北京市西城区人民政府办公室

北京市西城区密码管理局 文件

西政办发〔2016〕13 号

关于组织 2016 年北京市西城区电子政务网络与信息系统安全检查工作的通知

西城区各有关单位：

根据国务院办公厅、北京市政府办公厅关于对政府信息系统实施安全防护管理、检查的有关办法规定，依据北京市经济和信息化委员会、北京市密码管理局《关于开展 2016 年北京市电子政务网络与信息系统安全检查工作的通知》（京经信委发〔2016〕29 号）要求，经研究，区政府办、区密码管理局（区委机要局）定于 2016 年 6 月至 11 月联合开展西城区电子政务网络与信息系统安全检查，并迎接北京市安全检查工作组的现场抽查。现就有关事项通知如下：

一、 检查目的

掌握全区政务信息安全总体状况，查找存在的安全问题和薄

弱环节并及时整改；进一步增强全区党政机关信息安全意识，落实信息安全制度和技术防范措施，切实提高安全防护水平，确保全区电子政务网络与信息系统安全稳定运行。

二、 检查原则

（一）全区电子政务网络与信息系统安全实行“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，检查采取各单位自查、组织技术监测和现场抽查相结合的方式进行。

（二）全区电子政务网络与信息系统安全检查中，涉及保密工作事项的，按照国家保密管理规定和标准执行；涉及密码工作事项的，按照国家密码管理规定执行；涉及信息安全等级保护工作事项的，按照国家信息安全等级保护管理规定执行。

（三）各单位在时限内自行组织全面检查，边查边改，针对薄弱环节进行安全加固。

三、 检查范围

（一）在用办公网络。包括政务外网和政务内网。

（二）电子政务信息系统。包括自行建设运维、委托建设运维或建设在政务云平台上的信息系统，以及电子政务内网上建设部署运维的信息系统。其中重要业务系统和门户网站为检查重点。

四、 工作组织

区政府办、区密码管理局（区委机要局）联合成立电子政务网络与信息系统安全检查工作组，开展自查检测，并配合北京市开展相关迎检工作。

（一）区密码管理局负责电子政务内网与信息系统、密码技术与产品的安全检查及党委系统网络与信息系统的安全检查工作。

（二）区政府办负责区级政府部门和15个街道办事处网络与信息系统的安全检查工作。

（三）区政府办、区密码管理局检查工作组共同配合北京市检查工作组于6月至11月对西城区信息系统安全组织技术检测和现场抽查。

五、 检查内容

全面检查各单位信息安全工作开展情况，包括安全管理制度落实情况、信息安全等级保护工作开展情况、门户网站整合与安全防护情况、密码技术与产品使用情况、信息技术服务外包管理情况、应急管理工作情况、系统安全漏洞排查及整改情况等。

（一）安全管理制度落实情况。检查各单位对国家和北京市信息安全法规、政策、标准的落实情况和信息安全责任制建立及落实情况，包括信息安全主管领导、信息安全管理机构、信息安全工作人员履职以及岗位责任，资产管理、存储介质管理、运行维护管理、年度教育培训制度、信息安全经费投入等情况。

（二）信息安全等级保护开展情况。检查各单位信息系统总体情况以及系统定级、备案和测评等。

（三）内网安防情况。检查有关单位接入内网的网络或终端安全防护情况。

（四）整合防护情况：检查有关单位门户网站整合与安全防护措施执行情况。

（五）密码技术与产品使用情况。检查有关单位在信息系统建设中的密码设备管理和使用情况是否符合有关要求。

（六）信息技术服务外包管理情况。检查有关单位的外包服务机构性质、服务类别、服务企业能力等。

（七）应急管理工作情况。检查各单位的信息安全事件应急预案制定和修订情况，预案演练情况，突发事件处置和信息报送情况，以及灾难备份与恢复措施情况。

（八）系统安全漏洞排查及整改情况。检查各单位在技术检测、单位自查和日常监测发现问题的整改情况。

六、检查方式

采取单位自查、技术检测、现场抽查相结合的方式。

（一） 单位自查。

各单位依据检查内容要求，组织开展自查。对自查过程中发现的问题和薄弱环节，要及时组织整改。

（二）技术检测。

区政府办组织专业技术队伍对党政机关重要系统开展不少于两次的远程技术检测。区密码管理局组织力量对政务内网信息系统情况开展技术检测，查找政务系统存在的安全漏洞、隐患，对发现的安全问题及时通报各相关单位组织整改。

（三）现场抽查。

安全检查工作组结合技术检测、日常监测和事件通报情况，选取部分单位进行现场抽查。抽查对象包括重要信息系统多、技术检测问题多以及未及时提交自查报告和未及时反馈技术检测整改结果的单位。

七、 检查结果评定

安全检查工作组结合各单位自查报告、技术检测、现场抽查情况，组织检查结果评定，并将评定情况向各单位反馈。

八、 时间安排

2016 年西城区电子政务网络与信息系统安全检查工作自 6 月开始，11 月结束，年底前进行结果通报。

（一）信息安全自查、检测

时间：2016 年 6 月 22 日至 7 月 8 日。

各单位要重点加强对电子政务网络与信息系统的安全检查，排查安全漏洞和安全隐患，强化电子政务信息安全保障和安全防护措施，按时完成信息安全自查纠正，并根据自查结果，填写《自查报告》和《政务信息系统安全检查情况报告》，于 7 月 8 日前以纸质版材料加盖单位公章与电子版（刻光盘）形式将检查情况统一报送区委机要局（区密码管理局）。

6 月，北京市及西城区开展第一轮安全技术检测，并通报检测结果，相关单位须及时进行整改。

（二）汇总分析、上报整改情况和自查报告

时间：2016 年 7 月 9 日至 7 月 31 日。

区政府办和区密码管理局收集、整理、分析各级各部门安全自查和整改反馈情况，汇总上报市经济信息化委和市密码管理局。

（三）信息安全检测和整改反馈

时间：2016 年 8 月 1 日至 9 月 30 日。

区政府办和区密码管理局采用技术手段，开展第二轮安全技术检测，结合前期各单位自查和北京市反馈情况，对全区重要、重点信息系统进行安全技术检测，各单位对存在问题进行整改落实。

（四）信息安全现场抽查

时间：2016 年 10 月 8 日至 10 月 31 日。

区政府办和区密码管理局对重点单位和信息系统进行现场检查，配合市安全检查工作组对我区重点单位进行现场抽查。

（五）综合评定

时间：2016 年 11 月 1 日至 11 月 30 日。

区政府办和区密码管理局向各单位通报 2016 年电子政务网络与信息系统安全检查结果，反馈北京市有关检查评定情况。

九、 相关工作要求

（一）各单位要切实加强领导，完善检查工作落实机制，明确责任，专人负责，对检查中发现的问题进行分析研究并及时整改，如实、完整填写《自查报告》和《政务信息系统安全检查情况报告表》并按时上报。我们将对自查工作不认真、报送材料不

及时、存在问题较多、整改不到位的单位作为重点检查、现场抽查对象。

（二）各单位可委托信息安全检测机构进行自查和整改，信息安全检测机构应具备相关的安全检测资质，并签订安全保密协议，明确安全保密责任和义务。

（三）各单位强化安全保密和风险控制，加强相关文档和数据的安全保密管理，确保被检查信息系统的安全正常运行。

（四）本次网络和信息系统安全检查情况将作为2016年度各单位年终绩效考评信息安全考核部分的重要依据。

附件：1.自查报告模版

2.政务信息系统安全检查情况报告表

西城区人民政府办公室　　西城区密码管理局

2016年6月22日

（联系人：区政府办　郁卓　　联系电话：88064740；

区密码管理局 樊月辉　联系电话：88064490）

附件 1

自查报告模版（参考格式）

2016 年 XXX 单位网络与信息系统安全自查工作总结报告

一、本单位安全检查工作组织开展情况。

概述此次安全检查工作组织开展情况。

二、本单位信息安全主要工作情况

对照检查要求，逐项详细描述本单位在制度落实、信息安全等级保护、网络整合及防护、密码产品使用、服务外包、应急处置等方面工作的检查结果。对本单位重要网络与信息系统基本情况进行梳理，并逐一简要介绍。

三、检查发现的主要问题及整改情况。

描述本单位安全检查特别是技术检测的结果，总结分析本部门在安全管理、技术防护等方面存在的主要问题和薄弱环节，以及针对这些问题的整改措施或整改计划。

四、对信息安全工作的意见和建议。