**广东乐育尚学科技有限公司**

**管理制度**

**————————————————★ ———————————————**

**广东乐育尚学科技有限公司个人信息安全管理规范**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **制度基本信息** | | | | | |
| **制度名称** | | 广东乐育尚学科技有限公司个人信息安全管理规范 | | | |
| **制度编号** | | LYSX-ISMS-WI-02 | | | |
| **制度层级** | | 公司级管理规范 | | | |
| **编制部门** | | 信息安全部 | | | |
| **发文部门** | | 信息安全部 | | | |
| **密级** | | □外部公开 ■内部公开 □秘密 □机密 □绝密 | | | |
| **修订历史记录** | | | | | |
| **版本** | **状态** | **修订内容说明** | **编制人** | **修订日期** | **发布日期** |
| V1.0 | 新建 |  |  | 2023-10 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 总则

* + 1. 为加强和完善公司的个人信息安全管理，提高个人信息安全保障能力，满足国家、行业的个人信息安全相关法律、行政法规、标准以及公司的个人信息安全管理需求，避免公司用户及员工个人信息未经授权的访问以及个人信息被篡改、被泄露、丢失或非法利用等，确保个人信息的保密性、完整性和可靠性，切实维护公司个人信息安全的发展利益，特制定本制度。

# 目的

* + 1. 本制度旨在规范广东乐育尚学科技有限公司个人信息安全管理的基本思路、数据分类分级管理，以及数据生存周期中各环节的个人信息数据安全管控，清晰、明确地提出个人信息安全的管理与技术要求，为合法、正当、安全、必要和诚信地进行个人信息数据处理活动，提供原则性指导和规则性指引。
    2. 本制度将作为公司个人信息安全管理的策略性文件，指导公司个人信息安全管控的运营和实施工作。

# 适用范围

* + 1. 本制度适用于广东乐育尚学科技有限公司本部及所属分、子公司。

# 术语和定义

* + 1. 数据

任何以电子或其他方式对信息的记录（定义来源《中华人民共和国数据安全法》）。

* + 1. 数据安全

通过管理和技术措施，确保数据有效保护和合规使用的状态（定义来源[GB/T 37988-2019]）。

* + 1. 保密性（Confidentiality）

使用信息不泄露给未授权的个人、实体、进程，或不被其利用的特性（定义来源[GB/T 25069-2010,定义2.1.1]）。

* + 1. 完整性（Integrity）

数据完整性旨在维护和保证数据在其整个生命周期中的准确性和一致性（定义来源[GB/T 29246-2017，定义2.40]、[大数据安全标准化白皮书]）。

* + 1. 可用性（Availability）

已授权实体一旦需要就可访问和使用的数据和资源的特性（定义来源[GB/T 25069-2010，定义2.1.20]）。

* + 1. 时效性

数据符合数据标准、数据模型、业务规则、元数据或权威参考数据的程度（定义来源[GB/T 36344-2018]）。

* + 1. 可访问性

数据能被访问的程度（定义来源[GB/T 36344-2018]）。

* + 1. 数据安全能力

组织在组织建设、制度流程、技术工具以及人员能力等方面对数据安全保障（定义来源[GB/T 37988-2019]）。

* + 1. 个人信息

以电子或者其他方式记录的与已识别或者可识别的自然人有关的个人信息，不包含匿名化处理后的信息。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：关于个人信息的判定方法和类型参见《附则一》。

注3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

（定义来源[GB/T 35273—2020]、《个人信息保护法》）

* + 1. 个人敏感信息

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、未满14周岁（含）未成年人的个人信息等。

注2：关于个人敏感信息的判定方法和类型参见《附则二》。

注3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。

（定义来源[GB/T 35273—2020]）

* + 1. 用户画像

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

（定义来源[GB/T 35273—2020]）

* + 1. 个人信息主体

个人信息所标识或者关联的自然人（定义来源[GB/T 35273—2020]）。

* + 1. 个人信息控制者

有能力决定个人信息处理目的、方式等的组织或个人（定义来源[GB/T 35273—2020]）。

* + 1. 个人信息处理者

是指自主决定处理目的、处理方式等个人信息处理事项的组织、个人（定义来源[中华人民共和国个人信息保护法]）。

* + 1. 个人信息的处理

包括个人信息的收集、存储、使用、加工、传输、共享、转让、公开披露、删除等活动（定义来源[中华人民共和国个人信息保护法]、[GB/T 35273—2020]）。

* + 1. 数据脱敏

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法（定义来源[GB/T 37988-2019]）。

* + 1. 匿名化

通过对个人信息的技术处理无法识别特定自然人且不能复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

（定义来源[GB/T 35273—2020]）、[中华人民共和国个人信息保护法]）

* + 1. 去标识化

个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。（定义来源[GB/T 35273—2020]、[[中华人民共和国个人信息保护法]）

* + 1. 自动化决策

通过计算机程序自动分析、评估个人的行为习惯兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。（定义来源[中华人民共和国个人信息保护法]）。

* + 1. 个人信息删除

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态（定义来源[GB/T 35273—2020]）。

* + 1. 公开披露

向社会或不特定人群发布信息的行为（定义来源[GB/T 35273—2020]）。

* + 1. 转让

将个人信息控制权由一个控制者向另一个控制者转移的过程（定义来源[GB/T 35273—2020]）。

* + 1. 共享

个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程（定义来源[GB/T 35273—2020]）。

* + 1. 删除

在实际日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态（定义来源[GB/T 35273—2020]）。

* + 1. 个性化展示

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动（定义来源[GB/T 35273—2020]）。

* + 1. 大数据

具有数量巨大、种类、流动速度快、特征多变等特性，并且难以用传统数据体系结构和数据处理技术进行有效组织、存储、计算、分析和管理的数据集（定义来源[GB/T 37983-2019]）。

* + 1. 数据消费者

大数据参考架构中的一种逻辑功能构件，是使用大数据应用提供者提供的应用的末端用户或其他系统（定义来源[GB/T 35589-2017]）。

* + 1. 大数据平台

采用分布式存储和计算技术，提供大数据的访问和处理，支持大数据应用安全高效运行的软硬件集合（定义来源[GB/T 37983-2019]）。

* + 1. 收集

负责处理与数据提供者的接口和数据引人（定义来源[GB/T 35589-2017]）。

* + 1. 预处理

包括数据雁阵、清洗、标准化、格式化和存储（定义来源[GB/T 35589-2017]）。

* + 1. 分析

基于数据科学家的需求或垂直应用的需求，确定分析数据的算法来产生新的分析，解决技术目标，从而实现从数据中提取知识的技术（定义来源[GB/T 35589-2017]）。

* + 1. 可视化

提供给最终的数据消费者处理中的数据元素和呈现分析功能的输出（定义来源[GB/T 35589-2017]）。

* + 1. 组织

由作用不同的个体为实施共同的业务目标而建立的结构。

注：组织可以是一个企业、事业单位、政府部门等。(定义来源[GB/T 37973-2019])

# 引用及参考的内部文件

* + 1. 本制度主要引用及参考《广东乐育尚学科技有限公司信息安全管理制度》、《广东乐育尚学科技有限公司信息系统账号及权限管理规范》、《广东乐育尚学科技有限公司违规管理制度》等内部文件。

# 数据安全管理原则

* + 1. 公司所有的数据活动应严格遵循以下数据安全管理原则：
    2. 职责明确原则

1. 设立数据安全组织架构，按照合理的数据安全分工原则，设置不同的数据安全岗位，并定义相关职责。
2. 根据组织架构的岗位职责要求，分配具备相应数据安全能力的人员，并为其设定角色，定义具体职责。
3. 根据数据安全的监管要求和公司业务需求，明确主要数据活动的实施主体及安全责任。
4. 应遵循“谁主管、谁负责”，“谁使用、谁负责”原则。如各业务线／平台/部门为数据责任主体，对各业务线／平台/部门产生及通过其他法、正当渠道获取、保管、使用的数据承担管理职责。
   * 1. 责任不随数据转移原则
5. 数据转移给其它组织时，责任不随数据转移而转移，应遵循“谁输出，谁负责”原则。
6. 数据控制者应在数据转移前，做好风险评估，确保数据转移后的风险可承担。
7. 公司应通过合同或其它有效措施，明确界定接收方的数据范围和要求，确保其提供同等或更高的数据保护水平，明确接收方的数据安全责任。
8. 公司应采取有效措施，确保数据转移的安全事件责任可追溯。
   * 1. 分类分级管理、确保安全可控原则
9. 应依法确定数据的密级及开放条件，加强数据分类分级管理。
10. 明确不同类别、等级的数据具有相应的数据安全管理要求，提高数据安全的监管力度，确保安全可控。
    * 1. 公开透明原则
11. 以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。
    * 1. 最小必要原则
12. 在采集数据前，公开数据处理规则，明示处理目的、方式和范围，确保处理目的具备明确、合理性。
13. 采取相应的管理策略、管理措施和技术手段实施有效管理，保证只采集与处理与目的直接相关的最小数据范围，不得过度收集数据。
    * 1. 最小授权原则
14. 应严格控制数据活动中的数据访问权限，保证在满足业务需求的基础上最小化权限。
15. 公司应加强对数据访问授权申请审批流程的管理。
16. 确保赋予数据活动主体的最小化操作权限和所需的最小数据集。
17. 及时收回过期的数据访问权限。
18. 保证在满足业务需求的基础上最小化权限，不得越权、私自处理数据。
    * 1. 目的明确原则
19. 数据处理目的要具备明确、清晰、合法和必要性等。
    * 1. 选择同意原则
20. 向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意。
    * 1. 主体参与原则
21. 向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。
    * 1. 安全合规原则

公司应制定安全规则、管理规范和操作流程，采取相应的安全管理策略、管理措施和技术手段实施有效管理，确保各项数据处理活动，主要安全合规原则如下：

1. 公司应理解并遵从数据安全相关的法律法规、合同、标准等。
2. 正确处理个人信息、敏感数据和重要数据。
3. 实施合理的跨组织数据保护的策略和实践。
   * 1. 可审计原则
4. 应对数据活动中的各项操作信息进行日志记录，且保证日志记录不可伪造和篡改。
5. 采取有效技术措施保证对数据活动的所有操作可追溯。
   * 1. 安全基线通用原则
6. 公司所有数据载体都应满足其承载数据的密级所对应的安全基线要求。
7. 数据的所有者应根据数据安全要求，实施与之相匹配的数据安全防护措施。

# 数据安全角色和职责

* + 1. 组织架构和职责分工

为更好地决策、推动和落实公司的数据安全管理工作，满足国家相关法规、行业监管要求以及公司数据安全要求，建立数据安全组织架构，主要分为数据安全委员会、数据安全管理小组和数据安全执行小组和数据安全审计小组四大组织，详细如图1所示：

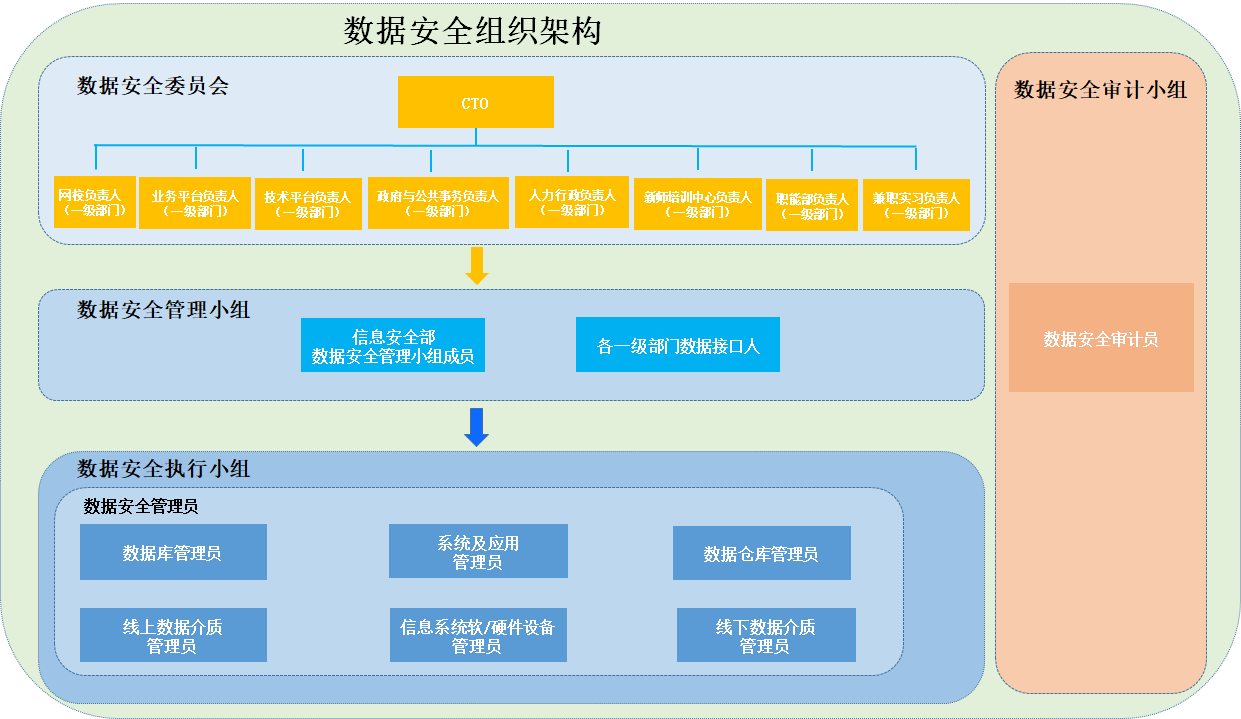


图 1 数据安全组织架构图

主要组织角色和职责分工如下：

* + 1. 数据安全委员会职责

作为公司数据安全组织架构的最高决策层，主要成员包括CTO、各一级部门负责人。

主要职责如下：

1. 为公司数据安全提供必要的资源。
2. 对重大数据安全活动做出决策。
   * 1. 数据安全管理小组职责

作为公司数据安全组织架构的管理层，主要成员包括信息安全部数据安全管理小组、各一级部门数据接口人。

主要职责如下：

1. 负责按照数据安全委员会的决策，落地执行数据安全管理工作。
2. 全局分析、掌控数据的数据安全风险，制定并落实数据安全相关制度和监管机制，推动数据安全工作的执行与监督管理。
3. 协助数据安全执行人员（如各业务线／平台/部门）结合各自业务场景，准确、合理地细化相关的数据安全操作规则与指南。
   * 1. 数据安全执行小组职责

作为公司数据安全组织架构的支持层，主要成员包括数据库管理员、数据仓库管理员、线下数据介质管理员等多种类型数据安全管理员。

主要职责如下：

1. 严格遵守公司数据安全管理规范的要求，从管理和技术两个层面，严格落实执行日常数据安全工作，并做好相关监控与审计工作。
2. 严格对各类数据的访问和操作行为等进行日志监控与审计，做好相应日志记录，及时判断风险并处理风险。
3. 数据安全执行小组应结合各自业务场景，细化数据安全操作规则与指南。
   * 1. 数据安全审计小组职责

作为公司数据安全组织架构以上三层组织的监督层，主要成员包含数据安全审计管理员。

主要职责如下：

1. 定期执行数据安全内部审计工作，发现数据安全问题，及时推动整改。
2. 负责对数据安全决策层、管理层及执行层的数据安全治理工作进行监督审计。
3. 配合外部审计机构进行数据安全审计工作。
4. 保管数据安全审计报告，为外部审计机构开展审计工作提供有效依据。
   * 1. 组织架构成员及职责分工

定岗定员，专业化分工，详细如表1所示：

| **序号** | **组织成员** | **职责** |
| --- | --- | --- |
| 1 | CTO | 1. 为公司数据的安全提供必要的资源，包括为数据安全工作提供人力、财力、物力保障等。 2. 对重大数据安全事项进行决策，包括建设方案、奖惩机制等。 |
| 2 | 各一级部门负责人 | 各一级部门负责人是本部门的数据控制者，承担所负责业务线的数据安全最终责任，主要职责包括：   1. 对本部门内部的数据安全活动和项目提供资源，包括为数据安全工作提供人力、财力、物力保障等。 2. 参与有关信息处理活动的重要决策，直接向CTO汇报工作。 3. 指派本部门内部的一级数据接口人（可以指定为自己，也可根据不同业务职能指派多个接口人）。 4. 数据安全的审批职责可以下放给数据接口人，但承担所负责业务线的数据安全最终责任。 |
| 3 | 信息安全部  数据安全管理小组成员 | 由信息安全部组建，主要职责为：   1. 随时关注国家、行业及监管机构的数据安全合规要求动态，调研、分析相关数据安全法律法规、标准和规定等，根据公司的风险承担能力和财务情况，制定适宜公司的数据安全管理规划和相关制度文档，并定期做好相关更新、优化和调整。 2. 承担维护数据安全制度运转的保障工作，以更好地适应和支撑公司的业务发展。 3. 制定公司数据安全管理规划、制度和流程，建立数据安全管理的责任与机制。 4. 与各数据接口人对接，讨论及制定数据安全解决方案，沟通、指导并推进数据安全管理规范的落地执行。 5. 重点审批各部门涉及C3、C4级数据的使用需求，对其合理性进行评估。 6. 为数据接口人、全体员工培训和宣贯数据安全相关管理规范的要求，组织开展数据安全意识培训。 7. 定期进行数据安全审计 8. 开展数据安全风险评估，提出数据安全整改建议，督促整改安全隐患。 9. 配合公司风控、内审和外审机构对数据安全开展的审计工作。 10. 与监督、管理部门保持沟通，通报或报告个人信息保护的事件处置等情况。 |
| 4 | 各一级部门数据接口人 | 数据接口人由一级部门负责人指派，不可与各一级部门数据负责人职责重复，是数据安全的第一道防线，主要职责为：   1. 与信息安全部数据安全小组对接，并协调资源执行数据安全制度在本部门的落地。 2. 承担维护数据安全制度运转的保障工作，可结合各自业务情况，将数据安全相关管理制度进行细化，并及时做好更新、调整和优化，以更好地适应和支撑公司的业务发展。 3. 配合梳理本部门的数据使用场景及安全需求。 4. 组织开展数据安全自查和风险评估工作。 5. 对本部门的数据使用(包括数据提取、数据权限等)申请根据合理性、必要性进行严格审批。 6. 数据安全事件的应急处置。 7. 制定各类数据安全事件应急预案（如数据安全事件应急预案、个人信息安全事件应急预案等），并根据相关法律法规变化情况，以及数据安全事件处置情况，及时更新应急预案。确保应急预案每年至少完成一次重新修订和评审。 8. 应定期（每年至少一次）组织内部相关人员进行应急响应培训和应急演练（如数据备份恢复演练、数据安全事件应急响应、个人信息安全事件应急演练等）。 9. 在产品或服务上线发布前进行检测，避免未知的个人信息被超范围、非授权地收集、使用、共享等。 10. 定期梳理本部门数据资产情况，维护管理数据资产表。 11. 其他与数据安全相关的工作。 |
| 5 | 各系统及应用管理员、数据库管理员、数据仓库管理员、网络设备管理员、各业务/平台/部门的线上和线下数据介质管理员 | 1. 协助本部门数据接口人，制定本部门数据安全实施细则，包括加密、脱敏、系统改造及日志监控等工作。 2. 严格执行数据安全管理制度及配套实施细则的要求。 3. 制定数据安全实施方案。 4. 协助本部门数据接口人，制定数据安全事件应急预案（如个人信息安全事件应急预案等），组织定期演练。 5. 跟踪部门内发现的数据安全问题并给出解决建议。 6. 对部门内出现的数据安全事件应及时上报，并配合数据安全管理者采取适当的处理措施处理相关安全事件，并做好相关数据安全事件记录以及事件处理报告。 7. 建立《数据安全事件处置库》文档，记录所有数据安全事件（包含但不限于常见数据安全事件、已发生数据安全事件等）的处理流程与处置方案等内容，为后续相关事件处置提供有力支撑与指导。 8. 记录数据活动的相关日志，集中进行日志管理，并实时进行审计日志进行分析、监控。 9. 配合内审和外审、信息安全部数据安全管理小组的相关数据数据安全工作 10. 配合本部门数据接口人、信息安全部数据安全小组等，定期梳理所负责系统的数据资产情况，及时更新数据资产表。 11. 其他与数据安全相关的工作。 |
| 6 | 数据安全审计员 | 1. 执行数据安全内部审计工作，及时发现安全问题，推动整改。 2. 负责对数据安全决策层、管理层及执行层的数据安全治理工作进行监督审计。 3. 配合外部审计机构进行数据安全审计工作。 4. 应妥善保管数据安全审计报告，为外部审计机构提供有效审计依据等。 |

表 1 数据安全组织成员及职责分工表

# 数据分类分级

* + 1. 数据分类分级应遵循如下原则：

1. 科学性原则：按照数据的多维特征及其相互间逻辑关系进行科学和系统化的数据分类分级。
2. 稳定性原则：应选择分类对象的最稳定的本质特征作为数据分类的基础和依据。
3. 实用性原则：数据分类要确保每个类别下要有数据，不设没有意义的类目，数据类目划分要符合对数据分类的普遍意识。数据分级要确保分级结果能够为数据保护提供有效信息，应提出分级安全要求。
4. 明确性原则：同一层级的数据类目间应界限分明。当数据类目名称不能明确各自界限时，可以用注释来加以明确。
5. 扩展性原则：充分考虑国际国内发展趋势，定期征询相关专家咨询组织和各部门意见，不断完善分级分类规则。
   * 1. 数据分类标准

本制度中所指的“数据”是信息的表现形式和载体，是指公司所持有的一切数据，包括但不限于各类应用系统（Web应用和APP）采集或产生的数据、各类应用服务产生的数据（如Wiki等）、数据库存储或产生数据、数据仓库存储或产生数据、自动化工具（如软件开发工具包SDK、统计分析工具、Shell脚本）采集的数据、网络设备及终端设备产生的数据、终端设备数据外部传入的数据、线下数据载体记录的数据，以及其它形式记录、处理后的数据等，如数字、文字、语言、图像、视频、程序代码、配置命令、源数据、二次加工（如匿名化、去标识化）后的数据、邮件信息、通知信息、企业一般管理数据、分析类信息（如日志告警、自动化分析构建的用户画像等）、日志记录、消费信息和账单、商业秘密、个人信息、保密商务信息等。

综合分析公司的数据特征及适用场景，遵循以上数据安全分类分级原则，将公司数据主要划分为用户类、员工类、企业运营管理类、合作伙伴类四大类，并制定如下分类标准

数据分类标准如下：

1. 用户类

公司产品和服务中涉及到的用户个人数据，如在用户注册、交易支付、使用产品和服务过程中的用户基本信息、交易信息等。

1. 员工类

公司所有员工、人员（包含签订劳动合同的员工、实习生以及其他签署劳动协议、劳务协议、派遣协议、顾问合同等的人员）的人事信息（如个人信息、家庭信息、关键岗位信息、薪酬信息等）等。

1. 企业运营管理类

公司经营、管理所产生的数据，如财务数据、业务发展及经营数据、资产数据、信息系统数据等。

1. 合作伙伴类

来源于公司所属产品和服务的合作企业相关数据（如合作渠道、服务供应商的企业基本信息、合作数据等），以及合作伙伴的数据（如资产供应商的交易信息、测评服务商的整改建议书等）。

* + 1. 数据分级标准

根据数据的价值和知密范围，以及数据的保密性、完整性和可用性遭受篡改、破坏、泄露、丢失或被非法利用，对自然人、法人和其他组织，以及社会秩序、公共利益和国家安全等带来的潜在影响，将以上类别的数据进行数据分级，按照敏感程度由低到高分为公开数据（C1级）、内部受限数据（C2级）、机密数据（C3级）、绝密数据（C4级）四个级别。数据安全分级标准如下表2所示：

| **数据级别标识** | **数据重要程度标识** | **定级标准** |
| --- | --- | --- |
| C1 | 低敏感级 | 1. 适合对外向任何人开放，或可被公开获取、使用。 2. 数据的完整性、保密性、可用性遭受篡改、破坏、泄露、丢失或非法利用后，对个人、法人和其它组织、社会秩序和公共利益的影响程度是“轻微”或“无” |
| C2 | 较敏感级 | 1. 公司确定为内部公开的信息，可以允许内部员工获取该信息不需要任何特殊授权。 2. 数据的完整性、保密性、可用性遭受篡改、破坏、泄露、丢失或非法利用后，对个人、法人和其它组织、社会秩序和公共利益造成一定的损害。影响程度是“中等”或“轻微”。 |
| C3 | 敏感级 | 1. 仅数据责任主体、数据使用协同部门及相关人员可见（经数据责任主体授权）的数据（有条件开放与非开放数据），该类数据访问需要得到特别授权，知密范围应控制在使用角色级，经共享申请和审核后，符合条件的，按照特定方式提供给指定使用对象。 2. 数据的完整性、保密性、可用性遭受篡改、破坏、泄露、丢失或非法利用后，极易对个人、法人和其它组织、社会秩序和公共利益造成显著损害，明显影响部门开展业务和提供服务等。且在一定时期和阶段弥补损害需要耗费较大资源。影响程度是“中等”或“严重”。 |
| C4 | 极敏感级 | 1. 非开放数据，仅少数人授权可见或完全不可见，其安全防护级别要求最高，且其使用必须被全程监控，不允许出现错误或要求错误在极短时间内可恢复等。 2. 数据的完整性、保密性、可用性遭受篡改、破坏、丢失或非法利用后，会对个人、法人和其它组织、社会秩序和公共利益造成严重损害，在一定时期和阶段弥补损害难以弥补或无法弥补。影响程度是“严重”。 |

表 2 数据分级标准

注意： 影响程度定义见附件四。

* + 1. 数据分类分级参考

按照数据分类分级标准，对公司所有数据进行归类汇总，具体如下表3所示：

| **数据类型** | **数据级别标识** | **数据范围** | **举例** |
| --- | --- | --- | --- |
| 用户类 | C1 | 不适用 | 无 |
| C2 | 除个人敏感信息以外的个人信息 | 个人基本资料：年龄、性别、国籍等。 |
| C3 | 除具有唯一标识符外的个人敏感信息 | 性取向、民族、好友列表、个人上网记录、交易信息等 |
| C4 | 具有唯一标识符的个人敏感信息 | 姓名、电子邮箱地址、电话号码、个人身份信息、银行卡号、个人身份信息、地址信息等 |
| 法律法规规定不可公开的个人信息 | 学生的考试成绩、名次等学业信息（如成绩单）、未满14周岁（含）的未成年人个人信息等，个人信息参考表A.1。 |
| 企业运营管理类 | C1 | 由公司确定为外部可公开的信息 | 公司发布的年报、招聘信息、公司特别声明、官方网站公开的网页信息、新媒体报道、对外公开的交易信息、对外发布的融资信息、对外披露的财务信息等。 |
| C2级别经过模糊化（如匿名、脱密、脱敏、去标识化等技术）处理后降级的数据 | 公司内部公开资料经模糊化处理后可公开的数据，如脱敏后的制度文档、记录表单等。 |
| C2 | 公司内部公开文档资料 | 制度规范、操作流程、记录表单模板、培训计划、员工行为规范、培训资料、内部公开的统计报表（仅反应部门业绩）等。 |
| 公司内部定期发布的公开信息 | 内部公告、内部通知、内部产品福利信息、公司福利政策等 |
| 不能唯一标识物体的信息 | 笔记本/ 台式机类型、型号，浏览器类型等 |
| C3、C4级别经过模糊化处理（包含匿名、脱敏、脱敏）后降级至C2级别的数据。 |  |
| C3 | 具有唯一标识的物体信息 | 设备识别码、SN号等、设备标签等 |
| 公司部门内部或项目级别的非核心数据 | 部门内非核心的代码或算法，加解密密钥，所有业务级、应用级、平台级、IT设备等的参数配置，业务数据及后台运营数据，商务数据等。 |
| C4级别数据过模糊化处理（包含匿名、脱敏、脱敏）后降级至C3级别的数据。 |  |
| C4 | 公司财务数据 | 公司盈余或盈余预测、财务状况和资产价值的变动、资本投资计划或该计划的变动、重大的借款或融资活动、债务拖欠、发行新的股票或债务，财务数据，包括会计方法和冲销的变动等。 |
| 企业核心管理数据 | 如有关并购或变卖重要子公司或资产的谈判、新签订的重大合同或重大合同意向书、新推出的重大产品或服务、重大的市场计划或该计划的变动、有关公司高管层或董事会成员的重大诉讼、行政处罚行为、政府调查或质询，重大人员变动，以及任何能够极大影响公司盈余或发展前景的行业环境或竞争态势的人员、业务统计报表等 |
| 知识核心产权数据 | 核心产品相关项目文档（需求/设计/开发/实施文档、流程图等）、代码、算法、加解密密钥等 |
| 网络运维认证鉴权数据 | 设备登录、平台、数据库管理类账户密码、数字证书、密钥等。 |
| 员工类 | C1 | 不适用 | 无 |
| C2 | 除个人敏感信息外的个人信息 | 性别、主管/所属部门、入职时间等 |
| 员工公司内部发布的言论和信息 | 企业微信的聊天记录、内部网站的评论信息等 |
| C3 | 职务信息 | 转正时间、职位名称等 |
| 除具有唯一标识符外的个人敏感信息 | 出生日期、好友列表、工作经历、婚姻状况、薪资调整历史数据等 |
| 员工电脑信息 | 个人网页浏览记录、群组列表等 |
| C4 | 员工真实身份标识 | 个人身份信息，见表B.1 |
| 个人财务信息 | 银行账号、信用卡账号、收支流水记录、薪资信息等 |
| 员工高敏感数据 | KPI绩效信息、任职级别、家庭详细住址等 |
| 合作伙伴类 | C1 | 不适用 | 无 |
| C2 | 不适用 | 无 |
| C3 | 不适用 | 无 |
| C4 | 企业合作伙伴业务信息 | 知识产权、商业信息、敏感信息、学校不允许公开的信息 |

表 3 数据分类分级标准模板

* + 1. 数据级别推导原则
    2. 数据升级原则

1. 两个及以上的数据项组成的数据集，能够形成更重要的新敏感数据，或更高级别的用户隐私数据，甚至形成一个具有唯一标识性的新数据，本数据安全级别应不低于各数据项最高者。如学生姓名（C2）、学生身份证号（C4），组成的数据集的数据安全级别为C4级。
2. 通过统计、分析或加工某数据项（组）的多条记录，形成的某项指标（如地域分布、年龄分布、间接或直接用户画像）的数据级别不低于该数据项（组）的级别。
   * 1. 数据降级原则
3. 为了充分利用数据资源，公司允许数据以直接或间接的方式进行降级处理，可通过数据脱敏、去标识化、匿名化等技术实现数据降级。
4. 数据降级后的数据定级应严格按照数据分类分级标准进行判定。

# 数据安全管理要求

* + 1. 本制度在数据整个生存周期安全和通用安全两方面，分别提出相应安全要求，各业务线/平台/部门须根据此要求执行数据安全工作，同时可根据本业务线/平台/部门的特殊业务场景，在不违反以下原则的情况下进行安全要求的细化，并报安全部备案。
    2. 数据生存周期主要分为数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁六大阶段，详细如下：

1. 数据采集：组织内部系统中新产生数据，以及从外部系统收集数据的阶段。
2. 数据传输：数据从一个实体传输到另一个实体的阶段。
3. 数据存储：数据以任何数字格式进行存储的阶段。
4. 数据处理：组织在内部对数据进行计算、分析、可视化等操作的阶段。
5. 数据交换：组织与组织或个人进行数据交换的阶段。
6. 数据销毁：对数据及数据存储媒体通过相应的操作手段，使数据彻底删除且无法通过任何手段恢复的过程。
   * 1. 数据生存周期安全主要分为数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全。
     2. 数据采集安全主要包含数据分类分级、数据采集安全管理、数据源鉴别及记录等。
     3. 数据采集过程中应遵循合法、正当、诚信、最小必要和最小化授权同意等原则。
     4. 采集个人信息应当遵循公开、透明原则，公开个人处理规则，通过弹窗、文本链接及附件等简洁、明显且易于访问的方式，向用户明示、告知个人信息处理主体、处理的目的、方式、处理范围及保存期限等。（如隐私政策附件）
     5. 收集个人信息应当限于实现处于目的的最小范围，不得过渡收集个人信息。
     6. 数据采集活动包括数据获取和创建过程，采集内容包括但不限于：
7. 系统运行过程中产生的业务数据。
8. 以及各种系统、程序和服务运行过程产生的运维和日志数据。
9. 产品、服务程序主动收集的数据，如IMEI、GPS位置信息等。
10. 产品、服务过程中用户填写的数据，如手机号、收货地址等。
    * 1. 数据采集安全要求，主要如下：
11. 根据数据分类分级的定义，对采集数据的敏感级别进行识别，对不同敏感级别的数据实施相应的安全管理策略和保障措施。
12. 对外提供服务的应用系统向用户采集个人信息时，应明确、合理定义并公开数据采集的原则、目的、方式、用途，明确数据采集源和采集范围，只采集满足业务所需的最小数据集。通过隐私政策的形式，声明并取得被采集人的明示同意。
13. 定期评估和检查产品和服务是否满足个人信息保护等法律法规，产品和服务在需求设计阶段需要主动进行个人信息、个人隐私采集的安全评估。并将评估结果作为业务能否上线的准入要求，公司审批通过后方能收集。
14. 不得非法收集他人个人信息。对于未满十四周岁未成年人的个人信息，应当取得未成年人的父母或者其他监护人的同意后，才可以进行收集。
    * 1. 数据存储安全包括线上存储安全和线下存储安全。
      2. 数据线上存储安全要求
15. 为确保数据的可用性，需制定数据备份及恢复测试策略，并按要求定期执行。
16. 存放在服务器或共享存储空间中，应当严格控制访问权限，必须获得相应的数据授权后才可以访问。
17. 应对存储数据进行分类分级，对敏感数据进行加密处理。
18. 对于不需要还原密文的场景，必须采用随机带盐值的 HASH 算法进行存储。其中，散列函数推荐使用 SHA1+盐等哈希算法，一用户一盐。
19. 客户端场景下，手机、电脑上存储的个人信息、敏感信息，也应做加密存储。
20. 个人信息存储期限应为实现个人信息主体授权使用的目的所必须的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外。并且超出该场景的个人信息存储期限后，应对个人信息进行删除或匿名化处理。
21. 收集个人信息后，应立即进行去标识化处理，并采取技术和管理方向的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。
22. 针对个人敏感信息的存储，确保个人生物识别信息应与个人身份信息分开存储。
23. 不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：
24. 仅存储个人生物识别信息的摘要信息。
25. 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能。
26. 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。
27. 当公司停止运营产品或服务时，应采取如下措施：
28. 及时停止继续收集个人信息。
29. 将停止运营的通知以逐一送达或公告的形式通知个人信息主体。
30. 对其所持有的个人信息进行删除或匿名化处理。
31. 对于需要还原密文的场景，必须使用业界认可且不易被攻破的加密算法，例如对称加密至少使用 AES-256，非对称加密建议秘钥长度 1024 以上。加密机制设计参考表4和图2。

|  |  |
| --- | --- |
| **关键项** | **描述** |
| 统一平台 | 公司应建设统一的数据加解密服务平台，为各业务提供接入服务 |
| 平台组件 | 平台应实现密钥管理服务KMS、业务主密钥CMK、数据密钥DEK |
| 数据接口服务 | 提供统一的数据接口服务，减少应用直接访问数据库操作敏感数据 |
| 一用户一密钥 | 为每个用户提供单独的密钥，减少被破解的风险和概率 |
| 二级加密 | 加解密平台应设计为多层加密系统，对密钥进行二次加密，防止单点突破和泄漏 |
| 访问控制与审计 | 对不同的业务调用方，应设置单独的API\_KEY，记录和审计每次调用 |

表 4 数据加密服务涉及关键项

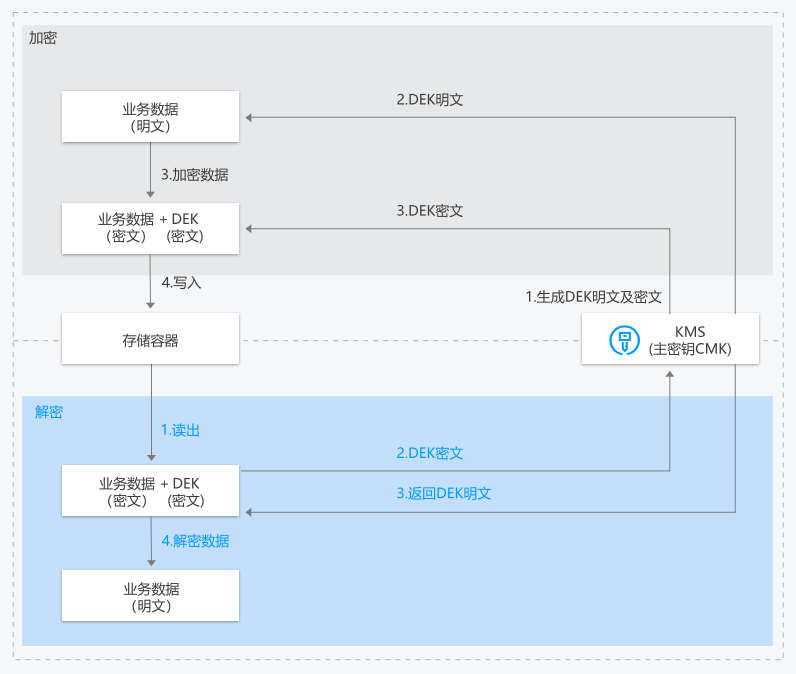


图 2数据存储加解密设计图

* + 1. 数据线下存储安全要求

1. 公司员工应确保敏感数据的安全，禁止使用非加密移动存储设备拷贝、存储敏感数据。
2. 原则上禁止将敏感数据存放在本地电脑，敏感数据的获取与使用需在公司提供的平台中完成。
3. 涉及“敏感数据”的纸质文档应当保存在有锁的柜子中或独立的封闭区域（如档案室等），并且有门禁等进出记录。
4. 涉及“敏感数据”的纸质文档不再使用后，应当立即以安全的销毁方式进行销毁。
   * 1. 数据使用安全
     2. 数据展示安全要求
5. C1级别数据对外展示不受限制。
6. C2及以上级别数据只对已授权用户展示，且应用系统中的个人敏感信息实现脱敏展示，包括但不限于姓名、证件号码（如身份证号、护照号）、银行卡号、地址、手机号码、固定电话、邮箱等。
7. 通过界面展示个人信息的（如显示屏幕、纸面等），在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。
8. 为准确评价个人用户状况，可使用直接用户画像，而用户推送商业广告目的时，则应使用间接画像，确保使用个人信息时消除明确身份指向性，避免精准定位到特定个人。
   * 1. 数据脱敏安全要求
9. 所有包含敏感数据的应用系统应具备脱敏功能，采用自动扫描工具对系统中敏感数据进行扫描，识别敏感信息并脱敏处理。
10. 敏感数据脱敏必须由应用程序后端执行，避免通过查看源代码获取明文信息。
11. 应建设自动化扫描工具，对敏感数据进行自动发现、打标和监控。
12. 测试环境禁止使用线上真实数据用于系统测试，若必须使用线上数据测试时必须脱敏处理。系统上线后进行线上验证时，读写操作不允许影响线上用户及数据安全。
13. 数据脱敏降级应遵循业务适配原则，业务方根据原始数据特点、应用场景不同制定脱敏规则。
14. 数据脱敏应保持信息属性，如保留原数据的格式、原数据类型、原数据之间的依存关系、语义完整性、引用完整性、数据统计特征等。
15. 公司构建并维护通用敏感数据集合，各部门在此基础上细化各自的数据脱敏规则。通用敏感数据集包括但不限于：姓名、身份证号、银行卡号、手机号码、地址，以及学生的考试成绩、名次等学业信息。其中身份证号、银行卡号、手机号码、地址应进行全脱敏或半脱敏展示，具体脱敏方式如表5所示：

|  |  |
| --- | --- |
| **敏感数据** | **脱敏规则** |
| 姓名 | 展示第一个字，后面都隐藏。如：张\* |
| 手机号 | 显示前3位和后4位，中间隐藏。如：139\*\*\*\*1097 |
| 固定电话号码 | 显示前3位和后4位，中间隐藏。如：010\*\*\*\*1097 |
| 邮箱 | 显示邮箱前缀前3个字符，其余部分隐藏。如：wei\*\*\*\*\*@qq.com |
| 证件号码 | 身份证号：显示前 5位＋ \*（实际位数）＋后 3 位，如：11010\*\*\*\*\*\*\*\*\*\*25X 其他证件：显示前4位，其余隐藏。如：2384\*\*\*\*\*\*\*\*\*\* |
| 银行卡号 | 显示前4位和后4位，中间隐藏。如：6226\*\*\*\*\*\*\*\*1097 |

表 5 通用脱敏规则表

* + 1. 数据水印安全要求

1. 内部应用系统，如客服等面向员工的系统，页面应具备自动添加水印功能识别用户信息，如包含用户名或编号。
2. 从内部应用系统中截图、下载、打印的网页或数据文档，应自动添加水印。
   * 1. 自动化决策处理的使用安全要求
3. 针对公司具有自动化决策处理的产品或服务，应严格遵守合法、正当、必要、诚信、最小化、公开透明等处理原则，不能滥用个人信息，不能滥用算法，禁止“大数据杀熟”，保证自动化决策的透明和结果公平、公正。
4. 公司具备自动化决策处理的产品或服务，禁止通过大数据技术根据用户的个人特征（如学生的学习偏好、学习习惯等）推送特定的商品或服务，或为了“获客”“拉新”针对新人或特殊群体，推行损害其消费合法权益的优惠营销策略。
5. 通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征（如性格、购买习惯、经济状况等）的选项，或者向用户提供便捷的拒绝方式。
6. 在自动化技术规划设计、正式使用前，应开展个人信息安全影响评估，并依据结果采取有效的保护个人信息主体的措施。
7. 应对正式上线具备自动化决策机制的信息系统，定期开展个人信息安全影响评估，并依据评估结果改进保护用户个人的安全防护措施。
8. 应向用户提供针对自动决策结果的投诉渠道，并支持对自动化决策结果的人工复核。
   * 1. 数据传输安全

根据公司内部和外部的数据传输要求，采取适当的加密保护措施，保证传输通道、传输节点和传输数据的安全，防止传输过程中的数据泄露、篡改、丢失。

* + 1. “敏感数据”在传输时，必须遵守以下安全要求：

1. 敏感数据通过网络传输过程中应使用公司认可的加密传输协议，如 HTTPS 加密传输方式，使用数字签名保证数据在传输过程中的一致性和不可否认性。使用的加密算法和签名技术应符合国家相关法律法规要求。
2. 应选择安全的加密协议和加密套件，禁用过期的协议和算法，如SSLv3、RC4、DES等。
3. 推荐在应用层进行二次加密或HASH，如用户登录接口传输HASH后的password字段。
4. 通过邮件发送“敏感数据”时，必须进行加密，并通过其他方式（如短信、电话）约定解密密钥。
5. 使用 U 盘或其他移动介质传输“敏感数据”时，需要对文件进行加密。
6. 禁止通过任何外部即时聊天工具、外部第三方存储设（如网盘、云盘）等传送公司敏感数据。
   * 1. 数据交换（共享）安全
     2. 数据交换安全要求
7. 敏感数据在对外部合作方、内部跨部门提供前必须进行审批，并提请安全部开展数据安全评估，审批流程参考本制度中《数据安全管理流程》，安全部评估合作数据范围、字段、数据保护方式是否符合安全要求。
8. 外部系统之间数据接口的调用应能够提供 token授权、签名、时间戳超时等机制，防止接口数据被篡改或重复调用。
9. 应限制接口调用的次数和频次，防止大量访问以及大量占用资源的情况，保证系统的可用性。
10. 应实现对接口的运行情况实时监控及报警，及时发现数据传输错误或异常。
11. 提供的数据遵循最小必要原则，敏感数据应进行加密、脱敏等方式处理后提供。
12. 未经用户授权同意不得将用户留存在的注册信息泄露给第三方合作方。但是，经过处理无法识别特定个人且无法复原的除外。
    * 1. 数据交换安全协议
13. 严格遵循《网络安全法》的要求，制定对外数据共享和披露细则，明确所有对外数据共享和披露必须保护用户隐私。涉及到用户个人信息，未经用户授权，不得向第三方提供。
14. 向供应商、合作伙伴等商业机构提供敏感数据，除按照本制度中《数据使用申请审批管理》中的使用申请审批流程进行审批外，还应在双方合作协议中明确数据保护的安全责任与义务，并包含违约惩罚机制。
    * 1. 数据销毁安全

应建立针对数据内容的清除、净化机制，实现对数据的有效销毁，防止因对存储介质上数据内容的恶意恢复而导致数据泄漏风险。

数据销毁需遵循以下安全要求：

1. 敏感数据存储介质禁止二次利用。删除敏感数据时，应对介质进行消磁或彻底格式化，并使用专用工具在存储区域填入无用信息进行覆盖，处理手段包括但不限于多次擦除并填充垃圾信息、消磁、砸毁等方式。
2. 对敏感数据物理删除前，需由操作人员进行登记，并提交给业务数据负责人批准，所有的敏感数据清理都应记录备案。
3. 终端设备闲置后报废后，应当对硬盘进行低格处理，方可以进行转个人或转给其他员工使用。
4. 在数据使用期限到期之后，原则上申请人必须删除保存在本地、邮箱、服务器或共享存储空间上的数据。
5. 涉及“敏感数据”的纸张不得暴露在公共区域，并且在不需使用时及时销毁。
6. 涉及“敏感数据”的纸质文档销毁时，应当使用碎纸机销毁。
7. 产品和服务应提供用户注销服务，注销后应进行匿名化处理，已加密的个人信息，可以采取销毁加密密钥的方式实现个人信息的销毁。
8. 针对数据销毁，设置相关监督角色，做好数据销毁监督工作。
   * 1. 通用安全要求
     2. 数据资产管理
9. 应建立数据资产安全管理策略，对数据安全全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程。
10. 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定相应强度的安全保护要求。
11. 应定期评审数据的类别和级别，如需要变更数据所属类别或级别，应根据变更审批流程执行变更，并同步更新数据资产清单。
12. 应对数据资产和对外数据接口进行登记管理，建立相应的资产清单。
13. 针对当前环境下数据安全措施、产品、工具的梳理。
14. 全面梳理各系统的敏感数据资产，包含敏感数据的分布情况梳理、访问情况梳理、授权情况梳理，以及采取的数据安全管理措施现状进行梳理。
15. 信息安全数据安全管理小组、各部门数据接口人应根据数字资产的梳理情况，以及数据资产类别和级别，进行综合分析、汇总，及时发现安全管理和技术防护存在的安全问题，推动数据安全管理与技术整改，提高数据安全防护能力，降低风险发生概率。（如，临时活动采集的敏感数据，未统一进行加密处理等）
    * 1. 鉴别与访问控制
16. 公司承载敏感数据的系统/平台/功能服务，应集中加入统一用户身份鉴别管理系统，通过对账户信息进行安全认证，实现统一单点登录管理。
17. 针对大数据平台/数据仓库/数据库等的数据访问必须遵循统一的身份鉴别机制。采用统一单点登录身份认证技术对用户进行身份鉴别管理。
18. 基于用户和角色的认证统一体系，应遵从账户/角色（基于角色的访问控制）模型，实现通过角色进行权限管理，对用户进行批量授权管理，降低集群的管理难度，通过角色创建访问组件资源的权限，可以细颗粒度地管理资源（如文件、目录、表、数据库等访问权限），将角色授予用户/用户组，简化用户/用户组的权限配置。
19. 应根据数据访问主体身份，以及被访问数据的密级，实现对各类数据的访问授权。对于C3级及以上的数据，需要严格执行数据安全申请审批流程。
    * 1. 数据安全监控和审计

针对数据生存周期各环节开展安全监控和审计，以保证对数据的访问和操作得到有效的监控和审计，执行有效的日志审计管理，以实现对数据生存周期各环节中可能存在的未授权访问、数据滥用和数据泄露、篡改、丢失等安全风险的防控。 主要包含管理和技术两方面安全要求。

1. 管理层面要求
2. 各业务线/平台/部门应按照数据的重要程度，对数据生存周期各环节的数据访问和操作，建立相应的监控与审计规则、方案，如实时监控、定期批量监控等。
3. 各业务线/平台/部门应对电子记录（如各系统及应用、数据库、数据仓库等）和非电子记录（如纸质）形式的数据载体中的数据，以系统或部门为单位，设立相应的数据安全监控和审计岗位，指定具体人员，负责对数据生存周期各环节的数据访问和操作行为中的安全风险进行监控与审计，能够识别数据泄露、篡改、丢失风险，并及时应对。
4. 应对各系统和应用、软硬件设备或服务的审计日志记录进行统一集中管理，实现异地备份存储。
5. 定期进行内部审计或外部审计，协同推动数据安全管理工作的开展与改进。
6. 审计过程形成的记录应对安全事件的处置、应急响应和时候调查提供支撑。
7. 应检测或防止非授权访问、篡改、删除审计记录。
8. 审计数据被授权修改时，对该操作进行审计。
9. 只有具有相应权限的用户，才可以读取对应的审计数据。
10. 应及时处理审计过程中发现的违规使用、滥用、恶意操作等情况。
11. C3 及以上密级数据均保存所有访问的日志，用于审计。敏感数据的更新、批量查询和导出必须保存日志记录，日志内容至少包括操作员、操作时间、操作内容、操作结果、操作方式等。
12. 应定期审核C2及以上密级数据的定级、共享、外发、删除、降级，确保操作合理性。相关授权文档、访问日志等记录应保存至少6个月，确保安全事件的事后追溯、定位问题原因及划分事故责任提供有力依据。
13. 技术层面要求
14. 在数据生存周期各环节中，针对用户管理、权限管理、用户登录、数据获取/访问/修改等操作行为进行完整日志记录，做好集中统一管理。
15. 根据相关的系统审计日志，进行实时监控、分析，实现事中可发现，事后可追溯和取证分析。
16. 应具备对数据的异常或高风险操作进行自动识别和实时预警的能力。
17. 新域名申请与新业务系统上线，均需要进行数据安全审计。
18. 日志中的数据为C3及C4级别，业务记录的日志中包含明文敏感数据字段的，应统一进行加密、脱敏处理。特殊日志除外。
19. 定期进行内部审计或外部审计，落实数据安全技术层面改进。
20. 新域名申请与新业务上线前，均需要进行数据安全审计。
21. 应对数据使用行为进行审计，发现违反规则、恶意操作等行为时及时处置。
22. 应建立自动化审计系统，监测记录个人信息处理活动。
    * 1. 第三方接入管理

公司提供的产品（如APP）或服务中接入或调用第三方的产品或服务（如软件开发包SDK、第三方API接口）等时，应遵循以下安全管理要求：

1. 未经用户同意，不得向第三方应用提供个人信息。
2. 公司产品或服务接入的第三方产品或服务具备收集个人信息功能时，应向个人信息主体（即用户）明确告知个人信息处理者（包含但不限于公司、部门等）的名字和联系方式、处理目的、处理方式和个人信息的种类等事项，获得用户明示同意。（如APP以“弹窗”方式明确告知用户，并获得用户授权同意）。应严格遵守《个人信息安全规范》、《移动互联网应用程序（APP）个人信息安全防范指引》等中的相关规定。
3. 针对接入的第三方产品或服务，收集的个人信息完全由第三方接入管理时，应满足以下要求：
4. 应建立第三方接入产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件。
5. 应与第三方产品或服务提供方通过合同等形式，明确双方的安全责任及应实施的个人信息安全措施。
6. 应向用户明确标识产品或服务由第三方提供。
7. 应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅。
8. 应要求第三方严格遵守《个人信息安全规范》，向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式。
9. 应监督第三方产品或服务建立个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用。
10. 公司提供的产品或服务嵌入第三方自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，为确保合作过程中的技术监督和行为审计，应采取以下措施：
11. 通过技术检测确保其个人信息收集、使用行为符合数据安全规范要求。
12. 对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出合同约定或最小化必要的行为，及时切断接入。
    * 1. 通用基线安全要求

公司所有新建或已投入使用的应用系统应遵循本章的基线安全要求。

1. 所有包含C2及以上密级数据介质或文档都应明确标识敏感级别。
2. 公司所有涉及C3及以上密级数据的系统应具备以下功能要求，主要如下：
3. 所有访问应认证鉴权，细化到个人账户。
4. 应有安全的登录机制，具有中等级以上认证强度。C4级数据需要采用双因子认证机制。
5. C3及以上密级数据应存储于具备正当安全防护措施的存储设备中，C4级数据需要加密存储。
6. C3及以上密级数据应加密传输。
7. 从数据仓库到数据应用产品时，C3及以上密级数据不应下载到本地设备编辑或处理，C3及以上密级数据在业务系统中应脱敏展示。
8. 禁止应用系统和管理后台私自开发 C3及以上密级数据的导出、下载功能，如有特殊需求需报备数据安全管理小组邮箱进行评估。
9. C3及以上密级数据分发应至少选择以下一种手段进行保护：
10. 采用数据水印技术，确保对分发后的数据的追踪，在数据泄露、篡改、丢失行为发生后，对造成数据泄露的源头可回溯。
11. 采用数据加密技术，对关键字段进行加密。
12. 采用数据脱敏技术，对关键数据进行脱敏处理。
13. C2及以上密级数据的访问必须建立清晰的访问控制策略，且授权只能用于已明确授权的用途。授权必须通过申请审批流程，且应记录审批过程并可查询。
14. 数据使用审批应明确数据访问频次以及是否批量查询与下载，明确工作开展必需的字段。
15. 密级与安全要求保持一致性，C3、C4 级数据跨系统使用必须经过审批，提供保证数据安全要求一致的防护方案。
16. 授权使用数据时，应明确数据使用期限，C3及以上级别的数据的访问权限应设置时效性，最长授权时间不得超过6个月，到期后应清理数据。

# 数据使用申请审批管理

* + 1. 数据使用场景主要分为内部使用和外部使用。针对数据的不同使用场景，结合提取的数据量大小以及数据的敏感级别，分别制定相应的数据使用申请审批管理流程。
    2. 内部使用申请审批管理
    3. 涉及“敏感数据”的权限申请、访问获取等流程必须经过相应授权审批，并且数据的访问和使用只能用于已明确授权的用途。数据的申请、审批、使用应遵循以下要求：

1. 禁止外包人员申请公司的C3、C4 数据权限。
2. 外包人员的临时权限有效期不得超过3个月。
3. 应用系统之间的数据交互权限申请默认为长期权限，不需要设置有效期。
4. 生产数据不得明文导入测试环境使用。
   * 1. 数据的内部使用包括申请本部门数据或申请目标部门数据，具体申请审批流程如图3所示：



图 3 数据内部使用申请审批流程图

* + 1. 申请审批流程详细描述见下表6：

|  |  |  |
| --- | --- | --- |
| **步骤** | **任务描述** | **相关负责人** |
| 1 | 1. 申请人提出数据权限申请，申请形式可以通过邮件审批，发送给相关方并抄送数据安全管理小组邮箱。数据接口人保留数据申请邮件记录，以便后续复核； 2. 申请人应当基于业务需求提出数据提取申请，申请时应说明的信息包括：申请人、申请人所在部门、申请人的岗位信息、申请字段、原因、数据预估量、使用期限、获取方式等，申请原因需详细描述，细化到项目或任务。 | 申请人 |
| 2 | 申请人所在部门直接领导开始逐级审批，根据申请内容审核是否有此业务需要。若审核通过，则进入步骤3；若审核不通过，则驳回申请 | 申请人逐级领导 |
| 3 | 本部门一级数据接口人对申请的必要性、合理性进行审批。如不通过，则驳回申请；如通过，则需要继续判断是否跨部门提取数据。如涉及跨部门提取，则进入步骤4；如不涉及跨部门提取，则需要继续判断是否涉及C3、C4级别数据。如涉及，则进入步骤5；如不涉及，则直接进入步骤6 | 本部门一级数据接口人 |
| 4 | 目标部门一级数据接口人对申请的必要性、合理性进行审批。如不通过，则驳回申请；如通过，则需要继续判断是否涉及C3、C4级别数据。如涉及，则进入步骤5；如不涉及，则直接进入步骤6 | 目标部门一级数据接口人 |
| 5 | 信息安全部数据安全管理小组对申请的安全性、合理性进行审批。如不通过，则驳回申请，并提出安全建议，申请人修改方案重新提交申请；如通过，则进入步骤6 | 信息安全部数据安全管理小组 |
| 6 | 技术人员根据审批结果，按要求提供技术支持，提供数据，流程结束。 | DBA、大数据等技术人员 |

表 6数据内部使用申请审批流程

* + 1. 外部使用申请审批管理
    2. 外部使用指申请数据共享给其他个人信息处理者，或者开放接口与第三方进行数据交互，或数据接口合作，或者向监管单位报送数据等情况，数据对外使用需遵循以下安全要求：

1. 除向监管单位报送的特殊情况外，C3、C4 级别的敏感数据必须脱敏后提供给第三方，并且不能被逆向破解。
2. 敏感数据脱敏展示必须在服务器端进行脱敏处理，禁止在客户端脱敏屏蔽。
3. 第三方访问公司的 C3、C4 级数据，必须签订保密合同，同时由信息安全部数据安全小组审阅数据安全保护措施及脱敏情况后方可以交互。
4. 共享给第三方的数据提供给第三方后，申请过程中接触到数据的人员应及时从其办公电脑中永久删除，最长不得超过30天。
   * 1. 数据的外部使用具体申请审批流程如图4所示：



图 4 数据外部使用申请审批流程图

* + 1. 申请审批流程详细描述见下表7：

|  |  |  |
| --- | --- | --- |
| **步骤** | **任务描述** | **负责人** |
| 1 | 1. 申请人应当基于业务需求提出数据提取申请。申请形式可以通过邮件审批，抄送给数据安全管理小组邮箱。数据接口人保留数据申请邮件记录，以便后续复核； 2. 申请时应说明的信息包括：申请人、申请人所在部门、申请人的岗位信息、申请字段、原因、数据预估量、使用期限、获取方式等，申请原因需详细描述，细化到项目或具体任务。 | 申请人 |
| 2 | 申请人所在部门直接领导开始逐级审批，需对申请的必要性、合理性进行审批，如审批通过，则进入步骤3 | 申请人逐级领导 |
| 3 | 本部门一级数据接口人根据收到的数据提取申请，应首先判断申请的合理性，如不合理，则驳回申请；如合理，则需要继续判断申请是否涉及跨部门数据访问或提取。如涉及跨部门的情况，则进入步骤4；如不涉及，则直接进入步骤5 | 本部门一级数据接口人 |
| 4 | 目标部门一级数据接口人根据收到的数据提取申请，应首先判断申请的必要性、合理性，如不通过，则驳回申请；如通过，则直接进入步骤5 | 目标部门一级数据接口人 |
| 5 | 信息安全部数据安全管理小组对申请的安全性、合理性进行审批。如不通过，则驳回申请，并提出安全建议，申请人修改方案重新提交申请；如通过，则进入步骤7 | 信息安全部数据安全管理小组 |
| 7 | 技术人员根据审批结果，按要求提供技术支持，进行技术对接或提供申请人所需数据 | DBA、大数据等技术人员 |
| 8 | 数据申请人将数据提供给合作方，流程结束 | 申请人 |

表 7数据外部使用申请审批流程

* + 1. 例外情形
    2. 纯粹因合理地履行公司职责而使用或披露公司C2 及以上密级数据的不在此限。
    3. 因适用法律或具有法律效力的指令的要求而使用或披露的亦不在此限，遇此情形，所使用或披露的范围应仅限于该适用法律或具有法律效力的指令所明确规定的内容，且员工应在使用或披露之前经过数据责任主体、法务部、风控部、信息安全部等部门及数据安全委员会审批。
    4. 对于技术成本过高或短期难以实现等特殊情况，经由安全部确认后，可适当放宽要求。

# 数据安全事件处理流程

* + 1. 数据安全事件主要是指由于人为原因、软硬件缺陷或故障、自然灾害等情况，导致网络或信息系统中的数据遭受破坏，以至于对个人、法人和其它组织、社会秩序和公共利益造成相应影响的安全事件。
    2. 根据数据安全事件发生的原因、表现形式等，将数据安全事件划分为数据篡改事件、数据假冒事件、数据泄漏事件、数据窃取事件、数据丢失事件、其它数据破坏事件等。

1. 数据篡改事件： 是指未经授权将信息系统中的数据更换为攻击者所提供的数据而导致的数据安全事件，例如系统数据在没有获得授权的情况下被改变。
2. 数据假冒事件：是指通过假冒他人收发数据而导致的数据安全事件，例如网络钓鱼事件。
3. 数据泄露事件：是指因误操作、软硬件缺陷等因素导致信息系统中的敏感、个人隐私等数据暴露给未经授权者而导致的数据安全事件。例如：
4. 数据库中未加密数据，被黑客利用数据库漏洞，实现数据库非授权访问，非法获得相关数据，导致数据泄露的安全事件。
5. 公司员工因恶意泄露公司数据，导致公司数据泄露的安全事件，如非法数据买卖。
6. 数据窃取事件：是指未经授权而利用可能的技术手段恶意主动获取信息系统中数据而导致的数据安全事件。例如：
7. 网络明文传输数据，被黑客通过相关工具拦截获取的安全事件。
8. 黑客通过传播病毒邮件，员工不小心点击邮件中所带的附件或者邮件中的链接地址，病毒自动运行感染计算机，以盗取用户的用户名密码信息等。
9. 数据丢失事件：是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的数据删除、丢失而导致的数据安全事件。例如：
10. 硬盘故障或损坏，导致数据丢失的安全事件。
11. 员工误操作，员工在操作电脑时，不小心误删重要数据，导致数据丢失。
12. 其它数据破坏事件：是指不能被包含在以上5个类别之中的数据破坏事件。
    * 1. 数据安全事件分级主要考虑以下因素：
13. 信息密级：衡量因数据安全事件中所涉及数据的重要程度的要素。
14. 声誉影响：衡量因数据安全事件对公司品牌所造成的负面影响范围和程度的因素。
15. 业务影响：衡量因数据安全事件对公司或事发部门正常业务开展所造成的影响程度和损害的要素。
16. 资产损失：衡量因恢复系统正常运行和消除数据安全事件负面影响所需付出资金代价的要素。
    * 1. 根据数据安全事件的分级考虑因素，将数据安全事件划分为特别重大事件、重大事件、较大事件和一般事件。具体判定标准如下：
      2. 特别重大事件（I级）

特别重大安全事件是指能够导致特别严重影响或破坏的数据安全事件，包含以下情况：

1. 数据泄露的数量特大，例如：
2. 个人信息泄露五万条以上。
3. 个人敏感信息泄露五千条以上。
4. 产生特别重大的影响或损失，即数据安全事件已扩散至全国且对公司具有广泛性的影响，严重威胁到客户资金及核心数据安全，以及严重扰乱社会秩序，并对公司的品牌、声誉、财产、形象造成严重损害，且在一定时期和阶段难以弥补或无法弥补损害。

举例：

1. C3、C4级别数据被泄露导致大范围社会传播事件，严重影响公司声誉。
2. 对外发布公司内部的C3级数据、大范围传播损害公司形象利益的言论事件，直接影响公司投资者关系或者公司股票价格等事件。
   * 1. 重大事件（II级）

重大事件是指能够严重影响或破坏的数据安全事件，包含以下情况：

1. 数据泄露的数量重大。例如：
2. 个人信息泄露五千条以上。
3. 个人敏感信息泄露五百条以上。
4. 产生重大的影响或损失，即数据安全事件已扩散至公司外部，但只限于部分行业或区域，明显威胁到客户资金及核心数据安全，对社会秩序造成显著影响，并对公司的品牌、声誉、财产、形象造成重大影响，且在一定时期和阶段弥补损害需要耗费较大资源。

举例：

1. C3、C4级别数据遭受非法访问或传播事件。
2. 未经授权对外发布公司内部的C3级别数据、大范围传播损害公司形象利益的言论事件。
   * 1. 较大事件（III级）

较大事件是指能够导致较严重影响或破坏的数据安全事件，包含以下情况：

1. 数据泄露的数据较大。
2. 产生较大的影响或损失，即数据安全事件已扩散至公司外部，但是仍处于公司内部可控、可处理的范围，对社会秩序和公司品牌、声誉、财产、形象造成一定的影响，且对公司造成一定的轻微经济损失或无经济损失。
3. 个人信息泄露五千条以下。
4. 个人敏感信息泄露五百条以下。

举例：

1. 公司信息系统、网站、部门范围内的网络通信或者应用系统受到影响，并关系到业务正常运行的事件和应用系统的用户账户被非法使用，遭受非法访问和泄露、传播损害公司形象利益的言论等事件，但是这些事件仅出现社会舆论小范围报告，没有给公司带来实际的损失和影响的事件。
   * 1. 一般事件（IV级）

一般事件是指不满足以上条件的数据安全事件，包含以下情况：

1. 数据泄露数量小于以上事件的数量，可以在内部处理的可控数量。
2. 产生一般的影响，即数据安全事件影响范围局限于公司内部，未对社会秩序和公司声誉造成任何影响，但存在客户资金及敏感信息相关安全风险的可能性。

举例：

1. 公司内小范围出现的网络延时或故障，信息系统功能缺陷或短暂不可用，导致个人用户或业务受影响等技术层面的事件，或部分员工无意识的违反数据安全管理制度等管理层面的事件，但是这些事件未给公司带来实际的损失和影响的事件。
   * 1. 数据安全事件定级基本原则
2. 定级应依据就高不就低原则。
3. 当处理某一数据安全事件时，如果在处理的过程中出现事件泛化和蔓延，事件等级应直接提高一级，直至重大事件为止。
   * 1. 数据安全事件评估
4. 数据安全管理员应根据数据安全发展事态或弱点导致的业务损失、社会影响以及被影响的业务重要程度等，判定安全事态的等级。
5. 经评估确认的数据安全事件，数据安全管理员应第一时间启动应急处理流程，相关团队成员必须积极配合响应。
6. 经评估确认，非数据安全事件的常规安全问题，由各相关团队自行负责跟进处理，并及时向数据安全管理小组和各部门数据接口人报告处置情况。
   * 1. 数据安全事件应急响应
7. 数据安全事件发生时，应立即启动应急处理流程。
8. 数据安全事件主要通过内部发现或者外部公开通报两种获取方式。
9. 同时，数据安全管理员应通过邮件或其他公司内部通讯工具等，及时并同时进行逐级上报，并且根据数据安全事件的等级，逐级上报相关人员，具体如下：
10. 一般事件：上报数据管理员所属部门领导、信息安全部数据安全管理小组成员，部门内部直接解决完成，同时，做好相关事件记录和事件处理报告。
11. 较大事件：数据管理员所属部门领导、信息安全部数据安全管理小组成员、各一级部门数据接口人，公司内部完全有能力解决，事件属于可控范围。并且做好相关事件记录和事件处理报告。另外，还应将事件相关情况以用户可接受到的方式（如短信、电话、邮件、推送通知、“弹窗”提示等）方式告知受影响的用户，
12. 重大事件：上报数据管理员所属部门领导、信息安全部数据安全管理小组成员、各一级部门数据接口人及各一级部门负责人，抄送CTO，交由公司内部相关部门直接处理。并且由于事件影响范围重大，须在事件处理完成后，由公司统一以公开、合规、正当的发布方式向受影响的用户通报事件相关处理情况。
13. 特别重大事件：上报至CTO，由数据安全委员会及时召开会议，集中讨论、制定和决策数据安全应急处置方案，并且须在事件处理完成后，应由数据安全委员会及时将事件相关处理情况上报至相关执法机关或有关监管部门（如网安等），以及由公司统一以公开、合规、正当的发布方式向受影响的用户通报相关事件处理情况。
14. 数据安全事件处置过程中，应严格遵循公司数据安全管理相关要求，处置方案应通过充分验证、测试以及评审，防范风险泛化和蔓延。
15. 数据管理员应对数据安全处置过程中的各阶段操作做好《数据安全事件记录》的详实记录，并事后整理《数据安全事件处理报告》，其中，事件记录内容应包含事件主题、发生原因、时间、地点、涉及的数据信息与数量（包含但不限于个人信息等）、影响性、处理方法与步骤、相关参与人员以及处理结果、是否已联系相关执法机关或有关部门等。
16. 数据安全管理小组应持续监督数据安全事件处置进度，及时发现可能存在的问题，并协调资源跟进处理。
17. 数据安全管理小组应根据需要及时向外部有关机关或相关监管机构、数据所有者做好汇报。
18. 针对个人信息安全事件，数据安全管理人员应及时将事件相关情况（如给用户的合法权益带来的危害等）以邮件、信函、电话、网站、推送通知、“弹窗”提示等用户可接收到的方式，告知受影响的用户，并对其进行安抚和沟通。难以逐一告知受影响的用户时，应采取有效、合理的方式发布与公众有关的警示信息。其告知内容包括但不限于以下内容：
19. 安全事件的内容和影响。
20. 已采取或将要采取的处置措施。
21. 针对用户自主防范和降低风险的建议。
22. 针对用户提供的补救措施。
23. 公司个人信息保护负责人和公司数据安全小组的联系方式（如邮箱）。
24. 数据安全事件处置情况的对外披露原则（如对数据主体，或外部监管机构等）应遵循本制度相关要求。
    * 1. 数据安全事态监测
25. 公司应通过培训、宣贯、引导、奖励等多种方式，合理、合规、有效地收集公司数据安全事件。
26. 数据安全事件应遵循“谁主管、谁负责，谁使用、谁负责”的原则，对各类数据安全事件和可能引发数据安全事件的有关信息进行收集、评估和持续监测，建立相应数据安全监测预警机制，通过远程监测等方式，收集、识别公司数据安全事件。
27. 公司应建立舆情监测和威胁情报机制，并设立专职团队，通过爬虫抓取、流量监测、舆情监控、外部合作等多种方式，合理、合规、有效地收集公司数据安全事件。
28. 公司应建立数据安全监控和异常分析机制，并设立专职团队，通过基线、日志、行为、流量等多种方式收集数据安全异常信息，有效地收集识别公司数据安全事件。
29. 公司应建立安全事件和弱点的统一上报机制，集中管理，并通过邮件、短信、其它流程平台以及公司其它内部通讯工具等，实现安全事件的有效沟通、评估、响应和跟踪。
    * 1. 数据安全事件总结复盘
30. 数据安全事件响应结束后，数据安全管理小组应组织相关人员进行事件总结和复盘，回顾整个事件或故障的处理过程，将事件经验教训沉淀形成知识库，避免出现重复的安全问题。
31. 数据安全事件响应结束后，数据管理员应及时整理《数据安全事件记录》、《数据安全事件处理报告》，并由各部门数据接口人和数据安全管理小组成员进行审核、备案，使得公司安全事件记录可追溯。
32. 数据安全管理小组应每年牵头组织各部门级主管，回顾公司整体数据安全事件，评估安全防御体系，分析造成事件或问题的根本原因，是否存在可优化的防御机制或响应流程，提升公司整体数据安全事件响应能力。
    * 1. 数据安全事件监督与管理
33. 数据安全管理小组应定期（至少每年一次）提取有代表性的数据安全事件，分析造成信息 的原因，组织公司相关人员进行数据安全事件培训和宣贯，提高安全技能和意识培训。
34. 根据相关法律法规变化情况，以及事件处置情况，及时更新、调整数据安全事件应急预案（包含但不限于个人信息安全事件应急预案、数据备份恢复演练），确保每年至少进行一次相关应急预案修订与评审，确保应急预案的有效性与合理性。
35. 每年应至少组织一次相关应急预案的演练，做好相关应急演练计划、演练记录以及应急演练报告，提高应急实战能力。并且演练结束后，根据应急演练结果，及时完善、更新应急预案内容。
36. 针对公司数据安全事件处理流程的有效性、职责的明确性、响应的及时性、资源的充分性等，数据安全管理小组应定期（每年至少一次）进行检查审计，以不断改进数据安全事件处理流程。
37. 数据安全管理小组应定期或不定期对应急预案、演练情况进行检查，对为有效落实预案各项规定进行通报批评，督促限期改正。

# 日常数据安全防护建议

* + 1. 安全使用电子邮件建议

1. 收发公司业务数据时，必须使用公司内部邮箱或内部通讯工具。
2. 发送敏感内容时，可将敏感内容加密压缩，通过附件发送，并通过其他方式告知接收方密码。
3. 发送前应再次检查收件人地址、内容、附件是否正确无误。
4. 定期删除敏感邮件。
   * 1. 安全使用终端设备建议
5. 电脑丢失后及时跟IT部门报告。
6. 离开座位时，应设置电脑为退出状态或锁屏状态。
7. 仅从官方应用商店下载安装应用。
8. 及时安装应用更新。
9. 手机损坏或丢失后，应首先向IT部门或信息安全部门报告。
   * 1. 安全使用移动存储介质建议
10. 尽量减少U盘使用。
11. 每次使用移动介质（移动硬盘或U盘）前应对U盘进行病毒扫描。
12. 移动介质（移动硬盘或U盘）内临时存储的公司敏感数据应及时清除。
13. 移动介质（移动硬盘或U盘）用完及时拔掉，不使用时保存在安全的地方，如带锁的柜子中。
    * 1. 密码安全
14. 按照《广东乐育尚学科技有限公司信息系统账号及权限管理规范》中的密码设置规则要求，进行密码设置。
    * 1. 办公环境中的信息安全
15. 应主动防止陌生人尾随进入办公区域。
16. 办公区域内遇到可疑人员应及时向行政部门与前台报告。
17. 应将复印或打印的资料及时取走。
18. 离开座位时，应将贵重物品、含有敏感信息的资料锁入柜中，并妥善保管钥匙。
19. 处理纸质上含有公司C3及以上级别的数据时，请使用碎纸机或交至公司统一进行回收。
20. 会议结束后，请及时清除会议室白板及其它类似设备上的信息。

# 咨询与疑问

* + 1. 如果员工自身对本制度提到的事项产生疑问， 或在执行落实过程遇到各类问题，可通过公司数据安全管理小组邮箱咨询。

# 违规处罚措施

* + 1. 公司禁止违反本制度的行为，鼓励员工举报各类泄漏 C2、C3、C4 级数据的行为。
    2. 公司将严厉处罚违反本制度而导致泄漏数据的行为。造成公司数据泄露或存在泄露隐患的，视情节轻重，予以违规者和其直接管理者相应处罚。
    3. 针对情节特别严重的，上报公安机关予以追究刑事责任。
    4. 处罚原则及处罚措施同时参考《广东乐育尚学科技有限公司违规管理制度》

**附件一 个人信息**

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。个人信息举例参考表A.1。

表A.1 个人信息举例

|  |  |
| --- | --- |
| 个人基本资料 | 个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等 |
| 个人身份信息 | 身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等 |
| 个人生物识别信息 | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| 网络身份标识信息 | 个人信息主体账号、IP 地址、个人数字证书、微信账户、支付宝账户、微博账户、淘宝账户等 |
| 个人健康生理信息 | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、  护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、  现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等。 |
| 个人教育工作信息 | 个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等。 |
| 个人财产信息 | 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、  信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑  换码等虚拟财产信息。 |
| 个人通信信息 | 通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等。 |
| 联系人信息 | 通讯录、好友列表、群列表、电子邮件地址列表等 |
| 个人上网记录 | 指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等 |
| 个人常用设备信息 | 指包括硬件SN序列号、设备MAC地址、软件列表、唯一设备识别码（如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM卡IMSI信息等）等在内的描述个人常用设备基本情况的信息 |
| 个人位置信息 | 包括行踪轨迹、精准定位信息、住宿信息、经纬度等 |
| 其他信息 | 婚史、宗教信仰、性取向、未公开的违法犯罪记录、用户画像或特征标签、家庭成员信息（包含关系码、成员姓名、出生年月、民族码、国籍/地区码、健康状况码、成员工作单位、从业码、专业技术职务码、职务级别码十个个人信息，以及电话、电子信箱两个个人敏感信息）等 |

参考来源：《GBT 35273-2020信息安全技术 个人信息安全规范》。

**附件二 个人敏感信息**

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。明确未满14周岁（含）未成年人的个人信息和涉及自然人隐私的信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。个人敏感信息举例参考表B.1。

表B.1 个人敏感信息举例

|  |  |
| --- | --- |
| 个人财产信息 | 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息 |
| 个人健康生理信息 | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息等 |
| 个人生物识别信息 | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| 个人身份信息 | 身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等 |
| 网络身份标识信息 | 个人信息主体账号、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等的组合。 |
| 其他信息 | 个人电话号码、性取向、婚史、宗教信仰、种族、民族、政治观点、未公开的违法犯罪记录、通信记录和内容、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、住址、精准定位信息、考试成绩和名次等学业信息等。 |

参考来源：《GBT 35273-2020信息安全技术 个人信息安全规范》、《未成年人学校保护规定》。

**附件三 法人和其它组织基础信息**

法人和其他组织基础信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定法人和其他组织身份或者反映特定法人和其他组织经营情况的各种信息，如机构名称、机构住所、法定代表人姓名、法定代表人身份证件号码、纳税人识别号等。

法人和其他组织基础信息的示例，见表C.1。

表C.1 法人和其他组织基础信息举例

|  |  |
| --- | --- |
| 基本信息 | 组织机构代码、机构名称、机构类型、机构住所、邮政编码、电话号码、法人代表人姓名、成立日期、注册或登记号、行政区划等 |
| 组织机构代码信息 | 组织机构代码证颁证日期、组织机构代码证废置日期、组织机构代码证变更事项、组织机构代码证变更内容、组织机构代码证变更日期等 |
| 注册或登记信息 | 注册或登记机构名称、经济行业代码、经营或业务范围、年检年度、年检结果、注销或撤销日期、法定代表人身份证件类型、法定代表人身份证件号码、注册或开办资金金额、注册或开办资金币种、分支机构组织机构代码、分支机构名称、分支机构注册或登记号、分支机构住所、法人证书变更事项、法人证书变更内容、法人证书变更日期、营业执照吊销日期、营业执照吊销原因等。 |
| 税务信息 | 纳税人识别号、税务登记机关名称、税务登记日期、注销税务登记日期等。 |

**附件四 影响程度分类表**

影响程度，是一个定性的说明方式。在事件没有实际发生并产生影响的情况下，无法以具体量化指标或者参数来衡量。即便在实践中，由各类事件、事故引发的直接和间接后果也难以简单衡量或者量化。

影响程度的判定，应综合考虑数据类型特征。数据类型根据业务条线划分并确定，不同业务对应不同的数据类型，体现不同的业务特点，因此，结合数据类型分析，有利于更加准确地判断影响程度。例如：用户个人隐私安全属性遭到破坏产生的影响程度通常要高于信息披露类数据；涉及个人信息的数据安全属性（保密性）遭到破坏产生的影响程度通常要高于已公开披露信息，个人隐私数据类型的数据安全属性遭到破坏产生的影响程度通常要高于非实时的行情信息类数据等。为便于确定“影响程度”，如下表提供影响程度的参考说明，供判定影响程度时参考下表8。

|  |  |
| --- | --- |
| **影响程度** | **参考说明** |
| 严重 | 1、可能导致全部业务无法开展，造成重大经济损失。  2、可能引发或导致重大或特别重大事件。  3、可能引发公众广泛诉讼或集体诉讼，甚至引发群体性事件。  4、可能导致监管部门严重处罚（包括取消经营资格、长期暂停相关业务等）的情况。 |
| 中等 | 1、可能导致部分业务无法开展，造成较大经济损失。  2、可能引发或导致较大事件。  3、可能引发一定数量客户对本机构诉讼。  4、可能导致监管部门较严重处罚（包括一段时间内暂停经营资格或业务等）的情况。 |
| 轻微 | 1、可能导致个别业务短时间无法开展，造成轻微的经济损失。  2、可能引发或导致一般事件。  3、可能导致至监管部门轻微处罚（包括罚款、公开批评等）的情况。  4、可能对本机构声誉造成一定程度损害。 |
| 无 | 1、不造成任何影响。 |

表 8影响程度分类表

**相关参考文献**

《中华人民共和国民法典》（第六章 隐私权和个人信息保护）

《中华人民共和国数据安全法》

《中华人民共和国网络安全法》

《中华人民共和国个人信息保护法》

《中华人民共和国未成年人保护法》

《未成年人学校保护规定》

《关键信息基础设施安全保护条例》

《GBT22239-2019信息安全技术网络安全等级保护基本要求》

《信息安全技术 网络安全等级保护大数据基本要求》

《GB/T 35273-2020 信息安全技术 个人信息安全规范》

《上海教育数据管理办法（试行）》

《上海教育数据安全管理规范》

《上海教育数据分级分类规范》

《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》

《GB/T 36073-2018 数据管理能力成熟度评估模型》

《GB/T 37973-2019 信息安全技术 大数据安全管理指南》

《GB/T 38667-2020信息技术 大数据 数据分类指南》

《GB/T 37964-2019信息安全技术 个人信息去标识化指南》

《GB/T 39725-2020 信息安全技术 个人信息安全影响评估指南》

《科学数据管理办法》

《国家网络安全事件应急预案》

《移动互联网应用程序个人信息保护管理暂行规定（征求意见）》

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》