保密管理体系认证技术规范

文件编号：CTS TBGL024-2026

版本号：B/2

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

首次发布：2022-12-20 **首次实施：2022-12-20** **修订实施日期：20260423**

江西腾标认证有限公司

目录

1. 范围

本文件规定了组织建立、实施、保持和持续改进 保密管理体系认证技术规范 的要求。本文件适用于

1) 组织建立、实施、保持和改进 保密管理体系认证技术规范 管理方针和目标；
2) 认证机构对组织进行保密管理体系认证技术规范认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 19000-2016 质量管理体系 基础和术语
- GB/T 19001-2016/ISO 9001:2015 质量管理体系 要求
- GB/T 22080-2016/ISO/IEC 27001:2013 信息技术 安全技术 信息安全管理体系 要求
- GB/T 35770-2022/ISO 37301:2021 合规管理体系 要求及使用指南

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

GB/T 19000-2016以及下列术语和定义适用于本文件。

3.1 保密管理

组织为保护涉密信息，确保其机密性、完整性和可用性，在组织内建立、实施、保持和持续改进的一系列相互关联或相互作用的要素。

3.2 涉密信息

一旦泄露，可能对国家安全、公共利益或个人、组织的合法权益造成损害或影响的信息。

3.3 商业秘密

不为公众所知悉，具有商业价值，并经权利人采取相应保密措施的技术信息和经营信息。

3.4 秘密等级

根据涉密信息一旦泄露对国家安全、公共利益或组织利益造成的损害程度，划分的密级等级，如：国家秘密分为绝密、机密、秘密；商业秘密可分为核心商密、普通商密等。

3.5 保密风险

涉密信息的机密性、完整性、可用性或可控性遭到破坏的可能性及其后果的组合。

3.6 保密控制措施

为管理保密风险，确保涉密信息安全而实施的策略、程序、指南、实践或组织结构。

3.7 保密承诺书

涉密人员或相关方为履行保密义务，明确其保密责任而签署的书面声明。

3.8 最高管理者

在最高层指挥和控制组织的一个人或一组人。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨和战略方向相关，并影响其实现保密管理体系预期结果的能力的各种外部和内部因素。

- **外部因素**：法律法规要求（如《中华人民共和国保守国家秘密法》、《中华人民共和国数据安全法》、《中华人民共和国网络安全法》等）、监管机构要求（如国家保密局、国防科工局、行业主管部门等）、行业标准与规范、国际环境、地缘政治风险、市场竞争环境、技术发展趋势等。
- **内部因素**：组织的价值观、保密文化、规模、所有制性质、涉密业务范围、涉密等级、组织结构、员工构成、资源状况、信息系统与网络环境、设施设备状况、以往泄密事件记录等。

4.2 理解相关方的需求和期望

组织应确定：

a) 与保密管理体系有关的相关方；

b) 这些相关方的相关要求。

相关方包括但不限于：

- **内部相关方**：员工（特别是涉密人员）、管理层、股东。
- **外部相关方**：政府及监管机构（国家保密行政管理部门、公安、国安、行业主管部委等）、顾客（尤其是涉密项目委托方）、供方和承包商（如涉密载体印制单位、信息系统集成商、运维服务商）、认证机构、行业协会。

组织应建立、实施并保持程序，以识别相关方，并促其参与到与保密管理相关的已识别的议题中。与相关方的沟通应为一个**持续的过程**，而非一次性沟通。组织应将促进相关方参与所产生的输出形成文件。

4.3 确定保密管理体系的范围

组织应确定保密管理体系的边界和适用性，以确定其范围。

在确定范围时，组织应考虑：

a) 4.1中提及的各种外部和内部因素；

b) 4.2中提及的相关方的要求；

c) 组织的涉密场所、部门、产品和服务、活动过程。

范围应作为成文信息可获得。

4.4 保密管理体系及其过程

4.4 保密管理体系及其过程

4.4.1 组织应按照本标准的要求，建立、实施、保持和持续改进保密管理体系，包括所需过程及其相互作用。

组织应确定保密管理体系所需的过程及其在整个组织中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；

b) 确定这些过程的顺序和相互作用；
c) 确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；
d) 确定这些过程所需的资源并确保其可获得；
e) 分配这些过程的职责和权限；
f) 按照 6.1 的要求应对风险和机遇；
g) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；
h) 改进过程和保密管理体系。
4.4.2 在必要的范围和程度上，组织应：
a) 保持成文信息以支持过程运行；
b) 保留成文信息以确信其过程按策划进行。

5. 领导作用

5.1 领导作用和承诺

最高管理者应通过以下方面，证实其在保密管理体系方面的领导作用和承诺：
a) 对保密管理体系的有效性负责；
b) 确保制定保密管理方针和目标，并与组织战略方向一致；
c) 确保将保密管理体系要求融入组织的业务过程；
d) 确保提供建立、实施、保持和改进保密管理体系所需的资源（包括经费、设施、设备、人员等）；
e) 沟通有效的保密管理的重要性，提升全员保密意识；
f) 确保保密管理体系实现其预期结果；
g) 指导和支持人员为保密管理体系的有效性做出贡献；
h) 推动持续改进；
i) 支持其他相关管理者在其职责范围内发挥领导作用。

5.2 方针

最高管理者应制定、实施和保持保密管理方针，方针应：
a) 与组织的宗旨相适应；
b) 为制定保密目标提供框架；
c) 包括满足适用要求（如国家保密法规、行业标准、顾客要求）的承诺；
d) 包括持续改进保密管理体系的承诺；
e) 包括“保守国家秘密、保护商业秘密、预防泄密风险”的承诺。
方针应：

- 形成文件并可获得；
- 在组织内得到沟通（包括签署《保密承诺书》、张贴、培训等）；
- 适当时可为相关方所获取。

5.3 组织的岗位、职责和权限

最高管理者应确保组织内相关岗位的职责和权限得到分配和沟通。

最高管理者应**指定一名或多名管理者**（如分管保密工作的负责人、保密办公室主任），不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限：

a) 确保保密管理体系符合本文件的要求；

b) 向最高管理者报告保密管理体系的绩效，供其评审并作为持续改进的依据；

c) 确保在整个组织内提高对保密管理重要性的意识；

d) 协调与保密管理体系有关的内部和外部沟通。

同时，最高管理者应明确保密工作机构（或归口管理部门）及各业务部门在保密管理中的具体职责。

6. 策划

6.1 应对风险和机遇的措施

在策划保密管理体系时，组织应考虑4.1提及的因素和4.2提及的要求，并确定需要应对的风险和机遇，以：

a) 确保保密管理体系能够实现其预期结果；

b) 预防或减少不利影响（如泄密事件、合同违约、法律制裁、声誉损失）；

c) 实现持续改进。

组织应**建立并保持合规义务登记册**，以识别和跟踪与保密相关的法律法规、标准及其他要求。

组织应策划：

a) 应对这些风险和机遇的措施；

b) 如何将措施纳入保密管理体系过程并实施；

c) 如何评价这些措施的有效性。

6.2 保密目标及其实现的策划

组织应在相关职能（如保密办、人力资源、信息中心等）和层级（如公司级、部门级）上建立保密目标。

保密目标应：

a) 与保密方针一致；

b) 可测量（如果可行，如保密培训覆盖率、保密检查完成率、保密违规次数、泄密事件数）；

c) 考虑适用的要求；

d) 予以监视；

e) 予以沟通；

f) 视情况予以更新。

策划如何实现保密目标时，组织应确定：

a) 要做什么；

b) 需要什么资源；

c) 由谁负责；

d) 何时完成；

e) 如何评价结果。

6.3 变更的策划

当组织确定需要对保密管理体系进行变更时（如涉密业务调整、组织机构重组、法律法规更新、引入新信息系统），变更应系统地予以策划和实施。组织应考虑：

a) 变更的目的及其潜在后果；

b) 保密管理体系的完整性；

c) 资源的可获得性；

d) 职责和权限的分配或再分配。

7. 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进保密管理体系所需的资源。

资源包括：人力资源（保密管理专员、涉密人员）、基础设施（涉密场所、涉密计算机及办公自动化设备、保密防护设备、三合一设备、视频监控系统等）、过程运行环境（符合保密要求的物理环境、电磁环境）、监视和测量资源（监控报警系统、出入控制系统）、财务资源（保密专项经费）、技术资源（保密技术、加密系统、审计系统）。

7.2 能力

组织应：

a) 确定在其控制下工作的人员所需的能力，这些人员从事的工作可能影响保密管理体系绩效；

b) 基于适当的教育、培训或经验，确保这些人员具备所需能力；

c) 适用时，采取措施获得所需的能力，并评价所采取措施的有效性；

d) 保留适当的成文信息作为能力的证据（如保密教育培训记录、涉密人员资格审查记录、上岗证书）。

注：涉密人员上岗前应经过保密教育培训，掌握保密知识技能，签订保密承诺书。涉密人员在岗期间应接受持续的保密教育和培训。

7.3 意识

组织应确保在其控制下工作的人员知晓：

a) 保密方针；

b) 相关的保密目标；

c) 他们对保密管理体系有效性的贡献，包括改进绩效的益处；

d) 不符合保密管理体系要求的后果；

e) 在保密管理过程中个人的角色和职责；

f) 报告泄密风险和事件的程序。

7.4 沟通

组织应确定与保密管理体系相关的内部和外部沟通，包括：

a) 沟通什么（保密制度、保密要求、泄密风险、事件通报等）；

b) 何时沟通（入职、离岗、日常、发现风险时）；

c) 与谁沟通（内部员工、上级监管部门、顾客、供方等）；

d) 如何沟通（保密会议、内部文件、OA系统、培训、书面通知等）；

e) 谁来沟通（指定发言人、保密办公室）。

组织应建立、实施和保持程序，以确保与涉密项目相关的内外部相关方进行有效的保密沟通。

7.5 成文信息

7.5.1 总则

组织的保密管理体系应包括：

a) 本文件要求的成文信息（如保密手册、保密制度、操作规程、涉密载体台账、保密检查记录等）；

b) 组织确定的为确保保密管理体系有效性所必需的成文信息。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的标识（如密级标识、编号、版本号、受控状态）、格式以及评审和批准。

7.5.3 成文信息的控制

应控制保密管理体系所要求的成文信息，以确保：

a) 在需要的场所和人员处均可获得并适用；

b) 予以妥善保护（如防止非法泄露、不当使用、修改或破坏）。

为控制成文信息，适用时，组织应关注下列活动：发放、访问、检索和使用；存储和防护（如保险柜、加密存储、防盗设施）；版本控制；保留和处置（符合档案管理及保密期限要求）。涉密成文信息的管理应遵循“最小知悉范围”原则。

8. 运行

8.1 运行的策划和控制

组织应策划、实施和控制满足保密管理要求所需的全过程，并实施第6章所确定的措施。

组织应：

a) 确定保密管理的工作要求；

b) 建立下列内容的准则：

1. 过程准则（如定密准则、风险评估方法、载体销毁标准）；
2. 保密工作的接收准则（如涉密人员上岗审查通过标准、涉密计算机入网标准）；

c) 确定符合保密要求所需的资源；

d) 按照准则实施过程控制；

e) 在必要的范围和程度上，确定并保持、保留成文信息，以：

3. 确信过程已经按策划进行；
4. 证实保密管理工作符合要求。

8.2 涉密人员管理

8.2.1 人员审查与选聘

组织应建立涉密人员审查程序，基于风险评估结果确定涉密人员岗位，对拟进入涉密岗位的人员进行背景审查，确保其符合保密要求。

8.2.2 保密教育与培训

组织应制定并实施年度保密教育培训计划，对涉密人员进行岗前保密教育、在岗保密培训和离岗保密提醒。培训内容应包括保密法规、保密制度、保密技能和案例分析。

8.2.3 涉密人员考核与监督

组织应定期对涉密人员遵守保密制度的情况进行考核和监督。考核结果应作为奖惩、晋升、岗位调整的依据。

8.2.4 离岗管理

涉密人员离岗（包括离职、退休、调离岗位）时，应办理涉密载体清退、涉密设备移交、保密承诺书签署等手续，并进行离岗保密谈话。

8.3 涉密载体管理

8.3.1 制作与收发

涉密载体的制作、收发应履行登记、签收手续，明确秘级、保密期限、知悉范围。绝密级载体应指定专人负责。

8.3.2 传递与使用

传递涉密载体应采取必要的安全措施（如机要交通、专人护送、加密传输）。使用涉密载体应在符合保密要求的场所进行，并严格控制知悉范围。

8.3.3 复制与保存

复制涉密载体应经审批，并履行登记手续。保存涉密载体应配备符合要求的保密柜、密码保险柜等设施。

8.3.4 销毁

涉密载体的销毁应经审批，并在监督下进行，确保信息无法恢复。销毁记录应长期保存。

8.4 涉密场所与设备管理

8.4.1 涉密场所管理

组织应划定涉密场所，设置物理隔离和明显的保密标识，并采用门禁、视频监控、入侵报警等措施进行安全防护。

8.4.2 涉密设备管理

涉密计算机、办公自动化设备等应根据最高密级进行管理，并采取身份鉴别、访问控制、病毒防护、补丁管理、违规外联监控等安全措施。

8.4.3 设备维修与报废

涉密设备的维修应在本单位内部进行，并由专人全程陪同。**涉密设备的报废**应经审批，进行信息清除和物理销毁，并记录在案。

8.5 信息系统与网络安全管理

组织应建立涉密信息系统安全保密策略，基于风险评估确定安全保护策略，包括但不限于：用户权限管理、访问控制、日志审计、移动存储介质管理、病毒防范、漏洞扫描、入侵检测等。涉密信息系统严禁连接到非涉密网络或互联网。

8.6 保密检查与违规处理

8.6.1 保密检查

组织应建立保密检查制度，定期或不定期对各部门的保密工作责任制落实、制度执行、人员管理、载体管理、场所设备管理、信息系统安全等情况进行检查。

8.6.2 违规处理

对违反保密规定的人员，组织应根据情节轻重，给予**批评教育、通报、经济处罚或行政处分**。涉嫌违法犯罪的，应移交司法机关处理。

8.7 泄密事件处置与报告

组织应**建立并维护泄密事件应急预案**。一旦发生或发现泄密事件，应立即启动预案，采取有效措施防止事态扩大，并按照国家法律法规和上级要求，在规定时限内向保密行政管理部门和相关主管部门报告。

8.8 外部提供过程、产品和服务的控制

组织应确保外部提供的过程、产品和服务（如涉密载体印制、信息系统集成与运维、保密技术检测、涉密会议服务等）符合保密管理体系的要求。

组织应：

a) 向外部供方明确保密要求（如资质要求、保密协议、信息反馈制度）；

b) 评价和选择外部供方，确保其具备满足保密要求的能力（如持有相应的保密资质）；

c) **与外部供方签订保密协议，明确责任和义务**；

d) 对外部供方的保密绩效进行监视和评价。

9. 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a) 需要监视和测量什么（如保密培训完成率、保密检查问题整改率、违规事件数、泄密事件数、目标完成度）；

b) 适用的监视、测量、分析和评价的方法，以确保有效的结果；

c) **确保用于监视与测量的资源（如监控系统、审计系统）的准确性**；

d) 何时实施监视和测量；

e) 何时对监视和测量的结果进行分析和评价。

组织应评价保密管理体系的绩效和有效性，并保留适当的成文信息。

9.1.2 合规性评价

组织应根据法规要求（如《保守国家秘密法》、《数据安全法》等）和相关方对保密的要求，建立、实施并保持程序，以定期评价组织对适用法律法规、标准及其他要求的遵守情况。

合规性评价应至少每年进行一次，并**保留合规性评价报告作为成文信息**。

9.2 内部审核

组织应按策划的时间间隔进行内部审核，以提供有关保密管理体系是否符合本文件要求，以及是否得到有效实施和保持的信息。

组织应：

a) 策划、建立、实施和保持审核方案，包括频次、方法、职责、策划要求和报告；

b) 规定每次审核的准则和范围；

c) 选择审核员并实施审核，确保审核过程的客观性和公正性；

d) 确保将审核结果报告给相关管理者；

e) 及时采取必要的纠正和纠正措施。

9.3 管理评审

最高管理者应按策划的时间间隔评审组织的保密管理体系，以确保其持续的适宜性、充分性和有效性。

管理评审应考虑：

a) 以往管理评审所采取措施的实施情况；

b) 与保密管理体系相关的内外部因素的变化（如法规更新、业务调整）；

c) 有关保密管理体系绩效和有效性的信息，包括趋势：

1. 保密检查发现的问题及整改情况；
2. 保密违规和泄密事件发生情况；
3. 涉密人员管理情况；
4. **外部供方（如外包服务商）的保密绩效**；
5. 审核结果；
6. 目标的实现程度；
7. 不合格及纠正措施；
8. **合规性评价的结果**。

d) 资源的充分性（如保密经费、设备设施是否充足）；

e) 应对风险和机遇所采取措施的有效性；

f) 改进的机会（包括引入新的保密技术、完善制度等）。

管理评审的输出应包括与下列事项相关的决定和措施：

a) 改进的机会；

b) 保密管理体系所需的变更（如制度修订、流程优化）；

c) 资源需求（如增加保密经费、采购新设备）。

10. 改进

10.1 不合格和纠正措施

当发生不合格（如制度未执行、违规操作、泄密事件、检查不符合项）时，组织应：

a) 对不合格做出应对，并适用时：

1. 采取措施控制和纠正不合格；
2. 处置后果。

b) 通过下列活动，评价是否需要采取措施以消除产生不合格的原因，避免其再次发生或在其他场合发生：

3. 评审和分析不合格；
4. 确定不合格的原因；
5. 确定是否存在或可能发生类似的不合格。

c) 实施所需的措施；

d) 评审所采取的纠正措施的有效性；

e) **推荐预防措施**；

f) 必要时，对保密管理体系进行更改。

组织应保留成文信息作为不合格性质和随后所采取措施的证据，以及纠正措施结果的证据。

10.2 持续改进

组织应持续改进保密管理体系的适宜性、充分性和有效性。

组织应考虑分析和评价的结果、管理评审的输出，确定是否存在持续改进的需求或机会（如优化保密流程、应用新的保密技术、加强保密文化建设等），并将其作为变更管理的一部分加以实施。

————————————