Information Security Policy

INDEX

10000 Highway 55
Minneapolis, MN 55441
USA

Rua Visconde de Pirajá 66
Rio de Janeiro, RJ 22410-000
Brazil

1. OBJECTIVE

The purpose of this policy is to establish a standard to secure information – in physical or electronic form – that are sensitive for FIELO and its clients.

2. SCOPE

All Fielo staff is subject to this policy. Internal use only.

3. DEFINITIONS

- **Computer:** Any device used to access and/or store information
- **Computer System:** Group of devices, software and network that may include external access to Internet.
- **Staff:** Employees and entities working on behalf of FIELO
- **Sensitive Data:** Customer information or information related to internal projects or Fielo business marked as classified. See Data Classification.

4. RULES

4.1. Computer and Email Usage

To support your work, FIELO may give you access to computers, computer files, email system, and software. You cannot use a password, access a file, or retrieve any stored information without authorization. To make sure that all staff follow this policy, we may monitor computer and email usage.

You cannot use your email to ask other people to contribute or to tell them about business outside of FIELO company, outside organizations, or any other non- business matters.

FIELO buys and licenses computer software for business purposes. We do not own the copyright to of this software or its documentation. Unless the software developer authorizes us, we do not have the right to use the software on more than one computer.

You may only use software on local area networks or on multiple machines according to the software license agreement. FIELO prohibits the illegal duplication of software and its documentation.

If you know about any violation of this policy, notify your supervisor, the Human Resources Department, or your leader. Any member of the staff who violates this policy is subject to disciplinary action, up to and including termination of employment.

4.2. Internet Usage

All Internet data that written, sent, or received through Fielo computer systems is part of official FIELO records. That means that we may be legally required to provide that information to law enforcement or other parties. Therefore, you should always make sure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and legal.

The services and technology that you use to access the Internet are property of FIELO. Therefore, we reserve the right to monitor how you use the Internet. We also reserve the right to find and read any data that you write, send, or receive through our online connections or is stored in our computer systems.

You may not write, send, read, or receive data through the Internet that has content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person.

Examples of unacceptable content includes (but are not limited to) sexual comments or images, racial slurs, gender-specific comments, or other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

FIELO does not allow the unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet. As a general rule, if you did not create the material, do not own the rights to it, or have not received authorization for its use, you may not put the material on the Internet. You are also responsible for making sure that anyone who sends you material over the Internet has the appropriate distribution rights.

If you use the Internet in a way that violates the law or FIELO policies, you will be subject to disciplinary action, up to and including termination of employment. You may also be held personally liable for violating this policy.

The following are some examples of prohibited activities that violate this Internet policy:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and resources for personal gain
- Stealing, using, or disclosing someone else's code or password without authorization
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
- Violating copyright law
- Failing to observe licensing agreements.

- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions.
- Sending or posting messages or material that could damage the organization's image or reputation.
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals.
- Attempting to break into the computer system of another organization or person.
- Refusing to cooperate with a security investigation.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Using the Internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems
- Sending or posting messages that disparage another organization's products or services.
- Passing off personal views as representing those of the organization
- Sending anonymous email messages

It is prohibited to store sensitive data of FIELO on computers, it is responsibility of the Staff to keep this data in cloud storage provided by FIELO.

4.3. Password protection

Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of critical (organization) resources. As such, all (organization) staff and outside contractors and vendors with access to our systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4.3.1. IT Support Professionals

All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed every 90 days. All systems administrative-level passwords for production environments must be part of an ITSS administered global password management database. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user. Where SNMP (system network management protocol) is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

A keyed hash must be used where available (e.g., SNMPv3).

4.3.2. General Users

All user-level passwords (e.g., email, web, desktop computer, etc.) **must be changed every 90 days**. Passwords must not be included in email messages or other forms of electronic communication. Passwords must be at least 8 characters length.

All user-level and system-level passwords must be according to the guidelines described below.

- **Do not use USB sticks or any other internal device** without authorization from the admin.
- All machines have only one admin provided by Fielo.
- The Fielo machines come with Google Workspace sign in configured (login and register with the same rules as the password see below in 4.3.3)

4.3.3. Guidelines

General password construction guidelines are used for various purposes at (organization), i.e., user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins). It is important that everyone be aware of how to create strong passwords.

Poor, weak passwords have the following characteristics:

- The password can be found in a dictionary (English or foreign)
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, computer terms and names, commands, sites, companies, hardware, software, birthdays, and other personal information such as addresses and phone numbers.
- Word or number patterns like rabab, qwerty, swivels, 123321, etc. Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is creating a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

4.3.4. Password protection standards

- Password protected screen savers are mandatory for laptops.
- Change passwords at least once every 90 days.
- Do not write down passwords.
- Do not store passwords on-line without encryption.
- Do not use the same password for (organization) accounts as for other non (organization) access (e.g., personal ISP account, on-line banking, email, benefits, etc.).
- Do not share (organization) passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential (organization) information.
- Do not reveal a password over the phone to ANYONE.
- Do not reveal a password in an email message.
- Do not reveal a password to the boss.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., “my family name”)
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on vacation.
- Do not use the “Remember Password” feature of applications (e.g., Groupwise, Instant Messenger, Internet Explorer, Mozilla).
- If someone demands a password, refer them to this document or have them call the IT Service Desk.
- If an account or password is suspected to have been compromised, report the incident to IT security and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis by security personnel. If a password is guessed or cracked during one of these scans, the incident will be documented, and the user will be required to change their password.

4.4. Clean Desk

An effective clean desk effort involving the participation and support of all staff can greatly protect paper documents that contain sensitive information about our clients, customers, and vendors. The main reasons for a clean desk policy are:

- A clean desk can produce a positive image when our customers visit the company.

- It reduces the threat of a security incident as confidential information will be locked away when unattended.
- Sensitive documents on the desk can be stolen by a malicious entity.

4.4.1. Guidelines

- During extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.
- At the end of the working day the member of staff is expected to tidy their desk and to put away all office papers. FIELO provides locking desks and filing cabinets for this purpose.

4.4.2. Action

- Allocate time in your calendar to clear away your paperwork.
- Always clear your workspace before leaving for longer periods of time.
- If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shred bin.
- Before leaving a meeting room:
    - Always clean information posted to whiteboards.
    - Double check if you are not leaving any information in paper.
    - Consider scanning paper items and filing them electronically in your workstation.
    - Use the recycling bins for sensitive documents when they are no longer needed.
    - Lock your desk and filing cabinets at the end of the day.
    - Lock away portable computing devices such as laptops or PDA devices
    - Treat mass storage devices such as CDROM, DVD, USB drives or External HD as sensitive and secure them in a locked drawer.

4.5. Data Classification

A data classification policy provides a way to ensure that sensitive information is handled according to the risk that it poses the organization, the types of sensitive information handled by the organization and compliance requirements.

All documentation produced on behalf of Fielo should have a distinctive mark of the classifications below. In the absence of the classification, information will be considered “Public Use”. Any misguidance of information caused by the absence of its classification may cause its author subject to disciplinary action, up to and including termination of employment.

4.5.1. Public Use

The “Public Use” classification label applies to information that is available to the public and intended for distribution outside an organization. This information may be freely distributed without risk of harm. Any information that is produced for public consumption – such as new releases, job announcements, and sales brochures – are good examples.

4.5.2. Internal Use

The “Internal Use” classification label applies to information that is used in business processes, and the unauthorized disclosure, modification, or destruction of which is not expected to seriously affect the organization, customers, employees, or business partners. Any information that is used in routine business matters – such as internal policy manuals and company phone lists – are good examples.

4.5.3. Classified

The “classified” classification label applies to information that is used in sensitive business processes. The unauthorized disclosure, modification or destruction of this information will adversely affect an organization, its customers, employees, or business partners. Examples of sensitive information include intellectual property, contract negotiations, most personnel matters, personally identifiable information, protected health data, bank account numbers and payment card information of customers and employees.

5. Comodo endpoint secure

5.1. Protect System with comodo.

All machines delivered by Fielo to its collaborators come with the anti-virus comodo protect system that daily generates a scan of the machines in search of viruses or vulnerabilities in real time that can cause any type of invasion or loss of data by our collaborators.

5.2. Update the machine's Windows.

All the machines are updated by comodo automatically and its database is always in constant scanning for updates.

5.3. Virus warning on the machine

As soon as any kind of change of intruder or virus is detected, Comodo quarantines the file and sends an email immediately to Fielo Admin so that he can take appropriate action.

5.4. Machine Inventory

Comodo automatically detects machines where the programs are installed so we can have a complete inventory of hardware and software our employees are using.

6. Google Workspace

6.1. Log In

With the Google Sig in tool every computer is logged in via the Google Workspace login with the same password requirements as described above

6.2. FA Authentication

All users are needed to configure the 2-factor authentication tool to make more difficult for intruders to access the machine, as they need the employee's authorization via cell phone.

6.3. Google Drive Database

- The entire company database is at Google Workspace guidelines and security.
- All users are instructed to leave documents only on Google Drive.
- No documents are shared outside the company without Admin authorization (Google File Shared) and every document is traceable via Google's audit tool.

6.4. Google Mail

DLP (Data Loss Prevention) is implemented:

- Anti-virus scanning tool before the attachment is opened by anyone in the company.
- Anti Phishing tool (warns when an email could be a Phishing)
- Anti Phishing tool that warns when an email is external.
- All type of credit card, CPF, account bank data is not allowed to be typed in.
- Alert when login is done in a machine not recognized by the system.

6.5. Alert Center

- All unusual steps in Google Workspace are tracked and classified as priority LOW, MEDIUM and HIGH.
- Full auditing system in case of a data leak.

6.6. Google MDM

All our mobile devices are registered in the Google database and all devices can be deleted immediately if they are lost or stolen.

6.7. Google Audit

Google has a complete auditing tool in which we can trace any kind of abnormality or data leakage.