

测绘地理信息数据安全管理体系构建

李 瑞

汉中经纬科技咨询有限责任公司 陕西 汉中 723000

摘 要：本文探讨了测绘地理信息数据安全管理体系的构建，包括信息安全领导小组的设立、信息安全管理体系的制定与执行、信息安全技术措施的采用与实施。分析了数据采集、存储、传输、共享、使用与销毁等关键环节的安全管理措施，并提出了安全风险评估与应对方法，为测绘地理信息数据安全管理体系提供全面指导。

关键词：测绘地理信息；数据安全；管理体系；风险评估；预防措施

引言：随着信息技术的飞速发展，测绘地理信息数据在国土规划、资源管理、环境保护等领域发挥着越来越重要的作用。然而，数据泄露、篡改等安全问题也日益凸显，对国家安全、公共利益和个人隐私构成严重威胁。因此，加强测绘地理信息数据安全管理体系构建显得尤为重要。

1 测绘地理信息数据安全管理体系构建

1.1 信息安全领导小组的设立与职责

为了确保测绘地理信息数据的安全管理得到有效实施，必须设立一个专门的信息安全领导小组。这个小组应由来自不同部门、具有相关专业知识和经验的人员组成，以确保其决策的全面性和专业性。信息安全领导小组的主要职责包括：制定并执行信息安全战略，确保其与组织的整体战略相一致；监督信息安全管理体系的实施，确保其得到有效执行；协调各部门之间的信息安全管理工作，形成合力；对信息安全事件进行应急响应和处理，减少损失；以及定期组织信息安全培训和演练，提高全员的信息安全意识。领导小组应定期召开会议，讨论信息安全工作的进展情况，分析存在的安全隐患，制定针对性的改进措施。

1.2 信息安全管理体系的制定与执行

信息安全管理体系是测绘地理信息数据安全管理体系的基石。一套完善的管理制度应涵盖数据的采集、处理、存储、传输、使用和销毁等全生命周期的各个环节。在制度制定过程中，应充分考虑测绘地理信息数据的特点和应用场景，确保制度的针对性和可操作性。例如，对于数据的采集和处理环节，应明确数据采集的规范性和准确性要求，以及数据处理的安全防护措施；对于数据的存储和备份环节，应规定数据存储介质的选择和管理要求，以及数据备份策略的制定和执行方式^[1]。制度的执行是制度生命力的体现。为了确保制度得到有效执行，应建立相应的监督机制。这包括定期对制度执行情况进行检查、评估和审计，及时发现和纠正存在的问题。还

应建立奖惩机制，对遵守制度的人员给予表彰和奖励，对违反制度的人员进行处罚和问责。信息安全管理体系还应与时俱进，根据信息技术的发展和测绘地理信息数据的应用变化，不断进行修订和完善。这要求领导小组和相关部门保持对新技术、新应用的敏锐洞察力，及时调整和优化管理制度。

1.3 信息安全技术措施的采用与实施

信息安全技术措施是测绘地理信息数据安全管理体系的重要保障。为了确保数据的安全，应采用先进的信息安全技术，包括加密技术、访问控制技术、防火墙技术、入侵检测技术、数据脱敏技术等。加密技术可以对数据进行加密处理，确保数据在传输和存储过程中不被窃取或篡改。访问控制技术可以限制对数据的访问权限，确保只有经过授权的人员才能访问数据。防火墙技术可以阻止未经授权的访问和攻击，保护网络边界的安全。入侵检测技术可以实时监测网络中的异常行为，及时发现并应对潜在的安全威胁。数据脱敏技术可以对敏感数据进行脱敏处理，降低数据泄露的风险。在实施信息安全技术措施时，应遵循以下原则：首先，应根据数据的敏感程度和重要性，选择合适的安全技术措施；其次，应定期对安全技术措施进行评估和测试，确保其有效性和可靠性；最后，应加强对安全技术措施的管理和维护，确保其持续稳定运行。除了采用先进的安全技术措施外，还应加强对安全技术的研究和开发。这包括关注信息安全领域的最新研究成果和技术趋势，积极引进和应用新技术、新方法，提高测绘地理信息数据的安全防护能力。

2 测绘地理信息数据安全管理体系的关键环节

2.1 数据采集与处理安全管理

数据采集是测绘地理信息工作的基础，也是数据安全管理体系的起点。在数据采集过程中，规范性与准确性是至关重要的两个要求。规范性要求体现在采集工作的各个方面。采集方法必须科学、合理，符合测绘地理信息

行业的技术标准和规范。采集设备应经过严格校准和检验,确保其性能稳定、准确可靠。采集人员需具备相应的专业知识和技能,接受过系统的专业培训,能够熟练掌握采集方法和设备操作。此外,采集流程也应明确、具体,包括采集前的准备、采集过程中的操作规范以及采集后的数据检查和质量控制等环节。通过这些措施,可以确保数据采集工作的有序进行,减少因操作不当或设备故障等原因导致的数据错误和偏差。准确性要求是数据采集的核心目标。在采集过程中,应采取措施减少误差和偏差,确保数据的精确性和一致性。这包括使用高精度的采集设备、采用先进的采集技术、进行多次采集并取平均值等方法。还应对采集到的数据进行质量检查和错误纠正,及时发现并处理数据中的问题,如异常值、缺失值等。通过这些措施,可以提高数据的准确性和可靠性,为后续的数据处理和分析提供坚实的基础。数据处理是测绘地理信息工作的关键环节之一,也是数据安全管理的重要环节。在数据处理过程中,必须采取严格的安全防护措施,确保数据不被泄露、篡改或损坏。安全防护措施主要包括数据加密、访问控制、审计追踪等方面。数据加密是对敏感数据进行加密处理,确保数据在传输和存储过程中不被窃取或篡改。可以采用对称加密或非对称加密等技术手段,根据数据的敏感程度和重要性来选择合适的加密算法和密钥管理方式。访问控制是限制对数据的访问权限,只有经过授权的人员才能访问和处理数据。可以通过设置访问控制列表、角色权限管理等方式来实现^[2]。审计追踪是记录数据处理过程中的所有操作和行为,以便在发生安全问题时能够追溯和定位问题源头。可以通过日志记录、审计轨迹等方式来实现,确保数据处理过程的可追溯性和可审计性。

2.2 数据存储与备份安全管理

数据存储是测绘地理信息数据安全管理的环节之一。在数据存储过程中,应选择合适的存储介质,并采取有效的管理措施,确保数据的安全性和可靠性。存储介质的选择应根据数据的类型、大小、访问频率以及安全性要求等因素综合考虑。对于大量、长期存储的数据,应选择具有高容量、高稳定性、高可靠性的存储介质,如磁盘阵列、磁带库等。还应对存储介质进行定期检查和维护,确保其正常运行和延长使用寿命。在存储管理方面,应建立完善的存储管理制度和流程,包括数据的分类存储、备份策略制定、数据恢复机制等。通过对数据进行分类存储,可以根据数据的敏感程度和重要性采取不同的存储策略;通过制定备份策略,可以确保在数据丢失或损坏时能够及时恢复;通过建立数据恢复

机制,可以确保在发生数据丢失或损坏时能够迅速、准确地恢复数据。数据备份是数据存储安全管理的重要组成部分。应制定完善的数据备份策略,包括备份频率、备份方式、备份存储地点等方面。备份频率应根据数据的更新频率和重要性来确定,确保数据能够及时得到备份;备份方式应选择可靠、高效的备份技术,如增量备份、差异备份、全量备份等;备份存储地点应选择安全、可靠的存储环境,如异地备份、云存储等,确保备份数据的安全性和可用性。

2.3 数据传输与共享安全管理

数据传输是测绘地理信息数据在不同系统、不同地点之间传输的过程。在数据传输过程中,必须采取严格的安全加密措施,确保数据不被窃取、篡改或泄露。安全加密措施是数据传输安全的重要保障。可以采用SSL/TLS协议、IPSec协议等加密技术,对传输的数据进行加密处理,确保数据在传输过程中的机密性和完整性。还应对传输过程进行监控和记录,及时发现并处理传输过程中的安全问题。数据共享是测绘地理信息数据在不同部门、不同单位之间共享的过程。在数据共享过程中,必须加强对数据权限的控制和监管,确保数据只被授权的人员访问和使用。可以通过设置访问控制列表、签署数据共享协议等方式来实现。

2.4 数据使用与销毁安全管理

数据使用是测绘地理信息数据发挥其价值的重要环节。在数据使用过程中,必须遵守相关法律法规和标准规范,确保数据的合规使用。规范使用方面,应建立完善的数据使用制度和流程,包括数据的申请、审批、使用、归还等环节。通过严格的申请和审批流程,可以确保数据只被合法、合规的人员使用;通过明确的使用规则和归还要求,可以确保数据的合理使用和及时回收。数据销毁是测绘地理信息数据生命周期的最后一个环节。在数据销毁过程中,必须采取彻底、安全的销毁措施,确保数据不被泄露或恢复。可以采用物理销毁、数据擦除等技术手段,根据数据的敏感程度和重要性来选择合适的销毁方法。还应加强对销毁过程的监控和管理,确保销毁过程的合规性和安全性^[3]。对于涉及国家秘密或敏感信息的测绘地理信息数据,在销毁过程中还应严格遵守相关保密规定和要求,确保销毁过程的保密性。

3 测绘地理信息数据安全风险评估与应对

3.1 风险评估的方法与流程

风险评估是测绘地理信息数据安全管理的首要步骤,其目的在于通过系统化的方法,识别数据在采集、存储、传输、使用和销毁等全生命周期中可能面临的安

全威胁和脆弱性,并评估这些威胁和脆弱性对数据安全造成的潜在影响。风险评估的方法通常包括定性评估和定量评估两种。定性评估主要依赖于专家的经验 and 判断,通过对数据安全的各个方面进行主观评价,来识别潜在的安全风险。这种方法相对灵活,能够快速识别出主要的安全问题,但评估结果可能受到评估者主观因素的影响。定量评估则通过数学模型和统计方法来量化安全风险,如利用概率论和数理统计原理来计算数据泄露或损坏的可能性及后果。这种方法能够提供更为客观、准确的评估结果,但需要大量的数据支持和复杂的计算过程。风险评估的流程一般包括风险识别、风险分析、风险评价和风险报告四个步骤。风险识别是通过对测绘地理信息数据的全生命周期进行梳理,识别出可能存在的安全威胁和脆弱性。风险分析是对识别出的风险进行深入研究,分析其成因、影响范围和可能后果。风险评价是根据风险分析的结果,对风险进行量化评估,确定风险的等级和优先级。风险报告则是将风险评估的结果以报告的形式呈现出来,为决策提供依据。

3.2 常见安全风险类型与特点

在测绘地理信息数据安全中,常见的安全风险类型主要包括外部攻击、内部泄露、技术故障和人为错误等。外部攻击是指来自外部的黑客、病毒或恶意软件等对测绘地理信息数据的非法访问和破坏。这类风险通常具有隐蔽性强、攻击手段多样等特点,难以防范和预测。内部泄露是指由于内部人员的不当行为或疏忽,导致测绘地理信息数据被非法获取或泄露。这类风险通常与人员的安全意识、管理制度和监管措施等因素有关。技术故障是指由于硬件设备、软件系统或网络通信等技术问题,导致测绘地理信息数据的丢失、损坏或无法访问。这类风险通常与技术的可靠性、稳定性和兼容性等因素有关。人为错误则是指由于人员的操作失误、判断错误或疏忽大意,导致测绘地理信息数据的安全问题。这类风险通常与人员的专业技能、工作经验和责任心等因素有关^[4]。不同类型的安全风险具有不同的特点,但都对测绘地理信息数据的安全性构成严重威胁。必须针对

不同类型的风险采取不同的防范和应对措施,确保数据的安全可靠。

3.3 安全风险的预防与应对措施

针对测绘地理信息数据的安全风险,应采取一系列预防与应对措施来确保数据的安全性。在预防方面,首先应加强安全意识教育,提高全体人员对于数据安全重要性的认识,增强安全防范意识。其次应建立完善的安全管理制度和流程,明确数据的采集、存储、传输、使用和销毁等各个环节的安全要求,规范人员的操作行为。还应加强技术防护,采用先进的加密技术、访问控制技术和审计追踪技术等,确保数据在传输、存储和使用过程中的安全性。在应对方面,应建立完善的风险监测和预警机制,实时监测数据的安全状态,及时发现并预警潜在的安全风险。同时应制定详细的应急预案和处置流程,明确在发生安全风险时的应对措施和责任人,确保能够迅速、有效地应对安全风险。还应加强与相关部门的沟通协调,形成合力,共同应对测绘地理信息数据的安全风险。

结束语

测绘地理信息数据安全是保障国家安全、公共利益和个人隐私的重要手段。通过构建完善的管理体系,加强关键环节的安全管理,以及实施有效的风险评估与应对措施,可以确保测绘地理信息数据的安全可靠。未来,随着信息技术的不断发展,测绘地理信息数据安全将面临更多挑战和机遇,需要持续关注和深入研究。

参考文献

- [1]赵燕.浅谈大数据时代地理测绘信息服务[J].冶金与材料,2021,41(05):179-180.
- [2]王群.浅谈大数据时代测绘地理信息服务面临的机遇和挑战[J].华东科技,2022(03):93-95.
- [3]王福海,王勇敢,张东坡,彭际辉.智慧城市建设中地理信息数据挖掘技术研究[J].科技与创新,2024,(11):48-51.
- [4]饶兴元.基于数据挖掘的智慧城市建设中测绘地理信息共享系统[J].西部资源,2023,(05):88-90.