



## 信息安全指南

节选自利时律师事务所的信息安全政策

PSI 12002 - V 03 - 2024 年 3 月 5 日

## **INFORMATION SECURITY GUIDE**

*Excerpt extracted from the Licks Attorneys'  
Information Security Policy*

PSI 12002 - V 03 - March 5<sup>th</sup>, 2024

## 摘要 / SUMMARY

<b>1. 目标 .....</b>	<b>2</b>
1. Objectives .....	2
<b>2. 信息安全 .....</b>	<b>3</b>
2. Information Security .....	3
<b>3. 访问控制 .....</b>	<b>4</b>
3. Access Control .....	4
<b>4. 密码 .....</b>	<b>4</b>
4. Password .....	4
<b>5. 电子文件管理 .....</b>	<b>5</b>
5. Electronic File Management .....	5
<b>6. 信息分类和处理 .....</b>	<b>5</b>
6. Information Classification and Handling .....	5
<b>7. 物理和工作环境安全 .....</b>	<b>6</b>
7. Physical and Work Environment Security .....	6
<b>8. 资产使用 .....</b>	<b>7</b>
8. Asset Use .....	7
<b>9. 台面清理 .....</b>	<b>7</b>
9. Clean Desk and Desktop .....	7
<b>10. 信息传递 .....</b>	<b>8</b>
10. Information Transfer .....	8
<b>11. 移动设备使用和远程工作 .....</b>	<b>8</b>
11. Use of Mobile Devices and Remote Work .....	8
<b>12. 虚拟会议管理 .....</b>	<b>9</b>
12. Virtual Meetings Management .....	9
<b>13. 计算机程序的安装使用 .....</b>	<b>9</b>
13. Use and Installation of Computer Programs .....	9
<b>14. 备份 .....</b>	<b>10</b>
14. Backup .....	10
<b>15. 防恶意代码 .....</b>	<b>10</b>
15. Protection Against Malicious Codes .....	10
<b>16. 技术漏洞管理 .....</b>	<b>10</b>
16. Technical Vulnerabilities Management .....	10

<b>17. 加密控制与密钥管理 .....</b>	<b>11</b>
17. Cryptographic Control and Key Management .....	11
<b>18. 安全开发 .....</b>	<b>11</b>
18. Safe Development.....	11
<b>19. 网络安全 .....</b>	<b>12</b>
19. Network Security .....	12
<b>20. 与外部供应商的关系 .....</b>	<b>13</b>
20. Relationship with External Providers .....	13
<b>21. 个人信息的保护 .....</b>	<b>14</b>
21. Protection and Privacy of Personal Information.....	14
<b>22. 遵守法律和合同要求 .....</b>	<b>14</b>
22. Compliance with Legal and Contractual Requirements.....	14
<b>23. 受知识产权保护材料的使用 .....</b>	<b>15</b>
23. Use of Material Protected by Intellectual Property .....	15
<b>24. 例外处理 .....</b>	<b>16</b>
24. Exception Handling.....	16
<b>25. 纪律处分程序 .....</b>	<b>16</b>
25. Disciplinary Proceedings.....	16

## 1

# 目标

## Objectives

- 1.1. 本指南的内容遵循相关原则和准利时律师事务所的信息安全政策，旨在公布本所如何执行相关指南、要求和控制来确保接收、存储和转发信息的安全性。
  - 1.2. Licks 律师事务所的信息安全政策旨在实施信息安全最佳实践、责任分配、权利和义务的定义，以及访问和使用的预期，并促进保护客户、外部供应商和合作伙伴的信息数据的组织文化。
  - 1.3. 为建立关于信息创建、传输、处理、使用、存储、检索和清理的指南，本所遵循以下原则：
    - 1.3.1. 保密性：确保只有经过授权的人员、机构或流程才能访问信息
    - 1.3.2. 完整性：确保处理的信息保持信息所有者建立的所有原始特征；
    - 1.3.3. 可用性：确保授权人员、机构或流程在必要时能够访问信息；
    - 1.3.4. 真实性：验证发送信息者的身份以确保发件人无法否认信息的来源，例如，同时确保信息来自规定的来源，并且在处理过程中没有发生任何变化；
    - 1.3.5. 合法性：确保遵守当地法律。技术的使用必须遵守现行法律。
  - 1.4. Licks 律师事务所信息安全政策遵循识别、分析、评估、处理风险并将其降低到可接受水平的持续过程。
- 1.1. This guide follows the principles and guidelines of Licks Attorneys' current Information Security Policy, aims to publicize in a general way how Licks Attorneys implements guidelines, requirements, and controls for the security of information received, stored, and forwarded.
  - 1.2. Licks Attorneys' Information Security Policy aims to implement information security best practices, assigning responsibilities, defining rights, duties, and expectations of access and use, and promote an organizational culture of data and information protection for Licks Attorneys customers, external providers, and partners.
  - 1.3. To establish guidelines for the creation, transmission, processing, use, storage, retrieval, and disposal of information to preserve the following principles:
    - 1.3.1. Confidentiality: ensuring that access to information is available only to authorized persons, institutions, or processes;
    - 1.3.2. Integrity: ensuring that the information handled maintains all the original characteristics established by the information owner;
    - 1.3.3. Availability: ensuring that authorized persons, institutions, or processes obtain access to information whenever necessary;
    - 1.3.4. Authenticity: validating the identity of the person sending information. This generates non-repudiation, i.e., it ensures that the sender will not be able to deny the message's authorship, as well as that the information originates from the provided source;
    - 1.3.5. Legality: ensuring compliance with local laws, Both regarding the use of various technologies and data communication.
  - 1.4. The Licks Attorneys Information Security Policy follows the continuous process in which risks are identified, analyzed, evaluated, treated, and reduced to an acceptable level.

## 2

# 信息安全

## Information Security

2.1. 这是一套由 Licks 律师事务所批准、发布并传达给相关外部各方的信息安全政策。它由以下项目组成：

- 2.1.1. 访问控制;
- 2.1.2. 密码;
- 2.1.3. 电子文件管理;
- 2.1.4. 信息分类和处理;
- 2.1.5. 物理和工作环境安全;
- 2.1.6. 资产使用;
- 2.1.7. 台面清理;
- 2.1.8. 信息传递;
- 2.1.9. 移动设备使用和远程工作;
- 2.1.10. 虚拟的会议管理;
- 2.1.11. 计算机程序的安装使用;
- 2.1.12. 备份;
- 2.1.13. 防恶意代码;
- 2.1.14. 技术漏洞管理;
- 2.1.15. 加密控制和密钥管理;
- 2.1.16. 安全开发;
- 2.1.17. 网络安全;
- 2.1.18. 与外部供应商的关系;
- 2.1.19. 个人信息保护;
- 2.1.20. 个人信息和隐私是保护;
- 2.1.21. 遵守法律和合同要求;
- 2.1.22. 受知识产权保护材料的使用;
- 2.1.23. 例外处理;
- 2.1.24. 纪律处分程序。

2.1. This is a set of policies for Information Security approved by Licks Attorneys, published and communicated to relevant external parties. It consists of the following items:

- 2.1.1. Access Control;
- 2.1.2. Password;
- 2.1.3. Electronic File Management;
- 2.1.4. Information Classification and Handling;
- 2.1.5. Physical and Environmental Security;
- 2.1.6. Asset Use;
- 2.1.7. Clean Desk and Desktop;
- 2.1.8. Information Transfer;
- 2.1.9. Use of Mobile Devices and Remote Work;
- 2.1.10. Virtual Meetings Management;
- 2.1.11. Use and Installation of Computer Programs;
- 2.1.12. Backup;
- 2.1.13. Malicious Code Protection;
- 2.1.14. Technical Vulnerability Management;
- 2.1.15. Cryptographic Control and Key Management;
- 2.1.16. Safe Development;
- 2.1.17. Network Security;
- 2.1.18. Relationship with External Providers;
- 2.1.19. Personal Information and Privacy Protection;
- 2.1.20. Personal Information and Privacy Protection;
- 2.1.21. Compliance with Legal and Contractual Requirements;
- 2.1.22. Use of Material Protected by Intellectual Property Law;
- 2.1.23. How to handle exceptions;
- 2.1.24. Disciplinary Proceedings.

## 3

## 访问控制

### Access Control

- 3.1. 识别设备和密码保护身份，防止向 Licks 律师事务所或第三方冒充他人。
  - 3.2. Licks 律师事务所中使用的所有识别设备，例如访问卡、系统访问标识、证书和数字签名以及生物特征数据，都必须与个人相关联，并与巴西法律认可的官方文件相一致。
  - 3.3. 访客和外部供应商必须与本所成员区分开来。
- 3.1. Identification devices and passwords protect identity, preventing one person from impersonating another to Licks Attorneys or third parties.
  - 3.2. All identification devices used in Licks Attorneys, such as access badges, system access identifications, certificates, and digital signatures, and biometric data, must be associated with an individual and linked to their official documents recognized by Brazilian law.
  - 3.3. Visitors and external providers must be distinguished from members.

## 4

## 密码

### Password

- 4.1. Licks 律师事务所采用密码管理准则，密码不应公开或与他人共享。
  - 4.2. 首次访问 iManageShare 时，用户必须根据将直接发送给用户的指南创建密码，并遵守 Licks 律师事务所的信息安全政策中的规则。
- 4.1. Licks Attorneys adopts password management guidelines, which should not be exposed or shared with others.
  - 4.2. When accessing iManageShare for the first time, the user must create their password according to the guidelines that will be sent directly to the user, compliant with the rules described in Licks Attorneys' Information Security Policy.

## 5

## 电子文件管理

### *Electronic File Management*

5.1. Licks 律师事务所遵循国际安全规则来管理存储在特定平台上的电子文档。

5.1. Licks Attorneys follows international security rules to manage electronic documents, which are stored on specific platforms.

## 6

## 信息分类和处理

### *Information Classification and Handling*

6.1. 定义信息的关键程度可以:

6.1.1. 确定保护此类信息的最低限度的保障措施;

6.1.2. 确保处理所述信息的操作连续性。

6.2. 根据内部流程识别、存储、传输和处理信息。

6.3. 为防止数据和信息泄露, (对技术资产实施控制, 这一过程也由自动化机制执行。

6.4. 必须评估信息的关键程度, 以确定是否需要保护信息的机密性、完整性、可用性、真实性和合法性。

6.1. Defining the degree of criticality of the information makes it possible to:

6.1.1. Determine minimum safeguards to protect such information;

6.1.2. Ensure operational continuity for processing of said information.

6.2. Information is identified, stored, transmitted, and disposed of according to an internal process.

6.3. In order to prevent data and information leaks, controls are applied to technological assets, which are also conducted by automated mechanisms.

6.4. The degree of criticality of the information must be assessed to determine the need to protect the confidentiality, integrity, availability, authenticity, and legality of the information.



## 7

# 物理和工作环境安全

## Physical and Work Environment Security

### 7.1. 物理安全边界:

7.1.1. 办公楼必须有一个带安全锁的门, 设有基于访问卡或生物识别的系统;

7.1.2. Licks 律师事务所无法管理办公大楼的入口。但是, 办公室必须至少包括以下访问管控: 前台、带有门禁卡/二维码系统的旋转栅门、摄像头和防火系统;

7.1.3. Licks 律师事务所的设施配备了由闭路电视(CCTV)监控系统监控的安全摄像头。

### 7.2. 物理入口控制:

7.2.1. Licks 律师事务所设有前台以管控物理入口;

7.2.2. Licks 律师事务所通过访问卡的身份验证来管控物理进入;

7.2.3. 若访客需要进入 Licks 律师事务所的办公室, 则必须始终由本所成员陪同。

### 7.3. 办公室安全:

7.3.1. Licks 律师事务所的办公室中的关键信息受到保护, 不允许未经授权的人员访问;

7.3.2. 未经访问区域的经理事先授权, 除了遵照法院命令的权力机关和出于适当事由的客户外, 任何第三方不得使用手机、笔记本、相机或任何其他设备拍摄、录制音频或创建视频;

7.3.3. 装卸设备等物品的区域与 Licks 律师事务所的其余部分隔离开来, 该区域有受监控的通道, 并且需要检查收发的物品。

### 7.4. 针对外部和环境威胁的物理保护:

7.4.1. Licks 律师事务所适当配备了针对火灾、触电和民事抗议的物理保护装置。

### 7.1. Physical security perimeter:

7.1.1. The building must have a main entrance with a door protected with a secure lock, a system based on access badges or biometrics;

7.1.2. Entrance to the building is not manageable by Licks Attorneys. However, the facility must include at least the following physical access controls: a reception, turnstiles with access card/QR Code-based systems, cameras, and fire protection systems;

7.1.3. Licks Attorneys facilities are equipped with security cameras monitored by a Closed Circuit Television (CCTV) Monitoring System.

### 7.2. Physical entry controls:

7.2.1. Licks Attorneys has a reception to control physical access;

7.2.2. Licks Attorneys controls physical entry by means of an authenticated identity by access badge;

7.2.3. The granting of physical access of visitors to internal Licks Attorneys facilities must always be conducted by an accompanying member.

### 7.3. Security in rooms and facilities:

7.3.1. Licks Attorney's rooms that have information with a certain degree of criticality are protected to prevent access by unauthorized persons;

7.3.2. Any third parties, other than authorities in compliance with a court order and clients for suitable matters, are prohibited from photographing, recording audio, or creating videos using cell phones, notebooks, cameras, or any other devices without prior authorization from the manager of the visited area;

7.3.3. The areas for loading and unloading of equipment and other materials are isolated from the rest of Licks Attorneys and have supervised access, in addition to inspection of received or dispatched material.

### 7.4. Physical protection against external and environmental threats:

7.4.1. Licks Attorneys is equipped with physical protection against fire, electric shock, and civil protest, as appropriate.



## 8

## 资产使用

### *Asset Use*

- 8.1. 禁止在利时律师事务所的网络或任何设备上存储淫秽、非法或不道德的资料。
  - 8.2. 必须在特定网络上连接任何非利时律师事务所有的设备。如相关材料属于与刑事、行政或类似调查相关的司法记录或诉讼标的，经合伙人结合每个案件的具体情况考量，可对存储作出例外授权。
  - 8.3. 禁止将任何利时律师事务所拥有或许可的设备连接到公司网络，尤其是笔记本电脑和手机，因为它们会损害信息安全和服务质量。
- 8.1. The storage of obscene, illegal, or unethical material on the Licks Attorneys network or any equipment owned by it is prohibited. If the material is the subject of judicial records or proceedings related to criminal, administrative, or similar investigations, storage may be exceptionally authorized by a Partner, considering the specific circumstances of each case.
  - 8.2. Connection of any equipment that is not owned by Licks Attorneys must be made on a specific network.
  - 8.3. Connection to the corporate network of any equipment that is not owned or cleared by Licks Attorneys is prohibited, especially notebooks and cellphones, as they compromise Information Security and the quality of services.

## 9

## 台面清理

### *Clean Desk and Desktop*

- 9.1. 办公桌不允许放置可能包含关键信息的文件和可移动存储介质。
  - 9.2. 包含关键内容的文档和媒体在使用后立即存储在安全的设备中。
- 9.1. Work desks are kept clear of documents and removable storage media that may contain critical information.
  - 9.2. Documents and media containing critical content are stored in secure furniture immediately after use.

## 10

# 信息传递

## Information Transfer

- 10.1. 保密协议中描述了信息保密要求，并当产生可能影响它们的变化时进行严格分析。
- 10.2. 除非客户指定另一个平台，并且该平台必须经利克斯律师事务所信息技术团队验证，否则应使用 iManageShare 来共享或传输大量数据。
- 10.3. 包含标记为“机密”信息的电子邮件附件，建议优先通过 iManageShare 转发。
- 10.4. 即时消息系统：
  - 10.4.1. 利时律师事务所的官方即时通讯系统为 Microsoft Teams，可与非成员使用。但在采购利时律师事务所所需商品和服务的过程中，或与客户互动时，严禁使用官方即时通讯系统或任何其他即时通讯系统；若客户通过即时通讯系统发送信息，利时律师事务所成员必须通过公司电子邮件对回复进行正式确认。
  - 10.4.2. 禁止将 WhatsApp、Telegram 或任何其他即时通讯系统用作企业工具。
- 10.1. The requirements for information confidentiality are described in the Confidentiality Agreement and critically analyzed whenever a change occurs that may affect them.
- 10.2. iManageShare should be used for sharing or transferring large volumes of data, unless the Client specifies another platform, which must be validated by Licks Attorneys' Information Technology team.
- 10.3. Email attachments containing information classified as CONFIDENTIAL should preferably be forwarded via iManageShare.
- 10.4. Instant messaging system:
  - 10.4.1. The official instant messaging system for Licks Attorneys is Microsoft Teams, which can be used with non-members. However, the use of the official instant messaging system or any other instant messaging system is strictly forbidden in the process of purchasing goods and services to be obtained by Licks Attorneys or for interaction with clients; if the clients have sent the message through an instant messaging system, the Licks Attorneys member must formalize the reply by corporate e-mail;
  - 10.4.2. The use of WhatsApp, Telegram, or any other instant messaging system as a corporate tool is not allowed.

## 11

# 移动设备使用和远程工作

## Use of Mobile Devices and Remote Work

- 11.1. Licks 律师事务所遵循管理移动设备使用和执行远程工作的特定准则。
- 11.1. Licks Attorneys follows specific guidelines for managing the use of mobile devices and performing remote work.

## 12

# 虚拟会议管理

## Virtual Meetings Management

- 12.1. 只要有可能，应由利时律师事务所安排虚拟会议。也可以接受来自客户、实体，以及公共机构或媒体的邀请。
- 12.2. 由利时律师事务所组织的与第三方的虚拟会议应发出书面邀请，并且必须通过发送链接和密码在 Zoom 平台或通过发送链接在 Microsoft Teams 平台进行。
- 12.3. 当时利时律师事务所的成员或第三方需要远程加入会议时，必须使用 Zoom 平台。
- 12.4. 虚拟会议（包括网络研讨会、工作坊或类似活动）的录音必须事先通知受影响个人数据的持有人，他们有权反对在录音中记录其个人数据。
- 12.1. Whenever possible, scheduling virtual meetings should be performed by Licks Attorneys. Invitations from customers, bodies, and public bodies or the press are acceptable.
- 12.2. Every virtual meeting organized by Licks Attorneys with third parties requires a written invitation and must be carried out in the Zoom platforms, by sending a link and a password, or in Microsoft Teams, by sending the link.
- 12.3. The Zoom platform must be used when members of Licks Attorneys or third parties need to access the meeting remotely.
- 12.4. Recordings of virtual meetings, including webinars, workshops, or similar events, must be preceded by a notice to the holders of the impacted personal data, who shall have the right to object to the processing of their personal data in the recording.

## 13

# 计算机程序的安装使用

## Use and Installation of Computer Programs

- 13.1. 严禁使用未经许可的计算机程序副本。
- 13.2. 由外部机构免费提供给利时律师事务所并附有合法版权所有者授权的计算机程序必须提交给 IT 管理部门，以检查其完整性以及与利时律师事务所网络中现有资源的兼容性。
- 13.3. 禁止使用任何公共人工智能（AI）工具如 ChatGPT。除非《信息安全政策》中列明并已通知所有成员，否则亦禁止使用未经利时律师事务所 IT 团队、系统团队及管理层预先批准和正式认可的任何人工智能 AI 工具。
- 13.4. 在提供合同约定的全部或部分服务过程中若使用了人工智能资源，应按照先前制定的包含标准通知的指导准则，在服务交付信息中告知客户。
- 13.1. The use of unlicensed copies of computer programs is strictly prohibited.
- 13.2. Computer programs provided to Licks Attorneys by external institutions free of charge and accompanied by authorization from the legal copyright holder must be submitted to IT management to be checked for integrity and compatibility with existing resources in the Licks Attorneys network.
- 13.3. The use of any public artificial intelligence (AI) tool, such as ChatGPT, is prohibited. The use of any artificial intelligence (AI) tool that has not been pre-approved and formally endorsed by the IT team, Systems team, and Administration of Licks Attorneys is also prohibited unless listed in the Information Security Policy and communicated to all members.
- 13.4. The client will be informed in the delivery message of the requested service, following the previously established guidelines for including the standard notice, when AI resources have been utilized in the provision of the contracted services or part thereof.

## 14

## 备份

*Backup*

- 14.1. 利时律师事务所采用备份解决方案来保护所有接收、存储和转发的数据不丢失，以及清除存储和定期测试中的冗余。
- 14.2. 对于在利时律师事务所流通的所有数据，无论分类如何，备份都受到加密保护。

- 14.1. Licks Attorneys adopts backup solutions to protect all data received, stored, and forwarded against loss, as well as redundancy in storage and periodic testing.
- 14.2. For all data circulating at Licks Attorneys, the backup is protected by encryption regardless of classification.

## 15

## 防恶意代码

*Protection Against Malicious Codes*

- 15.1. Licks 律师事务所采用针对恶意软件的保护解决方案，包括检测和预防措施。
- 15.2. 任何源自网络或外部用户的计算机程序或文件都必须经过病毒防护系统的扫描。

- 15.1. Licks Attorneys adopts protection solutions against malware, with detection and prevention measures.
- 15.2. Any computer program or file originating from networks or external users must be scanned by virus protection systems.

## 16

## 技术漏洞管理

*Technical Vulnerabilities Management*

- 16.1. 使用专门设计的系统来识别，分析和解决技术漏洞。

- 16.1. Technical Vulnerabilities are identified, analyzed and addressed using a system specifically designed for this purpose.

# 17

## 加密控制与密钥管理

### *Cryptographic Control and Key Management*

- 17.1. 加密控制确保了传输和存储方式的安全，使得信息在被截获时难以解读。
- 17.2. 利时律师事务所使用加密来存储和传输具有最高关键性的信息。

- 17.1. Cryptographic controls ensure security in the means of transmission and storage, making it difficult for information to be interpreted in case of interception.
- 17.2. Encryption is used in Licks Attorneys to store and transmit information with the highest degree of criticality.

# 18

## 安全开发

### *Safe Development*

- 18.1. 计算机程序的开发是通过正式的过程并使用适当的方法进行的。
- 18.2. Licks 律师事务所制定计算机程序的最低信息安全要求。

- 18.1. The development of a computer program is carried out through a formal process and using appropriate methodology.
- 18.2. Licks Attorneys establish minimum Information Security requirements for a computer program.

## 19

## 网络安全

## Network Security

- 19.1. 管理网络资产的责任和程序被定义为仅授予活动所需的访问权限，并最大限度地减少因操作或维护故障而造成的损失。
- 19.2. 连接利时律师事务所的网络必须通过经身份验证的接口。
- 19.3. 网络分为公共接口和内部接口，两者之间的通信受到保护。
- 19.4. 利时 律师事务所的访客网络仅用于互联网访问。
- 19.5. 严禁浏览利时律师事务所限制的网站类型，除非与事务所的核心活动直接相关并经合伙人授权，尤其是在涉及以下内容，包括：
  - 19.5.1. 虐待儿童；
  - 19.5.2. 歧视；
  - 19.5.3. 使用毒品；
  - 19.5.4. 明显的暴力；
  - 19.5.5. 极端主义团体；
  - 19.5.6. 盗版；
  - 19.5.7. 非法或不道德的内容；
  - 19.5.8. 旨在创建匿名访问或规避对不正当目的地的封锁的第三方计算机程序。如：ExpressVPN 和 CyberGhost；
  - 19.5.9. 交友网站；
  - 19.5.10. 色情；
  - 19.5.11. 武器销售；
  - 19.5.12. 剽窃；
  - 19.5.13. 互联网广播和电视（除非出于合理的业务需要）；
  - 19.5.14. 从互联网收看、下载和共享文件和媒体；
  - 19.5.15. 病毒（恶意网站）；
  - 19.5.16. 钓鱼网站；
  - 19.5.17. 垃圾邮件网址；
  - 19.5.18. 娱乐；
  - 19.5.19. 游戏；
  - 19.5.20. 求职（除非出于合理的业务需要）。

- 19.1. The responsibilities and procedures for managing network assets are defined to only grant access necessary to the activity and minimize damages caused by a failure in operation or of maintenance.
- 19.2. Connections to the Licks Attorneys network must occur exclusively through authenticated access.
- 19.3. The networks are segregated into public access and internal access. Communications between these networks are protected.
- 19.4. The Licks Attorneys visitor network is available exclusively for internet access purposes.
- 19.5. It is strictly forbidden to browse sites of categories restricted by Licks Attorneys is strictly prohibited, unless directly related to the Firm's core activities and authorized by a Partner, especially when involving:
  - 19.5.1. Child abuse;
  - 19.5.2. Discrimination;
  - 19.5.3. Drug use;
  - 19.5.4. Explicit violence;
  - 19.5.5. Extremist groups;
  - 19.5.6. Piracy;
  - 19.5.7. Illegal or unethical content;
  - 19.5.8. Third-party computer programs aiming to create anonymous access or circumvent blockages made to undue destinations. Examples: ExpressVPN and CyberGhost (Proxy prevention);
  - 19.5.9. Dating Website Profiles;
  - 19.5.10. Pornography;
  - 19.5.11. Weapons Sale;
  - 19.5.12. Plagiarism;
  - 19.5.13. Internet radio and TV (unless for a legitimate business need);
  - 19.5.14. Streaming, downloading, and sharing of files and media from the internet;
  - 19.5.15. Viruses (malicious websites);
  - 19.5.16. Phishing;
  - 19.5.17. Spam URLs;
  - 19.5.18. Entertainment;
  - 19.5.19. Games;
  - 19.5.20. Job searches (unless for a legitimate business need).

## 20

## 与外部供应商的关系

### *Relationship with External Providers*

- |   |   |
|---|---|
| <p>20.1. 信息安全要求已与外部提供商达成一致并记录在保密协议中，以降低关于外部提供商访问 Licks 律师事务所资产的风险。</p> <p>20.2. 外部 IT 供应商也需签订该保密协议。</p> <p>20.3. Licks 律师事务所系统地监控外部供应商是否遵守保密协议。</p> | <p>20.1. Information Security requirements are agreed upon with the external provider and documented in the Confidentiality Agreement to mitigate the risks associated with external providers' access to Licks Attorney's assets.</p> <p>20.2. This agreement is extended to the supply chain of the external IT provider.</p> <p>20.3. Compliance with this policy by the external provider is systematically monitored by Licks Attorneys.</p> |
|---|---|

## 21

## 与云服务供应商关系

### *Relationship with Cloud Service Providers*

- |  |   |
|--|---|
| <p>21.1. 利时律师事务所根据《信息安全政策》的技术和合同要求，遵循供应商管理的内部流程，在云服务提供商的采购、使用、管理和退出全流程中对其进行评估。</p> <p>21.2. IT 团队确保云服务提供商正确实施信息安全控制措施，并按计划间隔评估其环境以检查是否存在漏洞。</p> <p>21.3. 利时律师事务所对外部供应商遵守本政策的情况进行系统性监控。</p> | <p>21.1. Licks Attorneys assesses cloud service providers throughout the acquisition, usage, management, and exit processes, in accordance with the technical and contractual requirements of the Information Security Policy, following internal procedures for provider (vendor) management.</p> <p>21.2. The IT team ensures the proper implementation of Information Security controls by cloud service providers, assessing the environment at planned intervals to check for the presence of vulnerabilities.</p> <p>21.3. Licks Attorneys systematically monitors compliance with this policy by external providers.</p> |
|--|---|



## 22

# 个人信息保护

## Protection and Privacy of Personal Information

22.1. 利时律师事务所管控所收集的个人信息类型、使用方式和时间、授权访问人员，以及个人数据持有人更正信息的方式。欲了解更多信息，请参看《隐私通知》

22.2. 同时遵守下列现行法律法规：

- 22.2.1. 隐私和保密的基本权利（根据联邦宪法）；
- 22.2.2. 个人身份证明文件的出示和使用（1968 年 12 月 6 日的第 5.553 号法律）；
- 22.2.3. 消费者法中的具体规定；
- 22.2.4. 银行和税收法；
- 22.2.5. 巴西民法典（2002 年 1 月 10 日第 10.406 号法律）；
- 22.2.6. LGPD – 巴西数据隐私法（2018 年 8 月 14 日的第 13.709 号法律，2019 年 7 月 8 日经第 13.853 号法律修订）。

22.1. Licks Attorneys controls the types of personal information collected, how and when it can be used, who has access to it, and how the holder of personal data may correct any inconsistencies therein. For further details, please refer to the [Privacy Notice](#)

22.2. The following laws and regulations in force are observed:

- 22.2.1. The fundamental rights to privacy and secrecy (per the Federal Constitution);
- 22.2.2. The presentation and use of personal identification documents (Law #5.553 from December 6, 1968);
- 22.2.3. Specific provisions in the consumer Code;
- 22.2.4. Banking and tax legislation;
- 22.2.5. Brazilian Civil Code (Law #10.406 from January 10, 2002);
- 22.2.6. LGPD – Brazilian Data Privacy Act (Law #13.709, from August 14, 2018, amended by Law #13.853, from July 8, 2019).

## 23

# 遵守法律和合同要求

## Compliance with Legal and Contractual Requirements

23.1. 适用于利时律师事务所的法律、法规和合同要求，以及直接负责遵守这些要求的人员已被识别、记录和更新。

23.1. The legislative, regulatory, and contractual requirements applicable to Licks Attorneys are identified, documented, and updated, as well as those directly responsible for compliance with these requirements.

## 24

# 受知识产权保护材料的使用

## Use of Material Protected by Intellectual Property

- 24.1. 禁止使用违反版权法的与文学、艺术或科学作品有关的任何文本；会议、演讲、布道和其他性质相同的作品；戏剧和戏剧音乐作品；编舞和哑剧作品，以书面或任何其他形式进行的舞台表演；音乐作品，无论是否有歌词；有声或无声的视听作品，包括电影作品；摄影作品以及通过与摄影类似的任何方法制作的作品；素描、绘画、蚀刻、雕塑、平版印刷和动态艺术作品；插图、地图和其他性质相同的作品；与地理、工程、地形、建筑、景观、布景和科学有关的项目、草图和雕塑作品；对原创作品的改编、翻译和其他转换，以新的智力创作形式呈现；电脑程序；收藏或汇编、选集、百科全书、词典、数据库和其他由于其内容的选择、组织或处理而构成智力创作的作品。
  - 24.2. 允许使用文学、艺术或科学作品来提供司法或行政证据，包括在任何作品中复制任何性质的已有作品的小片段或完整作品（例如雕塑），只要复制本身不是为了创作新作品，不影响复制品的正常使用，并且不损害原作者的合法权益。利时律师事务所成员在执业时制作的任何作品均被视为本所的版权作品，受法律保护。
  - 24.3. 允许使用付费网站进行研究、购买 PDF 文件或访问任何付费材料，前提是存在合理的业务需要、不侵犯任何版权并获得利时律师事务所的授权。
- 24.1. The use of any texts pertaining to literary, artistic or scientific works; conferences, speeches, sermons and other works of the same nature; dramatic and dramatic-musical works; choreographic and pantomimic works, the scenic execution of which is in writing or in any other form; musical compositions, whether or not they have lyrics; audiovisual works, with or without sound, including cinematographic works; photographic works and those produced by any process analogous to that of photography; works of drawing, painting, etching, sculpture, lithography and kinetic art; illustrations, geographical maps and other works of the same nature; projects, sketches and sculptural works related to geography, engineering, topography, architecture, landscaping, scenography and science; adaptations, translations and other transformations of original works, presented as new intellectual creation; computer programs; collections or compilations, anthologies, encyclopedias, dictionaries, databases and other works that, due to the selection, organization or disposition of their content, constitute an intellectual creation; in violation of copyright law, is forbidden.
  - 24.2. The use of literary, artistic, or scientific works to produce judicial or administrative evidence, in addition to the reproduction, in any works, of small excerpts of pre-existing works, of any nature, or of integral works, in the case of sculptural arts, whenever the reproduction itself is not the main objective of the new work and does not harm the normal exploitation of the reproduced work or cause undue harm to the legitimate interests of the authors, is allowed. Any works produced by Licks Attorneys members when performing their occupation are considered copyrighted works belonging to Licks Attorneys and protected under the law.
  - 24.3. The use of paid websites for research, purchase of PDF files, or access to any paid material is allowed, provided that there is a legitimate business need, no violation of any copyright and with Licks Attorneys' authorization.

## 25

## 例外处理

### *Exception Handling*

- |   |  |
|---|--|
| <p>25.1. 本政策的例外情况在内部程序或保密协议中得到解释、授权和规范。</p> <p>25.2. 定义和实施安全控制以最大限度地降低本政策的例外情况所固有的风险。</p> | <p>25.1. Exceptions to this policy are explained, authorized, and formalized in internal procedures or in the Confidentiality Agreement.</p> <p>25.2. Security controls are defined and implemented to minimize the risks inherent to exceptions to this policy.</p> |
|---|--|

## 26

## 纪律处分程序

### *Disciplinary Proceedings*

- |  |   |
|--|---|
| <p>26.1. 利时律师事务所在必要时执行纪律处分程序的具体准则。</p> | <p>26.1. Licks Attorneys follow specific guidelines for handling disciplinary proceedings when necessary.</p> |
|--|---|

#### ©信息安全指南

版权所有。除非另有说明，否则未经利时律师事务所书面许可，不得以任何电子或机械方式（包括影印和缩微胶卷）复制或使用本指南的任何部分。

#### 利时律师事务所

Av. Oscar Niemeyer, 2000  
Aqwa Corporate - 9º Andar  
Rio de Janeiro – RJ  
20220-297

电话: + 55 21 3550-3700

传真: + 55 21 3550-3777

comitesi@lickslegal.com

[www.lickslegal.com](http://www.lickslegal.com)

#### ©Information Security Guide

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or used by any means, electronic or mechanical, including photocopying and microfilm, without written permission from Licks Attorneys.

#### Licks Attorneys

Av. Oscar Niemeyer, 2000  
Aqwa Corporate - 9th Floor  
Rio de Janeiro - RJ  
20220-297

Phone: + 55 21 3550-3700

Fax: + 55 21 3550-3777

comitesi@lickslegal.com

[www.lickslegal.com](http://www.lickslegal.com)



Rio de Janeiro • Sao Paulo • Brasilia • Curitiba • Tokyo  
Lickslegal.com | Copyright © 2025 Licks Advogados  
info@lickslegal.com

