# 中共天津科技大学委员会文件

津科大党发〔2023〕63号

## 关于印发《天津科技大学网络安全事件应急处置预案（修订）》的通知

各基层党委（党总支）、各单位、机关各部门:

《天津科技大学网络安全事件应急处置预案（修订）》已经2023年10月12日学校党委常委会第32次会议研究通过，现予印发，请遵照执行。

附件：天津科技大学网络安全事件应急处置预案（修订）

中国共产党天津科技大学委员会

2023年10月22日

附件：

# 天津科技大学网络安全事件应急处置预案（修订）

为建立健全天津科技大学校园网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护在校师生利益，维护校园网络安全与稳定，根据《中华人民共和国网络安全法》、《国家网络安全事件应急预案》、教育部《教育系统网络安全事件应急预案》等相关法律法规，结合学校实际情况，制定本预案。

## 第一章 总则

**第一条** 网络安全事件定义。本预案所指网络安全事件是指除信息内容安全事件以外的由于人为原因、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，对学校造成负面影响的事件。可分为有害程序事件、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。

**第二条** 适用范围。本预案适用于在天津科技大学发生的网络安全事件的应对工作。有关信息内容安全事件的应对，另行制定专项预案。

**第三条** 安全事件等级划分。参照《国家网络安全事件应急预案》相关规定，根据事件的可控性、严重程度和影响范围，共

分为四级：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级）

（一）特别重大网络安全事件（Ⅰ级）

校内重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。重要敏感信息和关键数据丢失或被窃取、篡改、假冒，事态发展超出学校的控制范围。对国家安全、社会秩序、经济建设和公共利益构成特别严重威胁和影响的网络安全事件。

（二）重大网络安全事件（Ⅱ级）

校内重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。重要敏感信息和关键数据丢失或被窃取、篡改、假冒，事态发展超出网络安全和信息化办公室的处理能力。对国家安全、社会秩序、经济建设和公共利益构成严重威胁和影响的网络安全事件。

（三）较大网络安全事件（Ⅲ级）

校内重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。重要敏感信息和关键数据丢失或被窃取、篡改、假冒。对国家安全、社会秩序、经济建设和公众利益构成较严重威胁和影响的网络安全事件。

（四）一般网络安全事件（Ⅳ级）

除上述情况外，校内网络或信息系统遭受一定损失，系统效率、业务处理能力受到一定影响。不对国家安全、社会秩序、经

济建设和公共利益造成影响的网络安全事件。

**第四条** 工作原则。坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各部门力量共同做好网络安全事件的预防和处置工作。

## 第二章 组织机构与职责

**第五条** 网络安全和信息化领导小组（以下简称领导小组）是学校网络安全和信息化工作的领导机构，在应急工作中负责：统筹指导、指挥学校网络安全应急体系建设；决定Ⅰ、Ⅱ级网络安全事件应急响应启动，组织成立网络安全事件应急小组；统筹指导、指挥全局性网络安全事件应急响应工作。

**第六条** 网络安全和信息化办公室(以下简称网信办)为领导小组办公室所在单位，在应急工作中负责：制定学校网络安全相关制度和应急响应预案，定期进行网络安全事件应急演练；统筹组织学校的网络安全事件预防、监测，报告网络安全事件和预警信息，在网络安全应急处置工作中组织应急技术支撑队伍，提供技术支持与保障，并及时向领导小组报告情况。

**第七条** 学校各单位在应急工作中负责：本单位网站及信息系统的网络安全事件预防、监测、报告及应急处置工作；建立健全本单位网络安全应急响应机制，明确本单位网络安全联络员、网络信息监管员，人员发生变动时，需一周内报送网信办备案；积极支持配合领导小组及网信办进行应急响应处置工作。

## 第三章 监测预警

**第八条** 预警分级。建立学校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，教育系统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特别重大、重大、较大和一般网络安全事件。

**第九条** 事件与威胁监测。网信办负责对全校范围已发生的网络安全事件和威胁进行监测；各单位负责实施本单位网络与系统（网站）的网络安全事件和威胁监测，发生网络安全事件和网络安全威胁应立即报送至网信办。

**第十条** 预警研判和发布。网信办对监测信息进行研判，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并采取相应的防范措施。按照紧急程度、发展态势和可能造成的危害程度，及时向领导小组进行汇报，同时根据威胁程度发布橙色以下预警。红色预警一般由上级主管单位统一发布。对达不到预警级别但又需要发布警示信息的，网信办可发布风险提示信息。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。

**第十一条** 预警响应。红色预警响应学校进入应急状态，按照上级有关规定组织实施预警响应工作。橙色预警响应，网信办进入预警响应状态，协调相关技术支撑队伍对预警情况进行跟踪和态势分析，密切关注事态发展，做好监测分析和信息

搜集工作，及时上报领导小组。同时开展应急处置或准备、风险评估，若事态发展可能超过学校控制能力，应及时上报上级单位。黄色、蓝色预警响应，由各单位根据预案，组织做好预警响应工作。

## 第四章 应急处置

**第十二条** 各单位落实网络安全应急工作。在国家重大活动、会议期间，各单位应实行 24 小时值班制，加强对本单位网络和信息系统（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。

**第十三条** 事发紧急报告与处置。网络安全事件发生后，事发单位应立即启动应急预案，第一时间采取有效的应急处置措施，如执行断网、关闭服务器等，尽最大努力将损害和影响降到最小范围，注意保留相关证据，并及时报告网信办。网信办组织现场搜集相关信息，分析安全事件态势，形成紧急报告。紧急报告内容包括：时间地点、简要经过、事件类型与分级、影响范围、危害程度、初步原因分析、已采取的应急措施等。网信办及相关技术支撑队伍推进具体工作实施，根据具体情况调动相关物资、设备，必要情况下请求校外应急支援，提供现场安全保障，控制事态蔓延。相关人员保持 24 小时通讯畅通。

**第十四条** 若初判为III级以上网络安全事件，及时报告领导小组。由领导小组启动 I 级、II 级应急响应，成立应急小组，组织研究处置方案并进行指挥协调工作。若初判为 I 级网络安全事

件，应及时上报上级单位；对于人为破坏活动，同时报当地网信部门和公安机关。

**第十五条** 事中情况报告与处置。应急处置过程中，网信办及相关技术支撑队伍持续跟踪事态发展、检查影响范围，若为III级及以下事件有转化为II级事件的趋势，网信办应及时将事件危害程度、损失情况及现场处置情况上报领导小组；若为II级事件有转化为I级事件的趋势，领导小组应及时将事件危害程度、损失情况及现场处置情况上报上级部门。

**第十六条** 在网络安全事件应急处置后，应急小组将监测数据及其他处置情况报告领导小组，由领导小组确定结束应急处置，发布应急结束信号。

**第十七条** 应急响应工作结束后，相关单位迅速执行整改计划，研判网络安全现状，采取措施修整受损设施、数据，减少损失，消除隐患，恢复网络或系统（网站）至突发事件前状态，同时对事件损失进行统计、记录、分析。

**第十八条** 事后整改报告与处置。整改工作结束后，网信办组织技术人员与专家对事件发生及处置进行全面调查，实施取证工作，定位溯源，总结经验教训，完成《网络安全事件总结报告》，及时上报领导小组。

## 第五章 应急演练

**第十九条** 建立健全网络安全事件应急演练机制，制定详细演练方案，明确演练目标、参加演练的系统、涉及的形式、层次

和范围，设定灾难情况、演练流程、操作内容、业务验证测试、应急资源、职责分工、进度安排、演练的风险及其应对措施，确保应急预案内容切实可行。

**第二十条** 加强演练工作风险管理，谨慎开展应急演练。确保演练前组织、人员、资源到位。严格控制应急演练引起的系统变更风险，避免因演练导致服务中断、各项资源不可恢复。认真评估演练本身可能带来的风险和对业务的影响，制定完善的保障措施和应急回退方案。

**第二十一条** 记录演练开展的全过程和发现的问题，对演练的组织、过程、效果进行评估，编写应急演练总结报告。根据演练结果完善应急响应体系，维护更新防护设施。

**第二十二条** 将联网仪器设备纳入应急演练范围，保障联网仪器网络与数据安全。联网仪器应进行实名管理，由专人对联网仪器的基本信息、网络接入、账户管理、运维服务、数据安全、密码保护、安全审计进行管理，定期开展自查与应急演练。

## 第六章 工作保障

**第二十三条** 加强我校网络安全应急保障队伍与专家队伍建设，与机关团体、企事业单位等力量形成良好合作与互动。通过推动等级保护等工作提升学校对于网络安全事件的监测预警、安全防护、应急处置能力。

**第二十四条** 建立监督检查机制。本预案定期开展评估，根据实际情况适时修订。修订工作由网信办组织。

**第二十五条** 加强我校网络安全应急基础平台与管理平台建设及应急资源准备，为重要系统建立容灾环境，预留应急软硬件等应急物资，由领导小组负责统一调度。

**第二十六条** 学校每年提供专项经费，用于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。

## 第七章 附则

**第二十七条** 本预案由网络安全和信息化办公室负责解释。

**第二十八条** 本预案自发布之日起实施，学校原有相关预案与本预案不一致的按本预案执行。

天津科技大学办公室　　2023年10月22日印制