**16 安全事件处置管理规定**

**第一章 总则**

1. 为加强北京大学信息技术安全事件的管理，明确安全事件报告、处理和恢复的管理职责，保障网络与信息系统安全稳定运行，特制定本规定。
2. 本规定适用于北京大学所有单位。

**第二章 安全事件分类分级**

1. 技术安全事件是指由于自然、人为或软硬件本身缺陷及故障等原因，对网络基础环境和信息系统造成危害，进而对学校造成负面影响的事件。
2. 技术安全事件分为网络攻击事件、设备故障事件、灾害性事件等。
3. 按照事件的紧迫程度、形成的规模、行为方式和激烈程度、可能造成的危害和影响、可能蔓延发展的趋势等标准，技术安全事件可分为四级：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）、一般事件（Ⅳ级）。

**第三章 应急预案制定**

1. 北京大学网络安全和信息化委员会办公室组织制定校级网络安全总体应急预案。各二级单位应根据需要制定分项预案。
2. 机房、网络环境和信息系统负责人应制定分项应急预案，明确所负责设施、系统在发生服务中断、数据泄露、数据篡改等事件时，需采取的措施、应急联系人及启动的应急程序等。

**第四章 应急处置**

1. 安全事件发生后，单位安全管理员应协调信息系统管理员、信息系统负责人根据应急预案要求，及时开展事件处置和分析。
2. 信息系统负责人负责《信息技术安全事件情况报告》（见附件一）和《信息技术安全事件整改报告》的撰写（见附件二），并上报网信办。网信办根据事件级别和影响范围确定是否上报上级单位。
3. 各二级单位安全管理员应负责组织本单位安全应急预案培训，覆盖人员包括本单位信息系统负责人、信息系统管理员等系统相关人员。
4. 网信办和计算中心定期组织开展网络安全应急演练。

**第五章 附则**

1. 本规定是《北京大学网络安全管理办法》（试行）配套系列制度之一，从属于《北京大学网络安全管理办法》（试行）。
2. 其他校区参考本规定制定相应管理规定。
3. 本规定由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负责解释。
4. 本规定自发布之日起施行。

**附件一 《信息技术安全事件情况报告》**

信息技术安全事件情况报告

单位名称：（需加盖公章） 事发时间： 年 月 日 分

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮箱 |  |
| 事件分类 | □ 有害程序事件 □网络攻击事件  □ 信息破坏事件 □ 设备设施故障  □ 灾害事件 □其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| 事件分级 | □Ⅰ级 □Ⅱ级 □Ⅲ级 □Ⅳ级 | | |
| 事件概况 |  | | |
| 信息系统的基本情况（如涉及请填写） | 1. 系统名称： 2. 系统网址和IP地址： 3. 系统主管单位/部门： 4. 系统运维单位/部门： 5. 系统使用单位/部门： 6. 系统主要用途： 7. 是否定级□是 □否，所定级别：\_\_ \_\_ 8. 是否备案 □是 □否，备案号：\_\_\_\_\_\_\_\_\_\_ 9. 是否测评 □是 □否 10. 是否整改 □是 □否 | | |
| 事件发现与处置的简要经过 |  | | |
| 事件初步估计的危害和影响 |  | | |
| 事件原因的初步分析 |  | | |
| 已采取的应急措施 |  | | |
| 是否需要应急支援及需支援事项 |  | | |
| 安全负责人意见（签字） |  | | |
| 主要负责人意见（签字） |  | | |

**附件二 《信息技术安全事件整改报告》**

信息技术安全事件整改报告

单位名称：（需加盖公章） 报告时间： 年 月 日

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮件 |  |
| 事件分类 | □ 有害程序事件 □ 网络攻击事件  □ 信息破坏事件 □ 设备设施故障  □ 灾害事件 □其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| 事件分级 | □Ⅰ级 □Ⅱ级 □Ⅲ级 □Ⅳ级 | | |
| 事件概况 |  | | |
| 信息系统的基本情况（如涉及请填写） | 1.系统名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  2.系统网址和IP地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  3.系统主管单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  4.系统运维单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  5.系统使用单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  6.系统主要用途：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  7.是否定级 □是 □否，所定级别：\_\_\_\_\_  8.是否备案 □是 □否，备案号：\_\_\_\_\_\_\_\_\_\_  9.是否测评 □是 □否  10.是否整改 □是 □否 | | |
| 事件发生的最终判定原因（可加页附文字、图片以及其他文件） |  | | |
| 事件的影响与恢复情况 |  | | |
| 事件的安全整改措施 |  | | |
| 存在问题及建议 |  | | |
| 安全负责人意见（签字） |  | | |
| 主要负责人意见（签字） |  | | |