《大数据环境下会计信息安全管理技术规范》

编制说明

《大数据环境下会计信息安全管理技术规范》编制组

2026 年 2 月

《大数据环境下会计信息安全管理技术规范》
编制说明

1.任务来源

《大数据环境下会计信息安全管理技术规范》的任务来源是由中国智慧工程研究会批准立项，由浙江同济科技职业学院、北京中云国创数据科技有限公司、厦门科云信息科技有限公司、浙江龙盛集团股份有限公司、浙江广厦建设职业技术大学、厦门网中网软件有限公司等单位起草编制。

2.目的意义

本文件的制定旨在适应会计核算与财务管理在大数据、云平台与智能分析技术推动下的深度变革，针对会计信息在采集、传输、存储、处理与共享过程中面临的数据泄露、篡改、越权访问、接口滥用以及合规风险上升等问题，建立面向大数据环境的会计信息安全管理技术规范。随着企业财务共享中心、业财一体化平台、电子凭证与在线报销、智能审计与风险监测等应用的普及，会计信息系统从封闭式单体系统演进为多系统集成、跨部门协同与对外互联的复杂生态，会计数据的敏感性、价值密度与流转频次显著提高，一旦发生安全事件将对经营决策、资金安全、信用合规与外部披露产生直接影响。本文件通过统一安全管理目标、技术控制措施与运行保障要求，推动会计信息安全由“单点防护”向“体系化治理”、由“被动处置”向“主动预防与持续监测”转变，为企业、机构及相关服务单位开展会计信息安全建设与管理提供一致的技术依据。

3.编制思路和原则

3.1.编制思路

本文件在编制思路上坚持以数据全生命周期与分级保护为主线，围绕会计信息在大数据环境中的典型链路，构建“制度管理+技术控制+运营保障”相结合的整体框架。内容组织强调首先明确会计数据资产范围与分类分级规则，以此为基础对数据采集与接入、数据传输与交换、数据存储与备份、数据处理与分析、数据共享与对外服务以及数据销毁与留存等环节提出技术要求，并将身份鉴别、访

问控制、权限最小化、日志审计、加密与脱敏、接口安全与数据水印等关键能力纳入统一控制体系。同时，考虑大数据平台组件多、链路长、算存分离与多租户等特征，本文件强调在架构层面落实安全域划分与隔离策略，在平台层面落实资源与作业安全控制，在应用层面落实业务规则与流程校验，在运维层面落实变更管理、漏洞管理与持续监测，使安全控制与业务运行相协同，确保既能满足效率与共享需求，又能有效降低安全与合规风险。

3.2.编制原则

本文件的编制遵循合规性与可审计性原则，强调会计信息安全管理应满足相关法律法规与监管要求，并形成可审计、可追溯的证据链；遵循机密性、完整性与可用性协同保障原则，既防止数据泄露与越权访问，也防止数据被篡改、丢失或不可用，确保会计核算与报表生成的可靠性；遵循分级分类与最小授权原则，强调按数据敏感度和业务角色实施差异化控制，降低权限滥用与横向扩散风险；遵循安全与业务平衡原则，强调安全措施应与业务流程、系统性能与用户体验相协调，避免因过度防护影响财务运营效率；同时遵循持续运营与动态防护原则，强调通过监测告警、基线检查、风险评估与应急演练形成闭环治理，使安全管理能够适应业务变化与威胁演进。

4.编制过程

本标准修订讨论会均采用线上征集专家意见的形式，线上会议共计 2 次，会议期间广泛听取专家意见，并形成意见汇总表。

5.内容修订说明

本次修订主要围绕强化大数据环境特有的安全控制点与提升运行保障可落地性进行了完善。修订中进一步明确了会计数据资产的边界与分类分级方法，强化了数据治理与元数据管理要求，使数据安全控制具备清晰对象与统一口径；对数据共享交换与接口安全内容进行了补充完善，强调数据出域审批、访问令牌与鉴权机制、调用频控与异常检测，降低对外互联场景下的泄露风险；对加密、脱敏与访问控制的工程化要求进行了细化，强调关键字段保护与可用性兼顾，提升措施可执行性；同时强化了日志审计、溯源取证、备份恢复与业务连续性要求，

并补充了安全运营相关内容，包括漏洞与补丁管理、配置基线、异常行为分析与应急响应流程，使本文件从“技术条款集合”升级为“可运行的安全管理体系”，进一步提升在企业财务数字化与合规治理中的应用价值。

ICS 35.030
CCS L 80

T/WEA

团　　体　　标　　准

T/WEA XXXX—2026

大数据环境下会计信息安全管理技术规范

Specification for accounting information security management technology in big data environments

（征求意见稿）

2026－XX－XX 发布　　2026－XX－XX 实施

中国智慧工程研究会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国智慧工程研究会提出并归口。

本文件起草单位：

本文件主要起草人：

引　言

随着大数据、云计算、人工智能与移动互联等技术在财务管理领域的广泛应用，会计信息的采集、处理、存储、共享与利用方式发生深刻变化。会计信息从传统以账务系统为核心的结构化数据，扩展为覆盖业务系统、支付结算、供应链协同、电子发票、税务申报、资金管理、预算绩效、审计取证等多源异构数据，并呈现出数据规模大、类型多、流转快、关联强和跨域共享频繁等特征。在大数据环境下，会计信息成为组织经营管理、合规治理、风险控制与决策支持的重要数据资产，其安全管理水平直接影响财务报告质量、经营连续性、合规风险与声誉风险。

与此同时，大数据环境显著放大了会计信息安全风险的复杂性与系统性。一方面，会计信息在数据链路上涉及采集端、传输通道、数据中台、数据湖/仓、分析模型、接口共享与多方协同等多个环节，任何一个环节的薄弱都可能导致泄露、篡改、丢失或不可用；另一方面，会计信息通常包含资金往来、交易明细、成本费用、工资薪酬、纳税信息、供应商与客户信息等敏感内容，具备较强的合规约束性和攻击价值，成为网络攻击、内部舞弊、权限滥用与供应链攻击的重点目标。此外，云化部署、外包运维、第三方接口对接与跨区域数据流动等模式日益普遍，使得边界更加开放、责任界面更加复杂，对身份认证、访问控制、数据分级分类、加密与密钥管理、日志审计、数据脱敏、备份恢复与应急响应提出更高要求。

在实践中，部分组织在会计信息安全管理中仍存在共性问题：安全职责分工不清、数据分类分级缺失或执行不到位、权限体系粗放、日志审计不完备、接口共享缺乏边界控制、数据脱敏与匿名化措施不足、备份恢复与演练流于形式、外包与第三方管理缺乏安全评估与持续监督等。这些问题在大数据环境下更易叠加放大，导致会计信息安全事件的潜在影响范围扩大、发现难度增加、处置成本上升，并可能引发合规处罚、经营损失与社会信任危机。

为规范大数据环境下会计信息安全管理活动，有必要从组织管理与技术控制两方面建立系统化要求，形成覆盖会计信息全生命周期的安全管理框架，明确数据资产识别与分级分类、访问控制与职责分离、数据保护与防篡改、接口与共享安全、日志审计与安全监测、备份恢复与业务连续、第三方与供应链安全、事件响应与持续改进等关键控制要点，并提供可检查、可审计、可落地的实施路径。本文件在总结会计信息安全管理特点与大数据技术应用场景的基础上，提出相应技术要求与管理要求，旨在提升会计信息的机密性、完整性、可用性与可追溯性，支撑组织在数字化财务转型过程中实现安全合规、风险可控与价值可用。

大数据环境下会计信息安全管理技术规范

1 范围

本文件规定了大数据环境下会计信息安全管理的总体要求、数据分级分类与安全控制要求、身份认证与访问控制要求、数据保护与防篡改要求、数据共享与接口安全要求、日志审计与安全监测要求、备份恢复与业务连续要求、第三方与供应链安全要求、安全事件响应与持续改进等内容。

本文件适用于各类组织在大数据平台、数据中台、数据湖/仓及相关业务系统环境中开展会计信息安全管理与技术防护工作。

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 22239 信息安全技术　网络安全等级保护基本要求

GB/T 25070 信息安全技术　网络安全等级保护安全设计技术要求

GB/T 35273 信息安全技术　个人信息安全规范

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

会计信息 accounting information

反映组织经济业务活动及其财务状况、经营成果和现金流量等内容的各类数据、文件及其元数据，包括凭证、账簿、报表、明细、交易记录、预算与成本数据、税务相关数据及其关联记录。

3.2

大数据环境 big data environment

以分布式存储与计算为基础，支持海量数据采集、汇聚、处理、分析与共享的数据技术与系统运行环境，通常包括数据湖/数据仓库、数据中台、流式处理、数据服务接口及其运维管理体系。

3.3

会计数据资产 accounting data asset

在会计信息范围内具有管理、合规、经营或决策价值的可识别数据集合，包括结构化、半结构化与非结构化数据及其标签、元数据与血缘信息。

3.4

数据分级分类 data classification and grading

依据数据的重要程度、敏感程度、合规要求与影响范围等维度对数据进行类别划分与等级划分，并据此配置差异化安全控制措施的过程。

3.5

最小授权 least privilege

仅向用户或系统主体授予完成其职责所必需的最小权限集合，并对权限的使用进行控制与审计的原则。

3.6

职责分离 segregation of duties

将关键业务操作与关键安全操作在角色、岗位或主体之间进行分离，避免单一主体可独立完成全部关键步骤，从而降低舞弊与滥用风险的控制原则。

3.7

数据脱敏 data masking

对敏感数据进行遮蔽、替换、泛化或扰动等处理，使其在非授权或非必要场景下无法识别敏感内容，同时保持必要的业务可用性。

3.8

安全审计 security auditing

对会计信息访问、处理、共享、导出、配置变更及异常行为等活动进行记录、留存、分析与追溯的管理与技术活动。

4 总体要求

4.1 安全目标与原则

会计信息安全管理应以保障会计信息的机密性、完整性、可用性与可追溯性为目标，应覆盖会计信息全生命周期及其在大数据环境中的采集、汇聚、处理、分析、共享与归档等活动。

会计信息安全管理应坚持分级分类、最小授权、职责分离、源头控制与持续改进原则，应将安全控制嵌入数据处理链路与业务流程，确保安全措施可执行、可验证、可审计。

4.2 组织与职责

应建立会计信息安全管理组织体系，应明确财务管理部门、信息化部门、安全管理部门、数据治理部门以及外包/第三方的职责边界与协作机制。

应明确会计信息数据资产责任人、数据管理员、系统管理员、安全管理员与审计角色，并对关键岗位设置授权、复核与审计机制。

涉及会计信息安全的制度、策略、配置与重大变更应履行审批程序并留存记录。

4.3 安全制度与流程体系

应建立覆盖数据分级分类、访问控制、共享与导出、加密与密钥管理、日志审计、备份恢复、漏洞管理、供应链管理、安全事件响应与持续改进等制度与流程。

应形成与大数据平台相适配的安全技术基线与配置清单，基线变更应纳入变更管理并可追溯。

应建立定期检查与评价机制，对安全控制有效性进行验证，对发现的问题应闭环整改并复核。

4.4 系统与数据边界管理

应识别会计信息涉及的系统边界与数据边界，至少应覆盖业务源系统、财务核算系统、资金系统、税务相关系统、报表与分析系统、大数据平台及数据共享接口等。

应明确跨系统数据流向、数据处理目的、数据共享范围与责任界面，应建立数据血缘与处理链路记录，确保可追溯。

对跨区域、跨主体的数据共享与处理，应开展风险评估并落实相应安全控制措施。

4.5 风险评估与控制策划

应定期开展会计信息安全风险评估，识别威胁、脆弱性与影响范围，形成风险清单与控制策划。

风险评估应覆盖内部滥用、外部攻击、配置错误、接口暴露、权限过大、数据泄露、篡改与不可用等典型风险，并结合大数据环境特点评估风险扩散与联动效应。

对高风险场景应制定专项控制措施，必要时实施加固与持续监测。

5 数据分级分类与安全控制要求

5.1 一般要求

会计信息应实施分级分类管理，应依据数据敏感程度、重要程度、合规要求、影响范围及对财务报告与经营管理的影响等因素确定分类类别与分级等级。

分级分类结果应与访问控制、加密保护、脱敏策略、共享与导出控制、审计强度、备份与恢复目标等安全控制策略联动，并应在数据平台层面落地为可执行的策略与标签。

分级分类规则与数据标签应纳入数据治理体系，应支持版本管理与持续更新；规则变更应评估对历史数据与现行控制策略的影响，并保留变更记录。

5.2 分类框架与分级要素

会计信息分类宜至少包括：财务核算类、资金结算类、税务申报与发票类、成本与预算类、薪酬与人事相关类、供应商与客户往来类、经营分析与管理报表类、审计取证与稽核类、系统配置与权限审计类等。

分级要素宜至少包括：

a）敏感性：是否包含个人信息、商业秘密、交易明细、价格成本、薪酬等敏感字段；

b）重要性：对财务报表、合规申报、资金安全与经营决策的影响程度；

c）合规性：法律法规、监管要求与内部制度要求的约束强度；

d）影响范围：泄露、篡改或不可用可能造成的影响范围与后果。

分级结果宜划分为若干等级（如一级至四级），并应明确各等级数据的最低控制要求。

5.3 数据标识、标签与范围界定

应对会计数据资产建立数据目录与数据字典，应对数据表、字段、文件、主题域与数据服务接口进行标识，并为其附加分级分类标签。

应建立“数据对象—处理活动—使用场景—共享对象”的范围界定机制，明确数据用途与授权边界，防止数据被超范围使用。

数据标识与标签应贯穿数据采集、存储、计算、共享与导出全过程，应支持在权限校验、脱敏渲染、审计记录与备份策略中自动引用。

5.4 分级分类控制要求

不同分级等级的数据应配置差异化控制措施，至少应包括：

a）访问控制：按角色、岗位、业务范围与数据等级实施细粒度授权；

b）加密保护：对高敏感/高重要数据实施存储加密与传输加密；

c）脱敏与匿名化：对非必要使用场景实施字段级脱敏或结果集脱敏；

d）审计与监测：对高等级数据访问、导出、共享与配置变更实施更高强度审计与异常检测；

e）备份与恢复：对关键数据设置更严格的备份频率、保留周期与恢复目标；

f）共享与导出：对高等级数据共享实施审批、最小集合、最小字段与最短时限控制。

对涉及财务报表编制依据、资金支付指令、税务申报底稿等关键数据，应列为重点保护对象，应在访问授权、版本控制、防篡改与审计留痕方面实施强化控制。

为便于实施与检查，不同等级数据的最低控制要求宜按表1执行。

表1　会计信息分级控制要求矩阵

分级等级	典型数据示例（可结合本单位细化）	访问控制要求	加密与脱敏要求	审计与监测要求	备份与恢复要求	共享与导出要求
一级（公开/一般）	已公开的财务制度摘要、已发布的公开披露报表（公开版）	角色授权；可按业务域限制	可不强制加密；共享前校验口径	记录基础访问日志；异常频次告警	常规备份；按系统默认恢复目标	可共享；记录共享对象与用途
二级（内部）	内部管理报表、预算汇总、一般往来台账（脱敏后）	角色+业务范围控制；禁止越域访问	传输加密宜采用；展示宜脱敏关键字段	记录访问与导出日志；定期审计抽查	定期备份；明确保留周期	共享需登记；导出需审批或授权确认
三级（敏感）	交易明细、成本价格明细、供应商/客户明细、税务底稿	细粒度授权（表/字段/行列级）；临时授权到期回收；职责分离	传输加密应采用；存储加密宜采用；默认动态脱敏	高强度审计（含字段访问、批量查询）；异常行为实时告警	提高备份频率；异地副本；定期恢复验证	共享需审批；最小字段集；导出加水印/加密；限制批量
四级（核心/高度敏感）	工资薪酬明细、资金支付指令/账户敏感要素、关键合并报表编制依据、审计取证证据链	最小授权+双人复核/分级审批；特权隔离；强制多因素认证	传输与存储加密应采用；密钥分域管理；严格脱敏/仅授权明文	全量审计+防篡改留存；特权操作强告警；联动阻断策略	不可变/隔离备份宜采用；更严格RTO/RPO；演练频次提高	原则上不对外共享；确需共享须高等级审批；导出全程留痕、加密、可追溯
注： 表1为通用示例。组织可结合监管要求、业务特性与数据资产清单，将分级名称、典型数据示例与控制强度进一步细化，并固化为可执行的策略标签与审批规则。						

6　身份认证与访问控制要求

6.1　一般要求

会计信息系统及大数据平台应对访问主体实施身份识别与认证，应确保“人、账号、权限、行为”一致可追溯。访问控制应覆盖人员用户、系统服务账号、接口调用主体与自动化作业账号。

访问控制应与数据分级分类联动，应实现“按角色授权、按业务范围约束、按数据等级加严”的控制机制，并应支持细粒度授权与动态控制。

6.2　身份认证要求

应对用户实施身份认证，认证方式至少应包含账号口令认证；对高权限用户、远程访问用户、涉及高等级会计信息访问或导出的用户，宜采用多因素认证。

应建立口令策略与认证失败控制机制，至少应包括口令复杂度、定期更新、重试次数限制、异常登录告警与账户锁定策略。

应建立统一身份管理机制或等效机制，确保人员入转离与权限调整同步，避免“离岗不销权”“共享账号”“僵尸账号”等风险。

6.3 访问授权与最小授权

应采用基于角色的访问控制模型，并应结合岗位职责设置角色权限矩阵。权限授予应以最小授权为原则，应仅授予完成职责所必需的功能权限与数据权限。

应支持细粒度数据权限控制，宜支持主题域、数据集、表、字段、行级或列级权限控制；对涉及个人信息、薪酬、交易明细、资金支付等高敏感字段，应实施字段级保护与脱敏展示。

权限调整应履行审批程序并留存记录；临时权限应设置有效期与自动回收机制。

6.4 职责分离与关键操作控制

应对关键业务与关键安全操作实施职责分离，至少应在以下环节形成相互制约：

a）数据接入与数据发布；

b）权限配置与权限审批；

c）数据提取/导出与导出审批；

d）报表生成与报表发布；

e）配置变更与变更审核。

对高风险操作应实施强化控制，至少应包括二次确认、双人复核或分级审批等措施。高风险操作至少应包括：批量导出、脱敏策略关闭、权限批量变更、接口密钥变更、核心数据删除/作废、作业调度规则变更等。

6.5 特权账号与服务账号管理

应对特权账号实施严格管理，特权账号应与普通业务账号隔离，应限制数量并强化认证与审计；特权账号的使用应遵循按需启用、事后复核的原则。

系统服务账号、接口账号与自动化作业账号应纳入统一管理，应实行最小权限配置与密钥/口令轮换；服务账号不应具备超范围数据访问权限。

应对服务账号调用行为进行审计与异常检测，发现异常访问、异常频次或异常范围时应触发告警并处置。

6.6 导出、共享与临时访问控制

会计信息导出与共享应实行审批控制，应明确导出目的、范围、字段、接收方、保存期限与责任人。对高等级数据导出应加严审批并记录全链路。

应限制大规模导出与批量查询，对超阈值查询、异常频次访问与可疑聚合行为应触发风险告警。

对临时访问、外部审计取证、应急排查等场景，应设置临时访问策略，明确授权范围与时效，并应在事件结束后及时回收权限并开展复核。

7 数据保护与防篡改要求

7.1 一般要求

数据保护应覆盖会计信息在采集、传输、存储、处理、共享与归档全过程，应根据分级分类结果实施差异化保护。

对关键会计信息应具备防篡改能力或等效控制，应保证关键数据的版本链、证据链与审计链连续完整。

7.2 传输保护要求

会计信息在跨网络、跨域或跨系统传输时应采取保护措施，涉及高等级数据传输宜采用加密通道并进行双向鉴别。

接口调用应采用安全协议并实施鉴权控制，应防止重放、伪造与中间人攻击；接口调用应记录请求主体、时间、范围与结果状态。

7.3 存储加密与密钥管理

对高敏感会计信息宜采取存储加密或等效保护措施，存储加密应覆盖数据湖/仓、对象存储、备份介质以及交换文件落地存储等场景。

密钥管理应分级分域，密钥的生成、分发、存储、使用、轮换与销毁应受控并可审计；密钥应与数据存储分离管理，避免密钥与密文同域同权限存放。

密钥访问应实施最小授权，高权限密钥操作应双人复核或分级审批。

7.4 完整性校验与版本控制

应对关键数据对象建立完整性校验机制，宜采用哈希校验、校验码或签名等方式，对数据入湖/入仓、ETL处理、发布共享、备份恢复等关键节点进行校验。

会计信息在加工处理过程中应保留版本信息，应记录加工规则、作业版本、输入输出血缘与参数信息；对关键报表口径与指标计算规则变更，应保留版本与说明，确保历史可解释。

对需更正的会计信息应采用“更正/作废+重发”机制，不应覆盖删除原数据；应保留更正依据、审批记录与前后版本关联。

7.5 不可变存储与防删除控制

对具有凭证效力、审计取证价值或监管要求的关键会计信息，宜采用不可变存储或等效机制（如WORM、对象锁定、不可变快照等），防止未授权删除与篡改。

应控制删除权限与删除流程，关键数据删除应履行审批并进行审计记录；对批量删除、策略性清理等操作应设置强控制与事后复核。

7.6 脱敏与匿名化保护

在测试、开发、数据分析、共享接口与报表展示等非必要场景，应对敏感字段实施脱敏或匿名化处理。

脱敏策略应与数据分级分类联动，应支持字段级、结果集级与动态脱敏，并应记录脱敏策略版本与变更记录；不得以关闭脱敏策略替代授权控制。

8 数据共享与接口安全要求

8.1 一般要求

会计信息在大数据环境下的共享与接口服务应遵循“最小范围、最小字段、最小权限、最短时限、全程审计”的原则，应在满足业务需要的前提下控制共享边界，防止超范围共享与二次扩散。

共享与接口应与数据分级分类联动，对高等级会计信息应实施更严格的审批、加密、脱敏、限流与审计措施。

8.2 共享范围界定与审批

应建立会计信息共享目录与共享审批机制，应明确共享数据集、共享字段、用途、接收方、共享方式、保存期限与责任人。

跨部门、跨系统、跨组织共享会计信息前应开展风险评估，评估内容至少应包括合规约束、数据敏感等级、接收方安全能力、共享必要性与替代方案。

对涉及个人信息、薪酬、资金交易明细、成本价格等高敏感内容的共享，应优先采用脱敏、聚合统计或授权查询方式，不宜以明细数据全量共享方式实现。

8.3 数据服务网关与统一出口

会计信息数据服务宜通过数据服务网关或等效机制统一对外提供，应集中实施身份鉴别、鉴权、签名校验、限流熔断、审计记录与异常检测。

应避免绕过网关的直连访问，不应以共享存储目录、临时文件交换等不可控方式作为常态共享手段；确需采用文件交换的，应执行加密、审批与留存管理，并记录全链路。

8.4 接口鉴权与安全传输

接口应采用强鉴权机制，至少应支持令牌、密钥、证书或等效方式，并应绑定调用主体、调用范围与有效期。

接口调用宜采用加密通道，对高等级会计信息接口应采用双向鉴别或等效强校验，并防止重放与伪造。

接口密钥与令牌应纳入密钥管理体系，应定期轮换并可追溯；密钥泄露或疑似泄露时应立即吊销并更换。

8.5 字段级控制、脱敏与数据最小化

接口应支持字段级控制，应限制仅返回业务所需字段；对敏感字段应采用动态脱敏、静态脱敏或结果集脱敏。

对外提供的数据服务应优先提供聚合、统计、指标型服务，减少明细数据暴露；确需提供明细数据的，应明确用途与范围，并对下载、缓存与再分发进行控制。

共享数据应明确可用期限与回收机制，对临时共享应设置到期自动失效策略。

8.6 限流、配额与异常防护

应对接口调用设置限流与配额策略，应对高频查询、批量分页拉取、异常聚合与可疑扫描行为进行控制并触发告警。

应对接口异常返回、鉴权失败、参数异常、调用范围异常等进行监测与处置；对疑似数据爬取、批量导出或撞库等行为应执行阻断或升级处置。

对面向互联网或外部网络开放的接口，应加强边界防护与攻击防护，并进行定期安全测试。

9 日志审计与安全监测要求

9.1 一般要求

应建立覆盖会计信息全链路的日志审计体系，应实现“可记录、可留存、可检索、可分析、可追溯”，并支撑安全事件调查取证与责任界定。

安全监测应与日志审计联动，应对异常访问、异常导出、异常接口调用、异常权限变更、异常作业调度与异常数据变更等行为进行检测、告警与处置闭环。

9.2 审计范围与日志要素

审计范围至少应包括：

a）身份认证与登录：登录成功/失败、异常登录、会话创建与终止；

b）权限与配置：角色变更、授权变更、策略变更、脱敏规则变更、密钥变更；

c）数据访问与操作：查询、下载、导出、共享、删除/作废、更正、批量操作；

d）数据处理作业：ETL/ELT作业调度、作业版本、参数变更、作业失败与重跑；

e）接口调用：调用主体、调用范围、请求参数摘要、返回结果状态、异常信息；

f）备份与恢复：备份执行、校验结果、恢复申请与实施、恢复后验证。

审计日志应至少包含操作者标识、时间、来源、对象、动作、结果、影响范围等要素；对关键操作宜记录前后差异信息或引用信息。

9.3 日志留存与防篡改

审计日志应集中管理并按规定留存，留存期限应满足合规与追溯要求。

审计日志应采取防篡改措施或等效控制，宜采用只写存储、不可变快照、签名校验或集中审计平台固化等方式。

应限制日志访问权限，日志查询与导出应受控并纳入审计；不得由被审计对象自行管理全部审计日志权限。

9.4 安全监测与告警规则

应建立安全监测指标与告警规则，至少应覆盖：

a）异常登录与认证失败异常；

b）高等级会计信息的异常访问、异常字段访问与异常时间访问；

c）大规模导出、批量下载、接口高频拉取与可疑爬取；

d）权限提升、特权账号启用与异常权限变更；

e）脱敏策略关闭、加密策略变更、密钥异常访问；

f）作业链路异常、数据量突变、校验失败与血缘异常。

告警应分级分类管理，应明确响应时限、处置责任人与升级机制；重大告警应触发应急响应流程并保留处置证据。

9.5 安全运营与审计复核

应定期开展审计复核与安全运营分析，应形成周期性报告，报告至少应包含告警统计、风险趋势、整改闭环与改进建议。

对重复发生的异常或重大事件，应开展根因分析并制定纠正与预防措施，必要时调整策略、加固系统或优化流程。

宜建立安全基线核查机制，对关键配置漂移、异常开放权限与不合规接口进行持续检查。

10 备份恢复与业务连续要求

10.1 一般要求

会计信息系统与大数据平台应建立备份恢复与业务连续保障机制，应确保发生系统故障、误操作、恶意攻击、勒索软件或灾害事件时，会计信息能够在规定时间内恢复可用，并保持完整性与可追溯性。

备份恢复策略应与数据分级分类联动，应对关键会计信息、关键数据资产与关键配置数据设置更严格的备份频率、保留周期与恢复目标。

10.2 恢复目标与分级保障

应明确恢复时间目标与恢复点目标，并在制度或预案中固化。对影响财务核算、资金支付、税务申报、合并报表与监管报送等关键业务的数据与系统，应设置更高保障等级。

恢复目标应可验证，应通过定期恢复演练或抽样恢复验证其可达成性；当系统架构、数据规模或业务要求发生变化时，应及时调整恢复目标并重新验证。

10.3 备份范围与备份对象

备份范围至少应包括：

a）会计信息数据资产：数据湖/仓中的核心数据集、关键主题域与关键指标数据；

b）元数据与治理信息：数据目录、血缘关系、标签与分级分类信息、脱敏规则、数据质量规则；

c）平台配置与安全策略：身份与权限配置、审计策略、密钥配置引用信息（不应备份明文密钥）、接口配置与网关策略；

d）作业与模型：ETL/ELT作业脚本、调度配置、参数与版本信息；

e）审计日志与安全监测数据：关键日志的集中存储与不可变留存。

备份应保证“数据+元数据+配置+规则”可协同恢复，避免出现数据恢复但不可检索、不可追溯或无法按原口径计算的问题。

10.4 备份策略与不可变备份

备份策略可采用全量备份、增量备份、快照、复制与其组合。对关键会计信息应采用“本地多副本+异地副本”的多层保护，并宜具备离线或隔离副本。

为防范勒索软件与恶意删除风险，对关键会计信息与关键审计日志宜采用不可变备份或等效控制（如对象锁定、不可变快照、WORM介质等），并设置保留期限与访问隔离策略。

备份数据的访问应受控，备份介质与备份存储应与生产环境进行权限隔离，避免同一特权账号同时掌握生产删除与备份删除权限。

10.5 恢复流程与恢复后验证

应建立恢复申请、审批、实施与验证流程。恢复实施前应确认恢复源有效、版本正确、校验信息齐全；恢复过程中应记录关键操作、参数与异常信息。

恢复完成后应进行恢复后验证，验证至少应包括：数据可读取、口径可计算、元数据可检索、血缘与标签可用、权限与脱敏策略生效、关键审计链完整。

恢复验证不通过时，应启动问题处置与复验，必要时升级应急响应并进行根因分析。

10.6 恢复演练与持续优化

应定期开展恢复演练或抽样恢复验证，演练应覆盖关键数据资产、关键作业链路与关键共享接口。

演练应形成记录与报告，报告至少应包含演练范围、步骤、耗时、问题清单与整改措施；整改应闭环并复核。

应基于演练结果持续优化备份频率、保留周期、隔离策略与恢复流程，确保恢复能力随数据规模与业务变化同步提升。

11 第三方与供应链安全要求

11.1 一般要求

涉及云服务商、大数据平台供应商、外包运维单位、接口合作方、审计机构等第三方参与会计信息处理活动的，应建立第三方安全管理机制，应明确数据边界、责任界面与安全要求。

第三方安全管理应贯穿准入、合同约束、实施控制、持续监督与退出处置全过程，防止因供应链薄弱环节导致会计信息泄露、篡改或不可用。

11.2 准入评估与合同约束

引入第三方前应进行安全评估，评估内容至少应包括其安全管理体系、人员管理、技术能力、合规资质、历史安全事件与应急响应能力。

合同或协议中应明确：数据使用目的与范围、数据分级分类要求、访问控制与审计要求、加密与密钥管理要求、日志留存与取证配合、分包限制、数据保留与销毁要求、违规责任与赔偿条款等。

对涉及高等级会计信息处理的第三方，应加严准入要求并设置更严格的监督与审计条款。

11.3 第三方访问控制与运维管理

第三方访问应实行最小授权与临时授权，应设置有效期并实现到期自动回收。第三方远程运维应通过受控通道进行并实施强认证与全程审计。

第三方不应直接持有或长期保管明文密钥、管理员口令等敏感凭据；确需使用的，应采用堡垒机、受控凭据托管或等效手段，并记录访问全过程。

第三方运维操作应执行变更管理，应在受控窗口内实施并保留回退方案；重大操作应双人复核或现场监督。

11.4 供应链风险监测与退出管理

应对第三方服务持续监测其安全状态，至少应关注漏洞通报、配置变更、异常访问与安全事件。

第三方退出或合同终止时，应执行数据与权限清理，应回收账号、撤销接口凭据、归还或销毁数据副本，并形成退出验收记录。

对委托处理形成的成果数据与日志证据，应按要求移交并保证可追溯。

12　安全事件响应与持续改进

12.1　一般要求

应建立会计信息安全事件响应机制，应覆盖发现、研判、处置、恢复、通报与复盘全过程，并与组织整体应急预案衔接。

安全事件响应应以保护会计信息资产与业务连续为目标，应确保处置过程可追溯、证据可保全、责任可界定。

12.2　事件分级与响应流程

应建立事件分级标准，至少应依据影响范围、数据等级、业务影响与可控性进行分级。

应明确响应流程与责任分工，包括告警确认、影响评估、隔离与止损、取证与日志固化、恢复与验证、通报与整改等环节。

涉及高等级会计信息泄露、篡改或不可用的重大事件，应启动升级响应并按组织要求进行通报与联动处置。

12.3　证据保全与取证支持

事件处置应优先保证证据保全，应对关键日志、接口调用记录、权限变更记录、作业调度记录与数据版本链进行固化，防止证据被覆盖或篡改。

取证过程中应控制人员范围与操作权限，应记录取证人员、时间、对象与方法，确保取证链条可追溯。

12.4　整改闭环与持续改进

事件处置结束后应开展复盘与根因分析，应形成整改计划并闭环验证。

应将复盘结论用于优化分级分类规则、访问控制策略、监测告警规则、备份恢复策略与第三方管理要求。

应定期开展安全培训与演练，提升人员对会计信息安全风险的识别与处置能力。