云南腾电科技有限公司

信息安全管理程序

（YNTD-ITSS-0610）

编制人:谢广胜　　编制时间:2025.01.07

审核人:赵建中　　编制时间:2025.01.07

批准人:陆涛　　审批时间:2025.01.07

目录

1. 目的

本程序的目的是在运维服务交付过程中有效的管理信息安全。

满足信息管理系统运行和客户服务中的安全性需求以及合同、法律和外部政策等外部要求；

提供一个满足需求的基本的信息系统安全基线；

确保有效的信息安全措施在公司、运维服务部门和服务人员三个层面都得到贯彻。

2. 过程定义

安全管理是顺应信息安全的需要而产生的，其主要目标是确保信息的安全性。安全管理致力于确保服务的安全性在任何时候都能达到与客户约定的级别。

安全性在服务中被视为可用性管理的一部分。安全管理已经成为现代服务管理中一个重要的问题。

安全性是指不易遭到已知风险的侵袭，并且尽可能地规避未知风险的性能。提供这种性能的工具是安全措施。

安全措施的目标是要保护信息的价值，这种价值取决于机密性、完整性和可用性三个方面。

2.1. 范围

本程序适用于运维服务覆盖的所有部门。

2.2. 过程负责人

安全管理负责人

2.3. 主要输入

输入	来源
服务级别需求	服务级别协议。
配置管理	系统的配置项，记录和报告配置。

2.4. 主要输出

输出	去向
风险评估报告	信息安全管理负责人、部门经理。
信息安全报告	信息安全管理负责人、部门经理。
变更管理	服务实施过程中，服务交付过程的主要步骤。
服务报告管理	服务实施过程中，服务交付过程的主要步骤。

2.5. 职责权限

2.5.1. 安全管理负责人

一般由项目经理担任，负责整个安全管理流程的有效运作。

安全管理负责人职责：

监控安全管理流程；

根据组织安全需求，开发与维护安全计划；

处理与安全相关的问题和事件；

确保满足SLA中指定的安全需求；

完成包含流程结果，自评估及内部审计的信息安全风险评估报告；

人员组成：信息安全员管理员、部门经理等。

2.5.2. 客户服务负责人

一般由运维工程师担任负责安排项目中的信息安全风险评估；

做好用户的沟通，协调关于信息安全的问题。

2.6. 过程重要控制点

风险评估报告。

信息安全管理规范。

安全事件记录。

2.7. 过程测量指标

安全事件次数。

3. 术语

术语	定义
机密性	指保护信息免受未经授权的访问和使用。
完整性	指信息的准确性、完全性和及时性。
可用性	是信息在任何约定的时间内都可以被访问。这取决于由信息处理系统所提供的持续性。

4. 信息安全方针

公司信息安全方针为：全员参与、控制风险；积极预防、持续改进；

5. 信息安全策略

为了保证信息系统安全保护工作的整体、计划性及规范性， 保证各项措施和管理手段的正确实施，使信息系统信息数据的机密性、完整性及可使用性受到全面、可靠的保护，我们往往需要制定信息系统安全策略。

5.1. 信息安全策略定义

信息安全策略是单位内指导本单位及其信息系统如何管理和保护包括敏感信息在内的资产的规则、指南和惯例。

信息安全策略(Information Security Policies)是组织对信息和信息处理设施进行管理，保护和分配的原则，它告诉组织成员在日常的工作中什么是可以做的，什么是必须做的，什么是不能做的，哪里是安全区，哪里是敏感区，就像交通规则之于车辆和行人，信息安全策略是有关信息安全的行为规范。

5.2. 信息安全策略内容

5.2.1. 物理安全策略

旨在保护计算机服务器、数据存贮、系统终端、网络交换等硬件设备免受自然灾害、人为破坏，确保其安全可用。

制定物理安全策略，要重点关注存放计算机服务器、数据存贮设备、核心网络交换设备的机房的安全防范。其选址与规划建设要遵循 GB9361 计算机场地安全要求和GB2887 计算机场地技术条件，保证恒温、恒湿，防雷、防水、防火、防鼠、防磁、防静电，加装防盗报警装置，提供良好的接地和供电环境，要为核心设备配置与其功耗相匹配的稳压及 UPS 不间断电源。

5.2.2. 网络安全策略

旨在防范和抵御网络资源可能受到的攻击，保证网络资源不被非法使用和访问，保护网内流转的数据安全。

访问控制是维护网络安全、保护网络资源的重要手段，是网络安全核心策略之一。访问控制包括入网访问控制、网络授权控制、目录级安全控制、属性安全控制、网络服务器安全控制、网络监测和锁定控制、网络端口和节点的安全控制以及防火墙控制。安全检查（身份认证）、内容检查也是保护网络安全的有效措施。

网络加密手段包括链路加密、端点加密和节点加密， 链路加密是保护网络节点之间的链路数据安全，端到端加密是对从源端用户到目的端用户之间传输的数据提供保护，节点加密是对源节点到目的节点之间的传输链路提供保护。另外，数字认证在一定程度上保证了数据交互信息的安全。

5.2.3. 数据安全策略

旨在防止数据被偶然的或故意的非法泄露、变更、破坏， 或是被非法识别和控制，以确保数据完整、保密、可用。数据安全包括数据的存储安全和传输安全两个方面。

数据的存储安全系指数据存放状态下的安全，包括是否会被非法调用等，可借助数据异地容灾备份、密文存储、设置访问权限、身份识别、局部隔离等策略提高安全防范水平。

5.2.4. 软件安全策略

旨在防止由于软件质量缺陷或安全漏洞使信息系统被非法控制，或使之性能下降、拒绝服务、停机。软件安全策略分为系统软件安全策略和应用软件安全策略两类。

对通用的应用软件，可参照前款作法，通过加强与软件提供商的沟通，及时发现、堵塞安全漏洞。对量身定做的应用软件， 可考虑优选通过质量控制体系认证、富有行业软件开发和市场推广经验的软件公司，加强软件开发质量控制，加强容错设计，安排较长时间的试运行等策略，以规避风险，提高安全防范水平。

5.2.5. 系统管理策略

旨在加强计算机信息系统运行管理，提高系统安全性、可靠性。

要确保系统稳健运行，减少恶意攻击、各类故障带来的负面效应， 有必要建立行之有效的系统运行维护机制和相关制度。比如， 建立健全中心机房管理制度，信息设备操作使用规程，信息系统维护制度，网络通讯管理制度，应急响应制度等等。

要根据分工，落实系统使用与运行维护工作责任制。加强对相关人员的培训和安全教育，减少因为误操作给系统安全带来的冲击。要妥善保存系统运行、维护资料， 做好相关记录，要定期组织应急演练，以备不时之需。

5.2.6. 灾难恢复策略

旨在趁着系统还在运行的时候，制定一个灾难恢复计划，将灾难带来的损失降低到最小，使系统安全得到保障的策略。

主要需根据本单位及信息系统的实际情况，研究系统遇到灾害后对业务的影响，设计灾后业务切换办法，如定期备份数据，根据灾难类型，制订灾难恢

复流程，建立灾难预警、触发、响应机制， 组织相关培训和练习，适时升级和维护灾难恢复计划等等。

6. 信息安全管理过程描述

6.1. 风险评估计划和过程

6.1.1. 评估计划

信息安全风险评估工作共分为 4 个阶段：即准备阶段、识别阶段、分析阶段、规划验收阶段。

准备阶段：主要完成项目组织、项目实施方案确定、组织培训、项目启动的工作。

识别阶段：主要完成大量的现场识别工作，主要有资产识别、威胁识别、脆弱性识别、安全措施识别。

分析阶段：在识别的基础上进行大量整理并分析，得出风险评估各要素的风险状况，具体有资产影响分析、威胁分析、脆弱性分析、综合风险分析。

规划验收阶段：对综合风险进行梳理分析，制定风险控制规划和改进计划，完成风险评估。

6.1.2. 评估过程

现场评估工作主要分 5 个阶段：

第一阶段：网络设备资产调查和拓扑调查。获取信息系统现有网络设备资产和网络链路情况相关资料，进行现场核对，发现存在的偏差，及时和网管员沟通确认，最终根据信息资产调查的全面结果，形成网络设备资产列表和网络拓扑图。

第二阶段：对信息系统内所有服务器资产进行识别，确定评估对象外的与之相关联的资产作为最终评估对象，然后根据评估的资产在业务和应用流程中的重要程序为资产进行估价。

第三阶段：网络和安全设备测评和网络结构测评。根据资产调查结果和网络拓扑分析，确定本次项目网络和安全设备评估范围。依据确定的网络和安全

设备测评范围，开展网络设备现场测评工作。网络和安全设备测评过程中，由网络管理人员输入相关设备密码，评估人员依据测评表的内容，进行现场核查，同时记录核查结果和操作内容，为后期网络设备安全性分析提供有利依据。

第四阶段：主机系统、应用系统和存储数据备份的测评。 在确定最终评估对象的资产识别和估价完成后，根据实际的系统和应用系统确定与之相应的评测表。主机测评过程中，由系统管理人员输入相关设备密码，评估人员依据测评表的内容，进行现场核查，同时记录核查结果和操作内容，为后期主机设备安全性分析提供有利依据。

第五阶段：系统漏洞扫描，主要针对网络设备、安全设备、服务器、 PC 终端的漏洞扫描，并形成漏洞扫描报告。

6.2. 评估方法和工具

我们主要参考相关标准和指南采用最新的方法进行风险分析，表述出威胁源采用何种威胁方法，利用了系统的何种脆弱性，对哪一类资产，产生了什么样的影响，当前采取了何种安全措施进行防护，其有效性如何，描述残余风险状况，并描述采取何种对策来防范威胁，减少脆弱性。

资产的评估主要是对资产进行相对估价，而其估价准则就是依赖于对其影响的分析，主要从保密性、完整性、可用性三方面的安全属性进行影响分析，从资产的相对价值中体现了威胁的严重程度；威胁评估是对资产所受威胁发生可能性的评估；脆弱性的评估是对资产脆弱程度的评估，安全风险评估就是通过综合分析评估后的资产信息、威胁信息、脆弱性信息，最终生成安全风险信息。

测评内容	测评方式	测评方式	测评方式
管理测评	☐ 访谈	☐ 文档审核	☐ 观察现场
物理测评	☐ 访谈	☐ 文档审核	☐ 观察现场
网络状况测评	☐ 访谈	☐ 文档审核	☐ 验证
网络设备测评	☐ 验证	☐ 文档审核	☐ 漏洞扫描
主机设备测评	☐ 验证	☐ 文档审核	☐ 漏洞扫描

数据安全及备份恢复测评	☐ 访谈	☐ 验证	☐ 文档审核
应用系统测评	☐ 访谈	☐ 验证	☐ 文档审核

1.访谈：通过与服务事业部的相关人员进行交谈和问询，了解信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认；

2．文档审核：审核服务事业部网管员提交的有关信息系统安全的各个方面的文档，如：安全管理制度和文件、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料等等。通过对这些文档的审核与分析确认测评的相关内容是否达到了等级的要求；

3. 验证：主要是对一些需要上机进行确认的信息进行核实，以及对某些面谈和文档审核的内容进行核实；

6.3. 评估内容

评估内容主要分为安全技术测评和安全管理测评，其中安全技术测评主要是针对系统所处的物理安全、网络安全、主机系统安全、应用安全、数据安全。管理测评主要是针对管理机构、安全管理制度、人员、系统建设、日常运维管理。

6.4. 资产的评估和赋值

资产是风险评估的评估对象。在一个全面的风险评估中，风险的所有元素都以资产为中心，威胁、脆弱性以及风险都是针对资产而客观存在的。威胁利用资产自身的脆弱性使得安全事件的发生成为可能，从而形成了风险。因此，资产的评估是风险评估的一个重要的步骤，它被确定和分析的准确性将影响着后面所有因素的评估。

资产主要包括公司的网络设备、网络安全设备、终端、服务器、数据库、业务软件、数据等信息资产。

资产赋值的过程也就是对资产在机密性、完整性和可用性上的达成程度进行分析，并在此基础上得出综合结果的过程。

首先对机密性赋值，根据资产在机密性上的不同要求，将其分为五个不同的等级，分别对应资产在机密性上应达成的不同程度或者机密性缺失时对整个组织的影响。机密性赋值标准如下表所示：

赋值	标识	定义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害
3	中等	组织的一般性秘密，其泄露会使组织的安全和利益受到损害
2	低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害
1	很低	可对社会公开的信息，公用的信息处理设备和系统资源等

然后对完整性赋值，根据资产在完整性上的不同要求，将其分为五个不同的等级，分别对应资产在完整性上缺失时对整个组织的影响。完整性赋值标准如下表所示：

赋值	标识	定义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补。
4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补。
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但可以弥补。
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，对业务冲击轻微，容易弥补。
1	很低	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略。

最后对可用性赋值，根据资产在可用性上的不同要求，将其分为五个不同的等级，分别对应资产在可用性上应达成的不同程度。可用性赋值标准如下表所示：

赋值	标识	定义
5	很高	可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上，或系统不允许中断。
4	高	可用性价值较高，合法使用者对信息及信息系统的可用度达到每天90%以上，或系统允许中断时间小于 10 分钟。
3	中等	可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于30 分钟。
2	低	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于60 分钟。
1	很低	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%。

最终，资产价值依据资产在机密性、完整性和可用性上的赋值等级， 经过综合计算评定得出一个综合数值，根据这个数值，对应下表即可分析出资产的总体价值：

等级	标识	得分	描述
5	很高	4.6-5	非常重要，其安全属性破坏后可能对组织造成非常严重的损失。
4	高	3.6-4.5	重要，其安全属性破坏后可能对组织造成比较严重的损失。
3	中	2.6-3.5	比较重要，其安全属性破坏后可能对组织造成中等程度的损失。
2	低	1.6-2.5	不太重要，其安全属性破坏后可能对组织造成较低的损失。
1	很低	1-1.5	不重要，组织造成导很小的损失，甚至忽略不计

6.5. 威胁评估

6.5.1. 威胁概述

威胁是指可能对资产或组织造成损害事故的潜在原因。威胁可能源于对信息系统直接或间接的攻击，也可能源于偶发的或蓄意的内部、外部事件。威胁只有利用系统存在的脆弱点才能对系统造成影响和伤害，形成风险。

威胁调查主要通过调查问卷、现场观察、问询等方式对信息系统进行提取威胁评估需要的相关信息。

6.5.2. 威胁识别

威胁识别的任务主要是识别可能的威胁主体（威胁源）、威胁途径和威胁方式，威胁主体是指可能会对信息资产造成威胁的主体对象，威胁方式是指威胁主体利用脆弱性的威胁形式，威胁主体会采用威胁方法利用资产存在的脆弱性对资产进行破坏。

威胁主体：分为人为因素和环境因素。根据威胁的动机， 人为因素又可分为恶意和非恶意两种。环境因素包括自然灾害和设施故障。

威胁途径：分为间接接触和直接接触，间接接触主要有网络访问、语音、视频访问等形式，直接接触指威胁主体可以直接物理接触到信息资产。

威胁方式：主要有传播计算机病毒、传播异常信息(垃圾邮件、反动、色情、敏感信息)、扫描监听、网络攻击(后门、漏洞、口令、拒绝服务等)、越权或滥用、行为抵赖、滥用网络资源(P2P 下载等)、人为灾害(水、火等)、人为基础设施故障(电力、网络等)、窃取、破坏硬件、软件和数据等。

6.5.3. 威胁分析

威胁识别工作完成之后，我们将对资产所对应的威胁进行评估，我们将威胁的权值分为 1-5 五个级别，等级越高威胁发生的可能性越大。

威胁的权值主要是根据多年的经验积累或类似行业的历史数据来确定。对于那些没有经验和历史数据的威胁，我们主要根据资产的吸引力、威胁的技术

力量、脆弱性被利用的难易程度等制定了一套标准对应表， 以保证威胁等级赋值的有效性和一致性。

根据赋值准则，我们对威胁发生的可能性用频率来衡量赋值：

等级	标识	定义
5	很高	威胁发生的频率极高，几乎每月都会发生，如常见网络病毒感染、垃圾邮件攻击等
4	高	威胁发生的频率较高，每季度可能发生一次，如弱口令被破解、非授权访问尝试等
3	中等	威胁发生的频率中等，每半年至一年可能发生一次，如网络设备配置错误导致的安全漏洞、内部人员误操作等
2	低	威胁发生的频率较低，1-3年可能发生一次，如硬件设备意外故障、轻微的自然灾害影响等
1	很低	威胁发生的频率极低，3年以上才可能发生一次，如重大自然灾害直接破坏机房、高级持续性威胁（APT）针对本企业的定向攻击等

6.6. 脆弱性评估

脆弱性是指资产中存在的可能被威胁利用的缺陷或弱点，包括技术层面和管理层面的脆弱性，其存在会增加安全事件发生的可能性及造成的影响程度。脆弱性评估需结合资产特性、业务场景，从物理环境、网络架构、系统配置、数据管理、人员操作等多维度展开。

技术脆弱性主要体现在：网络设备缺少访问控制策略、服务器操作系统未及时更新安全补丁、数据库默认账户未禁用且密码简单、应用系统存在SQL注入或跨站脚本漏洞、数据传输未采用加密技术等。管理脆弱性主要体现在：安全管理制度缺失或不完善、人员安全意识薄弱、权限分配混乱且未定期审计、应急响应流程不明确、安全培训未常态化开展等。

脆弱性赋值同样采用1-5级标准，等级越高表示脆弱性越严重，被威胁利用的难度越低。赋值需综合考虑脆弱性的暴露程度、利用难度、影响范围，具体标准如下表：

等级	标识	定义
5	很高	脆弱性易被发现且利用难度极低，一旦被利用将导致核心资产完全失控，如管理员账户弱口令、核心系统存在公开漏洞且未修复
4	高	脆弱性较易发现，利用难度低，被利用后将造成重要资产受损，如普通用户权限过高、网络端口随意开放
3	中等	脆弱性需一定技术手段才能发现，利用难度中等，被利用后影响范围有限，如非核心系统补丁更新延迟、数据备份频率不足
2	低	脆弱性发现难度较大，利用条件苛刻，被利用后仅造成轻微影响，如办公终端缺少屏保密码、非敏感数据存储未加密
1	很低	脆弱性几乎难以发现，利用需特殊条件，被利用后无实质影响，如历史遗留的无用账户未及时清理（无权限）

6.7. 风险评估分析

风险评估分析是通过综合资产价值、威胁发生可能性及脆弱性严重程度，计算风险值并确定风险等级的过程，核心公式为：风险值=资产价值等级×威胁可能性等级×脆弱性严重程度等级。通过该公式计算得出的风险值，对应以下标准确定风险等级，为后续风险处置提供依据。

风险值范围	风险等级	处置优先级及应对措施
75-125	极高风险	最高优先级：立即启动应急响应，24小时内制定整改方案并实施，如核心数据库被入侵风险
36-74	高风险	高优先级：7个工作日内完成整改，期间采取临时防护措施，如服务器存在高危漏洞

8-35	中等风险	中优先级：30个工作日内完成整改，定期跟踪风险变化，如权限分配不合理
2-7	低风险	低优先级：纳入常规安全优化计划，季度内完成整改，如办公终端安全配置不规范
1	极低风险	观察优先级：无需立即整改，定期监测即可，如无权限的历史账户

风险评估分析需形成《信息安全风险评估分析报告》，明确各风险点的具体位置、影响范围、计算依据及初步处置建议，提交信息安全管理负责人及相关部门经理审核。

6.8. 7.9 设计安全规范

设计安全规范需以风险评估结果为核心依据，结合国家相关标准（如GB/T 22080-2016）、行业最佳实践及客户SLA中的安全要求，从物理环境、网络架构、系统安全、数据安全、人员管理等维度制定全面、可落地的安全规范体系，确保覆盖所有高风险及中等风险点。

各维度安全规范核心内容包括：

物理安全规范：明确机房准入管理流程（如双人双锁、门禁权限分级）、环境监控指标（温度18-24℃、湿度40%-60%）、设备巡检周期（每日巡检电源、空调，每周巡检消防设施）、应急处置措施（火灾、漏水应急流程）；

网络安全规范：规定网络分区策略（核心区、办公区、DMZ区隔离）、防火墙配置规则（最小权限原则）、VPN接入认证要求（双因素认证）、网络日志留存期限（不少于6个月）、定期漏洞扫描周期（每月一次）；

系统安全规范：明确操作系统（Windows、Linux）安全配置基线（如禁用不必要服务、开启审计日志）、服务器密码策略（长度≥12位，包含大小写字母、数字及特殊字符，每90天更换）、补丁更新流程（高危补丁72小时内安装）、终端安全管理（安装杀毒软件、开启U盘管控）；

数据安全规范：划分数据安全等级（绝密、机密、秘密、公开），规定不同等级数据的存储方式（绝密数据需加密存储）、传输协议（机密以上数据采

用SSL/TLS加密传输）、备份策略（核心数据每日全量备份+实时增量备份，异地存储）、销毁流程（电子数据采用多次覆写，纸质数据粉碎）；

人员管理规范：明确岗位安全职责（信息安全管理员、系统管理员职责分离）、人员入职安全培训要求（考核合格方可上岗）、权限申请与审批流程（最小必要权限）、离职人员权限回收机制（离职当日完成账号禁用及权限注销）。

安全规范需经各相关部门评审、信息安全管理负责人审核、公司管理层批准后发布实施，确保规范的权威性和可行性。

6.9. 实施安全规范

安全规范的实施需制定详细的实施计划，明确责任部门、责任人、实施步骤、完成时限及资源需求，确保各项规范落地执行。实施过程分为准备、执行、验证三个阶段：

准备阶段：成立实施专项小组，由信息安全管理负责人牵头，各部门指定联络员配合；组织全员进行安全规范培训，确保相关人员掌握规范要求及操作方法；准备所需的软硬件资源，如杀毒软件、加密工具、门禁设备等。

执行阶段：各责任部门按照实施计划推进规范落地，如IT部门完成网络分区配置、服务器安全基线加固、数据备份系统部署；行政部门完成机房门禁升级、消防设施检修；人力资源部门完善人员安全管理流程。实施过程中需做好记录，形成《安全规范实施记录表》，详细记录实施内容、时间、遇到的问题及解决措施。

验证阶段：实施完成后，由专项小组对安全规范的实施效果进行验证，通过现场检查、技术扫描（如漏洞扫描、配置核查）、数据测试等方式，确认各项规范是否达到预期要求。对未达标的项目，督促责任部门限期整改，直至验证通过。

6.10. 监控安全状况

为确保安全规范持续有效，需建立常态化的安全状况监控机制，实时监测信息系统的安全状态，及时发现并处置安全隐患及异常事件。监控范围涵盖物理环境、网络运行、系统状态、数据流转、人员操作等方面，具体措施如下：

物理环境监控：在机房部署温湿度传感器、烟感报警器、漏水检测仪，数据实时上传至监控平台，当指标超出阈值时自动触发报警（短信+邮件通知信息安全管理员）；门禁系统记录所有出入记录，每周进行审计。

网络安全监控：部署网络入侵检测系统（IDS）、网络入侵防御系统（IPS），实时监测网络流量中的异常行为，如端口扫描、恶意攻击、异常数据传输；利用网络管理平台监控网络设备运行状态，及时发现设备故障或配置异常。

系统安全监控：在服务器、终端部署安全管理软件，实时监控系统进程、日志信息，及时发现病毒感染、非授权访问、补丁缺失等问题；数据库审计系统监控数据库操作，重点监测批量数据导出、权限变更等敏感操作。

数据安全监控：通过数据防泄漏（DLP）系统监控敏感数据的传输和使用，防止数据非法外泄；定期检查数据备份情况，验证备份数据的完整性和可恢复性。

人员操作监控：定期审计用户账户权限及操作日志，发现权限滥用、非授权操作等情况及时处置；通过安全培训效果评估、日常抽查等方式，监控人员安全操作行为。

监控过程中发现的安全隐患及异常事件，需立即记录并按照《信息安全事件管理流程》进行处置，监控结果需形成《安全状况监控报告》，每周上报信息安全管理负责人，每月进行汇总分析。

6.11. 维护安全规范

信息安全环境处于动态变化中，如新的威胁技术出现、业务系统升级、法律法规更新等，都可能导致现有安全规范失效或不完善。因此，需建立安全规范的维护机制，确保规范持续适应安全需求。

维护工作包括日常更新和定期修订：日常更新主要针对紧急情况，如出现重大安全漏洞、新的法律法规发布时，及时对相关规范进行补充或调整，经信

息安全管理负责人审核后临时发布；定期修订每年度进行一次，由信息安全管理部门牵头，收集各部门对安全规范的意见和建议，结合年度风险评估结果、监控数据及行业发展趋势，对安全规范进行全面修订，修订流程与初始发布流程一致。

安全规范的维护记录需妥善保存，包括修订原因、修订内容、审批意见等，确保规范的可追溯性。

6.12. 风险的处置

风险处置是针对风险评估分析中识别的风险点，采取相应的处置措施，将风险控制在可接受范围内的过程。处置措施需结合风险等级及业务实际，主要包括风险规避、风险降低、风险转移、风险接受四种方式：

风险规避：对于极高风险且无法通过其他方式控制的风险，采取放弃相关业务活动或停止使用存在严重缺陷的资产的方式规避风险，如停止使用存在重大安全漏洞且无修复方案的老旧系统。

风险降低：针对高风险、中等风险点，通过技术手段或管理措施降低风险发生的可能性或影响程度，如为服务器安装防火墙、定期更新补丁以降低被攻击的风险；制定数据备份策略以降低数据丢失的影响。这是最常用的风险处置方式。

风险转移：对于部分难以自行控制的风险，通过购买保险、签订服务协议等方式将风险转移给第三方，如购买信息安全责任险，将数据泄露造成的经济损失风险转移给保险公司；委托专业的安全服务公司提供漏洞扫描服务。

风险接受：对于低风险、极低风险点，且处置成本高于风险可能造成的损失时，可选择接受风险，但需定期监测风险变化，确保风险等级未提升。

风险处置需制定《风险处置计划》，明确各风险点的处置方式、责任部门、完成时限及预期效果，处置完成后需进行验证，确保风险已降至可接受范围，并更新《风险评估报告》。

6.13. 剩余风险评估

在实施风险处置措施后，需对剩余风险进行评估，判断剩余风险是否在组织可接受的风险范围内。剩余风险评估的流程与初始风险评估一致，重点评估风险处置措施的有效性及未完全消除的风险点。

剩余风险评估需关注以下内容：风险处置措施是否达到预期效果，风险发生的可能性及影响程度是否降低；是否因实施风险处置措施产生了新的风险（如引入新的软件导致的兼容性漏洞）；现有剩余风险是否符合公司的风险接受准则。

若剩余风险仍超出可接受范围，需重新制定风险处置计划，采取进一步的处置措施；若剩余风险在可接受范围内，则将其纳入常态化监控，定期跟踪风险变化。剩余风险评估结果需形成《剩余风险评估报告》，提交信息安全管理负责人及公司管理层审核。

6.14. 信息安全事件管理

信息安全事件是指由于自然或人为因素，导致信息系统可用性降低、数据泄露或损坏、服务中断等，对组织造成或可能造成损失的事件。为规范信息安全事件的处置流程，减少事件造成的损失，需建立完善的信息安全事件管理机制。

信息安全事件分为四级：一级（特别重大事件）：导致核心业务系统中断24小时以上，或敏感数据大量泄露（超过10万条），造成重大经济损失或恶劣社会影响；二级（重大事件）：核心业务系统中断12-24小时，或敏感数据泄露1-10万条，造成较大经济损失；三级（较大事件）：一般业务系统中断6-12小时，或敏感数据泄露1000-10000条；四级（一般事件）：一般业务系统中断6小时以内，或敏感数据泄露少于1000条，影响范围较小。

信息安全事件管理流程包括事件发现与报告、事件研判与分级、事件处置与控制、事件调查与总结四个阶段：

事件发现与报告：任何人员发现信息安全事件后，需立即向信息安全管理员报告（可通过电话、邮件、即时通讯工具等方式），报告内容包括事件发生

时间、地点、现象、影响范围等。信息安全管理员接到报告后，需在30分钟内初步核实事件情况。

事件研判与分级：信息安全管理负责人组织专项小组对事件进行研判，根据事件影响范围、损失程度等确定事件等级，并立即向对应层级的管理层报告（一级事件向公司最高管理层报告，二级事件向部门经理及以上报告，三级及以下事件向信息安全管理负责人报告）。

事件处置与控制：根据事件等级启动相应的应急响应预案，采取止损措施，如隔离受感染的终端、关闭存在漏洞的服务、恢复备份数据等，防止事件扩大。处置过程中需做好详细记录，包括处置措施、时间、参与人员等。

事件调查与总结：事件处置完成后，专项小组对事件原因进行深入调查，明确责任主体，分析事件暴露出的安全漏洞，并制定整改措施。同时，形成《信息安全事件调查报告》，总结事件处置经验教训，优化应急响应预案及安全规范。

信息安全事件的处置需遵循“快速响应、果断处置、减少损失、追溯根源”的原则，确保事件得到及时、有效的处理。

7. 信息安全与其他流程的关系

信息安全管理并非独立运行，需与公司其他管理流程紧密结合，形成协同机制，确保安全要求贯穿于业务全流程。主要关联流程及协同方式如下：

与服务级别管理流程的关系：服务级别协议（SLA）中需明确信息安全相关的服务指标，如系统可用性、数据安全性等，信息安全管理流程需围绕这些指标制定安全措施，确保SLA的达成；同时，信息安全事件可能影响服务级别指标的实现，需及时向服务级别管理负责人反馈，共同制定应对措施。

与配置管理流程的关系：配置管理流程需将信息资产（如网络设备、服务器、软件）的配置信息纳入配置管理数据库（CMDB），信息安全管理流程依据CMDB中的配置信息开展资产评估、漏洞扫描等工作；当资产配置发生变更时，配置管理流程需及时通知信息安全管理部门，评估变更可能带来的安全风险。

与变更管理流程的关系：任何涉及信息系统的变更（如系统升级、网络拓扑调整、权限变更）都需经过信息安全评估，变更管理流程需将信息安全评估

作为必要环节，未经安全评估的变更不得实施；信息安全管理部门需参与变更方案的审核，提出安全建议，并在变更实施后验证安全措施的有效性。

与服务报告管理流程的关系：信息安全管理流程产生的安全状况报告、风险评估报告等需纳入服务报告体系，定期向客户及公司管理层提交，展示信息安全工作成效及存在的风险；同时，服务报告中反映的服务质量问题，需结合信息安全要求进行分析，提出改进措施。

与人力资源管理流程的关系：人力资源管理流程在人员入职、调岗、离职等环节需同步执行信息安全管理要求，如入职时进行安全培训、调岗时调整权限、离职时回收账号及设备；信息安全管理部门需为人力资源部门提供安全规范支持，共同做好人员安全管理。

8. KPI 指标

为量化信息安全管理工作成效，确保管理目标的实现，制定以下关键绩效指标（KPI），定期进行监测和评估：

指标名称	指标定义	目标值	统计周期
信息安全事件数量	全年信息安全事件发生数量	0 次	年度

KPI指标的监测结果需纳入月度及年度信息安全报告，针对未达标的指标，分析原因并制定改进措施，持续提升信息安全管理水平。

9. 相关文件

《服务级别协议》

《配置管理规范》

《变更管理流程》

《信息安全事件应急响应预案》

《机房管理规定》

《数据备份与恢复管理规范》

《员工信息安全行为准则》

10. 相关记录

《文件编制和变更履历表》

《信息安全风险评估报告》

《资产识别与赋值表》

《威胁评估记录表》

《脆弱性评估记录表》

《安全规范实施记录表》

《安全状况监控报告》

《风险处置计划》

《剩余风险评估报告》

《信息安全事件报告》

《信息安全事件调查报告》

《员工安全培训记录表》

《数据备份验证记录表》

《KPI指标监测统计表》