北京工商大学网络信息安全应急预案

（2021年11月修订）

**第一部分 总则**

**第一条** 为保障北京工商大学网络及信息安全，正确、迅速和有效地处置可能发生的网络通讯故障，提升学校应对网络信息安全事件能力，预防和减少网络信息安全事件造成的损失和危害，特制订本预案。

**第二条** 根据《中华人民共和国计算机信息系统安全保护条例》、《信息安全等级保护管理办法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律法规和文件精神，制定本预案。

**第三条** 本预案是北京工商大学网络信息安全事件的专项预案，适用于北京工商大学发生或可能发生网络信息安全事件情况下的应急处置工作。凡北京工商大学校内的互联网接入单位和互联网信息服务单位和个人必须遵守执行。

**第四条** 参照《国家网络信息安全事件应急预案》相关规定，本预案所指网络信息安全事件是指由于人为破坏、软硬件缺陷或故障、自然灾害等，对校园网络和信息系统（网站）或系统中的数据造成危害，对学校甚至社会造成负面影响的事件。

我校根据网络信息安全事件的可控性、严重程度和影响范围，将其定为四级：I级(特别重大)、Ⅱ级(重大)、Ⅲ级(较大)和Ⅳ级(一般)。相关事件对于国家有关法律法规有明确规定的，按国家有关规定执行。

I级(特别重大)——重要的网络信息安全系统发生大规模信息网络瘫痪，事态发展超出控制能力，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发公共事件；境外敌对势力、敌对组织利用电子邮件、短信息服务等渠道，有组织、大范围对我校传播反动有害信息等情况。一旦出现I级事件，由学校主管领导立即通报市教工委、教委及上级安全主管单位，并部署有关单位处置事件，消除影响，避免损失。

Ⅱ级(重大)——学校重点网站、重要信息网络受到黑客持续攻击或非法入侵，以及敌对势力、敌对组织利用网络技术手段传播反动信息，进行网上破坏活动等；重要的信息与网络安全系统瘫痪，对国家安全、社会秩序、经济建设和公共利益造成严重损害。出现Ⅱ级事件，需要立即处置，消除影响，并在10分钟之内口头上报市教工委、教委及上级安全主管单位。

Ⅲ级(较大)——部分区域的信息与网络安全系统瘫痪，对学校管理工作、信息系统运行造成一定损害，但不需要跨部门处置的突发安全事件。出现Ⅲ级事件，由负责单位进行处理，消除影响，减少损失，并将情况和处理结果报送学校主管领导。

Ⅳ级(一般)——信息与网络安全系统终端受到一定程度的损坏和对部分应用系统构成短时间影响，但不危害国家安全、社会秩序、经济建设和公共利益的突发安全事件。Ⅳ级事件由具体负责单位有关人员进行处理，消除影响，并记录事件相关信息情况进行备案。

**第二部分 组织机构**

**第五条**  应急领导机构为北京工商大学网络安全与信息化领导小组。在应急工作中主要职责：统筹指导学校网络信息安全应急体系建设；完善各项应急预案的制定和各项措施的落实；决定网络信息安全事件应急响应启动；指挥学校网络信息安全事件应急响应工作。

**第六条** 领导小组办公室设在信息网络中心，办公室在接到网络信息安全事件发生或可能发生的信息后，应加强与有关方面的联系，掌握最新发展动态，并做好启动本预案的各项准备工作。还要根据网络信息安全事件发展态势，视情况决定赶赴现场指导，组织派遣应急支援力量。

**第七条** 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，网络信息系统负责部门的领导班子主要负责人是网络信息安全工作第一责任人。

**第三部分 应急响应流程**

**第八条** 先期处置

当发生网络信息安全事件时，网络信息系统责任部门应做好先期应急处置工作，立即采取措施控制事态，做好处置记录，同时向领导小组办公室报告。先期处置工作包括且不限于：

1、控制事态发展，防控蔓延。事件发现人员应视情况及时采取断网（拔网线、一键关机）、关闭服务、阻断IP等技术措施及时控制事态发展，最大限度地降低事件危害。

2、及时报告信息。在先期处置的同时要及时进行汇报，由领导小组启动应急预案。

3、做好事件发生、发展、处置的记录和证据留存。在先期处置过程中应尽量保留安全日志信息、设备告警信息、路由配置信息、数据包信息等相关证据，采取手工记录、截屏、文件备份和影像设备记录等各种手段，对事件发生、发展、处置的过程、步骤、结果进行详细记录，尽可能保存原始证据，为事件处置、调查、处理提供客观证据。

**第九条** 应急指挥

本预案启动后，要抓紧收集相关信息，掌握现场处置工作状态，分析事件发展态势，研究提出处置方案，统一指挥网络与信息应急处置工作。需要成立现场指挥部的，应立即在现场开设指挥部，现场指挥部要根据事件性质迅速组建各类应急工作组，开展应急处置工作。

**第十条** 信息处理

应对事件进行动态监测、评估，及时将事件的性质、危害程度和损失情况及处置工作等情况，及时上报，不得隐瞒、缓报、谎报。要组织专家和有关人员研判各类信息，研究提出对策措施，完善应急处置计划方案。

**第十一条** 应急结束

网络信息安全事件经应急处置后，得到有效控制，事态下降到一定程度或基本得到解决，分析各监测统计数据后，确定是否结束应急。

**第四部分 保障措施**

**第十二条** 网络信息系统在建设系统时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在网络信息安全事件发生时，由北京工商大学网络安全与信息化领导小组负责统一调用。

**第十三条** 学校每年提供网络信息安全工作专项经费，用于网络信息安全应急技术支撑、宣传培训、预案演练等工作开展。

**第五部分 监督管理**

**第十四条** 要充分利用各种传播媒介及有效的形式，加强网络信息安全事件应急和处置的有关法律法规和政策的宣传，提高公众防范意识和应急处置能力。指定专人负责安全技术工作。并将网络信息安全事件的应急管理、工作流程等列为培训内容，增强应急处置工作的组织能力。

**第十五条** 定期开展应急预案演练，通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

**第十六条** 北京工商大学网络安全与信息化领导小组办公室要认真贯彻落实预案的各项要求与任务，建立监督检查和奖惩机制。北京工商大学网络安全与信息化领导小组办公室将不定期对各项制度、计划、方案、人员、物资等进行检查，作为奖惩依据。

**第六部分 附则**

**第十七条** 预案将根据实际情况适时修订，修订工作由学校网络安全和信息化领导小组办公室组织落实。

**第十八条** 本预案由学校网络安全和信息化领导小组负责解释。

**第十九条** 本预案自发布之日起实施。