Management Solutions

Security Policy

0. INTRODUCTION

The purpose of this Security Policy is to establish the principles for safeguarding information and systems against internal or external threats, whether deliberate or accidental, to ensure the confidentiality, integrity, availability, legality, and reliability of information. This Policy covers both the physical security of the Firm's facilities and the logical security of its IT environment.

The Security Policy and the Information Security Management System (ISMS) it is part of are subject to continuous review and improvement. Both the policy and the related manuals, processes, and records will be reviewed on an annual basis to ensure they stay current. Also, any necessary changes will be made to accommodate updates, including technological changes, testing plans, audit plans, and other relevant factors.

1. OBLIGATION TO KNOW AND COMPLY

All professionals of the Firm, regardless of their position or role, are bound by this Security Policy (hereinafter referred to as 'the Policy'). Therefore, they must stay informed by referring to the latest version available on the Intranet and act in accordance with its defined principles, communicating any doubts regarding its content to their direct manager or the CISO.

All managers are required to communicate the contents of this Policy to their teams, oversee its compliance, address any doubts or concerns raised by staff, and implement mechanisms to ensure adherence.

Failure to comply with the rules outlined in this Policy will be subject to the disciplinary and sanctioning authority of the Firm, in accordance with the principles and regulations established by current legislation. In this regard, any identified breach of internal policies or regulations in the countries where the Firm operates must be reported to our Global QA Head (either directly or through the Firm's ethics hotline), who will ensure that the criteria of independence, objectivity, confidentiality, data protection, communication secrecy, and the absence of retaliation for people reporting in good-faith, as specified in the Policy for the Management of Doubts and Non-Compliance, are upheld.

2. SCOPE OF APPLICATION

This policy applies to all Management Solutions professionals, regardless of the type of contract that determines their employment relationship, position or geographical area in which they work (including interns).

The scope of this policy may also extend to any other professional affiliated with Management Solutions (such as occasional collaborators) whose actions may pose a technological risk to the Firm. Therefore, the policy applies to all MS professionals and to all their interactions with third parties that involve access to the Firm´s data, resources, and/or the administration and control of its information systems.

The measures and provisions outlined in this document must be considered complementary to, and not in lieu of, the technical and organizational measures necessary to ensure the protection, confidentiality, integrity, and availability of personal data, as legislated by each country in which MS operates.

Specifically, these measures complement the provisions of the European Parliament Regulation adopted in April 2016 (2016/679) regarding the protection of natural persons with respect to the processing of their personal data and the free movement of such data (GDPR, applicable as of May 25, 2018), as well as the Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (LOPD GDD) approved by the Spanish government.

3. ROLES INVOLVED

The successful implementation of the security policy relies on the clear distribution of roles and responsibilities. Therefore, a management framework has been established to initiate and oversee its effective execution. The roles involved and their key responsibilities are outlined below:

Corporate Security Officer

The Corporate Security Officer is responsible for promoting security policies and ensuring their compliance across the Firm, aligning global guidelines with the local particularities of each Unit.

Additionally, the Corporate Security Officer may be supported by a Physical Security Officer and an IT Security Officer.

Local Security Officers

Each Unit in which the Firm operates has a Local Security Officer, responsible for ensuring compliance with the policy within their area of operation. This includes executing established controls and reporting any incidents that occur.

These controls and incident reports are directed to the appropriate Security Officer, depending on whether the issue pertains to physical security or IT security.

Information Security Committee and External Advisors

The Corporate Security Officer will rely on various specialists to ensure the adequacy, updating, and effectiveness of the defined policies, as well as their compliance:

- External advisors: Through external audits, they review and evaluate the robustness of the information systems. This includes, among other things, intrusion testing, ethical hacking, and traffic analysis, and they issue a comprehensive report on their findings.
- Information Security Committee: Composed of experienced professionals from within the Firm, this committee proposes measures and suggestions related to, among other things:
    - **Compliance**: The compliance function will assess, at the frequency determined by the Security Manager, whether the established security measures are being rigorously followed. Any failure or non-compliance detected will be documented in a report, detailing the issue and indicating the level of risk to the affected information.
    - **Production**: The Production team is responsible for administering, maintaining, and operating the Firm's systems. Their main responsibility in this context is to ensure the continuity of operations from a technological perspective and report on any operational disruptions or risks.
    - **Development**: The head of the Development department is responsible for suggesting, receiving, understanding, and implementing security requirements issued by the Information Security Committee with regard to the Firm's internal developments.
- Continuous Improvement: At least quarterly, the IT Security Officer will convene the IT Security Committee, composed of a team of experienced professionals. The committee's responsibility is to identify weaknesses in the security policy, assess the associated risks, and recommend corresponding improvements.

Head of HR

Notifies all personnel joining MS of their obligations regarding compliance with the Security Policy and all related rules, procedures, and practices. Likewise, she will be responsible for informing all MS professionals of this policy, communicating any updates or changes, ensuring the signing of the corresponding confidentiality commitments, and implementing ongoing training in security matters.

Head of Legal

Responsible for verifying compliance with this policy in the management of all contracts, agreements, and other documentation between MS and its employees or third parties. Additionally, provides legal advice to MS on information security matters.

Information and system users

Responsible for knowing, making known, complying with and enforcing compliance with the current Security Policy.

4. PHYSICAL SECURITY

The purpose of Physical Security is to prevent and impede unauthorized access to MS facilities (our offices and our Data Processing Centers -CPDs). It also aims to safeguard our professionals from incidents and to ensure the proper use of workstations, including the secure handling of documents and personal belongings that could pose a security risk.

4.1. Physical security of MS facilities

Office access security

Access to the Firm's offices is secured through various barriers or physical control measures:

- All buildings in which MS offices are located will have security surveillance as well as turnstiles accessible via swipe card and/or a reception system for visitor control. [1]
- Access to the office itself is granted by using magnetic cards or entering a password. Each office is assigned an Access Control Manager responsible for issuing the necessary access mechanisms (card/key) to authorized employees.
- All offices have a reception desk to control third-party access to the MS offices themselves, regardless of whether there is a reception desk at the building entrance. The access door should never remain open. If the locking system malfunctions, the entrance will be guarded at all times until the malfunction is resolved.
- No professional may give access to anyone who has not identified themselves as an MS employee without prior authorization from the Access Control Manager.

Any access-related incident must be reported to the Local Security Officer, who will then notify the General Services Manager.

Data Center Security

Currently, critical corporate services (systems and communications) are hosted in Data Centers in private cloud format. This ensures that all data subject to the LOPD (Ley Orgánica de Protección de Datos) is stored in

[1] Otherwise, the Country Head must implement alternative measures and submit them to the Corporate Security Officer for approval.

countries authorized under the LOPD. Specifically, we have a solution involving 2 Data Centers (TierIV Gold+ Tier III as backup) in High Availability (with associated disaster recovery plan).

4.2. Safety recommendations for professionals

Management Solutions considers the safety of its professionals to be a priority, and therefore sets out a series of recommendations based on our own experience as a Firm and on the standards published by some international public bodies:

General recommendations

- For cab transfers, use only officially accredited vehicles, previously reserved or located at reliable taxi ranks in hotels, workplaces and shopping centers. It is recommended to leave all luggage in the trunk to avoid attracting the attention of criminals who take advantage of moments when the vehicle is stopped (traffic lights, traffic jams, etc.) to break the windows and steal the personal belongings of travelers.
- It is not advisable to drive at night and if there is an alternative, it is always better to use toll highways and main roads rather than secondary roads. It is recommended to travel by private car or cab and, when possible, in a group.
- It is recommended not to go out flaunting jewelry or valuables (watches, cell phones, brand name clothes, etc.) and not to carry large sums of cash.
- In the event of an assault, it is recommended not to offer any resistance, even if the assailants are minors, as they may be armed and under the influence of drugs.
- If you receive a threatening phone call, do not continue the conversation, do not give any information and hang up the phone as soon as possible. Be sure to pay attention to the telephone number from which the call was received.
- Avoid ATMs if possible and, if necessary, look for one that is located inside more protected areas, such as shopping malls, and act with caution and discretion.
- Avoid tourism in sparsely populated beach areas, as well as mountain excursions in remote environments.
- In the case of credit card payments, it is advisable to carefully monitor the bank statements at a later date, as there are some cases of card cloning.
- When staying in hotels, use the safes available in most rooms.
- For those hiring staff: ask for references from domestic service and other employees.

Specific recommendations

In addition to the general application of the measures outlined in the previous section, it is important to be aware of specific measures that may be required in each country. Below are links to five websites of international organizations that provide highly relevant information in this area. For further details, it is advisable to consult the website of the respective national agency or embassy for each country.

- Ministry of Foreign Affairs of Spain.
- Gov.UK.
- Travel.State.Gov.
- Portal das Comunidades Portuguesas.
- Auswaertiges amt.

It is recommended to review these resources regularly, as the guidance and recommendations are subject to updates based on evolving circumstances.

4.3.

4.4. Clear desktop security

In order to ensure information security, maintain an orderly work environment and promote operational efficiency, Management Solutions establishes the policy that all employees must ensure that their desks are free of confidential documents, electronic devices, access credentials and other sensitive objects at the end of each workday or when absent for extended periods of time. All important material should be stored in locked drawers, filing cabinets or secure digital systems. This practice helps protect critical data, facilitates work area cleanliness, and projects a professional image to clients and employees.

5. LOGICAL INFORMATION SECURITY

The logical security of the Firm’s information and IT resources is structured through the establishment of clear guidelines regarding system access control, communication security, and the responsible use of these resources by professionals.

5.1. System Access Control

The main objective is to establish the necessary protocols for access to the Firm's systems, in order to prevent unauthorized access to information. Specific rules are therefore provided in relation to:

User administration

The process of registering and deleting users is managed by the system administrators, following notification from the Human Resources Department. Mechanisms are in place to ensure that personnel are granted access only to the data and resources necessary for the performance of their duties. Privilege management is defined at the group or user profile level, avoiding the assignment of privileges to individual users.

Identification and authentication of professionals

Access to the Firm’s computers is granted through unique user identifiers, which must be properly authorized and secured with a corresponding password and multi-factor authentication. Under no circumstances may the user identifier be shared with or transferred to a third party. In addition, minimum standards are established to ensure the quality and confidentiality of passwords, thereby maintaining an adequate level of security

Any access to the Firm's computers is made using a unique user identifier properly authorized and provided with its corresponding password and multiple authentication factor. Under no circumstances may the identifier be communicated and/or transferred to a third party. Likewise, a series of minimum quality standards are established in relation to the quality and confidentiality of passwords in order to ensure an adequate level of security. MiFi routers and corporate mobile devices are issued with an initial PIN. Corporate mobile devices are further secured through the activation of the Mobile Device Management (MDM) system.

Specific authorizations

In cases where specific authorizations are required – whether for the use of new information processing resources or for third-party access to any of the Firm's technological resources – such authorization must be granted by the IT Security Officer. This ensures compliance with all applicable security policies and requirements:

- New Technological Resources - The IT Security Officer will evaluate their purpose and intended use prior to granting authorization, specifying any additional controls required.
- Access by Third Parties - The IT Security Officer, in coordination with the owner of the affected information, will assess the associated risks and identify the specific controls required. All contracts where the provision of services is carried out within MS must include confidentiality commitments tailored to the specific case and must restrict permissions to the minimum necessary. Under no circumstances will third parties be granted access to information, processing facilities, or other critical service areas until the appropriate controls have been implemented and a formal contract or agreement – defining the terms and conditions of access – has been signed.

5.2. Systems and Communications Management

To ensure the secure operation of MS's information systems, the following specific security measures are implemented:

- Controls against malicious software: Implementation of firewalls, proxies, antivirus software, Endpoint Detection and Response (EDR) systems, anti-spam filters, restricted administration permissions, and control and inventory of installed software
- Communications security
- Encryption of personal computers
- Encryption of information media for its transport: For media containing information of enhanced or maximum confidentiality, security measures may be strengthened at the discretion of the responsible partner.
- Security of software installation on servers
- Backup copies of the information contained in the systems
- Management of removable computer media: As a general rule, the use of USB drives, external hard disks, CDs, DVDs, or similar devices is not permitted. For media containing information of enhanced or maximum confidentiality, security measures may be reinforced at the discretion of the responsible partner.
- Disposal of physical information media: All confidential information in physical format must be destroyed using designated shredding containers available in the offices or, if unavailable, paper shredders. For media containing information classified as enhanced or maximum confidentiality, security measures may be reinforced at the discretion of the responsible partner.
- Remote management and securitization of mobile terminals through the use of an MDM system.

5.3. Rules of Use

MS personnel must comply with the regulations governing the use of the Firm's technological resources in order to ensure the security and confidentiality of the information to be processed:

- Purpose of use - Information systems must be used solely to fulfill their designated functions within the Firm. Users must not use the systems or the information processed by them for any other purposes.
- Confidentiality - Users must not share their assigned user identifier or passwords with anyone else in the Firm, nor use them fraudulently to access unauthorized information. The only exception is when IT personnel require the password to perform support functions. In such cases, once the IT intervention is completed, the user must immediately change the password. Any consequences arising from non-compliance with this rule will be the sole responsibility of the owner of the user identifier.
- Truthfulness - Users are responsible for ensuring that the data entered and maintained in the systems is truthful, accurate, and complete.
- Duty of care - Professionals are required to diligently safeguard corporate devices provided by the Firm (such as computers and mobile phones) and must not leave them unattended at any time in locations such as restaurants or public transport. They must also ensure that such devices remain out of sight of third parties when left inside a private vehicle or similar environments.
- Incident notification – Any incident affecting information security and/or the operation of the Firm's IT resources must be reported by sending an email to *incidenciasms@managementsolutions.com*.
- Use of e-mail and the Internet:
    - Use of the Firm's IT resources must be strictly for professional purposes. The sending of confidential documentation without appropriate protection (e.g., encryption or encoding), as well as forwarding chain letters or similar content, is not permitted.
    - Web access is restricted through blacklists configured at both the corporate proxy and Microsoft Edge level. For users who have access to highly confidential information, web access will be further restricted through whitelists managed via the corporate proxy and Microsoft Edge.
    - Use of email and Internet browsing will be monitored to ensure compliance with usage policies. Internet browsing data will be retained for a period of 90 days.
    - For user profiles with access to information of enhanced or maximum confidentiality, more restrictive measures may be applied at the discretion of the partner responsible for the project.
- Installation or use of software - Installing software on corporate devices or using portable software outside the corporate platform is not permitted without prior authorization from the IT Security Officer. For users involved in projects processing Enhanced Confidentiality information, additional security measures may be applied at the discretion of the partner responsible for the project. In the case of users participating in projects where information of Maximum Confidentiality is processed, the use of software will be strictly limited to those programs authorized by the CCN.

- Backup of personal computers - MS professionals are responsible for performing regular backups of their personal computers. To facilitate this, an automatic replication tool (DVR) is provided to all professionals.
- Secure disposal of information: Project managers (partners and managers) must identify the requirements for deleting project-related information following the termination of a client contract. If the client agreement mandates secure deletion at the end of the project, a request must be submitted to the IT Security Officer to carry out the deletion using authorized tools and procedures in a traceable manner. This process is mandatory for documentation and data associated with Highest Confidentiality projects.
- Use of non-corporate devices such as smartphones, tablets, mass data storage tools, etc.
    - When a professional wishes to use non-corporate devices, they must request authorization from the Technology department and, if necessary, the installation of a corporate MDM/MAM license in order to uphold the Firm's security standards, particularly regarding secure access and the confidentiality of both the Firm's and the client's information.
    - If at any time information is downloaded or copied to any storage medium on the device (whether by copying, opening, or downloading a document), the professional must ensure that the medium is encrypted and that the decryption key is known only to them. Additionally, the information must be deleted immediately once the reasons justifying its temporary storage are no longer valid.
    - Under no circumstances will credentials be stored on non-corporate devices (e.g., saved in the browser).
- Secure access methods to corporate services from different devices:
    - Directly access via cable or corporate wireless network within MS offices, using corporate computers.
    - By VPN from outside the office using corporate computers and via WiFi or MiFi router.
    - By web interface for DVR service from outside the office. In the case of access from a non-corporate device, the storage of files and credentials (e.g. in the browser) is explicitly prohibited.
    - Through the corporate MDM/MAM client installed on the corporate mobile device or, upon request and authorization from Technology in accordance with MS policy, on non-corporate devices.

Any other form of access is not permitted.

Regarding the reduction of the **digital footprint**, professionals are required to:

- Configure browser settings to allow only the essential navigation records necessary for the proper functioning of the websites they access, thereby minimizing the disclosure of unnecessary information about their web usage.
- Additionally, when using desktop and personal devices, it is recommended to:
    - Share information via the cloud or DVR to reduce the number of duplicate copies of the same file.

- Duplicate files or those with numerous versions that do not add value should be deleted.
- Photos or videos that are repetitive or do not add value to the scope of work for which the devices are used must be deleted.
- When using e-mail:
    - Limit the number of recipients.
    - Delete emails that are of no interest to you or contain outdated information.
    - Unsubscribe from newsletters that are not useful.
    - Regularly empty the trash folder

All MS professionals, as well as external users and third parties performing MS functions where applicable, will receive appropriate training and regular updates on MS policies, standards, and procedures from the Quality and Internal Audit Department.

5.4. Audits and Usage Monitoring

The Firm reserves the right to perform any audits deemed necessary in the event of suspicion of non-compliance with this policy, monitoring the use of resources and information.

Therefore, any employee or supplier with access to our resources, systems, or information must be aware that their use may be monitored by the Firm. Thus, each time the system is accessed, the following warning will be displayed:

"In accordance with Management Solutions' Security Policy, we remind you of the obligation to use the technological resources provided by the Firm (such as laptops, cell phones, smartphones, multifunction equipment, etc.) with due diligence and exclusively for purposes related to the performance of your duties and/or collaboration services. Any other use may result in legal liability. In this regard, Management Solutions monitors the use of IT resources and, upon suspicion of possible violations of usage rules, will evaluate the need to investigate any access to and/or use of IT resources by the Firm's professionals and/or collaborators using our equipment that may pose a threat to the security of the Information Systems or cause other types of damage to the Firm. For further information, please refer to the Corporate Policies."

The areas that are systematically monitored are as follows:

- Inventory of applications installed on each device
- Monitoring of telephone consumption (fixed and mobile).
- Monitoring of videoconferencing service consumption
- Internet browsing:
- Monitoring of printing, copying and scanning of documents
- Network connection logs and remote access via VPN
- Event logs of the Windows operating system itself
- Email monitoring (date, time, subject, sender, receiver)
- Monitoring of the last connection from corporate or non-corporate devices with a MDM corporate license installed, including basic device information (brand, model, operating system version, operator, etc.).

6. Logs provided by Microsoft 365

TERMS AND DEFINITIONS

For the purpose of properly interpreting this document, the following definitions apply:

Information: Refers to any communication or representation of knowledge as data, in any form, including textual, numerical, graphic, cartographic, narrative or audiovisual form, and in any medium, whether magnetic, paper, computer screen, audiovisual or other.

Information system: Refers to an independent set of information resources organized for the collection, processing, maintenance, transmission and dissemination of information according to certain procedures, both automated and manual.

Information technology: Refers to hardware and software operated by MS or by a third party that processes information on its behalf, to perform a MS-specific function, regardless of the technology used, whether data computing, telecommunications or otherwise.

Information security: Information security is defined by adherence to the following key principles:

- Confidentiality: Ensuring that information is accessible only to individuals who are authorized to access it.
- Integrity: Safeguarding the accuracy and completeness of information and its processing methods.
- Availability: Guaranteeing that authorized users have access to information and associated resources whenever needed, regardless of their location (e.g., MS offices, external facilities, remote access via VPN, etc.).
- Authenticity: Ensuring the validity of information in terms of timing, format, and distribution. The authenticity of the source is also verified to prevent identity spoofing.
- Legality: Ensuring compliance with all applicable laws, regulations, standards, and internal provisions that MS is subject to.
- Reliability of information: Ensuring that the information generated is appropriate and sufficient to support decision-making and the performance of duties and responsibilities according to their nature.

Risk assessment: Risk assessment involves evaluating the threats and vulnerabilities associated with information and information processing facilities, the likelihood of their occurrence and their potential impact on MS's operations. Risk management refers to the process of identifying, controlling, and minimizing or eliminating security risks that could affect information. This is a cyclical process that must be conducted regularly.

Security incident: A security incident is an adverse event within the established security system that compromises the confidentiality, integrity, availability, legality, or reliability of information.