ICS 17.220.20
CCS X 04

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXX—XXXX

电力用户信息采集安全技术规范

Technical specification for security of power user information collection

征求意见稿

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国商业企业管理协会　　发 布

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。

本文件由国网湖北省电力有限公司信息通信公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：国网湖北省电力有限公司信息通信公司、XXX、XXX。

本文件主要起草人：XXX、XXX、XXX。

电力用户信息采集安全技术规范

1 范围

本文件规定了电力用户信息采集安全总则、信息采集的安全技术要求、系统安全管理要求、安全测试与验收以及安全评估与改进。

本文件适用于电力用户信息采集过程的设计、开发、实施和维护，覆盖电力用户信息从采集到存储、传输、处理的整个生命周期。

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 17215.303-2022 交流电测量设备 特殊要求 第3部分：数字化电能表

GB/T 17215.701-2011 标准电能表

GB/T 28452-2012 信息安全技术 应用软件系统通用安全技术要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南

GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息采集

通过技术手段从电力用户终端设备获取用电数据和相关信息的过程，包括数据的获取、传输、存储和处理。

3.2

身份认证

验证用户身份的过程，确保访问系统的用户是被授权的。常见的身份认证方法包括密码认证、生物特征认证（如指纹、虹膜）、智能卡认证等。

4 安全总则

4.1 基本要求

4.1.1 应确保只有被授权的人员才能访问和处理电力用户信息。

4.1.2 应确保电力用户信息在传输、存储和处理过程中不被篡改或破坏。

4.1.3 应保证电力用户信息的准确和完整，防止数据被篡改、删除或添加未经授权的内容。

4.2 基本原则

4.2.1 系统应确保用户仅具有完成其工作所需的最小权限，以减少因权限过大带来的安全风险。

4.2.2 系统应采用多层次、多维度的安全防护措施，覆盖信息采集、传输、存储和处理的各个环节。

4.2.3 系统应具备动态防御能力，能够及时检测和响应新的安全威胁和攻击行为，不断更新和改进安全措施。

4.3 基本安全策略

4.3.1 明确系统的安全保护目标，确保信息的机密性、完整性和可用性。

4.3.2 规定系统在信息采集、传输、存储和处理各环节应采取的安全技术和管理措施。
4.3.3 制定安全事件的应急响应预案，确保在发生安全事件时能够及时有效地处理和恢复系统。

5 信息采集安全技术要求

5.1 数据采集安全

5.1.1 采集设备认证

5.1.1.1 采集设备应符合 GB/T 17215.701-2011 以及 GB/T 17215.303-2022 的规定。
5.1.1.2 对设备的生产厂商和供应商进行资格审查，保证设备来源的可靠性。

5.1.2 采集权限控制

5.1.2.1 明确规定采集人员和系统的采集权限，按照最小权限原则进行授权。
5.1.2.2 对权限的变更和调整进行严格的审批流程。

5.1.3 加密传输

5.1.3.1 数据传输应符合 GB/T 37025-2018 第 7 章的规定。
5.1.3.2 数据采集设备与数据中心之间的通信应采用加密传输,防止数据在传输过程中被窃取或篡改。

5.1.4 身份认证

数据采集设备应进行身份认证，确保只有合法设备能够接入系统进行数据传输。

5.1.5 数据完整性

采集的数据应进行完整性校验，防止数据在传输过程中被篡改。

5.2 数据传输安全

5.2.1 网络隔离

数据传输网络应与其他网络进行隔离，防止外部网络对数据传输的干扰和攻击。

5.2.2 入侵检测

在数据传输网络中部署入侵检测系统（IDS），实时监控网络流量，识别和响应潜在的安全威胁和攻击行为。

5.2.3 访问控制

对数据传输网络的访问进行严格控制，确保只有授权的设备和人员才能访问数据传输网络。

5.3 数据存储安全

5.3.1 数据加密

存储在数据中心的用户数据应进行加密保护，防止数据泄露。。

5.3.2 备份恢复

定期对数据进行备份，并制定数据恢复计划，确保在数据损坏或丢失时能够及时恢复数据。

5.3.3 权限管理

对存储数据的访问进行严格的权限管理，确保只有被授权的人员才能访问和处理数据。

5.4 数据处理安全

5.4.1 安全审计

对数据处理过程进行安全审计，记录数据处理操作日志，定期检查和分析，发现和处理异常行为。

5.4.2 隐私保护

数据安全应符合GB/T 35273-2020第4章的规定，在数据处理过程中采取措施保护用户隐私，避免敏感信息泄露。

5.4.3 数据销毁

对不再需要的数据进行安全销毁，确保数据无法被恢复。

5.5 系统管理安全

5.5.1 安全策略

制定并实施系统安全策略，包括密码策略、访问控制策略、安全更新策略等，确保系统的安全运行。

5.5.2 应急响应

建立安全事件应急响应机制，制定应急响应预案，确保在发生安全事件时能够及时有效地处理和恢复系统。

5.5.3 安全培训

对系统管理人员进行定期的安全培训，提高其安全意识和技能，确保安全措施的有效实施。

6 信息采集系统安全管理

6.1 安全管理体系

6.1.1 建立专门的安全管理组织，明确各级管理人员和技术人员的职责和权限。
6.1.2 制定并实施信息安全管理制度，包括安全策略、操作规程和应急预案等，确保各项安全措施的落实。
6.1.3 定期评估安全管理体系的有效性，及时更新和改进管理措施。

6.2 安全策略与政策

6.2.1 应制定信息采集系统的安全策略，涵盖数据保护、访问控制、网络安全等方面。
6.2.2 严格执行安全策略和政策，确保各项安全措施在系统各个环节的落实。

6.3 访问控制管理

6.3.1 建立健全用户身份管理制度，确保用户身份的唯一性和可追溯性。采用多因素认证方式，提高用户身份认证的安全性。
6.3.2 对系统的访问权限进行严格管理，采用基于角色的访问控制（RBAC），确保用户只能访问与其职责相关的系统资源。
6.3.3 对用户的访问行为进行全面审计，记录访问日志，定期分析和评估，发现异常行为并及时处理。

6.4 安全监控与审计

6.4.1 部署安全监控系统，实时监控系统的运行状态和网络流量，发现并预警潜在的安全威胁。
6.4.2 对系统各类日志进行集中管理和分析，发现并处理异常事件。日志应保存一定时间，满足法规和审计要求。
6.4.3 定期进行安全审计，检查系统的安全措施落实情况和安全事件处理效果，评估系统的安全风险。

6.5 安全培训与意识提升

6.5.1 对系统管理人员和技术人员进行定期的安全培训，提高其安全意识和技能水平。
6.5.2 定期组织安全演练，模拟安全事件的应急响应，提高人员的应急处理能力。

7 信息采集系统安全测试及验收

7.1 安全测试内容

7.1.1 对系统进行全面的漏洞扫描，发现并修复安全漏洞，确保系统无已知漏洞。
7.1.2 模拟攻击者的行为，对系统进行渗透测试，发现潜在的安全漏洞和弱点，提出改进建议。
7.1.3 对系统的源代码进行安全审计，发现并修复代码中的安全漏洞和不安全的编程习惯。
7.1.4 检查系统的配置是否符合安全策略和标准，确保系统配置的安全性和合理性。

7.2 安全测试方法

7.2.1 在不知晓系统内部结构的情况下，对系统进行测试，模拟外部攻击者的行为，发现安全漏洞。
7.2.2 在了解系统内部结构的情况下，对系统进行测试，全面检查系统的安全性。
7.2.3 结合黑盒和白盒测试的方法，既从外部进行攻击模拟，又从内部进行详细检查。

7.3 安全测试工具

7.3.1 使用专业的漏洞扫描工具，对系统进行全面的漏洞扫描。
7.3.2 使用渗透测试工具，模拟攻击者的行为，对系统进行深入测试。
7.3.3 使用代码审计工具，对系统源代码进行安全审计。
7.3.4 使用配置检查工具，自动检查系统配置的安全性和合理性。

7.4 安全测试报告

7.4.1 应详细记录安全测试的结果，包括发现的漏洞、风险评估和改进建议，并根据测试结果，制定并实施相应的整改措施，修复发现的安全漏洞和弱点。
7.4.2 编写安全测试验收报告，记录测试过程、结果和整改情况，提交给相关管理部门审核。

7.5 安全验收流程

7.5.1 在安全测试完成后，进行初步验收，检查测试结果和整改措施的落实情况。
7.5.2 由独立的第三方或内部审计部门进行正式验收，审核系统的安全性和稳定性。
7.5.3 在验收合格后，签发系统安全验收合格证书，系统可以正式投入运行。
7.5.4 系统上线后，持续进行安全监控和定期安全测试，确保系统的长期安全性和稳定性。

8 安全评估与改进

8.1 安全评估概述

8.1.1 应识别系统存在的安全风险，评估系统的安全状态，提出改进建议，确保系统的安全性和稳定性。
8.1.2 根据系统的重要性和风险级别，制定安全评估的周期，确保及时发现和处理安全隐患。

8.2 安全评估方法

8.2.1 定期进行漏洞扫描和渗透测试，发现并修复系统中的安全漏洞，降低系统被攻击的风险。
8.2.2 检查系统的安全策略和措施是否符合应符合 GB/T 28452-2012 中第 8 章的要求。

8.3 安全评估工具

8.3.1 使用自动化漏洞扫描工具和风险评估工具，提高评估的效率和准确性。
8.3.2 结合专家经验进行手工评估，识别自动化工具无法发现的复杂安全问题。
8.3.3 邀请独立的第三方安全机构进行评估，提供客观、公正的评估结果。

8.4 安全评估报告

8.4.1 应详细记录安全评估的过程和结果，包括发现的安全问题、风险评估和改进建议。
8.4.2 对发现的安全问题进行分类和分级，明确其严重程度和处理优先级。
8.4.3 根据评估报告，制定详细的整改计划，明确整改措施、责任人和完成时间。

8.5 安全改进措施

8.5.1 及时修复评估中发现的安全漏洞，采用补丁管理、配置加固等措施，提升系统的安全性。
8.5.2 根据评估结果，优化系统的安全策略和措施，确保其有效性和适应性。
8.5.3 根据评估中发现的潜在威胁，更新应急预案，确保在安全事件发生时能够迅速响应和处理。
8.5.4 加强对系统管理人员和用户的安全培训，提高其安全意识和应对能力。

8.6 持续改进机制

8.6.1 应依据 GB/T 36626-2018 第 5 章的规定，建立系统的安全运维体系，并收集安全评估和事件处理的反馈意见，不断改进安全管理措施，提升系统的整体安全性。
8.6.2 应依据 GB/T 36626-2018 第 8 章的规定，建立应用软件系统的安全运维规程。持续监控系统的安全状态，及时发现和处理安全问题。
8.6.3 通过定期的安全评估和持续的安全改进，电力用户信息采集系统可以有效地防范和应对各种安全威胁，确保系统的长期安全性和稳定性。