编号：BZ-YJ01

霸州市人民政府门户网站信息安全应急预案

霸州市人民政府办公室

2018 年 7 月 9 日编制

霸州基层政务公开标准化规范化试点工作资料汇编

编制单位：霸州市人民政府办公室
公开范围：霸州市政府信息公开平台公开发布
联系地址：霸州市迎宾大厦　　联系电话：0316-7225576
邮政编码：065700　　编制日期：2018年7月

霸州市人民政府办公室
关于印发《霸州市人民政府门户网站信息安全应急预案》的通知

（2017）76号

各相关单位:

《霸州市人民政府门户网站信息安全应急预案》已经市领导同意，现印发给你们，请认真贯彻执行。

霸州市人民政府办公室

2017年10月10日

霸州市人民政府门户网站信息安全应急预案

为妥善应对和处置霸州市人民政府门户网站信息安全突发事件，确保网站正常运行，根据《中华人民共和国计算机信息网络国际联网安全保护管理方法》、国务院办公厅《关于加强政府信息系统安全和保密管理工作的通知》及省、廊坊市有关文件精神，结合我市政府门户网站实际情况，特制订本应急预案。

第一部分 总 则

本应急预案的适用范围：市政府办公室、市行政审批局负责建设管理的霸州市人民政府门户网站、市政府信息公开平台、市政务服务平台系统网络安全事件的应急处理。

本应急预案的内容：防范和消除政府门户网站及相关系统因木马、病毒感染、黑客攻击导致网站不能正常访问，数据被篡改、丢失；网站内容违反国家的法律法规、侵犯知识产权、含有危害国家安全和社会稳定的信息等；因软硬件故障、自然灾害、失窃等原因造成数据丢失、系统瘫痪等。

一、日常信息安全工作职责

市政府信息中心、市行政审批局网络管理人员根据分工做好以下工作：

（一）对政府门户网站、网络进行日常检查，分析风险、排除隐患、做好政府网站数据备份，形成日常工作机制，预防安全事故发生。

（二）制定相关安全事件的预警方案和解决方案。

（三）掌握网络、网站技术发展趋势，不断提升信息安全防范水平。

（四）及时处置各类突发信息安全事件。

二、信息安全应急处置原则

（一）报告原则：发生突发安全事件，第一时间向市政府信息中心负责人报告，积极协调政府门户网站信息安全应急小组成

员进行信息安全处置，并将处置情况及时上报市网信办，信息安全应急处置情况要及时向市委、市政府领导汇报。

（二）安全原则：处置安全事件时，要科学客观，首先保证人员安全，其次保证设备数据安全。

（三）效率原则：处置突发事件要及时迅速，讲究方法，善于协调，争取在最短时间内解决问题。

（四）协调配合原则：出现大规模故障后，根据工作需要，积极配合，协同处理，提高工作质量与效率。

三、安全应急事件处置

（一）安全事件定义分类

一般故障：指区域性网络安全事件，具体包括：局部网络瘫痪、个别设备故障、个别网站服务器不能正常工作等。

重大故障：指发生大规模或整体性网络瘫痪、核心网络安全设备损坏或被窃、政府网站服务器数据丢失、政府网站遭恶意篡改、遭受黑客攻击、中心机房长时间电力供应中断等。

特大故障：指机房发生火灾或遭受不可抗拒力破坏，造成机房损毁及人员伤害等。

（二）处置时限

发生突发安全事件，一般故障4小时内解决，重大故障24小时内解决。

（三）处置措施

1.发生突发信息安全事件，网络管理人员要迅速准确判断事

件原因，第一时间上报主管领导，酌情通知政府门户网站应急小组成员单位。

2.根据具体情况分析研判危害程度，启动应急预案。在保证人员、设备、数据安全的前提下，进行针对性处置。

3.属一般性故障的，市政府信息中心及市行政审批局网络管理人员及时进行处置；属设备损坏的，要及时报告，并根据领导安排进行合理处置；属系统故障的，通知设备供应商和系统软件维护公司进行处置；属遭受黑客攻击的，要及时取证留存，若情况严重，向市公安局网安大队报警，并联系设备供应商和系统软件维护公司进行处置。

4.事后总结本次事件处置情况，形成分析报告。

第二部分 政府网站信息安全应急处置

一、日常管理维护

（一）市政府信息中心每天对政府网站内容进行查看，密切监测政府网站运行及信息内容，每天通过开普云政府网站监测监管系统对“霸州市人民政府”门户网站进行数据监测和统计。市行政审批局网络管理人员每天对中心机房进行网络设备检测和检查，保障中心机房网络安全设备、服务器正常运行，网络畅通。保障中心机房供电系统（包括后备电源）、空调系统正常运行。

（二）市政府信息中心及时检查各服务器杀毒软件及软件防火墙升级情况，及时为服务器系统打补丁。

（三）市政府信息中心对政府网站服务器数据库每天2点进行定时备份（自动进行）。每月对政府网站、政府信息公开平台、政务服务平台服务器备份的数据进行光盘或移动硬盘备份，并由专人归档保存。

二、信息安全事件分类及应急处置措施

信息安全事件分类及应急处置措施适用于霸州市人民政府门户网站和霸州市政务服务平台系统，信息安全事件处置流程分为：分析确认、启动应急预案、故障修复、修复运行、详细备案、汇总上报。

（一）硬件类故障

指因自然灾害、供电不正常、人为因素等造成的服务器硬件损坏、丢失情况。

1.市政府信息中心、市行政审批局网络管理人员组织设备供应商和系统软件维护公司对中心机房软、硬件设备进行检测。包括5台核心网络安全设备、政府网站服务器、政务服务应用服务器和政务服务数据库服务器，按要求每月进行软、硬件的信息安全检测，并填写记录，每年度进行总结汇报。

2.发生硬件故障、网络故障、系统软件故障后要立即通知市政府信息中心、市行政审批局负责人，并联系设备供应商、系统软件维护公司进行处理。相关处理情况由市政府信息中心逐级向上级领导汇报，向应急小组成员单位进行通报。

（二）黑客攻击、非法信息和篡改类故障

指网站系统遭到网络攻击不能正常运行，或出现非法信息、页面被篡改等情况。

1.通过入侵检测系统发现有黑客正在对政府网站进行攻击时,首先应将被攻击的服务器等设备从网络中隔离出来，及时上报。当发现政府网站出现非法信息或页面被篡改，要第一时间保存有关记录、日志。报告市政府信息中心负责人，根据具体情况分析研判危害程度，启动应急预案，将有关情况上报市网信办。组织人员及时删除、恢复相关信息及页面，并通过硬件防火墙、入侵防御系统和网站防篡改设备进行技术检测，查找问题，修改漏洞。必要时向廊坊市、省政府主管部门进行报备，申请政府网站服务器临时关停,由系统软件维护公司修复和安全加固后再开启服务。

2.市政府信息中心、市行政审批局网络管理人员要妥善保存有关记录及日志或审计记录，追查非法信息来源，将有关情况进行及时上报。若情况严重，应保护现场，做好必要记录，保存非法信息或篡改页面，向市公安局网安大队报警。

3.市公安局网安大队应在接到报警后1小时内赶到现场，追查非法信息来源，并妥善保存有关记录、日志。在市公安局网安大队提取相关数据样本后，清理网站非法信息，修复篡改页面，并实施必要的安全加固措施。如情节严重，构成违法犯罪的，由市公安局网安大队立案侦查。

4.总结事件处理情况，逐级上报，并做好记录存档。

（三）病毒木马类故障

指政府网站服务器感染病毒木马，存在安全隐患。市政府信息中心、市行政审批局网络管理人员工作要求:

1.每周对服务器杀毒安全软件进行系统升级,并进行病毒木马、系统 bug 扫描，清除病毒木马程序，封堵系统漏洞。

2.发现政府网站服务器感染病毒木马，要立即对其进行查杀，并根据具体情况，酌情通知应急小组成员单位进行处置，并逐级报告。

3.由于病毒木马入侵服务器造成数据丢失或系统崩溃的,要第一时间报告市政府信息中心负责人,根据具体情况分析研判危害程度，启动应急预案，将有关情况上报市网信办，并联系相关单位进行数据恢复。必要时向廊坊市、省政府主管部门进行报备，申请政府网站服务器临时关停,由系统软件维护公司检测无故障后再开启服务。

4.分析后台数据库操作日志，判断是否发生数据失窃，检查、校验数据的完整性和有效性，恢复与重建被攻击或破坏的系统,用备份数据恢复网站数据。如情节严重，构成违法犯罪的，由市公安局网安大队立案侦查。

5.总结事件处理情况，逐级上报，并做好记录存档。

（四）系统类故障

指政府网站服务器操作系统、网站发布系统等软件故障造成政府网站不能正常运行。

1.市政府信息中心、市行政审批局网络管理人员要每月对3台服务器软件系统和数据库进行备份和存档。

2.发现此类问题，需要逐级上报，联系系统软件维护公司进行检测修复，并总结事件处理情况，做好记录存档。

三、应急保障要求

市政府信息中心、市行政审批局网络管理人员应急保障要求:

（一）记录政府网站信息安全应急小组成员单位联系电话，出现问题能及时联络处理。

（二）掌握核心网络安全设备、3台政府网站服务器的操作和使用,加强网络安全设备、系统软件等账号和密码的安全管理，掌握服务器软件系统及数据库的备份、恢复流程等。

（三）学习和掌握各类软硬件知识，提高应对和处理突发网络故障的能力。

第三部分 中心机房安全应急处置

一、用电安全

市行政审批局三楼中心机房用电安全要求:

（一）坚持正确的用电规范。

（二）不使用超负荷电器设备。

（三）不随意改变工程设计的供电线路。

（四）每两个月对中心机房各电源设备进行检查。遇节假日，需检查中心机房内电源和线路，确保设备安全稳定运行。

（五）机房供电中断后，应立即查明原因，并逐级上报。

1.机关内部线路故障，由物业公司工程部迅速恢复。

2.如果是供电公司的原因，应立即与市供电公司联系，迅速恢复供电。

（六）如果供电公司告知需长时间停电，应做如下安排:

1.预计停电3小时以内，由UPS后备电源供电。

2.预计停电3小时以上,请示主管领导,关掉非关键设备，确保关键设备供电。

3.预计停电超过6小时以上时，由市政府信息中心报政府网站主管领导批准后，向廊坊市、省政府主管部门申请临时关停报备。UPS后备电源使用完前，由市行政审批局网络管理人员关闭中心机房所有关键设备。

（七）发生火警事件发生后，中心机房管理人员应根据所属区域和现场情况，判断和选择正确的方法，及时上报主管领导，同时配合相关人员处置。

1.对于设备发生烟雾,机房主管人员协同相关人员寻找烟雾点并切断相关区域电源。

2.当设备发生可控制火情时,机房主管人员应协同相关人员进行灭火工作。

3.当机房发生不可控制火情时,应按火警火灾应急处理流程操作。

二、核心设备安全

（一）根据实际情况对核心设备进行检查，确保设备安全稳定运行。

（二）发生核心设备硬件故障后，工作人员应及时报告主管领导，并查找、确定故障设备及故障原因，进行先期处置，同时联系设备提供商共同检测并排除故障。

（三）若故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行，将故障设备脱离网络，进行故障排除工作。

（四）故障排除后，在网络空闲时期，替换备用设备。若故障仍然存在，应立即联系设备提供商进行返厂维修或调换设备。

三、数据安全与恢复

（一）发生业务数据损坏时，工作人员应及时报告主管领导，检查和备份系统当前数据，选择最近日期备份数据进行恢复。

（二）市政府信息中心负责政府网站服务器的数据备份与恢复，市行政审批局负责政务服务平台服务器的数据备份与恢复。若备份数据损坏，应及时调用异地备份数据进行恢复。

（三）备份数据系统恢复后，市政府信息中心、市行政审批局网络管理人员应检查基础数据的完整性，重新备份数据，并写出故障分析报告。

四、其他事项

（一）无关人员未经市行政审批局中心机房主管领导批准不得进入中心机房。

（二）对中心机房各设备和强电、弱电线路进行维护或改造

前，需经市行政审批局中心机房主管领导批准，并由机房网络管理人员、物业工程部人员陪同进行。

（三）对中心机房保洁时，应使用充分控干水份的抹布及拖把，不要使用干布或扫帚，避免扬尘。设备保洁时，注意不要触碰电源接口及网络接口等，以免漏电或导致线路接触不良。

霸州市人民政府门户网站信息安全应急小组联系人及电话

1. 市政府信息中心　孔维强　7225576　13832698875
2. 市行政审批局　李振峰　7285828　15930680766
3. 市网信办　邓宁宜　7212371　15033168258
4. 市工业和信息化局　杜立山　7861918　13473690869
5. 市公安局网安大队　李志强　7238783　15530656868
6. 联通公司霸州分公司　张翠清　18603167693
7. 金蝶软件公司廊坊分公司　王斌　15831927268
8. 廊坊市雨思计算机服务公司　王济伟　13932620680
9. 河北中信联信息技术有限公司　张凯强　15230167188

霸州市人民政府办公室　2017年10月10日印发