数字图书馆安全管理指南

全国数字图书馆建设与服务联席会议

二〇一七年九月

数字图书馆安全管理指南

第一条　为加强数字图书馆安全管理，保障数字图书馆建设和服务的有效有序进行，促进数字图书馆事业的健康发展，特制定本指南。

第二条　本指南中所称“数字图书馆安全管理”，是指保护数字图书馆中的信息系统相关资产免受任何可能的威胁和损失，保持其中信息资源保密性、完整性和可用性并保障其实现所设定信息服务和其它功能的行为。数字图书馆中的信息系统相关资产可包含物理资源、软件资源与信息资源等。其中信息资源是指以数字形式发布、存取和利用的信息资源总和。

第三条　在数字图书馆建设和服务过程中，应注意在全国或区域合作时统一协调信息安全政策与信息安全技术措施，加强在信息安全领域与其他合作方的交流。本指南在符合国家法律法规的框架下制订，除了参照本指南，指南中未提及部分应遵守国家和地方各级有关部门与信息安全相关的法律、法规、条例、规章等，并根据自身实际情况进行补充完善。

第四条　数字图书馆安全主要应关注以下相关要素，包括安全政

策、访问控制、信息资源安全、环境安全、备份与容灾、应急响应与安全公告等内容。数字图书馆安全管理是基于数字图书馆的服务目标，结合业务流程，对所有这些要素进行适当调配、组织，确保其正常发挥作用的完整体系。

第五条　数字图书馆安全管理是对确立数字图书馆安全目标，建立组织架构，明确职责，进行角色分配、风险评估、安全审计、系统分类、制订预案、事故处理、回顾检查和改进的过程进行管理，并通过持续的执行这些过程管理使数字图书馆的安全水平得到不断的提高。应摸清现有系统的情况，对其范围内的信息系统相关资产所面对的各种威胁和脆弱性进行评估，对已存在的或规划的安全措施进行鉴定，了解其弱点、威胁和风险所在，制订相应的对策和预案，实现安全管理的目标。

第六条　安全政策

数字图书馆安全政策应根据具体的建设目标和战略，制定有效的信息技术安全策略，对数字图书馆的建设、运行、维护和服务进行持续的监控、评估和改进，形成完整的规章制度与流程规范，并随着变化保持更新。

第七条　访问控制

1．建立全面的用户访问控制管理，避免系统的未授权访问。并应明确告知用户其被授权的权限，明确其权利及所承担的责任。

2．应使用各类访问控制技术手段，尤其是网络安全方面的技术手段，减少系统被非法利用与攻击的可能。利用应用与系统的分类，采用不同的防护手段等级划分不同的防护区域，使外部非法访问内部服务器的可能降低。

第八条　信息资源安全

1．信息资源包括购买信息、自建信息、购买的资源远程访问控制权限以及使用各类信息所产生的相关用户数据等。信息资源安全管理通过对资源进行分级、核查、维护以及采用加密、水印等技术手段，确保资源本身及其知识产权得到有效的保护。

2．信息资源的安全性因素还包括保护其依赖的软硬件资源。在信息资源保存与服务中，需要充分考虑保留与保护能保障其可操作性的相应的软件及硬件环境。

第九条　环境安全

1．环境安全的基本要求是确定物理环境安全区域，明确责任部门与人员，建立相关规章制度，并注意在防火、

防水、配电、温湿度控制、防静电、防雷及电磁防护等物理安全方面达到相关标准要求。

2. 对机房环境安全应注意出入人员管理，加强对出入人员及所携带设备的控制，有必要时加强门禁控制与视频监控手段。

第十条　备份与容灾

1. 可以根据需要分类分级制订备份与容灾预案，其中包括但不限于媒体退化、维护失败、人为失误、技术故障、日志记录和业务连续性方案等。

2. 应根据信息安全目标与资源情况制定备份策略，如选择本地备份、异地备份与多机系统等备份方式。根据应用与资源的特性合理选择备份介质、频率周期，并定期检查及测试备份内容与恢复程序，确保在预定的时间内正确恢复。在必要时可采用多系统热备的方案。

3. 容灾指利用技术、管理手段以及相关资源确保既定的数字图书馆关键数据、处理系统和关键业务在灾难发生后可以恢复和重续运营的过程。通常可采用异地备份、多系统热备等方案。异地备份应注意信息资源的加密与传输中的一致性，以确保可靠安全与运营恢复。

第十一条　应急响应与安全公告

1. 应急响应包括应急计划和应急措施两个方面。应急计划的制定至少应考虑紧急反应、阻止事件发展、恢复措施、事件溯源及问责五个因素。应急措施可以包括应急预案、软硬件备份、信息资源备份和快速恢复措施等。相关计划与措施都应注意做好测试、培训、演练与维护。

2. 应根据数字图书馆运行情况发布相关的安全预警信息，并根据安全事件的发展情况向公众或定义的用户群体发布公告信息。

第十二条　本指南由全国数字图书馆建设与服务联席会议制定、解释和修改，报文化部公共文化司备案。

相关文献:

1. GB/T 22081-2008(IDT ISO/IEC 27002:2005).信息技术-安全技术-信息安全管理实用规则
2. GB/T 18336.1-2001(IDT ISO/IEC 15408-1:1999).信息技术-安全技术-信息技术安全性评估准则-第1部分:简介和一般模型
3. GB/T 18336.1-2008(IDT ISO/IEC 15408-1:2005).信息技术-安全技术-信息技术安全性评估准则-第1部分:简介和一般模型
4. GB/T 18336.2-2008(IDT ISO/IEC 15408-2:2005).信息技术-安全技术-信息技术安全性评估准则-第2部分:安全功能需求
5. GB/T 18336.3-2008(IDT ISO/IEC 15408-3:2005).信息技术-安全技术-信息技术安全性评估准则-第3部分:安全认证需求
6. GB/T 22081-2008(IDT ISO/IEC 27002:2005).信息技术-安全技术-信息安全管理实用规则
7. GB/T22080-2008(IDT ISO/IEC 27001:2005).信息技术-安全技术-信息安全管理体系-要求信息安全等级保护管理办法 2010
8. GB 17859-1999 计算机信息系统安全保护等级划分准则
9. GB/T20269-2006 信息安全技术-信息系统安全管理要求