senhasegura

SSG 5010

Information Security Policy

Rating: Public

Version 5

July 2023

Summary

1 Objective

Establish guidelines that allow Employees and Third Parties of MT4 and national and international affiliates to have direction on information security-related standards of behavior appropriate to the business and legal protection needs of MT4 and national and international affiliates and their employees.

To guide the definition of specific Information Security norms and procedures, the conditions of use of IT resources, and the implementation of controls and processes to meet them.

Preserve the information as:

- Integrity: guarantee that the information is maintained in its original state, aiming to protect it, during storage or transmission, against undue alterations, whether intentional or accidental.
- Confidentiality: guarantee that access to information is obtained only by authorized persons.
- Availability: ensuring that authorized users can gain access to the information and corresponding assets whenever they need them.

2 Field of Application

With the corporate scope, this document applies to MT4 and national and international subsidiaries, considering all employees (contractors and trainees), service providers, and partners.

3 Abbreviations

- VPN - Virtual Private Network
- IT - Information Technology

- RH - Human Resources
- TIC - Information and Communication Technology

4 Definitions

- Physical Access - access to the physical infrastructure of the organization and its various control mechanisms, such as turnstiles, biometric devices, and security cameras.
- Logical Access - access to the organization's infrastructure, such as operating systems, intranet, databases, and various control mechanisms, such as login and authentication tokens.
- Remote Access - a connection between a remote device (terminal or device) to another computer that is not physically connected to MT4's private network and branches.
- Backups - copying physical or digital information for security, analysis, or data restoration.
- Database - collections of data linked together and organized to provide information.
- Confidentiality: a principle that says that information should be available only to those entitled or authorized to do so.
- Business Continuity - a set of practices to prevent the interruption of operations by planning action alternatives in case of incidents with a low probability of occurrence but that may cause severe damage to the organization.
- Mobile devices - portable technological equipment such as smartphones, tablets, and notebooks.
- Information security incidents - events related to Information Security.
- Integrity - the principle that information must be kept intact.
- Risk - the probability of occurrence and the impact it may cause, should it occur.
- Information Security - a set of practices to protect corporate information from misuse. It is supported by three pillars: Confidentiality, Integrity, and Availability.

- System - a digital tool that has a complex function directly related to the business, such as management systems.
- Software - a digital tool with no function directly related to the business but only supports it, such as Office Suite, Windows, etc.
- User/collaborator - is the one who uses resources made available by the IT area, software, or hardware to perform their job functions.
- Vulnerability - a weakness that can be exploited by a threat characterizing an incident.
- Homologation environment - environment with the same characteristics as production, where the systems (changes, etc.) are tested, with the objective of guaranteeing that it is in conformity with everything it proposes to do.
- Production environment - controlled environment containing the configuration items in production used to deliver IT services to customers.
- Information Classification - defines the information classification levels, directing everyone to the correct treatment.

5 Applicable Documents

- General Personal Data Protection Law, Law No. 13,709, of August 14, 2018
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 - GDPR
- ISO/IEC 27001: 2013
- ISO/IEC 27017: 2013
- SSG 4001 - Code of Ethics
- SSG 4006 - Standard Operating Term

6 Responsibilities

Area [Responsible]	Responsibilities	Authorities
IT - RDO	● Refine policies	● Review
Users	● Comply with policies	● Propose improvements
Top Management	● Establish policies	● Approval

7 Guidelines

1. The content of this policy is defined as MT4's intellectual property and is intended for internal use, third parties, and partners
2. In case of doubt about applying the guidelines in this policy, Employees should consult their immediate manager, IT, and/or Compliance Officer.
3. The content of this policy must be known and observed by all Employees, Third Parties and others who maintain or will maintain a relationship with MT4, as applicable, and its noncompliance is subject to the application of legal and disciplinary measures detailed in *SSG 4001 - Code of Ethics* and in document *SSG 4006 - Standard Operating Term.*
4. The application of the legal and disciplinary measures mentioned above do not exempt, dispense, or mitigate civil, administrative, and/or criminal liability for losses resulting from intentional or culpable acts resulting from the violation of the legislation in force, this policy, the applicable rules and procedures.
5. This policy makes each employee, third party and partner aware that the environments, systems, computers, tablets, e-mails, internet, connected networks, and media connected to equipment may be monitored and stored, as the Brazilian legislation provides.
6. The omitted cases will be decided by a collegiate formed by a IT, Legal, and Compliance representative.

7. All information, whether public, internal, restricted, or confidential, is the property of MT4, except for that externally sourced information that MT4 obtains through an agreement between both parties. All information is considered a valuable corporate asset that everyone must manage.
8. Information sharing is only allowed with the Immediate Manager's express authorization and the Compliance Area's approval. This process must be formalized and filed, including all interactions and approvals resulting from the request.
9. Information sent to Third Parties must be carried by an authorized carrier in a sealed envelope or transmitted securely.
10. Confidential information must always be protected and stored to prevent unauthorized access. When printing, sending, and disposing of information, attention must be redoubled.
11. When sending Confidential Information, whether by fax, e-mail, or other digital or physical media, it is necessary to make sure that the recipient can access the information and also have Information Security measures in place.
12. When using the communication media and work tools provided by MT4, the information sent and received is corporate information. Your activity may be monitored and stored to ensure that communication tools are used appropriately.
13. All employees are responsible for correctly disposing of media or other data storage media and always using a shredder or other method to restrict access to the information contained therein.
14. The shared information assets must be used in such a way that other employees are not affected or harmed in the criteria regarding Confidentiality, Integrity and Availability of their information. (Example: undue access, malicious code, breach of confidentiality, undue sharing of sensitive and classified information).
15. In accordance with Federal Law No. 13,709 of August 14, 2018 and with Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 it is considered sensitive personal data: personal data about racial or ethnic origin, religious conviction, political opinion, membership of a trade

union or organization of a religious, philosophical or political nature, data concerning health or sex life, genetic or biometric data when linked to a natural person and their fundamental rights.

16. Except for the purposes outlined in Article 7 of Federal Law No. 13,709 of August 14, 2018, and Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, all information related to the identified or identifiable natural person shall automatically be considered with restricted classification.
17. Observe the guidelines, regulations, and standards imposed by the Brazilian Authority, provided for in Federal Law No. 13,709 of August 14, 2018, and Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the treatment and protection of personal data, including those historical.

8 Information Classification and Treatment

1. Information shall be classified as to its degree of secrecy and confidentiality and level of protection at the time it is generated to ensure the desired confidentiality. Information shall be classified according to ISO/IEC 27001:2013 - Information Security as: Public, Internal Use, Restricted, Confidential.

    a. Public Information: is information that does not need sophisticated protection against leakage, because it can be public knowledge. Protection level: Public.

    b. Information for Internal Use: information that cannot be disclosed to people outside the organization but which, should it happen, will not cause significant harm. Level of protection: NP-1.

    c. Restricted Information: is strategic information that should be available only to restricted groups of employees. It can be protected, for example, by restricting access to a network folder or directory. Protection level: NP-2.

   d. Confidential Information: is information that, if disclosed internally or externally, has the potential to bring great damage to the entity's financial, image, or strategy (the highest level of confidentiality). Protection level: NP-3.

2. The classification of the degree of secrecy and confidentiality of the information and its level of protection must be done by the area manager, as well as the authorization to access it.

3. The regulations (policies, procedures, rules) must be classified according to the degree of secrecy and confidentiality of the information. The Compliance area is responsible for controlling the regulations, as well as for guiding and supporting the preparation and/or review of these documents.

4. Corporate e-mails must be sent with the standard signature provided by MT4.

9 Access Control

9.1 Physical Access

1. Every employee who needs physical access to MT4's offices must request access to the IT area so that the proper clearances (e.g., entrance gates, turnstiles, access controls, etc.) are made.

2. All physical access, except the janitorial and IT areas, must be approved by the immediate manager and the manager of the area being accessed.

3. Surveillance cameras monitor all offices and access is logged.

4. Service providers and visitors must always be accompanied by an employee responsible for their access.

9.2 Restricted Access to Areas

1. MT4 business or operations areas should control physical access. The following access-controlled regions are established:
    a. Administrative;
    b. Financial;
    c. Legal;
    d. Data Center;
    e. IT;
2. If there is no physical separation for these environments, it becomes even more imperative to take due care with the handling, oral and written transmission of confidential information.
3. The manager is responsible for ensuring those who pass through the premises are properly informed that this area is restricted.
4. Only IT employees or persons authorized by the area may access MT4's data centers.

9.3 Logical Access

9.3.1 Credentials

1. The identification of access to IT Resources must be made through a personal and untransferable credential, created by the User himself, through the observance of basic rules that aim to ensure the security of access and use of resources, being prohibited its sharing.

2. You are responsible for ensuring the confidentiality and secrecy of your passwords and logins.
3. Actions carried out with the User's identification and passwords, such as handling data in files, spreadsheets, and/or systems, will be the entire and exclusive responsibility of the User.
4. To prevent undue access to IT Resources by others, the User must turn off the computer or lock it whenever leaving the equipment.
5. Users who use Mobile Devices must have their device authentication enabled and IT can use tools to ensure this.
6. The use of shared credentials is discouraged. However, in situations where nominal credentials are not possible, sharing credentials must be done via the password vault.
7. Mechanisms implemented by IT can block access to prevent or mitigate attacks. To request unblocking, seek guidance from the MT4 IT Department.
8. Automatic mechanisms implemented by the IT Area may require Users to change their password, but Users can change their own password at any time they wish.

9.3.2 Internal Network

1. Access to technology resources through external connections will be allowed upon formal request, specific authorization, and use of strong authentication. Incoming connections and associated systems must maintain a level of security equal to or greater than that of internally accessed networks.
2. Connections to the corporate network will only be allowed to assets that meet at least the security criteria defined in the relevant standard. External connections to the corporate network will only be allowed through technologies made available by the IT area.

9.3.3 Internet and Wi-Fi

1. The internet provided by MT4 must be used for business purposes. This rule extends to the three wi-fi networks made available by MT4: corporate, devices, visitors. Security policies are in place to ensure the appropriate use of these networks.

    a. The corporate network is made available for employees to access the Internet and internal network resources via corporate mobile devices.

    b. The device network is made available for employees to access the Internet through MT4-managed mobile devices.

    c. The visitor network provides visitors with access to the Internet during their stay at MT4's facilities.

2. Employees should not send e-mail containing confidential information to their personal e-mail accounts or save it on their personal computers or other electronic devices other than MT4.

3. It is forbidden to access, on Mobile Devices and other tools made available by MT4, the following categories of sites: gambling, advertising, adult, obscene/offensive material, criminal/illegal activities, weapons, violence, hate speech, dating, games, chat, sites that make or allow remote control of computers (except by IT), hacking, forums, blogs, sites with sound and video transmission, that are not for professional purposes, and others that may be blocked.

4. The rules mentioned in this policy for use of Mobile Devices must be respected also when used outside of MT4.

9.3.4 E-mail

1. The corporate e-mail must be used exclusively for this purpose. Thus, sending chain letters, farewell e-mails, with words of inappropriate use and/or with jokes, among others, without corporate purposes, are not allowed.
2. All business matters must be conducted via MT4's electronic mail (email) system and/or IT approved messaging systems. Personal e-mail accounts, SMS, MMS or any instant messaging service and social media sites should not be used.
3. The IT area will set limits on the use of e-mail systems in order to ensure the smooth running of the service according to the resources made available, security and confidentiality.
4. At any time it deems necessary, the IT area can use mechanisms to block incoming or outgoing messages and file downloads that are not consistent with MT4's activities.
5. The user should not open suspicious e-mails.

10 IT Resources

10.1 Institutional IT Resources

1. The IT resources provided by MT4 (computers, systems, internet) are used by employees to perform the professional activities for which they have been assigned and are the property of MT4.
2. Access permissions to MT4's IT resources should be based on business needs, considering the Users' functional profile.
3. It is the responsibility of each Manager, to formally request the release, change, suspension, or revocation of access by their team members to any IT resource.

4. It is HR's responsibility to formally request any IT resources, for hiring new employees, layoffs and dismissals, changes in areas of activity, function or position, through the IT call center.
5. In order to control users' access privileges, any removal, whether temporary or permanent, including a change of area, must be formally informed by HR, so that the appropriate measures can be taken to cancel or provisionally suspend access and permission.
6. Every request for access to IT Resources must be formally documented and justified as to its real need.
7. Each manager is responsible for requesting the release, alteration, suspension or revocation of access to any IT resource for its contracted Third Parties, in case of: Hiring; Change in the scope of services; Termination of activities.
8. The access granted to Third Parties must be of a provisional nature, and the manager responsible for it must indicate, at the time of the request, the deadline for using the resources.
9. All IT equipment must be approved by the IT area.
10. Only IT employees or persons authorized by the area can perform the installation and/or uninstallation, as well as the hardware parameterization of the corporate equipment.
11. The use of technology equipment for use outside of MT4 will be permitted with formal authorization and should consider the risks pertinent to its use outside of MT4's security infrastructure.
12. The User is responsible for the conservation, integrity, use, and information contained in the Mobile Devices he uses.
13. The User for whom the corporate equipment is made available must sign the Terms of Responsibility specific to this equipment.
14. No user may use MT4's resources to deliberately propagate malicious code or programs.
15. No user may use MT4's resources to download or distribute pirated software. In addition, you may not upload any software licensed to MT4, or data owned by MT4 or its customers, without the express permission of the manager responsible for the Software or data.
16. The IT area will make available, through devices provided by MT4, access to the systems and corporate e-mails as a facility for Employees on the move and as an access contingency measure.

17. Employees who use any type of proprietary Device to access MT4's systems and corporate e-mails must comply with this policy.

10.2 Private IT Resources

1. Private ICT resources previously authorized to access the content provided by MT4 must be protected using access blocking methods and security tools, such as antivirus and firewall, in order to mitigate the risks of the institution being exposed to threats.
2. In an eventual need to access the technological resources made available by MT4 through personal equipment, the systems must be used in the web version, not being allowed to download files from MT4 on personal devices and local installations of the systems since our licensing contemplates this usage model. Also, the accesses are adherent to the implemented security issues.
3. Any private ICT resource brought onto the MT4 premises is the sole responsibility of its owner, including the data and software stored or installed on it.
4. MT4 is not responsible for any private ICT resource loss, theft, or malfunction.

11 Social Media

It is strictly forbidden to make, post or share comments, messages, or discussions about MT4, its clients, and information regarding any strategy made through social networks, chat rooms, wikis, virtual worlds, and blogs (Social Media), unless expressly authorized by the Communication and Marketing Department. For questions of conduct, the MT4 Code of Ethical Conduct and the MT4 Social Media Conduct Manual must be observed.

12 Information Storage

1. All corporate information must be stored on the MT4 data network in their respective directories.
2. No corporate information, files or data should be kept on local disks or any other storage media other than those made available by IT.

13 Backup

The IT area performs the backup of network directories through an automated process, and third-party services can be used to safeguard the data. Files located on desktops and mobile devices are not backed up.

14 Antivirus

With the objective of protecting MT4's files and electronic information from electronic viruses, the IT area must keep the virus prevention and detection control tool updated, respecting at least the periodicity recommended by the manufacturer.

15 Information Systems

1. The IT area is responsible for approving technical solutions and the Users for approving the functionalities of the systems.
2. Requests for developing or contracting new systems must be forwarded to the IT area, which must observe the best Information Security practices.
3. The homologation and production environments are segregated, thus guaranteeing data integrity.

4. MT4 must, through its Managers, establish deadlines and procedures for archiving and disposal of Information, establishing a data life cycle, complying with the legal and regulatory requirements to which it is submitted.
5. All software is registered and licensed for corporate use, and the End User is not allowed to install or use it for private purposes.
6. It is not allowed to install any kind of software that is not approved and authorized by the Manager responsible for the IT area.
7. It is not allowed to deactivate or change the configuration and/or parameterization of the programs installed in the equipment provided.
8. Unauthorized reproduction of the software installed on the equipment provided will constitute misuse of the equipment and is a legal infringement of the manufacturer's copyrights.

16 Manual Data Change

1. For the security of the information recorded and stored by MT4, it will not be allowed to change data directly in the database. The data imputed in the interface of the systems are stored securely, consistently and privately to ensure its protection, avoiding breach of integrity and traceability of corporate information for audit purposes.
2. If the information stored contains an error due to human or technological failure, which can bring harm to MT4, the following steps must necessarily be observed:
   a. Verification with MT4 departments of the actual need to change the information, and the possible remediation of the error in ways other than changing the data;
   b. If the problem cannot be solved by the step described in the item above, open an IT request justifying the need for change, forwarding it to your functional director for approval, and subsequent approval by the Board of Directors;

c. Upon approval by the board, the MT4 IT department will make the change, attaching the relevant technical justification and board approval to the process.

17 Technical Vulnerability Management

It is up to the IT area to continuously monitor the security of data and systems, by identifying the weaknesses and vulnerabilities of data exposure, which may entail some risk to the MT4, as well as to develop and monitor response plans.

18 Information Security Incidents

1. Every incident that puts Information Security at risk, including loss, theft, or robbery, must be formally and immediately reported to the Service Desk for evaluation of the situation and adoption of the necessary measures.

2. All incidents must be formally registered for later analysis. Such incident records shall be used as inputs for a critical analysis and action plan, if necessary, by the IT area.

3. The adoption of adjustment measures related to Information Security that may be necessary as a result of the incidents that occurred will be the responsibility of the IT Manager, who will be responsible for making them operational upon approval by the Board of Directors of the necessary measures and/or investments.

19 Contingency and Business Continuity Plan

The information technology structure has contingency mechanisms to reduce the risks of loss of confidentiality, integrity and availability of information assets. These mechanisms are detailed through normative documents, including a contingency plan.

20 Review History

Version	Date	Editor	Approver	Description
1	31/01/2022	RDO	Board of Directors	Document Creation
2	04/03/2022	RDO	Board of Directors	Public version
3	12/09/2022	Compliance	Board of Directors	Adequacy following LGPD 2018 and GDPR 2016
4	20/05/2023	Compliance	Board of Directors	Document Maintenance
5	07/10/2023	Compliance	Board of Directors	Template Adequacy