信息安全应急演练总结（精选4篇）

篇1：信息安全应急演练总结

按照《分局网络信息安全应急预案》的要求，为妥善应对和处置我局重要信息系统突发事件，确保重要信息系统安全、稳定、持续运行，防止造成重大损失和影响，进一步提高网络与信息系统应急保障能力，我局于10月30日开展了信息系统安全应急演练。此次演练总结如下：

一、应急演练的目的明确

信息系统安全应急演练是以防范信息系统风险为目的，建立科学有效、协调有序的网络与信息安全的应急管理机制和相关协调机制。以落实和完善应急预案为基础，全面加强信息系统应急管理工作。坚持以预防为主，对可能导致信息系统安全的风险进行有效地识别、分析和控制，减少重大信息系统安全发生的可能性，加强应急处置队伍建设，确保信息系统安全发生时反应快速、报告及时、措施得力、操作准确，最大限度地减轻降低事件可能造成的损失，确保我局计算机信息系统的实体安全、运行安全和数据安全。

二、精心准备演练工作

此次应急演练对具体演练内容进行了具体的划分，从应急指挥、应急响应、具体分工到配合专门人员具体处置，都制订了详细具体的工作措施，确保演练时反应快速、报告及时、措施得力、操作准确，做到了局所联动，较好地完成了这次应急演练活动。

演练前通过内网公告和短信提前告知演练内容、演练时间、注意事项等。参演人员：演练指挥部领导、演练实施组成员（含网监办人员，一所的信息员，和12315投诉中心相关人员）。

职责分工：指挥部领导下达各个环节演练指令；所的信息员，和12315投诉中心相关人员按照分工做好各项演练操作，记录演练时存在问题及解决方案等信息；网监办相关人员按照指挥部领导指令做好各项演练操作，协同指挥其他协助单位人员做好相关工作。同时，组织有关人员研判各类信息，研究提出对策措施。做好演练信息分析、报告和发布工作。

三、严格依照方案演练。

为了达到充分练兵的作用，市局网监办选择了两个可能发生的场景开展演练：网络攻击与防范和模拟视频设备发生故障，内容包括：某个服务器故障受到arp木马网络攻击、病源确定、处理病源故障及视频设备故障与启用软视频软件等。

此次演练过程中网监办全体人员认真参与，与参加演练各单位紧密配合协同作战，成功地完成了此次演练工作。

四、及时做好演练小结

演练好之后，市局参与演练对象马上对这次应急预案演练活动进行认真总结，并将情况反馈给所和各业务科室，要求所和业务科室针对演练中出现的问题要及时进行整改，设备需要更新的立即请示局领导进行解决，制度不完善的'立即着手完善，对于各岗位的责任制要再次加以明确和落实。并由信息办人员整理应急预案演练小结内容，报市局。

五、此次演练过程发现存在的问题及解决办法：

一是实战经验不足。有些场景之前没有演练过，只是简单的学习交流或者通过书本、案例等掌握方法，现场经验不足，而这正是演练的目的,以后还要多开展此类演练,提高应急处理效率,提升应急处理能力。

二是存在信息安全隐患。通过此次应急演练，发现我局信息系统仍然存在应急安全隐患，如部分电脑系统漏洞未更新，用户对资源的访问存在默认共享等。小组成员及时对发现的问题进行记录，事后进行了分析整改。

我局将根据此次演练经验，进一步检查信息系统应急保障措施和技术应急预案的完整性，以维护综合业务系统网络及设备的正常运行为宗旨，最大限度地减轻网络与信息安全突发事件的危害，进一步提高网络与信息系统应急保障能力，提高突发事件的应急处置能力。

篇2：信息安全应急演练总结

本次信息安全应急演练于日期在地点举行，共有参与人员多人，演练主要目的是测试和评估组织在应对信息安全事件时的响应能力和应急预案的有效性。本文档旨在对演练过程进行总结和评估，并提出改进建议。

演练过程

1.预演阶段：

在演练之前，我们进行了充分的准备工作，包括制定应急预案、确定演练目标和测试场景、组织参与人员等。预演阶段的准备工作为演练的顺利进行打下了基础。

2.演练步骤：

演练分为以下几个步骤进行：

-发现事件：模拟发现一起实际的信息安全事件，包括入侵、数据泄露等。

-应急响应：各参与人员按照预先制定的应急预案，快速响应并采取合适的措施进行应对。

-事后处理：演练完成后，对应急响应过程进行总结和评估，记录并整理相关数据和经验教训。

3.评估结果：

根据本次演练的表现和应急预案的执行情况，我们得出以下评估结果：

-响应速度：参与人员在演练中反应迅速，及时采取行动。

-协同配合：各部门之间的协同配合良好，信息共享和沟通顺畅。

-应急预案：应急预案在实际操作过程中发挥了重要作用，所设定的流程和措施得到了有效执行。

改进建议

根据本次演练的经验和评估结果，我们提出以下改进建议：

1.针对演练中发现的问题进行分析，及时修改和完善应急预案，并对参与人员进行培训和演练。

2.进一步加强各部门之间的合作和沟通，制定更加详细的信息共享机制和部门责任分工。

3.定期组织演练和验证应急预案的有效性，保持团队的应急响应能力和技能的熟练度。

结论

本次信息安全应急演练取得了较好的效果，充分发挥了应急预案的作用，提高了组织在应对信息安全事件时的响应能力。通过总结和评估，我们得出了改进方案，并将在以后的工作中不断完善和优化。信息安全是一个持续的挑战和工作，我们将继续努力提升应对能力，确保组织的信息安全。

篇3：信息安全应急演练总结

时间：2015年7月16日下午

地点：平舆县人民医院门诊楼、内儿病区、妇外病区

参加科室：二甲办、质控部、医务部、护理部、门诊部、药剂科、财务科、功能科、检验科、CT、MRI、临床科室2个（中医科、神经外科）。

演练步骤：

1、16：30门诊西药房发现发药时错误，电话报信息科9675。

2、信息科主班人员排查原因，发现中心机房UPS故障，导致信息系统完全瘫痪，故障需要2小时以上才能修复，信息科长将情况汇报给分管领导。信息安全应急领导小组副组长刘超指示启动信息应急预案。

3、接到启动信息系统应急预案后信息科及时通知相关职能科室启动相应的内部应急预案。

4、设置5名志愿者模拟住院患者，门诊患者分别模拟分诊、挂号、就诊、住院、检查、报告、取药全过程。

5、演练结束（按照信息系统应急预案，需要完成补录的部门完成补录为结束，补录过程录入到测试数据库中）。

6、信息科负责信息应急演练的总结和联席会议。

演练总结：

本次演练前信息科多次与各个科室沟通，科室内部进行培训学习。整个演练过程基本完成计划要求，但也存在一定的问题。

1、新入院患者首次评估不全面，入院宣教内容缺少疾病、饮食方面的知识。

2、身份识别制度落实不到位（无查看有效身份证，上治疗时无使用“开放式”提问）。

3、患者转交接制度落实不到位（转出科室登记本无接收科室人员签名，接收科室接危重患者时无带氧气袋）。

4、两个科室无使用“药品请领单”。

5、医疗设备使用前后的告知不完善。

6、手卫生依从性差（操作前后不洗手）。

7、基于演练，患者不是真实患者，医护人员无完全进入向对待真实患者的状态，缺乏人文关怀。

三、信息系统安全应急演练药剂组反馈

为配合这次演练，药剂科事先组织进行演习，介绍流程，整个过程基本完成计划要求，但也存在一定的问题。

1、处方书写不完整。门诊西药调剂室共收到处方3张，书写均不完善。2个处方药品规格书写错误。

2、药剂人员划价速度慢，划价后没有引导患者到收费处交费。

3、进行用药交代时，呼叫患者姓名错误，把医生姓名按患者姓名呼叫。

四、信息系统瘫痪应急演练医务部督导检查反馈

为验证医院信息系统安全应急处置预案的可行性，同时完善应急预案；提高相关部门及人员对于应急预案的知晓度和流程的熟练程度；落实核心制度、二甲条款内容，进一步提高医疗质量。平舆县人民医院医务部、护理部、药剂科、信息科、设备科等职能部门于2015年7月16日16:30对医院信息系统瘫痪进行了演练，本次演练采取个案追踪的方法，分别对高血压、胆囊炎、腰腿疼三个门诊患者及心肌梗死、脑出血两个住院患者的就诊、检查、收费、取药、紧急会诊、紧急检查、转诊、转科、办理住院、术前准备、术前检查、术前麻醉访视、紧急手术及急性心梗病人紧急溶栓治疗等内容进行了督导检查，此次追踪共涉及28个二甲条款，现将存在问题反馈如下：

（一）、门诊病人在诊治中存在问题：

1、医师在诊治患者时询问病史不详细；体格检查过于简单（高血压患者只测血压）；知情告知不详细；

2、患者取药时药房人员未能严格执行查对制度；

3、患者取药返回诊室后，只交代口服药物用法，未交代注意事项及复诊时间等；

4、完成本岗位诊疗工作后未能主动指导患者进入下一诊疗环节；

5、行医技检查时未收票据、未进行身份核查及未执行双签字。

（二）、急性心梗患者在诊治中存在问题：

1、患者入科室就诊后，主治医师在检查后未下口头医嘱时，护士即开始执行医嘱，行心电图检查；

2、护士在对患者身份核查时，只核查姓名，未对住院号及性别、年龄进行核查；

3、护士健康教育过于简单，未针对病情做出相应的健康教育；

4、医师在诊治过程中未对患者进行病情评估；

5、神志清醒的患者病情及注意事项应告知患者本人，需告知家属时应签署授权委托书。

6、行心电图检查时未进行身份核查。

（三）、脑出血患者在诊治中存在问题：

1、体格检查不全面，只查瞳孔、心肺，未检查肢体及神经系统；

2、医师下达口头医嘱，护士执行时未复述，心电图未下达医嘱，甘露醇滴注时未快速滴注；

3、急会诊会诊医师5分钟到达，会诊时主管医师不在床边，汇报病史简单

4、CT申请单用病危通知单书写，告知内容简单

5、危重患者未执行先诊疗后付费

6、CT室未见CT申请单，无姓名，报告单脑出血未显示左右侧

7、CT室报告危急值未严格按危急值报告流程执行。

整改措施：

1、进一步加强业务学习，提高自身素质，增强责任意识；

2、严格按核心制度、二甲条款内容执行并落实，提高医疗质量，保障医疗安全；

3、医务部将进一步加强督导检查，定期整改。

4、当信息系统瘫痪时办理住院手续应有编号，以便临床检查核对，待信息系统恢复后重新编号，如系统瘫痪时间长，所用纸制病历应保存完整，出院时附在电子病历中，并加以说明。

5、药品的领取：有备用药物用备用药品，无备用药用领药单。

篇4：信息安全应急演练总结

背景

信息系统安全是现代社会中至关重要的一项工作，为了应对可能出现的安全事件，及时做出应急响应至关重要。为了提高应急处理能力，我们组织了一次信息系统安全应急预案演练。

目的

本次演练旨在测试我们团队的应急响应能力和安全预案的有效性。通过模拟真实的安全事件场景，我们测试了团队的应急处置流程和各项任务的完成情况。

演练过程

1.制定演练计划：我们首先制定了演练计划，明确了演练的目标、时间和地点，确定了参与演练的人员和角色分工。

2.模拟安全事件：我们选择了一种常见的安全事件进行模拟，包括入侵攻击、系统故障等情况。通过模拟真实的情景，我们能够更好地了解团队成员的应对能力。

3.应急响应：在演练过程中，我们组织了应急响应小组，根据预先制定的安全预案进行响应。小组成员按照预案分工，及时出动，处理各类安全事件。

4.评估和总结：演练结束后，我们对演练过程进行了评估和总结。我们评估了演练的效果和存在的问题，并提出了改进建议。

演练效果

通过这次演练，我们发现了团队应急响应能力的长处和短处。演练中，团队成员对安全事件的辨识能力和应对能力得到了有效锻炼，能够快速反应并采取必要措施。然而，我们也意识到在一些环节上存在一定的不足，包括沟通协调、紧急处置决策等方面。

改进建议

基于本次演练的总结和评估，我们提出以下改进建议：

1.加强团队协作能力：加强内部团队的沟通和合作，培养团队的协作能力和应对多样化安全事件的能力。

2.完善应急预案：对现有的安全预案进行优化和完善，确保预案的实施能力和有效性。

3.继续定期演练：定期组织安全演练，以进一步强化团队成员的应急响应能力和安全意识。

结论

通过这次演练，我们对团队的应急响应能力和安全预案进行了有效的测试和评估。同时，我们也明确了改进建议，以进一步提升团队的应急处理能力和信息系统的安全性。

以上是关于信息系统安全应急预案演练总结的内容，希望能为团队今后的工

作提供指导和参考。