PRIVACY AND DATA SECURITY ADDENDUM

This Privacy and Data Security Addendum (this "Addendum") applies to suppliers of goods, services, and/or Software (each a "Supplier") to CHS Inc., a Minnesota cooperative corporation, ("CHS") and/or its Affiliates, where the provisions of this Addendum are imposed or required by contract with Supplier or by Supplier's accession to this Addendum.

This Addendum applies if, and to the extent, that Supplier receives or acquires any Covered Data and this Addendum states obligations of Supplier with respect to such Covered Data. Supplier will conform to the requirements of this Addendum at no additional cost to CHS.

1. **Defined Terms**. Without limiting anything else in this Addendum, the following terms will have the following meanings. Where this Addendum defines a term, the definition applies with respect to this Addendum and, except as otherwise stated in this Addendum, this Addendum does not modify any defined term, as such, in any agreement that refers to this Addendum.

(a) An "Affiliate" means any entity which is controlled by, controls or is in common control with Processor.

(b) "Authorized Supplier Person" means a natural person who is, directly or indirectly, an agent of Supplier that has a bona fide need to know and/or possess Covered Data, or have access to CHS Information Systems, for the purpose of performing obligations to one or more CHS Parties.

(c) "Cardholder Data" has the meaning given to that term by the PCI DSS.

(d) "CHS Information Systems" means computer, communication, and network equipment, systems, and services (voice, data, or otherwise) owned, controlled, or used by CHS or any CHS Affiliate, including, but not limited to, the corporate wide area network, the electronic switched network, Inter/intranet gateways, electronic mail, telephony, computer systems, system hardware, drives, electronic media, storage areas, software programs, files, and databases.

(e) "CHS Party" in any particular case is CHS or a CHS Affiliate (i) that contracts with Supplier, (ii) from which Supplier receives Covered Data, or (iii) on whose behalf or for whose benefit Supplier collects or receives Covered Data.

ADENDO DE PRIVACIDADE E SEGURANÇA DE DADOS

O presente Adendo de Privacidade e Segurança de Dados (o presente "Adendo") se aplica a fornecedores de mercadorias, serviços e/ou Software (individualmente, um "Fornecedor") à CHS Inc., uma sociedade cooperativa de Minnesota ("CHS") e/ou suas Afiliadas, quando as disposições do presente Adendo forem impostas ou exigidas por contrato com o Fornecedor ou por acessão do Fornecedor ao presente Adendo.

O presente Adendo se aplica se e na medida em que o Fornecedor receber ou adquirir quaisquer Dados Cobertos e o presente Adendo declarar obrigações do Fornecedor em relação aos Dados Cobertos. O Fornecedor estará em conformidade com as exigências do presente Adendo sem custos adicionais à CHS.

1. **Termos Definidos**. Sem limitar mais nada no presente Adendo, os termos a seguir terão os seguintes significados. Quando o presente Adendo definir um termo, a definição se aplica em relação ao presente Adendo e, salvo declaração contrária no presente Adendo, o presente Adendo não modifica qualquer termo definido, como tal, em qualquer acordo que se refere ao presente Adendo.

(a) Uma "Afiliada" significa uma pessoa jurídica que é controlada, controla ou está sob controle comum do Processador.

(b) "Pessoa Autorizada do Fornecedor" significa uma pessoa física que, direta ou indiretamente, seja um agente do Fornecedor que tem uma necessidade, de boa-fé, de conhecimento e/ou posse dos Dados Cobertos ou acesso aos Sistemas de Informações da CHS, para cumprir as obrigações a uma ou mais Partes da CHS.

(c) "Dados do Titular do Cartão" tem o significado atribuído a esse termo pelo PCI DSS.

(d) "Sistemas de Informações da CHS" significam equipamentos, sistemas e serviços de informática, comunicação e rede (voz, dados ou outros) de propriedade, controle ou uso da CHS ou qualquer Afiliada da CHS, incluindo, entre outros, a rede de área ampla corporativa, a rede comutada, gateways de inter/intranet, correio eletrônico, telefonia, sistemas de informática, hardware do sistema, drives, mídia eletrônica, áreas de armazenamento, programas de software, arquivos e bancos de dados.

(e) "Parte da CHS", em qualquer caso específico, é a CHS ou uma Afiliada da CHS (i) que contrata com o Fornecedor, (ii) de quem o Fornecedor recebe os Dados Cobertos ou (iii) em cujo nome ou para cujo benefício o Fornecedor coleta ou recebe os Dados Cobertos.

(f) "CIS Critical Controls" means the then-current Center for Internet Security Critical Security Controls for Effective Cyber Defense.[i]

(g) "Covered Data" means:
(i) CHS Personal Information;
(ii) Any usernames, login credentials, passwords, or other access information pertaining to any CHS Information Systems; and

(iii) Any other information held by CHS or any Affiliate of CHS, or that Supplier receives or collects as a part of its performance under an agreement with a CHS Party, that is both:
(A) Not readily ascertainable by the public by proper means; and
(B) The subject of efforts by CHS or its Affiliates to keep it from becoming readily ascertainable by the public by proper means.
(h) "Data Protection Laws" means all laws and regulations, including without limitation, laws and regulations of the European Union, the United States and the California Consumer Privacy Act, applicable to the Processing of Personal Data under the Agreement.

(i) "PCI DSS" means the then-current Payment Card Industry Data Security Standard as promulgated by the PCI Security Standards Council.

(j) "PCI Service Provider" means a service provider as defined by PCI DSS.
(k) "Permitted System" means a CHS Information System to which CHS or a CHS Affiliate expressly gives Supplier access and that is necessary for Supplier to perform its obligations to one or more CHS Parties.

(l) "Personal Information" means any information relating to an identified or identifiable person defined as such in any Data Protection Law(s) in combination with any one or more of the following pieces of unencrypted information: (1) social security number, (2) birth date; (3) driver's license number or government issued identification card, (4) student, military or passport identification number; (5) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (6) medical information, health insurance identification number or biometric data, (7) an individual's user name or email address in combination with a password or security question and answer that allows access to an online account; (8) account number or credit or debit card number, access code, or password that would permit access to an individual's financial account. This information does not include the last 4 digits of an individual's social security number or any information that is legally available in the public records

(f) "Controles Críticos do CIS" significam os então atuais Controles Críticos de Segurança do Centro de Segurança da Internet para Defesa Cibernética Efetiva.[ii]
(g) "Dados Cobertos" significam:
(i) Informações Pessoais da CHS;
(ii) Quaisquer nomes de usuários, credenciais de login, senhas ou outras informações de acesso pertencentes a quaisquer Sistemas de Informações da CHS; e
(iii) Quaisquer outras informações detidas pela CHS ou qualquer Afiliada da CHS ou que o Fornecedor recebe ou coleta como parte de sua execução nos termos de um acordo com uma Parte da CHS, que:
(A) Não sejam prontamente determináveis pelo público por meios adequados; e
(B) O objeto dos esforços da CHS ou suas Afiliadas de impedir que se tornem prontamente determináveis pelo público por meios adequados.
(h) "Leis de Proteção de Dados" significam todas as leis e regulamentos, incluindo, entre outros, leis e regulamentos da União Europeia, dos Estados Unidos e a Lei de Privacidade do Consumidor da Califórnia, aplicáveis ao Tratamento de Dados Pessoais nos termos do Acordo.
(i) "PCI DSS" significa o então atual Padrão de Segurança de Dados da Indústria de Cartões de Pagamento, conforme promulgado pelo Conselho de Normas de Segurança da PCI.
(j) "Prestador de Serviços da PCI" significa um prestador de serviços definido pelo PCI DSS.
(k) "Sistema Permitido" significa um Sistema de Informações da CHS a que a CHS ou uma Afiliada da CHS dá expressamente acesso ao Fornecedor e que é necessário para que o Fornecedor cumpra suas obrigações a uma ou mais Partes da CHS.
(1) "Informações Pessoais" significam quaisquer informações relacionadas a uma pessoa identificada ou identificável definida como tal na(s) Lei(s) de Proteção de Dados em combinação a uma ou mais informações não criptografadas abaixo: (1) número de seguro social; (2) data de nascimento; (3) número da carteira de habilitação ou carteira de identidade emitida pelo governo; (4) número de identificação de estudantes, militares ou passaportes; (5) quaisquer informações relacionadas ao histórico médico, condição mental ou física ou tratamento ou diagnóstico médico de uma pessoa por um profissional da saúde; (6) informações médicas, número de identificação de plano de saúde ou dados biométricos; (7) nome de usuário ou e-mail de uma pessoa em combinação com senha ou pergunta e resposta de segurança que permita acesso a uma conta online; (8) número de conta ou número de cartão de crédito ou débito, código de acesso ou senha que permitiria acesso à conta fina ceira de uma pessoa. Estas informações não incluem os últimos 4 dígitos do número

or a federal or a local agency. "Processing" of Personal Information means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

do seguro social de uma pessoa ou qualquer outra informação legalmente disponibilizada nos registros públicos ou em uma agência federal ou local. "Tratamento" de Informações Pessoais ignifica qualquer operação ou conjunto de operações realizadas sobre as Informações Pessoais ou conjuntos de Informações Pessoais, seja ou não por meio automático, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, restauração, consulta, uso, divulgação por transmissão, disseminação ou, de outra forma, disponibilização, alinhamento ou combinação, bloqueio, rasura ou destruição.

(m) "Security Breach" means any unlawful access to any CHS Covered Data stored on Supplier's equipment or in Supplier's facilities, or access to equipment or facilities resulting in any loss, disclosure, or alteration of CHS Covered Data. "

(m) "Violação de Segurança" significa qualquer acesso ilícito aos Dados Cobertos da CHS armazenados em equipamentos do Fornecedor ou em instalações do Fornecedor, ou acesso a equipamentos ou instalações que resultem em perda, divulgação ou alteração dos Dados Cobertos da CHS. "

2. **Privacy and Data Security Generally**. Supplier shall comply with the terms and conditions contained in this Addendum and will be responsible for any act or omission by any direct or indirect employee, contractor, or agent of Supplier (including, but not limited to, Authorized Supplier Persons) that, if done or omitted to be done by Supplier, would be a violation by Supplier of the requirements of this Addendum.

2. **Termos Gerais de Privacidade e Segurança de Dados.** O Fornecedor deverá cumprir os termos e condições contidos no presente Adendo e será responsável por qualquer ação ou omissão de qualquer funcionário direto ou indireto, contratado ou agente do Fornecedor (incluindo, entre outros, Pessoas Autorizadas do Fornecedor) que, se realizada ou omitida pelo Fornecedor, seria uma violação, por parte do Fornecedor, dos requisitos do presente Adendo.

3. **Privacy and Confidentiality**.

(a) Covered Data Included in Obligations under Agreements. Where any agreement between any CHS Party and Supplier contains any confidentiality obligation or obligation limiting the use or disclosure by Supplier of confidential information of CHS or any CHS Affiliate (whether styled "Confidential Information," "Proprietary Information," or otherwise), the obligations with respect to such information will apply to Covered Data regardless of whether Covered Data is, by the terms of the agreement, included in the scope of the applicable term.

3. **Privacidade e Confidencialidade**

(a) Dados Cobertos Incluídos em Obrigações em Acordos. Quando qualquer acordo entre uma Parte da CHS e o Fornecedor contiver qualquer obrigação de confidencialidade ou obrigação que limite ou uso ou divulgação, por parte do Fornecedor, de informações confidenciais da CHS ou de qualquer Afiliada da CHS (denominadas "Informações Confidenciais", "Informações Privadas" ou outros), as obrigações relacionadas a essas informações se aplicarão aos Dados Cobertos, independente da inclusão dos Dados Cobertos, pelos termos do acordo, no escopo do termo aplicável.

(b) Obligations Generally with Respect to Covered Data. Supplier will:

(i) Keep and maintain all Covered Data in strict confidence, using such degree of care as is necessary to avoid unauthorized access, use, or disclosure, and, in each case, use all protections, safeguards, and care required by applicable law;

(ii) Comply with all law that applies to the collection, use, sharing, storage, protection, transfer, and disposal of such Covered Data;

(iii) Not create, collect, receive, access, or use Covered Data in violation of law;

(iv) Use and disclose Covered Data solely and exclusively for the purposes for which the Covered Data, or access to it, is provided by the CHS Party, and

(b) Obrigações Geralmente Relacionadas aos Dados Cobertos. O Fornecedor:

(i) Conservará e manterá todos os Dados Cobertos em absoluto sigilo, utilizando o grau de cuidado necessário para evitar acesso, uso ou divulgação não autorizada e, em cada caso, usará todas as proteções, defesas e cuidados exigidos pela lei aplicável;

(ii) Cumprirá todas as leis que se aplicam à coleta, uso, compartilhamento, armazenamento, proteção, transferência e descarte dos Dados Cobertos;

(iii) Não criará, coletará, receberá, acessará ou usará os Dados Cobertos em violação à lei;

(iv) Usará e divulgará os Dados Cobertos só e exclusivamente para os objetivos aos quais os Dados Cobertos ou seu acesso são fornecidos pela Parte da

not use, sell, rent, transfer, distribute, or otherwise disclose or make available Covered Data for Supplier's own purposes or for the benefit of any person other than the applicable CHS Party or its designee(s); and

(v) Not, directly or indirectly, disclose Covered Data to any third party without the written consent of the applicable CHS Party.

(c) Compliance with CHS Privacy Statement(s). Supplier will undertake no act or omission that, if done or omitted to be done by the applicable CHS Party, would violate the published public-facing privacy statement or privacy policy of the CHS Party. The CHS Global Privacy Notice can be found here: https://chsinc.com/privacy-policy.

4. **Processing of CHS Covered Data Where Other Contractual Requirements Apply**. Where CHS reasonably deems it necessary in order to comply with applicable law (including, but not limited to, the law of non-US countries that require contractual arrangement in order to legally export Personal Data and law requiring Business Associate Agreements), Supplier will, promptly when requested by any CHS Party, enter into such agreements as CHS reasonably requires in order to comply with applicable law.

5. **Return and/or Destruction of Covered Data**.

(a) Return or other Provision of Covered Data. At the termination or completion of services in connection with which Supplier holds Covered Data, Supplier will, at CHS's option and upon request made by CHS within 30 days after such termination or completion, provide to CHS, in industry-standard electronic form as requested by CHS, such Covered Data as Supplier holds as of the time immediately before termination or completion. If the relevant agreement associated with such services does not provide for compensation for such provision of Covered Data, and does not require provision of such Covered Data at no charge to CHS, CHS sill pay to Supplier the actual cost of media and personnel necessary to provide the Covered Data as required by this Section 7.

(b) Deletion and Destruction of Covered Data. If and when Supplier is required to destroy Covered Data, Supplier will destroy such Covered Data using methods at least as complete and reliable as those contained in NIST Special Publication 800-88, as amended, or its successor document. Where Supplier is permitted to retain Covered Data in de-identified or anonymized form, Supplier will de-identify and anonymize the Covered Data according to NISTIR 8053, as amended,

CHS e não usará, venderá, alugará, transferirá, distribuirá ou, de outra forma, divulgará ou disponibilizará os Dados Cobertos para os próprios objetivos do Fornecedor ou para o benefício de qualquer pessoa diferente da Parte da CHS aplicável ou seu(s) designado(s); e

(v) Não divulgará, direta ou indiretamente, Dados Cobertos a qualquer terceiro sem a autorização escrita da Parte da CHS aplicável.

(c) Cumprimento da(s) Declaração(ões) de Privacidade da CHS. O Fornecedor não se comprometerá em qualquer ação ou omissão que, se realizada ou omitida pela Parte da CHS aplicável, violaria a declaração de privacidade ou política de privacidade publicada e disponibilizada ao público da Parte da CHS. O Avido de Privacidade Global da CHS pode ser encontrado aqui: https://chsinc.com/privacy-policy.

4. **Tratamento de Dados Cobertos da CHS Quando Outros Requisitos Contratuais se Aplicarem**. Quando a CHS considerar, de forma justificada, necessário para cumprir a lei aplicável (incluindo, entre outros, a lei de países diferentes dos Estados Unidos que exigem o arranjo contratual para exportação legal de Dados Pessoais e a lei que exige Acordos de Associação Comercial), o Fornecedor, assim que solicitado por qualquer Parte da CHS, celebrará esses acordos, conforme exigência justificada da CHS, para cumprir a lei aplicável.

5. **Devolução e/ou Destruição de Dados Cobertos**.

(a) Devolução ou outra Provisão de Dados Cobertos. No término ou conclusão dos serviços sobre os quais o Fornecedor detém os Dados Cobertos, o Fornecedor, à escolha da CHS e a pedido desta até 30 dias após esse término ou conclusão, fornecerá à CHS, em formato eletrônico no padrão da indústria, conforme solicitação da CHS, os Dados Cobertos detidos pelo Fornecedor a partir do momento imediatamente anterior ao término ou conclusão. Se o acordo relevante associado a esses serviços não prever remuneração pela provisão de Dados Cobertos e não exigir a provisão desses Dados Cobertos sem custos à CHS, a CHS pagará ao Fornecedor o custo real da mídia e do pessoal necessários para prover os Dados Pessoais, conforme exigência nesta Seção 7.

(b) Supressão e Destruição de Dados Cobertos. Se e quando o Fornecedor for exigido a destruir os Dados Cobertos, o Fornecedor destruirá esses Dados Cobertos utilizando métodos, pelo menos, tão completos e confiáveis quanto aqueles contidos na Publicação Especial NIST 800-88, conforme aditada, ou seu documento sucessor. Quando o Fornecedor tiver permissão de reter Dados Cobertos de forma não identificada ou anonimizada, o Fornecedor não identificará ou anonimizará os Dados Cobertos de

or its successor document or, where required by law, as provided for under such law.

6. **Business Continuity Planning**.

(a) At all times at which Supplier holds Covered Data, Supplier will have in place a bona fide business continuity plan that will ensure that Supplier is able to continue to services when the provision of such services is interrupted for any reason outside of Supplier's reasonable control ("Business Continuity Plan"). Supplier shall maintain and update the Business Continuity Plan at least annually for each of its operational sites related to the provision of services. Supplier will put the Business Continuity Plan in effect if a site becomes unable to perform such services or deliver services for a period of more than five calendar days. Supplier will perform a timely assessment after the occurrence of any event that may delay the performance of maintenance and support or the delivery of services for a period of more than five calendar days. Supplier will activate the Business Continuity Plan if Supplier determines that Supplier will be unable to perform services for a period of more five calendar days.

(b) The Business Continuity Plan shall contain, at a minimum, provisions for (a) a risk assessment and business impact analysis, (b) a prevention/mitigation plan, and (c) a resumption of services plan.

(c) Supplier will provide a copy of the Business Continuity Plan within 10 calendar days of CHS's request for the then-current Business Continuity Plan.

(d) At CHS's request, and at no additional charge to CHS, Supplier will participate in any tests implemented by CHS or discussions initiated by CHS for purposes of evaluating, coordinating and integrating the business continuity plans of its suppliers with CHS' overall business continuity plan. As reasonably requested by CHS, Supplier will reasonably adjust the Business Continuity Plan to better conform to and integrate with CHS' business continuity plan.

7. **Information Security**.

(a) Supplier will implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

(b) Supplier will implement administrative, physical, and technical safeguards to:

acordo com NISTIR 8053, conforme aditado, ou documento sucessor ou, quando exigido por lei, conforme previsto em tal lei.

6. **Planejamento de Continuidade dos Negócios**.

(a) Sempre que o Fornecedor detiver Dados Cobertos, o Fornecedor terá implantado um plano de continuidade dos negócios de boa-fé que garantirá que o Fornecedor pode continuar os serviços na interrupção da prestação dos serviços por qualquer motivo fora do controle razoável do fornecedor ("Plano de Continuidade dos Negócios"). O Fornecedor deverá manter e atualizar o Plano de Continuidade dos Negócios, pelo menos, anualmente para cada um dos seus locais operacionais relacionados à prestação de serviços. O Fornecedor implantará o Plano de Continuidade dos Negócios se um local se tornar incapaz de executar esses serviços ou entregar serviços por um período maior que cinco dias corridos. O Fornecedor executará uma avaliação hábil após a ocorrência de qualquer evento que venha a atrasar a execução da manutenção e suporte ou a entrega de serviços por um período maior que cinco dias corridos. O Fornecedor ativará o Plano de Continuidade dos Negócios se o Fornecedor determinar que não conseguirá executar os serviços por um período maior que cinco dias corridos.

(b) O Plano de Continuidade dos Negócios deverá conter, no mínimo, previsões para (a) uma avaliação de risco e uma análise de impacto de negócios, (b) um plano de prevenção/mitigação e (c) um plano de retomada de serviços.

(c) O Fornecedor entregará uma cópia do Plano de Continuidade dos Negócios até 10 dias corridos após o pedido da CHS para o então atual Plano de Continuidade dos Negócios.

(d) A pedido da CHS e sem encargos adicionais à CHS, o Fornecedor participará de quaisquer testes implantados pela CHS ou discussões iniciadas pela CHS para avaliar, coordenar e integrar os planos de continuidade dos negócios de seus fornecedores com o plano geral de continuidade dos negócios da CHS. Conforme solicitado de forma justificada pela CHS, o Fornecedor ajustará razoavelmente o Plano de Continuidade dos Negócios para ter melhor conformidade e integrar o plano de continuidade dos negócios da CHS.

7. **Segurança da Informação.**

(a) O Fornecedor implantará e manterá um programa escrito de segurança da informação, incluindo políticas, procedimentos e avaliações de risco apropriadas que sejam revisados, pelo menos, anualmente.

(b) O Fornecedor implantará defesas administrativas, físicas e técnicas para:

(i) Protect Covered Data from unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage; and

(ii) Take all necessary steps in mitigating damage, losses, costs and expenses caused by the events set forth in Section 9(b)(i).

(c) Supplier shall notify CHS of any significant changes to administrative, physical, or technical safeguards that could reasonably be expected to adversely affect the protection of Covered Data from unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage.

(d) Where Supplier receives, stores, and/or Processes Covered Data using Supplier's own systems and facilities, Supplier will implement, and maintain, CIS Critical Controls, including, but not limited to, the following controls, each as is more fully explained in the CIS Critical Controls.

(i) Inventory of Authorized and Unauthorized Devices. Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

(ii) Inventory of Authorized and Unauthorized Software. Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

(iii) Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

(iv) Continuous Vulnerability Assessment and Remediation. Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

(v) Controlled Use of Administrative Privileges. The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

(vi) Maintenance, Monitoring, and Analysis of Audit Logs. Collect, manage, and analyze audit logs of

(i) Proteger os Dados Cobertos de acesso não autorizado, exfiltração, aquisição ou divulgação, destruição, alteração, perda acidental, uso inadequado ou danos; e

(ii) Tomar todas as providências necessárias na mitigação de danos, perdas, custos e despesas causados pelos eventos estabelecidos na Seção 9(b)(i).

(c) O Fornecedor deverá notificar a CHS sobre quaisquer alterações significativas para as defesas administrativas, físicas ou técnicas que tenham expectativa razoável de afetar de forma negativa a proteção de Dados Cobertos de acesso não autorizado, exfiltração, aquisição ou divulgação, destruição, alteração, perda acidental, uso inadequado ou danos.

(d) Quando o Fornecedor receber, armazenar e/ou Tratar Dados Cobertos utilizando sistemas e instalações próprios do Fornecedor, o Fornecedor implantará e manterá Controles Críticos do CIS, incluindo, entre outros, os seguintes controles, cada um com demais explicações nos Controles Críticos do CIS.

(i) Inventário de Dispositivos Autorizados e Não Autorizados. Gerenciar ativamente (realizar inventário, rastrear e corrigir) todos os dispositivos de hardware na rede para que somente dispositivos autorizados recebam acesso e os dispositivos não autorizados e não gerenciados sejam encontrados e impedidos de receber acesso.

(ii) Inventário de Softwares Autorizados e Não Autorizados. Gerenciar ativamente (realizar inventário, rastrear e corrigir) todos os softwares na rede para que somente os softwares autorizados sejam instalados e possam operar e os softwares não autorizados e não gerenciados sejam encontrados e tenham sua instalação ou execução impedida.

(iii) Configurações Seguras para Hardware e Software em Dispositivos Móveis, Notebooks, Estações de Trabalho e Servidores. Estabelecer, implantar e gerenciar ativamente (rastrear, reportar, corrigir) a configuração de segurança de notebooks, servidores e estações de trabalho utilizando um processo rigoroso de gestão de configuração e controle de alterações para impedir que os invasores explorem serviços e configurações vulneráveis.

(iv) Avaliação e Remedição Contínuas de Vulnerabilidade. Adquirir, avaliar e agir continuamente sobre novas informações para identificar vulnerabilidades, remediar e minimizar a janela de oportunidades para os invasores.

(v) Uso Controlado de Privilégios Administrativos. Os processos e ferramentas utilizados para rastrear/controlar/prevenir/corrigir o uso, atribuição e configuração de privilégios administrativos em computadores, redes e aplicativos.

(vi) Manutenção, Monitoramento e Análise de Registros de Auditoria. Coletar, gerenciar e analisar

events that could help detect, understand, or recover from an attack.

(vii) E-Mail and Web Browser Protections. Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and e-mail systems.

(viii) Malware Defenses. Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

(ix) Limitation and Control of Network Ports, Protocols, and Services. Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

(x) Data Recovery Capability. Use processes and tools to properly back up critical information with a proven methodology for timely recovery of it.

(xi) Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

(xii) Boundary Defense. Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

(xiii) Data Protection. Use processes and tools to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

(xiv) Controlled Access Based on the Need to Know. Use processes and tools to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

(xv) Wireless Access Control. Use processes and tools to track/control/prevent/ correct the security use of wireless local area networks, access points, and wireless client systems.

(xvi) Account Monitoring and Control. Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion -- in order to minimize opportunities for attackers to leverage them.

registros de auditoria de eventos que podem ajudar a detectar, entender ou se recuperar de um ataque.

(vii) Proteções de E-mail e Navegador. Minimizar a superfície de ataque e as oportunidades para que invasores manipulem o comportamento humano através de sua interação com navegadores e sistemas de e-mail.

(viii) Defesas contra Malware. Controlar a instalação, disseminação e execução do código malicioso em diversos pontos no empreendimento, enquanto otimiza o uso da automação para permitir a rápida atualização da defesa, reunião de dados e ação corretiva.

(ix) Limitação e Controle das Portas, Protocolos e Serviços de Rede. Gerenciar (rastrear/controlar/corrigir) o uso operacional contínuo de portas, protocolos e serviços em dispositivos em rede para minimizar janelas de vulnerabilidade disponibilizadas aos invasores.

(x) Capacidade de Recuperação de Dados. Usar processos e ferramentas para realizar de forma adequada o back-up de informações críticas com uma metodologia comprovada para recuperação hábil destas.

(xi) Configurações Seguras para Dispositivos de Rede, como Firewalls, Roteadores e Interruptores. Estabelecer, implantar e gerenciar ativamente (rastrear, reportar, corrigir) a configuração de segurança dos dispositivos de infraestrutura de rede utilizando um processo rigoroso de gestão de configuração e controle de alterações para impedir que os invasores explorem serviços e configurações vulneráveis.

(xii) Defesa de Interface. Detectar/prevenir/corrigir o fluxo de redes de transferência de informações de níveis diferentes de confiança com foco em dados que danificam a segurança.

(xiii) Proteção de Dados. Utilizar processos e ferramentas para prevenir a exfiltração de dados, mitigar os efeitos dos dados exfiltrados e garantir a privacidade e a integridade de informações sensíveis.

(xiv) Acesso Controlado com Base na Necessidade de Conhecimento. Utilizar processos e ferramentas para rastrear/controlar/prevenir/corrigir o acesso seguro a ativos críticos (por exemplo, informações, recursos, sistemas), de acordo com a determinação formal cujas pessoas, computadores e aplicativos tem necessidade e direito de acesso a estes ativos críticos com base em uma classificação aprovada.

(xv) Controle de Acesso Sem Fio. Utilizar processos e ferramentas para rastrear/controlar/prevenir/corrigir o uso de segurança de redes de área local sem fio, pontos de acesso e sistemas sem fio do cliente.

(xvi) Monitoramento e Controle de Conta. Gerenciar ativamente o ciclo de vida do sistema e as contas de aplicativo - sua criação, uso, inatividade, supressão - para minimizar oportunidades para que invasores as alavanquem.

(xvii) Security Skills Assessment and Appropriate Training to Fill Gaps. For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

(xviii) Application Software Security. Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

(xix) Incident Response and Management. Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

(xx) Penetration Tests and Red Team Exercises. Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

(e) Audits.

(i) Supplier will, with respect to each system that holds, contains, or Processes Covered Data:

(A) Cause examinations to be performed by one or more qualified third parties as stated in, and contemplated by, Statement on Standards for Attestation Engagements No. 16 ("SSAE 16") and reports issued by such third party(ies) attesting that Supplier's management's description of Supplier's system fairly presents the system that was designed and implemented, at either a specific date not earlier than one year prior to the date of determination (in the case of a Type 1 report) or implemented throughout a specified time period that includes a date not earlier than one year prior to the date of determination (in the case of a Type 2 report); and

(B) For so long as such system holds, contains, or processes Covered Data, cause the system to conform in all material respects with management's assertions with respect to the system upon which the then-most-recent SSAE 16 report as of the date of determination.

(ii) Supplier will, upon CHS's request, make available to CHS for review, as applicable, Supplier's latest Payment Card Industry (PCI) Compliance Report, WebTrust reports, Systrust reports, SSAE 16 audit reports, and any reports relating to its ISO/IEC 27001 certification. CHS shall treat such audit reports as Supplier's confidential information for the purposes of

(xvii) Avaliação de Habilidades de Segurança e Treinamento Apropriados para Cobertura de Lacunas. Para todos os cargos funcionais na organização (priorizando as missões críticas para o negócio e sua segurança), identificar o conhecimento, as habilidades e as capacidades específicos para dar suporte à defesa do empreendimento; desenvolver e executar um plano integrado de avaliação, identificação de lacunas e remediação através da política, planejamento organizacional, treinamento e programas de conscientização.

(xviii) Segurança do Software do Aplicativo. Gerenciar o ciclo de vida de segurança de todos os softwares desenvolvidos e adquiridos internamente para prevenir, detectar e corrigir as fraquezas de segurança.

(xix) Resposta e Gestão de Incidentes. Proteger as informações da organização, bem como sua reputação, desenvolvendo e implantando uma infraestrutura de respostas a incidentes (por exemplo, planos, funções definidas, treinamento, comunicações, supervisão de gestão) para descobrir rapidamente um ataque e, então, conter de forma eficaz o dano, erradicar a presença do invasor e restaurar a integridade da rede e dos sistemas.

(xx) Testes de Penetração e Exercícios do *Red Team*. Testar a força geral das defesas de uma organização (a tecnologia, os processos e as pessoas) estimulando os objetivos e as ações de um invasor.

(e) Auditorias.

(i) O Fornecedor, em relação a cada sistema que detém contém ou Trata Dados Cobertos:

(A) Providenciará a realização dos exames por um ou mais terceiros qualificados, conforme declarado e contemplado pela Declaração sobre Normas de Engajamentos de Atestação nº 16 ("SSAE 16") e relatórios emitidos por terceiro(s) atestando que a descrição da administração desse Fornecedor do sistema do Fornecedor apresenta de forma relativa o sistema que foi projetado e implantado, em uma data específica não anterior a um ano antes da data de determinação (no caso de relatório Tipo 1) ou implantado durante um período especificado que inclui uma data não anterior a um ano antes da data de determinação (no caso de relatório Tipo 2); e

(B) Desde que o sistema detenha, contenha ou trate Dados Cobertos, fará com que o sistema entre em conformidade, em todos os aspectos relevantes, com as afirmações da administração em relação ao sistema em que o relatório SSAE 16 mais recente na data de determinação.

(ii) O Fornecedor, a pedido da CHS, disponibilizará à CHS para revisão, quando aplicável, o Relatório de Conformidade da Indústria de Cartões de Pagamento (PCI) mais recente do Fornecedor, relatórios WebTrust, relatórios Systrust, relatórios de auditoria SSAE 16 e quaisquer relatórios relacionados a sua certificação ISO/IEC 27001. A CHS deverá tratar

confidentiality obligations, if any, under any then-existing agreement(s) between Supplier and any applicable CHS Party. Supplier will promptly remedy any exception or failure noted in any SSAE 16 report or other audit report.

(f) Upon CHS's request, to confirm Supplier's compliance with this Addendum and any applicable laws, regulations, and industry standards, Supplier will permit CHS or CHS's agents to perform an assessment, audit, examination, or review of all controls in Supplier's physical and/or technical environment in relation to all Covered Data being handled, received or acquired and/or services being provided to CHS under the applicable agreement, and this Addendum. Supplier shall cooperate fully with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and applicable software that processes, stores, or transports the Covered Data for CHS pursuant to the applicable agreement and this Addendum. In addition, upon CHS's request, Supplier shall provide CHS with the results of any audit by or on behalf of Supplier performed that assess the effectiveness of Supplier's information security program as relevant to the security and confidentiality of the Covered Data shared during the course of the applicable agreement and this Addendum.

(g) PCI DSS. If, and to the extent that, any of the Covered Data is Cardholder Data that Supplier receives or Processes as a PCI Service Provider, Supplier will, unless expressly permitted otherwise in writing by the applicable CHS Party:

(i) Be, at all times while holding or Processing Cardholder Data, a Level 1 Service Provider with current onsite assessments and all other qualifications and certifications necessary to that designation under PCI DSS;
(ii) Deliver to CHS Supplier's Attestation of Compliance promptly upon completion thereof, in such form and containing such information as required under PCI-DSS, dated not more than one year after the previous AOC (if any) delivered by Supplier to CHS;
(iii) If requested by CHS, agree upon a responsibility matrix or other documentation identifying which PCI DSS requirements of CHS will be managed by Supplier; and
(iv) Otherwise comply with all requirements of PCI DSS with respect to the Cardholder Data.

relatórios de auditoria como informações confidenciais do Fornecedores para os objetivos de obrigações de confidencialidade, se houver, nos termos de quaisquer acordos existentes entre o Fornecedor e qualquer Parte da CHS aplicável. O Fornecedor remediará imediatamente qualquer exceção ou falha observada em qualquer relatório SSAE 16 ou outro relatório de auditoria.

(f) A pedido da CHS, para confirmar a conformidade do Fornecedor com o presente Adendo e quaisquer leis, regulamentos e padrões industriais aplicáveis, o Fornecedor permitirá que a CHS ou os agentes da CHS executem uma avaliação, auditoria, exame ou revisão de todos os controles no ambiente físico e/ou técnico do Fornecedor em relação a todos os Dados Cobertos sendo manejados, recebidos ou adquiridos e/ou serviços sendo prestados à CHS nos termos do acordo aplicável e do presente Adendo. O Fornecedor deverá cooperar de forma integral com a avaliação provendo acesso ao pessoal com conhecimento, premissas físicas, documentação, infraestrutura e softwares aplicáveis que tratam, armazenam ou transportam os Dados Cobertos para a CHS, conforme o acordo aplicável e o presente Adendo. Além disso, a pedido da CHS, o Fornecedor deverá fornecer à CHS os resultados de qualquer auditoria realizada por ou em nome do Fornecedor que avaliam a eficácia do programa de segurança de informação do Fornecedor como relevante à segurança e à confidencialidade dos Dados Cobertos compartilhados durante o curso do acordo aplicável e do presente Adendo.

(g) PCI DSS. Se e na medida em que qualquer Dado Coberto for um Dado do Titular do Cartão que o Fornecedor recebe ou Trata como um Prestador de Serviços da PCI, o Fornecedor, salvo permissão expressa contrária, por escrito, pela Parte da CHS aplicável:

(i) Será, sempre que detiver ou Tratar os Dados do Titular do Cartão, um Prestador de Serviços Nível 1 com avaliações presenciais atuais e todas as outras qualificações e certificações necessárias para essa designação sob o PCI DSS;
(ii) Entregará à CHS o Atestado de Conformidade do Fornecedor logo após sua conclusão, na forma e contendo as informações exigidas sob o PCI-DSS, com data de até um ano após o AOC anterior (se houver) entregue pelo Fornecedor à CHS;
(iii) Se solicitado pela CHS, ajustará uma matriz de responsabilidade ou outra documentação que identifica quais requisitos do PCI DSS da CHS serão gerenciados pelo Fornecedor; e
(iv) De outra forma, cumprirá todos os requisitos do PCI DSS em relação aos Dados do Titular do Cartão.

8. **Access to CHS Information Systems**.

(a) Use of Permitted Systems. Supplier will use any Permitted Systems solely to carry out Supplier's obligations to the applicable CHS Party(ies). Supplier will use Permitted Systems for no other purpose.

(b) Conditions of Use. Supplier will use the Permitted Systems solely accordance with the terms of such agreement(s) as is (are) then in place between one or more CHS Parties and Supplier and such further conditions and policies as the applicable CHS Party makes available to Supplier from time to time. Such conditions and policies of use may include (and be described as) policies, procedures, technical requirements, and/or protocols.

(c) Access by Authorized Supplier Persons. Supplier will limit access to the Permitted Systems to Authorized Supplier Persons. Supplier will provide to CHS the name of each Authorized Supplier Person. Each Authorized Supplier Person must establish and maintain a unique identifier for access and follow the same security rules as CHS's personnel. Supplier shall ensure that individuals other than Authorized Supplier Persons (including, without limitation, past employees and current employees who do not have an active role in providing goods, services, or software to CHS or its Affiliates) shall have no access to CHS Information Systems.

(d) Specific Prohibitions. Except as expressly authorized by a CHS Party in a signed writing (whether in a statement of work, project specification, work order, or separate written direction) Supplier shall not (i) attempt to reverse engineer, disassemble, reverse translate, decompile or in any other manner decode any element of the CHS Information Systems; (ii) make modifications, enhancements, adaptations or translations, in whole or in part, to or of any element of the CHS Information Systems; (iii) make copies of any element of the CHS Information Systems; (iv) probe host computers or networks; (v) breach or examine the security controls of a host computer, network component or authentication system; (vi) monitor data on any network or system; (vii) interfere with the service of any user, host or network, or overload a server, network connected device, or network component; (viii) originate malformed data or network traffic that results in damage to, or disruption of, a service or network connected device; (ix) forge data or misrepresent the origination of a user or source.

8. **Acesso aos Sistemas de Informações da CHS**.

(a) Uso de Sistemas Permitidos. O Fornecedor utilizará quaisquer Sistemas Permitidos exclusivamente para executar as obrigações do Fornecedor à(s) parte(s) da CHS aplicável(is). O Fornecedor não usará Sistemas Permitidos para nenhum outro objetivo.

(b) Condições de Uso. O Fornecedor utilizará os Sistemas Permitidos exclusivamente de acordo com os termos desse(s) acordo(s) que for(em) implantado(s) entre uma ou mais Partes da CHS e o Fornecedor e demais condições e políticas que a Parte da CHS aplicável disponibilizar ao Fornecedor de tempos em tempos. Essas condições e políticas de uso poderão incluir (e ser descritas como) políticas, procedimentos, requisitos técnicos e/ou protocolos.

(c) Acesso de Pessoas Autorizadas do Fornecedor. O Fornecedor limitará acesso aos Sistemas Permitidos às Pessoas Autorizadas do Fornecedor. O Fornecedor proverá à CHS o nome de cada Pessoa Autorizada do Fornecedor. Cada Pessoa Autorizada do Fornecedor deve estabelecer e manter um identificador único para acesso e seguir as mesmas regras de segurança como pessoal da CHS. O Fornecedor deverá garantir que as pessoas físicas diferentes das Pessoas Autorizadas do Fornecedor (incluindo, entre outros, ex-funcionários e atuais funcionários que não têm função ativa na provisão de mercadorias, serviços ou softwares à CHS ou suas Afiliadas) não tenham acesso aos Sistemas de Informações da CHS.

(d) Proibições Específicas. Salvo autorização expressa de uma Parte da CHS em um documento assinado (em um descritivo de serviços, especificação de projeto, ordem de serviço ou instrução escrita separada), o Fornecedor não deverá (i) tentar aplicar engenharia reversa, desmontar, aplicar tradução reversa, descompilar ou, de qualquer outra forma, decodificar qualquer elemento dos Sistemas de Informações da CHS; (ii) realizar modificações, aprimoramentos, adaptações ou traduções, integral ou parcialmente, para ou de qualquer elemento dos Sistemas de Informações da CHS; (iii) fazer cópias de qualquer elemento dos Sistemas de Informações da CHS; (iv) sondar computadores ou redes de host; (v) violar ou examinar os controles de segurança de um computador, rede, componente ou sistema de autenticação de host; (vi) monitorar dados em qualquer rede ou sistema; (vii) interferir com o serviço de qualquer usuário, host ou rede, ou sobrecarregar um servidor, dispositivo conectado em rede ou componente de rede; (viii) originar dados malformados ou tráfego de rede que resulte em danos ou interrupção de um serviço ou dispositivo conectado em rede; (ix) falsificar dados ou dar declaração falsa sobre a origem de um usuário ou fonte.

(e) Failure of Access. Supplier acknowledges that access to the Permitted Systems may be interrupted due to circumstances within or outside the reasonable control of the applicable CHS Party(ies). Nothing in this Addendum or any agreement between Supplier and any CHS Party will be a promise or covenant to deliver access to the Permitted Systems or that any Permitted System will be functional. Aside from the access as provided under this Addendum, no license under any patent, copyright, or any other intellectual property right in respect of CHS Information System is granted to Supplier by virtue of access to the Permitted Systems.

(f) Waiver of Liability. CHS excludes all representations, warranties, and covenants, express or implied, by CHS or any CHS Affiliate with respect to the CHS Information Systems, including, but not limited to, any representations, warranties, or conditions of accuracy, sufficiency, suitability, or non-infringement regarding Supplier's access to, or use of, any Permitted System. CHS and its Affiliates will have no liability whatsoever for any damages, losses, or expenses incurred by Supplier as a result of Supplier's or its Supplier Authorized Persons' access to the Permitted Systems (including, without limitation, the inadvertent accessing of a computer virus or other harmful computer file or program), or of failure of the Permitted System(s) to be available or accessible.

(g) Supplier Systems. Where Supplier accesses Permitted Systems using Supplier's hardware, software, or networks, the following provisions will apply.

(i) Access Security. Supplier shall ensure that Authorized Supplier Persons obtain access to the Permitted Systems through a computer system that maintains authentication controls and includes a suitable firewall. Supplier shall follow all of CHS' security rules and procedures for restricting access to its computer systems.

(ii) Segregation Wall. Supplier will ensure that Authorized Supplier Persons are effectively isolated from its personnel who are assigned to the account of a known or potential competitor of CHS or of any Affiliate of CHS. Supplier will establish and document physical and electronic procedures to segregate and protect all information, data and communications (including, but not limited to, Covered Data).

9. **Security Breach Procedures**.

(a) Supplier will provide to the applicable CHS Party name and contact information for one or more representatives of Supplier (which may be a live-staffed

(e) Falha de Acesso. O Fornecedor reconhece que o acesso aos Sistemas Permitidos poderão ser interrompidos devido a circunstâncias dentro ou fora do controle razoável da(s) Parte(s) da CHS aplicável(is). Nada contido no presente Adendo ou em qualquer acordo entre o Fornecedor e qualquer Parte da CHS será uma promessa ou compromisso de entrega de acesso aos Sistemas Permitidos ou que qualquer Sistema Permitido estará funcional. Apesar do acesso previsto nos termos do presente Adendo, nenhuma licença sob qualquer patente, direito autoral ou qualquer outro direito de propriedade intelectual relacionado ao Sistema de Informações da CHS é outorgada ao Fornecedor em virtude do acesso aos Sistemas Permitidos.

(f) Renúncia de Responsabilidade. A CHS exclui todas as declarações, garantias e compromissos, expressos ou implícitos, da CHS ou qualquer Afiliada da CHS em relação aos Sistemas de Informações da CHS, incluindo, entre outros, quaisquer declarações, garantias ou condições de precisão, suficiência, adequação ou não violação relacionadas ao acesso ou uso de qualquer Sistema Permitido pelo Fornecedor. A CHS e suas Afiliadas não terão qualquer responsabilidade por quaisquer danos, prejuízos ou despesas incorridas pelo Fornecedor em decorrência do acesso do Fornecedor ou Pessoas Autorizadas do Fornecedor aos Sistemas Permitidos (incluindo, entre outros, o acesso inadvertido de um vírus de computador ou outro arquivo ou programa de computador nocivo) ou de não disponibilização ou acessibilização do(s) Sistema(s) Permitido(s).

(g) Sistemas do Fornecedor. Quando o Fornecedor acessar os Sistemas Permitidos com uso de hardware, software ou redes do Fornecedor, as seguintes disposições se aplicarão.

(i) Segurança de Acesso. O Fornecedor deverá garantir que as Pessoas Autorizadas do Fornecedor obtenham acesso aos Sistemas Permitidos através de um sistema de informática que mantém controles de autenticação e inclui um firewall adequado. O Fornecedor deverá seguir todas as regras e procedimento de segurança da CHS para restrição de acesso a seus sistemas de informática.

(ii) Muro de Segregação. O Fornecedor garantirá que as Pessoas Autorizadas do Fornecedor sejam efetivamente isoladas do seu pessoal atribuído à conta de um concorrente conhecido ou potencial da CHS ou de qualquer Afiliada da CHS. O Fornecedor estabelecerá e documentará procedimentos físicos e eletrônicos para segregar e proteger todas as informações, dados e comunicações (incluindo, entre outros, os Dados Cobertos).

9. **Procedimentos de Violação de Segurança**.

(a) O Fornecedor fornecerá à Parte da CHS aplicável o nome e o contato de um ou mais representantes do Fornecedor (que poderão ser um help

help desk) who will serve as CHS's primary security contact and be available to assist CHS 24 hours per day, seven days per week as a contact in resolving obligations associated with any actual or suspected Security Breach.

(b) In the case of any actual or suspected Security Breach, the following provisions will apply.

(i) Supplier will notify the applicable CHS Party of the actual or suspected Security Breach as soon as practicable, but in any case not later than 24 hours after Supplier becomes aware of the actual or suspected Security Breach. If the agreement or other terms and conditions under which Supplier provides goods, services, or software to the CHS Party provide for a specific CHS Party contact, supplier will notify that CHS Party contact and also send an e-mail notification to CHSinformationsecurity@chsinc.com. If the agreement or other terms and conditions under which Supplier provides goods, services, or software to the CHS Party do not provide for a specific CHS Party contact, Supplier will notify CHS Information Security by e-mail at CHSinformationsecurity@chsinc.com and/or IT Service Center Phone: 651-355-5555 or 800-852-8185. Supplier will also provide to CHS any other notice required by law.

(ii) Immediately following Supplier's notification to the CHS Party of an actual or suspected Security Breach, Supplier will coordinate with the CHS Party and its designees to investigate the actual or suspected Security Breach. Supplier will reasonably cooperate with the CHS Party in the CHS Party's handling of the matter, including, without limitation: (A) assisting with any investigation; (B) providing CHS with physical access to the facilities and operations affected; (C) facilitating interviews with Supplier's employees and others involved in the matter; and (D) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by the CHS Party or its designees.

(iii) Supplier will, at its own expense, immediately contain and remedy any Security Breach, including, but not limited to, taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards. Supplier shall reimburse CHS and its Affiliates for all costs incurred by CHS in responding to, and mitigating damages caused by, any Security Breach, including, but not limited to, all costs of notice and/or remediation.

(iv) Except as is required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Supplier will not

desk com atendentes humanos) que prestarão serviços como contato de segurança principal da CHS e serão disponibilizados para auxiliar a CHS 24 horas por dia, sete dias por semana, como contato na resolução de obrigações associadas a qualquer Violação de Segurança real ou suspeita.

(b) No caso de qualquer Violação de Segurança real ou suspeita, as disposições a seguir se aplicarão.

(i) O Fornecedor notificará a Parte da CHS aplicável sobre a Violação de Segurança real ou suspeita, assim que prático, mas, em qualquer caso, até 24 horas após o Fornecedor tomar conhecimento da Violação de Segurança real ou suspeita. Se o acordo ou outros termos e condições sob quais o Fornecedor fornece mercadorias, serviços ou software à Parte da CHS fornecer um contato específico da Parte da CHS, o Fornecedor notificará esse contato e também enviará uma notificação de e-mail para CHSinformationsecurity@chsinc.com. Se o acordo ou outros termos e condições sob os quais o Fornecedor fornece mercadorias, serviços ou software à Parte da CHS não previr um contato específico da Parte da CHS, o Fornecedor notificará a Segurança da Informação da CHS pelo e-mail CHSinformationsecurity@chsinc.com e/ou pelo Telefone do Centro de Serviços de TI: 651-355-5555 ou 800-852-8185. O Fornecedor também fornecerá à CHS qualquer outro aviso exigido em lei.

(ii) Logo após a notificação do Fornecedor à Parte da CHS sobre uma Violação de Segurança real ou suspeita, o Fornecedor coordenará com a Parte da CHS e seus designados para investigar a Violação de Segurança real ou suspeita. O Fornecedor cooperará de forma razoável com a Parte da CHS no manejo da questão, por parte da Parte da CHS, incluindo, entre outros: (A) auxiliar com qualquer investigação; (B) fornecer CHS acesso físico às instalações e operações afetadas; (C) facilitar entrevistas com colaboradores do Fornecedor ou outros envolvidos na questão; e (D) disponibilizar todos os registros, arquivos, relatórios de dados e outros materiais relevantes necessários para cumprir a lei, regulamento, normas industrias relevantes ou conforme razoavelmente exigido, de outra forma, pela Parte da CHS ou seus designados.

(iii) O Fornecedor, às suas custas, conterá e remediará imediatamente qualquer Violação de Segurança, incluindo, entre outros, a tomada de toda e qualquer providência necessária para cumprir os direitos de privacidade, leis, regulamentos e normas aplicáveis. O Fornecedor deverá reembolsar a CHS e suas Afiliadas por todos os custos incorridos pela CHS na resposta e mitigação de danos causados por qualquer Violação de Segurança, incluindo, entre outros, todos os custos de notificação e/ou remediação.

(iv) Salvo exigência em lei ou exigência contrária de atuação urgente para mitigar ou evitar mais prejuízos ou danos a pessoas ou bens, o Fornecedor não informará

inform any third party of any Security Breach without first obtaining CHS's prior written consent. Where Supplier informs any third party of a Security Breach as required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Supplier will give notice to the applicable CHS Party concurrently with such other notice.

(v) Except as is required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, CHS will have the sole right to determine: (A) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise, in CHS's discretion; and (B) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

(vi) Supplier will maintain and preserve all documents, records, and other data related to any Security Breach.

(vii) Supplier shall indemnify, defend, and hold harmless CHS and its Affiliates and their respective directors, managers, officers, employees, and agent from any and all claims, suits, damages, liabilities, obligations, costs, and expenses (including, but not limited to, reasonable attorneys' fees and the costs of any credit monitoring or other services required to mitigate such Security Breach for customers, end users, and other persons whose information was released as part of such Security Breach) arising from or otherwise related to any Security Breach.

10. **Coordination of this Addendum with Other Agreements**.

(a) The obligations in this Addendum are, wherever possible, to be regarded as additional to any other obligations in any agreement between Supplier and any CHS Party.

(b) Where possible, the provisions of this Addendum will be construed as consistent with those of other terms, conditions, and agreements between Supplier on the one hand and CHS and/or its Affiliates on the other hand.

(c) Where the provisions of this Addendum cannot be construed consistently with the provisions of other terms, conditions, and agreements between Supplier on the one hand and CHS and/or its Affiliates on the other hand, the provision containing or imposing the greater restriction or protection benefitting the CHS Party will prevail.

a qualquer terceiro sobre qualquer Violação de Segurança sem primeiro obter a anuência prévia e escrita da CHS. Quando o Fornecedor informar a qualquer terceiros obre uma Violação de Segurança, conforme exigido em lei ou de outra forma para atuação urgente para mitigar ou evitar mais prejuízos ou danos a pessoas ou bens, o Fornecedor entregará uma notificação à Parte da CHS aplicável em simultaneidade com qualquer outra notificação.

(v) Salvo exigência em lei ou exigência contrária de atuação urgente para mitigar ou evitar mais prejuízos ou danos a pessoas ou bens, a CHS terá o direito exclusivo de determinar: (A) se a notificação da Violação de Segurança deve ser fornecida a quaisquer pessoas físicas, reguladores, agências policiais, agências de proteção ao crédito ou outros, conforme exigido em lei ou regulamento ou, de outra forma, a critério da CHS; e (B) o conteúdo dessa notificação, vindo qualquer tipo de remediação a ser oferecida às pessoas afetadas e a natureza e extensão dessa remediação.

(vi) O Fornecedor manterá e preservará todos os documentos, registros e outros dados relacionados a qualquer Violação de Segurança.

(vii) O Fornecedor deverá indenizar, defender e isentar a CHS e suas Afiliadas e seus respectivos conselheiros, administradores, diretores, colaboradores e agentes de e contra qualquer reivindicação, processo, dano, passivo, obrigação, custo e despesa (incluindo, entre outros, honorários advocatícios razoáveis e custos de qualquer monitoramento de crédito ou outros serviços necessários para mitigar a Violação de Segurança aos clientes, usuários finais e outras pessoas cujas informações foram liberadas como parte dessa Violação de Segurança) decorrentes ou, de outra forma, relacionados a qualquer Violação de Segurança.

10. **Coordenação do presente Adendo com Outros Acordos**.

(a) As obrigações do presente Adendo devem, quando possível, ser consideradas adicionais a quaisquer outras obrigações em qualquer acordo entre o Fornecedor e qualquer Parte da CHS.

(b) Quando possível, as disposições do presente Adendo serão interpretadas de forma consistente com aquelas dos outros termos, condições e acordos entre o Fornecedor, de um lado, e a CHS e/ou suas Afiliadas, de outro lado.

(c) Quando as disposições do presente Adendo não puderem ser interpretadas de forma consistente com as disposições de outros termos, condições e acordos entre o Fornecedor, de um lado, e a CHS e/ou suas Afiliadas, de outro lado, a disposição contendo ou imposto maior restrição ou proteção que beneficia a Parte da CHS prevalecerá.

Service Provider:_____	Provedor de Serviços:_____
Name: _____	Nome: _____
Title: _____	Título: _____
Signature: _____	Assinatura: _____
Date: _____	Data: _____

[i] The Center for Internet Security Critical Security Controls for Effective Cyber Defense work is licensed under a Creative Commons Attribution – Non Commercial – No Derivatives 4.0 International Public License. The link to the license terms can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode. Users of the CIS Critical Security Controls framework are also required to refer to https://www.cisecurity.org/controls/cis-controls-list/ when referring to the CIS Critical Security Controls in order to ensure that users are employing the most up to date guidance.

[ii] A obra Controles Críticos de Segurança do Centro para Segurança da Informação para Defesa Cibernética Efetiva é licenciada nos termos de uma Licença Pública Internacional de Atribuição da Creative Commons - Não Comercial - Sem Derivativos 4.0. O link para os termos da licença pode ser encontrado em https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode. Os usuários da estrutura dos Controles Críticos de Segurança do CIS também devem consultar https://www.cisecurity.org/controls/cis-controls-list/ ao consultar os Controles Críticos de Segurança do CIS para garantir que os usuários usem as orientações mais atualizadas.