合同编号：BJSGS2503640CGN00

合同编号：

# 北京市药品监督管理局
# 信息化系统运行维护—安全和基础运维服务—
# 政务云安全运维合同书

2025 年 4 月

合同编号：BJSGS2503640CGN00

甲方：北京市药品监督管理局

通讯地址：通州区留庄路 6 号院 2 号楼

邮政编码：101117

乙方：中国电信股份有限公司北京分公司

通讯地址：北京市东城区朝阳门北大街 21 号

邮政编码：100010

北京市药品监督管理局（以下简称“甲方”）和中国电信股份有限公司北京分公司（以下简称“乙方”），按照《中华人民共和国政府采购法》和《中华人民共和国民法典》等有关规定，根据 北京汇诚金桥国际招标咨询有限公司 组织 公开招标 的结果，就甲方委托乙方实施 信息化系统运行维护—安全和基础运维服务—政务云安全运维 （以下也称为“该项目”）建设的有关事宜，本着平等互利的原则，经友好协商，签订本合同，以资共同信守。

合同组成：

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。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. 投标文件(投标时已提供)

d. 招标文件(含招标文件补充通知)

e. 中标人的投标文件及有关澄清资料

第一条　项目概况

1、项目名称：信息化系统运行维护—安全和基础运维服务—政务云安全运维。

2、合同总额（含税）：乙方服务期限内的合同总金额为人民币大写：叁佰玖拾伍万陆仟壹佰叁拾壹圆陆角肆分整小写：￥3956131.64元。

3、项目服务地点及内容：

1）服务地点：北京市药品监督管理局

2）服务内容和目标：保障业务系统的稳定运行，以风险管理为导向强化采购人信息安全保障体系，健全各项安全保护措施，提升采购人网络信息安全防护水平。根据国家相关政策规范、标准指南等文件，为药监局政务云上业务系统建立和完善信息安全保障体系，按照北京市药品监督管理局的要求，提供基础支撑服务、安全服务、密码服务及灾备服务工作。具体服务内容包括：基础软件租用、主机杀毒服务、主机防护服务、主机安全服务、主机漏洞扫描、数据库审计服务、WAF 防护、日志收集与分析服务、渗透测试、网页防篡改、云端 APT 防护、本地数据备份服务、应急预案、应急响应、应急演练、安全通告、管理制度修订、安全巡检、强身份认证服务、签名验签服务、时间戳服务、加解密服务、SSL 安全服务（国密）、远程运维接入服务（国密）、数据库透明加密服务、应用数据库加密授权-数据库透明加密代理、应用数据库加密授权-数据库透明加密 SDK、全球服务器 OV 通配符证书、设备证书、国密浏览器、日志审计服务、灾备服务等服务。以此增强系统安全防护能力、隐患检测能力、应急响应能力和系统恢复能力，保障 2025 年药监局政务云上业务系统稳定安全运行。

**第二条　项目期限**

自合同生效且乙方提供有效服务之日起12个月。

**第三条　项目实施具体内容**

项目实施具体服务内容详见附件《北京市药品监督管理局政务云安全运维方案》。

**第四条　双方责任**

1、甲方应积极配合乙方的工作，按需提供相关的技术资料、数据和信息等，并保证所提供资料的完整性、准确性和合法性。

2、甲方应明确其具体安全需求，双方以通过甲方确认的《北京市药品监督管理局政务云安全运维方案》作为工作依据；如甲方需求发生重大变化，应书面通知乙方，由此增加乙方投入的，甲方应向乙方支付所增加的费用。

3、甲方应按照合同约定及时向乙方支付合同款项。

4、甲方应及时对乙方提供的各项服务工作进行确认。

5、乙方应指派专人与甲方就安全服务的相关事项进行沟通、协调与确认。

6、乙方在安全服务中，若涉及对甲方网络或系统进行调整的，应通知甲方作好相

应的系统数据备份等准备工作，并明示具体的操作方法、采用的操作工具、操作步骤、参与的人员以及可能出现的风险，经甲方签字确认后再开展工作。

7、因乙方原因导致甲方信息系统破坏、数据丢失的，乙方应及时采取措施协助甲方进行系统和数据的恢复，并就甲方的损失承担赔偿责任。

8、乙方保证其提供的货物、设施设备及服务（包括其中所含的软硬件）没有任何病毒、后门程序、恶意代码等安全隐患（包括但不限于：恶意收集数据、恶意查删正常信息等属于本合同未列明的功能），不存在任何质量瑕疵和权利瑕疵。

9、乙方就本次采购所提交投标文件中承诺服务标准/内容高于/多于本合同的，以乙方承诺服务标准/内容为准。

**第五条　合同款的支付与结算**

1、合同总金额（含税）为人民币大写：叁佰玖拾伍万陆仟壹佰叁拾壹圆陆角肆分整，小写：￥3956131.64元。

2、支付方式双方约定。

自本合同签订生效之日起，且财政资金批复到位后，30天内，甲方支付乙方本合同80%的服务费款项，本合同到期前3个月内扣除违约金（如有）、赔偿金（如有）后支付剩余20%款项。乙方应于甲方支付相应费用前，先行向甲方出具符合甲方要求的等额增值税发票。否则，甲方有权拒绝付款，且不因此承担违约责任。

3、履约保证金支付：合同签订后，乙方按照合同总额10%的比例向甲方支付履约保证金人民币【395613.164】元（大写：叁拾玖万伍仟陆佰壹拾叁元壹角陆分肆厘）。待项目结束并验收合格后，甲方无息退还履约保证金。

4、乙方账户信息如下：

公司名称：中国电信股份有限公司北京分公司

纳税人识别号：91110101681953105M

开户银行：工行阜外大街支行

账号：0200049219022523842

联系人：张彦博

联系电话：13370163173

**第六条　项目验收**

1、项目验收按照国家相关标准执行。

2、在运维工作结束后，乙方需向甲方提交工作总结等有关验收材料。乙方提交验收材料后，甲方应在15个工作日内依据采购文件、乙方的中标文件及相关服务标准等组织验收，验收完毕后出具书面验收报告。

3、乙方应对提交的验收材料作出全面检查和整理，并列出清单，作为甲方验收和使用的技术条件依据，清单应随提交的验收材料交给甲方。

**第七条　技术支持与售后服务**

1、乙方在服务期内，提供全天候7*24小时热线电话技术支持服务解答甲方在服务过程中的技术问题。同时，乙方将在本合同项目实施过程中，根据甲方业务系统连续运行较高等特点，来制定应急响应流程方案，根据不同的事件故障类型予以响应，对发生的问题1小时内响应，2小时内到达现场，尽快予以解决。

2、乙方将成立专门技术队伍，保证本项目拥有一支稳定的服务保障队伍，遇到突发情况时能够及时解决问题。项目经理及团队成员有明确分工和侧重点，确保服务人员均掌握一般的安全服务方法并能解决普遍性安全问题。

**第八条　违约及争议**

1、如因乙方原因未按合同规定的时间提供服务，则每逾期一日，乙方应按合同总额的0.5%计算，向甲方支付逾期履行违约金，但违约金累计总额不超过合同总额的10%。

2、乙方提供服务不符合本合同约定的，应按合同总额的5%向甲方支付违约金，造成甲方损失的，应予赔偿。

3、除本合同另有约定外，当发生以下情形之一时，甲方有权解除合同并有权要求乙方支付合同总价款5%的违约金；违约金不足以弥补甲方全部损失的，乙方应当予以补足：

（1）乙方或其工作人员违反本合同约定的保密义务；

（2）乙方提交的服务内容侵犯（或可能侵犯）其他任何第三方知识产权或其他合法权益；

（3）乙方部分转让或全部转让其应履行的合同义务；

（4）乙方所提供服务存在严重瑕疵或重大缺陷；

（5）乙方资质、提供服务人员等情况的真实性存在重大瑕疵或相应的资质失效；

（6）给甲方既有硬件、软件或其他财产、人身重大损害（包括损失额超过拾万元

整或造成重大负面影响的）；

（7）乙方严重违反本合同规定的条款并在甲方给予书面通知后7个工作日内仍未采取合理有效且被甲方书面认可的补救措施。

4、如发生违约事件，守约方以书面方式通知违约方，内容包括违约事件、违约金、支付时间和方式等；违约方在收到上述通知后，应于3天内答复守约方，并支付违约金。如双方不能就此达成一致意见，将按照本合同所规定的争议解决条款解决双方的纠纷。

5、本合同所约定的甲方损失包括但不限于甲方经济利益的减损、甲方为证实乙方违约行为所支付的调查取证、公证费用、甲方为寻求救济所支付的诉讼费、保全费、律师代理费、咨询费、公证费、鉴定费和法院执行费用、调查取证费、差旅费等全部损失及费用。

**第九条　保密义务**

1、任何一方对本合同条款的书面资料，以及对方提供的技术资料和数据负有保密责任，不得以任何形式、任何理由透露给第三方。

2、在合同执行期间及之后的任何时间内，一方对在履行合同过程中获知的对方商业秘密、技术秘密等信息必须严格予以保密。非经授权或履行法定义务之必要，任何一方不得向第三方披露对方的上述信息。

3、乙方向甲方提供保密承诺书，保密承诺书以附件形式体现。

4、本条款不因合同的不生效、无效或者部分无效、终止或者部分终止而失去对双方的约束力。

**第十条　诉讼**

若甲乙双方在合同执行的过程中发生争议，经双方友好协商无法达成一致，任何一方均有权向甲方所在地法院提起诉讼。

**第十一条　重大事故处理**

1、突发重大事故时，乙方发现后应第一时间通报甲方，并配合甲方查明原因；

2、因乙方非人为因素导致发生重大事故，未及时通报及响应，造成后果或影响的；乙方承担相关责任；

3、若因乙方因素，包括但不限于人为失误乃至恶意破坏行为，导致严重后果或不良影响，甲方有权无条件终止合同，并要求乙方退还尚未履行合同期限所对应的款项，同时乙方需承担违约责任，必要时甲方将依法追究其法律责任。

第十二条　廉政承诺

1、协议双方承诺共同加强廉洁自律、反对商业贿赂；

2、甲方及其工作人员不得索要礼金、有价证券和贵重物品:不得在乙方报销应由本单位或个人支付的费用；不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬；不得参加乙方安排的超标准宴请和娱乐活动；

3、乙方不得向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品；不得为其报销应由甲方单位或个人支付的费用；不得向甲方工作人员支付劳务报酬；不得安排甲方工作人员参加超标准宴请及娱乐活动。

第十三条　关于其他事宜的约定

1、乙方保证甲方在使用乙方提供的任何产品、服务时，不受第三方提出侵犯知识产权的指控。如果任何第三方提出与乙方提供的任何产品、服务有关的侵权指控，乙方须与第三方交涉并承担因此发生的一切法律责任和费用。如因此给甲方造成损失的，乙方应予全额赔偿。

2、本合同履行期间，双方如有任何修改或补充意见，应协商一致签订修改或补充协议。修改或补充协议是本合同的组成部分，签字盖章后与本合同具有同等法律效力。

3、附件作为本合同的重要组成部分，与本合同具有同等法律效力。

4、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。

5、本合同自甲乙双方法定代表人或授权代表签字并加盖公章之日起生效。

6、本合同一式 肆 份，双方各执 贰 份，均具有同等法律效力。

合同编号：BJSGS2503640CGN00

(签署页无正文)

甲方：北京市药品监督管理局

负责人或授权代表（盖章）签字：

日期：2025.4.21

乙方：中国电信股份有限公司北京分公司

法定代表人或授权代表（盖章）签字：

日期：2025.4.21

附件 1：　项目明细

| 序号 | 分项名称 | 单价（元） | 数量 | 合价（元） | 备注/说明 |
|---|---|---|---|---|---|
| 1 | 密码服务-强身份认证服务 | 25000 | 2 | 50000 | 服务期限 5 个月 |
| 2 | 密码服务-签名验证服务 | 25000 | 3 | 75000 | 服务期限 5 个月 |
| 3 | 密码服务-时间戳服务 | 25000 | 2 | 50000 | 服务期限 5 个月 |
| 4 | 密码服务-加解密服务 | 25000 | 2 | 50000 | 服务期限 5 个月 |
| 5 | 密码服务-SSL 安全服务（国密） | 25000 | 2 | 50000 | 服务期限 5 个月 |
| 6 | 密码服务-远程运维接入服务（国密） | 2500 | 5 | 12500 | 服务期限 5 个月 |
| 7 | 密码服务-数据库透明加密服务 | 40000 | 2 | 80000 | 服务期限 5 个月 |
| 8 | 密码服务-应用数据库加密授权-数据库透明加密代理 | 50000 | 1 | 50000 | 服务期限 12 个月 |
| 9 | 密码服务-应用数据库加密授权-数据库透明加密 SDK | 30000 | 1 | 30000 | 服务期限 12 个月 |
| 10 | 密码服务-全球服务器 OV 通配符证书 | 20000 | 1 | 20000 | 服务期限 12 个月 |
| 11 | 密码服务-设备证书 | 2000 | 5 | 10000 | 服务期限 12 个月 |
| 12 | 密码服务-国密浏览器 | 200 | 5 | 1000 | 服务期限 12 个月 |
| 13 | 密码服务-日志审计服务 | 10000 | 1 | 10000 | 服务期限 12 个月 |
| 14 | 基础支撑服务-商用操作系统 | 500 | 180 | 90000 | 服务期限 5 个月 |
| 15 | 基础支撑服务-商用操作系统 | 1200 | 82 | 98400 | 服务期限 12 个月 |
| 16 | 基础支撑服务-数据库服务 | 9000 | 36 | 324000 | 服务期限 5 个月 |
| 17 | 基础支撑服务-中间件 | 2316 | 34 | 78744 | 服务期限 5 个月 |
| 18 | 安全服务-主机杀毒服务 | 0.05 | 180 | 9 | 服务期限 5 个月 |
| 19 | 安全服务-主机杀毒服务 | 0.12 | 82 | 9.84 | 服务期限 12 个月 |
| 20 | 安全服务-主机防护服务 | 1000 | 180 | 180000 | 服务期限 5 个月 |
| 21 | 安全服务-主机防护服务 | 2400 | 82 | 196800 | 服务期限 12 个月 |

| | | | | | |
|---|---|---|---|---|---|
| 22 | 安全服务-主机安全加固服务 | 500 | 180 | 90000 | 服务期限 5 个月 |
| 23 | 安全服务-主机安全加固服务 | 1200 | 82 | 98400 | 服务期限 12 个月 |
| 24 | 安全服务-主机漏洞扫描 | 400 | 180 | 72000 | 服务期限 5 个月 |
| 25 | 安全服务-主机漏洞扫描 | 960 | 82 | 78720 | 服务期限 12 个月 |
| 26 | 安全服务-数据库审计服务 | 3860 | 36 | 138960 | 服务期限 5 个月 |
| 27 | 安全服务-WAF 防护 | 5000 | 12 | 60000 | 服务期限 5 个月 |
| 28 | 安全服务-日志收集与分析服务 | 390 | 180 | 70200 | 服务期限 5 个月 |
| 29 | 安全服务-日志收集与分析服务 | 936 | 82 | 76752 | 服务期限 12 个月 |
| 30 | 安全服务-渗透测试 | 3000 | 12 | 36000 | 服务期限 5 个月 |
| 31 | 安全服务-渗透测试 | 7200 | 4 | 28800 | 服务期限 12 个月 |
| 32 | 安全服务-网页防篡改服务 | 24000 | 2 | 48000 | 服务期限 5 个月 |
| 33 | 安全服务-云端 APT 防护 | 20000 | 1 | 20000 | 服务期限 5 个月 |
| 34 | 安全服务-云端 APT 防护 | 48000 | 1 | 48000 | 服务期限 12 个月 |
| 35 | 安全服务-本地数据备份服务 | 1.6 | 409648 | 655436.8 | 服务期限 5 个月 |
| 36 | 安全服务-应急预案 | 33600 | 1 | 33600 | 服务期限 12 个月 |
| 37 | 安全服务-应急响应 | 19200 | 2 | 38400 | 服务期限 12 个月 |
| 38 | 安全服务-应急演练 | 18000 | 2 | 36000 | 服务期限 12 个月 |
| 39 | 安全服务-安全通告 | 0 | 52 | 0 | 服务期限 12 个月 |
| 40 | 安全服务-管理制度修订 | 48000 | 1 | 48000 | 服务期限 12 个月 |
| 41 | 安全服务-安全巡检 | 10200 | 12 | 122400 | 服务期限 12 个月 |
| 42 | 安全服务-灾备服务 | 700000 | 1 | 700000 | 服务 1 次 |
| 总价（元） | | | | 3956131.64 元 | 无 |

合同编号：BJSGS2503640CGN00

附件 2：保密承诺书

我公司确认承担贵单位“信息化系统运行维护—安全和基础运维服务—政务云安全运维”运维工作，在为贵单位提供运维服务期间，可能会接触到敏感信息（以下统称“保密信息”）（包括但不限于工作秘密、技术秘密等），为维护贵单位合法权益，现正式提交保密承诺书，我公司承诺将按照保密承诺书有关规定严格履行保密责任。

1、“保密信息”范围：

1.1 国家秘密：根据《中华人民共和国保守国家秘密法》确定，关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知情的事项。

1.2 工作秘密：贵单位一切与工作有关的信息资料或其他性质的资料，包括但不限于：工作文件、业务工作数据、人员机构信息等。

1.3 技术秘密：指贵单位的计算机信息系统、网络架构、信息安全体系结构、软件、数据库系统及数据、文档及技术指标等。

1.4 其他保密信息：包括但不限于项目服务工作过程中获取的有关数据、流程、分析成果；贵单位的内部管理资料、其他项目的信息及资料。上述保密信息的表现形式不限，即包括书面、电子文件、图形等其他任何形式的信息。

2、我公司已知悉：

2.1“保密信息”的所有权归贵单位所有，我公司不享有“保密信息”的所有权、排他独占使用权、再许可使用权或其他权利。我公司对“保密信息”使用的方式和程度仅限于取得贵单位事先同意，并限于服务合同和承诺书中约定的范围内，且该等使用必须是为完成贵公司所安排的工作或为贵公司利益所为。

3、我公司进一步同意并做出以下承诺：

3.1 保密义务

**北京市药品监督管理局：**

保证对所获悉的贵单位保密信息按照下列规定进行保密，并在缺少相关保密条款约定时，应至少采取审慎的保护措施进行保密：

1）严格遵守国家保密局、公安部、市食药监管局等单位制定的法律、法规和相关保密制度。

2）未经信息管理部门同意，不得将保密信息透露给其他无关人员或任何第三方。

3）对于直接参与项目工作的人员，不能将工作中接触到的保密信息私自发布、传播、复制或仿造。

3.2 赔偿

我公司承诺若违反本承诺书中任何一项规定，一旦有证据证明有违反本承诺书的事实存在，贵单位即有权追究本公司相关责任，并要求本公司赔偿因此造成的一切损失，包括但不限于实际损失、取得的商业利益及其他因服务提供商擅自使用、披露或许可他人使用上述“保密信息”而产生的损失。同时，贵单位有权终止合同。

3.3 合同服务到期后，贵单位有权收回已提供的所有资料。

3.4 本承诺书经本公司盖章后生效。

服务提供商（盖章）：中国电信股份有限公司北京分公司

日期：2025年 4 月 21 日

合同编号：BJSGS2503640CGN00

附件 3：

# 保密承诺书

我了解有关保密法规制度，知悉应当承担的保密义务和法律责任。本人郑重承诺：

一、认真遵守国家保密法律、法规和规章制度，履行保密义务；

二、不提供虚假个人信息，自愿接受保密审查；

三、不违规记录、存储、复制国家秘密信息，不违规留存国家秘密载体；

四、不以任何方式泄露所接触和知悉的国家秘密；

五、未经单位审查批准，不擅自发表涉及未公开工作内容的文章、著述；

六、在实际工作中，凡定为“不宜公开事项”，包括内部会议、文件、尚未正式发布的决定、技术标准、研究成果、合同及其附件等内容，未经单位审查批准，不擅自对外公布或宣传；

七、离岗时，自愿接受脱密期管理，签订保密承诺书。

违反上述承诺，自愿承担党纪、政纪责任和法律后果。

承诺人签名：张秀博

承诺人身份证号码：140521198909250068

工作单位（盖章）：

2025 年 4 月 21 日

附件 4：中标通知书、服务方案

1 中标通知书

合同编号：BJSGS2503640CGN00

# 北京汇诚金桥国际招标咨询有限公司

## 中 标 通 知 书

中国电信股份有限公司北京分公司：

兹通知，贵单位在我公司组织的“信息化系统运行维护—安全和基础运维服务—政务云安全运维（项目编号：BJJQ-2025-036）”公开招标采购中，经评标委员会评定，确定为本项目的中标人，中标金额为：

人民币大写：叁佰玖拾伍万陆仟壹佰叁拾壹元陆角肆分

人民币小写：￥3956131.64 元

请贵单位于本通知书发出之日起 30 日内，持此通知书与北京市药品监督管理局洽谈合同事宜、签订政府采购合同，并于合同签订之日起 2 个工作日内，将合同正本原件（纸质一份、电子扫描件一份）递交到我公司办理合同备案。

请贵单位自合同签订之日起 5 个工作日内，到我公司办理投标保证金退还事宜。

北京汇诚金桥国际招标咨询有限公司

二零二五年四月三日

## 2 服务方案

### 2.1 服务内容

本次项目服务范围、服务周期清单如下：

| 服务项 | 描述 | 单位 | 服务期限（月） | 数量 |
|---|---|---|---|---|
| 密码服务 | 强身份认证服务 | 1 套 | 5 | 2 |
| | 签名验证服务 | 1 套 | 5 | 3 |
| | 时间戳服务 | 1 套 | 5 | 2 |
| | 加解密服务 | 1 套 | 5 | 2 |
| | SSL 安全服务（国密） | 1 套 | 5 | 2 |
| | 远程运维接入服务（国密） | 1 账号 | 5 | 5 |
| | 数据库透明加密服务 | 1 套 | 5 | 2 |
| | 应用数据库加密授权-数据库透明加密代理 | 1 套 | 12 | 1 |
| | 应用数据库加密授权-数据库透明加密 SDK | 1 套 | 12 | 1 |
| | 全球服务器 OV 通配符证书 | 1 套 | 12 | 1 |
| | 设备证书 | 1 套 | 12 | 5 |
| | 国密浏览器 | 1 套 | 12 | 5 |
| | 日志审计服务 | 1 次 | 12 | 1 |
| 基础支撑服务 | 商用操作系统 | 1 主机 | 5 | 180 |
| | 商用操作系统 | 1 主机 | 12 | 82 |
| | 数据库服务 | 1 套 | 5 | 36 |
| | 中间件 | 1 套 | 5 | 34 |
| 安全服务 | 主机杀毒服务 | 1 主机 | 5 | 180 |
| | 主机杀毒服务 | 1 主机 | 12 | 82 |
| | 主机防护服务 | 1 主机 | 5 | 180 |
| | 主机防护服务 | 1 主机 | 12 | 82 |

| 服务项 | 描述 | 单位 | 服务期限（月） | 数量 |
| --- | --- | --- | --- | --- |
| | 主机安全加固服务 | 1 主机 | 5 | 180 |
| | 主机安全加固服务 | 1 主机 | 12 | 82 |
| | 主机漏洞扫描 | 1 主机 | 5 | 180 |
| | 主机漏洞扫描 | 1 主机 | 12 | 82 |
| | 数据库审计服务 | 1 个 | 5 | 36 |
| | WAF 防护 | 1 个 | 5 | 12 |
| | 日志收集与分析服务 | 1 个 | 5 | 180 |
| | 日志收集与分析服务 | 1 个 | 12 | 82 |
| | 渗透测试 | 1 个 | 5 | 12 |
| | 渗透测试 | 1 个 | 12 | 4 |
| | 网页防篡改服务 | 1IP | 5 | 2 |
| | 云端 APT 防护 | 1 套 | 5 | 1 |
| | 云端 APT 防护 | 1 套 | 12 | 1 |
| | 本地数据备份服务 | 1GB | 5 | 409648 |
| | 应急预案 | 1 次 | 12 | 1 |
| | 应急响应 | 1 次 | 12 | 2 |
| | 应急演练 | 1 项 | 12 | 2 |
| | 安全通告 | 1 次 | 12 | 52 |
| | 管理制度修订 | 1 次 | 12 | 1 |
| | 安全巡检 | 1 次 | 12 | 12 |
| 灾备服务 | 灾备服务 | 1 次 | / | 1 |

2.2 密码服务方案

2.2.1 服务目标

依据《信息安全技术 信息系统密码应用基本要求》GB/T 39786-2021 的标

准规范，完成北京市政务云平台密码保障体系建设，实现北京市政务云平台与北京市共性密码支撑平台互联互通，并具备云上密码服务能力。完善网络和通信安全、设备和计算安全、应用和数据安全层面国产密码应用，从而为北京市药品监督管理局业务系统提供更加完善的安全服务，包括身份认证、数据签名验签、数据加解密、数据库透明加解密、时间戳、数据传输安全、远程运维接入安全等功能，有效为北京市药品监督管理局业务系统提供商用密码应用评估所需的密码服务。

2.2.2 强身份认证服务

对业务应用提供基于数字证书的强身份认证服务，实现北京市药品监督管理局政务云安全运维项目的用户身份鉴别，确保用户身份的真实、可靠，符合国家和北京市密码应用工作相关要求。

2.2.2.1 加密算法选择

依据强身份认证服务的招标要求，并展开密码算法需求分析。采用国产密码算法 SM2 展开身份校验计算，通过私钥进行身份信息计算，通过公钥展开身份信息验证。

2.2.2.2 密码策略

身份认证服务可以覆盖终端用户及业务系统间的强身份认证，提供多种认证方式，包括：基于 Ukey 的身份认证、基于协同签名的身份认证等，用户能够根据访问主体的安全要求，访问客体的重要程度，以及访问环境等因素，综合选择认证方式及访问控制手段。

身份认证服务能够实现个人用户、单位用户等各类业务主体的身份鉴权，验证其真实身份是否与其宣称的身份相符，能够有效保障保护业务主体合法身份和权限不被盗用，保证业务主体身份真实性、合法性。

2.2.2.2.1 基于 UKey 的身份认证

该认证方式适用于终端用户的身份认证，采用 UKey 作为数字证书载体，存储用户的密钥及数字证书，利用 UKey 内置的密码算法，实现对用户身份的认证，同时支持基于 PIN 码、实现双因子认证，保证用户身份的高安全性。

2.2.2.2.2 基于 UKey 的身份认证流程

基于 UKey 的身份认证流程如下图所示：

2.2.3 签名验证服务

对业务应用提供数据签名、签名验证等服务，确保数据的真实性、完整性和不可抵赖性。确保北京市药品监督管理局政务云安全运维项目符合国家和北京市密码应用工作相关要求。

2.2.3.1 加密算法选择

依据签名验签服务的招标要求，并展开密码算法需求分析。采用国产加密算法 SM4 展开身份信息数据加密，公钥算法 SM2 展开身份校验计算，散列算法 SM3 展开数据完整性保护。

2.2.3.2 密码策略

签名验签服务能够面向业务系统提供数据签名和验签、基于数字证书的身份认证、基于数字证书的加密和解密等安全保护，有效地解决共享信息的机密性、真实性、完整性、不可否认性等安全问题。

签名验签服务基于非对称密钥对实现，支持符合国密规范《GM/T 0003-2012》的签名算法。支持数据签名验签功能，对关键操作数据进行签名，保证数据的完整性和不可抵赖性。提供 PKCS1、PKCS7 attach、PKCS7 detach、XML Sign 等多种格式的数字签名和数字签名验证功能，能够有效地解决其共享信息的真实性、完整性、不可否认性等安全问题。

2.2.3.2.1 数据签名

数据签名支持符合国密规范《GMT 0003.2-2012》的签名算法。提供 PKCS1、PKCS7 attach、PKCS7 detach、XML Sign 等多种格式的数字签名功能。可对原文或摘要进行签名计算。

2.2.3.2.2 数据验签

数据验签支持符合国密规范《GMT 0003.2-2012》的验签算法。提供 PKCS1、PKCS7 attach、PKCS7 detach、XML Sign 等多种格式的数字签名验证功能。可对原文或摘要进行签名验证计算。数据验签通过签名设备进行运算，数据验签支持原文验签和摘要验签，根据业务场景的不同，数据验签支持业务系统传递数字证书和证书 DN 两种模式。

2.2.4 时间戳服务

对业务应用提供时间戳签名及验证等服务，保证业务操作过程中行为时间的不可否认性。确保北京市药品监督管理局政务云安全运维项目符合国家和北京市

密码应用工作相关要求。

2.2.4.1 加密算法选择

本项目的可信时间算法采用国密算法 SM3 以及 SM2 展开，通过 SM3 Hash 算法确定授时中心可信时间源信息，通过 SM2 非对称加密算法进行时间戳服务中心数字身份确认，保障来源可信。

2.2.4.2 密码策略

时间戳服务遵循 RFC3161 国际标准，基于国家标准时间源，采用 PKI 技术，符合国密规范《GM/T 0033-2014》的时间戳服务功能，为业务应用提供精准、安全和可信的时间认证服务，适用于涉及法律效力问题的应用场景。密码服务管理平台通过对时间戳服务的整合、封装，对各业务系统提供统一时间戳服务。

2.2.4.2.1 时间戳签名验签

时间戳签名服务的本质是将数据原文的 Hash 值和权威时间源绑定，在此基础上通过时间戳服务中心的数字签名，产生不可伪造的时间戳文件，通过电子数据及对应可信时间戳文件有效证明电子数据的完整性及产生时间。时间戳验证服务采用公私钥技术对时间戳的签名信息进行验算，以确定该时间戳是否为指定时间戳服务器所签发。

时间戳签名服务采用精确的时间源、高强度高标准的安全机制、能够为用户提供精确的且不可抵赖的时间戳服务。同时能够通过 HTTP 协议申请严格遵循国际标准（RFC3161）和 RFC2630 两种时间戳协议的时间戳，采用标准的时间戳请求、时间戳应答以及时间戳编码格式。

2.2.4.2.2 时间戳签名验签流程

进行时间戳签发时，业务系统需要对数据原文进行 Hash 运算，得到原文摘要值，然后通过时间戳签发接口，将原文摘要值发送至密码服务管理平台。密码服务管理平台接收到服务请求后，调取相应的时间戳服务器对原文摘要值进行时间戳运算并进行签名，最终将时间戳签名后的结果返回至业务系统。

2.2.5 加解密服务

对业务数据提供加解密服务，确保北京市药品监督管理局政务云安全运维项目重要数据的机密性，确保符合国家和北京市密码应用工作相关要求。

2.2.5.1 加密算法选择

结合业务系统对于重要敏感数据的加密需求，采用经典国密算法 SM4 展开计

算。

2.2.5.2 密码策略

加密解密服务基于对称加解密、非对称加解密、数字信封等密码技术，提供数据机密性保护。关键业务数据传输及存储时，对关键数据字段进行加密处理，应用前需预先进行解密操作，防止关键业务数据被窃取。

2.2.5.2.1 数据存储加解密

数据存储加解密基于对称密钥实现，对称密钥支持符合国密规范《GM/T 0002-2012》的 SM4 算法加解密。进行数据加密与解密，支持 ECB、CBC、OFB 模式。具体可分为三种实现方式：

一，密钥存储于密码设备中，每次加解密运算均由密码设备直接参与；

二，密钥存储于密钥管理系统中，每次加解密运算都拆分为两部分，一部分是密钥本身的解密运算，一部分是对数据的加解密运算；

三，密钥存储于业务端本地，通过非对称算法实现密钥分配，每次加解密运算需要先到密码云服务平台解密密钥，再进行本地运算。

2.2.5.2.2 数据传输加解密

业务系统采用数字信封技术进行传输加解密，该技术采用对称密码算法对消息进行加密，采用非对称密码算法对对称密钥加密，能够有效保证数据传输的安全性。支持基于 SM2 密码算法的数字信封，支持符合标准规范的 PKCS7 数字信封构建、数字信封解析。并支持由内部密钥保护到外部密钥保护的数字信封转换。

2.2.5.2.3 数据存储加解密流程

(一)密码设备存储密钥

业务系统将待加解密的数据传输至密码云服务平台。密码云服务平台接收到加解密请求后，调用存储于密码设备的加密密钥执行加解密运算。

密钥管理系统存储密钥

业务系统将待加密或解密的数据和应用主密钥 ID 传输至密码云服务平台。密码云服务平台接收到加解密请求后，调用匹配应用主密钥，并利用 KEK 解密应用主密钥后执行加解密运算。

本地存储密钥（数据密钥）

业务系统采用对称加密算法对本地数据进行加密存储。首先，需要解密数据密钥，提供在线解密和离线缓存两种模式。数据密钥解密完成即可在业务系统本

地执行加解密运算，运算完毕后立即清除解密后的数据密钥。

2.2.5.2.4 数据传输加解密流程

当业务系统间进行数据传输时，首先由发送方制作数字信封，并将其发送至接收方。接收方接收到数据后，向密码云服务平台发起数字信封解密请求。最终，密码云服务平台将解密后的数据明文回传至接收方，完成数据安全传输。

2.2.6 SSL 安全服务（国密）

面向北京市药品监督管理局云上各业务系统，基于 SSL/TLS 提供基于国密算法传输加密、身份鉴别、SSL 卸载、SSL 加壳等功能。

2.2.6.1 加密算法选择

结合北京药监业务系统对于 SSL 安全服务的需求，采用 SM2 算法展开客户端与服务端之间的密钥安全传输服务，采用 SM4 对传输数据进行数据加密。

2.2.6.2 密码策略

SSL 安全服务提供高性能的加解密服务，国密算法 SM4 的计算吞吐率≧6Gbps。

SSL 安全服务提供高安全身份鉴别级别，支持 SSL/TLS 协议族，支持单、双向身份认证，支持高强度加密算法，为应用提供可靠的身份认证方案，支持多种证书状态验证模式，包括 CRL（支持 LDAP、FTP、HTTP 协议）、OCSP 方式；

SSL 安全服务提供 SSL 卸载服务，通过将应用访问过程中 SSL 的加解密过程转到安全认证网关之上，从而减少服务器端的性能压力，提升客户端的访问响应速度。

SSL 安全服务提供代理加壳服务，实现基于数字证书的服务器端与客户端的双向认证，多种形式的证书透传功能能够非常方便地在应用层实现基于数字证书的安全认证。

2.2.7 远程运维接入服务（国密）

为北京市药品监督管理局政务云安全运维项目运维人员提供远程运维的接入服务，确保符合国家和北京市密码应用工作相关要求。

2.2.7.1 加密算法选择

通过进行堡垒机的改造加强运维密码信道能力，通过国密算法 SM2 校验运维人员身份，通过国密算法 SM3 确保运维数据不被篡改，通过国密算法 SM4 来展开运维数据及日志的加解密。

2.2.7.2 密码策略

采用国产密码算法，为云上租户提供安全可靠的远程运维接入解决方案。在设备计算安全方面主要是从登录设备人员的身份鉴别、访问控制信息完整性、远程管理安全通道、日志记录完整性来进行服务。

其中访问控制信息完整性通过堡垒机实现运维人员对被管理资产进行授权，同时解决系统资源访问控制。可以调用签名验签服务配合堡垒机，对系统资源的访问控制进行完整性保护

1）身份鉴别及远程管理通道安全

提供租户侧符合 GM/T 0024-2014《SSL VPN 技术规范》的 SSL 安全服务（国密），基于 SM2/3/4 算法 SSL 建立通信信道，运维人员由第三方 CA 机构颁发国密个人认证证书及智能密码钥匙，通过国密浏览器构建 HTTPS 通道配合账号口令登录堡垒机，堡垒机支持国密算法和 SSH v2 协议及以上对数据库和服务器等设备的远程管理通道安全。

2）系统资源访问控制信息完整性

提供云租户堡垒机通过与密码云签名验签服务对接集成，采用 SM2\SM3 算法，实现系统资源访问控制信息完整性保护。

2.2.8 数据库透明加密服务

对业务应用提供数据库透明加密、解密等服务，满足密评中应用和数据安全层面对重要数据存储机密性要求；支持国密 SM3 杂凑算法采用 HMAC 方式进行数据存储完整性保护；支持在业务系统透明访问的前提下，实现数据存储加密和查询解密。服务确保符合国家和北京市密码应用工作相关要求。

2.2.8.1 加密算法选择

采用国产加密算法 SM4 展开重要敏感数据加密，公钥算法 SM2 展开身份校验计算，散列算法 SM3 展开数据完整性保护。

2.2.8.2 服务方案

数据库库透明加密服务是一款基于数据库安全防护技术，面向客户敏感数据进行细粒度管控，在业务系统透明访问的前提下，实现数据存储加密和查询解密，确保数据处于有效保护的数据安全防护类产品。能够有效防范 DBA 风险，避免存储介质丢失、数据文件泄漏、数据库拖库，可能引起的数据泄漏。

系统为接入的第三方应用自动分配 APPID 和 APPSecret 密钥，当应用访问加

密插件时可以对应用的身份进行鉴权，建立双向认证机制，确保只有合法的插件才能获取到策略和密钥，从而确保敏感数据加密过程中的安全。

同时，为了保障密钥合规性，数据库透明加密服务需与密码云服务平台打通，由密码云服务平台对密钥生命周期进行统一管理。

2.2.9 应用数据库加密授权-数据库透明加密代理

提供数据库透明加密代理集成模式，在代理模式下，应用只需调整调用数据库的地址及账户，即可完成使用，支撑系统轻集成。

2.2.9.1 加密算法选择

采用国产加密算法 SM4 展开重要敏感数据加密，公钥算法 SM2 展开身份校验计算，散列算法 SM3 展开数据完整性保护。

2.2.10 应用数据库加密授权-数据库透明加密 SDK

提供数据库透明加密 SDK 集成模式，在 SDK 模式下，支持通过在应用以配置方式免改造实施。

2.2.10.1 加密算法选择

采用国产加密算法 SM4 展开重要敏感数据加密，公钥算法 SM2 展开身份校验计算，散列算法 SM3 展开数据完整性保护。

2.2.11 全球服务器 OV 通配符证书

为北京市药品监督管理局政务云安全运维项目提供 OV 通配符 SSL 证书，表明系统单位真实身份，能够验证一个域名以及该域名所有二级子域名的所有权，以及网站域名所有者的真实身份。证书支持谷歌、火狐、IE 等全球主流浏览器。

2.2.11.1 加密算法选择

结合北京药监业务系统对于 OV 通配符 SSL 证书的需求，采用 SM2 算法展开客户端与服务端之间的密钥安全传输服务，采用 SM4 对传输数据进行数据加密。

2.2.11.2 服务方案

SSL 服务器证书，是遵守 SSL 协议的一种数字证书，由全球信任的证书颁发机构(CA)验证服务器身份后颁发。将 SSL 证书安装在网站服务器上，可实现网站身份验证和数据加密传输功能。

OV 通配符 SSL 证书是 Wildcard SSL Certificate 的缩写，可以保护一个域名以及该域名所有的二级子域名，不限制子域名数量，且添加新的子域名无须重新审核和另外付费。

网站部署全球信任的 SSL 证书后，浏览器可直观展示认证标识和网站认证信息。

2.2.12 设备证书

为北京市药品监督管理局政务云安全运维项目提供设备 SSL 证书。

SSL 证书遵循国家标准 GM/T 0024-2023《SSL VPN 技术规范》的服务器 SSL 证书，支持相关软件，包括但不限于 360 和统信，支持 SM2/SM3/SM4 国产密码算法和国密安全协议，通过自主可控的密码技术，保护数据传输安全和服务器身份可信，应支持 360、奇安信等国密浏览器，支持谷歌、火狐、IE 等全球主流浏览器等。确保符合国家和北京市密码应用工作相关要求。

2.2.12.1 加密算法选择

结合北京药监业务系统对于设备证书的需求，采用 SM2 算法展开客户端与服务端之间的密钥安全传输服务，采用 SM4 对传输数据进行数据加密。

2.2.12.2 遵循的行业标准和规范

设备证书符合《GMT 0020-2012 证书应用综合服务接口规范》《GM/T 0024-2023 SSL VPN 技术规范》

2.2.13 国密浏览器

为北京市药品监督管理局政务云安全运维项目运维人员提供国密浏览器，系统运维人员能够通过国密浏览器与业务系统构建基于国密算法 SSL 协议的网络通道。确保符合国家和北京市密码应用工作相关要求。

2.2.13.1 加密算法选择

国密浏览器通过在浏览器客户端与服务端之间构建密文安全传输信道，通过采用国产加密算法 SM4 展开重要敏感数据加密，公钥算法 SM2 展开身份校验计算，散列算法 SM3 展开数据完整性保护。

2.2.14 日志审计服务

日志分析管理系统能够不间断地对应用服务器、数据库服务器、数据库管理系统等各类不同日志进行集中采集，并集中管理，实现日志完整性保护。主要用于保障云上租户堡垒机运维日志记录的完整性。

2.2.14.1 加密算法选择

采用国产加密算法 SM4 展开日志数据加密，公钥算法 SM2 展开身份校验计算，散列算法 SM3 展开数据完整性保护。

## 2.3 基础支撑服务方案

### 2.3.1 商用操作系统服务

#### 2.3.1.1 服务内容

服务内容：根据北京市药品监督管理局政务云安全运维项目系统现状和需求，提供信息系统政务云平台上正常运行所需要的主流商业操作系统服务，根据实际应用需求支持国产 Linux 操作系统（银河麒麟/中标麒麟/统信等）的各种主流版本，并提供操作系统的安装部署和各种故障处理。

服务范围：针对不少于 262 台云主机展开，其中 180 台云主机提供 5 个月的操作系统租用服务，其中 82 台云主机提供 12 个月的操作系统租用服务。可以根据项目实际云主机划分需求动态调整。

### 2.3.2 数据库服务

服务内容：按照北京市药品监督管理局政务云安全运维项目的要求，提供所需数据库 5 个月租用服务，根据实际应用需求支持提供主流的国产数据库（金仓/达梦/TiDB 等），为数据库及数据库集群提供功能完善的数据库管理平台，协助完成数据库、数据库集群及数据库管理平台的安装、配置和调试，并提供对数据库、数据库集群及数据库管理平台的维护服务。

服务范围：数据库服务针对不少于 36 台云主机展开，可以根据项目实际数据库需求动态调整。

### 2.3.3 中间件服务

服务内容：为北京市药品监督管理局政务云安全运维项目提供中间件软件，根据项目需求能够提供消息中间件及缓存中间件的服务能力，包括但不限于东方通、金蝶、宝兰德等。协助完成中间件软件的安装和调试，并提供维护服务。

服务范围：针对不少于 34 台云主机展开，可以根据项目实际数据库需求动态调整。

## 2.4 安全服务方案

### 2.4.1 主机杀毒服务

#### 2.4.1.1 服务内容

针对云主机提供恶意代码检测和拦截服务，及时发现和拦截各种恶意代码、病毒木马等，并有效阻断。

通过云主机杀毒服务，对云主机进行定期的病毒查杀，通过在虚拟云主机上

安装统一的杀毒软件控制中心，再在待保护云主机安全装主机杀毒客户端，进行主机杀毒服务。

针对虚拟化中出现的杀毒风暴、更新风暴及虚拟机差时防护等问题以轻型代理的方式提供全时的安全防护，安装部署杀毒软件，利用服务器端的最新木马库对虚拟机进行扫描和查杀，并可以对宿主机系统提供全面的安全保障。支持杀毒软件的集中控制，并且对网络性能无影响。

2.4.1.2 服务方式

采用适配云环境的防病毒软件，对虚拟机环境进行有效的病毒防护和查杀。

2.4.1.3 服务频率

服务期内持续不间断。

2.4.1.4 服务成果

此项服务完成后，将提供如下服务成果（包含但不限于）：

针对云主机服务期内提供每个月一份《主机杀毒服务报告》。

**2.4.2 主机防护服务**

2.4.2.1 服务内容

针对信息系统主机提供防护服务。

2.4.2.2 服务方式

采用适配云环境的主机防护软件，对虚拟云主机进行有效的防护。

2.4.2.3 服务频率

服务期内持续不间断。

2.4.2.4 服务成果

此项服务完成后，将提供如下服务成果（包含但不限于）：

针对云主机服务期内每个月提供一份《主机防护服务报告》。

**2.4.3 主机安全加固服务**

2.4.3.1 服务内容

通过技术手段对入云业务系统进行安全策略加强、调优，加强网络、系统和设备抵御攻击和威胁的能力。

安全加固服务通过全面了解服务器操作系统运行状况和安全状况，采取补丁修补，并优化和加强账号口令、日志审核、文件系统、权限控制、服务和进程等的安全性能。包括各种操作系统：Windows、Linux、各种 Unix 等。用户按照其

信息保护策略实施安全措施，主机中的主要组成系统包括操作系统和软件配置等，往往在一定时间段内是保持相对稳定的。

2.4.3.2 服务方式

通过人工服务的方式对云主机进行安全加固。

2.4.3.3 服务频率

云主机服务期内持续不间断。

2.4.3.4 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云主机服务期内提供 2 份《主机安全加固服务报告》。

**2.4.4 主机漏洞扫描**

2.4.4.1 服务内容

根据现有云主机的情况，通过对云主机进行漏洞扫描，分析业务系统所存在的风险隐患。

本项服务能够全方位检测 IT 系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

2.4.4.2 服务方式

采用适配云环境的主机漏洞扫描软件，通过与人工服务相结合的方式对云主机进行漏洞扫描。

1、开启控制中心虚拟机，部署主机漏洞扫描工具；

2、在用户允许下，收集漏洞扫描所需虚拟主机的 ip 地址和相关资料信息；

3、扫描完成后，对虚拟主机存在的问题进行分析和汇总，且出具漏洞扫描报告等。

2.4.4.3 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云主机服务期内提供 2 份《主机漏洞扫描服务报告》。

**2.4.5 数据库审计服务**

2.4.5.1 服务范围

针对入云业务系统数据库展开，可以根据项目实际数据库需求动态调整。

2.4.5.2 服务内容

对数据库系统的操作行为和访问行为进行分析和审计，及时发现高危操作行为和访问行为，并进行预警。

2.4.5.3 服务方式

在虚拟机部署数据库审计系统，通过虚拟网络旁路监听或代理实现数据库审计。

2.4.5.4 服务频率

入云业务系统的数据库在服务期内持续不间断。

2.4.5.5 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对入云业务系统的数据库在服务期内每个月提供 1 份《数据库审计服务报告》。

**2.4.6WAF 防护**

2.4.6.1 服务内容

WEB 应用防护基于对 Web 流量的解码和分析，对 Web 应用中的各类攻击，如 SQL 注入、XSS 注入、跨站请求伪造攻击、Cookie 篡改以及应用层 Web 攻击等问题，有效解决网页挂马、敏感信息泄露等安全问题，充分保障 Web 应用安全。

2.4.6.2 服务方式

通过在虚拟机上部署 WAF 防护系统来实现。

2.4.6.3 服务频率

北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的子系统服务期内持续不间断。

2.4.6.4 服务成果

此项服务完成后，将提供如下服务成果（包含但不限于）：

针对北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的子系统服务期内每个月提供 1 份《WAF 防护服务报告》。

**2.4.7 日志收集与分析服务**

2.4.7.1 服务内容

通过日志收集与分析的方式，对业务系统访问日志和运行日志进行数据分析，发现安全风险和入侵行为，当存在安全问题时，提出相关内容并给出解决建

议。

安全日志分析服务主要包括云主机日志安全配置、日志的收集和存储、可疑问题的通知处置以及安全事件的审计溯源。

2.4.7.2 服务方式

此项服务由我公司派遣专业安全工程师用户方现场进行调研查看、数据采集。提供日志数据总览展示、日志高效存储、配置管理、日志管理、事件管理、实时监测、报告报表、安全审计、安全功能、支撑功能等。

2.4.7.3 服务频率

云主机服务期内持续不间断。

2.4.7.4 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云主机在服务期内每个月提供1份《日志收集与分析服务报告》。

**2.4.8 渗透测试**

2.4.8.1 服务范围

北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的子系统。

2.4.8.2 服务内容

从攻击者的角度去分析目标所存在的安全隐患以及脆弱性，以全面了解和掌握应用系统所面临的安全威胁和存在的风险。采用专业测试工具针对云上业务系统环境主机、网络设备、应用系统等进行受控的、非破坏性的渗透测试，通过模拟黑客对目标系统进行渗透测试，对系统的任何弱点、技术缺陷或漏洞进行主动分析，评估系统抗攻击能力，全面了解和掌握应用系统所面临的安全威胁和存在的风险，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，以切实保证信息系统安全。

渗透测试实施内容主要包括渗透测试准备、渗透测试实施、渗透测试报告编写等主要阶段。

2.4.8.3 服务方式

我公司将组织一支专业队伍进行系统攻防测试工作，在用户的授权与监督下，通过专业的扫描工作和手工检测确认的方法进行。系统攻防测试主要采用以下工作方式：

1、访谈：通过问卷调查和当面沟通的方式进一步了解系统架构、功能模块构成、数据交互处理等技术细节问题；

2、工具扫描：通过各种扫描专业工具挖掘系统相关设备的路由路径、开放服务与端口、文件存储目录等信息，并检测应用程序编码所存在的安全漏洞。

3、手工检测确认：参考工具扫描结果，技术人员结合自身经验，通过构造特殊输入语句、编写检测脚本或程序代码、必要时搭建测试环境的方式，对系统可能存在的安全隐患进行验证。

2.4.8.4 服务频率

北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的子系统服务期内提供 2 次。

2.4.8.5 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的子系统服务期内提供 2 份《渗透测试报告》。

**2.4.9 网页防篡改服务**

2.4.9.1 服务内容

通过不是网页防篡改软件，对市药监局业务系统 Web 站点目录提供全方位的保护，防止黑客、病毒等对目录中的网页、文档、图片、数据库等任何类型的文件进行非法篡改和破坏。

2.4.9.2 服务方式

网页防篡改服务通过以下几功能联合实现，概况、服务器管理、安全防护、安装部署等功能实现网页防篡改功能。

通过在互联网应用虚拟机上部署网页防篡改系统来实现。在 Web 服务器一键安装 Agent，简单配置防护策略即可实现防护，全部操作都有可视化界面。提供统一管理平台，查看所有的服务器信息和安全状态，并下发安全策略配置信息。

2.4.9.3 服务频率

服务期内持续不间断。

2.4.9.4 服务成果

针对每个互联网应用在服务期内每个月提供 1 份《网页防篡改服务报告》。

**2.4.10 云端 APT 防护**

2.4.10.1 服务内容

通过威胁情报、入侵检测、异常检测、病毒木马检测、恶意代码基因图谱检测、未知威胁沙箱行为检测、恶意流量人工智能检测进行网络流量的实时分析，监控并识别可疑的威胁行为。

2.4.10.2 服务方式

云端 APT 防护系统是基于互联网攻防对抗威胁情报和企事业单位数据中心内部的安全态势要素数据，充分利用企事业单位公司现有的安全系统、安全设备，逐步演进为“安全数据集中存储、安全威胁分析与预警场景不断扩充、分析能力与数据对外开放”的高价值安全信息存储及、分析、预警和联动处置的运营平台。

通过在虚拟机上部署云端 APT 防护系统进行实现。

**2.4.11 本地数据备份服务**

2.4.11.1 服务范围

北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的子系统。

2.4.11.2 服务内容

针对入云系统数据库提供本地数据备份和恢复服务，并提供备份策略配置和维护服务。

本地数据备份服务支持对入云系统数据的本地备份服务和异地备份服务，默认提供非结构化数据保护、Windows/Linux/Unix 操作系统备份保护及对应平台的数据库、文件备份保护。

2.4.11.3 服务方式

通过在虚拟机中部署数据备份系统来实现。

采用 B/S、C/S 混合架构，其中管理控制台采用 B/S 架构，便于管理员进行系统运维管理；客户端采用 C/S 架构，便于进行备份数据传输。

2.4.11.4 服务频率

北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的子系统服务期内每日备份。

2.4.11.5 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对北京市药品监督管理局政务云安全运维项目涉及到的系统及其包含的

子系统服务期内每个月提供1份《本地数据备份服务报告》。

2.4.12 应急预案

2.4.12.1 服务范围

针对药监局在政务云上业务系统展开。

2.4.12.2 服务目的

修订与完善网络与信息安全应急预案，能够提升对网络与信息安全突发性危害事件的防范和应急处理能力，形成科学、有效，快速反应的应急响应机制，最大限度地减轻网络与信息安全突发公共事件对业务造成的影响，保障网络与信息系统的正常运行和数据安全。

2.4.12.3 服务内容

研究制定市药监局应急预案体系，内容将包含制定相应应急响应组织、预防、预警机制、事件定义分类、应急响应程序、事件上报处理机制、后期处理机制等内容，具体将分为综合预案、专题预案以及特定预案。在预案修订与完善的咨询服务过程中，将与市药监局相关人员保持紧密的沟通合作，以确保预案的科学性、指导性和合理性。

2.4.12.4 服务频率

药监局在政务云上业务系统服务期内提供1次。

2.4.12.5 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对药监局在政务云上业务系统服务期内提交1份《应急预案》（修订版）。

2.4.13 应急响应

2.4.13.1 服务范围

针对云上业务系统展开。

2.4.13.2 服务内容

在信息系统发生安全事件时及时响应，执行应急响应流程，通过专家级技术支持和特殊时期现场值守人员快速响应，及时抑制和消除用户信息系统安全事件，减少损失和负面影响，提高药监局信息系统业务连续性。

2.4.13.3 服务方式

根据对事件进行处理的地点不同，我公司安全服务人员的应急响应服务分为远程应急响应和本地应急响应：

1、远程应急响应

应急工程师在接到用户相关人员通过电话、Email、传真方式的请求后，如果无法通过相同的方式为用户解决问题，经与用户网络相关人员确认后，用户方网络相关人员提供主机或设备的临时支持账号，由应急工程师远程登录主机、网络设备、安全设备进行监测和服务，问题解决后出具详细的安全响应服务报告。如远程系统无法登陆，或无法通过远程访问的方式替用户解决问题，用户确认后，转到本地紧急相应流程，同时此次远程响应无效，归于本地应急响应类型。

2、现场应急响应

我公司将委派安全服务人员在第一时间赶往用户网络事发地点，在现场为用户查找事发原因并解决相应问题，并出具详细的安全响应服务报告。

2.4.13.4 服务频率

云上业务系统服务期内按需提供。

2.4.13.5 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云上业务系统服务期内提交 2 份《应急响应报告》（每半年一份）。

**2.4.14 应急演练**

2.4.14.1 服务范围

针对云上业务系统展开。

2.4.14.2 服务目的

开展应急预案演练是应急管理工作的重要内容，是检验应急预案实用性、应急机制科学性、应急体制合理性、应急程序的适用性的必要途径。根据应急预案规定的流程协助用户进行相应的模拟演练，一方面使用户相关方熟悉应急流程，提高对安全事件的响应能力；另一方面验证预案的正确性和适用性，并对演练过程进行总结分析，根据需要对应急预案进行修订，逐步完善应急预案。

2.4.14.3 服务内容

我公司会根据信息化主管部门要求，不定期地进行网络信息安全方面的应急演练，模拟实战对业务信息系统开展防御演练。

我公司会根据用户的安排每年至少进行 1 次网络信息安全应急演练。应急演练模拟实际攻防环境，包括网络攻击、应用系统防御、病毒入侵等方面的内容。应急演练结束后我公司会对演练进行总结，以提高运维人员实际处理突发事件的

能力。

2.4.14.4 服务方式

应急演练分为桌面流程推演、技术性实操演练两种开展方式。

1、桌面流程推演

桌面流程推演将模拟影响范围广、牵涉部门多、经济损失大和危害程度深的较严重类信息安全事件，如网络核心或主要汇聚节点发生瘫痪故障、门户网站遭恶意篡改等。

2、技术性实操演练

我公司安全服务人员将协助用户方开展技术性实操演练，在双方协商的基础上，确定演练对象和演练方案，明确所涉及的信息系统、模拟的安全事件类型和应急响应流程与处置方法。

2.4.14.5 服务频率

云上业务系统服务期内提供 2 次。

2.4.14.6 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云上业务系统服务期内提交 2 份《应急演练报告》（每半年一份）。

**2.4.15 安全通告**

2.4.15.1 服务范围

针对云上业务系统展开。

2.4.15.2 服务目的

跟踪最新的系统、网络和设备发现的安全问题而设置的，搜集整理的漏洞信息、系统补丁信息、病毒信息，及时有针对性地发布，确保用户在第一时间内得到相关的网络安全信息，以此提高用户方的安全防范意识。

2.4.15.3 服务内容

组织专人定期搜集整理漏洞信息、系统补丁信息、病毒信息等安全状态信息，形成安全通告信息，并定期以电子邮件的方式发送给用户信息安全负责人，确保用户在第一时间内得到相关的安全态势信息。

信息安全通告内容通常包括：本周信息安全疫情、专家预防建议、重点网站系统安全状况跟踪趋势、最新信息安全资讯、最新发布漏洞及解决建议、安全小常识等内容。

2.4.15.4 服务方式

本项服务主要是由安全工程师进行远程信息收集，整理编制成信息安全通告，每周的《信息安全周报》以邮件发送用户的方式开展；每月的《信息安全通告》主要通过编制书面报告的方式，提交给用户方。

2.4.15.5 服务频率

云上业务系统每周 1 次，整个服务期共 52 次。

2.4.15.6 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云上业务系统服务期内提交 52 份《安全通告》。

**2.4.16 管理制度修订**

2.4.16.1 服务范围

针对云上业务系统展开。

2.4.16.2 服务目的

参考信息安全等级保护管理要求，进一步修订和完善北京市药品监督管理局安全管理制度，使北京市药品监督管理局满足国家相关信息安全要求。

2.4.16.3 服务内容

我公司会基于北京市药品监督管理局实际信息化组织结构情况，参考信息安全等级保护管理要求，从安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等方面修订和完善安全管理制度，健全相应的安全管理组织架构，明确相应岗位和职责，完善安全管理和操作流程。

2.4.16.4 服务方式

提供现场和远程服务。

安全管理制度修订的工作步骤如下：

实施前期调研：采用调研访谈的方式，了解用户信息化组织机构、人员职责、系统运维管理机制、现有安全管理制度等情况，结合等级保护差距分析结果，分析系统安全管理现状和制度建设完善的需求。

构建管理框架：在总结分析用户信息安全管理现状的基础上，以等级保护标准所规定的管理要求为依据，开展制度修订，并提交用户相关负责人进行审核确认；

制定管理制度：以安全管理框架为依据，结合用户实际情况、业务系统特点

和现有安全管理制度，开展制度文件修订；

制度审核修订：将编写完成的制度文件提交用户方，并召集运维管理人员，就制度文件初稿进行审核、修订和完善，最终形成安全管理制度修订版。

2.4.16.5 服务频率

云上业务系统服务期内提供 1 次。

2.4.16.6 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云上业务系统合同签订后 1 个月内提交 1 份《安全管理制度》，并组织实时修订。

2.4.17 安全巡检

2.4.17.1 服务范围

针对云上业务系统展开。

2.4.17.2 服务目的

通过安全巡检服务，保证北京市药品监督管理局云上业务系统的持续稳定运行，重点搜集分析当月日志信息，并做好工作记录。为用户信息系统的整体持续、高效运行提供保障。

2.4.17.3 服务内容

我公司会根据服务合同要求的安全巡检指标，通过现场安全值守人员定期对云上业务系统云主机操作系统、数据库、中间件性能、状态、策略进行安全巡检，分析历史状态或事件记录，可以发现系统数据库中隐藏的安全隐患，并及时落实补救措施，重点搜集分析当月日志信息，并做好巡检记录。

2.4.17.4 服务方式

安全巡检服务主要通过检查、测试分析等方式进行。同时，根据用户业务情况和系统现状，制定详细的调查表，并由专业安全服务人员进行填写，以获得业务系统基础数据。具体包括应用信息系统调查表、物理资产调查表、软件资产调查表、各相关设备调查表等表格。主要通过现场安全值守人员完成。

在充分理解和掌握用户信息系统的资产情况、网络部署情况、核心业务信息系统实际运行状况的前提下，结合信息安全专家对各种信息技术产品和工具的知识和经验，对网络和相关信息系统的安全状况进行检查和判断，对网络安全和信息系统安全提出专业的完善和改进建议，针对发现的隐患提供相应的安全防护解

决方案。

2.4.17.5 服务频率

云上业务系统人工巡检频次每周 1 次。

2.4.17.6 服务成果

在本项服务完成时，将提交（但不限于）如下文档：

针对云上业务系统服务期内每个月提交 12 份《安全巡检报告》。

**2.5 灾备服务**

服务内容：根据《北京市政务云管理办法》要求，为部署在政务云上的市药监局业务系统建立同城或异地灾备机制，确保数据安全和业务连续性。

服务范围：针对入云业务系统数据展开，可以根据项目实际数据需求动态调整。

服务成果（包括但不仅限于）：服务期内提供 1 份《灾备服务报告》。

**3 服务团队和人员安排**

为了确保市药监局业务系统安全稳定运行，中国电信将组建专业的服务团队，其中项目经理具备 10 年（含）以上信息化项目工作经验，具备有效的信息化相关专业高级工程师证书、信息系统项目管理师证书。项目团队具备相关技术资质证书（信息安全工程师、CISP 注册信息安全专业人员、CISAW 信息安全保障人员认证等）。

中国电信将向药监局提供拟派参加本项目的主要人员名单、项目组织结构以及各自职责的划分，并附上核心项目人员简历。所报项目组成员一旦确定，服务期内不擅自更改。