POLÍTICA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

I – APRESENTAÇÃO:

1.1 Esta POLÍTICA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO tem por finalidade estabelecer as normas e os padrões corporativos que devem ser observados para o gerenciamento e a proteção dos dados e das informações no ambiente físico e tecnológico.

1.2 Conquanto a Privacidade enfoque a proteção da coleta, compartilhamento e utilização de dados e informações, e a Segurança busque a proteção desses dados e informações de ataques cibernéticos, entendemos que a reunião de ambas as políticas – Privacidade e Segurança – possam ser tratadas como um todo, por terem em essência o objetivo comum de proteger dados e informações afetas à execução das atividades empresariais da BRITI.

1.3 A BRITI é comprometida com a proteção de dados e informações dos seus colaboradores, clientes, prestadores de serviços e quaisquer terceiros que interajam com seus clientes, de modo que o cumprimento desta Política é de caráter obrigatório, em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e demais normas aplicáveis.

II – DISPOSIÇÕES INTRODUTÓRIAS:

2.1 As normas previstas nesta Política aplicam-se a todos os diretores, prepostos, colaboradores e prestadores de serviços que interagem com a BRITI, direta ou indiretamente na execução dos serviços por ela prestados.

2.2 Para fins desta Política considera-se:

2.2.1 Equipe de Tecnologia da Informação: equipe da BRITI, responsável pelo suporte e manutenção de seu servidor e de todos os sistemas operacionais utilizados pela BRITI;

2.2.2 Colaborador: o profissional contratado pela BRITI para prestar serviços com vínculo empregatício ou com vínculo de prestação de serviços, nas hipóteses de terceirização permitidas em lei.

2.3 O dever de sigilo sobre dados e informações confidenciais, que os colaboradores, prepostos e prestadores de serviços tenham tido durante o período em que mantiveram relações contratuais com a BRITI deverá ser mantido, indeterminadamente, isto, durante e após a rescisão contratual, sob pena de responder pelos danos causados pela divulgação de informações confidenciais.

2.4. Para fins do disposto na cláusula anterior toda informação que o colaborador tiver acesso em razão do desempenho de suas funções e atividades, seja ela oral ou escrita, transmitida em documentos físicos ou eletrônicos, de natureza técnica, comercial, fiscal, financeira, pessoal, ou de qualquer outra natureza, ainda que aqui não especificada, será considerada confidencial, e somente poderá ser revelada com o consentimento prévio e escrito do titular do dado ou da informação confidencial, ou em virtude de ordem judicial, ou ainda, em cumprimento de dever legal.

III – TRATAMENTO DE DADOS:

3.1 A BRITI não utiliza dados dos seus clientes (seja pessoa física ou jurídica) para fazer campanhas publicitárias, marketing digital, ou qualquer espécie de ação dessa natureza.
3.2 Considera-se tratamento de dados qualquer atividade que utilize um dado pessoal na execução de suas operações.
3.3 Na BRITI, o tratamento de dados é feito sempre em razão das obrigações contratuais e legais. Desse modo, embora não exista compartilhamento de dados para fins de marketing ou comercialização, a BRITI poderá compartilhar dados pessoais de clientes, de seus colaboradores e de terceiros vinculados aos seus clientes, para órgãos da Fazenda e Administração Pública, Direta ou Indireta, Juntas Comerciais ou autoridades delegadas, para fins de registro de sociedades no Registro do Comércio ou em Cartórios de Títulos e Documentos, cumprimento de obrigações trabalhistas e tributárias (acessórias e principais), e também para prestar informações exigidas em lei, independente do consentimento do titular dos dados, ex.: declarações do IBGE, Coaf, etc.
3.3.1 Colaboradores e a equipe de tecnologia da informação, poderão ter acesso controlado a dados (pessoais ou não) armazenados pela BRITI.
3.4 O compartilhamento de dados fora das hipóteses previstas na cláusula anterior (3.3 e 3.3.1) é proibido e só poderá ser feita nas situações a seguir transcritas, observando-se sempre os princípios da finalidade, adequação, necessidade, transparência e, outros pertinentes:

a) com o consentimento expresso ou a pedido do titular;
b) em situações que venham de encontro à satisfação dos interesses do cliente, como por exemplo, o nome e o contato telefônico para fornecedores ou terceiros que possa atendê-lo no bom exercício das suas atividades, obtido o consentimento prévio;
c) quando se tratar de cumprimento de dever legal;
d) em razão de ordem judicial.

3.5 Os dados pessoais poderão ser armazenados eletronicamente durante e após a contratualidade, pelo tempo em que o serviço prestado puder ser objeto de questionamento judicial.
3.6 Nossos colaboradores, clientes, fornecedores e terceiros que interagem com nossos clientes têm direito de requerer a correção sempre que observarem qualquer erro, inexatidão ou desatualização em relação aos seus dados pessoais.
3.7 A eliminação de dados pessoais de qualquer pessoa que interaja com a BRITI poderá ser requerida desde que o dado armazenado não esteja sob o tempo de guarda estabelecido para o cumprimento de obrigação legal ou regulatória, ou para a finalidade prevista na cláusula 3.5.

IV – SEGURANÇA DOS DADOS E DA INFORMAÇÃO:

4.1 A segurança dos dados tratados pela BRITI é extremamente relevante. Adotamos todas as providências cabíveis para minimizar os potenciais riscos e proteger os dados que armazenamos. Nossos procedimentos estão em constante revisão e monitoramento.
4.2 Não é admitido o uso dos equipamentos de informática e comunicação, sistemas e informações para a realização de atividades pessoais dos colaboradores, exceto para situações pessoais que

venham a ser imprescindíveis à garantia da saúde e integridade física do colaborador ou dos seus familiares, ou esteja relacionada a direitos fundamentais garantidos constitucionalmente.

4.3 O uso de senhas é pessoal e intransferível, cabendo a cada colaborador a sua guarda e responsabilidade, devendo providenciar imediatamente sua alteração em caso de qualquer suspeita de violação, hipótese em que também deverá se reportar, imediatamente, à Equipe de Tecnologia da Informação.

4.3.1 Como medida de resistência a ataques maliciosos, as senhas de acesso ao servidor, programas, sistemas, contas de e-mail, utilizados pela BRITI deverão: a) possuir códigos diferentes para cada sistema; b) possuir o máximo de caracteres permitido; c) ser heterogêneos e combinativas (números, símbolos, letras maiúsculas e minúsculas); d) nunca coincidir com outras senhas de uso pessoal (banco, cadastros em sites, etc); e) sofrer alteração periódica com observância dos requisitos anteriormente citados.

4.3.2 Sempre que houver a configuração de um novo sistema, alterar imediatamente a senha que porventura tenha sido configurada de fábrica ou enviada por e-mail.

4.4 A coleta de dados dos clientes para o cumprimento das obrigações contábeis, fiscais e empregatícias, deverá ser feita, preferencialmente, por meio eletrônico, através de e-mail ou de plataforma disponibilizada pela BRITI. O envio e recebimento de documentos por outro meio só poderá ser utilizado quando houver solicitação do cliente nesse sentido, caso em que este se responsabilizará pela segurança da informação.

4.5 Todo e qualquer incidente que afete a segurança da informação deverá ser comunicado imediatamente à equipe de tecnologia da informação.

4.6 Os documentos físicos enviados pelo cliente ou colaboradores deverão ser digitalizados em ambiente de segurança tecnológica (no servidor ou em nuvem), e não em máquina local. A BRITI armazenará os documentos físicos pelo tempo em que for necessário cumprimento das suas obrigações legais.

4.7 É vedada a reprodução fotográfica de documentos que contenham dados pessoais. É admitida a eventual reprodução de documentos que não contenham dados pessoais, com o objetivo único e exclusivo de melhor executar os lançamentos contábeis e administrativos, devendo, ao final, serem eliminados através de processo de fragmentação. É vedado o uso de cópias para rascunho ou para qualquer outra finalidade estranha à execução dos serviços prestados pela BRITI.

4.8 A saída do usuário de qualquer programa ou plataforma na rede mundial de computadores, cloud server, conta de e-mail, servidor ou qualquer sistema operacional que exija login e senha de usuário deverá ser efetuada no campo próprio.

V – COMPUTADORES, E-MAIL, INTERNET E RECURSOS TECNOLÓGICOS:

5.1 É responsabilidade de cada colaborador usuário de equipamentos eletrônicos e de informática, sistemas e programas operacionais submeter-se às orientações da equipe de tecnologia da informação, não executando nenhuma espécie de programa nem realizando qualquer tipo de procedimento que favoreça a entrada de códigos maliciosos e/ou indesejados, capazes de trazer vulnerabilidades ao ambiente de produção ou de colocar em risco a segurança dos dados armazenados

em sistemas operacionais utilizados pela BRITI.

5.2 Não poderão ser instalados softwares e hardwares na rede corporativa sem a permissão da equipe de tecnologia da informação. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

5.3 Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. Na menor suspeita de vírus ou desinstalação de antivírus, deverá o colaborador reportar a suspeita à equipe de tecnologia da informação e não executar nenhuma espécie de procedimento.

5.4 O correio eletrônico de qualquer endereço de domínio da BRITI só pode ser utilizado para fins estritamente relacionados às atividades do colaborador, sendo **terminantemente proibido**:

a) o envio de mensagens para múltiplos destinatários, que não tenham vínculo entre eles ou com o assunto tratado na mensagem;
b) a divulgação de informações não autorizadas ou imagens de tela, sistemas, documentos e afins, sem autorização expressa e formal concedida pelo titular do dado;
c) o acesso a links ou a operacionalização de arquivos enviados por e-mails que contenham ameaças eletrônicas como: spam, mail bombing, vírus de computador, ou que contenham mensagens nitidamente estranhas ao ambiente corporativo, ou ainda que contenham arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança da informação.

5.5 Qualquer informação acessada, transmitida, recebida ou produzida na rede mundial de computadores da BRITI está sujeita a divulgação, controle, monitoramento e auditoria. Toda e qualquer tentativa de alteração dos parâmetros de segurança estabelecidos pela equipe de tecnologia da informação, será considerada falta grave, passível de rescisão contratual por justa causa.

5.6 O uso da internet deve ser eminentemente ético e restringir-se ao exercício das funções laborais, podendo a BRITI bloquear qualquer arquivo, site, domínio ou aplicação armazenados na sua rede de internet, visando assegurar o cumprimento de sua Política de Segurança da Informação.

5.7 Os sites de notícias, atualização, entidades governamentais e quaisquer outros que possibilitem a atualização, capacitação e aprimoramento profissional são de livre acesso ao colaborador.

5.8 O uso da internet para a prática de atos ilícitos, inclusive para a prática de qualquer ato contrário à Lei 13.709/18 (LGPD), provocará a rescisão do contrato de trabalho por justa causa, além das medidas administrativas e penais cabíveis ao caso, hipótese em que a BRITI cooperará ativamente com as autoridades competentes, inclusive com a ANPD (Autoridade Nacional de Proteção de Dados).

5.9 O uso de pen-drive é proibido e só poderá ser utilizado mediante autorização da equipe de tecnologia da informação, desde que comprovados os princípios da Finalidade, Adequação, Necessidade e Segurança no armazenamento e tráfego das informações nele gravadas.

5.10 A BRITI, na qualidade de proprietária dos equipamentos e detentora dos direitos de licenças dos sistemas operacionais utilizados para coleta, armazenamento e arquivamento de informações, reserva-se o direito de inspecioná-los a qualquer tempo, independente de aviso prévio, visando monitorar e controlar a eficiência dos mecanismos de segurança.

5.11 Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais

dos equipamentos, em especial os referentes à segurança e à geração de logs, salvo a ocorrência de justificativa técnica, devidamente orientada pela equipe de tecnologia da informação.

VI – DISPOSIÇÕES FINAIS:

6.1 Esta Política de Privacidade e Segurança da Informação será revisada periodicamente. A BRITI reserva-se o direito de alterá-la, sempre que necessário, sem aviso prévio e independente de consentimento.
6.2 Em conformidade ao art. 48 da Lei nº 13.709, a BRITI comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano relevante ao Titular.
6.3 Qualquer dúvida ou esclarecimento sobre a aplicação desta Política poderá ser enviada ao Encarregado de Dados da BRITI:

RAFAEL PETRELLA
E-mail: rafael.petrella@zoomholding.com.br

PRIVACY AND INFORMATION SECURITY POLICY

I – INTRODUCTION:

1.1 This PRIVACY AND INFORMATION SECURITY POLICY is intended to establish the corporate rules and standards that must be observed for the management and protection of data and information within physical and technological environments.

1.2 While Privacy focuses on protecting the collection, sharing, and use of data and information, and Security seeks to protect such data and information against cyberattacks, we understand that both policies — Privacy and Security — may be addressed together, as they essentially share the common objective of protecting data and information related to the execution of BRITI's business activities.

1.3 BRITI is committed to protecting the data and information of its employees, clients, service providers, and any third parties interacting with its clients. Therefore, compliance with this Policy is mandatory, in accordance with Law No. 13,709/2018 (Brazilian General Data Protection Law – LGPD) and other applicable regulations.

II – INTRODUCTORY PROVISIONS:

2.1 The rules set forth in this Policy apply to all officers, representatives, employees, and service providers who interact with BRITI, directly or indirectly, in the performance of the services provided by BRITI.
2.2 For the purposes of this Policy, the following definitions shall apply:
2.2.1 Information Technology Team: BRITI's team responsible for the support and maintenance of its server and all operating systems used by BRITI;

2.2.2 Employee: the professional hired by BRITI to provide services either under an employment relationship or under a service provision relationship, in cases of outsourcing permitted by law.

2.3 The duty of confidentiality regarding confidential data and information to which employees, representatives, and service providers had access during the period in which they maintained contractual relationships with BRITI shall be maintained indefinitely, both during and after termination of the contractual relationship, under penalty of being held liable for damages caused by the disclosure of confidential information.

2.4 For the purposes of the preceding clause, any information to which the employee has access as a result of the performance of their duties and activities, whether oral or written, transmitted through physical or electronic documents, of a technical, commercial, tax, financial, personal, or any other nature, even if not specified herein, shall be deemed confidential and may only be disclosed with the prior written consent of the data subject or owner of the confidential information, or pursuant to a court order, or further in compliance with a legal obligation.

III – DATA PROCESSING:

3.1 BRITI does not use its clients' data, whether from individuals or legal entities, for advertising campaigns, digital marketing, or any other activity of a similar nature.

3.2 Data processing means any activity that uses personal data in the execution of its operations.

3.3 At BRITI, data processing is always carried out due to contractual and legal obligations. Therefore, although there is no sharing of data for marketing or commercialization purposes, BRITI may share personal data of clients, its employees, and third parties linked to its clients with tax authorities and Public Administration bodies, whether direct or indirect, Boards of Trade or delegated authorities, for the purposes of registering companies with the Commercial Registry or with Registry Offices of Deeds and Documents, complying with labor and tax obligations, whether ancillary or principal, and also providing information required by law, regardless of the data subject's consent, such as IBGE, COAF declarations, among others.

3.3.1 Employees and the Information Technology Team may have controlled access to data, whether personal or not, stored by BRITI.

3.4 The sharing of data outside the cases provided for in the preceding clause, namely clauses 3.3 and 3.3.1, is prohibited and may only occur in the situations set forth below, always observing the principles of purpose limitation, adequacy, necessity, transparency, and other applicable principles:

a) with the express consent or at the request of the data subject;
b) in situations aimed at satisfying the client's interests, such as providing the name and telephone contact to suppliers or third parties who may assist the client in the proper performance of their activities, provided that prior consent has been obtained;
c) when necessary to comply with a legal obligation;
d) pursuant to a court order.

3.5 Personal data may be stored electronically during and after the contractual relationship, for as long as the service provided may be subject to judicial challenge.

3.6 Our employees, clients, suppliers, and third parties interacting with our clients have the right to request correction whenever they identify any error, inaccuracy, or outdated information regarding their personal data.

3.7 The deletion of personal data of any person interacting with BRITI may be requested, provided that the stored data is not subject to the retention period established for compliance with a legal or regulatory obligation, or for the purpose provided for in clause 3.5.

IV – DATA AND INFORMATION SECURITY:

4.1 The security of the data processed by BRITI is of utmost importance. We adopt all appropriate measures to minimize potential risks and protect the data we store. Our procedures are subject to constant review and monitoring.

4.2 The use of information technology and communication equipment, systems, and information for employees' personal activities is not permitted, except in personal situations that are essential to ensuring the health and physical integrity of the employee or their family members, or when related to constitutionally guaranteed fundamental rights.

4.3 The use of passwords is personal and non-transferable, and each employee is responsible for keeping and safeguarding their passwords. Passwords must be changed immediately in the event of any suspicion of breach, in which case the employee must also immediately report the matter to the Information Technology Team.

4.3.1 As a measure to resist malicious attacks, passwords used to access BRITI's server, software, systems, and e-mail accounts must:

a) use different codes for each system;

b) contain the maximum number of characters allowed;

c) be heterogeneous and combined, using numbers, symbols, uppercase and lowercase letters;

d) never match other passwords used for personal purposes, such as banking or website registrations;

e) be changed periodically, in compliance with the requirements set forth above.

4.3.2 Whenever a new system is configured, any password that may have been factory-set or sent by e-mail must be changed immediately.

4.4 The collection of client data for compliance with accounting, tax, and employment obligations must preferably be carried out electronically, by e-mail or through a platform made available by BRITI. The sending and receipt of documents by any other means may only be used when requested by the client, in which case the client shall be responsible for information security.

4.5 Any and all incidents affecting information security must be immediately reported to the Information Technology Team.

4.6 Physical documents sent by clients or employees must be digitized in a technologically secure environment, whether on the server or in the cloud, and not on a local machine. BRITI shall store physical documents for as long as necessary to comply with its legal obligations.

4.7 The photographic reproduction of documents containing personal data is prohibited. The occasional reproduction of documents that do not contain personal data is permitted solely and

exclusively for the purpose of better performing accounting and administrative entries, and such documents must subsequently be destroyed through a shredding process. The use of copies as drafts or for any other purpose unrelated to the performance of the services provided by BRITI is prohibited.
4.8 Users must log out of any program or platform on the internet, cloud server, e-mail account, server, or any operating system that requires a user login and password, using the appropriate logout field.

V – COMPUTERS, E-MAIL, INTERNET, AND TECHNOLOGICAL RESOURCES:

5.1 Each employee who uses electronic and information technology equipment, systems, and operating software is responsible for complying with the guidance provided by the Information Technology Team, and must not run any type of program or perform any procedure that may facilitate the entry of malicious and/or unwanted code capable of creating vulnerabilities in the production environment or placing at risk the security of data stored in operating systems used by BRITI.
5.2 Software and hardware may not be installed on the corporate network without permission from the Information Technology Team. All updates and security patches for the operating system or applications may only be carried out after due validation in the respective testing environment and after being made available by the manufacturer or supplier.
5.3 Systems and computers must have antivirus software versions installed, activated, and permanently updated. Upon the slightest suspicion of a virus or antivirus uninstallation, the employee must report the suspicion to the Information Technology Team and must not perform any procedure.
5.4 The electronic mail of any BRITI domain address may only be used for purposes strictly related to the employee's activities, and the following is **strictly prohibited:**

a) sending messages to multiple recipients who have no connection with one another or with the subject matter of the message;
b) disclosing unauthorized information or screenshots of systems, documents, and similar materials, without the express and formal authorization granted by the data subject;
c) accessing links or opening files sent by e-mail that contain electronic threats such as spam, mail bombing, computer viruses, or that contain messages clearly unrelated to the corporate environment, or files with executable code, including .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, or any other extension that may pose a risk to information security.

5.5 Any information accessed, transmitted, received, or produced on BRITI's internet network is subject to disclosure, control, monitoring, and audit. Any attempt to change the security parameters established by the Information Technology Team shall be considered serious misconduct, subject to termination of the contractual relationship for cause.
5.6 Internet use must be primarily ethical and restricted to the performance of work-related duties. BRITI may block any file, website, domain, or application stored on its internet network in order to ensure compliance with its Information Security Policy.
5.7 News, update, government entity, and any other websites that enable professional updating, training, and development are freely accessible to employees.
5.8 The use of the internet to commit unlawful acts, including any act contrary to Law No. 13,709/2018 (LGPD), shall result in termination of the employment contract for cause, in addition to any applicable

administrative and criminal measures, in which case BRITI shall actively cooperate with the competent authorities, including the ANPD (Brazilian National Data Protection Authority).

5.9 The use of USB flash drives is prohibited and may only occur upon authorization from the Information Technology Team, provided that the principles of Purpose Limitation, Adequacy, Necessity, and Security in the storage and transfer of the information recorded therein are duly demonstrated.

5.10 BRITI, as the owner of the equipment and holder of the license rights to the operating systems used for the collection, storage, and archiving of information, reserves the right to inspect them at any time, regardless of prior notice, in order to monitor and control the effectiveness of security mechanisms.

5.11 Under no circumstances shall any change to the configuration of the equipment's operating systems be permitted, especially those related to security and log generation, except in the event of a technical justification duly guided by the Information Technology Team.

VI – FINAL PROVISIONS:

6.1 This Privacy and Information Security Policy shall be reviewed periodically. BRITI reserves the right to amend it whenever necessary, without prior notice and regardless of consent.

6.2 In accordance with Article 48 of Law No. 13,709/2018, BRITI shall notify the Data Subject and the Brazilian National Data Protection Authority (ANPD) of the occurrence of any security incident that may result in relevant risk or damage to the Data Subject.

6.3 Any questions or requests for clarification regarding the application of this Policy may be sent to BRITI's Data Protection Officer:

RAFAEL PETRELLA
E-mail: rafael.petrella@zoomholding.com.br

Revisão	Alteração	Data
00	Inicial – documento específico para BU	03/06/2026