|  |  |
| --- | --- |
| 网络与信息安全事件应急预案 | |
|  | |
| 文件名称： | 网络与信息安全事件应急预案 |
| 文件编号： | zyy20180201 |
| 实施日期： | 2018年2月1日 |
|  | |
| 广州市中医医院发布 | |

**修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 修订日期 | 修订人 | 主要修订内容 | 版本 |
| 2016.3.1 |  | 增加安全演练相关内容 | V2.0 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**广州市中医医院**

网络与信息安全事件应急预案

1. 总则
2. 为了建立健中医院网络与信息安全事件应急工作机制，提高中医院应对网络与信息安全事件的应急处置能力，预防和减少网络与信息安全事件造成的损失和危害，保护中医院和用户合法权益，制定本应急预案。
3. 中医院网络与信息安全事件是指中医院信息系统运行异常或者数据损毁、泄露，对用户合法权益造成损害或者对医院造成不良影响的事件。
4. 本预案适用于中医院供应链中心网络与信息安全事件应急处置工作。
5. 组织与职责
6. 组织体系及职责划分：
7. 中医院网络与信息安全事件应急处置指挥中心，由中医院技术总监担任总指挥,在因故无法担任的情况下，由中医院运维副总监担任总指挥，成员安全小组发生事件的部门负责人，在中医院重大突发事件应急处置工作领导小组的领导下，负责中医院信息安全应急处置工作的指挥协调和组织实施。
8. 技术中心负责中医院网络与信息安全事件的应急处置，协助对事件的调查，指导中医院及供应链中心做好相关技术系统的应急处置工作，组织技术人员定期对各相关技术系统网络与信息安全事件进行应急预案的演练、培训、修改和完善。
9. 财务部负责中医院网络与信息安全事件所需经费的相关工作。
10. 副院长负责中医院网络与信息安全事件危机处置情况向有关机构的报送工作。
11. 人事行政中心负责中医院网络与信息安全事件引起的公共安全方面的处置工作和信息安全事件引起的法律风险的评估及配合处置工作。
12. 事件分级
13. 根据网络与信息安全事件对用户合法权益造成损害，或者对医院造成不良影响的程度，事件分为特别重大事件、重大事件、较大事件、一般事件。
14. 特别重大事件是指对用户合法权益造成特别严重损害或者对医院造成特别严重影响的网络与信息安全事件。符合下列情形之一的为特别重大事件：

一、中医院有效用户数在10万人以上的现场交易系统或网上交易系统全部中断，影响交易时间累计2小时以上的；

二、中医院10万人以上的用户数据发生损毁或者错误等异常情况，影响当日或者后续正常交易的；

三、中医院10万人以上的用户数据发生泄露的；

四、其他对用户合法权益、医院造成特别严重影响的事件。

1. 重大事件是指对用户合法权益造成严重损害或者对医

药电商市场造成严重影响的网络与信息安全事件。符合下列情形之一，且未达到特别重大事件的为重大事件：

一、中医院有效用户数在1万人以上的现场交易系统或网上交易系统全部中断，影响交易时间累计30分钟以上的；

三、中医院1万人以上的用户数据发生损毁或者错误等异常情况，影响当日或者后续交易日正常交易的；

四、中医院1万人以上的用户数据发生泄露的；

五、其他对用户合法权益、医院造成严重影响的事件。

1. 较大事件是指对用户合法权益造成较大损害或者对医药

电商市场造成较大影响的网络与信息安全事件。符合下列情形之一，且未达到重大事件的为较大事件：

一、中医院现场交易系统或网上交易系统全部中断、部分中断，影响交易时间累计在5分钟以上的。

二、中医院现场交易系统发生故障,影响交易时间累计2小时以上的；

三、中医院1万人以下的用户数据发生泄露的；

四、其他对用户合法权益、医疗行业造成较大影响的事件。

1. 一般事件是指对用户合法权益造成损害或者对医药电商

市场造成影响的网络与信息安全事件。符合下列情形之一，且未达到较大事件的为一般事件：

1. 中医院现场交易系统或者网上交易系统全部中断、部分中断，

影响交易时间累计在5分钟以下的；

1. 其他对用户合法权益、医疗行业造成影响的事件。
2. 事件报告

第十条 中医院应建立信息安全风险监测预警体系，发现信息安全隐患时，应当尽快加以核实，采取必要的防范措施，如有重大情况应当及时进行预警报告。预警报告应当包括：事件基本情况（包括预警发生的时间、地点、经过等），可能造成的影响范围和后果，已采取的防范措施及相关建议、需要有关部门和单位协调处置的有关事宜。

第十一条 中医院发生网络与信息安全事件,内部应急报告流程:

1. 当中医院发生网络与信息安全事件后，将影响或已导致交易无法正常进行并确认无法迅速恢复时，须按照中医院规定的报告流程立即向相关部门、技术副院长级上报，请求启动相关信息系统应急预案。不得迟报、漏报、谎报或瞒报，更不得自作主张，轻率处理，避免严重事态发生。
2. 网络与信息安全事件报告的内部联系电话：

见《网络与信息安全事件联络手册》（该手册另行通知下发）

第十二条中医院发生网络与信息安全事件,外部应急报告流程:

一、中医院现场交易系统发生故障，可能导致或已经造成交易中断、严重缓慢的，应立即报告，并每隔30分钟至少上报一次，直至信息系统恢复正常运行。如有重要情况应立即报告。

二、中医院其他信息系统发生故障，影响用户正常业务办理，原则上30分钟内无法恢复业务正常运行的，应立即报告，并每隔1小时至少上报一次，直至业务和信息系统恢复正常运行；如有重要情况应立即报告。

三、中医院发生用户数据损毁或者泄露的事件，应立即报告，在事件解决前，如有重要情况应当立即报告。

四、中医院发生涉及计算机犯罪的事件，应立即报告，在事件解决前，如有重要情况应当立即报告。

1. 网络与信息安全事件对外联系人及电话：

见《网络与信息安全事件联络手册》（该手册另行通知下发）

第十三条 中医院进行应急报告时应当先进行电话报告，随后书面报送《网络与信息安全事件情况报告书》（见附件1），内容包括：事件发生时间、地点、简要经过、影响范围初步评估、影响程度初步评估、影响人数初步评估、经济损失初步评估、后果初步判断、原因初步判断、事件性质初步判断、已采取的措施及效果、需要有关部门和单位协助处置的有关事宜、报告单位、签发人和报告时间、联系人与联系方式、与本事件有关的其他内容。

第十四条 中医院应当在网络与信息安全事件应急处置结束、系统恢复正常运行后5个工作日内，组织内部调查，准确查清事件经过、原因和损失，查明事件性质，认定并追究事件责任，提出整改措施，并进行事件总结报告。

一、事件基本情况，包括事件发生时间、地点、经过、影响范围、影响程度、损失情况等；

二、应急处置情况，包括事件报告的情况、采取的措施及效果；

三、事件调查情况，包括事件原因、事件级别、责任认定和结论；

四、事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。暂时无法确定事件原因、责任和结论的，应当提交事件的初步分析报告，同时尽快查找原因，认定并追究事件责任，采取整改措施，并在事件应急处置结束、系统恢复正常运行后30个工作日内提交事件补充报告。

第十五条中医院接到安全扫描中医院关于系统漏洞、安全隐患、产品缺陷的信息安全通报书后，应当立即核实情况，采取必要的处置措施，并根据要求进行事件总结报告。

事件总结报告内容应当包括：事件基本情况，可能或者已经造成的影响范围和后果，已采取的防范措施及相关建议。

1. 应急准备

第十六条 应急准备

1. 技术中心负责人、值班负责人应负责信息安全应急值守。
2. 中医院系统管理员、网络管理员、数据库管理员、安全管理员及供应链中心信息技术人员应根据各相关信息系统制定相应的应急预案，具体处置方案应包括各种可能发生的技术故障的应急处置流程、报告流程等，并应针对各种技术故障拟定统一的解释口径和通知公告模板。
3. 中医院系统管理员、网络管理员、数据库管理员、安全管理员及供应链中心信息技术人员应熟练掌握各相关信息系统应急预案的应急处置操作，能有效处置网络与信息安全事件。
4. 中医院应与相关单位签订通信、消防、电力设备、空调设备、软硬件产品、安全服务等的应急响应及服务保障协议。协议内容应包括双方联系人、联系方式、服务内容及范围、应急处理方式等。应定期检查和评估协议的执行情况，确保服务保障措施落实到位，确保在应急处置中相关单位能提供及时有效的技术支持。
5. 中医院应建立有效的应急通讯联络系统，确保信息畅通。
6. 中医院应制定应急处置联络手册，明确详细的联络方式，并及时更新，在发生变化时及时通知相关单位。应急处置联络手册至少包括应急处置组织体系及相关关联单位的应急联络方式。
7. 中医院应指定通报联络人，明确联络方式。通报联络方式至少包括应急值守电话与传真。应将通报联络人及其联络方式及时通知监管部门、行业协会和相关单位。
8. 中医院应实行7×24小时联络制度，通报联络人必须保持应急值守电话可用。
9. 中医院应对有关领导和员工定制应急工作卡片，明确有关领导和员工在网络与信息安全事件应急处置中的关键任务、主要的应急联络人和联络方式。
10. 中医院应准备信息系统技术资料和软件备份。至少包括网络拓扑图、设备配置参数、各种系统软件和应用程序、安装使用手册、应急操作手册等。
11. 中医院应准备充足的重要设备备品配件，并进行定期评估、检测和维护。
12. 中医院应事先储备一定数量的通讯、消防、应急照明等应急设备或物资并定期盘点，对于有时效性的应急物资应做到及时更新。
13. 中医院应准备应急保障资金，确保应急处置中能及时采购应急设备或物资。
14. 应急处置

第十七条 中医院信息系统发生网络与信息安全事件应遵循“谁主管谁负责、谁运行谁负责”，“统一指挥、密切协同；注重预防、减少风险；科学处置、及时报告；以人为本、公平优先”的原则。

第十八条 在中医院信息系统在发现可能导致异常的风险隐患时，尽快加以核实，立即采取必要的防范措施，如有重要情况应按照有关规定进行预警报告。解除预警后，按相同路径进行报告。

第十九条 在中医院信息系统发生网络与信息安全事件后，系统管理人员须首先向信息技术部负责人报告故障情况，随即填写《网络与信息安全事件应急操作报告》（附件2）。经批准或授权批准后，启动相关系统应急预案（可先口头报告，口头批准，事后补办），迅速采取应急措施，尽快恢复网络和系统的正常运行。

第二十条 系统管理员应及时向信息技术部负责人通报故障处理变化情况和故障处置进展情况。信息技术部负责人及时向中医院信息技术分管领导及中医院网络与信息安全事件应急处置工作小组成员通报故障处理变化情况和故障处置进展情况。

第二十一条 在供应链中心发生网络与信息安全事件后，供应链中心电脑负责人须分别向信息技术部负责人和供应链中心总经理报告事件情况，随即填写《网络与信息安全事件应急操作报告》（附件2）。经批准或授权批准后，启动供应链中心信息系统应急预案（可先口头报告，口头批准，事后补办），迅速采取应急措施，尽快恢复网络和系统的正常运行。

第二十二条 供应链中心电脑负责人应保持联系方式畅通，及时向信息技术部负责人和供应链中心总经理通报故障处理变化情况和故障处置进展情况。供应链中心总经理及时向运营管理负责人和总经理办公室负责人通报故障处理变化情况和故障处置进展情况。

第二十三条 应在应急处置中，注意保证工作人员的人身安全。

第二十四条 应在应急处置结束前，保证专人24小时值班。

第二十五条应急处置人员应保持联系方式畅通，及时向有关方面通报事件处置进展情况。

第二十六条 在网络与信息安全事件发生后，按本预案应急报告有关规定报告事件情况，并保持持续报告，直至系统恢复正常运行，报告要素应完备、及时、准确，不得迟报、漏报、谎报或瞒报。

第二十七条 应做好应急处置的相关记录，保留有关证据，如涉及网络入侵、攻击的事件，可取得当地公安网监部门的支持，积极稳妥地进行应急处置。

第二十八条 人事行政中心应指导供应链中心按照中医院相关制度要求做好供应链中心公共安全事件的处置工作。必要时，请求公安机关协助维护现场秩序。

第二十九条 在在网络与信息安全事件发生后，应按中医院相关制度规定向新闻媒体说明事件情况。

1. 调查处理

第三十条在网络与信息安全事件发生后，应进行内部调查、责任追究和采取整改措施，并形成事件总结报告。

第三十一条 应按照有关规定报送事件总结报告。暂时无法确定事件原因、责任和结论的，应先给出事件的初步分析判断，并组织力量尽快查找原因，认定事件责任，给出事件结论，采取整改措施，追究责任，并提交补充报告。

第三十二条 应积极配合监管部门和相关单位组织的事件调查工作，如实说明情况，提供证据，不得拒绝、阻碍、干扰调查和取证工作。

1. 演练和完善

第三十三条 应急演练

一、中医院应根据各信息系统应急预案的内容，制定详细的应急演练计划。计划至少包括演练的目的、内容、时间、参与方、方式、前期准备情况、统计与记录要求、系统恢复与验证要求等内容。

二、中医院每半年应至少组织一次信息安全应急演练。

三、中医院各项内容的应急操作演练需经信息技术部负

责人批准或授权批准。

四、中医院应记录演练情况，演练记录至少保存两年。

五、中医院应对演练中发现的问题进行改进。

第三十四条 应急培训

一、中医院应定期开展应急培训，并形成培训记录。

二、中医院应急培训内容应包括应急预案、医药电商安全应急处置的有关规定。

第三十五条、应急预案更新和完善

* + 1. 每次应急预案演练结束后，应立即依据例行演练的记录报告进行一次评估，修订和完善各系统的应急预案。
    2. 由于新业务上线、新技术的推出、运行环境的变化等引起信息技术系统发生变化，应立即依据相关规则修订和完善相关系统的可能发生技术故障的应急处置流程、报告流程、拟定统一口径和通知公告模板等。
    3. 每次更新完善后的应急预案,必须加注更新完善日期即版本号，以便与前期版本区别。

1. 附则

第三十六条 本预案由中医院信息技术部负责解释。如本预案与中医院其他制度发生冲突以本预案为准。

### 附录

一、相关记录

|  |  |  |
| --- | --- | --- |
| 1 | 网络与信息安全事件情况报告书 |  |
| 2 | 网络与信息安全事件应急操作报告 |  |

附件1、网络与信息安全事件情况报告书

网络与信息安全事件情况报告书

报告时间： 2018年 月 日 时 分第 次

|  |  |  |  |
| --- | --- | --- | --- |
| 单位名称 |  | 报告人 |  |
| 联系电话 |  | 传 真 |  |
| 签发人 |  | 联系方式  （含手机） |  |
| 事件发生时间、  地点 |  | | |
| 事件简要经过 |  | | |
| 事件影响范围、影响程度、影响人数、经济损失情况 |  | | |
| 已采取的措施及效果 |  | | |
| 备注 |  | | |

注：单位名称处需加盖公章或信息技术负责人签字。

附件2、网络与信息安全事件应急操作报告

网络与信息安全事件应急操作报告

报告时间： 年 月 日 时 分

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 申请部门 |  | | 系统负责人 |  |
|  | | | | |
| 部门或供应链中心负责人意见 | |  | | |
| 技术中心负责人意见 | |  | | |
| 归档编号 | |  | | |

注：由于应急操作的特殊性，本报告可以执行先口头下达后书面补充的原则