中共天津科技大学委员会文件

津科大党发〔2023〕68号

关于印发《天津科技大学网络数据安全事件应急预案（试行）》的通知

各基层党委（党总支）、各单位、机关各部门:

《天津科技大学网络数据安全事件应急预案（试行）》已经2023年10月20日学校党委常委会第33次会议研究通过，现予印发，请遵照执行。

附件：天津科技大学网络数据安全事件应急预案（试行）

中国共产党天津科技大学委员会

2023年11月2日

附件：

天津科技大学网络数据安全事件应急预案（试行）

为深入贯彻落实习近平总书记关于网络强国的重要思想，提升学校网络数据安全事件应急处置能力和水平，编制本预案。

一、总则

（一）编制目的

建立健全网络数据安全事件应急工作机制，构建网络数据全生命周期安全保障体系，提高网络数据安全事件应对能力，有效预防和减少网络数据安全事件造成的损失和危害，保护个人、组织合法权益，维护国家主权、安全和发展利益。

（二）编制依据

《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》《关键信息基础设施安全保护条例》《国家网络安全事件应急预案》和《天津市促进大数据发展应用条例》《教育部教育系统网络安全事件应急预案》《天津市教育系统网络数据安全事件应急预案》等相关法律规定。

（三）适用范围

本预案所指网络数据安全事件是指发生在学校，由于人为原因、软硬件缺陷或故障、自然灾害等，导致网络数据的保密

性、完整性或可用性遭到破坏，损害国家安全、公共利益和公民、组织合法权益的事件，可分为网络数据篡改事件、网络数据破坏事件、网络数据泄露事件、网络数据丢失事件、网络数据被非法获取事件、网络数据被非法利用事件和其他网络数据安全事件。涉及国家秘密的网络数据安全事件处置按照国家和本市有关规定执行。

（四）工作原则

坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，深入贯彻落实习近平总书记关于网络安全、数据安全、个人信息保护系列重要论述和对天津工作“三个着力”重要要求，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“谁管业务，谁管业务数据，谁管业务数据安全”“谁主管谁负责、谁使用谁负责、谁运维谁负责”，充分发挥各方面力量共同做好网络数据安全事件的应急处置工作。

（五）事件分级

根据教育系统网络数据的级别、规模和发生安全事件后的影响范围，教育系统网络数据安全事件分为四级：特别重大网络数据安全事件、重大网络数据安全事件、较大网络数据安全事件、一般网络数据安全事件。

1.符合下列情形之一的，为特别重大网络数据安全事件（Ⅰ级）：

（1）核心数据遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用，对国家安全、国民经济命脉、重要民生、重大公共利益等构成严重威胁、造成严重影响的网络数据安全事件。

（2）重要数据遭到大规模篡改、破坏、泄露、丢失或者被非法获取、非法利用，对国家安全、经济运行、社会稳定、公共健康和安全构成特别严重威胁、造成特别严重影响的网络数据安全事件。

（3）其他对国家安全、经济运行、社会稳定和公共利益构成特别严重威胁、造成特别严重影响的网络数据安全事件。

2.符合下列情形之一且未达到特别重大网络数据安全事件的，为重大网络数据安全事件（II 级）：

（1）核心数据遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用，对国家安全、国民经济命脉、重要民生、重大公共利益等构成威胁、造成影响的网络数据安全事件。

（2）重要数据遭到较大规模篡改、破坏、泄露、丢失或者被非法获取、非法利用，对国家安全、经济运行、社会稳定、公共健康和安全构成严重威胁、造成严重影响的网络数据安全事件。

（3）100 万以上个人信息遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用，对个人和组织合法权益构成严重威胁、造成严重影响的网络数据安全事件。

（4）其他对国家安全、经济运行、社会稳定和公共利益构成严重威胁、造成严重影响的网络数据安全事件。

3.符合下列情形之一且未达到重大网络数据安全事件的，为较大网络数据安全事件（III级）：

（1）重要数据遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用，对国家安全、经济运行、社会稳定、公共健康和安全构成较严重威胁、造成较严重影响的网络数据安全事件。

（2）10万以上100万以下个人信息遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用，对个人和组织合法权益构成较严重威胁、造成较严重影响的网络数据安全事件。

（3）其他对国家安全、经济运行、社会稳定和公共利益构成较严重威胁、造成较严重影响的网络数据安全事件。

4.一般网络数据安全事件（IV级）：

未达到上述情形，但对国家安全、公共利益或个人、组织合法权益构成一定威胁、造成一定影响的网络数据安全事件，为一般网络数据安全事件。

二、组织机构与职责

（一）领导机构与职责

学校网络安全和信息化领导小组(下文简称学校网信领导小组)统筹协调全局性网络数据安全事件应急工作，指导各单位网络数据安全事件应急处置工作。按照上级要求，配合做好特别重大网络数据安全事件处置的统筹指挥和组织协调。

（二）办事机构与职责

在学校网信领导小组的领导下，网络安全和信息化办公室（下文简称网信办）负责网络数据安全应急管理工作，对接上级

网络数据安全应急办公室，向学校网信领导小组报告网络数据安全事件情况，负责统筹协调学校网络数据安全事件应急工作，做好网络数据安全事件的预防、监测、报告和应急工作。

（三）各二级单位、机关处室职责

各二级单位、机关处室要按照“谁管业务，谁管业务数据，谁管业务数据安全”“谁主管谁负责、谁使用谁负责、谁运维谁负责"的原则，承担各自网络数据安全责任，全面落实各项工作。

三、监测与预警

（一）预警分级

按照网络数据的级别、规模和发生安全事件后的影响范围，网络数据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、较大和一般网络数据安全事件。

（二）预警监测

网络安全和信息化办公室通过多种渠道监测、发现已经发生或可能发生的网络数据安全事件，将掌握的情况立即通知相关单位。各二级单位负责做好本单位网络数据安全监测工作，一旦发生网络数据安全事件，应当立即上报网信办，不得迟报、谎报、瞒报、漏报。

（三）预警研判和发布

网络安全和信息化办公室对监测信息进行研判，对发生网络数据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。认为可能发生较大以上（含较大）数据

安全事件的信息，应立即向学校网信领导小组报告。

经研判，网信办提出发布黄色及以上预警的建议，报经学校网信领导小组批准后统一发布。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。

预警信息包括事件的类别、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。

（四）预警响应

预警信息发布后，各相关单位根据发布的预警级别，启动相应预案，组织技术力量立即响应，履行承担的职责。

1.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。

2.橙色预警响应

（1）网络安全和信息化办公室进入预警响应状态，在上级单位的统一领导下，负责学校应急处置准备或支持保障工作。重要情况报学校网信领导小组，重大事项及时通报相关单位。

（2）网络安全和信息化办公室组织指导相关应急支撑队伍、相关数据处理者开展应急处置或准备工作，做好网络数据安全检查、隐患排查工作，落实容灾备份措施，加强风险评估和控制工作。

3.黄色预警响应

网络安全和信息化办公室启动应急预案，加强对网络数据安全事件监测和事态发展趋势信息的搜集分析工作，组织指导

应急支撑队伍、相关数据处理者开展应急处置或准备工作，做好网络数据安全检查、隐患排查工作，落实容灾备份措施，加强风险评估控制工作，工作情况报学校网信领导小组。

4.蓝色预警响应

在网信办指导下，启动应急预案，开展预警响应。

5.预警级别的变更和解除

预警发布部门根据实际情况，确定是否解除预警，及时发布预警解除信息。

四、应急处置

（一）事件报告

网络数据安全事件发生后，事发单位应立即启动应急预案，立即组织本单位的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，控制事态，消除隐患，注意保存证据，经分析研判，初判为较大以上（含较大）级别的网络数据安全事件的，应立即报告网信办。对于人为破坏活动，应同时报当地网信部门和公安机关。网络安全和信息化办公室组织研判，认定为较大级别的网络数据安全事件的，报学校网信领导小组。

（二）应急响应

网络数据安全事件应急响应分为Ⅰ级、II 级、III 级、IV 级等四级，分别对应教育系统特别重大、重大、较大和一般网络数据安全事件。

1.Ⅰ级响应

发生特别重大网络数据安全事件时，上级有关部门决定启动 I 级响应，在学校网信领导小组指挥下，网络安全和信息化办公室会同相关部门配合开展应急处置工作。

2. II 级响应

发生重大网络数据安全事件或接到上级有关部门相关事件通报时，网络安全和信息化办公室报经学校网信领导小组同意后启动 II 级响应。

（1）网络安全和信息化办公室进入 24 小时应急值班状态，在学校网信领导小组统一领导下，履行应急处置工作的统一领导、指挥、协调职责。

（2）数据处理者具体落实事件应对处置要求，最大限度组织和控制事件影响，制定解决方案并实施。

（3）处理中需要有关技术支撑单位配合和支持的，网信办商请有关部门予以协调支持。

3. III 级响应

发生较大网络数据安全事件时，由学校网信办启动III级响应。

（1）事件发生单位进入应急状态，按照相关应急预案做好应急处置工作。

（2）数据处理者具体落实事件应对处置要求，最大限度组织和控制事件影响，制定解决方案并实施。

（3）相关部门跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报网络安全和信息化办公室。网络安全和信息化办公室视情将有关重大事项及时通报有关单位。

（4）处理中需要有关单位提供技术配合和支持的，商请相关单位予以协调支持。

4. IV 级响应

事发单位指导数据处理者落实事件应对处置要求，最大限度控制事件影响，制定解决方案并实施。

（三）应急结束

1. I 级响应结束

按照上级有关部门要求执行。

2. II 级响应结束

由学校网信领导小组决定，报教育部和市网络数据安全应急办公室批准后执行。

3. III级响应结束

由网信办建议，报学校网信领导小组批准后执行。

4. IV 级响应结束

由数据处理者决定，并报网信办。

五、调查与评估

特别重大网络数据安全事件、重大网络数据安全事件由上级相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学校网信领导小组及市教育两委。较大网络数据安全事件由网络安全和信息化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学校网信领导小组。一般网络数据安全事件由数据处理者自行组织开展调查处理和总结评估工作，并将调查评估结果汇总报网信办。

网络数据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。网络数据安全事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。

六、预防工作

（一）日常管理

学校按照职责做好网络数据安全事件日常预防工作，制定完善应急预案，做好网络数据安全检查、隐患排查、风险评估和容灾备份，健全网络数据安全信息通报机制，及时采取有效措施，减少和避免网络数据安全事件的发生及危害，提高应对网络数据安全事件的能力。

（二）演练

网络安全和信息化办公室定期组织演练，检验和完善预案，提高实战能力。

（三）宣传教育

学校应加强网络数据安全事件预防和处置的有关法律、法规和政策的宣传教育，充分利用网络安全周等各种活动形式和传播媒介，开展网络数据安全基本知识和技能的宣传活动，提高在校师生的网络数据安全意识。

（四）工作培训

学校定期组织网络数据安全培训，将网络数据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，加强网络数据安全特别是网络数据安全事件应急预案的学习，提高网络数据

安全管理和技术人员的防范意识及安全技能。

（五）重要时间节点的预防措施

在国家重大活动、重要会议期间和本市重大活动、重要会议期间，学校将加强网络数据安全事件的防范和应急响应，确保网络数据安全。网信办加强网络数据安全监测和分析研判，及时排查可能造成重大影响的风险和隐患，重点部门、重点岗位保持24小时值班，及时发现和处置网络数据安全事件隐患。

七、工作保障

（一）机构和人员

学校落实《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》等法律要求，把责任落实到具体部门、具体岗位和个人，建立健全应急工作机制。

（二）人才队伍保障

网信办配备必要的网络数据安全专业技术人才。各二级单位、相关处室配备相应的数据安全专人开展相关工作。做好网络数据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。

（三）物资保障

加强对网络数据安全应急装备、工具的储备，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

（四）经费保障

学校为网络数据安全事件应急处置提供必要的经费保障，

支持网络数据安全应急技术支撑队伍建设、宣传教育培训、预案演练、物资保障等工作开展。

（五）责任与奖惩

网络数据安全事件应急处置工作实行责任追究制。学校可对在网络数据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表彰和奖励；对迟报、谎报、瞒报和漏报网络数据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给予处分；构成犯罪的，依法追究刑事责任。

八、附则

本预案由网信办负责解释，自印发之日起实施。

附件：1.网络数据安全事件分类

2.名词术语

附件 1：

网络数据安全事件分类

网络数据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，导致网络数据的保密性、完整性或可用性遭到破坏，损害国家安全、公共利益和公民、组织合法权益的事件。可分为以下事件:

1.网络数据篡改事件：是指未经授权将信息系统中的数据更换为攻击者所提供的数据而导致的网络数据安全事件;

2.网络数据破坏事件：是指因误操作、人为蓄意、软硬件缺陷或遭受攻击等因素导致信息系统中数据被损毁的网络数据安全事件;

3.网络数据泄漏事件：是指因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的敏感数据暴露于未经授权者而导致的网络数据安全事件;

4.网络数据丢失事件：是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的数据丢失而导致的网络数据安全事件;

5.网络数据被非法获取事件：是指未经授权用户利用可能的技术手段恶意主动获取信息系统中数据而导致的网络数据安全事件;

6.网络数据被非法利用事件：是指未经授权用户利用可能的技术手段恶意获取并使用信息系统中数据而导致的网络数据安全事件;

7.其他数据安全事件：是指不能被包含在以上子类之中的网络数据安全事件。

附件 2：

名词术语

1.核心数据，关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据。

2.重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

3.个人信息，是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

4.数据处理者，是指在数据处理活动中自主决定处理目的和处理方式的个人和组织。数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。