Requisitos de segurança da informação

1. Introdução

O Fornecedor e a CWT firmaram um contrato sob o qual o Fornecedor concordou em fornecer serviços e/ou produtos sob os termos desse contrato (“ **Contrato** ”). O Fornecedor concorda que cumprirá e fará com que Terceiros agindo em seu nome cumpram os requisitos de segurança da informação contidos neste documento (“ **Requisitos de Segurança da Informação ”)** e as medidas de segurança da informação exigidas (“ **Medidas de Segurança Técnicas e Organizacionais** ”). Os Requisitos de Segurança da Informação e Medidas de Segurança Técnica e Organizacional são incorporados e fazem parte do Contrato.

2. Definições

2.1 Salvo disposição em contrário ou expandida neste documento, os termos definidos terão o mesmo significado estabelecido no Contrato. Os seguintes termos definidos se aplicam a estes Requisitos de Segurança da Informação . Se houver um conflito entre a definição contida no Contrato e as aqui contidas, a definição neste documento deverá prevalecer no que se refere aos Requisitos de Segurança da Informação.

“**Afiliadas**”, salvo definição em contrário no Contrato, significa, com referência a quais das partes, que na data de assinatura do Contrato, direta ou indiretamente: (i) controle uma parte; ou (ii) seja controlada, direta ou indiretamente, por uma parte; ou (iii) seja controlada por empresa ou entidade que controle direta ou indiretamente uma parte. Para esses fins, “controle” significa o direito de exercer mais de 50% (cinquenta por cento) do direito de voto ou direito de propriedade similar; mas apenas enquanto tal controle continuar a existir.

“Funcionário Autorizado” significa os funcionários do Fornecedor que precisam conhecer ou acessar Informações Confidenciais e Informações Pessoais para permitir que o Fornecedor cumpra suas obrigações nos termos do Contrato.

“**Parte Autorizada” ou “Partes Autorizadas” significa os** Funcionários Autorizados do Fornecedor (i); e (ii) Terceiros que tenham necessidade de conhecer ou acessar Informações Pessoais e Informações Confidenciais para permitir que o Fornecedor cumpra suas obrigações nos termos do Contrato, e que estejam vinculados por escrito por confidencialidade e outras obrigações suficientes para proteger Informações Pessoais e Informações Confidenciais de acordo com os termos e condições do Contrato e deste documento.

“Informações Confidenciais” significa qualquer informação comercialmente sensível, proprietária ou de outra forma confidencial relacionada a (a) CWT, seus parceiros e suas Afiliadas; (b) um cliente da CWT e funcionários, contratados, subcontratados ou fornecedores do cliente CWT; (c) Pessoal da CWT; (d) seus parceiros independentes e joint ventures; ou (e) o conteúdo e/ou finalidade do Contrato, seja oral, por escrito ou que por qualquer outro meio possa, direta ou indiretamente, chegar à posse do Vendedor ou de Partes Autorizadas como resultado ou em conexão com o Acordo. Para evitar dúvidas, todo Produto de Trabalho constituirá Informação Confidencial.

"CWT" , a menos que definido de outra forma no Contrato, significa a entidade CWT descrita no Contrato, bem como suas Afiliadas.

" **Zona Desmilitarizada** " ou " **DMZ** " é uma rede ou sub-rede que fica entre uma rede interna confiável, como uma rede local (LAN) privada corporativa e uma rede externa não confiável, como a Internet pública. Uma DMZ ajuda a impedir que usuários externos obtenham acesso direto a sistemas internos e outros recursos.

"Processo de Gerenciamento de Incidentes" é um processo e procedimento documentado e desenvolvido pelo Fornecedor a ser seguido no caso de um ataque real ou suspeito, intrusão, acesso não autorizado, perda ou outra violação envolvendo a confidencialidade, disponibilidade ou integridade de Informações Pessoais e Informações Confidenciais da CWT.

"Mascarar" é o processo de cobrir informações exibidas em uma tela.

"Dispositivos Móveis e Portáteis" significa computadores, dispositivos, mídias e sistemas móveis e/ou portáteis capazes de serem facilmente transportados, movidos, transportados ou transportados que são usados em conexão com o Contrato. Exemplos de tais dispositivos incluem laptops, tablets, discos rígidos USB, cartões de memória USB, Personal Digital Assistants (PDAs), telefones celulares ou de dados e qualquer outro dispositivo sem fio, periférico ou removível com capacidade de armazenar Informações Confidenciais e Informações Pessoais .

"Informações Pessoais" , a menos que definido de outra forma no Contrato, significa conforme definido no Regulamento (UE) 2016/679 e outras leis globais aplicáveis de segurança da informação, proteção de dados e privacidade, significa qualquer informação relacionada a uma pessoa física identificada ou identificável, que pode ser identificado direta ou indiretamente, em especial por referência a um número de identificação ou a um ou mais fatores específicos de sua identidade física, fisiológica, mental, econômica, cultural ou social. As Informações Pessoais são de propriedade da CWT, não do Fornecedor.

"Gateway de Segurança" significa um conjunto de mecanismos de controle entre duas ou mais redes com diferentes níveis de confiança que filtram e registram o tráfego que passa ou tenta passar entre as redes e os servidores administrativos e de gerenciamento associados. Exemplos de gateways de segurança incluem firewalls, servidores de gerenciamento de firewall, caixas de salto, controladores de borda de sessão, servidores proxy e dispositivos de prevenção de intrusão.

"Autenticação Forte" significa o uso de mecanismos de autenticação e metodologias de autenticação que requerem vários fatores de autenticação, incluindo pelo menos dois dos seguintes: (1) Conhecimento - algo que o usuário sabe, por exemplo , senha ou número de identificação pessoal, (2) Propriedade - algo o usuário possui, por exemplo, token, cartão inteligente, telefone celular e (3) Inerência - algo que o usuário é, por exemplo, impressão digital.

"Criptografia Forte" significa o uso de tecnologias de criptografia com comprimentos mínimos de chave de 256 bits para criptografia simétrica e 1024 bits para criptografia assimétrica, cuja força fornece garantia razoável de que protegerá as informações criptografadas de acesso não autorizado e é adequada para proteger a confidencialidade e privacidade da informação encriptada , e que incorpora uma política documentada para a gestão das chaves de encriptação e processos associados adequados para proteger a confidencialidade e privacidade das chaves e palavras-passe utilizadas como entradas para o algoritmo de encriptação. A criptografia forte inclui, mas não se limita a: SSL v3.0+/TLS v1.2, protocolo de encapsulamento ponto a ponto (PPTP), AES 256, FIPS 140-2 (somente governo dos Estados Unidos), RSA 1024 bit, SHA1/SHA2 /SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4 ou WPA2.

"Medidas de Segurança Técnica e Organizacional" significa quaisquer atividades exigidas por estes Requisitos de Segurança da Informação acessar, gerenciar, transferir, processar, armazenar, reter e destruir informações ou dados; divulgar e notificar as partes afetadas exigidas pelo Contrato e pelas leis aplicáveis de privacidade e proteção de dados; e para proteger informações ou dados para garantir disponibilidade, integridade, confidencialidade e privacidade, ou notificar indivíduos sobre qualquer falha em proteger tais informações ou dados. As medidas incluem, mas não se limitam àquelas exigidas ou interpretadas como exigidas pelo Regulamento Geral de Proteção de Dados da UE (GDPR), Diretiva de Serviço de Pagamento da UE, Lei de Privacidade do Consumidor da Califórnia, NYS DFS 23 NYCRR 500 , Lei Gramm-Leach Bliley dos Estados Unidos (GLBA), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde dos Estados Unidos (HIPAA), os requisitos de privacidade de dados da UE/Suíça e quaisquer outras leis internacionais e dos EUA, interpretações legais oficiais ou precedentes de casos relativos a informações ou dados sob o Contrato .

"**Terceiros"** ou "**Terceiros**" significa Vendedor consultores subcontratados , pessoal temporário, contratados ou fornecedores e/ou agentes adicionais agindo em nome do Fornecedor e inclui qualquer definição de Terceiro sob a lei aplicável da UE, dos EUA ou de outra lei internacional.

"**Fornecedor**" significa a entidade contratante estabelecida no Contrato em conjunto com suas Afiliadas e seus Terceiros.

3 . <u>Organização da Segurança da Informação</u>

O Fornecedor deverá , no mínimo :

3.1 Garantir que apenas as Partes Autorizadas tenham acesso a Informações Pessoais e Informações Confidenciais.

3.2 Implementar medidas de segurança técnica e organizacional que não sejam menos rigorosas do que as melhores práticas de segurança da informação para proteger a integridade, disponibilidade e confidencialidade de Informações Confidenciais, Informações Pessoais e outras informações não públicas e impedir o acesso não autorizado, aquisição, divulgação,

destruição, alteração , perda acidental, uso indevido ou dano das Informações Pessoais ou Informações Confidenciais.

3.3 Estabelecer, implementar e manter a consistência com as melhores práticas do setor , políticas e um programa de Medidas de Segurança Organizacional, Operacional, Administrativa, Física e Técnica e Organizacional apropriadas para (1) impedir qualquer acesso por Partes não Autorizadas a Informações Pessoais e Informações Confidenciais em de uma maneira não autorizada pelo Contrato ou por estes Requisitos de Segurança da Informação e (2) cumprir e cumprir todas as leis e regulamentos aplicáveis e os padrões da indústria aplicáveis.

3.4 Fornecer às Partes Autorizadas que terão acesso a Informações Pessoais e Informações Confidenciais supervisão, orientação e treinamento sobre as Medidas de Segurança Técnica e Organizacional, incluindo treinamento que forneça exercícios práticos alinhados com os cenários de ameaças atuais e forneça feedback aos participantes do treinamento . O Fornecedor deverá fornecer treinamento de Medidas de Segurança Técnica e Organizacional mediante a contratação de um Funcionário Autorizado e antes do acesso de uma Parte Autorizada a Informações Confidenciais e Informações Pessoais. O treinamento de atualização deve ser fornecido pelo menos anualmente e o mais rápido possível após qualquer mudança material nas Medidas de Segurança Técnica e Organizacional do Fornecedor.

3.5 Fornecer treinamento especializado específico para as Partes Autorizadas com funções de segurança significativas, incluindo, mas não se limitando a recursos humanos ou funções de tecnologia da informação e qualquer função de administrador de tecnologia. No mínimo, o treinamento especializado deve incluir, conforme aplicável à função, procedimentos de segurança da informação, uso aceitável de recursos de segurança da informação, ameaças atuais aos sistemas de informação, recursos de segurança de sistemas específicos e procedimentos de acesso seguro.

3.6 Tome medidas razoáveis para evitar o acesso não autorizado ou a perda de Informações Pessoais e Informações Confidenciais e dos serviços, sistemas, dispositivos ou mídia que contenham essas informações.

3.7 Empregar processos e procedimentos de avaliação de risco para avaliar regularmente os sistemas usados para fornecer serviços ou produtos à CWT. O Fornecedor deve remediar tais riscos o mais rápido possível e proporcional ao nível de risco para Informações Pessoais e Informações Confidenciais devido a ameaças conhecidas no momento da identificação. Operar um processo para permitir a comunicação de riscos ou incidentes suspeitos para a equipe de segurança do Fornecedor.

3.8 Na medida em que o Fornecedor executa serviços de acordo com o Contrato nas instalações da CWT ou usando serviços, sistemas, dispositivos ou mídia de propriedade, operados ou gerenciados pela CWT, o Fornecedor fará com que todas as Partes Autorizadas cumpram todas as políticas da CWT disponibilizadas ao Fornecedor , mediante sua solicitação, que são aplicáveis a tal acesso. O Fornecedor deverá notificar imediatamente a CWT por escrito quando uma Parte Autorizada não precisar mais acessar as Informações Pessoais ou

Informações Confidenciais para que o Fornecedor forneça produtos ou serviços à CWT , incluindo, sem limitação , quando uma Parte Autorizada for rescindida ou não estiver mais realizando serviços ao abrigo do Acordo.

3.9 Manter registros das Partes Autorizadas e dos recursos do Fornecedor que acessam, transferem, mantêm, armazenam ou processam Informações Pessoais e Informações Confidenciais.

3.10 Realizar verificações abrangentes de antecedentes de todas as Partes Autorizadas antes da contratação, na medida permitida por lei . A verificação abrangente de antecedentes de indivíduos deve incluir , no mínimo, o histórico de emprego anterior do indivíduo, antecedentes criminais, histórico de crédito, verificações de referência e quaisquer requisitos adicionais de verificação de antecedentes padrão do setor.

3.11 Ter um ou mais funcionários qualificados designados com a responsabilidade de manter seu programa de segurança da informação e deve informar sobre seu programa de segurança da informação pelo menos anualmente ao conselho de administração do Fornecedor ou órgão administrativo equivalente. O Fornecedor deve garantir que seu pessoal de segurança tenha experiência e treinamento razoáveis e necessários em segurança da informação, incluindo a manutenção do conhecimento sobre ameaças e contramedidas em constante mudança. Mediante solicitação, o Fornecedor deverá fornecer à CWT um ponto de contato para todos os itens relacionados à segurança da informação.

3.12 Exigir compromissos contratuais de não divulgação ou confidencialidade das Partes Autorizadas antes de fornecer acesso a Informações Pessoais e Informações Confidenciais.

3.13 Garantir que todas as Partes Autorizadas que possam estar realizando trabalhos sob o Contrato ou que possam ter acesso a Informações Pessoais ou Informações Confidenciais estejam em conformidade com estas Medidas de Segurança Técnica e Organizacional, que serão evidenciadas por um contrato por escrito não menos restritivo do que estes Requisitos de Segurança da Informação .

4. <u>Segurança Física e Ambiental</u>

O Fornecedor deverá , no mínimo :

4.1 Certifique-se de que todos os sistemas do Fornecedor e outros recursos destinados ao uso por vários usuários estejam localizados em instalações físicas seguras com acesso limitado e restrito apenas a indivíduos autorizados.

4.2 Monitorar e registrar, para fins de auditoria, acesso às instalações físicas contendo sistemas e outros recursos destinados ao uso por vários usuários usados em conexão com o desempenho do Fornecedor de suas obrigações sob o Contrato.

4.3 Exigir que todas as Partes Autorizadas cumpram uma política de limpeza de mesa e bloqueiem as telas das estações de trabalho antes de deixar as áreas de trabalho.

4.4 Recolher todos os ativos da empresa após a rescisão do contrato de trabalho ou rescisão do contrato.

4.5 Limite e monitore o acesso físico às suas instalações de acordo com os seguintes requisitos:

a. O acesso do visitante é registrado, que é mantido por 3 (três) meses incluindo o nome do visitante, empresa que representa e o nome do funcionário que autoriza o acesso físico. Os visitantes devem ser sempre acompanhados por um funcionário do Fornecedor .
b. O acesso é restrito ao pessoal apropriado, com base na necessidade de conhecimento.
c. Todos os funcionários devem usar um crachá fornecido pela empresa e todos os visitantes ou Terceiros devem usar um crachá de convidado/visitante fornecido pela empresa.
d. O acesso é revogado imediatamente após a rescisão do pessoal do Fornecedor ou Terceiro , e todos os mecanismos de acesso físico , como chaves, cartões de acesso, etc., são devolvidos ou desativados.
e. O centro de dados ou sala de computadores está bloqueado e o acesso é limitado apenas àqueles que precisam de acesso para desempenhar suas funções de trabalho.
f. Onde permitido por lei, use câmeras de vídeo para monitorar o acesso físico individual a áreas sensíveis e revise esses dados regularmente. As imagens de vídeo devem ser armazenadas por um período mínimo de três (3) meses.
g. equipamento usado para armazenar, processar ou transmitir Informações Pessoais e Informações Confidenciais deve ser fisicamente protegido, incluindo pontos de acesso sem fio, gateways, dispositivos portáteis, hardware de rede/comunicações e linhas de telecomunicações.

4.6 Implemente controles para minimizar o risco e proteger contra ameaças físicas.

4.7 Mantenha todos os ativos de hardware processando ou manipulando Informações Pessoais e Informações Confidenciais de acordo com os requisitos de manutenção recomendados pelo fabricante .

4.8 redes e tomadas de rede acessíveis ao público lógica e fisicamente da rede interna do Fornecedor e restrita apenas a usuários autenticados ou desabilitados por padrão.

4.9 Proteja qualquer dispositivo que capture dados de cartão de pagamento por meio de interação física direta contra adulteração e substituição, inspecionando periodicamente as superfícies do dispositivo para detectar adulteração ou substituição; fornecer treinamento para que o pessoal esteja ciente da tentativa de adulteração ou substituição de dispositivos.

4.10 Controle e separe os pontos de acesso, como áreas de entrega e carregamento e outros pontos de todos os centros de acesso, gerenciamento, armazenamento ou processamento de Informações Pessoais e Informações Confidenciais.

4.11 Garanta que os data centers do fornecedor tenham dispositivos de aquecimento, resfriamento, supressão de incêndio, detecção de água e detecção de calor/fumaça. Os data centers e salas de computadores dos fornecedores devem estar livres de materiais combustíveis (por exemplo , caixas, papel, etc.) ou armazenados em armários de metal.

5. Controle de acesso

O Fornecedor deverá , no mínimo :

5.1 Tome todas as medidas razoáveis para impedir que qualquer pessoa que não seja Partes Autorizadas acesse Informações Pessoais e Informações Confidenciais de qualquer maneira ou para qualquer finalidade não autorizada pela CWT e pelo Contrato.

5.2 Separe as informações da CWT dos dados de outros clientes do Fornecedor ou dos aplicativos e informações do próprio Fornecedor usando servidores fisicamente separados ou usando controles de acesso lógico onde a separação física de servidores não for implementada.

5.3 Identificar e exigir que os proprietários apropriados revisem e aprovem o acesso aos sistemas usados para acessar, processar, gerenciar ou armazenar Informações Pessoais e Informações Confidenciais pelo menos trimestralmente para remover o acesso não autorizado ; e manter e rastrear aprovações de acesso.

5.4 Remover acesso a sistemas que gerenciam Informações Pessoais e Informações Confidenciais dentro de 24 horas após a Parte Autorizada encerrar seu relacionamento com o Fornecedor; e manter procedimentos razoáveis para remover o acesso a tais sistemas dentro de três dias úteis quando não for mais necessário ou relevante para o desempenho de suas funções . Todos os outros IDs de usuário devem ser desabilitados ou removidos após 90 dias corridos de inatividade.

5.5 Restrinja o acesso do administrador do sistema (também conhecido como root, privilegiado ou superusuário) aos sistemas operacionais destinados ao uso por vários usuários apenas para indivíduos que exijam esse acesso de alto nível no desempenho de seus trabalhos. Use IDs de administrador do sistema de check-out com credenciais de login de usuário individual e logs de atividades para gerenciar o acesso de alta segurança e reduzir o acesso de alto nível a um número altamente limitado de usuários. Exigir que os administradores de aplicativo, banco de dados, rede e sistema restrinjam o acesso dos usuários apenas aos comandos, dados, sistemas e outros recursos necessários para que eles executem funções autorizadas. As funções administrativas do sistema e as listas de acesso devem ser revisadas pelo menos uma vez por ano.

5.6 Imponha a regra de privilégio mínimo (ou seja , limitando o acesso apenas aos comandos, informações, sistemas e outros recursos necessários para executar funções autorizadas de acordo com a função de trabalho).

5.7 Exigir autenticação forte para todos os acessos administrativos fora do console , qualquer acesso remoto e todos os acessos administrativos em ambientes de nuvem .

5.8 Proibir e empregar Medidas de Segurança Técnica e Organizacional para garantir que as Informações Pessoais não possam copiar, mover ou armazenar Informações Pessoais em discos rígidos locais ou recortar e colar ou imprimir Informações Pessoais.

5.9 Ative o uso de recursos de acesso remoto somente quando necessário, monitore enquanto estiver em uso e desative imediatamente após o uso.

5.10 Exigir autenticação forte para se conectar a recursos internos do fornecedor que contenham informações pessoais e informações confidenciais.

6. <u>Identificação e autenticação</u>

O Fornecedor deverá , no mínimo :

6.1 Atribua IDs de usuário exclusivos a usuários individuais e atribua mecanismos de autenticação a cada conta individual.

6.2 Use um processo de gerenciamento de ciclo de vida de ID de usuário documentado, incluindo, mas não limitado a, procedimentos para criação de conta aprovada, remoção de conta oportuna e modificação de conta (por exemplo, alterações de privilégios, extensão de acesso, funções/funções) para todo o acesso a Informações Pessoais e Informações confidenciais e em todos os ambientes (por exemplo, produção, teste, desenvolvimento etc.). Tal processo deve incluir a revisão dos privilégios de acesso e validade da conta a ser realizada pelo menos trimestralmente.

6.3 Restrinja todo o acesso a Informações Pessoais e Informações Confidenciais àqueles que usam um ID de usuário e senha válidos e exija que IDs de usuário exclusivos empreguem um dos seguintes: senha ou frase secreta, autenticação de dois fatores ou um valor biométrico.

6.4 Exigir complexidade de senha e atender aos seguintes requisitos de construção de senha: um mínimo de doze (12) caracteres de comprimento para senhas do sistema e quatro (4) caracteres para senhas de tablet e smartphone. As senhas do sistema devem conter três (3) dos seguintes: letras maiúsculas, minúsculas, números ou caracteres especiais. As senhas também não devem ser iguais ao ID do usuário ao qual estão associadas, conter uma palavra do dicionário, números sequenciais ou repetidos e não ser uma das últimas 24 senhas. Exija a expiração da senha em intervalos regulares que não excedam noventa (90) dias. Mascare todas as senhas quando exibidas.

6.5 Limite as tentativas de logon com falha a não mais que cinco (5) tentativas de logon com falha em 24 horas e bloqueie a conta do usuário ao atingir esse limite em um estado persistente. O acesso à conta de usuário pode ser reativado posteriormente por meio de um processo manual que exige a verificação da identidade do usuário.

6.6 Verifique a identidade do usuário e defina as senhas de uso único e redefina para um valor exclusivo para cada usuário. Solicitar sistematicamente a mudança após o primeiro uso.

6.7 Use um método seguro para a transmissão de credenciais de autenticação (por exemplo, senhas) e mecanismos de autenticação (por exemplo, tokens ou cartões inteligentes).

6.8 Restrinja as senhas de conta de serviço e proxy a um mínimo de 20 caracteres , incluindo maiúsculas, minúsculas e caracteres numéricos, bem como símbolos especiais. Altere a conta de serviço e as senhas de proxy pelo menos uma vez por ano e após a rescisão do contrato de trabalho de qualquer pessoa com conhecimento da senha.

6.9 Encerre as sessões interativas ou ative um protetor de tela seguro e com bloqueio que exija autenticação, após um período de inatividade não superior a quinze (15) minutos.

6.10 Use um método de autenticação baseado na confidencialidade das Informações Pessoais e das Informações Confidenciais. Sempre que as credenciais de autenticação forem armazenadas, o Fornecedor deve protegê-las usando Criptografia Forte.

6.11 Configure os sistemas para expirar automaticamente após um período máximo de inatividade da seguinte forma : servidor (15 minutos), estação de trabalho (15 minutos), dispositivo móvel (4 horas), protocolo de configuração dinâmica de host (7 dias), rede privada virtual (24 horas).

7. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

O Fornecedor deverá , no mínimo :

7.1 Exiba um banner de aviso nas telas ou páginas de login conforme especificado por escrito pela CWT para produtos ou serviços da marca CWT ou para produtos e software desenvolvidos para a CWT.

7.2 Devolva todos os dispositivos de acesso de propriedade ou fornecidos pela CWT assim que possível, mas em nenhum caso mais de quinze (15) dias após o mais rápido de:

a. vencimento ou rescisão do Contrato;
b. o pedido da CWT para a devolução de tais bens; ou
c. a data em que o Fornecedor não precisa mais de tais dispositivos.

7.3 Empregar uma metodologia de gerenciamento de aplicativos eficaz que incorpore Medidas de Segurança Técnicas e Organizacionais ao processo de desenvolvimento de software e garanta que as Medidas de Segurança Técnicas e Organizacionais, conforme representadas pelas melhores práticas do setor, sejam implementadas pelo Fornecedor em tempo hábil.

7.4 Siga os procedimentos de desenvolvimento padrão do setor , incluindo a separação de acesso e código entre ambientes de não produção e produção e a segregação de tarefas associada entre esses ambientes.

7.5 Garantir que os controles internos de segurança da informação para desenvolvimento de software sejam avaliados regularmente e reflitam as melhores práticas do setor e revisem e implementem esses controles em tempo hábil.

7.6 Gerencie a segurança do processo de desenvolvimento e garanta que as práticas de codificação seguras sejam implementadas e seguidas, incluindo controles criptográficos apropriados, proteções contra códigos maliciosos e um processo de revisão por pares.

7.7 Realize testes de penetração em aplicativos funcionalmente completos antes de serem lançados em produção e posteriormente, pelo menos uma vez por ano e após quaisquer modificações significativas no código-fonte ou na configuração que se alinhem com OWASP, CERT, SANS Top 25 e PCI-DSS. Corrija quaisquer vulnerabilidades exploráveis antes da implantação no ambiente de produção.

7.8 Use dados anônimos ou ofuscados em ambientes de não produção. Nunca use dados de produção de texto simples em qualquer ambiente de não produção e nunca use Informações Pessoais em ambientes de não produção por qualquer motivo. Certifique-se de que todos os dados e contas de teste sejam removidos antes da liberação da produção.

7.9 Revise o código-fonte aberto ou gratuito aprovado pela CWT, software, aplicativos ou serviços quanto a falhas, bugs, problemas de segurança ou não conformidade com os termos de licenciamento de código aberto ou gratuito. O Fornecedor deverá notificar a CWT com antecedência sobre o uso de qualquer código-fonte aberto ou gratuito e, se aprovado para uso pela CWT, fornecer à CWT o nome, versão e URL do código-fonte aberto ou gratuito. O Fornecedor declara e garante que (a) qualquer código-fonte aberto ou livre que usar em seus produtos ou serviços será licenciado sob licenças de código-fonte aberto ou livre "permissivas" e não sob licenças Restritivas, Recíprocas, Hereditárias ou Copyleft; (b) O fornecedor tem o direito de alterar livremente, adaptar código-fonte aberto ou livre e combinar código-fonte aberto ou livre ou conter código-fonte aberto ou livre com código proprietário sem colocar restrições a tais emendas, adaptações ou combinações ou código proprietário que contenha código-fonte aberto ou livre e como estes podem ser licenciados posteriormente (coletivamente, " **trabalhos derivados** ") e (c) tais trabalhos derivados não estarão sujeitos a nenhuma licença de código aberto ou livre que exija o licenciamento do trabalho derivado ou sua disponibilização sem custo a terceiros sob os termos de licença de código aberto ou de código livre.

7.10 Não compartilhar nenhum código criado sob o Contrato, independentemente do estágio de desenvolvimento, em qualquer ambiente compartilhado ou não privado, como um repositório de código de acesso aberto, independentemente da proteção por senha.

8. Software e integridade dos dados

O Fornecedor deverá , no mínimo :

8.1 Em ambientes onde o software antivírus está disponível comercialmente, tenha um software antivírus atual instalado e em execução para verificar e remover ou colocar em quarentena vírus e outros malwares prontamente de qualquer sistema ou dispositivo.

8.2 Separe as informações e recursos de não produção das informações e recursos de produção.

8.3 Garanta que as equipes usem um processo de controle de alterações documentado para todas as alterações do sistema, incluindo procedimentos de retrocesso para todos os ambientes de produção e processos de alteração de emergência. Inclua testes, documentação e aprovações para todas as alterações do sistema e exija a aprovação da gerência para alterações significativas em tais processos.

8.4 Crie e mantenha uma zona PCI se o Fornecedor processar ou armazenar dados do titular do cartão.

8.5 Para aplicativos que utilizam um banco de dados que permite modificações em Informações Pessoais e Informações Confidenciais, habilite e mantenha recursos de log de auditoria de transações de banco de dados que retêm logs de auditoria de transações de banco de dados por no mínimo um (1) ano com três meses imediatamente disponíveis para análise.

8.6 Revise o software para encontrar e corrigir vulnerabilidades de segurança durante a implementação inicial e após quaisquer modificações e atualizações significativas.

8.7 Realize testes de garantia de qualidade para os componentes de segurança (por exemplo, testes de funções de identificação, autenticação e autorização), bem como qualquer outra atividade projetada para validar a arquitetura de segurança, durante a implementação inicial e após quaisquer modificações e atualizações significativas.

9. <u>Segurança do Sistema</u>

O Fornecedor deverá , no mínimo :

9.1 Crie e atualize regularmente as versões mais recentes de fluxo de dados e diagramas de sistema usados para acessar, processar, gerenciar ou armazenar Informações Pessoais e Informações Confidenciais.

9.2 ativamente os recursos do setor (por exemplo , , www.cert.org e listas de correspondência e sites de fornecedores de software pertinentes) para notificação oportuna de todos os alertas de segurança aplicáveis relativos aos sistemas do Fornecedor e outros recursos de informação.

9.3 Gerencie com eficiência as chaves criptográficas reduzindo o acesso às chaves pelo menor número de custodiantes necessário, armazenando chaves criptográficas secretas e privadas criptografando com uma chave pelo menos tão forte quanto a chave de criptografia de dados e armazenando separadamente da chave de criptografia de dados em um local seguro dispositivo criptográfico, no menor número de locais possíveis. Altere as chaves criptográficas

do padrão na instalação e pelo menos a cada dois anos e descarte com segurança as chaves antigas.

9.4 Analise os sistemas internos e externos e outros recursos de informação, incluindo, mas não se limitando a, redes, servidores, aplicativos e bancos de dados, com software de verificação de vulnerabilidades de segurança padrão do setor aplicável para descobrir vulnerabilidades de segurança, garantir que esses sistemas e outros recursos sejam adequadamente reforçadas e identificar quaisquer redes sem fio não autorizadas pelo menos trimestralmente e antes do lançamento para aplicativos e para alterações e atualizações significativas dentro de prazos resultantes de análises de risco com base em políticas e padrões de TI razoáveis e geralmente aceitos.

9.5 Certifique-se de que todos os sistemas e outros recursos do Fornecedor sejam e permaneçam protegidos, incluindo, mas não limitado a, remover ou desabilitar a rede não utilizada e outros serviços e produtos (por exemplo, finger, rlogin, ftp e simples Transmission Control Protocol/Internet Protocol (TCP/ IP) serviços e produtos) e instalar um firewall de sistema, wrappers de protocolo de controle de transmissão (TCP) ou tecnologia similar.

9.6 Implantar um ou mais Sistemas de Detecção de Intrusão (IDS), Sistemas de Prevenção de Intrusão (IPS) ou Sistemas de Detecção e Prevenção de Intrusão (IDP) em um modo de operação ativo que monitore todo o tráfego que entra e sai dos sistemas e outros recursos em conjunto com o Contrato em ambientes em que tal tecnologia esteja comercialmente disponível e na medida do possível.

9.7 Manter um processo de classificação de risco para descobertas de avaliação de vulnerabilidade alinhadas com as melhores práticas do setor para corrigir vulnerabilidades de segurança em qualquer sistema ou outro recurso, incluindo, mas não limitado a, aqueles descobertos por meio de publicações do setor, verificação de vulnerabilidades, verificação de vírus e revisão de logs de segurança , e aplique os patches de segurança apropriados prontamente com relação à probabilidade de que tal vulnerabilidade possa ser ou esteja em processo de exploração. As descobertas e patches de avaliação de vulnerabilidade crítica devem ser corrigidos imediatamente após a disponibilidade e, em nenhum caso, mais de 7 dias após o lançamento. As descobertas e patches de avaliação de alta vulnerabilidade devem ser corrigidos em até 30 dias após o lançamento. As descobertas e correções de avaliação de vulnerabilidade média devem ser corrigidas dentro de 90 dias corridos. As descobertas e patches de avaliação de baixa vulnerabilidade devem ser corrigidos em 120 dias corridos.

9.8 Realize testes de penetração de rede e segmentação interna e externamente pelo menos anualmente e após qualquer atualização ou modificação significativa de infraestrutura ou aplicativo.

9.9 Remover ou desabilitar software não autorizado descoberto nos sistemas do Fornecedor e empregar controles de malware padrão do setor, incluindo a instalação, atualização regular e uso rotineiro de produtos de software antimalware em todos os serviços, sistemas e dispositivos que possam ser usados para acessar Informações Pessoais e CWT Informação

confidencial. Use software antivírus confiável e com as melhores práticas do setor sempre que possível e garanta que essas definições de vírus permaneçam atualizadas.

9.10 Manter o software atualizado em todos os serviços, sistemas e dispositivos que podem ser usados para acessar Informações Pessoais e Informações Confidenciais da CWT, incluindo a manutenção apropriada do(s) sistema(s) operacional(is) e instalação bem-sucedida de patches de segurança razoavelmente atualizados.

9.11 Atribua responsabilidades de administração de segurança para configurar sistemas operacionais de host a indivíduos específicos.

9.12 Altere todos os nomes de conta padrão e/ou senhas padrão.

10. <u>Monitoramento</u>

O Fornecedor deverá , no mínimo :

10.1 Retenha os dados de log para Informações Pessoais e Informações Confidenciais por pelo menos 12 meses a partir da data em que os dados de log foram criados e disponibilize o log e esses dados à CWT dentro de um prazo razoável e mediante solicitação, a menos que especificado em outro lugar no Contrato. Os logs devem ser projetados para detectar e responder a incidentes e incluir, mas não se limitar a:

a. Todo o acesso de usuário individual a Informações Pessoais e Informações Confidenciais
b. Todas as ações realizadas por aqueles com privilégios administrativos ou de root
c. Todo o acesso do usuário às trilhas de auditoria
d. Tentativas de acesso lógico inválidas
e. Uso e alterações nos mecanismos de identificação e autenticação

10.2 primárias do sistema de Terceiros do Fornecedor para sistemas que contenham quaisquer Informações Pessoais e Informações Confidenciais e ter um programa formal de garantia de terceiros para garantir que os terceiros ou subcontratados do fornecedor tenham controles e certificações de segurança apropriados. os dados residem em um ambiente de nuvem.

10.3 Restrinja o acesso aos logs de segurança a indivíduos autorizados e proteja os logs de segurança contra modificações não autorizadas.

10.4 Implemente um mecanismo de detecção de alterações (por exemplo , monitoramento de integridade de arquivos) para alertar a equipe sobre modificações não autorizadas de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; configurar o software para realizar comparações críticas de arquivos semanalmente.

10.5 Revise, pelo menos uma vez por semana, todos os logs de auditoria de segurança e relacionados à segurança em sistemas que contenham Informações Pessoais e Informações Confidenciais quanto a anomalias e documente e resolva todos os problemas de segurança registrados em tempo hábil.

10.6 Revise diariamente todos os eventos de segurança, logs de componentes do sistema armazenando, processando ou transmitindo dados do titular do cartão, logs de componentes críticos do sistema e logs de servidores e componentes do sistema executando funções de segurança.

11. <u>Gateways de segurança</u>

O Fornecedor deverá , no mínimo :

11.1 Exigir Autenticação Forte para acesso administrativo e/ou de gerenciamento a Gateways de Segurança, incluindo, mas não limitado a, qualquer acesso para fins de revisão de arquivos de log.

11.2 Ter e usar controles, políticas, processos e procedimentos documentados para garantir que usuários não autorizados não tenham acesso administrativo e/ou de gerenciamento aos Gateways de Segurança e que os níveis de autorização do usuário para administrar e gerenciar Gateways de Segurança sejam apropriados.

11.3 Tenha controles fortes em torno da segurança de email, como configurar protocolos de autenticação DKIM e SPF que ajudam a validar uma mensagem de email de origem confiável e validada. Implementação de DMARC em servidores de recebimento de e-mail.

11.4 Pelo menos uma vez a cada seis (6) meses, certifique-se de que as configurações do Security Gateway sejam reforçadas selecionando uma amostra de Security Gateways e verificando se cada conjunto de regras padrão e conjunto de parâmetros de configuração garante o seguinte:

uma. O roteamento de origem do Internet Protocol (IP) está desabilitado,
b. O endereço de loopback é proibido de entrar na rede interna,
c. Filtros anti-spoofing são implementados,
d. Os pacotes de transmissão não são permitidos de entrar na rede,
e. Os redirecionamentos do protocolo ICMP (Internet Control Message Protocol) estão desabilitados,
f. Todos os conjuntos de regras terminam com uma instrução “DENY ALL” e
g. Cada regra é rastreável a uma solicitação de negócios específica.

11.5 Certifique-se de que as ferramentas de monitoramento sejam usadas para validar que todos os aspectos dos Security Gateways (por exemplo, hardware, firmware e software) estejam continuamente operacionais.

Certifique-se de que todos os Gateways de Segurança estejam configurados e implementados de forma que todos os Gateways de Segurança não operacionais neguem todo o acesso.

11.6 Os pacotes de entrada da rede externa não confiável devem terminar dentro da zona desmilitarizada (“ **DMZ** ”) e não devem ter permissão para fluir diretamente para a rede

interna confiável. Todos os pacotes de entrada que fluem para a rede interna confiável devem se originar apenas na DMZ. A DMZ deve ser separada da rede externa não confiável por meio de um Security Gateway e deve ser separada da rede interna confiável por meio de:

uma. outro Gateway de Segurança, ou
b. o mesmo Security Gateway usado para separar a DMZ da rede externa não confiável, caso em que o Security Gateway deve garantir que os pacotes recebidos da rede externa não confiável sejam imediatamente excluídos ou, se não forem excluídos, roteados apenas para a DMZ sem nenhum outro processamento de tais pacotes de entrada executados de forma diferente de possivelmente gravar os pacotes em um log.

O seguinte deve estar localizado apenas na rede interna confiável:

uma. Quaisquer Informações Pessoais e Informações Confidenciais da CWT armazenadas sem o uso de Criptografia Forte,
b. A cópia do registro oficial das informações
c. Servidores de banco de dados,
d. Todos os logs exportados e
e. Todos os ambientes usados para desenvolvimento, teste, sandbox, produção e quaisquer outros ambientes; e todas as versões de código-fonte.

11.7 As credenciais de autenticação não protegidas pelo uso de criptografia forte não devem estar localizadas na DMZ.

12. Segurança de Rede

O Fornecedor deverá , no mínimo :

12.1 Mediante solicitação da CWT, fornecer à CWT um diagrama de rede lógico documentando sistemas e conexões com outros recursos, incluindo roteadores, switches, firewalls, sistemas IDS, topologia de rede, pontos de conexão externos, gateways, redes sem fio e quaisquer outros dispositivos que deem suporte à CWT.

12.2 Mantenha um processo formal para aprovar, testar e documentar todas as conexões de rede e alterações nas configurações do firewall e do roteador. Configure firewalls para negar e registrar pacotes suspeitos e restringir para permitir apenas tráfego apropriado e autorizado, negando todos os outros tráfegos através do firewall. Revise as regras de firewall a cada seis meses.

12.3 Instale um firewall em cada conexão com a Internet e entre qualquer DMZ e a zona de rede interna. Qualquer sistema que armazene Informações Pessoais deve residir na zona de rede interna, separada da DMZ e de outras redes não confiáveis.

12.4 Monitore o firewall no perímetro e internamente para controlar e proteger o fluxo de tráfego de rede que entra ou sai da fronteira ou limite, conforme necessário.

12.5 Instale tecnologias de detecção de ameaças, como Network Detection and Response (NDR), Endpoint Detection and Response (EDR) e Extended Detection and Response (XDR), que oferecem uma solução abrangente para detectar e responder a vários ataques cibernéticos ou ataques de ransomware.

12.6 Manter um processo e controles documentados para detectar e lidar com tentativas não autorizadas de acessar Informações Pessoais e Informações Confidenciais da CWT.

12.7 Ao fornecer serviços e produtos baseados na Internet para a CWT, proteja as Informações Pessoais e as Informações Confidenciais com a implementação de uma DMZ de rede. Os servidores Web que prestam serviços à CWT devem residir na DMZ. Qualquer sistema ou recurso de informação que armazene Informações Pessoais e Informações Confidenciais (como servidores de aplicativos e bancos de dados) deve residir em uma rede interna confiável. O fornecedor deve usar DMZ para serviços e produtos de Internet .

12.8 Restrinja o tráfego de saída não autorizado de aplicativos que processam, armazenam ou transmitem Informações Pessoais e Informações Confidenciais para endereços IP na DMZ e na Internet.

12.9 Ao usar tecnologias de rede sem fio baseadas em radiofrequência (RF) para executar ou oferecer suporte a serviços e produtos para CWT, o Fornecedor deve garantir que todas as Informações Pessoais e Informações Confidenciais transmitidas sejam protegidas pelo uso de tecnologias de criptografia apropriadas suficientes para proteger a confidencialidade das Informações Pessoais e Informações Confidenciais; desde que, no entanto, em qualquer caso, tal criptografia não use comprimentos de chave não inferiores a 256 bits para criptografia simétrica e 2048 bits para criptografia assimétrica. Verifique, identifique e desative regularmente pontos de acesso sem fio não autorizados.

12.10 Segurança na Nuvem – Quando os dados da CWT residem na nuvem, ou o fornecedor usa um ambiente de nuvem de terceiros, incluindo, mas não limitado a, Infraestrutura como Serviço (IaaS), Software como Serviço (SaaS) e Plataforma como Serviço (PaaS), o fornecedor deve implementar ou avaliar o Cloud Security Posture Management para descobrir e corrigir automaticamente ameaças, configurações incorretas, uso indevido e violações de conformidade em nuvens públicas.

13. <u>Requisitos de conectividade</u>

13.1 Caso o Fornecedor tenha, ou venha a ser fornecido, conectividade com recursos de Informações Pessoais e Informações Confidenciais da CWT em conjunto com o Contrato, além do exposto, se o Fornecedor tiver ou for fornecido conectividade com o ambiente da CWT, o Fornecedor deverá, a um mínimo:

uma. Use apenas as instalações e metodologias de conexão mutuamente acordadas para interconectar o ambiente da CWT com os recursos do Fornecedor.

b. NÃO estabelecer interconexão com o ambiente da CWT sem o consentimento prévio por escrito da CWT.
c. Fornecer à CWT acesso a quaisquer instalações aplicáveis do Fornecedor durante o horário comercial normal para manutenção e suporte de qualquer equipamento (por exemplo, roteador) fornecido pela CWT sob o Contrato para conectividade com recursos de Informações Pessoais e Informações Confidenciais.
d. Use qualquer equipamento fornecido pela CWT sob o Contrato para conectividade ao ambiente da CWT apenas para o fornecimento desses serviços e produtos ou funções explicitamente autorizados no Contrato.
e. Se a metodologia de conectividade acordada exigir que o Fornecedor implemente um Security Gateway, mantenha registros de todas as sessões usando tal Security Gateway. Esses logs de sessão devem incluir informações suficientemente detalhadas para identificar o usuário final ou aplicativo, endereço IP de origem, endereço IP de destino, portas/protocolos de serviço usados e duração do acesso. Esses logs de sessão devem ser retidos por no mínimo seis (6) meses a partir da criação da sessão.
f. Permitir que a CWT colete informações relacionadas ao acesso, incluindo o acesso do Fornecedor, ao ambiente da CWT. Essas informações podem ser coletadas, retidas e analisadas pela CWT para identificar possíveis riscos de segurança sem aviso prévio. Essas informações podem incluir arquivos de rastreamento, estatísticas, endereços de rede e os dados ou telas reais acessados ou transferidos.
g. Suspender ou encerrar imediatamente qualquer interconexão com o ambiente da CWT se os Fornecedores acreditarem que houve uma violação ou acesso não autorizado ou mediante instruções da CWT se a CWT, a seu exclusivo critério, acreditar que houve uma violação de segurança ou acesso não autorizado ou uso indevido das instalações de dados da CWT ou quaisquer informações, sistemas ou outros recursos da CWT.

14. <u>Dispositivos móveis e portáteis</u>

O Fornecedor deverá , no mínimo :

14.1 Não armazenar Informações Pessoais e Informações Confidenciais em Dispositivos Móveis e Portáteis, a menos que seja totalmente criptografado usando Criptografia Forte.

14.2 Use criptografia forte para proteger informações pessoais e informações confidenciais transmitidas, usadas ou acessadas remotamente por dispositivos móveis e portáteis com reconhecimento de rede.

uma. Ao usar Dispositivos Móveis e Portáteis com reconhecimento de rede que não sejam laptops para acessar e/ou armazenar Informações Pessoais e Informações Confidenciais, tais dispositivos devem ser capazes de excluir todas as cópias armazenadas de Informações Pessoais e Informações Confidenciais após o recebimento pela rede de um documento devidamente autenticado comando. (Observação: esse recurso costuma ser chamado de recurso de “limpeza remota”.)

b. Ter políticas, procedimentos e padrões documentados em vigor para garantir que a Parte Autorizada que deve estar no controle físico de um dispositivo móvel e portátil

com reconhecimento de rede que não seja um laptop e que esteja armazenando Informações Pessoais e Informações Confidenciais inicie imediatamente a exclusão de todos Informações Pessoais e Informações Confidenciais quando o dispositivo for perdido ou roubado.

c. Ter políticas, procedimentos e padrões documentados em vigor para garantir que Dispositivos Móveis e Portáteis que não sejam laptops e não estejam cientes da rede excluam automaticamente todas as cópias armazenadas de Informações Pessoais e Informações Confidenciais após tentativas consecutivas de login com falha.

14.3 Tenha políticas, procedimentos e padrões documentados em vigor que garantam que quaisquer Dispositivos Móveis e Portáteis usados para acessar e/ou armazenar Informações Pessoais e Informações Confidenciais:

uma. Estão em posse física das Partes Autorizadas ;

b. Estão fisicamente protegidos quando não estiverem em posse física das Partes Autorizadas ; ou

c. Ter seu armazenamento de dados apagado de forma imediata e segura quando não estiver em posse física de uma Parte Autorizada, ou fisicamente protegido, ou após 10 tentativas de acesso sem sucesso.

14.4 Antes de permitir o acesso a Informações Pessoais e Informações Confidenciais armazenadas em ou através do uso de Dispositivos Móveis e Portáteis, o Fornecedor deve ter e usar um processo para garantir que:

uma. O usuário é uma Parte Autorizada autorizada para tal acesso; e

b. A identidade do usuário foi autenticada.

14.5 Implementar uma política que proíba o uso de quaisquer Dispositivos Móveis e Portáteis que não sejam administrados e/ou gerenciados pelo Fornecedor ou CWT para acessar e/ou armazenar Informações Pessoais e Informações Confidenciais.

14.6 Revise, pelo menos anualmente, o uso e os controles de todos os Dispositivos Móveis e Portáteis administrados ou gerenciados pelo Fornecedor para garantir que os Dispositivos Móveis e Portáteis possam atender às Medidas de Segurança Técnica e Organizacional aplicáveis.

15. <u>Segurança em Trânsito</u>

O Fornecedor deverá , no mínimo :

15.1 Use Criptografia Forte para a transferência de Informações Pessoais e Informações Confidenciais fora das redes controladas pela CWT ou controladas pelo Fornecedor ou ao transmitir Informações Pessoais e Informações Confidenciais por qualquer rede não confiável.

15.2 Para registros que contenham Informações Pessoais e Informações Confidenciais em formato de papel, microfichas ou mídia eletrônica a serem transferidos fisicamente, transporte-os por

correio seguro ou outro método de entrega que possa ser rastreado, embalado com segurança e de acordo com as especificações do fabricante. Quaisquer Informações Pessoais e Informações Confidenciais devem ser transportadas em contêineres trancados.

16. <u>Segurança em Repouso</u>

O Fornecedor deverá , no mínimo :

16.1 Use Criptografia Forte para proteger Informações Pessoais e Informações Confidenciais quando armazenadas.

16.2 Não armazenar Informações Pessoais ou Informações Confidenciais eletronicamente fora do ambiente de rede do Fornecedor (ou da própria rede de computadores segura da CWT), a menos que o dispositivo de armazenamento (por exemplo, fita de backup, laptop, cartão de memória, disco de computador, etc.) esteja protegido por Criptografia Forte.

16.3 Não armazenar Informações Pessoais ou Informações Confidenciais em mídia removível (por exemplo, unidades flash USB, pen drives, cartões de memória, fitas, CDs ou discos rígidos externos), exceto: para fins de backup, continuidade de negócios, recuperação de desastres e intercâmbio de dados, conforme permitido e exigido pelo contrato entre o Fornecedor e a CWT. Se uma mídia removível for usada para armazenar Informações Pessoais ou Informações Confidenciais de acordo com as exceções observadas nesta subseção, as informações devem ser protegidas usando Criptografia Forte. A execução automática deve ser desabilitada para mídia removível e dispositivos de armazenamento .

16.4 Armazene e proteja adequadamente os registros contendo Informações Pessoais ou Informações Confidenciais em formato de papel ou microfichas em áreas cujo acesso é restrito a pessoal autorizado.

16.5 A menos que instruído de outra forma pela CWT por escrito, ao coletar, gerar ou criar Informações Pessoais ou Informações Confidenciais em papel e mídia de backup para, por meio ou em nome da CWT ou sob a marca CWT, certifique-se de que tais informações sejam Informações Pessoais ou Informações Confidenciais e, sempre que possível, rotular tais informações da CWT como “Confidenciais”. O Fornecedor reconhece que as Informações Pessoais e as Informações Confidenciais são e permanecerão de propriedade da CWT, independentemente da rotulagem ou da ausência dela.

17. <u>Devolução, Retenção, Destruição e Descarte</u>

O Fornecedor deverá , no mínimo :

17.1 Sem custo adicional para a CWT , mediante solicitação da CWT ou mediante rescisão do Contrato , forneça cópias de quaisquer Informações Pessoais e Informações Confidenciais à CWT dentro de trinta (30) dias corridos após tal solicitação ou rescisão do Contrato . O Fornecedor deverá devolver ou, a critério da CWT, destruir todas as Informações Confidenciais e Informações Pessoais da CWT, incluindo cópias de backup eletrônicas ,

impressas e seguras conforme previsto no Contrato ou, se não estiver previsto no Contrato, no prazo de noventa (90) calendários dias após: (a) vencimento ou rescisão do Contrato, (b) solicitação da CWT para a devolução de Informações Pessoais e Informações Confidenciais, ou (c) a data em que o Fornecedor não precisa mais de Informações Pessoais e Informações Confidenciais para realizar serviços e produtos sob o Contrato.

17.2 Caso a CWT aprove a destruição como alternativa à devolução de Informações Pessoais e Informações Confidenciais, certifique por escrito , por um funcionário do Fornecedor, a destruição como tornando as Informações Pessoais e as Informações Confidenciais irrecuperáveis e irrecuperáveis. O Fornecedor deve destruir completamente todas as cópias de Informações Pessoais e Informações Confidenciais em todos os locais e em todos os sistemas onde as Informações Pessoais e as Informações Confidenciais são armazenadas, incluindo, mas não se limitando às Partes Autorizadas previamente aprovadas. Essas informações devem ser destruídas seguindo um procedimento padrão da indústria para destruição completa, como DOD 5220.22M ou NIST Special Publication 800-88 ou usando um produto de desmagnetização recomendado pelo fabricante para o sistema afetado. Antes de tal destruição, o Fornecedor deverá manter todas as Medidas de Segurança Técnica e Organizacional aplicáveis para proteger a segurança, privacidade e confidencialidade das Informações Pessoais e Informações Confidenciais.

17.3 Descarte as Informações Pessoais e as Informações Confidenciais da CWT de forma a garantir que as informações não possam ser reconstruídas em um formato utilizável. Papéis, slides, microfilmes, microfichas e fotografias devem ser descartados por trituração ou queima. Materiais contendo Informações Pessoais e Informações Confidenciais da CWT aguardando destruição devem ser armazenados em contêineres seguros e transportados por terceiros seguros.

18. Resposta e Notificação de Incidentes

O Fornecedor deverá , no mínimo :

18.1 Ter e usar um Processo de Gerenciamento de Incidentes e procedimentos relacionados e pessoal, como Processo de Gerenciamento de Incidentes e procedimentos com recursos especializados. Imediatamente, e em nenhum caso mais de vinte e quatro (24) horas, notifique a CWT em iRespond@mycwt.com sempre que houver qualquer suspeita ou confirmação de ataque, invasão, acesso não autorizado, perda ou outro incidente relacionado às informações da CWT , sistemas ou outros recursos.

18.2 Após notificar a CWT, fornecer à CWT atualizações de status regulares, incluindo, mas não se limitando a, ações tomadas para resolver tal incidente, em intervalos ou horários mutuamente acordados durante a duração do incidente e assim que razoavelmente possível após o encerramento do incidente , forneça à CWT um relatório por escrito descrevendo o incidente, as ações tomadas pelo Fornecedor durante sua resposta e os planos do Fornecedor para ações futuras para evitar a ocorrência de um incidente semelhante.

18.3 Não relatar ou divulgar publicamente qualquer violação de informações, sistemas ou outros recursos da CWT sem antes notificar a CWT e trabalhar diretamente com a CWT para notificar funcionários governamentais regionais, nacionais, estaduais ou locais aplicáveis ou serviços de monitoramento de crédito, indivíduos afetados por tal violação, e quaisquer meios de comunicação aplicáveis, conforme exigido por lei.

18.4 Ter um processo em vigor para identificar imediatamente as violações dos controles de segurança, incluindo aquelas estabelecidas nestes Requisitos de Segurança da Informação pelo pessoal do Fornecedor ou Terceiros. Os infratores identificados estarão sujeitos à ação disciplinar apropriada, de acordo com as leis aplicáveis. Não obstante o acima exposto, os infratores permanecerão sob a autoridade do Vendedor ou de seus Terceiros. A CWT não será considerada empregadora do Fornecedor ou de seus funcionários de Terceiros .

19. <u>Gestão de Continuidade de Negócios e Recuperação de Desastres</u>

O Fornecedor deverá , no mínimo :

19.1 Desenvolva , opere, gerencie e revise planos de continuidade de negócios para cada local e planos de recuperação de desastres para cada tecnologia principal , a fim de minimizar o impacto da CWT nos serviços ou produtos do Fornecedor. Esses planos devem incluir: recursos nomeados específicos para funções de Continuidade de Negócios e Recuperação de Desastres, objetivos de tempo de recuperação estabelecidos e objetivos de ponto de recuperação, pelo menos backup diário de dados e sistemas, armazenamento externo dos dados e backup de sistemas e registros, registro planos de proteção e contingência compatíveis com os requisitos do Contrato, armazenar tais registros e planos de forma segura fora do local e garantir que tais planos estejam disponíveis para o Fornecedor conforme necessário.

19.2 Mediante solicitação da CWT, forneça à CWT um plano de continuidade de negócios documentado que garanta que o Fornecedor possa cumprir suas obrigações contratuais sob o Contrato e este documento , incluindo os requisitos de qualquer declaração de trabalho ou acordo de nível de serviço aplicável. Tais planos devem exercer a recuperação enquanto protegem a integridade e confidencialidade das Informações Pessoais e Informações Confidenciais.

19.3 Ter procedimentos documentados para o backup seguro e recuperação de Informações Pessoais e Informações Confidenciais que devem incluir, no mínimo, procedimentos para o transporte, armazenamento e descarte das cópias de backup de Informações Pessoais e Informações Confidenciais e, mediante solicitação da CWT, fornecer tais procedimentos documentados para CWT.

19.4 Certifique-se de que os backups de todas as Informações Pessoais e Informações Confidenciais armazenadas ou software e configurações para sistemas usados pela CWT sejam criados pelo menos uma vez por semana.

19.5 Os planos de continuidade de negócios e recuperação de desastres devem ser atualizados pelo menos anualmente, ou com a frequência necessária por mudanças significativas no ambiente de negócios e/ou tecnologia.

19.6 Esses planos também devem ser exercidos de forma compreensível pelo menos anualmente, ou após qualquer mudança material na continuidade dos negócios ou nos planos de recuperação de desastres às custas e despesas exclusivas do Fornecedor. Esses exercícios devem garantir o funcionamento adequado das tecnologias impactadas e a conscientização interna de tais planos.

19.7 Revise imediatamente seu plano de continuidade de negócios para abordar fontes ou cenários de ameaças adicionais ou emergentes e forneça à CWT um resumo de alto nível dos planos e testes dentro de um prazo razoável mediante solicitação.

19.8 Certifique-se de que todos os locais do Fornecedor ou contratados pelo Fornecedor que hospedam ou processam Informações Pessoais e Informações Confidenciais da CWT sejam monitorados 24 horas por dia, sete (7) dias por semana contra intrusão, incêndio, água e outros riscos ambientais.

20. Conformidade e Acreditações

O Fornecedor deverá , no mínimo :

20.1 Reter registros completos e precisos relacionados ao desempenho de suas obrigações decorrentes destes Requisitos de Segurança da Informação e da conformidade do Fornecedor em um formato que permita avaliação ou auditoria por um período não inferior a três (3) anos ou mais, conforme necessário de acordo com uma ordem judicial ou processo civil ou regulatório. Não obstante o acima exposto, o Fornecedor só será obrigado a manter registros de segurança por um período mínimo de um (1) ano após qualquer execução contínua do Contrato.

20.2 Permita que a CWT, sem custo adicional para a CWT, mediante aviso prévio razoável, conduza avaliações periódicas de segurança ou auditorias da Medida de Segurança Técnica e Organizacional usada pelo Fornecedor, durante as quais a CWT fornecerá ao Fornecedor questionários escritos e solicitações de documentação. Para todas as solicitações, o Fornecedor deverá responder com uma resposta por escrito e provas, se aplicável, imediatamente ou mediante acordo mútuo. Mediante solicitação da CWT para uma auditoria pela CWT, o Fornecedor deve agendar uma auditoria de segurança para começar dentro de dez (10) dias úteis a partir de tal solicitação. A CWT pode exigir acesso a instalações, sistemas, processos ou procedimentos para avaliar o ambiente de controle de segurança do Fornecedor.

20.3 Mediante solicitação da CWT, certifique- se de que está em conformidade com este documento juntamente com as certificações de suporte para as versões mais recentes do PCI-DSS, ISO 27001/27002, SOC 2, Cyber Essentials ou avaliação semelhante para o Fornecedor e para qualquer subcontratado ou terceiro processamento, acesso, armazenamento ou gerenciamento em nome do Fornecedor. Se o Fornecedor não puder certificar a

conformidade, ele deverá fornecer um relatório por escrito detalhando onde está fora de conformidade e seu plano de remediação para se tornar compatível.

20.4 Caso a CWT, a seu exclusivo critério, considere que ocorreu uma violação de segurança que não foi relatada à CWT em conformidade com este Contrato e o Processo de Gerenciamento de Incidentes do Fornecedor, agende a auditoria ou avaliação para começar dentro de vinte e quatro (24) horas da notificação da CWT exigindo uma avaliação ou auditoria.

20.5 Dentro de trinta (30) dias corridos após o recebimento dos resultados da avaliação ou relatório de auditoria, forneça à CWT um relatório por escrito descrevendo as ações corretivas que o Fornecedor implementou ou propõe implementar com o cronograma e status atual de cada ação corretiva. O fornecedor deve atualizar este relatório para a CWT a cada trinta (30) dias corridos relatando o status de todas as ações corretivas até a data de implementação. O Fornecedor deve implementar todas as ações corretivas dentro de noventa (90) dias após o recebimento da avaliação ou relatório de auditoria pelo Fornecedor ou dentro de um período de tempo alternativo, desde que tal período de tempo alternativo tenha sido mutuamente acordado por escrito pelas partes em não mais de trinta (30) dias do recebimento do Fornecedor da avaliação ou relatório de auditoria.

20.6 Conformidade com PCI DSS - Na medida em que o Fornecedor lida com números de contas de pagamento ou qualquer outra informação de pagamento relacionada, o Fornecedor deve estar atualmente em conformidade com a versão mais atual do Payment Card Industry (PCI-DSS) para o escopo completo dos sistemas que lidam com essas informações e continuar tal cumprimento. Se qualquer subcontratado ou terceiro estiver processando, acessando, armazenando ou gerenciando dados de cartão de crédito em nome do Fornecedor, o fornecedor deverá obter um PCI AOC desse subcontratado ou terceiro e disponibilizá-lo à CWT mediante solicitação. Caso o Fornecedor não esteja ou não esteja mais em conformidade com o PCI-DSS para qualquer parte do escopo completo dos sistemas que lidam com dados aplicáveis ao PCI, o Fornecedor notificará imediatamente a CWT, procederá imediatamente, sem atraso indevido, para remediar tal não conformidade e fornecerá status regular de tal remediação à CWT mediante solicitação.

21. <u>Padrões, Melhores Práticas, Regulamentos e Leis</u>

Caso o Fornecedor processe, acesse, visualize, armazene ou gerencie Informações Pessoais ou Informações Confidenciais pertencentes ao pessoal da CWT, parceiros, Afiliados , clientes da CWT; ou funcionários, contratados, subcontratados ou fornecedores do cliente CWT ; O Fornecedor deve empregar Medidas de Segurança Técnica e Organizacional não menos rigorosas do que o exigido pelas diretrizes, regulamentos, diretivas e leis globais, regionais, nacionais, estaduais e locais aplicáveis.

22. <u>Modificação</u>

A CWT reserva-se o direito de atualizar ou modificar estes Requisitos de Segurança da Informação periodicamente, publicando a versão mais recente no site da CWT. A menos que o Fornecedor forneça uma notificação por escrito se opondo a tais atualizações ou

modificações dentro de trinta (30) dias após a publicação, o Fornecedor será considerado como tendo aceitado.

Versão 6.1
Data: abril de 2024