TERMO DE RESPONSABILIDADE, CONFIDENCIALIDADE, SIGILO, SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

Pelo presente Termo de Confidencialidade ("Termo") e na melhor forma de direito, as partes abaixo qualificadas neste contrato.

CONSIDERANDO QUE:

A) O Terceiro, por meio da CONTRATADA, indicada no preâmbulo, foi contratado para prestar serviços para a CONTRATANTE;

B) Em virtude da natureza dos serviços prestados, o Terceiro acaba tendo acesso a Informações Confidenciais (conforme abaixo definido);

C) As Partes desejam ajustar as condições de revelação dessas Informações Confidenciais já disponibilizadas e aquelas que no futuro serão disponibilizadas em função da relação existente, bem como definir as regras relativas ao seu tratamento; e

D) As Partes têm absoluta necessidade de conservar tais Informações Confidenciais sob sigilo;

Resolvem as Partes celebrar o presente Termo, que se regerá pelas cláusulas e condições a seguir estabelecidas:

1. Do Objeto:

1.1. Este Termo de Responsabilidade, Confidencialidade, Sigilo, Segurança da Informação e Proteção de Dados Pessoais ("Termo") tem como objeto formalizar as responsabilidades, obrigações e deveres assumidos pelo Terceiro, no exercício das atividades profissionais desempenhadas junto à CONTRATANTE, de forma a prover a necessária e adequada proteção das Informações Confidenciais, além de manter o sigilo e garantir a proteção dos dados pessoais que já teve acesso e/ou que venha a ter acesso.

1.2. O Terceiro declara ter ciência e concordar com todas as cláusulas e condições deste Termo, bem como com as demais normas, políticas e procedimentos internos da CONTRATANTE que lhe sejam aplicáveis.

1.3. Este Termo será válido durante todo o período em que os Terceiros relacionadas à CONTRATADA Terceiro mantiver qualquer tipo de relação contratual com a CONTRATANTE.

2. Das Definições:

2.1. "**Informação Confidencial**" ou "**Informações Confidenciais**" - significa toda e qualquer informação revelada, fornecida e/ou comunicada, direta ou indiretamente, por escrito ou verbalmente, de forma eletrônica ou não, indicada ou não como confidencial, incluindo, sem limitação, dados (incluindo Dados Pessoais), estatísticas, planos de negócios, métodos operacionais, lista e/ou informações cadastrais de clientes, fornecedores e/ou parceiros comerciais, conceitos, ideias, materiais, políticas, textos, fotografias, desenhos, gráficos, estudos, documentos, especificações, padrões, procedimentos, técnicas, fórmulas, *know how*, códigos fonte de software, programas de computador, segredos de comércio, estratégias comerciais, planos de negócio, características de produtos (pré-existentes, novos ou em desenvolvimento), informações sobre softwares e/ou hardwares, informações sobre negociações em andamento, planos de marketing e comerciais, informações contábeis, financeiras e/ou de natureza publicitária, projeções financeiras, informações envolvendo direito de propriedade industrial ou direitos autorais, informações sobre projetos, técnicas e/ou métodos, demonstrações, contratos, apresentações, relatórios, listas, preços, pesquisas de mercado e/ou decisões gerenciais, ou qualquer outro documento fornecido e/ou disponibilizado pela CONTRATANTE, ou ainda por qualquer sociedade que integre seu grupo econômico, por seus fornecedores ou parceiros comerciais.

2.2. **"Ativo da Informação ou "Ativos da informação" s**ão todos os dados, informações e recursos que têm valor para uma organização e suportam suas operações. No preâmbulo deste termo incluem todos os tipos dados (financeiros, operacionais, de clientes, etc.), software, hardware, documentação.

3. Da Confidencialidade:

3.1. O Terceiro se compromete a manter em absoluto sigilo e confidencialidade todas as Informações Confidenciais, relacionadas à CONTRATADA, bem como de suas afiliadas, seus diretores, conselheiros, representantes, empregados, seus clientes, parceiros, fornecedores ou quaisquer outros terceiros com os quais a CONTRATANTE mantenha vínculos profissionais ou comerciais, somente com o objetivo de cumprimento dos serviços a serem executados pelo Terceiro.

3.2. O Terceiro não poderá, em hipótese alguma, divulgar, reproduzir, transmitir, compartilhar, produzir cópias ou *back-up*, por qualquer meio ou forma, reter, duplicar, modificar, adulterar, subtrair ou adicionar qualquer elemento, ou utilizar de qualquer outra forma as Informações Confidenciais, salvo se prévia e expressamente autorizado pela CONTRATANTE ou por determinação judicial ou legal, devendo, neste último caso, comunicar previamente a CONTRATANTE da necessidade de divulgação das Informações Confidenciais, somente devendo ser reveladas as Informações Confidenciais determinadas por lei ou requeridas pela autoridade judicial ou

administrativa competente. Qualquer contato com veículos de comunicação a respeito dos serviços executados e/ou das Informações Confidenciais, bem como sua divulgação, através de releases, notas, entrevistas, posts, vídeos, dentre outros, seja na imprensa, em redes sociais e/ou em qualquer outro meio de comunicação, somente poderão ser realizados com o consentimento, prévio e por escrito, do departamento de comunicação da CONTRATANTE.

3.2.1. O Terceiro deverá destruir todo e qualquer documento por ele(a) produzido que contenha Informações Confidenciais da CONTRATANTE, quando não mais for necessária a manutenção desses ou quando, independentemente de justificativa, a CONTRATANTE solicitar sua destruição, comprometendo-se a seguir os métodos adequados de sanitização e descarte seguro (conforme ISO/IEC 27040 e NIST SP 800-88) e, não reter quaisquer reproduções, sob pena de incorrer nas responsabilidades previstas neste Termo, sendo obrigado a apresentar evidências da destruição quando solicitado pela CONTRATANTE.

3.2.2. Não obstante a devolução ou destruição das Informações Confidenciais, de acordo com os termos estabelecidos no presente documento, o Terceiro permanecerá vinculado às obrigações de confidencialidade pelo prazo previsto abaixo.

3.3. A obrigação de sigilo e confidencialidade prevista neste item permanecerá em vigor mesmo após a rescisão do contrato de prestação de serviços celebrado entre a empresa a qual o Terceiro está vinculado e a CONTRATANTE, por um período mínimo de 05 (cinco) anos, respondendo o Terceiro e a empresa a qual está vinculado pelos prejuízos morais e materiais a que derem causa em virtude de seu descumprimento.

4. Da Segurança dos Ativos da Informação:

4.1. O Terceiro se compromete a cumprir integralmente todas e não se limitando, às obrigações abaixo:

4.1.1. Cumprir integralmente as normas, políticas, padrões e procedimentos internos da CONTRATANTE relacionados à segurança da informação, privacidade e confidencialidade, vigentes durante toda a execução contratual;

4.1.2. Adotar medidas técnicas e organizacionais adequadas e compatíveis com as melhores práticas internacionais, incluindo, mas não se limitando a, as normas ISO/IEC 27001, ISO/IEC 27002 e NIST SP 800-53, a fim de garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações e ativos tecnológicos envolvidos.

4.1.3. Não realizar quaisquer manutenções, instalações, execução de programas ou scripts e/ou alterações nas configurações e/ou na estrutura dos ativos de informática disponibilizados pela IGUÁ, sem a devida autorização, prévia e expressa da IGUÁ;

4.1.4. Verificar sempre a segurança física dos equipamentos e ambientes em que as

informações estão armazenadas ou processadas.

4.1.5. Utilizar somente softwares licenciados, autorizados e de fontes confiáveis e homologadas pela IGUÁ.

4.1.6. Assegurar que os dispositivos utilizados para armazenamento de informações — incluindo, mas não se limitando a mídias magnéticas, eletrônicas e ópticas —, bem como os ambientes tecnológicos e canais de comunicação utilizados (tais como servidores, banco de dados, sites, links, hiperlinks e banners), estarão livres de:

• Programas de computador maliciosos ("malwares"), incluindo, sem limitação, spyware, adware, trojans, rootkits, keyloggers, backdoors, bots, miners e Remote Access Trojans (RATs), ou quaisquer outros recursos que possam comprometer a segurança da informação;

• Recursos, falhas ou vulnerabilidades que possam ocasionar perda de integridade, confidencialidade ou disponibilidade de dados ou informações pertencentes à Iguá ou a terceiros com os quais esta mantenha relacionamento comercial.

4.1.7. Manter todos os ambientes tecnológicos, sistemas, aplicações, componentes, bibliotecas, ferramentas, infraestrutura e dispositivos sob sua responsabilidade devidamente atualizados, de modo a assegurar a proteção contra vulnerabilidades conhecidas e a conformidade com as melhores práticas de gestão de segurança da informação.

4.1.8. Adotar processos formais de gestão de versões e backlevel, contemplando identificação, avaliação, priorização e aplicação tempestiva de atualizações de segurança, patches, correções de software e firmware, bem como a substituição ou descontinuação de tecnologias obsoletas ou não suportadas pelos respectivos fabricantes.

4.1.9. Avaliar e implementar em prazo compatível com o risco as atualizações de segurança críticas, observando critérios de impacto operacional e continuidade de serviços.

4.1.10. Implementar e manter controles que assegurem a proteção das informações em trânsito e em repouso, incluindo, mas não se limitando a, criptografia, autenticação multifator, registro e monitoramento de logs de auditoria, e demais medidas que garantam rastreabilidade e prevenção a acessos não autorizados.

4.1.11. Todo software, aplicação, integração ou serviço de tecnologia fornecido pelo terceiro/empresa CONTRATADA deverá ser projetado, desenvolvido e mantido de acordo com boas práticas de desenvolvimento seguro, com correção tempestiva de vulnerabilidades e aplicação de atualizações de segurança.

4.1.12. Projetar, implementar e manter arquitetura tecnológica robusta, segura e escalável, capaz de garantir a disponibilidade, continuidade e desempenho adequado dos serviços prestados à IGUÁ, observando princípios de resiliência operacional, redundância e tolerância a falhas.

4.1.13. Dimensionar adequadamente a capacidade de seus ambientes tecnológicos, adotando políticas de monitoramento proativo, prevenção de sobrecarga e gestão de

capacidade, de forma a assegurar desempenho contínuo e confiável na prestação dos serviços.

4.1.14. Manter registros e evidências documentais que comprovem a observância das medidas de segurança adotadas, incluindo treinamentos realizados, controles de acesso aplicados, revisões periódicas, logs de auditoria e registros de atualizações de segurança, comprometendo-se a apresentá-los à CONTRATANTE sempre que solicitado.

4.1.15. Manter política interna de segurança da informação atualizada, contendo diretrizes, controles e procedimentos compatíveis com os requisitos técnicos, normativos e de proteção de dados definidos ou indicados pela CONTRATANTE, de modo a garantir a integridade, confidencialidade e disponibilidade das informações tratadas.

4.1.16. O Terceiro reconhece que é o único responsável por sua conduta e quaisquer danos causados aos **ativos da informação** disponibilizados pela IGUÁ, decorrentes de sua negligência, imprudência, culpa, mal uso ou conduta dolosa.

4.1.17. Reportar imediatamente qualquer incidente de segurança, ameaça ou violação suspeita ou confirmada, bem como a colaborar com a investigação, correção e mitigação dos efeitos desses incidentes.

5. Das Penalidades:

5.1. O descumprimento de quaisquer das obrigações previstas neste Termo poderá resultar em sanções contratuais, cíveis e criminais, nos termos da legislação aplicável, do contrato assinado entre as Partes e das normas internas da CONTRATANTE.

5.2. O Terceiro e a empresa a qual está vinculado serão responsabilizados pelos prejuízos causados à CONTRATANTE e/ou a terceiros em decorrência do descumprimento deste Termo.

6. Da Aceitação:

6.1. O Terceiro declara ter lido e compreendido integralmente este Termo, bem como ter tido a oportunidade de esclarecer todas as dúvidas eventualmente surgidas.

6.2. O Terceiro aceita integralmente as condições deste Termo e se compromete a cumpri-las fielmente.

6.3. Este Termo entra em vigor na data de sua assinatura ~~do Terceiro~~ e permanecerá em vigor durante todo o período em que o Terceiro mantiver qualquer tipo de relação contratual com a CONTRATANTE.

6.4. As obrigações de segurança da informação prevista neste item permanecerá em vigor mesmo após a rescisão do contrato de prestação de serviços celebrando entre a empresa a qual o Terceiro está vinculado e a CONTRATANTE.

6.5. Este Termo, celebrado de forma irretratável e irrevogável, constitui o entendimento integral entre as Partes, obrigando as Partes e seus sucessores, a qualquer título.

7. Do Monitoramento de Acessos:

7.1. A CONTRATANTE, a seu exclusivo critério, poderá realizar o monitoramento constante de todos os acessos aos seus sistemas e informações, sensíveis ou não, incluindo o registro de atividades, horários de acesso, endereços IP e demais informações relacionadas aos acessos realizados pelo Terceiro, bem como poderá, a qualquer tempo, realizar auditorias técnicas, scans de vulnerabilidade e testes de intrusão para verificar a aderência do Terceiro às obrigações previstas neste termo.
7.2. O Terceiro reconhece que o monitoramento de acessos tem como objetivo garantir a segurança da informação e a proteção dos ativos de informática, bem como identificar possíveis atividades suspeitas e/ou não autorizadas.
7.3. O Terceiro se compromete a manter vigilância e não realizar quaisquer atividades que possam comprometer a segurança da informação e/ou violar as políticas internas da CONTRATANTE, sob pena de responsabilização contratual, civil e/ou criminal.
7.4. A CONTRATANTE poderá utilizar as informações obtidas por meio do monitoramento de acessos para fins de investigação e correção de problemas relacionados à segurança da informação.
7.5. O Terceiro fica ciente de que o monitoramento de acessos é uma medida adotada para garantir a segurança da informação e que a sua privacidade será respeitada, salvo nos casos em que a CONTRATANTE julgar necessário utilizar as informações para fins de investigação e/ou tomada de medidas disciplinares.
7.6. A CONTRATANTE se reserva o direito de, a seu exclusivo critério, a qualquer momento, sem necessidade de comunicação prévia, fiscalizar o uso dos ativos de informática e tomar as medidas necessárias para preservar sua integridade e segurança.

8. Da Lei Geral de Proteção de Dados:

8.1. O(s) Terceiro(s), na condição de Operador(es), compromete(m)-se a cumprir as obrigações estabelecidas pela Lei Geral de Proteção de Dados – "LGPD" (Lei nº 13.709/2018) e eventuais regulamentos, incluindo o tratamento adequado e seguro dos dados pessoais da CONTRATANTE, dos seus fornecedores, parceiros comerciais e dos seus clientes, quando obtiver acesso.
8.2. O Terceiro fica ciente de que é responsável pela proteção dos dados pessoais que lhe forem confiados, bem como pelo cumprimento das obrigações previstas na LGPD, como a adoção de medidas de segurança adequadas e a observância dos princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização.

8.3. O Terceiro se compromete a notificar a CONTRATANTE, imediatamente sobre:

(i) qualquer incidente de segurança que possa comprometer a proteção dos dados pessoais tratados;

(ii) qualquer pedido recebido diretamente dos titulares de dados, sem responder a esse pedido, a menos que tenha sido de outra forma autorizado pela CONTRATANTE para fazê-lo; e

(iii) qualquer suspeita ou ameaça, por ele(a) detectada, que implique (a) riscos à confidencialidade, integridade e/ou disponibilidade dos dados pessoais; (b) incidente de segurança da informação; ou (c) violação de dados pessoais compartilhados, acessados, comunicados, divulgados ou transmitidos pela CONTRATANTE ao Terceiro.

8.3.1. O Terceiro garante que em caso de incidente de segurança deverá adotar as medidas necessárias para minimizar os danos e prejuízos decorrentes do incidente.

8.4. O Terceiro se compromete a manter sigilo absoluto sobre os dados pessoais que lhe forem confiados, bem como a não os divulgar ou compartilhá-los, não fazer cópias para si ou utilizar os dados pessoais para enriquecimento de base, sem autorização prévia e expressa da CONTRATANTE, exceto nos casos previstos em lei.

8.5. O Terceiro reconhece que a violação das disposições previstas na LGPD pode ensejar a aplicação de sanções administrativas, civis e penais, conforme previsto na legislação brasileira, sem prejuízo da rescisão contratual e responsabilização pelos danos comprovadamente causados.

9. SOBRE O USO DE INTELIGÊNCIAS ARTIFICIAIS (IA)

9.1. Na hipótese de a CONTRATADA desenvolver, implementar, disponibilizar ou utilizar sistemas de inteligência artificial ("IA") no âmbito deste Contrato, obriga-se a:

I – assegurar que os sistemas de IA sejam desenvolvidos, implementados e operados em conformidade com a legislação vigente, em especial a Lei nº 13.709/2018 (LGPD), e demais normas ou regulamentos aplicáveis, nacionais ou internacionais;

II – adotar medidas técnicas e organizacionais adequadas para garantir funcionamento seguro, transparente, auditável e rastreável do sistema, incluindo documentação de critérios utilizados, testes de acurácia e mitigação de vieses ou riscos de discriminação;

III – manter política de governança de IA compatível com o nível de risco, incluindo monitoramento contínuo, revisão periódica e atualização em caso de alterações legislativas, regulatórias ou de melhores práticas de mercado;

IV – garantir que decisões automatizadas que produzam efeitos relevantes sobre titulares de dados pessoais estejam sujeitas à supervisão humana, permitindo revisão, contestação ou modificação das decisões, observando a LGPD e consentimento expresso da CONTRATANTE;

V – abster-se de utilizar quaisquer dados da CONTRATANTE, incluindo dados pessoais, mesmo que anonimizados, para treinamento de modelos de IA, salvo mediante autorização formal prévia;

VI – implementar controles adequados para prevenir, detectar e responder a incidentes de

segurança ou privacidade decorrentes do uso de sistemas de IA, incluindo acessos não autorizados, manipulação de dados, falhas de integridade, vieses discriminatórios, exposição de informações sigilosas ou uso indevido dos recursos de IA;

VII – implementar ações corretivas e preventivas em prazo acordado entre as Partes e cumprir todas as obrigações legais e regulatórias aplicáveis, incluindo comunicação a autoridades competentes, quando exigido.