首都经济贸易大学后勤基建处文件

首经贸勤〔2024〕1号

关于印发《后勤基建处信息化网络管理办法（2024年修订）》的通知

各中心、办公室:

经2024年5月6日后勤党政联席会议讨论通过，现将《后勤基建处信息化网络管理办法（2024年修订）》印发给你们，请遵照执行。

后勤基建处

2024年5月6日

后勤基建处信息化网络管理办法
（2024年修订）

第一章 总　则

第一条 为全面提高后勤基建处系统信息化水平，为“数字化办公和生产”提供信息技术支撑，依据国家《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2019号），参考《首都经济贸易大学信息系统及服务器管理办法》和《首都经济贸易大学校园网管理条例》等，结合后勤基建处系统实际，制定本办法。

第二条 本办法适用于后勤综合信息系统以及向网络信息中心申请备案的其他未列入系统。

第二章 管理职责

第三条 成立后勤基建处信息化领导小组，全面负责信息安全工作。信息化领导小组是后勤信息化网络安全最高管理机构，具体分工如下:

组　长：后勤党委书记、后勤基建处处长

副组长：后勤基建处副处长

组　员：各中心、办公室主要负责同志

信息化领导小组办公室设在综合办公室，直接对信息化领导小组负责，负责协助主要负责人对信息系统实施方技术人员的身份、背景、专业资格和资质等进行审查，并作为信息安全

管理工作的职能部门负责专职安全管理员、专（兼）职审计管理员、系统管理员及网络管理员的指派，定义各岗位职责。信息化网络安全各岗位负责人员由办公室授权后生效。

第四条 信息化领导小组的职责为:

1.信息安全管理: 确定后勤基建处信息安全工作的总体方向、总体原则和安全工作方法，批准后勤综合信息系统安全策略及发展规划，确定各中心、办公室工作职责，领导并监督各项安全工作的实施，对重要安全事件的处理进行决策;

2.信息安全风险控制: 审核后勤综合信息系统风险评估方案，并授权网络信息中心实施风险评估，对所提出的整改意见进行组织协调，落实相关风险控制措施;

3.制度制定及发布: 负责规划、监督、指导信息安全安全管理制度体系文件的起草、审查、发布、清理等，提供充足的资源和支持，确保安全管理制度体系能持续恰当有效运作，并持续改善安全管理制度体系;

4.制度评审及修订: 主持并监督后勤基建处信息化网络管理制度的管理评审，确保评审会议所提出行动项目在规定时间完成;

5.信息系统安全保护: 负责信息安全工作的监督、检查、指导，协调各中心、办公室协同工作，支持和推动信息安全保护工作在后勤基建处实施;

6.信息系统建设及变更: 负责对信息系统的安全建设进行

总体规划，制定近期和远期的安全建设工作计划，信息系统项目实施方案审批、过程管理及测试验收，影响重要业务功能、影响网络性能以及影响整体形象的重大系统变更审批;

7.信息系统安全事件管理: 定期审阅安全事件报告，统筹较大、重大及特别重大安全事件处理。

第五条 后勤基建处主要负责人任信息化网络安全主管，是信息化网络管理第一责任人，其具体职责包括:

1.负责后勤基建处网络信息安全的管理、监督、检查;

2.负责后勤基建处网络系统及平台的规划和建设;

3.负责后勤基建处网络发布信息的审核，确认信息是否发布;

4.负责后勤基建处安全管理员、审计管理员、系统管理员及网络管理员的培训。

第六条 安全管理员的岗位职责为:

1.定期组织信息系统漏洞扫描和信息安全风险评估工作，形成信息系统和整体安全现状报告，并向信息化领导小组进行汇报;

2.负责制定信息系统总体网络访问控制策略和规则，并对其进行监控和审计工作，定期发布策略执行情况;

3.对网络、系统、审计管理员进行安全指导;

4.定期收集信息安全漏洞和公告信息，告知相关安全运维管理人员;

5.协调信息安全应急响应组织和技术支撑单位。

第七条 安全审计员的岗位职责为:

1.定期审计信息系统信息安全策略执行情况，收集信息系统日志和审计记录，并提供审计报告;

2.对安全、网络、系统、应用、数据库管理员的操作行为进行监督，安全职责落实情况进行检查。

第八条 系统管理员的安全职责为:

1.依照网络信息中心扫描结果进行漏洞修补，确保安全补丁保持2个月内最新补丁;

2.对系统进行日常安全运维管理，定期更改系统账号，并定期提交安全运行维护记录或报告;

3.在发生系统异常和安全事件时，对系统进行应急处置。

第九条 网络管理员的安全职责为:

1.依照网络信息中心要求进行漏洞修补;

2.在发生系统异常和安全事件时，及时发现上报网络信息中心，对网络设备、安全设备进行应急处置。

第十条 关键事务岗位应配备多人共同管理，定期轮岗，关键岗位人员配备坚持“权限分散、不得交叉覆盖”的原则，安全管理员和安全审计员不能由一人身兼。

第十一条 信息系统的安全技术岗位可由其他相关管理员兼任，其中网络安全管理、系统安全管理等工作可分别由网络管理员、系统管理员执行。

第十二条 重要业务系统操作人员应在日常工作中认真执行信息系统安全策略和技术安全规范中的各项要求。

第三章 制度管理

第十三条 综合办公室负责组织信息化网络相关制度文件的起草、编制、修订、补充等，并将实施成果向领导小组汇报。综合办公室应确定一名熟悉相关内容职工为负责人，涉及多部门时牵头组建联合小组共同起草。

第十四条 各安全岗位人员负责依据信息化网络相关制度文件的内容进行宣贯、培训、执行、检查、落实等，同时负责协助评审进行以及制度的实施修订。

第十五条 报审制度应由起草部门负责人签署后报信息化领导小组审查。多部门联合起草的，应由起草部门负责人共同签署后报信息化领导小组审查。信息化领导小组对送审稿提出审查结论，对草案涉及的有关争议问题以及修改情况作重点说明，并由信息化领导小组负责人签署书面审查报告反馈起草部门。

第十六条 制度草案经信息化领导小组审议且原则通过后，起草部门根据审议中提出的修改意见对草案进行修改，经信息化领导小组签发,以管理制度规范形式公布。

第十七条 文件发布遵照统一格式，进行版本控制。

第四章 系统审批及信息发布

第十八条 物理访问、系统接入等其他对信息系统（包括业

务网、主机房、各业务信息系统）的访问和修改操作，均由系统使用部门主任或其授权的其他人员负责审批并监督后续的访问过程。

第十九条 重要操作，如业务系统功能上的重大调整、重大升级变更、网络架构大的调整，均需要由系统涉及部门主任召集相关人员论证后初审，初审的结果报信息化领导小组做最后审批后进行。

第二十条 系统变更分类与审批原则：

1.信息系统变更主要分两大类别：功能优化类变更和系统完善类（bug 修订，补丁修复）变更;

2.功能优化类变更发起人为各中心、办公室业务经办人员;

3.系统完善类变更的发起人为各中心、办公室业务经办人员、系统管理人员;

4.两类变更的审批办法和流程基本一致，需要有效识别各类系统变更的风险，并严格按照审批程序有效规避风险、落实相关责任方。

第二十一条 系统变更审批流程如下：

1.变更由上述变更发起人发起，根据变更的具体内容填写相关的变更管理表单;

2.功能优化类变更审批由业务经办部门主任审批后，报主管处领导及后勤基建处主要负责人审批;

3.功能优化类变更审批初审通过后，由综合办公室安排专

人评估变更的风险和可行性，如评估结果可行，交由系统运维人员具体实施，完成系统变更。

第二十二条 系统完善类变更由系统管理员发起，要求系统管理员在发起变更的同时，需要就本次变更潜在风险和风险规避措施进行描述，报请后勤基建处主要负责人进行审批后具体实施完成变更。

第二十三条 各办公室、中心的所有请示，需上传至后勤管理系统 2.0，经办公室主任、主管（副）处长以及处长审核通过后方可实施。

第二十四条 针对通过处长信箱（邮箱）及微信公众平台途径收集的师生反馈信息，网络信息管理员需及时告知相关科室或中心负责人审核并根据落实情况进行回复。对于无法落实的信息，回复中需明确原因。

第二十五条 后勤基建处网站及各新媒体平台发布内容，需遵照后勤基建处网络信息发布流程进行发布。

第二十六条 后勤基建处网络信息发布流程：

1.各办公室、中心拟稿，经本部门负责人及主管（副）处长审核后，发送至办公室网络管理员；

2.网络信息管理员对内容进行初步审校后，报送办公室主任审批；

3.后勤党委书记进行审定，对通过的内容批准发布；

4.网络管理员通过网站或新媒体平台等途径发布。

第五章 内部沟通管理

第二十七条 信息化领导小组定期组织信息安全专题会，参会人员至少要包括后勤基建处主要成员和执行层涉及管理人员。在发生小范围内信息安全事件时，办公室可根据实际需要随时召集发起信息安全工作会，就信息安全管理各项制度和执行情况做出及时调整和部署。

第二十八条 信息安全专题会应就网络信息中心反馈问题进行通报，讨论提出解决办法和规避措施，对运维人员的工作内容进行确认和审核。

第六章 人员安全及培训

第二十九条 人员录用应通过后勤基建处审核。录用部门应明确被录用人员的安全技能要求，在录用过程中依据技能要求进行考察，对被录用人的身份、背景、专业资格和资质等进行审查，安全管理员、安全审计员、网络管理员、系统管理员等关键岗位人员，需要签订保密协议。

第三十条 违反制度的职工，依照其违规程度及影响，适度进行惩戒，情节严重的解除劳动合同。

第三十一条 对关键岗位转岗人员需在保密承诺文档上签字，承诺相关保密义务，所在部门及时上报主管（副）处长及主要负责人，所有相关领导在保密承诺文档签字可办理转岗手续。

第三十二条 离职人员由所在部门及时上报相关领导，获得

相关领导签字的保密承诺文档后才能办理离职手续，设备上保留数据应进行安全处理，包括备份需要留存的数据以及删除不必要的数据，及时联系相关二级单位在相关系统中取消离职者的权限，禁用账户，释放相关资源。

第三十三条 定期对系统用户进行网络安全培训，明确信息安全体系及个人安全职责，以加强对有害信息的识别能力及防范能力。对网络信息管理员的培训内容，还应涵盖国家及学校关于网络安全的相关规定。

第三十四条 对单位安全管理员和系统管理员定期开展由供应商或厂家提供的专业安全技术培训及网络安全相关规定培训，帮助安全管理人员和系统管理员了解掌握系统管理。

第七章 信息系统建设

第三十五条 与外单位的外包（服务）合同应明确规定合同参与方的安全要求、安全责任和安全规定等相关安全内容，并采取相应措施严格保证对协议安全内容的执行。

第三十六条 信息系统建设项目实施之前，由外包单位制定详细的项目实施方案，实施方案需要经信息化领导小组批准认可后方可实施。项目实施方案应包括项目时间限制、进度控制和质量控制等方面内容，项目实施单位在实际项目实施中应按照项目实施方案内容对项目实施过程进行进度和质量控制，并定期向后勤基建处提交阶段性项目报告等文档。

第三十七条 在项目实施过程中，使用主动控制的方法：

1. 预测和估计潜在的风险，在问题发生之前采取有效的防范措施;

2. 评价项目的现状和进展趋势，分析其影响并提出建设性意见;

3. 对项目状态持续不断的跟踪、监测，有效而经济地预防意外事故。

第三十八条 项目进度控制措施:

1. 组织措施:

(1) 明确项目控制人员的具体职责;

(2) 进行项目工作结构的分解，创建控制时间;

(3) 确定项目进度工作制度，如项目控制会议;

2. 经济措施: 确保项目资金的提供;

3. 信息管理:

(1) 对影响项目进度的干扰和风险因素进行分析;

(2) 进行计划进度和实际进度的比较;

(3) 定期制作各种进度情况报告。

第三十九条 质量控制关键点:

1. 加强质量意识: 提高所有实施人员特别是负责人的质量意识;

2. 明确质量责任: 项目经理级有关部门负责人和项目组成员明确在保证项目质量工作中的责任;

3. 提高人员素质: 选择满足实施需求且高质量的人员组建

项目组;

4.制定质量标准：建立一套完整的质量标准化体系，根据项目计划工作内容由责任人逐一制定。

第四十条 项目质量的保证措施:

1.项目总体目标明确、清晰、量化。如果项目实施过程发生变化，要重新考虑项目目标;

2.将项目总体目标分解为阶段目标，并将工作任务分解为最小单位;

3.根据工作任务，在计划中设定检查控制点;

4.对每项工作任务进行评价，并对各种问题进行总结;

5.评价整个项目。评价总结工作在项目结束后进行，目的是系统分析项目工作成果是否达到项目目标要求。

第四十一条 项目风险控制和管理:

1.风险识别：确定各阶段工作的风险种类、对项目的影响;

2.风险量化：对风险及风险产生的影响进行评估;

3.应对计划：制定风险管理计划，采取措施增大制约风险的机会;

4.风险控制：不断对风险管理计划进行更新，并对风险因素采取预防和纠正措施。

第四十二条 项目执行过程中必须严格执行项目计划，尽量避免项目需求变更和人员变更。如果出现不可预知的因素导致项目变更，必须及时调整项目目标、项目计划，并通知信息系

统项目管理人员签字确认。

第四十三条 信息化领导小组负责信息系统测试验收，由系统建设实施单位项目经理与信息化领导小组共同拟定《系统验收计划》以及《系统交付清单》，确认《系统验收计划》和《系统交付清单》后，系统建设实施单位派出代表和验收小组一起进行项目验收。验收完毕后，验收小组在《项目验收报告》上签字确认。《项目验收报告》中需要给出测试通过的结论，如果报告中提出了存在的问题，项目要继续建设。

第八章 信息资产管理

第四十四条 后勤基建处信息资产具体分为:

1.主机设备: 各类承载业务系统和软件的计算机系统及其操作系统，包括安装在服务器上各类应用系统以及构建系统的平台软件（数据库等）;

2.网络设备: 交换机、负载均衡、光纤转换器、路由器、缓冲服务器、调制解调器、多层交换机，无线 AP、AC、BAS、Hub、RAS、VoIP 网关等构成信息系统网络传输环境的设备等构成信息系统网络传输环境的设备;

3.存储设备: 磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等;

4.安全设备: VPN 网关、防火墙、内容过滤网关、入侵检测系统、防病毒网关、加密机、安全网闸等构成信息系统信息安全环境的设备，软件;

5.数据：保存在电子媒介上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等；

6.服务：信息服务，对外依赖该系统开展的各类服务；网络服务，各种网络设备、设施提供的网络连接服务；办公服务，为提高效率而开发的管理信息系统，包括各种内部配置管理、文件流转管理等。

第四十五条 根据资产在业务价值和可用性上的赋值等级，将资产划分为五级，级别越高表示资产越重要。

级别	重要性	描述
5	很高	资产的重要程度很高，其安全属性破坏后可能导致系统受到非常严重的影响
4	高	资产的重要程度较高，其安全属性破坏后可能导致系统受到比较严重的影响
3	中等	比较重要，其安全属性被破坏后可能对组织造成中等程度的损失
2	低	不太重要，其安全属性被破坏后可能对组织造成较低的损失
1	很低	不重要，其安全属性被破坏后对组织造成非常低的损失，甚至忽略不计

等级	硬件资产	软件资产	数据资产	文档资产	备注
VH（很高）	关键	关键	内部秘密	内部秘密	对应关键业务
H（高）					对应关键业务
M（中）	重要	重要	内部公开	内部公开	对应重要业务
L（低）	一般	一般			对应一般业务
VL（很低）	一般	一般	公开	公开	对应一般业务或其他

第四十六条 各中心、办公室有责任协助综合办公室核实和维护信息资产的信息，并建立《信息系统资产清单》。信息资产属性发生变更时，各中心、办公室要及时告知综合办公室，对《信息系统资产清单》进行变更、保存、复核存档。变更包括地理位置变动、信息资产配置信息、补丁信息等变更。

第四十七条 闲置资产根据资产类别实施分类归档管理，闲置资产应在资产清单中进行标注。涉及敏感信息或资产级别 3 级以上的闲置资产应在安全管理员处进行备案。可重用的闲置资产中，内容涉及敏感信息或资产分级 4 级以上，应使其不可重用。所有资产分级 4 级及以上的闲置资产应存储在安全、保密的环境中。包含有敏感信息的介质或资产级别 3 级及以上要可靠和安全地存储和销毁,对记录纸、设备和介质提供收集和销毁；销毁敏感部件或资产级别 3 级及以上要做记录，以便保持审计踪迹。

第九章 存储介质管理

第四十八条 系统管理员负责管理的系统所属相关存储介质的标识、传递、访问、保密以及销毁等；安全管理员负责对单位相关存储介质的管理过程进行监督。

第四十九条 安装和使用存储介质时，禁止非授权访问。

第五十条 将存储介质给第三方使用，需要系统管理员确认机密信息已经删除。

第五十一条 含有内部信息的存储介质对外部人员保密，严禁第三方人员带离。当存储介质中含有机密信息、被邮递或在内部传输时，必须被放在有标记的密封套或包装盒中。机密信息被邮递或是传输到外部时，内部标签需要明确标记为机密，外盒或封套不标记机密字样。

第五十二条 含有机密信息的存储介质，要存放在保险柜保存。

第五十三条 计算机存储介质不再用于存储保密信息前，必须进行格式化。

第五十四条 存储介质的销毁首先要提交销毁申请，经安全管理员确认方可执行销毁。

第五十五条 存储介质上删除保密信息后，必须执行重复写操作防止数据恢复。

第五十六条 含有保密信息存储介质的报废处理方式是切碎或者烧毁，磁带、磁盘、光盘、硬盘等存储介质的报废处理方式为切碎或者烧毁。

第十章 安全补丁管理

第五十七条 网络管理员需根据网络信息中心反馈的系统漏洞检测结果，及时及时联系信息系统实施方技术人员安装系统补丁，并留存记录。

第十一章 恶意代码防范

第五十八条 综合办公室负责通知各部门和系统维保方进行计算机防病毒产品安装及升级办法，防病毒软件中心应设置自动扫描工作，并由安全管理员确认扫描结果。

第五十九条 各系统管理人员禁止私自安装非单位下发的防病毒软件和卸载已安装的防病毒软件或禁用其功能。

第六十条 各系统管理员禁止运行未经审核批准的软件，对于外来的（如：网络下载、可移动磁盘等介质）程序和文档，应在运行或打开前进行计算机病毒的检测和清除。

第六十一条 使用 web 方式接收电子邮件时，不得随意打开来历不明或可疑的电子邮件，须开启防病毒软件的邮件接收监控功能监控邮件附件。

第六十二条 职工在遇到或怀疑发生防病毒软件不能查杀的病毒事件，防病毒软件病毒库无法更新或防病毒运行异常时，应第一时间报告综合办公室系统管理员，由综合办公室联系网络信息中心给予技术指导。

第六十三条 职工出差所携带办公用计算机需在出差归来后进行病毒检测和查杀后方可接入网络。

第十二章 系统备份及恢复

第六十四条 业务系统备份采取定期备份与动态备份相结合的原则。定期备份按一定周期有计划进行。

第六十五条 数据备份采用增量备份，数据备份策略的制定应综合系统性能、存储容量、数据量增长速度、业务需求、备份方式、存储介质、存储介质型号、有效期等因素。备份策略的制定应考虑在特殊日、版本升级日增加备份。

第六十六条 数据备份应采用性能可靠、不宜损坏的介质，如磁带、光盘等。备份数据的物理介质应按一定的文件命名规则进行贴标签管理，注明数据的来源、备份日期、恢复步骤等信息，并置于安全环境保管。

第六十七条 数据备份时，要仔细检查备份作业或备份程序的执行结果，核实目标备份与源备份内容一致，确保备份数据的完整性和正确性。

第六十八条 数据备份时，应及时记录备份情况，包括备份作业，备份周期、时间、内容、数据保存期限，介质型号、介质容量、业务种类、转存情况、异地备份记录、相关变更记录等信息，并进行当日备份的问题记录。

第六十九条 操作系统备份要求:

1.操作系统层的备份范围包括操作系统和系统运行所产生的登录和操作日志文件;

2.操作系统应每半年至少备份一次;

3.操作系统运行所产生的登录和操作日志文件应每月至少备份一次;

4.在操作系统安装系统补丁，进行系统升级，修改系统配置或其它可导致系统改变的情况发生前后必须进行操作系统备份;

5.操作系统层的备份由系统管理员负责实施;

6.所有操作系统层的备份完成后应至少保留三次全备。

第七十条 数据库备份要求:

1.数据库层的备份范围包括数据库的日志文件、数据文件和系统程序文件。

2.数据库日志文件包括归档日志文件、告警日志文件和跟踪文件。

3.在安装数据库补丁、应用系统补丁、数据库升级或其它导致数据库改变的操作发生前后必须备份完整的数据库数据文件和数据库程序文件，备份后应执行备份介质异地存放。

4.数据库数据文件应每周至少备份一次;

5.数据库归档日志应每天进行增量备份;

6.当数据库发生故障时，如需进行系统恢复，应先备份故障数据库的数据文件;

7.数据库层备份由数据库管理员负责实施;

8.所有备份的数据库日志文件和数据库程序文件备份应至少保留六个月。

第七十一条 应用系统备份要求:

1.应用系统层备份包括应用系统程序文件和日志文件;

2.应用系统程序文件和日志文件应每月至少备份一次，备份后应执行备份介质异地存放;

3.根据补丁级别，在安装应用系统补丁前后视要求执行系统备份;

4.应用系统备份由应用系统管理员负责监督实施。

第七十二条 所有的应用系统备份应至少保留六个月。

第七十三条 在解决故障的过程中，如需恢复生产系统中的数据库环境，必须首先提出申请，获得后勤基建处主要负责人批准后才可实施。

第七十四条 数据恢复前，必须根据情况对所需要恢复的数据进行必要的备份，防止有用数据的丢失。

第七十五条 数据恢复必须严格按照相关规定执行，出现问题时由综合办公室相关人员申请网络信息中心进行现场技术支持。

第七十六条 数据恢复后，必须进行验证、确认，确保数据恢复的完整性和可用性。

第七十七条 由数据备份人员根据不同业务系统的实际拟定需要测试的备份数据项目以及测试的周期。

第七十八条 对于因设备故障、操作失误等造成的一般故障，需要恢复部分设备上的备份数据，遵循异常事件处理流程，由

综合办公室向网络信息中心申请批准后，指导第三方工程师恢复。

第七十九条 对于因灾难等原因造成的重大事故，遵循持续性管理流程，启动灾难恢复计划进行恢复。

第十三章 安全事件处置及应急处理

第八十条 综合办公室是主要安全事件受理、联系部门，负责受理信息安全事件，协调组织安全事件解决，并反馈处理结果；安全管理员是安全事件具体受理人员，负责协调组织相关人员处理安全事件。

第八十一条 各中心、办公室应配合综合办公室做好安全事件的解决，如发现安全事件，由各部门安全联络员及时上报综合办公室。

第八十二条 出现以下情况，启动突发事件应急处理机制：

1.出现信息系统重大事件的情况，包括但不限于以下情况：

(1)系统发生软、硬件故障，可能导致或已经造成业务中断；

(2)系统发生网络与信息安全事件后，原则上1个小时内依然没有解决问题的；

(3)造成重大经济损失或群体性事件的技术事故；

2.出现火灾、地震、洪水等不可抗力因素，无法正常办公和运行的情况；

3.其他因维护安全稳定等专项工作规定的，需要进行应急决策的情况。

第八十三条 突发事件报告路线:

1.报告人: 由突发事件部门负责人向后勤基建处主要负责人报告;

2.报告方式: 达到突发事件触发条件十分钟内，相关报告人必须以电话方式对上级进行工作报告。

第八十四条 信息安全突发事件发生后，根据突发事件的严重程度，由应急领导小组指定的人员及时发布相关信息，发布相关信息应严格按照信息安全事件相关通告规定和要求发布相关信息，同时其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。

第八十五条 信息安全事件发生后，应急工作小组对信息安全事件进行评估，确定信息安全事件的类别与级别。

第八十六条 根据业务信息系统突发事件的发生原因、性质和机理，业务信息系统突发事件主要分为以下三类:

1.攻击类事件: 指信息系统因计算机病毒感染、非法入侵等导致业务中断、系统宕机、信息系统瘫痪等情况;

2.故障类事件: 指信息系统因计算机软硬件故障、停电、人为误操作等导致业务中断、系统宕机、信息系统瘫痪等情况;

3.灾害类事件: 指因爆炸、火灾、雷击、地震、台风等外力因素导致信息系统损毁，造成业务中断、系统宕机、信息系统瘫痪等情况。

第八十七条 按照突发事件的性质、严重程度、可控性和影

响范围，将其分为一般故障、严重故障、重大故障、特级故障四级。

1.一般故障：信息系统中单个系统故障，但未影响业务系统运行，也未造成社会影响或经济损失的突发事件;

2.严重故障：信息系统中单个分单位节点故障导致分单位业务中断，可能造成较大业务影响或较大经济损失的突发事件;

3.重大故障：信息系统中多个分单位节点或总单位骨干节点故障引起的多个业务系统长时间中断，可能造成重大社会影响和巨大经济损失的突发事件;

4.特级故障：特指发生不可预见的灾难性事故，如火灾、水、灾和地震等。

第八十八条 当启动突发事件应急决策机制时，由相关业务部门分管（副）处长提议，经后勤基建处主要负责人同意后，综合办公室负责召集相关工作小组会议。会议由相关业务部门进行事件描述和损害程度评估，信息化领导小组成员对相关业务部门提出的评估意见、处置预案进行分析，合规管理部提出法律意见，经小组会议集体讨论一致后，形成决策处理意见交相关业务部门具体负责实施。会议决策意见由负责综合办公室形成会议纪要，合规管理部负责监督事件处理的全程。

第八十九条 信息化领导小组在以下条件同时满足时，可决定解除应急状态，并向学校报告:

1.各种安全事件已得到有效控制，情况趋缓;

2.突发安全事件处理已经结束，设备、系统已恢复运行;

3.上级应急部门发布的解除应急响应状态指令;

4.应急管理部门应及时向现场应急工作组传达解除应急状态响应的指令，恢复正常生产工作秩序。

第九十条 安全事件应急处理结束后，对本次应急安全事件进行深入的调查和评估，综合分析中存在的关键点和薄弱点，正确认识系统面临的威胁和风险，提出该类安全事件的整改措施，同时对安全事件的责任进行认定。

第十四章 检查与考核

第九十一条 后勤基建处全体职工均需遵照办法中的细则执行。对于违反本办法的办公室、中心及个人，将视情节轻重追究责任。

第十五章 持续改进

第九十二条 为保证本策略文件的时效性、可有性，需根据相关审核规定进行评审和修订，修订后重新发布。

第十六章 附　则

第九十三条 本办法由后勤基建处负责解释。

第九十四条 本办法自公布之日起施行。原《后勤基建处信息化网络管理办法（2022年修订）》（首经贸勤〔2022〕7号）废止。

后勤基建处综合办公室　　2024年5月6日印发