

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



4MDG – Governança de Dados Mestres
ZH SOLUÇÕES ESPECIALISTAS LTDA
CNPJ: 11.955.326/0001-99

(11) 4113-2510
www.4mdg.com.br
atendimento@4mdg.com.br

R. Antônio Ayrosa, 191
Vila dos Remédios
São Paulo – SP
CEP: 05103-000

 GOVERNANÇA DE DADOS MESTRES	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 1/14
	Política de Segurança da Informação			

Sumário

1. OBJETIVO 3

2. ÂMBITO DE APLICAÇÃO 3

3. DEFINIÇÕES..... 3

4. DIRETRIZES 5

4.1 DECLARAÇÃO 5

4.2 USO ACEITÁVEL DOS ATIVOS..... 5

4.3 MESA LIMPA TELA LIMPA 5

4.4 USO DA INTERNET 6

4.5 USO DO E-MAIL..... 7

4.6 USO DE MÍDIA REMOVÍVEL 7

4.7 RESTRIÇÕES SOBRE O USO E INSTALAÇÕES DE SOFTWARE 7

4.8 SENHAS 8

4.9 ARMAZENAMENTO DE ARQUIVOS 8

4.10 USO DE AUTENTICAÇÃO COM CONTAS MICROSOFT CORPORATIVAS 9

4.11 USO DO WHATSAPP..... 9

4.12 CONTRA MALWARES 9

4.13 TREINAMENTO E CONSCIENTIZAÇÃO 9

4.14 SEGURANÇA FÍSICA..... 10

4.15 RELATO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 12

5. SANÇÕES 12

6. REFERÊNCIAS 13

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 2/14
	Política de Segurança da Informação			

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 3/14
	Política de Segurança da Informação			

1. OBJETIVO

Este documento é um conjunto de normas que tem como finalidade orientar o gerenciamento das informações, protegendo e garantindo os pilares de confidencialidade, integridade e disponibilidade em observância a norma NBR ISO/IEC 27001:2022

2. ÂMBITO DE APLICAÇÃO

Esta política de segurança da informação se aplica a:

- Quaisquer softwares fornecidos ou sob o controle da 4MDG;
- Quaisquer comunicações enviadas ou recebidas;
- Quaisquer dados pertencentes, controlados ou processados, incluindo dados mantidos em sistemas externos;
- Locais a partir dos quais os dados são acessados, incluindo uso interno e externo;
- Ativos de informação mantidos, processados ou armazenados nas instalações ou locais externos;
- Informações em trânsito pelas redes de voz ou dados.

Todos os colaboradores da 4MDG (empregados, prestadores de serviço, representantes ou subcontratados de terceiros e estagiários) devem conhecer esta política.

A adesão a esta política é obrigatória e o não cumprimento pode levar a sanções disciplinares.

3. DEFINIÇÕES

Ativo de informação: qualquer dado, sistema, software, hardware, documento ou recurso físico que tenha valor para a organização e necessite de proteção adequada.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 4/14
	Política de Segurança da Informação			

Controle de acesso: medidas para garantir que o acesso a ativos seja autorizado e restrito com base nos requisitos de negócios e segurança.

Autenticação: processo de fornecer garantia de que uma característica alegada de uma entidade, como a identidade de um usuário ou dispositivo, é correta. A autenticação é fundamental para garantir que apenas indivíduos ou sistemas autorizados possam acessar determinados recursos ou informações.

Confidencialidade: propriedade de que a informação não seja disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados.

Integridade: propriedade de precisão e completude das informações.

Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Privacidade: controle sobre a coleta, armazenamento, uso e compartilhamento de dados pessoais, em conformidade com as legislações aplicáveis.

Parte interessada: pessoa ou organização que pode afetar, ser afetada por, ou perceber-se afetada por uma decisão ou atividade. Ex.: clientes, colaboradores, fornecedores, acionistas, órgãos reguladores, e parceiros de negócios.

Violação de privacidade: situação em que dados pessoais são processados de forma inadequada, resultando em violação de um ou mais requisitos de proteção à privacidade, comprometendo a confidencialidade, integridade ou disponibilidade desses dados.

Sistema de Gestão de Segurança da Informação (SGSI): consiste em políticas, procedimentos, diretrizes, recursos e atividades associados, geridos coletivamente por uma organização com o objetivo de proteger seus ativos de informação.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 5/14
	Política de Segurança da Informação			

Sistema de Gestão de Privacidade da Informação (SGPI): conjunto de políticas, processos e controles implementados para gerenciar e proteger dados pessoais, assegurando que a organização esteja em conformidade com as legislações de privacidade e garantindo que os direitos dos titulares dos dados sejam respeitados em todas as operações da organização.

4. DIRETRIZES

4.1 DECLARAÇÃO

“A 4MDG está comprometida em implementar e monitorar seus controles de segurança da informação para garantir a confidencialidade, integridade, disponibilidade e autenticidade de todo ativo de informação atendendo as regulamentações e requisitos contratuais de seus clientes, colaboradores, parceiros e partes externas interessadas sempre buscando a melhoria contínua de seus processos e serviços.”

4.2 USO ACEITÁVEL DOS ATIVOS

Todos os colaboradores têm a responsabilidade de proteger as informações e os ativos de informação sob sua responsabilidade que devem ser usados de maneira aceitável e de acordo com esta e outras políticas e processos relacionados ao SGSI.

4.3 MESA LIMPA TELA LIMPA

- Os dispositivos de computação desacompanhados ou não sendo utilizados são protegidos com uma tela ou mecanismo de bloqueio controlado por senha ou mecanismo de autenticação semelhante (isso inclui laptops, tablets, smartphones e estações de trabalho).
- As estações de trabalho são bloqueadas por tempo de inatividade. Ao ausentar-se, a estação de trabalho deve ser bloqueada usando Ctrl-Alt-Del, opção “Bloquear”, ou a tecla

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 6/14
	Política de Segurança da Informação			

Windows e 'L'. Isso impedirá que pessoas acessem qualquer informação a qual não esteja autorizada, enquanto o dispositivo estiver desacompanhado.

- Ao acessar informações confidenciais ou que contenham dados pessoais em uma tela, os usuários devem garantir que pessoas não autorizadas não consigam visualizar tais informações. As telas dos computadores nas quais informações confidenciais ou pessoais são processadas ou visualizadas devem ser posicionadas de tal forma que não possam ser visualizadas por pessoas não autorizadas.
- Informações confidenciais ou de acesso restrito, como em papel ou em meio de armazenamento eletrônico, devem ser protegidas quando não utilizadas, especialmente quando o escritório é desocupado no final do expediente. Deve-se também tomar cuidado ao imprimir documentos confidenciais ou de acesso restrito para evitar a divulgação não autorizada.
- Nada de papéis soltos ou anotações expostas:
 - Anotações com senhas, post-its com dados, ou rascunhos de trabalho devem ser descartados adequadamente (ex.: triturados) ou arquivados.
- Armazenamento seguro de mídias removíveis:
 - Pendrives, HDs externos e mídias similares devem ser guardados com segurança após o uso.
- Nada de itens pessoais sobre a mesa:
 - Evitar objetos pessoais como brinquedos, enfeites, comidas, bolsas ou objetos não relacionados ao trabalho.

4.4 USO DA INTERNET

- O uso da Internet deve ser realizado de modo consciente segundo a necessidade para execução das atividades laborais e, eventualmente, pessoais. O uso abusivo, que possa comprometer o bom desempenho laboral, ou conscientemente colocar em risco ativos da informação da empresa, pode resultar em advertências verbais ou formais, de acordo com a gravidade.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 7/14
	Política de Segurança da Informação			

- O acesso à Internet em ativos da empresa é monitorado e controlado, salvo se houver necessidade explícita de acesso irrestrito para a execução da atividade laboral relacionada à função. O acesso irrestrito é autorizado por gestor ou diretor.

4.5 USO DO E-MAIL

- O uso do e-mail corporativo para fins pessoais é impróprio e não é permitido em nenhum momento. O sistema de e-mail fornecido pela 4MDG deve ser utilizado para enviar e receber informações da 4MDG e não deve ser usado de forma insultuosa ou ofensiva.
- Se você receber um e-mail impróprio ou abusivo, deve relatá-lo imediatamente ao seu superior, que tomará as medidas cabíveis. Se o remetente for conhecido por você, informe-o de que ele deve interromper o envio do material. E-mails que parecem suspeitos, podem ser tentativas de "phishing" ou malware, devem ser relatados imediatamente como um incidente de segurança da informação.

4.6 USO DE MÍDIA REMOVÍVEL

Entende-se por mídia removível qualquer tipo de memória que pode ser removida conferindo portabilidade para os dados que foram armazenados nela. Alguns exemplos de mídias removíveis são: pendrive, cartões de memória, HDs externos, entre outros.

- A utilização de mídias removíveis não é permitida pela 4MDG. Em situações excepcionais, deve-se solicitar autorização ao gestor imediato, e cada caso será avaliado individualmente.

4.7 RESTRIÇÕES SOBRE O USO E INSTALAÇÕES DE SOFTWARE

- Os softwares são gerenciados e controlados de acordo com as políticas da empresa em relação ao gerenciamento de ativos e contratos de licença. Todos os softwares usados em dispositivos gerenciados pela empresa devem ser instalados de acordo com as diretrizes internas de licenciamento de software atuais.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 8/14
	Política de Segurança da Informação			

- Violar os direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredo comercial, patente ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, mas não se limitando a, instalação ou distribuição de produtos "pirateados" ou outros produtos de software que não sejam apropriadamente licenciados, pode deixar o colaborador sujeito a ação disciplinar.

4.8 SENHAS

- Senhas e outras formas de autenticação secreta, tais como chaves criptográficas e padrões de desenho, utilizadas para acessos a dispositivos, redes e sistemas, são de uso exclusivo do usuário, portanto não devem ser compartilhadas. Da mesma forma, o usuário não deve utilizar a senha de outra pessoa.
- Ao suspeitar de que uma senha ou outra forma de autenticação secreta possa ter sido comprometida, o colaborador deve alterá-la imediatamente em todos os dispositivos, redes e sistemas em que ela esteja sendo utilizada e comunicar imediatamente à área de TI.
- A Política de Senhas determina regras sobre o cumprimento de senhas e o uso de frases secretas.

4.9 ARMAZENAMENTO DE ARQUIVOS

- Para garantir a segurança e a integridade dos dados, todos os colaboradores devem armazenar seus arquivos exclusivamente no Drive da organização.
- É proibido armazenar arquivos de trabalho em dispositivos pessoais, unidades de armazenamento externas ou outros serviços de armazenamento em nuvem.
- Não utilize as permissões de compartilhamento do Google/Microsoft Drive para conceder acesso a colegas ou equipes. Se necessário realizar algum compartilhamento solicite a área de TI.
- Não desative nenhuma configuração de segurança ou backup sem autorização explícita da área de TI.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 9/14
	Política de Segurança da Informação			

4.10 USO DE AUTENTICAÇÃO COM CONTAS MICROSOFT CORPORATIVAS

- Não utilize sua conta Microsoft corporativa para se autenticar em qualquer plataforma, aplicativo ou serviço que não tenha sido explicitamente autorizado pela organização.
- Caso necessite utilizar uma nova plataforma ou serviço, consulte a área de TI para avaliação e homologação antes de usar sua conta Microsoft corporativa para autenticação.

4.11 USO DO WHATSAPP

- O uso do WhatsApp deve ser limitado a comunicações rápidas e não sensíveis que não envolvam dados confidenciais.
- Evite discutir informações confidenciais da empresa pelo WhatsApp. Sempre que possível, utilize os canais de comunicação internos e seguros da organização para discussões sensíveis.
- Para utilizar o WhatsApp no ambiente corporativo, é obrigatório configurar o backup para ser realizado diariamente e habilitar a autenticação de dois fatores.

4.12 CONTRA MALWARES

Todas as estações de trabalho da empresa possuem software antivírus instalado e configurado para atualizar automaticamente suas assinaturas. Além disso, as estações de trabalho são verificadas periodicamente para detectar e remover malware, programas maliciosos ou indesejados. A desinstalação do software antivírus é estritamente proibida.

4.13 TREINAMENTO E CONSCIENTIZAÇÃO

A 4MDG reconhece que a proteção das informações e o cumprimento das políticas de segurança dependem, em grande parte, do conhecimento e comportamento seguro de seus colaboradores.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 10/14
	Política de Segurança da Informação			

Para isso, a empresa mantém um programa contínuo de treinamento e conscientização em segurança da informação e privacidade, com as seguintes atividades:

- Treinamento Inicial: todos os novos colaboradores, prestadores de serviço, estagiários e terceiros devem participar de um treinamento de segurança da informação durante o processo de integração (onboarding).
- Treinamentos Periódicos: todos os colaboradores ativos devem participar de reciclagens de segurança da informação ao menos uma vez por ano, ou sempre que houver atualização relevante nas políticas ou nos riscos identificados.
- Conteúdo dos Treinamentos: os treinamentos abordam temas como: boas práticas de proteção de informações, uso seguro de sistemas, políticas de senhas, proteção contra malware, privacidade de dados (LGPD), prevenção de incidentes de segurança e resposta a incidentes.
- Campanhas de Conscientização: periodicamente, a 4MDG promove campanhas internas de conscientização, reforçando boas práticas e alertando para novas ameaças ou tendências de segurança.
- Obrigações dos Colaboradores: é responsabilidade de cada colaborador participar dos treinamentos obrigatórios, aplicar os conhecimentos adquiridos no seu dia a dia, e buscar suporte sempre que identificar dúvidas ou situações de risco.

O não cumprimento das obrigações de treinamento e conscientização pode ser considerado uma violação desta Política e estará sujeito às sanções cabíveis.

4.14 SEGURANÇA FÍSICA

A 4MDG adota medidas de segurança física para proteger os ativos de informação contra acessos não autorizados, danos, perdas ou interferências.

CONTROLE DE ACESSO

- O crachá é de uso pessoal e intransferível. O uso é obrigatório para acesso ao prédio e blocos internos.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 11/14
	Política de Segurança da Informação			

- Visitantes devem ser previamente autorizados e identificados na recepção.
- Mantenha portas e acessos restritos fechados e trancados quando não houver supervisão.
- Não permita o acesso de terceiros não autorizados às salas da 4MDG.
- Visitantes devem estar sempre acompanhados de um colaborador.

POSTO DE TRABALHO

- Adotar a prática de mesa limpa e tela limpa conforme item 4.3 desta Política.
- Equipamentos eletrônicos devem ser retirados da estação de trabalho ao término das atividades:
 - Levar o notebook para casa, ou
 - Guardá-lo no armário pessoal trancado.
- A chave do armário não deve ser compartilhada ou copiada. Em caso de perda comunique imediatamente a direção.
- Não compartilhar mesas de trabalho sem autorização prévia.

USO DE EQUIPAMENTOS

- É proibido conectar dispositivos pessoais não autorizados (como pendrives e HDs externos) a equipamentos corporativos.
- Mantenha equipamentos organizados e longe de bordas para evitar quedas e danos.

SEGURANÇA DE DOCUMENTOS FÍSICOS

- Qualquer documento físico com dados pessoais, sensíveis ou estratégicos deve ser mantido em local trancado.
- Nunca descarte papéis com dados corporativos sem triturá-lo ou picotá-lo.
- Se observar documentos sensíveis deixados expostos, comunique imediatamente ao responsável.

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 12/14
	Política de Segurança da Informação			

4.15 RELATO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Se você identificar um incidente de segurança da informação, deve notificar imediatamente através do e-mail suporte@4mdg.com.br ou abrir chamado no sistema Freshdesk. Em casos críticos e de urgência, entre em contato pelo telefone (11) 96467-2188 com as seguintes informações:

- Descrição detalhada do incidente.
- Data e hora do ocorrido.
- Sistemas ou dados afetados.
- Qualquer evidência disponível (prints, logs, mensagens de erro).

Mantenha a confidencialidade do incidente, discutindo-o apenas com as pessoas autorizadas envolvidas na resolução.

5. SANÇÕES

A falha de contratados, colaboradores temporários, públicos, parceiros ou organizações terceirizadas em cumprir a política de segurança da informação da 4MDG pode resultar na rescisão dos contratos e relações, suspensão de serviços e ou instauração de processo judicial. Aos colaboradores que desrespeitarem as normas estabelecidas neste documento, serão aplicadas as seguintes sanções, imediatamente à ocorrência do ato faltoso:

- 2 advertências verbais;
- 2 advertências por escrito;
- 1 suspensão de 1 dia;
- 1 suspensão de 3 dias;
- 1 suspensão de 5 dias;
- Dispensa por justa causa.

Objetiva-se que o referido rol de penalidades seja aplicado de forma gradativa, porém, e conforme permite a legislação vigente, quando a gravidade do ato assim demandar, a

	POLÍTICA		Nº.: PL 1021-01	Rev.: 02
	Classificação da Informação: uso público		Data: 11/03/2026	FL.: 13/14
	Política de Segurança da Informação			

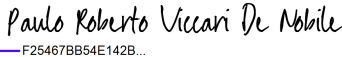
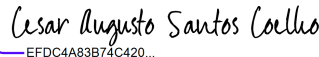
penalidade será mensurada e aplicada proporcionalmente ao ato faltoso cometido, ainda que a medida anterior não tenha sido levada a efeito.

A ordem acima poderá ser alterada de acordo com a gravidade da falta.

6. REFERÊNCIAS

ABNT. (2022). *NBR ISO/IEC 27001:2022*. Rio de Janeiro: ABNT.

IDENTIFICAÇÃO DAS ALTERAÇÕES		
Revisão	Data da revisão	Alterações efetuadas
00	21/10/2025	- Elaborado por Paulo Roberto Viccari de Nobile.
01	10/11/2025	- Ajustes do item 4.11 Uso do WhatsApp; da fonte dos tópicos do item 4.14 Segurança Física, remoção da palavra identificação da frase “O crachá é de uso pessoal e intransferível” e ajustes do segundo parágrafo do item 4.8 Senhas.
02	11/03/2026	- Ajustes na classificação da informação e formatação do documento.

Elaboração		Aprovação	
Paulo Roberto Viccari de Nobile		Cesar Coelho	
Assinado por:  F25467BB54E142B...		Assinado por:  EFDC4A83B74C420...	
Data:	11/03/2026	Data:	11/03/2026

Área envolvida	Responsável	Data	Assinatura
NA	NA	NA	NA
NA	NA	NA	NA

Certificado de Conclusão

Identificação de envelope: 9F39BC81-E378-4E8D-AA92-9B837AFD16F7

Status: Concluído

Assunto: Complete com o Docusign: POL 1021-01 Rev. 02 Política de Segurança da Informação

Envelope fonte:

Documentar páginas: 14

Assinaturas: 2

Remetente do envelope:

Certificar páginas: 5

Rubrica: 0

Debora Silva

Assinatura guiada: Ativado

R ANTONIO AYROSA 191

Selo com Envelopeld (ID do envelope): Ativado

Sao Paulo, SP 05.103-000

Fuso horário: (UTC-08:00) Hora do Pacífico (EUA e Canadá)

debora.silva@4mdg.com.br

Endereço IP: 2804:7f0:d823:2

Rastreamento de registros

Status: Original

Portador: Debora Silva

Local: DocuSign

12/03/2026 10:33:40

debora.silva@4mdg.com.br

Eventos do signatário

Cesar Augusto Santos Coelho

cesar@4mdg.com.br

Nível de segurança: E-mail, Autenticação da conta (Nenhuma)

Assinatura

Assinado por:

Cesar Augusto Santos Coelho

EFDC4A83B74C420...

Adoção de assinatura: Estilo pré-selecionado

Usando endereço IP:

2804:14c:165:30c5:317e:5a0e:8965:7083

Registro de hora e data

Enviado: 12/03/2026 10:35:30

Reenviado: 12/03/2026 15:29:30

Reenviado: 13/03/2026 07:13:51

Reenviado: 13/03/2026 07:13:55

Reenviado: 13/03/2026 09:06:49

Reenviado: 13/03/2026 10:42:41

Reenviado: 13/03/2026 10:52:37

Visualizado: 13/03/2026 10:57:15

Assinado: 13/03/2026 10:57:21

Termos de Assinatura e Registro Eletrônico:

Aceito: 13/03/2026 10:57:15

ID: b561c0df-da14-426d-8968-104b3abdf7

Paulo Roberto Viccari De Nobile

paulo.nobile@4mdg.com.br

Nível de segurança: E-mail, Autenticação da conta (Nenhuma)

Assinado por:

Paulo Roberto Viccari De Nobile

F25467BB54E142B...

Adoção de assinatura: Estilo pré-selecionado

Usando endereço IP:

2804:1b3:a640:bada:f4c2:d286:19d6:bd47

Enviado: 12/03/2026 10:35:31

Reenviado: 12/03/2026 15:29:31

Reenviado: 13/03/2026 07:13:52

Reenviado: 13/03/2026 07:13:56

Reenviado: 13/03/2026 09:06:50

Reenviado: 13/03/2026 10:42:42

Reenviado: 13/03/2026 10:52:38

Visualizado: 13/03/2026 10:53:51

Assinado: 13/03/2026 10:53:58

Termos de Assinatura e Registro Eletrônico:

Aceito: 13/03/2026 10:53:51

ID: 4cd62b1a-f87a-40a2-981a-08b1959daf1f

Eventos do signatário presencial

Assinatura

Registro de hora e data

Eventos de entrega do editor

Status

Registro de hora e data

Evento de entrega do agente

Status

Registro de hora e data

Eventos de entrega intermediários

Status

Registro de hora e data

Eventos de entrega certificados

Status

Registro de hora e data

Eventos de cópia

Status

Registro de hora e data

Eventos com testemunhas

Assinatura

Registro de hora e data

Eventos do tabelião	Assinatura	Registro de hora e data
Eventos de resumo do envelope	Status	Carimbo de data/hora
Envelope enviado	Com hash/criptografado	12/03/2026 10:35:31
Entrega certificada	Segurança verificada	13/03/2026 10:53:51
Assinatura concluída	Segurança verificada	13/03/2026 10:53:58
Concluído	Segurança verificada	13/03/2026 10:57:21
Eventos de pagamento	Status	Carimbo de data/hora
Termos de Assinatura e Registro Eletrônico		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, ZH SOLUCOES ESPECIALISTAS LTDA (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact ZH SOLUCOES ESPECIALISTAS LTDA:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: servicos@zhespecialistas.com

To advise ZH SOLUCOES ESPECIALISTAS LTDA of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at servicos@zhespecialistas.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from ZH SOLUCOES ESPECIALISTAS LTDA

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to servicos@zhespecialistas.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with ZH SOLUCOES ESPECIALISTAS LTDA

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to servicos@zhespecialistas.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify ZH SOLUCOES ESPECIALISTAS LTDA as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by ZH SOLUCOES ESPECIALISTAS LTDA during the course of your relationship with ZH SOLUCOES ESPECIALISTAS LTDA.