lavet en beredskabsplan for TIMEmSYSTEM.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Brugerstyring <ul style="list-style-type: none"> ▶ TIMEmSYSTEM opbevarer ind- og uddatamateriale, så uvedkommende ikke kan få adgang til at gøre sig bekendt med kundedata, der er indeholdt i mTIME-systemet. ▶ TIMEmSYSTEM har indført procedurer og kontroller, der sikrer, at kun medarbejdere, der er autoriseret hertil, har adgang. ▶ TIMEmSYSTEM vedligeholder en liste over medarbejdernes adgang og autorisation til at tilgå kundens systemer, og TIMEmSYSTEM følger op på disse mindst en gang årligt for vurdering af, om der fortsat er behov for adgang, herunder opfylder kravene i indgået aftale om brugeradministrationen. ▶ TIMEmSYSTEM tildeler medarbejdere med adgang til systemet et personligt login, som er personhenførbart, og som ikke må deles med andre, heller ikke ansatte i TIMEmSYSTEM. ▶ TIMEmSYSTEM har indført procedurer og kontroller, der sikrer, at medarbejdernes login overholder krav til længde, specialtegn, store bogstaver mv. og de øvrige krav til adgang og adgangskoder i den indgåede aftale. 	<p>Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM.</p> <p>Vi har observeret, at TIMEmSYSTEM opbevarer ind- og uddatamateriale, så uvedkommende ikke kan få adgang til de personoplysninger, der er indeholdt i mTIME.</p> <p>Vi har stikprøvevis observeret, at TIMEmSYSTEM ikke har adgang til ind- og uddatamateriale med undtagelse af support-afdelingens medarbejdere.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's checkliste over til- og fratrådte medarbejdere. Vi har foretaget inspektion af liste over tilsyn med brugeradgange i 2023, Password Policy og Policy for skærmlås fra Active Directory og konfiguration af brugere og brugerrettigheder i styringsværktøjet Manage Optimize Processes.</p> <p>Vi har observeret, at den i Active Directory konfigurerede Password Policy og Policy for skærmlås stemmer overens med TIMEmSYSTEM's password politik samt politik for skærmlås.</p> <p>Vi har observeret, at TIMEmSYSTEM's medarbejdere er oprettet med et personligt login, der er personhenførbart.</p> <p>Vi har observeret, at TIMEmSYSTEM har indført procedurer og kontroller til sikring af, at medarbejdernes login overholder de krav, som er specificeret i indgåede aftaler.</p>	<p>Ingen afvigelser konstateret.</p>

Sikkerhed		
Kontrolmål ▶ <i>At sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.</i> ▶ <i>At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger.</i> ▶ <i>At sikre, at der er lavet en beredskabsplan for TIMEmSYSTEM.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Kryptering ▶ TIMEmSYSTEM har opsat stærk kryptering ved transmittning af personoplysninger via eksterne kommunikationsforbindelser. ▶ TIMEmSYSTEM har indført procedurer og kontroller, der sikrer, at adgang ved brug af hjemmearbejdspladser sker i overensstemmelse med den indgåede aftale, at adgang opnås gennem en VPN-klient, der autentificeres via sikkerheden i TIMEmSYSTEM's Active Directory, og at adgang til data er sikret med login til server, der afvikler mTIME.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's password politik og observeret, at den stemmer overens med gældende procedurer. Vi har foretaget inspektion af TIMEmSYSTEM's krypteringscertifikat i forbindelse med eksterne kommunikationsforbindelser. Vi har observeret, at TIMEmSYSTEM anvender TLS-kryptering ved transmittning af personoplysninger via eksterne kommunikationsforbindelser, samt at adgang fra hjemmearbejdspladser sker via krypteret VPN-forbindelse. Vi har observeret, at TIMEmSYSTEM gør brug af to-faktor godkendelse. Vi har foretaget inspektion af udtræk af Password Policy og Policy for skærmlås fra Active Directory og observeret, at disse stemmer overens med TIMEmSYSTEM's password politik.	Vi har konstateret, at databehandleren fra 01.01.2023 til 30.04.2023 har anvendt forældet transportkryptering, men fra 01.05.2023 ved overgang til Cloud Factory som underdatabehandler er overgået til opdateret TLS kryptering. Ingen yderligere afvigelser konstateret.
Fysisk sikkerhed ▶ TIMEmSYSTEM har indført procedurer og kontroller for fysiske sikkerhedsforanstaltninger i forhold til adgang til TIMEmSYSTEM's bygning, lokaler, kontorer og øvrige faciliteter.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedurer for fysisk sikkerhed til TIMEmSYSTEM's bygning, lokaler, kontorer og øvrige faciliteter. Vi har observeret, at indgangen til TIMEmSYSTEM's lokaler altid er låst både i og udenfor arbejdstiden, og at gæster modtages af en receptionist ved indgangen til kontoret.	Ingen afvigelser konstateret.

Sikkerhed		
Kontrolmål ▶ At sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester. ▶ At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger. ▶ At sikre, at der er lavet en beredskabsplan for TIMEmSYSTEM.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Reparation og service af udstyr ▶ TIMEmSYSTEM har indført procedurer og kontroller, for reparation og service af udstyr samt ved salg og kassation af anvendt udstyr, herunder datamedier.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure og kontroller for afskaffelse af udstyr. Der har ikke været nogle sager, og vi har derfor ikke haft mulighed for at teste.	Ingen afvigelser konstateret.
Logning og monitorering ▶ TIMEmSYSTEM foretager logning og sikrer, at loggen som minimum indeholder oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører, eller det anvendte søgekriterium.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for logning i mTIME. Vi har observeret, at TIMEmSYSTEM foretager logning af personoplysninger, og at loggen indeholder oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, oplysningerne vedrører, eller anvendte søgekriterium. Vi har observeret, at der foretages følgende logning i mTIME: <ul style="list-style-type: none"> ● Registreringer ● Medarbejdersgodkendelse ● Ledergodkendelse ● Fraværsgodkendelse Vi har observeret, at logning i mTIME findes i databasen, og kan tilgås i brugerinterfacet.	Ingen afvigelser konstateret.

Sikkerhed		
Kontrolmål ▶ At sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester. ▶ At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger. ▶ At sikre, at der er lavet en beredskabsplan for TIMEmSYSTEM.		
Kontrolaktivitet	Test udført af BDO	Resultat af test
It-beredskabsplan ▶ Der er udarbejdet en it-beredskabsplan for TIMEmSYSTEM for de dele, der ikke er outsourcet.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har inspiceret en it-beredskabsplan. Vi har observeret, at serviceleverandøren har etableret en it-beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til data i tilfælde af en fysisk eller teknisk hændelse. Vi har inspiceret dokumentation for afprøvning af it-beredskabsplanen.	Ingen afvigelser konstateret.
Egenkontrol ▶ TIMEmSYSTEM foretager en dokumenteret gennemgang af de sikkerhedsmæssige foranstaltninger mindst en gang årligt.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's årshjul. Vi har observeret, at TIMEmSYSTEM løbende gennemgår og afprøver de sikkerhedsmæssige foranstaltninger samt tilsyn med underleverandører, anonymiseringskørsler, og at relevante sletninger er foretaget.	Ingen afvigelser konstateret.

Applikationskontroller		
Kontrolmål ► <i>At sikre, at mTIME understøtter, at der bliver angivet korrekte oplysninger til EU ved anvendelse af mTIME i forbindelse med kunders EU-projekter.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Kontrol af projektrapport i mTIME <ul style="list-style-type: none"> ► TIMEmSYSTEM er konfigureret således, at statistikken tager højde for, at det kun er data, som er personaleledergodkendt, som bliver vist i projektrapporten. ► TIMEmSYSTEM er konfigureret således, at det er de korrekte timer, som bliver vist i projektrapporten. ► TIMEmSYSTEM er konfigureret således, at rapporten udvælger de korrekte data, når rapporten afgrænses til kun at vise en specifik medarbejder, som har indtastet timer på flere projekter. 	<p>Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester statistikken for, at det kun er data, som er personaleledergodkendt, som bliver vist i projektrapporten.</p> <p>Vi har observeret, at det kun er data, som er godkendt af personaleleder, der bliver vist i projektrapporten.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf det fremgår, at TIMEmSYSTEM tester, at det er de korrekte timer, som bliver vist i projektrapporten.</p> <p>Vi har observeret, at det er de korrekte timer, som bliver vist i projektrapporten.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at rapporten udvælger de korrekte data, når rapporten afgrænses til kun at vise specifikmedarbejder, som har indtastet timer på flere projekter.</p> <p>Vi har observeret, at rapporten udvælger de korrekte data, når rapporten afgrænses til kun at vise specifikmedarbejder, som har indtastet timer på flere projekter.</p>	<p>Vi har konstateret, at medarbejderen siden version 5.13.0 kan generere sin egen rapport, selvom den ikke er blevet personaleledergodkendt. Vi har konstateret, at fejlen er rettet i version 5.13.8.2996.</p> <p>Ingen yderligere afvigelser konstateret.</p>

Applikationskontroller		
Kontrolmål ▶ <i>At sikre, at mTIME understøtter, at der bliver angivet korrekte oplysninger til EU ved anvendelse af mTIME i forbindelse med kunders EU-projekter.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
Kontrol af logning i mTIME <ul style="list-style-type: none"> ▶ TIMEmSYSTEM er konfigureret således, at det bliver logget, når en opgørelse bliver genåbnet. ▶ TIMEmSYSTEM er konfigureret således, at det er det korrekte, som bliver skrevet i "Vis log", når en opgørelse bliver brugergodkendt, og at det ikke er muligt at manipulere med loggen. ▶ TIMEmSYSTEM er konfigureret således, at det er det korrekte, som bliver skrevet i "Vis log", når en opgørelse bliver personaleledergodkendt, og at det ikke er muligt at manipulere med loggen. ▶ TIMEmSYSTEM er konfigureret således, at der bliver vist de korrekte brugerinitialer i "Vis log", når der bliver logget på som en anden, og bruger godkender opgørelse. 	<p>Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at det bliver logget, når en opgørelse bliver genåbnet.</p> <p>Vi har observeret, at det bliver logget, når en opgørelse bliver genåbnet.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at det er det korrekte, som bliver skrevet i "Vis log", når en opgørelse bliver brugergodkendt, og at det ikke er muligt at manipulere med loggen.</p> <p>Vi har observeret, at brugere godkender opgørelsen månedligt, hvorefter knappen til medarbejdergodkendelse fjernes, og ikke kan ændres i registrering længere.</p> <p>Vi har observeret, at godkendelsen logges med brugerens navn og brugerinitialer samt dato.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at det er det korrekte, som bliver skrevet i "Vis log", når en opgørelse bliver personaleledergodkendt, og at det ikke er muligt at manipulere med loggen.</p> <p>Vi har observeret, at brugere godkender opgørelsen månedligt, hvorefter det ikke er muligt at trykke på knappen.</p>	<p>Vi har konstateret, at siden den 22-11-2023 har det ikke været muligt at se oplysningerne i "Vis log" for version 5.13.12.2884.</p> <p>Ingen yderligere afvigelser konstateret.</p>

Applikationskontroller		
Kontrolmål ► <i>At sikre, at mTIME understøtter, at der bliver angivet korrekte oplysninger til EU ved anvendelse af mTIME i forbindelse med kunders EU-projekter.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	<p>Vi har observeret, at godkendelsen logges med p-lederens navn og brugerinitialer samt dato.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at der bliver vist de korrekte brugerinitialer i "Vis log", når der bliver logget på som en anden, og bruger godkender opgørelse.</p> <p>Vi har observeret, at der bliver vist de korrekte brugerinitialer i loggen.</p>	
Kontrol af godkendelsesproces i mTIME <ul style="list-style-type: none"> ► TIMEmSYSTEM er konfigureret således, at en medarbejder ikke kan rette i registreringerne, når en opgørelse er blevet brugergodkendt. ► TIMEmSYSTEM er konfigureret således, at en almindelig medarbejder uden særlige rettigheder ikke kan personaleledergodkende sin egen opgørelse. ► TIMEmSYSTEM er konfigureret således, at det ikke er muligt at genåbne opgørelse som personaleleder, når systemindstillingen 'MaaPersonalledeGenaabne' er sat til nej. 	<p>Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at en medarbejder ikke kan rette i registreringerne, efter opgørelse er blevet brugergodkendt.</p> <p>Vi har observeret, at det ikke er muligt at rette i registreringerne, når en opgørelse er blevet brugergodkendt.</p> <p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at en almindelig medarbejder uden særlige rettigheder ikke kan personaleledergodkende sin egen opgørelse.</p> <p>Vi har observeret, at det ikke er muligt for en almindelig medarbejder uden særlige rettigheder at personaleledergodkende sin egen opgørelse.</p>	Ingen afvigelser konstateret.

Applikationskontroller		
Kontrolmål ► <i>At sikre, at mTIME understøtter, at der bliver angivet korrekte oplysninger til EU ved anvendelse af mTIME i forbindelse med kunders EU-projekter.</i>		
Kontrolaktivitet	Test udført af BDO	Resultat af test
	<p>Vi har foretaget inspektion af TIMEmSYSTEM's vejledning for mTIME samt "Testspecifikation mTIME- Registreringer på EU alias og EU-projektrapport", hvoraf fremgår, at TIMEmSYSTEM tester, at det ikke er muligt at genåbne opgørelse som personaleleder, når systemindstillingen 'MaaPersonalledereGenaabne' er sat til nej.</p> <p>Vi har observeret, at personaleleder ikke kan genåbne en opgørelse, når systemindstillingen 'MaaPersonalledereGenaabne' er sat til nej.</p>	

**BDO STATS AUTORISERET
REVISIONSAKTIESELSKAB**

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

BDO Statsautoriseret revisionsaktieselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO netværk bestående af uafhængige medlemsfirmaer. BDO er varemærke for både BDO netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.700 medarbejdere, mens det verdensomspændende BDO netværk har ca. 115.000 medarbejdere i mere end 166 lande.

Copyright - BDO Statsautoriseret revisionsaktieselskab, cvr.nr. 20 22 26 70.



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.”

Nicolai Tobias Visti Pedersen

Partner, Statsautoriseret revisor

På vegne af: BDO Statsautoriseret revisionsaktiesels...

Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d

IP: 77.243.xxx.xxx

2024-01-19 07:23:18 UTC



Khanh Bao Nguyen-Cong

Direktør og Partner

På vegne af: TIMEsystem ApS

Serienummer: kbn@timemsystem.com

IP: 176.22.xxx.xxx

2024-01-19 07:24:18 UTC

Mikkel Jon Larsen

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670

Partner, chef for Risk Assurance, CISA, CRISC

På vegne af: BDO Statsautoriseret revisionsaktiesels...

Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff

IP: 62.66.xxx.xxx

2024-01-19 08:38:40 UTC



Penneo dokumentnøgle: WOD3J-MHQ5N-TIVJW-PYF3Q-6OEYN-4CLD2

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstempelt med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**