合同编号：_____

# 北京市国防动员办公室
# 首都信息发展股份有限公司
# 业务合同

**项目名称：** 人防信息系统运维类项目软件运维服务项目（2026年度人防工程信息管理平台运维租赁服务项目）

**甲　　方：** 北京市国防动员办公室

**乙　　方：** 首都信息发展股份有限公司

**签订地点：** 北　京

**甲方：北京市国防动员办公室**

**乙方：首都信息发展股份有限公司**

鉴于:

甲乙双方本着互惠互利、共同发展的原则，依照《中华人民共和国民法典》的规定，经友好协商，就乙方向甲方提供人防信息系统运维类项目软件运维服务项目服务相关事宜达成如下合作条款。

下列文件是构成本合同不可分割的部分:

a. 招标文件及针对其颁发的补遗和修改文件;
b. 投标文件;
c. 合同附件。

## 第一条 技术服务内容

详见附件: “人防信息系统运维类项目软件运维服务项目”采购技术需求。

## 第二条 双方责任

（一）甲乙双方中的任何一方均不得向第三方转让其依据本合同所应当承担的义务。

（二）甲乙双方应共同确保本合同项目工作的顺利进行。

（三）乙方应在平台出现技术问题的 0.5 小时内予以响应，进行技术支持、提供初步解决方案；并应当在收到甲方通知后 8 小时内进行修复，情况紧急的，乙方应当在 3 小时内修复完成。

## 第三条 合同金额

本合同价款，乙方向甲方提供相关服务的所有费用、报酬和支出总计人民币大写：人民币壹佰叁拾肆万元整（￥1,340,000 元）。

## 第四条 付款方式

（一）本合同签订后 30 个工作日内，甲方向乙方支付人民币（大写）柒拾万元整（¥700,000 元）。付款前，乙方应向甲方交付等额的中华人民共和国法定增值税普通发票(税率 6%）。

（二）本合同约定事项履行完毕并通过验收后 30 个工作日内，甲方向乙方支付人民币（大写）陆拾肆万元整（¥640,000 元），付款前，乙方应向甲方交付等额的中华人民共和国法定增值税普通发票(税率 6%）。

## 第五条 保密条款

（一）甲乙双方均须将其由于本合同而接受或获得的所有信息视为专有信息并保守秘密（“保密信息”）。本合同所述的保密信息是指甲乙双方拥有的与本合同及其项目相关的商业信息、财务信息和技术信息等，同时还包括标有保密字样的资料和一些显而易见的应该保密的资料。保密信息归信息披露方所有，对方不得透露或未经授权使用这些保密信息。

（二）乙方从甲方处得到的所有保密信息只能用于本合同项目的业务和应用分析，以使本合同项目的业务流程重组、需求分析、项目计划、软件开发概要设计及其他有关信息更加明确。

（三）甲乙双方不得以任何方式把本合同的细节和任何信息透露给第三方或除下述人员以外的任何人：

1、与本合同项目有直接关系且必须了解有关保密信息的人员，即雇佣人员、代理商、转包商和其他供应商；

2、具有合法权利或职责的接受方的专业顾问；

3、其他可以了解保密信息的个人或团体。

（四）甲乙双方须在保密信息不再需要之后销毁保密信息，并不得为任何目的继续

使用该等保密信息

（五）本合同终止时，甲乙双方均须将载有对方保密信息的文件、资料或软件按对方的要求归还或予以销毁，并从任何记忆装置或电子媒介中删除该等保密信息。

（六）发生下列情况，甲乙双方对保密信息不负有任何义务：

1. 在无保密义务的前提下，已经由对方所拥有的；

2. 已经被公众了解或知晓的；

3. 在不违反本合同规定下，从有权提供信息的第三方合法获得的；

4. 未使用对方任何保密信息而独立开发的；

5. 根据法院命令或根据具有司法管辖权的政府或行政主管机构的要求而必须透露的；

6. 依国家有关法律、法规规定，向有关中介机构、国家政府部门及公众披露的。

## 第六条　项目档案管理

甲乙双方必须安排专人管理本合同项目的技术档案，并负责完成相关材料的积累、登记、立卷、整理和存档工作。

## 第七条　项目验收

（一）甲方按照本合同第一条内容对项目进行验收。

（二）如本合同项目档案资料不完整，甲方将不予验收，乙方应按甲方的要求在指定期限内改正，并重新提交甲方验收，直至通过。

## 第八条　知识产权

（一）甲方拥有因实施本合同而获得的所有权利。

（二）未经对方同意，甲乙双方中任何一方不得使用、复制对方的商标、企业名称、

标识、商业信息、技术及其他享有知识产权的产品和资料等。

（三）在本合同履行过程中，若需使用乙方拥有知识产权的软件产品，乙方同意授予甲方在本合同项目范围内永久的、免费的、不可撤销的使用许可。因履行本合同而对乙方软件产品进行的任何修改、优化、适配或新增功能，其产生的知识产权及其他权利均归甲方所有。

## 第九条　合同终止

发生下列情形，本合同立即终止，引发合同终止的一方须承担因此而给对方造成损失的赔偿责任。

（一）甲乙双方中的任何一方违反本合同的有关规定，且在另一方以书面形式告知违约事实三十（30）日后仍未采取改正措施；

（二）甲乙双方中的任何一方丧失从事本合同业务的资格；

（三）甲乙双方中的任何一方的营业执照被吊销或注销；

（四）甲乙双方中的任何一方进入、或被其他第三方申请进入破产或清算程序；

（五）甲乙双方在签署本合同时所考虑及依据的经济、法律及政策规范的基础发生了未能预见的根本性变化，并导致本合同无法继续执行。

## 第十条　违约责任

（一）本合同生效后，各方均应全面履行本合同约定的义务。任何一方不履行或不完全履行本合同约定义务的，应当承担相应的违约责任，并赔偿由此给守约方造成的损失。因不可抗力或情势变更造成的不能履行除外。

（二）乙方未达到本合同第二条第三款之规定的，每逾期 1 小时，乙方应向甲方支付总合同金额 0.1 %的违约金，若同一事件导致的延误超过超出 2 日的，或在单个季度内累计发生 3 次 以上（含 3 次）此类延误，则视为乙方根本违约，甲方有权单方解除合同。乙方应向甲方退还剩余服务期款项。合同的解除并不因此免除乙方支付违约金及其他有关责任。

（三）未经甲方准许，乙方不得将从甲方处了解的有关情况或将甲方向乙方提供的材料以及本项目方案泄露给第三方，否则应承担由此给甲方造成的全部损失。

（四）甲方擅自变更或解除本合同，乙方不退还甲方已支付的费用；乙方擅自变更或解除本合同，应退还已收取的费用。

（五）任意一方更换联系人或联系方式的，应提前 1 日告知对方，否则因此造成的工作延误或其他损失由过失方承担全部责任。

## 第十一条　争议解决和法律适用

（一）甲乙双方应以友好协商方式解决本合同履行过程中产生的争议，经协商无法解决争议时，甲乙双方均可向甲方住所地人民法院提起诉讼。

（二）本合同适用中华人民共和国法律。

## 第十二条　其他条款

（一）本合同附件为本合同不可分割的组成部分，具有同等法律效力。本合同附件包括：

附件：“人防信息系统运维类项目软件运维服务项目”采购技术需求。

（二）本合同未尽事宜将由甲乙双方另行商定。本合同的任何补充和修改仅能以双方签字盖章的书面文件进行。

（三）本合同自签订之日起生效，有效期为一年，自双方签字并盖章之日起生效。

（四）本合同中任何被视作无效或不可执行的部分，将不会影响本合同其他条款或部分的有效性与可执行性。

（五）本合同一式肆份，双方各执两份，具有同等法律效力。

甲方：北京市国防动员办公室

地址：北京市西城区槐柏树街北里 8 号

邮编：100053

电话：

（盖章）

法定代表人(或授权代表人)签字：

日期：2026 年 7 月 6 日

乙方：首都信息发展股份有限公司

地址：北京市东城区隆福寺街 95 号隆福大厦 5 层

邮编：100010

电话：010-88511155

（盖章）

法定代表人(或授权代表)签字：

日期：2026 年 7 月 6 日

**附件：“人防信息系统运维类项目软件运维服务项目”采购技术需求**

**项目目标：**为保障人防工程信息管理平台安全、稳定、高效运行，支撑市、区两级国动部门工程建设审批、质量监督、执法监察、日常使用管理等核心业务有序开展。本次运维服务涵盖数据运行维护、应用软件及其运行软环境运行维护两大核心任务，确保平台数据准确合规、系统持续可用、运行安全稳定、功能适配业务需求。

**（一）数据运行维护**

**1. 常规运维**

数据监控：监控数据管道、接口、数据库的运行状态与性能指标。如数据传输异常则触发短信提醒，运维人员及时跟进。

预防性检查：配合完成平台等保测评、等保备案相关工作；修订完善平台数据运维规范及方案；配合开展平台安全监测相关工作。构建并固化数据清洗规则库，按周期执行，跨表、跨系统比对关键字段，提前发现并修正，确保一致性、合规性及安全性。

常规检查：定期开展平台数据质量抽检，保障数据完整性、准确性、一致性。建立数据质量核查清单，按比例对关键业务表进行数据准确性、完整性、及时性抽检。

**2. 响应支持**

数据问题处理：开展平台数据质量评估、数据统计核查、数据质量常态化监控；执行数据备份及恢复操作，保障数据安全可追溯。对数据错误与质量问题进行处置和评估，确保数据的完整性和准确性。

服务请求处理：及时响应业务处室提出的各类数据相关需求，高效完成需求对接、处理与反馈。响应并处理业务部门提交的数据服务请求（工单），包括：临时数据统计与提取、加工、数据一致性核查、数据质量争议确认、数据回退等。制定和执行数据备份策略（如全量、增量备份），定期进行恢复性演练，确保在数据丢失或损坏时可快速

恢复。

应急响应要求：建立数据类突发问题应急处置机制，快速处理数据异常、丢失、错误等问题。制定与维护数据安全专项应急预案，响应业务处室提出的数据恢复与应急服务需求，并及时处置和恢复由数据错误、丢失或异常引发的线上故障。

**3. 优化改善**

诊断分析：定期开展平台系统自检，排查数据及系统运行潜在风险与问题。

问题解决：依据自检结果，定位并解决数据异常、系统报错等问题。

系统改进：基于自检结果与业务实际需求，对平台数据管理、数据流转环节进行优化改进。优化数据常规运维和响应支持工作流程，提出优化方案并实施改进。

4. 评估分析

数据修改影响评估：开展数据修改影响评估并形成规范工单；评估应用软件变更、中间件变更对平台数据的影响，规避数据风险。对客户提出的数据操作请求，在操作前评估其对数据一致性及下游应用的潜在影响，确保变更安全、可追溯。

数据分析与汇总：开展业务数据分析，按月完成运维工作汇总，形成月度工作成果。

应用软件变更对数据影响的评估：对应用软件变更开展评估，分析其对数据逻辑与结构的潜在影响，预防变更导致的数据一致性与完整性问题。

**（二）应用软件及其运行软环境的运行维护**

**1. 常规运维**

事件与请求管理：对项目运维管理周报的撰写与校核，分析维护事件、识别系统风险与问题，并统一受理、判断和分配各项服务请求。

应用系统运行的监控指标体系设计：持续梳理和定义关键监控点，制定覆盖性能、可用性及业务流程的量化指标，并建立动态更新机制，以支撑常态化监控与主动预警。

应用系统运行监控：对平台各应用系统开展监控点巡检，及时处置巡检发现的异常情况，保障系统稳定运行。

客户回访：面向全市 16+1 区开展用户调研，收集系统使用问题与优化建议；定期开展用户满意度调查，持续提升服务质量。

培训及问题分析：提供日常培训、咨询解答、新增功能培训等。为平台经办人提供使用咨询解答，分析问题成因，形成标准化处置指引。

**2. 响应支持**

服务受理：受理经办人提出的系统使用、功能操作等问题，建立台账闭环处理。

非故障请求处理：为用户提供系统操作、功能使用等常态化技术支持。处理由业务需求或用户操作引发的各类服务请求，包括用户账号的新建与配置、访问权限的分配与调整，以及并处理因操作不当或流程误解所产生的系统使用性问题。

故障诊断及处理：负责平台数据库、报表工具、中间件、操作系统的日常维护；快速诊断系统故障，完成问题处置与修复。数据库维护、报表工具维护、中间件维护、操作系统维护等运维服务。问题排查、定位、诊断、分析、处置、检测、跟踪、复盘。

新用户和新功能上线：完成新用户开通，新功能上线部署，配套开展用户操作培训。

应急响应：提供应急保障值守服务；组织应急演练，及时处置系统安全隐患。编制项目应急预案，配合安全监测、配合等保测评及等保备案等工作。在重要节日、重大活动前提供全面的安全排查服务，在保障期间提供 7*24 小时值守服务，安全排查主要是依据安全服务商安全通报，关注安全资讯，及时关注本项目各系统技术平台组件安全漏洞情况，事先排查安全风险。在重保期间安排值守人员，提供 7*24 小时人员监控，并根据应急预案事前开展演练，确保紧急事件得到较好的处置。

**3. 优化改善**

功能性改进：根据业务变化，调整系统功能，适配实际业务需求。

性能优化改进：针对系统响应慢、卡顿等问题，开展性能优化提升工作。响应业务优化需求，实施功能增强、效能提升与瓶颈治理、接口兼容性与标准化整改。

适应性改进：根据要求调整系统对接方式，保障平台与外部系统、政务网络兼容适配。业务连续性及适配性保障，主动响应业务部门因政策、流程或模式变革提出的系统变更需求。跨系统生态协同与联调共治：积极介入因第三方系统升级、标准变更或新系统引入所引发的链式改造。主导制定跨系统协同技术方案

预防性改进：开展系统安全漏洞加固；针对中间件、数据库开展性能与安全优化改进。依据应用系统开展渗透测试、漏洞扫描与风险评估的报告结果，对发现的安全威胁实行分级分类处置。对于服务器漏洞扫描，深入分析扫描结果，完成对系统漏洞的精准识别、风险定级与影响范围评估，彻底清零重大安全隐患。

**其他要求**

人员团队要求：供应商必须成立专门的运维服务团队，运维团队应包含驻场人员和二线技术人员。团队人员熟悉政务信息化运维和开发流程，技术开发人员拥有 3 年以上系统开发经验，运维人员拥有 2 年以上信息化运维经验。

驻场服务：派驻不少于 2 名人员驻场，驻场服务要求每周 5*8 小时现场服务，建立 24 小时服务热线，保证全体用户电话咨询和问题反馈能够第一时间得到响应。驻场服务内容包括：主要是派驻运维人员现场解答系统使用咨询、处置系统问题、辅助业务办理、文件递送等。

培训服务：根据市国动办要求进行相关的系统使用和管理培训工作，在培训会议前，提供培训材料、培训课件等辅助培训资料等，配备专门的培训讲师，开展使用培训工作，帮助使用人员能够全面理解各业务系统的作用和使用方式，同时针对系统使用过程中常

见问题进行有针对性的详细讲解，在培训过程中，将系统使用中遇到的问题全部解决，提供培训方案需有针对性和切实可行性。

信息化业务辅助服务：配合参加信息化相关会议，落实政策要求并编制实施方案；按期完成运维周报、系统应用月报等报告编制。

保密管理：所有运维人员须签订保密承诺书，严格遵守数据安全与保密规定，不得擅自修改、泄露、传播采购人业务数据及内部信息。

服务考核标准：项目团队应全面落实办件数据汇聚工作，确保数据完整率、准确率、及时率达标。若因平台技术问题引发数据报送失误，导致北京市国防动员办公室在季度考核中扣分的，每出现一次，按当期运维服务费总额的0.5%予以扣除。

运维服务标准参见下表：

| 序号 | 服务内容 | 服务标准 |
| --- | --- | --- |
| 1 | 服务配置完成率 | 100% |
| 2 | 日常巡检次数 | 2 |
| 3 | 系统故障率 | 1% |
| 4 | 故障响应率 | 100% |
| 5 | 故障排除率 | 100% |
| 6 | 重大节假日7*24小时值守率 | 100% |
| 7 | 日常5*8小时值守率 | 100% |
| 8 | 系统正常运行率 | 99% |
| 9 | 数据同步准确率 | 90% |
| 10 | 使用人员满意度 | 95% |

附件

# 网络安全责任书
# （2026年度人防工程信息管理平台运维租赁服务项目）

甲方（委托方）：北京市国防动员办公室

统一社会信用代码：11110000000021565F

乙方（受托方）：首都信息发展股份有限公司

统一社会信用代码：911100006336972074

为明确甲乙双方的网络安全责任，根据《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》及相关法律法规的规定，特签订本责任书，甲乙双方共同遵守。

1.甲方委托乙方进行2026年度人防工程信息管理平台运维租赁服务项目的运行维护工作，乙方必须严格遵守网络安全、数据安全法律法规和甲方的网络安全、数据安全各项管理规定。

2.乙方应建立和健全网络安全管理制度，加强网络安全管理，加强运维人员的管理，落实各项安全保护技术措施，确保本系统安全稳定运行，不发生数据泄露问题。

3.乙方应设立网络安全运维人员，明确安全工作职责，并定期组织安全检查，及时解决网络安全问题。

4.甲方人员安排本单位人员负责操作系统、数据库、机房等核心管理权限。

5.重大活动时期，乙方应落实应急值守制度，运维人员要保

持24小时通信畅通，做好设备硬件、网络环境、应用系统的实时安全监测工作，随时准备应对各种突发事件。并接受甲方的监督检查。

6.乙方应协助甲方编制应急演练方案，开展本系统网络安全应急演练，根据演练情况修订网络应急预案。

7.乙方应协助甲方完成本系统等级保护测评、数据安全风险评估，商用密码应用安全性评估和安全漏洞整改等工作。

8.乙方应协助甲方完成市委网信办、市公安局、市政务服务和数据管理局网络安全检查的迎检自查工作，消除安全隐患。

9.乙方更换运维服务人员时，必须征得甲方的同意，否则不得更换运维服务人员。

10.乙方运维服务人员须经甲方同意，并且在操作前将具体处理流程完整告知甲方，经甲方确认同意后方可执行。数据库的运行维护工作必须在甲方人员陪同下开展。

11.乙方运维人员必须在甲方指定的场所实施运维工作。

12.甲方要按照“最小授权原则”，合理分配运维服务人员操作权限，减小运维服务人员误操作或滥用权限导致发生网络安全事件。严禁乙方运维服务人员拥有管理权限。

13.本系统使用的软硬件产品和服务，乙方要协助甲方及时掌握其相关安全预警信息，对软硬件产品和服务的风险漏洞，应在厂商和安全机构修复方案公开发布后立即配合甲方开展安全整改工作。

14.本系统所使用的软件产品，乙方要协助甲方判定软件的授权、维保期限，禁止使用超过授权使用期限或维保期限的软件。

15.乙方应协助甲方完成本系统的资产登记管理和供应链产品清单的更新工作。

16.本系统使用的软件产品，乙方进行安装、升级维护时，要从安全可控的渠道获取软件安装包、升级包、补丁包，并开展相应的可用性、安全性及完整性检测分析，确保符合要求后进行软件安装、更新升级，并同步更新相关配置，确保本系统稳定运行。

17.本系统所使用的软硬件产品，乙方应协助甲方与相关厂商、供应商、集成商沟通协调，共同开展软硬件产品运维。

18.运维服务合同到期后，乙方要按照上交文档、资料和设备，运维工作相关的电子数据，不得留存。运维服务合同到期，按照合同约定，自动顺延的运维项目，乙方按照甲方要求留存相应资料。

19.重保期间、重大演习演练期间，暂停信息系统的升级、调试、变更和安全性测试等工作。

20.严禁乙方擅自删除、修改系统中涉及安全的重要设置，严禁未经授权开展安全漏洞的测试与验证工作，测试验证完成后应及时清理恶意文件或测试账号，对无法清理或删除的应及时与甲方沟通，配合厂商、供应商、集成商开展隐患清理与安全整改。

21.乙方应建立完整的系统运行维护档案。

22.乙方严禁将本系统的相关数据向未经授权的第三方透露。

23.对于违反本责任书约定、网络安全保护管理法规及有关规定的行为，甲方有权向乙方追责。造成重大网络安全事故和泄密事件的，将依法追究相关责任人的责任，构成犯罪的，由司法

机关追究刑事责任。

24.本责任书自加盖公章或合同专用章之日起生效，有效期与合同的服务期限保持一致。责任书一式肆份，甲方持贰份，乙方持贰份，具有同等法律效力。

甲方（盖章）：

乙方（盖章）：