Information Security Policy

MiracleDevs

Information Security Policy

Miracle Devs - V1 - 16/11/2022

Information security is a fundamental pillar of the work we do at Miracle Devs. Our clients, internal collaborators, and suppliers trust us to keep their data safe and available, and we are committed to honoring that trust. To order, structure, monitor, and ensure the confidentiality, integrity, and availability of information, we implement and maintain an information management system, in accordance with the ISO 27001:2013 standard. The set of policies, procedures, and evidence collection that is part of our ISMS helps us ensure information security, manage risks, achieve continuous improvement, and pursue the integral growth of our organization.

Every person or organization that receives access to Miracle Devs' digital assets is also responsible for their care and proper use. For this, it is essential to be familiar with the general guidelines of our ISMS, starting with this Information Security Policy.

The internal authority responsible for Miracle Devs' security is the Information Security department. Any incident reports, requests for clarification, or security-related inquiries should be made through that department and its representatives.

1. Inventory and Classification of Assets

It is important to consider that all Miracle Devs' assets, whether physical devices, files, documents, code repositories, or databases, are inventoried and classified in our ISMS.

2. Passwords and MFA

Passwords must comply with the practices detailed in the corresponding access control policy. Likewise, two-step authentication or MFA must be enabled for all services that allow it.

3. Phishing y Malware

Antivirus and other preventive mechanisms against such attacks will be automatically updated on the company's devices. Likewise, people must take precautions not to fall victim to phishing attacks or other forms of social engineering attacks.

4. Security Practices in Development

Any developer working on code for production environments must be familiar with the Secure Development policy. The guidelines and tools established in that document will be used as a security standard to evaluate both internal projects and third-party code.

5. Training

Miracle Devs will maintain a periodic training space on security topics, both at the code level and at the general level to prevent phishing, malware, or other attacks.

6. Risk Analysis and Incident Treatment

As part of our ISMS, our job is to continuously analyze the risks associated with our information assets and manage them properly by establishing the necessary controls. Although the Information Security team is responsible for this task, all stakeholders related to digital assets can collaborate by reporting and informing about perceived risks or threats.

In case of suspicion or certainty of a security incident involving company assets, it is necessary to notify the Information Security department promptly.

Each of these aspects is developed in detail in its corresponding policy. This document aims to establish the general guidelines of Miracle Devs' ISMS and does not replace the need for each area to familiarize itself with its specific policies, as well as the processes and evidence collection mechanisms.

The responsibility of keeping the company's assets safe ultimately lies with the people and organizations that access them on a daily basis. Using best practices, knowing our ISMS, and exercising carefulness and consideration in resource management are fundamental aspects of becoming the company we want to be.

Nicolás Badano
CEO Miracle Devs