

保险职业学院

网络信息安全应急预案

第一章 总则

第一条 为科学应对网络与信息安全突发事件，建立健全网络与信息安全应急响应机制，有效预防、控制和最大限度的消除各类网络与信息安全突发事件的危害和影响，制定本应急预案。

第二条 本预案根据《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》、中国人寿《关于强化网络安全保障能力的指导意见》及湖南省教育厅《关于印发〈湖南省教育网络与信息安全工作实施方案〉的通知》等法律法规和规章制度制定。

第三条 近年来随着互联网的发展，信息安全问题已覆盖各个领域。特别是信息与网络犯罪有快速蔓延之势。反动邪教组织和境内外敌对势力利用互联网从事各种违法犯罪活动，严重影响着社会稳定、经济发展。近年来，随着我国信息化进程的迅速发展，网络安全亟需不断加强。

第四条 学院网络信息安全突发事件应急工作，由保险职业学院网络安全和信息化领导小组统一领导和协调，按照“统一领导、归口负责、综合协调、各司其职”的原则组织实施。

第五条 本预案适用保险职业学院网络信息系统安全应急处理工作。本方案为内部应急方案，仅在我院内部执行。如方案规定的内容与法律法规相悖时，以法律法规为准。

第二章 组织机构及职责

第六条 保险职业学院网络安全和信息化领导小组(以下简称“领导小组”), 承担网络与信息安全突发事件的组织处理领导工作, 是处理网络与信息安全的领导与协调机构, 领导小组办公室(以下简称“办公室”), 是网络与信息安全应急工作的具体工作部门。

第七条 领导小组负责研究决定网络与信息安全应急工作的有关重大问题; 通过网络信息安全制定的相关应急预案, 决定网络与信息安全突发事件应急预案的启动与部署。

第八条 办公室组织制订信息安全常识、应急知识的宣传培训和应急救援队伍的业务培训与演练; 组织、协调对突发事件的具体处置; 汇总有关网络与信息安全突发事件的各种重要信息, 进行综合分析并上报; 负责应急处置和事后恢复与重建的具体工作。

第九条 重大安全事件的处置由领导小组直接领导并指挥, 办公室协调学院各单位具体进行。

第三章 信息系统应急预案

第十条 通信系统应急预案

（一）发生通信线路中断、路由故障时，网络系统管理员应在 2 小时之内检查故障线路、进行初步故障定位并通知运维管理部门处置并及时恢复。

（二）如果通讯系统出现比较严重的问题，对单位的正常运转造成较大的影响，需立即向院分管领导报告，并通知相关运营商处置；

（三）对有简单故障的设备，运维管理人员可以修理发生故障的设备，应在 1 小时内解决相应问题并做好运维记录；

（四）发现需要更换设备，应及时更换相应故障设备，尽快恢复线路，并作好运维记录；

（五）运维管理部门发现无法及时修理时，应立即通知相关厂家的维修人员，由厂家维修人员尽快解决；

（六）如发现交换机发生故障，应立即通知厂家的维修人员来修理，不能擅自修理；

（七）如发现线路问题，应与线路提供商联系，敦促对方尽快恢复故障线路；

（八）网络运行管理部门应将应急处理过程备案，重大运维事故应向相关主管部门上报备案。

第十一条 黑客攻击应急预案

（一）保险职业学院网站由学院信息中心负责建设和维护，对网站和各应用系统中出现的网页篡改、黑客入侵等现象进行全天候监控，并及时处理。

（二）全院师生在使用网络和信息设备时，发现有黑客入侵迹象应立即通知信息中心处置，并停止一切操作，切断受攻击计算机与网络的物理连接；

（三）网络管理员根据调查情况，立即采取相应的防范措施；

（四）利用网络安全监控设备，立即对内部网内所有信息设备采取防范措施，防止黑客用同样的手段再次入侵；

（五）由网络管理员判断损失情况，对损失的数据和资料立即采取相应的补救措施；

（六）对受攻击的主机设置进行更改，对原有的用户名和口令更改，对设备使用者的其他账户进行更改；

（七）如果有可能泄露单位内部网的相关信息，立即更换所有内部网的设置，对所有用户的账号和密码进行更改，修改一切有可能泄露的信息；

（八）如果受攻击的为服务器，则立即对服务器上的所有相关信息进行更改；

（九）如有必要，停止使用受攻击的主机和服务器，启用备用服务器；

（十）对受攻击设备加强监控，随时注意异常情况；

（十一）积极追查攻击者相关信息，对其发出警告，在警告无效的情况下，采取进一步的行动，乃至采取法律手段；

第十二条 网络病毒应急方案

（一）发生病毒感染情况的时候，马上停止所有操作，切断网络连接，并通知系统维护人员和安全管理员；

（二）在感染病毒的计算机上运行杀毒软件，全面检查计算机系统，将病毒彻底清除；

（三）如果是服务器发生病毒感染，应立即停止服务器所运行的所有程序和相关服务，防止病毒进一步扩散，并通知系统维护人员和安全管理员；在服务器端运行杀毒软件，全面检查计算机系统，清除病毒；

（四）服务器查杀病毒的同时，所有与服务器连接的计算机都要进行病毒查杀；

（五）启动备用服务器，同时，将原有服务器与网络彻底断绝物理连接；

（六）若病毒已将系统破坏，导致系统无法恢复，应将感染病毒的计算机上的重要数据备份到其他存储介质，确保计算机内重要的数据不会丢失；

（七）对备份数据进行病毒检测，防止病毒交叉感染；

（八）数据无法恢复，经分管院领导同意后，可与反病毒部门联系，由他们来协助恢复，保证数据信息不泄露，并由安全管理员做好记录；如为涉密数据，按安全保密有关规定处理；

（九）如为病毒服务器问题，需在处理后填写《网络信息安全事件报告表》上报相关管理部门。

第十三条 系统备份应急预案

（一）配合上海数据中心灾备系统使用规范，信息中心定期做好应用数据库、安全文档管理、电子档案、办公系统、网站系统等主要应用系统数据备份工作。

（二）发现数据由于某些原因丢失，记录故障时间和相关信息；注意保护数据现场。

（三）如果是硬盘错误，则需要用备用硬盘替换；如果是硬盘数据丢失，要尽力采取措施修复或复制出数据。在相关技术人员确信无法挽救数据后，保分管院领导批准，方可作废弃处理。

（四）利用存储备份系统恢复离故障点最近时间的数据，尽可能地降低损失。

（五）数据灾难恢复后，提交故障报告，分析并总结故障原因。

第四章 应急处理流程

第十四条 预案启动

当发生网络与信息安全事件时，由领导小组启动应急预案，负责指挥应急处理工作，办公室负责技术指挥和处理。

第十五条 现场应急处理

事件发生后，办公室应组织现场应急处理工作组，尽最大可能收集事件相关信息，分别事件类别，确定来源，保护证据，以便缩短应急响应时间。检查威胁造成的结果，评估事件带来的影响和损害。抑制事件的影响进一步扩大，限制潜在的损失与破坏。

在事件被抑制之后，要进行综合分析，找出事件根源，明确相应的补救措施并彻底清除。

第十六条 报告和总结

认真回顾并整理发生事件的各种相关信息，尽可能地把所有情况记录到文档中，并将安全事件处理完毕后，在5个工作日内将处理结果上报相关管理部门并备案。

第十七条 应急行动结束

根据网络与信息安全事件的处置进展情况和现场应急处理工作组意见，组织相关部门对处置情况进行综合评估，确定应急行动是否结束。

第五章 保障措施

第十八条 技术支撑保障

充分发挥集团网络安全预警平台作用，优化学院监控、预警与应急处理流程，进一步提高安全事件的发现和分析能力：利用技术手段，逐步完善发现、预警、处置、通报应急处理的联动机制。

第十九条 应急队伍保障

不断加强专业安全应急人才培养和引进，进一步强化安全宣传教育，努力建设一支高素质、高技术的安全核心人才和管理队伍，提高安全防御意识。

第二十条 物质条件保障

在年度资金预算中，安排一定的资金用于预防或应对网络安全突发事件，提供必要的资源支持，为安全应急处理工作提供可靠的物资保障。

第二十一条 技术储备保障

领导小组要经常组织相关技术人员进行专业技术培训，在允许的条件下，还可以邀请专家和科研力量，开展应急运作机制、应急处理技术等研究工作。

第六章 培训和演习

第二十二条 人员培训

为确保网络与信息安全应急预案高效运行，办公室将不定期举办不同类型的培训，以便不同岗位的应急人员都能熟悉掌握安全应急处理的知识和技能。

第二十三条 应急演习

为提高安全突发事件应急响应水平，办公室定期组织预案演练。通过演习，进一步明确应急响应各岗位责任，对网络与信息预案中存在的问题和不足给予及时补充和完善。

第七章 附则

本预案通过演习、实践检验，以及根据应急力量变更、新技术、新资源的应用和应急事件发展趋势，及时进行修订和完善。

第二十四条 本预案自发布之日起实施。

第二十五条 本预案日常工作和解释由信息中心负责。

附表

网络信息安全事件报告表

[illegible]