团 体 标 准

信息系统安全保密管理规范

编 制 说 明

《信息系统安全保密管理规范》小组

二〇二五年八月

目　录

《信息系统安全保密管理规范》团体标准

编制说明

一、工作简况

（一）任务来源

当前，数字化转型深入发展，信息系统已成为国家秘密、工作秘密和敏感信息处理的核心载体与关键渠道。然而，海量信息在产生、传输、存储和处理过程中，面临日益严峻复杂的安全保密风险挑战，包括外部网络攻击、内部管理疏漏、新技术应用带来的未知隐患等。实践中，尽管存在国家层面的法律法规要求，但在具体行业、特定领域或不同规模的组织机构内，信息系统的安全保密管理仍存在标准不统一、要求不具体、可操作性不强等问题。许多单位缺乏系统性、精细化的管理规范指导，导致安全保密措施碎片化、防护水平参差不齐，难以有效应对新型威胁和满足实际管理需求，亟需一套更具针对性、实操性的标准来填补细粒度管理空白。

制定《信息系统安全保密管理规范》团体标准具有重要的现实意义和战略价值。首先，它能有效凝聚行业共识，为特定行业或领域内的组织提供清晰、统一、可落地的信息系统安全保密管理框架和实施路径，显著提升管理的规范性和精细化水平。其次，该标准能有力弥补现有法规在具体操作层面的不足，通过明确管理要求、细化技术防护措施、规范操作流程，指导各单位建立健全覆盖信息系统全生命周期的安全保密防护体系，切实筑牢信息安全的制度防线和技术屏障。最终，通过推广实施这一标准，将全面提升相关组织和行业整体的信息风险防控能力，为国家秘密和工作秘密安全、维护关键信息基础设施稳定运行、保障数字经济健康发展提供坚实的标准化支撑。

（二）编制过程

为使本标准在信息系统安全保密管理市场管理工作中起到规范信息化管理作用，标准起草工作组力求科学性、可操作性，以科学、谨慎的态度，在对我国现有信息系统安全保密管理市场相关管理服务体系文件、模式基础上，经过综合分析、充分验证资料、反复讨论研究和修改，最终确定了本标准的主要内容。

标准起草工作组在标准起草期间主要开展工作情况如下：

1、项目立项及理论研究阶段

标准起草组成立伊始就对国内外信息系统安全保密管理相关情况进行了深入的调查研究，同时广泛搜集相关标准和国外技术资料，进行了大量的研究分析、资料查证工作，确定了信息系统安全保密管理市场标准化管理中现存问题，结合现有产品实际应用经验，为标准起草奠定了基础。

标准起草组进一步研究了信息系统安全保密管理需要具备的特殊条件，明确了技术要求和指标，为标准的具体起草指明了方向。

2、标准起草阶段

在理论研究基础上，起草组在标准编制过程中充分借鉴已有的理论研究和实践成果，基于我国市场行情，经过数次修订，形成了《信息系统安全保密管理规范》标准草案。

3、标准征求意见阶段

形成标准草案之后，起草组召开了多次专家研讨会，从标准框架、标准起草等角度广泛征求多方意见，从理论完善和实践应用多方面提升标准的适用性和实用性。经过理论研究和方法验证，起草组形成了《信息系统安全保密管理规范》（征求意见稿）。

（三）主要起草单位及起草人所做的工作

1、主要起草单位

协会、企业等多家单位的专家成立了规范起草小组，开展标准的编制工作。

经工作组的不懈努力，在 2025 年 8 月，完成了标准征求意见稿的编写工作。

2、起草人所做工作

广泛收集相关资料。在广泛调研、查阅和研究国际标准、国家标准、行业标准的基础之上，形成本标准草案稿。

二、标准编制原则和主要内容

（一）标准编制原则

本标准依据相关行业标准，标准编制遵循“前瞻性、实用性、统一性、规范性”的原则，注重标准的可操作性，本标准严格按照《标准化工作指南》和 GB/T 1.1《标准化工作导则 第一部分：标准的结构和编写》的要求进行编制。标准文本的编排采用中国标准编写模板 TCS 2009 版进行排版，确保标准文本的规范性。

（二）标准主要技术内容

本标准报批稿包括 8 个部分，主要内容如下：

1　范围

本文件规定了信息系统安全保密管理的术语和定义、基本要求、职责分工、密品管理、风险评控、事件处置。

本文件适用于信息系统安全保密管理。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。

其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统 information system

由计算机及其相关设备、设施（含网络）构成的，按照一定应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

4 基本要求

4.1 目标与原则

4.1.1 本文件应确立信息系统安全保密管理的整体框架，旨在保障信息的机密性、完整性和可用性，防范未授权访问、篡改、泄露及破坏。

4.1.2 安全保密管理应遵循以下核心原则：

—— 最小授权原则：访问权限应仅限于完成职责必需的最小范围；

—— 全程可控原则：信息全生命周期应实施闭环管控；

—— 责任到人原则：每项操作应可追溯至具体责任人；

—— 适度安全原则：防护强度应与信息密级、业务价值及风险等级相匹配。

4.2 管理体系要求

4.2.1 组织应建立纵向贯通、横向协同的安全保密管理体系，明确决策层、管理层和执行层的职责边界。

4.2.2 最高管理者应：

—— 批准安全保密方针并分配资源；

—— 定期组织管理评审，评估体系有效性；

——　对重大泄密事件承担领导责任。

4.2.3　各部门宜设立专职保密管理员，负责日常监督与合规检查。

4.3　基础保障措施

4.3.1　组织应制定覆盖物理环境、网络架构、应用系统及数据资源的分层防护策略。

4.3.2　所有信息系统上线前应通过安全风险评估，重大变更后应重新评估。

4.3.3　人员管理应满足：

——　涉密岗位人员上岗前应接受背景审查与保密培训；

——　离岗人员应及时撤销权限并签署保密承诺；

——　外部协作人员可签订保密协议并限定临时权限。

4.4　持续改进机制

4.4.1　组织宜建立安全保密绩效指标，包括但不限于：

——　安全事件平均响应时间；

——　年度内控合规率；

——　员工培训覆盖率。

4.4.2　应每年至少开展一次内部审计，审计结果应作为管理评审输入。

4.4.3　当发生重大技术变革、业务调整或法规更新时，应及时修订管理策略。

5　职责分工

5.1　决策层职责

5.1.1　组织最高管理者应承担安全保密管理最终责任，包括批准安全保密战略方针与资源配置计划、签发机构级保密管理制度、授权组建保密管理委员会并任命其负责人。

5.1.2　保密管理委员会应审议年度保密工作计划与预算，协调跨部门重大保密事项决策，对泄密事件定级并启动问责程序。

5.1.3　委员会主席宜由分管安全的副总裁级人员担任；最高管理者可委托委员会处理日常保密治理事务，但应保留重大事项终审权。

5.2　管理层职责

5.2.1　安全保密主管部门应制定保密管理实施细则，组织实施全系统风险评估与整改督查，管理保密资质认证全流程。

5.2.2　信息技术部门应依据保密要求设计系统架构，部署技术防护措施，定期执行渗透测试与漏洞修复，实时监控网络异常行为。

5.2.3　人力资源部门应建立涉密人员背景审查机制，实施分级保密培训，管理保密责任书签订及离岗审计流程，并将保密绩效纳入部门考核指标。

5.2.4　管理层部门应建立月度联席会议机制，共享风险信息并协同处置隐患。

5.3　执行层职责

5.3.1　业务部门负责人应确保本部门业务操作符合保密规范，指定专职保密联络员并督导日常检查工作，每季度提交保密自查报告。

5.3.2　保密管理员应维护涉密载体全生命周期台账，审核权限变更申请并监督最小授权执行，协助安全事件调查与应急响应。

5.3.3　系统用户应妥善保管身份认证介质，定期更新高强度口令，及时报告设备异常或可疑行为，不应擅自复制、外传敏感信息。

5.3.4　所有执行层人员离岗时应签署保密承诺书并完成权限清退。

5.4　监督协同机制

5.4.1　内部审计部门应独立评估保密管理体系有效性，每半年审计关键控制点并追踪整改闭环，审计结果应直报决策层。

5.4.2　法务部门宜参与对外保密协议审查，界定泄密事件法律责任，提供合规争议司法解释。

5.4.3　纪检监察机构可对重大违规行为启动问责调查；各部门应配合监督机构调取日志、访谈人员及封存证据，不应隐匿或篡改原始记录。

5.5　外包责任界定

5.5.1　采购部门应将保密要求纳入供应商准入标准，监督服务商签署具有法律效力的保密承诺书，对高风险服务商可要求提供履约担保。

5.5.2　外包服务商应遵守委托方保密制度，限制其人员接触非授权信息，主动通报服务过程中的安全隐患。

5.5.3　信息技术部门应对外包系统实施隔离部署并保留数据主权，每季度对服务商进行现场安全检查；因服务商过失导致泄密的，采购部门应追究其违约责任并纳入黑名单。

5.6　责任追究原则

5.6.1　对按预案处置紧急事件造成次要数据损毁的情形，或已履行报告义务但因不可抗力未能阻止泄密的情形，可豁免个人责任。

5.6.2　对故意规避技术防护措施、瞒报迟报重大安全事件、未及时撤销离职人员权限等行为，应追究直接操作人员及主管领导责任。

5.6.3　责任追究应遵循客观公正原则，综合考量过错程度、损害后果及补救措施；处理结果宜记入人员档案并影响职务晋升评聘。

6　密品管理

6.1　基础要求

6.1.1　组织应明确定义密品范围，涵盖涉密电子设备、存储介质、纸质文件、专用软硬件系统及其他承载敏感信息的实体或虚拟载体。

6.1.2　应建立密品全生命周期管理制度，覆盖生成、标识、传输、使用、

存储、维修及销毁各环节，制度内容应符合 GB/T 39786 的有关规定。

6.1.3　所有密品应实施分类分级管控，依据密级设定差异化管理措施；绝密级密品可独立制定专项管理规程。

6.2　介质管理

6.2.1　涉密存储介质应统一配发并登记唯一序列号，建立介质台账动态跟踪流转状态，台账内容至少包含介质类型、密级、责任人、存放位置及使用日志。

6.2.2　移动存储介质使用前应进行病毒查杀与恶意代码检测，不应在非涉密设备接入；外出携带高密级移动介质时，宜配备物理防拆装置及定位追踪功能。

6.2.3　介质维修应由授权机构在指定安全环境执行，维修前应清除全部数据；无法现场维修的，可启用安全容器密封运输至定点单位。

6.3　电子数据管理

6.3.1　涉密电子数据生成时应自动嵌入密级标识与水印信息，标识内容应包含下列内容：

——　生成时间；

——　责任部门；

——　访问权限规则。

6.3.2　核心数据库应实施多重加密保护，密钥管理职责与数据管理职责须分离；日常操作可启用安全沙箱环境隔离敏感数据处理过程。

6.3.3　数据跨网络传输应使用经国家认证的密码设备，传输链路宜采用端到端加密协议；批量传输高密级数据前应执行内容脱敏审查。

6.4　使用控制

6.4.1　密品使用场所应设置门禁与视频监控系统，绝密级场所宜部署电

磁屏蔽及红外入侵检测装置；进出记录应留存至少 180 日。

6.4.2　人员接触密品前应完成身份双因子认证，操作过程应受权限控制系统约束；高密级密品使用过程可要求全程录像备查。

6.4.3　密品外借应履行审批登记手续，借用人应签署保密承诺书；外借周期超过 30 日的，借出部门应每半月核查密品状态。

6.5　处置管理

6.5.1　纸质涉密载体销毁应使用碎纸机具并达到国家保密标准规定的颗粒度要求，销毁过程应双人监销并填写处置凭证。

6.5.2　电子存储介质销毁前应执行不可逆数据擦除，擦除效果应通过专业设备验证；物理销毁可采取消磁、熔毁或粉碎方式，残骸处置应符合环保规定。

6.5.3　涉密设备报废应拆除存储部件单独处置，设备主体流转前应清除全部敏感标识；处置过程记录应永久保存备查。

6.6　审计改进

6.6.1　应每季度对密品台账进行账实符合性核查，重点审计高流转频率介质与关键数据库访问日志；审计发现账实不符的，须在 24 h 内启动溯源调查。

6.6.2　密品管理绩效宜纳入部门年度考核指标，考核内容可包括制度执行率、处置合规率及风险事件下降率等维度。

6.6.3　发生重大管理漏洞的，责任部门应在一个月内提交整改方案；涉及技术防护缺陷的，可启动专项预算升级防护体系。

7　风险评控

7.1　总体要求

7.1.1　组织应建立系统化风险评控机制，覆盖信息系统规划、建设、运

行及废弃全生命周期，确保保密风险可控可追溯。

7.1.2　风险评控流程应包含风险识别、分析、评估、处置及监控五阶段，每阶段输出文档宜纳入保密管理体系文件库。

7.1.3　应每年至少开展一次全面风险评估；遇重大系统变更或安全事件时，可启动专项风险再评估。

7.2　组织与职责

7.2.1　保密管理委员会应审批风险评估方法论与接受准则，监督高风险处置方案落实。

7.2.2　安全保密主管部门应主导风险评估实施，协调业务部门提供资产清单与流程说明。

7.2.3　信息技术部门应配合提供网络拓扑、系统架构及防护措施技术参数。

7.2.4　内部审计部门应独立验证风险评估结果真实性，核查处置措施有效性。

7.3　风险识别

7.3.1　应识别关键信息资产，包括硬件设施、业务数据、应用系统及服务能力。

7.3.2　应梳理资产面临威胁，涵盖外部攻击、内部违规、技术故障及自然灾害。

7.3.3　应分析系统脆弱性，涉及配置缺陷、协议漏洞、管理缺失及物理隐患。

7.3.4　可参考国家漏洞库、行业安全通告及历史事件报告完善识别维度。

7.4　风险分析

7.4.1　应量化风险值，计算公式为：风险值=可能性×影响严重度；可

能性与严重度宜采用五级刻度制。

7.4.2　可能性分析应考虑威胁频率、脆弱性暴露程度及现有防护强度。

7.4.3　影响严重度评估应覆盖保密性损害、完整性破坏、可用性中断及法律责任四维度。

7.4.4　对难以量化的风险，可采用专家德尔菲法进行定性分级。

7.5　风险评估与处置

7.5.1　应依据风险值矩阵划定风险等级：

——　极高风险：应 48 h 内制定处置计划；

——　高风险：应两周内明确处置方案；

——　中风险：宜三个月内实施处置；

——　低风险：可纳入常规监控改进。

7.5.2　处置策略选择应遵循以下优先级：

——　消除风险：通过架构改造或下线资产彻底规避；

——　转移风险：采用保险或外包服务分担责任；

——　降低风险：部署技术控制或管理补偿措施；

——　接受风险：经决策层审批后备案监控。

7.5.3　风险接受应满足前置条件：

——　处置成本显著超过潜在损失；

——　残余风险值低于组织风险阈值；

——　制定专项应急预案并定期演练。

7.6　监控与改进

7.6.1　应建立风险指标看板，动态跟踪以下数据：

——　未闭合高风险数量及超期时长；

——　中低风险转化率；

—— 残余风险覆盖率。

7.6.2 每季度应召开风险评控联席会议，达成以下目标：

—— 分析新威胁趋势与防护策略失效案例；

—— 调校风险计算参数与等级阈值；

—— 审议处置措施延迟执行原因及问责建议。

7.6.3 风险评控全流程文档应保存十年以上，包括：

—— 资产清单与威胁模型；

—— 风险评估报告及审批记录；

—— 处置方案验证证据；

—— 应急演练报告。

7.7 外包风险管理

7.7.1 供应商准入评估应增加以下内容：

—— 其自身安全管控成熟度等级；

—— 近三年服务泄密事件统计；

—— 关键岗位人员背景审查机制。

7.7.2 服务过程监管应执行以下措施：

—— 按月审查服务商安全日志；

—— 对高风险服务实施第三方渗透测试；

—— 合同终止时审计数据清除效果。

7.7.3 因供应商过失导致风险事件的，应同时追究以下责任：

—— 采购部门供应商选型失职责任；

—— 监管人员过程监控疏漏责任；

—— 服务商合同违约责任。

8 事件处置

8.1　总体要求

8.1.1　组织应建立安全保密事件分级分类标准，明确事件定义范畴覆盖数据泄露、系统入侵、设备失窃及违规操作等场景。

8.1.2　应制定全流程处置预案，包含监测预警、分析定级、应急响应、恢复整改及追责改进五阶段；预案每年度应组织跨部门评审修订。

8.1.3　所有事件处置过程应确保业务连续性优先，避免因响应措施导致次生灾害。

8.2　组织与职责

8.2.1　应急响应小组应包含以下核心角色：

——　指挥决策员：授权启动预案并调配资源；

——　技术分析员：负责溯源取证与影响评估；

——　公关协调员：统一对外信息发布口径；

——　法律顾问：确认合规责任与诉讼风险。

8.2.2　全员应履行事件即时报告义务，发现异常后须在 30 min 内通过专用通道上报；隐瞒不报或延迟报告者应追责。

8.2.3　外部技术支援机构应签署保密协议，其操作过程应受安全保密主管部门全程监督。

8.3　监测与定级

8.3.1　应部署以下监测手段：

——　网络流量异常检测系统；

——　主机进程行为监控工具；

——　数据库敏感操作审计平台；

——　物理区域门禁异常告警装置。

8.3.2　事件定级应综合评估以下要素：

—— 受影响资产密级与数量；

—— 已泄露数据敏感程度；

—— 系统服务中断时长；

—— 社会负面影响范围。

8.3.3 定级结果划分四类：

—— 特别重大事件：全面业务停摆或核心数据大规模泄露；

—— 重大事件：关键系统受损或高密级数据泄露；

—— 较大事件：局部功能失效或敏感数据泄露；

—— 一般事件：低风险告警或未造成实质损害。

8.4 应急响应

8.4.1 特别重大事件响应流程：

a) 立即隔离受影响系统并暂停关联业务；

b) 2 h 内上报国家监管机构；

c) 48 h 内完成初步取证分析；

d) 每日三次向决策层报送处置进展。

8.4.2 遏制措施选择原则：

—— 网络攻击类：切断攻击源 IP 并封锁恶意进程；

—— 数据泄露类：冻结账户权限并追踪扩散路径；

—— 设备失窃类：远程擦除数据并触发定位追踪。

8.4.3 证据保全应执行以下操作：

—— 对受侵设备制作只读镜像备份；

—— 完整记录操作人员命令行历史；

—— 截获网络攻击载荷并存储哈希值。

8.5 恢复与整改

8.5.1　业务恢复前提条件：

——　确认攻击媒介已彻底清除；

——　验证备份数据完整性与一致性；

——　获得应急指挥组书面授权。

8.5.2　整改措施应覆盖以下层面：

——　技术层面：修复漏洞并强化访问控制策略；

——　管理层面：修订制度并补充培训内容；

——　物理层面：升级门禁系统或调整监控布局。

8.5.3　事件根因分析应追溯至：

——　直接技术缺陷；

——　流程执行疏漏；

——　人员意识欠缺；

——　第三方管理失控。

8.6　追责与改进

8.6.1　责任追究应区分：

——　直接责任人：违规操作或渎职人员；

——　管理责任人：制度缺失或监管失职干部；

——　技术责任人：防护措施失效的运维主体。

8.6.2　整改效果验证应执行：

——　技术措施渗透测试复测；

——　管理流程穿行测试检查；

——　人员保密知识重新考核。

8.6.3　事件闭环材料应包含：

——　处置过程时间线记录；

—— 损失影响定量评估报告；

—— 制度修订对比说明；

—— 人员追责处理决定。

8.7 外部事件协同

8.7.1 向监管机构报告应包含：

—— 事件发现时间与上报时间；

—— 受影响系统功能及数据范围；

—— 已采取的紧急处置措施；

—— 初步判定的事件根源。

8.7.2 涉及用户数据泄露时应：

—— 按法规时限通知受影响个人；

—— 提供免费身份保护服务；

—— 开放申诉渠道接受质询。

8.7.3 与执法机构协作应遵循：

—— 提供经脱敏处理的取证样本；

—— 配合调取日志应经法律审核；

—— 案件侦办期间不应公开细节。

三、主要试验和情况分析

结合国内外的行业测试标准和企业内部工厂管控的项目进行要求规定和试验验证。

四、标准中涉及专利的情况

无

五、预期达到的效益（经济、效益、生态等），对产业发展的作用的情况

信息系统安全保密管理企业规范运营，在国际市场上有机会与其他各国（相关）企业竞争。

六、与有关的现行法律、法规和强制性国家标准的关系

与现行法律、法规和强制性标准没有冲突。

七、重大意见分歧的处理依据和结果

标准制定过程中，未出现重大意见分歧。

八、标准性质的建议说明

本标准为团体标准，供社会各界自愿使用。

九、贯彻标准的要求和措施建议

无。

十、废止现行相关标准的建议

本标准为首次发布。

十一、其他应予说明的事项

无。