数字图书馆安全管理指南

第一条 为促进数字图书馆事业的进展，对数字图书馆的运行必须实施严格的安全治理，以保证数字图书馆建设和服务有序进行，特制定本指南。

第二条 本指南中所称“数字图书馆安全治理”，是指爱护数字图书馆中的信息系统相关资产免受任何可能的威逼和缺失，保持其中信息资源完整性和可用性并保证事实上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公布、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和谐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。除了参照本指南，应遵守国家和地点各级有关部门与信息安全相关的法律、法规、条例、规章等，并依照自身实际情形进行补充完善。

第四条 数字图书馆安全要紧应关注以下相关要素，包括安全政策、过程治理、访问操纵、信息资源安全、备份与容灾、环境安全、应急响应与安全公告等内容。数字图书馆安全治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 数字图书馆安全政策应依照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、爱护和服务进行连续的监控、评估和改进，并形成完整的规章制度与流程规范。

第六条 过程治理

1．数字图书馆安全过程治理是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、回忆检查和改进的过程进行治理，并通过连续的执行这些过程治理使数字图书馆的安全水平得到不断的提高。

2．应摸清现有系统的情形，对其范畴内的信息系统相关资产所面对的各种威逼和脆弱性进行评估，对已存在的或规划的安全措施进行鉴定，了解其弱点、威逼和风险所在，制订相应的计策和预案，实现安全治理的目标。

第七条 访问操纵

1．建立全面的用户访问操纵治理，幸免系统的未授权访问。并应明确告知用户其可访问的权限，明确其权益及所承担的责任。

2．应尽量关闭网络设备与主机系统不必要的服务端口，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纳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、自建信息及购买的资源远程访问操纵权限等。信息资源的安全性因素还包括爱护其依靠的软硬件资源。在信息资源储存与服务中，需要充分考虑保留与爱护能保证其可操作性的相应的软件及硬件环境。

2．信息资源安全治理通过对资源进行分类、核查和爱护，确保其得到有效的爱护。

第九条 备份与容灾

1．能够依照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、爱护失败、人为失误、技术故障、日志记录和业务连续性方案等。

2．应依照信息安全目标与资源情形制定备份策略，如选择本地备份、异地备份与多机系统等备份方式。依照顾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复原程序，确保在预定的时刻内正确复原。在必要时可采纳多系统热备的方案。

3．容灾指利用技术、治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能够复原和重续运营的过程。通常采纳异地备份与多系统热备的方案。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复原。

第十条 环境安全

1．环境安全的差不多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、温湿度操纵、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治理，加强对来访人员的操纵，有必要时加强门禁操纵与视频监控手段。

第十一条　应急响应与安全公告

1．应急响应包括应急打算和应急措施两个方面。应急打算的制定至少应考虑紧急反应、阻止事件进展、复原措施三个因素。应急措施能够包括应急预案、软硬件备份、信息资源备份和快速复原措施等。相关打算与措施都应注意做好测试、培训、演练与爱护。

2．应依照数字图书馆运行情形公布相关的安全预警信息，并依照安全事件的进展情形向公众或定义的用户群体公布公告信息。

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、说明和修改，由文化部社会文化司批准公布。