**信息安全规定**

1 / 22

**目** **录**

**1** **目标** ............................................................. [4](#_bookmark1)

**2** **定义及术语** ....................................................... [4](#_bookmark2)

2.1 数据中心 ...................................................... [4](#_bookmark3)

2.2 信息资产 ...................................................... [4](#_bookmark4)

2.3 信息安全 ...................................................... [5](#_bookmark5)

2.4 安全事件 ...................................................... [5](#_bookmark6)

**3** **适用范围** ......................................................... [5](#_bookmark7)

3.1 人员范围 ...................................................... [5](#_bookmark8)

3.2 系统范围 ...................................................... [6](#_bookmark9)

**4** **职责分工** ......................................................... [6](#_bookmark10)

**5** **规定内容** ......................................................... [6](#_bookmark11)

5.1 安全培训及责任 ................................................ [6](#_bookmark12)

5.2 信息分类与分级 ................................................ [7](#_bookmark13)

5.3 信息系统定级 .................................................. [8](#_bookmark14)

5.4 信息资产管理 .................................................. [8](#_bookmark15)

5.5 信息系统运营 ................................................. [10](#_bookmark16)

5.6 系统开发与部署 ............................................... [10](#_bookmark17)

5.7 数据安全管理 ................................................. [11](#_bookmark18)

5.8 漏洞分级管理 ................................................. [12](#_bookmark19)

5.9 安全事件管理 ................................................. [12](#_bookmark20)

5.10 网络安全管理 ................................................ [13](#_bookmark21)

5.11 信息系统访问管理 ............................................. [14](#_bookmark22)

5.12 主机系统安全管理 ............................................. [15](#_bookmark23)

5.13 办公终端安全管理 ............................................. [16](#_bookmark24)

2 / 22

**6** **违反处罚** ........................................................ [17](#_bookmark25)

6.1 违反上报 ..................................................... [17](#_bookmark26)

6.2 处罚细则 ..................................................... [17](#_bookmark27)

**7** **评审及更新** ...................................................... [18](#_bookmark28)

**附录一、《敏感服务端口开放管理规定** **1.0** **版》** ........................... [19](#_bookmark29)

3 / 22

**1** **目标**

为保障公司经营活动能够持续、稳定和安全地进行，减少由信息安全风险产生的 经济或名誉损失，满足国家法律和法规、上市公司相关规定对公司信息安全保障能力 的要求，需要确保与公司经营活动密切相关的信息系统和资产的安全，防止公司、员工和用户的保密信息被泄漏或篡改。

本规定参考 《中华人民共和国网络安全法》、《数据安全法》 和 《员工手册》 要求， 依据信息安全的现状进行设计、制定和编写，是公司对信息安全管理要求的具体体现。

**2** **定义及术语**

**2.1** **数据中心**

提供硬件设备存放空间、电力、网络接入等基础服务的物理建筑如公司租赁的 IDC 机房 （称 IDC 机房） 、 办公区机房（称 OFFICE 机房） 或者各类云计算中心。

**2.2** **信息资产**

信息是通过在数据上施加某些约定而赋予这些数据的特殊含义，它是一种对公司 具有价值的重要资产 ， 与信息相关的资产包括但不限于以下几类：

■ 电子数据： 以电子技术手段形成的包括文字 、 图形、数字等资料 ， 并以数字化 形式存储、处理、 传输的数据，如财务报表 、 组织架构 、 采购文件、商务合同等。

■ 文档资料 ：以纸质形式存在的资料，包括会议记录 、 制度规范 、 商业规划 、 商 业专利 、 产品设计 、 用户手册等。

■ 软件资产：系统软件、 应用软件、开发工具、 源代码 、 软件使用许可证等。

■ 硬件资产 ：计算和通讯服务， 其它技术设备（供电、空调设备）、机房等各种 基础网络服务等 ， 还包含员工 PC、通讯设备等办公资产。

4 / 22

**2.3** **信息安全**

信息安全的目的是保护信息系统硬件、软件及相关数据，不因偶然或恶意原因遭 到破坏 、 篡改或泄漏。 组织应该通过实施技术或管理类的安全控制措施以降低风险发 生的几率及造成的影响，保障信息系统安全持续运行 、 组织业务活动的连续性 。 它包 含以下三个基本目标 ：

■ 保密性 ：确保信息在传输 、 存储 、 使用等过程不会泄露给非授权用户或实体。

■ 完整性 ：确保信息在传输 、 存储 、 使用等过程不会被非授权用户或实体篡改。

■ 可用性 ：确保授权的用户或实体对信息和资源的正常使用不会被异常地拒绝。

**2.4** **安全事件**

由于自然 、 人为和软硬件本身缺陷或故障等原因，对信息系统造成危害产生负面 影响的事件，信息安全事件主要包括（但不限于）以下三类：

■ 攻击类事件： 指网络与信息系统因计算机病毒感染 、 非法入侵等导致业务中 断、系统宕机、网络瘫痪等情况。

■ 故障类事件： 指网络与信息系统因计算机软硬件故障、人为误操作等导致业务 中断、系统宕机、网络瘫痪等情况。

■ 灾害类事件： 指因爆炸 、 火灾 、 雷击、地震 、 台风等外力因素导致网络与信息 系统损毁 ， 造成业务中断、系统宕机、网络瘫痪等情况。

**3** **适用范围**

**3.1** **人员范围**

公司所有员工 、 合作方的相关人员 、 其它与公司信息安全管理相关的人员。

5 / 22

**3.2** **系统范围**

所有接入公司数据中心的网络， 使用基础技术支撑平台进行运营， 并对公司内部 或外部提供服务的相关信息系统。

**4** **职责分工**

■ 公司管理层 ：发起本规定的制定，界定规定的实施范围，对规定进行审批 、 签

发，并为规定执行提供资源支持。

■ 安全部门和人力资源中心 ：参与制定、编写、 修订规定 ， 检查执行情况等。

■ 安全责任人 ：监督部门员工遵守安全规定、 负责对接安全部门，对业务部门的整体安全风险负责。

■ 公司的员工 ：执行此规定，对规定提出合理化的建议。

■ 第三方人员 ：参与公司信息安全管理的相关人员执行此规定。

**5** **规定内容**

**5.1** **安全培训及责任**

■ 对于新员工，在转正期内参加《信息安全规定》 的线上学习和考 试，考试不通过不能转正。

■ 对于在职员工，每年参加一次《信息安全规定》 的线上学习和考试，考试不通过不能晋升。

■ 员工必须严格遵守与公司签署的劳动合同中保密条款的有关规定。

■ 员工必须清晰了解并履行本信息安全规定的职责 ， 有责任和义务向安全部门报告与公司相关的安全漏洞 、 事件或线索。

6 / 22

**5.2** **信息分类与分级**

**数据分类：** 依据数据来源、内容和用途、监管合规进行，如公司、业务、客户数据。

**数据分级：** 依据数据对组织的价值（事故影响） 、 内容的保密性（对第三方价值） 、 司 法管辖权制约（如网络安全法、数据安全法 等司法风险）三个要素对数据进行密级的划分。创建时将密级标签化，事前防御、事中监控、事后审计，定期重新评估。示例如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **分类** | **信息项** | **事故影响** | **对第三方价值** | **司法风险** | **分级** |
| **公司数据** | 商业合同等直接影响公司权益和利益的重要决策文件、技术资料 | 技术泄密、财务和运营数 据提前外泄引发商业风险 | 对手商业布局 、 合作方利益受损 | 违反数据安全法 | **绝密数据** |
| **公司数据** | 公司的各种规划、财务报表、统计资料、重要会议记录、公司经营情况 | 商业风险 | 对手商业布局 、 合作方利益受损 | 违反数据安全法 | **机密数据** |
| **公司数据** | 公司人事档案、合同、协议、员工工资性收入、尚未进入市场或尚未公开的各类信息 | 商业风险 | 对手商业布局 、 合作方利益受损 | 违反数据安全法 | **秘密数据** |
| **客户数据** | 用户客户的电  话号码 、 身份  证号码 、 银行  卡号等 | 商业的信誉受 损、 出现用户  流失等 | 牟取暴利 、 第  三方利用数据  挖掘用户或从  事诈骗犯罪 | 网络安全  法对 PII 相关  保护的要求 | **绝密数据** |
| **业务数据** | 架构设计 、 后  端代码等 | 核心商业竞争  力的丧失 | 价值较大 、 竞  争者分享市场 | 违反数据安全法 | **机密数据** |
| **业务数据** | 设计原型 、 前  端代码等 | 影响一般、产  品信息外泄 | 价值较大 、 竞  争者了解动向 | 违反数据安全法 | **秘密数据** |
| **公司数据** | 管理制度、人  事任免 | 影响一般 | 价值一般 | 无 | **公开数据** |
| **业务数据** | 产品介绍 、 操  作指南等 | 无影响 | 价值较低 | 违反数据安全法 | **公开数据** |

7 / 22

**5.3** **信息系统定级**

信息系统指日常办公（OA、ERP等）、业务运营运维（客服、运维监控、BI等）、产品线（具体产品）等所有公司信息系统。信息系统定级设置系统承载的信息级别、产出价值和业务依赖度三个等级属性，定级时采用其中的最高级别。

■ 承载的信息级别 ：系统传输、存储 、 处理了什么级别的信息 ， 信息泄露、篡 改、 无法访问可能导致公司在经济、 声誉 、 司法诉讼方面受到影响的程度 ， 参考信息 识别及分类规范 ， 信息级别由低到高分： L1 级 、 L2 级 、 L3 级。

■ 业务的产出价值 ：系统支撑业务产生了经济收入或其他形式直接或间接收益， 在公司经营活动中份额 、 收入贡献值。 业务价值由低到高分 ：L1 级 、 L2 级 、 L3 级。

■ 业务的依赖度 ：是否有其他业务依赖此业务正常开展 ， 此业务无法正常提供服 务将对其他业务产生影响 。 业务依赖度由低到高分 ：L1 级 、 L2 级 、 L3 级。

**5.4** **信息资产管理**

■ 域名使用管理： 域名由运维部门统一运维管理，域名注册及解析申请应由业务负责人审批，并进行记录备案。

■ 信息资产备案 ：信息资产，包括IP类、域名类、应用类、数据库类等，要进行备案记录及按密级重要性等进行分级。

■ 公网 IP 使用 ：用于系统开发 、 测试 、 存储核心和保密数据的服务器应使用私 网 IP ， 特殊情况应通过安全部门备案 、 评估风险和实施加固后再使用。

■ 公网端口使用 ：限制敏感服务和敏感端口 （见附录一） 没有设置网络访问白名 单策略就完全开放在公网， 根据敏感服务完全开放公网的潜在风险对其划分为两类 ： 禁止全开放 （不允许其完全开放公网） 和强限制开放 （不建议其完全开放公网，特殊 情况的可以向安全部门备案，由安全部门评估风险后确定是否可以在实施网络隔 离的条件下允许其开放公网） 两类 （见附录一） 执行不同的访问控制策略。

8 / 22

■ 业务系统及应用备案 ：上线和下线前由其系统管理员通过资产管理系统进行备案定级和变更 ， 系统管理员填写定级属性后确定属性级别，依 据 5.3 节定级标准来定级，安全部门可协助和纠正错误的定级结果。

■ 合作系统管理： 因项目合作需要托管于我方数据中心的合作方设备 ， 上线前业 务部门须与合作方签署正式的具有法律约束的合同协议并进行信息系统的备案定级 ， 部署于数据中心内网隔离的环境中 ， 同时实施内网白名单的访问控制策略 。 若发生安 全事件需及时通报给安全部门 ， 依据安全部门要求进行安全的应急响应。

■ 系统软件管理： 系统所需软件应该从其官方网站或可信任的第三方网站下载， 通过邮件、 QQ 、 微信等接收到的文件 ， 需要注意安全性 ：打开之前和文件的发送 方确认文件内容 ， 使用杀毒软件进行病毒和木马的查杀等 ， 防止被钓鱼攻击。

■ 项目资料管理 ：全部项目资料应托管到公司指定的公共仓库 ， 个人电脑中的资 料在结项或离岗时应及时删除 ， 项目代码部署后应及时删除其版本控制信息如.git。

■ 文档分级管理： 根据信息保密程度不同可将文档划分为 绝密级 、 机密级 、 秘密级 、公开级 ， 存档的纸质或电子文档必须在编写时标注密级 ， 按照要求使用和共享 ：

A．公开文档 ：文档泄露不会对公司利益造成损害 ， 可以外发。 如 ：宣传材料、产品手册等。

B． 秘密文档 ：文档泄露会对公司利益造成损害 。 如 ：公司人事档案、合同、协议等。

C．机密文档 ：文档泄露会对公司利益造成严重损害 ， 仅限内部授权的人员、通过指定通道使用，不能外发。如 ：财务报表、系统设计、后端代码等文档。

D．绝密文档 ：文档泄露会使公司利益受到特别严重损害 ， 仅限内部授权的人 员、通过指定通道分享 ， 不能留存（复印 、 拍照 、 摄像等）和外发。如 ：工艺流程 、 产品运营数据 、 企业规划战略 、 商业合同协议等文档。

9 / 22

**5.5** **信息系统运营**

■ 物理安全 ：员工进入数据中心需提前向相关部门申请入室授权 ， 携带个人身份证件由运维工程师陪同进入数据中心，根据授权范围开展相关工作。

■ 网络安全 ：禁止员工在数据中心或办公网中部署 VPN 等隧道服务或架设无线 接入点 ， 实现网络扫描 、 监听等危险性操作 ， 安全部门将持续监控。

■ 初始化加固 ：数据中心系统初始化时，系统管理员应该根据安全部门提供 的安全配置工具进行系统的安全加固 ， 完善用户创建 、 远程管理、网络防火墙 、 系统 文件 、 日志审计等配置 ；最小化安装系统软件包 、 运行必要的应用和服务 ；密码满 足 ：8 位及以上长度，含大小写字母、数字和特殊字符 ， 每 90 天更新一次。

■ 安全监控 ：部署的防病毒 、 防篡改 、 防泄漏等安全防护软件。

■ 权力滥用 ：盗取他人权限 、 入侵系统或用系统资源用于个人目的将被追责。

■ 职责分离 ：操作系统管理员与应用系统管理员不可兼职 ， 操作系统管理员必须 创建专门的操作系统维护账号进行日常维护。建议设置独立的数据库管理员，数据库 管理员必须创建专门的服务支撑账号进行日常服务支撑。

**5.6** **数据安全管理**

■ 数据所有者： 受收集或创建数据的组织指派 、 拥有数据权力和责任者，如部门 主管或业务经理，云计算环境的云客户，国际惯例认为其对数据安全负法律责任。

■ 数据处理者： 代表数据所有者操作数据者，如数据库管理员、云服务提供商。

■ 基本安全防护 ：存储有高、中级别信息的数据库 、 Hadoop 分布式存储以及业 务的前 、 后台服务须部署在内网， 敏感服务应该根据附录一执行开放策略。

■ 分类与分级保护 ：数据库管理员依据《数据分级与等级保护》 的要求，对相关系统数据进行定级， 由数据保护级别来执行数据的备份方式和频率，定期对备份数据进行检查，确保数据的可恢复性及有效性。

■数据访问： 原则上不允许直接访问数据或数据库 ， 必须通过具有审计功能的数 据库管理平台 （DMS）进行管理。

11 / 22

**5.8** **漏洞分级管理**

首先 ， 安全部门对发现的安全漏洞依据通用漏洞的评级标准、资产的重要 性 、 威胁的影响范围来计算漏洞的风险等级，漏洞的分级和处置要求如下：

■ 低危漏洞-V1 级：需要在 7 天内修复漏洞并反馈。

■ 中危漏洞-V2 级：需要在 3 天内修复漏洞并反馈。

■ 高危漏洞-V3 级：需要在 1 天内修复漏洞并反馈。

然后 ， 安全部门将安全漏洞录入到禅道系统，以工单形式来跟踪漏洞的 状态 ， 系统每天会以邮件方式通知到业务的安全责任人。

最后 ， 业务的安全责任人收到安全漏洞的通知后，参考漏洞管理流程进行处理。 若漏洞因一些情况暂时不能处理，需要及时反馈，经过业务经理批准后可延后处理。

漏洞归属者需要根据漏洞管理规范操作，不能违规忽略 、 延期或关闭安全漏洞。

**5.9** **安全事件管理**

■ 事件上报： 员工在发现（或外部报告）系统存在篡改、木马 、 病毒 、 拒绝服务 等安全事件或异常时应及时报告安全部门处理 ， 不允许瞒报 、 私自对安全事件进行处理。

■ 事件通报： 安全部门通过安全监控 、 漏洞检查 、 外部报告等发现安全事件或异常后 ， 将及时通知事发系统或设备的管理人员处理。

■ 事件处理： 安全部门依照安全事件响应流程对事件进行调查分析并记录 ， 首先对报告的事件或异常进行确认，如果事发系统为重要级别的应用系统应先上报总 监及以上领导并等待处理意见。在事件调查分析阶段一般应将事发系统或设备临时离 线，事发系统或设备管理人员应按照安全部门的 要求进行配合 。 安全部门应 对事件的原因、事件级别、分析过程进行详细记录并填写《安全事件记录单》 ，对相关证据要进行备份。

12 / 22

■ 漏洞修复 ：在安全事件分析结束后 ， 安全部门将依据结果给出处理要求， 系统管理人员需要按照处理要求实施处理措施， 操作完毕后经安全部门评估满足要求方可重新上线。

■ 事件记录 ：安全部门就事件原因进行评估，如发现是因未遵守安全规定所导致的事件，将事件详情及《安全事件记录单》上报给经理以上领导及事发部门经理以上领导。

■ 事件学习 ：安全部门应就事件发生原因及分析结果，对事发系统或设备管理人员进行教育，事发系统或设备管理人员应依据此安全事件发生的原因及分析的结 果 ， 检查其它可能存在同样隐患的系统或设备， 并对发现的漏洞及时处理。

**5.10** **网络安全管理**

为加强网络安全管理，防范网络入侵行为，保障网络运行安全 ， 安全部门特编制相关规定，详细内容可参考《网络安全使用指导》 。

■ 网络架构 ：网络架构的设计应满足网络的可靠性 、 可扩展性和可管理性等要 求。保证主要通信线路上冗余设计，网络 IP 地址的统一规划及管理。

■ 互联与接入 ：业务服务网络环境根据需求可划分为开发、 测试、运维 、 预发布 和生产等环境的若干种组合。安全域间应遵循默认禁止和最小授权原则配置 ， 默认情 况下生产和预发布环境对外仅可开放 80 和 443 端口 ， 且预发布环境对外须设置网络 白名单 ， 其他环境一律禁止开放公网。 内部办公系统严禁对外网开放，远程访问仅允 许通过 VPN 接入。

■ 网络运维 ：网络和安全设备的管理应通过堡垒机， 登录认证应采用双因子认证 技术，口令的设置及管理应满足《信息系统访问控制管理规定》 ， 禁止使用出厂默认 口令。网络和安全设备应开启日志审计功能，重要的安全事件追溯和审计日志至少需 留存 6 个月。

13 / 22

■ 网络监控 ：应建立网络监控系统，监控通信链路、设备性能、运行状态 ， 出现 异常应及时发出告警通知相关人员，监控问题应及时通知相关部门负责人或业务负责 人并要求期限内完成整改。

**5.11** **信息系统访问管理**

为明确信息系统访问控制要求，规范账号权限管理，防止未授权的访问和操

作 ， 安全部门特编制相关规定，详细内容可参考《信息系统访问控制 管理规定》 及《云服务资产访问安全管理规范》 。

■ 身份鉴别 ：对外的业务系统均须对接用户中心。 内部人员（包括 外包人员及临时员工） 使用的业务系统均须对接统一账号管理平台 （SSO） 。 对 于公司的重要信息系统如 L3 级系统， 登录模块应采用双因素认证方式 ， 采用的口令 方式验证的，需使用强口令、定期更改等策略。

■ 账号权限 ：账号的创建应根据可审计原则保证唯一可追溯性 ， 禁止分配历史账 号 、 共享账号 。 权限分配应遵循权限最小化原则 ， 根据用户的岗位和职责进行合理分 配 。 应日志记录账号的创建、 锁定与删除 ， 权限的设置与变更操作。系统中应设置账 号登录失败锁定和超时退出策略。

■ 流程管理 ：新员工入职时，由公司统一开通知音楼账号 ， 根据员工属性 （全职 员工， 兼职员工， 临时员工等）进行基础权限的分类及授权 。 其他非知音楼账号认证 登录的系统或通过知音楼账号登录的高级权限，员工应通过流程平台 、 邮件或其他规 定的申请渠道向业务系统所属部门单独申请 。 当员工离职时 ， 应按照离职流程回收其 相应的信息资产以及账号权限。 人力资源部应对离职或转岗员工的账号清理流程的完 成情况进行确认，在离职或转岗员工的账号未完成清理的情况下，不得办理离职证明 和转岗手续。

14 / 22

■ 第三方账号 ：未经授权不得为第三方人员开设账号权限， 若有工作需要， 应确 保第三方人员已与公司签订有关安全保密协议 ， 且已与其明确了公司的安全管理要 求。 第三方人员的系统操作必须被记录 ， 记录形式包括但不限于现场监督记录 、 远程 操作监控、系统录屏 、 审计日志、系统日志、网络日志等， 记录应至少保留 6 个月。

■ 复核监督 ：系统管理员应至少半年对其管理的系统账号进行梳理复核。对系统 存量账户进行识别和分类，主要分为特权账号 、 普通账号、问题账号 。 梳理后通知系 统所属部门负责人和使用部门负责人，确认后针对系统账户和权限进行变更 、 锁定、 删除等措施。

■ 云资产访问 ：由于云端的特殊性安全部门针对云资产服务的账号授权、网 络及密钥、服务开放原则与访问管理等编制了相关规定 ， 详细内容可参考《云服务资 产访问安全管理规范》 。

**5.12** **主机系统安全管理**

为统一业务平台的主机系统安全技术规范， 指导业务平台主机的安全配置和 维护，提高业务平台各系统总体安全水平，保障公司经营活动能够持续、稳定和安全 的进行。特编制相关规定， 详细内容可参考《系统安全规范》 。

■ 主机安全管理 ：所有的云主机、 IDC 主机，包括生产环境 、 测试环境和开 发环境等必须通过堡垒机进行登录 ， 并有运维部统一进行管理。 外网访问堡垒机需要 拨 VPN 接入内网后才可访问。 操作系统须关闭不需要的系统服务、 默认共 享，减少系统负荷 ， 降低风险 。 系统上线前运维部门应参照《安全配置指南》 对 主机系统、 应用、数据库等进行安全加固。

■ 鉴别与控制 ：对用户进行严格的访问控制， 根据用户角色 （特权用户、运维用 户、 普通用户） 。 应具有登录失败处理功能，如一分钟 3 次登录失败则锁定 30 分

15 / 22

钟 。 还应配置并启用结束会话 、 登录连接超时自动退出等相关措施， 时间设置参数应 为 10 分钟以内。

■ 入侵与病毒防范 ：针对业务平台中 Windows 、 Linux 主机系统需要采用适当的 主机入侵检测系统进行入侵行为的检测与防护 ， 并且主机系统应具备防范病毒 、 木马 等恶意代码的能力。

■ 安全审计 ：针对业务平添中 Windows 、 Linux 主机系统需要安装安全审计软 件，对系统和数据库进行操作审计 ， 部署实施由运维部门负责。

**5.13** **办公终端安全管理**

为加强办公终端的安全管理和规范办公终端的合理使用，防范和降低员工在 访问信息系统或数据的过程中因办公终端使用不当导致的安全问题。特编制相关规 定， 详细内容可参考《办公终端安全管理规范》 。

■ 基本原则 ： “谁领用、 谁保管、 谁维护” ， 使用人应保持良好的办公终端使用 环境，保持办公终端的清洁 。 “谁使用、 谁负责” ， 使用人应合理使用办公终端， 禁 止实施与工作无关或危害信息安全的活动， 因使用不当等个人原因 ， 造成公司配 发的办公终端损坏或遗失， 一律由使用人赔偿。

■ 硬件管理 ：新采购的办公终端设备应由内部 IT 部门登记 、 标识 、 预装操 作系统和合规软件后 ， 再配发给使用人 。 当需要使用移动存储设备连接到办公终端 的， 须进行病毒查杀后方可接入。

■ 软件管理 ：所有计算机办公终端必须安装防病毒软件与数据放泄露软件 （DLP） 。 对特殊专业使用的终端设备必须安装合适的防病毒软件， 并及时升级操作 系统补丁和病毒库。重新配发归还办公终端前 ， 应由内部 IT 部重装系统后再进行配 发。

16 / 22

■ 网络接入 ：办公终端接入办公网， 应采取技术控制措施对接入办公网的办公终 端设备进行认证。如因工作需要，需将非计算机或者笔记本电脑接入内部帮 公网的， 必须经安全部门同意并检查后 ， 方可接入。

■ 维护和处置 ：办公终端发生故障后 ， 应联系内部 IT 部门进行维修，如特殊原 因，需送至第三方维修 ， 内部 IT 部需在送修前拆除硬盘或擦除硬盘上的数据，防止信 息外泄 。 办公终端无法修复的，经内部 IT 部核验后回收报废设备， 使用人无权自行处 理。办公终端报废前需内部 IT 部统一处理， 擦除报废办公终端上的磁盘数据。

**6** **违反处罚**

**6.1** **违反上报**

对发现有违反该规定或安全要求的情况或线索 ， 全员可通过以下方式进行举报 ：

**6.2** **处罚细则**

对于违反《信息安全规定》 的行为， 除了《信息安全红线 和处罚规定》 特别定义的信息安全红线内容和其执行的处罚外 ， 安全部门对其进 行损失和影响评定，由相关部门参考违规行为造成影响的大小进行处罚：

■ 若违反信息安全规定相关要求可直接导致，机密、保密和内部数据的泄露 ， 或数据完整性遭受破坏 ， 或系统资源被利用，或信息系统可用性和业务连续性受到影 响，或公司经济或品牌受损的情况 ， 将按照安全黄线标准进行处罚。

■ 安全黄线处罚规定：对于第一次触犯员工， 给予书面警告 ， 已邮箱形式通报当 事人及安全责任人。对于二次触犯员工或未在规定时间内完成整改的，处罚标准升级 为红线处罚标准。

■ 若违反信息安全规定相关要求并导致，机密、保密和内部数据的泄露，或数据 完整性遭受破坏 ， 或系统资源被利用，或信息系统可用性和业务连续性受到影响，或

17 / 22

公司经济或品牌受损的情况 ， 将按照《信息安全黄线和红线处罚规定》 安 全红线标准进行处罚。

■若已造成显著损失， 必须通报部门总经理，由部门总经理决定处罚措施， 安全部门认为所属部门总经理的处罚措施不恰当 ， 可以要求部门总经理对其重新进行 处理。 安全部门有权对其不当行为进行通报和案例分享。

**7** **评审及更新**

■ 安全部门每年会组织相关人力资源部门对本规定进行评审，如果规定 存在不足应进行更新以满足安全需求。

■ 发生重大信息安全事故后 ， 安全部门会组织技术委员会等部门对本规 定进行技术评审，如果规定存在不足应进行更新以满足安全需求。

18 / 22

**附录一、** **《敏感服务端口开放管理规定** **1.0** **版》**

**1.** **安全性策略：**

策略 ：限制敏感服务和端口完全开放在公网， 使用非默认端口的敏感服务亦适用 本策略要求。

说明 ：完全开放公网指没有设置任何网络白名单 （如 Linux 的 iptables 或 Windows 防火墙设置） 策略。

管理： 根据服务完全开放公网的潜在风险对其分： 禁止类开放、 强限制开放两类 执行网络访问控制。

监控 ：扫描器持续识别公网端口开放情况，发现违规开放的将邮件通知安全 部门和业务部门负责人。

**2.** **开放和申请：**

禁止全开放：不允许其完全开放公网，特殊情况需业务负责人发起申请。

强限制开放：不建议其完全开放公网，特殊原因下使用的申请流程如下：

日常的流程 ：服务器管理员邮件申请 （发送给 ：security@baiducom） ->安全 部门备案和评估 （1 个工作日给出安全评估结果） ->安全部门网络组或服务器管 理员实施内网隔离后实施公网开放策略。

加急的流程 ：服务器管理员邮件申请 （发送给 ：安全部门负责人， 抄送给 ： security@baiducom） -> 安全部门负责人审核->安全部门备案和评估 （1 个小 时给出安全评估结果） ->运维部门网络组或服务器管理员实施内网隔离后实施公 网开放策略。

**3.** **敏感服务端口列表：**

19 / 22

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 敏感服务 | 默认端口 | 协议 | 服务完全开放的风险 | 开放管理 |
| FTP 服务 | 20,21 | TCP | 未授权操作资源、存放非法 数据、 控制服务器等 | 强限制开 放 |
| SSH 服务 | 22 | TCP | 不安全的密码设置被撞库成 功后直接控制服务器 | 强限制开 放 |
| Telnet 服务 | 23 | TCP | 不安全的密码 、 流量被劫持 泄露数据、 控制服务器 | 强限制开 放 |
| DNS 服务 | 53 | TCP | 允许区域传送 、 DNS 劫持、 缓存投毒 、 欺骗 | 禁止全开 放 |
| DHCP 服务 | 67,68 | UDP | 劫持和欺骗 | 禁止全开 放 |
| NTP 服务 | 123 | UDP | 被利用于对其他主机发起网 络拒绝服务攻击 | 禁止全开 放 |
| NetBIOS 服务 | 135,137,138,139 | UDP | 勒索病毒 “永恒之蓝”使用 的文件共享端口 | 禁止全开 放 |
| SNMP 服务 | 161 | UDP | 默认密码导致服务器采集的 信息外泄、服务器被控制 | 禁止全开 放 |
| LDAP 服务 | 389 | TCP | 服务数据外泄、服务被拒绝 服务攻击导致不可用 | 禁止全开 放 |
| SMB 服务 | 444,445 | TCP | 勒索病毒 “永恒之蓝”使用 的文件共享端口 | 禁止全开 放 |
| RExec 服务 | 512,513,514 | TCP | 未授权远程执行主机命令控 制服务器等 | 禁止全开 放 |
| RSync 服务 | 873 | TCP | 未授权访问资源导致数据泄 露、服务器被控制 | 强限制开 放 |
| NFS 服务 | 111,1025,2049 | TCP | 未授权挂载磁盘进行读写操 作导致服务器被控制 | 强限制开 放 |
| MSSQL 服务 | 1433,1434 | TCP | 无密码 、 弱密码 、 默认密码 等导致数据泄露 | 禁止全开 放 |
| Oracle 服务 | 1521 | TCP | 无密码 、 弱密码 、 默认密码 | 禁止全开 |

20 / 22

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | 等导致数据泄露 | 放 |
| SSDP 服务 | 1900 | UDP | 被利用于对其他主机发起网 络拒绝服务攻击 | 禁止全开 放 |
| Zookeeper 服务 | 2181 | TCP | 未授权访问 | 禁止全开 放 |
| Mysql 服务 | 3306 | TCP | 无密码 、 弱密码 、 默认密码 等导致数据泄露 | 禁止全开 放 |
| RDP 服务 | 3389 | TCP | 不安全的密码设置被撞库成 功后直接控制服务器 | 禁止全开 放 |
| SVN 服务 | 3690 | TCP | SVN 泄露、未授权访问 | 禁止全开 放 |
| SysBase 、 DB2 服务 | 5000 | TCP | 无密码 、 弱密码 、 默认密码 等导致数据泄露 、 注入漏洞 | 禁止全开 放 |
| PostgreSQL 服务 | 5432 | TCP | 无密码 、 弱密码 、 默认密码 等导致数据泄露 | 禁止全开 放 |
| VNC 服务 | 5800,5900 | TCP | 不安全的密码设置被撞库成 功后直接控制服务器 | 禁止全开 放 |
| Redis 服务 | 6379 | TCP | 不安全密码设置导致数据泄 露、服务器被控制 | 禁止全开 放 |
| WebLogic 控制 台 | 7001,7002 | TCP | Java 反序列化 、 弱口令 | 禁止全开 放 |
| Zabbix 服务 | 8069 | TCP | 远程执行、 SQL 注入等 | 禁止全开 放 |
| Jboss 、 Jenkins 和 Resin 等 | 8080,8089 | TCP | Java 反序列化 、 弱口令 | 禁止全开 放 |
| WebSphere 控制 台 | 9090 | TCP | Java 反序列化 、 弱口令 | 禁止全开 放 |
| ElasticSearch 服 务 | 9200,9300 | TCP | 不安全密码和组件策略设置 导致数据泄露 | 禁止全开 放 |
| MemCache 服务 | 11211 | UDP | 不安全密码设置导致数据泄 | 禁止全开 |

21 / 22

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | 露、被控制发起 DDoS 攻击 | 放 |
| MongoDB 服务 | 27017,27018 | TCP | 无密码 、 弱密码 、 默认密码 等导致数据泄露等 | 禁止全开 放 |
| SAP  Management | 50000 | TCP | 远程执行 | 禁止全开 放 |
| Hadoop 服务 | 50070,50030 等 | TCP | 不安全密码和组件策略设置 导致数据泄露 | 禁止全开 放 |

22 / 22