Política de Segurança da Informação e Segurança Cibernética

Data de Efetivação: 1 de janeiro de 2022

Índice

1. Resumo

O objetivo deste documento é estabelecer a Política de Segurança da Informação e Segurança Cibernética da Avenue Holdings e de todas as empresas que fazem parte de seu grupo, incluindo subsidiárias, empresas controladoras e afiliadas (todas em conjunto ou individualmente, referidas como “Avenue”), visando a Confidencialidade, Integridade e Disponibilidade das informações da Avenue e daquelas que estão sob sua custódia.

Information Security and Cybersecurity Policy

Effective Date: January 1st, 2022

Contents

1. Summary

The purpose of this document is to establish the Information Security and Cybersecurity Policy of Avenue Holdings and all companies within its group, including subsidiaries, parent companies and affiliates (jointly or individually referred to as “Avenue”), aiming at the Confidentiality, Integrity and Availability of Avenue’s information and that in its custody.

A política descreve as diretrizes e a conduta adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados (acidentais ou intencionais).

O detalhamento das diretrizes aqui dispostas serão objetos de normas e procedimentos específicos compondo o Sistema de Gestão de Segurança da Informação e Segurança Cibernética.

2. Escopo ou Raciocínio

Linhas de negócio	Todas
Funções	Todas
Locais	Todos
Entidades legais	Todos

Descrição do Escopo

Todos os administradores, sócios, funcionários e estagiários, consultores, prestadores de serviço ou qualquer terceiro que trabalhe para ou em nome das empresas do grupo Avenue (“Usuários”) estão sujeitos ao cumprimento dos termos desta Política e outros procedimentos relacionados à segurança da informação independentemente de cargo, departamento ou função.

3. Alterações

Versão	Data	Resumo
1.0	Dezembro/2019	Criação da Política
2.0	Outubro/2020	Atualização da Política
3.0	Abril/2021	Atualização da Política
4.0	Janeiro/2021	Atualização da Política

4. Disposições Iniciais

A Segurança da Informação e a Segurança Cibernética são caracterizadas pela preservação da Confidencialidade, Integridade e Disponibilidade das informações, ativos, ambiente e espaço cibernético.

O espaço cibernético engloba a internet, os sistemas de informação, os dispositivos móveis e as tecnologias digitais que são suporte aos negócios, infraestrutura e os serviços.

A metodologia de Segurança da Informação e Segurança Cibernética da Avenue se divide em três fases:

• **Prevenção** – treinamento dos Colaboradores, comunicação interna, análise de risco, difusão de uma cultura organizacional ética e estruturação de diretrizes para prevenção de incidentes relacionados à segurança da informação;

• **Detecção** – controles internos para o monitoramento constante da infraestrutura de hardwares e softwares da Avenue; e

• **Resposta** – plano de remediação ágil e eficaz com foco em mitigar danos e riscos reputacionais em caso de incidentes.

5. Diretrizes

5.1 Proteção da Informação

A informação pode estar presente de diversas formas, tais como: sistemas, drives locais e em nuvem, banco de dados, mídia impressa, dispositivos eletrônicos, equipamentos, comunicação oral, dentre outros.

The policy describes the guidelines and appropriate conduct for the handling, control, and protection of information against destruction, modification, improper disclosure, and unauthorized access (accidental or intentional).

The details of the guidelines set out here will be the subject of specific rules and procedures that make up the Information Security and Cybersecurity Management System.

2. Scope or Rationale

Lines of Business	All
Functions	All
Locations	All
Legal Entities	All

Scope Description

All directors, partners, employees and interns, consultants, contractors or any third party working for or on behalf of the Avenue group companies (“Users”) are subject to compliance with the terms of this Policy and other procedures related to information security regardless of job title, department or function.

3. Changes

Version	Date	Summary
1.0	December/2019	Policy Creation
2.0	October/2020	Policy Update
3.0	April/2021	Policy Update
4.0	January/2021	Policy Update

4. Initial Provisions

Information Security and Cybersecurity are characterized by preserving the Confidentiality, Integrity, and Availability of information, assets, environment, and cyberspace.

Cyberspace encompasses the Internet, information systems, mobile devices, and digital technologies that support business, infrastructure, and services.

Avenue’s methodology for Information Security and Cybersecurity is divided into three phases:

• **Prevention** - training of Employees, internal communication, risk analysis, dissemination of an ethical organizational culture, and structuring of guidelines for prevention of information security incidents;

• **Detection** - internal controls for the constant monitoring of the Avenue’s hardware and software infrastructure; and

• **Response** - an agile and effective remediation plan focused on mitigating damage and reputational risk in case of incidents.

5. Guidelines

5.1 Information Protection

Information may be present in many forms, such as: systems, local and cloud drives, databases, print media, electronic devices, equipment, oral communication, among others.

Independente da forma, toda informação gerada, adquirida, armazenada e/ou processada, pela Avenue ou através de parceiros de negócio e/ou prestadores de serviço é de sua propriedade e deve ser protegida de riscos e ameaças que possam comprometer sua Confidencialidade, Integridade e Disponibilidade.

5.2 Proteção dos Dados Pessoais

A proteção dos Dados Pessoais é semelhante à proteção de outros dados e inclui proteger a confidencialidade, integridade e a disponibilidade das informações. A Avenue tem os seguintes controles de segurança em vigor para proteger Dados Pessoais:

• Inventário de Dados;

• Proteção dos Dados Pessoais alinhada à matriz de classificação de dados pessoais;

• Controles de acesso ao usuário para usuários individuais e fornecedores terceirizados com acesso aprovado nos termos desta Política;

• Criptografia dos Dados Pessoais; e

• Anonimização dos Dados Pessoais.

Quanto maior o risco e capacidade prejudicial de dano aos clientes e aos titulares dos dados, maior deve ser seu nível de classificação desta informação.

5.3 Tratamento da Informação

As informações da Avenue e de seus clientes devem ser tratadas de forma ética e sigilosa, utilizadas com transparência e apenas para finalidade para a qual foi coletada.

A segregação de função deve ser observada em todo ciclo de vida da informação de forma a evitar o conflito de interesse.

O acesso às informações e recursos só pode ser realizado mediante autorização e respeitando a diretriz de menor privilégio, no qual os usuários têm acesso somente aos recursos imprescindíveis para o desempenho de suas atividades.

Os colaboradores que manipulam as informações devem ser identificados unicamente e são responsáveis pelas ações realizadas.

O colaborador é totalmente responsável pela correta utilização dos recursos disponibilizados e pelos atos executados com suas senhas, devendo manter sua confidencialidade.

Todos os envolvidos no tratamento da informação da Avenue e de seus Clientes devem se comprometer com a Confidencialidade assinando um Acordo de Confidencialidade.

5.4 Privacidade e Direitos de Propriedade

O tratamento da informação deve ser realizado respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade, privacidade e proteção de propriedade intelectual.

O tratamento de dados pessoais e dados pessoais sensíveis devem ser realizados em conformidade com a Lei Geral de Proteção de Dados (LGPD).

As diretrizes para o tratamento de dados pessoais na Avenue estão dispostas na Norma de Tratamento de Dados Pessoais.

5.5 Gestão da Segurança da Informação e Segurança Cibernética na Avenue

Regardless of the form, all information generated, acquired, stored and/or processed, by Avenue or through business partners and/or service providers is its property and must be protected from risks and threats that may compromise its Confidentiality, Integrity and Availability.

5.2 Protection of Personal Data

Protection of Personal Data is similar to the protection of other data and includes protecting the confidentiality, integrity, and availability of the information. Avenue has the following security controls in place to protect Personal Data:

• Data Inventory;

• Personal Data Protection aligned to the personal data classification matrix;

• User access controls for individual users and third-party suppliers with approved access under this Policy;

• Encryption of Personal Data; and

• Anonymization of Personal Data.

The higher the risk and damaging capacity to harm clients and data subjects, the higher the level of classification of this information should be.

5.3 Information Treatment

Information about Avenue and its clients must be treated ethically and confidentially, used transparently, and only for the purpose for which it was collected.

Segregation of functions must be observed throughout the information life cycle in order to avoid conflict of interest.

The access to information and resources can only be made upon authorization and respecting the guideline of least privilege, in which users have access only to those resources that are indispensable for the performance of their activities.

Employees who handle the information must be uniquely identified and are responsible for their actions.

The employee is entirely responsible for the correct use of the resources made available and for the acts carried out with their passwords and must maintain their confidentiality.

Everyone involved in handling information about Avenue and its Clients must commit to Confidentiality by signing a Confidentiality Agreement.

5.4 Privacy and Property Rights

Information handling must be carried out with respect for copyrights, software licensing rules, property rights, privacy, and intellectual property protection.

The processing of personal data and sensitive personal data must be carried out in compliance with the General Data Protection Act (LGPD).

The guidelines for handling personal data at Avenue are set out in the Personal Data Handling Policy.

5.5 Information Security Management and Cyber Security at Avenue

A segurança da informação e segurança cibernética devem ser monitoradas e controladas por equipe especialista para garantir a proteção do ambiente da Avenue contra as seguintes ameaças, mas não se limitando a:

- Acesso não autorizado;
- Infecção por código malicioso;
- Invasão;
- Violação de dados;
- Vazamento de dados.

Os riscos e vulnerabilidades devem ser identificados, avaliados quanto ao impacto para o negócio da Avenue, bem como enviados para tratamento de forma a proteger o ambiente.

O Comitê de Segurança da Informação e Segurança Cibernética é responsável pelo de acompanhamento, recomendação e aprovação das ações de segurança da informação e segurança cibernética.

A Avenue possui processos e procedimentos que asseguram a continuidade do negócio e que garantem que a Avenue possa responder rapidamente a ocorrência de um incidente de segurança da informação e segurança cibernética.

5.5.1 Classificação da Informação

As informações produzidas, processadas e armazenadas pela Avenue são classificadas e protegidas de acordo com seu nível de confidencialidade e grau de risco ao negócio.

As regras estão dispostas na Norma de Classificação, rotulação e tratamento da informação.

5.5.2 Gestão de Ativos

Os ativos de informação são identificados de forma individual, inventariados e protegidos de acesso indevido.

As regras estão dispostas na Norma de Gestão de Ativos.

5.5.3 Gestão de Acessos

Os acessos são concedidos de acordo com os princípios de menor privilégio e da segregação de função de forma a evitar fraudes e acesso indevido.

Os processos de concessão e exclusão são automatizados de forma a garantir os princípios da Gestão de Acessos.

Os acessos são revisados periodicamente pelos responsáveis pelas informações da Avenue.

As regras estão dispostas na Norma de Gestão de Identidade e Acessos.

5.5.4 Gestão da Continuidade dos Negócios

A Avenue possui processos e procedimentos que garantem a continuidade do seu negócio, utilizando o ambiente de computação em nuvem que permite uma rápida recuperação de seus serviços e produtos, bem como escalabilidade e alta disponibilidade.

Para gestão de continuidade do negócio a Avenue possui a Política de Continuidade do Negócio e o Plano de Continuidade do Negócio.

5.5.5 Monitoramento e segurança do ambiente

A Avenue monitora todo ambiente que suporta seus produtos e serviços de forma a garantir a proteção de seus dados e informações.

Information security and cybersecurity shall be monitored and controlled by expert staff to ensure the protection of Avenue's environment from the following threats, but not limited to:

- Unauthorized access;
- Infection by malicious code;
- Invasion;
- Data breach;
- Data Leakage.

Risks and vulnerabilities must be identified, assessed for impact to Avenue's business, as well as sent for treatment to protect the environment.

The Committee for Information Security and Cybersecurity is responsible for monitoring, recommending, and approving information security and cybersecurity actions.

Avenue has processes and procedures in place to ensure business continuity and to ensure that Avenue can respond quickly if an information security and cybersecurity incident occurs.

5.5.1 Information Classification

The information produced, processed, and stored by Avenue is classified and protected according to its level of confidentiality and degree of business risk.

The rules are laid out in the Classification, Labeling and Information Handling Policy.

5.5.2 Asset Management

Information assets are individually identified, inventoried, and protected from unauthorized access.

The rules are laid out in the Asset Management Policy.

5.5.3 Access Management

Access is granted according to the principles of least privilege and segregation of duties to avoid fraud and improper access.

The granting and exclusion processes are automated in order to guarantee the principles of Access Management.

The accesses are periodically reviewed by those responsible for Avenue's information.

The rules are laid out in the Identity and Access Management Policy.

5.5.4 Business Continuity Management

Avenue has processes and procedures that ensure the continuity of its business, using the cloud computing environment that allows a fast recovery of its services and products, as well as scalability and high availability.

For business continuity management, Avenue has a Business Continuity Policy and the Business Continuity Plan.

5.5.5 Monitoring and security of the environment

Avenue monitors any environment that supports its products and services to ensure that its data and information is protected.

As regras estão dispostas na Norma de Monitoramento e Segurança do ambiente.

5.5.6 Gestão de incidentes de segurança da informação

Os eventos de segurança da informação são comunicados e monitorados de forma a tomar ações corretivas rapidamente minimizando os impactos decorrentes de um incidente.

Para gestão de incidentes de segurança a Avenue possui a Política de Resposta a Incidentes e o Plano de Resposta a Incidentes.

5.5.7 Desenvolvimento Seguro

Os sistemas da Avenue são desenvolvidos baseados nas melhores práticas de desenvolvimento seguro de forma a proteger os dados e informações de ameaças que comprometam a segurança.

As regras estão dispostas na Norma de Desenvolvimento Seguro.

5.5.8 Conscientização e Treinamento

Todos os colaboradores devem ser conscientizados e treinados quanto às melhores práticas de segurança da informação de forma a compreender o seu papel e responsabilidade, com o objetivo de fortalecer a cultura e a proteção das informações da Avenue e de seus clientes.

5.5.9 Segurança dos parceiros de negócio e prestadores de serviços

Os parceiros de negócio e prestadores de serviços da Avenue devem observar as diretrizes na Política para fornecedores disponível na página da Avenue, bem como garantir os princípios de Confidencialidade, Integridade e Disponibilidade na execução dos serviços contratados.

Os parceiros de negócio e os prestadores de serviços devem ser avaliados antes da contratação, bem como monitorados durante a vigência do contrato.

As regras estão dispostas na Norma de Gestão de Fornecedores.

5.5.10 Gestão do ambiente de computação em nuvem

O ambiente de processamento e armazenamento de dados da Avenue são todos hospedados em ambiente de computação em nuvem que possuem alguns riscos inerentes a este modelo, para isto as seguintes diretrizes devem ser observadas na gestão deste ambiente:

• **Segurança dos acessos remotos** – o acesso seguro para administração e manutenção dos recursos em nuvem devem ser garantidos;

• **Acesso administrativo** – o acesso para administração do ambiente de nuvem é restrito a pessoas autorizadas pela Diretoria da Avenue.

6. Desligamento de Colaboradores

O desligamento de colaboradores e/ou usuários deve ser imediatamente informado à área de TI com a data de rescisão acordada.

A área de TI encerrará o acesso do colaborador e/ou usuário desligado, bloqueando os privilégios de acesso imediatamente ou na data de desligamento acordada.

Parceiros também devem notificar imediatamente a Avenue nos casos em que um empregado de sua empresa com acesso às redes da Avenue seja desligado.

7. Reporte de Incidentes

The rules are laid out in the Monitoring and Security of the Environment Policy.

5.5.6 Management of information security incidents

Information security events are reported and monitored for corrective action to be taken quickly and to minimize the impact of an incident.

For security incident management, Avenue has the Incident Response Policy and the Incident Response Plan.

5.5.7 Secure Development

Avenue's systems are developed based on the best practices of secure development to protect data and information from threats that compromise security.

The rules are laid out in the Safe Development Policy.

5.5.8 Awareness and Training

All employees should be made aware of and trained on the best practices of information security to understand their role and responsibility, with the goal of strengthening the culture and protection of information for Avenue and its clients.

5.5.9 Safety of business partners and service providers

Avenue's business partners and service providers must observe the guidelines in the Supplier Policy available on the Avenue website, as well as ensure the principles of Confidentiality, Integrity and Availability in the execution of the contracted services.

Business partners and service providers should be assessed prior to contracting, as well as monitored during the period of the contract.

The rules are laid out in the Supplier Management Policy.

5.5.10 Cloud computing environment management

Avenue's data processing and storage environment are all hosted in cloud computing environments that have some risks inherent to this model, for this the following guidelines should be observed in managing this environment:

• **Remote access security –** the secure access for administration and maintenance of cloud resources must be guaranteed;

• **Administrative access** – the access for administration of the cloud environment is restricted to persons authorized by Avenue's Board of Directors.

6. Employee Termination

The termination of employees and/or users must be immediately informed to the IT area with the agreed termination date.

IT will terminate the access of the terminated employee and/or user by locking down access privileges immediately or on the agreed-upon termination date.

Partners must also notify Avenue immediately in cases where an employee of their company with access to Avenue's networks is terminated.

7. Incident Reporting

Um incidente de segurança da informação ocorre quando uma ameaça explora uma vulnerabilidade violando os princípios da confidencialidade, integridade e disponibilidade.

Os incidentes de segurança da informação envolvendo dados e informações da Avenue e de seus clientes devem ser registrados e tratados de forma a minimizar o impacto.

As suspeitas e/ou incidentes de Segurança da Informação envolvendo o tratamento de dados pessoais e dados confidenciais da Avenue devem ser informados imediatamente através do e-mail securityincident@avenue.us ou abertura de ticket no Jira.

8. Seguro Cibernético

A Avenue contrata seguro cibernético, a fim de garantir uma maior proteção para a empresa e seus clientes com relação a segurança da informação.

9. Teste de penetração

Um teste de penetração é um ataque de software controlado e planejado na infraestrutura de segurança cibernética de uma instituição com o objetivo de identificar falhas de segurança. A área de TI coordena testes de penetração nos sistemas e redes da Avenue, no mínimo, anualmente.

Os resultados das avaliações de vulnerabilidade devem ser armazenados pela área de TI e posteriormente considerados nos processos de avaliação de risco realizados pela área de Compliance.

10. Penalidades

O descumprimento desta política implicará em advertências formais e dependendo da gravidade e risco poderá resultar no desligamento do colaborador.

11. Responsabilidades do Departamento

Comitê de Segurança da Informação

• Apoiar e garantir que as políticas e normas sejam cumpridas;

• Garantir que haja um processo educativo e campanhas de sensibilização para promover a cultura de segurança da informação e privacidade.

Data Protection Officer (“DPO”)

• Receber comunicações da ANPD e adotar as providências internas necessárias para o endereçamento de eventuais solicitações;

• Orientar os Colaboradores a respeito das práticas e procedimentos a serem adotados em relação à proteção de Dados Pessoais;

• Monitorar as estratégias da Avenue com relação à proteção de dados pessoais, por meio de atribuição de responsabilidades, conscientização e treinamento de equipes envolvidas na operação de Tratamento de Dados Pessoais;

• Estabelecer, monitorar e dar a assistência necessária para a criação e efetividade de políticas, procedimentos e medidas de segurança da informação, especialmente aquelas voltadas para a proteção de dados pessoais; e

• Manter registro das operações de Tratamento conduzidas pela Avenue.

Equipe de Segurança da Informação

• Manter esta política sempre atualizada e revisá-la, pelo menos, anualmente;

An information security incident occurs when a threat exploits vulnerability by violating the principles of confidentiality, integrity, and availability.

Information security incidents involving Avenue and its clients’ data and information must be recorded and handled in a way that minimizes impact.

Suspicions and/or incidents of Information Security involving Avenue’s handling of personal data and confidential data should be reported immediately by emailing securityincident@avenue.us or opening a ticket on Jira.

8. Cyber Insurance

Avenue contracts cyber insurance to ensure greater protection for the company and its clients with regard to information security.

9. Penetration test

A penetration test is a controlled and planned software attack on an institution’s cybersecurity infrastructure with the aim of identifying security flaws. The IT department coordinates penetration tests on Avenue’s systems and networks at least annually.

The results of the vulnerability assessments must be stored by the IT area and subsequently considered in the risk assessment processes carried out by the Compliance area.

10. Penalties

Failure to comply with this policy will result in formal warnings and, depending on the severity and risk, may result in the employee’s termination.

11. Department Responsibilities

Committee of Information Security

• Supporting and ensuring that policies and rules are adhered to;

• Ensuring that there is an educational process and awareness campaigns to promote information security and privacy culture.

Data Protection Officer (“DPO”)

• Receiving communications from the ANPD and adopt the necessary internal measures to address eventual requests;

• Guiding the Collaborators as to the practices and procedures to be adopted in relation to the protection of Personal Data;

• Monitoring Avenue’s strategies with regard to the protection of personal data, by assigning responsibilities, raising awareness and training teams involved in the operation of Personal Data Processing;

• Establishing, monitoring, and providing the necessary assistance for the creation and effectiveness of information security policies, procedures, and measures, especially those for the protection of personal data; and

• Keeping record of Treatment operations conducted by Avenue.

Information Security Team

• Keeping this policy up to date at all times and reviewing it at least annually;

• Monitorar o ambiente de segurança da informação, a fim de garantir a Confidencialidade, Disponibilidade e Integridade das informações da Avenue e de seus clientes;

• Garantir a conformidade com esta política.

Equipe de TI

• Configurar e manter a infraestrutura da Avenue de acordo com as melhores práticas de Segurança da Informação e regulamentações aplicáveis.

Líderes

• Conscientizar os colaboradores sob sua responsabilidade.

Colaboradores

• Notificar incidentes de segurança da informação;

• Zelar pela segurança das informações da Avenue e de seus Clientes;

• Cumprir as diretrizes dispostas nesta política.

12. Definição dos termos

Ativo de Informação	Qualquer ativo que processe, armazene ou, inclusive, a própria informação
Colaborador	Todos os administradores, sócios, funcionários e estagiários da Avenue
Computação em nuvem	É o fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, pela Internet para oferecer inovações mais rápidas, recursos flexíveis e escalabilidade.
Confidencialidade	Garantia de que a informação não estará disponível e nem será divulgada a indivíduos, entidades ou processos sem autorização.
Continuidade do negócio	Capacidade de uma organização de continuar a entrega de produtos e serviços em um nível aceitável após incidentes e interrupções
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
Data Protection Officer (DPO) ou encarregado	Pessoa responsável por atuar como canal de comunicação entre a Avenue, os titulares de dados pessoais e a ANPD
Disponibilidade	Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
Informação	Ativo essencial para o negócio, pode estar na forma escrita, impressa, verbal ou em meio digital ou físico.
Integridade	Corresponde à preservação da precisão, consistência e confiabilidade das informações. Garantia de que a informação não será corrompida, comprometida ou danificada por processamentos sistêmicos, terceiros ou colaboradores.
Violação de dados	Violação de segurança que leva à destruição acidental ou ilícita, à perda, à divulgação não autorizada ou o acesso a dados protegidos e transmitidos, armazenados ou transformados de outro modo.
Usuário	Colaborador e/ou prestador de serviços autorizado a utilizar informações, sistemas ou recursos da Avenue

13. Regulações, Leis e Orientações Externas

• Monitoring the information security environment to ensure the Confidentiality, Availability, and Integrity of Avenue's and its clients' information;

• Ensuring compliance with this policy.

IT Team

• Configuring and maintaining Avenue's infrastructure in accordance with Information Security best practices and applicable regulations.

Leaders

• Raising awareness of the collaborators under their responsibility.

Collaborators

• Notifying information security incidents;

• Ensuring the security of Avenue's and its Clients' information;

• Complying with the guidelines set forth in this policy.

12. Definition of terms

Information Assets	Any asset that processes, stores or even the information itself
Collaborator	All Avenue's managers, partners, employees, and interns
Cloud Computing	It is the provisioning of computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet to deliver faster innovation, flexible resources, and scalability.
Confidentiality	Assurance that the information will not be made available or disclosed to unauthorized individuals, entities, or processes.
Business Continuity	An organization's ability to continue the delivery of products and services at an acceptable level after incidents and interruptions
Personal data	Information related to an identified or identifiable natural person
Sensitive Personal Data	Personal data concerning racial or ethnic origin, religious conviction, political opinion, membership of a trade union or of a religious, philosophical, or political organization, data concerning health or sex life, genetic or biometric data when linked to a natural person;
Data Protection Officer (DPO) or person in charge	Person responsible for acting as a communication channel between Avenue, the personal data subjects and the ANPD
Availability	Ensuring that authorized users get access to the information and corresponding assets whenever necessary.
Information	An essential asset for the business, it can be in written, printed, verbal, digital, or physical form.
Integrity	It corresponds to preserving the accuracy, consistency, and reliability of the information. Guarantee that the information will not be corrupted, compromised, or damaged by systemic processing, third parties, or collaborators.
Data breach	Security breach leading to accidental or unlawful destruction, loss, unauthorized disclosure of or access to protected and transmitted, stored or otherwise transformed data.
User	Employee and/or service provider authorized to use Avenue's information, systems, or resources

13. External Regulations, Laws and Guidelines

Os requisitos desta política devem ser aplicados de acordo com os estatutos, leis, regras, regulamentos e orientações externas das jurisdições em que a companhia opera.

Resolução CMN No. 4.893 de fevereiro/2021

Instrução CVM No. 612 de agosto/2021

Lei 13.709 de agosto/2021

FINRA Rule Cybersecurity 3110

FINRA Rule Cybersecurity 3129

FINRA Rule Cybersecurity 4530 e 4530.01

FINRA Rule Cybersecurity 248.201 – 202

FINRA Rule Cybersecurity 248.1-100

FINRA Rule Cybersecurity 240.17ª

Norma ABNT ISO/IEC 27001

Norma ABNT ISO/IEC 27002

Norma ABNT ISO/IEC 27004

Norma ABNT ISO/IEC 27701

Norma ABNT ISO/IEC 16167

Norma ABNT ISO/IEC 27017

NIST (National Institute of Standards and Technology)

14. Aprovações

Todas as aprovações são feitas através do Shrepoint.

The requirements of this policy shall be applied in accordance with the statutes, laws, rules, regulations, and external guidelines of the jurisdictions in which the company operates.

CMN Resolution No. 4,893 of February/2021

CVM Instruction No. 612 of August/2021

Law 13.709 of August/2021

FINRA Rule Cybersecurity 3110

FINRA Rule Cybersecurity 3129

FINRA Rule Cybersecurity 4530 and 4530.01

FINRA Rule Cybersecurity 248.201 – 202

FINRA Rule Cybersecurity 248.1-100

FINRA Rule Cybersecurity 240.17ª

ABNT Rule ISO/IEC 27001

ABNT Rule ISO/IEC 27002

ABNT Rule ISO/IEC 27004

ABNT Rule ISO/IEC 27701

ABNT Rule ISO/IEC 16167

ABNT Rule ISO/IEC 27017

NIST (National Institute of Standards and Technology)

14. Approval

All approvals are processed in Shrepoint.