安徽智慧校园网络安全风险评估报告编制编写

产品名称	安徽智慧校园网络安全风险评估报告编制编写
公司名称	河南世耀诚实业集团有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:文案定制 服务方向:专业领域
公司地址	南阳市卧龙区工业路华龙广告二楼
联系电话	13140513661 18338218580

产品详情

智慧校园的信息化建设构建依托于一系列的基础设施和应用系统，随着智慧校园建设的深入推进，智慧校园各构件内与构件间的风险就组成了整个体系的网络安全风险，这些网络安全风险将使智慧校园建设的成果时刻面临着巨大的不确定性。

尽早识别风险，排除网络安全隐患，是确保整个智慧校园建设成果安全、可靠的重要内容，要做好智慧校园建设、维护好智慧校园建设的成果，就必须对其中的安全风险进行识别，建立健全的安全风险控制体系。

01、智慧校园体系架构下构成网络安全风险的因素

智慧校园总体框架(GBT36342-2018)于 2018 年正式发布，在国家大力推进教育信息化的背景下，总体框架的发布无疑为高校智慧校园建设提供了有力的标准支持和指导。

智慧校园作为更高 级的教育信息化形态，充分利用物联网、云计算、移动互联网、GIS系统等信息技术手段，将物理空间与信息空间有机衔接，通过建设让师生在任何时间、任何地点，可以使用智慧校园中的任何智能终端设备获取智慧校园建设成果的资源和服务。

按《智慧校园总体框架》分层的要求来看，智慧校园主要包含:基础设施层、支撑 平台层、应用平台层、应用终端等。从这个分层来看，智慧校园相比于数字化校园面临着更复杂的网络安全挑战。

1、基础设施层

包括弱电管网基础设施，“ 云服务 ”基础设施和教学信息化基础设施，为上层信息化应用的建设提供基础支持;其中包括数据中心机房、网络机房、防火、强弱电源供应稳定;

该层是智慧校园平台的基石，为智慧校园各上层提供基础支持，为大数据分析提供数据库支持，同时也是智慧校园大数据产生的地方，包感知设备、通信网络设备以及数据库与服务器等，作为物理空间中比较真实的存在，该层中的设备、环境面临着物理空间中水、火
等自然、人为或设备折旧导致性能不足的威胁。

2、支撑平台层

包括学校中的各种基础业务系统(统一身份认证等)和数据交换共享、分析平台;数据交换稳定性、数据处理准确性、平台接口授权泄露风险。

该层为各类应用系统提供数据、业务驱动和支持，通过统一的数据交换、统一的数据接口以及数据处理能力(如数据挖掘、数据分析、数据可视化等)，提供了整个架构的“ 云计算 ”能力，相较于基础设施层，该层的内容为应用平台层的建设提供了抽象能力，这层主要面临的问题是平台、数据授权信息的泄露。

3、应用平台层

包含学校中为师生提供服务的应用系统，按教学服务、科研管理、管理服务分类，主要有移动校园、服务门户、一站式服务大厅、校园卡一卡通系统、教务系统、办公系统、人事管理系统等，该层是真实承载学校具体业务系统的平台，为师生提供泛在资源和服务。作为智慧校园中资源和服务的提供层，这里的信息系统安全面临着病毒入侵、网站挂马、DDoS 攻击等。

4、应用终端

应用终端定义了可以访问应用平台层的方式和工具，学校中的老师、学生以及管理人员，通过移动终端、电脑终端，自助服务设备等方式使用智慧校园的资源和服务，这里既有数字校园建设时期提供的自助服务终端，也有移动互联网时代用户自持的终端设备，不法分子及其利用老旧的终端设备上存在的漏洞或智能终端上执行恶意程序窃取用户的信息、发送诈骗信息等，从而造成较大的危害。

通过上面对智慧校园架构体系的分析，我们认识到在智慧校园体系架构下，随着传感设备、终端设备的接入越来越多、应用平台建设越来越丰富、应用终端越来越多样、碎片化，智慧校园面临着越来越多的网络安全风险和挑战，通过合理的风险评估，才能更好地应对风险，降低风险转化为实质性伤害的影响。

02、智慧校园建设中网络安全的风险评估

风险评估是指在风险事件发生前或发生后，我们对其造成影响和损失的可能性进行的一种量化评估工作。通过量化方式来评测某一事件或主体造成的影响或损失的可能程度。

在智慧校园框架下，合理利用风险评估的理论，做好风险评估工作是提高智慧校园网络安全的一项重要措施。通过对智慧校园的网络安全进行风险评估，能够有效地预警风险，从而加强风险的管理，从而根据不同的风险类型制定相应的管理策略。这里我们从风险是识别、风险评价、风险处置、风险控制四个方面对智慧校园框架网络安全进行研究，以便形成应对高校智慧校园网络安全事件和因素分析的方法。

1、风险识别

风险识别的内容基于智慧校园框架的四个层次进行，通过专家小组的方式获得到每一层次中的风险点。基于层次对风险进行识别，能够较为全面、清晰掌握风险的内容，便于对识别到的风险进行层次化管理。识别到的部分风险项见表 1。

2、风险评价

风险评价的常用方法有安全检查表、危险性预分析、危险和可操作性研究、矩阵法、严重潜在伤害评价等。本文采用格雷厄姆风险评价方法(LEC 法)作为定量风险评价方法，LEC评价法用三个指标来确定风险发生的危害性，即“ 风险项 ”发生的可能性L、风险项目发生的频繁程度E以及风险发生后可能造成的后果C，通过专家判断对风险项的三个指标进行赋值，带入以下公式求得风险的危险值 D。

$D = L \times E \times C$

L取值范围为 0.1-10，L的值越大表明风险发生的可能性越大;E取值范围
0.5-1，E取值越大说明风险发生的频繁程度越高; C取值范围
1-100，值越大表明风险发生后的后果越严重。LEC 三个指标的取值。

3、风险处置

L、E、C 赋值后，三者乘积就是代表风险发生的危险程度D值。对照表5可以获得相应风险项的危险程度。由表5可见，D值越大说明风险发生后造成的危害越大，我们将识别到的风险项按LEC方法计算D值并标注其风险等级，针对不同的风险等级采取相应的应对措施。

低级风险等级:1、2风险等级由“ 风险项 ”的责任部门做风险记录，并安排工作人员对其进行监视;

中、高 级风险:对于风险等级2以上的风险项，如果有对应的风险体系合同条款约束的，应按照条款的约束加强监控;没有响应风险管理合同体系的，应当指派专门的风险管理负责人制定风险管理计划，确保风险能够消除或减小到可以承受的程度。

在采取措施对风险进行降低后，应该评价剩余的风险可接受程度，并对剩余风险进行监控和评审。

4、风险监控

在进行风险识别后，对识别到的风险项指定风险监控责任人，当风险扩大到不可接受的程度时，须立即向单位负责人上报，及时控制。应对智慧校园各层次中的设备、系统配备状态监控和预警措施，一旦发现异常情况，立即发出预警告知风险责任人。同时，充分利用智慧校园的大数据技术优势，分析研判引起风险生的用户行为和日志，一旦触发风险预警规则，立即预警风险责任人。