数 据 分 级 与 等 级 保 护

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 角 色 | 姓 名 | 版 本 | 时 间 | 操 作 |
| 编写人 | 安全团队 | V1.0 | 2021/09/01 | 创 建 |
| 签发人 | CTO | V1.0 | 2021/10/01 | 签 发 |

**目** **录**

[1 数据保护概述 ...................................................4](#_bookmark1)

[1.1 数据保护范围 ................................................4](#_bookmark2)

[1.2 商业影响范围 ................................................4](#_bookmark3)

[2 数据分级标准 ...................................................5](#_bookmark4)

[3 数据安全技术 ...................................................6](#_bookmark5)

[3.1 数据保密技术 ................................................6](#_bookmark6)

[3.1.1 数据加密 ................................................6](#_bookmark7)

[3.1.2 数据变换 ................................................7](#_bookmark8)

[3.1.3 数据脱敏 ................................................7](#_bookmark9)

[3.1.4 数据防泄漏...............................................7](#_bookmark10)

[3.2 数据保密实践 ................................................8](#_bookmark11)

[3.2.1 基本要求 ................................................8](#_bookmark12)

[3.2.2 数据传输 ................................................8](#_bookmark13)

[3.2.3 数据存储 ................................................8](#_bookmark14)

[3.2.4 数据使用 ................................................9](#_bookmark15)

[3.2.5 数据销毁 ................................................9](#_bookmark16)

[3.3 数据权限管理 ................................................9](#_bookmark17)

[3.4 数据 ACL 实践 ..............................................10](#_bookmark18)

[3.4.1 核心数据实践............................................10](#_bookmark19)

[3.4.2 信息系统实践............................................10](#_bookmark20)

[3.4.3 其它数据实践............................................11](#_bookmark21)

[3.5 数据运营实践 ...............................................11](#_bookmark22)

[3.5.1 基础设施安全............................................11](#_bookmark23)

[3.5.2 资源安全措施............................................12](#_bookmark24)

[3.5.3 运营监控审计............................................12](#_bookmark25)

[4 数据安全管理 ..................................................12](#_bookmark26)

[4.1 数据管理分工 ...............................................12](#_bookmark27)

[4.2 数据备份容灾 ...............................................13](#_bookmark28)

[4.3 数据恢复测试 ...............................................14](#_bookmark29)

[5 维护更新计划 ..................................................14](#_bookmark30)

[6 编写人 .......................................................14](#_bookmark31)

[7 生效日期......................................................14](#_bookmark32)

[8 签发人 .......................................................14](#_bookmark33)

[附件一：信息系统-角色-权限控制矩阵表 ..............................15](#_bookmark34)

[附件二：信息系统账户权限申请表....................................16](#_bookmark35)

1 数据保护概述

为保障公司信息系统数据管理工作， 我们通过评估数据泄露所带来的商业风险来对数 据资产进行分级，指导我们建立数据分级和保护措施， 确保所有用户对公司系统资源的访 问是经过授权和认证的，保障各操作、应用以及数据库系统的安全，保证各类数据正常访 问，防止对信息系统数据的非法使用或滥用，保证信息系统安全、稳定、高效运行。

本规定参考 《中华人民共和国网络安全法》 和 《数据安全法》 要求， 依据某某科技公司的信息安全现状进行设 计、制定和编写 ，适用于公司各事业部。本规定体现了公司管理者对数据保护的要求 ，它 得到了公司管理者的充分认可并授权自签发之日起在公司内部执行。

1.1 数据保护范围

数据分级标准覆盖某某科技公司的各业务部门数据 ，它覆盖业务系统、公司运营中信息 采集、 处理、 存储、 传输、 分发、 备份、 恢复、 清理和销毁 ，它不包括员工个人数据—— 跟公司商业无关信息。 它不包括数据可用性评估 ，相关需求可以参考业务连续性计划。

1.2 商业影响范围

评估在数据保密性或完整性被破坏的情况下 ，可能给公司带来的潜在商业影响包括：

■至关重要的公司业务损失

■负面的财务影响 （财物损失、错失商机、数据价值）

■损害公司的声誉

■违反相关法律、 法规或公司法的要求

2 数据分级标准

通过理解数据安全需求和监管需求，对数据进行分级， 然后定义数据的安全策略、标 准、控制和措施，管理用户、密码、用户组成员，管理数据访问视图和权限，监控用户身 份认证和访问行为，审计数据安全。

|  |  |  |
| --- | --- | --- |
| **级别设置** | **分级要求** | **分级实例** |
| 核心数据-高 | 丢失会对业务造成严重影 响，会导致重大经济损失， 严重导致业务无法进行。 | 用户账号费用数据、用户消费凭据、用户订单、数据库数据，页面数据、程序源码、 财务数据、员工信息、重要日志数据 |
| 重要数据-中 | 丢失会对业务造成部分影 响，可以保持业务正常进 行，不对学生学习造成严重 影响，对产品有质损。 | 重要服务器日志、统计数据、页面访问 日志、系统访问日志、登录日志、流量 数据、服务器上报数据、监控数据、安 装程序、脚本、系统或程序配置文件等 |
| 普通数据-低 | 仅用作日常归档或测试，部 分数据丢失对业务影响小。 | 测试数据、开发文件、测试机文件、测 试用例等 |

表 1. 数据分级标准

基于商业价值、敏感性、防范范围以及信息扩散后影响对核心资产进行识别，创建时

对其进行标识，事前防御或审批，事中监控，事后审计，文档集中存储，定期降密。

3 数据安全技术

3.1 数据保密技术

3.1.1 数据加密

数据加密指发送发对信息经过加密密钥转换后变成无意义的密文 ，而接收方需将密文 经过解密密钥还原得到明文。 在数据的传输与存储中 ，公司的核心数据要进行加密 ，以免 中间人劫持或入侵获取 ，同时避免数据被开发人员、 管理人员直接获取。

■ 加密对象 ：用户手机号、 身份证号、 银行卡号、 住址、 HTTPS 证书、 APP 等。

■ 加密技术 ：对称加密算法 AES、 DES、 3DES 等用于用户信息存储 ，非对称加密算 法 ECC、 RSA 等用于 HTTPS 证书和 APP 完整性校验。

■ 加密环境： 在云计算环境中 ，但数据进入到 IAAS、 PAAS、 SAAS 前需完成选择性 加密 ，可以使用应用层、 ODBC/JDBC 层、数据库层、 文件存储层或者磁盘层的加密方法。

■ 密钥管理 ：在 IDC 内所有的密钥管理功能和工具都是由内部 IT 运营团队来配置和维护的，而在云计算环境中可采用密钥共享模式或是完全由服务商管理和维护。 IaaS 云计算的私钥应由云计算消费者在内部的密钥管理平台维护 ，而对于 PaaS 和SaaS 云计算服务模式，大部分密钥管理功能都是由云计算服务商内部管理的， 其公共密钥部署中密钥管理和安全都是共享的-控制权都在于消费者本身 ，其他所有密钥管理的责任则主要是由供应商承担的。 对于混合云计算密钥管理一般共享，而私有云计算是在内部网络环境中配备密钥管理工具和程序。

3.1.2 数据变换

数据在进行后端存储时 ，为了避免关键数据被内部员工泄露或者是黑客通过漏洞入侵 数据库导致被拖库所引发的数据泄露 ，需要对敏感数据在入库前进行不可逆的变换 ，通过 存储变换后的数据（无法还原信息） 以减低数据泄露可能带来的风险。

■ 变换对象 ：用户密码等。

■ 变换技术 ：数据加 Salt 后经过 SHA-1、 SHA-256 变换等生成信息的摘要。

3.1.3 数据脱敏

数据保护的原则是通过数据和人员分级实现最小化授权管理，但是在复杂的商业环 境中该原则难以满足 ，需要对敏感信息应用脱敏规则进行数据变形 ，使得数据本身安全等 级降低 ，且保留其原始数据格式和属性， 从而可以在开发、测试和云计算等不同风险环境 下安全地使用脱敏后的真实数据， 实现敏感数据的可靠保护。

■ 脱敏对象 ：用户名、手机号码、固定电话、邮件地址、住址、 身份证号等用户信息， 电话、唯一标识、公司合同、交易金额、投资项目等商业信息。

■ 脱敏技术 ：变换（替换数据字段、 数据重新排序、 数据部分截断）、掩码（数据 部分模糊长度不变）、去锐化（数据舍弃精度维持其分布） 。 原则是保留数据真实的含 义、防止被不法分子利用。

3.1.4 数据防泄漏

数据防泄漏的目标是：杜绝核心数据通过员工、客户泄漏，经过网络、打印泄漏，因

为内部设备丢失、非法设备接入等泄漏 ，保护公司核心数据的安全。

■ 基本防御策略 ：数据加密存储 ，管理员根据用户角色在线下发相应的密级，强制 低密级终端用户不能访问高密级文档 ，加解密对终端用户无感知， 系统有自动备份功能。

■ 基本转发策略 ：转发的数据需要经过审批授权，且管理员可以对其施加限制：阅 读次数、 阅读时间、 打印、截屏、编辑、 另存为、对象拖拽、 删除、自毁等， 常见应用可 以通过白名单机制自动实现数据的加解密， 授权用户凭密钥才能访问转发的数据。

■ 基本监控能力 ：具备基本的操作监控能力，对打印事件按照策略进行动作如禁止 打印或者打印加水印等，对 USB、光驱、软驱、红外、蓝牙等介质的访问进行管理-认证 接入、禁止访问、只读访问、允许访问等，对数据资产终端有一定的管理能力。

■ 审计报警能力 ：具备文件加解密、审批解密、离线申请、文件操作、密级转换、 文件转发、 USB 设备外发、文件备份等日志审计能力 ，日志内容至少包括：时间、终端名 称、所属级别、操作事件、事件描述等 ，且能根据日志审计及时发现员工的违规行为。

3.2 数据保密实践

3.2.1 基本要求

■ 数据控制能力：无论数据服务形式如何，业务线需对数据拥有知情权和控制权。

■ 数据托管要求 ：服务商有责任和义务保障用户数据的私密性、完整性和可用性。

3.2.2 数据传输

■ 核心数据传输 ：用SSL/TLS（建议用 256 位及以上密钥 ）来实现端到端加密。

3.2.3 数据存储

■ 基本存储位置 ：业务线需明确数据存储、 迁移的位置 ，不得将数据存储在国外。

■ 核心数据加密 ：数据在存储过程中必须加密， 根据业务选择不同加密层级。

■ 核心数据密钥 ：使用国际通用的 PKI 体系来生成、存储、使用、管理密钥。

■ 数据备份容灾：根据《信息安全技术信息系统灾难恢复规范》对数据按照备份标准进行备份。

3.2.4 数据使用

■ 数据访问控制 ：根据数据分级细化数据访问控制表， 核心数据实现最小化授权。

■ 核心数据保护：核心数据展示中涉及敏感信息或二次使用的，需要有脱敏措施。

3.2.5 数据销毁

■ 数据销毁要求 ：检查需销毁数据的全部备份位置 ，确保全部数据含备份无遗漏。

■ IDC 数据销毁 ：服务器借出、 业务变更等至少需要对硬盘进行一次格式化操作。

■ IDC 硬盘下线： 建议对硬盘进行消磁并物理折弯处理 ，确保数据无法恢复。

■ 云端数据销毁：数据删除后对数据进行二次检查，确保没有数据残留在云端。

3.3 数据权限管理

有效的身份认证与访问控制是确保客户数据不被非授权访问的关键 ，数据访问应该 按照权限设置、 权限校验来进行控制。 数据权限的管理与数据、 用户、 角色、组织相关。 核心数据权限管理包括三大模块 ：基础同步功能、权限申请配置、 权限审计功能。

■基础同步功能 ：数据归属和管理信息、公司组织架构、员工角色信息同步。

■权限申请配置 ：数据和账户权限的申请、 角色和账户权限的配置。

■ 数据权限审计 ：数据权限审计、 角色授予审计、 账户权限审计。

3.4 数据 ACL 实践

3.4.1 核心数据实践

■ 关键岗位管理 ：上岗前需要调查背景 ，特殊岗位需要认证上岗 ；在岗的要定期进 行培训 ，定期进行组织信息安全自检 ；离岗前划定解密期、离任审计、同业竞争协议等。

■ 用户身份标识 ：用户身份标识须唯一，需要能映射到角色信息和组织内的身份。

■ 用户登录认证 ：使用 AD、 LDAP、 Kerberos 等身份验证机制进行校验，用户的 密钥为强口令或证书、 多因素认证等形式，验证功能有基本的防撞库能力如图灵测试。

■ 资源访问矩阵 ：用户的权限由相关系统负责人进行设定， 或者由用户申请经过审 批流程后由系统负责人确认并分配该用户的权限。 资源访问矩阵可根据类似 RBAC 授权 ， 使用统一的访问控制精确地允许或拒绝某个用户对特定资源执行的某操作。

■ 用户鉴权方式 ：访问控制采用集中式权限管理、统一的鉴权审计机制。

■ 审计日志格式 ：至少包含访问时间、访问地址、使用的用户名、操作对象、 操作 类型和操作细节等信息。

■ 审计内容要求：至少包含账户创建、变更、销毁、 登录、 访问和登出等行为。

3.4.2 信息系统实践

■ 系统开发设计 ：核心系统开发项目的分析阶段就识别具体数据安全要求 ，建立数 据到流程和数据到角色关系矩阵， 实现数据安全角色、参数和权限的定义。

■ 系统安全实现 ：核心系统具备完善的登录验证和访问控制能力， 上线前解决登录 验证、会话管理、越权访问和注入等全部中高危安全漏洞，部署数据库监控防护组件。

■ 系统代码管理 ：核心系统代码使用数据仓库管理并最小化授权，根据组织架构信 息同步更新用户权限，用户操作记录可审计。

■ 系统数据访问 ：核心数据有行权限（基于数据值将数据表中的数据范围进行限 制 ）、列权限（基于视图可以允许广泛地获取某些列，并对密级高的列进行访问限制 ）。

■ 系统数据保密 ：核心数据和服务器需明确标记， 建议部署终端数据防泄漏软件。

3.4.3 其它数据实践

■ 个人终端要求 ：涉及核心数据的个人终端建议部署数据防泄漏软件。

■ 归档信息要求 ：文档须标识密级，核心文档须登记存放的位置，对其访问必须通 过 OA 向相关部门申请， 审批后才能进行操作，相关审批和操作记录须留存 1 年及以上。

3.5 数据运营实践

3.5.1 基础设施安全

■ 网络边界 ACL ：使用网络防火墙或安全组策略来构建数据存储的安全区域 ，实现 对基础网络的访问控制。

■ 远程登录管理 ：数据服务器位于 IDC 时 ，运维人员不在公司的通过 VPN 接入办 公网然后访问堡垒机进入生产环境进行运维管理。 数据服务器位于云计算环境时，通过跳 板机的内网对其进行运维管理。 一般不允许直接通过公网对数据服务器进行运维管理。

■ 入侵检测组件 ：通过部署主机和网络等异常检测组件或者是购买云安全服务实现 对数据的监控、 用户活动的监控以及终端的监控 ，从而获得对环境的安全感知能力。

■ 日志审计服务： 收集各类服务器、网络、应用和数据库等日志 ，及时进行审计。

3.5.2 资源安全措施

■ 网络安全隔离： 根据不同业务类型构建出的一个物理或逻辑上隔离的网络环境 ， 采取的措施有： 私有 IP 地址、划分网段和vlan、 VPC 等 ，设置安全域网络访问策略。

■ 远程访问能力：如果数据资源位于 IDC 或云主机上，数据资源必须位于私网内或 者设置访问白名单，远程管理线路需要与业务访问线路分开 ，避免流量攻击时无法维护。

■ 主机安全隔离： 根据主机上业务情况设置针对服务级别的防火墙策略 ，云计算环 境下虚拟机间必须具备包状态检查和网络过滤能力、资源访问的隔离能力。

■ 数据风险感知 ：在数据库服务器上部署数据库防火墙组件，及时感知到SQL 注 入、拖库等行为，结合基础的审计功能还可以发现撞库、无口令等行为。

3.5.3 运营监控审计

所有数据的访问、下载都需要记录行为，这是事中发现威胁，事后追查原因的关键。 通过对业务监控、运维日志、权限异常日志、来源地址异常、敏感数据访问的日志记录， 及时发现违反内部访问控制风险、账户窃取和废旧后利用、 SQL 注入、后门恶意行为等。

4 数据安全管理

4.1 数据管理分工

■ 安全工程师 ：参与规范制定 ，完善数据分级和等级保护规定 ，协同业务线落地。

■ 数据所有者 ：负责业务的管理人员，决定并负责数据的分类、级别调整，负责定 义用户访问准则， 实施必要的安全控制，落实数据备份需求，批准数据泄露活动， 处理与 其负责数据有关的安全违规行为， 对数据的保护和应用负最终责任。

■ 数据看管员 ：负责数据的保护与维护工作， 实施和维护安全访问控制、执行数据 的常规备份，定期验证数据的完整性，从备份介质还原数据，保存活动记录等安全需求。

■ 数据分析员 ：负责保证以最佳方式存储数据，从而为需要访问和应用数据的公司 与个人提供最大的便利，与数据所有者合作帮助建立数据结构符合并支持公司业务目标。

■ 审计员 ：定期进行巡查，确保采取并安全地维护了正确的控制措施，确保组织遵 循了定制的策略和适用的法律法规，目标是找出忽略的问题并帮助修复这些问题。

4.2 数据备份容灾

依据国内外标准和要求， 数据备份和容灾标准如下 ：

|  |  |  |
| --- | --- | --- |
| **级别设置** | **备份标准** | **容灾标准** |
| 核心数据-高 | 建议物理异地存储，保存三份，按照时间戳每天或每 若干小时做全量数据备份，数据库、财务数据以及其 他重要的业务数据要做主从热备份，同时按照时间戳 每天或每若干小时做全量物理隔离数据备份。 | RTO （恢复时间） <24 小时 |
| 重要数据-中 | 建议做到二份备份，按照时间戳每天或每若干小时做 全量物理隔离数据备份。 | RTO （恢复时间）  <48 小时 |
| 普通数据-低 | 业务根据实际需求评估是否需要备份。 | RTO （恢复时间）  <72 小时 |

表 2. 数据备份容灾标准

4.3 数据恢复测试

演练先事先设定一个场景——可能会面对的场景，开始演练之前应该确定特定的参数 和演练的范围，测试团队必须在测试内容与如何合理决定成功与否方面达成一致。

■ 演练周期——至少应该对重要系统进行一年一次的演习。

■ 演练类型——模拟测试， 应急响应团队集中在一起执行应急响应计划。

5 维护更新计划

■ 每年应组织安全团队、 业务部门对本规定进行评审和更新以满足安全需求。

■ 发生重大安全事故后， 应组织安全团队、 业务部门对本规定进行评审和更新以满 足安全需求。

6 编写人

安全团队。

7 生效日期

2021 年 10 月 1 日。

8 签发人

CTO 。

附件一： 信息系统-角色-权限控制矩阵表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **系统-角色-权限控制矩阵表** | | | | | |
| **角色**  **（职位）** | **用户** | | | | |
| **创建（** **Y|N** **）** | **读取（** **Y|N** **）** | **编辑（** **Y|N** **）** | **删除（** **Y|N** **）** | **记录类型** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

表 3. 信息系统-角色-权限访问控制矩阵表

附件二 ：信息系统账户权限申请表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **系统账户权限申请表** | | | | | |
| **工号** |  | **用户名** |  | **岗位** |  |
| **邮箱** |  | **手机号** |  | **IP** **地址** |  |
| **申请角色名称** ： | | | | | |
| **申请原因说明** ： | | | | | |
| **申请角色类别** ： 非关键角色  关键角色 | | | | | |
| **申请使用时间：** | | | | | |
| **特殊需求说明：** | | | | | |
| **相关附件列表：** | | | | | |
| **本部门直接领导确认** | | | | | |
| **（审批为选择关键角色时，增加风险提示和保密承诺说明）** | | | | | |
|  | | | | | |
| **主管部门领导确认** | | | | | |
| **（审批为选择关键角色时，增加风险提示和保密承诺说明）** | | | | | |
|  | | | | | |

表 4. 系统账户权限申请表