合同编号：

网络运维费平谷法院基础环境运维服务采购项目

合同编号:

项目名称：网络运维费平谷法院基础环境运维服务采购项目

服务名称：网络运维费平谷法院基础环境运维服务采购项目

买　　方：北京市平谷区人民法院

卖　　方：北京中汇天成科技有限公司

签署日期：2026.4.9

合　　同　　书

北京市平谷区人民法院（买方）网络运维费平谷法院基础环境运维服务采购项目（项目名称）中所需（信息化运维服务）经（北京国壹咨询有限公司）以号竞争性磋商文件在国内　/　（竞争性磋商）招标。经评标委员会评定（北京中汇天成科技有限公司）为成交供应商。买、卖双方同意按照下面的条款和条件，签署本合同。

1、合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书

b. 成交通知书

c. 协议

d. 竞争性磋商文件（含澄清文件）

e. 响应文件　（含竞争性磋商文件补充通知）

2、服务和数量

本合同服务：信息化运维服务

数量：1

服务的质量约定：

服务期：自 2026 年 5 月 1 日起至 2027 年 4 月 30 日

3、合同总价

本合同总价为壹拾柒万陆仟柒佰元人民币，含 6%增值税普通发票。

分项价格：176,700.00

4、付款方式

本合同的付款方式为：分四期结算支付

第一期：合同签订之日起 1 个月内，向乙方支付 6 个月服务费；

第二期：服务当年 11 月 30 日前，向乙方支付 1 个月服务费；

第三期：服务当年 12 月 31 日前，向乙方支付 1 个月服务费；

第四期：服务期限届满后，向乙方支付本合同剩余全部服务费。

向乙方支付每一期服务费前，乙方应向甲方开具与当期应付服务费等额、合法、有效的发票，乙方按发票金额支付。

5、本合同的服务时间及服务地点

服务时间：自 2026 年 5 月 1 日起至 2027 年 4 月 30 日

服务地点：买方指定

6、合同的生效

本合同经双方全权代表签署、加盖单位公章后生效。

买　方：北京市平谷区人民法院

名　称：(印章)

2026 年 4 月 9 日

授权代表(签字)：

地　　址：北京市平谷区府前西街 21 号

邮政编码：101200

电　　话：010-89966803

开户银行：

帐　　号：111102260000286608

卖　方：北京中汇大成科技有限公司

名　称：(印章)

2026 年 4 月 9 日

授权代表(签字)：

地　　址：北京市丰台区花乡纪家庙 155 号 K22A

邮政编码：100070

电　　话：010-63729113

开户银行：招商银行股份有限公司北京万达广场支行

帐　　号：110910707110818

合同一般条款

1 定义

本合同下列术语应解释为：

1.1“合同”系指甲乙双方签署的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

1.2“合同价”系指根据本合同规定乙方在正确地完全履行合同义务后甲方应支付给乙方的价格。

1.3“货物”系指乙方根据本合同规定须向甲方提供的一切货物。

1.4“服务”系指根据合同规定乙方承担有关的服务任务，及合同中规定乙方应承担的其它义务。

1.5“合同一般条款”系指本合同一般条款。

1.6“甲方”系指采购人。

1.7“乙方”系指中标人，即提供本合同项下提供服务的公司或实体。

1.8“项目现场”系指本合同项下实施服务的现场。

1.9“日”系指日历日。

2、服务周期

服务合同期限：自 2026 年 5 月 1 日起至 2027 年 4 月 30 日。

3、服务内容/要求

3.1 详见招标文件第四章的规定，并与供应商投标文件的规格偏差表（如果被采购人接受的话）相一致。

3.2 若服务规范中无相应说明，则以国家有关部门最新颁布的相应标准及规范为准。

4、支付

本合同服务费分四期结算支付：

第一期：合同签订之日起 1 个月内，向乙方支付 6 个月服务费；

第二期：服务当年 11 月 30 日前，向乙方支付 1 个月服务费；

第三期：服务当年 12 月 31 日前，向乙方支付 1 个月服务费；

第四期：服务期限届满后，向乙方支付本合同剩余全部服务费。

向乙方支付每一期服务费前，乙方应向甲方开具与当期应付服务费等额、合法、

有效的发票，乙方按发票金额支付。

5、履约保证金

成交供应商在签订合同后10天内，按竞争性磋商文件中提供的履约保证金保函格式或买方可以接受的其他形式向买方提交合同总价10%的履约保证金。如派驻人员不符合要求、故障排除不及时等服务商过失，可视为违约进行处罚。甲方于该合同项目验收合格后10日内，将履约保证金退还至乙方指定账户。

6、价格

6.1　合同总价与投标价格一致。

7、服务质量保证

7.1 乙方应提供优质服务，保证服务质量，且不能低于合同规定的内容和标准。甲方将定期或不定期的对乙方提供的服务实行动态跟踪、检查。

7.2 乙方在收到甲方或使用单位关于服务质量问题的通知后三日内，应迅速查处并做出书面答复。

7.3 如果乙方在收到通知三日后没有弥补缺陷，甲方或使用单位可采取必要的补救措施，但风险和费用将由乙方承担。

8、转让

8.1 乙方不得将自己应履行的全部或部分合同义务转给第三方。

9、违约责任

9.1 乙方应遵守国家法律、法规的有关规定，严格按照本合同条款履行相关义务，否则甲方有权终止本合同，乙方应承担相应的违约责任。

9.2 因乙方服务失误造成的损失应由乙方赔偿全部损失。.

9.3 乙方有以下行为，甲方有权从乙方服务费中扣除相应罚款，最高不超过3000元。

乙方未按照合同约定提供服务，经甲方提出，没有明显改进的；

乙方未按合同约定人数提供服务工作人员，持续时间超过两个星期的。

10、索赔

10.1 如果在合同履行过程中，由于乙方违反合同规定义务导致甲方受到损失，乙方应按照甲方的实际损失予以赔偿。合同另有约定的按照约定执行。

10.2 乙方如有发生违约事项，甲方可单方面解除合同并要求乙方支付合同总金额5%的违约金。

11、不可抗力

11.1　本条所述的“不可抗力”系指那些双方在订立合同时无法控制、不可预见的事件。这些事件包括：战争、水灾、地震、甲方机构发生变化以及双方同意的事件。

11.2　在不可抗力事件发生时，一方应尽快以书面形式将不可抗力的情况和原因通知对方。同时必须在14日内，以挂号形式递交有关政府部门的证明。如果不可抗力超过120日，双方将通过友好协商就合同的执行达成协议。

12、税

12.1　中国政府根据现行税法对甲方征收的与本合同有关的一切税费均应由甲方负担。

12.2　中国政府根据现行税法对乙方征收的与本合同有关的一切税费均应由乙方负担。

13、争端的解决

13.1　合同履行或与合同有关的一切争端应通过双方友好协商解决。如果友好协商不能解决，任何一方当事人可以向有管辖权的人民法院提起诉讼。

13.2　在诉讼期间，除正在进行诉讼的部分外，本合同其他部分应继续执行。

14、违约终止合同

14.1　在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面违约通知书，提出解除部分或全部合同：

14.1.1 如果乙方未能在合同规定的限期或甲方同意延长的限期内提供部分或全部服务；

14.1.2 如果乙方未能履行合同规定的其它义务。

14.2　如果甲方根据上述第14.1条的规定，解除了全部或部分合同，甲方可以依其认为适当的条件和方法购买与未交服务类似的服务，乙方应对购买类似服务所超出的那部分费用负责。但是，乙方应继续执行合同中未解除的部分。

15、破产终止合同

15.1　如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方，终止合同而不给乙方补偿，该终止合同将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权力。

16、合同修改

16.1　任何对合同条款的变更或修改均须双方签订书面的修改文件。

17、通知

17.1　本合同任何一方给另一方的通知，都应以书面方式发送，而另一方应以书面形式确认并发送到对方明确的地址。

18、计量单位

18.1　除技术规范中另有规定外，计量单位均使用国家法定计量单位。

19、适用法律

19.1　本合同按照中国法律进行解释。

20、合同生效及其它

20.1 本合同应经双方法定代表人或授权代表签字并加盖供应商公章后生效。

20.2 下述合同附件为本合同不可分割的部分并与本合同具有同等法律效力：

1)服务内容及分项价格表

2)详细服务方案

3)服务周期

4)服务承诺

21、其他约定：

1.政府采购项目的采购合同内容的确定应以招标文件和投标文件为基础，不得违背其实质性内容。政府采购项目的采购合同自签订之日起七个工作日内，买方应当将合同副本报同级政府采购监督管理部门和有关部门备案。合同将在双方签字盖章并由卖方递交履约保证金后开始生效。

2.本合同一式__贰__份，具有同等法律效力。买方和卖方各执__壹__份。

附件一：技术文件

总体要求

1、服务地点：北京市平谷区人民法院指定

2、服务期限：自 2026 年 5 月 1 日起至 2027 年 4 月 30 日

一. 概况

确保关键信息基础设施与网络系统安全是保障北京市法院信息系统稳定、高效运行的前提。北京市平谷区人民法院结合了北京法院系统业务需求、网络规模、应用分布以及使用情况，在信息安全防护体系建设过程中，依据信息安全等级保护三级基本要求，以重点部位、重点业务进行重点保护为指导原则，北京市平谷法院网络划分为内网、互联网以及政务外网三大安全区域，逐一建立并完善其安全措施。经过信息安全防护体系建设，从不同层面增强了北京市平谷区人民法院信息系统的安全防护水平，形成了纵深防御体系，现已具备网络边界防护、安全威胁检测、安全事件审计与跟踪、病毒监控与阻断、数据库管控、运维审计、互联网行为审计以及操作系统行为管控等功能。具体部署的安全防护措施包括：

1) 防火墙
2) 核心防火墙
3) 防毒墙
4) 入侵检测系统
5) 安全审计系统
6) 网络版防病毒软件
7) 漏洞扫描系统
8) 终端安全管理系统
9) 数据库审计系统
10) 运维审计系统
11) 准入控制系统
12) 泰合安管平台系统

二．项目目标

北京市平谷区人民法院信息安全防护系统依据信息安全等级保护标准，结合当前信息安全技术发展态势和法院实际信息安全需求建立信息安全保障体系，通过安全运维等服务全面保障法院内网、互联网信息系统的完整性、保密性和可用性。

三．安全设备维护

3.1 本院内网主要设施

本院内网主要设施有边界防火墙 1 台、核心防火墙 2 台、防毒墙 1 台、入侵检测系统 1 台、漏洞扫描系统 1 台、安全审计系统 1 台、防病毒软件系统 1 套、终端安全管理系统 1 套、运维审计系统 1 台、数据库审计系统 1 台，准入控制系统 1 台、泰合安管平台系统 1 套，共计 10 台安全设备，3 套安全软件。

3.2 本院内网维护

3.2.1 边界防火墙

（1） 防火墙工作状况巡视。每天 1 次对所有防火墙的运行状况进行查看并将巡视结果记录到防火墙运行日志当中。

（2） 防火墙日志审查。每天 1 次对防火墙工作状况进行巡查，同时对各个防火墙的日志进行审查，并记录是否有异常事件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 防火墙策略巡查。每周 1 次对各个防火墙的策略设置进行巡查，并和备份的防火墙策略进行比对，查看防火墙策略是否被异常修改或丢失。

（4） 防火墙策略备份。每月 1 次对各个防火墙策略进行备份。同时，在主动修改了防火墙策略的情况下，要及时备份防火墙策略。

（5） 防火墙数据备份。每周 1 次对各个防火墙的日志和数据库进行备份。

（6） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（7） 防火墙密码保护。每年 1 次对防火墙的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。各个防火墙密码要求不使用同一个密码。（可根具秘密的相应程度作对应调整）防火墙策略修改。

（8） 防火墙资产管理。对防火墙进行资产标示与分类管理，定期对防火墙进行除尘处理。

（9） 防火墙规范操作。按操作规程实现防火墙的启动/停止、加电/断电等操作。

（10） 防火墙信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（11） 防火墙安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

（12） 在网络结构发生改变、应用系统要求和防范攻击的情况下，可以按照需要对防火墙策略进行必要的修改，在修改完成后要及时备份防火墙策略。凡是测试过程中发生的策略修改要在测试完成后立即恢复到原来状态。

3.2.2 核心防火墙

（1） 防火墙工作状况巡视。每天 1 次对所有防火墙的运行状况进行查看并将巡视结果记录到防火墙运行日志当中。

（2） 防火墙日志审查。每天 1 次对防火墙工作状况进行巡查，同时对各个防火墙的日志进行审查，并记录是否有异常事件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 防火墙策略巡查。每周 1 次对各个防火墙的策略设置进行巡查，并和备份的防火墙策略进行比对，查看防火墙策略是否被异常修改或丢失。

（4） 防火墙策略备份。每月 1 次对各个防火墙策略进行备份。同时，在主动修改了防火墙策略的情况下，要及时备份防火墙策略。

（5） 防火墙数据备份。每周 1 次对各个防火墙的日志和数据库进行备份。

（6） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（7） 防火墙密码保护。每年 1 次对防火墙的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。各个防火墙密码要求不使用同一个密码。（可根具秘密的相应程度作对应调整）防火墙策略修改。

（8） 防火墙资产管理。对防火墙进行资产标示与分类管理，定期对防火墙进行除尘处理。

（9） 防火墙规范操作。按操作规程实现防火墙的启动/停止、加电/断电等操作。

（10） 防火墙信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（11） 防火墙安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

（12） 在网络结构发生改变、应用系统要求和防范攻击的情况下，可以按照需要对防火墙策略进行必要的修改，在修改完成后要及时备份防火墙策略。凡是测试过程中发生的策略修改要在测试完成后立即恢复到原来状态。

3.2.3. 防毒墙

（1） 防毒墙工作状况巡视。每天 1 次对所有防毒墙的运行状况进行查看并将巡视结果记录到防毒墙运行日志当中。

（2） 防毒墙日志审查。每天 1 次在对防毒墙工作状况巡查的同时，对各个防毒墙进行日志审查，并记录是否有异常事件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 防毒墙策略巡查。每周 1 次对各个防毒墙的策略设置进行巡查，并和备份的防毒墙策略进行比对，查看防毒墙策略是否被异常修改或丢失。

（4） 防毒墙策略备份。每个月 1 次对各个防毒墙策略进行备份。同时，在主动修改了防毒墙策略的情况下，要及时备份防毒墙策略。

（5） 防毒墙数据备份。每周 1 次对各个防毒墙的日志和数据库进行备份。

（6） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（7） 防毒墙密码保护。每年 1 次对防毒墙的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。

各个防毒墙密码要求不使用同一个密码。（可根具秘密的相应程度作对应调整）

（8） 防毒墙资产管理。对防毒墙进行资产标示与分类管理，定期对防毒墙进行除尘处理。

（9） 防毒墙规范操作。按操作规程实现防毒墙的启动/停止、加电/断电等操作。

（10） 防毒墙信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（11） 防毒墙安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

（12） 在网络结构发生改变、应用系统要求和防范攻击的情况下，可以按照需要对防毒墙策略进行必要的修改，在修改完成后要及时备份防毒墙策略。凡是测试过程中发生的策略修改要在测试完成后立即恢复到原来状态。

3.2.4 入侵检测系统

（1） 入侵检测系统工作状况巡视。每天 1 次对所有入侵检测系统的运行状况进行查看并将巡视结果记录到入侵检测系统运行日志当中。

（2） 入侵检测系统日志审查。每天 1 次在对入侵检测系统工作状况巡查的同时，对各个入侵检测系统进行日志审查，并记录是否有异常事件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 入侵检测系统策略巡查。每周 1 次对各个入侵检测系统的策略设置进行巡查，并和备份的入侵检测系统策略进行比对，查看入侵检测系统策略是否被异常修改。

（4） 入侵检测系统策略备份。每月 1 次对各个入侵检测系统策略进行备份。同时，在主动修改了入侵检测系统策略的情况下，要及时备份入侵检测系统策略。

（5） 入侵检测系统数据备份。每周 1 次对各个入侵检测系统的日志和数据库进行备份。

（6） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（7） 入侵检测系统密码保护。每年 1 次对访问入侵检测系统的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。各个入侵检测系统密码要求不使用同一个密码。（可根据秘密的相应程度作对应调整）。

（8） 入侵检测系统资产管理。对入侵检测系统进行资产标示与分类管理，定期对入侵检测系统进行除尘处理。

（9） 入侵检测系统规范操作。按操作规程实现入侵检测系统的启动/停止、加电/断电等操作。

（10） 入侵检测系统信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（11） 入侵检测系统安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

（12） 入侵检测系统策略修改。在网络结构发生改变、应用系统要求和防范攻击的情况下，可以按照需要对入侵检测系统策略进行必要的修改，在修改完成后要及时备份入侵检测系统策略。凡是测试过程中发生的策略修改要在测试完成后立即恢复到原来状态。

3.2.5 漏洞扫描系统

（1） 漏洞扫描系统工作状况巡视。每天 1 次对所有漏洞扫描系统的运行状况进行查看并将巡视结果记录到漏洞扫描系统运行日志当中。

（2） 漏洞扫描系统日志审查。每天 1 次在对漏洞扫描系统工作状况巡查的同时，对各个漏洞扫描系统进行日志审查，并记录是否有异常事

件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 漏洞扫描系统策略巡查。每周 1 次对各个漏洞扫描系统的策略设置进行巡查，并和备份的漏洞扫描系统策略进行比对，查看漏洞扫描系统策略是否被异常修改。

（4） 漏洞扫描系统策略备份。每月 1 次对各个漏洞扫描系统策略进行备份。同时，在主动修改了漏洞扫描系统策略的情况下，要及时备份漏洞扫描系统策略。

（5） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（6） 漏洞扫描系统密码保护。每年 1 次对访问漏洞扫描系统的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。各个漏洞扫描系统密码要求不使用同一个密码。（可根据秘密的相应程度作对应调整）。

（7） 漏洞扫描系统资产管理。对漏洞扫描系统进行资产标示与分类管理，定期对漏洞扫描系统进行除尘处理。

（8） 漏洞扫描系统规范操作。按操作规程实现漏洞扫描系统的启动/停止、加电/断电等操作。

（9） 漏洞扫描系统信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（10）漏洞扫描系统安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

3.2.6 安全审计系统

（1） 安全审计系统工作状况巡视。每天 1 次对所有安全审计系统的运行状况进行查看并将巡视结果记录到安全审计系统运行日志当中。

（2） 安全审计系统日志审查。每天 1 次在对安全审计系统工作状况巡查的同时，对各个安全审计系统进行日志审查，并记录是否有异常事件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 安全审计系统策略巡查。每周 1 次对各个安全审计系统的策略设置进行巡查，并和备份的安全审计系统策略进行比对，查看安全审计系统策略是否被异常修改。

（4） 安全审计系统策略备份。每月 1 次对各个安全审计系统策略进行备份。同时，在主动修改了安全审计系统策略的情况下，要及时备份安全审计系统策略。

（5） 安全审计系统数据备份。每周 1 次对各个安全审计系统的日志和数据库进行备份。

（6） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（7） 安全审计系统密码保护。每年 1 次对访问安全审计系统的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。各个安全审计系统密码要求不使用同一个密码。（可根据秘密的相应程度作对应调整）。

（8） 安全审计系统资产管理。对安全审计系统进行资产标示与分类管理，定期对安全审计系统进行除尘处理。

（9） 安全审计系统规范操作。按操作规程实现安全审计系统的启动/停止、加电/断电等操作。

（10） 安全审计系统信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（11） 安全审计系统安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

3.2.7 防病毒软件系统

（1） 防病毒软件系统工作状况巡视。每天 1 次对所有防病毒软件系统的运行状况进行查看并将巡视结果记录到防病毒软件系统运行日志当中。

（2） 防病毒软件系统日志审查。每天 1 次在对防病毒软件系统工作状况巡查的同时，对各个防病毒软件系统进行日志审查，并记录是否有异常事件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 防病毒软件系统策略巡查。每周 1 次对各个防病毒软件系统的策略设置进行巡查，并和备份的防病毒软件系统策略进行比对，查看防病毒软件系统策略是否被异常修改。

（4） 防病毒软件系统策略备份。每月 1 次对各个防病毒软件系统策略进行备份。同时，在主动修改了防病毒软件系统策略的情况下，要及时备份防病毒软件系统策略。

（5） 防病毒软件系统数据备份。每周 1 次对各个防病毒软件系统的日志和数据库进行备份。

（6） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（7） 防病毒软件系统密码保护。每年 1 次对访问防病毒软件系统的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。各个防病毒软件系统密码要求不使用同一个密码。（可根据秘密的相应程度作对应调整）。

（8） 防病毒软件系统资产管理。对防病毒软件系统进行资产标示与分类管理，定期对防病毒软件系统进行除尘处理。

（9） 防病毒软件系统规范操作。按操作规程实现防病毒软件系统的启动/停止、加电/断电等操作。

（10）防病毒软件系统信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（11）防病毒软件系统安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

3.2.8 终端安全管理系统

（1） 终端安全管理系统工作状况巡视。每天 1 次对所有终端安全管理系统的运行状况进行查看并将巡视结果记录到终端安全管理系统运行日志当中。

（2） 终端安全管理系统日志审查。每天 1 次在对终端安全管理系统工作状况巡查的同时，对各个终端安全管理系统进行日志审查，并记录是否有异常事件发生。如果有异常事件-发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 终端安全管理系统游戏库升级。每月 1 次对终端安全管理系统游戏库进行升级，做好记录与统计

（4） 终端安全管理系统策略巡查。每周 1 次对各个终端安全管理系统的策略设置进行巡查，并和备份的终端安全管理系统策略进行比对，查看终端安全管理系统策略是否被异常修改。

（5） 终端安全管理系统策略备份。每月 1 次对各个终端安全管理系统策略进行备份。同时，在主动修改了终端安全管理系统策略的情况下，要及时备份终端安全管理系统策略。

（6） 终端安全管理系统数据备份。每周 1 次对各个终端安全管理系统的日志和数据库进行备份。

（7） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（8） 终端安全管理系统密码保护。每年 1 次对访问终端安全管理系统的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特

殊字符，并且密码不能循环使用。各个终端安全管理系统密码要求不使用同一个密码。（可根据秘密的相应程度作对应调整）。

（9） 终端安全管理系统资产管理。对终端安全管理系统进行资产标示与分类管理，定期对终端安全管理系统进行除尘处理。

（10）终端安全管理系统规范操作。按操作规程实现终端安全管理系统的启动/停止、加电/断电等操作。

（11）终端安全管理系统信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（12）终端安全管理系统安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

3.2.9 运维审计系统

（1） 运维审计系统工作状况巡视。每天 1 次对所有运维审计系统的运行状况进行查看并将巡视结果记录到运维审计系统运行日志当中。

（2） 运维审计系统日志审查。每天 1 次在对运维审计系统工作状况巡查的同时，对各个运维审计系统进行日志审查，并记录是否有异常事件发生。如果有异常事件-发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 运维审计系统策略巡查。每周 1 次对各个运维审计系统的策略设置进行巡查，并和备份的运维审计系统策略进行比对，查看运维审计系统策略是否被异常修改。

（4） 运维审计系统策略备份。每月 1 次对各个运维审计系统策略进行备份。同时，在主动修改了运维审计系统策略的情况下，要及时备份运维审计系统策略。

（5） 运维审计系统数据备份。每周 1 次对各个运维审计系统的日志和数据库进行备份。

（6） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（7） 运维审计系统密码保护。每年 1 次对访问运维审计系统的密码进行修改，密码要求长度为 8 位以上，需要带字母、数字和特殊字符，并且密码不能循环使用。各个运维审计系统密码要求不使用同一个密码。（可根据秘密的相应程度作对应调整）。

（8） 运维审计系统资产管理。对运维审计系统进行资产标示与分类管理，定期对运维审计系统进行除尘处理。

（9） 运维审计系统规范操作。按操作规程实现运维审计系统的启动/停止、加电/断电等操作。

（10）运维审计系统信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（11）运维审计系统安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

3.2.10 数据库审计系统

（1） 数据库审计系统工作状况巡视。每天 1 次对所有数据库审计系统的运行状况进行查看并将巡视结果记录到数据库审计系统运行日志当中。

（2） 数据库审计系统日志审查。每天 1 次在对数据库审计系统工作状况巡查的同时，对各个数据库审计系统进行日志审查，并记录是否有异常事件发生。如果有异常事件发生，则需要具体分析异常事件发生的原因并进行记录。

（3） 数据库审计系统策略巡查。每周 1 次对各个数据库审计系统的策略设置进行巡查，并和备份的数据库审计系统策略进行比对，查看运维审计系统策略是否被异常修改。

（4） 数据库审计系统数据备份。每周 1 次对各个运维审计系统的日志和数据库进行备份。

（5） 故障处理。在每日巡检和监控中，发现的问题需及时处理，并将处理过程和结果进行保存，由专人归入安全知识库。

（6） 数据库审计系统资产管理。对数据库审计系统进行资产标示与分类管理，定期对运维审计系统进行除尘处理。

（7） 数据库审计系统规范操作。按操作规程实现数据库审计系统的启动/停止、加电/断电等操作。

（8） 数据库审计系统信息分析。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

（9） 数据库审计系统安全管理，定期进行漏洞扫描，补丁升级，特征库升级等。

四．重大安全保障服务需求

安全保障提供的服务包括配合重大时期安全保障和安全监控。

4.1 重大时期安全保障

在国家法定节假日和特殊时期等重大时期，信息安全事件的发生几率都会大为增加。为确保本院在重大时期时信息系统能够正常运行，需要在原有信息安全防护体系的基础上，通过调整安全防护措施，进一步加强本院重大时期的信息安全保障工作，全力提升本院信息系统整体安全保障水平。

4.2 安全监控

安全监控是对本院主链路设备进行连通性检查，并记录全部防火墙端口流量和收集相关设备日志，同时对防火墙端口流量和收集相关设备日志，并提供预警、故障处理、策略核对、设备升级等服务。

五．安全检查服务需求

主要是对信息系统开展安全自查工作以及协助本院完成国家信息化主管部门或上级领导部门对本院信息系统的安全检查工作。安全检查主要内容包括涉密计算机检查、服务器安全检查、非涉密计算机安全检查等。

5.1 安全防护设备检查

对本院安全设备进行检查，主要是对防火墙、入侵检测系统、防毒墙、安全审计系统、漏洞扫描系统等安全防护设备进行检查。

5.2 政务外网安全检查

对本院政务外网服务器进行检查查操作系统有无多余的或过期的账户、管理员账户与弱口令、补丁安装、组策略、共享资源、本地服务以及系统进程等，检查病毒及恶意代码防护措施、应用服务、安全防护以及安全加固措施。

5.3 内网计算机安全检查

对本院内网计算机进行检查，主要检查病毒及恶意代码防护措施、桌面安全管理软件、计算机名与人员信息。

六．安全制度维护服务需求

信息系统的安全不但取决于信息系统采用的安全技术和安全设备，更重要的是对信息系统、信息系统采用的安全措施和应用系统的运行进行管理。根据信息安全建设目标、安全策略制定系统的安全管理制度是达到管理目的的保证。安全管理制度的内容应该全面覆盖安全工作涉及的方方面面，同时还应提出确保安全管理制度起到真正的规范和约束作用的方法。通过对所制定的各项制度的执行情况进行质量考核和对有关人员的工作进行评比，以便促进制度的更好落实，确保高质量地完成各项安全管理任务。

根据本院对信息安全的需求，参照国际、国内有关信息安全方面标准，制订出本院专网系统信息安全管理有关规定和管理工作规范，使本院专网系统信息安全工作有章可循，信息安全管理工作有法可依。

根据国家有关法规和标准的规定，结合北京市高级人民法院专网系统信息安全策略以及相关技术方案，参照本院专网系统信息安全实施规划，分阶段起草和颁布以下本院专网系统信息安全法规制度。对于涉密信息和信息系统有关制度的制定应该要求本院保密部门参加制定和检查工作。

6.1 制度修订

为确保本院安全管理制度起到真正的规范和约束作用， 确保安全制度符合信息安全现状，保证安全管理制度的有效性与适用性，需要对安全管理制度进行修改、完善与补充。

制度修订工作需要每年将对信息安全需求进行收集，并结合信息安全现状进行分析，在有制度不符合信息安全现状或需求时，向本院行管部门领导提出合理建议，并对安全管理制度进行修订。

6.2 制度审核

为确保本院信息系统的整体安全，本院信息化主管部门将安排信息安全服务团队与其一起完成对本院的其他制度进行安全审核。

制度审核是对本院信息系统中实体管理安全、软件管理安全、人员管理安全及维修管理安全等相关制度进行信息安全方面的审核分析，发现制度存在的安全问题或安全隐患，向本院相关部门领导提出合理的建议，确保本院信息系统符合信息安全相关要求。

七．安全应急响应服务需求

应急响应服务主要包括安全应急预案编写与修订工作、安全应急演练工作、信息安全应急响应工作等服务内容。

7.1 信息安全应急预案编写与修订

对涉及本院安全系统的编写应急预案，给出安全整改合理化建议，保证本院信息系统所有子系统应急演练符合相关的标准和规定，满足对系统的安全防护需求。

7.2 信息安全应急演练

按照安全应急预案进行安全应急响应演练服务，对本院安全事件进行安全响应和应急响应，在最短时间内解决安全问题，包括应急响应、处理、恢复服务和入侵调查分析等。

7.3 信息安全应急响应服务

根据本院信息系统总体需求，本院信息系统需要采用驻守服务、远程支持、现场支持等方式，保证在病毒爆发、非法网络入侵、网络故障等重大事件发生时，

能够及时进行处理。针对本院信息系统的实际情况，安全应急响应服务应分为三个等级进行管理，各等级的具体服务内容请参见下表：

表 1 安全应急服务内容表

服务等级	服务内容	适用对象
一级	基本的反应策略与流程； 5×8 小时事件响应、处理及恢复服务； 电话、传真、email 技术支持； 48 小时内现场技术支持； 事故处理报告。	日常运营期间，不影响用户业务的普通安全事件处理。
二级	完整的反应策略与流程； 7×24 小时事件响应、处理及恢复服务； 电话、传真、email 技术支持； 24 小时内现场技术支持； 事故处理报告。	节假日期间，较为严重的安全事件。
三级	完整的反应策略与流程； 7×24 小时事件响应、应急响应、处理及恢复服务； 电话、传真、email 技术支持； 通过最快的交通工具到现场技术支持； 安全专家现场守候服务； 事故处理报告；	重大事件、节日期间，用户业务重要性、时效性很强，发生严重影响用户业务开展、需要立即解决的网络突发事故。

	安全突发事故反应预演； 两周内跟踪服务。	

八．安全培训服务需求

8.1 培训目的

为提高北京市平谷区人民法院信息化管理人员的能力和水平，整体提高信息安全防护意识与技术手段，促进信息化建设健康发展，必须加快对高素质的信息安全管理和技术人才的培养，在做好信息系统安全运维工作的同时，更需要有计划、有组织的对现有信息化管理人员进行信息安全培训。根据文件要求，我公司将针对全市法院安全运维管理、安全信息技术等工作制订业务培训计划，制作培训教程。

8.2 培训内容

为保障安全培训工作顺利开展，我公司计划充分利用北京本院信息系统资源开展系统安全培训工作，如通过视频会议、培训会议、远程指导等方式向相关技术人员做统一安全培训等。

同时，可根据本院信息化管理部门的要求，编写本院信息安全运维工作中使用的技术白皮书。

我公司至少提供一次信息安全意识教育培训，具体的培训计划将与本院信息办公室领导沟通协商后确定。

九．安全保密要求

本院属于国家机要单位，要求为法院服务的工作人员（包括安装工程师、驻地工程师以及销售人员，后文通称“法院服务人员”）必须严格遵守法院的相关信息保密规定。

（1）法院服务人员未经批准，严禁查看、下载、复制法院局域网网络信息内容。

（2）法院服务人员未经批准，严禁查看、下载、复制法院办公用电脑的信息内容。

（3）法院服务人员未经允许严禁拍摄法院内部工作人员、庭审现场、文件、办

公环境、机房及设备等各种视频或照片（公司产品照片除外）。严禁将任何视频或照片发布到微信、微博、邮件、论坛等网络媒体上。

（4）因工作需要配发的法院门禁卡、工作服等只限法院服务人员使用，严禁外借他人。如有遗失，应第一时间向法院管理人员汇报，降低损失和不良影响。

（5）法院服务人员不得将与工作无关的人员带入法院工作区内。