中国新高教集团数据保护政策

一、总则

（一）政策目的

为规范集团各信息系统的数据处理活动，保护用户个人信息安全和隐私权益，防范数据安全风险，依据相关法律法规，制定本政策。

（二）适用范围

本政策适用于集团及各院校信息系统在运营、维护、管理过程中涉及的所有数据处理活动。

（三）基本原则

1. 合法正当原则。数据处理应具有明确、合理的目的，采取对个人权益影响最小的方式。

2. 最小必要原则。仅收集必需的最少个人信息，不得过度收集。

3. 公开透明原则。向用户公开数据处理规则，主动接受监督。

4. 安全保障原则。采取必要措施，防止个人信息泄露、篡改、丢失。

二、数据存储安全

（一）存储环境要求

各信息系统服务器部署在符合国家标准的 IDC 机房或云服务环境。

1. 所有用户数据应存储在中国境内，不得向境外传输或存储。

2. 采用可靠的存储介质，定期检测设备健康状况。

（二）数据备份与恢复

1. 实施定期数据备份，备份数据应存储在独立存储设备并加密。

2. 重要数据应实施异地备份，防范区域性灾难风险。

三、数据共享与传输

（一）内部共享

各信息系统之间进行数据对接和共享时，应遵循以下要求:

1. 仅共享业务必需的字段，不得整库共享。

2. 数据传输应采用加密通道，使用 SSL/TLS 或 VPN 技术。

3. 记录数据共享日志，日志保留不少于六个月。

（二）第三方共享

与第三方共享数据时，应遵循以下要求:

1. 选择具有相应资质和安全能力的第三方服务商。

2. 签订业务合作协议时，明确第三方的数据保护义务和违约责任。

3. 定期审查第三方的数据保护措施。

（三）数据出境

原则上不向境外传输用户数据。如因特殊情况确需向境外提供数据，应当通过国家网信部门安全评估，向用户告知并取得同意。

四、技术安全措施

（一）访问控制

1. 实施统一身份认证机制，用户须经身份验证方可访问相应信息系统。

2. 实施基于角色的访问控制（RBAC），按照最小权限原则分配权限。

（二）网络安全

1. 部署防火墙，限制不必要的网络访问。实施网络隔离。

2. 部署入侵检测或入侵防御系统，定期进行漏洞扫描。

（三）应用安全

遵循安全开发生命周期（SDL），对用户输入进行严格验证和过滤，防止 SQL 注入、XSS、CSRF 等攻击。

（四）数据传输安全

1. 所有网络传输应使用 HTTPS 协议（TLS 1.2 或更高版本）。

2. 与第三方系统对接时，应使用加密通道。

（五）安全监控与审计

1. 记录用户登录、数据访问、数据修改、权限变更等关键操作。

2. 对异常行为进行实时监控和告警。审计日志应保护其完整性。

五、管理安全措施

（一）组织管理

1. 成立中国新高教集团数据安全管理小组，明确数据保护职责分工，定期审视安全管理措施的有效性。

2. 指定数据保护专员，负责数据保护的日常管理。

（二）人员管理

1. 所有可能接触用户数据的工作人员应签署《保密协议》。

2. 对关键岗位人员进行背景审查。员工离职时应立即收回所有系统权限。

（三）供应商管理

1. 对第三方服务商进行尽职调查，评估其数据保护能力。

2. 签署协议，明确服务商的数据保护义务。定期审查服务商的数据保护措施。

（四）风险评估

新功能上线前、重大变更前应进行专项评估，对识别出的风险制定应对措施。

（五）应急处理

发生数据安全事件时，应立即启动应急预案，采取补救控制措施，依法向主管部门报告，并及时通知受影响的用户。每年至少组织一次数据安全应急演练，并定期开展全员安全意识培训。

六、附则

（一）解释权

本政策由中国新高教集团数智中心负责解释。

（二）生效时间

本政策自发布之日起施行。

中国新高教集团有限公司

2026 年 3 月 10 日