苏州大学博物馆网络安全管理条例

为贯彻落实《中华人民共和国网络安全法》《苏州大学网络安全管理条例》（苏大委〔2018〕138号），建立健全博物馆网络安全管理体系，落实博物馆网络安全工作责任制，提升博物馆网络安全整体水平，进一步保障博物馆网络正常运行，制定本条例。

第一章 总则

第一条 本条例所称网络安全是指苏州大学校园网内的网络系统和信息系统的安全，包括设备设施安全、系统运行安全和内容数据安全等多个方面。

第二条 博物馆网络安全管理的目标是，完善网络安全技术体系和运行体系，不断提高网络安全保护能力，确保博物馆网络安全、稳定运行，保障博物馆信息化建设持续发展。

第三条 博物馆全体教职员工都必须遵守《中华人民共和国网络安全法》。使用校园网络系统或信息系统的用户，应接受并配合上级主管部门、公安司法机关或学校的网络安全检查。

第四条 博物馆网络安全管理以“谁主管谁负责、谁运维谁负责、谁使用谁负责”为原则，落实网络安全分级责任制；以国家标准《信息系统安全等级保护基本要求》为指导，综合防范、突出重点，保障博物馆网络安全。

第二章 组织机构与职责

第五条 成立博物馆网络安全管理工作小组，由常务副

馆长任组长，信息技术与安保部主任为副组长，领导班子其他成员为组员，负责博物馆网络安全工作，确定博物馆网络安全工作的政策方针，制定相关规章制度。提出博物馆网络安全工作的任务和要求，审定博物馆网络安全工作计划，组织查处博物馆网络安全事件。

第六条 博物馆网络安全管理工作小组贯彻执行上级网络安全部门的政策和要求，贯彻落实网络安全与信息化工作领导小组的任务要求，负责博物馆网络安全具体管理工作。主要职责如下：

1．根据网络安全实际情况，拟订博物馆网络安全工作计划；

2．统筹协调和监督管理各科室网络安全工作，并检查网络安全管理制度落实情况；

3．监控本单位所属信息系统和自建网络系统的运行状态，及时发现和消除安全隐患。如果发现危及全校网络安全的情形或者有害信息后，及时向网络安全与信息化工作领导小组办公室报告；

4．组织审核拟在博物馆内实施的网络安全方案和方法，组织论证拟在校园网内部署的网络安全设备和系统；

5．核定本单位校园网内信息系统安全等级及其安全管理制度；

6．发布涉及网络安全的通知、公告；

7．组织开展经常性的全馆网络安全宣传教育；

8．协助公安司法机关查处各种有关网络安全的违纪、违法行为。

第七条 本单位党政主要负责人是本单位的网络安全第一责任人，对本单位的网络安全负领导责任。

第八条 信息技术与安保部主任为网络安全管理员，承担本单位网络安全的具体工作，并及时向学校相关部门报备网络安全管理员相关信息。

第九条 本单位网络安全管理员一般应具有相关专业知识背景，在正式上岗前，应当参加网络安全培训，掌握网络安全相关技术，了解学校网络安全体系，理解网络安全制度，熟悉本单位网络安全措施。

第三章 网络系统安全

第十条 博物馆网络系统为学校主干网络。

第十一条 学校主干网络由学校统筹建设和管理。

第十二条 本馆根据工作需要可建设内部网络系统，以“谁主张谁负责、谁运营谁负责、谁使用谁负责”为原则。

第十三条 加强各楼宇内弱电间的管理，涉及校园网络的弱电间原则上由信息技术与安保部单独使用，任何人未经批准，均不得擅自进入。本馆建设的弱电管网由信息技术与安保部统一管理，任何人使用弱电管网需提供设计和施工方案，并经博物馆网络安全管理工作小组审核通过后，方可施工。

第十四条 除信息技术与安保部外，严禁其他个人未经

博物馆网络安全管理工作小组同意，以任何方式登录校园网络主干的各类设备，实施修改、设置、删除等操作。严禁任何施工单位或个人以任何理由损毁校园网络设备设施。

第四章 信息系统安全

第十五条 博物馆各信息系统实行安全等级保护。由博物馆网络安全管理工作小组参照国家标准《信息系统安全等级保护基本要求》，审核确定校园网内各信息系统的安全等级。信息系统不仅包括关键信息系统和各个面向全校的重要业务系统，也包括各级各类应用业务系统，还包括各级各类网站系统。

第十六条 关键信息系统由博物馆网络安全管理工作小组统筹建设和管理。信息技术与安保部负责由统一身份认证平台、云计算平台、共享数据中心等构成的关键信息系统的具体建设和运营工作，按信息系统安全等级保护的要求，制定安全管理制度和操作规程，采取相应的安全保护技术措施，保障信息系统免受干扰、破坏或者未经授权的访问，防止信息系统数据泄露或者被窃取、篡改。

第十七条 信息系统安全管理制度应当明确安全负责人和各项安全保护责任,应当明确各项安全保护技术措施。

第十八条 信息系统安全保护技术措施至少包括下列项：

1．完善系统安全配置，定期进行漏洞扫描、系统加固或升级；

2．开启日志审计服务，有效检测、记录系统运行状态；

3．分类管理数据，对重要数据进行备份、加密处理；

4．实施用户分类管理，用户账号应能标识系统访问的不同角色，应尽量避免使用系统默认账号，账号只能具有符合用户角色的最小权限；

5．系统管理员密码应满足强度要求。

第十九条 信息系统的注册用户应该实名认证，由信息系统的运营者负责实名认证的实施。

第二十条 在建设阶段须充分考虑信息系统的安全防护。关键信息系统和各单位所属重要信息系统，应当具有支持业务稳定、持续运行的性能，并且安全技术措施必须同步规划、同步建设、同步使用。

第二十一条 根据工作需要新建或升级在校园网内运行的信息系统，应事先向博物馆网络安全管理工作小组提出申请；同时应就信息系统设计方案向信息技术与安保部征求意见。在上线运行前，信息系统须通过由信息技术与安保部组织的安全检测。

第五章 应急处置

第二十二条 博物馆网络安全管理工作小组按照规定通报网络安全监测预警信息。本馆全体教职员工应当根据国家、地方网络安全部门发布的预警信息及时做好相应防范工作，必须按照博物馆网络安全管理工作小组通报的预警信息，做好相应处置工作。

第二十三条 博物馆网络安全管理工作小组协调信息技

术与安保部和各科室，制定网络安全事件应急预案。网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第二十四条 网络安全管理员必须熟悉本单位网络安全事件应急处置措施，定期开展网络安全事件应急预案演练。

第二十五条 校园网内发生网络安全事件，应当立即启动网络安全事件应急预案，各科室和相关人员须按照应急预案规定进行处置。

第六章 奖惩

第二十六条 博物馆网络安全管理工作小组定期开展全馆网络安全工作的检查，每年向学校网络安全与信息化工作领导小组汇报各单位网络安全工作汇总信息。

第二十七条 对拒不执行网络安全管理相关制度、漠视网络安全工作以至造成重大事故和案件的个人，将追究责任。对触犯法律的，将移送公安司法机关处理。

第二十八条 对损坏校园网络系统或信息系统设备设施的个人，博物馆将视其情节轻重追究责任，如触犯法律应移交公安司法机关处理。

第七章 附则

第二十九条 对于涉及国家秘密的网络系统或信息系统，按照国家保密工作部门的相关规定和标准进行保护，接受学校保密委员会办公室监督指导。

第三十条 本条例自制定之日起施行，由网络安全管理工作小组负责解释。

博物馆

二〇二三年五月二十四日