ANEXO

PROTEÇÃO DE DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO

1. Definições e Interpretação

1.1. Para os efeitos deste Anexo, os termos abaixo definidos terão os seguintes significados:

1.1.1. "Controlador de Dados" significa uma pessoa que, isoladamente ou em conjunto com outra(s), determina a(s) finalidade(s) e os meios de Tratamento de Dados Pessoais.

1.1.2. "Dados Pessoais" significa qualquer informação relacionada ao Titular.

1.1.3. "Dados Compartilhados" significa os Dados Pessoais que as Partes transferem entre si em decorrência do Contrato.

1.1.4. "Funcionários" significam não apenas os empregados e colaboradores, mas também subcontratados e fornecedores de serviços das Partes.

1.1.5. "Lei de Proteção de Dados" significa a Lei nº 13.709/2018 que protege os direitos e liberdades fundamentais das pessoas e, em particular, o seu direito à privacidade, no que diz respeito ao Tratamento de Dados Pessoais e suas alterações posteriores, bem como normas complementares.

1.1.6. "Tratar" (e variantes do termo, como "Tratamento") significa executar qualquer operação ou conjunto de operações sobre dados, seja ou não por meios automáticos, como coletar, gravar, organizar, armazenar, adaptar, alterar, recuperar, consultar, copiar, usar, divulgar, compartilhar, deletar, bloquear.

1.1.7. "Sistema" significa um sistema, rede, serviço ou solução de tecnologia de informação ou comunicação (incluindo todos os ativos que ou fazem parte ou são utilizados para o seu fornecimento).

1.1.8. "Titular" significa uma pessoa física identificada ou identificável, nos termos da Lei de Proteção de Dados.

1.1.9. "Violação de Dados" significa qualquer violação de segurança que resulte na destruição acidental ou ilegal, dano, perda, alteração, divulgação não autorizada ou acesso aos Dados Pessoais transmitidos, armazenados ou de outra maneira Tratados;

2. Proteção de Dados

2.1. As Partes reconhecem que, como parte da execução do Contrato, armazenam, coletam, processam ou de qualquer forma Tratam Dados Pessoais na categoria de Controlador para Controlador.

2.1.1. Tanto a Principia quanto a Contratada serão consideradas, no sentido dado pela legislação aplicável, como “Controladoras de Dados”.

2.2. Cada Parte Tratará os Dados Compartilhados em conexão com os propósitos do Contrato e de acordo com o princípio da necessidade (art. 6º, inciso III, da Lei de Proteção de Dados). Caso seja estabelecido outro propósito para o Tratamento de tais Dados Compartilhados, tal Tratamento deve ser feito com observação à Lei de Proteção de Dados aplicável.

2.3. Cada Parte garante à outra que os Dados Compartilhados:

(a) são adequados, relevantes e limitados ao necessário para a consecução do objeto do Contrato;
(b) são precisos e, sempre quando necessário, atualizados; e
(c) estão de acordo com a Lei de Proteção de Dados aplicável, de modo a permitir que a outra Parte os Trate.

2.4. Cada Parte deverá cumprir a Lei de Proteção de Dados aplicável ao Tratamento de Dados Pessoais que receber da outra Parte.

2.5. Cada Parte deverá cooperar com a outra Parte em relação a:

(a) ameaça ou comprometimento da confidencialidade, integridade ou disponibilidade dos Dados Compartilhados, incluindo consulta à outra Parte sobre as medidas que possam ser razoavelmente necessárias ou apropriadas para investigar, mitigar ou remediar qualquer Violação de Dados;
(b) comunicações, solicitações (de correção ou exclusão de Dados Pessoais, por exemplo), objeções ou quaisquer outras comunicações recebidas de Titulares, autoridades reguladoras ou qualquer outra pessoa, referentes a Dados Compartilhados; e
(c) questionamentos razoáveis da outra Parte relacionados a (i) medidas técnicas e organizacionais implementadas por essa Parte para assegurar a proteção dos Dados Compartilhados que recebe da outra Parte, e (ii) o inventário de Tratamento mantido por aquela Parte em relação aos Dados Pessoais que recebe dessa Parte.

2.6. A Contratada deverá notificar a Principia no prazo de 24 (vinte e quatro) horas, se tomar conhecimento de quaisquer dos eventos descritos no item 2.5 (a) acima ou se receber qualquer comunicação do tipo descrita no item 2.5 (b) acima.

2.6.1. A Contratada não deverá responder diretamente a qualquer comunicação do tipo descrita no item 2.6 (b) acima sem o prévio consentimento da Principia.

2.7. Cada Parte implementará e manterá as medidas técnicas e organizacionais necessárias para proteger os Dados Compartilhados de eventual destruição acidental ou ilegal, dano, perda, alteração, divulgação não autorizada ou acesso indevido, incluindo as medidas estabelecidas no item 3 abaixo e, se for o caso, as seguintes medidas:

(a) a anonimização e encriptação dos Dados Compartilhados;
(b) a capacidade de garantir a confiabilidade, integridade, disponibilidade e resiliência contínuas dos Sistemas e serviços de Tratamento;
(c) a capacidade de restaurar a disponibilidade e o acesso a Dados Compartilhados em tempo hábil no caso de um incidente físico ou técnico; e
(d) processo para testar, avaliar e monitorar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do Tratamento.

2.8. A Contratada assegura que, levando em conta a natureza dos Dados Compartilhados, as medidas técnicas e organizacionais implementadas sob o item 2.7 acima levam em consideração a melhor técnica, os custos de implementação e a natureza, contexto e propósitos do Tratamento, e os riscos que são apresentados pelo Tratamento, em particular de destruição acidental ou ilegal, dano, perda, alteração, divulgação não autorizada ou acesso indevido aos Dados Compartilhados.

2.9. Cada Parte divulgará os Dados Compartilhados recebidos da outra Parte somente para seus Funcionários na medida necessária para a consecução do objeto do Contrato e o adequado Tratamento de tais dados.

3. Requisitos Técnicos de Segurança da Informação ("Diretrizes de Segurança")

3.1. A Contratada deverá realizar suas obrigações nos termos do Contrato de Parceria e proteger os Dados Compartilhados, em conformidade com padrões de segurança da informação, incluindo, no mínimo, as medidas de segurança, técnicas e organizacionais descritas abaixo ("Medidas de Segurança"):

Tipo de Medida de Segurança	Detalhamento da Medida de Segurança
Conformidade com Políticas Internas	1. A Contratada deve manter políticas internas ("Políticas") que: (a) requerem que os Funcionários mantenham os Dados Compartilhados confidenciais e respeitem as medidas técnicas e organizacionais da Contratada estabelecidas para proteger tais dados; e (b) regem, minimamente: (i) o uso de computadores, dispositivos portáteis, e-mail e internet; e (ii) a maneira de proteger os Dados Compartilhados. 2. A Contratada deve: (a) treinar seus Funcionários e terceiros envolvidos (como terceiros contratados) em relação a estas políticas e aos aspectos de tecnologia da informação e de segurança relacionados; e (b) requerer que seus Funcionários e terceiros envolvidos respeitem essas políticas.

Controles de Acesso aos Sistemas utilizados pela Contratada	3. A Contratada deve Tratar os Dados Compartilhados somente (a) por meio de dispositivos efetivamente controlados pela Contratada; ou (b) por meio de aplicativos controlados pela Contratada; e, em ambos os casos, que apresentem trilha de auditoria que possa ser acessada em caso de investigação, devendo proteger adequadamente os Dados Compartilhados armazenados e em transferência.
Controle do sistema e segurança da infraestrutura subjacente	4. Se os Dados Compartilhados forem Tratados em um Sistema da Contratada, ou se a Contratada Tratar os Dados Compartilhados em um Sistema da Principia, a Contratada deve: (i) restringir o acesso a Sistemas que contenham Dados Compartilhados, inclusive restringindo: (a) o número de pessoas com acesso privilegiado; (b) o acesso dos usuários apenas às partes do Sistema necessárias para a realização dos seus respectivos trabalhos; e (c) o tempo de acesso dos usuários; (ii) revisar os privilégios de acesso de usuário utilizados pela Contratada ou em seu nome para acessar os Sistemas da Principia com a frequência exigida pelas políticas de segurança da Contratada; (iii) assegurar que os Funcionários que têm acesso ao Sistema ajam de forma responsável e com o devido cuidado; (iv) manter listas de controle de acesso aos sistemas de produção e permissões concedidas a usuários; (v) desativar ou revogar os direitos de acesso do usuário quando este não precisar mais de tais direitos de acesso; (vi) possuir um processo para garantir que os direitos de acesso ao Sistema da Contratada e a outros Sistemas (por exemplo, Sistema da Principia) aos quais a Contratada (pessoalmente ou por meio de terceiros) tem acesso permitido, sejam revogados a partir do momento do término do vínculo contratual; (vii) quando a Contratada precisar ter acesso a quaisquer Dados Compartilhados, ou de cópias, para fins de desenvolvimento ou testes de software, proteger os Dados Compartilhados com as mesmas restrições de acesso ao Sistema aplicadas aos Dados Compartilhados em ambientes de produção; (viii) manter as especificações de recursos técnicos e organizacionais (abrangendo a autenticação, autorização e auditoria do sistema computacional) necessárias para garantir a confidencialidade, integridade e disponibilidade dos dados Tratados; (ix) assegurar que os Dados Compartilhados estejam apenas em servidores de rede que preencham os seguintes requisitos: (a) sejam efetivamente controlados pela Contratada; (b) sejam seguros; e (c) tenham sistemas de acesso restrito; e (x) instalar e manter atualizadas proteções adequadas contra softwares maliciosos.

	5. A Contratada deve controlar o acesso aos seus Sistemas: (i) mantendo a segurança da Internet através de *firewalls* e outras medidas que controlam tentativas não autorizadas de acesso a aplicativos, sites ou serviços disponíveis na Internet, ou de acesso a dados transmitidos por meio da Internet; (ii) restringindo aos Funcionários autorizados o acesso a recursos do Sistema (inclusive às definições de configuração do Sistema) e a outras ferramentas relativas à segurança do Sistema; (iii) fornecendo e cancelando nomes/contas de usuários finais; (iv) habilitando autenticação e acesso único (*single-sign-on*) que requer nome/conta e senha válidos de um usuário individual; (v) implementando uma política de senha que exija que toda senha seja segura como, por exemplo, tenha 8 ou mais caracteres e contenha pelo menos três dos quatro grupos de caracteres a seguir: (a.1) letras minúsculas (de A a Z); (a.2) letras maiúsculas (de A a Z); (a.3) algarismos (0 a 9); e (d) caracteres especiais (tais como, "$", "#", "%", "!", etc); (vi) finalizando automaticamente as sessões individuais ociosas após um período de até 24 (vinte e quatro) horas; e (vii) gerenciando as permissões, os acessos e as senhas dos usuários.
Procedimentos Internos de Gerenciamento de Segurança	6. A Contratada deverá possuir e implementar procedimentos internos de gestão de segurança abrangendo os seguintes aspectos: (i) a(s) forma(s) de gerar e utilizar cópias de dados do Sistema, de programas e de ferramentas de programas para backup e restauração de Sistemas, bem como a forma de criar e manter os dados do Sistema necessários para testes e para a migração do Sistema; (ii) a proteção adequada de todas as cópias necessárias para backup, arquivamento do Sistema, entre outros; (iii) a(s) forma(s) de proteger os Sistemas contra acessos não autorizados; (iv) a(s) forma(s) que os Sistemas registram quem os acessou, indicando a data e o escopo do acesso; (v) a(s) forma(s) de realizar revisões e manutenção das mídias dos Sistemas utilizados para o Tratamento de Dados; (vi) a(s) forma(s) de descartar com segurança as informações que já não precisam ficar armazenadas; e (vii) os procedimentos para detectar e prevenir incidentes de segurança, incluindo: (a) gestão de ativos; (b) avaliação de impacto; e (c) pronta correção e escalonamento de todas as partes envolvidas.
Procedimento	7. A Contratada deve manter e fazer cumprir os procedimentos relativos à

de Dados Compartilhados	transmissão e proteção das informações e dos Dados Compartilhados, que incluem: (i) orientação para a retenção e descarte de registros; (ii) políticas que regulem o *download*, o uso e o armazenamento de *software* e de dados de terceiros; (iii) a garantia da segurança da informação aos Dados Compartilhados transmitidos eletronicamente (diretamente ou por meio de servidores intermediários) entre Sistemas (seja nas instalações da Contratada ou de terceiros); (iv) gerenciamento de mídias removíveis e portáteis, em conformidade com as boas práticas de segurança, incluindo, conforme apropriado: (a) o armazenamento em ambiente seguro, de acordo com as especificações dos fabricantes, (b) a garantia de transmissão, apagamento e descarte seguro; e (c) o armazenamento de mídias de backup em local remoto, a uma distância suficiente para evitar quaisquer danos em função de desastre nas instalações principais; (v) proteção dos Dados Compartilhados armazenados ou em transferência por meio da utilização de boas práticas de segurança, como controles de acesso e criptografia; (vi) restrição do acesso aos Dados Compartilhados aos Funcionários que necessitam do acesso para a consecução do Contrato, e assegurar que tais Funcionários Tratem os Dados Compartilhados apenas na medida do necessário para tanto.
Transmissões	8. A Contratada não poderá transmitir, ou solicitar que qualquer usuário transmita, as senhas em texto claro e visível por meio dos Sistemas ou entre os Sistemas. 9. A Contratada não poderá transmitir, ou permitir a transmissão por qualquer Funcionário seu, para a Principia ou entre seus Funcionários, quaisquer dados não estruturados utilizando meios que não os Sistemas da Contratada. Como parte disso, para fins de hospedagem ou de transmissão de dados não estruturados como parte da consecução da finalidade do Contrato de Parceria, a Contratada não deverá utilizar e nem permitir a utilização de: (i) contas de e-mail não-empresariais; (ii) FTP inseguro; ou (iii) serviços comerciais de compartilhamento de arquivos disponíveis ao consumidor em geral. 10. A Contratada não deverá enviar qualquer tipo de mídia física (por exemplo: CD, DVD, pen drive) contendo Dados Compartilhados a qualquer destinatário (inclusive à Principia) por meio de qualquer serviço postal ou correio.

Revisões	11. A Contratada deverá adotar medidas de revisões adequadas para garantir: (i) a conformidade com estas Diretrizes de Segurança; e (ii) que as medidas tomadas em conformidade com estas Diretrizes de Segurança sejam eficazes no cumprimento das boas práticas de segurança.