INFORMATION SECURITY POLICY

OF COSTA & LEMOS SOCIEDADE DE ADVOGADOS

Introduction

This Information Security Policy ("ISP") aims to establish rules, controls and responsibilities regarding the treatment of information performed by COSTA & LEMOS SOCIEDADE DE ADVOGADOS ("Firm"), in compliance with the requirements of the Brazilian data protection legislation, including, without limitation, Law No. 13,709/2018 - Data Protection General Law ("LGPD").

This ISP shall be strictly observed by all partners, employees, interns, service providers, consultants, and correspondents of the Firm.

CHAPTER I - SECURITY REQUIREMENTS

1. All access to data, whether stored on physical or computer media, must be controlled, in order to ensure access only to authorized persons. Authorizations must be reviewed, confirmed and registered continuously by the partners.

2. The Firm's data and information systems must be protected against threats and unauthorized actions, accidental or otherwise, in order to reduce risks and ensure their integrity, secrecy and availability.

CHAPTER II - SPECIFIC RULES ON THE USE OF PROGRAMS AND E-MAIL

3. It is not allowed to run programs with the purpose of decoding passwords, monitoring networks, reading third-party data, spreading computer viruses, partially or totally destroying files, or making services unavailable.

4. It is not allowed to execute programs, install equipment, store files or promote actions that may facilitate the access of unauthorized users to the data stored by the Firm.

5. Only licensed software may be used by the Firm's partners, employees, interns and consultants. The Firm respects the copyrights of the software it uses, and recognizes that it must pay fair value for the software, and monitors any misuse of unlicensed programs.

6. It is not permitted to send confidential information to unknown external unprotected e-mails. In such cases, a password must be applied to the file containing the data.

7. The use of electronic mail for sending and receiving professional e-mails should only occur through the Firm's electronic mail.

8. The use of electronic mail for sending messages that may compromise the Firm's image before its clients and the community in general, or that may cause moral and financial damage to the Firm, is prohibited.

9. In the event of receiving links or attached files from unknown senders or with suspicious characteristics, they may only be opened or accessed after prior analysis by a specialist in the area of Information Security.

10. It is forbidden to use e-mail to send spam (messages with advertising content), as well as to send chain e-mails (referring to missing children, etc.).

CHAPTER III - MACHINES AND WORKSTATIONS

11. Workstations, including portable equipment and physical documents, must be protected from damage or loss, as well as from improper access, use or exposure.

12. Workstation access must be terminated at the end of the workday by turning off the computer and other equipment.

13. When leaving their desks, all partners, employees, interns, service providers, consultants, and correspondents who are on the Firm's premises must lock their workstations (desktops or notebooks) with a password.

14. Confidential or corporate information, or information whose disclosure may cause damage to the Firm and/or its clients or third-party service providers, suppliers or partners in general, must only be used in equipment with appropriate controls.

CHAPTER IV - MOBILE DEVICES (NOTEBOOKS, CELL PHONES AND TABLETS)

15. When traveling by car, it is recommended that notebooks be placed in the trunk or in an inconspicuous location.

16. Notebook should be placed in discreet backpacks or briefcases, rather than in conventional briefcases. It is not recommended that the notebook computer be placed in airport trolleys, nor that it be checked in with the luggage.

17. In public places (such as hotel reception, restaurants and airports), it is recommended to keep the notebook near and always in sight, avoiding distance from the equipment.

18. In hotels, whenever possible, we recommend keeping the notebook in the apartment safe. It is essential to evaluate if, on short trips, it is really necessary to take your laptop with you.

19. For laptops, tablets and cell phones, it is always recommended to use a screen lock with a password.

20. It is forbidden to use public or unknown connection networks to connect mobile devices that store data processed by the Firm.

CHAPTER V - GOOD SECURITY PRACTICES

21. No confidential information shall be left on view, whether on paper or on any devices, electronic or otherwise.

22. When using a collective printer, the printed document must be collected immediately.

23. The confidential document should never be used as a draft, and should be destroyed immediately upon disposal.

24. Confidential matters should not be discussed or commented upon, names or dealings, inside or outside the work environment, in public places, or close to visitors, either on the phone or with a colleague, relative or supplier.

25. All professionals are required, upon joining the Firm, to sign the confidentiality and non-disclosure agreement, assuming their commitment to the information handled by the Firm.

26. When a partner, employee, intern or consultant ceases to be a partner, employee, intern or consultant, the corporate e-mail is deactivated, and the commitments assumed both through the confidentiality agreement, and through this ISP, must be maintained, even after termination.

27. In case of termination of employment or contract, for any reason, the involved party must return all confidential information generated and handled as a result of the activity, or issue a statement stating that he/she destroyed it.

28. All products resulting from the work of partners, employees, trainees, service providers, consultants or correspondents, carried out in the context of the relationship with the Firm, belong to the Firm.

29. A backup copy of all data stored by the Firm shall be kept updated on a quarterly basis.

30. It is recommended to use cloud storage tools (Dropbox, One Drive, Google Cloud, etc.) for the documents produced by the Firm. In this case, a full and true copy of all content stored in the cloud should be kept in an external hard drive, kept at the Firm's headquarters.

31. Partners, employees, interns and consultants of the Firm must manage their recorded files, excluding unnecessary files.

32. It is forbidden to access sites with inappropriate content.

33. The use of 3G modem is not allowed considering the susceptibility of illegal access occurring through this type of connection.

34. In case it is necessary to transport files through removable media (External HD or PenDrive) and the necessary authorization is granted, it is recommended that the files be deleted immediately after use, in order to avoid leakage of sensitive information.

35. Only partners are duly authorized to speak on behalf of the Firm for the media: Blogs, Twitter, Facebook, LinkedIn or Discussion Groups (forums, newsgroups and the like).

CHAPTER VI - SPECIFIC RULES FOR HOME OFFICE

36. The following guidelines must be observed when work for the Firm is being performed in Home Office:

- Install antivirus programs in the case of using personal desktop or notebook computer for the execution of the work in Home Office. If the antivirus is being installed for the first time, scan the desktop or notebook completely beforehand;

- Only install software that is necessary for the job;

- Do not allow other people to use the computer that is used to perform the Firm’s tasks;

- Only use the home Wi-Fi or wired network, but use a password with a strong pattern, with more than 8 characters, containing capital and lowercase letters, numbers and symbols;

- Work from an isolated room in the house and, if possible, with a closed door;

- Make family members aware of the importance and relevance of their work in order for the Home Office to be productive;

- Maintain tidiness practices while in Home Office, keeping documents and notes in drawers and blocking the computer/notebook;

- Only use reliable software approved by the Firm for videoconferences;

CHAPTER VII - FINAL PROVISIONS

37. Security violations must be immediately reported to the partners of the Firm, who will analyze and investigate the occurrence, determining the necessary measures, with a view to correcting the failure or restructuring the processes, in order to resolve the issue and minimize its effects.

38. This Policy shall become effective as of August 1, 2019 and is valid indefinitely, and may be revised and amended at any time.