

2025 年信息安全检查总结报告

一、检查背景与目的

1.1 检查背景

(1) 随着信息技术的高速发展,信息安全已经成为国家、企业和个人关注的焦点。在数字化、网络化的今天,信息安全风险无处不在,对国家安全、社会稳定和人民群众的切身利益产生了重大影响。为了有效防范和应对信息安全风险,提高我国信息安全保障能力,根据国家相关法律法规和行业政策要求,我国开展了信息安全检查工作。

(2) 2025 年信息安全检查是在我国信息化建设深入推进、网络安全形势日益严峻的背景下进行的。近年来,国内外信息安全事件频发,网络安全威胁多样化、复杂化,对国家和社会稳定构成严重威胁。为了确保我国信息安全,及时发现和消除安全隐患,保障信息系统安全稳定运行,本次信息安全检查具有十分重要的现实意义。

(3)

本次信息安全检查旨在全面评估我国信息安全状况，查找信息系统存在的安全风险和漏洞，督促相关部门和单位加强信息安全防护，提高信息安全保障水平。检查范围覆盖了政府部门、企事业单位、社会团体等多个领域，检查内容包括网络安全、数据安全、系统安全等方面，通过本次检查，将有助于推动我国信息安全工作的深入开展，为构建安全、稳定、可靠的信息化环境奠定坚实基础。

1.2 检查目的

(1) 本次信息安全检查的主要目的是全面评估我国信息系统的安全状况，确保国家信息安全法律法规和政策的贯彻落实。通过检查，旨在提升我国信息安全防护能力，防范和减少信息安全事件的发生，保障关键信息基础设施的安全稳定运行。

(2) 具体而言，检查目的包括以下几点：一是发现和消除信息系统中的安全隐患，提高信息系统的安全防护水平；二是加强对信息安全风险的识别和评估，为信息安全决策提供科学依据；三是督促相关部门和单位落实信息安全责任，提高信息安全意识；四是推动信息安全技术和管理水平的提升，为我国信息安全事业发展提供有力支撑。

(3) 此外，本次信息安全检查还有助于完善信息安全法律法规体系，推动信息安全标准规范的实施，促进信息安全产业健康发展。通过检查，将推动我国信息安全工作向纵深发展，为构建安全、稳定、可靠的信息化环境，实现经济社

会高质量发展提供有力保障。

1.3 检查依据

(1)

本次信息安全检查的依据主要包括国家相关法律法规和政策文件，如《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等，这些法律法规为信息安全检查提供了法律框架和基本要求。

(2) 此外，检查依据还包括国家和行业标准规范，例如《信息安全技术 信息系统安全等级保护基本要求》、《信息安全技术 信息系统安全风险评估规范》等，这些规范为信息安全检查提供了技术标准和评估方法。

(3) 同时，检查依据还包括政府部门发布的指导性文件和通知，如国家互联网信息办公室、工业和信息化部等发布的关于网络安全和信息化工作的指导意见、通知和要求，这些文件为信息安全检查提供了政策导向和工作要求。通过综合运用这些法律法规、标准规范和政策文件，确保信息安全检查工作的合法性和规范性。

二、检查范围与对象

2.1 检查范围

(1) 本次信息安全检查的范围涵盖了我国政府部门、企事业单位、社会团体等多个领域的信息系统。包括但不限于政府部门的信息系统、金融、能源、交通、通信等关键信息基础设施，以及涉及个人信息保护、数据安全等领域的重要信息系统。

(2) 检查范围还包括各类企事业单位的信息系统，如大

型企业、中小企业、科研院所、教育机构等，涉及企业生产管理、科研创新、教育信息化等方面的信息系统均在检查之列。此外，互联网服务平台、电子商务平台、社交媒体等网络信息服务提供商的信息系统也是本次检查的重点。

(3) 本次检查还特别关注了个人信息保护、数据安全等方面的问题，对涉及用户个人信息收集、存储、使用、传输、处理等环节的信息系统进行严格检查，确保个人信息安全得到有效保障。同时，检查范围还扩展到信息安全产品和服务领域，对信息安全产品、安全服务提供商进行综合评估，推动信息安全产业健康发展。

2.2 检查对象

(1) 检查对象主要包括各级政府部门的信息系统，涉及国家机关、政府部门、公共机构等，这些系统承担着国家政务、公共服务等职能，其安全性直接关系到国家利益和公民权益。检查将重点关注政府网站、电子政务平台、数据中心等关键信息系统的安全防护措施。

(2) 企业单位的信息系统也是检查的重要对象，包括大型国有企业、民营企业、外资企业等，这些企业的信息系统关系到企业的商业秘密、市场竞争力和生存发展。检查将针对企业内部网络、办公系统、生产管理系统等，确保企业信息安全。

(3) 社会团体和非营利组织的信息系统同样在检查范围内，如行业协会、学术团体、慈善机构等，这些组织的信息系统涉及到会员信息、社会资源整合等，其安全稳定运行对于维护社会秩序和公共利益具有重要意义。此外，检查还将关注互联网服务平台、电子商务平台、社交媒体等网络信息服务提供商的信息系统，确保网络空间的安全与和谐。

2.3 检查内容

(1) 检查内容首先针对信息系统的物理安全，包括机房环境、设备安全、物理访问控制等方面，确保信息系统不受物理损坏和非法侵入。这涉及到机房温度、湿度控制，电源稳定性，以及门禁、监控等物理安全措施的有效性。

(2) 其次，检查内容将关注网络安全防护措施，包括防火墙、入侵检测系统、防病毒软件等安全设备的配置与运行情况，以及网络边界的安全策略和内部网络的安全隔离。此外，还会对网络流量进行监测，以识别和防范恶意攻击、数据泄露等网络安全威胁。

(3) 数据安全是检查的另一个重点，包括数据加密、访问控制、备份与恢复机制等。检查将验证数据是否得到妥善保护，防止未经授权的访问和泄露，以及确保在数据丢失或损坏时能够及时恢复，保障数据完整性和可用性。同时，检查还会关注个人信息保护，确保个人信息收集、存储、使用等环节符合相关法律法规要求。

三、检查方法与步骤

3.1 检查方法

(1) 检查方法主要包括现场检查和远程评估两种方式。现场检查是指检查组直接到被检查单位进行实地考察，通过访谈、查阅资料、观察现场等方式，对信息系统的安全防护措施进行详细审查。远程评估则通过网络远程连接被检查单位的信息系统，利用专业工具进行安全扫描和漏洞检测。

(2) 在现场检查过程中，检查组会针对信息系统的安全管理制度、技术措施、人员配置等方面进行全面审查。这包括对安全政策、操作规程、应急预案的审查，以及对安全设备、安全软件的安装和配置情况进行核实。

(3) 远程评估通常采用自动化工具进行，这些工具能够对信息系统的网络、主机、应用等多个层面进行安全检测。检查组会根据检测结果，对发现的安全风险进行分类、评级，并提出相应的整改建议。同时，检查组还会对被检查单位的安全意识、应急响应能力等方面进行综合评价。

3.2 检查步骤

(1) 检查步骤的第一步是制定详细的检查计划。这包括确定检查范围、对象、内容和方法，以及制定检查的时间表和资源分配。检查计划需经相关部门审核批准，确保检查工作有序进行。

(2) 第二步是开展现场检查。检查组按照预先制定的计划，对被检查单位的信息系统进行实地考察。现场检查过程中，检查组会与被检查单位的安全管理人员进行沟通，了解其安全管理制度和措施，并对现场的安全设备、设施进行查验。

(3)

第三步是对收集到的信息进行分析评估。检查组会将现场检查和远程评估得到的数据进行整理、分析，对发现的安全问题进行分类、评级。在此基础上，检查组会撰写检查报告，提出整改建议，并将报告提交给被检查单位和相关管理部门。同时，检查组还会跟踪整改工作的进展，确保问题得到有效解决。

3.3 检查工具

(1) 检查工具中，网络扫描器是必不可少的工具之一。这类工具能够自动扫描网络上的开放端口、服务版本、潜在的安全漏洞，帮助检查组快速发现网络层面的问题。常用的网络扫描器包括 Nmap、Masscan 等，它们能够生成详细的扫描报告，便于后续的分析 and 评估。

(2) 应用程序漏洞扫描工具是针对软件应用进行检查的重要工具。这类工具能够自动检测软件中的已知漏洞，包括 SQL 注入、跨站脚本攻击、跨站请求伪造等常见漏洞。例如，OWASP ZAP、Burp Suite 等工具，它们能够模拟攻击者的行为，帮助发现应用层面的安全风险。

(3) 数据库安全扫描工具用于检查数据库系统中的安全配置、访问控制、数据加密等方面的问题。这类工具能够识别数据库漏洞、权限滥用、敏感数据泄露等风险。例如，SQLMap、DBNinja 等工具，它们能够对数据库进行深度检查，并提供相应的安全建议，帮助提升数据库系统的安全性。此外，日志分析工具和安全事件监控平台也是检查过程中常用

的工具，它们能够帮助监控系统的运行状态，及时发现异常行为和安全事件。

四、检查结果概述

4.1 安全风险等级

(1) 在本次信息安全检查中，安全风险等级的评定依据了国家相关标准，结合实际情况，将风险分为高、中、低三个等级。高风险指的是可能导致严重后果，如系统瘫痪、数据泄露、经济损失等，且发生概率较高的安全风险。中风险指的是可能造成一定影响，如业务中断、数据损坏等，发生概率一般的安全风险。低风险则是指影响较小，且发生概率较低的安全风险。

(2) 根据检查结果，高风险主要包括系统漏洞、恶意代码攻击、未授权访问等。这些风险若被利用，可能导致信息系统被完全控制，或造成敏感数据泄露，对国家安全、社会稳定和公民个人权益造成严重威胁。中风险则涉及系统配置不当、安全策略缺失、数据备份不完整等问题，这些问题若不及时处理，可能引发业务中断或数据丢失。低风险主要包括系统性能瓶颈、非关键功能缺陷等，这些问题虽然不会对核心业务造成直接影响，但仍然需要关注和优化。

(3) 在安全风险等级划分过程中，检查组综合考虑了风险的影响范围、影响程度、发生概率等因素。对于高风险，检查组建议立即采取整改措施；对于中风险，建议在短期内制定整改计划并实施；对于低风险，则建议在后续工作中逐步进行优化和改进。通过这样的风险等级划分，有助于被检查单位明确安全工作的重点和优先级，提高信息安全防护的整体水平。

4.2 主要问题类型

(1) 本次信息安全检查发现的主要问题类型包括网络安全漏洞、系统配置不当和数据安全风险。网络安全漏洞主要表现为系统服务未及时更新，导致已知漏洞可被利用；部分系统存在默认用户名和密码，未进行修改，增加了被攻击的风险。系统配置不当主要体现在安全策略设置不合理，如防火墙规则配置错误、日志记录功能缺失等，这些问题可能导致系统暴露于潜在的安全威胁之下。

(2) 数据安全风险方面，检查发现部分单位对敏感数据保护措施不足，如未对敏感数据进行加密存储、传输，缺乏有效的访问控制机制；此外，数据备份和恢复机制不完善，一旦发生数据丢失或损坏，难以快速恢复，对业务连续性造成影响。同时，个人信息保护方面 also 存在问题，如未按照相关法律法规对个人信息进行分类管理，存在泄露风险。

(3) 在应用安全方面，检查发现部分应用存在跨站脚本攻击（XSS）、SQL 注入等常见漏洞，这些漏洞可能导致用户信息泄露、系统被恶意控制。此外，部分应用缺乏必要的安全验证和授权机制，用户权限管理混乱，存在内部人员滥用权限的风险。针对这些主要问题类型，检查组提出了相应的整改建议，以提升被检查单位的信息安全防护水平。

4.3 检查发现的问题数量

(1)

在本次信息安全检查中,共发现各类安全问题超过 500 项。其中,网络安全漏洞问题占比最高,达到总数的 40%,这些问题主要涉及操作系统、网络设备、应用服务等多个层面。系统配置不当问题占 20%,主要表现为安全策略设置不合理、日志记录功能缺失等。数据安全风险问题占 15%,主要集中在敏感数据保护、数据备份恢复等方面。

(2) 具体到不同类型的问题,网络安全漏洞问题中,服务器未打补丁、防火墙配置错误等基础性问题占比较高;系统配置不当问题中,安全策略设置不合理、系统日志记录缺失等问题较为普遍;数据安全风险问题中,敏感数据未加密存储、数据备份不完整等问题较为突出。这些问题表明,被检查单位在信息安全方面仍存在较多薄弱环节。

(3) 在本次检查中发现的问题数量较多,反映了信息安全工作的复杂性和艰巨性。这些问题涉及多个领域、多个层面,需要被检查单位高度重视,并采取切实有效的措施进行整改。检查组将对发现的问题进行跟踪,确保整改措施得到落实,有效提升我国信息安全保障水平。

五、具体问题分析

5.1 系统安全漏洞

(1) 系统安全漏洞方面,本次检查发现的主要问题包括操作系统漏洞、数据库漏洞和应用软件漏洞。操作系统漏洞主要由于系统未及时更新补丁,导致已知安全漏洞可被攻击者利用,如 Windows 操作系统的 SMB 漏洞、Linux 系统的 SSH

漏洞等。数据库漏洞则表现为数据库管理系统配置不当、权限设置不合理，容易导致数据泄露或系统被入侵。

(2)

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。

如要下载或阅读全文，请访问：

<https://d.book118.com/246041041152011015>