# 2 网络安全工作人员管理规定

## 第一章　总则

第一条　为进一步加强北京大学网络安全工作人员和第三方人员的网络安全管理工作，明确工作人员在录用前、工作期间以及调岗和离职各个过程中的网络安全管理要求及第三方人员的安全管理要求，特制定本规定。本规定为北京大学网络安全系列制度之一，在《北京大学网络安全管理办法》指导下执行。

第二条　本规定所称人员，是指与网络安全技术相关的人员。

第三条　本规定所称第三方人员，是指因合作开发、项目参与、技术支持或其他服务而涉及的软件开发商、产品供应商、系统集成商、设备维护商和安全服务商等非北京大学在职员工或聘用人员。

## 第二章　校级网络安全工作相关人员职责

第四条　计算中心是北京大学网络安全工作的技术支撑单位，设置校级安全管理员、校级审计管理员、校级网络管理员等岗位。其中校级安全管理员为专职。各岗位职责如下：

**(一) 校级安全管理员**

(1)　在网络安全和信息化委员会工作小组的指导下，负责组织落实学校网络安全工作的规划和建设；

(2)　协调各部门开展网络安全工作，协调督促落实网络安全责任制；

(3)　负责学校网络安全类规章制度的起草和修订，

(4)　负责网络安全事件的威胁预警、应急响应和处置工作；

(5) 负责开展网络安全培训、宣传工作。

**(二) 校级审计管理员**

(1) 负责对校级关键信息系统、网络运行设备、安全设备的审计报告进行审计和分析，标识并记录潜在风险。如发现违规行为及时向主管领导汇报；

(2) 负责反馈审计过程中发现的安全缺陷和问题，及时通知到人；

(3) 基于审计结果，定期编写校级审计报告。

**(三) 校级网络管理员**

(1) 根据校园网总体规划及安全规划，开展校园网网络架构设计及优化；

(2) 根据校园网和信息系统的业务需求及安全要求，负责网络硬件和软件的配置、部署、备份和升级；

(3) 具体负责校园网日常管理和运行维护，确保稳定运行，及时响应并解决各类网络问题；

第五条 校级网络安全岗位人员应签订《网络安全岗位保密承诺书》（见附件二），并严格履行承诺书中的要求。

## 第三章 各二级单位安全工作相关人员职责

第六条 网络安全工作须纳入各二级单位常规工作。

第七条 各二级单位应根据本单位网络和信息系统建设情况，设置如下网络安全相关岗位：安全管理员、信息系统负责人、信息系统管理员、信息系统审计员、网络管理员及机房管理员。具体各岗位职责可参考如下：

**(一) 安全管理员**

(1) 负责本单位网络安全技术工作，统筹协调本单位网络技术安全工作；

(2) 落实执行学校网络安全工作要求和规章制度，可根据本单位实际情况制定细化的安全管理制度；

(3) 协调本单位机房、网络、信息系统的安全建设和安全运维，负责本单位信息系统信息更新、统筹开展本单位信息系统等级保护工作；

(4) 协调本单位安全漏洞和网络安全事件的应急处置，及时反馈漏洞整改和事件处置情况；

(5) 主动配合学校相关部门组织的网络安全检查；

(6) 定期组织开展本单位师生员工网络安全意识教育和网络信息素养培训，并向网信办报备。

**(二) 信息系统负责人**

(1) 根据学校和本单位网络安全工作要求，组织开展所负责系统安全建设和运维；

(2) 负责本信息系统的安全等级保护定级、信息上报与更新；

(3) 负责组织落实系统立项阶段安全方案设计、建设阶段安全开发、上线阶段安全功能测试和运维阶段的安全管理方案、安全操作规程等方案和制度的制定；

(4) 对系统中发现的安全漏洞或风险进行及时修复和处置，确保信息系统安全运行。

**(三) 信息系统管理员**

(1) 根据学校和本单位网络安全工作要求，具体落实信息系统安全建设和运维；

(2) 具体负责信息系统安全策略配置、日志记录、数据备份、数据库的管理维护等相关工作；

(3) 落实信息系统的补丁升级、安全漏洞修复、安全风险处置和安全事件应急处理；

(4) 配合开展信息系统相关安全检查、安全审计等工作。

**(四) 信息系统审计员**

(1) 负责信息系统的安全审计工作，对安全管理方案和安全操作规程实施内部审核，对制度的执行情况进行监督检查，如发现违规行为及时向主管领导汇报；

(2) 检查信息系统操作系统、中间件、应用系统、数据库等部分的安全审计功能启用情况，确认以日志的形式记录安全管理方案中规定的操作过程和操作结果工作正常；

(3) 定期完成信息系统审计工作，记录日常审计过程，详细记录可疑事件发生的现象、时间，反馈给信息系统负责人、提出处理意见和建议；

(4) 负责信息系统审计报告的编写和审计资料归档整理。

**(五) 网络管理员**

(1) 根据校园网络总体规划及安全规划，负责本单位网络架构的设计与实施；

(2) 根据网络和信息系统业务需求及安全要求，执行网络配置、优化和扩展；

(3) 负责本单位网络日常监控、维护与故障排查，确保本单位网络的稳定性。

**(六) 机房管理员**

(1) 负责对本单位机房的日常管理，落实学校的机房安全管理制度；

(2) 严格控制并记录机房内人员及设备的进出；

(3) 负责机房的门禁、电源、空调等设备的日常管理以及防火、防雷、防盗等机房安全和日常维护工作；

(4) 定期对机房内的所有设备和设施，包括 UPS、消防系统、空调和照明，进行巡查和检测，记录其状态，并及时处理相关问题。

第八条 网络安全岗位工作人员应签订安全承诺书，并严格履行承诺书中的要求。具体包括：单位党政负责人作为网络安全工作第一责任人应与北京大学签订《北京大学二级单位网络安全承诺书》（见附件一）；参与三级（含）以上等保信息系统安全相关建设、运维、管理等工作的关键岗位人员，应与本单位签订《网络安全岗位承诺书》（见附件三）；信息系统负责人及信息系统管理员应向计算中心提交《信息系统安全承诺书》（见《信息系统建设安全管理规定》附件七）。

## 第四章 安全工作人员聘用管理

第九条 人员聘用管理是指学校各二级单位在聘用网络安全相关工作岗位员工前的安全管理要求，主要包括明确安全职责、审核人员信息和签署网络安全承诺书。

第十条 聘用单位应对被聘用人员的身份、安全背景、专业资格或资质等进行严格审查，并针对其技术技能进行实际考核。

第十一条　参与三级（含）以上等保信息系统安全相关建设、运维、管理等工作岗位员工均需签署《网络安全岗位承诺书》（见附件三）。

## 第五章　人员转岗和离岗

第十二条　各二级单位应及时终止离岗人员所涉及网络或信息系统的访问权限，变更转岗人员的访问权限。

第十三条　对离岗人员，各二级单位应完成离职交接工作，包括但不限于：收回岗位相关身份证件、钥匙、徽章以及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。根据身份变化，调整学校相关信息系统中的人员身份属性和访问权限。

第十四条　各二级单位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。

## 第六章　网络安全教育和培训

第十五条　学校统筹开展校级网络安全教育和培训，每年根据上级部门要求和工作需要，制定下一年度网络安全教育和培训计划，并落实相关经费。

第十六条　各二级单位应按网信办要求制定本单位网络安全年度培训计划，并及时向网信办报备。网络安全培训计划模板见附件四。

第十七条　新员工在正式上岗前，应由所在二级单位安全管理员组织开展网络安全培训，明确岗位所要求遵守的网络安全管理制度、技术规范以及操作流程。

第十八条　各单位网络安全相关人员应定期参加网络安全培训（每年至少一次），培训内容包括但不限于学校统筹安排的安全培训和校内外其他培训。其中，工作人员参加非学校统筹安排的网络安全培训应向网信办报备培训记录。

## 第七章　第三方人员管理

第十九条　第三方人员在现场操作或访问设备前，必须填写附件五《第三方人员访问申请表》，明确指出其访问的区域、设备或系统等详细信息。在得到本单位安全管理员或相关工作负责人的正式授权后，才能进行访问操作；

第二十条　第三方人员所在单位应与各二级单位签署第三方保密协议（参见附件六），承诺本单位工作人员对所接触的北京大学人员、设备、系统、文档、数据等承担协议约定的保密义务。

第二十一条 第三方人员现场操作或访问设备，安全管理员或相关工作负责人应安排人员全程陪同，应告知有关安全管理规定，不应透露与工作无关的信息，不得任其进行与工作无关的操作。接入重要网络设备和服务器应记录第三方人员操作，事后可追溯；

第二十二条 原则上不允许第三方人员进行远程运维。如因工作需要必须远程运维，须经安全管理员或相关工作负责人审批（参见附件五），在访问结束后应及时关闭访问通道。

第二十三条 应防范第三方人员带来的以下安全风险：

(一) 第三方人员物理访问所造成的设备、资料失窃；

(二) 第三方人员误操作所导致各种软硬件故障；

(三) 第三方人员资料、信息外传所导致的泄密；

(四) 第三方人员对计算机系统的滥用和越权访问；

(五) 第三方人员给计算机系统、软件留下后门。

第二十四条 未经安全管理员或相关工作负责人同意，禁止第三方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。

第二十五条 未经安全管理员或相关工作负责人同意，第三方人员不得在机房内拍照或录像。

第二十六条 如第三方人员违反本规定，根据违规的严重性，学校和相关单位有权采取包括但不限于警告、暂停合作、终止合作及法律追究等措施。

## 第八章 奖惩

第二十七条 学校定期对在网络安全工作中的先进集体和先进个人，给予表扬和奖励；对于存在违规行为的集体和个人，根据其违规的严重程度给予相应的纪律处分。

第二十八条 符合下列条件之一的集体和个人，进行通报表扬并给予奖励：

(一) 在网络安全检查、检测手段和方法方面有创新；

(二) 及时发现或者有效消除信息系统重大缺陷和安全隐患；

(三) 在紧急情况下保护信息系统安全免遭损失；

(四) 在网络安全工作的其他方面做出显著成绩。

第二十九条 若集体或个人存在以下情形，应根据违规的严重性，采取相应措施，包括但不限于批评教育、通报批评、行政处分等。对于严重违反学校规定的情况，应按学校的相关规章程序进行

处分。如其行为构成犯罪，应提交至有关法律机关处理并追究刑事责任：

(一) 入侵信息系统；

(二) 非法删除、修改、增加、干扰信息系统的功能、数据、程序，造成严重后果；

(三) 泄露本单位信息系统安全防护技术、方法、措施、安全产品性能、效果和应用范围，造成后果；

(四) 使用已经禁用或者不符合规定的信息系统、安全产品，造成严重安全隐患；

(五) 其他危害信息系统安全。

## 第九章 附则

第三十条 本规定是《北京大学网络安全管理办法》（试行）配套实施细则，从属于《北京大学网络安全管理办法》（试行）。

第三十一条 所有学校分支机构、附属单位和其他校区参照执行。

第三十二条 本规定的具体解释权归北京大学网络安全和信息化委员会办公室及北京大学计算中心。

第三十三条 本规定自发布之日起施行，并对所有相关方具有约束力。

**附件一 北京大学二级单位网络安全承诺书**

# 北京大学二级单位网络安全承诺书

本单位充分认识到网络安全的重要性，并郑重承诺按照以下条款行事。对所列事项负责，如有违反，由本单位承担由此带来的法律责任和行政后果。

一、本单位承诺严格遵守《中华人民共和国网络安全法》以及国家其他网络安全的有关法律、法规和行政规章制度。

二、本单位承诺执行《北京大学网络安全管理办法》（试行）和《北京大学突发事件应急处置总体预案》等学校网络安全有关工作的规章制度和工作要求。

三、本单位承诺完善本单位的网络安全管理办法，建立相应工作机制，明确相应工作队伍，健全安全责任制和相关规章制度、操作规程。

四、本单位承诺加强网络技术安全工作，提高信息系统安全防护能力，配合学校信息系统安全监测工作，对监测发现和通报的安全问题进行限时整改。

五、本单位承诺加强信息内容安全管理，完善相应制度，落实相应责任，防范网络舆情风险。

六、本单位承诺提升应急响应能力，制定本单位应急预案，组织开展应急演练。遭遇网络安全事件时，迅速进行报告与处理，并按照要求及时进行整改和处置。

七、本单位承诺规范本单位数据采集和使用，不采集超越职能范围的数据，保障数据安全。

八、本单位承诺加强网络安全教育，组织相关人员参加培训，提

高人员的安全意识和技术防护能力。

九、本单位承诺不利用网络危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

十、本承诺书自签署之日起生效。

单位负责人（签字）：

单位盖章：

日期：

**附件二 网络安全岗位保密承诺书（模板）**

# 网络安全岗位保密承诺书

在任职期间，本人会接触或掌握的工作秘密信息，现就有关保密事项承诺如下：

一、工作秘密信息是指工作中接触到的、不应为第三方所知悉的工作内容，一旦泄露会给工作带来网络安全风险、法律纠纷、经济损失或不良社会影响。

二、在工作中遵守相关规章制度和工作要求，维护于工作期间所知悉或持有的工作秘密信息。因工作需要，确需告知、交付或转移给第三方人员或予以公开，须征得单位同意。

三、工作期间，除征得单位同意，不故意从外部将带有已知漏洞的软件、系统、技术或者工具携入，并擅自使用。

四、离职时须根据工作要求将所持有的工作秘密信息移交指定人员，并办理相关手续，包括但不限于删除与工作秘密相关信息。承诺离职后不在任何场所使用或者披露工作秘密信息。

五、若违反以上约定内容，产生网络安全风险、法律纠纷、经济损失和不良的社会影响，承诺依法承担违约责任。

本承诺书由_____（单位名称）保存。

承诺人签字：

日期：

**附件三 网络安全岗位承诺书（二级单位模板）**

# （单位/信息系统名称）网络安全岗位责任和保密承诺书

为切实加强北京大学网络安全管理，落实安全责任制，全面提升学校网络与信息系统安全的技术保障能力，本人承诺履行如下岗位安全责任：

- **安全管理员**

1. 负责本单位网络安全技术工作，统筹协调本单位网络技术安全工作；

2. 落实执行学校网络安全工作要求和规章制度，可根据本单位实际情况制定细化的安全管理制度；

3. 协调本单位机房、网络、信息系统的安全建设和安全运维，负责本单位信息系统信息更新、统筹开展本单位信息系统等级保护工作；

4. 协调本单位安全漏洞和网络安全事件的应急处置，及时反馈漏洞整改和事件处置情况；

5. 负责配合学校相关部门组织的网络安全检查；

6. 组织开展本单位师生员工网络安全意识教育和网络信息素养培训，并向网信办报备。

- **信息系统负责人**

1. 根据学校和本单位网络安全工作要求，组织开展所负责系统安全建设和运维；

2. 负责本信息系统的安全等级保护定级、信息上报与更新；

3. 负责组织落实系统立项阶段安全方案设计、建设阶段安全开发、上线阶段安全功能测试和运维阶段的安全管理方案、安全操作规程等方案和制度的制定；

4. 负责系统的安全漏洞修复及安全风险处置，确保信息系统安全运行。

- **信息系统管理员**

1. 根据学校和本单位网络安全工作要求，具体落实信息系统安全建设和运维；

2. 具体负责信息系统安全策略配置、日志记录、数据备份、数据库的管理维护等相关工作；

3. 落实信息系统的补丁升级、安全漏洞修复、安全风险处置和安全事件应急处理；

4. 配合开展信息系统相关安全检查、安全审计等工作。

- **信息系统审计员**

1. 负责信息系统的安全审计工作，对安全管理方案和安全操作规程实施内部审核，对制度的执行情况进行监督检查，如发现违规行为及时向主管领导汇报；
2. 检查信息系统操作系统、中间件、应用系统、数据库等部分的安全审计功能启用情况，确认以日志的形式记录安全管理方案中规定的操作过程和操作结果工作正常；
3. 定期完成信息系统审计工作，记录日常审计过程，详细记录可疑事件发生的现象、时间，反馈给信息系统负责人、提出处理意见和建议；
4. 负责信息系统审计报告的编写和审计资料归档整理。

- **网络管理员**

1. 根据校园网络总体规划及安全规划，开展本单位网络建设；
2. 根据网络和信息系统业务需求及安全要求，开展本单位网络建设；
3. 负责本单位网络日常运行维护。

- **机房管理员**

1. 负责对本单位机房的日常管理，落实学校机房安全管理制度；
2. 负责机房人员、设备的进出管理；
3. 负责机房的门禁、电源、空调等设备的日常管理以及防火、防雷、防盗等机房安全和日常维护工作；
4. 负责对机房各类设备、UPS、消防设施、空调状态、照明等进行巡检记录，及时发现并解决问题。

在任职期间，本人会接触或掌握的工作秘密信息，现就有关保密事项承诺如下：

一、工作秘密信息是指工作中接触到的、不应为第三方所知悉的工作内容，一旦泄露会给工作带来网络安全风险、法律纠纷、经济损失或不良社会影响。

二、在工作中遵守相关规章制度和工作要求，维护于工作期间所知悉或持有的工作秘密信息。因工作需要，确需告知、交付或转移给第三方人员或予以公开，须征得单位同意。

三、工作期间，除征得单位同意，不故意从外部将带有已知漏洞的软件、系统、技术或者工具携入，并擅自使用。

四、离职时须根据工作要求将所持有的工作秘密信息移交指定人员，并办理相关手续，包括但不限于删除与工作秘密相关信息。承诺离职后不在任何场所使用或者披露工作秘密信息。

五、若违反以上约定内容，产生网络安全风险、法律纠纷、经济损失和不良的社会影响，承诺依法承担违约责任。

本承诺书由二级单位保存。相关工作人员变换工作岗位时失效。

承诺人签字：

| 岗位名称 | 姓名 | 签字 | 日期 |
| --- | --- | --- | --- |
| 安全管理员 | | | |
| 信息系统负责人 | | | |
| 信息系统管理员 | | | |
| 信息系统审计员 | | | |
| 网络管理员 | | | |
| 机房管理员 | | | |

## 附件四 网络安全培训计划（模板）

| 安全培训组织方 | | | | | |
|---|---|---|---|---|---|
| 序号 | 安全培训类别 | 培训对象 | 预算 | 培训方式 | 计划培训时间 |
| *1* | *北京大学安全管理制度培训（校内）* | | | | |
| *2* | *网络安全法（讲座）* | | | | |
| 3 | *安全技术认证类（外部）* | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## 附件五 第三方人员访问申请表

<table>
<tr><td>第三方人员</td><td></td><td>工作单位</td><td></td></tr>
<tr><td>联系方式</td><td></td><td>随行人员</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>是否远程运维</td><td colspan="3">□是 □否</td></tr>
<tr><td colspan="4">工作事由:<br>（如远程运维需说明原因）<br>申请日期:</td></tr>
<tr><td colspan="4">工作起止时间</td></tr>
<tr><td>经办人</td><td></td><td>审核人</td><td></td></tr>
<tr><td colspan="4">审核意见:</td></tr>
<tr><td colspan="4">访问情况记录</td></tr>
<tr><td colspan="4">实际开始时间、结束时间，完成的工作等结束时间:<br>经办人签字:<br>日期:</td></tr>
</table>

附件六 第三方保密协议（模板）

编号：_____

# XXX 项目

# 第三方保密协议（模板）

甲　　方：_____

乙　　方：_____

签订日期：_____年_____月_____日

乙方在与甲方合作期间，乙方员工已经（或将要）知悉甲方的工作秘密。为明确乙方的保密义务，本着诚信原则，经甲乙双方平等协商，自愿签订如下保守工作秘密协议：

乙方确认在签署本协议之前已经详细审阅了协议内容，并已理解协议各条款含义。_____（乙方单位法定代表人签字、盖章）

**第一条** 本协议所称的乙方为与甲方签订项目合同的承建单位，承建单位有义务约束其参建员工履行此保密协议，如乙方员工违反保密协议条款，所造成损失及后果由乙方承担。

**第二条** 本协议所称工作秘密是指不为公众所知悉，涉及个人隐私、国家敏感信息、与甲方工作有关的内部信息或技术信息、经营信息，以及其他双方约定或甲方内部规定保密的信息。本协议所称甲方的工作秘密不限于甲方单位本身的工作秘密，还包括因业务往来所知悉的合作单位的工作秘密，以及甲方依照法律规定（如在缔约过程中知悉的对方当事人的秘密）或有关协议的约定（如技术合同、合作协议等）对外承担保密义务的事项等。具体包括但不限于技术方案、项目设计、技术指标、计算机软件、数据库、实验结果、图纸、技术资料、涉及工作秘密的业务函电、投资计划、合作计划、客户资料、采购资料、定价政策、不公开的财务资料、业务策略、技术方法、经营方法、招投标中的标底及标书内容等信息。

**第三条** 除为履行本协议第一条所述的项目合同而使用和披露工作秘密之外，乙方无条件承担下列保守工作秘密义务：

1. 不刺探非本为履行项目合同目的所需要的工作秘密；

2. 不向不承担相应保密义务的任何第三人披露甲方的工作秘密；

3. 不得允许（出借、赠与、出租、转让等处分甲方工作秘密的行为皆属于“允许”）或协助不承担相应保密义务的任何第三人使用甲方的工作秘密；

4. 不利用所知悉的甲方的工作秘密从事有损甲方或甲方关联单位利益的经营、交易等行为；

5. 如发现工作秘密被泄露，应当采取有效措施防止泄密进一步扩大，并及时向甲方的相关部门报告；

6. 采取一定的技术手段和措施，并在内部建立完善的规章制度防止秘密泄露；其他本着诚实信用原则应当承担的保守工作秘密义务。

**第四条** 违反保密义务的法律责任：

1. 如乙方因前款所称的违约行为造成甲方损失的，应当承担损失赔偿责任；

2. 前款所述损失赔偿按照如下第__种方式计算：

①损失赔偿额为甲方因乙方的违约行为所受到的实际经济损失以及可举证之期待利益损失。

如果甲方的损失依照本条①款所述的计算方法难以计算的，损失赔偿额为不低于乙方因违约行为所获得的全部利润的合理数额，或者不低于甲方工作秘密许可使用费的合理数额。

甲方因调查和追究乙方的违约行为而支付的合理费用，以及因此导致劳动合同解除而给甲方造成的人员录用费、培训费等的损失也应当包含在损失赔偿额之内；

②损失赔偿额为项目合同总金额的 10%。

3. 因乙方的违约行为同时侵犯了甲方的合法权利（包括但不限于专

利、著作权等知识产权）的，甲方有权根据本协议要求乙方承担违约责任，同时根据国家有关法律、法规要求乙方承担侵权责任。

**第五条** 本协议自甲乙双方签署完毕之日起生效，保密期限为永久。

**第六条** 本协议约定的保守工作秘密的义务并不限于甲乙双方保持合作关系期间，乙方应谨慎保守所知悉的甲方工作秘密，除非：

1、乙方所知悉的甲方工作秘密已为公众所知悉。

2、甲方明确公示已对该工作秘密进行了解密，该信息已不再具有工作秘密的特性。

**第七条** 因履行本协议发生争议的，甲乙双方可自愿平等协商解决。协商不成的，应当向北京市海淀区有管辖权的人民法院提起民事诉讼。

**第八条** 本协议未尽事宜，按照国家法律或政府主管部门的有关规章、制度执行。

| | |
|---|---|
| 甲　　方：（盖章） | 乙　　方：（盖章） |
| 法定代表人或委托代理人：（签章） | 法定代表人或委托代理人：（签章） |
| 签订日期：　　年　　月　　日 | 签订日期：　　年　　月　　日 |