CLÁUSULAS E CONDIÇÕES GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Por este instrumento, a **CIELO S.A. – INSTITUIÇÃO DE PAGAMENTO**, com sede na Alameda Xingu, nº 512, Andares 21º ao 31º, Alphaville, Centro Industrial e Empresarial, CEP: 06455-030, na cidade de Barueri, Estado de São Paulo, inscrita no CNPJ/ME sob nº 01.027.058/0001-91, neste ato representada na forma de seu Estatuto Social, doravante designada de "CIELO" e a CONTRATADA neste ato representada na forma de seu contrato social, doravante designada "CONTRATADA".

Considerando que:

I – A CONTRATADA participou ou participará de um processo de seleção de fornecedores, de acordo com critérios internos definidos pela CIELO, podendo ou não ser escolhida por esta última para a venda de bens e/ou prestação de serviços para a CIELO;

II - O presente instrumento somente produzirá seus efeitos jurídicos na hipótese de a CONTRATADA ser escolhida pela CIELO. Caso a CONTRATADA não seja escolhida pela CIELO para vender os bens e/ou prestar os Serviços objeto do processo de concorrência, este instrumento não produzirá qualquer efeito ou gerará qualquer direito à CONTRATADA.

III – Este instrumento integra para todos fins e efeitos de direito eventual contrato que venha a ser firmado entre CIELO e CONTRATADA.

A CONTRATADA formaliza por meio do presente instrumento sua aderência e concordância com os termos e condições relacionados a seguir:

1 A CONTRATADA, cuja prestação de serviços envolver acesso a dados e/ou transações de cartões de pagamento, deverá estar em conformidade com o padrão PCI-DSS (última versão disponível). A certificação PCI DSS deverá ser renovada anualmente**,** e compartilhada com a CIELO quando está solicitar o relatório de conformidade. O escopo da certificação deve contemplar os processos, transmissão e/ou armazenamento de informações objeto do contrato e as entidades envolvidas no processamento, armazenamento e transmissão de dados de cartões.

1.1 Informações de cartão de crédito e débito (ex.: Visa, Mastercard, American Express, etc) devem ser tratadas como confidenciais e protegidas contra uso indevido, conforme regras determinadas pelo padrão de segurança para cartões de pagamento (*PCI DSS - Payment Card Industry Data Security Standard);*

1.2 Dados confidenciais de autenticação do cartão de pagamento não devem ser armazenados após a autorização (mesmo se estiverem criptografados). Estes incluem:

- Conteúdo completo de qualquer trilha magnética do cartão de pagamento;
- Código ou valor de verificação do cartão (o número de três ou quatro dígitos

impresso na frente ou atrás do cartão de pagamento) usado para verificar as transações com cartão não presente, nominados CAV2/CVC2/CVV2/CID, dependendo da bandeira;

- PIN *(Personal Identification Number)* ou o PIN block criptografado;
- O número do cartão (PAN) deve ser mascarado quando exibido (os primeiros seis e quatro últimos dígitos são o número máximo de dígitos a serem exibidos);
- Nunca enviar PANs sem tecnologia de proteção de envio de mensagem ao usuário final, para evitar que essas sejam interceptadas e identificadas por fraudadores;
- O número do cartão (PAN) deve ser criptografado em caso de armazenamento em bases de dados;

1.3 Protocolos robustos de criptografia e de segurança (por exemplo, SSL/TLS, IPSEC, SSH etc.) devem ser utilizados para proteger os dados do portador de cartão de pagamento durante a transmissão por redes públicas, abertas (exemplos de redes abertas e públicas incluem, mas não se limitam, a: Internet, tecnologias sem fio, GSM, GPRS, 3G etc.).

2 A CONTRATA deverá cumprir a legislação e as regulamentações aplicáveis à prestação de serviço, bem como, mas não se limitando, à Lei 12.965/2014 (Marco Civil da Internet) e à Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), quanto às condições gerais de coleta, uso, armazenamento, descarte, tratamento e proteção de dados nos sites e plataformas.

3 A CONTRATADA deverá garantir a confidencialidade, integridade, autenticidade e disponibilidade de dados da CIELO que estão sob sua responsabilidade, sendo armazenados ou processados em ambiente local (on-premise) ou nuvem.

4 A CONTRATADA é responsável por manter o sigilo das informações confidenciais e internas da CIELO conforme estabelecido no Termos e Condições para Fornecimento de Bens e/ou Serviços firmado entre as Partes.

5 A CONTRATADA deverá possuir um modelo de gestão de Segurança da Informação e Privacidade e Proteção de Dados, com o papel de elaborar, divulgar e atualizar as políticas e diretrizes de segurança e proteção de dados pessoais, que deverão ser apresentadas à CIELO em caso de solicitação.

6 A CONTRATADA deverá designar um responsável pelo modelo de gestão de Segurança da Informação, que deverá atuar na gestão e no cumprimento das diretrizes e um encarregado em Privacidade e Proteção de Dados, responsável pela estrutura e governança do programa de privacidade e proteção de dados pessoais.

7 A CONTRATADA deverá possuir uma política de Segurança da Informação e/ou Cibernética e uma política de Privacidade e Proteção de Dados, revisada periodicamente e divulgada a todos os funcionários e terceiros.

8 A CONTRATADA deverá exercer o comportamento seguro, para que as informações da CIELO que estão sob sua responsabilidade não sejam alteradas, acessadas e/ou destruídas indevidamente.

9 A CONTRATADA deverá treinar periodicamente todos seus colaboradores em relação ao conteúdo de suas políticas de Segurança da Informação e Cibernética e Privacidade e Proteção de Dados. A CIELO poderá a qualquer tempo solicitar comprovação deste treinamento.

10 A CONTRATADA deverá disponibilizar aos empregados envolvidos na execução dos serviços, objeto de eventual contrato a ser firmado entre CIELO e CONTRATADA, treinamento obrigatório de segurança da informação, no mínimo uma vez ao ano. O treinamento deverá ser ministrado pela CONTRATADA, de acordo com o seu ramo de atividade. ACIELO poderá a qualquer tempo solicitar comprovação deste treinamento.

11 Na hipótese de a CONTRATADA admitir novos colaboradores para a execução dos serviços, deverá disponibilizar treinamento de Segurança da Informação nos primeiros 30 (trinta) dias de atividade.

12 A CONTRATADA, cuja prestação de serviço envolver o desenvolvimento de sistemas, deverá fornecer treinamentos obrigatórios, no mínimo uma vez ao ano, que contemple os principais aspectos de segurança da informação e também de boas práticas no desenvolvimento de sistemas, contendo minimamente os seguintes escopos: (i) OWASP Proactive Controls (https://owasp.org/www-project-proactive-controls/); (ii) OWASP Top 10 Web Application Security Risks (https://owasp.org/www-project-top-ten/); (iii) OWASP API Security Project (https://owasp.org/www-project-api-security/); (iv) OWASP Top 10: Web, API, Mobile, Proactive Controls, Segurança em Containers (Docker e Kubernetes), Segurança e Vulnerabilidades Web/HTTPe Segurança em banco de dados.

13 A CONTRATADA deverá apresentar o certificado individual de execução dos treinamentos acima listados para os profissionais alocados nos projetos da CIELO em até 03 (três) meses após assinatura de contrato.

14 A CONTRATADA compromete-se a responder aos reportes e envio de evidências solicitadas pela Gerência de Segurança da Informação da CIELO, contendo autoavaliação (self-assessment) dos requisitos de segurança determinados em contrato.

15 A CONTRATADA deverá permitir que colaboradores e/ou prestadores de serviço autorizados da CIELO possam proceder com a verificação *in-loco* de conformidade dos controles incluídos neste termo.

16 As inconformidades identificadas deverão ser corrigidas e um plano de ação deverá ser enviado à CIELO com um prazo para regularização. As vulnerabilidades classificadas como alta, conforme metodologia própria de análise de riscos da CIELO não poderão ser corrigidas num prazo superior a 90 (noventa) dias.

17 A CONTRATADA deverá documentar e manter atualizados os processos e procedimentos internos relacionados à prestação do serviço e aos requisitos de Segurança da Informação e Privacidade.

18 Todas as informações de propriedade da CIELO, bem como as de seus clientes e colaboradores, devem ter sua utilização restrita à prestação do serviço contratado e devem ser tratadas como confidenciais, sendo assegurado o acesso dos profissionais às informações apenas na medida necessária à execução de suas tarefas;

19 A CONTRATADA deve ter estabelecido um processo de provisionamento de acesso do usuário para conceder e/ou revogar os direitos de acesso de todos os tipos de sistemas e serviços, principalmente para os que manipulam informações da CIELO.

20 A CONTRATADA deverá estabelecer um processo restrito e controlado para concessão e uso de direitos e acesso privilegiados.

21 A CONTRATADA deverá possuir usuário e senha individuais e intransferíveis para identificação dentro dos sistemas. O sigilo da senha de acesso deve ser mantido, sendo de responsabilidade da CONTRATADA a sua guarda. Ações efetuadas dentro de sistemas são de responsabilidade da CONTRATADA por meio de usuário definido.

22 A CONTRATADA deverá ter estabelecido um processo de autenticação ao usuário para que ele possa acessar os sistemas que processam as informações da CIELO.

23 A CONTRATADA deverá disponibilizar mecanismos com dois fatores de autenticação distintos para o acesso remoto dos seus colaboradores, tais como senha e certificado digital e/ou token.

24 O acesso às áreas onde são processadas ou armazenadas informações sensíveis deve ser controlado e restrito a pessoas autorizadas. A CONTRATADA deverá manter, de forma segura e para fins de auditoria, um registro de todos os acessos físicos às áreas críticas/seguras.

25 Trilhas de auditoria (logs) devem ser criados automaticamente ao acessar os sistemas da CONTRATADA, contendo informações como: identificação do usuário, tipo de evento, data e hora do evento, resultado do evento, origem do evento. Os registros devem ser coletados em um local central ou mídia, protegidos contra acesso não autorizado através de segregação lógica e/ou física;

26 A CONTRATADA fará análises críticas dos registros das trilhas de auditoria (logs) para assegurar que eles continuam íntegros e que os controles não foram comprometidos. As trilhas de auditoria (logs) devem ser armazenadas pelo período mínimo de um ano, ou pelo período definido por lei.

27 Ao utilizar a rede da CIELO, a CONTRATADA deverá ter ciência de que seus acessos podem ser gravados e servirão como fonte de informações e evidências em caso de necessidade e as atividades realizadas nas estações de trabalho e servidores, bem como os acessos e utilização realizados no e-mail corporativo, internet e dados armazenados no SharePoint e sistemas da CIELO como um todo serão monitorados, registrados e poderão ser utilizados em caso de exigência legal e controle interno.

28 A CIELO reserva-se ao direito de monitorar e/ou bloquear o uso da Internet. A CONTRATADA não deve acessar sites contendo material de cunho ofensivo, racista, pornográfico, redes sociais ou que possa comprometer a segurança das informações de propriedade da CIELO.

29 Os recursos de tecnologia eventualmente disponibilizados pela CIELO são exclusivos para a execução das atividades relacionadas com o contrato. Não é permitida a utilização dos recursos de tecnologia com finalidade pessoal.

30 Indiferente ao formato de conexão com o ambiente da CIELO, a CONTRATADA deverá utilizar mecanismos de controle ao vazamento de dados por qualquer meio digital, incluindo:

- Ferramenta de Prevenção de Perda *(DLP – Data Loss Prevention);*
- Bloqueio de acesso à provedores de e-mails que não sejam formalmente utilizados pela CONTRATADA (ex.: gmail, outlook, yahoo e IG);
- Bloqueio de acesso à serviços de armazenamento em disco virtual na nuvem em contas fora da corporação (ex.: conta pessoal no Google Drive, OneDrive);
- Bloqueio de acesso à serviços de compartilhamento de arquivos de código fonte (ex.: GitHub) utilizando contas pessoais e/ou upload de arquivos em sites desta categoria.
-

- Bloqueio de comunicação com servidores FTP que não são de propriedade da CONTRATADA ou que não tenham necessidade formalizada e aprovada;
- Bloqueio de leitura e/ou movimentação de arquivos para mídias removíveis;
- Bloqueio de acesso à sites de mensagens instantâneas e a não permissão de baixar as versões desktop;
- Revogação de privilégios de administração das estações de trabalho para os usuários e bloqueio a edição de privilégios em grupos de acessos;

31 A CONTRATADA deverá utilizar protocolos de comunicação seguros (HTTPS, SFTP, TLS 1.2) para a transferência de arquivos entre a CONTRATADA e parceiros.

32 O acesso externo/remoto da CONTRATADA ao ambiente da CIELO deverá utilizar métodos seguros na comunicação entre cliente-servidor e proteção dos dados transmitidos (ex.: VPN, VDI).

33 Caso seja necessário o acesso remoto de colaboradores da CONTRATADA, a estrutura de acesso remoto deve ser disponibilizada e mantida pela própria CONTRATADA, sendo o acesso ao ambiente da CIELO roteado por meio do canal estabelecido entre a CONTRATADA e a CIELO, como túnel VPN ou link dedicado.

34 A CONTRATADA deverá manter a identificação e a segregação dos dados dos clientes da CIELO por meio de controles físicos ou lógicos, quando aplicável.

35 A CONTRATADA deverá garantir que software de antivírus/anti-malware estejam instalados e atualizados e que o sistema operacional, serviços e aplicações encontrem-se atualizados com as mais recentes correções de segurança (patches, hotfixes, etc.) e possuam opções de segurança ativadas, como firewall local e outras configurações. Além disso, deverá garantir que o sistema operacional, serviços e aplicações sejam produtos oficiais.

36 A CONTRATADA, cuja prestação de serviço envolver o desenvolvimento de sistemas, deverá trabalhar proativamente para identificar vulnerabilidades e/ou fragilidades de segurança nos códigos desenvolvidos pela CIELO, e quando identificada alguma vulnerabilidade nos códigos entregues por meio de processos de verificação internos da CIELO, a correção destes deverá ser realizada sem a cobrança de horas adicionais, quando identificada a responsabilidade da CONTRATADA.

37 A CONTRATADA deverá ter documentado, atualizado e regularmente testados procedimentos de cópia de segurança (backup) e de recuperação, de modo a garantir a integridade e disponibilidade das informações.

38 As mídias utilizadas para fins de arquivamento e/ou backup devem ser manuseadas e mantidas em ambiente seguro, de forma que somente colaboradores autorizados e prestadores de serviços contratados para este fim tenham acesso. Neste sentido, a CONTRATADA deverá restringir o acesso físico ao local, para evitar que pessoas não autorizadas roubem ou danifiquem os backups e proteger o local contra agentes nocivos naturais (poeira, calor, umidade, etc.).

39 Para a transferência das mídias deverá ser utilizado um meio seguro que mantenha a integridade das informações.

40 Toda mídia que não seja mais necessária ou que tenha atingido o fim de sua vida útil, deverá ser destruída ou inutilizada para que nenhum dado possa ser extraído.

41 A estrutura de gerenciamento de Segurança da Informação da CONTRATADA deverá manter e controlar a segurança do seu ambiente por meio de uma equipe multifuncional que coordena a identificação, o agrupamento e a resolução de incidentes de segurança, independentemente da estrutura do negócio.

42 A CONTRATA deverá ter estabelecido um processo de resposta a incidentes cibernéticos com monitoramento 24x7.

43 No caso de incidente, a CONTRATADA deverá notificar imediatamente a CIELO por meio do e-mail csirtcorp@cielo.com.br, sobre a ocorrência de incidentes, irregularidades ou eventos suspeitos que afetem ou possam afetar a segurança das informações e proteção de dados de propriedade da CIELO.

44 Caso a CONTRATADA realize a contratação de uma empresa para apoiar a prestação de serviço neste escopo de contrato, deverá notificar a CIELO, e assegurar que esta esteja aderente aos requisitos aqui estabelecidos.

45 Em caso de rescisão do contrato a CONTRATADA deverá: (i) assegurar a transferência de dados e/ou documentos de propriedade da CIELO para ela ou para empresa designada para prestação de serviço, garantindo a exclusão deles após a confirmação da integridade e da disponibilidade dos dados recebidos; e (ii) entregar e/ou destruir, a qualquer tempo, no formato indicado pela CIELO;

46 A CONTRATADA obriga-se a manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas;

47 Havendo atualização das políticas de Segurança da Informação e Cibernética, a CONTRATADA será informada para que as atualizações e/ou alterações sejam realizadas.

48 O presente instrumento permanecerá em pleno vigor e efeito enquanto perdurar o fornecimento de bens e/ou a prestação de serviços à CIELO.

Este instrumento é firmado na presença das testemunhas abaixo.

São Paulo, de de 2023.

_____

CIELO S.A. – INSTITUIÇÃO DE PAGAMENTO

_____

Testemunhas:

1._____ **2.**_____

Nome: Nome:

CPF/ME: CPF/ME: