奥邦检验认证集团有限公司企业标准

CTS_ABG 67011-2024

电信组织信息安全管理体系 要求

Information technology - Security techniques -
Telecommunication organization information security management systems - Requirements

2024-06-28 发布　　2024-06-28 实施

奥邦检验认证集团有限公司发布

目录

前 言

本文件按照 GB/T1.1—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。

本文件规定了电信组织信息安全管理体系的要求，旨在指导电信组织（涵盖基础电信运营商、虚拟运营商、电信设备制造商、电信服务提供商等领域）建立、实施、维护和持续改进信息安全管理体系，确保电信设施运行、服务交付及相关信息（含通信内容、用户数据、网络配置数据等）全生命周期的机密性、完整性和可用性，满足行业合规要求与关键通信基础设施风险管控需求。

本文件由奥邦检验认证集团有限公司技术部提出并起草。

本文件主要起草人：袁海、邵优良。

本文件由奥邦检验认证集团有限公司 2024 年 06 月 28 日批准。

本文件自 2024 年 06 月 28 日起实施。

本文件由奥邦检验认证集团有限公司负责解释。

电信组织信息安全管理体系 - 要求

1 范围

本文件规定了在电信组织范围内建立、实施、维护和持续改进信息安全管理体系的要求，包括针对电信行业关键信息（涵盖通信内容数据、用户身份信息、网络拓扑数据、设备配置数据、应急通信方案等）全生命周期（收集、存储、传输、处理、共享、销毁）的风险评估、安全控制及合规管理。

本文件适用于所有从事电信行业相关业务的组织，包括基础电信运营商（如移动通信、固定通信运营商）、虚拟网络运营商（MVNO）、电信设备研发制造企业、电信服务提供商（如云计算服务、增值电信服务企业），以及为电信行业提供技术支持的供应链合作方（如网络设备供应商、远程运维服务商、软件系统开发商），可作为电信组织信息安全管理与认证的依据。

本文件不适用于军事通信领域的信息安全管理，该领域信息安全管理应遵循国家军事通信相关标准要求。

2 规范性引用文件

下列文件的内容通过文中的引用而构成本文件的规范性条款。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。

ISO/IEC 27011:2024《信息安全、网络安全和隐私保护-基于 ISO/IEC 27002 的电信组织信息安全控制措施》

GB/T 22080-2025《网络安全技术 信息安全管理体系 要求》（ISO/IEC 27001:2022）

GB/T 35273-2020《信息安全技术 个人信息安全规范》

ITU-T X.1051《电信组织信息安全管理指南》

IEC 62351-6《电力系统管理及其信息交换-数据和通信安全-第 6 部分：通信网络和系统安全》

3 术语和定义

3.1 电信组织信息

指与电信设施运行、服务交付及相关管理活动相关的信息，包括通信内容数据（如语音通话记录、短信内容、数据传输内容）、用户身份信息（如用户姓名、身份证号、联系方式）、网络拓扑数据（如基站位置、传输链路布局）、设备配置数据（如路由器参数、交换机配置）、应急通信方案（如灾害应急通信预案、网络中断恢复流程）等。

3.2 电信设施

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。