Cybersecurity Policy

Index

1. INTRODUCTION

Fundação Mendes Gonçalves (Foundation Mendes Gonçalves) and Casa MG have approved this Cybersecurity Policy (hereinafter, the "Policy") in recognition of the fact that cybersecurity is a fundamental pillar for the protection of digital assets, sensitive data and operational continuity of both Fundação Mendes Gonçalves and Casa MG, and in acknowledgment ofthe growing sophistication of cyberattacks.

The purpose of this Policy is to clearly and unequivocally establish the principles, guidelines and approach adopted by Fundação Mendes Gonçalves e Casa MG regarding the management of cybersecurity risks, which are intrinsic to its activity and operations, in order to ensure the continuity, integrity and confidentiality of the organisations' data and systems.

Fundação Mendes Gonçalves and Casa MG are committed to the adoption of best cybersecurity and data protection practices, in accordance with relevant national and international laws, regulations and guidelines, including the National Cybersecurity Framework and the General Data Protection Regulation (GDPR), ensuring that all its operations and processes are compliant with relevant legal and regulatory standards. The policy also aims to support the achievement of the organization's strategic objectives, promoting a safe and resilient environment, that favours the trust of customers and beneficiaries, employees and partners.

2. SCOPE OF APPLICATION

This policy applies to all employees of Fundação Mendes Gonçalves and of all entities of Casa MG (members of governing bodies and departments, as well as to the persons at the service of Fundação Mendes Gonçalves and Casa MG under employment contracts, internship contracts or of any other nature) and all its partners (Clients or Beneficiaries, Suppliers and Service Providers) who have access to systems, networks, devices and data of Fundação Mendes Gonçalves and Casa MG.

The guidelines established herein cover the entire Information Technology (IT) infrastructure of Fundação Mendes Gonçalves and Casa MG, namely:

- **Digital services and applications**, such as management platforms, Enterprise Resource Planning (ERP) systems, CRM (Customer Relationship Management) and specialized software used in the organisations;
- **Devices**, such as computers, servers, mobile devices, tablets, printers and any other equipment that accesses or stores data of the organisations;

- **Network infrastructure and connectivity**, including Firewalls, Virtual Private Networks (VPNs), physical and virtual servers, Wi-Fi networks, network segmentation, and security devices;
- **Remote and hybrid work environments**, ensuring that external access to the organisations' network follows established security protocols;
- **Data storage and management**, covering local and cloud databases, backup solutions and data retention policies;
- **Digital means of communication**, such as organisations' emails, videoconferencing tools, instant messaging applications, and file sharing.

3. SECURITY OBJECTIVES

To fulfil their commitment to the promotion of cybersecurity and information security, Fundação Mendes Gonçalves and Casa MG have adopted the following Security Objectives:

Identify	• Understand the context of Fundação Mendes Gonçalves and Casa MG, of the assets that support the critical processes of its activity and the relevant associated risks.
Protect	• Implement measures to protect the organisational processes and assets of Fundação Mendes Gonçalves and Casa MG, regardless of their technological nature.
Detect	• Define and implement measures aimed at identifying incidents in a timely manner, i.e. real adverse effects on the security of networks and information systems.
Respond	• Define and implement appropriate action measures if an incident is detected.
Recover	• Define and implement activities aimed at managing recovery plans and measures for processes and services affected by a cybersecurity incident.

To this end, Fundação Mendes Gonçalves and Casa MG have internally defined a ***framework* of responsibilities,** composed of the respective Boards of Directors, the Chief Information Security Officer (CISO) appointed by the Administration, Mendes Gonçalves - Sistemas e Tecnologias de Informação, Lda. and external service providers.

4. IDENTIFY

This objective is related to the identification by Fundação Mendes Gonçalves and Casa MG of the different dimensions of their organisations, in terms of their networks and information systems, people, assets and data.

Thus, to achieve this security objective, both are committed to:

- ✓ **identify and classify information assets** (data, employees, equipment, systems and facilities) according to their relevance and criticality to the activities of Fundação Mendes Gonçalves and Casa MG, so that they can be adequately protected throughout their life cycle;
- ✓ **identify and typify suppliers**, namely suppliers that are considered critical by Fundação Mendes Gonçalves and Casa MG, and ensure that they fit the needs and requirements of Cybersecurity;
- ✓ **identify, assess and treat the Cybersecurity risks inherent to the activity** of Fundação Mendes Gonçalves and Casa MG and to which their assets are exposed;
- ✓ **establish a procedure for identifying, assessing and treating risk** in accordance with the risk tolerance of Fundação Mendes Gonçalves and Casa MG.

Fundação Mendes Gonçalves and Casa MG believe in a process of continuous improvement of their procedures, policies, plans and processes in the light of the updating of good practices in the industry and the foundational sector and international cybersecurity references and standards. Considering this, the **Identify** objective also aims to (i) promote implementing strategies for improvement opportunities , namely proposals resulting from audits, penetration tests or other internal or external projects in the field of Cybersecurity and (ii) define indicators that support Cybersecurity reporting models to be presented internally to the CISO and, when applicable, to other governing bodies of Fundação Mendes Gonçalves and Casa MG.

5. PROTECT

The **Protect** objective aims to develop and implement safeguards necessary for the development of the activity of Fundação Mendes Gonçalves and Casa MG, allowing them to limit or

contain the impact of the occurrence of a cybersecurity incident. To this end, Fundação Mendes Gonçalves and Casa MG recognize the need to:

- ✓ **establish and implement controls to protect the information assets** of Fundação Mendes Gonçalves and Casa MG from theft, intrusion, abuse or other forms of unlawful treatment;
- ✓ **ensure the availability and reliability of the equipment, infrastructures and** systems that support the activity of Fundação Mendes Gonçalves and Casa MG;
- ✓ **promote a culture of awareness and commitment to Cybersecurity** among members of the Board of Directors, Department Heads and Employees, motivating them to become aware of and take responsibility for their intervention, to minimize the risk of information security incidents;
- ✓ **ensure the protection of personal data**, under the terms provided for in the applicable legislation;
- ✓ **promote the sharing of relevant information on Cybersecurity**, through secure and timely channels, with stakeholders from Fundação Mendes Gonçalves and Casa MG, official entities and other interest groups;
- ✓ **contribute to the generalization of Cybersecurity awareness.**

Fundação Mendes Gonçalves and Casa MG have implemented a set of protection measures for the protection of equipment, systems and networks:

5.1. Network Segmentation and Protection

Network segmentation is essential to prevent the spread of threats and unauthorized access. Fundação Mendes Gonçalves and Casa MG have also implemented *firewalls* in order to filter traffic, block malicious access and prevent denial of service attacks, namely DoS (**Denial of Service**)[1] and DDoS (**Distributed Denial of Service**)[2] attacks, such as IDS (**Intrusion Detection System**)[3] and IPS (**Intrusion Prevention System**).[4]

[1] A DoS attack occurs when a system, service, or network is overloaded with malicious traffic, making it inaccessible to legitimate users. This can be done by sending a large volume of requests or by exploiting system vulnerabilities.

[2] DDoS attack is a variation of DoS, but carried out from multiple sources simultaneously, usually through a botnet (network of compromised devices). This makes the attack harder to block as it comes from multiple locations at once.

[3] An IDS monitors networks and systems for suspicious or malicious activity. It alerts security administrators, but it does not directly interfere with network traffic.

[4] An IPS goes beyond the IDS by automatically blocking suspicious or malicious activity as soon as it is detected. It can stop the spread of attacks before they cause damage.

5.2. Authentication and Remote Access

Fundação Mendes Gonçalves and Casa MG adopt a robust security model for remote access, based on Multi-Factor Authentication (MFA) and VPN with advanced encryption. At Fundação Mendes Gonçalves and Casa MG, VPN is mandatory for any remote access to the organisations' systems, preventing direct accesses that may compromise network security and ensuring a protected digital environment for Employees and partners. All data that travels over this connection is encrypted with advanced protocols.

5.3. Device and Software Management

All devices used by Employees – including computers, laptops, corporate smartphones and tablets – are provided, configured and managed exclusively by the IT Department common to Fundação Mendes Gonçalves and Casa MG, which ensures that strict security standards are applied to all hardware and software used in the corporate environment. The use of personal devices to access the corporate network is strictly prohibited, following the "No BYOD" (No Bring Your Own Device) policy. This restriction is essential to reduce security risks, ensuring that all devices that access the systems of Fundação Mendes Gonçalves and Casa MG are properly controlled and protected against cyber threats, malware and unauthorized access.

5.4. Physical Access Control

Access to critical areas is restricted and controlled by biometric authentication and MIFARE cards - smart card technology based on Radio Frequency Identification, ensuring that only authorized Employees can enter sensitive or restricted access locations. The entire physical infrastructure is also monitored by closed-circuit television (CCTV) cameras 24/7, and security teams carry out surveillance rounds to prevent improper access.

5.5. Control of System Updates

Fundação Mendes Gonçalves and Casa MG have implemented a program that allows controlling which updates are installed on each computer, ensuring that all systems are up to date and protected against security vulnerabilities.

5.6. Management of Sensitive Data and Information

Fundação Mendes Gonçalves and Casa MG store the sensitive data to which they have access in a safe and secure manner, including financial and strategic information. The retention of this data follows strict guidelines, ensuring that the information is stored only for as long as necessary and permanently deleted after this period in accordance with all legislation in force.

6. DETECT

The **detection** of the occurrence of cybersecurity events depends on the continuous monitoring of networks and information systems and the implementation of detection processes. To achieve this goal, Fundação Mendes Gonçalves and Casa MG are committed to:

- ✓ **monitor Cybersecurity anomalies and events, in a timely manner, and understand the potential impact** of these events;
- ✓ **continuously monitor networks and information systems** to identify cybersecurity events and verify the effectiveness of the protection measures applied;
- ✓ **implement and maintain anomalous event detection processes**;
- ✓ **evaluate the effectiveness of the controls** implemented at the Fundação Mendes Gonçalves and Casa MG to mitigate the **identified risks;**
- ✓ **identify and mitigate vulnerabilities and opportunities for improvement in the infrastructure** of Fundação Mendes Gonçalves and Casa MG.

6.1. Periodic scans and auditing

The detection and mitigation of vulnerabilities in the systems of Fundação Mendes Gonçalves and Casa MG are carried out by performing periodic **scans of their systems and networks and continuous monitoring** of their networks and information systems.

Fundação Mendes Gonçalves and Casa MG conduct regular audits of their systems, processes and technological infrastructures to ensure that all safety guidelines are met effectively. These audits aim to ensure compliance with internal cybersecurity policies, identify opportunities for continuous improvement, detect and correct vulnerabilities before they can be exploited by cyber threats, and assess the effectiveness of data protection measures.

6.2. Protection mechanisms

Detection also results from the mechanisms adopted in relation to the *Protect* objective and which allow the timely detection of the occurrence of cybersecurity events.

6.3. Formation and establishment of reporting channels

For enhancing the ability to detect incidents, all Employees of Fundação Mendes Gonçalves and Casa MG receive training to be able to identify phishing attempts and social engineering attacks, and to report any suspicious e-mail to the company Mendes Gonçalves – Sistemas e Tecnologias de Informação, Lda., immediately.

7. RESPOND

Fundação Mendes Gonçalves and Casa MG recognize that timely response to security incidents is paramount to mitigate the impact of security incidents and ensure compliance with legal or regulatory requirements.

The security objective **Respond** corresponds to the commitment to develop and implement practices in this regard and, to this end, Fundação Mendes Gonçalves and Casa MG commit to:

- ✓ **plan the response to detected incidents**;
- ✓ **ensure that information security incidents are reported** in accordance with the legislation in force and with the internal procedures defined for this purpose;
- ✓ **ensure that the analysis of incidents allows for effective response** and support for the recovery activities;
- ✓ **make best efforts to contain, mitigate and/or resolve the incident that has occurred;**
- ✓ **reduce the damage to the activity inherent to the occurrence of information security incidents**, as well as minimize their impact on the stakeholders of Fundação Mendes Gonçalves and Casa MG (internal and external);
- ✓ **accumulate experience and promote the continuous improvement of** cybersecurity incident response processes.

The CISO will be dedicated to monitoring these topics, strengthening its commitment to the protection of information security. The response process is ensured by an external service provider that offers Fundação Mendes Gonçalves and Casa MG a robust response plan.

8. RECOVER

The **Recover** objective is marked by the commitment to develop and implement practices to restore any capacity and/or service of Fundação Mendes Gonçalves and Casa MG that has been compromised following a cybersecurity event, with a view to reducing the impacts of the incident that occurred. Thus, to achieve the objective of safety, Fundação Mendes Gonçalves and Casa MG undertake to:

- ✓ **ensure that has the capacity to continue the provision of its services**, including its critical business functions, in the event of serious information security incidents or cyberattacks, under the conditions defined in the applicable regulations, standards and specific procedures;
- ✓ **ensure the redundancy of equipment, infrastructures and information systems** that support critical activity and business functions, thus avoiding single points of failure;

- ✓ **minimize the negative impacts** that may arise from the occurrence of serious security incidents, both for the reputation of the organisations and for all their stakeholders.

In this context, Fundação Mendes Gonçalves and Casa MG have developed a robust **backup policy** and strategy, which ensure the continuous protection of essential information, ensuring that both can recover data quickly and maintain their uninterrupted operations, even in the face of adverse scenarios. These include:

- ✓ Add critical system configurations to backups;
- ✓ Automate backup and recovery systems, ensuring efficiency and consistency of their operation;
- ✓ Separate backup storage from the corporate network, protecting them from threats to the internal network;
- ✓ Duplicate critical backups to a distinct location;
- ✓ Perform daily backups to ensure fast and secure recovery of critical data, ensuring operational continuity in the event of a system failure, cyberattack, or human error;
- ✓ Store backups for 14 days and replicate them in secure locations to increase resilience, ensuring redundancy and protection against information loss;
- ✓ Encrypt all backups to prevent unauthorized access and follow strict security protocols, ensuring that data is recoverable without compromising the integrity of the information;
- ✓ Perform regular restore tests, verifying the effectiveness of stored copies and ensuring that they can be recovered quickly and accurately whenever needed.

Fundação Mendes Gonçalves and Casa MG have also implemented a **Disaster Recovery Plan** considered essential to maintain the resilience and continuity of their operations. The plan aims to (i) minimise downtime and reduce operational impact in the event of a major failure, (ii) ensure data integrity and recovery, ensuring that critical information is not lost, (iii) protect the continuity of critical services, allowing the organisations to return to operation quickly, and (iv) avoid financial losses and reputational damage caused by prolonged failures.

9. COMMUNICATION AND AWARENESS

Fundação Mendes Gonçalves and Casa MG make this Policy available to their Employees, suppliers and partners and internally develop training and awareness-raising actions for their Employees, to enhance a culture of compliance and resilience, ensuring the understanding and compliance with the good safety practices implemented by Fundação Mendes Gonçalves and Casa MG.

10. POLICY APPROVAL, MONITORING AND REVIEW

The Board of Directors of Fundação Mendes Gonçalves and Casa MG is responsible for defining and approving the Policy, as well as reviewing it. The Policy is reviewed every two years, with the support of the IT Department, considering its adequacy to legal and regulatory requirements, the effectiveness of the measures implemented and the occurrence of organizational changes that justify its review.

Fundação Mendes Gonçalves and Casa MG carry out regular audits of their systems, processes and technological infrastructures to ensure that all safety guidelines are met effectively and that safety objectives are being met. Audits aim to ensure compliance with internal cybersecurity policies, identify opportunities for improvement, detect and correct vulnerabilities before they can be exploited by cyber threats, and assess the effectiveness of data protection measures.

The audits will be conducted internally, by Mendes Gonçalves - Sistemas e Tecnologias de Informação, Lda., or by external specialized companies, ensuring an impartial assessment of risks and opportunities for improvement.

In addition, Fundação Mendes Gonçalves and Casa MG adopt continuous monitoring systems, analysing unauthorized access attempts, anomalous traffic patterns, and possible data breaches. From these analyses, compliance reports are generated, allowing Fundação Mendes Gonçalves and Casa MG to always be aligned with best practices and safety regulations.

Employees must report any incident or vulnerability they identify to the IT Department by sending an email to: **ciberseguranca@casamg.pt**.