中国残疾人福利基金会
网络安全及信息化工作管理制度

第一章　网络安全方针

1.总则

本方针为本会网络安全管理体系的纲领性文件，明确提出网络安全管理方面的工作要求，指导网络安全、管理体系的运行建设。网络安全方针是本会领导层对网络安全目标的具体表述，为网络安全管理体系运行的所有相关文件提供指引，其它文件在制定时不得违背本文件中的规定或与网络安全方针发生抵触。网络安全方针经过网络安全及信息化工作领导小组讨论通过。

本方针适用于本会网络安全相关的各项活动。

2.范围

本方针的管理范围包括本会及相关业务所拥有、控制、管理和使用的所有硬件、软件、信息、服务、环境设施、人员和无形资产等信息资产。本方针的适用对象包括本会及其有关的集成商、软件开发商、产品提供商、顾问、商业合作伙伴、临时工作人员和其他第三方机构或人员。

3.组织与职责

各部门须执行本网络安全方针，并可依据实际情况逐步

制定与本部门相关的实施细则，网络安全及信息化工作领导小组办公室作为网络安全管理体系的具体实施部门，须制定网络安全管理体系实施细则并予以落实。

所有成员和员工须遵守网络安全及信息化工作领导小组制定的网络安全方针和相关管理制度。

4.网络安全方针

4.1 网络安全总体目标

本会网络安全管理工作总体目标是“保障业务安全运行”，具体目标为：

（1）杜绝重大网络安全事件的发生；

（2）重要信息资产的管控率达到 99%；

（3）重要业务系统的可行性达到 99%；

（4）网络安全风险识别率与控制率均达到 90%。

4.2 网络安全管理总体原则

（1）动态管理原则；网络安全管理推行管理与技术并重原则以及“计划、执行、检查、改进”动态循环管理原则；

（2）分级保护原则；必须建立合适的信息资产分级保护制度，基于“谁主管谁负责，谁建设谁负责，谁运营谁负责”的原则，确定资产责任人，落实信息资产的保护、管理责任；

（3）全员责任制原则：全体成员的参与对于网络安全工作成效至关重要，所有成员都具有其所承担工作所必须的

安全意识、知识、技术和能力。

（4）网络安全与信息化工作领导小组承诺对网络安全工作提供一切必要支持，以保护信息资产的安全。

（5）各部门配合网络安全及信息化工作领导小组办公室识别并评估本部门面临的网络安全风险，积极主动采取恰当措施予以防范。

4.3 网络安全保障体系

（1）本会的网络安全保障体系由网络安全管理组织保障、网络安全管理制度保障、网络安全技术保障、网络安全运行保障以及应急响应恢复保障五部分共同组成。并主要通过采取安全检查和审计两项措施，建立并巩固网络安全事前、事中和事后控制三道防线。最终形成管理、技术和监督并举的网络安全保障体系。

（2）网络安全组织保障：发展和完善“三级”网络安全组织。在本单位现有信息化管理组织架构的基础上，按照基于角色的层次化管理模型，建立强有力的网络安全组织架构。网络安全与信息化工作领导小组是本会网络安全决策的机构。具体关于本会的安全组织职责详见《网络安全组织管理办法》。

（3）网络安全管理制度保障：首先在本单位范围内建立网络安全管理体系文件，描述对信息资产有效安全管理方法，规定人员安全操作流程与规范，制定系统配置规格、使

用策略等。本会将依据实际情况逐步在各部门推进安全管理制度。

（4）网络安全技术保障：采用纵深防御的原则，结合“横向隔离，纵向认证”的要求，实现不同层次的身份鉴别、访问控制、数据完整性、数据保密性和抗抵赖等安全功能。

（5）网络安全运行保障：建立日常安全运行与维护机制，形成完善的运行保障机制，确保各业务和信息系统的运行稳定可靠，及时、准确、快速地处理生产问题，强调执行过程安全。

（6）应急响应保障：针对各种突发灾难事件，建立灾难恢复与业务持续性计划，形成快速响应、快速恢复的机制，能控制事态发展，保障生命财产安全，将灾难造成的损失降到本会可以接受的程度，并能迅速恢复正常生产运行状态。

（7）采取安全检查和审计两项措施，通过内部审计以及外部审计等方式，在本会内持续开展网络安全检查和审计工作。

（8）各部门在本会网络安全方针指导下，持续有效地开展网络安全管理工作。

第二章　网络安全组织管理规定

1. 总则

本办法针对本会网络安全组织的相关事务，规定了本会

的网络安全组织结构和角色职责，为网络安全管理有效性提供组织保障。本文件适用于本会。

2.网络安全组织架构

在网络安全风险约束框架下建立符合业务发展需要的网络安全管理组织架构，网络安全组织架构由网络安全管理层和网络安全执行层组成，概览如下：

组织架构

网络安全管理层——

网络安全及信息化领导小组：

组长：理事长

副组长：分管网络安全及信息化工作副理事长

成员：各部门负责人

网络安全及信息化工作领导小组办公室设在宣传活动部。宣传活动部负责人兼任网络安全及信息化工作领导小组办公室主任。

网络安全执行层——

宣传活动部网络安全责任岗人员

“集善云”平台技术服务团队

各信息系统负责人

各信息系统外包技术团队

3.网络安全管理层角色和职责

3.1 网络安全及信息化工作领导小组

网络安全及信息化工作领导小组是网络安全管理的最高决策机构，负责本会整体网络安全管理工作。制定网络安全规划和策略。负责网络安全管理的重大事项的决策和监督。

主要职责：

（1）统筹网络安全总体战略规划，审定网络安全工作的发展战略与总体规划、制度；确定网络安全目标与战略规划，领导和推动网络安全工作和发展。

（2）决策网络安全的重大事项，包括：全面负责网络安全管理工作，研究决定网络安全管理的各类重大事项、听取网络安全建设汇报和进行争议仲裁；对网络安全方针进行审核，确保其符合管理需求；决策网络安全组织，明确职责，确保网络安全工作有配套资源的保障与支持。

（3）部署网络安全检查及评估工作；保证网络安全风险的有效识别与处置、报告；评估决策网络安全管理体系，确保网络安全管理的标准化与统一性。

（4）指导组织重大网络安全事件的防范和应急处置，听取事件处置报告，推进网络安全管理应急响应机制的建立。

（5）定期召开网络安全管理体系运行工作会议，听取网络安全管理体系运行工作报告，掌握网络安全管理体系运行状况。

（6）负责对网络安全管理体系进行评审，审批和发布

网络安全方针、网络安全规定、管理办法以及与网络安全管理相关的重大事项。

3.2 网络安全及信息化工作领导小组办公室

负责网络安全管理的具体工作。负责本会整体层面的具体日常网络安全管理、建设和监督考核工作；监督各部门网络安全管理、建设和审核工作的落实。

主要职责：

（1）负责网络安全规划，从安全管理、制度防范、技术防范三个方面，建立全面的、系统的网络安全体系。

（2）负责网络安全管理体系运行日常工作，包括组织、发起网络安全相关会议，安排会议议程，组织会议材料，部署和跟踪会议决议的执行情况。

（3）负责组织制定和修订网络安全管理制度文件并提交网络安全及信息化工作领导小组审批和发布。

（4）负责根据相关管理制度，指导、管理、监督各部门网络安全建设工作的落实与开展。

（5）组织检查网络安全管理工作，跟踪与验证各部门的网络安全改进计划。

（6）负责组织开展网络安全普及教育，提高所辖人员的计算机安全意识。

（7）完成网络安全及信息化工作领导小组交办的其他工作。

3.3 各部门相关负责人

贯彻和执行网络安全及信息工作化工作领导小组的决议，配合网络安全及信息化工作领导小组办公室的检查和审计工作，推行和落实本部门的网络安全策略和控制措施。

主要职责：

（1）各部门的主要负责人系本部门的网络安全管理的第一责任人，负责本部门网络安全管理工作，负责保护本部门所拥有和管理的信息资产的安全。

（2）负责按照网络安全管理体系的要求，对本部门所拥有和管理的信息资产进行维护，包括资产的识别和分类、安全需求级别确定等工作。

（3）推动部门内安全策略和控制措施的落实，努力实践本部门网络安全管理程序。

（4）配合网络安全及信息化工作领导小组完成网络安全相关工作，并引导、推广和监督执行安全策略。

（5）配合网络安全及信息化工作领导小组制定网络安全自查内容，配合网络安全的检查、审核资料和数据的提取。

（6）负责向网络安全及信息化工作领导小组报告网络安全事件和违反网络安全规定的行为，协助对违规行为进行调查和处理。

4.网络执行层角色和职责

4.1 宣传活动部网络安全责任岗人员

执行及落实网络安全管理层工作决议，配合网络安全及信息化工作领导小组办公室开展具体工作。

（1）与网络安全属地管理单位进行日常工作衔接。

（2）接收、传达网络安全及信息化工作文件，并进行有效解构。

（3）撰写并上报年度网络安全自查、迎检工作推进方案。

（4）密切关注网络安全相关事态发展，并进行分析，完成向各部门进行预警的工作。

（5）完成“集善云”平台日常运维工作。

（6）完成其它网络安全及信息化工作。

4.2“集善云”平台技术服务团队

配合宣传活动部网络安全责任岗人员完成“集善云”平台日常运维技术环节工作，并做好对云平台的安全防护常规工作，并就敏感时间节点的云平台网络安全防护重点保护期组织7×24小时人员监控。

（1）完成全部云平台技术运维支撑工作。

（2）妥善保存云平台全部运行日志。

（3）完成云平台日常安全巡检，对漏洞及病毒进行每日安装补丁、查杀工作。

（4）出具云平台安全中心日报、周报。

（5）配合本会对重大网络安全突发事件进行技术决策、处置、善后等工作。

4.3 各信息系统负责人

完成所管理信息系统的日常管理工作，配合网络安全及信息化工作领导小组办公室开展具体工作。

（1）与宣传活动部网络安全责任岗人员进行日常工作衔接。

（2）提供年度网络安全自查、迎检工作中信息系统运行状况信息。

（3）接收网络安全相关事件预警信息，及时传达给信息系统外包技术团队。

（4）督促外包技术团队做好网络安全自查、漏洞及病毒处置工作。

（5）完成其它网络安全及信息化工作。

4.4 各信息系统外包技术团队

配合各信息系统负责人完成日常运维技术环节工作，并做好信息系统的安全防护常规工作，并就敏感时间节点的云平台网络安全防护重点保护期组织 7×24 小时人员监控。

（1）完成信息系统技术运维支撑工作。

（2）妥善保存信息系统全部运行日志。

（3）完成信息系统日常安全巡检，对漏洞及病毒进行每日安装补丁、查杀工作。

（4）配合本会对重大网络安全突发事件进行技术决策、处置、善后等工作。

5.对外联络机制

5.1 与政府机构保持联系

当发生重大安全事件时，由网络安全及信息化工作领导小组办公室在必要时代表本单位与网络安全属地管理单位及相关政府机构联络，处理任何需要政府机构介入的安全问题。

5.2 从外部获取建议与支持

网络安全及信息化工作领导小组办公室可就以下问题向外部安全专家或特定外部组织寻求网络安全方面的建议：

（1）相关安全信息的最佳实践和最新状态的知识；

（2）网络安全管理体系的应用和维护所需的技术支持；

（3）协助进行网络安全风险评估及网络安全管理体系的建立和维护；

（4）协助并支持网络安全控制措施的制定和实施；

（5）尽早接受到关于攻击和脆弱点的警告、建议和补丁；

（6）协助进行网络安全事件及犯罪取证调查；

（7）支持并维护安全基础设施建设；

（8）分享和交换新的技术、产品、威胁和脆弱点的信息。

6.信息化项目管理中的网络安全

（1）无论什么类型的项目，项目管理中应考虑网络安全问题；

（2）网络安全要整和到组织的项目管理方法中，作为项目的一部分；

（3）项目早期阶段要进行风险评估，识别必要的控制措施；

（4）网络安全是项目每个阶段的组成部分；

（5）定期评审和处理项目管理中网络安全带来的影响。

第三章　网络安全检查与审计管理办法

1.总则

为本会对网络安全检查工作提供检查工作程序和实施依据，并通过定期进行有效的安全检查，确保信息系统安全运行，制定本办法。

本文件适用于本会内部网络安全检查与审计工作。

2.定义

（1）安全自查：指本会内部或外部机构对网络安全整体执行情况进行的自我评价活动。安全自查依据本会现行的管理制度、信息系统安全体系规范和技术标准、有关法律、法规和标准要求进行。

（2）安全例行检查：指按照已制定的检查周期所作的

检查。

（3）安全专项检查：指根据本会、监管机构或相关单位要求的安全运行状况所作的不定期的检查。

3.内容

3.1 通用要求

（1）安全自查应当遵循全面、审慎、有效、独立的原则。

（2）网络安全及信息化工作领导小组办公室应牵头建立自查机制，制定自查计划，定期开展自查活动。自查计划要根据实际情况及时进行补充和调整。

（3）应当定期对信息系统进行安全自查，自查内容应包括安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况。

（4）可根据实际需要组织专项检查，对于信息系统发生的重大事故和问题，要进行专项检查，对重大事件实施全面的监控和评价。

（5）对于新系统，包括设备、主机、应用系统上线或安装前必须经过安全测试，测试方式应包括系统安全配置，漏洞评估，恶意代码检测，根据测试结果进行整改后方可上线。

（6）必须对检查工具、检查过程信息和检查结果信息的使用和访问采取控制措施加以保护，以防止任何可能的风

险。

3.2 安全自查准备

（1）网络安全及信息化工作领导小组办公室应协调组织相关部门或人员根据网络安全相关的国家法律法规、发布的相关制度和技术标准、业界规范标准确定安全检查内容和安全自查方案。

（2）网络安全及信息化工作领导小组办公室应协调相关各部门或第三方服务商对安全自查方案进行测试，必要时可进行安全检查的风险论证。

（3）网络安全及信息化工作领导小组办公室应明确检查要点、检查方式、检查工具、检查所涉及的范围和检查所需配合单位，报网络安全及信息化工作领导小组进行审批。

3.3 安全自查实施

（1）网络安全及信息化工作领导小组办公室应组织相关部门或人员按照自查周期进行安全例行检查，根据需要组织安全专项检查。

（2）安全自查应按照所规定的检查要点、检查方式、使用规定的检查工具进行检查。

（3）应选择对各信息系统运行影响最小的方式和时间进行检查。

（4）安全自查可采用抽查的方式进行，抽查的采样量应能确保安全检查结果的准确性、代表性并符合系统实际运

行情况。

（5）自查过程中应做好检查结果的记录工作。

3.4 安全自查报告

检查完成后由网络安全及信息化工作领导小组办公室负责组织编写自查报告并提出整改建议。

3.5 安全自查整改

（1）相关部门应按照检查报告中整改的时间要求，针对检查报告中所提出的问题制定整改实施计划并组织整改。

（2）网络安全及信息化工作领导小组办公室应对整改措施的落实情况进行跟踪，验证整改措施的实施结果是否有效，必要时可进行复查确认。

3.6 检查工具的使用

（1）在安全检查过程中如果需要使用安全工具，只能使用经过审核过安全工具。

（2）安全检查工具只能在检查设备或者被检查的设备上运行，并由检查人员负责操作。

（3）在信息系统中使用检查工具前，各信息系统管理人要组织进行测试工作，对其可能产生的影响进行评估和论证。

第四章　网络安全风险评估管理办法

1.总则

本办法定义了本会在开展网络安全风险评估工作过程中的风险识别、评估和处置的标准、方法和程序，规范了各部门进行信息安识别和风险处置的工作流程。

本文件适用于本会的风险评估活动及相关资质第三方。

2.内容

2.1 流程

信息资产风险评估过程为五个阶段：启动、信息资产分类分级、风险识别与评价、风险处置计划与实施、风险评估的持续改进。

2.2 标准及方式

按照 GB20984-2007 标准，本会每年至少进行一次信息资产风险评估活动，由网络安全及信息化工作领导小组办公室负责组织各部门完成。信息资产风险评估活动中的具体实施活动，可以与该年度的内部或外部的安全自查、督查、审计活动结合进行，风险评估的过程数据或结论可以直接引用等级保护测评、安全自查或审计的数据或结论。

2.3 重大事件界定

当出现重大事件可能影响到信息资产的安全或出现内、外部的安全检查、督查需求时，网络安全及信息化工作领导小组办公室可组织启动局部或全部的风险评估活动，重大事件包括但不限于以下事件：

（1）有关法律法规及标准的最新要求。

（2）上级主管部门的最新要求或下达的安全检查督查要求。

（3）外部和内部的最新安全要求或提议时。

（4）业务活动出现涉及网络安全的重要变更时。

（5）信息资产的属性发生较大变化并影响到其CIA{机密性(C)、完整性(I)和可用性(A)}属性时。

（6）出现严重的安全事件并影响到信息资产的CIA{机密性(C)、完整性(I)和可用性(A)}属性时。

2.4 处置

各部门应将发现或已发生并可能影响到信息资产安全或风险的各类事件及时通知本部门负责人。

本会网络安全管理体系建设、运行情况也同时纳入到信息资产风险评估的范畴之内，将其视为宣传活动部的无形资产，在风险评估活动中对体系的符合性和体系运行的有效性进行评估。

第五章 人员安全管理办法

1.总则

本办法旨在加强本会范围内人员的网络安全管理，确保组织人员网络安全策略目标的实现。本文件适用于本会网络安全控制管理。

2.内容

2.1 内外部人员管理

（1）本规定中所指“人员”不仅包括本会的正式员工，同时包括借调、轮岗、派遣的内部人员，如：咨询、运维支持、技术支持等人员以及第三方人员，其工作内容和性质与正式员工一致。所有人员的网络安全管理应严格遵照本办法执行，并根据本办法的各项要求进行管理和考核。

（2）第三方人员网络安全管理的具体要求见《供应商管理办法》（详情见第七章）及其他相关安全管理规定文件。

2.2 人员招聘入职管理

（1）各部门应根据本部门已规划和上报的岗位设置情况，明确各岗位网络安全职责具体要求。

（2）网络安全及信息化工作领导小组对重要岗位或敏感岗位的网络安全职责要求进行统一审核和备案，根据需要配合相关部门完成人员的招聘工作。

（3）网络安全及信息化工作领导小组办公室负责确定各部门的重要岗位或敏感岗位人员名单，每年底进行更新。对于重要岗位或敏感岗位需要进行应聘人员的背景调查时，相关部门负责对其工作经历、诚信、犯罪记录等信息进行调查核实，并保存相关调查记录，格式参见《入职人员背景调查表》。

（4）新进员工签订劳动合同时，合同中应明确规定员工需承担的包括保密要求在内的网络安全责任，也可以根据

岗位情况和人员情况，与部分员工签订单独的保密协议，保密协议模板见《员工保密协议模板》。

2.3 人员在职与转岗管理

（1）员工在职期间，必须遵守本会网络安全相关管理规定，履行合同、保密协议所规定的网络安全职责，发现网络安全事件及时报告，并配合网络安全及信息化工作领导小组办公室进行事件的处理。

（2）为保证员工能够充分履行网络安全职责，网络安全及信息化工作领导小组办公室应积极开展提高员工网络安全意识与技能的各项培训，并对培训效果进行回顾。

（3）如果员工岗位发生变化，相关部门应检查重要信息资产的交接情况，并对员工转岗前后的各信息系统内的个人账号和访问权限及时进行更新。

（4）对员工在职期间违反本会网络安全管理制度的行为，本会将给予严肃处理。

2.4 人员离职安全管理

（1）员工离职时，人员所在部门应依照该员工签署的保密协议，审核其脱密期，并明确告知其在离职后的仍然有效的网络安全保密责任。

（2）员工离职时应根据员工离职交接单所列出的信息资产归还交接清单，及时交还本会相关信息资产和物品，尤其是要归还本会所有敏感资料，并由归还资产的接收部门进

行审核和确认。

（3）离职员工所在部门应及时通知相关部门关闭离职员工账号及访问权限，同时由各个信息系统的管理部门或管理人员完成该用户账号和访问权限的回收确认，包括应用系统权限、办公系统及邮箱权限等。

第六章 网络安全培训与考核管理办法

1.总则

为了提高本会所有人员网络安全意识和相关人员的安全技能，向全体人员宣讲网络安全管理的各项法规制度，将可能的风险降到最低，明确网络安全培训与考核管理过程与职责，特制定本办法。

2.内容

2.1 安全培训管理

安全培训主要包括安全意识培训、安全技能培训以及专业技术培训。

安全意识培训会因不同的对象有所调整，建议全员参与，在某些情况下可以要求有关的第三方组织参加。培训的内容可以包括：

（1）对在职成员进行必要的网络安全教育培训，让职工了解和掌握网络安全法律法规，加强全体职工的安全生产意识。

（2）为提高本会员工的综合素质，采用各种方式对职工进行内部在职培训。如举办安全知识讲座、安全知识竞赛、简报、发放宣传品等形式。

（3）在本会内组织举办定期或不定期的业务学习班。由专业人员对职工进行业务培训。

（4）根据本会业务发展需要，对相关业务骨干人员组织送培，到相关业务单位进修及相关机构委托培养。

（5）安全技能培训主要是针对信息系统使用者或管理人员进行的，如系统安全配置，安全运维等 IT 安全技术相关内容。

（6）专业技术培训是专门针对网络安全工作需要设立的，如 ISO 27001、CISSP 等专业安全培训。

（7）培训类型可采用内部培训或外部培训，由本会聘请专家顾问以及其他专业人员对职工进行培训。

（8）网络安全培训应由各部门负责人进行汇总登记（详见《网络安全培训汇总登记表》）。

2.2 安全考核管理

（1）不定期进行全面的网络安全考核，由网络安全及信息化工作领导小组办公室负责组织相关部门或人员成立考核小组进行网络安全考核工作。

（2）内部员工可以通过安全问卷的方式进行考核。

（3）网络安全考核结果应及时汇总、登记。

第七章 服务商管理办法

1.总则

本办法旨在控制本会网络安全及信息化工作的外包服务商及相关人员可能带来的网络安全及风险，加强和规范对外包服务商的网络安全管理。本文件适用于各部门针对第三方外部服务商及相关人员的网络安全管理。

2.内容

2.1 服务商安全管理

在服务商与本会开展合作前，接口部门需负责对服务商进行调查，必要时可进行资质、人员背景等，并填写《服务商调查表》，或根据本部门有关服务商合作的相关管理规定填写相应表格；也可通过工作联系单或其它方式对服务商人员的真实身份进行确认。

服务商接口部门负责识别外包服务商进入可能带来的网络安全风险，应特别注意：

（1）服务商是否有能力满足本会对网络安全风险监管的要求；

（2）服务商是否允许本会对其实施有效的网络安全管理的监督和考核；

以下为服务商的类型：

（1）网络服务提供商：提供有线、无线或其它形式的通信线路、数据链路及网络服务的单位，例如电信、移动；

（2）设备维护服务提供商：提供桌面 PC 电脑、网络设备、主机、小型机及服务器、打印机、扫描仪、空调等硬件及系统的厂商维护；

（3）软件及系统平台维护服务提供商：操作系统、应用套装软件、外购系统平台的厂商维护和问题支持，包括驻场软件开发商，即需要进入本会场所进行短期或中长期软件开发的软件开发商；

（4）咨询审计检查等服务提供商：提供各类 IT 咨询及审计、检查等服务的服务提供商，包括外部咨询单位、外部审计机构、国家等级保护检查测评单位等。

以下为可能识别出的供应商网络安全风险：

① 物理访问引起的设备、资料失窃；

② 误操作导致各种软硬件故障；

③ 资料、信息外传导致泄密；

④ 对信息系统的滥用和越权访问；

⑤ 给信息系统、软件留下后门；

⑥ 对信息系统的恶意攻击。

在本规定基础上，对于特定服务内容的供应商（包括软件和硬件等设备供应商和服务提供商、网络通信等服务提供商、IT 系统开发等合作服务提供商、咨询单位、审计和安全检查机构），还需遵循其它管理制度，实施进一步的有效管控。

对于本会涉及国家机密的计算机信息系统建设项目，服务商资质必须符合国家相关保密制度的要求。

2.2 服务商管控要求

在与服务商进行合作前，接口部门应与服务商签订服务合同或协议，并明确保密的相关要求。在合同或协议中，应明确定义服务交付物、服务交付等级以及相应的保密和安全控制要求，并对供应商提供服务的能力进行评定，必要时通过招标方式以确定合格供应商，从而降低供应商访问资产时的风险。针对供应商保密的要求应至少包括且不限于以下内容：

（1）与本会有业务往来的服务商，应承诺不泄露非公开信息；

（2）服务商应严格遵守本会现有的各项网络安全管理规定；

（3）明确在服务提供期间所涉及知识产权的归属；

（4）明确违反保密协议或保密合同的后果及责任。

针对各项服务，服务商需提供服务人员的姓名、技术能力评定、联系方式等信息，服务人员需持有效身份证明进入本会的工作现场。

服务商接口人员应将本会和本部门现有的安全管理规定要求及时全面地对服务商进行告知，并对后果和责任进行充分说明。

2.3 服务商人员管控要求

对服务商人员的操作管理要求如下：

（1）服务商人员使用的任何设备必须经由本会认可；

（2）服务商人员使用的接入设备必须与内部网络进行物理或逻辑隔离，或者遵照本会的相关规定执行；

（3）服务商人员工作期间，应确保本会的各类设施资源的完整性；

（4）服务商人员如有需要接入内网，应向接口部门提交申请，接口部门应依据相关规定和具体情况进行处理；

（5）应当对服务商人员的逻辑访问权限实施最小访问原则，接口部门定期对其权限进行检查；

（6）当服务完成之后，服务商人员离开时，供应商接口部门或接口人员应及时通知本会相关部门，关闭供应商人员的帐户和所有访问权限；

（7）服务商人员有责任关注并及时报告系统或服务中已发现或疑似的安全弱点或技术薄弱点；

（8）服务商人员不得私自拷贝信息系统中的任何数据和程序；

（9）服务商人员不得私自将信息系统的软硬件携入与携出所在信息系统的运行场所；

（10）服务商人员未经允许，不得使用任何信息系统；

（11）供应商人员使用信息系统必须遵守《信息系统帐

号管理规定》;

（12）供应商人员必须保证信息系统账号的安全，不能泄露给无关的第三方;

（13）服务商密码管理必须遵守《信息系统密码管理规定》;

（14）服务商人员不得擅自进入非指定的区域，各部门可根据实际情况针对供应商人员进出重要场所制定相应的管理细则。

（15）服务商人员因工作需要借用本会敏感数据或重要数据的，应向接口部门提交申请并由相关部门进行审批;

（16）服务商人员所借用的数据信息应遵循明确的使用期限，并到期及时删除相关数据。

2.4 服务商服务交付检查与应急

（1）网络安全及信息化工作领导小组办公室负责服务商的整体管理，各部门接口人员和接口部门负责服务商的具体日常管理工作。

（2）对于关键软件开发商，相关部门负责人对其进行重点检查和管控。必要时可要求服务商提供其在网络安全管理方面的资证材料并对服务商进行实地考察，以验证其提供合同承诺的服务和安全保障的能力。资证材料包括企业的相关资质证书、服务商人员的个人资质证书等。

（3）服务商接口部门应负责监督、管理和检查供应商

服务交付的质量，作为本会对服务商在合同执行期间服务交付质量的考核依据，用以保证服务商服务及交付的质量和安全性。

（4）对于服务商外包开发商所交付的软件产品，应进行软件安全性的评估。

（5）网络安全及信息化安全领导小组办公室应对服务商进行定期网络安全检查，以确保本规定、相应保密协议等网络安全控制措施的有效落实，该检查每年至少进行一次，检查结果应及时报备网络安全及信息化安全领导小组。

（6）对于不符合本规定要求的情况，接口部门应责令服务商采取整改措施，并及时通知网络安全部；情节严重时，应通知网络安全领导小组办公室等相关部门根据合同或者协议采取相应处罚，直至终止与服务商的合作和追究其相关法律和经济责任。

第八章 信息系统等级保护管理办法

1.总则

本办法是为了规范网络安全等级保护管理，提高网络安全保障能力和水平，维护信息系统安全运行，保障和促进信息化建设，根据公通字2007[043]网络安全等级保护管理办法，特制定本规定。

本规定适用于本会信息系统等级保护建设过程，管理对

象为等级保护建设过程中所有管理人员、维护人员、使用人员。

2.内容

2.1 系统定级

（1）信息系统定级坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

（2）信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

（3）根据《GB/T 22240 网络安全等级保护定级指南》中等级保护定级因素对系统进行定级。

（4）网络安全及信息化工作领导小组办公室指定各部门负责人编写信息系统定级报告，并组织相关人员和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。

（5）审定通过的定级报告报送相关等级保护主管部门进行审批。

2.2 安全方案设计

（1）安全方案设计阶段的目标是根据信息系统的划分情况、信息系统的定级情况、信息系统承载业务情况，通过分析明确信息系统安全需求，设计合理的、满足等级保护要求的总体安全方案，并制定出安全实施计划，以指导后续的信息系统安全建设工程实施。对于已运营（运行）的信息系统，需求分析应当首先分析判断信息系统的安全保护现状与等级保护要求之间的差距。

（2）网络安全及信息化工作领导小组办公室协调相关部门和人员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。

（3）网络安全及信息化工作领导小组办公室协调相关部门和人员根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总

体建设规划和详细设计方案。

（4）网络安全及信息化工作领导小组办公室负责组织信息系统管理部门和有关安全技术专家对系统安全设计方案进行评审和论证。(见表:《系统安全设计方案评审表》)

2.3 系统建设

（1）产品采购和使用应按照国家相关部门要求和本会相关管理制进行产品采购。

（2）对于自行、外包软件开发过程参考《软件开发安全管理规定》进行管理。

（3）系统建设完成后可委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，对不符合等级保护要求的及时进行整改，并形成测试验收报告。

（4）网络安全及信息化工作领导小组办公室负责对第三方测试单位进行管理，并按照《服务商管理办法》对第三方人员行为准则进行严格管理。

（5）网络安全及信息化工作领导小组办公室组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认《系统测试验收报告评审表》。

2.4 系统备案

（1）已运营（运行）的第二级以上信息系统，应当在

安全保护等级确定后30日内，由网络安全及信息化工作领导小组办公室的相关人员到公安机关办理备案手续。

（2）新建第二级以上信息系统，应当在投入运行后30日内，由网络安全及信息化工作领导小组办公室的相关人员到公安机关办理备案手续。

（3）办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：

系统拓扑结构及说明；

系统安全组织机构和管理制度；

系统安全保护设施设计实施方案或者改建实施方案；

系统使用的网络安全产品清单及其认证、销售许可证明；

测评后符合系统安全保护等级的技术检测评估报告；

信息系统安全保护等级专家评审意见；

主管部门审核批准信息系统安全保护等级的意见。

2.5 系统测评

（1）测评机构应具有国家相关技术资质和安全资质的测评单位进行等级测评，第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：

在中华人民共和国境内注册成立（港澳台地区除外）；

由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

从事相关检测评估工作两年以上，无违法记录；

工作人员仅限于中国公民；

法人及主要业务、技术人员无犯罪记录；

使用的技术装备、设施应当符合本办法对网络安全产品的要求；

具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

对国家安全、社会秩序、公共利益不构成威胁。

（2）网络安全及信息化工作领导小组办公室相关人员负责对测评机构等级测评过程进行管理，负责对测评人员安全保密进行要求，必要时与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

（3）在系统运行过程中，应定期进行等级测评，三级及三级以上系统至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。

（4）在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。

2.6 系统终止

（1）信息系统被转移、终止或废弃时，由接口部门组织系统管理人员提出系统终止申请（见表《系统转移、终止或废弃申请表》），由网络安全及信息化工作领导小组办公室

进行审批，方可执行系统转移、终止或废弃。

（2）审批通过后由接口部门对系统所属软、硬件和介质等敏感信息按照相关规定进行处理(详见网络系统运维管理总则第二章)。

第九章 信息系统应急预案

1.总则

为提高本会处置网络与信息安全事件的能力，建立科学、有效、反应迅速的应急工作机制，提供一个应对网络和信息安全事件的应急响应计划框架，帮助做好网络和信息安全事件响应处理的准备，明确应急处理小组和人员的职责，以便在紧急情况下能够有序地、快速地处理网络和信息安全事件，恢复关键信息系统的服务，尽量降低业务所受的影响和信息资产遭受的损失，特编制本预案。

2.编制依据

本预案编制依据包括：《中华人民共和国计算机信息系统安全保护条例》、《国家网络与信息安全事件应急预案》、《计算机病毒防治管理规定》、《信息安全事件分类分级指南》（GB/Z 20986—2007）等。

3.分类分级

本预案所称网络与信息安全事件，是指本会重要信息系统突然遭受不可预知外力的破坏、毁损、故障，发生对组织

生产、经营、资金造成或者可能造成重大危害，危及安全的紧急事件。

3.1 事件分类

根据网络与信息安全事件的发生过程、性质和机理，网络与信息安全事件主要分为以下三类：

（1）自然灾害。指地震、台风、雷电、火灾、洪水等引起的网络与信息系统的损坏。

（2）事故灾难。指电力中断、网络损坏或是软件、硬件设备故障等引起的网络与信息系统的损坏。

（3）人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏；以及未授权访问、不当应用、恶意对数据进行截取、篡改等，造成数据和信息的泄露和系统的损坏。

3.2 事件分级

根据网络与信息安全事件的可控性、严重程度和影响范围，一般分为四级：Ⅰ级(特别重大)、Ⅱ级(重大)、Ⅲ级(较大)和Ⅳ级(一般)。国家有关法律法规有明确规定的，按国家有关规定执行。

（1）Ⅰ级(特别重大)。重要网络与信息系统发生全组织性大规模瘫痪，事态发展超出信息科技中心的控制能力，对组织安全、生产秩序、经济活动和正常经营造成特别严重损害，或社会影响特别恶劣的事件。

（2）Ⅱ级(重大)。重要网络与信息系统造成全组织性瘫痪，对组织安全、生产秩序、经济活动和正常经营造成严重损害，需要跨部门、跨地区协同处置的事件。

（3）Ⅲ级(较大)。某一区域或组织下属某机构的重要网络与信息系统瘫痪，对组织安全、生产秩序、经济活动和正常经营造成一定损害，但不需要跨部门、跨地区协同处置的事件。

（4）Ⅳ级(一般)。重要网络与信息系统受到一定程度的损坏，对组织或下属机构有一定影响，但不危害组织安全、生产秩序、经济活动和正常经营的事件。

4.适用范围

本预案适用于本会范围内发生的网络与信息安全事件和可能导致网络与信息安全事件的应对工作。

5.应急预案体系

（1）本会各部门应加强信息系统安全防范意识，明确岗位职责、人员分工以及应急程序。应急预案要按照实际情况，定期修改完善。

（2）本会网络安全及信息化工作领导小组办公室应积极指导、协助各部门做好信息系统安全管理工作和重大事件的紧急应对及处理工作。由网络安全及信息化工作领导小组办公室负责运行和维护网络和信息系统突发事件应急体系，与相关部门联合建立应急机制。

6. 工作原则

（1）预防为主。立足安全防护，加强预警，重点保护基础信息网络和关系组织安全生产、资金、日常经营活动的重要信息系统，从预防、监控、应急处理、应急保障和打击犯罪等环节，在法律、管理、技术、人才等方面，采取多种措施，充分发挥各方面的作用，全组织共同构筑网络与信息安全保障体系。

（2）快速反应。在网络与信息安全事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

（3）安全第一。把保障组织利益以及生产、经营的安全作为首要任务，及时采取措施，最大限度地避免遭受损失。

（4）分级负责。按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”以及“条块结合，以条为主”的原则，建立和完善各级安全责任制及联动工作机制。根据部门职能，各司其职，加强部门间协调与配合，形成合力，共同履行应急处置工作的管理职责。

（5）常备不懈。加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发公共事件应急处置的科学化、程序化与规范化。

7. 角色和职责

7.1 网络安全及信息化工作应急领导小组

负责整体领导重大信息安全事件处理和决策工作，必要时可以调配人力和物力资源；同时保持和组织主要领导以及上级部门的及时沟通，并批准对外发布相关的信息，具体职责如下：

（1）对网络和信息安全事件应急管理工作进行指导、检查和监督；

（2）综合协调组织网络和信息安全事件接警和处置的协调工作；

（3）传达上级领导机关和领导小组指示，传达相关信息；

（4）必要时，做好新闻媒体访问的接待工作和对外新闻发布工作；

（5）必要时，向国家和上级主管部门报告网络和信息安全事件的发生情况；

（6）协调推进各部门应急体系建设和应急预案的编制、修订等。

领导小组组长由网络安全及信息化工作领导小组办公室主任负责，成员为各部门负责人。

7.2 网络安全及信息化工作应急响应小组

在领导小组的统一指挥下，负责处理网络和信息系统中突发安全事件的处理，具体职责如下：

（1）组织范围内网络和信息安全事件的日常运行管理和接警、应急处置工作；

（2）及时向应急响应小组领导和应急领导小组汇报网络和信息安全事件的预警和事件发生、处置情况；

（3）组织编制、修订各部门应急预案和各系统、网络安全事件应急处置手册；

（4）负责网络和信息安全技术的跟踪、引进和部署；

（5）负责建立和完善网络和信息安全事件检测预警网络，跟踪政府主管部门关于有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件等方面的预警，并积极布置落实各类预防措施。

应急响应小组组长由宣传活动部负责人担任，成员为宣传活动部相关人员。

应急响应小组成员应熟悉信息系统安全标准、网络、系统环境和应急响应流程，并且定期参与应急响应计划的演练。

应急响应小组负责安排人员 7×24 小时值班，做好组织网络和信息安全事件的接警、转报工作以及记录工作。

8.内容8.1 预防预警

（1）预防措施

各部门要认真做好网络和信息安全事件的风险评估和隐患排查工作，及时采取有效措施，避免和减少网络和信息安全事件的发生及其危害。

（2）监测

各部门要进一步完善网络与信息安全事件监测、预测、预警制度。各部门应建立网络和信息系统安全管理组织架构，确定各部门信息员为系统安全专（兼）职管理人员。要落实责任，制定本部门信息通报工作制度。按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全事件和可能引发网络与信息安全事件的有关信息的收集、分析判断和持续监测。

（3）预警分级

按照网络与信息安全事件可能造成的危害、紧急程度和发展态势，预警级别分为四级：I 级（特别严重）、II 级（严重）、III 级（较重）和 IV 级（一般），依次用红色、橙色、黄色和蓝色表示。

Ⅰ级预警（红色）。指发现新的网络与信息安全威胁，可能影响组织所有网络和重要信息系统，并有扩散到外部的可能性。

Ⅱ级预警（橙色）。指发现新的网络与信息安全威胁，可能影响组织基础运营网络或重要信息系统的全部业务，并有继续扩散的可能性。

Ⅲ级预警（黄色）。指发现新的网络与信息安全威胁，可能影响组织基础运营网络或重要信息系统的全部业务，无扩散性。

Ⅳ级预警（蓝色）。指发现新的网络与信息安全威胁，可能影响组织基础运营的部分网络或重要信息系统的部分业务，无扩散性。

（4）预警处理

对于政府和上级主管部门发布的预警信息或由本会内部报告的预警事项，应急响应小组应布置落实预防措施，并对相关部门的执行情况进行检查、监督。应急响应小组应将预防措施的落实结果报送应急领导小组。

8.2 报告程序

（1）当发生网络与信息安全事件时，事发部门必须立即将事件上报，不得瞒报、漏报和迟报；同时对于自己能够解决的信息安全事件依据《自行应急处理措施指南》进行处理，对于自己不能解决的信息安全事件应尽量保护好现场、维持现状，以便应急响应小组采取正确、有效的响应措施。

（2）在收到操作人员、技术支持人员、值班人员、运维人员等上报的事件报告后，事发部门应立即口头上报部门负责人。部门负责人接到报告后应认真做好相应记录，填写《重大信息安全事故报告表》，及时向应急响应小组组长汇报，紧急情况下可先进行口头汇报事后补写《信息安全事件受理单》，书面汇报应在事发后两个小时以内提交。当事件在Ⅲ级（较大）以上时，应急响应小组还应及时向应急领导小组汇报。

（3）重大和特别重大的网络与信息安全事件实行态势进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

（4）任何企图或实施阻拦、干扰、报复事件报告者的行为都被视为违反本规定，将进行严肃处理。

8.3 应急处置

（1）事件上报

如发现网络与信息安全事件，相关部门应立即上报至应急响应小组，并启动相应的预案，成立现场指挥部，采取现场处置措施，控制事态发展，详见《重大信息安全事故报告表》。

（2）事件响应

应急响应小组接报后，应立即详细了解安全事件情况，包括事件造成的影响、事件的严重性、扩散性、可能产生的损失以及现场处置和控制情况，必要时，应派人员到现场指挥；同时，应急响应小组要会同网络安全技术专家，尽早根据了解到的情况进行风险评估，判定事件等级，指导并做好事件处置工作，并建议是否启动组织应急程序；应急响应小组要将上述情况及时上报应急领导小组。

（3）事件通报

应急领导小组接到报告后，应及时向应急领导小组汇报情况，必要时还需向相关部门通报情况。

各部门均不得以任何原因或借口延误重大事件上报或压级上报，更不能隐瞒不报，否则，由于不报或延报产生的后果由事件报告部门承担。

（4）分级响应

根据网络与信息安全事件的可控性、严重程度和影响范围，对应事件四级分级，应急响应级别响应分为四级。

①Ⅰ、Ⅱ级应急响应。发生重大和特别重大安全事件，应急响应小组应立即向应急领导小组申请启动响应组织应急预案，必要时成立应急指挥部，统一指挥、协调事实施应急处置。应急指挥部人员由应急领导小组指定，指挥长负责统一指挥。在事件影响较大时，组织无法独立解决时，可请求政府主管部门协助。应急响应小组应将应急处置方案、网络和计算机设备、安全设备与软件等报送应急指挥部或应急领导小组，并同时做好相关的准备工作，后者根据事件情况进行评估后，批准应急处置方案，并下达指令实施应急处置。应急领导小组或指挥部要根据事件发展态势，视情况决定是否赶赴现场指导、组织外部应急支援力量，支持事发部门做好应急处置工作。

② Ⅲ、Ⅳ级应急响应。一般、较大信息安全事件，由事发部门自行负责应急处置工作，应急响应小组应直接负责协调、协助事发部门的应急处置工作，并将进程、结果报送网络安全及信息化工作领导小组办公室。

（5）应急处置手段

网络和信息安全事件发生后，首先应根据相应的系统应急手册启动相应的处置程序，控制事态发展。同时应视情况采取一定的应急处置手段，主要有：

封锁。对于扩散性较强的网络与信息安全事件，立即采取措施，切断其与网络的连接，保障整个系统的可用性，防止网络与信息安全事件扩散。

缓解。采取措施，缓解网络与信息安全事件造成的影响，保障系统的正常运行，尽量降低网络与信息安全事件带来的损失。

消除。分析网络与信息安全事件的特点，采取措施消除事件。

追踪。对于黑客入侵、DOS 攻击等人为破坏，需根据现场情况进行取证，采取一定的技术手段追踪对方信息，取证后提交公安机关处理。

恢复。消除事件后，应对系统进行检查，确保安全事件已被解决，安全隐患已被消除，部门负责人将事件的解决方案和处理结果进行反馈，经应急响应小组及相关领导认同以后方可关闭此次安全事件，恢复受侵害系统上线运行，否则按照事件报告流程重新提交；处置方案实施完毕。

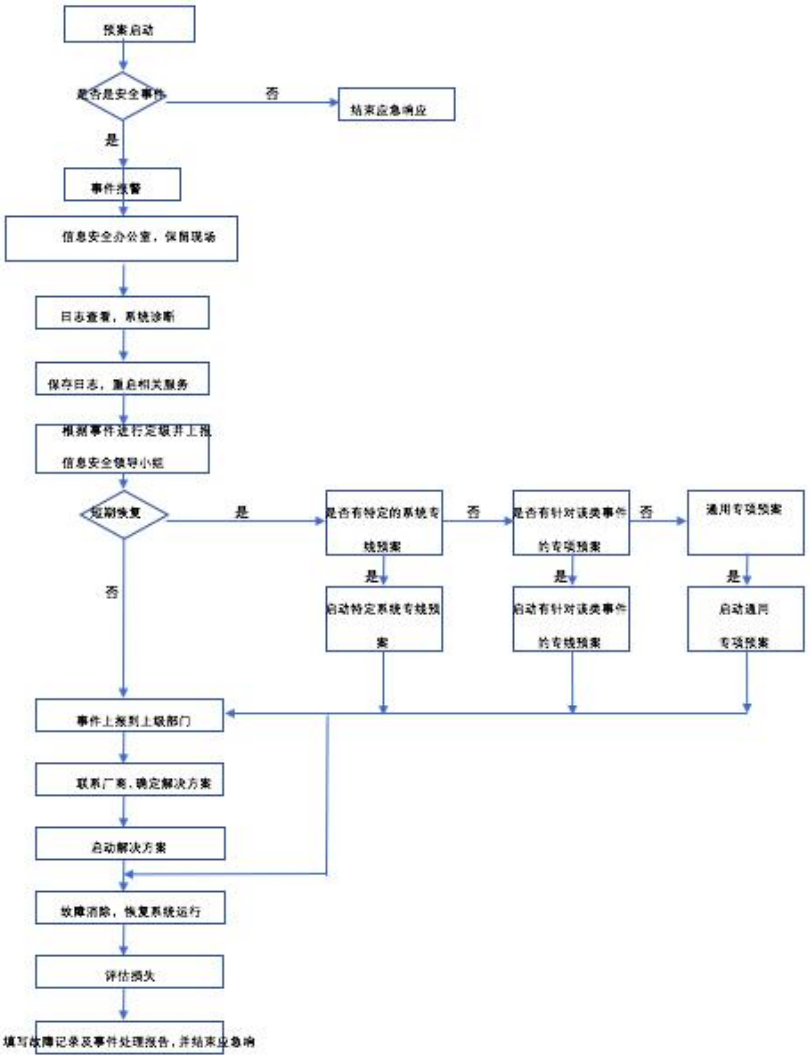
（6）处置结果检验

应急处置方案实施完毕后，应急响应小组应对处置结果

进行检验，若故障消除，则应保障好相关资料；若故障缓解，则应继续跟踪并做好后续解决工作；若处置失败，则及时向应急领导小组报告，提升响应级别，请求支援。处置结果应及时上报应急领导小组。

（7）应急结束

网络与信息安全事件经应急处置后，得到有效控制；或相关危险因素消除后，经应急领导小组批准，方可终止实施应急措施，转入常态管理，具体处理过程要填写《重大信息安全事件处理结果报告表》。



应急处置流程图

8.4 监督管理

（1）宣传教育和培训

本会要充分利用各种传播媒介及有效的形式，加强网络与信息安全事件应急和处置的有关法律法规和政策的宣传，开展预防、预警、自救、互救和减灾等知识的宣讲活动，普及应急处置的基本知识，提高全员防范意识和应急处置能力。要将网络与信息安全事件的应急管理、工作流程等列为各部门的培训内容，增强应急处置工作的组织能力。要加强对网络与信息安全事件的技术准备培训，提高技术人员的防范意识及技能。

（2）预案演练

要建立应急预案定期演练制度。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

第十章　附则

本制度经 2021 年 8 月 18 日第四届理事会第十二次会议审议通过并执行，由宣传活动部负责解释。