应急预案编号：SGCC-SGTC-WL-09

应急预案版本号：第 3 次修订-2024 年编制

国网技术学院（山东电力高等专科学校）网络与信息系统突发事件处置应急预案

国网技术学院（山东电力高等专科学校）

2024 年 6 月

1 总则

1.1 适用范围

1.1.1 本预案为国网技术学院（山东电力高等专科学校）（以下简称“学院”）突发事件应急预案中的专项预案，适用于学院应对和处置信息网络范围内因网络与信息系统问题引起的对学院培训、教学、经营、管理构成重大影响和威胁的突发事件。

1.1.2 本预案所称的网络与信息系统突发事件，是指突然发生，使信息网络和信息系统遭受故障、损毁、破坏、信息泄露等损害，造成或者可能造成严重影响学院业务应用正常运转，甚至影响社会正常秩序，需要采取应急处置措施予以解决的网络与信息系统事故紧急事件。

1.1.3 本预案用于指导和规范学院网络与信息系统处置应急预案，建立“自上而下、分级负责、条块结合”的应急救援与处置体系。

1.2 预警分级

学院网络与信息系统突发事件预警分为一级、二级、三级和四级，依次用红色、橙色、黄色和蓝色表示，一级为最高级别。预警级别确定可采取以下方式;

（1）经综合分析，可能发生特别重大、重大、较大、一般网络与信息系统突发事件时，分别对应一级、二级、三级、四级预警。

（2）学院网络与信息应急领导小组根据可能导致的影响范围、严重程度和社会影响，确定预警等级。

1.3 响应分级

学院网络与信息系统大面积中断和停运、网络安全事件等突发事件应急响应分为Ⅰ、Ⅱ、Ⅲ、Ⅳ级，响应级别确定可采取以下方式:

（1）发生特别重大、重大、较大、一般事件时，分别对应Ⅰ、Ⅱ、Ⅲ、Ⅳ级应急响应;

（2）学院网络与信息应急领导小组根据网络与信息系统中断或停运，以及网络安全事件影响范围、严重程度和社会影响等，确定响应级别。

2 组织机构及职责

2.1 学院网络与信息应急领导小组及主要职责

学院网络与信息系统突发事件应急组织机构和职责参照公司总部设置，常设网络与信息系统突发事件应急领导小组（以下简称“学院网络与信息应急领导小组”），统一组织领导学院网络与信息系统突发事件防范及应对工作。

学院网络与信息应急领导小组组长由分管院领导担任，成员由办公室、发展策划部、财务资产部、安全实训部、党委组织部、党委党建部、网络学习服务中心、综合服务中心等相关部门主要负责人组成。

主要职责:

（1）贯彻落实国家和公司有关网络与信息系统突发事件应急处理的法律法规及相关政策规定;

（2）领导协调学院网络与信息系统突发事件应急处置工作;

（3）宣布学院进入和解除应急状态，决定启动、调整和终止应急响应;

（4）领导、协调事件相关抢险救援、恢复重建等工作。

2.2 学院网络与信息应急办及主要职责

学院网络与信息应急领导小组下设办公室（以下简称“学院网络与信息应急办”），是学院网络与信息应急领导小组的日常办事部门，落实学院网络与信息应急领导小组部署的各项任务。办公室设在网络学习服务中心，组长由网络学习服务中心负责人担任，成员由网络学习服务中心相关人员组成。

主要职责:

（1）执行网络与信息系统应急领导小组下达的应急指令、重大应急决策和部署，协调各方应急资源，组织应急处置;

（2）组织制定学院网络与信息系统应急工作相关制度、标准、规范和预案，定期组织评估和复核，并监督、检查贯彻执行情况;

（3）根据网络与信息系统事故及可能的发展情况进行评估，判断相应的事故级别，提供启动、结束相应突发事件应急预案的参考意见;

（4）及时了解和掌握信息系统突发事件与应急处置工作情况，向网络与信息系统应急领导小组报告应急处置过程中发现的重大问题，并协调解决。

3 监测预警

3.1 风险监测

3.1.1 学院网络与信息应急办应密切监测可能引起网络与信息

系统突发事件的各类风险。网络学习服务中心负责组织信息专业机构运维范围内的网络与信息系统突发事件的监测工作；涉及由其他部门负责管理的系统或终端由该部门负责组织网络与信息系统突发事件风险的监测工作。

3.1.2 在风险监测中，可通过以下方式获取风险预警信息:

（1）通过各类系统及在线监测手段，实时监视网络与信息系统运行与安全情况,并及时将风险预警信息上报国网信息调度。

（2）通过各类系统及在线监测手段实时监测基础设施、基础平台、互联网出口、信息内外网络、业务应用系统、对外网站、信息内外网邮件系统、桌面终端计算机等的安全运行情况，加强对设备、系统及机房环境的巡检，对事件进行预测分析。

（3）相关部门按照“谁主管谁负责、谁运行谁负责”的原则，对所负责的业务系统的运行与安全情况进行监测。

（4）学院网络与信息应急办及相关部门应与公司、各级政府有关部门建立相应的网络与信息系统监测、预报、预警、联动机制，实现安全态势、安全漏洞（隐患）、风险处置建议等相关信息的实时共享。

3.1.3 在通过 3.1.2 所列举方式获得网络与信息系统突发事件重大风险信息后，应按照本预案第 5 章的信息报告要求及时上报，并保留汇报内容记录。

3.2 预警发布

3.2.1 预警程序

（1）学院网络与信息应急办或相关部门接到网络与信息系统突

发事件预警信息后，立即汇总相关信息，分析研判，提出学院网络与信息系统突发事件预警建议，报学院网络与信息应急领导小组批准，由学院网络与信息应急办发布;

（2）学院网络与信息应急办接到政府应急管理部门或公司网络安全应急机构发布的网络与信息系统突发事件预警通知后，立即会同相关部门汇总相关信息，分析研判，提出学院网络与信息系统突发事件预警建议，报学院网络与信息应急领导小组批准，由学院网络与信息应急办发布。

3.2.2 发布内容

网络与信息系统预警信息内容包括发布单位、发布时间、风险等级、风险类型、涉及系统、涉及设备、预警原因、通过何种监控手段、告警具体信息、影响范围、处置要求等重点。

3.2.3 发布方式

预警信息通过电子邮件、传真等方式进行发布。

3.3 预警响应

3.3.1 一级、二级预警行动

发布网络与信息系统突发事件一级、二级预警信息后，应采取以下部分或全部措施:

学院预警行动:

（1）学院网络与信息应急办或相关部门组织收集相关信息，密切关注事态发展，必要时向学院网络与信息应急领导小组报告;

（2）学院网络与信息应急办组织相关部门开展应急值班;

（3）加强与政府相关部门的沟通，及时报告事件信息；做好新

闻宣传和舆论引导工作;

（4）学院网络与信息应急办组织采取有效措施控制事态发展，组织应急抢修、应急物资等准备工作，合理安排网络与信息系统运行方式、做好异常情况处置和应急信息的发布。

3.3.2 三级、四级预警行动

发布网络与信息系统突发事件三级、四级预警信息后，应采取以下部分或全部措施:

学院预警行动:

（1）学院网络与信息应急办或相关部门密切关注事态发展，收集相关信息，必要时向学院网络与信息应急领导小组报告;

（2）学院网络与信息应急办组织采取有效措施控制事态发展，组织应急抢修、应急物资等准备工作，合理安排网络与信息系统运行方式、做好异常情况处置和应急信息的发布。

3.4 预警调整和解除

3.4.1 预警调整

学院网络与信息应急办或有关部门可根据预警阶段网络与信息系统安全运行情况、预警行动效果，提供对预警级别调整的建议报学院网络与信息应急领导小组批准后发布。

3.4.2 预警解除

有事实证明突发事件不可能发生或者危险已经解除，应按照“谁发布、谁解除”的原则及时宣布预警解除信息，终止已采取的有关措施。如直接进入应急响应状态，则预警自动解除。

4 应急响应

4.1 应急处置指导原则

4.1.1 统一领导，分级负责

落实国家和公司关于网络与信息系统突发事件的总体部署，在学院统一领导下，按照“综合协调、统一领导、分级负责”的原则，建立系统化、分层次的应急组织和指挥体系。组织开展网络与信息系统突发事件预防、应急处置、运行恢复、事件调查及通报等各项应急工作。

4.1.2 基础保障，技术支撑

坚持“依法合规、开放可信、实战对抗、联动防御”的安全防护策略，落实公司网络安全防护措施，以管理信息大区、互联网大区监测系统为监测与审计工具，以督查、巡检为依托，采用先进适用的预测、预防、预警和应急处置技术，不断改进和完善应急处置装备和手段，提升应对网络与信息系统突发事件的技术支撑能力，建立健全学院应对网络与信息系统突发事件的长效机制。

4.1.3 预防为主，常备不懈

坚持“安全第一、预防为主、综合治理”的方针，加强网络与信息系统突发事件的超前预想，做好应对网络与信息系统突发事件的预案准备、应急资源准备、保障措施准备，编制各现场处置方案，形成定期开展应急培训和演练的常态机制，提升对各类网络与信息系统突发事件的应急响应和综合处置能力。

4.1.4 统筹全局，突出重点

综合运用技术和管理手段，减少突发事件对学院网络与信息系统的影响，并建立与通信系统应急联动预警响应机制，保障支撑学

院生产、经营、管理的网络与信息系统安全，加大对关键网络和重要信息系统监控及应急处置力度，加强对网络与信息系统突发事件的通报考核工作，保证重点信息基础设施的平稳运行，有效控制损失，为国家网络安全提供强有力的支撑。

4.1.5 快速响应，协同应对

充分发挥学院优势，加强与政府网络与信息系统应急主管部门的沟通协作及纵向信息报送，建立健全公司“上下联动、区域协作”快速响应机制，整合内外部应急资源，协同开展突发事件处置，确保及时响应和有效处置突发事件。

4.1.6 以人为本，减少危害

充分发挥学院专业人员的作用，切实提升应急处置人员的业务素质、防护意识和指挥能力。把保障学院正常生产、经营、管理秩序作为首要任务，最大程度减少突发事件造成的经济损失和利益损害。

4.2 先期处置

突发事件发生后，学院在全面了解情况，做好信息报送的同时，启动预案响应措施，立即组织学院应急队伍开展相关工作；根据先期处置效果，及时发布公告，通知学院信息客服做好用户解释工作并与业务部门保持沟通。必要时，相关部门迅速调集应急抢修物资，做好各项应急准备工作。

4.3 响应启动

（1）事发部门启动学院应急响应，并立即向学院网络与信息应急办、总值班室报告。

（2）学院网络与信息应急办接到事发部门相关报告后，了解相关信息，分析研判，根据影响范围和严重程度对响应等级进行建议，报学院网络与信息应急领导小组批准。

（3）发生重大及以上网络与信息系统突发事件，学院网络与信息应急办启动应急响应，协同相关部门、事发部门组织开展应急处置工作。

（4）发生较大及以下网络与信息系统突发事件，学院网络与信息应急办或相关部门跟踪、监督事发部门应急处置工作。

4.4 指挥协调

4.4.1 初判发生网络与信息系统特别重大突发事件，重点开展以下工作:

学院网络与信息应急领导小组研究启动 I 级应急响应状态，学院网络与信息应急办协调、组织、指导处置工作，并将处置情况汇报学院应急领导小组;

学院网络与信息应急办召开首次会商会议，就有关重大应急问题做出决策和部署;

学院网络与信息应急办进入 24 小时应急值守状态，及时跟踪事件发展情况，收集汇总分析事件信息;

学院网络与信息应急领导小组组长负责指挥决策；委派学院网络与信息应急办组长作为现场工作组组长带队，赶赴事发现场指导处置工作;

对事发部门做出处置指示，责成有关部门立即采取相应应急措施，按照处置原则和部门职责开展应急处置工作;

组织学院网络安全队伍为突发事件的分析、处置提供技术支撑，为突发事件中的安全隐患消缺和加固修复提供技术支撑。

4.4.2 初判发生网络与信息系统重大突发事件，重点开展以下工作:

学院网络与信息应急领导小组研究启动II级应急响应状态，学院网络与信息应急办协调、组织、指导处置工作，并将处置情况汇报学院应急领导小组;

学院网络与信息应急办召开首次会商会议，就有关重大应急问题做出决策和部署;

学院网络与信息应急办进入 24 小时应急值守状态，及时跟踪事件发展情况，收集汇总分析事件信息;

学院网络与信息应急领导小组组长负责指挥决策；委派学院网络与信息应急办组长作为现场工作组组长带队，赶赴事发现场指导处置工作;

对事发部门做出处置指示，责成有关部门立即采取相应应急措施，按照处置原则和部门职责开展应急处置工作;

组织学院网络安全队伍为突发事件的分析、处置提供技术支撑，为突发事件中的安全隐患消缺和加固修复提供技术支撑。

4.4.3 初判发生网络与信息系统较大突发事件，由事发部门负责处置，重点开展以下工作:

学院网络与信息应急领导小组研究启动III级应急响应状态，指导协调处置工作，并将处置情况汇报学院应急领导小组;

学院网络与信息应急办或相关部门开展应急值守，及时跟踪事

件发展情况，收集汇总分析事件信息;

学院网络与信息应急领导小组根据需要派出学院网络与信息应急办负责人、相关部门负责人赶赴现场指导应急处置;

组织学院网络安全队伍为突发事件的分析、处置提供技术支撑，为突发事件中的安全隐患消缺和加固修复提供技术支撑。

4.4.4 初判发生网络与信息系统一般突发事件，由事发部门负责处置，学院重点开展以下工作:

（1）学院网络与信息应急领导小组研究启动Ⅳ级应急响应状态，指导协调处置工作，并将处置情况汇报学院应急领导小组;

（2）学院网络与信息应急办或相关部门开展应急值守，及时跟踪事件发展情况，收集汇总分析事件信息;

（3）学院网络与信息应急办或相关部门根据需要派出相关处室负责人赶赴现场指导参与应急处置;

（4）组织学院网络安全队伍为突发事件的分析、处置提供技术支撑，为突发事件中的安全隐患消缺和加固修复提供技术支撑。。

4.5 响应措施

应对网络与信息系统大面积中断和停运、网络安全事件等突发事件，学院及相关事发部门应采取以下一项或多项措施。

4.5.1 系统抢修

（1）事发部门调集本单位应急队伍、物资，组织开展抢修工作;

（2）事发部门运维检修机构负责应急处置工作，对问题进行定位、排查、处置、验证、反馈，调整网络与信息系统运行方式，在评估问题影响并判断风险等级后，应对问题处置进度保持及时跟踪

与信息发布，通过信息客服做好用户解释工作并与业务部门保持沟通；在整个应急处置期间，须同时执行汇报制度，向学院数字化职能管理部门报告;

（3）事发部门在故障事件处置过程中如需要技术支持，可通过学院数字化职能管理部门上报。由上级单位安排相关技术支持人员。如情况需要，可申请调配应急队伍进行协助排查处置;

（4）必要时事发部门可组织系统研发单位技术人员参与抢修;

（5）事发部门如不能消除或有效控制突发事件发展和影响范围，应在采取处置措施的同时，由学院数字化职能管理部门向上级报告，由上级负责协调指挥。

4.5.2 客服响应

学院信息客服协同事发部门做好用户解释和沟通工作。

4.5.3 舆论引导

学院党委党建部（党委宣传部）及时收集有关舆情信息，组织开展对外新闻发布工作。

4.5.4 物资保障

学院网络学习服务中心协同综合服务中心物资处组织应急物资供应，协调应急物资运输畅通;相关各部门提供可调用的应急物资相关信息。

4.5.5 事态评估

学院网络与信息应急办对网络与信息系统大面积中断和停运、网络安全事件等突发事件影响范围、影响程度、发展趋势及恢复进度进行评估，并将评估情况报学院网络与信息应急领导小组。

4.6 响应调整和终止

4.6.1 响应调整

学院网络与信息应急领导小组或应急指挥部根据事件危害程度、救援恢复能力和影响范围等综合因素，按照事件分级条件，决定是否调整响应级别。

4.6.2 响应终止

满足下列条件，由学院网络与信息应急领导小组研究决定结束应急响应，由学院网络与信息应急办宣布本单位应急响应终止:

国家应急相关部门或公司数字化部宣布网络与信息系统恢复正常状态;

受损网络信息设备（设施）基本恢复，网络与信息系统恢复正常运行。

5 信息报告

5.1 报告程序

5.1.1 内部报告程序

（1）预警阶段

事发部门向学院网络与信息应急办报告有关信息。

应急响应阶段

重大及以上事件响应阶段：事发部门向学院网络与信息应急办、学院应急办报告有关信息。

较大及以下事件响应阶段：事发部门向学院网络与信息应急办报告有关信息。必要时学院网络与信息应急办向学院网络与信息应急领导小组报告。

5.1.2 外部报告程序

（1）预警阶段

重大及以上事件预警阶段：事发部门向学院网络与信息应急办、学院应急办报告有关信息后，必要时，经学院网络与信息应急领导小组批准，学院网络与信息应急办向公司相关部门报告预警相关情况，由学院网络与信息应急办或总值班室向公司相关部门报告预警相关情况，提出预警建议，按照相关规定通知重要用户。

较大及以下事件无需对外部报告。

（2）应急响应阶段

重大及以上事件响应阶段：事发部门启动应急响应，开展应对网络与信息系统大面积中断和停运、网络安全事件等突发事件的响应措施，及时向学院网络与信息应急办、学院应急办报告应急响应信息。必要时，经学院网络与信息应急领导小组批准，学院网络与信息应急办向公司相关部门报告相关情况。

较大及以下事件无需对外部报告。

5.2 报告内容

5.2.1 预警行动阶段

事发部门向学院网络与信息应急办、相关部门报告预警发布和预警结束情况，以及信息网络运行、信息系统风险及发展趋势、已采取措施等信息。

5.2.2 应急响应阶段

网络与信息系统突发事件发生后，事发部门向学院网络与信息应急办、相关部门报告突发事件发生时间、地点和范围，对网络、

信息系统以及社会的影响，已采取的措施等;

事发部门向学院网络与信息应急办、相关部门报告网络信息设备（设施）受损、事件处置进展及发展趋势，应急抢修队伍、应急物资、应急装备需求等情况;

学院网络安全队伍向学院报告协同处置、安全加固及安全隐患复核等情况;

必要时，学院网络与信息应急办或学院应急办和相关部门按照规定向上级政府部门报告以下基本情况：事件信息来源、时间、地点、基本经过、影响范围、已造成后果、初步原因和性质、事件发展趋势和拟采取的措施以及信息报告人员的联系方式等。

5.3 报告要求

（1）学院发生网络与信息系统突发事件，应严格按照规定的报送流程和时限要求报告山东省教育厅（中共山东省委教育工委）、国家电网有限公司。

（2）事发部门向学院网络与信息应急办、相关部门汇报信息，必须做到数据源唯一、数据正确。

（3）预警阶段和较大级、一般级事件响应执行每天定点“零报告”制度。

（4）特别重大级、重大级事件响应执行每天两次定点“零报告”制度。

（5）事发部门根据公司要求，完成相关信息报送。

5.4 信息发布

（1）突发事件处置期间，学院网络与信息应急办协助学院党委

党建部（党委宣传部）开展突发事件信息发布和舆论引导工作;

（2）发布信息主要包括突发事件的基本情况、采取的应急措施、取得的进展、存在的困难以及下一步工作计划等;

（3）信息发布和舆论引导工作要做到及时主动、正确引导、严格把关;

（4）业务部门会同网络学习服务中心，共同制定发布信息的内容规范，涵盖业务、技术、管理等各项信息。

6 后期处置

6.1 善后处置

（1）贯彻“考虑全局、突出重点”原则，开展善后处理。

（2）督促相关部门认真开展隐患排查和治理工作，避免次生事故发生，确保系统稳定。

（3）督促事发部门整理受损情况，做好记录分析，加快抢修恢复速度，提高抢修恢复质量，尽快恢复系统正常运行。

6.2 处置原则与内容

6.2.1 处置和恢复原则

事发部门要贯彻“考虑全局、突出重点”原则，对善后处理、恢复重建工作进行规划和部署，制定抢修恢复方案。

事发部门在信息系统新建、重建中，要充分考虑采用高可用架构，符合公司运行管理及研发安全相关要求，采用必要的网络安全防护措施，同时加强运行期信息系统改造。要积极采用新的技术手段，开展技术支撑手段建设，提升在监测及预警、故障定位与影响分析、故障处置自动化过程中的技术支撑能力。

6.2.2 处置和恢复内容

事发部门要根据恢复重建方案，积极组织对受损网络与信息系统设备、设施和数据的恢复重建工作。当应急处置导致原有运行方式发生变化时，通过重建措施恢复原有运行方式或优化更新运行方式。

6.3 事件调查

学院网络与信息应急办组织调查收集事件详细资料，研究事件发生的原因，分析网络与信息系统突发事件发展过程，吸取教训，提出具体事故防范对策与措施，发布通报，督促相关部门落实防范措施。对事件调查按照《国家电网公司安全事故调查规程》（国家电网安监〔2020〕820号）（国家电网安监〔2020〕820号）要求和公司“四不放过”原则进行。

6.4 应急处置评估

网络与信息系统突发事件应急处置结束后，学院应对使用的应急预案和应急救援处置过程进行全面总结、评估，找出不足并明确改进方向，及时对应急预案的不足之处予以修订。

7 应急保障

7.1 应急队伍保障

学院应急队伍通过与外部厂商应急人员沟通协作，汲取外部力量，保证有效应对学院系统内各类网络安全与信息系统突发事件，确保第一时间有效展开抢修工作，保障网络与信息系统有效运行。

7.2 应急物资保障

学院建立健全网络与信息系统突发事件的应急物资装备储存、

调拨和紧急配送机制，确保网络与信息系统突发事件所需的物资装备的应急供应。物资包括但不限于有车辆、备品备件、常用工具和常用工具软件等。

7.3 技术保障

7.3.1 重视研究涉及网络信息系统安全的重大问题，从信息系统建设和改造项目的规划、立项、设计、建设、运行等各环节，提出应对信息系统突发事件的技术保障要求。

7.3.2 在信息系统各项目建设和服务合同中应包含相关设备厂商、技术服务厂商在信息系统应急方面的技术支持内容。

7.3.3 应根据本预案制定具体预案，并对各个专项制定专项应急预案，形成预案体系。各专项预案中应详细定义应急处置流程、应急人员、应急操作方法等，保证对信息系统事件的准确处置。

7.3.4 应注意收集各类信息系统突发事件的应急处置实例，总结经验和教训，开展信息系统事件预测、预防、预警和应急处置的技术研究，加强技术储备。

7.4 经费保障

应保障应急培训、演练、添置应急装备物资等所需经费。

7.5 其他保障

7.5.1 应急期间，应保证有关应急联系人员的手机应保持24小时开机状态。

7.5.2 制订全面覆盖在运信息系统和主要威胁的现场处置方案。

8 附件

8.1 学院概况

国家电网有限公司技术学院分公司（山东电力高等专科学校）（以下简称“学院”）作为公司唯一直管的普通高等职业院校，成为公司发展链、价值链的重要组成部分和重点建设的公司企业大学。

8.2 风险评估的结果

8.2.1 危险源分析

学院网络与信息系统覆盖范围广、集成度高，运行维护难度大，存在造成网络与信息系统突发事件的众多危险源。

（1）内部危险源

网络与信息系统相关软硬件自身缺陷、网络与信息系统机房基础设施故障、网络与信息系统相关设备老化或超负荷运行、员工安全意识薄弱、员工违规操作（或误操作）、员工恶意破坏、信息泄露、内网移动存储设备病毒侵入等导致发生网络与信息系统突发事件。

（2）外部危险源

机密性：外部人员通过技术手段进行后门攻击、漏洞攻击等网络攻击或通过社会工程学攻击渗透进入学院环境，导致敏感信息或业务系统数据遭到泄漏。

完整性：外部人员通过技术手段进行后门攻击、漏洞攻击等网络攻击或通过社会工程学攻击渗透进入学院环境，导致业务系统数据遭到篡改。

可用性：外部人员利用计算机病毒、蠕虫、木马、僵尸网络、网页内嵌恶意代码等有害程序破坏系统可用性；外部人员通过社会工程学攻击渗透进入学院环境，以及人为破坏网络线路，造成服务

器对外服务不可用；各类自然灾害及社会安全事件造成网络与信息系统、系统数据或基础设施遭到破坏导致发生网络与信息系统突发事件。

8.2.2 危害程度分析

根据事件发生的根本原因或故障点进行分类，分析事件危害程度具体如下:

（1）基础设施类：包括机房电源、空调、消防等物理环境设备故障，自然灾害、人员违规操作或误操作、远控设备被恶意控制导致信息机房内设备无法稳定运行等。

基础设施类故障可能造成学院信息系统设备损坏或报废、信息网络中断、业务应用系统服务中断，影响学院正常生产、经营、管理秩序，甚至造成对内对外信息服务、业务服务瘫痪，严重损害公众利益，威胁国家安全及企业安全。

（2）信息网络类：包括支撑信息网络的信息设备软硬件、网络链路故障，导致信息网络中断等。

信息网络类故障可能造成业务应用系统服务中断、上下级联贯通不可用，影响学院正常生产、经营、管理秩序，严重损害公众利益，威胁国家安全及企业安全。

（3）平台类：包括支撑平台类系统的信息设备软硬件故障，造成业务系统不能访问。

平台类故障可能造成对内对外信息服务、业务服务瘫痪，影响学院正常生产、经营、管理秩序，严重损害公众利益，威胁国家安全及企业安全。

（4）业务应用类：包括支撑业务应用系统的信息设备软硬件故障，业务系统访问异常，业务应用系统数据丢失或遭恶意篡改等。

业务应用类故障可能影响系统重要数据的保密性、完整性和可用性，扰乱学院正常生产、经营、管理秩序，甚至造成对内对外信息服务、业务服务瘫痪，企业业务数据丢失或错乱，并严重损害公众利益，威胁国家安全及企业安全。

（5）网络安全类：包括敏感信息泄露，敏感信息发布和服务网站遭受攻击和破坏，页面信息遭受篡改，大面积有害信息通过网络和信息系统传播，大面积病毒、蠕虫、木马等恶意程序爆发等。

网络安全类事件可能造成学院信息网络中断、信息网络拥塞、业务应用系统服务中断和有害程序或信息传播，影响学院正常生产、经营、管理秩序，甚至造成对内对外信息服务、业务服务瘫痪，严重损害公众利益，威胁国家安全及企业安全。

（6）数据安全类：包括系统数据违规导入、导出、修改、删除等数据安全事件，数据安全类事件可能造成学院信息泄露、数据遭篡改、数据丢失，严重损害公众利益，威胁国家安全及企业安全。

（7）其他故障类：包括人为外力破坏及其他原因引起的网络和信息系统事故。

其他故障可能造成学院信息网络中断、业务应用系统服务中断、信息泄露、数据丢失和有害程序或信息传播，影响学院正常生产、经营、管理秩序，甚至造成对内对外信息服务、业务服务瘫痪，严重损害公众利益，威胁国家安全及企业安全。

8.2.3 事件分级

根据学院网络与信息系统突发事件对社会和学院生产、经营、管理的影响范围、严重程度、可能产生的后果及损失等因素，将网络与信息系统突发事件分为：特别重大、重大、较大、一般四级。

8.2.3.1 特别重大事件

出现下列情况之一，为学院特别重大网络与信息系统突发事件：

（1）国家确定为特别重大网络与信息系统事故的事件。

（2）《国家网络安全事件应急预案》（中网办发文〔2017〕）或《国家电网有限公司网络与信息系统突发事件应急预案》（国家电网数字〔2024〕33号）中确定为特别重大网络安全事件的事件，包括：重要网络与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；国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁；其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

（3）导致发生《国家电网公司安全事故调查规程》（国家电网安监〔2020〕820号）中五级设备或信息系统事件。

（4）学校网络与信息应急领导小组视网络与信息系统突发事件危害程度，恢复能力等综合因素，研究确定为特别重大网络与信息系统突发事件。

8.2.3.2 重大事件

出现下列情况之一，为学院重大网络与信息系统突发事件：

国家确定为重大网络与信息系统事故的事件。

《国家网络安全事件应急预案》（中网办发文〔2017〕）或《国

家电网有限公司网络与信息系统突发事件应急预案》（国家电网数字〔2024〕33号）中确定为重大网络安全事件的事件，包括：重要网络与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；国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁；其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

（3）导致发生《国家电网公司安全事故调查规程》（国家电网安监〔2020〕820号）中六级设备或信息系统事件。

（4）学校网络与信息应急领导小组视网络与信息系统突发事件危害程度，恢复能力等综合因素，研究确定为重大网络与信息系统突发事件。

8.2.3.3 较大事件

出现下列情况之一，为公司较大网络与信息系统突发事件：

（1）《国家网络安全事件应急预案》（中网办发文〔2017〕）或《国家电网有限公司网络与信息系统突发事件应急预案》（国家电网数字〔2024〕33号）中确定为较大网络安全事件的事件，包括：重要网络与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；国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁；其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

（2）导导致发生《国家电网公司安全事故调查规程》（国家电

网安监〔2020〕820号）中七级设备或信息系统事件。

（3）学校网络与信息应急领导小组视网络与信息系统突发事件危害程度，恢复能力等综合因素，确定为较大网络与信息系统突发事件的。

8.2.3.4 一般事件

出现下列情况之一，为公司一般网络与信息系统突发事件:

（1）《国家网络安全事件应急预案》（中网办发文〔2017〕）或《国家电网有限公司网络与信息系统突发事件应急预案》（国家电网数字〔2024〕33号）中确定为一般网络安全事件的事件，包括：除特别重大网络安全事件、重大网络安全事件和较大网络安全事件情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

（2）导致发生《国家电网公司安全事故调查规程》（国家电网安监〔2020〕820号）中八级设备或信息系统事件。

（3）学校网络与信息应急领导小组视网络与信息系统突发事件危害程度，恢复能力等综合因素，确定为一般网络与信息系统突发事件的。

8.3 预案体系与衔接

8.3.1 其他应急预案衔接

本预案是学院为应对网络与信息系统突发事件而制定的专项应急方案，明确了应急工作程序和具体的应急救援措施，是学院应急预案体系的重要组成部分。

本预案与学院总体应急预案和自然灾害类、部分事故灾难类和

部分社会安全类应急预案等预案相关联。本预案还与《国家网络安全事件应急预案》（中网办发文〔2017〕）、《国家电网有限公司网络与信息系统突发事件应急预案》（国家电网数字〔2024〕33号）相衔接，并根据国家预案、相关政策法规和政府管理要求变化，及时进行修订、完善。