目 录

山东科技大学网站管理办法.....1
山东科技大学网络安全等级保护管理规定.....7
山东科技大学网络安全责任追究制度.....15
山东科技大学信息系统建设管理办法.....19
山东科技大学域名管理办法.....33
山东科技大学信息系统运维安全管理办法.....38
山东科技大学外包服务信息安全管理办法.....44
山东科技大学网络安全事件报告与处置办法.....54
山东科技大学网络安全漏洞整改流程.....58
山东科技大学电子邮箱及电子邮件系统管理办法.....70
山东科技大学数据中心机房安全管理办法.....75
山东科技大学网络安全教育和培训管理办法.....84
山东科技大学校园网用户上网守则.....86
山东科技大学网络安全事件应急响应综合预案.....89
山东科技大学网络安全基线配置标准.....126

山东科技大学文件

山科大发〔2020〕44号

关于印发《山东科技大学网站管理办法》《山东科技大学网络安全等级保护管理规定》的通知

各校区管委，各部门、各单位:

《山东科技大学网站管理办法》《山东科技大学网络安全等级保护管理规定》已经校长办公会研究通过，现予印发，请遵照执行。

山东科技大学

2020 年 6 月 18 日

山东科技大学网站管理办法

第一章 总 则

第一条 为规范学校网站管理，推进学校信息化建设，根据《互联网信息服务管理办法》等政策法规和学校相关管理制度，结合工作实际，特制定本办法。

第二条 本办法适用于各部门、各单位(以下简称“各单位”)利用学校互联网络域名或互联网 IP 地址设置互联网站的备案和运营管理。

第三条 学校的一级网站域名为：sdust.edu.cn，校内二级网站，原则上使用学校统一的域名机制，二级网站格式为：*.sdust.edu.cn，其中“*”为二级单位汉语拼音首字母组合。

第二章 管理部门与职责

第四条 网络安全与信息化办公室（以下简称“网信办”）的管理职责:

（一）为各单位网站的建设与管理提供技术支持。

（二）对各单位网站进行备案。

（三）提供网站发布和域名服务。

（四）为管理范围内的网站提供物理安全、操作系统安全、防火墙建设和数据备份。

第五条 网站主办单位的管理职责:

（一）负责本单位网站的建设与管理。

（二）明确网站负责人和信息化联络员。

（三）负责本单位网站的安全和管理，网站运行过程中，一旦发生异常，应及时保存异常内容，并迅速向网信办和宣传部报告。

（四）负责联系网站服务厂商提供相应的技术支持、建设与运行维护、数据安全、运维队伍培训等工作。

（五）保证备案信息内容的真实准确，保证网站的互联网络域名或 IP 资质所包括的所有信息内容合法。

（六）配合有关部门的信息安全检查、网站信息内容检查、保密审查工作。

第六条 信息化联络员的职责：

（一）负责本单位信息化建设工作与网信办的联系与沟通。

（二）负责本单位信息系统的运维和信息安全管理。

（三）负责本单位信息系统安全隐患、事件的整改与报告。

第七条 各单位设立网站需经宣传部审查，网站信息内容受宣传部监管。

第三章 网站设立与备案

第八条 各单位网站的建设实行准入制，所有接入校园网的网站，由各单位提出申请，提交宣传部审核、网信办备案后方可建立。未履行备案手续的，不得设立互联网站。

第九条 各单位党政“一把手”作为本单位网站的第一责任人，负责网站建设和管理工作，并指定至少一名信息化联络员承担具体工作。

第十条 不允许任何单位或个人利用学校互联网络域名或互联网 IP 地址等设立个人网站，任何单位或个人不得利用学校互联网络域名或互联网 IP 地址从事有偿互联网信息服务。

第十一条 学校网站涉及以下服务项目的，须依照法律、行政法规以及国家有关规定，获得国家有关主管部门许可之后，再向学校提交审核备案手续:

（一）从事互联网新闻信息服务。

（二）提供由互联网用户向公众发布信息的服务。

（三）提供互联网信息搜索服务。

（四）从事文化、出版、视听节目、教育等互联网信息服务。

第十二条 在履行备案手续时，应当向网信办提供以下材料:

（一）设立互联网站的目的，信息服务功能说明，服务项目简介。

（二）网站管理人员基本情况，其中网站责任人应为网站主管部门的在编在职教职工。

（三）网站主管部门主要负责人签署的审核意见。

（四）从事本办法第十一条所列举的互联网信息服务项目的，提供国家有关主管部门的许可文件。

第十三条 网站主办单位在备案有效期内需要变更其备案信息的，应当在相关变更发生之日起 30 日内向网信办履行备案变更手续。

第十四条 网站主办单位在备案有效期内需要终止提供服务的，应当在服务终止之日起 30 日内向网信办履行备案注销手续。

第十五条 网信办对互联网站备案实行年度审核。网站主办单位应当在每年规定时间向网信办履行年度审核手续。

第十六条 在年度审核时，网站主办单位未在规定时间提交年度审核信息的，网信办有权责令其限期改正；拒不改正的，关闭该网站并注销备案。

第十七条 网站主办单位或个人违反国家有关法律法规或学校有关规章制度，应暂停或终止服务的，网信办应暂时关闭网站，或关闭网站并注销备案。

第四章 网站运营与维护

第十八条 网站管理人员的密码应符合复杂度要求，密码 8 位以上，包含大小写字母、数字及特殊符号，密码至少每三个月更换一次。

第十九条 网站管理人员要妥善保管账号和密码，严禁转借他人使用。如出现账号丢失或密码遗忘等问题，需持相关证件到网信办更改。

第二十条 在学校网站及各单位网站上设置的其他网站或网页链接，须经网站建设第一责任人审核批准，同时确保链接的有效性和合法性。

第二十一条 校内各网站未经合法授权，不得提供不符合著作权法的在线播放或者下载服务。

第二十二条 各单位应加强对网站系统的配置安全管理，定期检查和补丁升级，确认当前网站访问权限设置符合业务和管理上的要求。

第二十三条 严禁任何未经授权的网站系统维护操作。服务厂商在现场提供技术支持时，须由网站管理人员全程陪同。

第五章 附 则

第二十四条 本办法实施前利用学校互联网络域名或互联网 IP 地址设立互联网站的，应当自本办法施行之日起 60 天内依照本办法的有关规定补办备案手续。

第二十五条 本办法由网络安全与信息化办公室负责解释。

第二十六条 本办法自发布之日起施行。

山东科技大学网络安全等级保护管理规定

第一章 总 则

第一条 为加强学校网络安全管理,确保学校网络信息系统（以下简称“信息系统”）安全，依据《中华人民共和国网络安全法》和《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）的相关要求，结合工作实际，制定本规定。

第二条 网络安全管理遵循“确保安全、注重防范、分工负责、规范管理”的原则，以确保网络运行安全和网络信息安全为核心，以抓好安全防范为重点，各部门分工负责、协同配合、责任到人，认真遵守有关网络安全的法律法规和制度规定，共同做好网络安全管理工作。

第三条 按照国家有关网络安全的政策要求，结合实际，制定并完善安全策略、安全管理制度、日常操作规程和记录表单，构建学校网络安全管理制度体系。

第四条 本规定适用于信息系统的安全管理。

第五条 本规定所指信息系统是山东科技大学规划和建设范围内的计算机信息系统，包括所有非涉密信息系统。

第二章 组织机构和职责

第六条 在山东科技大学网络安全和信息化领导小组(以下简称“领导小组”）领导下，山东科技大学网络安全和信息化领导小组办公室（以下简称“领导小组办公室”）负责信息系统的

统一规划、责任分工和资源分配，按照“谁主管谁负责、谁使用谁负责”的原则，由山东科技大学网络安全与信息化办公室（以下简称“网信办”）负责信息系统的建设管理和运行维护。

第七条 网信办是学校信息化工作安全管理和运行维护的部门，负责指定信息系统的系统管理员、安全管理员和安全审计员。系统管理员主要负责系统的日常运行维护，安全管理员主要负责系统的日常安全管理工作，安全审计员主要负责对系统管理员和安全管理员的操作进行审计和评估。安全管理员和安全审计员不得为同一人。

第八条 各部门、各单位负责所属信息系统的建设管理和运行维护工作，负责指定本单位信息化联络员。信息化联络员负责协调本单位在信息系统运维、网络信息安全、信息化建设等方面与网信办的沟通与配合工作。

第九条 各部门、各单位应结合具体情况，制定信息系统安全管理的相关制度，建立健全保障信息安全的工作机制，采取措施落实有关安全要求，确保信息系统与信息的安全。

第三章 规划建设和测评审批

第十条 信息系统按照国家网络安全等级保护要求确定保护等级，进行规划、设计、建设和运行维护管理，并采取相应安全保护措施。

第十一条 网信办统一负责信息系统的定级工作，并报青岛市公安局备案。

第十二条 信息系统应根据其等保定级、行政级别、地域分

布、连接范围等合理划分安全域，安全域之间应采取必要的隔离措施。

第十三条 信息系统安全体系的规划、建设由网信办负责，统一采用防火墙、防病毒系统、入侵防御系统等安全措施。信息安全体系应与信息系统同步规划、同步建设、同步使用。

第十四条 信息系统的设计、建设须选择具有相应信息系统集成资质的单位承担设计、开发、建设和运行维护任务。信息系统建设工程的监理、检测工作应选择具有相应信息系统工程监理、检测资质的单位承担。

第十五条 重要信息系统投入使用前，有关风险评估、安全方案设计、论证、等级保护测评和密码评估等所需经费，应由系统建设使用单位在系统规划时，按照一定比例统一纳入系统建设经费预算。

第十六条 信息系统中使用的安全设备、系统软件、应用软件须采用国家主管部门认定或认可的产品和设备，优先选用国产设备和系统。

第十七条 信息系统设计方案必须通过论证以后方可实施。网信办参与设计方案的论证、审查。设计方案中涉及密码技术产品的，须报青岛市密码管理局审批。

第十八条 信息系统应要求有完善的鉴别和认证、访问控制、日志审计功能和数据验证功能，杜绝木马和后门，建立源代码控制和软件版本控制机制。

第十九条 重要信息系统建成后，选择网络安全等级保护测评机构开展测评。网络安全等级保护测评机构应根据“中国信息

安全等级保护网”提供的《全国等级保护测评机构推荐目录》进行选择。测评前应与测评机构签订工作协议和保密协议，对测评机构和测评人员的测评活动进行严格的监督与管理。信息系统通过测评后方可投入使用。

第二十条 信息系统不再使用时，网信办负责废止管理工作。密码设备退装、销毁等必须符合密码设备管理的有关规定。

第二十一条 网信办负责规范对服务提供商的安全管理工作，代表学校与服务提供商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务，定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

第四章 使用管理与运行维护

第二十二条 做好统筹联动，加强各类管理人员、各部门、院系之间在网络安全工作方面的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。

第二十三条 建立对外联系机制，拓展与外联单位的沟通与合作渠道。外联单位包括供应商、业界专家、专业的安全公司、安全组织、上级主管部门、兄弟单位、安全服务机构、电信运营部门、执法机关等。

第二十四条 信息系统应具备文档化的系统安全管理策略，每 6 个月对系统安全管理策略进行审核，如果系统、环境等发生较大变化时，应及时更新安全管理策略。

第二十五条 信息系统应当处于安全可控环境中，其机房建设应符合与网络安全等级相对应的标准要求，具有防火、防水、

防雷、防静电、防盗监控和供电、温控保障设施。服务器和交换设备应放置在安全可控的区域，建立相关制度进行环境和设备的运维管理。

第二十六条 信息系统所有计算机应及时升级病毒库，进行病毒查杀；及时安装操作系统、数据库和应用系统补丁程序。

第二十七条 信息系统应当采取身份鉴别、访问控制、安全审计、违规外联监控等技术保护措施。审计日志记录至少保存 1 年。

第二十八条 建立系统备份与恢复策略，对关键系统、关键设备和关键数据至少每 3 个月进行一次全量备份。

第二十九条 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录。

第三十条 通过信息系统发布信息，按照“谁发布、谁负责”的原则进行严格审批，建立审批程序，明确责任单位和责任人，做好发布信息的记录工作。

第三十一条 严格限制通过互联网直接向重要信息系统复制信息，确需复制的应采取严格的技术防护措施，防止病毒、木马等的导入传播。

第三十二条 在信息系统中，对用户的授权应按照最小授权原则，只授予其满足开展工作所需的最小访问权限，不得随意扩大用户的访问范围或提高权限等级。安全审计员应做好对授权管理和访问控制策略的监督、审核工作。

第三十三条 提升数据安全防护能力，确保数据完整性、保

密性和可用性，加强个人信息保护和剩余信息保护。

第五章 监测预警与应急处置

第三十四条 建立山东科技大学网络安全监测预警和信息通报制度，通报内容包括网络安全态势与风险预警情况、重要漏洞告警及处置措施建议、重大网络安全事件、信息系统高危安全隐患等，按照国家相关规定及省、市有关主管部门的要求，报送网络安全监测预警信息，并及时发现和处理网络攻击和异常行为等。

第三十五条 信息系统安全监测是网络安全检查的重要内容。领导小组办公室结合不同时期的工作需要，组织开展信息系统安全监测预警。对存在安全漏洞隐患的信息系统责任单位通报监测预警信息，限期整改。

第三十六条 领导小组办公室协调有关部门建立健全网络安全风险评估和应急工作机制。制定网络安全事件应急预案，并定期组织演练。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。

第三十七条 网络安全事件发生的风险增大时，领导小组应当按照规定的权限和程序，根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门和人员及时收集、报告有关信息，加强对网络安全风险的监测。

（二）组织有关部门和专业人员，对网络安全风险信息进行

分析评估，预测事件发生的可能性、影响范围和危害程度。

（三）在全校范围发布网络安全风险预警，发布避免、减轻危害的措施。

第三十八条 发生网络安全事件，应当立即启动网络安全事件应急预案。领导小组办公室对网络安全事件进行调查和评估，要求相关部门采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时发布有关的警示信息。

第六章 安全教育与培训

第三十九条 网信办通过多种形式在全校范围内开展网络安全知识培训和网络安全形势教育，不断增强广大师生网络安全防护意识。网络安全教育注重发挥校园网络的传播媒介作用，充分利用校园网传播网络安全知识和相关法律法规等。

第四十条 各部门、各单位要加强人员在录用、调岗和离岗环节的网络安全教育和管理。

第四十一条 信息系统安全管理人员包括系统管理员、安全管理员及安全审计员，须进行安全培训，经考核合格后方可上岗。

第四十二条 信息系统安全管理人员应定期参加网信办组织的专业培训，了解网络安全形势，学习最新网络安全知识，不断提高安全防护意识，增强做好网络安全工作的能力。

第七章 评价与惩戒

第四十三条 领导小组办公室负责对学校信息系统的等级保护工作进行监督，每年组织一次考核评价，将结果纳入单位的

年度绩效考核。

第四十四条 对违反有关规定，造成信息安全隐患的部门，应责令其限期整改；情节严重的，按照有关规定处理。

第八章 附 则

第四十五条 本规定由网络安全和信息化领导小组办公室负责解释。

第四十六条 本规定自发布之日起施行。

山东科技大学办公室 2020 年 7 月 20 日印发

山东科技大学网络安全和信息化领导小组文件

网信领导小组〔2020〕1号

关于印发《山东科技大学网站安全责任追究制度》的通知

各校区管委，各部门、各单位:

《山东科技大学网站安全责任追究制度》已经山东科技大学网络安全和信息化领导小组研究通过，现予印发，请遵照执行。

山东科技大学网络安全和信息化领导小组

2020 年 6 月 18 日

山东科技大学网络安全责任追究制度

第一章 总 则

第一条 为明确网络与信息安全事故责任主体（以下简称“责任主体”),做好网络与信息安全事故的责任认定和追究工作，结合学校实际情况，制定本制度。

第二条 责任主体的范围包括各部门、单位或个人等。山东科技大学网络安全和信息化领导小组（以下简称“领导小组”）负责追究责任主体的事故责任，称为“责任追究主体”。

第三条 网络与信息安全事故的责任认定实行“谁主管谁负责、谁使用谁负责”的原则，由领导小组组织实施。

第四条 发生网络与信息安全事故后,应根据安全事件造成的影响及相关责任主体的处置态度，作出如下处理:

（一）批评教育。包括责令责任主体检查、诫勉谈话等。

（二）通报批评。在事发部门、单位范围内对责任主体发文通报，责令整改，并由责任主体向学校主管领导作出书面检查。

（三）问责追责。将事故纳入责任主体的年度考核，取消当年年度考核评优资格,降低或扣除责任主体的年度绩效;依照发生网络与信息安全事故的严重程度,对责任主体和相关责任人处以罚款、赔偿事故损失、降职，直至解聘等。

（四）报警处理。严重损坏社会或国家利益的，上报当地公安部门处理。

第五条 责任追究应当坚持公平公正、有责必究、过罚相当、

教育与惩戒相结合的原则。

第二章 责任追究范围和适用

第六条 责任主体未按规定落实相关网络与信息安全管理制度及技术规范，导致一般安全事件发生的，应对其进行批评教育。

第七条 责任主体未按规定落实相关网络与信息安全管理制度及技术规范，导致较大安全事件发生的，应对其进行通报批评。

第八条 责任主体未按规定落实相关网络与信息安全管理制度及技术规范，导致重大或特别重大安全事件发生的，应当予以问责追责，情况十分严重的应报警处理。

第九条 有下列情形之一者，减轻或不追究责任主体的责任：

（一）因不可抗力导致发生的网络与信息安全事故。

（二）有充分证据证明完全落实了相关安全要求，由未知原因导致网络与信息安全事故发生的。

第十条 责任主体主动承认过错并及时修补管理或技术漏洞，视减少损失、挽回影响程度，予以从轻或减轻责任追究。

第三章 责任追究程序和实施

第十一条 责任追究程序包括调查、对调查报告审核、作出责任追究决定等。

第十二条 网络安全和信息化领导小组办公室负责对网络与信息安全事故的调查和对事故责任的初步定性，并对调查报告

进行审核。

第十三条 调查报告的审核重点:

（一）事故的事实是否清楚;

（二）证据是否确实、充分;

（三）性质认定是否准确;

（四）责任划分是否明确。

第十四条 对责任主体的追究决定由领导小组作出,相关部门实施。

第四章 附 则

第十五条 本制度由网络安全和信息化领导小组办公室负责解释。

第十六条 本制度自发布之日起施行。

山东科技大学网络安全和信息化领导小组文件

网信领导小组〔2020〕2号

关于印发《山东科技大学信息系统建设管理办法》的通知

各校区管委，各部门、各单位:

《山东科技大学信息系统建设管理办法》已经山东科技大学网络安全和信息化领导小组研究通过，现予印发，请遵照执行。

山东科技大学网络安全和信息化领导小组

2020 年 6 月 18 日

山东科技大学信息系统建设管理办法

第一章 总 则

第一条 为规范学校信息系统建设与运行维护工作,加强信息系统安全管理,提高信息系统建设与运行维护水平,根据《中华人民共和国网络安全法》《信息安全技术 网络安全等级保护基本要求》(GB/T22239-2019)、《信息技术 软件生存周期过程》(GB/T8566-2007)、《计算机软件文档编制规范》(GB/T8567-2006)等国家、省、市有关法规政策和学校相关管理制度,结合学校工作实际,特制定本办法。

第二条 本办法适用于列入学校信息化建设项目或在学校信息化基础平台上运行的信息系统,其他信息系统建设管理可参照本办法执行。

第三条 信息系统是指为满足学校教学、科研、管理和服务而建设的信息收集、传递、存储、加工、维护和使用的人机交互系统。学校信息系统主要包括业务信息系统(应用系统)和公共服务信息系统。

第四条 信息系统建设涉及到的单位主要包括建设单位、开发单位和对接单位。建设单位是指负责建设信息系统的学校机关部门或学院、研究院等二级单位;开发单位是指通过合法采购流程确定的具体承担信息系统开发工作的软件公司等;对接单位是指信息系统需要对接集成的系统所属单位。

第五条 信息化建设管理应遵循“统一规划、资源共享、安

全高效、管理有序”的原则，按照“同步规划、同步建设、同步运行”的要求，加强信息化建设管理。

第六条 信息系统在建设时应充分考虑数据共享，减少信息的重复收集，应与公共服务信息系统和其他业务系统之间互联互通，避免建成“信息孤岛”。

第七条 信息系统的建设与运行维护分为规划和审核、需求分析、系统设计、系统开发、系统测试、安全检测、初步验收、上线试运行、运行维护等九个阶段。

第二章 组织机构和职责

第八条 网络安全与信息化办公室（以下简称“网信办”）的主要职责：

（一）制定信息系统建设相关管理制度。

（二）协调解决信息系统建设与运行维护过程中出现的重大问题。

（三）审核信息系统建设与运行维护的各阶段工作。

（四）监督各单位在信息系统建设与运行维护过程中严格遵守各项规章制度并认真履行各自职责。

（五）组织实施上线运行的信息系统安全等级保护测评与备案。

（六）负责信息化基础平台运营环境的物理安全、系统安全及网络安全等。

第九条 建设单位的主要职责：

（一）牵头成立信息系统建设项目组，项目组组长一般由建

设单位主要负责人担任,成员主要包括建设单位相关科室负责人、开发单位项目经理、技术人员等。

(二)监督开发单位严格遵守合同及各项规章制度并认真履行职责。

(三)初步审核确认开发单位在信息系统建设各阶段形成的文档,协调对接单位,配合开发单位完成需求调研、系统设计及系统开发工作,负责系统测试、初步验收组织及上线试运行工作。

(四)配合网信办、开发单位完成信息系统安全等级保护测评及备案工作。

(五)负责信息系统的应用安全及数据安全,其中,自行提供信息系统运营环境的单位,还需负责其运营环境的物理安全、系统安全及网络安全等。

第十条 开发单位的主要职责:

(一)负责信息系统的需求调研、系统设计及开发工作。

(二)配合建设单位完成系统测试、安全整改、上线试运行及运行维护工作。

第十一条 对接单位的主要职责:

(一)配合建设单位和开发单位完成系统对接集成方案编制及对接开发工作。

(二)配合建设单位完成系统对接测试工作。

第三章 需求管理

第十二条 项目申报。各建设单位应在每年年底向网信办申报下一年度的信息化建设项目,并提交《信息化项目需求申请表》

（附件 1）进行审核。网信办根据学校信息化需求及信息化经费等情况论证申报项目，并将论证结果上报网络安全和信息化领导小组审定，审定结果由网信办统一反馈给各建设单位。

第十三条 需求调研。需求调研在信息系统建设合同签订后进行，开发单位根据合同规定的建设内容制定需求调研计划，经项目组确认后开展调研工作，建设单位负责协调安排本单位及对接单位相关人员相互配合。

第十四条 需求分析说明书编制。开发单位在需求调研结束后进行需求分析，并向项目组提交需求分析说明书。需求说明书一般应包括：需求总体描述、业务需求、系统接口及对接需求、安全需求、系统管理需求等部分。

第十五条 需求分析说明书审核。项目组对需求分析说明书进行初审，并由组长签字确认，审核通过后方可启动系统设计。

第四章 系统设计

第十六条 系统定级。应根据网络安全等级保护要求对系统进行定级。

第十七条 系统设计说明书编制。开发单位根据需求分析说明书和系统定级结果，进行系统设计，提交系统设计说明书。系统设计说明书应包括系统架构、数据结构、功能模块、集成接口、安全措施（等级保护三级系统设计内容应包含密码技术相关内容）等内容。项目组对系统设计说明书进行初审并由组长签字确认。

第十八条 数据交换与共享方案编制。对于学校基础数据库已有数据，信息系统必须通过统一数据交换与共享平台从学校基

础数据库获得，不得直接通过系统采集；信息系统所产生的基础数据应通过统一数据交换与共享平台推送至学校基础数据库。

第十九条 系统对接与集成方案编制。面向师生服务的信息系统，必须与学校统一身份认证系统进行认证集成。

第二十条 系统设计说明书及相关方案审核。建设单位将相关说明书及方案一并提交到网信办，由网信办视情况聘请专家进行论证，审核通过后方可启动系统开发。

第五章 系统开发

第二十一条 开发计划。开发单位必须在系统开发前制定详细、合理的项目开发计划，项目组负责审核并由组长签字确认。

第二十二条 工程监理。项目应依据实际情况实施工程监理，按照信息系统工程监理的有关规定，委托工程监理单位对项目建设进行工程监理。

第二十三条 组织实施。开发单位根据系统设计说明书及系统对接与集成方案，按照开发计划规定的进度进行信息系统开发。项目组按照开发计划中的时间节点要求，对开发单位的工作进行检查督促，并协调对接单位配合开发单位的对接集成开发。

第二十四条 开发规范。开发单位在系统开发过程中应结合国家、行业及学校相关规范和标准等制定系统开发规范，并严格遵照执行。

第二十五条 需求变更。在系统开发过程中，建设单位和开发单位均可根据实际情况及合同约定提出需求变更，变更内容经项目组讨论确定后拟定需求变更说明书，开发单位根据该说明书

对相关设计说明书、系统对接集成方案及开发计划进行修订，修订后的内容由项目组审核，并经组长签字确认生效。

第二十六条 延期处理。由于客观条件发生变化等原因造成项目未能按实施计划的时间节点完成的，开发单位必须至少提前一个月，向建设单位提交项目延期说明书，经项目组审核后由组长签字确认。未经确认的项目延期，开发单位需承担违约责任。

第二十七条 开发环境。系统的开发环境由开发单位或建设单位提供，不得使用学校信息化基础平台资源。

第六章 系统测试

第二十八条 测试文档。开发完毕需进行测试的信息系统，由开发单位提交测试文档，至少应包括：功能测试用例、安全性测试用例（如等保三级系统还应包含密码应用安全性测试相关内容）、测试报告（含单元测试、集成测试、性能测试等）、系统安装部署文档及系统安装文件。项目组对测试文档进行审核并由组长签字确认后方可进行系统测试。

第二十九条 测试环境。需在学校信息化基础平台上运行的信息系统由建设单位向网信办申请测试服务器，测试环境的管理与维护由建设单位指定专人负责，网信办对测试环境进行安全审计。

第三十条 测试数据。建设单位负责为开发单位提供与信息系统数据格式一致的测试数据；信息系统使用学校基础数据的，由网信办提供测试数据。测试数据一律不得直接使用真实数据。

第三十一条 测试步骤。开发单位按照系统安装文档部署测

试环境；建设单位依据需求、设计文档、技术参数要求，完成系统综合测试，并形成综合测试报告。

第三十二条 测试整改。对于测试中发现的问题，开发单位应积极进行整改，直至测试通过。

第三十三条 更新测试。系统测试完毕后，开发单位如需对系统进行更新，必须先向项目组提交系统更新包及相应的更新安装说明和更新测试材料，项目组审核后，方可安装到测试环境进行更新测试。

第七章 安全检测

第三十四条 技术检测。建设单位或开发单位负责依照项目安全保护等级及相关规定进行技术检测。检测手段主要包括对信息系统源代码进行代码审计、对信息系统进行漏洞扫描等。

第三十五条 安全检测报告及整改意见。建设单位或开发单位应根据技术检测结果出具安全检测报告及整改意见。如因特殊原因无法提供源代码的，应由开发单位委托具有中国计量（CAM）认证和中国合格评定国家委员会（CNAS）认可实验室证书等资质的第三方软件代码测评机构，出具代码审计合格报告。

第三十六条 安全整改。开发单位根据整改意见对系统进行整改，直至安全检测通过为止。

第八章 初步验收

第三十七条 初步验收条件。信息系统完成综合测试，通过安全检测，可进行初步验收。

第三十八条 初步验收组织。建设单位负责组织由项目组及

网信办专家组成的初步验收小组对信息系统进行初步验收。

第三十九条 初步验收形式及内容。初步验收小组应听取开发单位工作报告及系统演示并对各阶段文档进行审阅，依照合同及需求分析说明书的内容，对信息系统完成情况及质量进行评价并提出意见和建议。

第四十条 初步验收报告。初步验收通过后，应形成信息系统初步验收报告，并由项目组长签字确认。

第九章 上线试运行

第四十一条 上线试运行申请。建设单位向网信办提交《信息系统上线试运行申请表》（附件 2）及初步验收报告，经审核批准后方可上线试运行。

第四十二条 运行环境。建设单位可向网信办申请学校信息化基础平台资源用于信息系统的运行。建设单位自行提供运营环境的，须严格按照网络安全保护等级要求进行配置。

第四十三条 运行文档。在学校信息化基础平台上运行的信息系统，建设和开发单位必须在申请运营环境的同时，向网信办提交系统安装部署说明、系统维护手册、系统使用手册、系统测试报告及安全检测报告等文档，以及系统最终版本的安装文件。

第四十四条 安装部署。网信办根据建设单位需求及相关规定，进行运营环境配置及信息系统的安装部署。

第四十五条 权限配置。建设单位应指定专人，负责信息系统中各类用户账号管理及权限配置。上线试运行前，所有测试账号或由开发单位使用的账号由建设单位删除或收回。

第四十六条 试运行期限。系统试运行期一般不少于 1 个月、不多于 3 个月。试运行期满且情况良好的，可进行竣工验收。竣工验收通过，信息系统方可上线正式运行。

第四十七条 归档管理。信息系统的开发合同、设计文档、测试文档、系统代码、验收报告等，按《高等学校档案管理办法》要求移交档案馆。系统安装部署说明、系统维护手册、系统使用手册、系统测试报告及安全检测报告等文档移交网信办。

第十章 运行维护

第四十八条 运行维护工作原则。建设单位负责信息系统的维护与管理，制定运维工作制度，建立运维工作机制，确保运行维护工作的持续性和有效性。

第四十九条 系统更新流程。对信息系统进行更新时，由建设单位和开发单位在测试环境完成更新测试，测试通过后填写并向网信办提交《信息系统更新申请表》（附件 3）。

第五十条 数据备份。为保证数据备份的及时性、准确性，由建设单位负责进行业务数据备份，备份的保留周期一般为 6 个月，建设单位有特殊要求的，可委托网信办进行数据备份工作。

第五十一条 故障处理。建设单位根据业务要求制定信息系统故障处理应急预案；网信办制定应急响应综合预案。由建设单位牵头，协调有关部门按照“分级负责、协同处理、快速反应、有力保障”的原则进行故障处理。

第五十二条 用户服务。建设单位应通过服务电话、电子信箱等多种渠道主动收集和解答用户对信息系统的咨询、意见和建

议，并根据用户意见及时对系统进行调整与更新。

第十一章 安全管理

第五十三条 安全监测。建设单位应对信息系统的运行状况进行监控。网信办定期对信息系统进行安全技术检测。

第五十四条 安全事件整改。网信办会同建设单位及开发单位，依照《网络安全事件报告与处置流程》，对发现的安全事件进行整改和处置。

第五十五条 等保测评与备案。信息系统上线运 3 个月之内，依照《信息安全技术网络安全等级保护基本要求》，由网信办组织完成信息系统的网络安全等级保护测评与备案工作。

第十二章 监督评价与责任追究

第五十六条 监督评价。网信办负责对学校各类信息系统的建设、运维服务和安全保障进行监督，每年组织一次考核评价，将考核评价结果纳入单位的年度绩效考核，并作为各单位后续信息化建设经费审批的主要依据。

第五十七条 责任追究。因违反本办法之规定造成信息系统建设无法通过验收或在运行过程中造成事故的，追究相关责任人的责任。

第十三章 附 则

第五十八条 本办法由网络安全与信息化办公室负责解释。

第五十九条 本办法自发布之日起施行。

附件 1：

项目编号:

信息化项目需求申请表

建设单位		申请日期	
申请人		项目名称	
申请原因			
项目需求及建设目标			
项目内容			
建设单位及相关部门负责人签字	签字: 日期: 年 月 日		
网信办审核意见	签字: 日期: 年 月 日		
领导小组审批意见	签字: 日期: 年 月 日		

注：此表可添加附页

附件 2：

项目编号:

信息系统上线试运行申请表

建设单位		**日期**	
申请人		**项目名称**	
XXX 项目各子系统已通过初步测试，申请进入项目的上线试运行阶段，请予以审批。 申请人: 日期: 年 月 日			
审批意见	签字: 日期: 年 月 日		

注：附初步验收报告

附件 3：

项目编号:

信息系统更新申请表

建设单位		**申请日期**	
申请人		**项目名称**	
变更描述	现状描述:		
	需求变更描述:		
审批意见	签字: 日期: 年 月 日		

山东科技大学域名管理办法

第一章 总 则

第一条 为规范学校互联网络域名管理,推进学校信息化建设，根据《互联网信息服务管理办法》《中国互联网络域名管理办法》及有关法规政策和学校管理制度，结合学校实际，制定本办法。

第二条 本办法适用于各部门、各单位(以下简称“各单位”)网站。

第三条 各单位设立互联网站，应使用学校互联网络域名。除以下情况外,各单位不得申请非学校互联网络域名或者解析到非校园网所属 IP 地址:

（一）上级主管部门要求使用非学校互联网络域名或 IP 地址。

（二）因国际交流合作，需要使用非学校互联网络域名或 IP 地址。

第四条 以下本文所指“域名”，如无特殊说明均特指学校互联网络域名。

第五条 网络安全与信息化办公室（以下简称“网信办”）负责域名注册、注销和管理工作。

第二章 域名管理

第六条 网信办为各单位网站提供域名服务，域名为:

.sdust.edu.cn，其中“”为二级单位汉语拼音首个字母组合。

第七条 域名服务遵循“先注册先使用”原则，为维护学校利益和公众利益，网信办可对部分保留字进行必要保护。

第八条 学校校园网域名的解析由网信办负责技术实现。网信办依法设立域名服务器，未经网信办授权，校内其他任何单位不得设立域名服务器。

第九条 每个备案的网站，只能申请注册一个域名，学校域名不接受个人申请注册。

第十条 域名使用单位应当遵守国家有关互联网络的法律、行政法规和规章。因注册或使用域名而侵害他人合法权益的责任，由域名使用单位承担。

第十一条 网信办有义务配合国家主管部门开展网站检查工作，必要时按要求暂停或中止相关的解析服务。

第十二条 学校不对任何单位及个人提供组织机构代码证复印件及其他资质文件用于非学校互联网络域名的登记和注册。

第三章 域名注册

第十三条 学校一级域名由网信办向有关域名注册管理机构办理申请、注册手续。

第十四条 学校一级域名之下的域名，各单位应详细填写《域名申请表》(见附件)，由主管领导签字盖章后，提交到网信办，网信办将根据实际情况反馈审核意见。

第十五条 各单位或组织可以因以下用途申请注册使用学校互联网络二级及以下域名:

（一）各单位，部省级及以上科研机构、教学基地，以学校名义参加的国际合作科研机构，学校批准设立的研究院（所）、委员会、中心等组织，设立单位网站。

（二）各单位经批准建设的学校主要信息系统。

（三）经学校批准开展的重要活动（会议），其主办方设立活动（会议）专门网站。

（四）其他需要申请域名的情况。

第十六条 申请注册的域名名称应使用组织机构名称、信息系统业务名称、活动（会议）主题的汉语拼音首字母组合。

第十七条 域名注册申请单位应当提交真实、准确、完整的域名注册信息，域名注册完成后，该域名即可由注册单位使用。

第十八条 域名注册信息发生变更的，域名使用单位应当在变更后 30 日内，向网信办提交《域名申请表》，申请变更注册信息。

第四章 域名注销

第十九条 出现下列情形之一时，域名使用单位应提交《域名申请表》向网信办申请注销所注册域名：

（一）域名对应的网站或信息系统不再设立。

（二）因活动（会议）注册使用域名，活动（会议）已经结束。

（三）域名使用部门不再使用所注册域名。

第二十条 已注册的域名出现下列情形之一时，网信办应当予以注销，并视需要以书面形式通知域名使用部门：

（一）域名使用部门申请注销域名的。

（二）域名使用部门提交的域名注册信息不真实、不准确、不完整的。

（三）域名对应的信息系统/网站未按学校规定履行备案手续的。

（四）依据人民法院、仲裁机构或域名争议解决机构作出的裁判，应当注销的。

（五）违反相关法律、行政法规及本办法规定的。

第五章 附 则

第二十一条 本办法由网络安全与信息化办公室负责解释。

第二十二条 本办法自发布之日起施行。

附件

域名申请表

申请单位		**联系人**	
联系人电话		**电子邮箱**	
类型	□注册 □变更 □注销		
申请理由			
域名注册			
添加域名		**端口号**	
对应 IP		**服务器地点**	
域名变更			
原域名		**新域名**	
原 IP		**新 IP**	
域名注销			
曾用域名		**曾用域名对应 IP**	
申请单位盖章： 负责人签字： 日期： 年 月 日			
网络安全与信息化办公室审核意见：(盖章) 负责人签字： 日期： 年 月 日			
完成时间		**完成人签字**	

山东科技大学信息系统运维安全管理办法

第一章 总 则

第一条 为加强学校信息安全保障能力，建立健全安全管理体系，规范信息系统的安全运维工作，提高整体的网络与信息安全管理水平，确保信息系统的安全可靠运行，根据《中华人民共和国网络安全法》《信息安全等级保护管理办法》《中华人民共和国密码法》等国家、省、市有关法规政策和学校管理制度，结合学校实际，制定本办法。

第二条 本办法适用于学校信息系统运行与维护安全管理。

第三条 信息系统运维安全管理应遵循“谁建设谁管理，谁使用谁负责”的原则，严格落实信息系统管理责任；依照“积极预防、全面保障、动态管理、持续改进”的原则，加强信息系统运维安全管理。

第四条 数据中心机房安全管理详见《数据中心机房安全管理办法》。

第五条 联网终端、服务器、网络与安全等设备以及应用系统的安全基线配置规范参考《网络安全配置基线》。

第六条 漏洞和风险管理见《网络安全漏洞整改流程》。

第二章 组织机构和职责

第七条 网络安全和信息化领导小组（以下简称“领导小组”）负责信息系统运维安全管理的领导和统筹工作。

第八条 网络安全与信息化办公室（以下简称“网信办”）负责为信息系统安全运行提供可靠的运行环境，协助系统使用部门进行系统变更管理，负责所用密码产品的管理等工作。

第九条 信息系统建设单位负责所建系统的运维安全管理，包括数据备份与恢复、恶意代码防范和密码管理等工作。

第三章 网络设备运维安全管理

第十条 设备运维

（一）定期巡查服务器及磁盘阵列运行情况，填写《服务器操作系统巡检记录表》（见附件），发现异常应及时处理。

（二）主机事故（如数据丢失、宕机等）上报网信办，视情启动信息系统安全应急预案，进行有效处置。

（三）重要信息系统的服务器和磁盘阵列设备要有容灾措施。

（四）对送出维修或报废的介质应首先清除介质中的敏感数据。

第十一条 网络运维

（一）网络运维管理人员应保证网络设备的业务处理能力满足业务高峰期需要，如主要网络设备（核心交换机、路由器）CPU 及内存使用率峰值均低于 70%。

（二）网络访问权限应遵循最小权限原则，仅开放其工作或业务所需要的最小网络访问权限。

（三）校外地址访问校内资源需通过 VPN 连接。

第十二条 网络设备安全配置

（一）严禁任何未经授权的网络设备维护操作。服务厂商在

学校内提供技术支持时，须由运维管理人员全程陪同。

（二）网络配置信息变更应制定严密的变更计划，操作应按既定方案进行，遵循“双人在场、不得单人进行变更”的操作原则，加强监督与复核。

（三）运维管理人员应确保网络设备和安全设备的密码符合复杂度要求，密码 8 位以上，包含字母、数字及特殊符号，密码至少每三个月更换一次。

（四）网络设备应设置登录失败处理及登录超时锁定策略。

（五）核心网络、主干网络传输设备应有容灾措施。

第十三条 网络监控

应对网络运行状况进行监控。网络设备需开启日志记录功能，定期对日志文件进行归档保存，以便于日志的查询、分析和审计；所有网络日志留存不少于 6 个月。

第四章 信息系统运维安全管理

第十四条 信息系统配置安全管理

（一）信息系统的访问权限应遵循最小权限原则，仅开放其工作或业务所需要的最小网络访问权限。

（二）应定期对信息系统的访问权限进行核查，确认当前网络访问权限设置符合业务和管理上的需求，对于不符合的部分应当予以及时更正、调整。

（三）信息系统应开启日志记录功能，定期对日志文件进行归档保存，以便于日志的查询、分析和审计；所有日志留存不少于 6 个月。

（四）信息系统的管理密码应符合复杂度要求，密码 8 位以上，包含字母、数字及特殊符号，密码至少每三个月更换一次。

（五）信息系统应设置管理地址限制，仅允许运维管理人员使用的设备进行登录管理。

（六）信息系统应设置登录失败处理及登录超时锁定策略。

（七）信息系统应通过加密的传输协议进行远程管理，不得使用明文传输协议。

第十五条 信息系统访问控制

（一）信息系统应设置管理地址限制，仅允许运维管理人员使用的设备进行登录管理。

（二）信息系统应设置登录失败处理及登录超时锁定策略。

（三）运维管理人员对用户访问权限的限制应基于用户的角色分工、业务应用要求和用户的工作需要。

第五章 数据备份与恢复管理

第十六条 应加强数据的备份和恢复管理，确保备份数据的可用性、完整性和保密性，保障业务连续性。

第十七条 数据备份策略应包括：备份对象、责任人、操作步骤、频率、方式、存储介质、命名规则、保存期以及有效性测试周期等；数据恢复策略应包括：责任人、触发条件、操作步骤等。

第十八条 备份数据应存储在访问受控的专用存储设备或者存储介质中，定期对备份介质进行测试并记录测试结果，确保备份介质内的数据可恢复。

第十九条 重要系统的业务数据及系统配置信息的备份应至少保留两份，一份为本地备份、一份为异地备份，异地备份存储环境要与本地环境相同。

第二十条 进行数据恢复时，要制定恢复计划，经系统所属单位批准。

第六章 恶意代码防范管理

第二十一条 设置可集中管理的防病毒系统，对服务器端的病毒代码库、补丁库进行监控，确保能同服务商保持同步更新。

第二十二条 系统补丁更新应经过评估、测试，确认对系统稳定性没有影响后，再进行相关补丁更新工作。

第二十三条 应定期对信息系统和网络进行漏洞扫描，发现安全漏洞及时修补。

第七章 密码管理

第二十四条 信息系统建设单位负责密码的管理工作，遵循密码相关国家标准和行业标准，使用国家密码管理主管部门认证核准的密码技术和产品，规范密码管理。

第八章 附 则

第二十五条 本办法由网络安全与信息化办公室负责解释。

第二十六条 本办法自发布之日起施行。

附件

服务器操作系统巡检记录表

服务器基本信息				
业务系统				
配置信息	信息资产编号		CPU	
	主机名		内存	
	操作系统		IP 地址	
	硬盘分区	C： ； D： ； E： ；		

系统运行情况检查			
序号	检查内容	检查方法	检查结果
1	操作系统版本检查	运行命令 winver，记录操作系统版本。	正常□ 异常□
2	CPU 利用率检查	查看 CPU 利用率，非业务高峰期低于 50％。	正常□ 异常□
3	内存利用率检查	查看内存利用率，非业务高峰期低于 75％。	正常□ 异常□
4	硬盘空间使用率检查	通过磁盘管理器查看各系统分区磁盘使用率，系统盘使用率低于 8 0％。	正常□ 异常□
5	网络连接情况检查	运行命令 ping，测试网关通信情况，查看延时及是否有丢包现象。	正常□ 异常□
6	Host 文件及 DNS 检查	查看 Hosts 文件及 DNS 配置，DNS 解析是否正常。	正常□ 异常□

安全检查			
序号	检查内容	检查方法	检查结果
7	检查系统补丁更新情况	查看系统补丁是否及时更新，重要补丁是否已安装。	正常□ 异常□
8	查看系统杀毒软件安装情况	查看系统杀毒软件版本，相应的病毒库版本。	正常□ 异常□
9	查看系统日志	查看系统日志中无错误日志或者错误日志不影响系统运行。	正常□ 异常□

异常问题记录	处理结果记录:

巡检人: 日期:

山东科技大学外包服务信息安全管理办法

第一章 总 则

第一条 为加强对外包服务的信息安全管理，明确管理责任和管理要求，抵御外来风险，提高信息安全管理水平，《中华人民共和国网络安全法》《信息安全技术网络安全等级保护基本要求（GB/T22239-2019）》《关于境内企业承接服务外包业务信息保护的若干规定》等国家、省、市有关法规政策和学校管理制度，结合学校实际，制定本办法。

第二条 本办法适用于学校所有信息系统。本规定所指外包包括外包服务公司、外包服务人员、第三方信息系统和第三方终端。

（一）外包服务公司（以下简称“外包公司”）是指以签订项目合同方式，提供网络安全和信息系统技术开发、系统运维、安全检查、等保测评、应急处置等服务的外部公司或部门。

（二）外包服务人员（以下简称“外包人员”）是指上述外包公司委派的工作的人员。

（三）第三方信息系统（以下简称“第三方系统”）是指外包公司为提供服务需要所部署的信息系统。

（四）第三方终端是指外包人员携带并在校园网内部使用的信息通信终端。

第三条 应遵循“合规性、预防性、有限授权、监督制约”的原则，加强外包服务信息安全管理。

第二章 组织机构和职责

第四条 网络安全和信息化领导小组（简称“领导小组”）负责外包服务信息安全管理的领导和统筹工作。

第五条 网络安全与信息化办公室（以下简称“网信办”）负责对外包服务信息安全管理进行合同备案和监督检查。

第六条 各部门、各单位（以下简称“各单位”）负责外包服务的基本情况调查、合同签订和服务管理等，并将外包服务合同提交网信办备案。

第三章 外包公司安全管理

第七条 各单位与外包公司签订的合同中应包含保密协议（见附件一），保密协议的条款中应明确相关信息安全的要求及处罚要求。

第八条 应在合同中明确外包公司在信息安全方面的职责和合同终止后的有效期限。

第九条 外包公司应在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确。

第十条 外包公司在学校以往的服务项目中出现过重大的信息安全违规事件，不得再引入该合作公司。

第四章 外包人员安全管理

第十一条 各单位应与外包人员签署《保密承诺书》（见附件二），明确保密范围、保密责任、违约责任、有效期限等内容。

第十二条 外包人员开设账户访问系统需提交《信息系统账号开通申请表》(见附件三),各单位审批后由专人开设账户、分配权限、并登记备案,服务结束后应及时清除其所有的访问权限。

第十三条 外包人员的账号口令必须满足信息系统管理规定,必须使用 8 位以上的复杂口令。外包人员的账号、认证、授权管理和安全审计应纳入系统集中管控。

第十四条 禁止外包人员在未授权的情况下通过远程方式接入,因特殊情况需要通过远程登录,须经网信办审批授权后,临时开通远程登录功能,用毕及时撤销。

第十五条 外包人员离岗时,各单位应及时完成外包人员的账号撤销、设备安全检查审核、技术资料移交等工作。

第十六条 外包人员在学校以往的服务项目中出现过重大的安全违规事件,该人员不得再继续为学校提供服务。

第五章 第三方系统安全管理

第十七条 第三方系统需与内部系统互联时,应提交《信息系统接入申请表》(见附件四),经网信办审核通过后进行连接。

第十八条 第三方系统在入网前必须通过安全评估和安全测试,确保第三方系统符合内部系统安全技术要求。

第十九条 外包公司应妥善保存第三方系统所有系统信息、客户信息、操作日志等,保存期限不少于 6 个月。

第六章 第三方终端安全管理

第二十条 第三方终端如需接入学校网络或服务器，其终端应符合下述要求:

（一）必须安装病毒库更新至最新的杀毒软件，且终端经查杀后，没有病毒。

（二）必须将系统补丁更新至最新。

（三）除业务需要，不得安装任何漏洞扫描软件或手工对学校网络进行探测。

（四）不得安装任何监控软件对学校网络数据进行捕捉和分析。

第二十一条 第三方终端需与内部系统互联时，应提交《信息系统接入申请表》，经网信办审核通过后进行连接。网信办应对第三方终端进行安全审核、检查。

第七章 检查和监督

第二十二条 网信办应定期检查外包服务涉及的网络链路、安全设备、网络设备和服务器等的运行状况，审查外包服务涉及的安全策略、审计数据、恶意代码、补丁升级等安全相关事项的工作情况。

第二十三条 网信办根据不同时期及重大活动阶段，依据网络安全关注重点对外包服务进行专项的信息安全检查和审查，确保外包服务的可用性和数据的可靠性。

第八章 附 则

第二十四条 本办法由网络安全与信息化办公室负责解释。

第二十五条 本办法自发布之日起施行。

附件一

保密协议

甲方：_____

乙方：_____ 项目名称：_____ 项目组成员：_____

乙方因参与甲方关于_____项目的有关工作，已经（或将要）知悉甲方关于该项目的商业秘密。为了明确乙方的保密义务，甲、乙双方本着平等自愿、公平诚信的原则，依据《中华人民共和国劳动法》、《中华人民共和国反不正当竞争法》订立本保密协议。

第一条 保密的内容和范围

甲、乙双方确认，乙方应承担保密义务的甲方关于该项目的商业秘密范围包括但不限于：

1. 学校各信息系统所涉及的全部软、硬件管理用户名称及密码，以及软、硬件系统相关的配置信息。
2. 学校各信息系统数据库内的数据内容：包括人员信息、文档内容、消费记录等。
3. 学校购置或拥有自主产权的计算机软件、数据、参考资料、合同文件、图纸以及其他相关资料等。
4. 由学校信息系统为资源产生的其他衍生内容，包括数据统计信息、查询内容、报表内容等。
5. 学校内部各监控系统采集的视频内容等。

第二条 乙方在向甲方提供服务，应履行以下义务：

1. 乙方应自觉维护甲方的利益，严格遵守甲方的相关规定。
2. 乙方要加强服务人员管理，服务期内人员的任何行为都视为经过乙方授权。

3. 乙方不得向任何个人和机构泄露甲方的任何资料信息；不得利用所掌握的甲方工作秘密牟取私利；在未得到甲方书面许可的情况下，不得将任何数据给披露任何其他人士或机构。
4. 服务期结束后乙方人员要马上清除服务期间接触的甲方数据，并不得向任何个人和机构提供甲方的工作和数据信息。

第三条 乙方若违反本协议约定安全保密义务，甲方有权采取以下措施：

1. 乙方违约行为造成甲方经济损失的，有权要求乙方进行民事赔偿，并按照合同额的_____扣减该项目的服务费用。
2. 乙方违约行为构成犯罪的，拟请有关机关依法追究其刑事责任。

第四条 无论乙方因何种原因离开项目，乙方离去之后仍对其在甲方工作期间接触、知悉的甲方工作秘密承担如同工作期间一样的保密义务。

第五条 双方因履行本协议发生争议的，可向甲方所在地劳动仲裁机构申请仲裁或向人民法院提起诉讼。

第六条 双方一致同意对本协议补充、修改时，以书面方式签订补充或变更协议。

第七条 双方确认，在签署本协议前已仔细审阅过协议的内容，并完全了解协议各条款的法律含义。

第八条 本协议一式两份，甲乙双方各执一份，具有同等法律效力，自甲方签字盖章、乙方签字后生效。

甲方：（盖章） 乙方：（盖章）

甲方代表： 乙方代表：

年 月 日 年 月 日

附件二

保密承诺书

我了解保密政策相关法律、法规和纪律，知悉应当承担的保密义务和责任。本人承诺：

一、遵守国家保密政策、法律、法规和纪律，履行保密义务，自愿接受保密审查。

二、按照统一授权和要求进行技术开发，妥善保管系统开发相关的操作系统、数据库、中间件、服务器、应用软件等平台的源代码、用户名和密码等，不以任何形式向其他人员违规授权或透露。

三、不越权进行信息检索和查询，不违规记录、存储、复制系统内的任何数据信息，不携带任何系统内信息离开工作现场，不违规留存这些信息的载体。

四、不以任何方式泄露、篡改、破坏系统内学校、个人基本信息和业务信息。

五、不以任何方式窃取其他开发人员、工作人员等的账号和密码，不使用其他人员账户登录系统进行开发或测试，不在系统生产环境中进行任何违规业务操作。

若违反上述承诺，自愿承担党纪、政纪责任和法律后果。

工作单位：（可打印）_____

姓　　名：（可打印）　身份证号：（可打印）_____

承诺人签名：

年　　月　　日

注：本承诺书必须由开发人员本人签名，不允许别人代签！

附件三

信息系统账号开通申请表

<table>
<tr><td>外包公司名称</td><td colspan="5"></td></tr>
<tr><td>外包人员
（使用责任人）</td><td></td><td>联系电话</td><td></td><td>邮箱</td><td></td></tr>
<tr><td>使用期限</td><td colspan="5">20　年　月　日—— 20　年　月　日</td></tr>
<tr><td>所在系统</td><td colspan="5"></td></tr>
<tr><td>账号类型</td><td colspan="5">☐ 管理员账号，备注____
☐ 测试账号
☐ 业务账号</td></tr>
<tr><td>账户名称</td><td colspan="5"></td></tr>
<tr><td>申请理由</td><td colspan="5"></td></tr>
<tr><td colspan="6">单位意见：
☐ 有必要性，同意申请。
☐ 暂无必要性，不同意。

签字：
日期：　年　月　日</td></tr>
<tr><td colspan="6">备注：</td></tr>
</table>

附件四

信息系统接入申请表

<table>
<tr><td>外包单位名称</td><td colspan="5"></td></tr>
<tr><td>外包人员
（使用责任人）</td><td></td><td>联系电话</td><td></td><td>邮箱</td><td></td></tr>
<tr><td colspan="2">申请接入系统/终端名称</td><td colspan="4"></td></tr>
<tr><td>使用期限</td><td colspan="5">20　年　月　日—— 20　年　月　日</td></tr>
<tr><td colspan="6">申请理由：（需详细写明系统/终端接入申请原因、接入方式和用途）

签字：
日期：　年　月　日</td></tr>
<tr><td colspan="6">网络安全与信息化办公室意见：
☐ 有必要性，同意申请。
☐ 暂无必要性，不同意。

签字：
日期：　年　月　日</td></tr>
<tr><td colspan="6">备注：</td></tr>
</table>

山东科技大学网络安全事件报告与处置办法

第一章 总 则

第一条 为了切实做好学校网络安全事件的防范和应急响应工作，提高学校预防和控制网络安全事件的能力和水平，减轻或消除网络安全事件的危害和影响，根据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《信息安全事件分类分级指南（GB/Z20986-2007）》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》《教育信息化“十三五”规划》等相关规定以及学校制定的《山东科技大学突发事件总体应急预案》及各专项应急预案等文件，制定本办法。

第二条 本办法适用于学校各部门、各单位（以下简称“各单位”）发生的校园网络与信息安全事件的报告与处置工作。

第三条 本办法中所称的校园网络与信息安全事件是指攻击事件、故障事件、灾害事件以及不能归为以上分类的其他网络安全事件，具体内容见《网络安全事件应急响应综合预案》。

第四条 依据“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，逐级落实网络与信息安全责任，实现明确责任、突出重点、自主防护、保障安全的目标。

第二章 安全事件等级划分与判定

第五条 安全事件等级划分。依照《信息安全事件分类分级指南（GB/Z20986-2007）》，综合信息系统损失和社会影响程

度两个方面，对学校网络与信息安全事件分为四个等级，分别为：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级），具体内容见《网络安全事件应急响应综合预案》。

第六条 安全事件判定。各单位一旦发生安全事件，应根据安全事件等级划分迅速自主判定安全事件等级。网络安全与信息化办公室（以下简称“网信办”）在接到报告后，根据事件情况，进一步做出判定。必要时网信办报告网络安全和信息化领导小组（以下简称“领导小组”），由领导小组判定。

第三章 安全事件的报告与处置

第七条 特别重大事件（Ⅰ级）以及重大事件（Ⅱ级）的报告与处置。报告与处置分为三个步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

（一）事发紧急报告与处置

1. 工作人员一旦发现上述安全事件，应立即通知网信办，对事件进行拍照，并保留现场。

2. 紧急通知内容包括：事件发现时间、位置、内容、处理等。

3. 网信办根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，并进一步判定安全事件等级，对确认属于特别重大事件（Ⅰ级）以及重大事件（Ⅱ级）安全事件的，应及时报告领导小组。

4. 紧急报告内容包括：时间地点、简要经过、事件类型与

分级、影响范围、危害程度、初步原因分析、已采取的应急措施。

5. 领导小组接到报告后，应立即组织相关单位人员赶赴现场进行紧急处置。

6. 报警处理。网信办协助公安机关做好相关取证和处置工作。

（二）事中情况报告与处置

1. 事中情况报告应在安全事件发现后 1 日内以书面报告的形式进行报送，报送内容和格式见《网络安全事件应急响应综合预案》附件 4-网络安全事件报告表。

2. 事中情况报告由应急响应实施小组负责人组织编写，由网信办负责人审核签字后，报送领导小组。

3. 安全事件的事中处置包括：掌握损失情况、分析事件原因、修复系统漏洞、恢复系统服务、减少负面影响。

（三）事后整改报告与处置

1. 事后整改报告应在安全事件处置完毕后 4 个工作日内以书面报告的形式进行报送，报送内容和格式见《网络安全事件应急响应综合预案》附件 5-网络安全事件应急响应结果报告表。

2. 事后情况报告由应急响应实施小组负责人组织编写，由网信办负责人审核签字后，报送领导小组。

3. 安全事件事后处置包括：总结事件教训、研判安全现状、排查安全隐患、加强制度建设、提升防护能力。

第八条 较大事件（III级）的报告与处置。

（一）工作人员一旦发现较大事件（III级），应立即通知网信办工作人员，对事件进行拍照，并保留现场。

（二）紧急通知内容包括：事件发现时间、位置、内容、处理等。

（三）网信办根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，并进一步判定安全事件等级，对确认较大事件（III级）安全事件的，由网信办进行处理。

（四）网信办应立即组织应急响应实施小组赶赴现场进行处置，必要时联系维护支撑单位协助处理。

（五）在事件处置完毕后 6 天内向领导小组报送整改报告，报告内容和格式见《网络安全事件应急响应综合预案》附件 5-网络安全事件应急响应结果报告表。

第九条 一般事件（IV级）的报告与处置。各单位发生一般安全事件，应及时、自主组织应急处置工作，或联系网信办予以协助。在事件处置完毕后 6 天内向网信办报送整改报告，报告内容和格式见《网络安全事件应急响应综合预案》附件 5-网络安全事件应急响应结果报告表。

第四章 配套制度与问责

第十条 各单位应建立健全本单位安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练。

第十一条 未按规定落实相关网络与信息安全管理制度及技术规范，导致网络安全事件发生的，按有关规定处理。

第五章 附 则

第十二条 本办法由网络安全与信息化办公室负责解释。

第十三条 本办法自发布之日起施行。

山东科技大学网络安全漏洞整改流程

第一章 总 则

第一条 为了规范学校信息系统安全漏洞整改流程，确保尽早发现安全漏洞,及时消除安全隐患,加快安全处置响应时间，保障信息资产安全，根据《中华人民共和国网络安全法》《信息安全技术安全漏洞划分指南（GB/T30279-2013）》《信息安全技术信息安全漏洞管理规范（GB/T30276-2013）》等法律法规，结合学校实际，特制定本流程。

第二条 本流程适用于学校信息系统、操作系统、数据库、中间件、网络设备和安全设备的漏洞预防、发现、处置和跟踪等流程。

第三条 安全漏洞主要指信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷，这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中,一旦被恶意主体利用，就会对信息系统的安全造成损害，影响信息系统的正常运行。

第二章 组织机构与职责

第四条 网络安全与信息化办公室（以下简称“网信办”）工作职责:

（一）负责学校信息安全漏洞的检测、评估、通报、应急处置和整改督办工作。

（二）为学校各部门、各单位（以下简称“各单位”）信息系统的漏洞整改工作提供建议和技术支持。

第五条 按照“谁主管、谁负责，谁使用、谁负责”的原则，各单位负责对本单位所建设、管理、使用的信息系统的信息安全漏洞进行自查、整改、验证、跟踪、报告等工作。

第三章 级别定义和处理时间

第六条 根据潜在危害、重复利用的可能性、利用的困难程度、影响的用户范围和发现的难易程度进行评估，根据评估的风险等级从低至高，将信息安全漏洞划分为四个等级，依次为低、中、高和紧急漏洞。

第七条 根据相关机构或相关安全软件有明确定义安全等级的漏洞按照其标准确定等级，没有明确级别的，网信办依据DREAD模型（见附件一）负责对信息安全漏洞的危险等级进行评估，确定漏洞的危害等级，对不同等级的信息安全漏洞采取不同的处置措施。

第八条 依据信息系统部署的方式和级别，以及发现的安全漏洞级别，明确安全漏洞整改时效（见附件二）。

第四章 漏洞处理流程

第九条 根据安全漏洞生命周期中漏洞所处的不同状态，将漏洞管理行为对应为预防、发现、评估、修补、验证、跟踪等阶段（见附件三）。

（一）漏洞的预防

信息系统所属单位应依据已发布的安全配置标准，对计算机操作系统进行安全加固、及时安装补丁、关闭不必要的服务、安装安全防护产品和开启相应的安全配置等。

（二）漏洞的发现

1. 来自教育主管部门、公安部门以及相关主管部门的安全漏洞和安全威胁通报。

2. 来自信息安全服务厂商等的安全漏洞通知，渗透测试结果及风险评估报告。

3. 学校自查发现的信息安全漏洞。

（三）风险的评估

1. 网信办应在规定时间内验证通报、自行发现或收集到的漏洞是否真实存在，并依据 DREAD 模型，确定漏洞的风险等级。

2. 根据风险等级判断是否需要对风险进行处理，可接受风险不处理，不可接受风险需要处理。

3. 网信办把需要处理的安全漏洞通知到相关的负责人并发出《山东科技大学网络安全隐患整改通知书》（见附件四），在漏洞未整改完成前，仅发送给信息系统涉及的管理人员和需要进行配合的厂商，对敏感信息进行屏蔽。

4. 网信办应依据确定的风险等级，采取必要的安全保护管控措施，限制访问区域。

（四）漏洞的修补

1. 安全漏洞所涉及的单位应根据本制度的要求，在规定时间内修复安全漏洞，整改完成后填写《网络安全隐患整改情况反馈表》（详见附件五）。

2. 修补方式包括:及时更新厂商官方提供的漏洞修复补丁;正确配置相关应用、系统和口令等策略;开发人员修正代码中的安全漏洞或功能缺陷。

3. 系统管理人员在安装厂商发布的操作系统及应用软件补丁时，应保证补丁的有效性和安全性，并在安装之前进行测试，避免因更新补丁而对产品或系统带来影响或新的安全风险。

4. 在无法安装补丁或更新版本的情况下，各部门应共同协商安全漏洞的解决措施。

（五）结果验证

由网信办对修复结果进行测试和检查、确保漏洞成功修复。

（六）漏洞的跟踪

1. 网信办应建立漏洞跟踪机制，对曾经出现的漏洞进行归档，并定期统计漏洞的修补情况，以便确切地找出信息系统的短板，为安全策略的制定提供依据。

2. 网信办应定期对安全漏洞的管理情况、安全漏洞的解决措施和实施效果进行检查和审计，包括预防措施是否落实到位，漏洞是否得到有效预防，已发现的漏洞是否得到有效处置，漏洞处理过程是否符合及时处理和安全风险最小化原则等。

第十条 如因特殊原因，系统管理人员或厂商不能按照规定的时效要求完成漏洞修复的，可申请延期； 不能进行修复的漏洞，需采取可实行的补救措施，报网信办负责人审批。

第十一条 各单位应按照流程及时完成漏洞整改，如有接到整改通知后不整改或整改不力等情况，网信办将进行通报，情节严重的按有关规定处理。

第五章 附 则

第十二条 本流程由网络安全与信息化办公室负责解释。

第十三条 本流程自发布之日起施行。

附件一

DREAD 模型

充分考虑漏洞被利用的难易程度以及对学校网络和系统的影响情况，采取 DREAD 模型对安全漏洞进行风险等级划分，并对各级别漏洞进行举例。

（一）在量化风险的过程中，对每个威胁进行评分，并按照如下公式计算风险值:

$$Risk = D + R + E + A + D$$

表 1 安全漏洞等级评估模型

DREAD 模型			
类别 \ 等级	高（3）	中（2）	低（1）
Damage Potential 潜在危害	获取完全权限;执行管理员操作;非法上传文件等	泄露敏感信息	泄露其他信息
Reproducibility 重复利用可能性	攻击者可以随意再次攻击	攻击者可以重复攻击，但有时间或其他条件限制	攻击者很难重复攻击过程
Exploitability 利用的困难程度	初学者在短期内能掌握攻击方法	熟练的攻击者才能完成这次攻击	漏洞利用条件非常苛刻
Affected users 影响的用户范围	所有用户，默认配置，关键用户	部分用户，非默认配置	极少数用户，匿名用户
Discoverability 发现的难易程度	漏洞很显眼,攻击条件很容易获得	在私有区域，部分人能看到，需要深入挖掘漏洞	发现该漏洞极其困难
说明：每一项都有 3 个等级，对应着权重，从而形成了一个矩阵。			

（二）最后得出安全漏洞风险等级。

表 2 风险等级对应分数

计算得分	安全漏洞风险等级
0-5 分	低风险
6-10 分	中风险
11-13 分	高风险
14-15 分	紧急

（三）各级别漏洞案例参考。

表 3 各级别漏洞案例

风险等级	评级标准
紧急	直接获取系统权限的漏洞（服务器权限、客户端权限）。包括但不仅限于远程命令执行、任意代码执行、上传获取 webshell、SQL 注入获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）。浏览器 use after free 漏洞、远程内核代码执行漏洞以及其它因逻辑问题导致的远程代码执行漏洞。
	直接获取重要业务或通用系统权限的漏洞（服务器权限、客户端权限），如：struts。
	严重的敏感信息泄漏。包括但不仅限于核心 DB（资金、身份、交易相关） 的 SQL 注入漏洞。
高	直接导致业务拒绝服务的漏洞。包括但不仅限于远程拒绝服务漏洞。
	严重的逻辑设计缺陷和流程缺陷。包括但不仅限于伪造任意号码发送消息、任意账号资金消费、任意账号密码修改漏洞。
	敏感信息泄漏。包括但不仅限于非核心 DB SQL 注入、源代码压缩包泄漏、可获取大量用户交易信息的接口、服务器、应用加密可逆或明文的敏感信息泄露。

风险等级	评级标准
	越权访问。包括但不仅限于绕过认证直接访问管理后台、后台弱密码。
	大范围影响用户的其他漏洞。包括但不仅限于可造成自动传播的存储型 XSS（包括存储型 DOM-XSS）、涉及交易、资金、密码的 CSRF。
	影响到服务器的本地提权漏洞。
	能直接盗取用户身份信息的漏洞。包括重要业务（如在线、EPOS、委托结算、无卡支付等）的重点页面的存储型 XSS 漏洞、普通站点的 SQL 注入漏洞。
中	需交互方可影响用户的漏洞。包括但不仅限于反射型 XSS（包括反射型 DOM-XSS）、CSRF、URL 跳转漏洞。
	本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃）。
	普通越权操作。包括但不仅限于不正确的直接对象引用。
	普通信息泄漏。包括但不仅限于客户端明文存储密码、客户端密码明文传输以及 web 路径遍历、系统路径遍历。
	普通的逻辑设计缺陷和流程缺陷。
低	轻微信息泄漏。包括但不仅限于路径信息泄漏、文件信息泄露、异常信息泄露。
	难以利用但存在安全隐患的漏洞。包括但不仅限于可引起传播和利用的 Self-XSS。

附件二

安全漏洞整改时效

（一）应用系统安全漏洞整改时效要求如下:

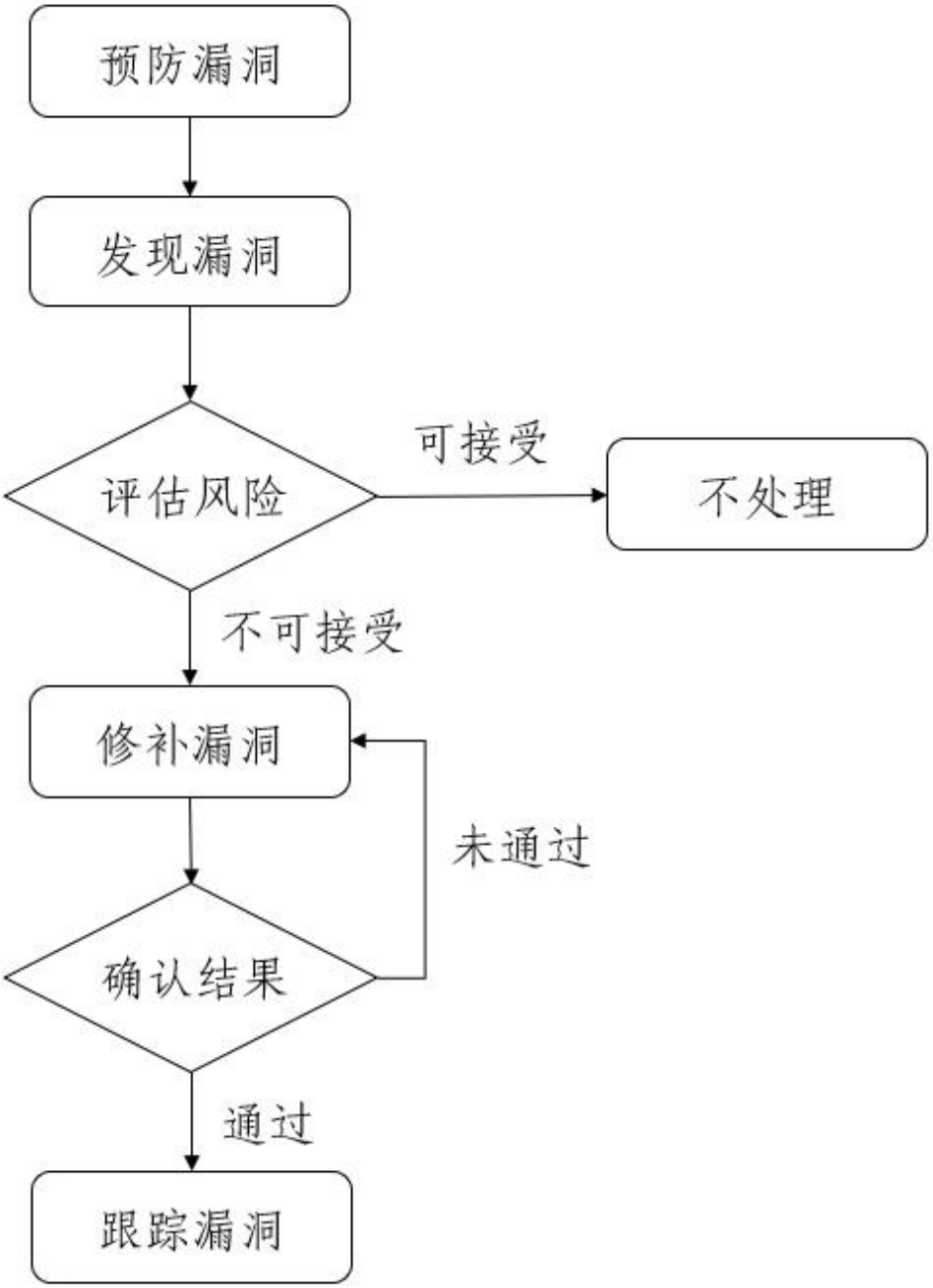
应用系统安全级别	整改时效		
	紧急风险漏洞	高风险漏洞	中风险安全漏洞
高级	3 个工作日	5 个工作日	10 个工作日
中级	5 个工作日	10 个工作日	10 个工作日
低级	1 个月内	1 个月内	1 个月内

（二）操作系统安全漏洞整改时效要求如下:

所处网络区域	整改时效	
	紧急或高风险漏洞	中风险漏洞
对外提供服务区域	Window 操作系统 3 个月内；Linux&unix 操作系统 6 个月内；对于影响特别严重，易受攻击的漏洞，根据网信办的通告立即整改完成。	Window 操作系统 3 个月内；Linux&unix 操作系统 6 个月内。
对内提供服务区域	Window 操作系统 6 个月内；Linux&unix 操作系统 12 个月内；对于影响特别严重，易受攻击的漏洞，根据网信办的通告立即整改完成。	Window 操作系统 6 个月内；Linux&unix 操作系统 12 个月内。

附件三

漏洞处理流程



附件四

山东科技大学
网络安全隐患整改通知书

〔20XX〕第 XXX 号

XXX 部门：

经 XXXX 检测发现，你单位所属 XXXX 系统存在高危漏洞和安全隐患（见附件），请立即组织技术力量进行整改、清理，尽快消除安全隐患，并按照国家信息安全等级保护制度和公安机关政府网站安全监管工作规范的相关要求，对网站/信息系统进行全面检测和安全整改。

请于 XXXX 年 X 月 X 日 XX 时前，将网络安全隐患整改情况反馈表（见附件）通过学校办公系统发送至网络安全与信息化办公室 XXX 邮箱。

在网络安全隐患整改期间，学校将采取必要的安全保护管理和技术措施，确保全校网络与信息系统安全。

联系人：XXX 联系电话：XXX

技术联系人：XXX 联系电话：XXX

网络安全与信息化办公室

XXXX 年 X 月 X 日

附件：漏洞检测报告

一式两份，一份交被检查单位，一份网信办留存。

附件五

网络安全隐患整改情况反馈表

单位名称		联系人	
联系电话		电子邮箱	
安全隐患网站或信息系统名称			
域名或 URL			
安全隐患整改情况			
今后防范措施			
网络安全分管领导签字: 年 月 日（单位盖章）			

山东科技大学电子邮箱及电子邮件系统管理办法

第一章 总 则

第一条 为规范学校电子邮箱的使用和管理，保障学校电子邮件系统安全高效运行，根据《网络安全法》和《互联网电子邮件服务管理办法》等有关法律法规，结合学校实际，制定本办法。

第二条 电子邮件系统由学校统一建设、管理和运维，为在职教职工、在校学生和各单位（以下简称“用户”）免费提供互联网电子邮件服务，电子邮箱后缀为@sdust.edu.cn。未经批准，各单位不得自行单独建设电子邮件系统。

第三条 电子邮箱是通过学校电子邮件系统为用户提供的用于工作与学习交流的电子信息空间。电子邮箱分为个人邮箱和公务邮箱，个人邮箱是指分配给在职教职工和在校学生使用的电子邮箱；公务邮箱是指经单位申请，分配给单位用于处理学校公务的电子邮箱，公务邮箱命名规则为单位汉语拼音首字母组合。

第四条 电子邮箱仅提供给学校在职教职工、在校学生及各单位使用，不接受校外人员或单位申请，毕业生离校后，其个人邮箱保留一年。电子邮箱所有权属于山东科技大学，电子邮箱用户拥有使用权。

第二章 组织机构和职责

第五条 网络安全与信息化办公室（以下简称“网信办”）的职责：

（一）负责电子邮件系统的规划、建设、管理和运维。

（二）负责为电子邮箱用户提供开通、终止、咨询及异常处理等服务。

（三）负责电子邮箱使用的监督、检查和安全防护。

第六条 各部门、各单位负责本单位范围内电子邮箱使用的监督检查，及时纠正未正确使用学校电子邮箱的情况。

第七条 电子邮箱用户应严格遵守相关法律法规及本办法规定，自觉维护电子邮箱安全。

第三章 电子邮箱的开通和终止

第八条 个人邮箱开通。网信办负责为在职教职工开通个人邮箱。

第九条 公务邮箱开通。单位申请，明确责任人和使用人，公务邮箱的责任人和使用人必须为学校在岗在编教职工。

第十条 电子邮箱终止与注销。电子邮箱终止后，所有功能停止服务，用户信息及电子邮件数据继续保存六个月，六个月后，电子邮箱注销，用户信息及电子邮件数据删除。

第四章 电子邮箱使用管理

第十一条 办公用邮箱一律使用学校邮件系统的邮箱(后缀为@sdust.edu.cn），禁止将公共邮箱或免费邮箱用于办公，已用于办公的公共或免费邮箱需更换为学校邮件系统的邮箱。

第十二条 各单位通过电子邮件向教职工和学生发送通知等公务信息时，应使用公务邮箱。公务邮箱的使用人负责邮件收

发与日常管理，严禁将邮箱授权给他人或其他单位使用，不得使用公务邮箱从事非学校公务活动。

第十三条 电子邮箱用户必须设置8位以上复杂密码，密码应包含字母、数字、特殊符号且区分大小写，不能包含账户名、单位简称、办公电话号码等容易猜解的信息。

第十四条 用户应妥善保管所使用的电子邮箱账号和密码，并对使用其电子邮箱开展的所有活动负责。如发现他人未经许可使用其电子邮箱时，应立即通知网信办处理。

第十五条 电子邮箱账号应专人专用，不能多人使用一个账号。

第十六条 应安装杀毒软件定期对办公电脑进行全盘扫描杀毒，对每次收到的电子邮件，使用前均检查病毒。

第十七条 不打开可疑邮件、垃圾邮件、不明来源邮件等提供的附件或网址，对这类邮件直接删除。

第十八条 电子邮箱用户必须遵守《中华人民共和国网络安全法》《中华人民共和国保守国家秘密法》《中华人民共和国计算机信息系统安全保护条例》《计算机软件保护条例》等计算机及互联网相关的法律法规。遵守使用电子邮件服务的网络协议、规定、程序和惯例，不得利用电子邮箱发送连锁邮件、垃圾邮件或商业邮件，不得利用电子邮件散布电脑病毒、木马软件、间谍软件等恶意软件干扰网络服务。

禁止利用电子邮箱从事以下活动：

（一）反对宪法所确定的基本原则的。

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。

（三）损害国家荣誉和利益的。

（四）煽动民族仇恨、民族歧视，破坏民族团结的。

（五）破坏国家宗教政策，宣扬邪教和封建迷信的。

（六）散布谣言，扰乱社会秩序，破坏社会稳定的。

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。

（八）侮辱或者诽谤他人，侵害他人合法权益的。

（九）含有法律、行政法规禁止的其他内容的。

（十）损害学校利益的。

第十九条 除法律、法规规定的情形外，任何人不得以任何方式私自查阅、截获、监控他人邮件，也不得向第三方提供电子邮箱用户的注册信息。公安机关、检察机关或有关部门依照法律规定的程序需对电子邮箱通信内容进行检查时，应由分管网络安全与信息化工作的校领导批准后，网信办配合执行。

第五章 责任追究

第二十条 对于违反本方法有关规定的单位或个人，暂停其电子邮箱使用权并责令改正；拒不整改的，终止其电子邮箱使用权并对相关单位或个人进行约谈或通报批评；造成学校损失的，追究直接责任人的相关责任。

第六章 附 则

第二十一条 本办法由网络安全与信息化办公室负责解释。

第二十二条 本办法自发布之日起施行。

山东科技大学数据中心机房安全管理办法

第一章 总 则

第一条 为加强对学校机房的管理，有效保障机房内基础设施和计算机信息系统的安全、稳定、高效运行，依据《中华人民共和国网络安全法》《信息安全等级保护管理办法》等国家、省、市有关法规政策和学校管理制度，结合学校实际，制定本办法。

第二条 本办法适用于学校数据中心机房的管理。

第三条 本办法所指数据中心机房（以下简称“机房”）是指容纳并集中运行学校信息系统的主机、服务器、存储、网络等设备、设施的核心机房。

第四条 机房日常管理工作，由网络安全与信息化办公室（以下简称“网信办”）负责。

第五条 机房管理应遵循以下原则:

（一）安全第一原则。机房的运行和使用必须严格遵守相关安全规定，保障人员、设施、设备及环境的安全，其中首先要保障人员的人身安全。

（二）设备专用原则。机房仅放置投入运营的信息系统所需设施、设备，含开发、测试用计算机设备。

（三）统一管理原则。机房的运行和使用由网信办统一管理。

（四）规范操控原则。在机房内进行的所有工作都应严格按照本制度相关规定执行，不得违规操作。

第二章 人员准入管理

第六条 机房进出控制采用电子门禁系统，门禁准入仅授权给网信办管理人员。

第七条 机房门禁准入人员调离工作岗位，离岗时必须作注销处理。

第八条 非授权人员需进入机房时，首先向网信办提出，根据工作需要，由相关人员全程陪同进出机房，并在《机房进出登记表》（见附件一）中进行登记。

第三章 人员行为管理

第九条 严禁将各种液体、食品等与工作无关的物品带入机房。

第十条 机房工作人员应严格按照各信息系统操作规程规范操作。只允许使用经本单位授权的软件，严禁在任何计算机上使用非授权软件。

第十一条 所有进入机房人员只能在工作任务相关的区域内从事授权活动，严禁从事非授权活动和与工作无关的活动。

第十二条 未经许可不得将机房内任何物品带出机房。

第十三条 由网信办陪同人员负责监督进入机房的第三方工作人员的各项行为。

第四章 机房环境管理

第十四条 机房内禁止乱堆乱放设备、资料、工具等，保持机房干净整洁。

第十五条 机房周围要保持清洁，凡路口、过道、门窗附近，不得堆放物品和杂物。

第十六条 机房内的温度应保持在+15℃至+25℃，相对湿度应保持在 20%至 60%，且保持正常通风，防止不良气体及灰尘侵入。

第十七条 严禁擅自调整机房温湿度或开关新风、空调等设施设备，如需调整，必须经网信办批准，由设备责任人按照操作规程进行。

第十八条 机房应设置相应的火灾自动报警系统和充足的消防设备，各种灭火器材应定位放置，随时保持有效，人人会使用。

第十九条 机房内不得堆放与工作无关的物品、器械。

第二十条 机房内部不能有水源，机房地板应高于机房外部地面。

第二十一条 机房内选用低辐射显示器设备，采用距离防护、噪声干扰、屏蔽等措施，把电磁泄露抑制到最低限度。

第二十二条 机房应有防雷地线和其他防雷措施。

第二十三条 保持机房内清洁、干燥、空气流通，注意防潮、防尘、防鼠。

第二十四条 机房内动力环境监测系统、入侵报警系统、自动灭火系统等的维护保养由网信办管理。

第五章 机房用电管理

第二十五条 机房必须使用专用的 UPS（不间断电源系统）

为各信息系统设备供电，禁止其它非机房内设备使用机房专用UPS。要为机房提供功率足够的备用供电线路或发电机作为备用电源，并定期进行切换测试。

第二十六条 机房内非计算机类设备，如吸尘器、电烙铁等，禁止使用 UPS 电源。

第二十七条 机房内位置固定的设备必须使用质量可靠的固定电源插座。

第二十八条 未经网信办批准，禁止任何人擅自在机房内进行架设电缆、安装插座、离合配电开关等涉及用电安全的操作。

第二十九条 网信办指定专业人员每月一次对机房内电源设备、配电柜、插座、电缆、开关等进行巡检，发现问题需及时更换供电故障设备和器件。

第三十条 因办公大楼供电线路维护等原因,需要断开总配电室的机房专用空气开关时，应事先通知网信办，经协商同意后方可实施断开操作,并在机房电源后备设备的有效后备时间内恢复供电。

第三十一条 办公大楼停电后，网信办应密切监视 UPS 设备的工作状态和后备时间，随时准备启用备用供电系统。

第三十二条 机房内所有供电线路和综合布线的改造、总供电负荷增减等操作，必须制定完整的改造方案，由专业人员按照技术规范进行。

第六章 设备管理

第三十三条 所有信息系统设备进出机房均应履行审批登

记手续。

第三十四条 设备进入机房前，应明确设备用电、场地、散热、承重等需求信息。网信办确定安放位置后指派专业人员核定用电负荷并完成设备承重、散热、配电等的准备工作。安装条件准备就绪后，设备方可进入机房。

第三十五条 设备进入机房时，在指定位置安放。未经批准，任何人禁止随意变动设备位置。

第三十六条 机房内设备如需移出机房，经网信办同意后方可移出，并与相关部门或人员办理设备移交手续。

第三十七条 机房内的交换机为整个校园网络的核心设备，任何人不得随意开关交换机。

第三十八条 服务器由相应的系统管理员管理维护，其他任何人不得操作和开关与自己无关的服务器。

第三十九条 机房线路保持整齐有序，电源线和网络线要分开布线，网线要有标签标记，临时线路要用完收起。

第四十条 为了便于区分使用,服务器及网络设备要有标签标记，标明配置、操作系统、应用等。

第四十一条 设备维护要保留电子日志、纸质文档。

第四十二条 服务器及设备资料要分类摆放整齐，以便使用。

第四十三条 机房内设备由网信办进行管理，并建立设备的配置、变更档案。

第七章 机房巡检管理

第四十四条 中心机房

中心机房的巡检工作由网信办人员负责。

巡检周期：每周一次。

巡检内容：交换机、路由器、防火墙、服务器、PC机、UPS、电源、消防设备、空调、照明、报警装置、温度及湿度。

巡检方式：就地巡检。

第四十五条 巡检要求

（一）发现问题及时解决，如有必要及时通知相关人员和相关部门，防止工作延误。

（二）巡检完毕应搞好环境卫生，认真填写机房巡检记录表（见附件二）。

（三）对机房进行巡检时应遵循机房安全管理制度。

第八章 机房安全管理

第四十六条 机房内严禁存放易燃、易爆、腐蚀性、强磁性和强热源物品，严禁明火。

第四十七条 消防设施应按照规定摆放，非主管部门的专业技术人员，任何人不得随意触摸、移动消防设施。

第四十八条 机房内紧急安全通道仅用于紧急情况下人员撤离使用，正常情况下严禁随意打开安全通道门。

第四十九条 严禁在安全通道上堆放物品，保持通道畅通。

第九章 附 则

第五十条 本办法由网络安全与信息化办公室负责解释。

第五十一条 本办法自发布之日起施行。

附件一

机房进出登记表

日期	姓名	所属单位	事由	进入时间	离开时间	陪同人员签字

附件二

机房巡检记录表

巡视人员		维护日期	
维护记录			
序号	条目	内容（正常方框内打勾）	备注
1	UPS 运行情况	□ 负载 不大于 85% □ 查看运行日志是否有异常 □ 三相输入、输出电压是否正常 □ 电压范围是否正常 □ 蓄电池是否完好，正常	
2	消防系统情况	□ 系统是否有告警日志 □ 机房温感、烟感状态是否正常	
3	服务器运行情况	□ CPU 运行状态是否正常 □ 内存占用情况是否正常 □ 硬盘空间是否足够 □ 指示灯状态是否正常 □ 网络连接是否正常	
4	网络设备运行情况	□ 光猫指示灯状态是否正常 □ 转换器是否正常 □ 光纤是否破损 □ 网络连通性是否正常	
5	存储设备运行情况	□ 系统日志是否正常 □ 指示灯状态是否正常	
6	其他	□ 系统性能是否正常 □ 指示灯状态是否正常 □ 网络连接是否正常 □ 温度是否正常	

山东科技大学网络安全教育和培训管理办法

第一章 总 则

第一条 为了规范学校网络安全教育和培训工作，进一步提高对网络安全重大意义的认识，促进工作人员培训工作的日常化、全员化、制度化，确保各项工作顺利进行，结合学校实际，制定本办法。

第二条 本办法适用于学校全体师生。

第三条 网络安全教育包括网络安全政策法规、安全意识、岗位职责、基础知识、操作规程等。

第四条 网络安全教育应坚持以人为本、预防为主的原则，结合实际工作，分层次、有重点、有针对性地进行。

第二章 组织机构和职责

第五条 网络安全与信息化办公室（以下简称“网信办”）负责学校网络安全教育和培训的规划、指导工作，负责学校信息化联络员的网络安全教育和培训组织工作。

第六条 各部门、各单位（以下简称“各单位”）负责本单位师生的网络安全教育和培训工作。

第三章 培训和考核

第七条 新生入学后应进行网络安全培训并接受考核，内容包括学校规章制度、上网方式及方法、网络安全常识及信息安全培训等。

第八条 各单位应定期对师生进行网络安全意识教育，了解网络安全法律法规、网络安全重要性以及网络安全最新动态。

第九条 新入职的教师和工作人员在正式上岗前，应进行网络安全方面的培训，明确岗位所要求遵守的本单位网络安全制度和技术规范。

第十条 针对系统维护人员和管理员应定期开展安全技术教育培训，明确如何安全地使用有关系统，包括各业务应用系统、主机操作系统、内部网站以及联网设备等。

第十一条 针对安全管理员和系统管理员应根据实际情况进行相关的培训，并参加认证考试，以提高网络安全管理人员的理论和实践能力。

第十二条 网络安全培训所采用的形式包括举办安全知识讲座、报告会、座谈会，观看安全教育片，参观安全教育展览，以及参加网络安全演练等。

第十三条 各单位应对培训进行签到、记录和内容审定等工作，通过网上签到或者现场签名等方式对培训过程进行记录。

第十四条 应对培训对象进行考核，考核的方式可根据培训内容、时间、要求，通过多种形式进行考核和评估；考核内容包括网络安全知识、安全技能、操作行为等。

第十五条 各单位的工作人员应自觉接受安全教育和安全监督检查。

第四章 附 则

第十六条 本办法由网络安全与信息化办公室负责解释。

第十七条 本办法自发布之日起施行。

山东科技大学校园网用户上网守则

第一条 为加强对校园网的管理，保障校园网的正常运行和健康发展,维护相关方的正当权益,更好地为广大上网师生(以下简称“用户”）提供服务，依据学校实际情况，制定本守则。

第二条 本守则适用于全校师生，包括外籍教师和计划外用工。

第三条 用户必须遵守《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》《中华人民共和国网络安全法》和国家、山东省及学校有关计算机、互联网等方面的法律法规和制度。

第四条 用户必须接受校园网络安全与信息化办公室（以下简称“网信办”）对校园网络资源的统一分配，对有意干扰网络资源分配者，网信办将撤消其端口的使用权。

第五条 在校园网络上严禁制作、查阅、复制或传播下列信息:

（一）反对宪法所确定的基本原则的。

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。

（三）损害国家荣誉和利益的。

（四）煽动民族仇恨、民族歧视，破坏民族团结的。

（五）破坏国家宗教政策，宣扬邪教和封建迷信的。

（六）散布谣言，扰乱社会秩序，破坏社会稳定的。

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。

（八）侮辱或者诽谤他人，侵害他人合法权益的。

（九）含有法律、行政法规禁止的其他内容的。

第六条 在校园网络上严禁下列行为:

（一）破坏、盗用、篡改计算机网络中的信息资源。

（二）故意泄露、窃取、篡改个人电子信息，擅自利用网络收集、使用个人电子信息，出售或者非法向他人提供个人电子信息。

（三）违背他人意愿、冒用他人名义发布信息。

（四）攻击、入侵、破坏计算机网络、信息系统及设备设施。

（五）故意阻塞、中断校园网络，恶意占用网络资源。

（六）故意制作、传播、使用计算机病毒、木马、恶意软件等破坏性程序。

（七）故意大量发送垃圾电子邮件、垃圾短信等，干扰正常网络秩序。

（八）盗用他人账号、盗用他人 IP 地址。

（九）私自转借、转让用户账号造成危害。

（十）私自开设二级代理和路由接纳网络用户。

（十一）上网信息审查不严，造成严重后果。

（十二）以端口扫描和私搭 DHCP 服务器等方式，破坏网络正常运行。

（十三）私自将外网串接到校园网络。

（十四）其它违反法律法规或危害网络与信息安全的行为。

第七条 对于私自占用网络资源，破坏网络和信息系统，违反网络用户行为规范的行为，由网信办根据事件的涉及范围、严重程度进行查处，并按学校有关规定处理。

第八条 本守则由网络安全与信息化办公室负责解释。

第九条 本守则自发布之日起施行。

山东科技大学网络安全事件应急响应综合预案

（2020 年 3 月修订）

目　　录

1　总　则.....93

1.1　编制目的.....93

1.2　编制依据.....93

1.3　适用范围.....93

1.4　工作原则.....93

2　组织机构与职责.....95

2.1　领导小组.....95

2.2　应急响应实施小组.....95

2.3　应急响应专家小组.....96

3　事件分级分类.....97

3.1　事件分类.....97

3.2　事件分级.....97

3.3　事件定级.....98

4　监测与预警.....99

5　应急处置.....100

5.1　基本流程.....100

5.1.1　应急启动.....100

5.1.2　启动响应（Ⅰ级、Ⅱ级响应）.....100

5.1.3　事件级别调整.....101

5.1.4　结束响应.....101

5.2　专项应急处理.....102

5.2.1 非法言论.....102
5.2.2 黑客攻击.....103
5.2.3 网络病毒.....104
5.2.4 服务器软件系统故障.....105
5.2.5 业务数据损坏.....106
5.2.6 核心设备硬件故障.....107
5.2.7 通信网络故障.....107
5.2.8 中心机房断电.....108
5.2.9 中心机房火灾.....109
5.2.10 中心机房水情.....110
6 预防工作.....111
6.1 日常管理.....111
6.2 应急演练.....112
6.3 宣传培训.....112
6.4 重要活动期间的预防措施.....113
7 保障措施.....114
7.1 责任落实.....114
7.2 人力保障.....114
7.3 技术保障.....114
7.4 物资保障.....114
8 附 则.....116
8.1 预案管理.....116

8.2 预案实施时间.....116
8.3 预案解释.....116
9 附 件.....117
附件 1： 应急处置基本流程.....117
附件 2： 应急组织机构联系人清单.....118
附件 3： 应急物资清单.....119
附件 4： 网络安全事件报告表.....120
附件 5： 网络安全事件应急响应结果报告表.....122
附件 6： 应急演练方案（模板）.....124
附件 7： 应急演练记录单.....125

1 总 则

1.1 编制目的

为了切实做好学校信息安全事件的防范和应急响应工作,进一步提高本学校预防和控制信息安全事件的能力和水平,减轻或消除信息安全事件的危害和影响，保障校园网平稳、安全、有序运行，结合学校工作实际，制定本预案。

1.2 编制依据

根据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《信息安全事件分类分级指南（GB/Z20986-2007）》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》《教育信息化“十三五”规划》等相关规定以及学校制定的《山东科技大学突发事件总体应急预案》及各专项应急预案等文件，制定本预案。

1.3 适用范围

本预案适用于校园网运行及网络信息方面发生的有可能影响学校、社会和国家安全稳定的网络与信息安全突发事件,包括攻击事件、故障事件、灾害事件和其他类事件。

1.4 工作原则

校园网运行与网络信息安全事件的处理原则:

（1）依法管理:《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《信息安全事件分类分级指南（GB/Z20986-2007）》等法律法规和《国家突发公共事件总体应

急预案》《国家网络安全事件应急预案》《教育信息化“十三五”规划》等相关规定以及学校制定的《山东科技大学突发事件总体应急预案》及各专项应急预案等文件精神。

（2）分级负责、责任到人：学校一级由网络安全和信息化领导小组（以下简称“领导小组”）负责，各部门、各单位（以下简称“各单位”）二级由各单位主要领导负责，切实做到“责任落实，层层负责”。

（3）谁主管、谁负责，谁使用、谁负责：网络安全与信息化办公室（以下简称“网信办”）负责网络安全和系统安全，保障校园网的畅通运行和各服务器的正常运转;各单位负责其主管网站上的内容安全、业务系统的权限管理安全和系统内的数据安全，营造健康文明的网络环境，将有害信息造成的不良影响减小到最低限度。

2 组织机构与职责

学校应急响应工作机构按照角色划分为 3 个功能小组:领导小组，应急响应实施小组，应急响应专家小组。信息安全事件发生后，在领导小组的统一部署下，工作人员各司其职，并严格按照应急响应预案组织实施应急响应工作。

2.1 领导小组

对学校的信息安全工作进行全面的分析研究,制定工作方案,提供人员和物质保障,指导和协调各单位实施信息安全工作预案,处置各类危害校园信息安全的突发事件。具体职责包括:

（1）制定工作方案，提供人员和物质保障。

（2）审核批准应急响应策略、应急响应预案，批准和监督应急响应预案的执行。

（3）指导学校各单位的应急处置工作。

（4）启动定期评审、修订应急响应预案。

（5）组织协调有关部门查处利用计算机网络泄密的违法行为。

（6）负责组织的外部协作，牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置。

2.2 应急响应实施小组

当由于系统崩溃、病毒攻击、非法入侵等原因造成校园网运行异常或瘫痪时,根据信息安全事件的发展态势和实际控制需要,具体负责现场应急处置工作,尽快恢复学校网络的正常运行,具体职责包括:

（1）负责校园基础网络系统安全。

（2）负责计算机病毒疫情和大规模网络攻击事件的处置。

（3）负责校级网络与信息系统安全事件处置的技术支持。

2.3 应急响应专家小组

聘任校内外专家组成，主要职责是对网络安全中可能遇到的重大问题提供技术咨询，具体职责包括:

（1）对重大信息安全事件进行评估，提出启动应急响应的建议。

（2）研究分析信息安全事件的相关情况及发展趋势，为应急响应提供咨询或提出建议。

（3）分析信息安全事件原因及造成的危害，为应急响应提供技术支持。

3 事件分级分类

3.1 事件分类

校园网络与信息安全事件可分为三类:

（1）攻击事件：指校园网络与信息系统因病毒感染、非法入侵等造成学校网站或各单位网站主页被恶意篡改、交互式栏目和邮件系统发布有害信息;应用服务器与相关应用系统被非法入侵，应用服务器上的数据被非法拷贝、篡改、删除；在网站上发布的内容违反国家的法律法规、侵犯知识版权并造成严重后果等，由此导致的业务中断、系统宕机、网络瘫痪等。

（2）故障事件：指校园网络与信息系统因网络设备和计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪等。

（3）灾害事件：指因洪水、火灾、雷击、地震、台风等外力因素导致网络与信息系统损坏，造成业务中断、系统宕机、网络瘫痪等。

（4）其他类事件：指不能归为以上分类的网络安全事件。

3.2 事件分级

依照《信息安全事件分类分级指南（GB/Z20986-2007）》，根据安全突发事件的可控性、严重程度、影响范围和校园网络与信息系统的实际情况，安全事件分为四级：特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）和一般（Ⅳ级）。

3.3 事件定级

依据事件分级和事件分类，综合信息系统损失和社会影响程度两个方面，对学校网络与信息安全事件分为四级，特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）和一般（Ⅳ级）。

事件等级	标志性颜色	判断标准	解决时限
特别重大（I级）	**红色**	1.造成校园网络与信息系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于学校是不可承受的。 2.极大威胁国家安全，引起社会动荡，对学校有极其恶劣的负面影响，或者严重损害公众利益。	240 分钟
重大（II级）	**橙色**	1.造成校园网络与信息系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于学校是可承受的。 2.引起社会恐慌，对学校有重大的负面影响，或者损害到公众利益。	120 分钟
较大（III级）	**黄色**	1.造成校园网络与信息系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但学校是完全可以承受的。 2.可能影响到国家安全，扰乱社会秩序，对学校有一定的负面影响，或者影响到公众利益。	60 分钟
一般（IV级）	**蓝色**	1.造成校园网络与信息系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。 2.对国家安全、社会秩序、学校和公众利益基本没有影响，但对个别学生、教职工、法人或其他组织的利益会造成损害。	30 分钟

4 监测与预警

学校的网络通信平台、应用平台和信息系统，参照国家有关信息安全等级保护的要求，按照最终确定的保护等级采取相应的安全保障措施。不断完善网络安全防御系统，包括防火墙、堡垒机、上网行为管理、日志审计系统等，并对网络设备的安全性进行合理配置，根据实际需要做好升级更新工作。

建立健全安全事件预警预报体系，严格执行网络安全管理制度，加强对学校网络、网站、重要信息系统的监测、监控和安全管理，做好相关数据日志记录，设立内容过滤系统，确定合理规则，对校园网络进出信息实行过滤及预警。

做好服务器及数据中心的数据备份及登记工作，建立灾难性数据恢复机制。一旦发生校园网络与信息安全事件，根据事件影响范围和损失程度综合确定预警等级，并采取相应措施。

特殊时期，可根据领导小组的统一要求和部署，由应急响应实施小组进行统一安排，组织专业技术人员对校园网络和信息数据采取加强性保护措施，进行不间断的监控。

5 应急处置

5.1 基本流程

5.1.1应急启动

特别重大（Ⅰ级）以及重大（II级）事件发生时，直接启动的应急处置程序。

较大（III级）发生时，首先由应急响应实施小组进行处理，必要时联系维护支撑单位协助处理。

一般（IV级）事件发生时，由应急响应实施小组人员进行处理。

5.1.2启动响应（Ⅰ级、II级响应）

5.1.2.1 启动应急指挥体系

进入应急状态，领导小组履行应急处置工作的统一领导、指挥、协调职责，开展应急处置工作。

5.1.2.2 掌握事件动态

应急响应实施小组了解校园网受到事件波及或影响情况，及时将事态发展变化情况和处置进展情况上报领导小组。

5.1.2.3 决策部署

领导小组、应急响应专家小组和应急响应实施小组研究对策，对处置工作做出决策部署。

5.1.2.4 处置实施

领导小组组织应急响应专家小组和应急响应实施小组采取各种技术措施、管控手段，最大限度地阻止和控制事态发展，根据信息安全事件的分类，初步确定应急处置方式，区别对待。

对于能力范围内不能解决的，应立即邀请具备条件的单位进行技术协助。

应急处置人员在应急处置过程中应保留、收集相关证据。

相关信息通告由领导小组决定，并组织网络安全事件的应急新闻发布和舆论引导工作。未经批准，部门或人员不得擅自发布相关消息。

5.1.3事件级别调整

在应急处置过程中，各专项工作组监控事件动态变化，当认为需要调整事件级别时，按有关流程上报并调整事件响应级别。

5.1.4结束响应

通过应急处置成功解决信息安全事件后，尽快组织相关人员进行网络信息系统恢复，同时对信息安全事件应急响应进行总结。对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告。报告内容包括:

（1）问题或故障。

（2）原因分析。

（3）采取的应急措施或应急方案。

（4）结果评价。

（5）建议应采取的后续措施或需进一步考虑的解决方案。

（6）总结经验教训。

事件的调查处理和总结评估工作原则上在应急响应结束后30天内完成。

5.2 专项应急处理

5.2.1非法言论

（1）信息确认：确认网站上出现不良信息（或者网页被篡改），将被篡改的页面进行拍照、截图或导出。

（2）通知人员：通知领导小组和应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 网站 XXX 页面顶部出现不良信息，信息内容是 XXX，已拍照）。

（3）关闭网站：立刻关闭网站。

（4）保留日志和截图：将相关日志保存并导出，包括安全设备日志、系统日志、异常情况截图、各时间点记录等。

（5）确定攻击源：请有关厂商、网警协助确定网络攻击或信息破坏行为信息，确定攻击源。

（6）消除恶意程序：查找攻击源计算机，更新特征库，使用防病毒客户端或使用针对网络攻击或信息破坏程序的专杀工具查杀程序，如果网络攻击或信息破坏程序依旧不能清除恶意程序，则重新安装操作系统并安装防病毒客户端。

（7）加固系统：清除网络攻击、信息破坏程序或安装完操作系统后，应立即修改系统密码，更新系统补丁，升级防病毒客户端程序。

（8）网站恢复：恢复网站页面重新投入使用。

（9）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网

络与信息安全事件处理报告,在调查工作结束后一日内书面报告领导小组。

5.2.2黑客攻击

（1）信息确认：确认网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或黑客正在进行攻击，将被攻击的计算机、服务器进行拍照、截图或导出。

（2）断开网络：断开网络，并将受影响计算机、服务器的从网络中隔离出来。

（3）通知人员：确定事件类型，通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等(例如：20XX年X月X日X点X分,XXX服务器遭到黑客攻击,已隔离、拍照)。

（4）报警：领导小组会商后，认为情况严重，则立即向公安部门或上级机关报告。

（5）保留日志和截图：将相关日志保存并导出，包括安全设备日志、系统日志、异常情况截图、各时间点记录等。如果部份日志已经被黑客清除，可以通过日志恢复等方法，尽量找到更多的日志。

（6）确定攻击源：请有关厂商、网警协助确定黑客攻击信息，确定攻击源。

（7）阻断攻击途径：封锁或删除被攻破的登录账号，阻断可疑用户进入网络的通道。

（8）消除有害程序：更新特征库，使用防病毒客户端或使用针对有害程序的专杀工具查杀有害程序,如有害程序依旧不能清除，则重新安装操作系统并安装防病毒客户端。

（9）加固系统：清除病毒或安装完操作系统后，应立即更新系统补丁，升级防病毒客户端程序，恢复或加固核心交换机、防火墙设置。

（10）客户端、服务器恢复到日常状态。

（11）恢复核心交换机、防火墙设置。

（12）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.3网络病毒

（1）信息确认：确认计算机、服务器感染有害程序，将被攻击的计算机、服务器进行拍照、截图或导出。

（2）隔离系统：将受影响计算机、服务器的网络断开，拔出网线，使计算机、服务器保持单机状态。

（3）数据备份：对该设备的硬盘进行数据备份。

（4）通知相关人员：确定事件类型，通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX年X月X日X点X分，XXX服务器感染有害程序，已隔离、拍照）。

（5）保留日志和截图：将相关日志保存并导出，包括安全设备日志、系统日志、异常情况截图、各时间点记录等，如果部份日志已经被黑客清除，可以通过日志恢复等方法，尽量找到更多的日志。

（6）确定问题：请有关厂商协助确定有害程序信息，包括

有害程序类型、来源、感染途径、感染范围、已遭受的损失等。

（7）消除有害程序：更新病毒库，使用防病毒客户端或使用针对有害程序的专杀工具查杀有害程序，如有害程序依旧不能清除，则重新安装操作系统并安装防病毒客户端。

（8）清查其他系统：利用病毒检测软件对其他机器进行病毒扫描和清除工作。

（9）加固系统：清除病毒或安装完操作系统后，应立即更新系统补丁，升级防病毒客户端程序。

（10）客户端、服务器恢复到日常状态。

（11）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.4 服务器软件系统故障

（1）信息确认：确认软件遭到破坏性攻击，将软件故障情况进行拍照、截图或导出。

（2）启动备份服务器系统：由备份服务器接管业务应用，将故障服务器脱离网络。

（3）转移数据：取出系统镜像备份磁盘，保持原始数据。

（4）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 服务器软件遭到破坏性攻击，已启用备份服务器、拍照）。

（5）保留日志和截图：将相关日志保存并导出，包括安全

设备日志、系统日志、异常情况截图、各时间点记录等，如果部份日志已经被黑客清除，可以通过日志恢复等方法，尽量找到更多的日志。

（6）重新启动故障服务器系统：重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商，请求技术支援，作好技术处理。

（7）服务器软件系统恢复到日常状态。

（8）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.5 业务数据损坏

（1）信息确认：确认业务数据遭到损坏。

（2）备份数据：备份业务系统当前数据。

（3）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 数据遭到严重性损坏，已备份当前数据）。

（4）备份数据恢复：调用备份服务器备份数据进行修复，若备份数据损坏，调用异地备份数据。若短期内（<2 小时）无法恢复数据，立即向有关厂商请求紧急技术支援，并及时通知业务部门以手工方式开展业务或者暂缓上传上报数据。

（5）检查数据：检查历史数据和当前数据的差别，由相关系统运行负责人员补录数据。

（6）重新备份数据：备份业务系统当前数据。

（7）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.6核心设备硬件故障

（1）信息确认：确认核心设备硬件发生故障。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，XXX 设备硬件发生故障）。

（3）确定问题：查找、确定故障设备及故障原因，若故障设备在短时间内无法修复，系统管理员应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（4）设备修复：能够自行处理，应立即用备件替换受损部件，如果不能自行处理的，立即与设备提供商联系，请求派维修人员前来维修。

（5）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.7通信网络故障

（1）信息确认：确认通信线路故障（例如：中断、路由故障、流量异常、域名系统故障等）。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理等（例如：20XX 年 X 月 X

日 X 点 X 分，XXX 通信线路中断）。

（3）确定问题：查清通信网络故障位置，隔离故障区域，并通知相关通信网络运营商查清原因;同时及时组织相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接。

（4）通知业务部门：若短期内（<2 小时）无法恢复，及时通知相关部门。

（5）恢复通信网络：恢复通信网络，通知相关部门网络恢复，保证正常运转。

（6）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.8 中心机房断电

（1）启用备用电源：启用 UPS 设备当前的蓄电能力。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、内容、处理、供电时间等（例如：20XX 年 X 月 X 日 X 点 X 分，中心机房断电，能够继续供电 X 小时）。

（3）通知业务部门：通知所有使用部门，抓紧完成信息处理工作、停止应用。

（4）温度控制：实时检测中心机房的室内温度，空调停止运行的情况下，立即采取其它措施降温，如开门通风等。根据相关情况关闭非重要设备，如机房内温度过高，应立即通知应用部门停止应用并关闭所有设备。

（5）咨询及供电规划：立即向供电部门询问何时恢复供电，

并实时检测 UPS 的储存电能，并有计划地使用，如 UPS 电能不足以维持所有设备的运转，酌情关闭相关设备，保证关键设备的运作。

（6）电力恢复：开启设备，系统恢复到日常状态，通知相关部门系统恢复。

（7）总结汇报：对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.9 中心机房火灾

无论火情大小，首先保证人身安全。

火情较大时：

迅速撤离现场，拨打 119 报警，并通知领导小组和应急响应实施小组，报告火情（例如：20XX 年 X 月 X 日 X 点 X 分，中心机房火灾，人员全部撤离现场，已拨打 119 报警）。

火情较小时：

（1）火情控制：手持灭火器根据火情报警控制器显示的位置，到达火情发生位置，切断相应设备或机柜电源，若发现明火，立即使用手持式灭火器进行灭火。

（2）火情发展不能自动启动消防系统，需人工启动时，机房人员应在 30 秒内有序撤离机房，并拨打 119。

（3）通知相关人员：通知领导小组和应急响应实施小组，报告火情（例如：20XX 年 X 月 X 日 X 点 X 分，中心机房火灾，人员全部撤离现场，已拨打 119 报警）。

（4）总结汇报：分析火情原因、评估损害程度、总结经验教训、提出改进办法、完善整改措施，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

5.2.10 中心机房水情

水情较小时：

若为空调漏水，则关闭空调，联系空调维保厂商进行维修，维修完成后开启空调除湿功能进行除湿。

若为墙壁渗水，联系相关人员维修渗水墙壁，维修完成后开启空调除湿功能进行除湿。

水情较大时：

（1）水情控制：根据水情现场的实际情况，做出相应的反应和处置，切断相关电源、水源，关闭相关设备，确保损失降到最小。

（2）通知相关人员：通知领导小组或应急响应实施小组，报告事件发现时间、位置、水情状况、处理等（例如：20XX 年 X 月 X 日 X 点 X 分，中心机房空调排水管破裂，造成机房积水，已切断空调电源和 XXX 设备电源）。

（3）水情处理：根据水情情况排除积水，维护设备，排除水情隐患。

（4）系统恢复：确认水情隐患排除后，技术保障小组进行系统的恢复。

（5）总结汇报：分析火情原因、评估损害程度、总结经验教训、提出改进办法、完善整改措施，形成网络与信息安全事件处理报告，在调查工作结束后一日内书面报告领导小组。

6 预防工作

6.1 日常管理

各部门按职责做好网络安全事件日常预防工作，制定、完善相关专项应急处理方案，做好网络安全检查、隐患排查、风险评估和灾难备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

（1）建立健全应急保障体系。采用多种技术手段监控和保障单位信息系统安全，不断完善网络安全管理制度。

（2）全面落实网络安全等级保护基本要求。按照网络安全等级保护基本要求制定防护策略，设计防护方案，落实防护措施，检查防护效果，修补防护漏洞，保障网络安全。

（3）有效落实网络安全风险评估制度。在新系统上线、系统升级、网络改造、设备更新等关键信息技术资源发生重大变更及业务发生重大变化时，应重新识别、分析、控制风险。

（4）建设灾难备份系统。完善灾难备份相关制度、操作规范，对重要业务系统数据进行灾难备份，并定期开展灾备恢复演练。

（5）健全网络安全信息报告机制。各专项工作组应建立网络安全信息报告有关工作机制，公布信息报告流程和联系方式。各部门或个人发现校园网网络安全风险隐患和事件，均须及时向应急响应实施小组报告。各专项工作组收到网络安全信息报告后，应认真研判并及时发布预警和响应通知。

6.2 应急演练

网信办指导各部门组织应急演练，检验和完善预案，提高实战能力。

各部门每年至少组织一次预案演练，并根据演练结果对应急预案进行评审和修订。

发生应急事件并处理完成后，各部门应当对事件进行分析总结，进行风险评估，改进不足，弥补漏洞。

在应急预案更新后或遇有可预见的网络安全事件时，应及时开展应急演练，检验应急预案的可行性，提高有关人员的应急响应熟练程度。

应急演练以应急预案为基础，在演练前应确定演练的目标、范围及方式，制定详细、严谨的应急演练方案，避免对正常业务造成不必要的影响。应急演练如涉及上级部门或其他部门，应事先做好沟通协调工作，避免干扰其正常工作。

6.3 宣传培训

各单位应充分利用各种媒介和其他有效宣传形式，加强突发网络安全事件预防和应急处置的有关法律、法规、政策和应急响应预案的宣传，开展网络安全级别知识和技能的宣传活动。

网信办将网络与信息安全突发事件的应急管理、工作流程等作为网络安全培训内容，增强应急处置工作中的组织能力，加强网络安全特别是网络安全应急预案的培训，提高防范意识和技能。

各单位应当在网信办指导下，每年至少组织一次安全应急培训，对各级应急成员、各专项工作组成员和相关的业务、技术人

员进行应急知识培训。

6.4 重要活动期间的预防措施

在国家重要活动、会议等重要敏感时期，要加强网络安全事件的防范和应急响应，确保网络安全。领导小组统筹协调网络安全保障工作，各专项工作组加强网络安全监测和分析，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持 24 小时值班，及时发现和处置网络安全事件隐患。

7 保障措施

7.1 责任落实

要落实网络安全应急工作责任制，建立健全网络安全应急工作机制，压实领导责任，把责任落实到具体部门、具体岗位和个人。

对网络安全突发事件工作中做出突出贡献的先进集体和个人给予表彰或奖励。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的部门或个人，领导小组将给予约谈、通报或依法、依规给予问责或处分。

7.2 人力保障

加强学校信息安全人才培养，强化信息安全宣传教育，培养和建立一支高素质、高技术的信息安全核心人才和管理队伍，提高信息安全防御意识。

7.3 技术保障

加强学校网络安全管理平台建设，建立预警与应急处理的技术平台，进一步提高信息安全事件的发现和分析能力。从技术上逐步实现发现、预警、处置、通报等多个环节和不同的网络、系统、部门之间应急处理的联动机制。

7.4 物资保障

根据全省高校乃至全国网络信息系统安全防治工作所需经

费情况,将本年度信息安全应急响应经费纳入年度财政计划和预算，建立校园网专项资金用于校园网安全事件的处置，购买相应的应急设施，避免时间拖延造成不必要的损失，保证应急响应技术装备的及时更新，以确保应急响应工作的顺利进行。

8 附 则

8.1 预案管理

在领导小组领导下，各部门应做好应急预案的维护工作，确保应急预案的完整性、实用性、可行性，有效指导应急响应工作。

（1）将应急预案最新版本分发给相关人员。

（2）根据信息基础设施、人员、业务变动情况及时更新应急预案。

（3）在应急响应或演练结束后，分析评估应急预案的执行效果，根据需要对应急预案进行修订、完善。

（4）原则上应急预案应每年进行评估、修订，发布更新，以确保应急预案的准确性和有效性。

8.2 预案解释

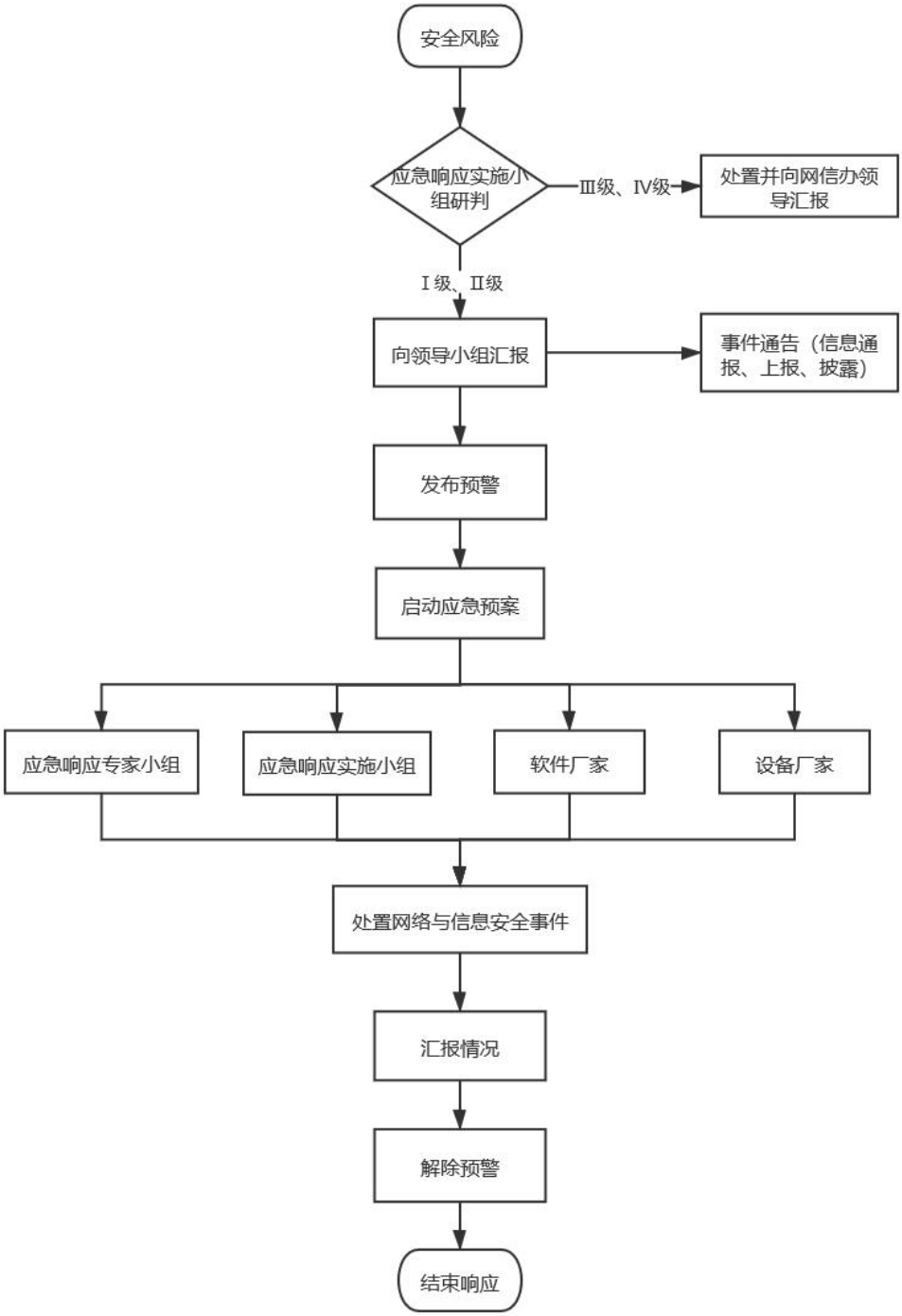
本预案由网络安全与信息化办公室负责解释。

8.3 预案实施时间

本预案自发布之日起施行。

9 附　件

附件 1：应急处置基本流程



附件 2：应急组织机构联系人清单

应急小组名称	姓名	所在部门	工作职责	联络方式	
				手机	紧急联系人及电话
网络安全和信息化领导小组					
应急响应实施小组					
应急响应专家小组					

附件 3：应急物资清单

应急物资清单					
序号	**物品名称**	**数量**	**存放位置**	**负责人/联系电话**	**备注**
1	备用服务器	3	中心机房	XXX 部门/人员	
2					
3					
4					
5					

附件 4：网络安全事件报告表

单位名称：(需加盖单位公章)

报告时间： 年 月 日 时 分

网络安全事件报告表	
发生事件的时间： 年 月 日 时 分	
发现事件的时间： 年 月 日 时 分	
报告人：	联系电话：
传真：	电子邮件：
通讯地址：	
发生网络安全事件的信息系统（设备、网络）或事项名称及用途：	
负责部门：	负责人：
网络安全事件的简要描述（如以前出现过类似情况也应加以说明）:	

网络安全事件的类型：

□攻击事件 □故障事件 □灾害事件 □其他类事件

网络安全事件的级别：

□特别重大（I级） □重大（II级） □较大（III） □一般（IV）

初步判定的事故原因：

受影响的资产：

□信息/数据_____.

□硬件_____.

□软件_____.

□通信设施_____.

影响范围和严重程度：

已经采取的措施：

计划采取的措施：

附件 5：网络安全事件应急响应结果报告表

单位名称：(需加盖单位公章)

报告时间： 年 月 日 时 分

<table>
<tr><th colspan="6">网络安全事件应急响应结果报告表</th></tr>
<tr><td>报告人</td><td></td><td>联系电话</td><td></td><td>传真</td><td></td></tr>
<tr><td>通讯地址</td><td colspan="2"></td><td>电子邮件</td><td colspan="2"></td></tr>
<tr><td>系统名称</td><td colspan="2"></td><td>主要用途</td><td colspan="2"></td></tr>
<tr><td colspan="6">信息系统的基本情况（如涉及请填写）

1. 系统网址和 IP 地址：_____

2. 系统主管单位/部门：_____

3. 系统运维单位/部门：_____

4. 系统使用单位/部门：_____

5. 是否定级 □是 □否，所定级别：_____

6. 是否备案 □是 □否，备案号：_____

7. 是否测评 □是 □否

8. 是否整改 □是 □否</td></tr>
<tr><td colspan="6">网络安全事件描述</td></tr>
<tr><td colspan="6">最终判定事件原因及责任人（可加页附文字、图片以及其他文件）</td></tr>
</table>

<table>
<tr><td colspan="2">事件影响状况评估</td></tr>
<tr><td>事件级别</td><td>□特别重大（I级） □重大（II级） □较大（III） □一般（IV）</td></tr>
<tr><td>影响时间</td><td></td></tr>
<tr><td>影响范围</td><td></td></tr>
<tr><td>事件后果</td><td></td></tr>
<tr><td colspan="2">主要处理过程及结果</td></tr>
<tr><td colspan="2">存在问题及建议</td></tr>
<tr><td colspan="2">网信办处理意见</td></tr>
<tr><td colspan="2">领导小组审批意见</td></tr>
</table>

附件 6：应急演练方案（模板）

应急演练方案（模板）

一、方案概述

（1）目的

（2）时间

（3）范围

（4）内容

（5）应急场景

二、应急演练人员

（1）领导人员

（2）应急演练成员

三、应急演练过程

（1）……

（2）……

（3）……

四、应急资源

（1）……

（2）……

（3）……

附件 7：应急演练记录单

<table>
<tr><td colspan="4">应急演练记录单</td></tr>
<tr><td>演练名称</td><td></td><td>演练时间</td><td></td></tr>
<tr><td>组织人</td><td></td><td>演练地点</td><td></td></tr>
<tr><td colspan="4">记录内容：</td></tr>
<tr><td colspan="4">改进建议：</td></tr>
<tr><td colspan="4">记录人：</td></tr>
<tr><td>参加部门/人员：</td><td colspan="3"></td></tr>
</table>

山东科技大学

网络安全基线配置标准

2020 年 6 月

目 录

第 1 章 概述 131

1.1 基线目的 131

1.2 标准说明 131

1.3 适用范围 131

第 2 章 终端安全基线 132

2.1 账户及口令 132

2.1.1 管理账户安全 132

2.1.2 密码有效期 132

2.1.3 密码复杂度 133

2.1.4 账户锁定策略 133

2.1.5 禁用远程服务 134

2.2 安全策略配置 134

2.2.1 开启安全审核 134

2.2.2 关闭危险端口 134

2.2.3 临时信息清除 135

2.2.4 运行杀毒软件 135

2.2.5 管理用户权限控制 136

2.3 实名注册及软件安装 136

第 3 章 服务器安全基线 137

3.1 账户及口令 137

3.1.1 管理账户安全 137

3.1.2 密码有效期.....137
3.1.3 密码复杂度.....138
3.1.4 账户锁定策略.....138
3.1.5 登录超时锁定.....139
3.1.6 远程管理加密.....139
3.1.7 双因子认证登录.....139
3.1.8 远程登录地址限制.....140
3.2 安全策略配置.....140
3.2.1 开启安全审核.....140
3.2.2 审核日志保护.....141
3.2.3 日志时间校准.....141
3.2.4 关闭危险端口.....141
3.2.5 访问控制策略.....142
3.2.6 运行杀毒软件.....142
3.2.7 临时信息清除.....143
3.2.8 管理用户权限控制.....144
3.2.9 服务器运行状态监控.....144
3.3 实名注册及软件安装.....145
第 4 章 网络、安全设备安全基线.....146
4.1 账户及口令.....146
4.1.1 管理账户安全.....146
4.1.2 口令加密存储.....146
4.1.3 密码复杂度.....147

4.1.4 账户锁定策略.....147
4.1.5 登录超时锁定.....148
4.1.6 远程管理加密.....148
4.1.7 登录地址限制.....149
4.2 安全策略配置.....149
4.2.1 开启安全审计.....149
4.2.2 审计日志保护.....149
4.2.3 日志时间校准.....150
4.2.4 访问控制策略.....150
4.2.5 入侵攻击防御.....150
4.2.6 网络系统运行状态监控.....151
第 5 章 应用系统开发安全基线.....152
5.1 身份与访问控制.....152
5.1.1 账户锁定策略.....152
5.1.2 登录图片验证码.....152
5.1.3 口令传输.....152
5.1.4 保存登录功能.....153
5.1.5 纵向访问控制.....153
5.1.6 横向访问控制.....153
5.1.7 敏感资源访问.....154
5.1.8 证书单轨制登录.....154
5.2 会话管理.....154
5.2.1 会话超时.....154

5.2.2 会话终止.....155
5.2.3 会话标识.....155
5.3 代码质量.....156
5.3.1 防范跨站脚本攻击.....156
5.3.2 防范 SQL 注入攻击.....156
5.3.3 防范路径遍历攻击.....156
5.3.4 防范命令注入攻击.....157
5.3.5 防范其他常见注入攻击.....157
5.3.6 防范上传后门脚本.....157
5.3.7 保证释放资源.....158
5.4 内容管理.....158
5.4.1 加密存储敏感信息.....158
5.4.2 避免泄露敏感技术细节.....158
5.5 密码算法.....159
5.5.1 密码算法安全.....159
5.5.2 密钥管理安全.....159
5.6 交付安全.....159
5.6.1 应用系统交付安全.....159
5.6.2 业务逻辑安全.....160

第1章 概述

1.1 基线目的

为做好网络安全防护，保证联网终端、服务器、网络与安全设备等以及应用系统的安全基线配置规范，特制定本标准。

1.2 标准说明

本标准是网络安全防护基本要求,联网设备和应用系统的安全配置应当满足本标准要求，可在本标准之上做更严格、更深化的安全配置和部署。

本标准配置范例以windows操作系统和华为网络设备为代表,具体安全配置应当根据设备和系统的实际情况参考范例配置。

1.3 适用范围

本标准适用校园网。

第 2 章 终端安全基线

2.1 账户及口令

2.1.1 管理账户安全

基线名称	终端管理账户安全基线要求
基线要求	不得使用 administrator、admin、sa 等默认用户名作为管理账户；禁用 guest 等来宾账户。
配置范例	进入“控制面板→管理工具→计算机管理”，在“系统工具→本地用户和组”: 缺省账户 Administrator→属性，Guest 账户→属性。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.2 密码有效期

基线名称	终端密码有效期安全基线要求
基线要求	账户口令的生存期不长于 90 天，修改密码 5 次内不得重复。
配置范例	进入“控制面板→管理工具→本地安全策略”，在“账户策略→密码策略”: 查看“密码最长存留期”和“强制密码历史”。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.3 密码复杂度

基线名称	终端密码复杂度安全基线要求
基线要求	操作系统账户不得使用空密码，不得使用全数字密码（如 11111、123456）和存在输入规律（如 1qaz2wsx）的弱密码，必须设置足够强壮的密码，最短密码长度 8 个字符，至少包含大写字母、小写字母、数字和字符中的 3 类；启用本机组策略中密码必须符合复杂性要求的策略。
配置范例	设置登录密码，至少 8 位，至少包含大写字母、小写字母、数字和字符中的 3 类。可采用“XXXX@****”组合设置密码，其中 XXXX 为长度不少于 3 位的大小写字母组合，可选择使用姓名拼音缩写，****为长度不少于 4 位的数字组合，可选择使用出生年月日或电话号码等。 进入“控制面板→管理工具→本地安全策略”，在“账户策略→密码策略”查看是否“密码必须符合复杂性要求”选择“已启动”。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.4 账户锁定策略

基线名称	终端账户锁定策略安全基线要求
基线要求	配置当用户连续认证失败次数超过 5 次（不含 5 次），锁定该用户使用的账户，锁定时间 20 分钟。
配置范例	进入“控制面板→管理工具→本地安全策略”，在“账户策略→账户锁定策略”: 查看“账户锁定阈值”设置。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.5 禁用远程服务

基线名称	终端远程服务安全基线要求
基线要求	PC 机不得开启远程桌面、Telnet、远程协助等服务。
配置范例	进入“我的电脑右键→属性→远程”，在“允许用户远程连接到此计算机”选项上不得勾选。
适用范围	PC 机。

2.2 安全策略配置

2.2.1 开启安全审核

基线名称	终端审核策略安全基线要求
基线要求	必须配置审核日志功能，审核登录事件、系统事件、账户管理、策略更改和权限使用 5 类操作行为，记录 5 类操作行为的成功和失败操作结果。
配置范例	进入“ 控制面板→管理工具→本地安全策略→审核策略”基线要求的策略全部选中“成功”和“失败”。
适用范围	PC 机。

2.2.2 关闭危险端口

基线名称	终端端口管理安全基线要求
基线要求	禁用 135、137、138、139 和 445 端口。
配置范例	点击“ 开始→运行”输入“regedit”进入“注册表编辑器”依次点击进入“HKEY_LOCAL_MACHINE→SYSTEM → CurrentControlSet → services → NetBT → Parameters”选项，在“Parameters”这个子项的右侧，点击鼠标右键，“新建→QWORD（64 位）值”，然后重命名为“SMBDeviceEnabled”，将“数值数据”的值改为 0，即可关闭 445 端口。
适用范围	PC 机。

2.2.3 临时信息清除

基线名称	终端临时信息保护安全基线要求
基线要求	在退出系统时删除临时文件夹，关机时清理虚拟内存页面文件，用户登录时不显示最后的用户名，不允许将 Everyone 权限应用于匿名用户，不允许在下次更改密码时存储 LAN Manager 的哈希值，不允许 SAM 账户和共享的匿名枚举。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→安全选项”禁用以下选项:“在退出时不删除临时文件夹”、“网络访问: 将 Everyone 权限应用于匿名用户”，启用以下选项:“关机: 清理虚拟内存页面文件”、“交互式登录: 不显示最后的用户名”、“网络安全: 不要在下次更改密码时存储 LAN Manager 的哈希值”、“网络访问: 不允许 SAM 账户和共享的匿名枚举”。
适用范围	PC 机。

2.2.4 运行杀毒软件

基线名称	终端杀毒软件安全基线要求
基线要求	必须安装并运行统一的企业版杀毒软件，并保持病毒库及时更新。
配置范例	安装市局指定的杀毒软件，并保证杀毒软件正常运行。
适用范围	PC 机。

2.2.5 管理用户权限控制

基线名称	终端权限控制安全基线要求
基线要求	系统重要操作如：提高计划优先级、管理审核和安全日志、取得文件或其他对象的所有权、创建一个页面文件、从远程系统强制关机、加载和卸载设备驱动程序、调试程序、执行卷维护任务和配置文件系统性能等仅允许管理用户组。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→用户权限分配”将“提高计划优先级”、“管理审核和安全日志”、“取得文件或其他对象的所有权”、“创建一个页面文件”、“从远程系统强制关机”、“加载和卸载设备驱动程序”、“调试程序”、“执行卷维护任务”和“配置文件系统性能”的“安全设置”调整为Administrators（管理用户组）。
适用范围	PC 机。

2.3 实名注册及软件安装

基线名称	终端实名注册及软件安装基线要求
基线要求	终端接入公安网必须进行实名注册，必须安装一机两用客户端、安全助手和终端安全接入客户端，办理公安网入网审批流程。
配置范例	终端使用者进行实名注册安装一机两用客户端，安装终端安全接入客户端并通过终端安全接入系统入网审批，下载安装公安网安全助手。
适用范围	PC 机。

第 3 章 服务器安全基线

3.1 账户及口令

3.1.1 管理账户安全

基线名称	操作系统管理账户安全基线要求
基线要求	不得使用 administrator、admin、sa 等默认用户名作为管理账户；禁用 guest 等来宾账户。
配置范例	进入“控制面板→管理工具→计算机管理”，在“系统工具→本地用户和组”: 缺省账户 Administrator－〉属性，Guest 账户→属性。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.1.2 密码有效期

基线名称	操作系统密码有效期安全基线要求
基线要求	账户口令的生存期不长于 90 天，修改密码 5 次内不得重复。
配置范例	进入“控制面板→管理工具→本地安全策略”，在“账户策略→密码策略”，查看“密码最长存留期”和“强制密码历史”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统） 。

3.1.3密码复杂度

基线名称	操作系统密码复杂度安全基线要求
基线要求	操作系统账户不得使用空密码，不得使用全数字密码（如 11111、123456）和存在输入规律（如 1qaz2wsx）的弱密码，必须设置足够强壮的密码，最短密码长度 8 个字符，至少包含大写字母、小写字母、数字和字符中的 3 类；启用本机组策略中密码必须符合复杂性要求的策略。
配置范例	设置登录密码，至少 8 位，至少包含大写字母、小写字母、数字和字符中的 3 类，可采用“XXXX@****”组合设置密码，其中 XXXX 为长度不少于 3 位的大小写字母组合，可选择使用姓名拼音缩写，****为长度不少于 4 位的数字组合，可选择使用出生年月日或电话号码等; 进入“控制面板→管理工具→本地安全策略”，在“账户策略→密码策略”查看是否“密码必须符合复杂性要求”选择“已启动”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.1.4账户锁定策略

基线名称	操作系统账户锁定策略安全基线要求
基线要求	配置当用户连续认证失败次数超过 5 次（不含 5 次），锁定该用户使用的账户，锁定时间 20 分钟。
配置范例	进入“控制面板→管理工具→本地安全策略”，在“账户策略→账户锁定策略”: 查看“账户锁定阀值”设置。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.1.5登录超时锁定

基线名称	操作系统登录操作超时锁定安全基线要求
基线要求	配置当用户操作空闲时间超过20分钟后，中断会话连接。
配置范例	进入“组策略→计算机配置→管理模板Windows组件→终端服务”，在“会话”中查看“空闲会话限制”时间，设置为20分钟。
适用范围	所有服务器（包含Windows、Linux及UNIX等操作系统）。

3.1.6远程管理加密

基线名称	操作系统远程管理安全基线要求
基线要求	服务远程管理必须采用RDP（SSL加密）或SSH等加密协议。
配置范例	进入“控制面板→管理工具→终端服务配置连接”，在“RDP—Tcp→属性”：查看“RDP—Tcp属性”设置，选择SSL。
适用范围	所有服务器（包含Windows、Linux及UNIX等操作系统）。

3.1.7双因子认证登录

基线名称	操作系统登录认证安全基线要求
基线要求	重要服务器远程登录时，应采用双因子认证方式，在用户名、密码的基础上增加证书、Ukey等鉴别因子，保证登录用户身份合法。
配置范例	通过堡垒机设备配合网络安全设备的访问控制策略实现。
适用范围	所有服务器（包含Windows、Linux及UNIX等操作系统）。

3.1.8远程登录地址限制

基线名称	操作系统远程登录安全基线要求
基线要求	严格限制能够远程登录服务器的接入方式和地址范围，采用白名单方式，仅允许必要的终端以固定的协议（如远程桌面、SSH） 远程登录到服务器。
配置范例	通过主机防火墙、网络设备或安全设备的访问控制功能实现。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2 安全策略配置

3.2.1 开启安全审核

基线名称	操作系统审核策略安全基线要求
基线要求	必须配置审核日志功能，审核登录事件、系统事件、账户管理、策略更改和权限使用 5 类操作行为，记录 5 类操作行为的成功和失败操作结果。
配置范例	进入“ 控制面板→管理工具→本地安全策略→审核策略”基线要求的策略全部选中“成功”和“失败”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.2审核日志保护

基线名称	操作系统审核日志保护安全基线要求
基线要求	对于服务器的审核日志，应在服务器本地以外，另外保存一份备份日志，保留期限不少于6个月，保证设备出现问题时，可以找到重要的日志信息。
配置范例	通过独立的日志服务器、审计系统或异地备份等方式，实现服务器日志的保护和备份。
适用范围	所有服务器（包含Windows、Linux及UNIX等操作系统）。

3.2.3日志时间校准

基线名称	操作系统日志时间准确性安全基线要求项
基线要求	必须配置时钟同步服务器，保证服务器日志记录时间的准确性。
配置范例	进入“ 控制面板→日期和时间→internet 时间→更改设置”配置正确的时钟同步服务器地址或域名。
适用范围	所有服务器（包含Windows、Linux及UNIX等操作系统）。

3.2.4关闭危险端口

基线名称	操作系统端口管理安全基线要求
基线要求	禁用135、137、138、139和445端口。
配置范例	点击“ 开始→运行”输入“regedit”进入“注册表编辑器”依次点击进入“HKEY_LOCAL_MACHINE→SYSTEM→ CurrentControlSet → services → NetBT → Parameters”选项，在“Parameters”这个子项的右侧，点击鼠标右键，“新建→QWORD（64位）值”，然后重命名为“SMBDeviceEnabled”，将“数值数据”的值改为0，即可关闭445端口。
适用范围	所有服务器（包含Windows、Linux及UNIX等操作系统）。

3.2.5访问控制策略

基线名称	操作系统访问控制安全基线要求
基线要求	服务器应配置严格的访问控制策略，仅允许必要的地址和端口访问本机 。
配置范例	访问控制策略采用白名单方式，如数据库服务器可通过防火墙配置访问控制列表，仅允许相关应用服务器、堡垒机和远程管理用户终端等通过特定端口访问。根据应用的用户数量和信息敏感程度，限制应用访问范围（特殊情况须由专家讨论决定）。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.6运行杀毒软件

基线名称	操作系统杀毒软件安全基线要求
基线要求	服务器必须安装并运行统一的企业版杀毒软件，并保持病毒库及时更新。
配置范例	必须安装市局指定的杀毒软件并保证杀毒软件正常运行。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.7临时信息清除

基线名称	操作系统临时信息保护安全基线要求
基线要求	在退出系统时删除临时文件夹，关机时清理虚拟内存页面文件，用户登录时不显示最后的用户名，不允许将 Everyone 权限应用于匿名用户，不允许在下次更改密码时存储 LAN Manager 的哈希值，不允许 SAM 账户和共享的匿名枚举。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→安全选项”禁用以下选项:“在退出时不删除临时文件夹”、“网络访问: 将 Everyone 权限应用于匿名用户”,启用以下选项:“关机: 清理虚拟内存页面文件”、“交互式登录: 不显示最后的用户名”、“网络安全: 不要在下次更改密码时存储 LAN Manager 的哈希值”、“网络访问: 不允许 SAM 账户和共享的匿名枚举”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.8管理用户权限控制

基线名称	操作系统权限控制安全基线要求
基线要求	系统重要操作如：提高计划优先级、管理审核和安全日志、取得文件或其他对象的所有权、创建一个页面文件、从远程系统强制关机、加载和卸载设备驱动程序、调试程序、执行卷维护任务和配置文件系统性能等仅允许管理用户组。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→用户权限分配”将“提高计划优先级”、“管理审核和安全日志” 、“取得文件或其他对象的所有权”、“创建一个页面文件” 、“从远程系统强制关机” 、“加载和卸载设备驱动程序” 、“调试程序”、“执行卷维护任务”和“配置文件系统性能”的“安全设置”调整为 Administrators（管理用户组）。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.9服务器运行状态监控

基线名称	操作系统运行状况监控安全基线要求
基线要求	重要服务器必须监控操作系统运行状况，监控范围包含 CPU、内存、硬盘等，设置服务水平阈值，在系统的服务水平降低到一定值时进行报警。
配置范例	通过虚拟机管理工具、服务器运行监控软件等工具软件实现对系统运行状态的监控和报警。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.3 实名注册及软件安装

基线名称	服务器实名注册及软件安装基线要求
基线要求	Windows 操作系统服务器接入公安网必须进行实名制注册安装一机两用客户端及公安网安全助手。其他操作系统必须在一机两用系统内申请设备保护，并填报相关设备信息。
配置范例	服务器安装一机两用客户端和公安网安全助手，或者申请保护设置。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

第 4 章 网络、安全设备安全基线

4.1 账户及口令

4.1.1管理账户安全

基线名称	网络、安全设备管理账户安全基线要求
基线要求	所有网络、安全设备不得使用 admin、root 等常见默认用户名，不同管理员应使用不同的管理账户。
配置范例	local—user XXXX。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.2口令加密存储

基线名称	网络、安全设备用户口令加密存储安全基线要求
基线要求	用户口令必须使用不可逆加密算法加密后保存于配置文件中。
配置范例	password cipher XXXX
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.3密码复杂度

基线名称	网络、安全设备密码复杂度安全基线要求
基线要求	不得使用空密码，不得使用全数字密码（如 11111、123456）和存在输入规律（如 1qaz2wsx）的弱密码，必须设置足够强壮的密码，最短密码长度 8 个字符，至少包含大写字母、小写字母、数字和字符中的 3 类;可采用“XXXX@****”组合设置密码，其中 XXXX 为长度不少于 3 位的大小写字母组合，可选择使用姓名拼音缩写，****为长度不少于 4 位的数字组合，可选择使用出生年月日或电话号码等。
配置范例	根据设备情况，选择密码复杂度符合要求的配置选项。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.4账户锁定策略

基线名称	网络、安全设备账户锁定安全基线要求
基线要求	网络、安全设备应启用登录失败处理功能，当用户连续认证失败次数超过 5 次（不含 5 次），锁定该用户使用的账户，锁定时间 20 分钟。
配置范例	password—control login—attempt 5 exceed lock—time 20
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.5登录超时锁定

基线名称	网络、安全设备登录操作超时锁定安全基线要求
基线要求	网络、安全设备必须启用登录操作超时锁定功能，可通过设备登录配置或安全设备（如防火墙、堡垒机）配置实现，操作空闲时间超过（最长）20 分钟后，断开会话连接。
配置范例	Line vty Exec—timeout 20 0
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.6远程管理加密

基线名称	网络、安全设备远程管理安全基线要求
基线要求	网络、安全设备远程登录时，使用 SSH 或 https 等加密方式。
配置范例	user—interface vty 0 4 authentication—mode scheme protocol inbound ssh local—user XXXX ….. service—type ssh
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.7登录地址限制

基线名称	网络、安全设备远程登录安全基线要求
基线要求	严格限制能够远程登录和管理网络、安全设备的登录地址范围，采用白名单方式，仅允许必要的终端以固定的协议（如 SSH、https 等） 远程登录和管理网络、安全设备。
配置范例	通过设备安全配置和网络、安全设备的访问控制策略实现。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2 安全策略配置

4.2.1开启安全审计

基线名称	网络、安全设备审计策略安全基线要求
基线要求	开启日志审计功能，审计系统日志，操作日志和告警日志等。
配置范例	根据具体设备自行配置，开启日志功能。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2.2审计日志保护

基线名称	网络、安全设备日志保护安全基线要求项
基线要求	日志信息通过SYSLOG 等方式传输至日志服务器备份保存，保留期限不少于 6 个月。
配置范例	搭建 SYSLOG 日志服务器，接收保存各类设备发送的 SYSLOG 日志。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2.3日志时间校准

基线名称	网络、安全设备日志时间准确性安全基线要求项
基线要求	开启 NTP 服务，保证日志功能记录的时间的准确性。所有网络、安全设备与 NTP SERVER 之间要开启认证功能。
配置范例	ntp-service authentication enable ntp-service unicast-server 192.168.1.1
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2.4访问控制策略

基线名称	网络系统访问控制安全基线要求
基线要求	在同一网络中，应当根据安全级别不同将网络划分为不同的安全区域，各个安全区域的边界处分别部署具有访问控制隔离功能的网络安全设备，并配置严格的访问控制策略。
配置范例	访问控制策略应采用白名单方式，控制粒度至少包含源、目的地址和端口号（协议）。
适用范围	所有网络系统。

4.2.5入侵攻击防御

基线名称	网络系统入侵防御安全基线要求
基线要求	在网络重要区域（如核心网络交换机、服务器汇聚交换机等）必须部署入侵防御或检测设备，对服务器区和其他重要区域的入侵行为进行检测和阻断。
配置范例	可选择入侵防御系统或入侵检测系统，必须能够对入侵行为进行发现和阻断，并提供入侵告警功能。
适用范围	所有网络系统。

4.2.6网络系统运行状态监控

基线名称	网络系统运行状态监控安全基线要求
基线要求	监控网络系统运行状况，监控范围包含所有网络设备运行情况和带宽、流量等信息。
配置范例	通过网络管理软件、IT 运维管理软件等工具软件实现对网络系统运行状态的监控和报警。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

第 5 章 应用系统开发安全基线

5.1 身份与访问控制

5.1.1 账户锁定策略

基线名称	Web 应用账户锁定策略安全基线要求项
基线说明	用户登录失败 3-5 次后，系统自动锁定账户不少于 15 分钟，并记录日志。
检测方式	尝试使用错误用户名口令失败登录多次，查看是否允许无限制尝试。
符合判定依据	用户登录失败 3-5 次后系统自动锁定账户。

5.1.2 登录图片验证码

基线名称	Web 应用登录图片验证码安全基线要求项
基线说明	用户登录需输入图片验证码，以防止固定密码暴力猜测账户。
检测方式	检查登录认证界面输入项，并右键点击图片查看链接属性。
符合判定依据	要求包含图片验证码输入项，并且图片链接属性不包含图片中验证码。

5.1.3 口令传输

基线名称	Web 应用口令传输策略安全基线要求项
基线说明	应采用密文方式传输用户登录密码。
检测方式	尝试登录系统，并使用抓包工具查看交互过程中在网络传输的内容。
符合判定依据	要求不得出现明文用户名和口令。

5.1.4保存登录功能

基线名称	Web 应用保存登录安全基线要求项
基线说明	不提供“保存登录”功能，不得在浏览器中缓存用户登录信息。
检测方式	检查登录界面是否提供了保存登录功能。
符合判定依据	不得提供“保存登录”功能，浏览器缓存中不能存在用户登录信息。

5.1.5纵向访问控制

基线名称	Web 应用纵向访问安全基线要求项
基线说明	合理进行纵向访问控制，不允许非授权用户访问管理功能。
检测方式	了解是否有不允许普通用户访问的功能，尝试直接在浏览器中访问功能链接。
符合判定依据	用户不得跨权限访问受控页面。

5.1.6横向访问控制

基线名称	Web 应用横向访问安全基线要求项
基线说明	合理进行横向访问控制，不允许用户访问其他用户的敏感数据。
检测方式	了解是否存在敏感信息，检查是否对个人敏感信息进行了有效保护。
符合判定依据	用户不得跨权限查看其它用户受保护的敏感信息。

5.1.7敏感资源访问

基线名称	Web 应用敏感资源访问安全基线要求项
基线说明	必须严格限制对敏感资源的访问，如重要用户数据、后台管理和日志记录等。
检测方式	查看服务器上敏感资源的访问权限设置。
符合判定依据	严格限制敏感资源的访问权限。

5.1.8证书单轨制登录

基线名称	Web 应用证书登录安全基线要求项
基线说明	必须使用公安数字证书作为用户身份认证与应用权限管理的依据。
检测方式	检查应用系统用户登录方式，是否只有证书登录一种方式。
符合判定依据	用户登录应用系统只能够使用公安数字证书登录。

5.2 会话管理

5.2.1会话超时

基线名称	Web 应用会话超时安全基线要求项
基线说明	当用户长时间不操作时，系统自动终止超时会话。
检测方式	登录系统后不操作，等待合理的时间间隔，检查系统是否会自动断开。
符合判定依据	要求预先设计的时间间隔后查看页面自动中止超时会话。

5.2.2会话终止

基线名称	Web 应用会话终止安全基线要求项
基线说明	系统需提供“退出”功能，允许用户强制终止当前的会话。
检测方式	登录系统后，点击系统提供的“退出”功能，检查浏览器能否自动关闭或者退至系统登录页面。
符合判定依据	点击系统提供的“退出”功能后，检查浏览器能够自动关闭或者退至系统登录页面；若退至登录页面，浏览器不得返回系统操作界面，必须重新做用户认证登录后，才能进行正常操作。

5.2.3会话标识

基线名称	Web 应用会话标识安全基线要求项
基线说明	应用系统会话标识必须是随机生成，防止攻击者猜测标识或依据当前标识推导后续的标识。
检测方式	检查系统会话标识的格式，检查会话标识方式，是否存在简单的逻辑关系。
符合判定依据	多个会话标识不得存在简单明了的逻辑关系，必须具有随机性。

5.3 代码质量

5.3.1 防范跨站脚本攻击

基线名称	Web 应用防范跨站脚本安全基线要求项
基线说明	应用系统应当对用户的输入内容进行预处理，不得未经检查将用户输入内容直接输出到用户浏览器，防范跨站脚本攻击。
检测方式	检查系统是否存在跨站脚本攻击漏洞。例如在能够回显的输入框输入<script〉alert(“xss”)</script〉。
符合判定依据	要求系统能够将输入内容中的控制字当作纯文本内容处理。

5.3.2 防范 SQL 注入攻击

基线名称	Web 应用防范 SQL 注入安全基线要求项
基线说明	系统必须对用户的输入内容进行预处理，防止用户利用输入内容构建 SQL 语句。
检测方式	检查系统是否存在 SQL 注入漏洞。例如在输入框中输入 “’” 字符。
符合判定依据	系统要使用诸如 prepared statement 等方式防止 SQL 注入，将输入内容中的控制字也当作纯文本处理。

5.3.3 防范路径遍历攻击

基线名称	Web 应用防范路径遍历安全基线要求项
基线说明	系统必须对用户的输入内容进行预处理，防止用户利用输入内容构建文件路径进行路径遍历攻击。
检测方式	尝试在 URL 与输入中构造文件路径并查看页面反应。
符合判定依据	不允许通过构造文件路径的方式直接查看文件。

5.3.4 防范命令注入攻击

基线名称	Web 应用防范命令注入安全基线要求项
基线说明	系统必须对用户的输入内容进行预处理，防止用户利用输入内容构造操作系统命令并执行。
检测方式	尝试在各个输入点进行命令注入攻击。
符合判定依据	命令注入攻击不得成功。

5.3.5 防范其他常见注入攻击

基线名称	Web 应用防范其它注入安全基线要求项
基线说明	系统不得存在 LDAP 注入、XML 注入、XPATH 注入、SMTP 注入等漏洞。
检测方式	尝试在各个输入点进行其它常见注入攻击。
符合判定依据	各类注入攻击不得成功。

5.3.6 防范上传后门脚本

基线名称	Web 应用防范上传漏洞安全基线要求项
基线说明	提供文件上传功能的系统，必须对上传的内容进行检测和处理，防止用户上传后门脚本。
检测方式	利用系统提供的上传功能，测试能否上传恶意文件。
符合判定依据	各类上传攻击不得成功。

5.3.7保证释放资源

基线名称	Web 应用释放资源基线要求项
基线说明	应用系统必须及时释放与回收资源，保证合法用户的正常使用。
检测方式	分析检查正常与异常流程中资源释放的动作。
符合判定依据	资源释放覆盖所有流程分支。

5.4 内容管理

5.4.1加密存储敏感信息

基线名称	Web 应用加密存储敏感信息基线要求项
基线说明	应用系统应当使用国产密码算法对账户、密码等敏感信息做加密保护。
检测方式	分析系统中敏感信息的存储与加密，是否使用安全的国产密码算法。
符合判定依据	要求敏感信息在存储时，必须使用安全的国产密码算法。

5.4.2避免泄露敏感技术细节

基线名称	Web 应用信息泄漏基线要求项
基线说明	应用系统不得向用户反馈详细的错误信息，只反馈页面友好错误提示。
检测方式	分析各个页面的源代码，查看提示页面，尤其是出错提示页面是否存在不安全的信息。
符合判定依据	各个页面不得包含技术性注释，各个提示页面不得包含 Web 服务器版本、源代码等信息。

5.5 密码算法

5.5.1 密码算法安全

基线名称	Web 应用密码算法基线要求项
基线说明	应用系统应当采用国产密码算法保护。
检测方式	检查系统中使用的密码算法，是否为国产密码算法。
符合判定依据	不得使用已经被证明为不安全的算法、自定义不安全算法或非国产密码算法。

5.5.2 密钥管理安全

基线名称	Web 应用密钥管理基线要求项
基线说明	采用国产密码算法保护的应用系统，必须妥善保管密钥，并制定和执行相应的密钥管理办法。
检测方式	检查系统中使用的密钥管理方式，是否存在不安全的密钥管理情形。
符合判定依据	制定有密钥管理办法，且得到严格执行。

5.6 交付安全

5.6.1 应用系统交付安全

基线名称	应用系统交付安全基线要求项
基线说明	开发公司交付应用系统时，交付内容中不得包含调试页面、后门管理页面、备份数据（如程序源码、认证信息和注释信息等）、默认超级用户等。
检测方式	通过常规页面检测和渗透测试等方式，检查是否存在调试页面、后门管理页面、备份数据（如程序源码、认证信息和注释信息等）和默认超级用户等。
符合判定依据	不存在调试页面、后门管理页面、备份数据（如程序源码、认证信息和注释信息等）及默认超级用户等。

5.6.2 业务逻辑安全

基线名称	应用系统业务逻辑安全基线要求项
基线说明	开发公司交付应用系统前应对系统的业务逻辑操作进行检查，避免存在业务漏洞。
检测方式	需由第三方测评机构进行软件安全测评或渗透测试，检测是否存在业务逻辑漏洞。
符合判定依据	提供相关测试证明文件或在验收前组织第三方测评机构进行软件安全测评或渗透测试，消除业务漏洞。