**2025年信息化安全运维服务项目附件**

**附件一 报名材料：**

**（注：以下附件1至附件3为实质性条款，没有对此作出完全响应的供应商将被拒绝）**

|  |
| --- |
| **报名信息** |
| 单位名称 | 联系人 | 联系电话（手机号） | 地址 | 邮箱 |
|  |  |  |  |  |
| **注：请报名供应商填写以上信息。** |

附件1 有效的营业执照或法人证书等证明文件，以自然人身份参与的提交自然人的有效身份证明

附件2 法定代表人/负责人身份证明

附件3 法定代表人/负责人授权书

**报名材料格式：**

**附件 1 有效的营业执照或法人证书等证明文件（复印件，须加盖供应商公章），以自然人身份参与的提交自然人的有效身份证明（复印件）**

## 附件 2 法定代表人/负责人身份证明(格式，原件)

**法定代表人/负责人身份证明**

供应商名称：

单位性质：

成立时间： 年 月 日

姓名： 性别： 年龄： 职务：

系 （供应商名称） 的法定代表人/负责人。

特此证明。

附：法定代表人/负责人的身份证明：有效的身份证正反面复印件，或有效的护照复印件。

供应商名称（盖章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 附件 3 法定代表人/负责人授权书（格式，原件）

**（非法定代表人/负责人签署报名材料的，应提交法定代表人/负责人授权书及其附件；若报名材料由法定代表人/负责人本人签署，则可不用提交。）**

**法定代表人/负责人授权书**

 本授权书声明：注册于 （国家或地区的名称） 的 （公司名称） 的在下面签字或盖章的 （法定代表人/负责人姓名） 代表本公司授权 （公司名称） 的在下面签字或盖章的 （被授权人的姓名） 为本公司的合法代理人，就2025年信息化安全运维服务项目的比选，以本公司名义处理一切与之有关的事务。

本授权书于\_\_\_\_\_\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_\_日生效，特此声明。

法定代表人/负责人签字或盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

被授权人签字或盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

公司盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

附：

被授权人姓名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

职　　　　务：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

电　　　　话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

被授权人的身份证明：有效的身份证正反面复印件，或有效的护照复印件。

**附件二**

# 采购需求

# 一、项目概述

## 1.项目背景

根据《网络安全法》《数据安全法》《个人信息保护法》等制度规定，网络安全工作是信息化工作的一项重要内容。为做好管委会的安全保障工作，规范突发事件处置工作相关要求，快速、准确、高效地应对突发事件，提高管委会的信息安全、业务安全、应急保障能力和水平，最大程度地减少应急突发事件对管委会的影响，保障管委会的系统安全，正常稳定的运行，需要开展信息化安全运维服务，以预防安全事件发生，避免安全问题。

## 2.项目目标

总体目标：通过全方位的信息安全服务，满足“事前可预防、事中可控制、事后可恢复”的信息安全保障需求，确保管委会各信息系统持续安全稳定运行。同时结合重点站区信息安全建设发展的需求，提高信息系统运行效率，提升管安全运维能力。

具体目标：保证安全设备良好运行；及时发现网络和系统中存在的安全隐患并加以改进，提高业务系统安全性和业务连续性；进一步提高应对网络安全事件的能力，并降低安全事件带来的损失和负面影响。

# 二、服务范围

本次服务范围为管委会各部门（单位），具体包括：管委会机关、北京站地区、北京西站地区、北京南站地区、北京北站地区、清河站地区、北京朝阳站地区、北京丰台站地区、城管分局机关、城市副中心办公区、北京首都国际机场办公区、北京大兴国际机场办公区等。

# 三、服务期限

本项目服务期为2025年1月1日——2025年12月31日。

# 四、服务地点

管委会机关:北京市西城区莲花池东路102号天莲大厦

北京站办:北京市东城区东镇江胡同2号行装综合楼

北京西站办:北京市西城区广莲路甲5号建设大厦

北京南站办:北京市丰台区南站路2号院供销弘泰大厦

北京北站办:北京西城区西直门外大街18号金贸大厦B座5层/C2座2层

清河站办:北京市海淀区清河交通枢纽办公楼

朝阳站办:北京市朝阳区姚家园北路与星火东路交叉口西50米

丰台站办:北京市丰台区正阳大街4号铁路公寓楼1层

城管分局机关：北京市西城区莲花池东路112号

城市副中心办公区：通州区新潞运河文创园B5号楼三层

北京首都国际机场办公区：北京市顺义区首都机场三经路03号中国服务大厦C区7层

北京大兴国际机场办公区：河北省廊坊市广阳区北京空港兴航达客运有限公司（北京大兴国际机场近端停车场北小楼）

# 五、服务需求

## 1.安全运营巡检

### 1.1服务内容

利用检测工具和人工检测等多种方式，定期对项目内信息系统的服务器、网络及安全设备的健康状态进行检测，包括设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，并实施必要的安全维护操作。

定期对网络设备、安全设备的配置策略进行维护，包括：配置策略比对、配置策略增添、配置策略删减、配置策略修订、配置策略备份、配置策略分析等；定期对网络设备、安全设备的日志进行分析维护，包括：日志配置、日志分析、日志备份等。

做好巡检记录，维护记录单，提交巡检报告。

### 1.2服务频率

每2月至少巡检1次，春节、两会、劳动节、国庆节等节假日或重点时期加强巡检。

### 1.3服务范围

管委会机关、北京站地区、北京西站地区、北京南站地区、北京北站地区、清河站地区、北京朝阳站地区、北京丰台站地区、城管分局机关、城市副中心办公区、北京首都国际机场办公区、北京大兴国际机场办公区等。

### 1.4服务成果

提交《系统巡检报告》。

## 2.脆弱性检测

### 2.1服务内容

针对信息系统服务器操作系统、数据库、中间件、网络及安全设备等，采用工具扫描和手工检查相结合的方式，进行脆弱性检查，以发现在网络、主机、应用等层面存在的安全隐患，通过专业化的技术分析，帮助采购人了解自身信息系统的脆弱性。

### 2.2服务频率

每年至少提供一次服务。

### 2.3服务范围

管委会机关、北京站地区、北京西站地区、北京南站地区、北京北站地区、清河站地区、北京朝阳站地区、北京丰台站地区、城管分局机关、城市副中心办公区、北京首都国际机场办公区、北京大兴国际机场办公区等。

### 2.4服务成果

提交《脆弱性检测报告》。

## 3.渗透测试

### 3.1服务内容

模拟黑客攻击等行为，对采购人指定域名进行非破坏性的渗透测试，分析应用系统所面临的安全威胁和存在的风险，编制渗透测试分析报告。渗透测试为开展安全加固及优化建设提供依据，并指导实施调优及加固工作，渗透测试报告应详细记录测试过程并对测试问题进行总结分析。

### 3.2服务频率

每年至少提供一次服务。

### 3.3服务范围

采购人指定的信息系统（管委会网站、财务内控系统、档案管理系统、视频监控系统及其子系统、交通数据处理平台及子系统等）。

### 3.4服务成果

提交《渗透测试报告》。

## 4.信息安全自查

### 4.1服务内容

需依据采购人实际的自查需求，开展信息安全自查协助服务。通过开展自查，进一步梳理、掌握重要网络与信息系统基本情况。信息安全自查内容包括：信息安全制度落实、安全防护工作落实、应急响应机制建设、安全教育培训等内容。使得采购人的信息安全自查方法得当，确保自查效果，及时从自查工作中发现潜在的安全风险，切实做好自查工作。

4.2服务频率

每年至少提供一次服务，并根据采购人要求，增加安全自查服务。

### 4.3服务范围

管委会机关、北京站地区、北京西站地区、北京南站地区、北京北站地区、清河站地区、北京朝阳站地区、北京丰台站地区、城管分局机关、城市副中心办公区、北京首都国际机场办公区、北京大兴国际机场办公区等。

### 4.4服务成果

提交《信息安全自查报告》。

## 5.安全加固

### 5.1服务内容

根据脆弱性检测等工作结果，结合采购人业务需求，通过技术手段对系统相关设备和配置，进行安全策略加强、调优，加强系统抵御攻击和威胁的能力，整体提高系统安全防护水平。

同时，根据信息化行业主管部门通知要求，对管委会信息化设备和信息系统自查后，进行整改，排除系统隐患，提升管委会信息安全技术水平。

### 5.2服务频率

每年至少提供一次服务，并根据采购人业务要求，增加安全加固服务。

### 5.3服务范围

管委会机关、北京站地区、北京西站地区、北京南站地区、北京北站地区、清河站地区、北京朝阳站地区、北京丰台站地区、城管分局机关、城市副中心办公区、北京首都国际机场办公区、北京大兴国际机场办公区等。

### 5.4服务成果

提交《安全加固报告》。

**6.应急演练**

### 6.1服务内容

根据应急预案规定的应急处理流程协助编制应急演练方案，并进行相应模拟演练，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订，使得相关人员了解应急流程和自己的责任，在安全事件发生时，能有条不紊开展工作，最大程序降低安全事件带来的负面影响和损失。

### 6.2服务频率

每年至少提供一次服务，并根据采购人业务要求，增加相关服务。

### 6.3服务范围

管委会机关、北京站地区、北京西站地区、北京南站地区、北京北站地区、清河站地区、北京朝阳站地区、北京丰台站地区、城管分局机关、城市副中心办公区、北京首都国际机场办公区、北京大兴国际机场办公区等。

### 6.4服务成果

提交《应急演练报告》和《应急演练方案》。

## 7.应急响应

### 7.1服务内容

在服务期间，提供7\*24小时应急响应服务，针对采购人发起的应急需求，能够快速响应。在信息系统发生安全事件时及时响应，执行应急响应流程，应通过专家级技术支持和快速响应，及时抑制和消除信息系统安全事件，减少损失和负面影响，提高信息系统业务安全性、连续性。

紧急安全事故包括：大规模病毒爆发、网络入侵事件、拒绝服务攻击、主机或网络异常事件等。在发生安全事件时按照安全事件的等级进行处理，并在事后进一步分析原因，提供详细的事件响应报告。

根据采购人需求，提供网络安全咨询和网络安全培训。

### 7.2服务频率

本项服务在服务期内按需提供。

### 7.3服务范围

管委会机关、北京站地区、北京西站地区、北京南站地区、北京北站地区、清河站地区、北京朝阳站地区、北京丰台站地区、城管分局机关、城市副中心办公区、北京首都国际机场办公区、北京大兴国际机场办公区等。

### 7.4服务成果

提交《安全事件应急响应报告》。

# 六、项目团队要求

供应商须为本项目组建稳定的、专业的、独立的服务团队，确定人员岗位分工和职责，须在北京设立专门的服务机构，专门负责本项目的安全服务工作。供应商应拥有网络安全方面专业的技术专家，能够及时关注网络及安全设备技术的发展，跟踪最新的网络和安全设备发现的问题或缺陷，搜集整理安全状态、设备漏洞信息、系统补丁信息、病毒信息等。

拥有稳定的服务保障队伍，并具有较强的技术保障实力，遇到突发情况时能够及时解决问题；服务团队有明确分工和侧重点，基本人员均掌握运维服务方法，能解决常见设备的故障问题。

需为本项目提供1名项目经理和至少2名项目核心技术人员作为支持。同时应为本项目组建安全运维团队，负责本项目的安全运维工作，具体要求如下：

项目经理：具备5年及以上网络安全工作经验；具有网络安全相关专业中级及以上职称。

项目核心人员：具备5年及以上网络安全工作经验；具有网络安全相关专业中级及以上职称。

项目团队人员：具备3年以上网络安全工作经验；具有网络安全相关专业中级及以上职称。

**七、本项目采购标的所属行业为：**

《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）中的**软件和信息技术服务业**。