大连汇扬网络科技

数 据 安 全 管 理 制 度

COMPANY INTRODUCTION

大 连 汇 扬 网 络 科 技 有 限 公 司

目录

Contents

01 总则

1.1 目的

数据是公司重要的资产。为保证信息的安全性、可靠性、完整性和有效性，公司制定和采取相应管理制度，进行对数据的保护，以避免其遭受外来的威胁和损害，防止未经授权地修改、泄漏和破坏。

1.2 使用范围

本制度适用于公司内所有员工，所有员工应认真学习本制度,支持本制度,并强制遵守。

1.3 职责

本制度将作为员工遵守情况及复查的基本原则。违反本制度者经查实公司有权根据情节轻重给出相应处罚。

02 管理规定

2.1 数据范围

2.1.1 数据管理范围包括所有利用计算机进行输入、存储、处理、再加工及输出的数据，包括但不限于文字材料、报表、各类原始凭证、图形、图像、源代码等；

2.1.2 数据按照重要性程度以及隐私性的要求，暂时由低至高划分为四个级别：

- L1公开数据：可以免费获得和访问的信息，没有任何限制或不利后果，例如公司联系方式等；
- L2内部数据：安全要求较低但不打算向外部公开的数据，例如公司组织架构图、公司规章制度等；
- L3机密数据；敏感数据，如果泄露可能会对运营产生负面影响，包括损害公司、其客户、合作伙伴或员工。例如包括客户信息、合同信息、员工信息和薪水信息等；
- L4绝密数据：高度敏感的公司数据，如果泄露可能会使组织面临财务、法律、监管和声誉风险。例如包括公司财务数据、业务所涉及到用户个人信息数据、各种软件源代码等知识产权相关数据等。

02 管理规定

大连汇扬网络科技

2.2 内部安全防范管理

2.2.1 公司内各类计算机系统用户，严禁运行未经检验和来历不明的软件，严禁在各自的计算机内安装与各自业务无关的软件，严禁安装运行各种游戏软件，严禁将计算机系统口令和个人密码告诉无关人员，未经许可严禁将计算机交由外部门人员操作。

2.2.2 员工应确保各自计算机内的数据资料的安全。未经许可，任何人严禁擅自拷贝或泄露L3及L4级别的公司数据。

2.2.3 防范计算机病毒：

- 公司内各计算机应当专人、专管、专用。
- 员工在计算机上安装的硬件、软件必须是正版产品。
- 谨慎地处理、使用共享软件。
- 对软盘、U盘、移动硬盘、光盘实行管理，在使用外来软盘、U盘、移动硬盘、光盘时，应首先检测其安全性。
- 决不执行不知来源的程序。
- 系统中的数据要定期进行备份。　密切注意自用计算机的配置参数(如引导扇区、中断向量表、应用程序长度、执行时间)和运行情况，发现异常，及时报告系统管理员，作出判断和处理。
- 确保杀毒软件病毒特征码的及时更新：由于病毒不断发展变化，要求计算机系统管理员密切注意所用杀毒软件病毒特征码的更新情况，做到及时更新。
- 不得进入各“黑客”站点访问，不允许在局域网及Internet上使用“黑客”软件，以防不明病毒。
- 不得打开不明Email，不得通过Email下载软件，如发生不明情况应及时向研究院知识工程及信息技术部报告。
- 严格限制远程访问者的权限及认证，以防不明攻击及感染病毒，特别限制匿名登陆。
- 公司内部禁止擅自使用各类盗版软件，个人如私自传入盗版软件并使用，由此造成的与知识产权相关的后果将由使用者本人负全责。

02 管理规定

2.3 数据流通管理

2.3.1 L2及以上级别的数据传输，必须通过点对点的方式、或在特定群组内传输，减少数据外流风险。

2.3.2 在公司内部，网上电子文件允许下载，但文件下载后一律视为非受控文件，文件使用者有责任关注此文件的最新版本，以保持此电子文件的现行有效性。

2.4 数据保护

2.4.1 各部门应按需求进行数据备份的计划和管理。

2.4.2 L3及L4级别的数据，需要保证存放数据在安全的地方，非相关工作具体责任人获得许可后方可进行查看和提取。L2及以上级别的数据，未经许可不得通过保存在电子设备上或通过书面的方式携带出公司，或在公司区域外公开讨论。

2.4.3 数据管理者应承担保存或处理数据的保护职责，防止数据的丢失、误用或破坏；L3及L4级别的数据，应采用多种记录手段保存，免遭意外风险。

2.4.4 无正当理由和有关批准手续，不得泄漏L3及L4级别数据给内部或外部的无关人员。

03 附则

本制度由企业合规部制定并负责解释。

企业合规部负责指导及协调本制度的实施，根据公司实际业务发展状况，企业合规部将在获得公司领导同意后酌情修正本制度，以使其符合公司的实际情况。

本制度未尽事宜以相关法律、行政法规、规范性文件以及公司各项规章制度的规定为准。

感谢
观看