XXXX系统应急预案

1. **指导思想**

为提高应对XXXX系统在运行过程中出现的各种突发事件的应急处理能力，有效预防与最大限度的降低信息系统各类突发事件的危害与影响，保障信息系统安全稳定运行，根据《北京大学网络安全管理办法》《北京大学安全事件处置管理规定》及有关法律、法规的规定，结合工作实际，制定本应急预案。

1. **适用条件**

（一）适用范围

本预案适用于XXX系统及相关网络、安全设备，包括但不限于：XXX系统、托管于计算中心的系统服务器及网络设备等。

（二）事件定义

XXX系统发生的无法正常对外提供服务、系统数据安全遭受威胁，以及其他有可能影响XXX系统安全稳定运行的网络安全事件。

（三）事件分类

XXX系统网络安全事件是指因下列原因导致系统无法安全平稳运行的突发性情况，主要包括：

1. 信息系统故障：信息系统软硬件故障或配套设施故障；
2. 外部服务中断：第三方无法合作或提供服务等；
3. 人为破坏：黑客攻击，内容篡改，恐怖袭击等；
4. 灾害事件：火灾，雷击，地震，重大疫情等。

（三）突发事件级别

根据《北京大学网络与信息安全类突发事件应急预案》，结合XXX系统实际情况，按照系统中断运行时间和对业务影响的范围，将XXX系统突发事件级别划分为四级：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）。

一般事件（Ⅳ级）：XXX系统发生可能中断运行X小时以上X小时以内的故障；

较大事件（Ⅲ级）：XXX系统发生可能中断运行X小时以上X小时以内的故障，系统数据被拷贝、篡改、删除等情况；

重大事件（Ⅱ级）：XX系统发生可能中断运行X小时以上X小时以内的故障，系统数据被拷贝、篡改、删除等情况；

特别重大事件（Ⅰ级）：XX系统发生可能中断运行X小时以上的故障，系统数据被拷贝、篡改、删除等情况。

（四）组织结构

XXX单位设立XX系统应急领导小组（以下简称“领导小组”）负责领导XX信息系统应急管理工作。领导小组由XXX组成，XX担任组长，XXX担任副组长。由XXX负责具体的应急管理工作。

1. **突发事件应急处置流程**

（一）应急处置整体流程

1、启动阶段

当发生大范围的信息系统中断事件时，启动总体应急预案。由XXX办公室判断事件严重程度及所属级别。当事件达到特别重大事件（Ⅰ级）和重大事件（Ⅱ级）时，应上报领导小组，召集成立应急团队，发布通报通知，同时做好服务对象、用户的解释与疏导工作，启动相应系统的应急预案。根据《北京大学网络与信息安全类突发事件应急预案》中要求，按规定上报。

2、处置阶段

处置阶段，应详细记录关键的处置过程。遇到需要进行重大操作的决策点，由XXX办公室主任向领导小组进行汇报，由领导小组成员与学校网信办和计算中心协调沟通后，进行决策。

3、结束阶段

确认服务恢复正常后，发布故障解除、系统恢复正常通知，XXX办公室主任向领导小组进行汇报，领导小组同意后解散应急团队，由XXX办公室牵头编写应急处置报告。

（二）具体信息系统软硬件故障处置流程

1、网络、安全设备故障处置流程

XXX系统的网络环境和安全设备依托于学校计算中心，在发生网络、设备安全故障时，首先由技术人员对故障进行判断，若非自身网络、安全问题，上报领导小组，并第一时间联系计算中心网络组成员进行排查处理。若预计故障恢复时间超过半小时，发布通报通知。

2、主机故障处理流程

XXX系统实体机托管于计算中心机房，虚拟机由计算中心提供，当主机出现故障时，在排除非应用系统原因后，进行如下处理：当实体机出现故障时，上报领导小组，同时联系相关实体机维保厂商到场处理。当虚拟机出现故障时，联系计算中心主机组进行处理，并同时关注是否需要启动部署于其上信息系统的应急预案。

3、数据安全风险处理流程

当XXX系统数据出现被拷贝、篡改、删除等情况，首先上报领导小组，并联系计算中心隔断网络连接，组织技术人员对进行情况诊断，根据诊断结果，确定系统恢复时间，及是否将备份系统上线。

4、应用系统安全风险处理流程

当应用系统无法正常对外提供服务，首先上报领导小组，由技术人员对故障进行诊断，根据诊断结果，确定系统恢复时间，及是否将备份系统上线。若为网络攻击事件，第一时间联系计算中心隔断网络连接，保留第一现场，便于信息收集、证据分析和威胁溯源，进行后续排查处理。

1. **预案培训与演练**

（一）预案培训

由XXX办公室进行组织，至少每年一次进行应急预案集中培训。各专项预案的培训频次，由专项预案制定科室自行掌握。

（二）应急演练

1、XXX办公室于每年第二季度组织各信息系统制定应急演练计划。

2、XXX办公室于5月发布本年度应急演练计划，组织根据具体的时间计划组织执行演练。

3、XXX办公室对应急演练过程做详细记录，包括操作时间、操作内容、操作人员、操作结果和异常情况等。

4、演练结束后，需撰写演练总结报告。

1. **附录**

（一）应急角色与职责列表

1、应急领导小组

由XXX组成，XXX担任组长，XXX担任副组长。负责领导和决策突发事件的应急处置。

2、XXX办公室

统一负责调度、执行应急管理具体工作。

3、各科室

配合XXX办公室进行应急管理工作。

4、计算中心

配合XXX办公室进行应急处置，提供技术指导。

（二）应急联络表

1、校内人员应急联络表

|  |  |  |
| --- | --- | --- |
| 姓名 | 所属单位 | 联系方式 |
|  |  |  |

2、外包厂商应急联络表

|  |  |  |
| --- | --- | --- |
| 姓名 | 所属单位 | 联系方式 |
|  |  |  |