Information Security Policy

Information

Meta's Policies are documents that aim to guide the company's relationships through pre-established principles.

Purpose

“Human Growth with Technology.”

Values

- We are people serving people.
- We think and act like owners.
- We are driven by performance.
- We grow and learn together.
- We strive for excellence and simplicity.
- We inspire, encourage, and celebrate a culture of innovation.

Meta

What can I find in this document?

The Information Security Policy is the document that guides and establishes META's corporate guidelines for the protection of information assets and the prevention of legal liability for all users. It must therefore be complied with and applied in all areas of the institution.

This ISPS is based on the recommendations proposed by the ABNT NBR ISO/IEC27002:2005 standard, recognized worldwide as a code of practice for Information Security management, as well as in accordance with the laws in force in our country.

With the intention of increasing the security of the technological infrastructure, the Acceptable Use Policy for Devices was developed in parallel, aiming to guide our users in the use of the information technology assets made available.

1. Objectives

To establish guidelines that enable META employees to follow Information Security behavior standards appropriate to the business needs and legal protection of the company and the individual.

To guide the definition of specific Information Security standards and procedures, as well as the implementation of controls and processes to ensure compliance.

Preserve META's information regarding:

• Integrity: ensuring that information is kept in its original state, in order to protect it, during storage or transmission, against unauthorized, intentional or accidental changes;

• Confidentiality: ensuring that access to information is obtained only by authorized persons;

• Availability: ensuring that authorized users have access to information and corresponding assets whenever necessary.

2.

The guidelines established herein must be followed by all employees and service providers and apply to information in any medium or format.

This policy informs each employee that the company's environments, systems, computers, and networks may be monitored and recorded, with prior notice, as provided for by Brazilian law.

It is also the responsibility of each employee to keep up to date with these policies, procedures, and related standards, seeking guidance from their manager or the Information Security team whenever they are not absolutely sure about the acquisition, use, and/or disposal of information.

3. Policy principles

All information produced or received by employees as a result of professional activities contracted by META belongs to that institution. Exceptions must be explicit and formalized in a contract between the parties.

Computer and communication equipment, systems, and information are used by employees to carry out their professional activities. Personal use of resources is permitted as long as it does not impair the performance, productivity, and security of systems and services.

META, through its Information Security team, may record all use of systems and services to ensure the availability and security of the information used.

4. Specific responsibilities

1. Employees in general

An employee is understood to be any individual, hired under the CLT (Consolidated Labor Laws) or as a service provider through a legal entity or otherwise, who performs any activity within or outside the organization. Each employee shall be fully responsible for any loss or damage suffered or caused to META and/or third parties as a result of failure to comply with the guidelines and rules referred to herein.

2. People and/or process managers

Have an exemplary attitude towards Information Security, serving as a role model for employees under their management.

Assign to employees, during the hiring and formalization of individual employment, service, or partnership contracts, the responsibility for complying with META's Security Policy.

Require employees to sign a Term of Commitment and Acknowledgement, assuming the duty to follow established rules, as well as committing to maintain secrecy and confidentiality, even when terminated, regarding all META information assets.

Before granting access to the institution's information, require casual employees and service providers who are not covered by an existing contract to sign a Confidentiality Agreement, for example, during the survey phase for the submission of commercial proposals.

Adapt the rules, processes, procedures, and systems under your responsibility to comply with this security policy, as well as with the company's terms.

3. Information custodians

3.1 Information Technology

Test the effectiveness of the controls used and inform managers of any residual risks.

Agree with managers on the level of service to be provided and incident response procedures.

Configure the equipment, tools, and systems provided to employees with all necessary controls to comply with the security requirements established by this policy and the complementary Information Security Standards.

Computer system administrators and operators may, due to their user privileges, access other users' files and data. However, this will only be permitted when necessary for the performance of operational activities under their responsibility, such as computer maintenance, backup, audits, or testing of the environment.

Segregate administrative and operational functions in order to restrict the powers of each individual to the minimum necessary and eliminate, or at least reduce, the existence of people who can delete logs and audit trails of their own actions.

Ensure special security for publicly accessible systems by safeguarding evidence that allows traceability for audit or investigation purposes.

Generate and maintain audit trails with sufficient detail to track possible failures and fraud. For trails generated and/or maintained electronically, implement integrity controls to make them legally valid as evidence.

Manage, protect, and test backup copies of programs and data related to critical processes relevant to META.

Implement controls that generate auditable records for the removal and transport of media containing information held by IT, in environments that are fully controlled by IT.

The Information Manager must be informed in advance of the end of the retention period so that they have the option to change it before the information is permanently discarded by the custodian.

When internal movement of IT assets occurs, ensure that a user's information is not irretrievably removed before making the asset available to another user.

Plan, implement, provide, and monitor the storage, processing, and transmission capacity necessary to ensure the security required by the business areas.

Assign each account or access device to computers, systems, databases, and any other information asset to an identifiable individual, whereby:

- individual employee users (logins) shall be the responsibility of the employee themselves.
- third-party users (logins) will be the responsibility of the contracting area manager.

Continuously protect all company information assets against malicious code and ensure that all new assets only enter the production environment after being free of malicious and/or unwanted code.

Ensure that no vulnerabilities or weaknesses are introduced into the company's production environment during change processes, ideally through code auditing and contractual protection for control and accountability in the event of third-party use.

Define formal rules for installing software and hardware in the corporate production environment, as well as in the approval and development environment, and enforce compliance within the company.

Conduct periodic audits of technical configurations and risk analysis.

Take responsibility for the use, handling, and storage of digital signatures and certificates.

Ensure, as quickly as possible, upon formal request, that user access is blocked due to termination of employment, incident, investigation, or other situation that requires restrictive measures to safeguard company assets.

Ensure that all servers, workstations, and other devices with access to the company network operate with their clocks synchronized with META's time servers.

Monitor the IT environment, generating indicators and historical data on:

- use of installed network and equipment capacity;
- response time for internet access and access to META's critical systems;
- periods of downtime in accessing the internet and META's critical systems;
- security incidents (viruses, Trojans, theft, unauthorized access, etc.);
- activity of all employees during access to external networks, including the internet (e.g., websites visited, emails received/sent, file uploads/downloads, among others).

3.2 Information Security

Propose specific methodologies and processes for Information Security, such as risk assessment and information classification systems.

Propose and support initiatives aimed at the security of META's information assets.

Publish and promote the versions of Information Security policies and standards approved by management.

Promote employee awareness of the relevance of Information Security to META's business through campaigns, lectures, training, and other internal marketing means.

Support the evaluation and adaptation of specific Information Security controls for new systems or services.

Critically analyze incidents in conjunction with management.

Maintain effective communication with management on issues related to the topic that affect or have the potential to affect META.

Seek alignment with the institution's corporate guidelines.

5. Monitoring and auditing of the environment

To ensure compliance with the rules mentioned in this policy, META may:

- implement monitoring systems on workstations, servers, email, internet connections, mobile or wireless devices, and other network components. The information generated by these systems may be used to identify users and their respective accesses, as well as the material handled;

- make public the information obtained by the monitoring and auditing systems, in the event of a court order, request from the manager (or superior) or by determination of the Information Security Committee;

- carry out, at any time, physical inspections of the machines it owns;

- install protective, preventive, and detectable systems to ensure the security of information and access perimeters.

6. Electronic mail

The purpose of this guideline is to inform Meta employees of the activities that are permitted and prohibited regarding the use of corporate email.

The use of META email is for corporate purposes and related to the employee's activities within the institution. The use of this service for personal purposes is permitted as long as it is done with common sense, does not harm the META Group, and does not impact network traffic.

We would like to add that employees are prohibited from using META email to:

- send unsolicited messages to multiple recipients, except when related to the legitimate use of the institution;

- sending messages by email from their department's address or using another person's username or email address that they are not authorized to use;

- sending any message by electronic means that makes the sender and/or META or its units vulnerable to civil or criminal action;

- disclose unauthorized information or screen images, systems, documents, and the like without express and formal authorization granted by the owner of such information asset;

- falsify addressing information, tamper with headers to hide the identity of senders and/or recipients, with the aim of avoiding the penalties provided for;

- delete relevant email messages when any of META's units are subject to any type of investigation.

- produce, transmit, or disclose messages that:

i. contain any act or provide guidance that conflicts with or contradicts the interests of META;

ii. contain electronic threats, such as spam, mail bombing, or computer viruses;

iii. contain files with executable code (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) or any other extension that poses a security risk;

iv. aims to gain unauthorized access to another computer, server, or network;

v. aim to interrupt a service, servers, or computer network through any illegal or unauthorized method;

vi. aim to circumvent any security system;

vii. aim to secretly monitor or harass another user;

viii. aim to access confidential information without the explicit authorization of the owner;

ix. attempt to improperly access information that may cause harm to any person;

x. include encrypted or otherwise masked images;

xi. contain attachments larger than 10 MB for sending (internal and internet) and 10 MB for receiving (internet);

xii. have content that is considered inappropriate, obscene, or illegal;

xiv. whether of a slanderous, defamatory, degrading, infamous, offensive, violent, threatening, pornographic nature, or of a similar nature;

xv. contains prejudiced persecution based on sex, race, physical or mental disability, or other protected situations;

xvi. has local or national political purposes (political propaganda);

xvii. includes material protected by copyright without the permission of the copyright holder.

xviii. E-mail messages must always include a signature in the following format:

- Employee name
- Management or department
- Company name
- Phone number(s)
- Email

7. Internet

All current META guidelines are basically aimed at developing eminently ethical and professional behavior in the use of the internet. Although the direct and permanent connection of the institution's corporate network to the internet offers great potential benefits, it opens the door to significant risks to information assets.

Any information that is accessed, transmitted, received, or produced on the internet is subject to disclosure and audit. Therefore, META, in full legal compliance, reserves the right to monitor and record all access to it.

The equipment, technology, and services provided for internet access are the property of the institution, which may analyze and, if necessary, block any file, website, email, domain, or application stored on the network/internet, whether on a local disk, workstation, or private areas of the network, in order to ensure compliance with its Information Security Policy.

By monitoring the internal network, META intends to ensure the integrity of data and programs.

The internet provided by the institution to its employees, regardless of their contractual relationship, may be used for personal purposes, provided that it does not interfere with the progress and productivity of work at the units.

Any attempt to alter security settings by any employee without proper accreditation and authorization will be deemed inappropriate, and the related risks will be reported to the employee and their manager. The use of any resource for illegal activities may result in administrative actions and penalties arising from civil and criminal proceedings, in which case the institution will actively cooperate with the competent authorities.

As it is in META's interest that its employees are well informed, the use of news sites or services, for example, is acceptable, provided that it does not compromise network bandwidth during strictly business hours, does not disrupt the smooth running of work, and does not imply conflicts of interest with its business objectives.

Only employees expressly authorized to represent Meta before the media may express themselves by email, interviews, podcasts, physical documents, or any other format.

Only employees authorized by the institution may copy, capture, print, or send screen images to third parties, in compliance with copyright law, image protection guaranteed by the Federal Constitution, and other legal provisions.

The disclosure and/or improper sharing of administrative information on discussion lists, websites or social networking sites, chat rooms, instant messengers or any other related technology that may arise on the internet is prohibited.

Employees with internet access may only download programs directly related to their activities at META and must take the necessary steps to regularize the license and registration of these programs, provided they are authorized by the manager.

The unauthorized use, installation, copying, or distribution of software protected by copyright, trademark, or patent on the internet is expressly prohibited. Any unauthorized software downloaded will be deleted by the Service Desk team.

Employees may not, under any circumstances, use META's resources to download or distribute pirated software or data, which is considered a criminal offense under national law.

Employees with internet access may not upload any software licensed to META or data owned by META to their partners and customers without the express authorization of the person responsible for the software or data.

The download and use of entertainment programs or games may be carried out by users whose professional activities are related to these categories. To this end, security groups shall be created and their members shall be defined by their respective managers.

Employees may not use META's resources to deliberately spread any type of virus, worm, Trojan horse, spam, harassment, disruption, or programs to control other computers.

Access to peer-to-peer software (Torrent and similar) is not permitted.

Access to proxy sites is not permitted.

8. Identification

Identification devices and passwords protect the identity of employee users, preventing and stopping one person from impersonating another before META and/or third parties.

The use of another person's identification devices and passwords constitutes a crime under the Brazilian Penal Code (art. 307 – false identity). This guideline aims to establish criteria for responsibility for the use of identification devices and should be applied to all employees.

All identification devices used at META, such as employee registration numbers, system access identifications, certificates, digital signatures, and biometric data, must be associated with a natural person and unequivocally linked to their official documents recognized by Brazilian law.

The user linked to such identification devices will be responsible for their correct use before META and civil and criminal law.

Therefore, any and all personal identification devices may not be shared with other people under any circumstances.

If there is a login shared by more than one employee, responsibility before META and civil and criminal law will lie with the users who use it. Only if the manager of shared use is identified as having knowledge or requested it will they be held responsible.

Sharing login details for system administration functions is prohibited.

META's Human Resources Department is responsible for issuing and controlling physical identity documents for employees.

Visitors, interns, temporary employees, regular employees, and service providers, whether individuals or legal entities, must be clearly identified. When accessing the local network environment for the first time, users must immediately change their password in accordance with the guidelines provided.

All users must create passwords with a minimum length of 14 characters and must understand the minimum requirements stipulated in the Password Policy, which are at least 3 of the 4 types of characters below:

- Capital letters (A-Z);
- lowercase letters (a-z);
- Numbers (0-9);
- Special characters (!, @, #, $, %)

It is the responsibility of each user to memorize their own password, as well as to protect and safeguard the identification devices assigned to them.

Passwords should not be written down or stored in unencrypted electronic files, such as Word documents, Excel spreadsheets, or other formats accessible in human language. In addition, they should not be based on personal information such as your first and last name, family members' names, date of birth, address, vehicle license plate number, company name, or department name. It is also essential to avoid obvious keyboard sequences, such as "abcdefgh" or "87654321." To enhance security, the names of partner companies, customers, and suppliers are automatically blocked by an automated solution.

After three (3) failed login attempts, the user's account will be locked. The account will be automatically unlocked after 15 minutes. However, in urgent cases, users may contact the Service Desk team via WhatsApp or email at ti@meta.com.br, providing their login and CPF (Individual Taxpayer ID) number.

A process must be established for identity confirmation before password renewal.

Passwords must be changed at least every 90 (ninety) days, and the last 5 (five) passwords cannot be repeated. Critical and sensitive systems for the institution and logins with administrative privileges must require password changes during the same period. All access must be immediately blocked when it becomes unnecessary.

Therefore, as soon as a user is terminated or requests termination, the Human Resources Department must immediately notify the Information Technology Department so that this measure can be taken. The same applies to users whose contract or service provision has ended, as well as to test users and other similar situations.

If an employee forgets their password, they must formally request a change through the above-mentioned means, appear in person at the responsible technical area, or use the online means for requesting a password change, available at: https://passwordreset.microsoftonline.com/passwordreset.

Access is monitored and, upon identification of brute force attacks, users will be automatically requested to change their password. If this request recurs, the user must contact the Information Security team so that appropriate measures can be taken and the attackers blocked.

9. Computers and technological resources

The equipment available to employees is the property of META, and it is the responsibility of each employee to use and handle it correctly for activities that are in the interest of the institution, as well as to comply with the recommendations contained in the operating procedures provided by the responsible managers.

Any physical or logical maintenance, installation, uninstallation, configuration, or modification is prohibited without the prior knowledge and supervision of a META Information Technology technician or someone they designate. Managers who need to perform tests must request them in advance from the Service Desk coordinator and will be legally and technically responsible for the actions taken.

All updates and security fixes to the operating system or applications may only be made after proper validation in the respective approval environment and after they have been made available by the manufacturer or supplier.

Systems and computers must have antivirus software installed, activated, and permanently updated. In case of suspected viruses or functionality issues, the user must contact the responsible technical department by registering a call with the help desk.

The transfer or disclosure of any software, program, or computer instructions to third parties, by any means of transport (physical or logical), may only be carried out with the proper identification of the requester, if positively verified, in accordance with the classification of such information and also with the actual need of the recipient.

Personal files not relevant to META's business (photos, music, videos, etc.) should not be stored on devices belonging to Meta, nor on the SharePoint provided by Meta. If such files are identified, they may be permanently deleted after prior notification to the user.

Documents that are essential for the activities of the institution's employees must be saved on the SharePoint provided by Meta. Such files, if saved only locally on computers (for example, on the C: drive), will not be guaranteed to be backed up and may be lost in the event of a computer failure, and are therefore the responsibility of the user.

META employees and/or privileged account holders must not execute any type of command or program that may overload existing services on the corporate network without prior request and authorization from the Information Technology department.

When using computers, equipment, and IT resources, certain rules must be followed.

- All computers for individual use must have a BIOS password to restrict access by unauthorized employees. These passwords will be set by META's Information Technology department, which will have access to them for equipment maintenance.

- Employees must inform the technical department of any foreign device connected to their computer.

- It is prohibited to open or handle computers or other IT equipment for any type of repair that is not performed by a META Information Technology technician or by third parties duly contracted for the service.

- Consumption of food, beverages, or tobacco at workstations and near equipment is strictly prohibited.

- All users must follow the rules and guidelines established in the Acceptable Use Policy for Devices.

Employees must maintain the configuration of the equipment provided by META, following the security controls required by the Information Security Policy and the institution's specific rules, assuming responsibility as custodians of information.

- All computer terminals must be password protected (locked) in accordance with the Password Policy and Acceptable Use Policy for devices when not in use.

- All technological resources acquired by META must have their default passwords changed immediately.

- Equipment must securely preserve event logs, including employee identification, dates, and times of access.

We have added some situations in which the use of META computers and technological resources is prohibited.

- Attempting or obtaining unauthorized access to another computer, server, or network.

- Circumventing any security systems.

- Accessing confidential information without the explicit authorization of the owner.

- Secretly monitoring others through electronic devices or software, such as packet analyzers (sniffers).

- Interrupting a service, servers, or computer network through any illegal or unauthorized method.

- Use any type of technological resource to commit or be an accomplice to acts of violation, sexual harassment, disturbance, manipulation, or suppression of copyright or intellectual property without the proper legal authorization of the owner.

- Hosting pornography, racist material, or any other material that violates the laws in force in the country, morality, good customs, and public order.

- Using pirated software, an activity considered a crime under national law.

10. Mobile devices

META wishes to facilitate mobility and the flow of information among its employees. Therefore, it allows them to use portable equipment.

The term "mobile device" refers to any electronic equipment with mobility features owned by the institution or approved and permitted by the responsible Information Technology department, such as notebooks and smartphones.

This guideline aims to establish criteria for handling, prevention, and responsibility for the use of mobile devices and should be applied to all employees who use such equipment.

META, as the owner of the equipment provided, reserves the right to inspect it at any time if necessary to perform security maintenance.

Employees therefore undertake not to use, reveal, or disclose to third parties, in any way, directly or indirectly, for their own benefit or that of third parties, any information, whether confidential or not, that they have or may become aware of as a result of their duties at META, even after the termination of their employment contract with the institution.

All employees must periodically make backup copies of the data on their mobile devices. They must also keep these backups separate from their mobile devices, i.e., not carry them together. META provides Microsoft's OneDrive system for storing your files.

Technical support for mobile devices owned by META and its users must follow the same support flow contracted by the institution.

All employees must use automatic lock passwords for their mobile devices.

Unauthorized reproduction of software installed on mobile devices provided by the institution constitutes misuse of equipment and a legal violation of the manufacturer's copyright.

The use of broadband networks in locations known to the employee, such as their home, hotels, suppliers, and customers, is permitted.

Under no circumstances will changes to the configuration of equipment operating systems be permitted, especially those related to security and log generation, without proper communication, authorization from the responsible area, and without the guidance, assistance, or presence of an IT Management technician. Employees are responsible for not maintaining or using any programs and/or applications that have not been installed or authorized by an IT Management technician at META.

In the event of theft or robbery of a mobile device provided by META, it is the employee's responsibility to immediately notify their direct manager and IT Management.

They must also seek the help of the police by filing a police report as soon as possible.

Third-party portable devices must undergo prior equipment evaluation and have META's antivirus tool installed.

Employees should be aware that misuse of mobile devices will result in them assuming all risks of misuse and being solely responsible for any direct or indirect damages, present or future, caused to META and/or third parties.

11. Data Center

Access to the Data Center should only be made through a strong authentication system. For example: biometrics, magnetic card, among others. All access to the Data Center through the strong authentication system must be recorded (user, date, and time) using proprietary software.

The "administrator" user of the strong authentication system will be in the possession and administration of the Infrastructure coordinator.

In locations where there are no information technology employees, people from other departments must be registered in the access system so that they can perform operational activities within the Data Center, such as: changing backup tapes, providing support for any problems, and so on.

Visitors or third parties may only access the premises when accompanied by an authorized employee.

Access to the Data Center, via key, may only occur in emergency situations, when the physical security of the Data Center is compromised, such as by fire, flood, structural damage to the building, or when the strong authentication system is not working.

If non-emergency access is required, the requesting area must request authorization in advance from any employee responsible for managing access, as listed in the Data Center Access Control Procedure, which can be obtained from the system.

The Datacenter must be kept clean and organized. Any procedure that generates waste or dirt in this environment may only be carried out with the collaboration of the General Services Department.

No food, beverages, smoking products, or flammable products are allowed.

The entry or removal of any equipment from the Data Center will only occur after the requesting employee has completed the release request and the Data Center manager has formally authorized it, in accordance with the terms of the Equipment Control and Transfer Procedure.

In the event of termination of employees or collaborators who have access to the Data Center, their exclusion from the strong authentication system and the list of authorized collaborators must be immediately arranged, in accordance with the process defined in the Data Center Access Control Procedure.

12. Backup

All backups must be automated by automated scheduling systems so that they are preferably performed outside business hours, in so-called "backup windows." These are periods when there is little or no access by users or automated processes to the computer systems.

Employees responsible for managing backup systems should perform frequent validations to identify corrective updates, new product versions, life cycle, and suggestions for improvements.

Backup media (such as DAT, DLT, LTO, DVD, CD, and others), when used, should be stored in a dry, air-conditioned, secure location (preferably in fireproof safes in accordance with ABNT standards) and as far away from the data center as possible.

When used, backup tapes must be properly identified, preferably with non-handwritten labels. The lifespan and use of backup media must be monitored and controlled by those responsible, with the aim of excluding media that may present recording or restoration risks due to prolonged use beyond the manufacturer's recommended period.

Media that present errors must first be formatted and tested. If the error persists, they must be rendered unusable.

Historical or special backup media should be stored in secure facilities, preferably with a vault structure, at least 10 kilometers away from the Data Center.

Essential backups, considered critical to the proper functioning of META's business, require a special retention rule, as provided for in specific procedures and in accordance with the Information Classification Standard. This is in accordance with existing tax and legal requirements in the country.

In the event of a backup or restore error, the process must be performed manually by the responsible team at the earliest opportunity after identification.

Restore tests should be performed periodically, as agreed between the teams involved. Currently, this period is defined as: every six months.

As this is a simulation, the executor must restore the files to a location other than the original, so as not to overwrite the valid files.

The employees responsible, as described in the appropriate procedures and in the responsibility spreadsheet, may delegate the operational task to a custodian when, for reasons of force majeure, they are unable to perform it. However, the custodian cannot be exempted from responsibility for the process.

13. Final provisions

Like ethics, security must be understood as a fundamental part of META's internal culture. In other words, any security incident is understood as someone acting against the ethics and good customs governed by the institution.

History			
Date	Version	Description	Author
06	0.1.0	Political Construction	IT
06	0.2	Nomenclature Adjustments	IT
06	0.	Technical Changes and Nomenclatures	IT
05	0.	Technical Changes	IT
06	0.5	Technical Management Change	IT
08	0.6.0	General Document Review	IT
09/2024	0.6.1	General Document Review	Information Security
03	0.7	Technical changes and links to current documentation and standards	Information Security

COVERAGE: BRAZIL

ADMINISTRATIVE RESPONSIBILITY: Jefferson Sanção Cardoso - CTO

LAST REVISION: MAR/2025

START DATE: JANUARY/2016 IT DIRECTOR: CLAUDIO CARRARA

NEXT REVIEW: MAR/2026

Meta Digital. Simple. Human.

Questions?

Contact: compliance@meta.com.br