INFORMATION SECURITY AND CYBERSECURITY POLICY

Introduction

Nomad offers financial and technology services in a digital environment, where information security and cybersecurity are essential to protect data, ensure service continuity, and maintain the trust of clients and partners.

This Information Security and Cybersecurity Policy ("Policy") sets forth general guidelines intended to promote transparency and guide clients, partners, vendors, suppliers, and other third parties regarding data protection and the integrity of services.

Scope

This Policy applies to Nomad Investment Services Inc., Nomad Wealth Management Ltda., Nomad Tecnologia e Participações Ltda., Nomad Fintech, Inc., as well as their affiliates, which together constitute the "Nomad Group."

For purposes of this Policy, all entities within the Nomad Group are considered in an integrated manner, reflecting their coordinated role in the provision of financial, technological, and operational services, as well as in data processing and the management of environments, systems, and information.

This Policy covers the data, information, systems, and services offered

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Introdução

A Nomad atua na oferta de serviços financeiros e tecnológicos em ambiente digital, no qual a segurança da informação e a cibersegurança são essenciais para a proteção de dados, a continuidade dos serviços e a confiança de clientes e parceiros.

Esta Política de Segurança da Informação e Cibersegurança ("Política") estabelece diretrizes gerais, com objetivo de promover transparência e orientar clientes, parceiros, fornecedores e demais terceiros quanto à proteção de dados e à integridade dos serviços.

Escopo

Esta Política aplica-se à Nomad Investment Services Inc., à Nomad Wealth Management Ltda., à Nomad Tecnologia e Participações Ltda., à Nomad Fintech, Inc., bem como às suas afiliadas, que, em conjunto, constituem o "Grupo Nomad".

Para fins desta política, todas as entidades do Grupo Nomad são consideradas de forma integrada, refletindo a atuação coordenada na prestação de serviços financeiros, tecnológicos e operacionais, bem como no tratamento de dados e na gestão de ambientes, sistemas e informações.

Esta Política abrange os dados, informações, sistemas e serviços oferecidos

and made available by the Nomad Group, including where third parties or strategic partners are involved.

Target Audience

This Policy is intended for clients, users, partners, vendors, service providers, and other third parties that interact with the Nomad Group's services, systems, data, or environments.

Clients and users must observe the security recommendations applicable to their use of the services, while partners, vendors, and third parties with access to Nomad data or environments must adopt appropriate information security and cybersecurity practices consistent with the risks involved.

Compliance with this Policy forms part of the relationship with the Nomad Group, including the expectation of cooperation in the prevention, identification, and handling of security incidents that may affect services, data, or operations.

Information Security and Cybersecurity Objectives

Nomad seeks to protect data, information, and services by preserving their confidentiality, integrity, and availability in a manner consistent with the sensitivity of the assets and the risks involved in its operations.

Nomad's information security and cybersecurity activities are guided by the identification and prioritization of risks,

e disponibilizados pelo Grupo Nomad, inclusive quando envolverem terceiros ou parceiros estratégicos.

Público-alvo

Esta política destina-se a clientes, usuários, parceiros, fornecedores, prestadores de serviço e demais terceiros que interajam com os serviços, sistemas, dados ou ambientes do Grupo Nomad.

Clientes e usuários devem observar as recomendações de segurança aplicáveis à utilização dos serviços, enquanto parceiros, fornecedores e terceiros com acesso a dados ou ambientes da Nomad devem adotar práticas adequadas de segurança da informação e cibersegurança, compatíveis com os riscos envolvidos.

A observância desta política integra a relação com o Grupo Nomad, incluindo a expectativa de cooperação na prevenção, identificação e tratamento de incidentes de segurança que possam impactar serviços, dados ou operações.

Objetivos de Segurança da Informação

A Nomad busca proteger dados, informações e serviços, preservando sua confidencialidade, integridade e disponibilidade de forma compatível com a sensibilidade dos ativos e com os riscos envolvidos em suas operações.

A atuação em segurança da informação e cibersegurança é orientada pela identificação e priorização de riscos, com o objetivo de reduzir impactos sobre clientes, parceiros, operações e serviços.

with the objective of reducing impacts on clients, partners, operations, and services.

Nomad seeks to preserve the continuity of its activities and the trust of clients and partners.

The protection of services and information involves shared responsibility among Nomad, its clients, and third parties that interact with its environments, systems, or data.

A Nomad busca preservar a continuidade de suas atividades e a confiança de clientes e parceiros.

A proteção dos serviços e das informações envolve responsabilidade compartilhada entre a Nomad, seus clientes e terceiros que se relacionem com seus ambientes, sistemas ou dados

How Nomad Protects Information, Systems, and Services

Nomad adopts controls to protect data and information throughout their processing, including measures consistent with their sensitivity and context of use, such as information classification, network filtering, encryption at rest and in transit, antivirus protection, and data loss prevention solutions.

Nomad restricts and manages access to systems, services, and information based on authentication, authorization, permission reviews, segregation of duties, and least-privilege principles.

Nomad monitors its technological environments to identify relevant security events and adopts incident response and escalation procedures in situations that may compromise data, services, or operations.

Nomad incorporates security practices into the development and evolution of systems, as well as into the identification, prioritization, and remediation of vulnerabilities.

Como a Nomad protege informações, sistemas e serviços

A Nomad adota controles para proteção de dados e informações ao longo de seu tratamento, incluindo medidas compatíveis com sua sensibilidade e com o contexto de uso, como classificação de informação, filtros de rede, criptografia em repouso e em trânsito, uso de antivírus e soluções de prevenção à perda de informação.

A Nomad restringe e gerencia o acesso a sistemas, serviços e informações com base em autenticação, autorização, revisão de permissões, segregação de funções e minimização de privilégios.

A Nomad monitora seus ambientes tecnológicos para identificar eventos relevantes de segurança e adota procedimentos de resposta e escalonamento de incidentes diante de situações que possam comprometer dados, serviços ou operações.

A Nomad incorpora práticas de segurança no desenvolvimento e na evolução de sistemas, bem como na

Nomad promotes information security and cybersecurity training and awareness initiatives for employees and third parties, with the aim of reinforcing secure behaviors and supporting incident prevention.

Nomad performs cyber assessments of relevant vendors and partners, taking into account the risks associated with the services provided and with access to data, systems, or environments.

Nomad adopts resilience and continuity measures to reduce the impact of failures or adverse events, including backups, resource redundancy, and recovery mechanisms appropriate to its services and operations.

identificação, priorização e tratamento de vulnerabilidades.

A Nomad promove treinamentos e ações de conscientização em segurança da informação e cibersegurança para colaboradores e terceiros, com o objetivo de fortalecer comportamentos seguros e apoiar a prevenção de incidentes.

A Nomad realiza avaliações cibernéticas de fornecedores e parceiros relevantes, considerando os riscos associados aos serviços prestados e ao acesso a dados, sistemas ou ambientes.

A Nomad adota medidas de resiliência e continuidade para reduzir impactos de falhas ou eventos adversos, incluindo cópias de segurança, redundância de recursos e mecanismos de recuperação adequados aos seus serviços e operações.

Risk Management, Governance, and Compliance

Nomad conducts information security and cybersecurity based on a structured risk management approach, considering threats, vulnerabilities, potential impacts, and the criticality of its services and operations.

Nomad maintains a governance structure focused on the definition, oversight, and continuous evolution of guidelines, controls, and responsibilities related to information security and cybersecurity.

Nomad observes legal, regulatory, and contractual requirements applicable to its operations, as well as recognized market

Gestão de riscos, governança e conformidade

A Nomad conduz a segurança da informação e a cibersegurança com base em uma abordagem estruturada de gestão de riscos, considerando ameaças, vulnerabilidades, impactos potenciais e a criticidade de seus serviços e operações.

A Nomad mantém uma estrutura de governança voltada à definição, supervisão e evolução de diretrizes, controles e responsabilidades relacionadas à segurança da informação e à cibersegurança.

A Nomad observa requisitos legais, regulatórios e contratuais aplicáveis às suas operações, bem como práticas reconhecidas de mercado, como parte do fortalecimento contínuo de sua postura de segurança.

practices, as part of the continuous strengthening of its security posture.

Nomad periodically reviews its security processes, controls, and guidelines, taking into account changes in the technological environment, regulatory context, and threat landscape.

A Nomad revisa periodicamente seus processos, controles e diretrizes de segurança, considerando mudanças no ambiente tecnológico, no contexto regulatório e no cenário de ameaças.

Relationship with Partners, Vendors, and Third Parties

Nomad expects partners, vendors, service providers, and other third parties that process data, access systems, or operate in environments related to its services to adopt appropriate information security and cybersecurity practices, consistent with the nature of the activities performed and the risks involved.

Nomad may conduct security assessments proportionate to the risk of the relationship, especially where there is data processing, access to confidential information, support for critical operations, or activity in technological environments relevant to service delivery.

Partners, vendors, and third parties must protect the information and access credentials under their responsibility, observing applicable requirements for confidentiality, integrity, availability, and proper use of the resources involved in the performance of contracted services.

Whenever they identify incidents, suspected compromise, or situations that may affect data, systems, services, or operations related to Nomad, partners, vendors, and third parties must promptly report the occurrence through the channels defined by Nomad and cooperate with

Relacionamento com parceiros, fornecedores e terceiros

A Nomad espera que parceiros, fornecedores, prestadores de serviço e demais terceiros que tratem dados, acessem sistemas ou atuem em ambientes relacionados aos seus serviços adotem práticas adequadas de segurança da informação e cibersegurança, compatíveis com a natureza das atividades desempenhadas e com os riscos envolvidos.

A Nomad pode realizar avaliações de segurança proporcionais ao risco do relacionamento, especialmente quando houver tratamento de dados, acesso a informações confidenciais, suporte a operações críticas ou atuação em ambientes tecnológicos relevantes para a prestação dos serviços.

Parceiros, fornecedores e terceiros devem proteger as informações e os acessos sob sua responsabilidade, observando requisitos aplicáveis de confidencialidade, integridade, disponibilidade e uso adequado dos recursos envolvidos na execução dos serviços contratados.

Sempre que identificarem incidentes, suspeitas de comprometimento ou situações que possam afetar dados, sistemas, serviços ou operações relacionados à Nomad, parceiros, fornecedores e terceiros deverão

analysis, containment, response, and impact mitigation actions.

Compliance with these duties forms part of the relationship maintained with the Nomad Group and complements applicable contractual, regulatory, and legal obligations.

comunicar a ocorrência de forma tempestiva pelos canais definidos pela Nomad, colaborando com as ações de análise, contenção, resposta e mitigação dos impactos.

A observância desses deveres integra a relação mantida com o Grupo Nomad e complementa as obrigações contratuais, regulatórias e legais aplicáveis.

Security Recommendations for Customers and Users

Nomad recommends that clients and users adopt security practices appropriate to the use of digital services, including protecting credentials, using strong and unique passwords, enabling additional authentication mechanisms whenever available, and remaining alert to communications, links, or suspicious requests that may indicate fraud, social engineering, or phishing attempts.

It is also recommended to keep devices and applications up to date, use trusted networks and devices, and avoid sharing sensitive information, authentication codes, or access credentials with third parties.

The adoption of these practices contributes to data protection, transaction integrity, and the safer use of services made available by the Nomad Group.

Recomendações de segurança para clientes e usuários

A Nomad recomenda que clientes e usuários adotem práticas de segurança compatíveis com o uso de serviços digitais, incluindo a proteção de credenciais, o uso de senhas fortes e exclusivas, a ativação de mecanismos adicionais de autenticação quando disponíveis e a atenção a comunicações, links ou solicitações suspeitas que possam indicar tentativa de fraude, engenharia social ou phishing.

Também é recomendável manter dispositivos e aplicações atualizados, utilizar redes e equipamentos confiáveis e evitar o compartilhamento de informações sensíveis, códigos de autenticação ou credenciais de acesso com terceiros.

A adoção dessas práticas contribui para a proteção dos dados, para a integridade das transações e para a utilização mais segura dos serviços disponibilizados pelo Grupo Nomad.

Final Provisions

This Policy may be reviewed and updated periodically in order to reflect changes in the regulatory, technological, or operational environment, or in the threat landscape applicable to the activities of the Nomad Group.

This Policy complements applicable legal, regulatory, and contractual obligations and must be interpreted together with the other documents and instruments governing the relationship between Nomad and its clients, partners, vendors, suppliers, and third parties, where applicable.

This Information Security and Cybersecurity Policy was last updated on April 10, 2026.

Disposições finais

Esta Política poderá ser revisada e atualizada periodicamente, de modo a refletir mudanças no ambiente regulatório, tecnológico, operacional ou no cenário de ameaças aplicável às atividades do Grupo Nomad.

A presente Política complementa obrigações legais, regulatórias e contratuais aplicáveis, e deve ser interpretada em conjunto com os demais documentos e instrumentos que regem a relação entre a Nomad, seus clientes, parceiros, fornecedores e terceiros, quando aplicável.

Esta Política de Segurança da Informação e Cibersegurança foi atualizada pela última vez em 10 de abril de 2026.