ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

网络信息安全漏洞检测与修复操作指南

Operation Guide for Network Information Security Vulnerability Detection and Repair

（工作组讨论稿）

（本草案完成时间：2026-4-15）

2026 - - 发布　　2026 - - 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。

网络信息安全漏洞检测与修复操作指南

1 引言

为深入贯彻落实国家网络安全战略，筑牢国家网络安全屏障，依据《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《网络安全等级保护条例》等国家法律法规及相关政策要求，结合广西产学研科学研究院在网络安全领域的研究积淀与实践经验，特制定本规范。本规范旨在建立科学、规范、可落地的网络信息安全漏洞检测与修复操作体系，统一各类组织漏洞管理的技术标准与流程规范，全面提升全社会网络安全防护能力，保障国家关键信息基础设施安全、公共利益及公民合法权益，为数字中国建设提供坚实的网络安全支撑。

2 范围

明确了网络信息安全漏洞检测与修复操作的总体要求、检测流程、分析评估、修复实施、验证确认及持续改进等全流程技术规范与管理要求，全面覆盖漏洞管理全生命周期，确保漏洞管理工作闭环可控、有据可依。适用于各类网络运营者、关键信息基础设施运营者、网络安全服务机构开展漏洞检测与修复相关活动，为其提供标准化、规范化操作指引；同时适用于网络安全主管部门开展监督检查、第三方评估机构开展符合性评价工作，为国家网络安全监管与合规治理提供技术依据，助力构建“监管有标准、运营有规范、服务有准则”的网络安全治理格局。

3 规范性引用文件

下列文件对于本规范的应用具有不可或缺的作用。凡是注日期的引用文件，仅所注日期的版本适用于本规范；凡是不注日期的引用文件，其最新版本（含所有修改单）适用于本规范，确保本规范与国家最新技术标准、合规要求保持一致。

GB/T 25069-2022 信息安全技术 术语

GB/T 30276-2020 信息安全技术网络安全漏洞管理规范

GB/T 30279-2020 信息安全技术网络安全漏洞分类分级指南

GB/T 28458-2020 信息安全技术网络安全漏洞标识与描述规范

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术网络安全等级保护测评要求

GB/T 35273-2020 信息安全技术个人信息安全规范

GB/T 20986-2023 信息安全技术网络安全事件分类分级指南

《网络安全等级保护条例》（国务院令第 751 号）

《关键信息基础设施安全保护条例》（国务院令第 745 号）

4 术语和定义

GB/T 25069-2022、GB/T 30276-2020、GB/T 30279-2020 界定的术语和定义，以及下列术语和定义，适用于本规范。本规范术语表述与国家标准保持统一，兼顾专业性与通用性，为全国范围内规范落地提供清晰支撑。

4.1 网络安全漏洞

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等全生命周期过程中，无意或有意产生的缺陷或薄弱点，该缺陷或薄弱点可能被攻击者利用，进而危害网络安全、数据安全、业务安全，甚至影响国家关键信息基础设施正常运行。

4.2 漏洞检测

依据国家相关技术标准，通过人工或自动化方式，对网络产品、系统或服务开展全面安全测试、分析与评估，识别并确认网络安全漏洞，明确漏洞基本信息与潜在风险的过程，是网络安全防护的前置关键环节，也是防范安全事件的重要基础。

4.3 漏洞修复

针对已确认的网络安全漏洞，结合国家网络安全等级保护、关键信息基础设施保护等相关要求，采取补丁更新、配置调整、架构优化、临时规避等科学有效措施，消除或降低漏洞被利用风险，保障系统安全稳定运行的过程，是筑牢网络安全防线的核心举措。

4.4 漏洞验证

对检测发现的疑似漏洞进行复现测试，确认漏洞的真实性、可触发性、危害程度及影响范围，为漏

洞分级、风险评估和修复优先级判定提供科学依据的过程，确保漏洞管理决策的准确性和针对性。

4.5 漏洞复测

漏洞修复完成后，按照国家相关技术规范，对修复措施的有效性开展再次检测，确认漏洞已成功修复且未引入新安全风险，保障漏洞修复工作落地见效，形成漏洞管理闭环的过程。

5 缩略语

本规范所用缩略语统一采用国家网络安全领域通用标准，确保跨部门、跨行业、跨区域沟通的一致性，为全国网络安全漏洞管理协同推进提供便利支撑。CVE：公共漏洞和暴露（Common Vulnerabilities and Exposures）；CVSS：通用漏洞评分系统（Common Vulnerability Scoring System）；CNNVD：中国国家网络安全漏洞库（China National Cybersecurity Vulnerability Database）；CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）；SCAP：安全内容自动化协议（Security Content Automation Protocol）

6 漏洞检测要求

漏洞检测工作须严格遵循国家网络安全相关法律法规及技术标准，坚持“全面覆盖、科学规范、精准高效、最小影响”的核心原则，确保检测工作合法合规、数据真实可靠，为漏洞管理后续各环节奠定坚实基础。

6.1 检测准备

6.1.1 检测范围确定：须明确检测对象的边界范围，全面覆盖各类关键网络资产，重点聚焦关键信息基础设施、核心业务系统及敏感数据存储载体，包括但不限于：操作系统（Windows Server 2019/2022、各类 Linux 发行版）、数据库系统（MySQL 8.0 及以上、Oracle 19c 及以上、Redis 6.x 及以上）、应用中间件（Nginx 1.20 及以上、Tomcat 9 及以上）、网络设备（路由器、交换机、防火墙）、安全设备（IDS/IPS、WAF）、工业控制系统、云平台组件及移动应用等，确保无检测盲区、无遗漏资产。

6.1.2 检测工具配置：须配备符合国家网络安全标准、具备相应资质的漏洞检测工具，确保工具的安全性、可靠性与有效性，为检测工作精准开展提供有力支撑，具体要求如下：漏洞扫描器：至少支持 CVE、CNNVD、CNVD 等主流漏洞库的检测规则，规则库更新滞后时间不超过 7 个自然日，确保能够及时检测各类新型漏洞；渗透测试工具集：涵盖网络层、系统层、应用层、移动端等各类测试工具，可

满足不同场景、不同类型漏洞的检测需求，保障检测全面性；源码审计工具：支持 Java、Python、C/C++、Go、JavaScript 等主流编程语言的代码安全检测，契合我国自主开发应用系统的安全检测需求；配置核查工具：支持等保 2.0、CIS Benchmark 等安全配置基线核查，确保检测工作符合国家网络安全等级保护相关要求，提升检测合规性。

6.1.3 授权管理：所有检测活动须严格遵循“合法授权、规范操作”的原则，提前取得被测系统所属单位的书面授权。授权文件应明确检测时间窗口（精确至小时）、检测 IP 范围、检测方式（主动扫描/被动监测/渗透测试）、紧急联系人及应急响应机制，防范检测过程对系统正常运行造成不必要影响。授权有效期不得超过 30 个自然日，确需延长的，须重新办理授权手续，确保检测活动全程合法合规、可追溯。

6.2 检测实施

6.2.1 自动化扫描：须使用合规的漏洞扫描器对目标系统开展全面扫描，扫描参数设置应科学合理，兼顾检测效果与系统运行安全，避免对业务系统造成影响，具体要求如下：扫描并发线程数不超过 50，避免对业务系统造成过大负载，保障核心业务正常运行；危险插件（如拒绝服务类、溢出类）须在业务低峰期（通常为 22:00 至次日 06:00）经审批后启用，最大限度降低对业务的影响；每次扫描须保存完整的扫描日志和原始报文，保存期限不低于 180 天，满足国家网络安全监管、审计及应急追溯需求；扫描频率：核心业务系统每月不少于 1 次，一般业务系统每季度不少于 1 次，关键信息基础设施相关系统应适当提高扫描频率，确保及时发现各类安全隐患。

6.2.2 人工渗透测试：在自动化扫描基础上，须开展专业人工渗透测试，聚焦高风险漏洞类型，重点检测以下漏洞，确保漏洞检测的全面性与精准性，有效防范新型、隐蔽性漏洞引发的安全风险：注入类漏洞（SQL 注入、命令注入、代码注入、LDAP 注入等）；跨站脚本漏洞（反射型、存储型、DOM 型）；认证与会话管理漏洞（会话劫持、会话固定、弱口令、权限绕过等）；安全配置错误（默认口令、目录列出、调试信息泄露等）；敏感数据泄露（明文传输、硬编码密钥、日志敏感信息等）；访问控制缺失（水平越权、垂直越权）；跨站请求伪造（CSRF/SSRF）；不安全的反序列化；使用含有已知漏洞的组件；业务逻辑漏洞（支付篡改、重放攻击、限额绕过等）。

6.2.3 源码安全检测：对于自主开发的应用系统，尤其是涉及关键信息基础设施、敏感数据处理的系统，须开展源码安全检测，从源头防范安全漏洞，保障系统开发安全，具体要求如下：检测覆盖率：核心模块代码覆盖率不低于 95%，一般模块不低于 85%，确保检测全面无遗漏；检测规则集：包含 OWASP Top 10、CWE Top 25 等主流安全缺陷规则，并结合我国网络安全实际需求补充定制化规则，提升检测针对性；人工审计：针对高危逻辑缺陷和密码学误用等问题，须辅以人工代码审查，提升检测精度，有

效防范技术工具检测盲区。

6.3 检测结果记录

检测结果须严格按照 GB/T 28458-2020 要求进行标识与描述，记录内容须完整、规范、可追溯，为漏洞分析评估、修复实施提供准确依据，同时满足国家网络安全监管和审计要求，具体记录内容如下：漏洞唯一标识符：遵循 CVE 或 CNNVD 命名规范，确保漏洞可精准定位、跨平台追溯；漏洞发现时间：精确至秒，明确漏洞发现节点，为修复时效管理提供准确依据；漏洞类型：按照 GB/T 30279-2020 规定的分类体系进行划分，确保分类标准统一、清晰；漏洞位置：明确资产名称、IP 地址、端口号、URL 路径、代码文件及行号，精准定位漏洞所在，便于后续修复；漏洞描述：包含触发条件、利用方法、可能造成的影响，重点说明对系统安全、数据安全及国家关键信息基础设施的潜在危害；漏洞证明：提供截图、数据包、复现步骤等支撑材料，确保漏洞真实性可验证、可追溯；检测人员信息：注明姓名、资质证书编号，明确责任主体，保障检测工作的专业性和可追溯性。

7 漏洞分析评估

漏洞分析评估须遵循国家网络安全漏洞分级标准，结合关键信息基础设施保护、网络安全等级保护等相关要求，科学分析漏洞风险，合理判定修复优先级，为漏洞修复决策提供科学、精准的依据，有效防范重大网络安全风险。

7.1 漏洞分级

须严格按照 GB/T 30279-2020 规定，结合 CVSS 3.1 评分标准，从被利用性、影响程度、波及范围等维度对漏洞进行分级。漏洞等级分为四级，明确不同等级漏洞的修复时限，确保漏洞修复工作有序推进，重点管控高风险漏洞，具体分级及要求如下：

7.1.1 超危漏洞：CVSS 3.1 评分在 9.0 至 10.0 之间。此类漏洞可被远程利用，无需用户交互即可实现系统完全控制或敏感数据泄露，可能对关键信息基础设施、公共利益造成重大危害，修复时限不超过 24 小时；

7.1.2 高危漏洞：CVSS 3.1 评分在 7.0 至 8.9 之间。此类漏洞可导致系统权限丢失、数据篡改或服务中断，可能影响核心业务正常运行，修复时限不超过 72 小时；

7.1.3 中危漏洞：CVSS 3.1 评分在 4.0 至 6.9 之间。此类漏洞可在特定条件下被利用，造成有限安全影响，修复时限不超过 15 个自然日；

7.1.4 低危漏洞：CVSS 3.1 评分在 0.1 至 3.9 之间。此类漏洞利用难度高或实际影响轻微，修复时

限不超过 30 个自然日。

7.2 影响范围评估

须从国家网络安全、公共利益、企业运营、公民权益等多维度，全面评估漏洞的影响范围，重点关注对关键信息基础设施、敏感数据的影响，为风险管控提供精准依据，具体评估内容如下：

7.2.1 业务影响：明确受影响系统的业务重要性等级（核心/重要/一般）、预计业务中断时长、数据损失量级，重点评估对关键业务、民生服务的影响程度；

7.2.2 数据影响：明确涉及的数据类型（个人信息、商业秘密、国家秘密）、数据量、数据敏感程度，严格落实数据安全保护相关要求，有效防范数据泄露、篡改风险；

7.2.3 合规影响：评估漏洞是否违反网络安全等级保护、关键信息基础设施保护、个人信息保护等法律法规要求，明确漏洞可能引发的合规风险和法律责任；

7.2.4 供应链影响：评估漏洞是否影响上下游系统、第三方服务及客户系统，防范漏洞通过供应链传导扩散，引发系统性网络安全风险。

7.3 修复优先级判定

综合考量漏洞等级、资产重要性、暴露面、已有防护措施及国家网络安全管控要求，科学确定修复优先级，实行分级分类管控，优先处置高风险漏洞，保障核心资产安全，具体优先级及要求如下：

7.3.1 P0 级（紧急修复）：超危漏洞+互联网暴露面+核心业务系统，尤其涉及关键信息基础设施的此类漏洞，须在 2 小时内启动修复，最大限度降低风险扩散；

7.3.2 P1 级（优先修复）：高危漏洞+互联网暴露面或超危漏洞+内网核心系统，须在 24 小时内启动修复，防范漏洞被利用引发安全事件；

7.3.3 P2 级（计划修复）：中危漏洞+互联网暴露面或高危漏洞+内网一般系统，须在 7 个自然日内启动修复，有序推进风险管控；

7.3.4 P3 级（例行修复）：低危漏洞或内网非核心系统漏洞，须在 30 个自然日内纳入修复计划，确保漏洞风险逐步清零。

8 漏洞修复实施

漏洞修复实施须遵循“科学合规、精准高效、最小影响、闭环管控”的原则，结合国家网络安全相关标准和要求，制定针对性修复方案，严格规范修复流程，确保修复工作落地见效，有效防范修复过程中引入新安全风险。

8.1 修复方案制定

根据漏洞类型、系统环境、资产重要性及国家合规要求，制定针对性强、可落地的修复方案，明确修复措施、责任主体、时间节点及回退方案，确保修复工作有序、高效推进。

8.1.1 补丁修复：补丁修复适用于软件产品已知漏洞，须严格遵循国家网络安全相关要求，规范补丁获取、验证、安装流程，有效防范补丁带来的兼容性和安全风险，具体要求如下：须从官方渠道获取补丁，校验数字签名和哈希值（MD5/SHA-256），确保补丁的真实性和完整性，严禁使用来源不明的补丁；补丁安装前须在测试环境中进行兼容性验证，验证内容包括功能测试、性能测试、回归测试，确保补丁不影响系统正常运行；操作系统补丁建议在发布后 15 个自然日内完成生产环境安装；应用系统补丁建议在发布后 30 个自然日内完成，关键信息基础设施相关系统须优先完成补丁安装，提升防护时效性。

8.1.2 配置加固：配置加固适用于配置类漏洞，须遵循国家网络安全等级保护、关键信息基础设施保护相关要求，按照最小权限原则开展配置加固，全面提升系统自身安全防护能力，具体要求如下：遵循最小权限原则，关闭非必要端口和服务（如 Telnet、FTP、RDP 非授权访问等），减少系统攻击面，降低被攻击风险；修改默认账户和默认口令，口令长度不低于 12 位，包含大小写字母、数字、特殊字符三类及以上，定期更换口令，有效防范弱口令攻击；启用日志审计功能，日志保存时间不低于 180 天，满足国家网络安全审计和应急追溯需求；配置访问控制策略，限制来源 IP、访问时段及操作权限，强化系统访问管控，有效防范未授权访问。

8.1.3 代码修复：代码修复适用于源码级漏洞，须结合国家网络安全相关标准和安全开发规范，从源头修复漏洞，全面提升自主开发系统的安全性，具体要求如下：输入验证：对所有外部输入进行严格的白名单验证，过滤特殊字符，有效防范注入类漏洞；参数化查询：使用预编译语句或 ORM 框架参数化接口防止 SQL 注入，规范代码开发流程，提升代码安全性；输出编码：根据输出上下文（HTML、JavaScript、CSS、URL）进行适当编码，有效防范跨站脚本漏洞；会话管理：使用安全的会话标识生成算法，设置合理的超时时间（不超过 30 分钟），强化会话安全管控；加密存储：敏感数据（口令、密钥、个人信息）须使用国密算法 SM2/SM3/SM4 或等效强度国际算法进行加密存储和传输，落实国家密码管理相关要求，切实保障数据安全。

8.1.4 临时规避措施：当无法立即实施根本性修复时，可采取临时规避措施，快速降低漏洞被利用风险，但临时措施不得替代根本性修复，具体要求如下：部署虚拟补丁（Web 应用防火墙规则、入侵防御系统签名），快速阻断漏洞利用路径，降低被攻击风险；实施网络隔离（防火墙策略、VLAN 划分），限制漏洞影响范围，防范风险扩散；启用增强监控（实时告警、流量分析、行为审计），及时发现漏洞

利用行为，做好应急处置准备；临时关闭受影响功能或服务，最大限度降低漏洞带来的安全风险。

8.2 修复过程管理

8.2.1 变更管理：漏洞修复须纳入规范的变更管理流程，严格遵循国家网络安全相关要求，规范修复操作，有效防范修复过程中引发系统故障或安全风险，具体要求如下：提交变更申请，明确修复内容、影响范围、回退方案，详细说明修复过程中的风险点及防控措施；经变更审批委员会批准后方可实施，关键信息基础设施相关系统的漏洞修复变更须提升审批层级，强化管控；修复操作须在业务低峰期进行，并提前通知相关业务部门、用户及应急联系人，做好应急准备，降低对业务的影响；记录修复操作的详细日志，包括操作时间、操作人员、操作内容、执行结果，确保修复过程可追溯，满足国家审计要求。

8.2.2 测试验证：修复实施后须在测试环境中完成全面测试验证，确保修复有效、无新增风险，验证合格后方可推进生产部署，具体要求如下：功能验证：确认受影响功能恢复正常，不影响系统核心业务运行；安全验证：确认漏洞已无法复现，修复措施有效阻断漏洞利用路径；性能验证：确认系统响应时间、吞吐量等指标退化不超过 10%，保障系统运行性能稳定；容性验证：确认修复措施未影响其他功能模块，与系统整体运行兼容。

8.2.3 生产部署：测试验证通过后，按计划有序开展生产环境部署，严格规范部署流程，有效防范部署过程中引发安全事件，具体要求如下：备份生产环境配置和数据，制定完善的回退方案，确保出现问题可快速恢复，降低损失；按照变更方案执行修复操作，严格遵循操作规范，避免人为失误；实时监控系统状态，密切关注系统运行指标和安全告警，发现问题立即启动回退方案；更新资产配置管理数据库（CMDB），确保资产信息与实际修复情况一致，为后续漏洞管理和安全管控提供支撑。

8.3 应急响应

对于 P0 级紧急修复，须严格按照国家网络安全应急响应相关要求，启动应急响应程序，快速处置漏洞风险，有效防范重大网络安全事件发生，具体要求如下：立即通知网络安全负责人和业务负责人，明确应急处置责任分工，启动应急响应流程；必要时暂停受影响系统对外服务或断开网络连接，快速阻断漏洞利用路径，防止风险扩散；在 4 小时内完成临时规避措施部署，最大限度降低漏洞带来的安全风险；在 24 小时内完成根本性修复或制定详细修复计划，明确修复时间节点和责任主体；按照《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》要求，对可能造成重大损失的漏洞事件，在 2 小时内向主管部门报告，积极配合监管部门开展处置工作。

9 漏洞复测与验证

漏洞复测与验证是确保漏洞修复成效的关键环节，须严格遵循国家相关技术标准，规范复测流程，明确验证标准，形成漏洞管理闭环，确保漏洞彻底修复、无新增风险。

9.1 复测要求

修复完成后须及时开展漏洞复测，复测工作须科学规范、精准高效，确保复测结果真实可靠，具体要求如下：复测方法须与初次检测方法一致或更为严格，确保复测的全面性和准确性；须针对原漏洞位置和关联功能进行重点测试，同时排查关联漏洞，防范漏洞遗漏；须开展回归测试，确认修复未引入新漏洞，保障系统整体安全；复测须由原检测人员或具备同等资质的人员执行，确保复测工作的专业性和客观性。

9.2 验证标准

漏洞验证通过标准须严格遵循国家网络安全相关要求，确保修复工作落地见效，具体标准如下：原漏洞已无法在相同条件下复现，漏洞利用路径被彻底阻断；未发现因修复引入的新安全缺陷，系统安全性能未受影响；系统功能正常运行，性能符合国家相关标准和业务需求；安全配置符合国家网络安全等级保护、关键信息基础设施保护等基线要求。

9.3 关闭确认

验证通过后，须按规范完成漏洞关闭确认流程，做好文档归档和信息通报，形成漏洞管理闭环，具体操作如下：在漏洞管理平台中将漏洞状态更新为“已修复”，完善漏洞管理台账，确保漏洞信息可追溯；生成漏洞修复报告，包含修复方案、验证结果、测试报告等内容，全面反映漏洞修复全过程；归档所有相关文档，保存期限不低于 3 年，重大漏洞事件相关文档保存期限不低于 5 年，满足国家审计和监管要求；若漏洞涉及第三方产品或服务，须将修复情况通报相关方，推动供应链漏洞协同治理，有效防范系统性风险。

10 持续改进

立足国家网络安全战略发展需求，结合网络安全技术发展趋势和法律法规更新情况，持续优化漏洞检测与修复体系，不断提升漏洞管理能力，筑牢国家网络安全防线，为数字中国建设提供持续保障。

10.1 漏洞数据分析

须每季度对漏洞数据进行统计分析，挖掘漏洞规律和薄弱环节，为漏洞管理优化和安全防护提升提供数据支撑，具体分析内容如下：

10.1.1 漏洞趋势分析：分析漏洞数量变化、等级分布变化、类型分布变化，精准掌握漏洞发展趋

势，提前做好防控准备；

10.1.2 修复时效分析：分析平均修复时长、超期修复比例、紧急修复次数，优化修复流程，提升修复效率；

10.1.3 根源分析：分析高频漏洞类型、高频漏洞系统、高频漏洞时段，精准定位安全防护薄弱环节，开展针对性防控工作；

10.1.4 改进方向：根据分析结果优化安全开发流程、加强薄弱环节防护、调整检测策略，全面提升整体网络安全防护水平，契合国家网络安全发展要求。

10.2 流程优化

根据漏洞管理实践、国家法律法规更新、网络安全技术发展（如云计算、人工智能、物联网等），持续优化检测与修复流程，确保流程的科学性、规范性和适用性，具体要求如下：每年至少组织一次漏洞管理流程评审，结合国家最新要求和实践经验，优化流程环节，提升管理效率；根据新技术应用（云计算、人工智能、物联网等）更新检测方法和工具，适应新型漏洞检测需求；根据新法规要求调整合规检测项，确保漏洞管理工作始终符合国家法律法规和监管要求；优化漏洞管理平台功能，提升自动化水平，推动漏洞检测、分析、修复、复测全流程自动化，提升管理效能。

10.3 人员能力建设

围绕国家网络安全人才培养要求，加强漏洞管理相关人员的能力建设，打造专业化、高素质的网络安全人才队伍，支撑漏洞管理工作高质量开展，具体要求如下：检测人员须持有 CISP、CISAW、CVE 等国家认可的安全资质证书，确保人员专业性；每年参加不低于 40 学时的网络安全技术培训，重点学习国家网络安全法律法规、新型漏洞检测与修复技术，持续提升人员专业能力；每半年组织一次漏洞检测与修复应急演练，提升人员应急处置能力，有效应对突发漏洞事件；建立漏洞挖掘与修复的技术交流机制，加强与国内网络安全机构、同行的技术交流，借鉴先进经验，提升整体技术水平，助力国家网络安全人才队伍建设。

11 文档与记录管理

文档与记录管理须严格遵循国家网络安全相关法律法规和审计要求，确保文档与记录的完整性、规范性、可追溯性，为漏洞管理、监管审计、应急追溯提供有力支撑，同时加强漏洞信息安全保护，有效防范敏感信息泄露。

11.1 文档要求

须建立并维护完善的漏洞管理文档体系，覆盖漏洞管理全生命周期，确保文档内容规范、更新及时，具体包括：漏洞检测计划与授权文件；漏洞检测原始记录与报告；漏洞风险评估报告；漏洞修复方案与变更记录；漏洞复测报告与验证记录；漏洞管理统计分析报告。

11.2 记录保存

各类记录须严格按照国家网络安全监管和审计要求保存，确保记录可追溯，保存期限满足相关法律法规要求，具体如下：漏洞检测原始数据：保存期限不低于 180 天；漏洞修复记录：保存期限不低于 3 年；重大漏洞事件处置记录：保存期限不低于 5 年；人员培训与考核记录：保存期限不低于 2 年。

11.3 信息安全

漏洞信息属于敏感信息，部分涉及国家关键信息基础设施的漏洞信息属于涉密信息，须严格按照国家信息安全和保密管理相关要求，实施严格的保护措施，有效防范信息泄露，具体要求如下：漏洞报告仅限授权人员查阅，传输须采用加密方式，确保信息传输安全；漏洞信息不得在公开渠道（论坛、社交媒体、即时通讯群组）传播，防范漏洞信息被攻击者利用；涉及关键信息基础设施的漏洞信息，须按国家有关保密规定进行管理，严格控制知悉范围，防范危害国家关键信息基础设施安全；与第三方共享漏洞信息时，须签订保密协议，明确保密责任和义务，防范漏洞信息通过第三方泄露，切实维护国家网络安全和公共利益。