Política de Segurança da Informação

Information Security Policy

hEDGEpoint

Folha de controle | *Control Sheet*

Informações Gerais | *General Information*

**Título	*Title:***	Política de Segurança da Informação	*Information Security Policy*
**Referência	*Reference:***	POL-CYB/GBL-001
**Versão	*Version:***	V2
**Vigência	Expiration Date:**	1 ano	*year*
**Departamento Responsável	*Responsible Department:***	Departamento de Segurança Cibernética	Cybersecurity Department
**Escopo	*Scope:***	Global
**Leis e Regulamentos Relacionados	*Related Laws and Regulations***	**Brasil	Brazil** • CVM N° 35, DE 26 DE MAIO DE 2021 • LEI N° 13.709, DE 14 DE AGOSTO DE 2018 (LGPD) • Resolução CMN n° 4.893 de 26/2/2021 (BCB) **EUA	US** • California Consumer Privacy Act (CCPA) • 9070 - NFA Compliance Rules 2-9, 2-36 and 2-49: Information System Security Programs **Europa	Europe** • Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR)
**Políticas e Procedimentos Relacionados	*Related Policies and Procedures***	• Política de Gestão de Identidades e Acessos	*Identity and Access Management Policy* • Política de Classificação da Informação	*Information Classification Policy* • Código de Conduta Ética e Integridade	*Code of Ethical Conduct and Integrity* • Política de Treinamento e Certificações	*Training and Certification Corporate Policy* • Política de Gestão de Continuidade de Negócios	*Business Continuity Management Policy* • Procedimento de Avaliação de Impacto nos Negócios	*Business Impact Analysis Procedure* • Procedimento de Desenvolvimento de Sistemas, Projetos e Inovações	*Development of Systems, Projects, and Innovations Procedure* • Procedimento de segurança para usuários finais de arquivos críticos não-sistêmicos	*Security proceeding for end users of non-standard critical files* • Termo de Referência do Comitê de Segurança da Informação	*Information Security Committee Term of Reference*
**Audiência	*Audience***	USO RESTRITO	*RESTRICTED USE*

Histórico de Versões | Version History

Versão | *Version*	Histórico | *Historic*	Data de Vigência | *Effective Date*	Autor | Author
2	Revisão dos Tópicos: Controle de Acesso (III e IV); Ambientes Lógicos (IV); Monitoramento; Gestão de Riscos Cibernéticos; Comitê de Segurança da Informação (CSI); Capacitação; Área de Data Privacy (DPO); Departamento Jurídico; Departamento de Recursos Humanos | Review of Topics: Access Control (III and IV); Logical Environments (IV); Monitoring; Cyber Risk Management; Information Security Committee (CSI); Training; Data Privacy Area (DPO); Legal Department; Human Resources Department.	14-03-2024 2024-03-14	Cybersecurity
1	Criação do Documento | *Document Creation*	30-08-2022 2022-08-30	Cybersecurity

Aprovado por | *Approved by:*	DocuSigned by: Franklin Cavalcante AC89F0FFFE794CE...	DocuSigned by: Enio Shiguemi Nagae 447834B4794149B...
	Franklin Cavalcante	**Enio Nagae**
	Gerente de Cybersecurity | *Cybersecurity Manager*	Head de Tecnologia | *Head of Technologies*
	DocuSigned by: Eduardo Roedel B50A785DDD434E3...	DocuSigned by: Sergio Lenharo 551897CBA04C452...
	Eduardo Roedel	**Sergio Lenharo**
	Diretor Executivo | *Executive Director*	Diretor Executivo | *Executive Director*

Sumário | *Summary*

1. Introdução | *Introduction*

A hEDGEpoint Global Markets ("HPGM" ou "Grupo HPGM") reconhece a importância da Segurança da Informação (SI), como meio para o cumprimento de sua missão, valores e estratégia de negócio, assim como investe constantemente no crescimento profissional de seus colaboradores e em tecnologias que garantam a qualidade e segurança de seus produtos e serviços.

Este documento dispõe sobre diretrizes e estratégias adotadas pela HPGM, relacionadas às atividades de segurança cibernética, modelo de governança de SI e proteção de suas informações, dados e recursos de TI.

Esta Política de Segurança da Informação (PSI) foi elaborada para garantir a sua aderência às Legislações vigente.

É responsabilidade de TODOS, independentemente de cargo ou função, estarem cientes e cumprirem a PSI da HPMG, além de aplicá-la constantemente nas suas atividades diárias, respeitando e disseminando seu conteúdo.

hEDGEpoint Global Markets ("HPGM" or "HPGM Group) recognizes the importance of Information Security (IS) to the fulfillment of its mission, values, and strategy of the business, as well as the result of constant investment in the professional development of its employees and technology, to ensure the quality and safety of our products and services.

This document provides guidelines and strategies to be adopted by HPGM Group related to cyber-security activities, the IT governance model and the protection of information, assets, and data.

This Information Security Policy (ISP) has been developed to ensure adherence to the Laws in force.

Regardless of job title or role, it is everyone's responsibility to be aware of and comply with HPGM's ISP. All employees must apply it constantly in their day-by-day activities, observing, and conveying the content.

2. Objetivo | *Purpose*

A PSI é o documento que expressa o posicionamento do Grupo HPGM em relação à proteção e preservação dos seus ativos (informação, dados e equipamentos tecnológicos) e tem como objetivo:

I. Declarar formalmente o comprometimento da Alta Direção do Grupo HPGM, na promoção de diretrizes estratégicas, responsabilidades, competências e apoio e melhoria contínua ao Sistema de Gestão de Segurança da Informação (SGSI), a fim de garantir a proteção dos seus ativos tangíveis e intangíveis;

II. Estabelecer as responsabilidades e os limites de atuação dos colaboradores do Grupo HPGM em relação à SI, reforçando a cultura interna e priorizando as ações necessárias conforme negócio;

III. Viabilizar a confidencialidade, disponibilidade e integridade das informações e mitigar os riscos cibernéticos a um nível aceitável de acordo com o apetite de riscos estabelecido pela HPGM, definindo mecanismos e controles de proteção dos ativos de sua propriedade.

The ISP expresses the position of HPGM Group concerning the protection and preservation of its assets (information, data, and hardware) and it has the following objectives:

I. Declare a formal commitment from the Executive Management of the HPGM Group to the promotion of the strategic framework, responsibilities, skills, and continuous support and improvement to the Information Security Management System (ISMS) in order to ensure the protection of its tangible and intangible assets.

II. To establish responsibilities and boundaries of the HPGM Group employees concerning IS, reinforcing an internal culture and prioritizing the necessary actions according to the business.

III. Enable the confidentiality, availability, and integrity of information and mitigate cyber risks to an acceptable level in accordance with the risk appetite established by HPGM, definition mechanisms, and controls for the protection of its assets.

3. Abrangência | *Scope*

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, estagiários, visitantes e

This is an internal document with legal value and immediate and indistinct applicability, for the employees, interns, visitors, and service providers who

prestadores de serviços que façam uso continuado ou eventual dos recursos tecnológicos do Grupo HPGM ou de sua rede de computadores.	make continuous or eventual use of the technological resources of HPGM Group including its computer network.
4. Princípios | *Principles*	
Preservar e proteger as informações do Grupo HPGM ou sob sua reponsabilidade de vulnerabilidades e ameaças, em todo o seu ciclo de vida, contida em qualquer suporte ou formato. Prevenir e reduzir impactos gerados pelos incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades profissionais. No âmbito de suas obrigações e responsabilidades, zelar por relações transparentes e éticas nos termos do Código de Conduta Ética e Integridade. Cumprir as legislações relacionadas ao negócio no que diz respeito à segurança da informação, assim como as legislações vigentes em cada país de atuação.	Preserve and protect the information of the HPGM Group, or under its responsibility, from vulnerabilities and threats throughout its lifecycle, contained in any media or format. Prevent and reduce the impacts of information security incidents, ensuring confidentiality, integrity, availability, authenticity, and legitimacy in the development of professional activities. Within the scope of their obligations and responsibilities, ensure transparent and ethical relationships in accordance with the Code of Ethical Conduct and Integrity. Comply with the industry related legislation regarding IS, including the laws in force in each country HPGM operates.
5. Diretrizes Gerais | *General Guidelines*	
Interpretação: Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas nos normativos só devem ser realizadas após prévia e formal autorização do Gestor do colaborador. **Publicidade:** Esta PSI e seus documentos complementares devem ser divulgados aos colaboradores pelo Departamento de Compliance da hEDGEpoint, visando dar publicidade para todos que se relacionam profissionalmente com a HPGM. **Propriedade:** As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade do Grupo HPGM e devem ser utilizados unicamente para fins profissionais. **Classificação da Informação:** Todas as informações de propriedade ou sob a responsabilidade do Grupo HPGM devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida, conforme "Política de Classificação da Informação". **Sigilo:** É vedada, a qualquer tempo, a revelação de informação de propriedade ou sob a responsabilidade do Grupo HPGM sem a prévia e formal autorização do Gestor da Informação, excetuando-se a informação pública. A informação é classificada como pública	**Interpretation:** This ISP and its supporting documents shall be interpreted in a restrictive way, in other words, activities that are not comprised under HPGM's policies and procedures should only be performed after a previous and formal consent from the employee's Manager. **Advertising:** This and its supplementary documents should be disseminated to the employees by the Compliance Department of hEDGEpoint, aiming to provide publicity to all those who have professional relations with HPGM. **Property:** All information created, accessed, manipulated, stored, or disposed of, in the exercise of the activities carried out by our employees, as well as the rest of the intangible and tangible assets that are made available, is property of or under the responsibility of HPGM Group must be solely used for business purposes. **Data Classification:** All information owned by or under the responsibility of the HPGM Group must be classified and protected with specific controls throughout its lifecycle, according to the 'Information Classification Policy'. **Confidentiality**: At any time, the disclosure of information owned by or under the responsibility of the HPGM Group without the prior and formal authorization of the Information Manager is

quando ela puder ser divulgada a todos, isto é, colaboradores, estagiários, visitante, prestadores de serviços e público em geral, sem que isso provoque impactos no negócio. Em caso de dúvida quanto a informação, procurar o Gestor imediato.

Uso dos Ativos: Os ativos de propriedade ou sob sua responsabilidade do Grupo HPGM devem ser utilizados somente para fins profissionais e de acordo com as orientações dos fabricantes e da empresa.

I. **Uso dos Recursos de TI:** Os Recursos de TI de propriedade ou sob a responsabilidade do Grupo HPGM devem ser utilizados somente para fins profissionais.

II. **Inventário dos Ativos:** O Departamento de Infraestrutura de TI mantém de modo atualizado um inventário de hardwares e softwares contendo, no mínimo, as informações necessárias do ativo e colaborador responsável pelo uso.

III. **Dispositivos Móveis Corporativos:** Os dispositivos móveis devem ser utilizados quando fornecidos ou autorizados previamente pelo Diretor da área e/ou pelos departamentos de HR e Compliance, a depender da necessidade, seguindo as recomendações de utilização de Rede Virtual Privada (VPN), ferramentas de gerenciamento e bloqueio remoto.

IV. **Repositórios Digitais e Dispositivos Removíveis:** Somente é permitido o uso do Sharepoint autorizado e fornecido pela HPGM para o armazenamento e transmissão de informações de propriedade ou sob a responsabilidade da empresa. É vedado aos colaboradores o uso de repositórios digitais ou dispositivos removíveis não autorizados pela HPGM.

V. **Aplicativos de Comunicação Instantânea:** Somente é permitido o uso de aplicativos de Comunicação Instantânea autorizados e fornecidos pela HPGM para troca de informações corporativas.

Controle de Acesso: A HPGM gerencia o acesso físico e lógico aos seus ambientes que contenham ativos e informações. Desse modo, o colaborador recebe uma identidade digital de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

I. O colaborador é responsável pelo uso, proteção e sigilo de sua identidade digital, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de suas credenciais, tal qual de terceiros.

II. Para garantir o controle de acesso aos ambientes físicos e lógicos, a HPGM utiliza os critérios do mínimo conjunto necessário (least privilege) e

prohibited, except for public information. Information is classified as public when it can be disclosed to everyone, that is, employees, interns, visitors, service providers, and the general public, without affecting the business. Any question regarding data classification must be submitted to the line manager.

Usage of Assets: The assets owned or under HPGM Group's responsibility shall be used solely for business purposes and according to the manufacturer's and HPGM's guidelines.

I. **Usage of IT Resources:** The IT resources of property or under HPGM Group's responsibility shall be used only for business purposes, in accordance with local legislation.

II. **Assets Inventory:** The Infrastructure IT team maintains an updated hardware and software inventory, including the asset identification and the person responsible for it.

III. **Corporate Mobile Devices:** mobile devices should be used when provided or previously authorized by the Area Director and/or the HR and Compliance departments, depending on the need, following the recommendations for using a Virtual Private Network (VPN), management tools, and remote locking.

IV. **Digital repositories and Removable Storage Devices:** only the usage of SharePoint, authorized and provided by HPGM Group, is permitted to store and transmit proprietary information belonging to or under the company's responsibility. The usage of digital repositories or removable devices not authorized by HPGM Group is not permitted.

V. **Instant Communication Application:** Only the use of Instant Messaging applications authorized and provided by HPGM for the exchange of corporate information is permitted.

Access control: The HPGM Group manages both physical and logical access to its environments containing assets and information. Therefore, employees always receive a non-transferable and privately disclosed digital identity for personal use.

I. The employee is responsible for the use, protection, and security of their digital identity, it is not allowed to share, give, save, replicate, publish or make any unauthorized use of his credentials including third parties.

II. To ensure proper Physical and Logical environment Access Control, HPGM uses the criteria of "least privilege access" and "need to know access" to define access levels for each employee, according to Access Management Policy.

estritamente necessários (need to know) ao definir os acessos de cada colaborador, conforme "Política de Gestão de Acessos".

III. Para garantir a autenticidade do acesso aos sistemas lógicos é utilizado múltiplo fator de autenticação nos sistemas, quando aplicável.

IV. É responsabilidade do Gestores das áreas de negócio, e quando necessário do proprietário do(s) sistema(s) definir aspectos de perfis adequados às funções executadas pelos colaboradores no acesso ao(s) sistema(s), conforme controle realizado via Matriz de Segregação de Funções (SoD).

Ambientes Lógicos: Os sistemas e Recursos de TI que suportam os processos e as informações do Grupo HPGM devem ser confiáveis, íntegros, seguros e disponíveis a quem deles necessitem para execução de suas atividades profissionais. A fim de garantir a segurança acima estabelecida, a HPGM utiliza os seguintes sistemas de proteção, ativos e atualizados:

I. Contra programas maliciosos e acessos indevidos, ferramentas como antivírus e firewall.

II. Para proteção de estações e servidores utiliza ferramentas de Endpoint Detection and Response (EDR) e gerenciamento de patches automatizados.

III. Contra mensagens eletrônicas indesejadas ou não autorizadas, ferramenta de AntiSpam.

IV. Para prevenção ao vazamento de dados é utilizada uma solução de Data Loss Prevention (DLP).

Desenvolvimento e Aquisição de Software: Tanto o desenvolvimento interno e externo de softwares como aquisições de mercado devem cumprir os requisitos de segurança da informação e controles de acesso previstos nesta PSI e demais Políticas Complementares, este processo vale também para "software as a service" (SaaS). Antes do desenvolvimento e/ou aquisição de softwares os Departamentos de Infraestrutura de TI e Cybersecurity devem ser consultados.

Para garantir a integridade e a segurança de nossos sistemas e dados, é imprescindível que o Departamento de TI seja consultado previamente, via cybersecurity@hedgepointglobal.com, à fase de desenvolvimento ou aquisição de quaisquer soluções de Computação de Usuário Final (EUC - End-User Computing). Esta consulta prévia é crucial para avaliar a adequação tecnológica, os riscos de segurança associados e a conformidade com as políticas internas e regulamentações aplicáveis.

Salvaguarda (backup): A HPGM mantém um processo de salvaguarda das informações e dos dados necessários para recuperação dos seus sistemas

III. To ensure the authenticity of access to logical systems, multi-factor authentication is used in these systems, when applicable.

IV. It is the responsibility of the Business area Managers, and when necessary, the owner of the system(s) to define aspects of profiles suitable for the functions performed by the employees when accessing the system(s), as controlled through the Segregation of Duties Matrix (SoD).

Logical Environments: All systems and resources that support the processes and information from HPGM Group should be reliable, thorough, safe, secure, and available to those who need them to carry their professional activities. To ensure the safety and security set forth above, HPGM Group uses protection systems and keep them active and updated:

I. Against malicious programs and unauthorized access, tools such as antivirus and firewall are used.

II. For protection of workstations and servers, Endpoint Detection and Response (EDR) tools and automated patch management are used.

III. Against unwanted or unauthorized electronic messages, an AntiSpam tool is utilized.

IV. For data leakage prevention, a Data Loss Prevention (DLP) solution is used.

Software Development and Acquisition: both internal and external software development, including purchases from the market, must comply with the data security requirements and access controls set in the ISP, and in any other Complementary Procedures, this process also applies to software as a service (SaaS). Before the development and/or acquisition of software, the IT Infrastructure and Cybersecurity departments must be consulted.

To ensure the integrity and security of our systems and data, it is essential that the IT Department is consulted in advance, via cybersecurity@hedgepointglobal.com, before the development or acquisition phase of any End-User Computing (EUC) solutions. This prior consultation is crucial for assessing technological suitability, associated security risks, and compliance with internal policies and applicable regulations.

Backup: the HPGM group maintains a backup process to allow the recovery of its systems, such process was designed to attend to operational and legal requirements, including business continuity in case of failure, incident, or any disruptive event.

Monitoring: HPGM Group monitors its physical and logical environments, aiming at the effectiveness of the implemented controls, the protection of its assets, its reputation, and the identification of events or alerts

(backup), a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas, incidentes ou eventos disruptivos.

Monitoramento: A HPGM monitora seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio, a reputação e a identificação de eventos ou alertas de incidentes referentes à segurança da informação. A HPGM se reserva ao direito de monitorar, auditar e/ou inspecionar a qualquer momento e sem prévio aviso nem justificativa, os recursos de TI, bem como deliberar por eventual retirada de qualquer uso cedido ao colaborador, sem prévio aviso ou justificativa, sempre que considerar necessário.

Serão realizados periodicamente (uma vez ao ano) testes e varreduras para a detecção de vulnerabilidades.

Gestão de Riscos Cibernéticos: O Departamento de Cybersecurity identifica e avalia os riscos relacionados à SI e Cibersegurança e adota as melhores práticas para o seu gerenciamento e controle. A "Determinação Do Risco De Cibersegurança" seguirá a mesma matriz de riscos definida pela área de Riscos Operacionais do Grupo HPGM.

Os critérios para aceitação de riscos cibernéticos, relaciona-se a situações específicas em que as ações de resposta ao risco são complexas ou dispendiosas para implementar em comparação com os possíveis efeitos do risco, considerando todos os impactos possíveis e o apetite de risco do Grupo HPGM, conforme a Política de Gestão de Risco Operacional.

Gestão de Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e na infraestrutura tecnológica do Grupo HPGM, devem preservar os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações e realizados somente pelo Departamento de TI, conforme diretrizes do CAB (Change Adivisory Board).

Continuidade do Negócio: Os procedimentos de gestão de Continuidade do Negócio devem ser executados em conformidade com a Política de Continuidade de Negócios do Grupo HPGM.

Investimentos: Os investimentos em SI na HPGM são estudados e deliberados pelo Departamento de Cybersecurity junto à Diretoria, e quando necessário alinhado com as áreas de negócio, considerando a viabilidade dos investimentos (custo x benefício) e os impactos na qualidade dos processos de negócio.

Comitê de Segurança da Informação (CSI): A HPGM estabeleceu um CSI responsável por atuar com independência e objetividade visando o melhor interesse do Grupo HPGM, além de envidar esforços

related to information security incidents. HPGM reserves the right to monitor, audit, and/or inspect at any time and without prior notice or justification, IT resources, as well as to decide on the eventual withdrawal of any usage granted to an employee, without prior notice or justification, whenever deemed necessary.

Periodic tests and scans for vulnerability detection will be conducted (once a year).

Cyber Risk Management: The Cybersecurity Department identifies and assesses risks related to IS and Cybersecurity and adopts best practices for its management and control. The "Determination of Cybersecurity Risk" will follow the same risk matrix defined by the Operational Risks area of HPGM Group.

The criteria for accepting cyber risks relate to specific situations where risk response actions are complex or costly to implement compared to the potential effects of the risk, considering all possible impacts and the risk appetite of the HPGM Group, according to the Operational Risk Management Policy.

Change Management: The progress and outcome of a change, mainly in the systems and infrastructure of the HPGM Group, need to follow the controls related to availability, integrity, confidentiality, and authenticity of the information and are executed only by the IT Department. According to the guidelines of the CAB (Change Advisory Board).

Business Continuity: The procedures of Business Continuity Management must be performed following HPGM's Business Continuity Policy.

Investments: IS investments are analyzed and decided by the Cybersecurity area together with the Head of IT and, when necessary, they are aligned with the business areas, considering the feasibility of the investment (cost/benefit) and its impacts on the quality of the business processes.

Information Security Committee (ISC): HPGM Group set an Information Security Committee responsible for acting, independently and objectively, in the best interests of HPGM Group, such committee is also responsible for the development and adoption of best practices in Corporate and Business Governance.

The CSI is composed of four (4) voting members, with decisions of the board approved only by unanimous votes. The CSI is subject to the Risk Directorate of the HPGM Group, with permanent operation, as per the Information Security Committee Policy, meeting monthly, or as needed, to address agendas related to Information Security (IS) and Information Technology (IT).

para o desenvolvimento e adoção das boas práticas de Governança Corporativa e negócios.

O CSI é composto por quatro (4) membros votantes com as decisões do colegiado aprovadas apenas pela unanimidade dos votos. O CSI está submetido à Diretoria de Risco do Grupo HPGM, com atuação permanente, conforme Política do Comitê de Segurança da Informação reunindo-se mensalmente, ou conforme a necessidade, para tratar de pautas relacionadas à Segurança da Informação (SI) e Tecnologia da Informação (TI).

É fundamental a participação de representantes de TI e SI, em Comitês de Riscos Operacionais e de Produtos, para analisar se algum assunto tratado nestes Comitês apresenta necessidade de avaliações no aspecto de SI e/ou TI.

Comunicação e Escalonamento de Incidentes de Segurança: A HPGM possui um canal de comunicação divulgado aos seus colaboradores para reportar possíveis casos de incidentes de segurança da informação: cybersecurity@hedgepointglobal.com. Confirmado o incidente de segurança classificado em médio ou alto, este deve ser registrado através de formulário para registro de incidentes relacionados a riscos operacionais, disponível na intranet da empresa através do seguinte endereço: FORMULÁRIO DE INCIDENTES DE RISCO OPERACIONAL. O escalamento de incidentes de segurança da informação segue as diretrizes definidas na Política de Escalamento de Gestão Riscos da HPGM.

Para o público externo é disponibilizado o canal ethicline@hedgepointglobal.com para o reporte de qualquer questão relacionada à cibersegurança.

Proteção de Dados Pessoais: A HPGM respeita a privacidade, e implementa a proteção da disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais.

Capacitação: A HPGM estabelece um plano periódico e anual de capacitação direcionado ao desenvolvimento, conscientização e manutenção das habilidades dos colaboradores sobre Cybersecurity. Estes treinamentos têm caráter obrigatório, sendo realizado todo início de cada ano, e os resultados de conclusão serão auferidos pelo departamento de RH.

Revisão e Atualização: A HPGM possui e mantem um programa de revisão/atualização desta PSI e das Políticas Complementares sempre que se fizer necessário, desde que não exceda o período máximo de 12 (dozes) meses, visando à garantia que todos os

It is essential for representatives from IT and IS to participate in Operational Risk and Product Committees, to analyze if any topic discussed in these Committees requires assessments in the SI and/or IT aspect.

Security Incident Reporting and Escalation: HPGM has a communication channel disclosed to its employees to report potential information security incidents: cybersecurity@hedgepointglobal.com.

Once a security incident classified as medium or high is confirmed, it must be registered through a form for recording incidents related to operational risks, available on the company's intranet at the following address: OPERATIONAL RISK INCIDENT FORM. The escalation of information security incidents follows the guidelines set out in the HPGM Risk Management Escalation Policy.

For the external public, the channel ethicline@hedgepointglobal.comis provided for reporting any cybersecurity-related issues.

Data Protection: HPGM group respects privacy and implements the protection of availability, integrity, and confidentiality of personal data throughout its life cycle, in any form of storage or media, handling it as confidential information.

Training: HPGM establishes a periodic and annual training plan aimed at the development, awareness, and maintenance of the skills of employees in Cybersecurity. These trainings are mandatory and is carried out at the beginning of each year, and the completion results will be assessed by the HR department.

Review and Update: HPGM Group keeps a program to review and update this ISP and the Complementary Policies whenever needed, provided that it does not exceed the maximum period of 12 (twelve) months, to ensure that all security and legal technical requirements are implemented and up to date.

Changes: Changes to this Information Security Policy should be made by the Cybersecurity team. Changes to the Supplementary Policies must be duly communicated to the Cybersecurity Department through the email address: cybersecurity@hedgepointglobal.com.

Exceptions: Can only be permitted on circumstances that are considered exceptions to this ISP, they should be temporary and approved in advance by the Head of the area and Head of IT, Cybersecurity Manager and/or IT Head to have an effect, in addition, they may be revoked at any time, by decision of the employee's manager or by the Head of IT, without prior notice.

requisitos de segurança técnicos e legais implementados estejam sendo cumpridos e atualizados. **Alterações:** As alterações desta PSI devem ser feitas pelo time de Cybersecurity, alterações nas Políticas Complementares devem ser devidamente comunicadas ao Departamento de Cybersecurity, por meio do endereço eletrônico: cybersecurity@hedgepointglobal.com. **Exceções:** As exceções somente são admitidas de forma excepcional a essa PSI, devendo ser temporárias e aprovadas previamente pelo Head da respectiva área, Gerente de Cybersecurity Manager e/ou Head de TI para produzirem efeito, além disso, podem ser revogadas a qualquer tempo por mera liberalidade do Gestor do colaborador ou do Head da área, sem aviso prévio. **Dúvidas:** Qualquer dúvida relativa a esta PSI deve ser encaminhada ao Departamento de Cybersecurity por meio do endereço eletrônico: cybersecurity@hedgepointglobal.com.	**Questions:** Any questions regarding this ISP must be submitted to the Cybersecurity Department through the e-mail address: cybersecurity@hedgepointglobal.com.

6. Responsabilidades | *Responsibilities*

6.1 Diretoria de TI | *Director of IT*

O Head de TI é responsável por: I. Analisar, aprovar e declarar formalmente o seu comprometimento com esta PSI. II. Aprovar os investimentos em SI na HPGM, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio. III. Analisar e aprovar, ou não, as exceções de forma excepcional a essa PSI.	The Head of IT is responsible for: I. Analyze, approve, and declare the commitment with this PSI formally. II. Approve the investment in Information Security at HPGM Group, considering the feasibility and its impact on the quality of business processes. III. Review and approve, or deny, the exceptions concerning this ISP.

6.2. Comitê de Segurança da Informação (CSI) | *Information Security Committee (ISC)*

As atribuições do Comitê de Segurança da Informação (CSI) estão descritas no Termo de Referência do Comitê de Segurança da Informação.	The responsibilities of the Information Security Committee (ISC) are described in the Cybersecurity Committee Term of Reference.

6.3 Departamento de Cybersecurity | *Cybersecurity Departament*

I. Promover e realizar a gestão do SGSI, garantindo a implementação de controles, modelos, padrões e recursos necessários para a proteção da informação. II. Promover a cultura de SI no Grupo HPGM;	I. Promote and carry out the management of the ISMS and ensure the implementation of the controls, templates, patterns, and resources that are necessary for the protection of the information. II. Promote an Information Security culture in the HPGM Group.

III. Analisar e priorizar ações necessárias, balanceando custo e benefício. IV. Auxiliar, sempre que necessário, na capacitação dos colaboradores em SI. V. Aprovar os investimentos em SI no Grupo HPGM, juntamente com a Head de TI, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio. VI. Analisar os incidentes de SI reportados e submeter relatório para deliberação do Head de TI, sempre que necessário. VII. Identificar e avaliar os riscos relacionados à segurança da informação e propor melhorias e recursos necessários às ações de segurança da informação. VIII. Realizar e acompanhar estudos de tecnologias, com o apoio da área de Infraestrutura, quanto a possíveis impactos na segurança da informação e/ou na Infraestrutura. IX. Manter atualizado os documentos que compõem o SGSI. X. Propor, processos e procedimentos internos relativos à segurança da informação no Grupo HPGM. XI. Monitorar os acessos aos ambientes lógicos do Grupo HPGM. XII. Avaliar se os requisitos de segurança da informação estão presentes antes da aquisição, manutenção ou desenvolvimento de softwares. XIII. Garantir o andamento e o resultado de mudanças preservem os controles relacionados à disponibilidade, integridade, confidencialidade, autenticidade e legalidade das informações, sobretudo nos sistemas e na infraestrutura tecnológica. XIV. Solicitar, quando couber, procedimento disciplinar para apuração de responsabilidades dos envolvidos em violações de segurança da informação, deliberar a violação com os Departamentos de RH, Compliance e Jurídico e notificar os devidos responsáveis para aplicar as penalidades, quando necessário.	III. Analyze and prioritize the actions needed, balancing the cost and benefits. IV. Assist, whenever it is necessary, in the IS training process of HPGM's employees. V. Approve the investment in Cybersecurity at HPGM Group, in conjunction with the Head of IT, considering the feasibility and its impact on the quality of the business processes. VI. Analyze the cyber security incidents and submit a report to the appreciation of the Head of IT, whenever necessary. VII. Identify and assess the risks related to information security and propose improvements and resources that are necessary to mitigate risks. VIII. Perform analysis and tests, with the assistance of the IT Infrastructure team, aiming for potential flaws and impacts on IS and/or in the IT Infrastructure of the company. IX. Keep updated all the documents that are part of the ISMS. X. Propose processes and procedures related to information security in the HPGM Group. XI. Monitor access to the logical environments. XII. Evaluate the information security requirements that are present before the acquisition, maintenance, or software development. XIII. Ensure that the progress and the outcome of changes do not negatively impact the existing controls related to availability, integrity, confidentiality, authenticity, and legitimacy of that information, particularly on systems and Infrastructure. XIV. Request, as appropriate disciplinary actions for determining the responsibilities of those involved in the information security violations, deliberate the violations with the HR, Compliance and Legal Departments and notify the relevant parties to apply penalties, when necessary.
6.4 Encarregado pelo Tratamento de Dados Pessoais (DPO) | *Data Privacy Officer (DPO)*	
I. Assegurar que as medidas de segurança e organizacionais de proteção de dados estejam em vigor.	I. Ensure that data protection security and organizational measures are in place.

II. Assegurar que os funcionários do Grupo HPGM estejam cientes das políticas e práticas de privacidade de dados e recebam treinamento adequado sobre elas. III. Monitorar a conformidade com leis e regulamentações de privacidade e proteção de dados (como o GDPR, LGPD, CDPA e CCPA) com o apoio das áreas de Compliance e Jurídico e garantir que os processos internos estejam alinhados. IV. Estabelecer processos para atender aos pedidos dos indivíduos relacionados a seus direitos, como acesso, retificação, exclusão, oposição, portabilidade, entre outros. V. Fornecer orientação sobre avaliações de impacto, implementação de medidas de privacidade por design e padrão, e outras considerações relacionadas à privacidade.	II. Ensure that HPGM Group employees are aware of data privacy policies and practices and receive appropriate training on them. III. Monitor compliance with privacy and data protection laws and regulations (such as GDPR, LGPD, CDPA, and CCPA) with the support of the Compliance and Legal departments and ensure that internal processes are aligned. IV. Establish processes to address individual requests related to their rights, such as access, rectification, deletion, objection, portability, among others. V. Provide guidance on impact assessments, implementation of privacy by design and standard measures, and other privacy-related considerations.
6.5 Departamento Jurídico | *Legal Department*	
I. Participar, apoiar e orientar, de acordo com os aspectos jurídicos, os processos de contratação e as exigências legislativas relacionadas à segurança da informação; II. Redigir, revisar e atualizar os contratos com terceiros (como fornecedores e parceiros), para assegurar que as cláusulas de segurança da informação sejam abrangentes e vinculativas. III. Aconselhar sobre as implicações legais de qualquer incidente de segurança da informação e orientar a organização durante o processo de notificação a reguladores e partes afetadas. IV. Representar o Grupo HPGM em quaisquer litígios ou disputas que possam surgir devido a incidentes de segurança ou violações de contrato relacionadas à segurança da informação. V. Fornecer aconselhamento proativo as áreas do Grupo HPGM sobre riscos legais relacionados à segurança da informação.	I. Participate, support, and guide, in accordance with legal aspects, the contracting processes and legislative requirements related to information security. II. Draft, review, and update contracts with third parties (such as suppliers and partners) to ensure that information security clauses are comprehensive and binding. III. Advise on the legal implications of any information security incident and guide the organization through the notification process to regulators and affected parties. IV. Represent the HPGM Group in any litigation or disputes that may arise due to security incidents or contract breaches related to information security. V. Provide proactive advice to the areas of the HPGM Group on legal risks related to information security.
6.6 Departamento de Recursos Humanos | *Human Resource Department*	
I. Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores. II. Lidar com quaisquer incidentes de segurança que envolvam funcionários, como vazamentos de dados intencionais, e trabalhar em conjunto com a	I. Provide security controls specifically related to the processes of hiring, termination, and modification of the activities of the employees. II. Handle any security incidents involving employees, such as intentional data leaks, and collaborate with the Cybersecurity, Compliance, and Legal departments to investigate and resolve such incidents.

área de Cybersecurity, Compliance e Jurídico para investigar e resolver tais incidentes. III. Custodiar e colher assinatura do "Termo de Ciência e Responsabilidade" na admissão de novos colaboradores. IV. Assegurar e controlar que todos os colaboradores recebam treinamentos adequados e atualizados para manter a segurança da informação.	III. Ensure and obtain signatures on the 'Acknowledgment and Responsibility Agreement' upon the admission of new employees. IV. Ensure that all employees receive adequate and up-to-date training to maintain information security.
6.7 Departamento de Compliance | *Compliance Department*	
Garantir a publicidade e disponibilidade das Políticas e Procedimentos (P&Ps) que compõe o SGSI do Grupo HPGM que é coordenado por Comunicação Interna.	Ensure the publicity and availability of the Policies & Procedures that comprise the Information Security Management System of Grupo HPGM, which is coordinated by Internal Communications.
6.8 Departamento de Comunicação e Marketing | *Communication and Marketing Department*	
I. Autorizar ou não, o uso das marcas, identidade visual e qualquer outro sinal distintivo atual ou futuro do Grupo HPGM – nos usos internos e externos, visando garantir uso adequado do padrão vigente no Brand System, bem como autorização formal por uso da marca por algum fornecedor, seja para padronizar ferramentas, ou outros usos como nos referir como caso de sucesso ou referência, por exemplo. II. Dar suporte através de campanhas e divulgação relacionados ao tema segurança da informação – por meio do time de comunicação interna.	I. Authorize or deny the usage of trademarks, visual identity, and any other current or future distinctive sign of the HPGM Group - in internal and external uses, to ensure adequate use of current standards in the Brand System, as well as formally authorize the usage of the brand by a supplier, whether to standardize a tool or for other cases, such as commercial references. II. Carry out campaigns and dissemination of Information Security, through the internal communication team.
6.9 Gestor da Informação | *Information Owner*	
I. Autorizar ou não, a revelação de qualquer informação de propriedade ou sob a responsabilidade do Grupo HPGM; II. Identificar violações ou qualquer ação duvidosa praticada pelos colaboradores no uso da informação do Grupo HPGM e comunicar ao time de Cybersecurity e ao time do Compliance.	I. Authorize or deny, the disclosure of any information owned or under the responsibility of the HPGM Group. II. Identify violations or any questionable actions related to the usage of HPGM Group's information, such facts should be communicated to the Cybersecurity team and Compliance team.
6.10 Gestores, Coordenadores e Líderes | *Managers, Coordinators and Leaders*	
I. Garantir e gerenciar o cumprimento desta PSI e demais documentos complementares pelos seus colaboradores; II. Identificar as possíveis vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade,	I. Ensure and manage compliance with this ISP and with other complementary documents by their employees. II. Identify and assess potential vulnerabilities and threats in the processes and activities for which

as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio. III. Autorizar, ou não, a utilização de Recursos de TI ou dispositivos móveis particulares por seus colaboradores para execução de qualquer atividade profissional no Grupo HPGM. IV. Garantir que os ativos de propriedade ou sob a responsabilidade, sejam utilizados com cuidado e de acordo com as orientações do fabricante e da empresa; V. Aplicar, após definição com o Departamento de Recursos Humanos, Compliance e Jurídico, as sanções de violação desta PSI e documentos complementares; VI. Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por seus colaboradores, comunicando o cybersecurity@hedgepointglobal.com imediatamente.	they are responsible, which must be dealt with diligence to reduce impacts on the business. III. Authorize, or deny, the usage of IT resources or private mobile devices by their employees for the execution of any professional activity in the HPGM Group. IV. Ensure that assets owned or under HPGM's responsibility are used with care and following manufacturer and company guidelines. V. Apply, after agreement with Human Resources and Legal Departments, the sanctions for the violation of this PSI or complementary documents. VI. Identify information security incidents or any suspect action carried out by their employees, by communicating the mailbox cybersecurity@hedgepointglobal.com immediately.
6.11 Colaboradores, Estagiários | *Employees, Interns*	
I. Estar ciente e manter-se atualizado com esta PSI e demais documentos complementares; II. Conhecer e assinar o "Termo de Ciência e Responsabilidade"; III. Utilizar os ativos de propriedade do Grupo HPGM ou sob sua responsabilidade de acordo com as orientações do fabricante, do desenvolvedor e da empresa, com cuidado e zelo; IV. Utilizar os ativos e informações do Grupo HPGM somente para fins profissionais, de forma ética e legal, respeitando os direitos e as permissões de uso concedidas; V. Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na Internet; VI. Não revelar qualquer informação de propriedade ou sob a responsabilidade do Grupo HPGM sem a prévia e formal autorização; VII. Utilizar as marcas e outros sinais distintivos, patentes, desenhos industriais, softwares e demais direitos de propriedade intelectual de titularidade do Grupo HPGM somente para finalidades profissionais e autorizadas pela empresa, de acordo com a atividade e função exercida;	I. Be aware of and keep up to date with this ISP and other supplementary documents. II. Read and sign the "Term of Responsibility". III. Use the assets owned by the HPGM Group or under its responsibility following the guidelines of the manufacturer, developer, and the company with care. IV. Use the assets and information of HPGM Group for professional purposes only, ethically, and legally, respecting the rights and permissions of the granted usage. V. Preserve the integrity, availability, confidentiality, authenticity, and legality of the information accessed or manipulated by not using, sending, transmitting, or sharing it improperly in any location or media, including on the Internet. VI. Do not disclose any information owned or under the responsibility of the HPGM Group without prior and formal authorization. VII. Use the trademarks and other distinctive signs, patents, industrial designs, software, and other intellectual property rights owned by the HPGM Group for professional purposes and only when previously authorized by the company, according to the activity and function performed.

VIII. Zelar pela segurança da sua identidade digital, não compartilhando, divulgando ou transferindo a terceiros; IX. Responder por toda e qualquer atividade realizada nos Recursos de TI, mediante o uso de sua identidade digital; X. Cumprir as legislações listadas no Capítulo de Informações Gerais deste documento e demais instrumentos regulamentares relacionados às atividades profissionais; XI. Reportar formalmente ao seu Gestor quaisquer eventos relativos à violação ou possibilidade de violação de segurança ou atividades suspeitas.	VIII. Ensure the security of your digital identity by not sharing, disclosing, or transferring to third parties. IX. Be responsible for any activity carried out on the IT resources, through the usage of your digital identity. X. Comply with legislations listed in Chapter General Information of this document and other regulatory instruments related to professional activities. XI. Formally report to your manager any event related to the security breach or possibility of a security breach or any suspicious activity.

7. Penalidades | *Penalties*

I. **Violações:** Qualquer atividade que desrespeite as disposições estabelecidas nesta Política ou em quaisquer das Políticas Complementares do Grupo HPGM deve ser considerada como uma violação e tratada, a fim de apurar as responsabilidades dos envolvidos de acordo com as "Medidas Disciplinares", visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente; II. **Tentativa de Burla:** A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.	I. **Violations:** any activity that violates the rules established in this policy or in any of the complementary policies of the HPGM Group must be considered a violation and the involved parties will be subject to "disciplinary measures". In this case, contractual and legal sanctions might be applied. II. **Attempt of Fraud:** When detected, an attempt to bypass established guidelines and controls should be treated as a violation.

8. Considerações Finais | *Final Considerations*

I. Esta Política deve ser revisada, no mínimo, a cada 12 (doze) meses, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais políticas específicas do Grupo HPGM. II. Documentos e arquivos pessoais, não devem ser armazenados nos equipamentos da HPGM. Todos os arquivos hospedados nos bancos de dados ou equipamentos serão considerados dados de propriedade da HPGM, sendo a transferência de arquivos constantemente monitorada. III. Este documento, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Departamento de Cybersecurity. IV. Consideramos evento de incidente operacional, qualquer situação que tenha ocorrido e que possa ocasionar problemas na execução dos processos relacionados a esta Política Corporativa. São exemplos de Eventos de Incidente Operacional:	I. This policy should be reviewed at least every twelve (12) months or whenever there is a need for changes on the criteria defined in the other specific policies of the HPGM Group. II. Personal documents and files should not be stored on HPGM equipment. All files hosted on our databases or equipment will be considered property of HGPM, with file transfers being constantly monitored. III. This document and the other documents that complement it are available on the intranet or, in case of unavailability, can be requested to the Cybersecurity Department. IV. We consider an operational incident event, any situation that has occurred and that may cause problems in the execution of the processes related to this Corporate Policy. Examples of Operational Incident Events are system unavailability, information integrity issues, typing errors, and others. Every event shall be reported, despite the

indisponibilidade de sistemas, problemas na integridade da informação, erros de digitação e outros. Todo evento deverá ser reportado, independente da sua correlação com perda financeira, ao Gerente responsável pelo processo e as Áreas de Compliance e Risco para o adequado tratamento, classificação e eventual reporte em níveis de alçada superior.	consequences of its association with financial loss, to the Manager responsible for the process and to the Compliance and Risk Areas for the appropriate treatment, classification, and eventual reporting at higher levels.