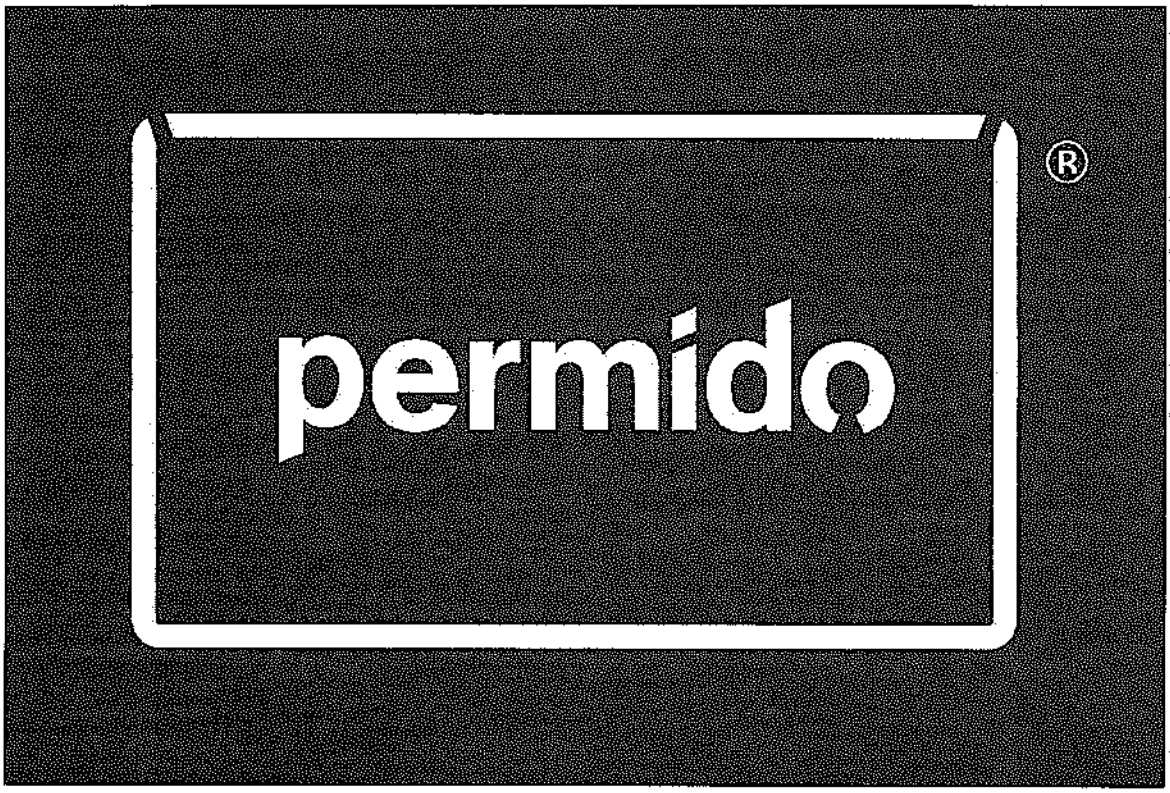

DATABEHANDLERAFTALE

Kunden

(herefter benævnt "Dataansvarlig")

og

Permido A/S
Linnés Allé 2
2630 Taastrup
Tlf.: +45 7023 1123

CVR-nr.: 32890806

(herefter benævnt "Databehandler")

(herefter samlet benævnt "Parterne" og hver for sig "Part")

har indgået følgende databehandleraftale ("Aftalen") om Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige:

1. Indledning

1.1 Permido A/S er et binavn for Zentura A/S.

1.2 Permido er produktet, der leverer sikker krypteret kommunikation mellem den dataansvarlige og dennes kunder og andre interne som eksterne kontakter.

1.3 Zentura A/S CVR-nr.: 32890806 står for driften af Permido. I det omfang persondata deles inden for gruppens selskaber (Permido A/S, Zentura A/S) repræsenterer denne Databehandleraftale også hele koncernens politik i forhold til dit privatliv og sikkerhed af dine persondata.

1.4 Hos Permido A/S tager vi beskyttelsen af dine oplysninger alvorlig. Derfor er Permido A/S også omfattet af Zentura's ISAE 3402 II certificering og Cloudcertifikatet.

2. Baggrund, formål og omfang

2.1 Som led i den Dataansvarliges indgåelse af aftale om levering af tjenesten, Permido Krypteret Mail (herefter benævnt "Permidoaftalen"), som beskrevet i Aftalens bilag 1, foretager Databehandleren behandling af personoplysninger, som den Dataansvarlige er ansvarlig for.

2.2 Databehandleren skal overholde lovgivningens til enhver tid stillede krav til databehandlere, herunder fra den 25. maj 2018; Persondataforordningen (Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) med tilhørende retsakter og heraf afledt national lovgivning.

2.3 Det er et krav i Persondatalovgivningen, at der mellem den dataansvarlige og databehandleren indgås skriftlig aftale om den behandling, som skal foretages; en såkaldt 'databehandleraftale'. Denne Aftale udgør sådan en databehandleraftale.

3. Personoplysninger omfattet af aftalen

3.1 Denne Aftale omfatter alle typer personoplysninger, som beskrevet i Aftalens bilag 1.

4. Geografiske krav

4.1 Den behandling af persondata, som Databehandleren foretager efter aftale med den Dataansvarlige, må alene foretages af Databehandleren eller underdatabehandlere, jf. pkt. 6, indenfor det Europæiske Økonomiske Samarbejde (EØS). Databehandleren er ingenlunde berettiget til at lade databehandling foregå udenfor EØS uden den Dataansvarliges skriftlige samtykke, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

5. Instruks

5.1 Omfanget af de opgaver, som Databehandleren skal levere og understøtte, betyder, at der i medfør af Parternes aftale, Permidoaftalen, vil ske forskellige former for behandling af personoplysninger. De forskellige former for behandling af personoplysninger er beskrevet i Aftalens bilag 1.

5.2 Denne Aftale og tilhørende instruks omfatter de kategorier af registrerede, som er anført i bilag 1.

5.3 Databehandleren skal så vidt muligt bistå den Dataansvarlige med opfyldelse af den Dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder, herunder om indsigt, berigtigelse, begrænsning eller sletning, hvis de relevante personoplysninger behandles af Databehandleren. Modtager Databehandleren sådan henvendelse fra den registrerede, orienterer Databehandleren den Dataansvarlige herom.

5.4 Den Dataansvarlige hæfter for alle Databehandlerens omkostninger ved sådan bistand, herunder til underdatabehandlere. Databehandlerens bistand afregnes til Databehandlerens til enhver tid gældende timetakst for sådant arbejde.

6. Brug af underdatabehandler

6.1 Den Dataansvarlige giver Databehandleren samtykke til anvendelse af underdatabehandlere, forudsat at de i Aftalen stillede betingelser for dette er opfyldt. Databehandleren underretter den Dataansvarlige om sådanne underdatabehandlere.

6.2 Underdatabehandleren er under Databehandlerens instruks. Databehandleren har indgået skriftlig databehandleraftale med underdatabehandleren, hvori det er sikret, at underdatabehandleren opfylder krav tilsvarende dem, som stilles til Databehandleren af den Dataansvarlige i medfør af Aftalen.

6.3 Omkostninger forbundet med etablering af aftaleforholdet til en underdatabehandler, herunder omkostninger til udarbejdelse af databehandleraftale og eventuel etablering af grundlag for overførsel til tredjelande, afholdes af Databehandleren og er således den Dataansvarlige uvedkommende.

6.4 Såfremt den Dataansvarlige måtte ønske at instruere underdatabehandlere direkte, kan dette alene ske efter drøftelse med og via Databehandleren. Hvis den Dataansvarlige afgiver instruks direkte overfor underdatabehandlere, skal den Dataansvarlige senest samtidig underrette Databehandleren om instruksen og baggrunden for denne. Hvor den Dataansvarlige instruerer underdatabehandlere direkte, a) er Databehandleren fritaget for ethvert ansvar, og enhver følge af sådan instruks er alene den Dataansvarliges ansvar, b) hæfter den Dataansvarlige for enhver omkostning, som instruksen måtte medføre for Databehandleren, herunder er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al arbejdstid, som en sådan direkte instruks måtte medføre for Databehandleren og c) den Dataansvarlige er selv ansvarlig overfor underdatabehandlere for enhver omkostning, vederlag eller anden betaling til underdatabehandleren, som den direkte instruks måtte medføre.

6.5 Databehandleren anvender p.t. de i Aftalens bilag 1 nævnte underdatabehandlere til de i bilaget anførte opgaver.

6.6 Den Dataansvarlige accepterer ved indgåelsen af nærværende Aftale, at Databehandleren er berettiget til at skifte eller tilføje en underdatabehandler, forudsat, at a) en eventuel ny underdatabehandler overholder tilsvarende betingelser, som stilles i nærværende pkt. 6 til nuværende underdatabehandlere.

7. Behandling og videregivelse af personoplysninger

7.1 Den Dataansvarlige indestår for at have den nødvendige hjemmel til behandling af personoplysningerne omfattet af nærværende Aftale.

7.2 Databehandleren må ikke uden skriftligt samtykke fra den Dataansvarlige videregive oplysninger til tredjemand, medmindre sådan videregivelse følger af lovgivningen eller af en bindende anmodning fra en retsinstans eller en databeskyttelsesmyndighed, eller det fremgår af denne Aftale.

8. Sikkerhed

8.1 Databehandleren skal træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen, jf. pkt. 2.2 ovenfor.

8.2 Databehandleren er via sit medlemskab hos Brancheforeningen for IT-hostingvirksomheder i Danmark ("Danish Cloud Community") certificeret indenfor IT-hosting ("Cloudcertifikatet") og skal dermed overholde certificeringsguidens krav til sikkerhed. Derudover skal Databehandleren, jf. pkt. 8.1, implementere og opretholde de i bilag 2 beskrevne sikkerhedsforanstaltninger og i øvrigt opfylde de i Permidoaftalen stillede krav.

8.3 Databehandleren er altid berettiget til at implementere alternative sikkerhedsforanstaltninger under forudsætning af, at sådanne sikkerhedsforanstaltninger som minimum opfylder eller giver større sikkerhed end de i Cloudcertifikatet og bilag 2, jf. pkt. 8.2, beskrevne sikkerhedsforanstaltninger og i øvrigt opfylder de i Permidoaftalen stillede krav til sikkerhed.

8.4 Databehandleren skal efter nærmere aftale med den Dataansvarlige, så vidt muligt, bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i forordningens artikel 32 (gennemførelse af passende tekniske og organisatoriske foranstaltninger), 35 (foretagelse af konsekvensanalyse vedrørende databeskyttelse) og 36 (forudgående høring). I den forbindelse er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådan aftale måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandlere.

8.5 Såfremt det i pkt. 8.4 anførte fører til skærpede krav til sikkerhedsforanstaltninger i forhold til det allerede aftalte mellem Parterne i medfør af denne Aftale, implementerer Databehandleren, så vidt det er muligt, sådanne foranstaltninger, forudsat at Databehandleren modtager betaling herfor, jf. pkt. 8.6 nedenfor.

8.6 Omkostninger forbundet med implementering af foranstaltninger, jf. pkt. 8.5, afholdes af den Dataansvarlige og er således Databehandleren uvedkommende. Databehandleren er endvidere berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådan implementering måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

9. Tilsynsret

9.1 Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige informationer til, at denne kan påse, at Databehandleren har truffet de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger.

9.2 I det omfang den Dataansvarlige tillige ønsker, at dette skal omfatte den behandling, som sker hos underdatabehandlere, oplyses Databehandleren om dette. Databehandleren indhenter herefter tilstrækkelige oplysninger fra underdatabehandleren.

9.3 Såfremt den Dataansvarlige ønsker at foretage tilsyn, som anført i dette pkt. 9, skal den Dataansvarlige altid give Databehandleren et varsel på mindst 30 dage i sådan forbindelse.

9.4 Dataansvarlig kan én gang årligt hente Databehandlerens sikkerhedsrevisionsrapport jf. pkt 9.5 på hjemmeside: https://help.permido.com//da/start.

9.5 Sikkerhedsrevisionsrapporten er udarbejdet af en alment anerkendt og uafhængig tredjepart, som garantere, at sikkerhedsrevisionsrapporten er udarbejdet i overensstemmelse med en anerkendt revisionsstandard (fx ISAE 3402 II med referenceramme til ISO 27002:2014 eller lignende). I sikkerhedsrevisionsrapporten tages der stilling til Databehandlerendes overholdelse af kravene til sikkerhedsforanstaltninger i overensstemmelse med Databehandlerens certificering hos Danish Cloud Community, jf. pkt 8.2 ovenfor og Aftalens bilag 2. Som medlem af Danish Cloud Community certificeres Databehandleren én gang om året til at bruge Cloudcertifikatet, som bl.a. indeholder en ISAE 3402 II med referenceramme til ISO 27002. Ved Databehandlerens fremsendelse af en kopi af det opdaterede Cloudcertifikat og tilhørende ISAE 3402-erklæring med referenceramme til ISO 27002 opfylder Databehandleren kravet i denne bestemmelse.

9.6 Såfremt den Dataansvarlige ønsker at få udarbejdet anden eller yderligere sikkerhedsrevisionsrapport udover de i pkt. 9.4 og 9.5 omtalte, eller at der i øvrigt ønskes foretaget tilsyn af Databehandlerens eller underdatabehandlerens persondatabehandling, herunder såfremt den Dataansvarlige ønsker sikkerhedsrevisionsrapport udarbejdet på et nærmere bestemt tidspunkt, aftales dette nærmere med Databehandleren. Databehandleren eller underdatabehandleren kan til enhver tid kræve, at en sådan sikkerhedsrevisionsrapport udarbejdes i overensstemmelse med en anerkendt revisionsstandard (fx ISAE 3402 med referenceramme til ISO 27002:2014 eller lignende) af en alment anerkendt og uafhængig tredjepart, som beskæftiger sig med sådanne forhold.

9.7 Den Dataansvarlige afholder alle omkostninger i forbindelse med tilsyn af sikkerhedsforhold, jf. pkt. 9 hos Databehandleren samt i forhold til underdatabehandleren, herunder er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådant tilsyn måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

10. Persondatasikkerhedsbrud

10.1 Såfremt Databehandleren måtte blive bekendt med et persondatasikkerhedsbrud, hvorved forstås et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, er Databehandleren forpligtet til uden unødig forsinkelse at søge at lokalisere sådan brud og søge at begrænse opstået skade i videst muligt omfang, samt i det omfang det er muligt reetablere eventuelt mistede data.

10.2 Databehandleren er endvidere forpligtet til uden unødig forsinkelse at underrette den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden. Databehandleren skal herefter uden unødig forsinkelse, i det omfang det er muligt, give skriftlig meddelelse til den Dataansvarlige, som så vidt muligt skal indeholde:

a) En beskrivelse af karakteren af bruddet, herunder kategorierne og det omtrentlige antal berørte registrerede og registreringer af personoplysninger.

b) Navn på og kontaktoplysninger for databeskyttelsesrådgiveren.

c) En beskrivelse af de sandsynlige konsekvenser af bruddet.

d) En beskrivelse af den foranstaltninger, som Databehandleren eller underdatabehandleren har truffet eller foreslår truffet for at håndtere bruddet, herunder foranstaltninger for at begrænse dets mulige skadevirkninger.

10.3 For så vidt det ikke er muligt at give de i pkt. 10.2 anførte oplysninger samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

10.4 Tilsvarende er underdatabehandlere pålagt uden unødig forsinkelse at underrette Databehandleren i overensstemmelse med pkt. 10.2 og 10.3.

11. Tavshedspligt

11.1 Databehandleren skal holde personoplysningerne, som behandles i henhold til Aftalen fortrolige, og er således alene berettiget til at anvende personoplysningerne som led i opfyldelsen af sine forpligtelser og rettigheder i henhold til Aftalen, herunder skal Databehandleren pålægge medarbejdere og eventuelle andre, herunder underdatabehandlere, der er autoriseret til at behandle de af Aftalen omfattede personoplysninger, fortrolighed om disse. Sådan fortrolighed finder tillige anvendes efter Aftalens ophør.

12. Forrang

12.1 Medmindre andet fremgår af Aftalen, har bestemmelser i Aftalen forrang i forhold til tilsvarende bestemmelser i andre aftaler mellem parterne, herunder Permidoaftalen.

13. Varighed og ophør af databehandleraftalen

13.1 Aftalen træder i kraft ved Parternes underskrift.

13.2 I tilfælde af at Permidoaftalen ophører, uanset årsag, ophører Aftalen også.

13.3 Aftalen kan ikke opsiges særskilt, men kan erstattes af en anden databehandleraftale om samme forhold. I modsat fald, er Databehandleren forpligtet af denne Aftale, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige.

13.4 Den Dataansvarlige skal snarest muligt og senest 14 dage efter ophør af Permidoaftalen skal oplyse Databehandleren skriftligt, hvorledes Databehandleren skal forholde sig til de behand-

lede personoplysninger. 30 dage efter ophøret af Permidoaftalen er Databehandleren berettiget til at slette alle personoplysninger, som er blevet behandlet under den ophørte Permidoaftalen på vegne af den Dataansvarlige.

14. Underskrift

14.1 Ovenstående tiltrædes hermed med virkning fra Parternes underskrift.

14.2 Nærværende Aftale er underskrevet i to ligelydende eksemplarer, hvoraf hver af Parterne beholder ét.

15. Bilag

Bilag 1: Beskrivelse af baggrunden for og formålet med Aftalen mv.
Bilag 2: Beskrivelse af sikkerhedsforanstaltninger
Bilag 3: Zentura IT Sikkerhedspolitik

, den

For den Dataansvarlige

Taastrup, den 4/5-2021

Christian Lindegaard Jensen

For Databehandleren

BILAG 1 – BESKRIVELSE AF BAGGRUNDEN FOR OG FORMÅLET MED AFTALEN MV.

1. Baggrunden for og formålet med Aftalen

1.1 Denne Aftale er indgået i forbindelse med Parternes indgåelse af aftale om levering af tjenesten, Permido Krypteret Mail, i hvilken forbindelse Databehandleren foretager behandling af personoplysninger på vegne af den Dataansvarlige til opfyldelse af aftalens formål.

1.2 Formålet med behandlingen af personoplysninger er overordnet set, at sikre din forsendelse af krypteret mails.

2. Typer af personoplysninger omfattet af aftalen

2.1 Aftalen og tilhørende instruks omfatter alle typer personoplysninger, som behandles af Databehandleren i henhold til den mellem Parterne indgåede aftale. Der er tale om følgende oplysningstyper:

Personoplysninger til oprettelse af en Permido konto:	**Personoplysninger i forbindelse med kundedata:**	**Personoplysninger for slutbrugerdata:**
Firmanavn	Firmanavn	Navn
Adresse	Navn	E-mailadresse
E-mailadresse	E-mailadresse	Telefonnummer
Telefonnummer	Telefonnummer	
CVR-nummer	Indholdet i selve de krypteret beskeder kan ikke tilgås af Zentura og slettes løbende.	Indholdet i selve de krypteret beskeder kan ikke tilgås af Zentura og slettes løbende.
Betalingsoplysning		

3. Brug af underdatabehandlere

3.1 Databehandleren anvender ved Aftalens indgåelse nedenstående, af den Dataansvarlige godkendte underdatabehandlere, til at foresta de anførte behandlingsopgaver.

System	Company name	CVR	Address	Description of data processing tasks	Personal Data
Backend	InMobile	31426472	Axel Kiers Vej 18I 8270 Højbjerg	SMS Gateway	Mobile number
Backend	CPSMS hos Compaya A/S	31375428	Palægade 4, 2. tv 1261 København K	SMS Gateway	Mobile number
Backend	Microsoft Office 365		One Microsoft Way Redmond WA 98052 USA	Office 365 applications used general purposes. (Ex. writing emails to customers). Exchange Online as mail-server. Onedrive for storing generalt documents.	Customer name, address, phone, email
Backend	Fenerum	40430989	Viby Ringvej 11, 1. tv 8260 Viby J Denmark	Used for invoicing	Customer name, address, phone, email
Backend	Stripe		San Francisco (HQ), CA United States	Creditcard payments	Customer payment information

			510 Townsend St, San Francisco		
Backend, Portal	Microsoft Azure Holland		One Microsoft Way Redmond WA 98052 USA	Permido's infrastructure used for sendeing at recieving encrypted mail is placed at Microsoft Azure Netherlands. Micosoft employees does not have acces to Permido data or servers.	Encrypted mails, unencrypted tmp flles, unecrypted log files
Backend	Interxion	25147022	InterXion Danmark ApS Industriparken 20A DK - 2750 Ballerup	The database where the encrypted Permido mails is store is placed in Zenturas Datacenter in Denmark.	Encrypted mails
Backend	E-conomic	29403473	Visma e-conomic a/s CVR: 29403473 Langebrogade 1 1411 København K. Danmark	Used for invoicing customers	Customer name, address, phone number, email
Customer communication	Mailchimp		The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	Mailchip opbevarer alle brugers navn og emailadresse. Brugerne kan til en hver tid framelde sig systemet. Mailchimp's GDPR funktioner er desuden slået til for at sikre compliance.	Customer name, email
Customer communication	Hubspot		HubSpot, Inc. 25 First Street, 2nd Floor Cambridge, MA 02141 USA	CRM system to store end user and reseller contact information, pipeline of opportunities. We store name, email adress, phone number, company name, website,	names, company adresses, email adress, phone number, company name, website,
Internal communication	Slack		San Francisco (HQ) CA United States 500 Howard St San Francisco	Internal communication	Customer name, email, communication

BILAG 2 – BESKRIVELSE AF SIKKERHEDSFORANSTALTNINGER

1. INDLEDNING

1.1 Dette bilag udgør det bilag, der refereres til i pkt. 8.2 i Aftalen.

1.2 Bilaget beskriver de sikkerhedsforanstaltninger, som Databehandleren anvender i forbindelse med den fysiske, tekniske og organisatoriske sikkerhed i forbindelse med Databehandlerens levering af tjenester.

1.3 Databehandleren er via sit medlemskab hos Brancheforeningen for IT-hostingvirksomheder i Danmark ("Danish Cloud Community ") certificeret indenfor IT-hosting ("Cloudcertifikatet").

2. FYSISK SIKKERHED

2.1 Brand, strømafbrydelser, oversvømmelser m.v.

For beskrivelse se venligst Bilag 3 Zentura IT Sikkerhedspolitik – Den gældende IT Sikkerhedspolitik kan til enhver tid rekvireres pr. email: (service@zentura.dk)

Indhold

IT Sikkerhedspolitik 2021

Indledning

Denne informationssikkerhedspolitik er den overordnede ramme for informationssikkerheden hos Zentura. Politikken understøtter Zentura IT's værdigrundlag som er:

Troværdighed, Service og Ansvarlighed

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

Version	Dato	Ændring	Godkender
1.0	31. august 2015	Komplet it-sikkerhedspolitik	CP
1.1	16. august 2017	Gennemgang og mindre rettelser	CLJ & AFH
1.2	03. oktober 2017	Mindre rettelser / stavefejl	CLJ
1.3	05. juli 2018	Opdatering af patchprocess og mindre rettelser	CLJ
1.4	23. januar 2019	Mindre opdatering	CLJ
1.5	25. februar 2019	Afsnit om adgang til trådløst netværk tilføjet.	CLJ
1.6	5. juni 2019	Årlig revidering af hele dokumentet.	CLJ
1.7	4. maj 2021	Mindre rettelser	CLJ

Vores kerneydelser

Vi er specialister i rådgivning, implementering, drift og vedligeholdelse af forretningskritiske it-løsninger, og tilbyder vores kunder forskellige typer af hosting. Vi har særlig fokus og kompetencer indenfor rådgivning, opsætning, opgradering, drift og vedligehold af Citrix løsninger. Vi sætter kvalitet og pålidelighed i højsædet, og da langt de fleste af vores produkter og services leveres i realtid, har vi naturligvis 24/7/365 kundeservice, monitorering og lover aldrig mindre end 99,7% tilgængelighed. For at garantere vores ydelser vedligeholder vi løbende vores systemer, vores kompetencer og vores dokumentation.

Vi er vores kunders' it-afdeling og håndterer alle aspekter forbundet hermed.

Vores it-sikkerheds fokusområder

Informationer og informationssystemer er nødvendige og livsvigtige for Zentura, og informationssikkerheden er derfor af vital betydning for virksomhedens troværdighed og funktionsdygtighed.

It-sikkerhed har højeste prioritet hos os og i de services vi tilbyder vores kunder. Vi lever af vores it, vi har derfor et beskyttelsesniveau der afspejler dette.

Vi har implementeret fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, som har til

hensigt at forhindre datakompromittering, tab, tyveri, misbrug. Tilsvarende har vi etableret foranstaltninger i forhold til forsyningssikkerhed, både hvad angår teknik og kommunikationssikkerhed. Vi har i vores interne organisering lagt væk på funktionsadskillelse, produktdokumentation og standardiserede arbejdsprocesser, med hvilke vi tilsikrer en høj grad af personuafhængig leverancesikkerhed. Adgange til vores systemer og data, som jo er kernen i vores forretning, er baseret på jobfunktion og altid efter vurdering af det konkrete behov. Fortrolighed, både om egne forhold og kundeforhold, er reguleret i hhv. medarbejder og kundekontrakter.

Gyldighedsområde

Vores it-sikkerhedspolitik er gældende for alle vores aktiviteter og services, uanset om disse udføres af ansatte i virksomheden eller en af vores samarbejdspartnere.

Det er vores administrerende direktør, som er den øverst ansvarlige for vores aktiviteter og services.

Medarbejdere, der bryder de gældende informationssikkerhedsbestemmelser, kan straffes disciplinært. De nærmere regler om dette fastsættes i overensstemmelse med den gældende personalepolitik.

Vores it-sikkerhedspolitik er ligeledes gældende for vores service- og underleverandører, som har adgang til Zenturas systemer.

Denne it-sikkerhedspolitik ajourføres efter behov, og gennemgås i sin helhed minimum én gang om året.

Risikovurdering og– håndtering

Vi arbejder målrettet og kontinuerligt på at minimere trusler mod vores forretning og services. For at strukturere arbejdet omkring risikovurdering, samler vi dette i en risikoanalyse, som bliver ajourført minimum én gang årligt, samt ved ændringer i trusselsbilledet.

Vi har i vores risikoanalyse registreret og gennemgået de risici vi i vores forretning er eksponeret mod og i. På baggrund af analysearbejdet har vi kategoriseret vores risici efter væsentlighed, og vi har klassificeret samtlige forhold i 4 niveauer, hvor P1 er det højeste niveau, og P4 det laveste. For særlige risici har vi udarbejdet detaljerede beredskabsplaner.

IT-sikkerhedsstyring

Vi har en samlet it-sikkerhedspolitik (indeværende dokument), samt en medarbejderrettet version af vores it-politik, som er målrettet brugere som ikke nødvendigvis er it-kyndige. Den medarbejderrettede it-politik er en del af personalehåndbogen, som alle medarbejdere får udleveret ved ansættelse. Alle medarbejdere har pligt til at holde sig orienteret om den til hver en tid gældende it-sikkerhedspolitik.

Organisering af sikkerhed

Intern organisering

Det er vores direktør, Christian Pedersen, som er den øverste ansvarlige for virksomhedens drift, herunder for informationssikkerheden i virksomheden. Den daglige ledelse, herunder ansvaret for it-sikkerhedspolitikker, dokumentation og opfølgning, er uddelegeret til driftschef Christian Lindegaard. Denne ledelsesforankring er med til at sikre, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger vi har fastlagt, gennemføres og efterleves. Alle medarbejdere modtager vores Personalehåndbog ved opstart, og såfremt en medarbejder, i ord eller handling bryder nærværende it-sikkerhedspolitik eller deraf afledte retningslinjer, vil medarbejderen blive udsat for disciplinære forholdsregler i overensstemmelse med Zentura's gældende regler og personalepolitik.

Mobile enheder og fjernarbejdspladser

Vi ønsker at sikre vores mobile enheder og fjernarbejdspladser på en måde der gør, at vi, og vores kunder, aldrig skal spekulere på hvorvidt medarbejderne har de bedste muligheder for at udføre deres arbejde – lige meget hvor de er, og hvornår de skal arbejde. Uden at sætte virksomhedens data i fare.

Derfor benytter vi internt præcis de samme mobile device management løsninger, som vi sælger vores kunder. Således sikrer vi os et ensartet højt sikkerhedsniveau uanset om vi er på kontoret eller arbejder hjemmefra. Vi benytter to-faktor-verificering til forbindelser uden for kontoret, og på kontoret benyttes udelukkende tynde klienter (Citrix Recievere).

Mobile enheder, som mobiltelefoner, underlægges en række ufravigelige policies. Vi tillader alene email, kalender og adressebogsadgang via mobiltelefon.

Får en medarbejder eksempelvis stjålet sin telefon foretages en fuld sletning (full wipe) af telefonen, og telefonens id annulleres på vores Exchangemiljø, hvorefter enheden ikke kan modtage data fra os. Det vil derefter ikke være muligt at tilgå vores netværk via den pågældende telefon.

Sikkerhed i forhold til HR

Inden ansættelse

Vi prioriterer integritet højt i alle aspekter af vores forretning. Dette afspejles ligeledes i vores personale, hvor vi forud for ansættelse indhenter referencer efter behov. Straffeattester kontrolleres også altid, også for eksterne konsulenter, som måtte få adgang til vores netværk. Vi godkender ikke konsulenter, ansatte eller andet personel, som er dømt for svindel eller anden kriminalitet der kan påvirke deres evne til at udføre deres arbejdsopgaver. Skal medarbejderen ansættes, udarbejdes kontrakt og en række andre praktiske opgaver initieres, jf. procesbeskrivelse 'Nyansættelse'.

Elever, for hvem ansættelseskontrakt arrangeres direkte mellem elev og skole, indhentes ligeledes

straffeattest. Elever anses for almindelige medarbejdere, hvorfor alle medarbejderregler, processer og procedurer også finder anvendelse for eleverne. Se desuden procesbeskrivelse 'Nyansættelse – Elev'.

For konsulenter, som skal have adgang til (dele af) vores netværk, udarbejdes altid opgavespecifik kontrakt og dedikeret fortrolighedserklæring (NDA) forud for opgavestart.

Det er virksomhedens COO, som er ansvarlig for at alle HR processer og procedurer overholdes, og virksomhedens størrelse taget i betragtning varetages disse opgaver typisk af ham selv.

Under ansættelse

Efteruddannelse af medarbejdere vurderes og tildeles løbende i dialog medarbejder og chef imellem, og mindst én gang årligt ved medarbejderudviklingssamtalen.

Ophør eller ændring i ansættelse

Ændres en medarbejders arbejdsområder, orienteres medarbejderen om de sikkerhedsmæssige forhold som måtte være forskellige fra medarbejderens nuværende rolle i forhold til den nye rolle. Medarbejderens systemadgange opdateres jf. procesbeskrivelse 'Ændring_medarbejder'.

Er der tale om ophør af et ansættelsesforhold de-aktiveres medarbejderens adgange mv, jf. procesbeskrivelse 'Fratrædelse_medarbejder'.

Styring af aktiver

Fortegnelse over aktiver

Virksomhedens aktiver registreres i et eDocs dokument. Her registreres al hardware og softwarelicenser. Småanskaffelser som tynde klienter, mus, tastaturer, og skærme registreres ikke. Servere og infrastrukturrelateret hardware konfigurationer og tekniske forbindelser er tillige dokumenteret i dedikeret driftsdokumentation (eksempelvis netværkstegninger, systemdokumentation), med henblik på at kunne genskabe en eller flere af virksomhedens services.

Ejerskab af aktiver

Virksomhedens direktør er ansvarlig for samtlige it-services, herunder infrastruktur som netværk, firewall og andre kommunikationsforbindelser. Det er driftschefen som er ansvarlig for at systemdokumentationen til enhver tid er opdateret.

Dataklassifikation

Klassifikation af data

Vi foretager ingen klassifikation af data, og vi differentierer ikke ydelser baseret på datatyper.

Håndtering af aktiver

Ingen af vores databærende aktiver har virksomhedsdata installeret lokalet, der er alene standard

Microsoft software installeret. Vores netværk, data mv. kan kun tilgås via Citrix, hvorfor selve aktivet i den forstand er værdiløst. Ved ansættelse udleveres en mobiltelefon, en bærbar computer (til brug for når vi sidder fysisk hos Kunder, hvormed vores medarbejdere altid kan tilgå Citrix, uden at være afhængige af Kundens it-udstyr), skærme, tastatur, mus, bordtelefon og en tynd klient. Ved ansættelsesophør tilbageleveres samme udstyr. Udstyret er ikke følsomt over for tyveri, idet ingen af tingene i sig selv kan give adgang til virksomhedsdata.

For licenser er vi, som hosting forretning, licenseret via vores SPLA aftaler. Opgørelse af licenser udarbejdes månedligt og indberettes direkte til relevante licensudbydere. Opgørelserne gemmes per måned, per år.

Fysiske dokumenter med fortrolig- og/eller kundespecifik dokumentation bliver samlet i dedikeret, aflåst beholder på kontoret, og når beholderen er fyldt, bliver indholdet af beholderen destrueret ved sikkerhedsgodkendt makuleringsfirma.

Mediehåndtering

Bortskaffelse af medier

Vi har ingen databærende medier, andet end serverrumsmedier. Hvis en disk går i stykker bliver den udskiftet af en af vores medarbejdere og bragt tilbage til kontoret. Herfra sørger hardware leverandøren for at afhente og destruere mediet, hvilket er en del af vores indkøbsaftale med vores sikkerhedsgodkendte leverandør. Ved udlevering af defekt hardware til destruktion kvittes med underskrift fra begge parter.

Får en medarbejder eksempelvis stjålet sin telefon foretages en fuld sletning (full wipe) af telefonen, og telefonens id annulleres på vores Exchangemiljø. Det vil derefter ikke være muligt at tilgå vores data via den pågældende telefon. Vi anvender ikke lokale medier som eksempelvis USB-sticks til opbevaring af data.

Adgangskontrol

Politik for adgangsstyring

Alle adgange tildeles efter funktionsbehov og jobroller. Vi gennemfører intern kontrol af tildelte adgange to gange årligt (april og oktober), ligesom opdatering af adgange er faste kontroller i vores HR processer for hhv. nyansættelse og ophør- eller ændring i ansættelse. I vores tildeling af adgange arbejder vi ud fra nødvendighedsprincippet, under hensyntagen til personuafhængighed, således at vi altid kan servicere vores kunder.

Alle brugere er personhenførbare, og der anvendes funktionsopdeling i rettighedstildeling for samtlige netværk og tilhørende AD-politikker. Som ekstra adgangskontrol, når man logger på uden for kontoret, benytter vi to-faktor-verificering. Dette gælder for alle, også vores kunder.

Adgang til netværk og netværksservices

Det er alene medarbejdere, som har rettigheder på netværk og netværksservices. Kunder har altid kun adgang til eget netværk, og ingen kunder har administratorrettigheder.

Adgang til netværk og netværksservices som switche, routere og firewalls varetages af os selv. Ingen andre end vores medarbejdere kan tilgå dette, ej heller leverandører. Fysisk er udstyret placeret i eget rack hos Interxion, hvor kun vores tekniske personale har adgang. Interxion har revisorerklæring fra uafhængig ekstern it-revisor, som er afgivet uden forbehold. Vores backup site, hvor vores management server og backup's er placeret, er ligeledes installeret i eget rack hos Global Connect (Nianet).

Vi har segmenterede netværk, og AD'er er aldrig trustede. Vi har et driftsnetværk, som er det netværk vi bruger til den daglige drift. Vi har et management netværk, som alene kan tilgås fra vores driftsnetværk, og herfra kontrolleres de fælles infrastrukturkomponenter og de andre netværk. Dertil har vi et netværk per kunde. Hvert netværk har eget AD med dedikerede policies.

Servicebrugere kan aldrig bruges til at logge på netværket.

Adgang til trådløst netværk

Zenturas trådløse netværk er delt op i et gæstenetværk og et internt netværk.

Gæstenetværket er til Zenturas gæster er alene en internetforbindelse adgangen er begrænset af en gangskoder der udløber efter et døgn. Der er ikke adgang fra gæstenetværket til Zenturas interne netværk.

Zenturas interne trådløse netværk må og kan kun benyttes af Zenturas medarbejdere.

Brugeradgange

Alle brugeradgange sker på baggrund af formel godkendelse, uanset om det er interne brugere eller kundebrugere. Brugeroprettelses- og nedlægningsprocedurer for interne brugere er beskrevet i dedikerede HR procesbeskrivelser. Review af interne brugere gennemføres minimum to gange årligt.

Kodeordet til administrative fællesbrugere (fx root passwords og admin) er dokumenteret og opbevaret i dedikeret og betryggende sikret database, som kun virksomhedens indehavere har adgang til. Samme er desuden fysisk opbevaret i et brandsikret skab på kontoret, samt i ekstern bankboks i landsdækkende bank. Det er alene virksomhedens to ejere som har adgang til disse fællesbrugere, herunder til de fysisk opbevarede passwords. Nøglerne til den fysiske bankboks opbevares privat hos virksomhedens indehavere.

Kunders brugere oprettes efter kundespecifikke aftaler, og kunder har aldrig adgang til andet end deres eget domæne. Passwords til kundeinstallationer gemmes og deles i Remote Desktop Manger, hvor alle brugere er personhenførbare, og hvor vi til hver en tid kan verificere hvem der har logget på hvilken kunde, hvad de har foretaget sig, hvornår de har logget på og hvor længe de har været logget på. Når en medarbejder har været logget på en server, skal medarbejderen lave en kort note om årsagen til logon, førend forbindelsen til serveren afbrydes. Brugeradministration er til hver en tid kundens ansvar.

Rettighedstildeling

Rettigheder tildeles alene på baggrund af funktion og jobrolle. Alle rettigheder på Zenturas egen infrastruktur er bundet op i Access grupper i Active directory, det er lavet i en ROLE/ACCESS model hvor ACCESS giver adgang til specifikke ressourcer og ROLE er en mængde af access grupper.

Brugeransvar

Hver medarbejder er ansvarlig for at sikre egen authentifikationsinformation, og retningslinjer for samme oplyses i it-afsnittet i vores Medarbejderhåndbog, som udleveres ved ansættelse. Vores passwords, herunder personlige passwords, genereres via Remote Desktop Manager. Zentura følger Microsoft standard for best practice om at password skal skiftes hver 3. måned (90 dage) og være af en vis kompleksitet.

Kontrol af adgang til systemer og data

Kontrol af adgange til vores systemer er af højeste prioritet. Vores produkt er sikre it-ydelser, og alle vores kunder anbefales at sætte samme høje sikkerhedsstandard, som os selv.

Da alle brugere er personhenførbare kan vi til hver en tid verificere hvem der har logget på hvilken kunde, hvad de har foretaget sig, hvornår de har logget på og hvor længe de har været logget på. Dette er gældende for samtlige af vores systemer. Ved 5 fejlslagne AD login forsøg, spærres kontoen i 30 min. Ved 3 fejlslagne SMS PASSCODE login forsøg, spærres SMS PASSCODE kontoen i 5 minutter. Dette gentages yderligere 3 gange. Fejler brugeren SMS PASSCODE indtastning 4. gang, lukkes brugeren ude permanent. Alle logins, succesfulde som fejlede, logges.

Vi benytter software til at gemme og dele kunde-adgangskoder. Brugerens rettigheder i dette software er funktionsspecifikke, ligesom alle andre adgange.

Det er alene virksomhedens ejere, som har adgang til root passwords, både de elektronisk opbevarede, og de fysisk opbevarede.

Kildekode til egenudviklet, intern, software kan kun tilgås af virksomhedens ejere. Der er ingen kunder der benytter den egenudviklede software.

Styring af adgang til kildekoder til programmer

Kildekode til egenudviklede programmer gemmes på Github. Alle versioner gemmes. Egenudviklede programmer bruges udelukkende til interne opgaver, de sælges ikke til kunder, og kan ikke tilgås udefra.

Kryptografi

Dataintegritet og beskyttelse af egne og kunders' oplysninger er af største betydning for vores forretning. Således er al trafik til og fra Zentura's netværk beskyttet med SSL certifkater som er trusted af GlobalSign, og vi benytter ikke nøgler under 2048 bit. Der benyttes ikke selfsigned certifikater til ekstern trafik.

Fysiske og miljømæssige sikringer

Fysisk skalsikring

Vi ønsker at beskytte vores udstyr og data bedst muligt, ingen for at sikre vores kunder den størst mulige sikkerhed for uafbrudt service og sikkerhed.

Al vores udstyrer placeret i eget rack hos Interxion, hvor kun vores tekniske personale har adgang. Vores backup udstyr er placeret i eget rack hos Nianet. Begge datacenterleverandører har revisorerklæringer, som vi årligt indhenter.

Vores fysiske kontor er placeret i Taastrup. Uden for vores kontoråbningstid (8-16) er alle indgangsdøre aflåst, og tyverialarm er sat til. Zentura deler kontorbygning med Orbicon, men har egen indgang der er aflåst når der ikke er Zentura medarbejdere tilstede. I kontortiden er døren ved den bemandede reception åben, alle andre døren kræver brug af adgangskontrol brik. Det skal bemærkes at ingen data kan tilgås blot ved at have adgang til vores fysiske kontor. Tyverialarmen tilsluttes automatisk på hverdage efter kl. 19. Tilslutning af tyverialarmen kan udskydes en time ad gange ved brug af medarbejderens udleverede adgangskontrolbrik. Alle medarbejdere har personlig registreret nøgle, til Zenturas aflåste område.

Beskyttelse mod eksterne og miljømæssige trusler

Al vores udstyr er placeret i eget rack hos Interxion, hvor kun vores tekniske personale har adgang. Vores backup udstyr er placeret i eget rack hos Nianet. For begge leverandører henviser vi til deres revisorerklæringer, som er afgivet uden forbehold.

Placering og beskyttelse af udstyr

Al vores udstyrer placeret i eget rack hos Interxion, hvor kun vores tekniske personale har adgang. Vores backup udstyr er placeret i eget rack hos Nianet. Begge leverandører har revisorerklæringer, som er afgivet uden forbehold.

Det er alene vores SMS PASSCODE service der kan blive berørt hvis vores fysiske kontor måtte holde op med at eksistere, idet de 3 modemmer er placeret i vores krydsfedt. Disse modems indeholder ingen data, det er alene distribution af GSM-trafik. Disse modems har ingen betydning for servicen, idet en webservice tager over, såfremt modems bliver utilgængelige.

Virksomhedens udstyr registreres i et Excel ark. Her registreres al hardware.

Databærende udstyr, som ikke længere er funktionelt, sørger hardware leverandøren for at afhente og destruere, hvilket er en del af vores indkøbsaftale med vores sikkerhedsgodkendte leverandør. Ved udlevering af defekt hardware til destruktion kvitteres med underskrift fra begge parter.

Databærende medier

Vi har ingen databærende medier, undtaget serverrumsmedier og mobiltelefoner. Fra mobiltelefon er der udelukkende adgang til e-mail, adressebog og kalender. Mobiltelefonen påtvinges desuden en række sikkerhedspolitikker, hvilket blandet andet giver os adgang til at slette indholdet af telefonen uden at have fysisk adgang til telefonen.

Sikkerhed i forbindelse med drift

Dokumenterede driftsprocedurer

For at tilse en ensartet høj kvalitet i vores ydelser, samt for at beskytte os mod personafhængigheder, har vi dokumenterede driftsprocedurer og SOP'er. I vores organisation er det ikke muligt at have 100% overlap på alle opgaver, systemer og kompetencer hvorfor det er afgørende at alle medarbejdere følger faste procedurer i deres daglige arbejde.

Alle kunder har eget VLAN, og der er ingen adgang VLAN i mellem. Alle kundespecifikke programmer mv, håndteres i tæt samarbejde med kunden og kundens programleverandør. En kundes programleverandør har aldrig adgang til andet end kundens domæne. Alle kundepasswords lagres i Remote Desktop Manager, hvor vi kan se hvilke medarbejdere der har tilgået hvilken kunde, hvornår logon er foregået, hvor længe man har været på, og hvad der er udført af handling.

Netværkssikkerhed

Management af vores kunder foregår via et VLAN i vores eget miljø. Dette kan kun tilgås via vores kontor i Taastrup, og via hjemmearbejdspladser med fast VPN. Det er alene virksomhedens driftstekniske ejere, som har fast VPN fra deres hjemmearbejdsplads. Har man ikke fast VPN, eller sidder på kontoret i Taastrup, kan man kun tilgå vores miljø via SMS PASSCODE igennem vores Netscaler Gateway. Fra vores eget driftsmiljø er der en række firewall regler der tillader trafik fra vores VLAN ud til vores kunders VLAN samt VPN forbindelser fra vores VLAN ud til relevante eksterne samarbejdspartnere. Det skal bemærkes, at der alene er åbnet for management porte til at sikre connectivity access, dvs. Citrix, SSH, HTTP(S), RDP og Telnet, og vi har således ikke eksempelvis fil adgang til kundenetværk fra vores driftsnetværk. Alt management af vores core-infrastruktur udstyr ligger i et andet netværk, som kun kan tilgås fra vores driftsnetværk, det vil sige at man skal først på vores driftsnetværk, og derfra via firewall regler bliver man verificeret og får adgang til de nødvendige ressourcer i core-netværket der skal til for at opnå rettigheder til eksempelvis at ændre konfigurationer på core-udstyret.

Vi har en dedikeret management server som kan tilgås direkte i core-netværket via RDP fra kontoret i Taastrup, eller fra hjemmearbejdspladser med fast VPN. I tilfælde af fejl på vores management server har vi en backup management server, som alene kan tilgås fra kontoret. De dublerede servere, og mulighed for adgang fra hjemmekontorer er etableret med det formål at sikre driftsstabilitet og uafbrudte services af vores miljø, idet at vi i tilfælde af nedbrud på core-udstyr kan tilgå management serveren remote via vores trusted locations.

Ændringsstyring

Vi prioriterer sporbarhed og driftssikkerhed i gennem hele vores forretning. Vi opdeler derfor vores ændringer efter type, og for alle ændringer klassificeret 'STD Change' skal der som minimum dokumenteres en ændringsbeskrivelse, en implementerings- og en roll-back plan. Ændringer der ikke påvirker SLA med kunderne kan udføres i kontortiden og klassificeres som 'SOP'. Ændringer der akut 'Emergency Changes' kan gennemføres indenfor kontor tid, såfremt det på forhånd er godkendt af kunden, i et aftalt service vindue.

STD (Standard Request for Change):

Væsentlige ændringer i vores generelle driftssystemer eller core infrastruktur, som påvirker en eller flere kunder. Ændringer af denne type, kræver godkendelse af virksomhedens CTO/COO. Eksempel på ændringer af denne type er netværksændringer, ny infrastruktur hardware, ny host, opgradering af Exchange.

Ændringer med lav risiko, som typisk kun berører en enkelt kunde. Disse ændringer kan udføres af alle support medarbejdere med rettigheder til at udføre opgaven. Eksempel på ændringer af denne type er genstart af kundeserver (i dialog med kunden), installation af Citrix receiver, skift af brugerpassword, lås en bruger op. Disse ændringer kan gennemføres indenfor kontortid, såfremt det på forhånd er godkendt af kunden.

Patching:

Internt på ZIT's driftmiljø har vi en WSUS01 (Windows Update Services) server som er sat op til auto approve opdateringer (Security/Critical/Definition Updates).

Alle interne servere og kunde servere patches i weekenden, medmindre der er aftalt et alternativt service vindue med kunden. Udrulning af patches sker med Ivanti Automation Manager. Active directory og Witness Servere patches fredag 02:00 / lørdag 02:00, alle andre typer patches søndag 02:00.

3. parts software opdateres på alle servere opdateres som en del af den regulære patch process med Ninite Pro

En gang om ugen udtrækkes en WSUS report som viser patchniveauet på alle servere. Ved failed updates analyseres årsagen og der oprettes om nødvendigt en Change Request og opdatering udbedres.

CORE udstyr: Vi patcher ikke vores core udstyr med mindre vi har direkte addresseret problemer og efter anvisning af vores producent. Vi anser det for større risiko at få lagt en opdatering på som introducere en ukendt fejl da vi ikke har en platform hvor vi har et komplet testmiljø.

Vi opdaterer vores NetScaler hver 2. måned da NetScaler er et sikkerhedsprodukt med direkte adgang til internettet.

Citrix XenServer: Patches kun efter behov men vi overvåger releases om der er noget kritisk relevant.

Core Infrastruktur: Opdateres ikke løbende, og altid manuelt.

Alle kundeinitierede ændringer registreres i vores ticket system.

Kapacitetsstyring

Tilgængelighed er en af vores kerneværdier, og vi sætter en ære i altid at levere den forventede kvalitet i ydelser til vores kunder. Vi har valgt en strategi for både vores storage og servere, hvor vi

løbende og uden gene for kunderne, kan udvide vores kapacitet.

Vi overvåger derfor vores kapacitet med Zabbix, og vi monitorerer både disk, cpu og trafik. I udgangspunktet opererer vi med 90% utilization af hver kundes platform. Vi har alarmer på disk plads og availability, samt udvalgte services på serverne.

Adskillelse af test og produktionsfaciliteter

I kraft af vores kunde specificerede og dedikerede struktur er det ikke muligt at oprettet et validt test setup. Da vi alene opererer med dedikerede løsninger vil vi som udgangspunkt ikke kunne lave et reelt test billede af f.eks. en Windows security update derfor tester vi ikke updates etc. inden implementering.

Beskyttelse mod Malware

Vi anser Malware som en af de største trusler mod vores forretning, og vores tekniske foranstaltninger sikrer den højst mulige grad af sikkerhed for, at malware ikke kan afvikles i vores miljøer. Vi minimerer risikoen både i form af perimeter sikkerhed, men også skadesafgrænsning, skulle en hændelse opstå.

Vi benytter SecureDNS, som fungerer ved at alle forespørgsler på alle platforme sendes til CSIS som validerer at det pågældende opslag ikke er oprettet i en database over trusler. Hvis dette er tilfældet omskrives det svar til et HoneyPot site hvor brugeren får en besked om de prøver at tilgå et website som er hacked eller på anden måde er skadeligt.

Hvis der kommer kendt ransomware ind på vores system vil opkald til Command & Control server blive blokeret og ransomware vil blive uskadeliggjort. Vi abonnerer desuden på Platinum Alert Service fra CSIS, hvor CSIS sender nyhedsbreve om hvilken trusler der er i markedet, 0 day angreb og evt. hvilket patch der kan sikre systemerne. Alle alerts sendes til servicedesk hvor disse evalueres efter vigtighed / konkret trussels niveau.

Vi benytter desuden Applocker, således at kun kendt software kan eksekveres på kundernes Citrix Servere.

Ingen brugere er Administrator i den context de arbejder i, dvs. ingen brugere kan installere software eller manipulere software på en sådan måde, at det kan inficere systemer på "administrator" niveau. Hvis en bruger får malware i deres profil kan vi blot fjerne bruger profilen og lave en ny brugerprofil.

E-mail skanning varetages af FuseMail, både for os selv, og for vores kunder. Det er obligatorisk, og kan ikke fravælges. FuseMail benytter flere filter samt de har et PVR (Pre Virus Recognition) system hvor store batches af ens karakteristika mails bliver lagt i karantæne indtil de er undersøgt manuelt, hvorefter de så bliver frigivet.

Backup

På Zentura's hosting platform laves der Nutanix snapshot backup hver nat. Det vil sige at der laves en fuld kopi af samtlige data: serversystem filer, brugerdata, fil-services, databaser og alle andre data. Et snapshot udgør en komplet kopi af serveren i det øjeblik snapshot'et tages - uden datatab overhovedet. Efter hvert snapshot kopieres en kopi af snapshot'et over i det modsatte datacenter. Disse snapshots opbevares i 4 dage på det primæresite, således at restore kan udføres uden forudgående kopiering fra det sekundære datacenter. Alle snapshots opbevares i 30 dage på det sekundære datacenter. Denne politik benyttes både på Zentura's og kundernes servere og data.

På kunder med egen infrastruktur benyttes kundes eget backup system til backup og kundens egen politik følges.

Logning og overvågning

Hændelseslogning

Vi ønsker at vi til hver en tid kan dokumentere og kontrollerer udvalgte netværksaktiviteter, dels for at sikre transparens over for vores kunder, dels for at kontrollere at der ikke er uønsket aktivitet fra udefrakommende, og for at kunne verificere at ingen medarbejdere foretager sig noget der ikke er i overensstemmelse med deres arbejdsopgaver.

Vi benytter Remote Desktop Manager som er et klient/server system som benytter sig af AD credentials for den enkelte konsulent. Remote Desktop Manager logger alt access til kunde / interne systemer hos Zentura med tidspunkt/identitet for den bruger der ønsker at interagere med et objekt i Remote Desktop Manager – dvs. ved Password View, Connection, Disconnection etc. vil dette medføre en log entry.

Ved logoff på et kunde system skal konsulenten udfylde en kommentar om hvad adgangen har været brugt til. Dette er krævet ved lukning af remote adgang. Logfiler/data om forbindelser gemmes på en central database hvor kun virksomhedens ledelse har adgang.

Vores domain Controllere køre NTP tids synkronisering med en ekstern tids server hvilket garantere validitet i logfiler.

Styring af software på driftssystemer

Vores politik og proces for installation af programmer på driftssystemer, herunder patch management, er identisk med vores procedure for Ændringsstyring.

Styring af tekniske sårbarheder

Vores kundesystemer er sat op på en sådan måde, at brugerne ikke selv kan installere programmer.

Kommunikationssikkerhed

Netværksforanstaltninger

Vores forretning taget i betragtning er det af yderste vigtighed at vores kommunikationskanaler og netværk ikke kompromitteres. Vi har derfor etableret manuelle som tekniske foranstaltninger til at

sikre og kontrollere integriteten i vores ydelser.

Alle vores netværk er beskyttet af firewall, og vores netværk er opdelt hhv. per kunde og internt per funktion. Vores datacenter har to separat fremførte linjer, og vores SMS PASSCODE service, som alle vores kunder benytter, er redundant og tilknyttet to forskellige teleudbydere.

Alle datacenter komponenter samt internetforbindelsen bliver overvåget. Alle kritiske fejl på kritiske datacenter komponenter bliver distribueret via alm e-mail, push-besked og sms til- og håndteret af vores service-support medarbejdere.

Dataoverførelser

Dataintegritet og fortrolighed er en del af den tryghed vi leverer til vores kunder- Vi overfører derfor aldrig data ukrypteret. Ved overførsel af kundedata etableres en VPN tunnel site-to-site. Medarbejdere, som konsulenter, har ubetinget tavshedspligt i alt hvad vedkommende måtte blive bekendt med i medfør af sin stilling/opgave, hvilket er reguleret i samtlige ansættelses- og konsulentkontrakter.

Leverandørforhold

Sikkerhed i leverandøraftaler

Alle vores leverandør og partneraftaler skal indeholde regulering af fortrolighed. Samtlige aftaler skal ligeledes indeholde sikkerhedsmæssige forhold, eksempelvis forhold om monitorering, fortrolighed, immaterielle rettigheder og leverancesikkerhed.

Styring af serviceydelser fra tredjepart

Vi har identificeret vores væsentlige leverandører, og de risici der er forbundet med disse behandles særskilt i vores risikoanalyse.

Generelt har vi kritiske leverandørafhængigheder til to leverandører, hhv. interxion og Global Connect (Nianet). Der indhentes årligt revisorerklæringer fra begge leverandører.

Dertil har vi en afhængighed til vores mailskannings leverandør FuseMail, om end denne er mindre kritisk, idet funktionaliteten kan varetages af adskillige andre firmaer. FuseMail er i proces med it-revision, hvorfor vi forventer at kunne indhente revisorerklæring fra FuseMail fremadrettet.

It-sikkerhedspolitik for leverandører

Hvor vi bruger underleverandører og/eller eksterne konsulenter fører vi tilsyn med de aftalte leverancer, og disse skal ydes og leveres i henhold til vores it-sikkerhedspolitik.

Kundens ansvar

Kundernes ansvar er defineret i vores generelle forretningsvilkår, hvori det fremgår, at dataansvar til hver en tid er kundens eget. Således er kunden ansvarlig for vores instruktion, herunder for bl.a.:

- At klassificere egne data og særlige behov i den forbindelse
- Give besked om oprettelse og nedtagning af brugere (egen bruger administration)
- Alle typer af servicebestillinger hos Zentura

- Anmeldelse til Datatilsynet
- Egen beredskabsplanlægning
- Indhente Databehandleraftaler

Styring af sikkerhedshændelser

Ansvar og procedurer

Alle medarbejdere har et ansvar for at bidrage til at beskytte Zenturas informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri.

Alle medarbejdere bliver derfor løbende uddannet i informationssikkerhed i relevant omfang. Som brugere af Zenturas informationer må alle medarbejdere overholde informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf. Medarbejderne må kun anvende virksomhedens informationer i overensstemmelse med det arbejde, de udfører i virksomheden, og skal beskytte informationerne på en måde, som er i overensstemmelse med informationernes følsomhed, særlige og/eller kritiske natur.

Alle medarbejdere kan rapportere en hændelse. Der er rapporteringspligt.

Alle hændelser skal registreres. Registreringer må ikke slettes.

Rapportering af informationssikkerhedshændelser

En informationssikkerhedshændelse, en trussel mod informationssikkerheden, eller mistanke om samme, skal til hver en tid rapporteres straks til virksomhedens direktør. Alle skal indberette en hændelse/mistanke om en hændelse, og afhængig af hændelses karakter er det virksomhedens direktør, som fastlægger en handlingsplan for hvordan hændelsen skal håndteres og kommunikeres, internt som eventuelt eksternt. Det er ligeledes hændelsens karakter, som afgør hvilke beviser der skal indsamles.

Medarbejdere, som bryder informationssikkerhedspolitikken eller deraf afledte retningslinjer, vil blive udsat for disciplinære forholdsregler i overensstemmelse med Zenturas gældende regler og personalepolitik.

Vurdering af informationssikkerhedsbrud

Alle trusler og hændelser i forhold til informationssikkerhed bliver evalueret og vurderet af virksomhedens direktør og virksomhedens ejere. Det er virksomhedens direktør, som er den øverste ansvarlige for vurdering af sikkerhedshændelser.

Alle hændelser registreres med truslens karakter, ligesom hændelses- og vurderingshistorik dokumenteres. Såfremt hændelsen har sammenhæng med en ticket, registreres ticketnummer ligeledes. Alle hændelser bliver løbende opdateret med en statusangivelse, indtil hændelsen er afsluttet.

Reaktion og læring af informationssikkerhedsbrud

Alle sikkerhedsbrud dokumenteres og der laves en Root Cause Analysis af hændelserne, som gennemgås med alle relevante medarbejdere, eksempelvis ved månedsmøderne.

Afhængig af hændelsens karakter udarbejderes og gennemføres en Emergency Change (EC), så vi undgår at hændelsen indtræffer igen.

Sikkerhedsrelaterede emner, generelle emner såvel som aktuelle emner, gennemgås desuden ved interne månedsmøder, hvor vi af hensyn til vidensdeling og oplæring har faste indlæg ud over gennemgang af de daglige her-og-nu aktiviteter. Det er virksomhedens direktør, som er ansvarlig for afholdelse af- og indlæg på disse møder.

Giver hændelsen anledning til reevaluering af én eller flere risici, opdateres virksomhedens risikoanalyse tilsvarende.

Indsamling af beviser

Afhængig af hændelsens karakter bliver logoplysninger mv. straks sikret. Alle for hændelsen relevante oplysninger gemmes minimum så længe undersøgelsen af hændelsen pågår.

Informationssikkerhedsaspekter ved beredskabsstyring

Beredskabsplan

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af alle tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger er besluttet ud fra en afvejning af risici i mod sikringsomkostninger og vores kunde SLAs. Risikoanalyse og beredskabsplaner omfatter skadebegrænsende tiltag, etablering af temporære nødløsninger og genetablering af permanent løsning.

I vores beskedskabsplan tages højde for forretningskontinuitet, og forretningspåvirkning, herunder recovery time objective.

Afprøvning af beredskab

Vores beredskabsplan testes ved udvalgte senarier minimum en gang om året

Disaster Recovery Planer

Årligt testes en eller flere udvalgte scenarier ud fra en katastrofetilgang. Alt efter scenarie udføres skrivebords- som faktisk test. Hver D/R test indeholder afsluttede en testevaluering.

Redundans

Vi tilstræber 24/7/365 tilgængelighed, hvorfor alle vores VM's er High Availability. Vores daglige backup gemmes på sekundær lokation hos Nianet, hvorfra vi kan gendanne samtlige af vores hosting services.

Vores SMS PASSCODE service sender sms'er via to forskellige WebSMS Service providers (InMobile

og Compoya) i et redundant setup for alle kunder. Såfremt begge Service providers er nede, skiftes automatisk over til et fysisk modem placeret på kontoret i Taastrup.

Overensstemmelse

De af vores kunder, som behandler personfølsomme data, er selv ansvarlige for korrekt og relevant anmeldelse til Datatilsynet og/eller anden relevant myndighed og overholdelse af relevant lovgivning. Dette er specificeret i vores Generelle Forretningsvilkår.

Review af informationssikkerheden

Det er virksomhedens administrerende direktør, som er ansvarlig for at virksomhedens aktiviteter udføres i overensstemmelse med interne politikker og procedurer. It-sikkerhed er af højeste prioritet for os, hvorfor vi årligt bliver revideret af ekstern, uafhængig, it-revisor.

Vi udfører desuden løbene egenkontrol.