上海静安区四季在线培训学校
网络安全管理制度

第一章　总则

第一条　为加强和规范上海静安区四季在线培训学校网络的安全管理，杜绝非授权的网络资源的访问、使用及控制，确保学校各网络的安全平稳运行，制定本规定。

第二条　本规定适用于网络运行维护部门及个人。

第三条　信息安全管理员负责网络安全管理流程的制订和维护、网络安全评估和检查、网络安全事件的处置。

第四条　网络管理员负责网络结构的调整和维护、网络设备的日常维护、监控和报警、网络设备（如交换机、路由器等）检查、加固和更新。

第二章　网络架构安全

第五条　网络拓扑管理

（一）网络整体的拓扑结构需进行严格的规划、设计和管理，一经确定，不能轻易更改。如因业务需要，确需对网络的整体拓扑结构进行调整和改变，需按照相应的变更与管理规程进行，并对变更后的网络拓扑进行核实。

（二）网络管理员负责维护与当前运行情况相符的网络拓扑结构图，并按照对应密级保护要求妥善保管。

第六条　网络冗余要求

为了避免关键链路节点的单点故障，防范拒绝服务攻击，应通过资源使用监控，及时发现资源瓶颈：

（一）关键网络设备，应保证主要网络设备（如核心交换机）的业务处理能力具备冗余空间，满足业务高峰期需要；

（二）网络带宽资源，应通过双链路、上网行为控制、QoS 和带宽升级等手段保证正常业务的访问要求；

（三）多媒体网络应用，应以不影响网络传输为原则，合理控制多媒体网络应用规模和范围，未经网络与信息安全工作领导小组批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。

第七条　网络区域划分与隔离

（一）网络系统应按照安全级别和功能，进行区域划分，各区域应根据其安全级别的不同采用适当的安全防护措施；

（二）各安全区域间互联时应该实施适当的隔离措施；

（三）开发测试环境应与生产网络隔离；

（四）只允许指定条件下的网络访问，逻辑隔离的网络实施缺省拒绝的访问控制。

第八条　IP 地址管理

IP 地址及其相关资料是学校网络系统的重要信息资源，不对外公开。IP 地址根据网络系统的区域、应用范围、目的与形式的不同进行划分，主要分为：服务器 IP 地址、网络设备 IP 地址、安全设备 IP 地址、语音通信设备 IP 地址、网络打印机 IP 地址等。IP 地址使用要求：

（一）服务器、网络设备、通信设备、安全设备、网络打印机的 IP 地址的设置采用固定分配方式；

（二）办公终端、IP 电话终端等的 IP 地址的设置采用自动获取方式。除有特殊需求使用固定 IP 地址分配方式的办公电脑外，其余办公电脑均采用自动获取 IP 地址的方式；

（三）任何部门或个人未经许可，不得盗用、擅自挪用、更改学校网络的 IP 地址；

（四）采用固定 IP 地址接入网络的用户，享有对该 IP 地址的专用权，同时须承担使用该 IP 地址所应担负的责任；

（五）网络管理员可以在特殊情况下（如发现某 IP 地址流量异常、被盗用、受到病毒攻击等），对相关 IP 地址及相关信息设备采取绑定、更换、封锁、关闭等强制性的控制措施。

第三章　网络设备安全配置

第九条　账号和口令

网络设备所使用的账户、口令方面的要求详见《上海静安区四季在线培训学校系统帐号和密码管理规定》。

第十条　日志管理

网络设备的运行日志，通过日志服务器的方式加以集中收集、进行记录。网络管理员定期查看网络设备日志中产生的错误或可疑项,处理结果应记录到日志检查记录中。

第十一条　备份管理

各类设备本地日志保留时间根据磁盘空间状况确定，清理重要本地日志前需进行备份，日志备份要求如下：

（一）每月至少一次将网络设备及网络安全设备生成的日志，进行集中备份；

（二）日志备份需保留至少 12 个月不能被改变，日志的备份介质应存放在安全区域，防止非授权人员查看、拷贝日志资料，防止对日志信息的删除和篡改，避免因为各种原因的损坏导致收集到的相关日志不可用。

（三）培训内容和培训数据信息须留存 1 年以上，其中直播教学的影像须留存至少 6 个月；

第十二条　软件版本升级

（一）原则上，从设备稳定性、网络协议的兼容性等方面考虑，不建议对网络设备的软件版本进行升级或打补丁。

（二）如设备软件存在重大安全漏洞隐患，确实需要升级或打补丁的，网络管理员应在厂商的指导下，先对少量设备进行升级测试，确认无误后再进行升级。在升级之前都要做好配置文件的备份工作。

第四章　网络访问策略

第十三条　总体策略

（一）网络访问策略必须基于业务需求，按照最小权限原则进行配置，禁止备注与业务无关的访问控制策略；

（二）学校网间互联安全实行统一规范、分级管理，未经网络与信息安全管理领导小组批准，任何部门或个人不得自行与外部机构实施网间互联；

（三）互联网出口、关键区域边界等必须加装防火墙，并配置访问控制策略；

（四）在访问控制设备上（如防火墙或核心路由器）禁用未经明确允许的

协议和端口；

（五）对于高风险网络区域（如开发测试区、生产区等），必要时需进行物理隔离，降低该区域的安全风险；

（六）网络管理员应对访问控制策略进行登记并妥善保管（参见附件 1），依据经批准的访问控制策略进行设置和修改；

（七）只有网络管理员才能拥有网络设备的超级管理员权限，若在特殊情况下（如系统维修、升级等）需要第三方人员对网络设备进行操作时，须由网络管理员全程陪同并填写操作记录（具体要求参见《第三方人员安全管理规定》）。禁止网络管理员将网络设备用户账号及口令直接交给第三方人员使用。

第十四条　互联网接入区

（一）只开放指定端口对外提供业务应用服务，如 WEB 服务的 80 等；

（二）只开放运维管理服务端口，如 22、161、162 等。

第十五条　办公管理区

（一）通过 MAC 地址绑定或其它认证方式进行安全准入控制；

（二）只能根据指定端口访问相关的办公系统，如 OA 系统、电子邮件系统，不能直接访问生产系统区域应用；

（三）原则上禁止直接访问互联网，实现内外网分离。

第十六条　开发测试区

（一）非授权用户禁止访问该区域；

（二）所有其他区域用户针对本区域的业务访问和运维工作必须通过访问控制设备，不得直接访问该区域系统。

第十七条　系统运维区

（一）服务器区：仅允许运维人员、安全管理人员、协议第三方人员访问，该区域只针对指定用户开放相应的运维端口，其它服务端口禁止访问；

（二）终端区：运维终端只能根据指定端口访问相关运维平台或 IT 系统，该区域设备原则上禁止直接访问互联网。

第十八条　生产系统区

（一）互联接入、系统运维管理、办公管理三区域针对相关区域开放指定端口；区域用户针对本区域的业务访问必须通过核心交换设备进行数据交换，禁

止直接访问该区域系统；

（二）对主机、数据库和中间件系统维护工作，必须首先通过系统运维区的堡垒主机进入系统，不允许跳过堡垒主机的访问行为。

第五章　网络接入管理

第十九条　本地接入

（一）所有终端接入学校网络，必须填写《网络接入申请表》（参见附件2），由业务部门领导审核、网络与信息安全工作领导小组办公室审批后才可接入。

（二）新上线系统接入网络，严格按照《上海静安区四季在线培训学校上线管理流程》执行。

（三）临时第三方人员一般不允许接入生产网和办公网，如因维护确需接入网络，必须填写《临时性终端接入申请表》（参见附件 3），由业务部门领导审批后才可接入。

第二十条　远程接入

应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起部门核准，提请网络管理员开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。

第二十一条　无线接入

（一）未经网络与信息安全管理小组允许，各终端用户不得自行架设无线接入点（AP）接入学校内部网络；

（二）员工必须使用内部无线网络；

（三）学校内部无线网络应采用 WPA 的加密级别，登录前需进行身份认证，30 分钟内无访问将自动退出返回登录界面。

第六章　网络监控与检查

第二十二条　网络监控

（一）网络管理员负责网络设备的日常检查，监测通信线路、用户行为、网络流量、网络设备性能参数和网络的运行情况，对关键设备要做到每日检查，发现问题应迅速解决，维护工作应保留记录（参见附件 4）；

（三）网络管理员负责建立 24 小时网络监控系统、安全监控的内容包括但不限于：

1.违规行为：用户非法 、私接设备等行为；

2.攻击行为：端口扫描、强力攻击、木马后门攻击

（四）在监控过程中，如发现网络异常、严重影响业务的问题，要及时与信息安全管理员联系，并按照信息安全事件处理流程进行处置。

第二十三条　安全检查

（一）信息安全管理员应定期（不低于半年一次）对所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告；

（二）信息安全管理员经网络与信息安全工作领导小组领导批准后，方可对网络进行安全检测、扫描。安全检测、扫描结果属敏感信息，未经授权不得对外公开；

（三）未经网络与信息安全工作领导小组授权，任何外部机构与人员不得检测或扫描机构内部网络。

上海静安区四季在线培训学校

2021 年 11 月 1 日