ISAE 3402 TYPE 2-ERKLÆRING FOR PERIODEN 1. DECEMBER 2017 TIL 30. NOVEMBER 2018 OM BESKRIVELSEN AF KONTROLLER, DERES UDFORMNING OG FUNKTIONALITET I TILKNYTNING TIL DRIFTEN AF IT-HOSTINGMILJØET

HOSTINGKOMPAGNIET A/S

BDO

INDHOLD

REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ERKLÆRING MED SIKKERHED OM BESKRIVELSEN AF KONTROLLER, DERES UDFORMNING OG FUNKTIONALITET I TILKNYTNING TIL DRIFTEN AF IT-HOSTINGMILJØET

Til: Ledelsen i Hostingkompagniet A/S
Hostingkompagniet A/S' kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Hostingkompagniet A/S' (serviceleverandøren) beskrivelse på side 5 - 22 i tilknytning til driften af IT-hostingmiljøet og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandørens ansvar

På side 4 i nærværende rapport har serviceleverandøren afgivet en udtalelse om egnetheden af den samlede præsentation af beskrivelsen samt hensigtsmæssigheden og funktionaliteten af de udformede kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandøren er ansvarlig for udarbejdelsen af beskrivelsen og udtalelsen, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret. Serviceleverandøren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom serviceleverandøren er ansvarlig for at anføre kontrolmålene og identificere de risici, som truer opnåelsen af kontrolmålene, samt udforme og implementere effektivt fungerende kontroller for at nå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA'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 serviceleverandørens beskrivelse samt om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som 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 International Auditing and Assurance Standards Board. 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 samt udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet 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 af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet på side 4.

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

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i serviceleverandørens udtalelse på side 4. Det er vores opfattelse:

a. at beskrivelsen af kontroller i tilknytning til driften af IT-hostingmiljøet, således som disse var udformet og implementeret i hele perioden fra 1. december 2017 til 30. november 2018, i alle væsentlige henseender er retvisende, og

b. at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. december 2017 til 30. november 2018, 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 fra 1. december 2017 til 30. november 2018.

Beskrivelse af test af kontroller

De specifikke kontroller, der er blevet testet, og resultater af disse test fremgår på side 24-41.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt serviceleverandørens kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, ved opnåelsen af en forståelse af kundernes informationssystemer, der er relevante for regnskabsaflæggelsen.

København, den 7. januar 2019

Per Sloth
Partner, chef for Risk Assurance
Registreret revisor

HOSTINGKOMPAGNIET A/S' UDTALELSE

Hostingkompagniet A/S har udarbejdet den medfølgende beskrivelse af kontroller i tilknytning til driften af it-hostingmiljøet. Beskrivelsen er udarbejdet til brug for vores kunder 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 ved vurdering af risiciene for væsentlig fejlinformation i regnskabet.

Hostingkompagniet A/S bekræfter, at den medfølgende beskrivelse, på side 5-22, giver en retvisende beskrivelse af kontroller i tilknytning til driften af it-hostingmiljøet i hele perioden fra 1. december 2017 til 30. november 2018. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

1. redegør for, hvordan driften af it-hostingmiljøet og de tilhørende kontroller var udformet og implementeret, herunder redegør for:
   - de typer af ydelser, der er leveret,
   - de processer i driften af it-hostingmiljøet, der omfatter sikkerhed, drift og vedligeholdelse af infrastruktur, servere og netværk,
   - relevante kontrolmål og kontroller udformet til at nå disse mål, og
   - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, kontrolaktiviteter og overvågningskontroller, som har været relevante for driften af it-hostingmiljøet.
   - 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.
2. indeholder relevante oplysninger om ændringer i forbindelse med driften af it-hostingmiljøet og tilhørende kontroller foretaget i perioden fra 1. december 2017 til 30. november 2018,
3. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontrolmål under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer, og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

Hostingkompagniet A/S bekræfter, at kontrollerne, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, er hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. december 2017 til 30. november 2018. Kriterierne for 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 anvendt 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. december 2017 til 30. november 2018.

København, den 28. december 2018

Hostingkompagniet A/S

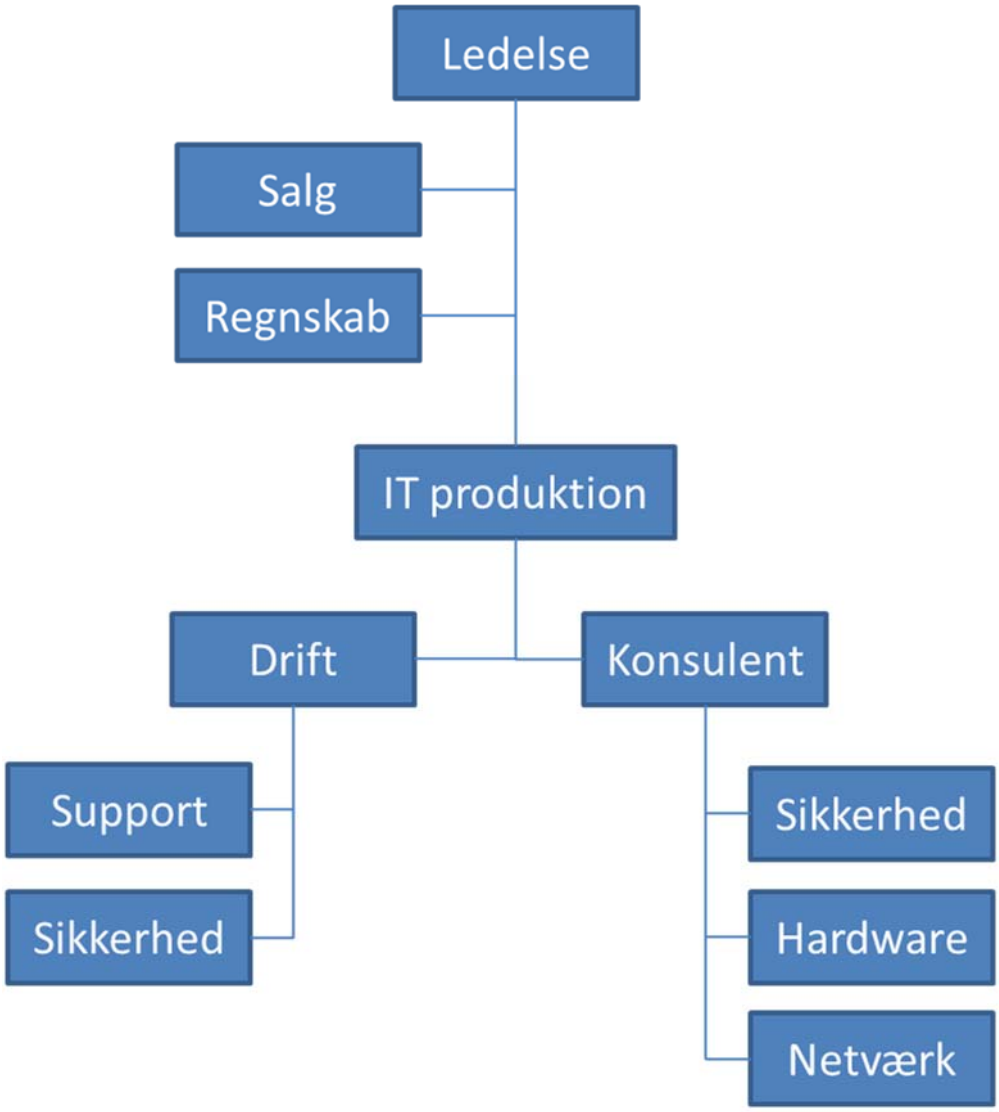
Peter Grunnet
Administrerende direktør

HOSTINGKOMPAGNIET A/S' BESKRIVELSE

Indledning

Hostingkompagniet A/S leverer professionelle it-løsninger med fokus på kvalitet, fleksibilitet og sikkerhed. Deres vigtigste opgave er at sikre, at it-driften kører så optimalt som muligt hos de over 200 virksomheder, der har outsourcet deres it-drift til Hostingkompagniet.

Hostingkompagniet organisation ser således ud:



Vores mål er at levere totale it-løsninger til små og mellemstore virksomheder hovedsagelig i Danmark. Det vil sige at vi tager ansvaret for hele it-paletten hos vores kunder, således at virksomhederne kun behøver at ringe ét sted hen. Vi tager dermed også dialogen med virksomhedens øvrige it-leverandører, så som ERP leverandøren eller datalinje leverandøren.

Hostingkompagniets leverance er typisk et hostet server-miljø med tilhørende lokal support til brugerne.

Der er i perioden fra 1. december 2017 til 30. november 2018 ikke foretaget væsentlige ændringer i driften af it-hostingmiljøet eller i de tilhørende kontroller.

1. IT-sikkerhedspolitik

Formålet med denne beskrivelse af informationssikkerheden i Hostingkompagniet er flere:

- Skabe et grundlag for Hostingkompagniets sikkerhedsmålsætning med henblik på udvikling, implementering, indførelse og effektiv styring af sikkerhedsmæssige kontroller, forholdsregler og sikringsforanstaltninger.
- Være generel referenceramme for sikkerheden i Hostingkompagniet hos både interne og eksterne brugere.
- Skabe grundlag for tillid til Hostingkompagniets informationsbehandling både internt og eksternt.
- Være referenceramme ved anskaffelse og kontrahering af informationsteknologiske produkter og tjenesteydelser.
- Danne baggrund for ISAE 3402 type 2 revisorerklæring.

Dette dokument udgør således den overordnede ramme for informationssikkerheden hos Hostingkompagniet og understøtter Hostingkompagniets værdigrundlag, samt den implementerede IT-sikkerhedspolitik, der er beskrevet (og bekræftet med underskrift fra alle medarbejdere) i Hostingkompagniets IT-sikkerhedshåndbog:

- Hostingkompagniet er en serviceorganisation, hvis primære formål er at overtage it-driften af små og mellemstore virksomheders it-installationer - enten ved at give adgang til servere i Hostingkompagniets center, eller ved en facility management aftale, hvor minimum én server bliver stående hos kunden.
- Hostingkompagniet ønsker at levere service der er ud over det forventede for den enkelte bruger. Hostingkompagniet ønsker en hurtig reaktionstid på kundeforespørgsler, således at myter omkring besværlige it-afdelinger, er usande når man har Hostingkompagniet som it leverandør.
- Hostingkompagniet ønsker at være en god og attraktiv arbejdsplads, som kan tiltrække højt kvalificeret medarbejdere.

Hostingkompagniets informationssikkerhedsindsats består af fire dele:

1. **Information sikkerhedsstrategi**. Beskriver de overordnede formål og principper for Hostingkompagniets arbejde med informationssikkerhed og er placeret som afsnit 2 i dette dokument.

2. **Risikovurdering**. Ved drift af IT er der altid en mængde risici der skal forsøges minimeret. Hostingkompagniets ledelse vurder hvilke elementer i driften der udgør en risiko. Disse listes og for hvert enkelt element vurderes risikoen, sandsynlighed for udfald og forebyggende aktiviteter for at mindske den samlede risiko.
3. **Informationssikkerhedspolitik**. Beskriver vores politik på de forskellige områder samt hvordan vi arbejder med at efterleve denne politik. Beskrevet i IT-sikkerhedshåndbogen.
4. **Dokumenterede procedurer**: Det nederste lag i Hostingkompagniets informationssikkerhedsindsats består af de faktiske procedurer eller processer, som vores medarbejdere arbejder efter i det daglige. Disse procedurer er dokumenteret i en række dokumenter, og der henvises i de enkelte afsnit af informationssikkerhedspolitikken til de procedurer, som er relevante for det pågældende område. Desuden er alle de dokumenterede procedurer samlet i ***procedure for IT-sikkerhedsstyring. U:\Certificering\Certificering2017\5.1 IT-Sikkerhedsstyrring (PG)***

Dette dokument er godkendt af Hostingkompagniets CEO og bestyrelse:

- Første gang i marts 2013.
- Senest 25-11-2018.
- Næste godkendelse: dec. 2019.

Som et led i den overordnede sikkerhedsstyring tager ledelsen på grundlag af den løbende overvågning og rapportering informationssikkerhedsindsatsen op til revurdering mindst én gang om året, i december måned.

2. Informationssikkerhedsstrategi

Data er på mange måder et vigtigt forretningsaktiv for Hostingkompagniet, hvad enten der er tale om vores egne eller vores kunders data. Derfor skal data beskyttes mod trusler, for at sikre, at vores og vores kunders forretning kan køre kontinuerligt. Formålet med denne informationssikkerhedsstrategi er at skabe rammen for de underliggende politikker og procedurer, som vil beskytte Hostingkompagniets data samt mindske effekten af sikkerhedshændelser.

Formålet med Hostingkompagniets informationssikkerhedsindsats er at beskytte data og informationsaktiver I vores varetægt mod enhver trussel, hvad enten truslen er intern eller ekstern, forsætlig eller uforsætlig.

Informationssikkerhedsindsatsen skal sikre den fysiske sikkerhed og omfatter alle former for informationssikkerhed, som f.eks. data, som gemmes på computere, overføres via netværk, trykkes eller skrives på papir, lagres på bånd, disk og disketter eller ytres mundtligt i samtale eller over telefonen.

Det er Hostingkompagniets ledelsesansvar at implementere informationssikkerhedsstrategien, herunder at de afledte politikker og procedurer overholdes af medarbejderne.

Det er Hostingkompagniets medarbejderes ansvar at overholde informationssikkerhedspolitikken og informationsprocedurerne. Det vil blive betragtet som misligholdelse af arbejdsforholdet, hvis det ikke sker, og som sådan underlagt de gældende arbejdsretlige regler.

Følgende principper ligger til grund for Hostingkompagniets informationssikkerhedsindsats:

- Data beskyttes mod uautoriseret adgang
- Data fortrolighed er sikret
- Dataintegritet opretholdes
- Juridiske krav angående IPR (Intellectual Property Rights), data beskyttelse og beskyttelse af persondata overholdes
- Beredskabsplaner udarbejdes, vedligeholdes og testes
- Medarbejderne modtager tilstrækkelig oplæring og uddannelse i informationssikkerhed
- Der indarbejdes procedure for overholdelse af persondataforordningen, som træder i kraft 25. maj 2018.
- Alle brud eller mistænker om brud på informationssikkerheden registreres og undersøges

3. Organisering af informationssikkerhed

Det er Hostingkompagniets politik til enhver tid at have en intern organisationsstruktur, der understøtter en effektiv indsats for at øge informationssikkerheden, samt at de samme principper kan gøres gældende i eksterne samarbejder.

Interne organisatoriske forhold
Hostingkompagniets ledelse er ansvarlig for:

- at designe it-sikkerhedssystemet
- at den enkelte medarbejder kender systemet og sin egen rolle i det
- at it-sikkerhedssystemets forskellige dele opdateres som angivet

Alle medarbejdere i Hostingkompagniet er ansvarlige for at overholde gældende procedurer og på anden vis gøre hvad de kan, for at hensigten i Hostingkompagniets informationssikkerhedspolitik tilgodeses. I praksis koordineres indsatsen af den tekniske direktør, som også har ansvaret for den daglige styring, jf. nedenfor.

Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen er placeret hos den tekniske chef – (25/11-2018 Lars Svava).

Desuden er ansvarsplaceringen beskrevet i de forskellige procedurer.

Godkendelsesprocedure ved anskaffelser af driftsmidler
Hostingkompagniet har en procedure, som beskriver processen ved interne anskaffelser af en genstand (software eller hardware) med en købsværdi på mere end 2.000 kr. Formålet med proceduren er at sikre, at nyanskaffelser er både forretningsmæssigt og informationssikkerhedsmæssigt fornuftige. (Proceduren gælder ikke køb til/for kunder)
Ved anskaffelser udfyldes formular ”Ansøgning om indkøb”. Formularen godkendes af den ansvarlige direktør for området (25/11-2018 Peter Grunnet). Når anskaffelsen er godkendt/afvist sendes der en besked til medarbejderen der har udfyldt formularen.

For Informationssikkerheden, er det primære indhold af proceduren følgende:

- Der laves en skriftlig indstilling eller forslag til anskaffelse. Indstillingen skal som minimum indeholde
  - Beskrivelse af anskaffelsen (funktion, mærke osv.)
  - Pris på anskaffelsen
  - Erstatning eller nyindkøb
  - Påvirkning af informationssikkerheden ved at købe, hhv. ikke at købe

Indstillingen laves af medarbejdere eller ledelse. Det er Hostingkompagniets CEO, der træffer beslutning om alle anskaffelser over 10.000 kr. Den tekniske chef kan træffe beslutninger om anskaffelser op til 10.000 kr.

Eksterne samarbejdspartnere
Det er Hostingkompagniets politik at gennemføre en risikovurdering samt at identificere og implementere relevante sikringsforanstaltninger, før der indledes eksterne samarbejder.

Partnere:

Hostingkompagniet samarbejder med forskellige partnere, som hver har sine samarbejdsaftaler med Hostingkompagniet. Nedenfor er beskrevet den overordnede struktur i samarbejdsforholdene.

Zitcom
Zitcom er infrastruktur partner til Hostingkompagniet. Det vil sige, at hele den infrastruktur som drifter Hostingkompagniets kunder afvikles på Zitcoms infrastruktur i Skanderborg.
Zitcom har selv en ISAE 3402 type 2 erklæring for deres hosting faciliteter, samt ISO 27001 certificering.

Dynamic Networks
DN er Hostingkompagniets partner på C5 hosting. DN består af 40 til 45 individuelle C5 konsulenthuse, som alle kan benytte Hostingkompagniets hostingfaciliteter til C5 hosting. DN har en lokal administrator adgang til de servere som alene drifter C5 kunder solgt gennem DN. Der findes en oversigt (log) over hvilke kunder / databaser der administreres af DN.

Diverse ERP-leverandører (udpeget af den enkelte kunde)
Kunder der har deres eget ERP-systemet, som de ønsker hostet på Hostingkompagniet infrastruktur, har ofte et behov for at Hostingkompagniet samarbejder med det pågældende ERP-hus. Det vil sige, at det er nødvendigt at der udveksles fortrolige informationer og at der i kortere perioder er behov for at denne leverandører får adgang til Hostingkompagniets infrastruktur, mere end blot via en almindelige brugeradgang. Dette administreres ved at hvis kundeserveren er dedikeret til kunden, udleveres lokal administrator rettigheder. Hvis det sker på en delt server, vil adgangen blive overvåget af en medarbejder fra Hostingkompagniet ofte via Teamviewer.

Microsoft / Crayon
Microsoft er Hostingkompagniet primære leverandør på software siden. Hostingkompagniet har en leje aftale med Microsoft, der giver adgang til at leje Microsoft licenser til slutkunder (CSP)
Crayon er distributør af Microsoft software til Hostingkompagniet.

Samarbejdsaftaler
Når Hostingkompagniet indgår et formaliseret eksternt samarbejde, er samarbejdet baseret på en samarbejdsaftale, som sikrer, at Hostingkompagniets sikkerhedsmålsætning ikke kompromitteres.

4. Sikkerhed ved installation og drift

Det er Hostingkompagniets politik at sikre, at alle ændringer og nye installationer ikke påvirker de eksisterende kundeforhold; dette er meget vigtigt, da Hostingkompagniet arbejder med delt miljø mellem kunder.

Ved installation af nye servere vil selve installationen ske i et lukket miljø, hvor der ikke er forbindelse for øvrige brugere ud over Hostingkompagniets interne medarbejdere.
Når et miljø er klar til overdragelse til en kunde, vil der altid blive logget ind på en af profilerne, og det testes at rettigheder er som beskrevet, og at funktioner kan tilgås som beskrevet. Dette er beskrevet i proceduren for oprettelse af Windows server.

Miljøet klarmeldes ved at kunden oprettes i virksomhedsportalen, og der skrives en ny ”case” der beskriver præcis hvad der er leveret til kunden. Samtidig sendes der en mail til kunden med kopi til den ansvarlige for området hos Hostingkompagniet om at miljøet er klart, og hvordan der kan logges ind på systemet. Dette er beskrevet i proceduren: ”Oprettelse af kundemiljø”.

Serveren vil ikke blive frigivet til produktionsmiljøet, før der er installeret anti-virus software på serveren, og funktionaliteten af serveren er testet.

Testresultatet dokumenteres i en kunde-fil der findes i hver kundes kundefolder (”oprettelse af kundemiljø – formular”):

Antivirus software bliver opdateret online fra producenten af softwaren (Microsoft End Point Protection). Antivirus softwaren fungerer således, at alle filer der åbnes eller downloades til serveren bliver scannet for virus, inden den pågældende kommando gennemføres. Dette giver noget overhead på serverens performance, men er en funktion, som Hostingkompagniet har anset for nødvendig for at undgå indtrængen af ondsindede vira.

Overvågning af driften
Der installeres overvågning på alle servere inden de overføres til drift via Vmware. Overvågningen er en klient der konstant overvåger tilstanden af serveren. Overvågningen fortæller om alle jobs og services på serveren afvikles tilfredsstillende. Derudover er alle fysiske servere konfigureret med SNMP overvågning, således at supporten i Hostingkompagniet får meddelelser fra systemet, hvis en service ikke køre, eller en disk er ved at løbe fuld m.m.
Overvågningen indeholder også en log over, hvornår en server har været lukket ned, eller andre vitale faktorer for en server. Det er den driftsansvarliges job at følge op på hændelser der kræver umiddelbar indgriben, hver morgen inden kl. 8.00. Dette er beskrevet i proceduren ”Overvågning”.

Backup software (Veeam, Tivoli Storage Manager)
Inden en server sættes i drift, bliver der installeret backup software. Standardrutinen for backup er, at der tages en fuld kopi af alle data ved opstart og at der derefter tages backup af alt data,

som ændres. Der gemmes flere versioner af det samme data, såfremt data ændres inden for de seneste 14 dage. Såfremt en kunde ønsker det, kan perioden på 14 dage sættes op eller ned.

Alle backup data bliver gemt på file niveau. Der tages også image backup så en server kan re-etableres fra nattens backup i løbet få timer.

Hvis et backupjob ikke er kørt eller det er gået ned under kørsel, vil der komme en besked til den backup ansvarlige. Når der modtages en besked om unormal kørsel af backup jobs, vil medarbejderen følge den backup procedure der er beskrevet vedrørende afvikling og overvågning af backup jobs.

Hvis der er problemer med gennemførsel af den natlige backup vil dette blive registreret af den backupansvarlige. Såfremt problemet ikke direkte kan løses ville dette blive eskaleret til den driftsansvarlige Lars Svava. Dette indføres i backup loggen, og der beskrives aktions hvis der skal ske noget i forbindelse med alerts fra backuppen.

Firewall
Alle servere står bag en fysisk firewall. Firewallens funktion er at holde uønskede brugere / angreb væk fra det interne it-miljø.
Firewallen styres af Hostingkompagniets med support fra Zitcom (Firewallen findes fysisk hos Zitcom som hostet firewall). Der lukkes kun op for porte i firewallen, såfremt det kan dokumenteres, at der er behov for dette. Som udgangspunkt er alle porte lukkede.
Det er standard at Windows firewall er slået til på alle servere.
Administration af firewallen er beskrevet i ”procedure ændringer i firewall”.

Styring af driftsrelaterede aktiver
Det er Hostingkompagniets politik, at der til enhver tid er korrekt overblik over firmaets driftsrelaterede aktiver, hvor der også redegøres for, hvert enkelt aktiv, samt hvilke ressourcer der er knyttet til det enkelte aktiv. Skemaet opdateres efter behov, dog minimum hver gang der installeret et nyt aktiv.

De væsentlige informationsrelaterede aktiver i Hostingkompagniet indeholder følgende datatyper:

1. Hostingkompagniets egne data som i alt overvejende grad er flade officepakke-filer plus indholdet af medarbejdernes mailbokse på nogle Exchange-servere.
2. Hostingkompagniets egen elektroniske infrastruktur (exchange server setup, SQL server setup, domæne-setup, web server setup, officepakke setup og øvrige applikationer).
3. Hostingkompagniets kunders data som består af SQL databaser, Exchange server data, billeddata, flade officepakkefiler mm.
4. Hostingkompagniets kunders elektroniske infrastruktur (exchange server setup, SQL server setup, domæne-setup, web server setup, officepakke setup og øvrige applikationer).

De ovennævnte typer informationsrelaterede aktiver sikres alle med hensyn til

- **Tilgængelighed** ved at samtlige data ligger på servere med spejlede diske. For data på Exchange 2016 server sikres tilgængeligheden også ved at der er oprettet et cluster med en redundant server som kan tage over hvis den ene mailboksserver skulle fejle eller skal vedligeholdes.
- **Integritet** ved at der hver nat tages fuld backup der lagres krypteret.

- **Fortrolighed** ved at der er opsat fil- og mapperettigheder, databaserettigheder og Active Directory-rettigheder som kun giver adgang til de som skal have adgang. For Exchange serverne er der lavet separate Exchange adresselister for hver eneste kunde og opsat på den enkelte brugerkonto hvem der skal have adgang til hvilke adresselister.

Sikring mod angreb på serverne håndteres ved at netværket kun er åbent for porte som kunderne har behov for adgang til samt ved at alle servere (med enkelte undtagelser, som håndteres manuelt) er sat til at hente sikkerhedsopdateringer fra Microsofts automatisk (alle servere kører Windows 2008 R2 eller nyere). Tredjepartsapplikationer opdateres manuelt med sikkerhedsrettelser med jævne mellemrum.

Det overordnede tekniske ansvar for de implementerede løsninger ligger hos ledelsen som udgøres af Lars Svava og Peter Grunnet

Styring af sikkerhedshændelser
Det er Hostingkompagniets politik at sikre, at svagheder og it-sikkerhedshændelser bliver rapporteret via overvågningssystemet, således at det er muligt at foretage rettidige og fornødne korrektioner.

Der er etableret en procedure, der sikrer, at it-sikkerhedshændelser bliver rapporteret til Hostingkompagniets ledelse hurtigst muligt. Denne procedure findes under ”overvågning”. Ledelsen vurderer, om der er tale om en reel it-sikkerhedshændelse og hvilke foranstaltninger der i givet fald skal iværksættes. Hostingkompagniets ledelse og medarbejdere diskuterer jævnligt det aktuelle it-trusselsbillede.

Alle it-sikkerhedshændelser der rapporteres via overvågningen, bliver dokumenteret. Hændelserne listes i loggen for hændelser, og der beskrives hvilke actions der etables for at afværge dem.

Beredskab
Det er Hostingkompagniets politik at sikre, at fejl eller incidents bliver registreret og udbedres med den hastighed, der svarer til fejlens karakter.

Fejl (incidents) kan blive registreret af Hostingkompagniet selv, eller de kan blive rapporteret af en eller flere kunder.

Der er åbent for indrapportering af fejl døgnet rundt på Hostingkompagniets vagttelefon og supportmailboks: support@hostingkompagniet.dk.

Når der meldes om en fejl fra en bruger, vil dette blive registreret i support systemet Freshdesk. Severity 1 til 4 vil ikke blive registreret med kode, men udelukkende blive registreret i Freshdesk ticket system. Fejl kan have forskellig karakter alt efter hvor alvorlig, fejlen er.

Beredskabet der træder i kraft er forskelligt alt efter hvilken karakter fejlen har:

- Ved server nedbrud (severity 5 og 6) vil fejlrettelsen gå i gang umiddelbart efter indrapporteringen, og blive rapporteret i dokumentet Severity hændelser U:\Certificering\Certificering2018\16.1 Styring af sikkerhedshændelser (LS).

- Ved severity 3 og 4 vil fejlrettelsen blive igangsat inden for de første 2 timer af normal arbejdsdag (hverdage kl. 8 til 16:30).
- Ved severity 1 og 2 vil fejlrettelsen blive påbegynde indenfor et døgn gældende fra først kommende hverdagsmorgen.

Kun fejl, der er indenfor Hostingkompagniet kontrol eller domæne, vil blive registreret med severity kode. Se proceduren: ” Problemhåndtering / fejlrapportering”

Mulige incident - og tilhørende beredskab

- Linie nedbrud - hos en kunde (uden for Hostingkompagniets kontrol)
- Linjenedbrud i hostingcenteret (severity 6)
- Server nedbrud (severity 6)
- Korrupt data hos en kunde (severity 5)
- Manglende adgang til server (severity 4)
- Glemt password (severity 2)
- Kan ikke printe (severity 2)

Logning og overvågning
Det er Hostingkompagniets politik, at alle it-systemer overvåges.

Alle systemer er konfigureret med en system-, application- og security log. Når der sker en hændelse bliver denne som hovedregel registeret i en eller flere af disse logs. Logfiler bliver ikke overvåget manuelt, men de benyttes såfremt overvågningen rapporterer en uregelmæssighed, som et værktøj til at finde årsagen til uregelmæssigheden.

Alle systemer henter deres tid fra den centrale domain controller, som er en præcis tidsangivelseskilde.

5. Medarbejdersikkerhed og udstyr

Det er Hostingkompagniets politik, at der er klare og formulerede sikkerhedsprocedurer for så vidt angår medarbejdere, både før ansættelse, under ansættelse og ved ansættelsens ophør, samt at disse procedurer understøtter vores overordnede informationssikkerhedsstrategi. Der ud over har Hostingkompagniet en fast politik omkring håndtering af brugernes rettigheder – både internt og eksternt – se brugerrettigheder i dette afsnit.

Før ansættelse
Ansættelse af nye medarbejdere foretages på baggrund af en præcis beskrivelse af medarbejderens tidligere udførte opgaver og ansvar til tilsvarende jobs. Derved sikres, at medarbejderen er kvalificeret til og interesseret i at varetage opgaverne, til gavn for både medarbejderen og Hostingkompagniet. Beskrivelsen af opgaver og ansvar indgår som bilag i medarbejderens ansættelseskontrakt. Denne procedure er iværksat pr. december 2012.
Inden der indgås aftale med en ansøger, efterprøver Hostingkompagniet, om ansøgeren har de nødvendige kvalifikationer. Det kan f.eks. ske ved at tage reference hos tidligere arbejdsgivere eller ved test. Resultatet af efterprøvningen vedlægges medarbejderens personalesag. Denne procedure er iværksat pr. december 2015.

Som bilag til ansættelseskontrakten udarbejdes og vedlægges:

- Beskrivelse af medarbejderens opgaver og ansvar
- Kopi af denne beskrivelse af informationssikkerheden i Hostingkompagniet
- Tavsheds- og fortrolighedserklæring. Ved ansættelse i Hostingkompagniet underskrives der en tavshedserklæring ved ansættelsen.
- Hostingkompagniets IT-sikkerhedspolitik for internet og e-mail: I IT sikkerhedshåndbogen er det beskrevet hvilken politik Hostingkompagniet har med hensyn til privat brug af firmaets Internet og firma e-mail adressen. Alle medarbejdere underskriver IT sikkerhedshåndbogen ved ansættelse.

I ansættelse kontrakten er det beskrevet hvilke aktiver medarbejderen får rådighed over som ansat i Hostingkompagniet, f.eks. mobiltelefon, Internettrafik og pc.

Alle dokumenter underskrives af medarbejderen som derved erklærer sig oplyst om og indforstået sine opgaver og ansvar. Ansættelseskontrakt inkl. bilag gemmes på medarbejderens personalesag. Denne procedure er etableret pr. 1/12 2012 og omfatter eksisterende og kommende medarbejdere.

Ansættelsesforholdet
I forbindelse med den årlige medarbejdersamtale tjekker den personaleansvarlige leder, om der har været ændringer i medarbejderens opgaver og ansvar, og i givet fald laves en opdateret beskrivelse. Ligeledes tjekker lederen, om der er foretaget ændringer i Hostingkompagniets beskrivelse af informationssikkerheden, og hvis det er tilfældet, gøres medarbejderen bekendt med ændringerne og deres evt. konsekvens. Alle opdaterede dokumenter underskrives og vedlægges medarbejderens personalesag samt udleveres til medarbejderen. Denne procedure er iværksat pr. 1/12 2012.
Hostingkompagniet ønsker, at alle medarbejdere til enhver tid er kvalificerede til at støtte op om firmaets målsætninger på it-sikkerhedsområdet. Derfor påhviler det såvel ledelsen som den enkelte medarbejder løbende at være opmærksom på, om dette er tilfældet og minimum en gang om året, ved medarbejdersamtalen, vurderer lederen og medarbejderen i fællesskab, om medarbejderen har behov for opkvalificering, i form af uddannelse, træning eller lignende. Denne procedure er iværksat pr 1/12 2012.

Hvis en medarbejder ikke lever op til sit ansvar som beskrevet i ansættelseskontrakt inkl. bilag, kan Hostingkompagniet iværksætte sanktioner mod medarbejderen, i henhold til den gældende lovgivning på området og som beskrevet i ansættelseskontrakten. Den fremgår af den enkelte personalesag, om der er iværksat sanktioner mod en medarbejder. Denne procedure er iværksat pr. 1/12 2012.

Ansættelsens ophør
Efter ansættelsens ophør gælder den tavshedserklæring, som medarbejderen har underskrevet, fortsat. Det betyder, at den nu tidligere medarbejder fortsat har tavshedspligt om forhold vedr. Hostingkompagniets og deres kunders forhold og data.
Når ansættelsen ophører, returnerer medarbejderen de aktiver, f.eks. mobiltelefon og pc, som er blevet udleveret som en del af ansættelsen, jf. listen over aktiver, som er bilag til ansættelseskontrakten.

Når ansættelsen ophører, inddrages den tidligere medarbejders rettigheder for så vidt angår adgang til systemer, data og fysiske lokationer.

Brugerrettigheder
Hvis medarbejderen tilhører teknisk afdeling, vil medarbejderen få udleveret to brugerkonti. En der benyttes i det daglige arbejde og kommunikation med kollegaer m.m., og en konto med domæne administrator adgang.
Der er dog to rettigheder medarbejderen ikke får – adgang til ledelsesdrevet og adgang til den "øverste" konto til domænet, der styre de øvrige administratorkonti.

6. Fysisk sikkerhed

Det er Hostingkompagniets politik at sikre, at virksomhedens fysiske udstyr er tilstrækkeligt sikret mod at lide skade, hvad enten det er tilsigtet eller utilsigtet. Denne politik er afspejlet i den måde, hvorpå vores lokationer er indrettet og udstyret er installeret, hvilket beskrives mere udførligt i de følgende afsnit.

Fysisk afgrænsning
Hostingkompagniet besidder kun en kontorlokation:

- Kontorfaciliteter Tuborgvej 5, 2900 Hellerup
- (Infrastruktur ligger hos Zitcom)

Der er udarbejdet en ISAE 3402 type 2 erklæring for Zitcom. Gældende perioden 1. januar til 31. december 2018. Denne findes som bilag 2.

Fysisk adgangskontrol
Kontor på Østerbro: Kontoret består af et stort lokale, hvor alle medarbejdere i Hostingkompagniet har deres faste arbejdspladser, samt flere fælles separate mødelokaler. Når man som gæst skal ind i bygningen på Tuborgvej 5, skal man ringe for at blive lukket ind. Al adgang til kontoret skal gennem konstant låste døre. Medarbejdere i Hostingkompagniet har alle fået udleveret en nøglebrik, således at man kan åbne de løste døre.

Sikring af kontorer, lokaler og udstyr
Kontor i Hellerup:
Kontoret er sikret som kontorfællesskab, med individuelle kontorer. Alle Hostingkompagniets digitale data gemmes på digitale medier, hvorfor der ikke findes fortroligt materiale på kontorlokationen.
Regnskabsbilag og printede kontrakter opbevares på kontoret, mens regnskaber mv. kun findes digitalt.
Primær hostinglokation hos Zitcom: Alle servere står i aflåste skabe og er beskyttede med adgangskode (password).

Beskyttelse af udstyr
Det er Hostingkompagniets politik at beskytte sit udstyr og derved undgå tab af, skader på eller kompromittering af vores informationsaktiver eller forstyrrelser af vores forretningsaktiviteter.

Placering af udstyr
Hostingkompagniets forretningskritiske udstyr er placeret i sikre områder hos Zitcom, jf. afsnittene ovenfor.

Forsyningssikkerhed (hos Zitcom):
Som it hoster er det helt afgørende, at servere o.l. kører så tæt på konstant som muligt. Derfor har Zitcom sørget for dobbelt forsyning af såvel internet som strøm:

Internet (hos Zitcom):
Hostingkompagniets servere er alle opstillet i det dedikeret område hos Zitcom, hvor Hostingkompagniets miljø er tilknyttet en redundant Internet forbindelse – det vil sige to forbindelser af hver 10 Gb. Der er automatisk fall-over fra den primære linje til en sekundære

Der er også redundant switche, således at Internet forbindelsen kan genetableres hurtigt, hvis en netværkskomponent holder op med at virke.

Strøm (hos Zitcom):
På hostinglokationen er der til hvert rack fremført både A og B strøm. Desuden er Hostingkompagniets underleverandør (Zitcom) forpligtet til at levere strøm såvel som nødstrøm (UPS/Dieselgenerator).
På den sekundære hostinglokation er der etableret nødstrøm (UPS) til minimum 4 timers drift
TDC-fiber (som også har netværksudstyr i server rummet)
Sikring af udstyr uden for virksomhedens overvågning
Medarbejdere kan tilgå Hostingkompagniets servere via bærbare pc'ere, som alle er sat op med krypteret password. Desuden opbevares al data centralt på serverne.
Sikker bortskaffelse eller genbrug af udstyr – se procedure beskrivelse af anskaffelse og bortskaffelse af udstyr.
Før Hostingkompagniet kasserer elektronisk udstyr, slettes al data fra udstyret. Dette er beskrevet i procedure: "Bortskaffelse".

7. Styring af brugerrettigheder

Det er Hostingkompagniets politik, at driftsafviklingen af virksomhedens informationssystemer til enhver tid er sikker, samt at ansvar og retningslinjer for styring og drift af virksomhedens informationssystemer er fastlagt.

Hostingkompagniet driftafvikler et fælles netværk således, at alle Hostingkompagniets kunder/it-brugere kan opnå hurtig og sikker adgang til systemer og data. Samtidig er der etableret sikkerhedsforanstaltninger således, at uvedkommende ikke kan opnå adgang til Hostingkompagniets it-systemer.

Ekstern serviceleverandør
I særlige tilfælde kan eksterne leverandører få adgang til Hostingkompagniets systemer og it-infrastruktur.

Når en ekstern bruger får adgang til en server, vil dette ske via et midlertidigt brugerlogin som vil blive nedlagt umiddelbart efter brug.

Såfremt adgang bliver giver til mere end det data der ejes af den kunde som den eksterne leverandør repræsenterer, vil adgangen kun blive givet under overvågning af en ledende medarbejder hos Hostingkompagniet.

For hver kunde registreres det hvem der er deres leverandør som skal have en form for adgang til kundens IT-system. Dette er dokumenteret i "oprettelse af ny kunde – formular".

Når kunder har dedikerede servere, vil det være muligt at få udleveret en lokal server administrationskonto. Sker det, vil den lovede SLA ikke være fuldt gældende, hvilket kunden også vil blive gjort opmærksom på.

Bliver der udleveret lokal administrator konti/password, bliver dette registreret i dokumentet på kunden over kundeoprettelsen.

Styring af driftsmiljøet
I Hostingkompagniet bliver alle systemer der er i drift overvåget 24 timer i døgnet 365 dage om året. Overvågningssystemet er samtidig med til at bestemme behovet for kapacitet, så Hostingkompagniet altid er på forkant med kapacitetsbehovet.

Overvågningssystemet er med til at sikre konsekvent og stabil drift.

Når overvågningen viser at der er uhensigtsmæssigheder i driften – en server der mangler kapacitet eller en server der ikke er tilgængelig, vil medarbejderen der er på vagt i supporten, tage action på denne alarm. Medarbejderen vil følge procedurerne der er beskrevet i procedureforskriften: "overvågning"

Skadevoldende programmer og mobil kode
Der er etableret registrering af system og dataanvendelse (logning) på alle servere som bliver gennemgået regelmæssigt. Ydermere er alle servere beskyttet med antivirus programmer.

Image backup
Der tages sikkerhedskopi af alle systemer og data. For hvert enkelt system bliver der taget stilling til frekvensen i forbindelse med sikkerhedskopiering. Der foretages jævnligt tests af sikkerhedskopierne. Proceduren for reetablering af data er beskrevet sådan at alle it-medarbejder i Hostingkompagniet kan udføre proceduren.

Der er udarbejdet beredskabsplan for følgende cases:

- Reetablering af kundemiljø, hvis en (fysisk) server skal erstattes (gået ned)
- Reetablering af en SQL server (virtuel)
- Reetablering af en Exchange server (virtuel)

Alle medarbejdere er orienteret og uddannet i hvordan man retablerer de forskellige IT miljøer i Hostingkompagniets samlede IT-miljø i henhold til beredskabsplanerne.

Netværkssikkerhed
Hostingkompagniets it-driftsafdeling har ansvaret for Hostingkompagniets overordnede it-infrastruktur. For alle netværksforbindelser og netværksenheder på OSI lag 1 har Hostingkompagniet A/S outsourcer driften til samarbejdspartneren Zitcom.

Adgangen fra eksterne netværk til Hostingkompagniet it-infrastruktur er beskyttet således at det kun er autoriserede brugere der kan opnå adgang. Adgangen til netværket er beskyttet af en Firewall som er under Hostingkompagniets A/S 's samarbejdspartner Zitcoms ansvar.

Databærende medier
Alle fysiske databærende medier i Hostingkompagniet er beskyttet ved at være anbragt i aflåst lokale. For at få adgang til online data afkræves et personligt password.

Alle databærende medier (diske) slettes med HP / Dell / IBM' værktøjer, inden de destrueres. Se procedure "bortanskaffelse".

Systemdokumentation er beskyttet ved dels at begrænse adgangsrettighed til Hostingkompagniets it-drifts afdeling, dels at anvende komplekse passwords.

Til sikker håndtering af passwords bruger Hostingkompagniet følgende to systemer: Virksomhedsportalen og Frechdesk. I begge systemer er data krypterer. Alle passwords og fortrolige informationer gemmes i en database hvortil der skal gives login/password for at få adgang. Proceduren for håndtering af passwords hedder " Adgang og password håndtering".

Informationsudveksling
Informationsudveksling (internet og e-mail) er et strategisk værktøj, som har til formål at sikre en fleksibel it-anvendelse for Hostingkompagniets brugere/kunder. Med henblik på at beskytte Hostingkompagniet og firmaets kunder mod skader forårsaget af brugen af e-mail og internet er der udarbejdet en skriftlig e-mail og internet politik.

Politikken for brug af IT og e-mails er beskrevet i proceduren for ansættelser.

8. Overensstemmelse med lovbestemte og kontraktlige krav

Det er Hostingkompagniets politik til enhver tid at honorere de krav som er gældende ifølge lovgivningen såvel som de krav, som Hostingkompagniet har forpligtet sig til at overholde via kontrakter.

I praksis betyder det bl.a.:

- Forpligtelser over for licenshavere af software, der benyttes af Hostingkompagniet både til eget brug og til udlejning til Hostingkompagniets kunder, skal til en hver tid opretholdes.
- Hostingkompagniet sikrer fortrolighed om egne og kundernes kritiske data.
- Hostingkompagniets og Hostingkompagniets kunders data skal beskyttes mod tab, ødelæggelse og forfalskning i overensstemmelse med lovgivningsmæssige og kontraktlige og forretningsbetingede krav.
- Alle kundedata klassificeres som forretningskritiske data, der skal beskyttes og sikres over for tredjepart, men samtidig skal det også sikres, at data kan tilgås i hele opbevaringsperioden, uanset systemmæssige eller teknologiske ændringer i tilhørende it-miljøer.

For at sikre ovenstående retningslinjer for håndtering af kritisk data har Hostingkompagniet implementeret Microsofts framework (retningslinjer) for adskillelse af data i et delt server miljø.

Alt data der gemmes i backuppen er krypteret, hvilket vil sige at såfremt backuppen bliver opsnappet eller stjålet af tredjepart, kan denne ikke læses.

Sikkerhed i forbindelse med systemrevision
Revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede for at minimere risikoen for forstyrrelser af Hostingkompagniets forretningsaktiviteter.
Følgende retningslinjer skal være etableret:

- Revisionskrav fra en hver kundes revision skal aftales med de relevante ledere og systemejere.
- Formålet med de planlagte revisionshandlinger skal aftales og følges op.
- De planlagte revisionshandlinger må kun omfatte læseadgang til systemer og data indenfor den specifikke kunde hvorom revisionskravet handler.
- De nødvendige ressourcer til at gennemføre de planlagte revisionshandlinger skal identificeres og stilles til rådighed. Der vil blive afregnet timebetaling for ressourceforbruget til gældende timetakst.
- Behovet for afvikling af særlige informationsbehandlingsopgaver skal identificeres og aftales.
- Al adgang i forbindelse med revisionen vil blive logget

Kundens egne kontroller og ansvar

Virksomheder der vælger at overlade driften af deres IT til Hostingkompagniet, vil igennem driftperioden få deres IT-driften efter procedurerne i denne ISAE 3402 type 2 erklæring. Der vil dog være punkter som kræver kundens egen kontrol, hvor ansvaret for korrekthed ligger hos kunden. Her kan nævnes:

- Ved restore af en backup bør kundens kontrollere at udgangspunktet efter restore er det samme som før restoren.
- Ansvaret for forretningssystemer og brugersystemer, som driftes af Hostingkompagniets hostingfunktion, er kundens eget ansvar. Kunden har ansvar for at udfører de nødvendige kontroller i forbindelse med anskaffelse, udvikling og ændringshåndtering.
- Såfremt kunden forlanger at få udleveret en lokal administratorkonto, med muligheder for installation og ændringer, er det kundens eget ansvar at kontrollere at de ændringer der foretages med denne administratorkonto ikke kompromitterer den øvrige drift.
- Det er kundens eget ansvar at egne datalinjer til det hostede miljø er funktionsdygtige og at transmissionen fungerer korrekt. Kunden er selv ansvarlig for de nødvendige kontroller i tilknytning til kontrolmålet.
- I henhold til Hostingkompagniets beredskabsstyring er beredskabet bygget op i henhold til den beskrevne beredskabsplan. Det er kundens eget ansvar orienterer sig om indholdet i beredskabsplanen og at deltage i den grad det er beskrevet i beredskabsplanen.

Kontrolmål og kontroller:

Kontrolmål	Kontrolaktiviteter
Område: It sikkerhedsstyring	
It-sikkerhedspolitik • At sikre, at der løbende sker en styring af IT-sikkerheden i Hostingkompagniet • At sikre, at IT-sikkerheden bliver implementeret og kommunikeret til alle interessenter • At sikre, at dokumentation af IT-sikkerheden bliver vedligeholdt og godkendt i hele organisationen.	• Hostingkompagniets ledelse foretager en årlig gennemgang af it-sikkerhedspolitikken. • It-sikkerhedspolitikken er godkendt af Hostingkompagniets ledelse. • It-sikkerhedspolitikken er accepteret og underskrevet af Hostingkompagniets medarbejdere.
Område: Informationssikkerhedsstrategi	
Risikoanalyse • At sikre, at de enkelte arbejdsprocesser i Hostingkompagniet ikke udgør en alvorlig risiko for Hostingkompagniet • At sikre, at der findes afhjælpning når risikoen er høj • At sikre, at risici afdækkes inden de forekommer	• Årlig gennemførelse af risikoanalyse, hvor der foretages en vurdering af kritiske hændelser. • Risikoanalysen er godkendt af Hostingkompagniets ledelse. Udførelse af løbende risikovurderinger.
It-strategi • At sikre, at it-strategien understøtter værdi- og visionsgrundlaget herunder de sikkerhedsmæssige aspekter for Hostingkompagniet	• Årlig gennemgang og opdatering af it-strategien. • It-strategien er godkendt af Hostingkompagniets ledelse.
Område: Organisering af informationssikkerhed	
Medarbejder informationssikkerhed • At sikre, at alle medarbejdere hos Hostingkompagniet er beviste om deres ansvar og til fulde bliver instrueret i sikkerhedspolitikker og lever op til instrukserne der er beskrevet i sikkerhedspolitikken, da Hostingkompagniet arbejder med forretnings kritisk data for mange kunder.	• Nye medarbejder skal vise at de besidder kundskab til håndtering af rutiner inden de på egen hånd udfører arbejde med kunde data og systemer. • Alle medarbejdere får ved ansættelse udleveret virksomhedens it-sikkerhedspolitik og skriver under på, at de er bekendte hermed og har i sinde at efterleve it-sikkerhedspolitikken. • Alle medarbejdere læser og skriver under på, at de er bekendte med og har i sinde at efterleve it-sikkerhedspolitikken efter den årlige opdatering af denne.
Godkendelse ved anskaffelser af driftsmidler • At sikre, at indkøb er i overensstemmelse med forretningsgrundlaget i Hostingkompagniet • At sikre, at de sikkerhedsmæssige aspekter ved ny hardware er overholdt • At sikre, at dokumentationskravet ved indkøb er overholdt	• Medarbejdere skal udfylde indkøbsformularen. • Indkøbsformularen godkendes af nærmeste leder • Indkøbshistorikken gennemgås en gang om året
Eksterne leverandører og samarbejdspartnere • At sikre, at aftalegrundlaget, når der indgås aftaler med enten leverandører eller partnere, er dækkende og tager højde for fremtidige mulige konflikter i samarbejdsforholdet • At sikre, at der etableres en juridisk gældende aftale mellem parterne • At sikre, at kontrakten opdateres hvis der er behov for dette • At sikre, at dokumentation af aftalen er korrekt og opdateret i en kontrakt. • At sikre, at uvedkommende ikke har adgang til steder, hvor der behandles data for såvel fysiske- som virtuelle rammer • At sikre, at aftalte ydelser også bliver udført i henhold til indgåede aftaler	• Ledelsen i Hostingkompagniet anvender en fast skabelon for etablering af kontrakter/aftaler med leverandører og partnere. • Skabelonen udfyldes ved indgåelse af en kontrakt/aftale. • Ledelsen udfører en årlig kontrol af indgåede aftaler • Ledelsen indhenter og gennemgår dokumentation fra leverandøren til sikring af overholdelse af aftale og kvalitet. • Hostingkompagniet udfører løbende kontrol af eksterne leverandører. • Ledelsen indhenter og gennemgår revisorerklæring fra Zitcom A/S.

Kontrolmål	Kontrolaktiviteter
Område: Sikkerhed ved installation og drift	
Sikkerhed ved installation og drift, herunder logning og backup i denne forbindelse • At sikre, at nye servere bliver installeret korrekt og sikkert i servermiljøet • At sikre, at dokumentation af nye servere og firewall opsætning er korrekt udført • At sikre, at alle servere hostet i Hostingkompagniets infrastruktur overvåges og beskyttes	• Den korrekte information for installationen beskrives inden et asset bliver installeret. • Det testes at dette asset virker korrekt inden det startes op i produktion. • Når dette asset er klar til overdragelse til kunden sendes der en klarmelding. • Oprettelser/ændringer/sletninger sker efter anmodning fra en IT-ansvarlig hos kunden. • Ingen udefrakommende får uhensigtsmæssigt adgang til kundernes netværk. • Der foretages backup af Hostingkompagniets infrastruktur. • Hostingkompagniet overvåger servere og andet kritisk hardware. • Den pågældende IT-Konsulent som får til opgave af IT-Chefen at installere og konfigurere anti-virus løsningen vil have ansvaret for at dette bliver udført. • Ved oprettelse og ændringer registreres dette i Hostingkompagniets Knack-system.
Beredskab • At modvirke afbrydelser af forretningsaktiviteter, og at beskytte kritiske forretningsprocesser mod virkningerne af større nedbrud af informationssystemer eller katastrofer, samt at sikre rettidig retablering	• Hostingkompagniet har udarbejdet en plan for retablering af driften • Hostingkompagniet har procedurer til sikring mod driftsforstyrrelser • Beredskabet testes med en given frekvens • Der foreligger dokumentation for beredskabet for alle incidents med Severity kode 5 og 6.
Område: Medarbejdersikkerhed og udstyr	
Ansættelse og afskedigelser af medarbejder • At sikre, ansættelser og afskedigelser sker efter anmodning fra ledelsen • At sikre, at dokumentation af ansættelser og afskedigelser gemmes	• Hostingkompagniet indhenter de nødvendige oplysninger om kvalifikationer. • Medarbejder underskriver ansættelseskontrakten og fortrolighedsaftale • Medarbejder underskriver på at de har læst og vil efterleve it-sikkerhedspolitikken • Ledelsen underskriver ansættelseskontrakten • Ansættelseskontrakt og underskrevne dokumenter arkiveres • Medarbejderen modtager en skriftlig opsigelse. • Medarbejderen afleverer alle informationsaktiver. • Password nulstilles • Den opsagte medarbejder underskriver en ophørsaftale for bekræftelse af fortrolighedsaftalen stadig er gældende.
Styring af software på driftssystemer • At sikre at Windows er opdateret med nyeste patches.	• Medarbejdere i supporten og Backoffice har rettigheder til at ændre på GPO'en som håndterer opdateringerne. • Der er sat jobs op til ugentligt, at sikre at alle opdateringer bliver lagt på alle servere.
Område: Fysisk sikring i Hostingkompagniet	
Fysisk adgangskontrol • At sikre, at der ikke er adgang for uvedkommende til Hostingkompagniets aktiver • At sikre, at medarbejdere kun har tildelt de fysisk adgange, som de har et funktionsmæssigt behov for	• Kontorbygningen er forsynet med adgangskontrol- system til sikring af, at kun autoriserede medarbejdere har adgang. • Kontorlokalet er forsynet med lås. • Kontoret er altid låst når der ikke er nogle medarbejdere på kontoret. • Kun medarbejdere der er godkendt og som har underskrevet en erklæring får udleveret en nøgle. • Der findes en liste over godkendte nøgler og hvem de er udleveret til.

Kontrolmål	Kontrolaktiviteter
Sikring af lokaler og udstyr samt forsyningssikkerhed • At sikre Hostingkompagniets servere og andet kritisk udstyr	• Indhentning af ISAE 3402 type 2-erklæring fra Zitcom A/S til kontrol af fysisk sikring af lokaler og udstyr. • Egenkontrol af Zitcom A/S
Område: Styring af netværk og brugerrettigheder	
Funktionsadskillelse • At sikre, at den logiske adgangskontrol efterlever it-sikkerhedspolitikkens krav til funktionsadskillelse • At sikre at medarbejdere kun har tildelt de rettigheder som de har et funktionsmæssigt behov for • At sikre, at brugerrettigheder for kunder kun ændres efter skriftlig anmodning om det pr. e-mail fra autoriserede personer hos kunden.	• Alle medarbejdere skal anvende passwords ved logon til PC'ere og systemer. • It-sikkerhedspolitikkens krav til passwords skal overholdes. • Oprettelse, ændring og nedlæggelse af brugere sker efter anmodning fra de medarbejderansvarlig leder. • Tildeling af brugerrettigheder sker efter funktionsmæssigt behov. • Der foretages periodisk gennemgang af brugere og tildelte rettigheder. • Kunden sender en e-mail med rettighedsændringer til support@hostingkompagniet.dk, som lander i ticketsystemet FreshDesk. • Hostingkompagniets medarbejder har ansvar for, at rettigheder kun ændres efter skriftlig anmodning herom fra kundens autoriserede medarbejder.
Styring af sikkerhedshændelser i driftsmiljøet • At sikre, at alle systemer der er i drift overvåges 24 timer i døgnet 365 dage om året • At sikre at medarbejdere er bekendt med rapportering af sikkerhedshændelser	• Alle systemer der er i drift overvåges 24/7-365. • Medarbejdere er bekendt med rapportering af sikkerhedshændelser.
Backup kontrol • At sikre, at alle servere tilmeldes backup • At sikre, at alt backup kontrolleres	• Når en backuprutine oprettes udføres dette som et led i korrekt oprettelse af en server. Når hele serveren er klar vil også backuprutinerne være korrekt opsat. • Den ansvarlige for den daglige vedligeholdelse af backupløsningerne gennemser dagligt rapporter genereret af de tre backup systemer, hvor eventuelle fejl er logget. Disse fejl noteres i den samlede backuplog. • Alle uregelmæssigheder opsamles.
Databærende medier • At sikre, at Bortskaffelse sker i overensstemmelse med Hostingkompagniets procedure herfor • At sikre, at dokumentationskravet ved bortskaffelse er overholdt	• Medarbejderen udfylder en formular for det udstyr der skal bortskaffes • Det sikres at eventuelt data bliver slettet på udstyret
Område: Overensstemmelse med lovbestemte og kontraktlige krav	
Overensstemmelse med lovbestemte og kontraktlige krav • At sikre, at love på området Hostingkompagniet befinder sig i overholdes. • At sikre, kundekontrakter bliver håndteret og behandlet korrekt i forhold til love og administration af disse. • At sikre, at dokumentationen for ændringer i forhold til handlingsprocedure bliver vedligeholdt	• Hostingkompagniets medarbejdere deltager løbende i kurser og seminarer omkring tiltag i lovgivningen på IT-området. • Hostingkompagniet tilpasser kontrakter og aftaler såfremt der sker ændringer i lovgivning der påvirker aftaleforholdet.

Kontrolaktiviteterne er uddybet i omstående skema, der udgør en integreret del af beskrivelsen.

KONTROLMÅL, KONTROLLER, TEST OG RESULTAT AF TEST

I nærværende testskema er relevante kontrolmål og indførte kontrolaktiviteter udformet til at nå kontrolmålene, beskrevet og udvalgt af Hostingkompagniet A/S.

I testskemaet har vi beskrevet de udførte test, som blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og de tilhørende kontroller fungerede effektivt i perioden fra 1. december 2017 til 30. november 2018.

Test af kontrollernes design og implementering er udført ved forespørgsel, inspektion, observation og genudførelse.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale hos Hostingkompagniet A/S 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, datatransmission 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 opnå yderligere bevis for, at kontrollen fungerer som forudsat.

For de ydelser, som Zitcom A/S leverer inden for drifts- og hostingydelser, har vi fra uafhængig revisor modtaget en erklæring om generelle it-kontroller relateret til drifts- og hostingydelser for perioden 1. januar til 31. december 2017. Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i Hostingkompagniet A/S' beskrivelse af driften af hostingmiljøet. Vi har således anvendt partielmetoden og alene vurderet erklæringen og testet de kontroller hos Hostingkompagniet A/S, der overvåger funktionaliteten af serviceunderleverandørens kontroller.

IT sikkerhedsstyring		
Kontrolmål: It-sikkerhedspolitik *1. At sikre, at der løbende sker en styring af IT-sikkerheden i Hostingkompagniet* *2. At sikre, at IT-sikkerheden bliver implementeret og kommunikeret til alle interessenter* *3. At sikre, at dokumentation af IT-sikkerheden bliver vedligeholdt og godkendt i hele organisationen.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Opdatering og godkendelse • Hostingkompagniets ledelse foretager en årlig gennemgang af it-sikkerhedspolitikken. • It-sikkerhedspolitikken er godkendt af Hostingkompagniets ledelse.	Vi har udført forespørgsler hos passende personale og inspiceret Hostingkompagniets "It-sikkerhedspolitik" og "Procedure for it-sikkerhedsstyring". Vi har observeret, at it-sikkerhedspolitikken er opdateret den 14. december 2018 og godkendt af Hostingkompagniets ledelse den 14. december 2018.	Ingen afvigelser konstateret.
Informering af medarbejdere • It-sikkerhedspolitikken er accepteret og underskrevet af Hostingkompagniets medarbejdere.	Vi har udført forespørgsler hos passende personale. Vi har observeret, at Hostingkompagniets medarbejdere har accepteret og underskrevet seneste it-sikkerhedspolitik.	Ingen afvigelser konstateret.

Informationssikkerhedsstrategi

Kontrolmål: Risikoanalyse og it-strategi

1. *At sikre, at de enkelte arbejdsprocesser i Hostingkompagniet ikke udgør en alvorlig risiko for Hostingkompagniet*
2. *At sikre, at der findes afhjælpning når risikoen er høj*
3. *At sikre, at risici afdækkes inden de forekommer*
4. *At sikre, at it-strategien understøtter værdi- og visionsgrundlaget herunder de sikkerhedsmæssige aspekter for Hostingkompagniet*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikoanalyse • Årlig gennemførelse af risikovurdering, hvor der foretages en vurdering af kritiske hændelser. • Risikovurderingen er godkendt af Hostingkompagniets ledelse. • Udførelse af løbende risikovurderinger.	Vi har udført forespørgsler hos passende personale og inspiceret Hostingkompagniets risikovurdering og observeret, at seneste udførte risikovurdering er foretaget den 29. maj 2018. Vi har observeret, at udførte risikovurdering er godkendt af Hostingkompagniets ledelse den 29. maj 2018. Vi har observeret, at de løbende risikovurderinger i perioden 1. december 2017 til 30. november 2018 er godkendt af Hostingkompagniets ledelse.	Ingen afvigelser konstateret.
It-strategi • Årlig gennemgang og opdatering af it-strategien. • It-strategien er godkendt af Hostingkompagniets ledelse.	Vi har udført forespørgsler hos passende personale og inspiceret Hostingkompagniets "It-strategi 2015-2020" og "Procedure for vedligeholdelse af it-strategi" samt "Informationssikkerhed i Hostingkompagniet". Vi har inspiceret dokumentation for opdatering af it-strategien. Vi har observeret, at it-strategien er godkendt af Hostingkompagniets bestyrelse den 29. maj 2018.	Ingen afvigelser konstateret.

Organisering af informationssikkerhed		
Kontrolmål: Medarbejder informationssikkerhed 1. *At sikre, at alle medarbejdere hos Hostingkompagniet er beviste om deres ansvar og til fulde bliver instrueret i sikkerhedspolitikker og lever op til instrukserne der er beskrevet i sikkerhedspolitikken, da Hostingkompagniet arbejder med forretnings kritisk data for mange kunder*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Kompetencer • Nye medarbejder skal vise at de besidder kundskab til håndtering af rutiner inden de på egen hånd udfører arbejde med kunde data og systemer.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for it-sikkerhedsstyring" og "Procedure for medarbejder informationssikkerhed". Vi har fået oplyst, at nye medarbejder uddannes ved sidemandsoplæring til sikring af, at de har de nødvendige kompetencer. Vi har observeret, at medarbejderne ved ansættelsen får udleveret fortrolighedsaftale og it-sikkerhedspolitik, som de underskriver.	Ingen afvigelser konstateret.
Informering af medarbejdere • Alle medarbejdere får ved ansættelse udleveret virksomhedens it-sikkerhedspolitik og skriver under på, at de er bekendte hermed og har i sinde at efterleve it-sikkerhedspolitikken. • Alle medarbejdere læser og skriver under på, at de er bekendte med og har i sinde at efterleve it-sikkerhedspolitikken efter den årlige opdatering af denne.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet. For det arbejde, vi har udført for at teste kontrolaktiviteterne, henviser vi til områderne: • Medarbejder sikkerhed og udstyr – ansættelse af medarbejdere. • IT sikkerhedsstyring – Informering af medarbejdere.	Ingen afvigelser konstateret.

Organisering af informationssikkerhed		
Kontrolmål: Godkendelse ved anskaffelser af driftsmidler *1. At sikre, at indkøb er i overensstemmelse med forretningsgrundlaget i Hostingkompagniet* *2. At sikre, at de sikkerhedsmæssige aspekter ved ny hardware er overholdt* *3. At sikre, at dokumentationskravet ved indkøb er overholdt*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Indkøb • Medarbejdere skal udfylde indkøbsformularen. • Indkøbsformularen godkendes af nærmeste leder • Indkøbshistorikken gennemgås en gang om året	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for anskaffelser af aktiver", "Procedure for anskaffelse af aktiver for Hostingkompagniet og kunder" og "Formular for anskaffelse af interne ressourcer". Vi har stikprøvevist inspiceret udfyldte formularer for anskaffelser af aktiver i 2018. Vi har stikprøvevist observeret, at anskaffelserne i 2018 er godkendt af Ledelsen i overensstemmelse med "Procedure for anskaffelser af aktiver". Vi har fået oplyst og observeret, at Hostingkompagniet i perioden 1. december 2017 til 30. november 2018 har anvendt et virtuelt miljø og derfor ikke anskaffet hardware i form af servere og andet kritisk udstyr, udover bærbare computere, skærme, mus mm.	Ingen afvigelser konstateret.

Organisering af informationssikkerhed

Kontrolmål: Eksterne leverandører og samarbejdspartnere

1. *At sikre, at aftalegrundlaget, når der indgås aftaler med enten leverandører eller partnere, er dækkende og tager højde for fremtidige mulige konflikter i samarbejdsforholdet*
2. *At sikre, at der etableres en juridisk gældende aftale mellem parterne*
3. *At sikre, at kontrakten opdateres hvis der er behov for dette*
4. *At sikre, at dokumentation af aftalen er korrekt og opdateret i en kontrakt.*
5. *At sikre, at uvedkommende ikke har adgang til steder, hvor der behandles data for såvel fysiske- som virtuelle rammer*
6. *At sikre, at aftalte ydelser også bliver udført i henhold til indgåede aftaler*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Partner og leverandøraftaler • Ledelsen i Hostingkompagniet anvender en fast skabelon for etablering af kontrakter/aftaler med leverandører og partnere. • Skabelonen udfyldes ved indgåelse af en kontrakt/aftale.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for leverandør- og partnerkontrakter". Vi har observeret, at Hostingkompagniet anvender en fast skabelon ved indgåelse af aftaler. Vi har observeret, at skabelonen er anvendt ved indgåelse af aftale med 1 partner, som er udvalgt af os. Vi har observeret, at der er indgået skriftlig aftale med en leverandør, som er udvalgt af os.	Ingen afvigelser konstateret.
Egenkontrol af eksterne leverandører • Ledelsen udfører en årlig kontrol af indgåede aftaler • Ledelsen indhenter og gennemgår dokumentation fra leverandøren til sikring af overholdelse af aftale og kvalitet. • Hostingkompagniet udfører løbende kontrol af eksterne leverandører. • Ledelsen indhenter og gennemgår revisorerklæring fra Zitcom A/S.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for egenkontrol af eksterne leverandører". Vi har inspiceret, ISAE 3402 type 2-erklæringen fra Zitcom A/S for perioden 1. januar 2017 til 31. december 2017. Vi har inspiceret Hostingkompagniets dokumentation for egenkontrol af aktive leverandører og observeret at: • Ledelsen har udført den årlige kontrol af indgåede aftaler den 6. juni 2018 • Der foretages løbende egenkontrol af leverandører, idet Hostingkompagniet selv varetager overvågning og drift. • Ledelsen har modtaget og gennemgået ISAE 3402 type 2-erklæring fra Zitcom A/S for perioden 1. januar 2017 til 31. december 2017 dateret den 15. februar 2018. Erklæringen er uden forbehold.	Ingen afvigelser konstateret.

Sikkerhed ved installation og drift

Kontrolmål: Sikkerhed ved installation og drift, herunder logning og backup i denne forbindelse

1. *At sikre, at nye servere bliver installeret korrekt og sikkert i servermiljøet*
2. *At sikre, at dokumentation af nye servere og firewall opsætning er korrekt udført*
3. *At sikre, at alle servere hostet i Hostingkompagniets infrastruktur overvåges og beskyttes*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Installation af et asset • Den korrekte information for installationen beskrives inden et asset bliver installeret. • Det testes at dette asset virker korrekt inden det startes op i produktion. • Når dette asset er klar til overdragelse til kunden sendes der en klarmelding.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for sikkerhed i driften". Vi har observeret, kundeoprettelser foretaget i perioden 1. december 2017 til 30. november 2018 og stikprøvevis efterprøvet overholdelse af de interne retningslinjer herfor og sammenholdt oprettelserne med indgåede kundeaftaler. Vi har observeret, håndtering og registrering af de enkelte kunders løsninger og udstyr. Vi har stikprøvevis observeret, at der i forbindelse med overdragelse til kunden fremsendes en klarmelding via e-mail.	Ingen afvigelser konstateret.
Netværk i driften • Oprettelser/ændringer/sletninger sker efter anmodning fra en IT-ansvarlig hos kunden. • Ingen udefrakommende får uhensigtsmæssigt adgang til kundernes netværk. • Der foretages backup af Hostingkompagniets infrastruktur. • Hostingkompagniet overvåger servere og andet kritisk hardware.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for Alerts for overvågning", "Procedure for styring af sikkerhedshændelser", "Procedure for firewall administration", "Procedure for beredskab og retablering af driften" samt "Procedure for backup". Vi har for de af os 7 udvalgte kunder observeret, at oprettelse, ændring og sletning af brugere, data mv. sker efter skriftlig anmodning herom fra den it-ansvarlige hos kunden. Vi har observeret, at Hostingkompagniet selv varetager konfiguration og drift af firewalls. Overvågning heraf varetages i samarbejde med Zitcom A/S. Vi har ved gennemgang af konfigurationen for de fysiske- og virtuelle-miljøer observeret, hvordan Hostingkompagniet sikrer adskillelse mellem de enkelte kundemiljøer samt adskillelse over til Hostingkompagniet interne miljø. Vi har stikprøvevist observeret, at der foretages backup af Hostingkompagniets infrastruktur.	Ingen afvigelser konstateret.

Sikkerhed ved installation og drift		
Kontrolmål: Sikkerhed ved installation og drift, herunder logning og backup i denne forbindelse *1. At sikre, at nye servere bliver installeret korrekt og sikkert i servermiljøet* *2. At sikre, at dokumentation af nye servere og firewall opsætning er korrekt udført* *3. At sikre, at alle servere hostet i Hostingkompagniets infrastruktur overvåges og beskyttes*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har observeret, at Hostingkompagniet overvåger: • Performance • Diskplads • Ramforbrug • Svartider • Server uden ping svar • Services der ikke kører Ved alarmer sendes besked til alle medarbejdere i support/helpdesk via e-mail.	
Anti-virus/malware beskyttelse • Den pågældende IT-Konsulent som får til opgave af IT-Chefen at installere og konfigurere anti-virus løsningen vil have ansvaret for at dette bliver udført. • Ved oprettelse og ændringer registreres dette i Hostingkompagniets Knack-system.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for anti-virus løsninger". Vi har observeret, at Hostingkompagniet anvender 2 forskellige antivirus-løsninger til sikring af deres kunder, der har mulighed for at vælge forskellige løsninger herfor. Vi har stikprøvevis efterprøvet standardopsætningen for Hostingkompagniets kunder for: • Netværk • Antivirus • Firewall • Overvågning Vi har observeret, at oplysningerne registreres i Hostingkompagniets Knack-system.	Ingen afvigelser konstateret.

Sikkerhed ved installation og drift		
Kontrolmål: Beredskab *1. At modvirke afbrydelser af forretningsaktiviteter, og at beskytte kritiske forretningsprocesser mod virkningerne af større nedbrud af informationssystemer eller katastrofer, samt at sikre rettidig retablering*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Beredskab • Hostingkompagniet har udarbejdet en plan for retablering af driften • Hostingkompagniet har procedurer til sikring mod driftsforstyrrelser • Beredskabet testes med en given frekvens • Der foreligger dokumentation for beredskabet for alle incidents med Severity kode 5 og 6.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerheds i Hostingkompagniet", "Procedure for beredskab" og "Procedure for beredskab og retablering af driften". Vi har observeret, at Hostingkompagniet har udarbejdet en plan for retablering af driften og procedurer til sikring mod driftsforstyrrelser, samt at disse er kendt af Hostingkompagniets medarbejdere. Vi har observeret, at Hostingkompagniet har udført test af beredskabet ved gendannelse af mails, filer, enkelte mapper og hele servere. I perioden 1. december 2017 til 30. november 2018 er der foretaget 10 tests. Vi har observeret, at der foreligger dokumentation for håndtering af incidents med Severity kode 5 og 6 i Knack - Severity.	Ingen afvigelser konstateret.

Medarbejdersikkerhed og udstyr		
Kontrolmål: Ansættelse og afskedigelser af medarbejder *1. At sikre, ansættelser og afskedigelser sker efter anmodning fra ledelsen* *2. At sikre, at dokumentation af ansættelser og afskedigelser gemmes*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Ansættelser • Hostingkompagniet indhenter de nødvendige oplysninger om kvalifikationer. • Medarbejder underskriver ansættelseskontrakten og fortrolighedsaftale • Medarbejder underskriver på at de har læst og vil efterleve it-sikkerhedspolitikken • Ledelsen underskriver ansættelseskontrakten • Ansættelseskontrakt og underskrevne dokumenter arkiveres	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for ansættelser og afskedigelser" og "Procedure for medarbejder informationssikkerhed". Vi har fået oplyst, at der ikke har været ansættelser i perioden 1. december 2017 til 30. november 2018, så det har ikke været muligt at efterprøve Hostingkompagniets procedurer og kontroller herfor. Vi har observeret, at ansættelseskontrakter og underskrevne papirdokumenter opbevares i aflåst kontorskab i Hostingkompagniets kontor, hvor det alene er ledelsen, der har adgang. Vi har observeret, at fortrolige elektroniske dokumenter opbevares på serveren, hvor det alene er ledelsen, der har adgang.	Ingen afvigelser konstateret.
Afskedigelser • Medarbejderen modtager en skriftlig opsigelse. • Medarbejderen afleverer alle informationsaktiver. • Password nulstilles • Den opsagte medarbejder underskriver en ophørsaftale for bekræftelse af fortrolighedsaftalen stadig er gældende.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for ansættelser og afskedigelser" og "Procedure for medarbejder informationssikkerhed". Vi har fået oplyst, at der ikke har været afskedigelser i perioden 1. december 2017 til 30. november 2018, så det har ikke været muligt at efterprøve Hostingkompagniets procedurer og kontroller herfor.	Ingen afvigelser konstateret.

Medarbejdersikkerhed og udstyr		
Kontrolmål: Styring af software på driftssystemer *1. At sikre at Windows er opdateret med nyeste patches.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Styring af software på driftssystemer • Medarbejdere i supporten og Backoffice har rettigheder til at ændre på GPO'en som håndterer opdateringerne. • Der er sat jobs op til ugentligt, at sikre at alle opdateringer bliver lagt på alle servere.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for styring af software på driftssystemer". Vi har observeret, at medarbejdere i supporten og Backoffice har de nødvendige rettigheder til ændring på GPO'en for håndtering af opdateringer. Vi har observeret, opsatte batchjobs, der sikrer at alle servere opdateres, samt at der er mulighed for Roll Back, hvis en opdatering fejler.	Ingen afvigelser konstateret.

Fysisk sikring i Hostingkompagniet		
Kontrolmål: Fysisk adgangskontrol *1. At sikre, at der ikke er adgang for uvedkommende til Hostingkompagniets aktiver* *2. At sikre, at medarbejdere kun har tildelt de fysisk adgange, som de har et funktionsmæssigt behov for*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fysisk adgang til kontor • Kontorbygningen er forsynet med adgangskontrol- system til sikring af, at kun autoriserede medarbejdere har adgang. • Kontorlokalet er forsynet med lås. • Kontoret er altid låst når der ikke er nogle medarbejdere på kontoret	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for fysisk sikring af Hostingkompagniet" og "Procedure for kontor sikkerhed". Vi har observeret, at kun autoriserede medarbejdere har adgang med nøgle. Vi har observeret, at kontorlokalet er forsynet med lås. Vi har observeret, at døren til kontorbygningen altid er aflåst og fået oplyst, at selve kontorlokalet aflåses, når der ikke er medarbejdere på kontoret.	Ingen afvigelser konstateret.
Udlevering af nøgler • Kun medarbejdere der er godkendt og som har underskrevet en erklæring får udleveret en nøgle. • Der findes en liste over godkendte nøgler og hvem de er udleveret til.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for fysisk sikring af Hostingkompagniet" og "Procedure for kontor sikkerhed". Vi har observeret, at samtlige medarbejdere har skrevet under på en fortrolighedsaftale og it-sikkerhedspolitikken. Vi har modtaget og inspiceret liste over udleverede nøgler til medarbejdere til Hostingkompagniets kontorbygning og lokaler. Vi har observeret, at listen over udleverede nøgler er kontrolleret den 18. juni 2018.	Ingen afvigelser konstateret.

Fysisk sikring i Hostingkompagniet		
Kontrolmål: Sikring af lokaler og udstyr samt forsyningssikkerhed *1. At sikre Hostingkompagniets servere og andet kritisk udstyr*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Sikring af lokaler og udstyr samt forsyningssikkerhed • Indhentning af ISAE 3402 type 2-erklæring fra Zitcom A/S til kontrol af fysisk sikring af lokaler og udstyr. • Egenkontrol af Zitcom A/S	Vi har udført forespørgsel hos passende personale hos Hosting-kompagniet. For det arbejde, vi har udført for at teste kontrolaktiviteterne, henviser vi til området 'Organisering af informationssikkerhed': • Eksterne leverandører og samarbejdspartnere • Egenkontrol af eksterne leverandører For udstyr på kontoret på Tuborgvej 5 i Hellerup henviser vi til området: Fysisk sikkerhed – Fysisk adgangskontrol.	Ingen afvigelser konstateret.

Styring af netværk og brugerrettigheder

Kontrolmål: Funktionsadskillelse

1. *At sikre, at den logiske adgangskontrol efterlever it-sikkerhedspolitikkens krav til funktionsadskillelse*
2. *At sikre at medarbejdere kun har tildelt de rettigheder som de har et funktionsmæssigt behov for*
3. *At sikre, at brugerrettigheder for kunder kun ændres efter skriftlig anmodning om det pr. e-mail fra autoriserede personer hos kunden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Anvendelse af password • Alle medarbejdere skal anvende passwords ved logon til PC'ere og systemer. • It-sikkerhedspolitikkens krav til passwords skal overholdes.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for adgang og password håndtering", "Procedure for adgang til HK system udefra" og "Procedure for sporbarhed ved anvendelse af Service Accounts". Vi har observeret, at alle medarbejdere skal anvende passwords for logon til pc'er og systemer. Vi har observeret, at Password Policy er sat op i henhold til Hostingkompagniets passwordpolitik. Vi har observeret, at medarbejderne overholder Hostingkompagniets password politik med skift af password efter 90 dage.	Ingen afvigelser konstateret.
Brugeradministration • Oprettelse, ændring og nedlæggelse af brugere sker efter anmodning fra de medarbejderansvarlig leder.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for vedligeholdelse af rettigheder" og "Procedure for adgang til HK system udefra". Vi har stikprøvevist observeret, at oprettelse, ændring og nedlæggelse af brugere sker efter anmodning fra de medarbejderansvarlig leder og registreres i Hostingkompagniets Freshdesk supportsystem samt Knack-systemet.	Ingen afvigelser konstateret.
Brugerrettigheder • Tildeling af brugerrettigheder sker efter funktionsmæssigt behov. • Der foretages periodisk gennemgang af brugere og tildelte rettigheder.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet" og "Procedure for vedligeholdelse af rettigheder". Vi har stikprøvevist observeret, at tildeling af brugerrettigheder sker efter et funktionsmæssigt behov. VI har observeret, at der foretages en gennemgang af brugere og brugerrettigheder 1 gang om måneden.	Ingen afvigelser konstateret.

Styring af netværk og brugerrettigheder		
Kontrolmål: Funktionsadskillelse *1. At sikre, at den logiske adgangskontrol efterlever it-sikkerhedspolitikkens krav til funktionsadskillelse* *2. At sikre at medarbejdere kun har tildelt de rettigheder som de har et funktionsmæssigt behov for* *3. At sikre, at brugerrettigheder for kunder kun ændres efter skriftlig anmodning om det pr. e-mail fra autoriserede personer hos kunden.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Registrering • Kunden sender en e-mail med rettighedsændringer til support@hostingkompagniet.dk, som lander i ticketsystemet FreshDesk.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for vedligeholdelse af rettigheder" og "Procedure for adgang til HK system udefra". Vi har stikprøvevist observeret, at anmodning om rettighedsændringer fra kunder sker via e-mail og oprettes i ticketsystemet FreshDesk.	Ingen afvigelser konstateret.
Ansvar • Hostingkompagniets medarbejder har ansvar for, at rettigheder kun ændres efter skriftlig anmodning herom fra kundens autoriserede medarbejder.	Vi har stikprøvevist observeret, at oprettelse, ændring og nedlæggelse af brugere og brugerrettigheder hos kunder, sker efter skriftlig anmodning herom fra autoriseret medarbejder hos kunden og registreres i Hostingkompagniets FreshDesk supportsystem samt Knack-systemet.	Ingen afvigelser konstateret.

Styring af netværk og brugerrettigheder		
Kontrolmål: Styring af sikkerhedshændelser i driftsmiljøet *1. At sikre, at alle systemer der er i drift overvåges 24 timer i døgnet 365 dage om året* *2. At sikre at medarbejdere er bekendt med rapportering af sikkerhedshændelser*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Overvågning og sikkerhedshændelser • Alle systemer der er i drift overvåges 24/7-365. • Medarbejdere er bekendt med rapportering af sikkerhedshændelser.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet. For det arbejde, vi har udført for at teste kontrolaktiviteterne, henviser vi til området 'Sikkerhed ved installation og drift': • Sikkerhed ved installation og drift, herunder logning og backup og backup i denne forbindelse.	Ingen afvigelser konstateret.

Styring af netværk og brugerrettigheder		
Kontrolmål: Backup kontrol *1. At sikre, at alle servere tilmeldes backup* *2. At sikre, at alt backup kontrolleres*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Kontrol af at backuprutiner er installeret korrekt • Når en backuprutine oprettes udføres dette som et led i korrekt oprettelse af en server. Når hele serveren er klar vil også backuprutinerne være korrekt opsat.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for backup" og "procedure for beredskab og retablering". For det arbejde, vi har udført for at teste kontrolaktiviteterne, henviser vi til området 'Organisering af informationssikkerhed': Sikkerhed ved installation og drift, herunder logning og backup i denne forbindelse.	Ingen afvigelser konstateret.
Kontrol af backuppen • Den ansvarlige for den daglige vedligeholdelse af backupløsningerne gennemser dagligt rapporter genereret af de tre backup systemer, hvor eventuelle fejl er logget. Disse fejl noteres i den samlede backuplog. • Alle uregelmæssigheder opsamles	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Procedure for backup" og "procedure for beredskab og retablering" Vi har observeret, Hostingkompagniets procedurer for kontrol af backup. Vi har stikprøvevis observeret håndtering af fejlede backups. Vi har inspiceret dokumentation for udførte restoretests af servere og filmapper.	Ingen afvigelser konstateret.

Styring af netværk og brugerrettigheder		
Kontrolmål: Databærende medier *1. At sikre, at Bortskaffelse sker i overensstemmelse med Hostingkompagniets procedure herfor* *2. At sikre, at dokumentationskravet ved bortskaffelse er overholdt*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Bortskaffelse • Medarbejderen udfylder en formular for det udstyr der skal bortskaffes • Det sikres at eventuelt data bliver slettet på udstyret	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "Procedure for bortskaffelse af aktiver" og "Formular for bortskaffelse". Vi har fået oplyst, at det er samme procedure der gælder for både Hostingkompagniets egne og kunders databærende medier, der skal tages ud af driften og destrueres. Vi har modtaget og inspiceret dokumentation for bortskaffelser af interne servere og switches samt for server fra kunde. Det sker i overensstemmelse med proceduren for bortskaffelse af aktiver. For det arbejde, vi har udført for at teste kontrolaktiviteterne for anskaffelse af databærende medier, henviser vi til området: Organisering af informationssikkerhed – Godkendelse ved anskaffelse af driftsmidler.	Ingen afvigelser konstateret.

Love og kontraktmæssige krav

Kontrolmål: Overensstemmelse med lovbestemte og kontraktlige krav

1. *At sikre, at love på området Hostingkompagniet befinder sig i overholdes.*
2. *At sikre, kundekontrakter bliver håndteret og behandlet korrekt i forhold til love og administration af disse.*
3. *At sikre, at dokumentationen for ændringer i forhold til handlingsprocedure bliver vedligeholdt.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Overensstemmelse med lovbestemte og kontraktlige krav • Hostingkompagniets medarbejdere deltager løbende i kurser og seminarer omkring tiltag i lovgivningen på IT-området. • Hostingkompagniet tilpasser kontrakter og aftaler såfremt der sker ændringer i lovgivning der påvirker aftaleforholdet.	Vi har udført forespørgsel hos passende personale hos Hostingkompagniet og inspiceret "Informationssikkerhed i Hostingkompagniet", "It-sikkerhedspolitik" og "Procedure for overholdelse af love og kontrakter". Vi har fået oplyst, at Hostingkompagniets medarbejdere uddannes løbende ved deltagelse i relevante kurser og certificeringer. Vi har inspiceret 7 kundekontrakter udvalgt af os. Vi har observeret Hostingkompagniets håndtering af softwarelicenser.	Ingen afvigelser konstateret.

BDO Statsautoriseret revisionsaktieselskab

Havneholmen 29
DK-1561 København V
CVR-nr. 20 22 26 70