济南壹软网络科技有限公司网络安全漏洞维护规则

1. 总则

1.1. 目的

为系统性地预防、发现、响应和修复本公司网络与信息系统中的安全漏洞，切实履行《中华人民共和国网络安全法》等法律法规规定的网络安全保护义务，降低安全风险，保障业务连续性，特制定本规则。

1.2. 范围

本规则适用于公司所有自建、运维或使用的网络基础设施、信息系统、服务器、终端设备及应用程序。

1.3. 原则

- 预防为主，防治结合：建立常态化安全检测与加固机制。
- 分级处置，及时响应：根据漏洞风险等级，明确修复时限与流程。
- 记录完整，可追溯可审计：全过程保留记录，形成完整证据链。
- 持续改进：定期回顾与更新本规则及安全措施。

2. 组织与职责

2.1. 网络安全负责人

- 为公司网络安全最终责任人，负责批准本规则，监督其执行，并对整体网络安全状况负责。

2.2. 技术部/运维部

- 作为本规则的主要执行部门，负责：
  - 定期执行漏洞扫描与渗透测试。
  - 对发现的漏洞进行分析、评估、修复与验证。
  - 保存和维护所有安全维护相关记录与日志。
  - 在发生安全事件时，执行应急响应流程。

2.3. 其他各部门

- 配合技术部进行与本部门相关系统的安全加固与整改工作。

3. 漏洞管理流程

3.1. 漏洞检测

- 定期扫描：技术部应至少每季度组织一次对公司全系统范围的自动化漏洞扫描。扫描工具与范围应覆盖主要资产。
- 专项检测：在以下情况发生时，应进行专项安全检测：
  - 新系统上线前或重大版本更新后。
  - 重大节假日前或有明确安全预警时。
  - 外部机构（如监管单位、第三方平台）通报漏洞时。

3.2. 漏洞评估与分级

- 对发现的漏洞，应根据其可利用性、影响范围、可能造成的危害程度，参考行业通用标准（如 CVSS 评分），进行风险评估并分级：
  - 高危：可导致系统被完全控制、核心数据泄露或服务瘫痪的漏洞。
  - 中危：可导致部分功能受损、非核心信息泄露的漏洞。
  - 低危：安全风险较低，或利用条件苛刻的漏洞。

3.3. 漏洞修复与验证

- 修复时限：
  - 高危漏洞：确认后应立即采取临时防护措施（如隔离、访问控制），原则上应在 7 个自然日内完成彻底修复。
  - 中危漏洞：应在 15 个自然日内完成修复。
  - 低危漏洞：应在下一个定期修复周期内（通常为下一季度） 安排修复。
- 修复验证：漏洞修复完成后，必须进行验证测试，确保漏洞已彻底消除，且未引入新的问题。验证结果需记录。

3.4. 应急响应

- 对于突发的、正在被利用的或外部紧急通报的“零日”高危漏洞，应立即启动应急响应流程，不受上述常规时限限制，遵循“发现 - 评估 - 处置 - 报告”的流程，优先进行遏制与修复，并按规定向有关部门报告。

4. 记录保存与管理

4.1. 必须保存的记录包括但不限于：

- 定期漏洞扫描报告原件。
- 漏洞风险评估与分级记录。
- 漏洞修复方案、操作日志、配置变更截图或代码提交记录。
- 漏洞修复验证报告。
- 安全设备（防火墙、WAF 等）的运行日志与策略变更记录。
- 本规则的培训、传达与执行情况记录。

4.2. 保存要求：

- 所有安全记录应妥善保管，确保其真实性、完整性和不可篡改性。
- 记录应至少保存 6 个月，涉及重要系统或事件的记录建议长期保存。
- 鼓励使用电子化管理系统进行存储，并做好备份。

5. 附则

5.1.

本规则经公司管理层批准后生效，自发布之日起施行。

5.2.

本规则由公司网络安全负责人负责解释与修订。

5.3.

本规则应根据法律法规、技术发展及公司业务变化进行定期评审和更新。

（公司盖章处）

发布日期：2025 年 12 月 23 日