合肥工业大学网络安全事件应急预案

第一章　总则

第一条 为了加强合肥工业大学网络信息安全工作，及时掌握和处置网络信息安全事件，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，维护正常工作秩序和营造健康的网络环境，根据国家有关法律法规，以及相关标准文件，结合合肥工业大学实际情况，制定本办法。

第二条 网络信息安全事件定义。本办法中的网络信息安全事件参照《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》《中华人民共和国计算机信息系统安全保护条例》《信息安全技术 信息安全应急响应计划规范》（GB/T 24363-2009）、《信息安全事件分类分级指南》（GB/Z 20986-2007）、《教育系统突发公共事件应急预案》、教育部《信息技术安全事件报告与处理流程（试行）》中对信息技术安全事件的定义。网络信息安全事件是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。

第三条 适用范围。凡是使用合肥工业大学 IP 地址进行建设、运营、维护和使用的网站和信息系统，都属于我校网络信息安全监管范围，合肥工业大学信息化建设与发展中心（以下简称“信息化中心”）有权对这些网站和信息系统采取监测、防御、处置等措

施，提高网站和信息系统的安全水平，减少被攻击和破坏的可能，降低在遭受攻击和破坏时的影响程度。本办法适用于合肥工业大学发生的信息网络安全事件的报告与处置工作。

第二章　管理机制和职责

第四条 信息化中心负责协调网络安全工作和相关监督管理工作。合肥工业大学其他有关机构依照本办法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

第五条 凡是使用合肥工业大学 IP 地址建设、运营、维护和使用的网站和信息系统的机构开展服务活动，必须遵守法律、行政法规，尊重社会公德，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。信息化中心依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。信息化中心为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第三章　网络信息安全事件的认定和处理

第六条 安全事件检查结果来源及等级划分。

（一）网络信息安全事件的检查来源

我校网络信息安全事件的检查来源，主要有以下几个渠道：

1. 信息化中心通过技术手段内部定期扫描等发现的网络安全事件；

2. 教育部信息中心检测到的网络安全事件;

3. 保密系统技术部门检测到的网络安全事件;

4. 公安系统技术部门检测到的网络安全事件;

5. 其它来源。

（二）合肥工业大学信息网络安全事件的分类和定义根据《信息安全事件分类分级指南》将安全事件划分为如下：校定三级（重大事件）、校定二级（较大事件）、校定一级（一般事件）和其他安全事件。

1. 校定三级安全事件 网站页面被篡改，或者学校公共服务信息系统后台数据库内容被修改或丢失，定义为校定三级安全事件。

2. 校定二级安全事件 网站或者软件已经被加入暗链接或者与主题无关的内容但是未造成恶劣影响的情况,定义为校定二级安全事件。

3. 校定一级安全事件 通过技术手段检查发现网站或者软件存在安全隐患但是未被攻击和利用的情况，定义为校定一级安全事件。

4. 其他事件 除上述三种事件的事件。

第七条 网络信息安全事件的报告与处置（校定一级到三级）。报告与处置分为两个步骤：事发紧急报告与处置、事后整改报告与处置。

（一）事发紧急报告与处置

1. 各单位一旦发现上述安全事件第一时间通报给各单位的网络安全与信息化专员或信息化中心网络安全科，专员/网络安全科应根

据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位安全责任人和主要负责人。

2. 二级单位安全责任人接到报告后，应立即组织技术人员赶赴现场进行紧急处置，同时以电话通讯的方式将相关情况通报至合肥工业大学信息化中心相关人员，涉及人为主观破坏事件应同时报告公安机关。

3. 信息化中心接到上述报告后，由学校专职网络安全管理人员判定安全事件等级，并及时报告校网络安全与信息化建设领导小组办公室（以下简称“校网信办”）。校网信办授权信息化中心通知相关机构按照网络安全事件相应级别，限时处置。如涉及主观破坏事件，影响严重，信息化中心负责组织应急处置并与学校党委宣传部、上级网信办、公安机关等部门联系。

（二）事后整改报告与处置

1. 事后整改报告应在相应级别限定天数内以书面报告的形式进行报送。整改报告由信息化中心协助相关机构编写，由二级单位主要负责人审核后，签字并加盖公章报送校网信办。校网信办负责将整改报告按规定流程报送上级相关部门。

2. 安全事件事后处置包括：及时掌握损失情况、查找和分析事件原因、修复系统漏洞、恢复系统服务，尽可能减少安全事件对正常工作带来的影响；进一步总结事件教训、研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力；如涉及人为主观破坏的安全事件应继续配合公安机关开展调查。

第八条 其他安全事件报告与处置。机构发生其他安全事件，由校网络安全和信息化建设领导小组办公室视具体情况酌情处理。

第四章　应急组织体系及职责

第九条 学校网络安全与信息化建设领导小组统筹协调合肥工业大学全局性网络安全事件应急工作，指导校属各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，成立学校网络安全事件应急工作组（以下简称工作组），负责组织指挥和协调事件处置，并根据有关规定，在上级主管部门指导、校内外单位的支持下，开展应对工作。网络安全事件应急工作的有关校内单位包括：

（一）党委宣传部

对涉及学校安全稳定和师生利益的突发、重大事件，应按相关预案第一时间进行合理处置；对其它特别紧急的事项，应当急事急办，随到随办。

（二）信息化建设与发展中心

信息化中心在网络安全应急预案中的职责包括：

1. 负责制订网络安全事件应急预案。

2. 统筹我校的网络安全应急预案的宣传教育工作。

3. 组织我校的应急预案演练工作。

4. 负责网络安全事件定级、处置、报告的检查工作。

5. 处理安全事件的定级、处置、报告工作。

6. 负责学校网络安全事件处置中的技术支持工作、核定安全事件等级，及时收集、通报和上报安全事件处置情况。

7. 负责网络安全的监测、预警、态势分析工作。

8. 负责校内网络安全事件应急响应协调工作。

9. 负责我校网络安全应急预案的教育培训工作。

10. 负责我校的网络安全应急预案演练指导工作。

11. 负责协助学校宣传部等内容类安全事件的技术处置工作。

（三）保卫处

保卫处在处理网络安全事件时负责:

1. 协助信息中心及各单位进行现场取证的工作。

2. 协助信息中心与公安机关的联系。

3. 下达来自公安机关网络安全事件处置要求等。

（四）总务部

总务部有责任全天候保证信息中心机房的供水供电,以及协调各楼宇物业管理公司保障接入机房的物理安全。

（五）学校各单位

学校各单位在处理网络安全事件时负责，包括:

1. 资产或使用权属于本单位的网络、设备、信息系统的应急预案制定。

2. 网络安全事件定级、处置及上报信息中心,配合信息中心做更加深入的处置。

3. 负责组织本单位的网络安全应急预案的培训教育工作。

4. 负责组织本单位的网络安全应急预案演练，并参与全校范围内的网络安全事件预案演练。

网络安全事件应急工作的有关校外单位包括：

（一）管理部门

包括教育部科学技术与信息化司、安徽省教育厅、省公安厅网警总队、省国家安全局、省保密局、合肥市公安局网警支队、安徽省互联网应急中心，分别为教育行业、公安机关以及本地区互联网的网络安全监管、监测、预警、协调部门，主要负责：

1. 当发现我校存在网络安全事件，将以电话、电子邮件、公文等各种形式通知我校，并通过网络安全管理平台对有关事件进行管理。

2. 接收我校在事发、事中、事后处理报告及整改结果。

（二）服务提供商

包括网络和信息系统的运维服务提供商、云服务提供商、物业公司等，应签订安全责任书，在应急处置过程中提供相应协助。

（三）供应商

包括设备提供商、软件厂商、运营商、电力等，应保持经常联络与协作，在应急处置过程中提供相应协助。

第十条 监测与预防

（一）应立足于以防为主策略，完善机房管理制度，对关键机房实施7×24小时监控,实施进入登记制度,禁止任何非授权人员进入，每天定期巡检。落实防火、防水、防盗、防雷电、防静电等技术防范措施，建设安全、可靠、稳定运行的机房环境。电力、UPS、电池、空调等动环设备必需定期巡检、检修。定期针对防火、动环故障处置、人员疏散进行培训及演练。

（二）核心设备和互联网、校区/校园互联线路应有备份，避免单点故障。保证核心网络设备安全,及时升级固件。禁止未授权访问，不同层次的管理员实行分权管理。设备系统日志、操作日志必需符合法律、法规要求。实时监控核心设备及通讯链路，及时发现并排除故障。

（三）做好系统及设备的配置管理，配置管理应遵循“最小配置”原则，定期对系统及应用进行病毒扫描、漏洞扫描，及时修复系统及应用安全漏洞，做好数据备份，对关键的系统需要建立灾难性数据备份与恢复机制。操作系统及应用系统日志必需符合法律、法规要求。实行网站备案制度，重要网站及重要信息系统必须要有防火墙（网络防火墙、应用防火墙）、入侵防护系统的保护。定期对系统账号权限、数据库访问进行审计。

（四）对重要信息系统必须实行监控机制,及时发现并解决问题。定期对网站及信息系统应用扫描及渗透测试,及时发现安全漏洞并修补。

（五）信息中心应加强对校园网络与应用的监控和安全管理。特定时期，可根据需要进行统一部署，加大对校园网及信息系统监控力度，及对网络和信息系统采取加强性保护措施。

第十一条 应急响应流程

事件发现与判定:

（一）事件发现

部分网络安全事件具有非常高的隐蔽性,及时发现网络安全事件

是非常重要的，网络安全事件的发现可分：从内部发现及外部发现两种情况。所谓内部发现，就是由校内的用户、网络与信息系统管理员或各种安全管理监测系统（监控系统、防火墙、入侵保护系统、反病毒系统）发现。外部发现通常由外部安全管理监测系统发现，并通过网络安全紧急响应机制通知信息中心。

（二）事件判定

安全事件采取自主判定原则，按“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，由信息资产的管理、运维单位根据事件类型、网络或信息系统重要程度、损失情况以及对本校和社会造成的影响程度判定安全事件。各单位可提请信息中心提供技术支持，对疑似的安全事件进行判定。

响应流程详见“合肥工业大学网络安全事件处理暂行办法细则”。

第五章　其他

第十二条 人事变动报告。合肥工业大学下属二级机构的信息技术安全工作主管领导和网络安全与信息化专员及其联络方式发生变更的，应及时报告信息化中心。

第十三条 相关配套机制。信息化中心建立健全本部门安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练；根据实际建立本部门值守制度，按照安全事件应急处置流程执行，做到安全事件早发现、早报告、早控制、早解决。

第十四条 问责机制。各部门应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，将对相

关部门进行约谈或通报。

第六章　附则

第十五条 本办法由校网络安全与信息化建设领导小组办公室负责解释。