ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL 000—2025

计算中心数据隐私保护与安全管理体系标准

Standards for Data Privacy Protection and Security Management System of Computing Centers（意见征集稿）

2025 - - 发布　　2025 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

计算中心数据隐私保护与安全管理体系标准

一、范围

本标准规定了计算中心数据隐私保护与安全管理体系的建立、实施、维护和持续改进的要求和指南，适用于广西产学研科学研究院计算中心及相关数据处理活动。本标准旨在帮助计算中心满足国家相关法律法规要求，保护数据隐私和安全，增强数据主体的信任。

本标准适用于以下具体场景和要求：

1. **数据全生命周期安全管理：**涵盖数据的采集、存储、使用、传输、共享、销毁等全生命周期的安全管理，确保数据在各个阶段的保密性、完整性和可用性。

2. **数据分类分级保护：**根据数据的敏感程度和重要性，对数据进行分类分级，并采取相应的安全保护措施。

3. **数据访问控制：**明确对客户数据的访问流程，建立访问控制策略，配备技术措施防范客户数据未授权访问等安全风险。

4. **数据存储与计算安全：**提供容灾备份、校验技术、密码技术等数据安全保护能力，配备存储和计算资源监控技术能力，及时发现预警存储和计算资源异常使用情形。

5. **数据传输安全：**提供数据加密、接口鉴权、安全审计等保护措施，加强数据安全风险监测预警，提供数据流量异常、违规导出等安全风险的发现、告警与处置能力。

6. **安全事件监测与应急处置：**建立网络安全事件分析策略，明确安全事件分析的对象和流程，对网络遭受攻击的事件进行分析，并对安全事件进行分类分级。

7. **组织与人员管理：**明确数据安全负责人和管理部门，设立数据安全管理岗位并明确岗位职责，配备相应人员，统筹负责客户数据处理活动安全管理。

通过本标准的实施，旨在提升计算中心的数据隐私保护和安全管理水平，确保数据在法律框架内的

合规使用，同时增强用户对计算中心数据处理活动的信任度。

二、规范性引用文件

本标准引用了以下文件：

- GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》
- GB/T 35273—2020《信息安全技术 个人信息安全规范》
- GB/T 39568—2020《信息安全技术 数据出境安全评估指南》
- ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 信息安全管理体系 要求》
- ISO/IEC 27701:2019《信息安全、网络安全和隐私保护 隐私信息管理体系 要求与指南》

三、术语和定义

- 数据隐私：指数据主体对其个人信息的控制权和保密权。
- 数据安全：指数据的保密性、完整性和可用性得到保障，免受未经授权的访问、泄露、篡改或破坏。
- 个人可识别信息（PII）：可用于识别个人身份的信息。
- PII 控制者：确定处理 PII 的目的和手段的组织。
- PII 处理者：代表 PII 控制者处理 PII 的组织。

四、数据隐私保护与安全管理体系要求

1. 管理职责

- 最高管理层承诺：最高管理层应制定并发布数据隐私保护与安全方针，明确数据隐私保护与安全目标，并确保资源的合理分配。

• 职责分配：明确各部门和人员在数据隐私保护与安全管理体系中的职责和权限，确保责任落实到人。

2. 风险评估

• 风险识别：识别与数据隐私和安全相关的风险，包括数据泄露、篡改、丢失等风险。

• 风险分析与评估：评估风险的可能性和影响程度，确定风险等级。

• 风险处理：根据风险评估结果，制定风险处理计划，采取相应的风险控制措施。

3. 数据分类分级

• 分类分级原则：根据数据的敏感程度、重要性等进行分类分级，明确不同类别和级别的数据保护要求。

• 分类分级实施：建立数据分类分级管理制度，对数据进行标识和管理。

4. 数据访问控制

• 访问控制策略：制定数据访问控制策略，明确数据访问的权限和流程。

• 身份认证与授权：采用身份认证和授权机制，确保只有授权人员才能访问相关数据。

• 访问审计：记录数据访问行为，定期进行审计，发现异常及时处理。

5. 数据加密与脱敏

• 数据加密：对敏感数据进行加密处理，确保数据在存储和传输过程中的保密性。

- 数据脱敏：对需要共享或对外提供的数据进行脱敏处理，防止数据泄露。

6. 数据存储与备份

- 存储安全：采用安全的存储技术，确保数据存储的完整性和可用性。
- 备份与恢复：制定数据备份计划，定期进行数据备份，并确保数据能够快速恢复。

7. 数据传输安全

- 加密传输：采用加密技术确保数据在传输过程中的保密性。
- 传输完整性：采取措施确保数据在传输过程中的完整性，防止数据被篡改。

8. 数据共享与交换安全

- 共享安全：制定数据共享安全策略，明确数据共享的条件和流程。
- 交换安全：采用安全的交换技术，确保数据在交换过程中的安全。

9. 数据销毁与清除

- 销毁策略：制定数据销毁策略，明确数据销毁的条件和流程。
- 清除措施：采用安全的清除技术，确保数据被彻底清除，无法恢复。

10. 安全事件管理

• 事件监测与预警：建立安全事件监测与预警机制，及时发现并处理安全事件。

• 事件响应与处置：制定安全事件响应与处置流程，确保在发生安全事件时能够快速响应并有效处置。

• 事件记录与分析：记录安全事件的相关信息，定期进行分析，总结经验教训。

11. 安全培训与意识提升

• 培训计划：制定全面的安全培训计划，涵盖数据隐私保护、数据安全法律法规、安全操作规程等内容。培训计划应明确培训对象、内容、时间、方式及考核标准。

• 新员工入职培训：新员工入职时，必须接受数据隐私与安全培训，了解企业的数据安全政策、流程和自身安全责任。

• 定期培训与更新：定期组织员工参加数据安全培训，至少每年一次。培训内容应根据最新的法律法规、技术发展和企业内部安全需求进行更新。

• 管理层培训：对管理层进行专门的数据安全培训，使其了解数据安全对企业运营的重要性，并能够有效领导和推动数据安全管理工作。

• 意识提升活动：通过内部宣传、安全竞赛、模拟攻击演练等方式，提升员工的数据安全意识，营造良好的安全文化氛围。

• 考核与反馈：对培训效果进行考核，确保员工掌握必要的数据安全知识和技能。同时，收集员工对培训的反馈意见，持续改进培训内容和方式。

12. 第三方管理

• 第三方评估与准入：对与计算中心合作的第三方供应商和服务提供商进行严格的安全评估，确保其具备足够的数据安全能力和合规性。

• 合同与协议：与第三方签订合同时，明确数据安全责任和义务，要求其遵守计算中心的数据隐私保护与安全管理体系标准。

• 监督与审计：定期对第三方的数据处理活动进行监督和审计，确保其按照合同要求和安全标准执行。

• 违规处理：对于违反数据安全协议的第三方，采取警告、罚款、终止合作等处罚措施，并要求其对造成的损失进行赔偿。

• 应急响应协同：与第三方建立应急响应协同机制，确保在发生数据安全事件时能够快速联动，共同应对。

13. 法律法规遵从性

• 法律法规识别：定期识别和更新与数据隐私保护和安全相关的法律法规，确保计算中心的活动符合国家、地方及行业的要求。

• 合规性评估：定期进行合规性评估，检查数据隐私保护与安全管理体系是否满足法律法规的要求，及时发现并纠正不符合项。

• 法律咨询与培训：定期邀请法律专家进行培训和咨询，提高员工对数据安全法律法规的理解和应用能力。

• 政策与标准更新：关注国家和行业发布的最新数据安全政策、标准和技术指南，及时将其纳入管理体系。

14. 持续改进

• 管理体系评审：定期对数据隐私保护与安全管理体系进行全面评审，评估体系的有效性、适用性和充分性。评审频率应不少于每年一次。

• 改进措施制定：根据评审结果，制定并实施改进措施，明确责任人、完成时间和预期效果。

• 技术与管理创新：鼓励采用新技术、新方法提升数据隐私保护和安全管理水平，如隐私增强技术、

人工智能安全监测等。

• 绩效指标与考核：建立数据隐私保护与安全绩效指标，对管理体系的运行效果进行量化考核。将考核结果纳入员工和部门的绩效评价体系。

五、技术与管理措施

1. 数据加密与脱敏

• 数据加密：对敏感数据采用 AES 对称加密算法进行加密，确保数据在存储和传输过程中的保密性。

• 数据脱敏：对需要共享或对外提供的数据进行脱敏处理，防止数据泄露。

2. 数据存储与备份

• 存储安全：采用双机冗余热备方案，确保数据存储的完整性和可用性。

• 备份与恢复：定期备份数据至异地服务器，确保在发生重大灾难时能够快速恢复数据。

3. 数据访问控制

• 访问控制策略：制定数据访问控制策略，明确数据访问的权限和流程。

• 身份认证与授权：采用多因素认证机制，确保只有授权人员才能访问相关数据。

• 访问审计：记录数据访问行为，定期进行审计，发现异常及时处理。

4. 数据传输安全

- 加密传输：采用加密技术确保数据在传输过程中的保密性。
- 传输完整性：采取措施确保数据在传输过程中的完整性，防止数据被篡改。

5. 数据共享与交换安全

- 共享安全：制定数据共享安全策略，明确数据共享的条件和流程。
- 交换安全：采用安全的交换技术，确保数据在交换过程中的安全。

6. 数据销毁与清除

- 销毁策略：制定数据销毁策略，明确数据销毁的条件和流程。
- 清除措施：采用安全的清除技术，确保数据被彻底清除，无法恢复。

7. 安全事件管理

- 事件监测与预警：建立安全事件监测与预警机制，利用技术手段实时监测数据访问、存储、传输等环节的异常行为，及时发现潜在的安全事件。
- 应急预案制定：制定详细的安全事件应急预案，明确事件分级、应急响应流程、责任分工、应急资源调配等内容。
- 应急响应团队：组建专业的应急响应团队，具备快速响应和处理各类数据安全事件的能力。
- 应急演练：定期开展安全事件应急演练，检验应急预案的有效性和应急响应团队的协同作战能力。
- 事件报告与处置：在发生安全事件时，按照应急预案要求及时报告事件情况，并采取有效的处置措施。

• 事件记录与分析：对安全事件进行详细记录，事后进行深入分析，总结经验教训。

六、附则

• 标准生效日期：本标准自发布之日起生效。

• 标准解释权：本标准由广西产学研科学研究院负责解释。

• 标准修订：本标准将根据国家法律法规的变化、技术发展以及计算中心的实际运行情况进行定期修订。