重庆高校使用“渝快政”的失密泄密风险及防控对策研究

王庆贺

重庆大学党政办公室 重庆 401331

【摘　要】：“渝快政”是重庆市统筹统建的一体化、智能化、数字化政务工作平台，重庆高校接入“渝快政”后，在提升办公效率的同时，也带来了失密泄密风险，究其原因在于人员保密意识淡薄、技术防护体系不完善、保密管理制度缺失、数据分级分类及共享管控不严。针对风险隐患，探索实践从强化保密教育培训、完善技术防护体系、健全保密管理制度、明确数据分级分类管控、强化多方协同联动五个方面提出防控对策，以保障高校涉密信息安全，推动平台规范使用。

【关键词】：“渝快政”；失密泄密；防控对策

DOI:10.12417/2982-3803.26.02.021

在数字重庆建设进程中，“渝快政”作为全市一体化政务服务平台的核心载体，凭借“高效便捷、一网通办、协同联动”的优势，被广泛推广至各级党政机关、事业单位。重庆高校作为人才培养、科学研究、社会服务的重要阵地，也逐步接入“渝快政”，用于办理各类政务及校内关联事项，很大程度上提升了行政办公效率，降低了师生办事成本。

1 重庆高校“渝快政”涉密风险防控意义重大

高校作为涉密信息集中的重点领域，涵盖科研涉密数据、学生个人信息、教职工档案、涉密学术成果等核心内容，“渝快政”在高校的全面推广使用，使得失密泄密风险隐患日益突出。加之部分高校对“渝快政”使用的保密管理重视不足、防护措施不到位，已出现多起将涉密信息、内部文件违规上传至“渝快政”，造成失密泄密风险隐患，这不仅损害师生合法权益、影响高校正常教学科研秩序，还危及国家安全和公共利益。《中华人民共和国保守国家秘密法》《中华人民共和国数据安全法》等法律法规明确要求，各类单位需加强政务平台使用中的保密管理，防范涉密信息泄露。在此背景下，系统查摆重庆高校“渝快政”使用中存在的失密泄密风险，探索科学有效的防控对策，对于保障高校涉密信息安全、推动“渝快政”在高校规范有序推广、助力数字重庆建设高质量发展，具有重要的理论和现实意义[1]。

2 重庆高校“渝快政”使用中失密泄密隐患根源

2.1 人员保密意识淡薄，违规操作引发失密泄密

人员是“渝快政”使用中保密管理的核心主体，也是失密泄密风险的首要诱因。据调查了解，人员保密意识淡薄已成为高校“渝快政”使用中最为突出的风险隐患。一是高校部分教职工日常工作中责任意识淡薄，对涉密信息的识别能力欠缺，未能精准划分公开内容与涉密材料的边界。在实际操作时，易将科研工作中涉及的保密数据、尚未公开的学术研究成果以及教职工个人涉密档案等敏感信息，经“渝快政”违规进行上传、转发或共享，进而引发信息泄露的潜在风险。二是部分教职工存在侥幸心理，随意泄露个人“渝快政”账号密码，将账号交由他人代为操作；此外，部分高校未及时注销退休、离职等教职工“渝快政”账号权限，他们仍可登录平台传输、获取相关信息。以上均为“渝快政”失泄密的风险点。

2.2 技术防护体系不完善，平台适配存在安全漏洞

“渝快政”自身的技术防护水平，以及高校与平台的适配程度，直接决定了涉密信息的安全保障能力。当前，重庆高校在“渝快政”技术防护与平台适配方面存在诸多短板，形成了显著的技术漏洞。一是“渝快政”与高校内部系统适配不佳，数据交互过程中缺乏有效的加密防护措施。部分高校未建立完善的数据加密传输机制，数据在“渝快政”与校内系统之间传输时采用明文传输方式，极易被网络黑客拦截、窃取，进而导致重要敏感信息泄露。二是高校自身的技术防护设施较为落后，未对“渝快政”使用环境实施有效管控。部分高校办公电脑未安装专业的防火墙和病毒查杀工具，或者安装后未及时更新病毒库和系统补丁，容易被恶意程序入侵。三是“渝快政”自身的保密功能存在短板，部分模块缺乏权限分级管控、操作日志追溯等功能，一旦发生涉密信息泄露情况，无法及时定位泄露源头、追溯责任人员，也难以采取有效的补救措施，导致泄露损失进一步扩大。

2.3 保密管理制度不完善，监管考核机制缺失

当前，重庆部分高校保密管理制度不够完善、不够具体，难以适应“渝快政”推广使用后的保密管理需求。

作者简介：王庆贺，男，山东滕州人，重庆大学党政办公室文书科科长。

项目名称：重庆大学网络思政实践项目——大数据时代下学校“大安全”工作实践研究——以“渝快政”安全管理为例（项目号：CQUWLSZ202504）阶段性成果。

一是管理制度针对性不足，部分高校的保密管理制度为通用性条款，未结合“渝快政”的使用特点，制定具体的保密管理要求。对于“渝快政”账号管理、数据交互、平台操作等关键环节。未明确具体的操作规范和禁止性条款，导致在使用“渝快政”时无章可循。

二是责任分工不明确，未建立“专人负责、分级管控、层层落实”的保密责任体系，多数高校未明确专门的部门和人员负责“渝快政”使用中的保密管理工作，出现涉密信息泄露后，无法明确责任主体，难以进行追责问责。三是监管考核机制缺失，部分高校未建立常态化的保密监管机制，未对“渝快政”的使用情况、账号权限使用情况进行定期检查，对违规操作行为发现不及时、处置不到位；未将“渝快政”使用中的保密表现纳入教职工绩效考核、评优评先体系，对违规操作、造成涉密信息泄露的人员未采取严厉的处罚措施，难以形成有效的约束和震慑作用。

2.4 数据分级分类不清晰，共享边界管控不严格

在“渝快政”使用中，普遍存在数据分级分类不清晰、共享边界管控不严格的问题，进一步加剧了失密泄密风险。一是数据分级分类不科学。据了解，在对“渝快政”中所涉及的高校信息开展全面梳理时，发现未依据信息等级、敏感程度，对科研数据、学生资料、教职工档案等内容实施分级分类标注，致使无法精准识别内部信息，误将高等级内部信息当作普通信息上传、共享。二是数据共享边界管控不力。部分高校在“渝快政”上过度共享信息，未严格遵循“最小必要”原则，限定信息共享范围和使用权限，将原本仅需校内特定部门查看的信息，共享至“渝快政”的公共模块或非授权部门，导致敏感信息被无关人员获取。

3 重庆高校使用“渝快政”失密泄密风险的防控对策

3.1 强化保密教育培训，提升全员保密意识和操作能力

将保密教育培训纳入常态化工作，构建“分层分类、全面覆盖”的教育培训体系，切实提升教职工保密意识、涉密信息识别能力和规范操作水平。一是明确培训对象，分层开展培训。针对高校行政管理人员、科研人员、教职工等不同群体，制定差异化的培训内容。对行政管理人员，重点培训“渝快政”账号管理、数据交互保密要求等内容；对科研人员，重点培训科研涉密数据识别、涉密成果保密管理等内容；对普通教职工，重点培训“渝快政”使用中的基本保密要求、个人账号安全保护方法等内容。二是丰富培训形式，增强培训实效。采取“线上+线下”“理论+案例”相结合的方式，开展多样化的保密教育培训活动。线下邀请保密管理专家、“渝快政”运营技术人员，讲解保密法律法规等内容；线上搭建保密培训平台，上传培训课件、案例视频、测试题库等内容，方便教职工随时学习、自主测试。三是健全培训考核机制，强化培训效果。将保密培训纳入教职工岗前培训、在岗培训，明确培训学时和考核要求，培训结束后组织专项考核；定期组织保密知识抽查测试，形成“培训—考核—奖惩”的闭环管理，切实提升培训效果[2]。同时，及时注销离退休教职工、离职教职工“渝快政”账号权限，防范此类人员引发的失密泄密风险。

3.2 完善技术防护体系，筑牢涉密信息安全技术屏障

联动“渝快政”运营方、高校以及相关技术企业，构建“平台防护+校内管控+数据加密”的全方位技术防护体系，补齐技术短板，筑牢涉密信息安全屏障。一是推动“渝快政”与高校内部系统适配升级，强化数据交互加密防护。联合运营方和专业技术企业，对校内管理系统与“渝快政”的数据交互接口进行升级改造，实现数据传输全程加密，防止数据被拦截、窃取。二是加强高校校内技术防护设施建设，规范“渝快政”使用环境。为所有办公电脑安装专业防火墙和病毒查杀工具，安排专人负责定期更新病毒库、系统补丁，及时防范恶意程序入侵；针对“渝快政”身份验证漏洞，联合平台运营方，升级身份验证方式，采用“人脸识别+密码+动态验证码”的多重验证模式，增加账号破解难度，防范非法人员冒充授权人员登录平台。三是优化“渝快政”保密功能，强化操作追溯和风险预警。向“渝快政”运营方提出功能优化建议，推动平台完善权限分级管控功能，根据不同岗位职责、工作需求，赋予不同的账号权限；完善操作日志追溯功能，对“渝快政”上的所有操作行为进行详细记录，一旦出现涉密信息泄露，可快速定位泄露源头；增设失密泄密风险预警功能，对违规上传涉密信息、超权限操作、异常登录等行为进行实时预警。

3.3 健全保密管理制度，强化监管考核和责任追究

结合“渝快政”使用实际，构建“制度完善、责任明确、监管严格、追责有力”的保密管理体系。一是制定针对性的保密管理制度，明确操作规范。结合《中华人民共和国保守国家秘密法》等法律法规和政策要求，制定《高校“渝快政”使用保密管理办法》，明确“渝快政”账号管理、数据交互、平台操作、账号注销等关键环节的操作规范和禁止性条款。二是明确保密责任分工，构建分级管控体系。成立保密工作领导小组，统筹推进“渝快政”使用中的保密管理工作。明确学校保密管理部门为“渝快政”保密管理的牵头部门，负责制定管理制度、组织培训、开展监管以及处置失密泄密事件等工作[3]。三是强化监管考核，严肃责任追究。建立常态化的保密监管机制，由学校保密管理部门牵头，联合相关部门，对“渝快政”的使用情况、账号权限使用情况、技术防护设施运行情况等，开展定期检查和不定期抽查。对发现的违规操作行为，及时责令整改；建立失密泄密事件追责问责机制，一旦发生失密泄密事件，追究直接责任人员、相关领导和管理部门的责任，倒逼各部门和

个人严格遵守保密规定。

3.4 明确数据分级分类，严格管控数据共享边界

建立科学的信息分级分类体系，严格规范数据共享流程，明确共享边界，防范数据共享过程中的失密泄密风险。一是开展信息全面梳理，科学划分分级分类。组织专人对“渝快政”中涉及的高校信息进行全面梳理，对各类信息进行分级分类标注，明确各类信息的识别标准和管理要求，制作信息分级分类目录，发放给全体教职工，引导其规范上传、共享和使用信息。二是严格管控数据共享边界，坚持“最小必要”原则。在“渝快政”上共享信息时，严格遵循“最小必要、按需共享”的原则，限定信息共享范围和使用权限，仅向完成相关工作所必需的部门和人员共享信息，严禁过度共享、违规共享。对高度敏感信息，严禁在“渝快政”公共模块共享，确需向相关部门共享的，需履行严格的审批程序，经学校保密工作领导小组批准后，采用加密传输、专人送达等方式共享，同时明确共享信息的使用期限和使用范围，严禁共享对象擅自转发、泄露共享信息。

3.5 强化多方协同联动，构建全方位防控工作格局

联动重庆市政务服务管理部门、“渝快政”运营方、相关技术企业等多方力量，构建“政府引导、高校主体、平台支撑”的全方位防控工作格局，形成防控合力。一是强化政府引导监管，完善政策支持。相关管理部门加强对高校使用“渝快政”的引导与监管，制定高校“渝快政”使用保密管理指导意见，明确高校保密管理的责任与要求，定期组织高校开展保密检查与交流培训；加强对“渝快政”运营方的监管，督促平台运营方完善平台保密功能、强化技术防护、规范数据管理，切实履行平台保密责任。二是强化平台支撑作用，提升服务保障能力。“渝快政”运营方主动加强与高校的沟通协作，及时了解高校的保密管理需求，优化平台保密功能，为高校提供技术支持与服务；建立平台与高校的保密联动机制，及时向高校推送平台安全漏洞、异常操作等信息，协助高校排查和处置失密泄密风险。三是强化与技术企业合作，提升技术防控水平。加强与专业保密技术企业的合作，引入先进的保密技术与设备，对校内技术防护体系进行升级改造，开展保密技术检测与漏洞排查，及时发现并修复安全隐患；邀请技术企业为高校保密培训提供支持，讲解最新的保密技术与防范方法，提升教职工的技术防范能力。

参考文献：

[1] 雍黎.重庆这个政务工作平台实现统一协同办公.科技日报,2021-11-12(第 007 版).

[2] 孙昌亮.建设市级电子政务平台的模式研究[J].通信设计与应用,2019(11):65-66.

[3] 宋赢硕,施勇,薛质.电子政务平台下政府信息公开安全性研究[J].信息安全与通信保密,2014(04):72-76.