FILHORINI
ADVOGADOS ASSOCIADOS

Data Security Policy

1. Legislative References

This **Data Security Policy** ("**Policy**") refers, notwithstanding references to other legal documents with more general scope, to the following legal documents, with which it must at least conform, unless a higher standard is established hereby:

- Law 8,906/1994, Statute of the Legal Profession
- Code of Ethics and Discipline of the Brazilian Bar Association
- Law 12,965/2014, Internet Civil Framework
- Law 13,709/2018, General Data Protection Law ("**LGPD**") and its Regulations

The references above shall automatically include any alterations introduced in those documents and their possible replacement, and in all cases the application of this Policy shall be guided by good practices.

2. Objective, Definitions and Scope

This **Policy** is applicable and must be observed by all the partners, employees and outsourced workers under any title (**Users**) of **Filhorini Advogados Associados** (**Firm**), and has the objective of establishing guidelines and operating standards of the informatics resources, seeking to assure the security, availability, integrity, confidentiality, legality, authenticity, accuracy, completeness and auditability of the data treated by the **Firm.**

The expression **Informatics Resources** includes all the communication and data processing and storage devices owned by the **Firm** or contracted by it for this purpose, including microcomputers and autonomous storage units, as well as all the

computer programs, ranging from operating systems, firewalls, VPNs, antivirus software, and various other programs and applications contracted thereby for the processing of data inherent to the stated purpose of the **Firm**, their protection and good functioning (hereinafter collectively **Informatics Resources**).

The **Firm** will contract and keep in adequate and permanent functioning the physical and logical security tools of equipment, systems and data, as well as conduct ongoing security monitoring, to assure the good functioning and security of the **Informatics Resources**.

The term "treatment" in this **Policy**, when associated with data or information, shall have the meaning specified in Law 13,709/18 (LGPD), even if such data and information are not necessarily of a personal nature.

The term **Datum** (or **Data** in the plural) refers to all information in a digital medium for treatment by the **Informatics Resources** of the **Firm.** The definition of **Data** includes all data or information defined as personal by the Internet Civil Framework and the LGPD, as well as those considered secret or confidential according to the Statute of the Legal Profession and Code of Ethics and Discipline of the Brazilian Bar Association. The **Data** kept in other physical media, such as letters, power-of-attorney instruments and certificates, among others, are equally protected in conformity with specific standards not included in this **Policy**.

This **Policy** has the objective of informing, standardizing and assuring good and secure treatment of the **Data** of the **Firm**. However, it does not exhaust the matter, and in complying with the guidelines established in this **Policy**, as altered from time to time, **Users** shall be guided by the principle of precaution, i.e., in case of any doubt, the doubtful procedure will not be carried out, and support will be sought from the **System Administrator**, or the person delegated thereby for support

tasks.

The **Users** shall be responsible for the correct use of the **Informatics Resources** and the good and secure treatment of the **Data**, through compliance with the guidelines established in this **Policy**, as updated from time to time, with all the legal and ethical obligations regarding scope applicable by law to lawyers also extending to **Users** who are not lawyers.

The failure to comply with a conduct or procedure defined in this **Policy**, irrespective of the result, and without prejudice to the applicable legal sanctions, shall be interpreted as a grave violation of the Internal Rules, subjecting the offending **User** to administrative sanctions, including those specified in labor legislation.

3. Utilization of Technology Resources

The **Informatics Resources** are available to the members of the **Firm** for the performance of their activities in line with its stated purpose, and all members are responsible for the proper use, security and preservation of the secrecy of the **Data** treated.

Only the partners, associate lawyers, administrative employees and service providers of the **Firm** shall be entitled to possess a **User** login, which will be assigned by the **System Administrator**. Visitors will not, as a rule, have access to the **Informatics Resources,** and if this is necessary for any reason, a special login for temporary, limited and supervised access must be requested from the **System Administrator**.

Only the informatics service provider is authorized to alter the configurations of the

computers, install software updates/upgrades, redeploy equipment and perform other similar activities.

4. Management of Information Security Incidents

The suspicion of any breach or fragility of information security, even if only potential, or of an event resulting from a technical failure in an **Informatics Resource** (in each case a "**Security Event**"), must be immediately reported to the **Administrative Department** (including the **System Administrator**) and the **Data Protection Officer (DPO)**, to enable corrective action to be taken as quickly as possible.

When any **Security Event** results from the commission or omission of a **User**, negligent or intentional, the communication must also be extended to at least one of the **Managing Partners**, for the suitable measures.

The communication of any **Security Event** must contain a description of the facts and list all the evidence that, in the opinion of the communicator, indicates the occurrence of a **Security Event**, to be investigated immediately, and as the case may be, ascertained and corrected.

Suspected Breach of Security of Personal Data. In case of a **Security Event** that involves **Personal Data**, even if this is only suspected, the **Firm** shall immediately: **(i)** take all measures to cease such event and mitigate its effects; **(ii)** identify the universe of the affected **Data**, even if only potentially; **(iii)** even in the absence of proof, communicate the occurrence or possible occurrence of a **Security Event** as soon as possible **(iii.a)** to the data subject(s) and to the **(iii.b)** National Data Protection Authority (ANPD), describing the situation, the measures taken,

and if pertinent, the recommendations to stop or mitigate the losses and damages; **(v)** thoroughly investigate the **Security Event,** documenting it and promoting all the fitting corrections and remedial measures; and **(v)** investigate and monitor the occurrence with the ANPD and the subjects of the affected or potentially affected **Data** until complete conclusion, with formal communication to all those involved.

5. Coordinated Actions

Information security is also preserved by means of coordinated collective actions, such as:

- Action by the person responsible for Human Resources:
  - To internally disclose, mainly to the **System Administrator**, the hiring, reassignment and dismissal of personnel, for the purpose of approval or removal of accesses of **Users**.
  - To organize training sessions upon hiring of new employees, and also periodically to all **Users,** about the internal policies of the **Firm** regarding Data Security, Privacy and Best Practices, including this **Policy** and others that may replace or complement it.
- Action by the **System Administrator**:
  - To grant or remove access permission according to the information from the person in charge of HR and existing technological resources;
  - To periodically review accesses;
  - The activity of the **System Administrator** may be outsourced to an individual or legal entity, who shall be responsible for the operation of the **Informatics Resources**, under the supervision of the Managing Partners.
- Action by the Managing Partners as part of the compliance procedures:

- To control the levels of authority in relation to availability of access;
- To monitor the accesses and information;
- To disclose this **Policy** to the new members of the **Firm,** and when applicable, to outsourced service providers;
- To evaluate the adequacy and sufficiency of the existing security procedures and verify them on an ongoing basis, including periodic auditing to identify deficiencies and irregularities that can compromise security and organizational performance, with ongoing promotion of correction and updating.

Good Practices and Principle of Precaution. The practices described above are not intended to be comprehensive or literal, and do not exclude good sense and good market practices, which must always be guided based on the Principle of Precaution, which recommends refraining from any act about which doubt exists regarding the results or their extent. In such situations, the **System Administrator** must be contacted.

6. Physical Security and Premises

The **Firm** maintains a physical structure and premises that are adequate for its size and activities, and relies on procedures for prevention of unauthorized physical accesses, damages to installations, fraud and sabotage.

Restricted Areas. No service provider, visitor, client and/or other third party may enter the secure area without being accompanied by at least one member of the **Firm**, who shall have the obligation of assuring respect for the provisions of this **Policy**, including regarding the third party.

The secure area is defined as all the rooms reserved for the partners, associate

lawyers, office service providers and other employees, besides the physical spaces where the **Informatics Resources** are installed, notably the informatics and telephone connection racks and servers.

The restrooms and meeting rooms are considered to be outside the secure area. In these spaces, WiFi internet access shall be provided, with a structure that does not involve the **Informatics Resources**.

7. Classification of Information

It is the responsibility of each partner to establish criteria related to the level of confidentiality of the **Data** (documents, reports and/or media) treated by his/her area, as follows:

(1) **Public** / (2) **Internal** / (3) **Confidential**

Public Information: Information that can be accessed by any **User,** client, supplier, service provider and the public in general, and that is not confidential in nature. In general, this includes information about the **Firm** and the services rendered by it for informative purposes, which can be made available at the **Firm's** website.

Internal Information: Information that is directly or indirectly related to the activities of the **Firm** and that can only be accessed by the partners and associate lawyers. The secrecy of all Internal Information and **Data** must be preserved and may not be disclosed to third parties, except to persons who have a need to know that information to perform their activities.

Confidential Information: Information that can only be accessed by qualified

persons, among them, for example:

(a) **Personal data** of partners, associate lawyers, outsourced service providers and employees under any title, must be restricted to the Human Resources Department and the partners;

(b) **Contracts of the Firm**. The contracts of the **Firm** with other law firms and legal professionals, service providers and others may only be accessed by the partners and administrative staff.

(c) **Contracts with Clients**. The agreements for provision of legal services may only be accessed by the partners and administrative staff.

(d) **Documents of Clients**. Documents of clients that are defined as secret, such as those identifying earnings, tax information, identity details and data related to health.

(e) **Strategic or Confidential Cases**. These are restricted to the partners and associate lawyers who are working on the case.

As a general rule, since the purpose of the **Firm** is to render legal services, the Internal Information must always be treated as confidential and secret.

The classification "Confidential Information" in general refers to information about clients and the matters related to their representation by the **Firm**, where the degree of confidentiality and secrecy is determined by law and whose disclosure not only is configured as a crime, but also can cause moral or pecuniary damages, not only to third parties, but also the market, is would be the case of strategic information about business transactions, changes of labor policies, or even private information such as that associated with divorce and inheritance.

In any event, it is important always to bear in mind that even in the most routine and ordinary cases, the existence is possible of confidential documents that must be segregated and treated as such, under the responsibility of the partners and associate lawyers handling the case.

Access to Confidential Information by service providers depends on the formalization of a Confidentiality Agreement.

All the requirements, conditions and necessities must be formally communicated to the **System Administrator**.

8. Ownership of Information

All the **Data**, i.e., the information generated, treated and stored in the technological environment of the **Firm,** are its property, irrespective of the origin, content or purpose, including the content of e-mails, text messages and correspondence.

9. Safekeeping and Deletion of Information

The partners and associate lawyers must observe the following general rules:

- Keep in drawers or cabinets with locks or other security mechanisms only the documents, papers and media strictly necessary that contain sensitive or critical information about the **Firm** and its clients;
- During temporary absences or after the end of the working day, all working materials that can compromise Information Security must be safeguarded;
- Only print or make copies of documents when absolutely necessary and discard documents adequately when they are no longer needed;

- Immediately retrieve printed documents from the printer, mainly those that contain sensitive and confidential information;
- When discarding papers, check whether they contain restricted information, and if so, shred them before discarding them.
- When working at home, keep physical documents in specific and adequate places, and only as strictly necessary to render services, do not leave them in view of third parties, and dispose of them adequately when they are no longer necessary.

10. Access Tokens and Passwords

The members of the **Firm** have individual and personalized passwords for access to information, which according to the activity of each person, allows him/her to include, exclude, alter or consult **Data**.

The passwords must have the following configurations:

- Not contain significant parts of the user name or the full name;
- Have at least six characters;
- Contain characters from three of the four following categories:
    - Uppercase letters from the English alphabet (A-Z)
    - Lowercase letters from the English alphabet (a-z)
    - Numeric characters (0-9)
    - Non-alphabetic characters (such as !, $, #, %)

The requirements for complexity are imposed when passwords are created or altered.

The passwords must be altered whenever solicited by the system and periodically by

the **User**, each three months. It is advisable for the **User** to alter the password completely, not just by changing a single character.

The password must never be disclosed to third parties (verbally or in writing in a public place), or memorized through automatic logins, macros or function keys.

The passwords are the personal responsibility of the **User**, and all accesses with his/her password will be attributed to him/her.

The password does not afford any right to privacy of the **User**.

11. Solicitation for Access by New Members

It is the exclusive responsibility of the person in charge of HR affairs to inform the **System Administrator** about the hiring of new members.

The accesses to the network and systems by new members must be approved in advance by the Managing Partners.

Likewise, the person in charge of HR affairs must report the severance of members to the **System Administrator** for the suitable measures.

12. Change of Access Profile

Requests to include/exclude access authorization of **Users** must be presented to the informatics service provider by the Managing Partners, or by the person in charge of HR affairs after express approval of the Managing Partners.

13. Logoff and Logout of Equipment

a) Screen Protection

The computers of the **Firm** have screen protection (screensaver) based on time of inactivity.

b) Logoff During Temporary Absences

When absent from the workstation (lunch hour, meetings, etc.), the **User** must block the password through the instruction "Block Computer", to protect against improper accesses, under his/her responsibility.

c) Logout and Turning off Equipment

The computers must be turned off at the end of the working period, with each **User** of the equipment being responsible for turning it off, or seeing that this is done.

14. Utilization of Laptops and other Computer Equipment

- The protection of the personal computer devices is the responsibility of the respective **User**;
- Each **User** is responsible for assuring the integrity of personal devices and the safekeeping and confidentiality of the information contained therein;
- **Users** may not alter the configuration of equipment received from the **Firm**.

- As a rule, confidential **Data** should not be kept stored in personal devices, and when away from the **Firm**, such **Data** stored in the cloud should accessed via the **VPN**.

Some safeguards must be observed:

➢ **Outside the Firm:**

- Always keep the devices with you.
- Pay close attention in restaurants, hotel lobbies, airports, airplanes and taxis.
- When transporting devices by car, always use the trunk or other non-visible place.
- Avoid carrying devices in the street.
- Under no circumstance may devices be taken to fitness centers and left in lockers or under the care of dressing room attendants, to bars and restaurants for events like happy hours, and left in hat rooms or on tables in places with large movement.

➢ **In case of theft and/or robbery:**

- Immediately report the occurrence at a police station.
- Report it to the Partner in charge and the **System Administrator.**
- If the device allows, remotely erase the data.

15. Computer Viruses

As a fundamental rule, the **Firm** does not use any illegal software and forbids its members to use such programs in its **Informatics Resources**. The **Firm's Informatics Resources** only contain programs and applications approved by the **System Administrator**.

The use of illegal ("pirated") software, as well as freeware and the like, is directly associated with contamination of the system by viruses, worms, Trojan horses and ransomware, so that the installation and use of such applications, especially over the internet, is flatly prohibited, and will be considered a grave fault.

The internet is also probably the most common route of contamination of systems, so **Users** must not access insecure sites, open files or click on links that are unknown and/or received from unknown sources or in a suspicious situation.

Although the **Firm** has an antivirus program installed in all its informatics devices, with automatic updating and verification in real time, the opening of contaminated files can still bring serious consequences.

In case of doubt about the sender or content when receiving e-mail, do not open attachments or click on links. Report the matter immediately to the informatics service provider and other team members.

16. Internet Access

It is not permitted to install programs downloaded from the internet in the **Firm's** computers without the express consent of the informatics service provider, except the programs offered by federal, state and/or municipal public bodies. **Users** must confirm they are not executing actions that can infringe the copyrights, trademarks, licenses or patents of third parties. When navigating on the internet, it is forbidden to visualize, transfer (download), copy or perform any other access to sites:

- of radio and TV stations;
- with pornographic content or images and videos related to sex;
- involving sharing and distribution of files;

- that advocate illegal activities;
- that denigrate, belittle or incite prejudice against determined classes;
- that promote participation in chat rooms;
- that permit transfer (download) of illegal files and/or programs.

The informatics service provider is authorized to monitor accesses. The partners can analyze all accesses, randomly or selectively.

17. Electronic Mail (Outlook)

The electronic mail (e-mail) system of the **Firm** is Outlook and must be used exclusively for professional purposes. All the messages and other content stored/exchanged by Outlook are the property of the **Firm** and may be monitored.

All information received through e-mail must be treated as Confidential Information owned by the **Firm**, including any personal e-mails.

The members are responsible for the messages sent in their name, and must pay heed to the following items:

The "***Reply all***" function should only be used in justified cases; otherwise use "Reply", only to the sender;

- Messages with files attached have a strong impact on the available space on the server, so never distribute messages with files attached without need;
- E-mail messages are classified as formal documents of the **Firm,** so they must be prepared with language coherent with the professional activity;
- Messages must not contain defamatory statements and/or offensive

language;

- Messages must not be hostile;
- Do not reply to "chain" messages or those with pornographic content, which can damage the image of the **Firm** and its members.

18. Instant Messages (MSG)

Users must bear in mind and observe that the communication by short text messages, be it directly over the cellphone network or via applications or platforms, is intended exclusively for coordinated acts, such as confirmation of sending e-mails and files and confirmation of meetings, among others.

Although various applications have the capacity to send and receive files, the use of this facility for the purpose of sharing professional information should be avoided. Instead, preference should be given to using the institutional e-mail of the **User** at the **Firm**, notably because certain applications are not contained in the **Firm's Informatics Resources**, so that such communications are not regularly backed up or scanned by antivirus applications, and the uploading of such files can pose a risk to the **Informatics Resources** as a whole.

Notwithstanding the foregoing, **Users**, between each other and with third parties, must give formal treatment and adopt an essentially professional form of treatment, to avoid ambiguities and forbidden behaviors.

19. Virtual Private Network (VPN) and Remote Access

The **Firm's Informatics Resources** include applications such as firewalls,

antivirus programs and a **VPN**, which permits their remote use via the internet.

However, for access outside the internal environment of the **Informatics Resources**, the **Users** are responsible for safeguarding the confidentiality of the information accessed outside the premises of the **Firm**, both with regard to physical security, by carrying on their personal devices only the data and information strictly necessary, and by using the protection of the **Firm's VPN** for remote access, with redoubled observation of the other rules and recommendations contained in this **Policy**.

20. Wireless Access

The **Firm** has wireless access to the internal network available to **Users** in most of the working rooms and also in the meeting rooms. The access by non-users must be by the wireless network for visitors, which does not permit access to the **Firm's** internal network.

The passwords for access to the wireless network by **Users** may not under any circumstance be shared with third parties, including visitors and service providers that do not need to have access to the **Firm's** internal network.

If third parties, including commercial partners, visitors, clients, service providers or others, need to access the **Firm's** internal network, either by wireless or wired means, a specific request must be submitted to the **System Administrator**, who after approving it, will supply a specific password and login with the adequate permission levels.

In the event of any suspicion that a password of a wireless **User** has been compromised, its substitution must be promptly requested and this fact (a **Security**

Event) must be reported immediately to the **System Administrator**.

21. Data Storage

The **Data** of the **Firm** is stored remotely (cloud), so that security backup copies are made regularly.

The location and nomenclature of the storage folders (directories) must obey the specific standardized instructions, as a rule oriented for each client, case and activity, to provide agility in the searches so that all **Users** can have access to the folder in question.

The work should preferably be carried out directly using the information contained in the working folder in the **Firm's** network, to assure the use by everyone of the same file, in the same version, and to avoid undue duplication and propagation of unauthorized copies.

Exceptionally, **Users** can make copies, either in a place other than the network or on their own personal devices, for the purpose of enabling the performance of work where concurrent access by multiple **Users** can hamper that work, or also in conditions where access to the internet is poor or nonexistent, always observing the rules and recommendations of this **Policy** and good practices.

In these situations, the file must be identified and handled adequately, so as not to hamper the work of other members of the group involved in rendering services. The copy must be deleted as soon as the need that gave rise to it ceases, and the working file, before being uploaded to the network, must be tested to detect electronic viruses, malware, Trojan horses and the like. Uploading without this verification will not be authorized.

Users must avoid keeping copies of folders in their computers or other devices, restricting such copies to work in progress and in the authorized situations described above, to avoid compromising the security of data due to loss or theft of equipment or hacking of computers (notebooks or others).

In particular, special attention must be given to external storage devices, such as hard drives and pen drives. As a general rule, only the **System Administrator** may copy data in such devices, in all cases registering their existence.

Exceptionally, the use of such devices can be authorized in specific situations to enable the transport and transfer of data when it is not possible or advisable to do so via the network, either for reasons of security or technical factors.

In any event, when the reasons authorizing the use of such devices end, they must be erased and formatted, preferably by the **System Administrator**.