**北京沃丰时代数据科技有限公司**

**数据分级分类标准规范**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 数据分级分类标准规范 | | |
| **文档编号** | ISMS-L3-04 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 孟庆鑫 | **编制日期** | 2018-12-11 |
| **评审人** | 周毅 | **评审日期** | 2023-03-23 |
| **批准人** | 张磊 | **批准日期** | 2023-04-23 |

**修订历史记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **状态** | **修订内容说明** | **修订日期** | **编制人** |
| V1.0 | 新建 | 新增 | 2018-12-11 | 孟庆鑫 |
| V1.1 | 修订 | 修订文档信息 | 2023-04-23 | 张帆 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**一、数据安全分级**

为了对信息数据更有效的进行保护，根据数据的敏感程度进行了四个等级的划分，分别为机密级别（L4）、秘密级别（L3）、内部级别（L2）、公开级别（L1），并根据不同的安全级别对数据分别使用对应级别的防护策略。

1. 机密（L4）

机密信息是指公司最重要和敏感的商业秘密信息，只限于与机密信息相关的人员获取，接触到机密信息的人员范围受到严格限制、必须有确实的业务需要并得到信息拥有者授权；不适当的泄漏会影响到公司的根本利益。

1. 秘密（L3）

秘密信息是指对公司有重要价值的商业秘密信息，只限于与秘密信息相关的人员间发放，接触到秘密信息的人员必须有确实的业务需要，不适当的泄漏会对公司带来重大影响。

1. 内部（L2）

内部信息是指只供在公司内部发放和传播的商业秘密信息，不适当的对外泄漏会对公司造成一定影响或损害。

1. 公开（L1）

公开（非敏感）信息是指公司公开或非商业秘密的信息，是可以在公司外部发放的信息。

根据数据资产的属性进行分级分类，其中属于敏感数据信息范围的包括：所有L3级别（秘密信息）、L4级别（机密信息），以及B2级别（业务内部信息），参见下图标黄部分。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *数据类型* | *分级* | | | |
| *公开信息（L1）* | *内部信息（L2）* | *秘密信息（L3）* | *机密信息（L4）* |
| *客户数据（C）* | *客户公开信息（C1）* | *客户内部信息（C2）* | *客户秘密信息（C3）* | *客户机密信息（C4）* |
| *业务数据（B）* | *业务公开信息（B1）* | *业务内部信息（B2）* | *业务秘密信息（B3）* | *业务机密信息（B4）* |

**二、客户数据信息（C - Customer）**

客户的基本信息，以及客户在使用公司产品及服务的生命周期中产生的信息。

### **客户可公开信息（C1）**

**范围：**  
任何可以由用户确认公开程度的数据，包括对所有人公开、对特定对象公开、不公开。  
**类型及示例：**

* 用户公开的个人信息，包括昵称、头像、自我介绍；
* 用户公开发表的分享、评论等信息；
* 用户需要提供的资质、正式发布的商品等信息。

### **客户内部信息（C2）**

**范围：**  
任何用于标识用户身份信息和交易信息的数据，用于在公司内部识别和定位用户，或用于为客户提供直接服务。  
**类型及示例：**

* 基础身份识别信息，如user id或具备类似唯一性识别功能的代码及字符串；
* 基础业务信息，如订单编号、商品内容等基础信息；
* 用户账户账号状态，如当前是否正常、当前限制及管制信息。

### **客户秘密信息（C3）**

**范围：**  
任何只对客户可用的或者关于客户的信息，该类信息属于用户未在网站上直接公开的自然、资质和行为信息。该类信息的泄露会给客户带来困扰。

**分类及示例：**

* 直接的联系信息，包括手机号码，电子邮箱、地址内容等；
* 用户静态信息：如用户公司的执照、对公帐号信息等，员工的姓名、性别、生日、出生地、年龄、职业，经过脱敏处理的身份证号、银行卡号等；
* 用户动态信息：业务情况、订单详情信息、财务信息、物流信息、交易信息、产品评价、各类评论、以及修改个人纪录等行为信息。用户浏览行为等信息；

### **客户机密信息（C4）**

**范围：**  
任何客户用来进行商业交易、证明用户或用户公司资质的信息，或者可以用来获取账户控制权的任何信息；任何存在合同义务限制其访问的客户信息。该类信息的泄露会给客户带来直接的经济损失。业务系统或内部沟通中不允许直接出现此类级别的明文信息。  
**分类及示例：**

* 认证信息：密码（包括登录密码、支付密码、完成交易或认证所需要的一次性密码）、 指纹、声纹、面部识别信息等用于校验的信息；
* 用户认证相关的cookie／session信息、客户私有的证书信息；密码提示问题和回答等；
* 特定敏感信息：未经脱敏的用户身份证号码及银行账户等信息。

**注意：与合作伙伴收集和共享任何客户信息均须得到信息安全委员会的评审。**

**三、业务数据信息（B - Business）**

公司及各部门在开展业务时所产生和使用的、与全部或部分客户群体直接相关的数据。

### **业务可公开信息（B1）**

**范围：**  
业务公开信息是指可以被公共访问和对外发布的信息，并且公开信息可以自由散布而不会产生任何安全或法律问题。  
**类型及示例：**

* 公司地址、联系电话、客服电话；
* 应当公开的公司基本资质；
* 经市场部发送的新闻。
* 公司在网上公开的信息，如：活动招商（参与）规则、前台类目、公告、经过公关公布并无歧义的信息。
* 公司产品手册类信息，如已公布产品使用手册等。

### **业务内部信息（B2）**

**范围：**

部门内部可进行公开和使用的数据，以及允许在部门间进行共享的数据；仅限相关业务员工使用；

影响：如果内部信息泄露，可能对该局部业务、客户或者员工造成较小或者不显著的负面影响。

**示例：**

* 公司内部规章制度、内部公告信息、内部通知；
* 公司组织结构和员工通讯录；
* 员工在内网发布的非涉密信息；
* 非业务类常规项目计划/方案；
* 公司内部公开的技术文档和业务文档；
* 公司制定的管理体系文件和相关资料。
* 公司内部公布的非敏感项目计划、方案、进度等；
* 内部业务培训材料；
* 其他管理层及安全技术委员会确定可以在全公司内公开的信息和数据；

### **业务秘密信息（B3）**

**范围：**  
公司及各部门层面关键业务数据；仅限相关业务员工使用，如果非授权的泄露将直接或间接对公司、客户或者员工造成不利影响，造成经济损失、商业损失、破坏公司声誉，并可能发生潜在法律责任的信息。  
**示例：**

* 需要限定访问对象的业务和技术信息，如源代码（含工作中产生的程序代码）；
* 网络体系结构、故障通告、安全报告（攻击、安全审计等）；
* 未公开的财务机密信息、一般预算信息；
* 关键项目的计划/方案/报告；
* 内部wiki；
* 法律文件，包括业务合同、授权、合作协议等；
* 采购流程中的机密信息；
* 公司或部门本年度业务目标（如年度收入指标、产品研发方向等），
* 产品的业务数据（包括尚未正式发布的产品测试效果数据）；
* 大型活动（或项目）的计划/方案；
* 各项业务的风险指标和财务指标；

### **业务机密信息（B4）**

**范围：**  
特定的公司业务信息，仅限专门指定的人员获取；在公司内部严禁非业务相关人员讨论和传播；非授权的泄露将直接对公司业务造成严重不利影响，甚至是对业务造成毁灭性的影响，牵扯到重大法律责任的信息。  
**示例：**

* 未公开的财务绝密信息；
* 内部人事资料、薪资体系、工资单、雇员人力资源信息；
* 公司商业秘密：公司级业务战略决策、市场计划、尚未公布的并购计划和财务报告；
* 核心技术: 未申请专利的发明创造、商业秘密及其他知识产权信息等, 以及由上述信息衍生的所有数据或文档；
* 内网账号的密码及验证信息；各种业务系统的管理账户、密码及操作记录；
* 机密的业务信息：如财务系统和核心业务系统密钥、推荐算法、排序算法和加密算法等核心算法；
* 核心项目文档（包含产品设计图）等相关材料。
* 业务相关的核心数据，如：客户名单、重要合作伙伴名单、合作授权价格等；
* 业务风险相关数据，如：各类安全和业务风险策略；公司已经发现但外部尚不知晓的业务规则漏洞或系统漏洞。

**注意：任何非公开的业务数据的对外共享，均必须经过信息安全委员会审批；**