BioHealth

Systems

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FRAMEWORK

This document is a simplified version for technical portfolio demonstration purposes, focusing on strategic structure and alignment with COBIT, ISO, or ITIL frameworks.

BioHealth

Systems

Company Name: BioHealth Systems

Document Type: Information Security Management System (ISMS) Framework

Reference Framework: ISO/IEC 27001:2022

Introduction

This document defines the information security governance model adopted by BioHealth Systems to protect its critical assets and ensure compliance with healthcare regulations (LGPD).

Leadership and Commitment

Information security at BioHealth is not just a technical function, but a responsibility of senior management.

- **ISP Approval:** The Information Security Policy (ISP) is reviewed and approved annually by the CEO.
- **Resources:** The organization is committed to allocating a specific budget for protection tools and staff training.

BioHealth
Systems

Security Policy Framework

BioHealth's ISMS consists of a hierarchical structure of documents:

- **Information Security Policy (Master Guideline):** General rules for all employees.
- **Specific Standards:**
  - Access Control Policy (Based on the “Least Privilege” principle).
  - Encryption Policy (For data at rest and in transit).
  - Acceptable Use Policy (Guidelines for using company devices).
- **Procedures (SOPs):** Step-by-step technical manuals (e.g., How to reset a password).

Selection of Controls (Based on Annex A of ISO 27001)

As a result of the risk analysis (Project 3), we prioritized the following control domains:

- **Organizational Controls:** Asset management and security in supplier relationships.
- **People Controls:** Onboarding process with security awareness training.
- **Physical Controls:** Restricted access to server rooms and medical record areas.
- **Technological Controls:** Implementation of Endpoint Detection and Response (EDR) and Vulnerability Management.

● Continuous Improvement (PDCA Cycle)

The ISMS operates under the PDCA cycle to ensure constant evolution:

- **Plan:** Define security objectives and assess risks.
- **Do:** Implement policies and controls.
- **Check:** Conduct internal audits and monitor incidents.
- **Act:** Correct failures and update processes based on results.

BioHealth
Systems

Success Indicators (SGSI Metrics)

- Percentage of employees trained in security (Target: 100%).
- Average time to detect critical vulnerabilities.
- Number of security incidents with financial or legal impact.

BioHealth

Systems

Disclaimer

This document represents a fictional case developed for professional and educational purposes and does not reflect any real organization.