合同编号：ZB-FW-2024-13

# 北京城管网络安全服务政府采购合同
# （第一包：基础网络安全）

甲　方：北京市城市管理综合行政执法局执法保障中心

法定代表人：袁荣林

地　址：北京市西城区三里河东路 39 号

邮　编：100045

联系人：王新烨

电　话：010-68538005

乙　方：奇安信网神信息技术（北京）股份有限公司

法定代表人：冯新戈

地　址：北京市西城区西直门外南路 26 号院 1 号楼 2 层

邮　编：100044

联系人：姜程子

电　话：010-62972893

根据《中华人民共和国民法典》有关规定，以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）等为项目主要实施依据，甲、乙双方本着互惠互利、诚实守信的原则，就乙方向甲方提供【北京城管网络安全服务（第一包：基础网络安全服务）】相关事宜达成本合同，以资共同遵守：

## 一、服务内容及期限

落实本地基础网络安全服务，统筹政务云安全工作，通过合理使用各类网络安全设备及工具，对系统的安全状态进行监控，及时发现正在发生的安全问题以及现有的潜在安全风险，并快速定位问题，处理问题。根据实际环境情况，有针对性加强安全管理，完善安全设备告警规则，定期做好专题培训，有力保障本地基础网络安全。

### （一）网络安全风险管理

#### 1.基础安全运维

结合市城管执法局业务与网络安全现状服务应提供一名政府部门安全运维经验丰富的人员在市城管执法局开展现场驻场服务工作，对网络安全设备运行监控、配置信息系统安全访问策略、及时响应信息系统故障并协助处置、排除网络信息系统安全隐患。

围绕业务系统开展常态化安全服务，对于发现的安全风险，统筹协调各业务系统运维团队、政务云安全服务商开展安全风险的分析跟踪工作，形成安全风险的闭环管理机制。

服务范围：市城管执法局所有业务系统及网络安全设备的安全管理，包含但不限于以下工作：

（1）安全设备运维报告：提供安全设备运行报告。

（2）系统配置管理：提供安全设备的配置管理、维护和恢复服务。

（3）协助市城管执法局开展安全风险隐患的跟踪处置。跟踪处置工作不限于上级监管单位通告的安全事件、自主发现的安全隐患。

（4）针对安全设备提供策略配置、安全性配置的技术支持服务。

（5）对安全设备的使用、软件安装提供技术支持服务。

服务频次：服务期内提供 1 人的驻场基础安全运维。

服务成果：安全运维月度总结报告。

**2. 漏洞扫描**

服务商根据市城管执法局网络安全现状与操作系统现状，在保障不影响业务系统正常运行且安全的前提下开展网络安全漏洞扫描工作，检查当前网络环境与业务系统对应的操作系统主机是否存在安全风险。针对发现的安全漏洞根据不同安全风险出具解决建议，持续跟踪漏洞整改情况，协助完成安全漏洞的整改加固工作。

服务范围：市城管执法局服务器主机、交换机、路由器、安全设备（防火墙、堡垒机、vpn、安全沙箱等）等。

服务频次：服务期内对本地及云上各开展 12 次。

服务成果：漏洞扫描报告及整改建议。

**3. 配置核查**

服务商根据市城管执法局网络安全现状，通过自动化与人工相结合的方式对当前市城管执法局运行在网络中的网络设备、安全设备、服务器、中间件、数据库开展配置核查，对配置存在的安全缺陷指导相应的业务支撑单位完成修复工作，确保配置满足国家网络安全法律法规与标准要求。

服务范围：市城管执法局服务器主机、交换机、路由器、安全设备（防火墙、堡垒机、vpn、安全沙箱等）等。

服务频次：服务期内开展 3 次。

服务成果：配置核查报告。

**4. 互联网敏感信息泄露检测**

服务商从红队视角分析市城管执法局的敏感信息泄露情况。探测范围覆盖互联网的各种信息泄露渠道。

敏感信息包含：仿冒网站信息、敏感目录信息、账号口令信息、文档泄露信息（网站业务代码、业务操作手册、运维文档、操作日志）、人员信息泄露（身份信息、联系方式、邮箱信息）等。

服务范围：各类网盘、文库、社交平台搜索引擎、代码托管平台等开放互联

网环境存在关于城管执法工作的敏感信息。

服务频次：服务期内开展 1 次。

服务成果：敏感信息泄露情报汇总表、敏感信息泄露情报分析报告。

**5. 安全预警**

服务商应实时关注国家应急响应中心、各类安全论坛等安全性组织发布的网络安全动态与信息安全漏洞与安全风险信息。针对网络安全态势、重大舆情信息、重要系统漏洞及补丁信息等信息，服务商应通过邮件、电话、当面沟通、微信公众号等形式以最快时间向市城管执法局告知漏洞危害、影响范围及应对方案，确保能够快速对预警信息进行收集、排查与处置。

服务范围：市城管执法局服务器主机、交换机、路由器、安全设备（防火墙、堡垒机、vpn、安全沙箱等）等。

服务频次：服务期内提供安全预警通报支撑。

服务成果：安全预警通告。

**6. 渗透测试**

服务商应在市城管执法局授权的前提下有组织有计划对指定的业务系统进行渗透测试。确保在业务系统稳定运行的基础上从主机、应用、中间件、业务逻辑处理等维度开展非破坏性的安全检测，检查是否存在漏洞，并在测试完成后提供渗透测试报告协助系统运维单位开展安全漏洞的整改加固工作与漏洞复测工作。渗透测试内容包含但不仅限于如下场景：

（1）应用渗透测试：包括 SQL 注入、XSS、XXE、CSRF、RFI、上传漏洞、信息泄露、远程命令执行、反序列化漏洞等。

（2）中间件渗透测试：对 IIS、apache 等常见中间件进行已知安全漏洞验证和默认策略安全检测。

（3）主机渗透测试：包括域传送漏洞、弱口令漏洞、未授权访问漏洞、脚本密码检查、本地提权漏洞、应用防护软硬件缺陷等。

（4）业务逻辑安全：业务逻辑安全测试范围包括用户或口令枚举、弱口令测试、平行/垂直越权、未授权访问、验证缺陷、业务逻辑限制缺陷等。

服务范围：市城管执法局指定的业务系统。

服务频次：对主机服务器部署的业务系统开展 1 次渗透测试初测与复测工作。

服务成果：渗透测试初测报告、渗透测试复测报告、漏洞汇总表。

**7.重保安全值守**

服务商应具备在重要时期的网络安全保障支撑能力，确保在重要时期能够安排保障值守人员开展7×24小时现场网络安全保障工作，提升在保障期间的问题处置效率，服务商应能够根据市城管执法局的安全保障要求开展保障工作，在发现安全问题时，能够及时进行处理，提高网络安全应急响应与保障能力。

服务范围：市城管执法局服务器主机、交换机、路由器、安全设备（防火墙、堡垒机、vpn、安全沙箱等）等。

服务频次：服务期内不少于30人天。

服务成果：重要时期安全值守工作总结。

**8.安全培训**

服务商应根据网络安全、数据安全与等级保护测评等相关法律法规，结合日常工作开展中存在的安全风险及隐患，开展有关日常安全意识、网络安全技术技能、网络安全法律法规等维度的安全培训，提升市城管执法局网络安全风险防范意识。

服务范围：市城管执法局工作人员及业务系统运维人员。

服务频次：服务期内4学时。

服务成果：安全培训课件、安全培训视频。

**（二）应急体系管理**

**1.应急演练**

服务商应在演练前制定应急预案，并在市城管执法局指定的场景下搭建应急演练环境，模拟发现确切的安全事件的情形，组织开展安全应急演练工作，检验市城管执法局安全保障体系是否具备安全事件的监测能力、应急演练预案是否合适、安全运维人员是否有基本的安全事件处置能力等。应急演练内容应不限于应急演练方案的制定、演练用例的生成、演练结果的评估等。并在演练结束后，应提供安全应急演练过程、安全保障体系缺陷、应急预案弱点、安全运维人员的安全事件处置能力评测以及相应的改进建议的应急演练报告。

服务范围：市城管执法局指定的应急演练场景。

服务频次：服务期内开展2次。

服务成果：应急演练方案、应急演练报告。

**2.红队评估**

服务商应具备组织开展红队评估的技术水平，并在市城管执法局授权的前提下有计划、有组织的开展红队评估工作。通过实战化方式，最大限度模拟 APT 攻击手法，以专业的团队视角对市城管执法局网络安全防护情况进行监测。以不采用破坏性攻击为底线，利用系统提权、控制业务、获取数据为目标的攻击手段，最大程度暴露安全风险及安全防护短板，深入评估安全防护能力。

评估点包括：

（1）系统：深入的红队攻击将测试并暴露多个领域的漏洞。

（2）整体 IT 架构防护能力：网络、应用、路由器、交换机、电子设备等。

（3）人员：市城管执法局执法保障中心、应用系统开发运营单位和网络运维单位等。

（4）安全监控能力：日志保存、审计能力、APT 攻击发现响应能力。

服务范围：市城管执法局指定业务系统。

服务频次：服务期内开展 1 次。

服务成果：红队评估工作方案、红队评估总结报告。

**3.应急响应**

服务商应具备 7×24 小时的应急响应协同处置能力水平。当市城管执法局发生大规模病毒爆发、网站被篡改、数据被恶意删除等确切的安全事件时，服务商应能够快速安排应急响应人员及时采取行动，限制事件扩散和影响的范围，控制潜在的损失与破坏，并协助开展安全事件攻击行为的溯源分析工作。服务商应在接到市城管执法局应急响应电话通知后 15 分钟做出响应，1 小时内到达现场开展响应处置工作。

服务范围：市城管执法局全部信息系统（包括：应用系统、网络设备、服务器、终端等）。

服务频次：服务期间内按需提供应急响应处置工作。

服务成果：应急响应报告。

**（三）威胁监测与分析**

**1.代码审计**

服务商应具备安全开展代码审计的能力。利用审计工具和人工专业代码安全审计人员相结合的方式进行代码安全审查。从应用系统开发框架、应用程序、客户端程序、接口及第三方组件和应用配置等方面进行深入的安全检测、审查和分析，从而发现应用系统源代码存在的安全缺陷和漏洞。为降低工具使用风险，规避代码泄露的安全隐患。代码审计内容包含但不仅限于如下：

（1）能够对源代码安全缺陷检测与分析，包括但不限于对跨站脚本、代码注入、API 误用、密码管理、配置管理、危险函数、异常处理、资源管理、代码质量等类别的安全缺陷检测、审查和分析。

（2）能够对应用系统中所使用的开源组件进行安全漏洞检测和分析，评估开源模块对软件整体造成的安全风险。

（3）能够对应用系统的业务应用安全规范进行分析，包括应用系统注册、登录、短信接口、文件上传、后台命令执行、输入和输出等应用软件编码安全进行检测、审查和分析。

服务范围：市城管执法局指定业务系统的代码审计，不少于 30 万行，Java 语言，含复测。

服务频次：服务期内开展 1 次。

服务成果：代码审计报告。

**2.安全软件更新（Windows 系统）**

服务商应在不造成业务影响的前提下对 44 台 Windows 服务器提供 1 年的终端安全管理系统软件更新，提供防病毒功能服务、补丁更新服务的授权，包括 Windows 服务器补丁管理功能模块，维保服务 1 年。对 50 台 Windows PC 终端安全管理系统进行软件更新，以及防病毒功能服务、补丁更新服务、运维管控服务的授权，维保服务 1 年。含每月一次原厂现场服务。

服务范围：市城管执法局环境中部署服务器版终端安全管理软件的系统。

服务频次：服务期内全年开展。

服务成果：软件升级授权、软件升级记录。

**3.安全软件更新（信创系统）**

服务商应在不造成业务影响的前提下对 47 台信创服务器终端安全管理系统进行软件更新，以及服务器杀毒服务和安全审计服务的授权，维保服务 1 年。对

448 台信创 PC 终端安全管理系统进行软件更新，以及通用终端防病毒服务、终端管控服务、终端审计服务的授权，维保服务 1 年。含每月一次原厂现场服务。

服务范围：市城管执法局环境中部署服务器版终端安全管理软件的系统。

服务频次：服务期内全年开展。

服务成果：软件升级授权、软件升级记录。

**4.全流量安全威胁检测**

服务商应通过对网络流量或日志进行实时动态分析。结合威胁情报、失陷主机行为特征分析规则和深度学习模型，发现隐藏在海量流量中的可疑活动和安全威胁，并对检测结果提供丰富的上下文信息与可视化分析，并进行持续监控，提升市城管执法局对网络的检测与响应能力。

服务范围：市城管执法局网络环境中业务数据流量。

服务频次：服务期内按需提供。

服务成果：全流量安全威胁检测报告。

**5.特权账号检测**

服务商应以攻击方视角检测市城管执法局账号、口令是否存在安全隐患，形成从风险检测、风险整改到账号口令运维的特权账号检测运维体系，做到风险整改闭环。主要对 IT 基础设施资源进行账号梳理，高效发现账号风险并及时处置；实现对特权账号全生命周期的管理，从而提升工作效率。

服务范围：市城管执法局网络环境中业务数据流量。

服务频次：服务期内开展 1 次。

服务成果：特权账号检测报告。

**（四）数据安全体系管理**

**1.数据安全 API 评估**

服务商通过对市城管执法局互联网及政务外网系统使用的 API 接口开展数据安全 API 评估，全面了解 API 接口当前的安全状况，分析系统所面临的各种风险，模拟攻击者检测可利用的漏洞，分析业务系统的 API 接口是否存在数据安全风险，并提供加固建议。

服务范围：市城管执法局互联网及政务外网上的重点业务系统的 API 接口、处理重要数据的接口开展 API 接口。

服务频次：服务期内开展不少于 560 个 API 接口。

服务成果：数据安全 API 接口安全风险报告。

（二）项目交付物（下表内容可根据甲方要求调整）

| 序号 | 交付物名称 | 相关材料 | 备注 |
|---|---|---|---|
| 1 | 网络安全风险管理类成果 | 安全运维月度总结报告 | 包含 12 份安全运维月度报告 |
| 2 | | 漏洞扫描报告及整改建议 | 包含 12 份漏洞扫描报告及整改建议 |
| 3 | | 配置核查报告 | 包含 3 份配置核查报告 |
| 4 | | 敏感信息泄露情报汇总表、敏感信息泄露情报分析报告 | |
| 5 | | 安全预警通告 | 根据实际情况提供 |
| 6 | | 渗透测试初测报告、渗透测试复测报告、漏洞汇总表 | |
| 7 | | 重要时期安全值守工作总结 | 根据实际情况提供 |
| 8 | | 安全培训课件和视频 | 根据实际情况提供 |
| 9 | 应急体系管理类成果 | 应急演练方案、应急演练报告 | |
| 10 | | 红队评估工作方案、红队评估总结报告 | |
| 11 | | 应急响应报告 | 根据实际情况提供 |
| 12 | 威胁监测与分析类成果 | 代码审计报告 | 根据实际情况提供 |
| 13 | | 软件升级记录、软件升级授权（Windows 系统和信创系统） | 包含 12 份软件升级记录，1 份软件升级授权 |
| 14 | | 全流量安全威胁检测报告 | 包含 12 份全流量安全威胁检测报告 |
| 15 | | 特权账号检测报告 | |
| 16 | 数据安全体系管理类成果 | 数据安全 API 接口安全风险报告 | |
| 17 | 服务满意度调查分析报告 | - | |
| 18 | 网络安全服 | 阶段性总结报告、年度总结报告等 | |

| | | | |
|---|---|---|---|
| | 务阶段性总结报告 | | |

服务期限：12 个月。自 2024 年 4 月 28 日起至 2025 年 4 月 27 日。

**二、付款**

1. 甲乙双方之间发生的一切费用均以人民币进行结算及支付。

2. 本合同价款总计人民币 壹佰肆拾贰万 元整（¥ 1420000.00 元）。合同价款系乙方完全履行本合同后甲方所需支付的全部费用，甲方无需再向乙方支付其他任何费用。

3. 乙方应在合同生效后的 10 个工作日内，甲方向乙方支付项目合同款项的 60%，即人民币 捌拾伍万贰仟 元整（¥ 852000.00 元）。

于 2024 年第四季度，甲方向乙方支付 2024 年预算安排剩余部分，即人民币 贰拾捌万肆仟肆佰捌拾 元整（¥ 284480.00 元）；

于 2025 年第一季度，甲方向乙方支付 2025 年预算安排的 50%，即人民币 壹拾肆万壹仟柒佰陆拾 元整（¥ 141760.00 元）；

于 2025 年项目完成并验收合格后，甲方向乙方支付项目尾款，即人民币 壹拾肆万壹仟柒佰陆拾 元整（¥ 141760.00 元）。

乙方须在甲方付款前，向甲方提供正式等额发票。

4. 乙方银行账户信息如下：

公司名称：奇安信网神信息技术（北京）股份有限公司

开户银行：招商银行北京建国路支行

账　　号：110902261210404

乙方保证上述信息真实、准确，乙方的上述账户信息发生变化的，应至少于甲方付款 5 个工作日前书面通知甲方（通知应加盖乙方公章或财务章）。如因乙方未及时通知或通知有误而影响甲方支付本合同款项，甲方将不承担逾期付款的任何责任，由此导致的错付、无法支付等所有法律后果均由乙方自行承担。

**三、甲方权利义务**

1. 甲方应向乙方人员提供必要的工作场地，并安排工作人员配合乙方工作。

2. 甲方负责向乙方提供与安全服务有关的必要数据、文件和资料，如甲方未能及时提供上述条件而导致乙方无法按期完成测试任务的情况，不视为乙方违约。

3. 如因甲方原因未能完全执行本合同项下约定的服务，由此引起的一切后果由甲方自行承担。

4. 甲方应按本合同约定按时向乙方支付合同款项。

5. 在合同服务范围内，如因乙方原因导致出现重大安全事故，甲方有权解除合同，要求乙方返还已经支付的所有合同价款，并要求乙方承担本合同总价款【1】%的违约金。给甲方造成损失的，乙方还应当全部赔偿。

**四、乙方权利义务**

1. 乙方应指派具有相应资格和能力的专业人员，按本合同约定内容和甲方要求向最终客户提供安全服务，保障市城管执法局网络安全。

2. 乙方保证提供服务的技术人员的数量和素质满足履行本合同的要求，未经过甲方同意不得随意更换本合同约定提供服务的技术人员；如果甲方认为乙方派出的人员不能胜任工作，甲方有权向乙方提出更换人员的要求，经甲方确认后，乙方应按甲方要求限期更换符合甲方要求的技术人员。

3. 乙方技术人员提供现场服务期间应严格遵守甲方相关制度和纪律。

4. 在项目过程中产生的成果，其知识产权成果归属甲方所有。乙方保证其提供的网络安全服务不侵犯任何第三方的知识产权、所有权或使用权，否则由此引发的一切责任由乙方承担。

5. 未经甲方事先书面同意，乙方不得将本合同服务内容转包、分包或以其他形式将本合同服务事项交由第三方完成，否则由此引发的一切责任由乙方承担。

6. 乙方承诺和保证其委派的技术人员是乙方的聘用员工，与乙方之间存在劳动关系。

7. 乙方将自行保障和负责其委派人员的人身及财产安全，乙方人员在服务过程中造成的人身伤害或财产损失，由乙方承担相应的法律责任。

8. 乙方应妥善保管甲方提供的与安全服务有关的必要数据、文件和资料，测试任务完成或本合同终止/解除后，乙方应将上述内容完整返还给甲方，如经甲方确认无需或无法返还的，乙方应及时将其彻底删除或销毁，乙方不得将甲方的上述数据泄露给任何第三方。

9. 乙方承诺配合网络安全审查，并承诺不利用提供产品和服务的便利条件非法获取甲方数据、非法控制和操纵甲方设备，无正当理由不中断产品供应或必要

的技术支持服务。

五、验收

1. 项目验收标准。项目服务内容全部按甲方要求实施完毕，乙方提供的运维服务满足运维服务标准：（1）重大网络安全事件发生次数为 0 次；（2）安全意识宣贯不少于 4 课时；（3）安全值守人天数不少于 30 人天；（4）文本报告能体现项目工作执行的全过程；（5）信息系统安全隐患检查率不低于 90%；（6）安全事件及时处理率不低于 90%；（7）应急响应时间在 30 分钟内；（8）系统正常运行率≥90%；（9）网络和系统用户满意度≥95%。

2. 合同中约定的各项内容全部执行完毕，项目交付物必须满足质量要求，各项交付物全部通过甲方审核并交付甲方，满足甲方验收条件。

3. 项目验收。乙方完成全部服务后【10】日内向甲方提交工作总结报告和验收申请表，甲方按本合同约定验收标准进行验收。如甲方对乙方提供的服务存在异议，应自收到乙方提供的测试验收报告后 3 个工作日内以书面形式向乙方提出，乙方应在【10】日内向甲方提交整改方案并按甲方要求限期整改。如果整改后仍不符合甲方要求的违约责任条款。由此产生的费用和责任由乙方承担。符合验收标准及交付相关文档后，具体时间和地点由甲乙双方商议安排，验收结果出具书面意见，双方共同签署项目验收报告。

4. 如甲方指定第三方进行验收的，第三方验收结果视为甲方验收，验收责任由甲方承认并承担。

六、责任限制

1. 合同任何一方无需就对方间接的、附带的损害和损失（包括但不限于：预期收益、利润、商业机会、营业中断、资讯丢失等）向对方承担责任。

2. 乙方无须就下列情形承担责任。

(1) 产品使用者操作、使用不当导致的损失；

(2) 乙方以外的任何单位和个人修改或改动产品所引致的损害。

但是乙方有义务协助甲方避免或减轻上述损失或损害的发生或扩大。

七、保密条款

1. 未经对方书面许可或本合同另有约定，任何一方不得向与履行本合同无关的第三方（有关法律、法规、政府部门、证券交易所或其它监管机构要求除外）

泄露本合同条款的任何内容以及本合同的签订及履行情况，以及通过签订和履行本合同而获知的对方及对方关联公司的任何信息。但为本合同履行之需任何一方可向其法律、会计、商业及其它顾问、授权雇员（“接收方代表”）披露前述信息，接收方代表应同意承担与本合同中所规定的保密义务相同或更严格的保密义务。

2. 在任何情形下，本条所规定的保密义务应永久持续有效，不因本合同变更、终止或解除而失效。

3. 本合同约定的保密义务适用于乙方及其人员，乙方人员违反保密义务的，视为乙方违约。

八、违约责任

1. 任何一方违反本合同的任何条款，或不承担或不及时、充分地承担本合同项下其应承担的义务即构成违约行为，守约方有权以书面通知要求违约方纠正其违约行为并采取充分、有效、及时的措施消除违约后果，并赔偿守约方因违约方之违约行为而遭致的全部损失。若违约方在收到守约方关于其违约行为的上述通知后 10 日内未纠正其违约行为，守约方有权以书面通知的方式单方提前终止本合同，并追究违约方之违约责任。

2. 在违约事实发生以后，经守约方的合理及客观的判断，该等违约事实已造成守约方履行本合同项下其相应的义务已不可能或不公平，则守约方有权以书面形式通知违约方提前终止本合同，违约方应赔偿守约方因违约方之违约行为而遭致的全部损失。

3. 甲方应按本合同规定，按期向乙方支付到期款项。如因甲方原因导致的甲方逾期支付，则每逾期一日，甲方需按逾期金额的 1‰向乙方支付违约金。如逾期 30 日甲方仍未支付，则乙方有权解除本合同，甲方应按合同总额【1】%向乙方支付违约金。但甲方因财政拨款延迟等原因导致的延期付款除外。

4. 乙方保证其有相应资质和能力签订和履行本合同。否则，乙方应按合同总额的【1】%向甲方支付违约金，并赔偿因此给甲方造成的全部损失。同时，甲方有权解除本合同，要求乙方退还甲方已支付的全部费用。

5. 乙方擅自将本合同服务内容转包、分包或以其他形式将本合同服务事项交由第三方完成，应按合同总额的【1】%向甲方支付违约金。同时，甲方有权解除本合同，要求乙方退还甲方已付全部款项。

6. 乙方未经甲方事先书面同意擅自更换驻场人员，或驻场人员擅自离岗，或未按甲方要求限期更换服务人员的，应每人每次向甲方支付合同总额【1】%的违约金。违约金不足以弥补甲方损失的，乙方应予以补足。累计超过【2】人次的，甲方还有权解除合同，并要求乙方退还甲方已支付的全部费用。

7. 乙方应保证其提供的服务均合法、合规且不侵犯第三方的合法权益。若违反本项约定，乙方应负责解决因此产生的一切纠纷，承担全部法律责任和经济赔偿，应按合同总额的【1】%向甲方支付违约金，并赔偿因此给甲方造成的全部损失。同时，甲方还有权解除本合同，乙方应退还甲方已支付的全部费用。

8. 乙方应保证满足合同中第七条规定的保密条款，如有违反，违约方应向守约方支付合同总额【1】%的违约金，并承担由此给守约方造成的一切损失。

9. 乙方违反本合同约定其他义务或履行合同义务不符合约定的，每发生一次，除应按甲方要求限期纠正外，应按合同总额的【1】%向甲方支付违约金。违约金不足以弥补损失的，乙方应予以补足。

10. 本合同约定损失包括但不限于守约方经济利益的减损、守约方为证实违约行为所支付的调查取证、公证费用、守约方为寻求救济所支付的诉讼费、保全费、律师代理费、咨询费和法院执行费用、评估鉴定费、差旅费等全部损失及费用。

**九、不可抗力**

1. 本合同中，不可抗力是指不能预见、不能避免并不能克服的客观情况，包括：战争、火灾、洪水、台风、地震、政策变化或其他人力不可抗拒之事件。

2. 因不可抗力事件导致本合同无法履行或迟延履行，双方均免责，但遭受不可抗力事件的一方应于不可抗力情形发生之日起【5】日内及时通知另一方，并在事件发生后 15 日内提供法定机构出具的有效证明。

3. 不可抗力事件解除后，双方将积极配合，继续履行本合同。

**十、争议解决**

双方对执行合同发生的争议，本着友好协商的原则解决；经协商不能解决的，则应向甲方所在地有管辖权的人民法院提起诉讼解决。

**十一、其他条款**

1. 对本合同的任何修改必须以书面的形式作出，并且由双方盖章后方为有效。

2. 双方因履行本合同或与本合同有关的一切通知都必须按照本合同中的地址，以书面形式或双方确认的传真或类似的通讯方式进行。采用信函形式的应使用挂号信或具有良好信誉的特快专递送达。如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。

3. 本合同载明的地址、电话、银行账号等发生变更的，变更一方应自变更之日起【5】日内以书面形式通知对方。否则变更一方应自行承担因通知不及时所造成的一切后果。

十二、合同的效力

1. 本合同一式【陆】份，甲、乙双方各执【叁】份，具有同等法律效力，自双方法定代表人或授权代表签字或签章并加盖公章之日起生效至合同履行完毕之日终止。

2. 本合同未尽事宜由双方友好协商解决，必要时双方可以另行签订补充合同。补充合同与本合同具有同等法律效力，补充合同与本合同有冲突的，以补充合同为准。

（本行以下无正文）

甲方：北京市城市管理综合行政执法局执法保障中心（盖章）

法定代表人或授权代表（签字或签章）：袁荣林

日期：2024年4月14日

乙方：奇安信网神信息技术（北京）股份有限公司（盖章）

法定代表人或授权代表（签字或签章）：

日期：2024年4月18日