NovaMente Soluções Cognitivas

Document 13 — Information Security Policy

Version 1.0 · January 2025 · HR & Culture Department

Introduction

NovaMente handles sensitive data at the core of its business — including mental health data processed through MindFlow, employee personal information, client contracts, and proprietary technology. The security of this information is not only a legal obligation under the LGPD and applicable data protection standards; it is a fundamental element of the trust that our clients, employees, and end users place in us. A single significant breach could cause real harm to individuals and irreparable damage to NovaMente's reputation. This policy defines how we protect information assets across the organization.

Classification of Information

NovaMente classifies information into four categories, each with corresponding handling requirements. **Public** information is approved for external distribution — marketing materials, published research, and public product documentation. **Internal** information is intended for NovaMente employees and authorized contractors only — policies, internal communications, and business processes. **Confidential** information is restricted to specific roles and teams — client contracts, financial results, personnel data, and strategic plans. **Restricted** information represents the highest sensitivity — source code, security credentials, encryption keys, and individually identifiable health data. Each level requires progressively more stringent access controls, transmission protocols, and storage requirements.

Access Control

Access to systems and information is granted on the principle of least privilege: employees receive access to the minimum set of systems and data necessary to perform their role. Access is provisioned by the Engineering team during onboarding, based on a role-access matrix maintained by the Engineering Head and the Legal team. All access requests beyond a role's default permissions must be submitted to the Engineering team with a documented justification and approval from the employee's department head.

Access is reviewed quarterly. When an employee changes roles or departs, their access is updated or revoked within one working day. The Engineering team maintains an audit log of access provisioning and deprovisioning. Former employees must have all access revoked on or before their last working day.

Authentication Standards

All NovaMente systems require authentication with a strong, unique password. Password reuse across systems is prohibited. Multi-factor authentication (MFA) is mandatory for all critical systems, including the product infrastructure, the HR system, the financial system, and any system that handles Restricted or Confidential data. NovaMente provides a company-managed password manager to all employees to facilitate compliance with these requirements.

Device and Endpoint Security

All company-issued devices must be configured in accordance with the standard security baseline maintained by the Engineering team. This includes full-disk encryption, automatic screen lock after five minutes of inactivity, up-to-date operating system and application patches, and endpoint protection software. Employees must not disable or circumvent any security controls on company devices.

The use of personal devices to access NovaMente systems is permitted only through the approved secure access method defined by the Engineering team, and only for Internal-classified information or below. Personal devices must not be used to access Confidential or Restricted information. If an employee's personal device is lost or stolen and was used to access NovaMente systems, they must notify the Engineering team immediately so that remote wipe procedures can be initiated if necessary.

Data Transmission and Storage

Confidential and Restricted information must only be transmitted over encrypted channels. Email is not an approved channel for transmitting Restricted information. Approved file sharing and collaboration platforms are defined by the Engineering team and listed in the internal knowledge base. Employees must not transmit sensitive information via personal email, consumer-grade messaging applications, or any unapproved third-party service.

Data must be stored in approved company systems. Storing Confidential or Restricted information in personal cloud storage accounts, personal devices, or unapproved systems is prohibited. When physical documents containing sensitive information must be destroyed, they must be shredded rather than discarded in general waste.

Incident Response

All employees have a responsibility to report actual or suspected security incidents immediately. This includes phishing attempts, malware infections, unauthorized access, device loss or theft, and accidental disclosure of sensitive information. Reports should be made to the Engineering team's security contact and the Legal team without delay. The Engineering team maintains an incident response procedure that defines the response steps, escalation path, and notification obligations for each category of incident.

Employees must not attempt to investigate or remediate a security incident independently. They should report it and follow the Engineering team's instructions. Attempting to cover up or delay reporting a security incident is a serious violation of this policy.

Security Awareness and Training

All employees complete security awareness training during onboarding and annually thereafter. The training covers the most common threats — phishing, social engineering, password attacks, and insider risk — and the behaviors that protect against them. The Engineering team also sends periodic security advisories when new threats or vulnerabilities become relevant. Employees are expected to read and act on these advisories promptly.