Política de Segurança da Informação Jas Brasil	Information Security Policy Jas Brasil
1. Objetivo A Política de Segurança da Informação ("PSI") tem como principal objetivo garantir a proteção das informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da JAS Brasil, estabelecendo as diretrizes de segurança a serem adotadas pela JAS Brasil, seus colaboradores e parceiros.	**1. Purpose** The purpose of the Information Security Policy ("PSI") is to ensure the protection of information considered important for the continuity and maintenance of JAS Brasil's business objectives, establishing the security guidelines to be adopted by JAS Brasil, its employees and business partners.
2. Definições **Informação**: é um dado ou conjunto de dados que tem significado em algum contexto para o receptor. A Informação pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente (discos, banco de dados, planilhas etc.), transmitida pelo correio ou por meios eletrônicos, apresentada em filmes e fotos e, até mesmo, verbal (conversas e apresentações). **Segurança da Informação**: é a proteção da Informação contra uma ampla gama de ameaças, a fim de garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos e oportunidades do negócio. **Ameaça**: causa potencial de uma Violação ou Incidente de Segurança, que pode resultar em dano para um sistema e/ou para a JAS Brasil.	**2. Definitions** **Information**: is data that has meaning in a context for the receiver. Information can exist in different forms. It can be printed or written on paper, stored electronically (disks, database, spreadsheets, etc.), transmitted by mail or electronically, presented in films and photos, and even verbally (conversations and presentations). **Information Security:** is the protection of Information against security threats to ensure business continuity, minimize risk and maximize return on investments and business opportunities. **Threat**: potential cause of a security violation or incident, which could result in damage to a system and/or to JAS Brasil.

Violação: qualquer incidente que resulte em acesso não autorizado a dados, aplicativos, redes ou dispositivos de computador.	**Violation**: any incident that results in unauthorized access to computer data, applications, network, or devices.
Incidente de Segurança: evento adverso relacionado à Violação na segurança de Dados Pessoais, o qual pode ocasionar risco para os direitos e liberdades do Titular dos Dados Pessoais.	**Security Incident**: adverse event related to Violation in the security of Personal Data, which may pose a risk to the rights and freedoms of the Personal Data Subject.
Dados Pessoais: Toda a Informação relacionada a uma pessoa natural identificada ou identificável, tais como nome, CPF, título eleitoral e RG, bem como outros que permitem identificar uma determinada pessoa natural com o auxílio de informações adicionais, tais como sexo, endereço, profissão e idade.	**Personal Data:** All information related to an identified or identifiable natural person, such as name, number of ID card, voter registration card, as well as others that allow the identification of a specific natural person with the help of additional information, such as gender, address, profession, and age.
Titular: Pessoa natural a quem se referem os Dados Pessoais objetos de tratamento.	**Data Subject:** Natural person to whom the Personal Data refer.
Encarregado ou Data Privacy Officer (DPO): Pessoa indicada pela JAS Brasil para atuar como canal de comunicação, entre a JAS Brasil, os Titulares e a Autoridade Nacional de Proteção de Dados.	**Data Privacy Officer or DPO:** person appointed by the controller to function as a communication channel between the controller, the Data Subjects, and the National Data Protection Authority.
3. Princípios de Segurança da Informação[1]	**3. Information Security Principles**[2]
Confidencialidade: garantia de que a Informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados. São características da confidencialidade: • **Exclusividade**: dados disponíveis exclusivamente para os usuários autorizados a acessá-los.	**Confidentiality**: ensure that the Information is not available or disclosed to unauthorized individuals, entities, or processes. Confidentiality attributes are: • **Exclusivity**: access to data is only available to authorized users.

[1] Fontes: ISO/IEC 27000: 2014 e Foundations of Information Security, Van Haren.
[2] Sources: ISO/IEC 27000: 2014 and Foundations of Information Security, Van Haren.

• **Privacidade**: consiste em limitar o acesso aos Dados Pessoais	• **Privacy:** consists of limiting access to Personal Data
Integridade: garantia de que a Informação seja mantida em seu estado original. São características da integridade: • **Completeza**: os dados estão completos, inteiros. • **Correção**: garante que os dados são verdadeiros e exatos. • **Precisão**: as saídas de dados podem ser reproduzidas de forma consistente. • **Validade**: os dados atendem aos critérios de aceitação (da exatidão, precisão, tempo de vida etc.) • **Verificação**: é possível verificar que os dados foram cadastrados, armazenados, recuperados, transferidos e exibidos corretamente.	**Integrity**: ensure that the Information is kept in its original state. Integrity attributes are: • **Completeness**: the data is complete, entire. • **Correction**: ensure the data is correct and accurate. • **Precision**: data outputs can be reproduced consistently. • **Validity**: data produce results that meets acceptance criteria (accuracy, precision, lifetime etc.) • **Verification**: it is possible to verify that data were registered, stored, retrieved, transferred, and displayed correctly.
Disponibilidade: garantia de que os usuários autorizados tenham acesso à Informação quando necessário. São características da disponibilidade: • **Prontidão**: os sistemas de informação precisam estar disponíveis quando necessários. • **Continuidade**: na ocorrência de alguma instabilidade / falha no sistema de informação, os usuários precisam continuar a trabalhar. • **Robustez**: capacidade suficiente para permitir que todos os usuários autorizados possam se utilizar do sistema.	**Availability**: ensuring that authorized users have access to the Information when necessary. Availability attributes are: • **Readiness**: information systems need to be available when needed. • **Continuity**: in the event of any instability / failure in the information system, users need to continue working. • **Robustness**: enough capacity to allow all authorized users to use the system.
4. Papéis e Responsabilidades	**4. Roles and Responsibilities**
A JAS Brasil entende que os sistemas de informação somente estarão protegidos com o comprometimento de todos. Elencamos a seguir as responsabilidades	JAS Brasil understands that information systems will only be protected with the commitment of everyone. We list below the responsibilities of each JAS Brasil

de cada um dos agentes da JAS Brasil na melhoria e manutenção da segurança nos ambientes de informação da empresa. As responsabilidades listadas devem ser vistas como o mínimo a ser garantido pelos agentes envolvidos, sem limitar ou impedir que cada um deles possa atuar de maneira mais abrangente em prol da segurança das informações.	agent in improving and maintaining security in the company's information environments. The responsibilities listed must be seen as the minimum to be guaranteed by the agents involved, without limiting or preventing each one of them from acting in a more comprehensive way in favor of information security.
Usuários dos sistemas: • Cumprir a PSI; • Seguir as Boas Práticas da JAS Brasil (**Anexo I** desta Política); • Responder pela guarda e proteção dos recursos computacionais disponibilizados para seu trabalho; • Responder pelo uso exclusivo e intransferível de suas senhas de acesso; • Comunicar à área de Tecnologia da Informação (TI) qualquer fato ou Ameaça à segurança dos recursos, como mau funcionamento, presença de vírus, fragilidade etc.; • Comunicar ao seu superior imediato ou ao Encarregado ao tomar conhecimento ou suspeitar de um evento que pode ser considerado um Incidente de Segurança; • Responder pelo prejuízo ou dano que vier a provocar a JAS Brasil ou a terceiros, em decorrência da não obediência as diretrizes de segurança estipuladas; • Participar de todas as ações de treinamento e conscientização em Segurança da Informação estabelecidas pela JAS Brasil.	**System Users**: • Comply with PSI; • Follow JAS Brasil Best Practices (see Exhibit I); • Respond for the safekeeping and protection of the computer resources made available for the work; • Respond for the exclusive and non-transferable use of access passwords; • Communicate to the Information Technology (IT) area any fact or threat to the security of resources, such as malfunction, presence of viruses, fragility, etc.; • Communicate to your immediate superior or to the Data Privacy Officer when you become aware of or suspect an event that could be considered a Security Incident; • Respond for the loss or damage that you may cause to JAS Brasil or to third parties, as a result of non-compliance with the safety guidelines; • Participate in all information security training and awareness actions established by JAS Brasil.
Responsáveis Hierárquicos: • Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores	**Line Managers**: • Support and ensure compliance with the PSI, serving as a model of conduct for employees and

e prestadores de serviços sob sua gestão; • Autorizar o acesso e definir o perfil de cada membro de sua equipe junto ao gestor de liberações da área de TI; • Comunicar à área de Tecnologia da Informação (TI) qualquer fato ou Ameaça à segurança dos recursos, como mau funcionamento, presença de vírus, fragilidade etc.; • Comunicar ao Encarregado ao tomar conhecimento ou suspeitar de um evento que pode ser considerado um Incidente de Segurança; • Assegurar que a sua equipe tenha treinamento para uso correto dos recursos computacionais e sistemas de informação; • Obter aprovação técnica do gestor de liberações da área de TI antes de compra de hardware, software ou serviços de informática; • Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a essa PSI.	service providers under their management; • Authorize access and define the profile of each member of your team within the responsible IT manager; • Communicate to the Information Technology (IT) area any fact or threat to the security of resources, such as malfunction, presence of viruses, fragility etc.; • Communicate to the Data Privacy Officer when becoming aware of or suspecting an event that could be considered a Security Incident; • Ensure that your team is trained regarding the correct use of computer resources and information systems; • Obtain technical approval from the IT responsible manager before purchasing hardware, software, or IT services; • Adapt the standards, processes, procedures, and systems under your responsibility to meet this PSI.
Área de TI: • Estruturar e propor (i) os mecanismos de gestão de Segurança da Informação para o cumprimento desta PSI e das diretrizes e normas de gestão da Segurança da Informação, (ii) o programa de conscientização e treinamento em Segurança da Informação, e (iii) os padrões e requisitos mínimos da Segurança da Informação nos ambientes de tecnologia; • Identificar, classificar e reportar à Diretoria da JAS Brasil (i) os riscos e vulnerabilidades de Segurança da Informação e (ii) as violações	**IT Area**: • Structure and propose: (i) the Information Security management mechanisms to comply with this PSI and with the Information Security management guidelines and standards, (ii) the Information Security awareness and training program, and (iii) the standards and minimum requirements of Information Security in technology environments; • Identify, classify, and report to JAS Brasil's Board of Directors (i) Information Security risks and vulnerabilities and (ii) PSI

a esta PSI e/ou às diretrizes e normas de Segurança da Informação; • Elaborar, propor e implementar medidas e controles para mitigação dos riscos relacionados à Segurança da Informação; • Garantir a alocação de recursos e investimentos necessários para manter os ativos de tecnologia atualizados e seguros. • Revisar essa PSI anualmente, inserindo / modificando os requisitos e diretrizes de Segurança da Informação.	violations and/or Information Security guidelines and standards violations; • Develop, propose, and implement measures and controls to mitigate risks related to Information Security; • Ensure the allocation of resources and investments necessary to keep technology assets up-to-date and secure. • Review this PSI annually, inserting / modifying Information Security requirements and guidelines.

Controle de Revisões / *Revision Control*

Versão Original – Data de Aprovação / *Original Version – Approval Date*	31 de dezembro de 2021
Área Responsável/*Resp. Area*	DPO – Thiago Ambrico (Legal Director - Latam) thiago.ambrico@jas.com Teams: thiago.ambrico
Classificação/*Classification*	Interna / *Internal*
Observações/*Observation*	Documento elaborado pelo escritório Mendonça de Barros Advogados e aprovado pelo departamento jurídico da JAS do Brasil / *Document prepared by MBarros Advogados and approved by legal department at JAS Brazil.*