编号：BZ-YJ02

霸州市政府信息公开平台信息安全应急预案

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《霸州市政府信息公开平台信息安全应急预案》的通知

（2018）105号

各相关单位:

《霸州市政府信息公开平台信息安全应急预案》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

2018年7月25日

（此件公开发布）

霸州市政府信息公开平台信息安全应急预案

为妥善应对和处置霸州市政府信息公开平台信息安全突发事件，确保政府信息公开平台正常运行，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》、《互联网网络安全应急预案》和国务院办公厅《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

信息公开平台主机托管实际情况，并根据《联通公司 IDC 主机托管协议》，特制订本应急预案。

第一部分 总 则

本应急预案的适用范围:市政府办公室负责建设管理的霸州市政府信息公开平台，涉及全市65个单位和部门政府信息公开系统网络安全事件的应急处理。

本应急预案的内容:防范和消除政府信息公开平台及相关软件系统因木马、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;因服务器主机软硬件故障、IDC 机房网络故障、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

市政府信息中心网管人员根据分工做好以下工作:

（一)对霸州市政府信息公开平台网络运行情况进行日常检查，分析风险、排除隐患、做好数据备份，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，积极协调政府信息公开平台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：IDC 机房主机络瘫痪、个别设备故障、系统软件故障、服务器不能正常工作等。

重大故障：指 IDC 机房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，政府信息公开平台服务器数据丢失，政府信息公开内容遭恶意篡改，遭受黑客攻击，IDC 机房长时间电力供应中断，网络长时间故障等。

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,网管人员要迅速准确判断事件原因，第一时间上报主管领导，通知政府信息公开平台信息安全应急小组成员单位，及时联系联通公司廊坊分公司 IDC 机房工程师，分析信息安全事件原因及范围。

2.根据具体情况分析研判危害程度,确定信息安全事件等级启动应急预案。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,市政府信息中心及联通 IDC 机房网管人员及时进行处置；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。

3.将信息安全事件情况进行汇总，及时上报市网信办，报市政府办公室领导,根据信息安全事件等级上报市委、市政府领导。

4.事后总结本次事件处置情况，查找不足，推进整改，形成分析报告，并存档备查。

第二部分 政府信息公开平台信息发布安全应急处置

一、日常管理维护

（一）市政府信息中心每天对政府信息公开平台内容进行查看，密切监测服务器主机运行及信息内容，通过软件系统远程监测服务器运行情况。联通公司廊坊 IDC 机房网管人员根据《IDC 主机托管协议》，对机房络设备检测和检查，保障中心机房网络网络畅通，保障机房供电系统、空调系统正常运行。

（二）市政府信息中心网管人员及时检查政府信息公开平台服务器杀毒软件及系统软件防火墙升级情况，及时为服务器系统更新补丁。

（三）市政府信息中心对政府信息公开平台服务器数据库每天2点进行定时备份（自动进行）。每月对政府信息公开平台服务器备份的数据进行远程异地备份，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信息公开平台系统，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.市政府信息中心网管人员组织设备供应商和系统软件维护公司对软、硬件设备进行检测。包括 IDC 机房托管的1台硬件

防火墙，政府信息公开平台服务器。按要求每月进行软、硬件的信息安全检测，并填写记录，每年度进行总结分析。

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负责人，并联系设备供应商、系统软件开发公司进行处理。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。

3、分析研判信息安全事件等级，根据危害程度和不能正常访问时间，确认事件等级，向市网信办报告。必要时向市委、市政府领导报告。

（二）黑客攻击、非法信息和篡改类故障

指政府信息公开平台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.发现有黑客正在对政府信息公开平台进行攻击,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。当发现政府信息公开平台出现非法信息或公开内容被篡改,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，并通过硬件防火墙等设备进行技术检测，查找问题，修复漏洞。将有关情况上报市网信办，必要时向廊坊市、省政府网信主管部门进行报备，申请政府信息公开服务器临时关停,由系统软件开发公司修复和安全加固后再开启服务。

2.市政府信息中心网管人员要妥善保存有关记录及日志或审计记录，方便追查非法信息来源，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2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

指政府信息公开服务器感染病毒木马，存在安全隐患。市政府信息中心网管人员工作要求:

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.发现政府信息公开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、省政府网信主管部门进行

报备，申请政府网站服务器临时关停，由系统软件开发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,用备份数据恢复政府信息公开平台数据。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

指政府信息公开平台服务器操作系统、信息公开发布系统等软件故障造成不能正常运行。

1.市政府信息中心网管人员要对服务器软件系统和数据库进行远程异地备份和存档,方便系统软件故障后的软件及数据的恢复。

2.发现此类问题，及时分析研判，并逐级上报。联系系统软件开发公司进行检测修复，并总结事件处理情况，具体防范措施，并做好记录存档。

三、应急保障要求

市政府信息中心网管人员应急保障要求:

（一)记录政府信息公开平台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）掌握硬件防火墙、政府信息公开平台服务器的的远程操作和使用，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信息安全事件的能力。

第三部分 廊坊IDC机房安全应急处置

一、服务器主机托管情况

霸州市政府信息公开平台系统服务器主机托管在联通公司廊坊分公司IDC机房中，托管设备包括：硬件防火墙1台，政府信息公开平台服务器主机1台，显示器1台等其它配件。服务器托管位置:IDC机房16/13机柜中，服务器IP：221.194.128.138，服务器型号：HP ProLiant DL380，托管H3C硬件防火墙1台。

IDC机房环境由联通公司廊坊分公司负责，由专职网络工程师负责维护机房不间断电源、空调系统及网络运行畅通。机房值班电话0316-2255555，每天24小时受理故障申告，在承诺时限内进行修复，期间需要市政府信息中心网管人员协助配合。

二、IDC机房安全应急处置流程

1.市政府信息中心网管人员发现霸州市政府信息公开平台不能正常访问后，进行远程检查，分析研判：是软、硬件问题、网络问题、还是系统软件问题。确认后按以下流程处置。

（1）确认是IDC机房网络故障时,及时联系联通公司管理人员，联系IDC机房网管人员，申请对机房网络故障进行排除。

（2）确认是IDC机房托管服务器硬件、软件故障或硬件防

火墙故障时，及时联系联通公司处置人员，联系 IDC 机房网管人员协助查看故障原因。联系硬件维护公司和系统软件开发公司技术远程协助解决。确实需要上门检查维修时，由市政府信息中心向联通公司廊坊分公司传真《IDC 机房进场维修申请单》。联系硬件维护公司和系统软件开发公司人员到 IDC 机房进场维修，共同检测并排除故障。

（3）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。

（4）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更换设备。

2.分析故障原因和处置方法，及时上报市网信办，市政府办公室领导，并做好记录存档。

三、数据安全与恢复

（一）发生政府信息公开平台数据损坏时，网管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联系系统软件开发公司对政府信息公开平台服务器的数据进行备份与恢复。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，系统软件开发公司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。

附件:霸州市政府信息公开平台信息安全应急小组联系人及电话

附件：

霸州市政府信息公开平台信息安全应急小组联系人及电话

1. 市政府办副主任	谭宝钢	7867581	13373060337
2. 市政府信息中心	孔维强	7225576	13832698875
3. 市政府信息中心	李　亮	7230400	13831620511
4. 市网信办	樊　江	7212371	15373235758
5. 市网信办	邓宁宜	7212371	15033168258
6. 市工业和信息化局	杜立山	7861918	13473690869
7. 市公安局网安大队	李志强	7238783	15530656868
8. 河北中信联信息技术有限公司	张凯强		15230167188
9. 联通公司廊坊 IDC 机房	陈　帆		18631618808
10. 联通公司廊坊 IDC 机房	贾工程师		18603165371
11. 联通公司霸州分公司	徐旭东		18633612881
12. 廊坊市雨思计算机服务公司	王济伟		13932620680

霸州市人民政府办公室　　2018 年 7 月 25 日印发