第三方人员访问控制管理制度

一、总则

1.为有效防范外部人员访问带来的信息安全风险,加强和规范外来人员的信息安全管理，保证信息资源的安全，制定本制度。

2.本制度适用于我校所有第三方人员管理。

二、定义

1. 本制度所述的外部人员包括软件开发商、产品供应商、系统集成商、设备维护商、服务提供商以及外学校借调人员和挂职人员等外来人员，外部人员分为临时外部人员和非临时外部人员。

2. 临时外部人员指因业务洽谈、技术交流、提供短期和不频繁的技术支持服务而临时来访的外部人员。

3. 非临时外部人员指因从事合作开发、参与项目工程、提供技术支持、顾问服务及外学校借调人员和挂职人员等外来人员,是必须在我校长期办公的外部人员。

三、外部人员访问信息安全管理

1. 外部人员的访问方式包括现场访问和远程网络访问。

2.接待人是指我校受访部门派出的，负责接待外部人员的接口人。

3.临时外部人员访问重要信息资源所在物理区域（如机房、重要服务器或设备等），需获准后方可进入。

4.接待人必须全程陪同临时外部人员，告知有关安全管理规定，不应透露与外部工作无关的信息，不得任其自行走动和未经允许使用我校的计算机设备。

5.非临时外部人员，由接待部门向保卫处提出申请，保卫处依照有关制度审核办理工作手续。

6.原则上禁止外部人员携带的电脑接入我校网络，如因工作需要（如软件开发测试）接入我校网络，必须向信息科技服务中心申请，并使用信息科技服务中心的设备或经过信息科技服务中心检查认可的设备。

7.第三方人员如有需要访问信息系统时，需要依照如下几个阶段进行：

（1）访问申请阶段，接待人根据第三方人员实际需要提出某时间段内访问网络、主机等相关信息的申请；

（2）审批申请阶段，接待人所属部门管理者审批申请。审批后备案；

（3）注销访问阶段，第三方人员访问结束，接待人终止访问申请，并备案；

8.不允许外部人员进行远程网络访问。如确因维护需要远程访问，必须上报审批后方可进行。

9.外部人员开发测试环境只能连接开发网，且必需采用防火墙进行有效隔离，严禁接入生产网。确需在线测试的项目，应上报分管领导批准，采取必要的防护措施，选择适当的时间进行。

10.外部人员在机房内的所有操作，都必需说明该操作可能引起的安全风险，并由接待人确认后才能操作。接待人必须对外部人员的操作进行全程监控，记录外部人员的操作内容并存档备案。

11.必须定期评估外部人员带来的安全风险，至少每年评估一次。必须防范外部人员带来的以下安全风险：

（1）外部人员的物理访问带来的设备、资料盗窃；

（2）外部人员的误操作导致各种软硬件故障；

（3）外部人员的资料、信息外传导致泄密；

（4）外部人员对计算机系统的滥用和越权访问；

（5）外部人员给计算机系统、软件留下后门；

（6）外部人员对计算机系统的恶意攻击。

12.需要学校信息科技服务中心业务部门负责人审批确认。外来人员在访问过程中，学校接待人员应能够确定其访问的内容；在访问终止后，学校接待人应及时关闭或督促相关技术负责人员关闭临时访问的通路，并清除所有访问权限，并记录访问结束时间。

四、第三方安全要求

1.非临时外部人员必须签署安全保密协议后才能进场工作。禁止外部人员试图了解和查阅与工作无关的我校资料以及访问与工作无关的信息系统，外部人员如因业务需要查阅我校资料或访问我校信息系统，必须获得相关负责人批准并详细登记，并确认已签署有效的保密协议。

2.未经批准，禁止外部人员携带移动存储介质进入我校，移动存储介质必须在接待人的监控下使用。

3.未经相关负责人特别许可，外部人员不得在办公区域和机房内摄影、拍照。