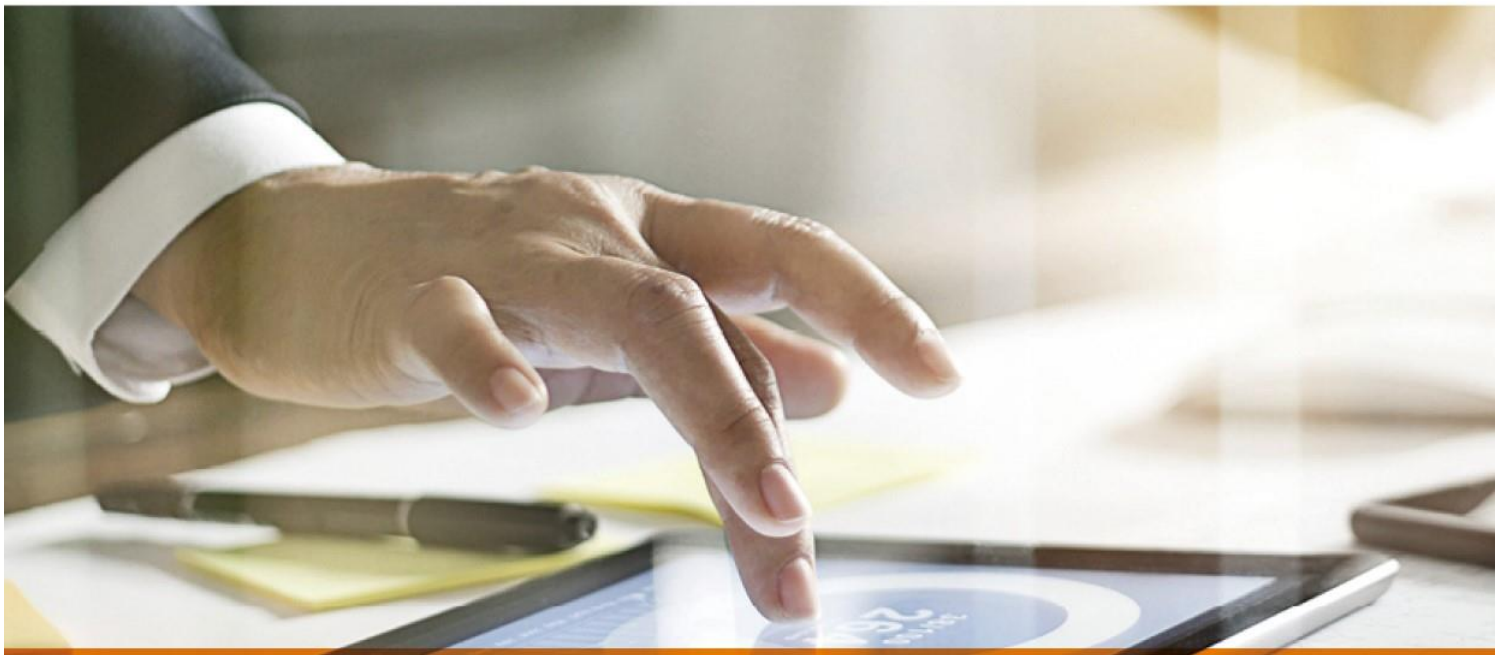
BEIERHOLM
VI SKABER BALANCE



Juni 2022

SYSTEMGRUPPEN A/S

ISAE 3402 TYPE 2 ERKLÆRING

CVR 21697974

Uafhængig revisors erklæring om de generelle it-kontroller i tilknytning til driften af hostingaktiviteter.

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:
SystemGruppen A/S' beskrivelse af de generelle it-kontroller for driften af hostingaktiviteter.

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

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

KAPITEL 1:

Ledelseserklæring

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt SystemGruppen A/S' hostingaktiviteter, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene til kontrolmiljøet samt databeskyttelsesforordningen er overholdt.

SystemGruppen A/S bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af SystemGruppen A/S' kontrolmiljø i tilknytning til drift af hostingaktiviteter i hele perioden 1. februar 2021 - 31. januar 2022. 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 SystemGruppen A/S' hostingaktiviteter 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 ved SystemGruppen A/S' hostingaktiviteter foretaget i forbindelse udførelse af revisionsopgaven

(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. februar 2021 - 31. januar 2022. 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. februar 2021 - 31. januar 2022.

(C) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere 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 SystemGruppen A/S' standardaftale samt tilhørende databehandleraftale, grundlaget for SystemGruppen A/S' hostingaktiviteter omkring de tekniske og organisatoriske sikringsforanstaltninger. Kriterierne for dette grundlag var:

(i) SystemGruppen A/S – Informationssikkerhedspolitik
(ii) SystemGruppen A/S – IT-sikkerhedsprocedurer

Aalborg, den 2. juni 2022

Direktør, Olafur B. Birgisson
SystemGruppen A/S, Gugvej 128, 9210 Aalborg SØ, CVR-nummer 21697974

KAPITEL 2:

SystemGruppen A/S' beskrivelse af de generelle it-kontroller for driften af hostingaktiviteter

Indledning

Formålet med nærværende beskrivelse er at levere information til SystemGruppen A/S' kunder og deres revisorer om leverede ydelser og understøttende forretningsgange.

Beskrivelsen omfatter de kontrolmål og kontroller hos SystemGruppen A/S, som omfatter størstedelen af vores kunder og er baseret på vores standardleverancer. Individuelle kundeforhold er ikke medtaget i denne beskrivelse.

Beskrivelse af SystemGruppen A/S

SystemGruppen A/S blev stiftet i 1999. SystemGruppen beskæftiger i dag 16 medarbejdere og har kontorer i Aalborg og Herning.

SystemGruppen er service leverandør inden for IT, og kerneaktiviteten hos SystemGruppen er hosting, serverdrift og IT-support.

SystemGruppen leverer hosting i et moderne og professionelt datacenter. Serverparken er placeret hos Curanet A/S. Denne samarbejdspartner varetager drift af fysiske servere, netværk og backupsystemer i datacentret.

Vi tilbyder ydelser lige fra enkle softwareløsninger til hele virksomhedens it-drift. SystemGruppen er specialiseret i hosting af komplekse it-løsninger, herunder Microsoft ERP-løsninger.

For at underbygge en robust og stabil IT-drift bestræber SystemGruppen sig at have høj grad af redundans både i den fysiske og den virtuelle del af hostingmiljøet.

SystemGruppen er Certificeret Microsoft Partner med sølv kompetence på cloud solutions.

Forretningsstrategi/ it-sikkerhedsstrategi

Det er SystemGruppens strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, således at selskabet og dets kunder ikke påføres uacceptable risici.

SystemGruppen har tre overordnede strategiske pejlepunkter:

- SystemGruppen hjælper virksomheder til en optimal brug af moderne informationsteknologi
- SystemGruppen arbejder primært med administrative systemer, netværksløsninger og internet/intranetløsninger
- SystemGruppen er en god arbejdsplads for en stabil og veluddannet medarbejderstyrke

SystemGruppen arbejder med IT-sikkerhed på et forretningsstrategisk niveau og arbejder derfor løbende med at sikre et højt service- og kvalitetsniveau. It-sikkerhedspolitikken revideres minimum én gang pr. år.

Ledelsen prioriterer gennem selskabet sikkerhedspolitik, at IT-sikkerheden skal være og er en vigtig del af selskabets virksomhedskultur.

For at sikre en ensartet leverance, som lever op til branchens bedste standarder, har vi valgt at underlægge driften af hosting- og driftsaktiviteterne en revisionsproces med det formål at leve op til kravene i en ISAE3402 erklæring. Revisionsprocessen gentages årligt, og resulterer i en revisionserklæring.

Erklæringen kan bidrage til kundens (dataejerens) kontrol af, hvorvidt SystemGruppen lever op til behandlingssikkerheden i den indgået databehandleraftale.

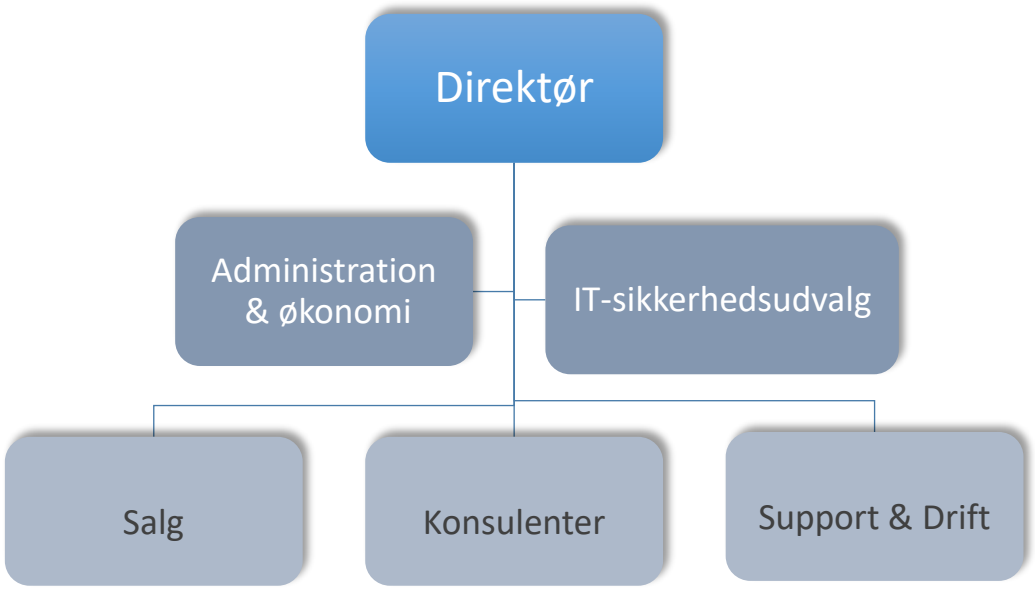
SystemGruppen har omkring it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27002, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Driftssikkerhed
- Kommunikationssikkerhed
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Rammen for hvilke kontrolmål og underliggende kontrolpunkter (sikkerhedselementer), som SystemGruppens ledelse har defineret relevant for arbejdet med et passende sikkerhedsmiljø er nærmere beskrevet i bilag 1.

SystemGruppen A/S' organisation og organisering af it-sikkerheden

Ansvar og organisering i SystemGruppen A/S fremgår af nedenstående organisationsdiagram:



Direktionen i SystemGruppen, som er den øverst ansvarlige for it-sikkerheden, sørger for, at der til stadighed er etableret procedurer og systemer, der understøtter overholdelsen af den til enhver tid gældende it-sikkerhedspolitik. For at understøtte dette har SystemGruppen etableret et it-sikkerhedsudvalg, som er ansvarlig for overordnede målsætninger for implementering af it-sikkerhed på serviceydelserne.

Det er den Tekniske Chef, som er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollerbart, hvor dette overhovedet er muligt, og være udtryk for "best pratice" inden for de enkelte kontrolaktiviteter på serviceområder, som tilbydes kunderne.

IT-sikkerhedsudvalget består p.t. af følgende medlemmer:

- Direktør, Olafur B. Birgisson
- Teknisk chef, Christoffer Klarskov Jacobsen

Udvalget mødes 1 gang årligt for at fastsætte og følge op på målsætninger i relationen til it -sikkerheden.

SystemGruppens ledelse har ansvaret for at SystemGruppen identificerer relevant lovgivning vedr. persondata og opdaterer relevante dokumenter, herunder databehandleraftaler.

Risikostyring i SystemGruppen A/S

Det er SystemGruppens politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde normal drift. SystemGruppen gennemfører risikostyring og interne kontroller på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering.

SystemGruppen har indarbejdet faste procedurer for risikovurdering af forretningen. Vi sikrer dermed, at de risici, som er forbundet med de services og ydelser, som vi stiller til rådighed, er minimeret til acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vi vurderer relevante i forbindelse med at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderingen ligger hos direktør Olafur B. Birgisson og skal efterfølgende forankres og godkendes hos virksomhedens ledelse.

Håndtering af it-sikkerhed

Ledelsen hos SystemGruppen 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 SystemGruppens struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

SystemGruppens kvalitetsstyringssystem er defineret ud fra den overordnede målsætning om at levere stabil og sikker it-drift til kunderne. For at kunne gøre det er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

SystemGruppens 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. Fejlen registreres i en log over sikkerhedsbrist. Når fejlen er udbedret, kontrollerer SystemGruppens Tekniske Chef fejlrettelsen og melder fejlen afhjulpet i loggen.

Alle virtuelle servere og netværksopsætninger er dokumenteret. Alle ændringer i systemerne laves på baggrund af en RFC (Request For Change). Alle RFC gemmes som dokumentation. Udførsel af ændringen

dokumenteres i SystemGruppens Sagssystem (Portlr). Konfigurationsfiler til netværksenheder (firewall, routere, switche og lignende) ligger gemt som strukturerede filer et centralt sted.
Sikkerhedspolitikken sætter de grundlæggende politikker for SystemGruppens infrastruktur og omhandler ikke forhold vedrørende specifikke produkter, ydelser eller brugere.

Sikkerhedspolitikken er udarbejdet, så SystemGruppen har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Minimum én gang om året gennemgås politikker, procedurer og den operationelle drift med henblik på forbedringer.

HR, medarbejdere og uddannelse

SystemGruppen er Certificeret Microsoft Partner med sølv kompetence på cloud solutions.

Alle udførende konsulenter har kompetencer inden for de områder, de beskæftiger sig med. Det dokumenteres ved hjælp af relevante certificeringer fra teknologiudbyderene. SystemGruppen er som nævnt certificeret Microsoft Partner, og kravene for at opretholde denne status er høje.

SystemGruppen skal leve op til en række krav fra Microsoft, herunder specifikke krav om at et bestemt antal konsulenter har bestået bestemte produktcertificeringer, som løbende skal fornyes. SystemGruppen sikrer via løbende produkttræning og kursusdeltagelse at opretholde denne høje certificeringsstatus.

Ved ansættelse bekræfter nye medarbejdere med sin underskrift, at de har læst SystemGruppens it-sikkerhedspolitik og at de forpligter sig til at overholde denne.

SystemGruppens direktør meddeler ændringer i sikkerhedspolitikken til medarbejderen umiddelbart efter at ændringerne træder i kraft.

Styring af aktiver

Alle enheder (computere og smartphones samt tablets) som SystemGruppens medarbejdere benytter er indmeldt i Microsoft Intune MDM. Medarbejdere kan ikke få adgang til SharePoint Online og Teams hvis ikke enheden er tilmeldt Intune og overholder en række politikker der er opsat i Intune (krav omkring kode, firewall aktiv, kryptering af harddisk etc.).

Intune overvåger hele tiden alle enheder og ændrer deres compliance status hvis ikke de overholder de satte politikker – dermed lukkes for adgangen til SystemGruppens data automatisk.

Brugerstyring/ adgangssikkerhed

Firewalls
Fysiske firewalls administreres af Curanet.

SystemGruppen administrerer således kun den logiske adgangssikkerhed. Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne.

Password:
Der gennemtvinges password skift hver 90. dag for alle i SystemGruppen.

Der er aktiveret en lockout politik, som betyder, at hvis man taster sit kodeord forkert 5 gange, bliver kontoen låst i 30 minutter, eller indtil SystemGruppens teknikere låser den op.

SystemGruppens IT-brugere modtager en mail 10 dage før password udløber. Denne mail gensendes indtil password er skiftet, eller den pågældende konto er udløbet.

Minimum password age:
Minimum password age er et døgn.

Krav til password:

- Adgangsordenes kompleksitet dikteres jf. Microsofts standard
- Kodeord skal være 12 karakter lang, og koden skal indeholde 3 ud af 4 typer karakterer; store og små bogstaver, tal og specieltegn
- Kodeord må ikke være en del af brugerens navn eller mailadresse
- Der må ikke bruges et password, som har været anvendt de sidste 24 gange

Pauseskærm
Pauseskærm er aktiveret hos alle SystemGruppens brugere for at beskytte dem mod uautoriseret adgang. Pauseskærm aktiveres via Group Policy, således den gennemtvinges på alle computere. Pauseskærmen aktiveres automatisk efter 10 min inaktivitet på den pågældende computer. Jf. SystemGruppens sikkerhedspolitik skal alle brugere slå pauseskærmen til, når de forlader arbejdspladsen.

Adgang til systemer
Der gives kun adgang til de systemer, der er relevante for den enkelte medarbejder.

Adgange styres centralt via GPO- og AD-rettigheder. Det kan også meldes ud på mail eller på informationsmøder, hvis der er politikker, man ønsker overholdt, eller politikker som tvinges ned over medarbejderne med GPO´er eller lignende. Disse politikker kan træde i kraft øjeblikkeligt.

De separate kundemiljøer adskilles vha. VLANs, som er opdelt gennem firewallen. Delte kundemiljøer separeres via AD sikkerhedsgrupper.

Når en medarbejder forlader SystemGruppen, afleverer vedkommende sin PC, telefon og nøgler til SystemGruppens lokaler. Medarbejderens konto bliver lukket samme dag, herunder VPN-adgang.

Log over oprettede medarbejdere og deres brugerrettigheder bliver gennemgået én gang pr. måned for at sikre at denne er ajourført.

Fysisk sikkerhed

Den fysiske sikkerhed i datacenteret varetages af Curanet. SystemGruppen har således ingen kontroller vedr. den fysiske sikkerhed.

SystemGruppen kontrollerer den fysiske sikkerhed vha. den årlige 3402 erklæring fra Curanet.

Fysisk sikkerhed hos kunder er kundernes eget ansvarsområde.

Drift af hostingaktiviteterne

Faste driftsopgaver udføres med faste intervaller. Disse opgaver styres af supporten med koordinatoren.

Derudover er der Firewalls og routere med redundans på relevante services.

Centrale servere/services køres der patch management på. Det aftales typisk med kunden, på hvilke tidspunkter dette skal udføres. Serveren vil hente nyeste opdateringer, og vil herefter genstarte (med mindre backup stadig er kørende). En rapport over, hvilke servere og hvilke opdateringer der er lagt på, og hvordan det er gået, sendes til kundeansvarlig og/eller kunden.

Backup

Formålet med backup er at sikre, at kundens data i SystemGruppens datacenter kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid.

Der er altid minimum 3 ugers backup-historik. En primær backup bliver placeret i datacenteret, mens en sekundær backup er placeret på en sekundær lokation.

SystemGruppen kontrollerer dagligt kundernes backup ved at gennemgå logs fra backupserverne. Denne kontrol og afhjælpning af evt. fejlbeskeder er beskrevet i en procedure for backup kontrol.

To gange hver dag laves der snapshots (volume shadow copy) af alle virtuelle filservere.

Restore test af backups er kundernes ansvar. Som udgangspunkt laver SystemGruppen således ikke restore test af backups. Dette er fremhævet i SystemGruppens standardaftale vedr. hosting jf. følgende formulering:

" SystemGruppen afvikler ikke test af restore samt validitetscheck af data, da det alene er Kunden, der kan godkende validiteten af genskabte data.

Tid forbrugt på restore af data, til testformål eller som er mistet som følge af forhold udenfor System-Gruppens kontrol, afregnes til gældende timesats."

Curanet sørger for, at harddiske og lagermedier der udgår fra driften, bliver destrueret på en måde, så det ikke er muligt at genetablere de ødelagte data igen. Alle genbrugte diske bliver formateret i overens-stemmelse med gældende branchestandarder.

I de tilfælde, hvor SystemGruppen har kopieret data til USB nøgler, skal data fra disse medier slettes (USB formateres) efter endt brug.

Overvågning

Overvågning finder sted inden for normal arbejdstid. Dvs. alarmer og meldinger fra den automatiske del af overvågningen vil kun blive set og reageret på inden for normal arbejdstid.

Overvågningen omfatter:

- Overvågning af backup jobs
- Overvågning af onlinestatus på servere
- Overvågning af diskforbrug
- Overvågning af CPU forbrug på virtuelle servere
- Overvågning af RAM forbrug på virtuelle servere
- Overvågning af services på servere

Overvågningen sker med udgangspunkt i en fastlagt baseline for de enkelte målepunkter. Målingerne fastholdes i en daglig statusrapport.

Overvågningen giver SystemGruppen mulighed for at kunne opdage fejl eller overbelastning i tide og derved kunne iværksætte proaktive handlinger for at formindske nedetid. Fejl der konstateres i forbin-delse med overvågningen håndteres jf. de fastlagte procedurer for håndtering af fejl og nedbrud.

Der er ikke specifik overvågning af brugere med administrator rettigheder. Dog er Security log aktiveret på alle servere, som kan bruges til dokumentation.

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.

Alle servere med adgang fra internettet og terminalservere med Windows opdateres manuelt 1 gang månedligt. Med mindre den pågældende leverandør har sendt en modsat anbefaling, læses alle patches ind. Der laves ikke test af patches, inden de indlæses.

SystemGruppen har udarbejdet en fall back plan i forbindelse med patch management. Formålet med fall back planene er at sikre, at systemerne kan komme tilbage i normal drift, hvis opdateringen ikke virker efter hensigten.

Ændringer i systemerne udføres jf. den fastlagte Request for Change procedure.
SystemGruppen har et beredskab, som kan udføre patches og opdateringer døgnet rundt på alle årets dage.

Kommunikationssikkerhed

For at beskytte vores kunder mod Cyberkriminalitet, har vi indført følgende systemer:

Anti-Spam
Alle indgående mails skal igennem et spam filter, hvor de scannes og checkes for Antivirus/malware og Cryptolocker/Extortions, hvis der er tvivl ligges mailen i karantæne. Kunden kan få fremvist mailen i en SSL sikret browser og kan bede om udlevering hvis der er tale om en falsk positiv.

Anti-virus
Alle servere er beskyttet med ESET Endpoint Antivirus. Dette beskytter mod mange forskellige typer malware. Scanningen kører i reel tid og hele tiden. Trusler sættes i karantæne.

Terminal servere
Alle terminal servere er konfigureret med AppLocker. AppLocker beskytter med afvikling af ukendte programmer. Styring af hvilke programmer brugerne må afvikles håndteres med Active Directory sikkerhedsgrupper. Programmer der ikke er eksplicit godkendt i systemet, blokeres automatisk.

Gateway Security
Alt internet trafik scannes og checkes med Fortigates sikkerhedspakke på alle vores firewall's, dette indbefatter blandt andet både antivirus og Intrusion Prevention Service (IPS) for at sikker at de data der hentes og sendes overholder gældende standard og ikke er fyldt med ondsindet data, Hvis der findes mistænkeligt indhold, droppes datapakken.

Leverandørforhold

SystemGruppen benytter kun velrenommerede, gennemprøvede kvalitetsleverandører, som er i stand til at levere den aftalte kvalitet. Alle SystemGruppens leverandører er oprettet i SystemGruppens kreditorsystem.

Minimum én gang årlig gennemgås de væsentligste leverandører for deres leveringsevne, kvalitet, pris og service.

Datakapacitet fremskaffes primært hos Curanet A/S og Microsoft Azure.

SystemGruppens egne servere er placeret i Curanet A/S lokaler i Skanderborg. Curanet varetager drift af serverne op til det virtuelle niveau i de respektive datacentre. Samarbejdet og ansvarsfordelingen reguleres af en formel aftale mellem parterne.

Samarbejdet og ansvarsfordelingen mellem SystemGruppen og Microsoft reguleres af Microsofts SLA for de forskellige Azure og MS365 services.

SystemGruppen sikrer kvaliteten af Curanets datacenter ved at indhente en kopi af den årlige 3402 erklæring. Tilsvarende kontrollerer SystemGruppen kvaliteten i Microsofts Cloud leverancer ved at undersøge, hvilke standarder Microsoft forpligter sig til at leve op til. Dette gøres ved regelmæssige besøg på Microsofts trustcenter hjemmeside:
https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings.

Styring af it-sikkerhedshændelser

Sikkerhedshændelser og svagheder i SystemGruppens systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Hændelsen registreres i SystemGruppens sagsstyringssystem (Portlr) med angivelse af, hvem der har anmeldt hændelsen. Ved en sikkerhedshændelse adviseres SystemGruppens Tekniske Chef med det samme – i dennes evt. fravær adviseres SystemGruppens direktør.

Alle medarbejdere hos SystemGruppen er bekendt med procedure for rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af SystemGruppens drift.

Ledelsen har ansvaret for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Beredskabsstyring

SystemGruppen har en beredskabsplan, som beskriver i hovedtræk, hvordan man skal håndtere en katastrofesituation. Planen indeholder overordnet en punktopstilling, hvoraf det fremgår, hvilke systemer og i hvilken rækkefølge man skal genetablere driften.

Ved alvorlige fejl sendes en mail til mailgruppen "SG Teknisk Afd". Mailen indeholder en kort fejlbeskrivelse og en tidshorisont på nedetiden. Som afslutning på fejl retning sendes en ny mail til mailgruppen om, at fejlen er løst og en uddybende fejlbeskrivelse.

Ved totalskade på datacenteret er der udarbejdet en plan for, hvordan datacenteret etableres hos en anden datacenter serviceleverandør baseret på den foreliggende backup.

Beredskabsplanen testet én gang pr. år jf. den procedurer som fremgår af planen.

Kundernes ansvar (komplementerende kontroller hos kunderne)

Ovenstående beskrivelse er baseret på ovennævnte ramme, hvilket betyder, at der ikke tages højde for den enkelte kundes aftale.

Ansvaret for de forretningssystemer og brugersystemer, som drives via SystemGruppens hosting aktiviteter, eller kundernes egne servere som driftes af SystemGruppen, er kundernes eget ansvar. Kunderne har ansvaret for sikring af nødvendige kontroller i forbindelse med systemudvikling, anskaffelse og ændringshåndtering.

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

Kunderne er ansvarlige for datatransmission til SystemGruppens hosting aktiviteter, og det er kundernes ansvar at skabe den nødvendige datatransmission til SystemGruppens datacenter. Kunden skal selv sikre de nødvendige kontroller i tilknytning til dette kontrolmål.

SystemGruppens beredskabsstyring er konstrueret omkring en overordnet beredskabsplan, som beskriver tilgangsmåde og handlinger ved behov for reetablering af SystemGruppens hosting aktiviteter. Der kan udarbejdes specifikke beredskabsplaner for den enkelte kunde efter behov i forhold til risiko ved afbrydelse i forretningsprocesser.

BILAG 1:

SystemGruppen A/S har arbejdet med følgende kontrolmål og sikkerhedsforanstaltninger fra ISO27002:2013

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

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

12. Driftssikkerhed
- 12.1. Driftsprocedurer og ansvarsområder
- 12.2. Malwarebeskyttelse
- 12.3. Backup
- 12.4. Logning og overvågning
- 12.5. Styring af driftssoftware
- 12.6. Sårbarhedsstyring

13. Kommunikationssikkerhed
- 13.1. Styring af netværkssikkerhed

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

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af de generelle it-kontroller, deres udformning og funktionalitet

Til kunder af SystemGruppen A/S' hostingaktiviteter og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om SystemGruppen A/S' beskrivelse i kapitel 2 (inkl. bilag 1), som er en beskrivelse af kontrolmiljøet i tilknytning til driften af SystemGruppen A/S' hostingaktiviteter i hele perioden 1. februar 2021 - 31. januar 2022, 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, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. SystemGruppen A/S anvender i forhold til grundlæggende kontrolmiljø eksterne samarbejdspartnere på følgende områder: datacenter (den fysiske sikkerhed omkring produktionsmiljøet).

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.

SystemGruppen A/S' ansvar

SystemGruppen A/S 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 – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vi er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om SystemGruppen A/S' 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 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 i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som SystemGruppen A/S 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 SystemGruppen A/S

SystemGruppen A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en SystemGruppen A/S, 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 SystemGruppen A/S' generelle it-kontroller til hostingaktiviteter, således som de var udformet og implementeret i hele perioden 1. februar 2021 - 31. januar 2022, 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. februar 2021 - 31. januar 2022, 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. februar 2021 - 31. januar 2022.

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 System-Gruppen A/S' 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 selv har udført ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Søborg, den 2. juni 2022

Beierholm
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Allan Nielsen
IT-auditor, Konsulent

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 ISO27002:2013.

Hvad angår periode har vi i vores test forholdt os til, om SystemGruppen A/S har levet op til kontrolmålene i perioden 1. februar 2021 - 31. januar 2022.

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som SystemGruppen 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 SystemGruppen A/S. 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 udviklingen og driften af hostingaktiviteter. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

SystemGruppen A/S' 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 hostingaktiviteter. 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 hostingaktiviteter arbejdes med en løbende vurdering af den risiko, som opstår, som følge af de forretningsmæssige forhold og deres udvikling. Vi har kontrolleret, at risikovurderingen er forankret ned igennem de organisatoriske niveauer. Vi har ved interview 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.

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
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 gennemgået SystemGruppen A/S' 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 af virksomhedens ledelse, og at den er gjort tilgængelig internt for medarbejderne.	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.

SystemGruppen A/S' 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. Der foreligger passende forretningsgange for medarbejdere omkring angivelse af tavshedserklæring.	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. Vi har ved interview med passende medarbejdere kontrolleret, at de er bekendt med deres roller og de tilhørende ansvarsområder. Gennem forespørgsler og stikprøve på ansættelsesaftaler har vi kontrolleret, at medarbejdere i SystemGruppen A/S er bekendte med deres tavshedspligt.	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 foreligger formelle politikker i forbindelse med anvendelse af mobilt udstyr og fjernarbejdspladser. Ifm. anvendelsen af fjernarbejdspladser hos SystemGruppen A/S har vi gennemgået, hvorvidt der er implementeret passende sikkerhedsforanstaltninger, i form af to faktor godkendelse.	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.

SystemGruppen A/S' 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 SystemGruppen A/S. 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 fortrolighedspligt via en underskrevet ansættelseskontrakt og via SystemGruppen A/S' sikkerhedspolitik.	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 i forhold til ansættelse og ansættelsesophør. Vi har ved interview kontrolleret, at væsentlige medarbejdere er bekendt med deres tavshedspligt. Vi har påset, at SystemGruppen A/S' ansættelseskontrakt har et afsnit omkring tavshed, som følge af information opnået ifm. arbejde udført hos SystemGruppen A/S.	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. Virksomheden skal sikre, at informationsaktiver får et passende beskyttelsesniveau.

SystemGruppen A/S' 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 ansvarlig for alle væsentlige aktiver.	Vi har gennemgået og kontrolleret virksomhedens centrale it-register for væsentlige it-enheder og kontrolleret at der er tildelt en ansvarlig for de væsentlige aktiver.	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.

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
Der foreligger dokumenterede og ajourførte retningslinjer for SystemGruppen A/S' adgangsstyring.	Vi har forespurgt på og kontrolleret at procedurer for adgangsstyring samt at disse er opdaterede.	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 påset dokumentation for at der anvendes passende autorisationssystemer i relation til adgangsstyring i SystemGruppen A/S. Vi har påset, at den formaliserede forretningsgang for tildeling og afbrydelse i brugeradgange er implementeret, 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 stikprøver påset at der eksisterer en formaliseret forretningsgang for opfølgning på kontrol af autorisationer i henhold til retningslinjerne. Vi har påset at der foretages løbende formel opfølgning på registrerede brugere mindst én gang om måneden.	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 på og gennemgået procedurer for tildeling af adgangskoder i SystemGruppen A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Adgange til systemer og netværk er beskyttet med password. Der er opsat kvalitetskrav til password, således at der kræves en minimumslængde (12 karakterer, indeholdende 3 ud af 4 typer karakterer; store og små bogstaver, tal og specialtegn) og maksimal løbetid (max 90 dage), lige som password opsætninger medfører, at password ikke skabes ud fra navn eller mailadresse og ikke kan genbruges (husker de seneste 24 versioner). Endvidere bliver brugeren lukket ude efter 10 minutters inaktivitet.	Vi har forespurgt, om der er etableret procedurer, der sikrer kvalitetspassword i SystemGruppen A/S. Vi har ved inspektion af GPO 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 • lockout efter inaktiv periode	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.

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er dokumenteret driftsafviklingsprocedurer for forretningskritiske systemer, og den 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. Vi har i forbindelse med revisionen af de enkelte driftsområder kontrolleret, at der foreligger dokumenterede relevante procedurer, samt at der sker løbende dokumentationen af de handlinger som udføres. Vi har påset, at der er etableret procedurer for on-boarding af nye kunder. Vi har kontrolleret at brugere med administrative rettigheder 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 kapacitetsovervågning som sikrer, at der kan ske skalering i forhold til kundebehov samt kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har ved stikprøve og interview med passende personale kontrolleret, 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: Malwarebeskyttelse

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

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
Der er etableret både forebyggende, opklarende og udbedrende sikrings- og kontrolforanstaltninger, herunder den nødvendige uddannelses- og oplysningsindsats for virksomhedens brugere af informationssystemer mod skadevoldende programmer.	Vi har forespurgt på og inspiceret de procedurer/kontrolaktiviteter, der udføres i tilfælde af virusangreb- eller udbrud. Vi har ved interview med passende personale kontrolleret, at der foretages aktiviteter, som gør medarbejdere opmærksomme på forholdsregler ved virusangreb eller udbrud. Vi har kontrolleret, at servere har installeret antivirusprogrammer og inspiceret dokumentation for, at der sker rettidig gennemgang og opdatering.	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.

SystemGruppen A/S' 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. Vi har stikprøvevist gennemgået backupprocedurer, til bekræftelse af at de er formelt dokumenterede. Vi har stikprøvevist gennemgået backup-log, for bekræftelse af at backup er gennemført succesfuldt, og at tilfælde af mislykket backup håndteres rettidigt.	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.

SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. SystemGruppen A/S har aktiveret security log på alle servere. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt.	Vi har forespurgt ledelsen om de procedurer/ kontrolaktiviteter der udføres, og påset, at security log er aktiveret. Vi har stikprøvevis påset, at security logs er aktiveret. Vi har ved interview med passende personale kontrolleret, at der foretages løbende og 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 driftsafdelingen. Kritiske alarmer afgives også pr. mail. Der indmeldes statusrapporter pr. mail fra forskellige systemer. Nogle dagligt – andre når der opstår en hændelse i systemet. Der sker en daglig kontrol af statusrapporter.	Vi har forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. Vi har påset, at der anvendes overvågningsværktøj, samt at dette er tilgængeligt for relevante medarbejdere. Vi har påset, at der afgives alarmer pr. mail ved opståede fejl. Vi har stikprøvevis gennemgået statusrapporter. Vi har påset, at der er etableret en driftsvagt, samt denne tjekker rapporter dagligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål: Styring af driftssoftware samt sårbarhedsstyring

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

SystemGruppen A/S' 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 change management i SystemGruppen A/S. Vi har ved stikprøvevis inspektion påset, at der anvendes passende procedurer for kontrolleret idriftsætning af ændringer til SystemGruppen A/S' produktionsmiljøer. Vi har påset at ændringer til produktionsmiljøet i SystemGruppen A/S 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 SystemGruppen A/S. 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 der er udarbejdet 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	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.		
SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
Netværk skal beskyttes mod trusler for at sikre netværksbaserede systemer og de transmitterede data.	Det er kontrolleret, at der er er implementeret den fornødne beskyttelse mod uautoriseret adgang, herunder: • at der er etableret funktionsadskillelse omkring centrale roller • at der er procedurer og ansvar for styring af netværk inkl. fjernarbejdspladser • at de fornødne lognings- og overvågningsprocedurer er etableret	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 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
SystemGruppen A/S' kontroller	Revisors test af kontroller	Resultat af test
Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til leverandører håndteres.	Det er kontrolleret, at der findes formelle samarbejdsaftaler i forbindelse med anvendelse af eksterne samarbejdspartnere. Vi har 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 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 indhentning af 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.

SystemGruppen A/S' 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 de 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.

SystemGruppen A/S' 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 hostingaktiviteter i SystemGruppen A/S. Vi har påset, • at der er udarbejdet passende rammer for udarbejdelse af beredskabsstyring • at der er udarbejdet og implementeret en beredskabsplan • at planen indeholder passende strategi og procedurer for kommunikation med SystemGruppen A/S' interessenter • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen • at der sker test og afprøvning af beredskabsplanen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.