BEIERHOLM
VI SKABER BALANCE

APRIL 2020

IST APS

ISAE 3402 TYPE 2 ERKLÆRING

CVR 25545079

Uafhængig revisors erklæring om kontrolmiljøet i tilknytning til it-driften for SaaS løsninger.

Herudover er der angivet et afsnit i beskrivelse vedrørende rollen som databehandler i henhold til Databeskyttelsesforordningen.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Beskrivelse af kontrolmiljø i tilknytning til it-driften af SaaS løsninger.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet.

Kapitel 4:
Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf.

KAPITEL 1:

Ledelseserklæring

IST ApS behandler personoplysninger på vegne kunder i henhold til databehandleraftale i tilknytning til anvendelse af IST SaaS løsninger.

Medfølgende beskrivelse er udarbejdet til brug for kunder og deres revisorer, der har anvendt IST SaaS løsninger, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne dvs. de dataansvarlige selv har udført, ved vurdering af, om kravene til kontrolmiljøet samt databeskyttelsesforordningen er overholdt.

IST ApS bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 2 (inkl. Bilag 1), giver en retvisende beskrivelse af IST ApS' kontrolmiljø i tilknytning til driften af IST SaaS løsninger i hele perioden 1. april 2019 - 31. marts 2020. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

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

- **De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger**
- **De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger**
- **De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige**
- **De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt**
- **De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne**
- **De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede**
- **De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet**
- **Kontroller, som vi med henvisning til IST SaaS løsningers afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen**
- **Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger**

(ii) Indeholder relevante oplysninger om ændringer i it-driften foretaget i perioden 1. marts 2019 - 31. marts 2020.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller 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 kontroller, som den enkelte kunde måtte anse som vigtig efter deres særlige forhold.

(B) **De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. april 2019 - 31. marts 2020. Kriterierne for dette udsagn er, at:**

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

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

(iii) **Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. april 2019 - 31. marts 2020.**

(C) **Der er etableret og opretholdt passende tekniske og organisatoriske sikringsforanstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlerne i henhold til databeskyttelsesforordningen.**

(D) **Den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2, er udarbejdet med baggrund i overholdelse af IST ApS' standardaftale samt tilhørende databehandleraftale. Kriterierne for dette grundlag var:**

(i) **IST ApS – Overordnet informationssikkerhedspolitik version 3.0**
(ii) **IST ApS – Informationssikkerhedspolitikker for udvalgte kontrolmål i ISO27002 version 1.4**
(iii) **IST ApS – Procedure og instruktioner version 1.8**

Roskilde, den 16. april 2020

Anne Brink Pedersen

Adm. Direktør Anne Brink Pedersen
IST ApS, Gammel Marbjergvej 9, 4000 Roskilde, CVR 25545079

KAPITEL 2:

Beskrivelse af kontrolmiljøet i tilknytning til driften af SaaS løsninger

Indledning

Formålet med nærværende beskrivelse er at levere information til IST ApS' kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører.

Desuden er formålet med beskrivelsen en afdækning af kontrolmiljøet, som er implementeret i forbindelse med it-driften af IST SaaS løsninger. Produktrammen for denne beskrivelse er følgende SaaS løsninger:

- **Folkeskole,**
- **Privat-, fri- og efterskole,**
- **Daginstitutioner,**
- **Pladsanvisning,**
- **SFO, Klub og**
- **Ungdomsskole**

Som supplement til overstående beskrivelse er der tilføjet et selvstændigt afsnit (overensstemmelse med rollen som databehandler) med beskrivelse af centrale krav i forbindelse med rollen som databehandler, kombineret med generelle krav fra databehandleraftaler.

Beskrivelse af IST ApS

IST ApS i sin nuværende form blevet etableret i 2017 og beskæftiger i dag ca. 100 medarbejdere. Fundamentet blev lagt med virksomheden Tabulex ApS tilbage i 1998, hvor de to iværksættere Poul Dige og Carlo Lund etablerede virksomheden på baggrund af to applikationer, der it-understøttede administrationen af lærernes tjenestetid og skemalægning på de danske skoler. Grundlaget for succesen, dengang som nu, er, at udvikling af it-systemer sker i tæt samarbejde med brugerne, domæneeksperter og udviklere med stor viden om forvaltningsområdet. Dette er en filosofi, der stadig udgør grundstenen i IST ApS i 2019.

IST ApS leverer egenudviklede it-systemer som software as a service. Leverancen omfatter 100% drift, service og support, konsulentydelser og kurser. Hertil løbende tilpasninger af funktionalitet således at systemerne lever op til gældende lovgivning og reguleringer.

Kundegruppen er danske kommuners skole- og daginstitutionsområde, erhvervsskoler, gymnasier, FGU'er og private uddannelsesinstitutioner.

Produktkataloget leverer en 360-graders leverance til kommuner og ungdomsuddannelser, der reelt betyder, at børn, forældre og personale forvaltes via vores systemer fra deres første kontakt med pladsanvisningen og daginstitutionen, til skolegang og afsluttende med et eksamensbevis fra ungdomsuddannelsen. Alle vores systemer udvikles, drives og forvaltes af dygtige medarbejdere med base i Danmark, og i samarbejde med koncernens kontorer i Sverige og Norge.

IST ApS er kvalitetsbevidst og har fokus på at levere den aftalte løsning til tiden og til den aftalte pris. Vi arbejder efter fastlagte processer, der sikrer ensartethed i vores arbejde.

Forretningsstrategi / it-sikkerhedsstrategi

Det er IST ApS' strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, således at selskabet ikke påføres uacceptable risici.

Som leverandør til den kommunale sektor, arbejder IST ApS med informationssikkerhed på et forretningsstrategisk niveau. Virksomhedens målsætning er at være kommunernes professionelle samarbejdspartner, der har en skarp holdning til at passe på data, som kommunerne betror os.

Det er IST ApS holdning, at vi altid skal sikre overholdelse af gældende lovgivning og gøre, hvad der er teknisk og økonomisk muligt, for at sikre databehandlingens fortrolighed, integritet og tilgængelighed på et højt niveau. Informationssikkerheden er i højsædet på alle niveauer af organisationen. Alle medarbejdere skal være vidende om vigtigheden af dette fokus og selv være medvirkende til løbende at forbedre arbejdet omkring sikkerhed.

Vores målsætning for informationssikkerheden er, at IST ApS gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed: At opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud.**
- **Integritet: At opnå en pålidelig og korrekt funktion af informationssystemerne med minimeret risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.**
- **Fortrolighed: At sikre fortrolig databehandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang.**

Det er IST ApS' mål at opretholde et informationssikkerhedsniveau, der som minimum:

- **Følger gældende lovgivning**
- **Følger god brancheskik**
- **Lever op til kundens ønsker, krav og forventninger til en professionel leverandør**

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger Samt Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger nr. 502 af 23/05/2018 udgør den lovgivningsmæssige ramme for behandling af persondata i it-services.

Kommunen kan supplere med yderligere instrukser formaliseret i en databehandleraftale, som indgås mellem kommunen (dataansvarlige) og IST ApS (databehandler). Vores ansvar er at foretage de nødvendige tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger behandles på en sikker og forsvarlig måde.

For at sikre en ensartet leverance, som lever op til branchens bedste standarder, har vi valgt at underlægge driften af SaaS løsninger en revisionsproces med det formål at leve op til kravene i en ISAE3402 erklæring. Revisionsprocessen gentages årligt, og resulterer i en revisionserklæring, der offentliggøres på vores hjemmeside www.ist.dk. Erklæringen kan bidrage til kommunens (dataansvarlig) kontrol af, hvorvidt IST ApS lever op til instruksen i den indgåede databehandleraftale.

IST ApS har omkring it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27001 og 2, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

- **Informationssikkerhedspolitikker**
- **Organisering af informationssikkerhed**
- **Medarbejdersikkerhed**
- **Styring af aktiver**
- **Adgangsstyring**
- **Fysisk sikkerhed og miljøsikring**
- **Driftssikkerhed**
- **Kommunikationssikkerhed**
- **Leverandørforhold**
- **Styring af informationssikkerhedsbrud**
- **Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring**
- **Overensstemmelse med lov- og kontraktkrav**

De implementerede sikringsforanstaltninger hos IST ApS fremgår af bilag 1 til denne beskrivelse.

IST ApS' organisation og organisering af it-sikkerheden

IST ApS er en del af en skandinavisk koncern - IST Group, bestående af selvstændige virksomheder i hhv. Sverige, Norge og Danmark.

IST ApS er organiseret efter følgende struktur.

Support & Consulting, der varetager kontakt med brugere i form af support, konsulentbistand, kurser, kontakt med myndigheder og samarbejdspartnere m.m. Afdelingen består af 23 dygtige medarbejdere.

I Development & Operations foregår udvikling og vedligeholdelse af de it-services, vi tilbyder vores kunder. Afdelingen har ansat 23 dygtige medarbejdere med kompetencer indenfor de udviklingsteknologier, vi benytter. It-arkitekten sikrer retningslinjerne for, hvordan vi udvikler vores it-services, så der er sammenhæng og progression. Den grundlæggende it-drift til SaaS løsninger varetages af virksomhedens egne medarbejdere. Vores 3 dygtige medarbejdere sikrer størst mulig tilgængelighed og driftsstabilitet.

Sales & Marketing beskæftiger 4 dygtige medarbejdere, der varetager kommunikation og kontakten med kunder i forbindelse med salg, organiserer produktdemoer, deltager på messer, afgiver tilbud og ordrer og giver feedback til *Solution Management* om, hvad der rører sig i markedet. *Solution Management* arbejder med, hvad der rører sig i vores markeder, og udvikler nye ideer til produkter og services, udarbejder business cases og konkurrentanalyser.

CEO – Administrerende Direktør udvikler Strategier og Mål, og er en del af Koncernledelsen i IST Group, CEO varetager HR funktionen.

IST ApS arbejder med en struktureret metode for at sikre, at alle processer og politikker er beskrevet i vores kvalitetsstyringssystem og ISMS. Dette for at sikre uafhængighed af enkeltpersoner. Incidents eller afvigelser af it-sikkerhedsrelateret karakter behandles på månedlige kvalitetsstyringsmøder, på baggrund af faste procedurer for håndtering af afvigelser.

Forankringen af it-sikkerhedsarbejdet i virksomheden er sikret ved etablering af en tværorganisatorisk informationssikkerhedsgruppe, der arbejder med at højne opmærksomheden på regler og procedurer blandt medarbejderne.

Risikostyring i IST ApS

Det er IST ApS' politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde en normal drift.

Som led i ovenstående it-sikkerhedsstrategi arbejder IST ApS med ISO27002, der er standard for it-sikkerhed, som primær referenceramme for it-sikkerheden. Arbejdsprocessen omkring it-sikkerhed er en kontinuerlig og dynamisk proces, som sikrer, at IST ApS til hver en tid er i overensstemmelse med sine kunders krav og behov.

IST ApS har indarbejdet faste procedurer for risikovurdering af forretningen. Det sikres dermed, at de risici, som er forbundet med de services, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når der ændres i eksisterende systemer eller implementeres nye systemer, som vurderes. Risikovurderingen er en del af den *it*-sikkerhedsansvarliges ansvar og skal efterfølgende forankres og godkendes hos virksomhedens øvrige ledelse.

Håndtering af it-sikkerhed

Ledelsen hos IST ApS har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt. Gennem den centrale it-sikkerhedspolitik har ledelsen beskrevet IST ApS' struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

IST ApS' it-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen/sikkerhedshullet omgående. Der følges bestemte procedurer som sikrer sporbarhed, forebyggende og korrigerende handlinger.

Alle servere og netværksenheder er dokumenteret i IST ApS' dokumentationssystem. Her logges alle ændringer af vores system. Konfigurationsfiler til netværksenheder (firewalls, routere, switche og lignende) ligger gemt i vores dokumentationssystem.

Sikkerhedspolitikken er udarbejdet, så IST ApS har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

På det generelle it-sikkerhedsområde har IST ApS implementeret de nødvendige procedurer og kontroller i forhold til de enkelte områder inden for ISO27002, der er defineret i bilag 1, som viser sikkerhedsstrukturen og de kontrolmål, der er implementeret hos IST ApS.

HR, medarbejdere og uddannelse

Medarbejdernes domæneviden og kompetencer er en vigtig forudsætning for IST ApS' forretning. Det er vigtigt at vedligeholde og udbygge de kompetencer, vi råder over, så vi er i stand til at imødekomme udfordringerne i en omskiftelig branche. Vi arbejder med årlige KPI for, hvor stor en del af vores budget der skal gå til efter/videreuddannelse, og der holdes årlige kompetencesamtaler, hvor der fastsættes virksomhedens krav og medarbejdernes ønsker til faglig udvikling.

Vi arbejder i HR-afdelingen med faste procedurer for bl.a. rekruttering, ansættelse og fratrædelser. Nye medarbejdere gennemgår et grundigt introduktionsforløb til alle afdelinger i virksomheden. Forløbet omfatter et kursus i informationssikkerhed, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd, dataklassifikation og særligt fokus på IST ApS' rolle som databehandler. Kurset afsluttes med, at medarbejderen skriver under på en instruks, der forklarer reglerne for omgang med kundedata, og at medarbejderen er blevet gjort bekendt med hvilket lovgrundlag, der er gældende.

IST ApS' medarbejdere har i begrænset omfang mulighed for at arbejde fra andre faciliteter end kontoret i Roskilde. Virksomheden har udarbejdet en procedure, der beskriver regler og gode råd til fjernarbejdsplads. Vi har etableret tekniske foranstaltninger, der sikrer en krypteret opkobling til kontorfaciliteter fra fjernarbejdspladser. Adgang til backend-systemer og driftsmiljøer er teknisk begrænset. Endelig er medarbejderen informeret om, at en eventuel fjernarbejdsplads også kan være omfattet af ekstern inspektion.

Alle medarbejdere har en fortrolighedsklausul i deres ansættelseskontrakter. Som en del af vores fratrædelsesprocedure indgår en exit-samtale med nærmeste leder, hvor vi minder om, at fortrolighedsklausulen fortsat er gældende efter endt ansættelse. Ved brug af eksterne konsulenter, benytter vi en NDA-skabelon.

For at sikre en kontinuerlig tilgang til informationssikkerhedskulturen har IST ApS en plan for awarenesskampagner. Planen beskriver, hvilke emneområder der skal arbejdes med i løbet af et år. Planen revurderes årligt af informationssikkerhedsorganisationen.

Fysisk sikkerhed

IST ApS har samarbejdet med Interxion siden 2008. Samarbejdet betyder, at vi har overladt de grundlæggende datacenteropgaver til en leverandør, der er ekspert i opbygning og drift af datacentre. Interxion er ansvarlig for fysisk sikring, brand-, og vanddetektion og -bekæmpelse, strøm og køling. Interxions datacenter giver flere lag sikkerhed og opfylder anerkendte internationale standarder for informationssikkerhed vedr. managementsystemer og business continuity management.

At være i stand til at tilbyde stabile og sikre it-services til vores kunder er naturligvis et centralt krav. Fordi Interxion er carrier-neutral, har IST ApS det bredeste udvalg af ISP-udbydere. Datacenteret er hjemsted for Danish Internet Exchange (DIX), og giver os den bedst mulige quality of service for internetforbundne datalinjer.

IST ApS' driftsmiljø er 100% ejet af virksomheden og vedligeholdes af eget driftspersonale. Vi har en 10 kvm stor privat celle, der er fysisk adskilt fra andre kunder hos Interxion. Alle adgange til cellen sker via personlige adgangskort og registreres i et centralt system.

Strøm og køling

Der er etableret redundant power setup med to uafhængige plugsets (Feed A) og (Feed B). Hertil et extra plugset (A+B Feed) via ATS (Powerswitch) for udstyr, der kun har ét strømudtag. Strømforsyningen til datacenteret har flere niveauer af sikring ved tab af bystrøm. Der er etableret fuldskala batteri-backup til begge strøm feeds. Hvis batterikapaciteten når et kritisk niveau, vil et antal dieselgeneratorer overtage strømproduktionen, der er i stand til at levere fuld kapacitet. Generatorerne er sat i et redundant setup med ekstra kapacitet, således at fejl i en generator ikke medfører mangel på redundans. Datacenteret har lokal dieselkapacitet til at køre mindst 24 timer, og der er forsyningsaftaler med olieselskab om 24/7/365 leverance af dieselolie. Der foretages jævnlige test af de enkelte komponenter i batteri og dieselgeneratorer, ligesom der én gang årligt foretages en fuldskala test af hele setuppet.

Sikring mod vand

Datacenteret er bygget med forhøjet gulvniveau, og der er etableret intelligent water leak detection systemer, der lokaliserer en eventuelt vandlæk. Bygningen er indrettet med sikring mod, at kondensvand kan dryppe på hardwaren. Dette gælder også i tilfælde af, at brandbekæmpelsesanlægget aktiveres. Ved hjælp af målere og termostater holdes en konstant temperatur og luftfugtighed i datacenteret.

Brandsikring

Der er etableret automatiseret og overvåget brandbekæmpelsessystem, der via sensorer måler varme og fugtighed. Anlægget er energenbaseret, og alle energenflasker overvåges for, om de holder det anbefalede tryk. Hertil er der jævnlig fysisk kontrol og periodisk udskiftning af flasker v. udløbsdato.

Fysisk sikring

Interxion har et omfattende sikkerheds-setup bestående af vagtpersonel i 24/7/365 rundering, og teknisk overvågning af perimeter, bygninger og gangarealer inden i centeret. Fysisk adgang foregår via vagtcentralen og kun med godkendt adgangskort. Identiteten af personer med adgang foregår via irisscanning eller fingeraftryk. Alle indgange til centeret er videoovervåget, og sluserne har vægtkontrol, der sikrer, at 2 personer ikke kan komme ind på samme tid.

Offsite lokation

Vi har etableret en sekundær backuplokation, der ligger mere end 15 km væk fra den primære lokation. Den sekundære lokation driftes ligeledes af Interxion og er opbygget efter samme principper som den primære driftslokation. Det er blandt andet hertil, at offsite backups overføres.

Kontrol med Interxion

IST ApS fører løbende kontrol med om Interxion, som leverandør til kritiske dele af vores driftsmiljø, hvorvidt de lever op til kvalitetskrav samt overholdelse af kravene fra SLA i tilknytning til deres ydelser. Interxion leverer årligt en SOC2 auditorrapport, som er resultatet af deres omfattende eksterne revision. IST ApS evaluerer rapporten og sammenholder den med egne observationer. Herefter vurderer vi, om leverandøren lever op til de aftalte serviceydelser, og hvorvidt der er grund til at tage aspekter op med dem.

Datalinjer og netværkssikkerhed

Dataforbindelsen til driftsmiljøet består af 2 uafhængige ISP'er med opgraderbar 1gbs kapacitet. I setuppet indgår én primær og én sekundær datalinje, hvor BGP automatisk afgør, hvilken det er bedst at benytte. Bryder den primære linje ned, routes trafikken automatisk via den sekundære. Når den primære er reetableret, routes trafikken igen via denne.

Vores samarbejde med ISP'en omfatter Ddos beskyttelse med automitigering indenfor kort tid. Mitigeringsstrategien er lagt i samarbejde med IST ApS' driftspersonel, og tilpasset vores normale trafikmønstre. Ved et Ddos angreb overstiges tærskelværdierne, og automitigeringen træder til.

Driftsmiljøets perimetersikkerhed består af 2 veldimensionerede firewalls, der er sat i et aktiv/passivt cluster. Forbindelsen gennem firewallen sikres via en gensidig overvågning i de to firewalls, der selv afgør, hvilken der er aktiv, og hvilken der er passiv.

Firewallen er regelbaseret og har som udgangspunkt en "deny all" trafikregel. Herpå er der udarbejdet et regelsæt, der tillader specifikke protokoller mod en given servergruppering (Eks: https -> Webservere).

Firewallen har en indbygget "Load balancer", der benyttes til at sikre fordelingen af den samlede trafik til flere servere. Endelig fortager firewallen inspektion af datapakker (IDS). Automatiseret scanning og blokering af trafik baseres på sårbarhedssituationen og holdes dagligt opdateret.

Hardware setup

Hardware i driftsmijøet er opbygget med et antal fysiske servere (Hypervisor), hvori flere virtuelle servere driftes. Hertil er der dedikeret et antal fysiske servere med specifikke formål (Databaseserver, filstorage m.m).

De virtuelle miljøer er fordelt i 2 clustere bestående af hver 3 fysiske hypervisors. Kapaciteten sikres ved, at alle virtuelle servere kan afvikles fra n-1 hypervisor. Dette betyder, at vi afvikler alle virtuelle servere på 2 af de 3 hypervisors.

Hypervisornes diskkapacitet håndteres af en central netværksbaseret løsning (SAN). SAN'et tilgås via fuld redundant switching mellem hypervisorne. Diskkapaciteten består af to fysisk adskilte diskenheder (noder), med hver 12 harddiske. Den samlede diskkapacitet er delt op i 2 logiske "diske", kaldet LUN. Hvert LUN replikeres mellem de to noder. Dette setup betyder, at alle virtuelle servere kan køre med blot én aktiv node.

Drift af SaaS løsninger

Faste driftsopgaver udføres med faste intervaller. Disse opgaver styres i IST ApS' driftsafdeling, som varetager kontrolleret vedligehold og drift af samtlige servere. Opgaven er beskrevet i tilhørende checklister.

Registrering af it-udstyr i produktion (aktiver)

IST ApS registrerer it-udstyr og services i virksomhedens CMDB (Configuration Management Database). Formålet er, at vi altid har en opdateret database med relevante data omhandlende it-udstyr, der er nødvendigt for, at vi kan levere it-services til kunder.

It-udstyr med en ip-adresse, der enten direkte eller indirekte indgår i produktionsmiljøer og/eller kontormiljøer, skal registreres og holdes opdateret i CMDB'en. Dette er eksempelvis: Netværksudstyr, Servere (Fysiske/virtuelle), Printere, PC'er, Mobile Enheder, Applikationer, Styresystemer, Services og Databaser.

I CMDB'en registreres nødvendige detaljer om aktivet og det omkringliggende it-miljø. Detaljeringsgraden afhænger af aktivtypen. Der registreres, hvilket netværk enheden er tilkoblet, IP-adresse, ansvarlig person/team, rolle (produktion, test/staging mv.), relationer til databaser, applikationer og andre services.

Driftsovervågning – NOC

Driftsmiljøet overvåges 24/7/365 via en automatiseret service. Der overvåges ressourcer for servere (Cpu, ram, disk, netværk) og tilgængelighed. Overvågningen omfatter også relevante it-services eksempelvis backups, tilgængelighed for kundevendte systemer og systemer til internt brug.

Den primære overvågning foregår internt i driftsmiljøet, men for også at dække den eksterne tilgængelighed har vi etableret en offsite overvågning. Ved fejl rapporteres til NOC, hvorefter fejlen bliver undersøgt. Er der tale om kritiske fejl i servere eller services, adviseres den vagthavende driftsmedarbejder direkte.

Driftens NOC er til internt brug i IST ApS, og er således ikke tilgængelig for kunder. Kunder, der oplever driftsproblemer, skal kontakte os via de supportkanaler, der er aftalt i kontrakter og Generelle vilkår. Vi har åbent for kundehenvendelser i dagtimerne mellem 8 og 17.

Driftsstatus kommunikeres via IST ApS' hjemmeside: https://www.ist.com/dk/drift

Logning

Logning er et værdifuldt værktøj til overvågning, fejlhåndtering og efterforskning. Da logs indeholder mange forskellige informationer, har vi adgangsstyring til logs afhængigt af, hvilke opgaver den enkelte medarbejder må udføre. IST ApS arbejder med logning på flere niveauer: Applikationslogs – der håndterer specifikke operationer i applikationer, Adgangslogs – der logger, hvornår brugere logger ind i applikationer, logning af, hvilke brugere der tilgår information af følsom og fortrolig karakter i vores applikationer og Syslog – overvågningslogning.

Backup

Formålet med backup er at sikre, at kundens data i IST ApS' hostingcenter kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid. Der tages backup på forskellige niveauer som virtuelle servere, konfigurationer og data. Dette sikrer, at vi har flere muligheder for at sætte ind ved behov for reetablering.

Der tages backup af relevante databaser og konfigurationer, med henblik på at muliggøre reetablering i en given nødsituation. Der er forskellige krav til frekvens af backups afhængigt af it-systemets kritikalitet.

Backuppolitikken for kundedatabaser beskriver, at der skal tages daglige backups, minimum én i døgnet. For mindst én af disse backups foretages en reetableringstest, der tester backuppens integritet. Hver backup gemmes på dedikerede backupservere placeret i driftsmiljøet. Desuden flyttes backups til en fysisk adskilt lokation.

Alle backups krypteres med AES-256 krypteringsnøgle, og transport af data mellem primær site og offsite foregår med krypterede datalinjer og SFTP.

Daglige backups af kundedatabaser opbevares i 30 dage. Herefter opbevares den sidste backup i hver måned. Backups, der er ældre end 5 år, slettes permanent.

Patch management / ændringshåndtering

Formålet med patch management er at sikre, at alle relevante opdateringer som patches, fixes og service packs fra leverandører implementeres for at sikre systemerne mod nedetid og uautoriseret adgang, og at implementeringen sker på en kontrolleret måde.

Vedligehold af Windows operativsystemer og tilhørende backend-systemer fra Microsoft, håndteres af Microsofts indbyggede WSUS (Windows Server Update Services), hvor sikkerheds- og kritiske patches installeres automatisk med faste intervaller.

Efter installation af operativsystemer følges en procedure, der sikrer, at det kun er relevante services og applikationer, der er tilgængelige på serveren. Umiddelbart inden en server sættes i produktion, følges en "Hardening"-proces, der sikrer, at de anbefalede sikkerhedsindstillinger er sat korrekt på serveren.

Styring af it-sikkerhedshændelser

Sikkerhedshændelser og svagheder i IST ApS' systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt. Der er etableret procedurer for hændelsesstyring og afvigerapportering, herunder sikkerhedsbrud. Procedurerne sikrer, at der arbejdes systematisk, foretages nødvendig dataindsamling og dokumentation, således at der efterfølgende er et godt grundlag at evaluere ud fra. Afvigerapporteringen er en del af vores Kvalitetsstyringssystem, og det er Management, der er ansvarlig for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Brugerstyring / adgangssikkerhed

Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne.

Tildeling af adgang til driftsmiljø skal ske i overensstemmelse med forretningsbetingede formål og informationernes klassifikation. Både fysisk og logisk adgang er baseret på principperne "need-to-know" og "least privillege", hvor der tildeles adgang til de informationer, som man skal bruge for at kunne udføre sine opgaver/sit job eller rolle.

Anmodning om adgang til interne it-systemer og produktionsmiljøer følger en fastlagt procedure, der sikrer en adskillelse i anmodning, godkendelse, verifikation og implementering. Adgangsstyringen dokumenteres i et centralt system.

Krav til password - alle brugere oprettet i IST ApS' centrale brugerdatabase skal skifte password hver 90. dag. Passwordet skal være på mindst 6 tal eller bogstaver, og de seneste 24 passwords kan ikke bruges igen. Herudover indeholder password politikken en regel om at et password maksimalt kan skiftes 1 gang dagligt. For at beskytte mod repeat passwords.

Beredskabsstyring

IST ApS' forretning er i stor grad baseret på den grundliggende it-infrastruktur, hvorfra it-services udbydes til kunderne. It-beredskabsplanen skal således ses som en samlet Business Continuity Plan (BCP) eller Forretningskontinuitetsplan.

Ved alvorlige fejl informeres den it-sikkerhedsansvarlige og Management i IST ApS. Den aktuelle beredskabsplan beskriver, hvorledes der skal informeres, fejlsøges og fejlrettes. For at gøre planerne så operationelle som muligt er der etableret procedurer for beredskabsstyring på flere niveauer. En overordnet BCP beskriver definitioner af beredskabsfaser, kritikalitet, eskalerings- og kommunikationsprocedure. Planen beskriver håndteringen af to af de værst tænkelige scenarier: Nedbrud i datalinjer og totalt datacenternedbrud.

BCP-planen suppleres af et antal reetableringsplaner for kundevendte it-services samt for kritiske interne systemer. For at sikre tilgængeligheden til reetableringsplanerne er disse lagret på flere forskellige medier og i hardcopy.

I løbet af kontrolperioden er der gennemført relevante afprøvninger af beredskabsplanen. Hertil skal der foregå en årlig kvalitetssikring af alle reetableringsplaner, hvorefter enkelte systemer vil blive udvalgt til en skrivebordstest.

Udviklingsmiljøet

Når IST ApS udvikler software (kunderettede it-services) bruges der dedikerede testmiljøer, hvorfra softwaren kan afvikles til udvikling og test. Disse miljøer er andre miljøer end dem, som kundernes software afvikles på.

Eventuelle fejl i data og systemintegrationer er således afgrænset til kun at have indflydelse på integriteten af testdata. Testdata er fiktive data oprettet i systemet til formålet (= ikke kundedata). Under de afsluttende testfaser kan der være behov for at teste med data, der ligner live-miljøernes.

Test- og udviklingsmiljøer afvikles fra produktionsmiljøet i et selvstændigt IP-segment. Tilgængeligheden til miljøerne er begrænset, så disse kun kan tilgås fra de udgående adresser for kontorerne i Roskilde, Svendborg, Växjö, Linköping, Stockholm og Oslo. Dette er styret via specifikke grupper i vores firewall, som også styrer, hvilke protokoller og porte systemerne kan tilgås med.

Der er fastlagte procedurer for udvikling, test og godkendelse i virksomhedens Kvalitetsstyringssystem.

Overensstemmelse med rollen som databehandler

Det er ledergruppen hos IST ApS' der er ansvarlig for at sikre, at alle relevante juridiske og kontraktuelle krav er identificeret og korrekt overholdt. Relevante krav kan fx være:

- EU's Databeskyttelsesfordning (GDPR)
- Dansk lov om Databeskyttelse
- Databehandleraftaler
- IST ApS Service Level Agreement
- IST ApS standardkontrakt eller andre relevante kilder

Tilstedeværelsen af alle nødvendige aftaler, et omfattende ISMS (ledelsessystem for styring af informationssikkerhed) samt andre relevante dokumenter sikrer overholdelsen af relevante juridiske og kontraktuelle krav. IST ApS er forpligtet til at inddrage juridiske eksperter efter behov for at sikre et passende niveau i forhold til overholdelsen af lovgivningen.

Desuden gennemgår ledergruppen regelmæssigt alle IST ApS' sikkerhedspolitikker, evt. med inddragelse af relevante interessenter. IST ApS' ISMS revideres regelmæssigt af en uvildig, ekstern part, og revisionsrapporten deles ved forespørgsel med alle IST ApS' kunder.

EU Databeskyttelsesforordningen (GDPR)

IST ApS' SaaS løsninger understøtter kundernes arbejdsprocesser i forbindelse med daginstitutions-, fritidstilbuds-, ungdomsskole-, folkeskole- og ungdomsuddannelsesområderne. IST ApS ejer ikke data, som kunderne indsamler, men udvikler og driver de it-services, som kunderne anvender til at udføre den nødvendige persondatabehandling. Ifølge Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er IST ApS databehandler, og kunden er dataansvarlig.

IST ApS samarbejder med juridiske eksperter med henblik på at sikre, at alle relevante juridiske krav er identificeret og imødekommet. IST ApS har også sørget for at have relevante kontrakter med alle nøgleinteressenter (herunder kunder, samarbejdspartnere, nøgleleverandører osv.) med henblik på at sikre overholdelse af loven. Desuden samarbejder IST ApS med sine kunder om at sikre, at kunderne er bekendt med og overholder de relevante GDPR-regler.

Ifølge GDPR sikrer efterlevelsen af ISO 27001 og 2 standarden et passende informationssikkerheds-niveau. Udover at overholde de relevante ISO-krav, sikrer IST ApS data privacy og datasikkerhed på et kontraktuelt niveau.

Databeskyttelsesrådgiver (DPO)

IST ApS er ejet af IST Group, som er en skandinavisk baseret virksomhed med hovedsæde i Växjö i Sverige. IST Group har en central forretningsstøtteenhed – Business Support - der servicerer de enkelte regioner med funktioner, der understøtter forretningen. Virksomhedens *Databeskyttelsesrådgiver* er organiseret i Business Support og kan kontaktes på privacy@ist.com.

Privatliv og beskyttelse af personoplysninger
Som nævnt er IST ApS databehandler for sine kunder, i og med at kunderne tilbydes en it-service, hvortil de kan overføre og behandle data og anvende dette til videre bearbejdning indenfor deres respektive forvaltningsopgaver. IST ApS er ikke ansvarlig for data, som kunderne uploader til deres IST ApS it-service. Med udgangspunkt i kategorier og fortrolighed af de typer af data, kunden overlader til behandling, skal IST ApS iværksætte alle nødvendige sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

Nedenfor beskrives IST ApS' procedurer for, hvordan IST ApS som databehandler opererer under instruks fra de dataansvarlige.

Databehandleraftaler
IST ApS indgår databehandleraftaler med alle sine kunder. Databehandleraftalen er en fastlagt procedure ved kontraktindgåelse, og der benyttes enten IST ApS' egen skabelon eller kundens skabelon. Disse aftaler beskriver IST ApS' rolle og ansvar som databehandler.

Som databehandler pålægges IST ApS et særligt ansvar defineret i Databeskyttelsesforordningen, udmøntet som krav i en databehandleraftale. IST ApS skal blandt andet:

- **Føre fortegnelse over, hvilke kategorier af persondata der behandles i de respektive it-services.**
- **Beskrive de tekniske og organisatoriske sikkerhedsforanstaltninger, som er iværksat med henblik på at værne om persondata.**
- **Bidrage til at opfylde kundens forpligtelser vedr. den registreredes rettigheder (jf. kapitel 3 i EU Databeskyttelsesforordningen - GDPR).**
- **Stille ekspertise til rådighed for kunden for at sikre efterlevelse af Artikel 32 – 34 i GDPR.**
    - **Artikel 32 – behandlingssikkerhed**
    - **Artikel 33 – Anmeldelse af brud på persondatasikkerheden**
    - **Artikel 34 – Underretning om brud på persondatasikkerheden for de registrerede**
- **Iagttage kundens krav vedr. overførsel af persondata uden for EØS.**
- **Registrere navn og kontaktinformation på leverandører, der er underdatabehandlere.**
- **Sikre, at krav vedr. persondatabehandling fra kunden matcher krav til en underdatabehandler.**

Formålsbestemthed og hjemmel
Som databehandler arbejder IST ApS med persondata på baggrund af kundernes instrukser, der beskriver en formålsafgrænsning for, hvad data må benyttes til. IST ApS er således ansvarlig for, at data indsamlet med ét formål ikke behandles i strid med dette.

Hjemmelen for behandling af persondata i IST ApS' udbudte it-services i SaaS løsninger, skal søges i den dataansvarliges overholdelse af retlig forpligtigelse eller opfyldelse af kontraktligt forhold. (GDPR Art. 6 L b og c). Der tages udgangspunkt i kundernes forvaltning af lovgivning på dagtilbuds-, fritids-, folkeskole- og ungdomsuddannelsesområdet. Hertil kan der være hjemmel i Forvaltningsloven, Regnskabs- og bogføringslov mm.

Adgang til kundedata
IST ApS tilbyder løsninger som *Software as a Service*, der driftes af IST ApS's driftsafdeling.

Udvikling, test og release varetages af vores egen udviklingsafdeling. Vi påtager os dermed det fulde ansvar for behandling af kunders data.

Generelt har medarbejdere i IST ApS ikke adgang til kundedata, medmindre specifikke arbejdsopgaver taler herfor.

IST ApS har indført principper for medarbejderes adgang til og arbejde med kunders data:

- **Det er kun betroede medarbejdere, der har adgang til kundedata, og kun ud fra et arbejdsbetinget behov.**
- **Omfattende introduktionsforløb med fokus på regler for omgang med kundedata og opfølgning via awarenes-kampagner.**
- **Procedure for tildeling og revision og kontrol af adgange til kundedata.**
- **Regler for behandling af kundedata i IST ApS' ISMS.**

IST ApS logger og overvåger adgangen til kundernes data for at sikre, at ingen uautoriserede personer får adgang, eller tildelte adgange misbruges.

Væsentlige ændringer i forhold til it-sikkerhed

Vi har i IST ApS det seneste år arbejdet fokuseret på at forbedre processer og procedurer for at højne it-sikkerheden. Vi har implementeret risikovurderinger og følger op på de handlinger, der skal til for at minimere de risici, hvor vi som Management vurderer, at den samlede risikofaktor er højere, end vi ønsker den.

Vi har igangsat en række aktiviteter for at øge opmærksomheden omkring sikkerheden og den enkelte medarbejders ansvar for, at den overholdes.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Dette kapitel beskriver det generelle kontrolmiljø for IST ApS' SaaS løsninger, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

IST ApS er ikke ansvarlig for adgangsrettigheder, herunder tildeling, ændring og nedlæggelse, i forhold til den enkelte kundes brugere og deres adgange til SaaS løsninger. Kunden er selv forpligtiget til at sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

Kunderne er ansvarlige for datatransmission til SaaS løsninger, og det er kundernes ansvar at skabe den nødvendige datatransmission til IST ApS' datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

BILAG 1:

IST ApS har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27001 og 2

0. Risikoanalyse og håndteringen

- 0.0. Vurdering af sikkerhedsrisici
- 0.1. Risikohåndtering

5. Informationssikkerhedspolitikker

- 5.1. Retningslinjer for styring af informationssikkerhed

6. Organisering af informationssikkerhed

- 6.1. Intern organisering
- 6.2. Mobilt udstyr og fjernarbejdspladser

7. Medarbejdersikkerhed

- 7.1. Før ansættelse
- 7.2. Under ansættelsen
- 7.3. Ansættelsesforholds ophør eller ændring

8. Styring af aktiver

- 8.1. Ansvar for aktiver
- 8.3. Mediehåndtering

9. Adgangsstyring

- 9.1. Forretningsmæssige krav til adgangsstyring
- 9.2. Administration af brugeradgang
- 9.3. Brugernes ansvar

12. Driftssikkerhed

- 12.1. Driftsprocedurer og ansvarsområder
- 12.3. Backup
- 12.4. Logning og overvågning
- 12.5. Styring af driftssoftware

13. Kommunikationssikkerhed

- 13.1. Styring af netværkssikkerhed

14. (Anskaffelse), udvikling og vedligeholdelse af systemer

- 14.1. Sikkerhedskrav til it-systemet
- 14.2. Sikkerhed i udviklings- og hjælpeprocesser

15. Leverandørforhold

- 15.1. It-sikkerhed i leverandørforhold
- 15.2. Styring af leverandørydelser

16. Styring af informationssikkerhedsbrud

- 16.1. Styring af informationssikkerhedsbrud og forbedringer

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

- 17.1. Informationssikkerhedskontinuitet
- 17.2. Redundans

18. Overensstemmelse

- 18.1. Overensstemmelse med lov- og kontraktkrav

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til kunder af IST SaaS løsninger og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om IST ApS' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af kontrolmiljøet i tilknytning til it-driften af IST SaaS løsninger, jævnfør databehandleraftale med kunder, i hele perioden 1. april 2019 - 31. marts 2020, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter tilknyttet anvendelsen af eksterne samarbejdspartnere. Brugen af underleverandører er nærmere oplistet i databehandleraftaler med kunderne.

Erklæringen behandler ikke kundespecifikke forhold. Desuden omfatter erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. kontrolbeskrivelsen kapitel 2, afsnittet om komplementerende kontroller.

IST ApS' ansvar

IST ApS er ansvarlig for udarbejdelsen af kontrolbeskrivelsen i kapitel 2 (inkl. bilag 1) og den medfølgende ledelseserklæring i kapitel 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet er præsenteret; for leveringen af de ydelser beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR's Etiske Regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd. Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om IST ApS' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til 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. Denne standard kræver, at vi overholder etiske krav samt 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 beskrivelse, udformning og funktionalitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risicierne for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi

anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som IST ApS har specificeret og beskrevet i kapitel 2 (inkl. bilag 1).

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

Begrænsninger i kontroller hos IST ApS

IST ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på datasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler 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 kriterier, der er beskrevet i kapitel 1 i ledelsens erklæring. Det er vores opfattelse,

a) at beskrivelsen af IST ApS' kontrolmiljø i tilknytning til driften af IST SaaS løsninger, således som det var udformet og implementeret i hele perioden 1. april 2019 - 31. marts 2020, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. april 2019 - 31. marts 2020, og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. april 2019 - 31. marts 2020.

Beskrivelse af test kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt IST ApS' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kontrolmiljøet er passende og om kravene i databeskyttelsesforordningen er overholdt.

Søborg, den 23. april 2020

Beierholm
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
IT-auditor, Manager

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Vi har struktureret vores arbejde i overensstemmelse med ISAE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør. For hvert kontrolmål indleder vi med et kort resumé af kontrolmålet, som det er beskrevet i referencerammen ISO27001 og 2, version 2017.

Hvad angår periode har vi i vores test forholdt os til, om IST ApS A/S har levet op til kontrolmålene i perioden 1. april 2019 - 31. marts 2020.

Under det grå felt er tre kolonner:

- **Første kolonne viser de aktiviteter, som IST ApS A/S jf. sin dokumentation har iværksat for at leve op til kravene.**
- **Anden kolonne viser, hvordan vi har valgt at teste, om det forholder sig som beskrevet.**
- **Tredje kolonne viser resultatet af vores test.**

De udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design, implementering og operationelle effektivitet er foretaget ved metoderne 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.**
Forespørgsler	**Forespørgsel til passende personale hos IST ApS. Forespørgsler har omfattet, hvordan kontroller udføres.**
Observation	**Vi har observeret kontrollens udførelse.**
Genudføre kontrollen	**Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.**

KONTROLMÅL - INDLEDNING:

Risikovurdering og – håndtering

Risikovurdering skal identificere og prioritere risici med udgangspunkt i driften af SaaS løsninger. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Gennem en risikovurdering er der sket identificering og prioritering af risici. Udgangspunkt for vurderingen er de i beskrivelsen definerede SaaS løsninger. Resultatet bidrager til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.	Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen. Vi har kontrolleret, at der for SaaS løsninger arbejdes med en løbende vurdering af den risiko, som opstår som følge af de forretningsmæssige forhold. Vi har kontrolleret, at risikovurderingen er forankret ned igennem virksomhedens organisation. Vi har kontrolleret, at der sker løbende behandling af virksomhedens risikobillede, og med dertil hørende løbende tilpasning af konsekvenser og sandsynlighed.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 5:

Informationssikkerhedspolitikker

Ledelsen skal udarbejde en informationssikkerhedspolitik, som bl.a. skal indeholde ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. Informationssikkerhedspolitikken vedligeholdes under hensyn til den aktuelle risikovurdering.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der er en skriftlig strategi, som bl.a. indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. It-sikkerhedspolitikken og de tilhørende støttepolitikker er godkendt af virksomhedens ledelse, og efterfølgende forankret ned gennem virksomhedens organisation. Politikken er tilgængelig for alle relevante medarbejdere. Politikken revurderes efter planlagte intervaller.	Vi har indhentet og revideret IST ApS' seneste it-sikkerhedspolitik. Gennem revisionen har vi kontrolleret, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Samtidig har vi ved revisionen kontrolleret, at de underliggende støttepolitikker er implementeret. Vi har kontrolleret, at politikken er godkendt og underskrevet af virksomhedens bestyrelse og direktion, og at den er gjort tilgængelig for medarbejderne via IST ApS' intranet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 6:

Organisering af informationssikkerhed

Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikkerhedsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering.

Virksomheden skal sikre, at fjernarbejdspladser og brugen af mobilt udstyr får et passende beskyttelsesniveau.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret. It-sikkerheden er koordineret på tværs af virksomhedens organisatoriske rammer.	Gennem inspektion og test har vi sikret, at det organisatoriske ansvar for it-sikkerhed er dokumenteret og implementeret. Vi har kontrolleret, at it-sikkerheden er forankret på tværs af organisationen i forhold til SaaS løsninger. Ved interview har vi kontrolleret, at den it-sikkerhedsansvarlige har kendskab til rollen og de tilhørende ansvarsområder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til anvendelsen er håndteret.	Det er kontrolleret, at der findes formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Vi har stikprøvevis inspiceret, at politikken er implementeret i forhold til medarbejdere med mobilt udstyr. Ifm. anvendelsen af fjernarbejdspladser hos IST ApS har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, så at området er afdækket i forhold til risikovurderingen for området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

Det skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Via fastlagte arbejdsprocesser og procedurer er det sikret, at alle nye medarbejdere får oplyst deres særlige ansvar og rolle i forbindelse med ansættelse i IST ApS. Herunder de fastlagte rammer for deres arbejde og den omkringliggende it-sikkerhed. Eventuelle sikkerhedsansvar er fastlagt og nærmere beskrevet gennem stillingsbeskrivelse og i form af vilkår i ansættelseskontrakten. Medarbejderne er bekendte med deres tavshedspligt via en underskrevet ansættelseskontrakt og via IST ApS' personalepolitik.	Vi har kontrolleret, at de af ledelsen udarbejdede forretningsgange og procedurer i forbindelse med ansættelse og ansættelsesophør er overholdt. Gennem stikprøver har vi testet, om ovenstående forretningsgange og procedurer er overholdt både i forhold til ansættelse og ansættelsesophør. Ved interview har vi kontrolleret, at væsentlige medarbejdere for SaaS løsninger er bekendt med deres tavshedspligt. Vi har gennemgået centrale medarbejderes stillingsbeskrivelser, og efterfølgende testet den enkelte medarbejders kendskab til arbejdsmæssige roller og tilhørende sikkerhedsansvar. Revision har påset, at IST ApS' personalepolitik er nemt tilgængelig, og har et afsnit omkring vilkår for fortrolighed, som følge af information opnået ifm. arbejde udført hos IST ApS.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 8:

Styring af aktiver

Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og funktionsmæssige informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig "ejer". Virksomheden skal sikre, at informationsaktiver i forhold til SaaS løsninger får et passende beskyttelsesniveau.

Der skal være betryggende kontroller, som sikrer, at datamedier bliver bortskaffet på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver. Der er udpeget en ejer for alle væsentlige aktiver i forbindelse med driften af SaaS løsninger.	Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder i tilknytning til driften af IST ApS' SaaS løsninger. Gennem observation og kontrol har vi kontrolleret relationer over til de centrale knowhow-systemer for driften af SaaS løsninger. Vi har ved observationer og forespørgsler kontrolleret, at IST ApS overholder de væsentligste sikringsforanstaltninger for området i henhold til sikkerhedsstandarden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Informationer og data i relation til SaaS løsninger er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed.	Vi har kontrolleret, at der findes en passende opdeling af aktiver for IST ApS' drift af SaaS løsninger. I den forbindelse har vi kontrolleret, at der er passende opdeling og tilhørende procedurer/forretningsgange ifm. beskyttelse omkring ejerskab mellem applikationer og data samt øvrige enheder. Vi har kontrolleret, at kontrakter og SLA anvendes som et centralt værktøj til at sikre definitionen, adskillelsen og afgrænsningen mellem IST ApS' ansvarsområder og overgangen til kundens ansvarsområde ifm. adgang til informationer og data. Derved påhviler der typisk kunden et eget ansvar med at sikre, at der er et passende beskyttelsesniveau på egne informationer og data.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er procedurer for, hvorledes der skal ske destruktion af databærende medier.	Vi har: • forespurgt ledelsen om hvilke procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået procedurerne for destruktion af databærende medier, til bekræftelse af, at de er formelt dokumenterede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 9:

Adgangsstyring

At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for IST ApS' adgangsstyring.	Vi har: • forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i IST ApS. • stikprøvevist påset, at procedurer for adgangsstyring eksisterer og er implementeret jf. IST ApS' retningslinjer. • gennem interview af nøglepersoner samt ved stikprøvevis inspektion påset, at adgangsstyring til driftsmiljøet følger IST ApS' retningslinjer, og at autorisationer tildeles i henhold til aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang. Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåges.	Vi har forespurgt ledelsen, om der er etableret procedurer for adgangsstyring i IST ApS. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende autorisationssystemer i relation til adgangsstyring i IST ApS. • at den formaliserede forretningsgang for tildeling og afbrydelse i brugeradgang er implementeret i IST ApS' systemer, og at der foretages løbende opfølgning på registrerede brugere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Interne brugeres adgangsrettigheder gennemgås regelmæssigt efter en formaliseret forretningsgang.	Vi har ved stikprøvevis inspektion påset, at der eksisterer en formaliseret forretningsgang for opfølgning på kontrol af autorisationer i henhold til retningslinjerne, herunder: • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med udvidede rettigheder hver 3. måned • at der foretages løbende formel ledelsesmæssig opfølgning på registrerede brugere med almindelige rettigheder hver 6. måned.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Tildeling af adgangskoder styres gennem en formaliseret og kontrolleret proces, som bl.a. sikrer, at der sker skift af standardpassword.	**Vi har forespurgt ledelsen, om der er etableret procedurer for tildeling af adgangskoder i IST ApS.** **Vi har ved stikprøvevis inspektion påset,** • **at der ved tildeling af adgangskode sker en automatisk systemmæssig kontrol af, at password skiftes ved første login.** • **at standardpassword ved implementering af systemsoftware mv. skiftes.** • **hvor dette ikke er muligt, at procedurer sikrer, at der sker manuelt skift af standardpassword.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**
Adgange til operativsystemer og netværk er beskyttet med password. **Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde (6 tegn) og maksimal løbetid (max 90 dage), lige som password opsætninger medfører, at password ikke kan genbruges (husker de seneste 24 versioner). Et password kan minimum skiftes i gang dagligt.** **Endvidere bliver brugeren lukket ude ved gentagne fejlslagne forsøg på login.**	**Vi har forespurgt ledelsen, om der er etableret procedurer, der sikrer kvalitetspassword i IST ApS.** **Vi har ved stikprøvevis inspektion påset, at der er etableret passende programmerede kontroller for sikring af kvalitetspassword, der sikrer efterlevelse af politikker for:** • **minimum længde for password** • **maksimal levetid for password** • **minimum historik for password** • **minimum dage for skrifte af password** • **lockout efter fejlede loginforsøg** • **password skal være kompleks**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Driftsprocedurer og ansvarsområder

En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter, og de heraf afledte kapacitetskrav.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der er dokumenteret driftsafviklingsprocedurer for forretningskritiske systemer, og de er tilgængelige for personale med et arbejdsbetinget behov. Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse.	Vi har: • forespurgt ledelsen om alle relevante driftsprocedurer er dokumenteret. • i forbindelse med revisionen af de enkelte driftsområder stikprøvevist kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. • foretaget inspektion af brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud. Der foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.	Vi har: • forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. • stikprøvevist gennemgået, at ressourceforbruget i driftsmiljøet bliver overvåget og tilpasset i forhold til det forventede og nødvendige kapacitetsbehov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Backup

At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der foretages sikkerhedskopiering af alle virksomhedens væsentlige informationsaktiver, herunder eksempelvis parameteropsætninger og anden driftskritisk dokumentation, i henhold til fastlagte retningslinjer.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået backupprocedurer, til bekræftelse af at de er formelt dokumenterede. • stikprøvevist gennemgået backup-log, for bekræftelse af at backup er gennemført succesfuldt, og at tilfælde af mislykket backup håndteres rettidigt. • gennemgået fysisk sikkerhed (bl.a. adgangsbegrænsning) for intern opbevaringslokation, til bekræftelse af at backup opbevares betryggende.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Logning og overvågning

At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerheds-relaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. IST ApS logger, når brugerne logger af og på systemerne. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter der udføres, og gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametre for logning er opsat, således at handlinger, udført af brugere med udvidede rettigheder, bliver logget. • stikprøvevist kontrolleret, at der foretages tilstrækkelig opfølgning på log fra kritiske systemer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der anvendes et centralt overvågningsværktøj, der afgiver alarmer, hvis kendte fejl opstår. Om muligt overvåges for, om en fejl er ved at opstå for at kunne handle proaktivt. Alarmer sker igennem en overvågningsskærm, der er monteret i projekt- og driftsafdelingen. Kritiske alarmer afgives også pr. mail og sms. Der indmeldes statusrapporter pr. mail fra forskellige systemer. Nogle dagligt – andre når der opstår en hændelse i systemet. Driftsvagten har til ansvar dagligt at kontrollere disse mails.	Vi har: • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • påset, at der anvendes overvågningsværktøj, samt at dette er tilgængeligt for samtlige medarbejdere. • påset, at der afgives alarmer pr. mail og sms ved opståede fejl. • gennemgået statusrapporter. • påset, at der er etableret en driftsvagt, samt at denne tjekker rapporter dagligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Styring af driftssoftware

At sikre, at der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Ændringer til driftsmiljøet følger de fastlagte procedurer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i IST ApS. Vi har ved stikprøvevis inspektion påset, • at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til IST ApS' produktionsmiljøer. • at ændringer til produktionsmiljøet i IST ApS følger de gældende retningslinjer, herunder at registreringer og dokumentation af ændringsanmodninger foretages korrekt. Vi har stikprøvevist inspiceret, at styresystemerne er opdateret efter gældende procedurer, samt at status herpå registreres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ændringer i eksisterende brugersystemer og driftsmiljøer følger formaliserede forretningsgange og processer.	Vi har forespurgt ledelsen, om der er etableret procedurer for patch management i IST ApS. Vi har ved stikprøvevis inspektion påset, at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til produktionsmiljøerne, herunder at krav til patch management kontroller sikrer: • at der sker registrering og beskrivelse af ændringsanmodninger • at ændringer er underlagt formelle konsekvensvurderinger • at der beskrives fall-back planer • at der sker identifikation af systemer, der påvirkes af ændringer • at dokumentationen opdateres, så den i al væsentlighed afspejler de påførte ændringer • at procedurer er underlagt styring og koordination i et "change board".	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og transmitterede data.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • at der er etableret et ansvar for procedurer for styring af netværksudstyr • at der er etableret funktionsadskillelse omkring centrale roller • at der er procedurer og ansvar for styring af netværksudstyr inkl. fjernarbejdspladser • at de fornødne lognings- og overvågningsprocedurer er etableret • at styringen af virksomhedens netværk er koordineret for at sikre en optimal udnyttelse og et sammenhængende sikkerhedsniveau.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal være etableret passende forretningsgange for håndtering af trusler i form af angreb fra internettet (cyber-angreb). I tilknytning hertil skal der være udarbejdet værktøjer til håndtering af beredskabet i tilfælde af cyber-angreb.	Det er kontrolleret, at der er er implementeret et passende antal forretningsgange samt tilhørende beredskabsplaner i forhold til håndtering af trusler i forbindelser med cyber-angreb. Vi har ved stikprøvevis inspektion påset: • at der er udarbejdet passende rammer for håndtering af cyber-angreb. • at der er udarbejdet og implementeret planer for håndtering af truslen. • at planerne har et tværorganisatorisk samarbejde mellem interne grupper.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 14:

(Anskaffelse), udvikling og vedligeholdelse af systemer

Sikre, at SaaS løsninger er håndteret med en passende it-sikkerhed, herunder en passende funktionsadskillelse mellem produktionsmiljøet og udviklingsmiljø.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
IST ApS har tilrettelagt systemudvikling og vedligeholdelsesaktiviteter baseret på egenudviklet projektmodel. Udviklingsorganisationen er opbygget med en central styregruppe, som har ansvaret for udformning af passende forretningsgange samt tilhørende ledelseskontroller. Alle ændringer, som skal idriftsættes i produktionsmiljøet, skal være godkendt af udviklingsgruppen for de enkelte SaaS løsninger. Softwareudvikling skal være placeret på selvstændige testmiljøer.	Vi har: • forespurgt ledelsen om, der er udarbejdet *eller* der findes en overordnet kvalitetsstyringsmodel for håndteringen af softwareudvikling. • i forbindelse med revisionen er det kontrolleret, at der findes procedurer og forretningsgange for udrulning af software-ændringer. Brugerstyringen sikrer, at der er en passende kontrol i forbindelse med håndteringen af den logiske adgangskontrol. Vi har kontrolleret, at medlemmer af de forskellige brugergrupper udfører periodevis kontrol. Vi har stikprøvevis kontrolleret at alle brugeraktiviteter bliver registeret og logget i central database. Logdatabasen bliver regelmæssigt gennemgået af den it-sikkerhedsansvarlige. Vi har kontrolleret, at der findes procedurer for adskillelse mellem produktionsmiljøet og miljøet for udvikling og vedligeholdelse. I forbindelse med vores revision har vi kontrolleret, at der findes adskilte testmiljøer til brug for softwareudviklingen. Stikprøvevis er det testet, at produktionsmiljøet for softwareudvikling sker fra et selvstændigt IP-segment.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
IST ApS' kontroller	**Revisors test af kontroller**	**Resultat af test**
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har stikprøvevist inspiceret, at samarbejdsaftaler med eksterne leverandører overholder kravene omkring afdækning af relevante sikkerhedsforhold i forhold til den enkelte aftale.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ved ændringer, der påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden. Der anvendes udelukkende anerkendte leverandører.	Vi har forespurgt ledelsen om relevante procedurer, som udføres ifm. udvælgelse af eksterne samarbejdspartnere. Vi har påset, at der er etableret passende procedurer for håndtering af samarbejdet med eksterne leverandører. Vi har gennem kontrol testet, at centrale leverandører har opdaterede og godkendte kontrakter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der skal udføres regelmæssig overvågning, herunder føres tilsyn med eksterne samarbejdspartnere.	Vi har påset, at findes passende processer og procedurer for løbende overvågning af eksterne leverandører. Vi har kontrolleret, at der udføres løbende tilsyn gennem uafhængig revisors rapporter.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

At opnå, at sikkerhedshændelser og svagheder i virksomhedens informationsbehandlingssystemer rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Sikkerhedshændelser rapporteres til ledelsen hurtigst muligt, og håndteringen sker på en ensartet og effektiv måde.	Vi har forespurgt ledelsen, om der er etableret procedurer for rapportering af sikkerhedshændelser. Vi har kontrolleret, at der er udarbejdet procedurer og forretningsgange for rapportering og behandling af sikkerhedshændelser, samt at rapporteringen tilgår rette steder i organisationen jf. retningslinjer. Vi har kontrolleret, at ansvaret for håndteringen af kritiske hændelser er klart placeret, og at de tilhørende forretningsgange sikrer, at der sker en hurtig, effektiv og metodisk håndtering af brud på sikkerheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Beredskabsstyring skal modvirke afbrydelser i virksomhedens forretningsaktiviteter, beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe samt sikre hurtig reetablering.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt for at fastlægge prioriteringen af afprøvning og vedligeholdelse.	Vi har forespurgt ledelsen, om der er udarbejdet beredskabsstyring for SaaS løsninger i IST ApS. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for udarbejdelse af beredskabsstyring. • at der er udarbejdet og implementeret beredskabsplaner. • at planerne har en tværorganisatorisk beredskabsstyring. • at planerne indeholder passende strategi og procedurer for kommunikation med IST ApS' interessenter. • at beredskabsplaner afprøves på regelmæssig basis. • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen.	Vi har ikke ved vores test konstateret væsentlige afvigelser

KONTROLMÅL 18:

Overensstemmelse med rolle som databehandler

Principper for behandling af personoplysninger:

Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med aftale.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der er fastlagt en ensartet ramme i form af standardkontrakter, Service Level Agreement samt databehandleraftale el.lign., som indeholder oversigt over, på hvilket grundlag behandling af personoplysninger foretages.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, og at procedurerne indeholder krav til lovlig behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der udføres alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har kontrolleret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks fra dataansvarlig. Vi har kontrolleret, ved en stikprøve på et passende antal behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsen underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har kontrolleret, at ledelsen sikrer, at behandling bliver gennemgået. Vi har kontrolleret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har kontrolleret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har kontrolleret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Databehandling:

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har kontrolleret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser
Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har kontrolleret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har kontrolleret, ved en passende stikprøvepopulation på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Vi har ikke ved vores test konstateret væsentlige afvigelser
Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har kontrolleret, at procedurerne er opdateret. Vi har kontrolleret via stikprøver om der i forbindelse med databehandlinger findes underliggende dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Vi har ikke ved vores test konstateret væsentlige afvigelser

Databehandlerens ansvar:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger medvirker til en betryggende behandlingssikkerhed.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har kontrolleret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren anvender til behandling af personoplysninger udelukkende underdatabehandlere, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på 3 underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere skal dette godkendes af den dataansvarlige.	Vi har kontrolleret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har kontrolleret, at der foreligger underskrevne underdatabehandleraftaler med alle de anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på 3 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • **Navn** • **CVR-nr.** • **Adresse** • **Beskrivelse af behandlingen**	**Vi har kontrolleret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.** **Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**

Bistå den dataansvarlige:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. **Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.**	**Vi har kontrolleret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder.** **Inspiceret, at procedurerne er opdateret.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**
Databehandleren har etableret procedurer, som i det omfang, at dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	**Vi har kontrolleret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for:** • **Udlevering af oplysninger** • **Rettelse af oplysninger** • **Sletning af oplysninger** • **Begrænsning af behandling af personoplysninger** • **Oplysning om behandling af personoplysninger til den registrerede.** **Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.**	**Vi har ikke ved vores test konstateret væsentlige afvigelser.**

Fortegnelse over behandlingsaktiviteter: Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over den behandling af personoplysninger, som er under databehandlerens ansvar.		
Der skal foreligge en fortegnelse over behandlingsaktiviteterne for den enkelte SaaS løsning kombineret med en tilhørende dataansvarlig.	Vi har kontrolleret dokumentationen for, at der foreligger en fortegnelse over behandlingsaktiviteterne for den enkelte SaaS løsning sammenstillet med en dataansvarlig.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der foretages løbende – og mindst en gang årligt – vurdering af, hvorvidt fortegnelsen er opdateret og korrekt.	Vi har kontrolleret dokumentationen for, at fortegnelsen over behandlingsaktiviteterne for den enkelte dataansvarlige er opdateret og korrekt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden: Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.		
Der foreligger skriftlige procedurer, som opdateres mindst en gang årligt, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet.	Vi har kontrolleret, at der foreligger opdaterede skriftlige procedurer for håndtering af brud på persondatasikkerheden, herunder at rettidig kommunikation til den dataansvarlige er beskrevet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Databehandler sikrer registrering af alle brud på persondatasikkerheden.	Vi har kontrolleret dokumentationen for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Vi har kontrolleret dokumentationen for, at ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige, herunder brud på persondatasikkerheden hos databehandlere, der er anvendt som underleverandører.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Databeskyttelsesrådgiver:

Der efterleves procedurer og kontroller, som sikrer, at der - i de tilfælde hvor det er krævet - er udpeget en databeskyttelsesrådgiver, som opfylder krav om tilstrækkelig kompetence, og som er anmeldt til tilsynsmyndigheden.

IST ApS' kontroller	Revisors test af kontroller	Resultat af test
Databehandler har udpeget en databeskyttelsesrådgiver som lever op til krav om tilstrækkelig kompetence.	Vi har kontrolleret dokumentationen for databehandlerens vurdering af, hvorvidt der skal udpeges en databeskyttelsesrådgiver eller ej.	Vi har ikke ved vores test konstateret væsentlige afvigelser
Kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.	Vi har kontrolleret dokumentationen for, at kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Kontaktoplysninger på databeskyttelsesrådgiveren er meddelt tilsynsmyndigheden.	Vi har kontrolleret dokumentationen for, at kontaktoplysninger på databeskyttelsesrådgiveren er meddelt tilsynsmyndigheden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsen har behandlet og godkendt udpegningen af databeskyttelsesrådgiveren.	Vi har kontrolleret dokumentationen for ledelsens behandling og godkendelse af udpegningen af databeskyttelsesrådgiveren, herunder sikring af databeskyttelsesrådgiverens kompetencer.	Vi har ikke ved vores test konstateret væsentlige afvigelser.