北京工商大学网络安全事件应急预案

（2022年01月修订）

**第一部分 总则**

1. 根据国家及北京市教委等关于网络和信息安全工作的总体要求，健全完善北京工商大学网络安全事件应急工作机制，规范网络安全事件处置工作流程，提高网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校信息系统（网络）安全稳定，特制订本预案。
2. 根据《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，《国家突发公共事件总体应急预案》、《突发事件应急预案管理办法》、《国家网络安全事件应急预案》、《关于加强教育行业网络与信息安全工作的指导意见》、《信息安全技术信息安全事件分类分级指南》（GB／Z20986—2007）、《教育系统网络安全事件应急预案》、《教育部办公厅关于印发<信息技术安全事件报告与处置流程（试行）>的通知》、《北京市网络与信息安全事件应急预案》、《北京市教育系统网络安全事件应急预案》等相关文件，制定本预案。
3. 本预案适用于北京工商大学及学校各二级单位。按照《国家网络安全事件应急预案》规定，本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件和其他事件。信息内容安全事件的应对，参照有关规定和办法。
4. 参照《国家网络安全事件应急预案》事件分级规定，根据北京工商大学信息系统(网络)实际情况，可能造成的危害，可能发展蔓延的趋势等，北京工商大学网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

特别重大网络安全事件（I级）——关键信息基础设施或统一运行的核心业务信息系统（网站）遭受特别严重损失，造成系统大面积瘫痪，丧失业务处理能力；网络病毒在全校信息系统（网站）范围内大面积爆发；学校50％（含）以上的二级单位网站及重要业务系统遭到破坏，或重要敏感信息、关键数据丢失或被窃取、篡改等；其他对学校网络信息系统安全造成特别严重影响和威胁的网络安全事件。

重大网络安全事件（Ⅱ级）——关键信息基础设施或核心业务信息系统（网站）遭受严重系统损失或破坏，业务处理能力受到重大影响；网络病毒在学校1 / 3（含）以上1/2以下的二级单位范围内爆发。学校有1 / 3（含）以上1/2以下的二级单位门户网站及重要业务系统遭到破坏，或重要敏感信息、关键数据丢失或被窃取、篡改等。

较大网络安全事件(Ⅲ级)——学校有1 / 3以下二级单位的门户网站及重要业务信息系统遭到破坏，业务处理能力受到影响；重要业务信息系统（网站）信息、数据丢失或被窃取、篡改等；网络病毒在学校1 / 3以下的二级单位范围内传播。

一般网络安全事件(Ⅳ级）——学校信息系统（网络）遭到破坏，在二级单位内造成一定影响的，为一般网络安全事件。

1. 工作原则

（一）统一指挥、密切协同。由北京工商大学网络安全与信息化领导小组（以下简称“领导小组”）统筹协调各二级单位网络安全应急指挥工作，建立与北京市教委等上级部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告、培训和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。北京工商大学网络安全与信息化领导小组办公室设在信息网络中心（以下简称 “领导小组办公室”）。

（二）分级管理、强化责任。各二级单位在学校领导小组领导下，负责本单位网络安全应急工作。按照“谁主管谁负责、谁运维谁负责”的原则，各二级党组织对本单位网络安全工作负主体责任。二级单位主要负责人是网络安全工作第一责任人。

（三）预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

**第二部分 组织机构与职责**

1. 北京工商大学网络安全与信息化领导小组在应急工作中的主要职责：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；统筹协调学校网络安全事件应急处置，指导各二级单位网络安全事件应急处置（发生特别重大网络安全事件时，由上级单位统一组织应急处置工作，具体要求以上级单位部署为准）。
2. 在领导小组的领导下，学校分管领导负责统筹网络安全应急工作，领导小组办公室负责网络安全应急管理事务性工作，对接上级网络安全职能单位，向领导小组报告网络安全事件情况，提出网络安全事件应对处置措施建议，组织相关部门应对处置网络安全事件。统筹组织网络安全监测工作，指导网络安全支撑单位做好应急处置的技术保障工作。
3. 各二级单位的领导班子主要负责人是网络信息安全工作第一责任人，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，参照本预案制定应急预案，明确各二级单位网络安全责任，全面落实各项工作。
4. 各二级单位应明确规范与网络信息系统建设方、服务方合作流程，应在签订的协议中明确各方责任，确保当网络与信息安全事件发生时能及时有效地响应和处置。

**第三部分 监测与预警**

1. 建立北京工商大学网络安全事件预警制度。按照紧急程度、发展态势和可能造成的危害程度，北京工商大学网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生的北京工商大学特别重大、重大、较大和一般网络安全事件。
2. 领导小组办公室通过多种渠道监测、发现已经发生的系统（网站）安全事件，将掌握的情况立即通知相关二级单位。

各二级单位应对网络和信息系统（网站）的运行状况进行密切监测，一旦发生网络安全事件，应当立即通过电话方式向领导小组办公室报告，不得迟报、谎报、瞒报、漏报。

1. 领导小组办公室组织对学校网络安全威胁进行监测，建立多方协作的信息共享机制，通过多种途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息，实现安全威胁信息的收集、校验、发布、跟踪。

各二级单位加强对本单位信息系统（网站）的网络安全威胁监测，对发生的威胁及时进行处置和上报。

1. 橙色以上（含红色）预警由上级单位发布。

北京工商大学可根据监测研判情况，发布北京工商大学的黄色以下（含黄色）预警。对发生网络安全事件的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时通知相关管理员；认为可能发生重大以上（含重大）网络安全事件的信息，应立即向市教委领导小组办公室报告。

预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施、时限要求和发布机关等。

1. 红色预警响应

（1）上级单位发布红色预警时，领导小组办公室组织预警响应工作，联系有关单位、专业机构和专家，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调调度各方资源，做好各项准备，重要情况报网络安全分管领导。

（2）组织跟踪和分析研判，密切关注事态发展，做好监测分析和信息搜集工作；开展应急处置或准备、风险评估；密切关注舆情动态，加强教育引导，采取有效措施管控风险。

（3）相关单位实行24小时值守，工作人员保持通信联络畅通。

（4）领导小组办公室做好与专业机构沟通协调的准备工作；安全技术支撑单位进入待命状态，研究制定应对方案，检查设备、软件工具等，确保处于良好状态。

1. 橙色预警响应

（1）上级单位发布橙色预警时，领导小组办公室启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（2）有关单位及时将事态发展情况报领导小组办公室，领导小组办公室密切关注事态发展，有关重大事项及时报告分管领导，并通报有关单位。

（3）相关应急技术支撑队伍保持联络畅通，检查应急设备、软件工具等，确保处于良好状态。

1. 黄色、蓝色预警响应

各二级单位根据预案，组织做好预警响应工作。

1. 预警发布单位根据实际情况，确定是否解除预警，及时发布预警解除信息。

**第四部分 应急处置**

1. 网络安全事件发生后，领导小组办公室应立即启动应急预案，立即组织应急队伍和工作人员根据不同的事件类型和事件原因，采取科学有效的应急处置措施，尽最大努力将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。

经分析研判，初判为特别重大、重大网络安全事件的，应按照“先口头、后书面”的原则报告领导小组办公室，口头报告应在事件发生15分钟内，书面报告应在事件发生2 小时内；对于人为破坏活动，应同时报当地网信单位和公安机关。

领导小组办公室组织研判，认定为比较重大（含）以上网络安全事件的，报分管领导和上级网络安全职能单位。

1. 网络安全事件应急响应分为I级、Ⅱ级、Ⅲ级、Ⅳ级等四级，分别对应北京工商大学特别重大、重大、较大和一般网络安全事件。
2. 发生特别重大网络安全事件，由上级单位研判确定并提出启动I级响应的建议，由上级单位统一组织应急处置工作，具体要求以上级单位部署为准。
3. 发生重大网络安全事件，由上级单位研判确定并提出启动Ⅱ级响应的建议，具体要求以上级单位部署为准。
4. 发生较大网络安全事件，由领导小组办公室向网络安全分管领导提出启动Ⅲ级响应的建议，经领导小屋批准后，组织实施。

（一）启动指挥体系

（1）领导小组进入应急状态，履行应急处置工作统一领导、指挥、协调的职责，并保持24小时联络畅通。

（2）领导小组办公室负责组织相关单位进行应对，在领导小组的统一领导、指挥下组织人员开展应急处置或支援保障工作，启动24小时值守，工作人员保持24小时联络畅通。

（二）掌握事件动态

（1）跟踪事态发展。领导小组办公室与事发二级单位保持联系，及时填写《北京工商大学网络安全事件情况报告》，将事态发展变化情况和处置进展情况上报领导小组办公室。

（2）检查影响范围。领导小组办公室立即全面了解全校的网络和信息系统是否受到事件的波及或影响，并将有关情况及时报网络安全分管领导。

（3）及时通报情况。领导小组办公室负责整理上述情况，重大事项立即报网络安全分管领导，同时报上级主管单位，并通报有关单位。

（三） 决策部署

领导小组办公室组织有关单位、专家组、应急技术支撑队伍等方面及时研究对策意见，对处置工作进行决策部署。

（四）处置实施

（1）控制事态防止蔓延。采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

（2）消除隐患恢复系统。根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患。对业务连续性要求高的受破坏网络与信息系统要及时组织恢复。

（3）调查取证。有关单位在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合网信单位和公安机关开展调查取证工作。

（4）信息发布。领导小组应做好网络安全突发事件的应急舆论引导，协调有关单位开展舆论引导和新闻发布工作。未经领导小组办公室批准，不得擅自发布相关信息。

（5）协调上级单位支持。处置中需要技术及工作支持的，由领导小组办公室根据实际，报请网络安全分管领导批准后，商上级单位予以支持。

（6）次生事件处置。对于引发或可能引发其他安全事件的，领导小组办公室应及时按程序上报。

1. 发生一般网络安全事件，对应Ⅳ级响应。北京工商大学按相关预案进行应急响应和处置，领导小组办公室根据情况协调有关单位应对。
2. 根据上级单位指示，决定I级、Ⅱ级响应结束及后续工作安排。领导小组办公室根据实际决定Ⅲ级响应的结束，及时上报上级单位。完成应急处置后，领导小组办公室自行解除Ⅳ级响应状态。

**第五部分 调查与评估**

1. 特别重大网络安全事件和重大网络安全事件由上级单位组织有关单位开展调查处理和总结评估工作。

较大网络安全事件由上级单位或领导小组办公室组织有关单位开展调查处理和总结评估工作，并将调查评估结果汇总报告网络安全分管领导及上级单位。

一般网络安全事件根据事件涉及范围，由领导小组办公室自行组织开展调查处理和总结评估工作。

网络安全事件总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。网络安全事件的调查处理和总结评估工作应在应急响应结束后5 天内完成。

**第六部分 预防工作**

1. 领导小组办公室统筹指导北京工商大学网络安全预防工作。
2. 各二级单位应做好网络安全事件日常预防工作，根据本预案制定完善相关的专项应急预案和配套的管理制度，建立完善的应急管理体制。按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统的安全保障能力。
3. 各二级单位应加强网络安全监测预警和通报，及时发现并处置安全威胁。各二级单位应全面掌握单位信息系统（网站）情况，建立本单位的网络安全监测预警和通报机制，并指导、监督系统负责人及时修复信息系统（网站）安全威胁，全面排查安全隐患，提高发现和应对网络安全事件的能力。
4. 领导小组办公室每年组织针对重大网络安全事件的跨部门应急演练，检验和完善预案，提高实战能力
5. 各单位应将网络安全教育作为学校安全教育的重要内容，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。同时，充分利用网络安全周等各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提高在校师生的网络安全意识。
6. 学校定期组织网络安全培训，将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

**第七部分 工作保障**

1. 各单位应落实网络安全应急工作责任制，将网络安全应急工作作为重点工作予以部署。按照“谁主管谁负责"的原则，把网络安全应急工作责任落实到具体岗位和个人，建立健全应急工作机制。
2. 学校明确网络安全技术支撑单位，加强信息系统（网络）安全应急技术支撑队伍建设和经费物资保障，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。
3. 学校加强信息系统（网站）监测通报，建立网络安全态势感知体系，做到早发现、早预警、早响应，提高应急响应、应急处置能力。
4. 加强与网络安全职能单位、网络安全专业机构、行业学会等单位的合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制。
5. 各单位为网络安全应急工作提供必要的经费保障，利用现有政策和资金渠道，支持学校网络安全应急技术支撑队伍建设、专家队伍建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。
6. 北京工商大学可对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予鼓励；对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

**第八部分 附则**

1. 本预案根据实际情况适时修订。修订工作由领导小组办公室组织。
2. 本预案由北京工商大学网络安全与信息化领导小组办公室负责解释。
3. 本预案自印发之日起实施。