网络和信息技术人员安全管理

（V2.1，2021年10月05日修订）

## 第一章 总则

1. 为了保障北京工商大学信息系统人员管理的安全性和规范性，提高工作人员在网络安全方面的业务水平、操作技能和协同能力，提升管理水平，特制定本规定。
2. 人员安全管理包括人员录用、岗位人选、人员转岗和离岗、人员考核、人员惩戒、人员教育和培训的安全管理。
3. 本制度适用于北京工商大学所有部门。

## 第二章 人员录用

1. 网络安全和信息化领导小组负责制定系统的网络安全运行维护人员录用规则。
2. 按照人事处管理流程对人员录用实施管理，并注意以下安全要求：

（一）录用部门应明确被录用人员的安全技能要求，在录用过程中依据技能要求进行考察，并对技能考核结果进行记录；

（二）规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查；

（三）对于可接触较多机密或更高级别信息资产或特殊工种的人员，需要签订保密协议。

## 第三章 人员转岗和离岗

1. 转岗和离岗人员，由所在部门及时通知人事处，只有具备经过人事处签字的保密承诺文档后才能办理转岗和离岗手续。
2. 人事处应通知网络安全管理部在24小时内终止离岗人员的所有访问权限，及时变更转岗人员的访问权限。
3. 对离岗人员，要理清离职交接单的各项交接内容，及时收回各种身份证件、钥匙、徽章以及机构为其提供的软硬件设备等，对设备上保留的数据进行安全处理，包括备份需要留存的数据以及删除不必要的数据。
4. 对关键岗位转岗和离岗人员需要向其重申调离后的保密义务，要求调离人员在保密承诺文档上签字，承诺相关保密义务后方可离开。
5. 应注意转岗人员的岗位变化，根据岗位需要，重新签署保密协议。

## 第四章 人员考核

1. 信息网络中心每年对所有网络安全运行维护岗位人员进行一次安全考核，并注意以下安全要求：

（一）应对所有人员进行安全意识考核；

（二）对涉及网络安全管理、检查和执行的岗位人员，应每年进行一次安全技能的考核，包括安全管理知识的掌握程度、所管理业务系统中安全产品的操作技能、所管理业务系统中使用的操作系统和应用软件的安全使用等；

（三）应将发生的安全事故、安全检查结果和安全审计结果纳入考核内容。

1. 安全考核结果应进行存档，以便查询，每次考核后，都应与上次考核进行对比。
2. 对于考核中发现有违反网络安全法规行为的人员或发现不适于承担网络安全关键岗位的人员要及时调离岗位。

## 第五章 人员惩戒

1. 人员违反安全策略和规定，依照其违规程度及影响，适度进行惩戒，情节严重的可与其解除劳动合同。
2. 如该安全违规涉及法律层面，则可追究该人员的刑事责任。

## 第六章 人员教育和培训

1. 新员工在正式上岗前，应进行网络安全方面的培训，明确岗位所要求遵守的网络安全制度、技术规范以及操作流程。
2. 针对信息系统的维护人员和管理人员应定期开展安全技术教育培训，明确如何安全使用有关系统，包括各业务系统、主机操作系统、以及计算机周边硬件设备等。
3. 应开展由供应商或厂家提供的专业安全技术培训，帮助相关安全管理人员和技术人员了解掌握正确、安全地安装、配置、维护系统。
4. 应在网络安全教育和培训后实行书面的考核，确认教育和培训的效果。对安全教育和培训的情况和结果进行记录并归档保存。
5. 日常的网络安全教育和培训应以内部培训为主，对于暂时没有条件实施内部培训的，可根据需要，邀请厂商、合作伙伴或者专业的培训机构实施培训。

## 第七章 外部人员管理

1. 外来人员包括软件开发商、产品供应商、系统集成商、设备维护商和服务提供商等外来人员。
2. 外来人员进入信息系统所在机房时，必须出示有效证件，并登记相关信息，包括来访人姓名、工作部门、接待人部门和姓名、进入时间等。
3. 外来人员访问重要区域（如机房、重要服务器或设备等），需出具相关证明，并在专人的陪同下方可进入。
4. 接待人必须全程陪同外来人员，告知有关安全管理规定，不应透露与外来工作无关的信息，不得任其自行走动和未经允许使用信息系统的服务器设备。
5. 原则上禁止外来人员携带的电脑接入信息系统网络。
6. 不允许外来人员进行远程网络访问。如确因维护需要远程访问，必须由运维部门批准后方可进行。
7. 外来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，接待人必须对外来人员的操作进行全程监控。
8. 外来人员维护网络、主机等设备的安全配置时必须符合相应的安全配置标准中相应规定。
9. 必须防范外来人员带来的以下安全风险：
10. 外来人员的物理访问带来的设备、资料盗窃；
11. 外来人员的误操作导致各种软硬件故障；
12. 外来人员的资料、信息外传导致泄密；
13. 外来人员对计算机系统的滥用和越权访问；
14. 外来人员给计算机系统、软件留下后门；
15. 外来人员对计算机系统的恶意攻击。
16. 未经批准，禁止外来人员私自将移动存储介质接入信息系统，移动存储介质必须在接待人的监控下使用。
17. 未经相关负责人特别许可，外来人员不得在办公区域和机房内摄影、拍照。

## 第八章 附则

1. 本规定的解释权归北京工商大学信息网络中心。
2. 本规定自发布之日起生效。