上海艾雷电子商务有限公司

数据安全守则

1. 引言

本守则旨在确保上海艾雷电子商务有限公司（以下简称“艾雷”或“公司”）数据的安全性、完整性和保密性，防止数据泄露、滥用或未经授权的访问、提高员工的信息安全意识和技能。

2. 基本原则

2.1. 遵守公司政策：所有员工必须严格遵守公司的数据安全政策和规定，包括访问控制、密码保护和设备管理等。

2.2. 信息安全意识：员工应时刻保持对数据安全的高度重视，了解常见的信息安全威胁和防范措施。

2.3. 安全软件管理：所有终端必须使用公司安装配置的安全管理软件，实行统一管理，用来保护终端不受病毒和木马的威胁，保证终端数据及网络安全。

2.4. 遵守国家法律：员工应以国家法律为准绳，熟悉并严格遵守《中华人民共和国个人信息保护法》和《中华人民共和国数据安全法》

3. 适用范围

本守则适用于所有员工，包括全职、兼职、实习生以及临时工。

4. 培训与教育

4.1. 入职培训：新入职员工在入职时必须接受数据安全培训，确保从一开始就具备基本的数据安全知识。

4.2. 定期培训：公司定期组织数据安全培训，帮助员工了解最新的安全威胁和防范措施。

4.3. 培训记录：建立员工数据安全培训档案，记录员工参加的培训情况和考核成绩等相关信息。

5. 数据安全管理办公室

5.1. 数据安全管理办公室承担公司数据管理的“规则制定、收集整合、存储管理、处理分析、安全保护、服务支持”职责。

5.2. 数据安全管理办公室的组织架构由数据安全管理办公室委员会和成员构成，数据安全管理办公室委员会由总经办全体人员构成，成员由各部门负责人、骨干人员经数据安全管理办公室委员会批准后构成。

6. 数据分类与处理

6.1. 数据分类：公司对敏感数据进行分类分级，针对不同种类和敏感级别的数据制定差异化的安全控制策略。

6.1.1. 敏感数据：敏感数据是指那些一旦泄露或被不当使用，可能会对个人、组织或企业造成损失或风险的数据。这类数据通常具有高度的隐私性和机密性，需要特别加以保护。敏感数据包括但不限于以下内容：

- 客户的个人隐私信息：如名称或者姓名、联系方式、个人信息的种类、身份证号、电话号码、家庭地址、收件地址、银行账户等。
- 公司的财务信息：如交易记录、资产状况、银行信息等。
- 公司的商业机密：如合作伙伴信息、设计图纸、数码源文件及代码、研发计划、销售及采购策略、公司商业计划、客户合约及其中约定需遵守的保密条款等。
- 公司的互联网信息：如各网络平台注册的账号和密码、各种云服务平台的注册登记信息等。

6.1.2. 内部数据：内部数据是指在组织或企业内部使用的数据，这些数据主要用于支持组织的运营、管理和决策。与敏感数据不同，内部数据不一定都具有高度机密性，但也需要进行适当的保护以防止未经授权的访问和使用。内部数据可能包括但不限于以下内容：

- 员工信息：如员工档案、薪资信息、考勤记录等。
- 业务数据：如销售数据、库存数据、采购数据等。
- 管理数据：如项目进度、绩效评估、会议纪要等。

6.1.3. 公开数据：公开数据是指那些公司对外部公开并可以被任何人自由获取和使用的数据。这类数据通常已经过处理，不再包含敏感或机密信息。公开数据可能包括但不限于以下内容：

- 公司公开数据：如威士忌年度报告、政策文件、公共项目信息等。
- 互联网数据：如公司在官网发布的信息、公司在社交媒体平台或公共媒体发布的信息等。

6.2. 数据管理

6.2.1. 数据存储

- 敏感数据和内部数据必须加密存储。
- 使用公司专用的网络共享文件存储并通过密码访问。
- 使用外部设备时需提交申请，认证通过后方可使用。
- 使用带加密功能的外部存储设备。
- 根据企业安全战略逐步推进数据资产保护措施。
- 禁止在未加密的设备或云服务上存储敏感数据和内部数据。

6.2.2. 数据传输

- 传输敏感数据和内部数据时必须使用公司指定渠道，如公司企业邮箱及钉钉软件。
- 禁止通过不安全的渠道（如公共 Wi-Fi、非加密邮件、个人即时通讯软件等）传输敏感数据和内部数据。

6.2.3. 数据处理

- 必须采取加密技术和其他安全措施，如 Excel 表单加密、移动硬盘加密、数据云盘加密等。
- 应确保数据的准确性、完整性和安全性。
- 禁止未经授权修改、删除或披露数据。

6.2.4. 数据备份

- 定期对重要数据进行备份。
- 备份数据应安全存储，并在必要时能够迅速恢复。

6.2.5. 数据访问

- 访问权限根据“最小权限原则、责任分离原则、数据保护原则”进行分配。

- 根据本守则中“数据分类”定义，不同分类的数据有不同访问权限及审批流程。
- 员工有权根据公司制定的规章制度，通过授权访问相关数据。这种访问权限是基于员工的工作职责和需要而设定的，确保员工能够高效地完成工作任务。
- 在数据的使用过程中，员工应遵守公司的数据使用规定，不得擅自复制、传播或篡改数据。员工需对数据的完整性、准确性和安全性负责。

7. 设备管理

7.1. 设备管理：员工使用的计算机和其他设备必须符合公司的安全标准，定期进行安全检查和维护。

7.1.1. 移动设备上的数据访问应通过公司安全软件认证。

7.1.2. 丢失或被盗的移动设备应立即报告并采取措施。

8. 密码与账号管理

8.1. 密码管理：员工应设置复杂且唯一的密码，并定期更换密码。禁止使用生日、电话号码等容易被猜测的密码。

8.2. 账号管理：员工应妥善保管自己的账号和密码，不得将账号借给他人使用。

9. 网络安全

9.1. 网络行为规范：员工在使用公司网络资源时，应遵守网络安全规范，不得进行任何可能导致数据泄露的行为。

9.2. 防范网络攻击：员工应学会识别和应对各种常见的网络攻击方式，如钓鱼邮件、恶意软件等，应统一安装公司安全管理软件客户端。

9.3. 桌面锁屏管理：一旦离开电脑，务必保证电脑处于锁屏或关机状态。

10. 应急响应与报告

10.1. 应急响应：一旦发现数据安全隐患或数据泄露事件，员工应立即采取措施，并在 2 小时内向直属上级和分管领导报告。

10.2. 保密承诺：所有员工必须签署数据安全及保密承诺书，承诺在工作中严格遵守公司的数据安全政策和规定。

11. 安全责任

接触、访问并使用数据的人员为数据管理第一责任人，对数据安全负责。

11.1. 保密责任：员工应对所接触的数据信息严格保密，不得将相关信息泄露给未经授权的第三方。员工应妥善保管工作资料，确保不会因个人失误导致数据泄露。

11.2. 监督责任：员工之间应相互监督，发现同事在数据安全管理方面存在违规行为时，应及时制止并向直属领导及分管领导反映。通过相互监督，共同维护公司的数据安全。

11.3. 违规责任：对于违反公司数据安全管理相关规定的，公司将进行严肃处理；对于给公司造成损失的，公司会主张相应赔偿；对于违反国家法律法规，对公司、社会造成影响的，公司会配合国家机关处理。

12. 持续改进

公司会定期审查和更新数据安全守则，以适应新的安全挑战和技术发展。

通过以上守则，希望每位员工都能提高自身的数据安全意识，共同努力保护公司的数据资产，确保公司的正常运营和声誉不受影响。

上海艾雷电子商务有限公司

2023 年 1 月 20 日