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.

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 medlem af Brancheforeningen for IT-hostingvirksomheder i Danmark ("Danish Cloud Community") og skal overholder deres certificeringskrav 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 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 garanterer, 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, aftalens bilag 2.

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 behandlede 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

Taastrup, den 8/12-2021

For den Dataansvarlige

Christian Lindegaard Jensen
For Databehandleren

Christian Lindegaard Jensen

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 forestå 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 files, 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

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)

Table of Contents

IT Security Policy 2021

Indledning

This information security policy is the overall framework for information security at Zentura. The policy supports Zentura's values which are:

Credibility, Service and Responsibility

As part of the overall security management, the management, on the basis of the ongoing monitoring and reporting, reviews the information security policy at least once a year.

Version	Date	Change	Approve
1.0	31 August 2015	Complete IT security policy	CP
1.1	August 16, 2017	Review and minor fixes CLJ & AFH	
1.2	03 October 2017	Minor corrections / misspellings	CLJ
1.3	05 July 2018	Update patch process and minor fixes	CLJ
1.4	January 23, 2019	Minor update	CLJ
1.5	February 25, 2019	Section on wireless network access added.	CLJ
1.6	June 5, 2019	Annual revision of the entire document.	CLJ
1.7	April 9, 2020	Annual revision of the entire document.	CLJ
1.8	28 May 2021	Annual revision of the entire document.	CLJ, DD
1.9	26 june 2021	Initial translation to English	CLJ, SH, DD
2.0	10 august 2021	Business Cloud 365 / Azure solution added.	SH

Our core services

We specialize in consulting, implementation, operation and maintenance of business-critical IT solutions, and offer our customers various types of hosting. We have special focus and competencies within consulting, setup, upgrading, operation and maintenance of Citrix solutions as well as Microsoft Azure solutions. We put quality and reliability first, and since the vast majority of our products and services are delivered in real time, we naturally have 24/7/365 customer service, monitoring and promise never less than 99.7% availability. To guarantee our services, we continuously maintain our systems, our competencies and our documentation.

We are our customers' IT department and handle all aspects related to this.

Our IT security focus areas

Information and information systems are necessary and vital for Zentura, and information security is therefore vital to the company's credibility and functionality.

IT security has the highest priority with us and in the services we offer our customers. We live off our IT, so we have a level of protection that reflects this.

We have implemented the necessary technical and organizational security measures, which are intended to prevent data compromise, loss, theft, misuse. Similarly, we have established measures in relation to security of supply, both in terms of technology and communication security. In our internal organization, we have put away on functional separation, product documentation and standardized work processes, with which we ensure a high degree of person-independent delivery security. Access to our systems and data, which is the core of our business, is based on job function and always after assessment of the specific need. Confidentiality, both about own relationships and customer relationships, is regulated in resp. employee and customer contracts.

Scope

Our IT security policy applies to all our activities and services, whether performed by employees of the company or one of our partners.

It is our CEO who is the one most responsible for our activities and services.

Employees who violate applicable information security regulations may be subject to disciplinary action. The detailed rules for this are determined in accordance with the applicable personnel policy.

Our IT security policy also applies to our service and subcontractors who have access to Zentura's systems.

This IT security policy is updated as needed and is reviewed in its entirety at least once a year.

Risk assessment and management

We work purposefully and continuously to minimize threats to our business and services. In order to structure the work around risk assessment, we gather this in a risk analysis, which is updated at least once a year, as well as changes in the threat picture.

In our risk analysis, we have registered and reviewed the risks we in our business are exposed to and in. Based on the analysis work, we have categorized our risks according to materiality, and we have classified all conditions in 4 levels, where P1 is the highest level, and P4 the lowest. For special risks, we have prepared detailed contingency plans.

IT Security Management

We have a comprehensive IT security policy (this document), as well as an employee-oriented version of our IT policy, which is targeted at users who are not necessarily IT-savvy. The employee-oriented IT policy is part of the personnel handbook, which all employees receive upon employment. All employees have a duty to stay informed about the IT security policy in force at any given time.

Organization of security

Internal organization

It is our director, Christian Pedersen, who is the chief responsible for the company's operations, including for the information security in the company. The day-to-day management, including responsibility for IT security policies, documentation and follow-up, has been delegated to Christian Lindegaard, Head of Administration. This management anchoring helps to ensure that the activities, standards, guidelines, controls and measures we have established, are implemented and complied with. All employees receive our Staff Manual at start-up, and if an employee, in word or deed, violates this IT security policy or guidelines derived therefrom, the employee will be subject to disciplinary action in accordance with Zentura's applicable rules and personnel policy.

Mobile devices and remote workstations

Business Cloud

We want to secure our mobile devices and remote workstations in a way that means we, and our customers, never have to wonder whether employees have the best opportunities to do their work - no matter where they are and when they have to work. Without compromising company data.

That is why we internally use exactly the same mobile device management solutions that we sell to our customers. Thus, we ensure a uniformly high level of security whether we are in the office or working from home. We use two-factor verification for connections outside the office, and in the office only thin clients (Citrix Recievere) are used.

Mobile devices, such as mobile phones, are subject to a number of mandatory policies. We only allow email, calendar and address book access via mobile phone.

For example, if an employee has his phone stolen, a full wipe of the phone is made, and the phone's ID is canceled on our Exchange environment, after which the device can not receive data from us. It will then not be possible to access our network via that phone.

Business Cloud 365

With regards to internal use of products like Sharepoint, One-drive, Exchange Online and other azure or Mircosoft 365 solutions we use Azure AD Conditional Access to enforce Multi-factor authentication from locations and WAN ip that was not designated as a trusted IP address . When signing on to a new device for the deadline MFA is need and then once every 30 days to make sure it's still the same user it's the case on all device Laptops, Phone and etc. All Zentura's windows 10 machines at managed by Intune (Microsoft Endpoint Manager) when connectiong from home the connect to the Citrix solution or AVD (Azure Virtual Desktop) when it has been put in to production. If a company laptop has been stolen, we can remotely wipe it via Intune. If a employees Mobile phone is lost they are required to remotely Wipe it, and we till remote the phone so it is not able to reconnected to our Exchange Online.

Security in relation to HR

Before hiring

We give high priority to integrity in all aspects of our business. This is also reflected in our staff, where we obtain references as needed prior to employment. Criminal records are also always checked, including for external consultants who may gain access to our network. We do not approve consultants, employees or other personnel who have been convicted of fraud or other crime that may affect their ability to perform their duties. Should the employee be hired, a contract is drawn up and a number of other practical tasks are initiated, cf. process description 'New employment'.

Students for whom the employment contract is arranged directly between student and school, a criminal record is also obtained. Students are considered ordinary employees, which is why all employee rules, processes and procedures also apply to students. See also process description 'New hire - Student'.

For consultants who must have access to (parts of) our network, a task-specific contract and a dedicated privacy statement (NDA) are always prepared prior to the start of the task.

It is the company's COO who is responsible for ensuring that all HR processes and procedures are complied with, and given the size of the company, these tasks are typically handled by himself.

During employment

Continuing education of employees is assessed and assigned on an ongoing basis in dialogue between the employee and the manager, and at least once a year at the employee development interview.

Termination or change of employment

If an employee's work areas are changed, the employee is informed about the safety conditions that may be different from the employee's current role in relation to the new role. The employee's system accesses are updated, cf. process description 'Change_Employee'.

In the event of termination of an employment relationship, the employee's accesses, etc. are deactivated, cf. process description 'Resignation_employee'.

Asset Management

List of assets

The company's assets are recorded in an eDocs document. All hardware and software licenses are registered here. Small acquisitions such as thin clients, mice, keyboards, and monitors are not detected. Servers and infrastructure-related hardware configurations and technical connections are also documented in dedicated operating documentation (for example, network drawings, system

documentation), in order to be able to recreate one or more of the company's services.

Ownership of assets

The company's director is responsible for all IT services, including infrastructure such as networks, firewalls and other communication connections. It is the operations manager who is responsible for ensuring that the system documentation is updated at all times.

Data classification

Classification of data

We do not classify data and we do not differentiate services based on data types.

Asset Management

Business Cloud

None of our data-bearing assets have enterprise data installed on the premises, which is only standard Microsoft software installed. Our network, data, etc. can only be accessed via Citrix, which is why the asset itself is worthless in that sense. When hiring, a mobile phone, a laptop (for use when we are physically with Customers, with which our employees can always access Citrix, without being dependent on the Customer's IT equipment), screens, keyboard, mouse, desk phone and a thin client are provided . Upon termination of employment, the same equipment is returned. The equipment is not sensitive to theft, as none of the items themselves can provide access to company data.

For licenses, we, as a hosting business, are licensed through our SPLA agreements. Statement of licenses is prepared monthly and reported directly to relevant license providers. The statements are saved per month, per year.

Physical documents with confidential and / or customer-specific documentation are scanned and stored in the customer folder, and the originals are subsequently shredded.

Business Cloud 365

None of our data-bearing assets have enterprise data installed on the premises, which is only standard Microsoft software installed. Our network, data, etc. can only be accessed via Citrix, which is why the asset itself is worthless in that sense. When hiring, a mobile phone, a laptop (for use when we are physically with Customers, with which our employees can always access Citrix, without being dependent on the Customer's IT equipment), screens, keyboard, mouse, desk phone and a thin client are provided . Upon termination of employment, the same equipment is returned. The equipment is not sensitive to theft, as none of the items themselves can provide access to company data.

For licenses, we, as a hosting business, are licensed through our SPLA agreements. Statement of

licenses is prepared monthly and reported directly to relevant license providers. The statements are saved per month, per year.

Physical documents with confidential and / or customer-specific documentation are scanned and stored in the customer folder, and the originals are subsequently shredded.

Media Management

Disposal of media

We have no data-bearing media other than server room media. If a disk breaks, it will be replaced by one of our employees and brought back to the office. From here, the hardware supplier picks up and destroys the media, which is part of our purchasing agreement with our security-approved supplier. Upon delivery of defective hardware for destruction, sign with signature from both parties.

For example, if an employee has his phone stolen, a full wipe is made of the phone, and the phone's ID is canceled on our Exchange environment. It will then not be possible to access our data via that telephone.

```
We do not use local media such as USB sticks for data storage.
```

Access control

Access Management Policy

All accesses are allocated according to functional needs and job roles. We carry out internal control of assigned access twice a year (April and October), just as updating access is regular checks in our HR processes for resp. new employment and termination or change of employment. In our allocation of access, we work on the basis of the principle of necessity, taking into account personal independence, so that we can always serve our customers.

All users are personally identifiable, and function allocation is used in the allocation of rights for all networks and associated AD policies. As additional access control when logging in outside the office, we use two-factor verification. This applies to everyone, including our customers.

Network access and network services

Only employees have rights to networks and network services. Customers always only have access to their own network, and no customers have administrator rights.

Access to networks and network services such as switches, routers and firewalls is handled by ourselves. No one other than our employees can access this, not even suppliers. Physically, the equipment is located in its own rack at Interxion, where only our technical staff has access. Interxion has an auditor's statement from an independent external IT auditor, which has been submitted without reservation. Our backup site, where our management server and backups are located, is also

installed in its own rack at Global Connect (Nianet).

We have segmented networks and ADs are never trusted. We have an operating network, which is the network we use for daily operations. We have a management network that can only be accessed from our operating network, and from here the common infrastructure components and the other networks are controlled. In addition, we have one network per customer. Each network has its own AD with dedicated policies.

Service users can never be used to log on to the network.

Access to wireless network

Zentura's wireless network is divided into a guest network and an internal network.

The guest network is for Zentura's guests only an internet connection access is restricted by a walk-in codes that expire after 24 hours. There is no access from the guest network to Zentura's internal network.

Zentura's internal wireless network may and may only be used by Zentura's employees.

User accesses

All user access is based on formal approval, whether it is internal users or customer users. User creation and shutdown procedures for internal users are described in dedicated HR process descriptions. Review of internal users is carried out at least twice a year.

The password for administrative common users (eg root passwords and admin) is documented and stored in a dedicated and reassuringly secured database, which only the company's management has access to. The same is also stored as a replica at an external public cloud provider, to which only Zentura's management has access, as well as in an external safe in a nationwide bank. Only the company's management has access to these common users, including the physically stored passwords. The keys to the physical safe are stored privately with the company's holders.

Customers' users are created according to customer-specific agreements, and customers never have access to anything other than their own domain. Passwords for customer installations are stored and shared in Remote Desktop Manger, where all users are personally identifiable, and where we can at any time verify who has logged in which customer, what they have done, when they have logged in and for how long they have been logged on. Once an employee has logged on to a server, the employee must make a brief note of the reason for the login before disconnecting from the server. User administration is at all times the customer's responsibility.

Rights allocation

Rights are granted solely on the basis of function and job role. All rights to Zentura's own infrastructure are tied up in Access groups in the Active directory, it is made in a ROLE / ACCESS model where ACCESS provides access to specific resources and ROLE is a set of access groups.

User Responsibility

Each employee is responsible for ensuring their own authentication information, and guidelines for the same are stated in the IT section of our Employee Handbook, which is handed out upon employment. Our passwords, including personal passwords, are generated through Remote Desktop Manager. Zentura follows Microsoft's standard for best practice of changing passwords every 3 months (90 days) and be of a certain complexity.

Control of access to systems and data

Controlling access to our systems is a top priority. Our product is secure IT services, and all our customers are recommended to set the same high security standard as ourselves.

Business Cloud

As all users are personally identifiable, we can at any time verify who has logged in to which customer, what they have done, when they have logged in and how long they have been logged in. This applies to all of our systems. In case of 5 failed AD login attempts, the account is blocked for 30 min. In case of 3 failed SMS PASSCODE login attempts, the SMS PASSCODE account will be blocked for 5 minutes. This is repeated 3 more times. If the user fails to enter SMS PASSCODE the 4th time, the user is locked out permanently. All logins, successful and unsuccessful, are logged.

Business Cloud 365

In regards to all business Cloud 365 customers with VM's(virual machines) in Azure or on-prem. All our users personally identifiable, when they are login on to customers VM's we can at any time verify who has logged in to which customer, what they have done, when they have logged in and how long they have been logged in. The way we can connect to customers VM's are using RDman(Remote Desktop Manager) and our users can only reatch that piece af software from our Citrix environment. In case of 5 failed AD login attempts, the account is blocked for 30 min. In case of 3 failed SMS PASSCODE login attempts, the SMS PASSCODE account will be blocked for 5 minutes. This is repeated 3 more times. If the user fails to enter SMS PASSCODE the 4th time, the user is locked out permanently. All logins, successful and unsuccessful, are logged.

We use software to store and share customer passwords. The user rights in this software are feature-specific, as are all other accesses.

Only the company's management has access to root passwords, both the electronically stored and the physically stored.

Source code for self-developed, internal, software (TeamWork) can only be accessed by the business owners. There are no customers who use the self-developed software.

Managing access to source code for applications

Source code for proprietary applications is stored on Github. All versions are saved. In-house developed programs are used exclusively for internal tasks, they are not sold to customers and can

not be accessed from the outside.

Cryptography

Data integrity and the protection of our own and customers' information are of the utmost importance for our business. Thus, all traffic to and from Zentura's network is protected by SSL certificates trusted by GlobalSign, and we do not use keys below 2048 bits. Self-signed certificates are not used for external traffic.

Physical and environmental fuses

Physical shell protection

We want to protect our equipment and data in the best possible way, none to ensure our customers the greatest possible security for uninterrupted service and security.

All our equipment located in our own rack at Interxion, where only our technical staff has access. Our backup equipment is located in its own rack at Global Connect. Both data center providers have auditor's statements, which we obtain annually.

Our physical office is located in Taastrup. Outside our office opening hours (8-16), all entrance doors are locked and burglar alarms are set to (19-07). Zentura shares an office building with WSP Denmark, but has its own entrance that is locked when Zentura employees are not present. During office hours, the door at the manned reception is open, all other doors require the use of an access control chip. It should be noted that no data can be accessed simply by having access to our physical office. The burglar alarm is automatically connected on weekdays after kl. 19. Connection of the burglar alarm can be postponed for one hour at a time using the employee's provided access control chip. All employees have a personally registered key to Zentura's locked area.

Protection against external and environmental threats

All our equipment is located in our own rack at Interxion, where only our technical staff has access. Our backup equipment is located in its own rack at Global Connect. For both suppliers, we refer to their auditors' statements.

Location and protection of equipment

All our equipment is located in our own rack at Interxion, where only our technical staff has access. Our backup equipment is located in its own rack at Global Connect. Both suppliers have auditor's statements, which are submitted without reservation.

Zentura has no services that may be affected if our physical office ceases to exist, all services are operated from those data centers or via cloud services.

The company's equipment is registered in an electronic form. All hardware is registered here.

Data-carrying equipment, which is no longer functional, is collected and destroyed by the hardware supplier, which is part of our purchasing agreement with our security-approved supplier. Upon delivery of defective hardware for destruction, sign with signature from both parties.

Data-bearing media

We have no data-bearing media, except server room media and mobile phones. From mobile phone there is only access to e-mail, address book and calendar. The mobile phone is also subject to a number of security policies, which among other things gives us access to delete the contents of the phone without having physical access to the phone.

Operational safety

Documented operating procedures

In order to ensure a consistently high quality in our services, as well as to protect us against personal dependencies, we have documented operating procedures and SOPs. In our organization, it is not possible to have 100% overlap on all tasks, systems and competencies, which is why it is crucial that all employees follow fixed procedures in their daily work.

Business Cloud

All customers have their own VLAN and there is no VLAN access in between. All customer-specific programs, etc., are handled in close collaboration with the customer and the customer's program provider. A customer's program provider never has access to anything other than the customer's domain. All customer passwords are stored in Remote Desktop Manager, where we can see which employees have accessed which customer, when logon has taken place, how long you have been on and what has been done by action.

Business Cloud 365

All customers have their own Microsoft 365 tenant so their are no possibility to gain access between any 2 customers. All customer-specific programs, etc., are handled in close collaboration with the customer and the customer's program provider. A customer's program provider never has access to anything other than the customer's domain. All customer passwords to access virtual machines in Azure or local server on-site at the customer's physical office are stored in Remote Desktop Manager, where we can see which employees have accessed which customer, when logon has taken place, how long you have been on and what has been done by action. In addition all major changes on a customer's virtual machines or Microsoft 365 environment are written in our internal changelog.

Network Security

Zentura Datacenter

Management of our customers takes place via a VLAN in our own environment. This can only be accessed via our office in Taastrup, and via home workstations with a fixed VPN. Only the company's operational technical owners have a fixed VPN from their home workplace. If you do not have a fixed VPN, or are sitting in the office in Taastrup, you can only access our environment via SMS PASSCODE through our Netscaler Gateway. From our own operating environment, there are a number of firewall rules that allow traffic from our VLAN to our customers' VLAN as well as VPN connections from our VLAN to relevant external partners. It should be noted that only management gates have been opened to ensure connectivity access, ie. Citrix, SSH, HTTP (S), RDP and Telnet, and we do not have, for example, file access to customer networks from our operating networks. All management of our core infrastructure equipment is in another network, which can only be accessed from our operating network, ie you must first on our operating network, and from there via firewall rules you are verified and get access to the necessary resources in the core the network required to obtain rights to, for example, change configurations on the core equipment.

We have a dedicated management server which can be accessed directly in the core network via RDP from the office in Taastrup, or from home workplaces with a fixed VPN. In case of errors on our management server, we have a backup management server, which can only be accessed from the office. The duplicate servers and the possibility of access from home offices have been established for the purpose of ensuring operational stability and uninterrupted services of our environment, as in the event of a breakdown of core equipment we can access the management server remotely via our trusted locations.

Business Cloud 365

Management of our customers with VM's in Azure takes place via a VLAN in our own environment. This can only be accessed via our office in Taastrup, and via home workstations with a fixed VPN. Only the company's operational technical owners have a fixed VPN from their home workplace. If you do not have a fixed VPN, or are sitting in the office in Taastrup, you can only access our environment via SMS PASSCODE through our Netscaler Gateway. All statements in the section called "Zentura Datacenter" is also applicable under this segment. might be subject to change when we move to a AVD(Azure Virtual Desktop) solution.

Change management

We prioritize traceability and reliability throughout our business. We therefore divide our changes by type, and for all changes classified 'STD Change', a change description, an implementation and a roll-back plan must be documented as a minimum. Changes that do not affect the SLA with the customers can be performed during office hours and classified as 'SOP'. Changes that are urgent 'Emergency Changes' can be implemented within office time, if it has been approved in advance by the customer, in an agreed service window.

STD (Standard Request for Change):

Significant changes in our general operating systems or core infrastructure that affect one or more

customers. Changes of this type require the approval of the company's CTO / COO. Examples of changes of this type are network changes, new infrastructure hardware, new host, upgrade of Exchange.

Low-risk changes that typically affect only a single customer. These changes can be performed by all support staff with the rights to perform the task. Examples of changes of this type are customer server restart (in dialogue with the customer), installation of Citrix receiver, change of user password, unlock a user. These changes can be implemented within office hours, provided it is approved in advance by the customer.

Patching of Zentura's Datacenter

Internally on Zentura's operating environment, we have a WSUS01 (Windows Update Services) server which is set up for auto approve updates (Security / Critical / Definition Updates).

All internal servers and customer server patches at the weekend, unless an alternative service window has been agreed with the customer. Patches are rolled out with Ivanti Automation Manager. Active directory and Witness Servers patches Friday 02:00 / Saturday 02:00, all other types of patches Sunday 02:00.

3rd party software is updated on all servers is updated as part of the regular patch process with Ninite Pro

Once a week, a WSUS report is drawn which shows the patch level on all servers. In the event of failed updates, the cause is analyzed and, if necessary, a Change Request is created and the update is rectified.

CORE EQUIPMENT: We do not patch our core equipment unless we have directly addressed issues and as directed by our manufacturer. We consider it a greater risk to have an update introduced which introduces an unknown error as we do not have a platform where we have a complete test environment.

We update our NetScaler every 2 months as NetScaler is a security product with direct internet access.

Citrix XenServer: Patches only as needed but we monitor releases if anything is critically relevant.

Core Infrastructure: Not updated continuously, and always manually.

All customer-initiated changes are registered in our ticket system.

Business Cloud 365

All our Azure/MS365 Customer with virtual servers in Azure checks of updates every night after 11mp CET using Azure's update feature which makes sure that the Servers are in a Compliant state with Windows updates.

Capacity management

Availability is one of our core values, and we take pride in always providing the expected quality of services to our customers. We have chosen a strategy for both our storage and servers, where we can continuously and without inconvenience to customers, expand our capacity.

Business Cloud & Business Cloud 365

We therefore monitor our capacity with Zabbix, and we monitor both disk, cpu and traffic. Basically, we operate with 90% utilization of each customer's platform. We have alarms on disk space and availability, as well as selected services on the servers.

Separation of tests and production facilities

Due to our customer specified and dedicated structure, it is not possible to create a valid test setup. As we only operate with dedicated solutions, we will basically not be able to make a real test image of e.g. a Windows security update therefore we do not test updates etc. before implementation.

Malware Protection

We consider Malware to be one of the biggest threats to our business, and our technical measures ensure the highest possible level of security so that malware cannot run in our environments. We minimize the risk both in terms of perimeter safety, but also damage delimitation, should an incident occur.

Zentura Datacenter

We use SecureDNS, which works by sending all queries on all platforms to Heimdal Security (CSIS), which validates that the relevant entry is not created in a database of threats. If this is the case, the response will be rewritten to a HoneyPot site where the user will be notified if they are trying to access a website that has been hacked or otherwise malicious.

If known ransomware enters our system, calls to the Command & Control server will be blocked and ransomware will be rendered harmless. We also subscribe to Platinum Alert Service from CSIS, where CSIS sends newsletters about what threats are in the market, 0 day attacks and possibly. which patch can secure the systems. All alerts are sent to the service desk where these are evaluated according to importance / specific threat level.

We also use Applocker, so that only known software can be executed on customers' Citrix Servers.

No users are Administrators in the context in which they work, ie. no users can install software or manipulate software in such a way that it can infect systems at the "administrator" level. If a user gets malware in their profile, we can simply remove the user profile and create a new user profile.

Email scanning is handled by Vipre, both for ourselves and for our customers. It is mandatory and

cannot be deselected. Vipre uses several filters and they have a PVR (Pre Virus Recognition) system where large batches of one's characteristic mails are quarantined until they are examined manually, after which they are then released.

Business Cloud 365

On all Azure Virtual Desktop(AVD) before know as Windows Virtual Desktop(WVD) we use Applocker, so that only known software can be executed on the customers AVD.

No users are Administrators in the context in which they work, ie. no users can install software or manipulate software in such a way that it can infect systems at the "administrator" level. If a user gets malware in their profile, we can simply remove the user profile and create a new user profile.

Email scanning is handled by Vipre or Mircosoft mailscanning this depends on which email encryption solution that customers is using, both for ourselves and for our customers. It is mandatory and cannot be deselected. Vipre and mircosoft uses several filters and they have a PVR (Pre Virus Recognition) system where large batches of one's characteristic mails are quarantined until they are examined manually, after which they are then released.

Backup

Business Cloud

On Zentura's hosting platform, Nutanix snapshot backups are made every night. This means that a full copy of all data is made: server system files, user data, file services, databases and all other data. A snapshot is a complete copy of the server the moment the snapshot is taken - with no data loss at all. After each snapshot, a copy of the snapshot is copied to the opposite data center. These snapshots are stored for 4 days on the primary site so that the restore can be performed without prior copying from the secondary data center. All snapshots are stored for 30 days on the secondary data center. This policy is used on both Zentura's and customers' servers and data.

On customers with their own infrastructure, the customer's own backup system is used for backup and the customer's own policy is followed.

Business Cloud 365

For customer's with data stored in Sharepoint, Onedrive, Teams and Exchange Online Datto is used as the backup solution in this case in extention with the Paper bin in the different interfaces.

Customer's with virtual server in Azure we use Microsoft_Azure DataProtection Backup center to backup the VM's daily and for File backups on the VM we use Shadowcopy that takes snapshots at 7am and 12pm.

Logging and monitoring

Event logging

We want us to be able to document and control selected network activities at all times, partly to ensure transparency towards our customers, partly to check that there is no unwanted activity from outsiders, and to be able to verify that no employees are doing anything there. are not in line with their duties.

Business Cloud

We use Remote Desktop Manager which is a client / server system that uses AD credentials for the individual consultant. Remote Desktop Manager logs all access to customer / internal systems at Zentura with time / identity for the user who wants to interact with an object in Remote Desktop Manager - ie. for Password View, Connection, Disconnection etc. this will result in a log entry.

When logging on to a customer system, the consultant must fill in a comment about what the access is to be used for. This is required by logon in connection with remote access. Logs / data about connections are stored in a central database where only the company's management has access.

Our domain Controllers run NTP time synchronization with an external time server which guarantees validity in log files.

Business Cloud 365

Logging and monitoring access to a customers virtual server in Azure are managed in the sameway that is states above under "Business Cloud".

Software management on operating systems

Our policy and process for installing programs on operating systems, including patch management, is identical to our Change Management procedure.

Management of technical vulnerabilities

Our customer systems are set up in such a way that users cannot install programs themselves.

Communication security

Network measures

Considering our business, it is of the utmost importance that our communication channels and

networks are not compromised. We have therefore established manual as technical measures to ensure and check the integrity of our services.

Business Cloud

All our networks are protected by firewalls, and our networks are divided resp. per customer and internally per function. Our data center has two separate lines, and our SMS PASSCODE service, which all our customers use, is redundant and connected to two different telecommunications providers.

All data center components as well as the internet connection are monitored. All critical errors on critical data center components are distributed via regular e-mail, push notification and text messages to and handled by our service support staff.

Business Cloud 365

All our BS365 customers has thier own MS365 tenant so it's impossible for 2 customers gaining access to the other. Regards to redundant lines and other sercurty measures of phiscal hardware is handle and maintained by them.

If a customers has a AVD server they can reach it frome any were in the world although MFA is required to connect to it.

Data transfers

Data integrity and confidentiality are part of the security we provide to our customers- We therefore never transfer data unencrypted. When transferring customer data, a VPN tunnel is established site-to-site. Employees, as consultants, have an unconditional duty of confidentiality in everything the person in question may become aware of in pursuance of their position / task, which is regulated in all employment and consulting contracts.

Supplier relationship

Security in supplier agreements

All our supplier and partner agreements must include regulation of confidentiality. All agreements must also contain security matters, such as matters of monitoring, confidentiality, intellectual property rights and delivery security.

Management of third party services

We have identified our significant suppliers, and the risks associated with these are dealt with separately in our risk analysis.

In general, we have critical supplier dependencies for two suppliers, resp. interxion and Global

Connect (Nianet). Auditor's statements are obtained annually from both suppliers.

In addition, we have a dependence on our mail scanning supplier Vipre, although this is less critical, as the functionality can be handled by several other companies. An auditor's statement has been obtained from Vipre in line with all other service providers we use.

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.

Vendor IT Security Policy

Where we use subcontractors and / or external consultants, we supervise the agreed deliveries, and these must be provided and delivered in accordance with our IT security policy.

Customer responsibility

The customers' responsibility is defined in our general terms and conditions, which state that data responsibility at all times is the customer's own. Thus, the customer is responsible for our instruction, including for, among other things:

- To classify own data and special needs in that regard
- Give notice of creation and dismantling of users (own user administration)
- All types of service orders at Zentura
- Notification to the Danish Data Protection Agency
- Own contingency planning
- Obtain Data Processor Agreements

Security incident management

Responsibilities and procedures

All employees have a responsibility to help protect Zentura's information from unauthorized access, alteration and destruction, as well as theft.

All employees are therefore continuously trained in information security to the relevant extent. As users of Zentura's information, all employees must comply with the information security policy and the guidelines derived therefrom. Employees may only use the company's information in accordance with the work they perform in the company and must protect the information in a way that is in accordance with the sensitivity, special and / or critical nature of the information.

All employees can report an incident. There is a reporting obligation.

All events must be recorded. Registrations must not be deleted.

Reporting of information security incidents

An information security incident, a threat to information security, or suspicion of the same, must be reported immediately to the company director at all times. Everyone must report an incident / suspicion of an incident, and depending on the nature of the incident, it is the company's director who determines an action plan for how the incident is to be handled and communicated, internally or possibly externally. It is also the nature of the incident that determines what evidence is to be collected.

Employees who violate the information security policy or guidelines derived therefrom will be subject to disciplinary action in accordance with Zentura's applicable rules and personnel policies.

Assessment of information security breach

All threats and incidents in relation to information security are evaluated and assessed by the company's director and the company's management. It is the director of the company who is the one most responsible for assessing security incidents.

All incidents are registered with the nature of the threat, just as the incident and assessment history is documented. If the incident is related to a ticket, the ticket number is also registered. All events are continuously updated with a status indication until the event is completed.

Response and learning of information security breaches

All security breaches are documented and a Root Cause Analysis of the incidents is made, which is reviewed with all relevant employees, for example at the monthly meetings.

Depending on the nature of the incident, an Emergency Change (EC) is prepared and implemented, so that we avoid the incident occurring again.

Safety-related topics, general topics as well as current topics, are also reviewed at internal monthly meetings, where we for the sake of knowledge sharing and training have regular contributions in addition to reviewing the daily here-and-now activities. The director of the company is responsible for holding presentations at these meetings.

If the incident gives rise to a re-evaluation of one or more risks, the company's risk analysis is updated accordingly.

Collection of evidence

Depending on the nature of the incident, logo information, etc. immediately secured. All information relevant to the incident is stored for a minimum as long as the investigation of the incident is ongoing.

Information security aspects of emergency management

Contingency plan

Disasters are sought to be avoided through well-planned physical security and monitoring of all technical installations and IT equipment. The scope of these measures is decided on the basis of a balance of risks against hedging costs and our customer SLAs. Risk analysis and contingency plans include damage mitigation measures, establishment of temporary emergency solutions and re-establishment of permanent solution.

Our message plan takes into account business continuity and business impact, including recovery time objective.

Testing of preparedness

Our contingency plan is tested in selected scenarios at least once a year

Disaster Recovery Planer

Annually, one or more selected scenarios are tested based on a disaster approach. Depending on the scenario, the desktop is performed as an actual test. Each D / R test contains completed a test evaluation.

Redundancy

We strive for 24/7/365 accessibility, which is why all of our World Cup's are High Availability. Our daily backup is stored in a secondary location at Global Connect, from where we can restore all of our hosting services.

Our SMS PASSCODE service sends text messages via two different WebSMS Service providers (InMobile and Compoya) in a redundant setup for all customers. If both service providers are down, you automatically switch to a physical modem located in the office in Taastrup.

Compliance

Those of our customers who process sensitive personal data are themselves responsible for correct and relevant notification to the Danish Data Protection Agency and / or other relevant authority and compliance with relevant legislation. This is specified in our General Terms and Conditions.

Review of information security

The company's CEO is responsible for ensuring that the company's activities are carried out in

accordance with internal policies and procedures. IT security is of the highest priority for us, which is why we are audited annually by an external, independent, IT auditor.

We also carry out the races self-inspection.