安全应用维护服务

合　同　书

北京市人力资源和社会保障局

北京国信博飞科技发展有限公司

合同编号：

合　同　书

项目名称：安全应用维护服务

委托方：（甲方）北京市人力资源和社会保障局

受托方：（乙方）北京国信博飞科技发展有限公司

签订地点：北京市

签订日期：2022 年 12 月

鉴于北京市人力资源和社会保障局安全应用维护服务通过公开招标方式确定乙方（北京国信博飞科技发展有限公司）为本项目中标人/成交供应商，依据《中华人民共和国民法典》的规定，甲乙双方经充分协商达成一致，签订本合同。

一、定义

本合同中的下列术语应解释为：

1. “合同”系指买卖双方签署的、合同格式中载明的买卖双方所达成的协议，包括所有的附件、附录和构成合同的其它文件。

2. “合同款”系指根据合同约定，乙方在完全履行合同义务后甲方应付给乙方的款项。

3. “人员”系指作为雇员由乙方所雇佣并被分配执行服务或其任何部分的人员。

4. “服务”系指由乙方根据合同所实施的工作。

5. “甲方”系指北京市人力资源和社会保障局。

6. “乙方”系指（北京国信博飞科技发展有限公司）。

7. “现场”系指合同约定服务实施地点。

8. “由甲方提供的支持”系指由甲方免费为乙方执行合同项下的服务而提供的数据、服务、设备以及便利。

二、合同文件

下列文件构成本合同的组成部分，应当认为是一个整体，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：

1. 本合同书
2. 中标/成交通知书（详见附件一）
3. 合同一般条款
4. 合同特殊条款
5. 合同附件 （技术文档、安全保密协议等）

三、服务内容

乙方负责“安全应用”的运维服务，乙方的服务内容详见附件二：《服务内容》；乙方的服务方案详见附件三：《安全应用维护服务方案》。

四、服务对象、地点和时间

乙方为甲方提供的运维服务针对用户包括：北京市人力资源和社会保障局用户，运维服务期间：合同约定服务期限，服务地点：北京市人力资源和社会保障局。

五、合同总价

本合同总价：人民币（大写）陆佰零捌万伍仟柒佰元整。本项目资金来源为财政资金，合同约定的付款期限及付款方式、付款额度以财政资金到位情况为准。因财政资金未到位而影响甲方支付的情况不视为甲方违约，乙方应予以理解并保证合同履行。

六、付款方式

本合同的付款方式为：一次性支付。

七、服务期限

自 2022 年 1 月 1 日起至 2022 年 12 月 31 日止。

八、合同的生效

本合同经双方各自的法定代表人或授权代表人签署、加盖单位公章或合同专用章并由中标人/成交供应商递交履约保证金之日起生效。

（此页无正文）

采购人（甲方）：北京市人力资源和社会保障局

名称：（印章）

2022 年 12 月 13 日

法定代表人或授权代表人：

地址：北京市通州区清风路 33 号院 4 号楼

邮政编码：101169

电话：010-55585416

开户银行：

账号：

中标人/成交供应商（乙方）：北京国信博飞科技发展有限公司

名称：（印章）

2022 年 12 月 13 日

法定代表人或授权代表人：

地址：北京市海淀区西直门北大街 32 号枫蓝国际 A-1108

邮政编码：100086

电话：010-88147251

开户银行：招商银行北京西直门支行

账号：110909307510688

合同一般条款

一、服务事项及内容

乙方为甲方所委托的安全应用维护服务项目提供服务，具体内容详见附件二。

二、服务期间

乙方为甲方提供服务期间为12个月，自2022年1月1日起至2022年12月31日止。

三、服务地点

本合同项下的服务履行地点为北京市人力资源和社会保障局。

四、合同款及支付方式

1. 本合同合同款总额为人民币￥6,085,700.00元，大写：人民币陆佰零捌万伍仟柒佰元整。

2. 双方签署合同后，甲方收到乙方正式服务发票及履约保函后，于2022年内支付乙方合同全款，即人民币￥6,085,700.00元（大写：人民币陆佰零捌万伍仟柒佰元整）。

3. 乙方应在甲方付款前向甲方开具正规合法发票，否则甲方有权暂不付款且不承担逾期付款的违约责任。因乙方原因（包括但不限于未开具发票、开具发票不符合甲方要求等）导致甲方因财政政策原因未能付款，相应责任由乙方承担。

五、履约保函

双方签署合同后20个工作日内，乙方应向甲方提供合同总价款10%的即人民币￥608,570.00元（大写：人民币陆拾万零捌仟伍佰柒拾元整）的履约保函。履约保函有效截止日为2022年12月31日（合同到期日）。

六、权利和义务

1. 甲方的权利和义务

（1）甲方有权得到符合合同要求的服务。

（2）甲方有权拒绝乙方所委派的但其业务素质不被甲方所认可，或不遵守甲方工作场所规章制度的服务人员，甲方要求更换服务人员的，乙方应在7日内完成更换。

（3）甲方应按合同约定向乙方支付维护合同款。

（4）甲方有权要求乙方提供与服务内容有关的相关信息。

（5）甲方有权随时当面问讯相关业务等问题，乙方必须配合，保障甲方工作的顺利进行。

（6）甲方需向乙方提供服务所必须的人力、设备和环境资源的配合。

（7）甲方在使用期间，如发现系统故障应立即向乙方通报，以确保乙方在第一时间内排除故障，并负责与有关其它供应商进行联系。

（8）甲方应保守乙方的技术秘密和商业秘密。

2. 乙方的权利和义务

（1）乙方有权按照合同的约定向甲方收取维护合同款。

（2）乙方有权得到甲方对于系统故障的及时通报。

（3）乙方应按照本合同要求的服务内容，及时有效的完成规定的运行维护工作，保证系统正常运行。

（4）乙方应制定运行维护相关工作制度、工作流程、工作标准，并建立相关设备档案及维护档案。对服务过程中的技术文档按照甲方要求妥善保存，对于服务过程中的重要事项如实记录，并经双方人员签字确认。

（5）乙方在履行服务过程中，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、操作步骤以及可能出现的风险，经甲方确认后方可开展工作。

（6）乙方在服务中接受甲方的监督，与甲方通力合作，接纳甲方的合理建议，根据甲方的要求对服务问题进行整改，提高服务质量，并根据需要向甲方提出合理化的设备更新或增容建议或新系统建设相关方案，协助甲方建立系统管理和使用管理制度。

（7）乙方定期对甲方系统进行预防性检查，并向甲方提交检测报告、故障分析报告、月报、年报等，确保系统运行达到规定的运行标准，确保系统的安全性和灾难恢复能力。因乙方维护不当造成的安全事故，乙方应负赔偿责任。

（8）乙方对程序开发类的服务成果应以计算机光盘和纸介质形式交付甲方。

（9）乙方应保守甲方的相关技术秘密、政务信息及相关内部事务信息。

（10）乙方选派的服务人员，应具备合同约定服务所必须的技能，获得相关认证，工作态度认真负责，在项目执行中能与甲方正常沟通，服从甲方的工作安排，遵守甲方的工作环境和行为要求。服务人员必须签署保密协议，必须明了其工作内容和要求。

（11）乙方应遵守甲方关于新冠疫情防范的各项要求，加强对本单位运维服务人员的管理及教育，并承担运维服务人员因漏报、瞒报个人健康、行程等情况所造成的后果。

七、违约条款

1. 乙方未按约定提供服务

如果乙方未按合同规定的服务条款提供服务或季度运维服务质量考核不合格的，应向甲方支付违约金，每发现一次，按合同款的3%支付违约金。给甲方造成损失的，还须承担赔偿责任，具体赔偿金额视损失情况而定。违约金和赔偿金的支付并没有免除乙方继续履行合同的义务。

乙方违反本合同所规定的保密义务，乙方应立即采取补救措施，乙方应支付违约金（合同款的20%）、并退回已收取的全部合同款，甲方有权单方面解除合同，并可提请司法机关依法追究违约方及相关人员的刑事责任。

2. 甲方未按约定支付合同款

如果甲方不能按期支付乙方合同款，则应从逾期支付的第31个工作日起，每日按迟延支付金额的0.5‰向乙方支付违约金。此项违约金总额不超过迟延支付价款的5‰。逾期支付超过30天以上时，乙方有权终止合同或暂停服务。乙方有权收回从服务开始之日至实际终止日期间履行部分的费用，并有权对由此引起的损失要求甲方予以赔偿。

八、服务质量考核条款

1. 甲方依据附件二对乙方提供的服务质量进行考核。由局大数据中心组织项目最终验收。

2. 如果乙方没有满足服务质量要求，乙方除应采用补救措施、支付违约金外，给甲方造成损失的，还应赔偿甲方的全部损失。

3. 乙方应在每月开展一次应用系统巡检，并提交巡检报告。每季度开展一次工作汇报，并向甲方提交书面季度服务工作总结报告，接受甲方的评审。甲方应当在收到月度服务工作总结报告后15日内对报告进行评审或提出质疑。15日内未提出质疑的，视为甲方通过评审。

九、知识产权

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. 本项目实施所产生的信息资源及全部技术成果（包括但不限于软件、源代码及技术资料）的知识产权（包括但不限于著作权、专利权、商标权、专有技术等权利）及衍生权利均由甲方享有，凡有必要或可能申请专利的技术成果，均须由甲方办理专利申请。甲方在办理专利申请过程中如需乙方配合，乙方应予配合。合同终止时，乙方应在合同终止之日起三十日内，将上述全部技术成果及衍生成果等全部实际交付给甲方。

3. 对在运维、开发过程中获知的甲方或为甲方提供服务的第三方的知识产权，都受本条款的保护。

十、保密条款

1. 自合同签订之日起，乙方有责任对甲方提供的各种技术文件（包括但不限于软件、咨询报告、服务内容）与工作业务信息进行保密，未经甲方书面批准不得提供给第三方。如有违反，乙方应承担相应的法律责任。此保密义务不因合同的终止而免除。

2. 乙方必须与甲方签订《安全保密协议》（详见附件四）。如违反《安全保密协议》，必须承担全部责任并赔偿甲方的一切损失，甲方有权追究乙方的法律责任并单方解除本合同。

3. 乙方必须遵守甲方的各项规章制定，严格按照工作规范组织进行运维工作，制定切实可行的措施保障人员安全，设备安全，生产安全。乙方必须制定合理的措施对运维人员进行管理和思想教育，加强保密意识，安全生产意识。

4. 甲、乙方应积极配合信息安全主管部门对信息安全进行监督检查。

十一、合同廉政承诺

1. 合同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。

十二、不可抗力

1. 如果合同任一方因战争、火灾、洪水、台风、地震和其他不可抗力原因，影响了合同的履行，则可根据受影响的程度顺延合同履行期限，这一期限应相当于事故所影响的时间。受不可抗力影响的一方在不可抗力影响的范围内，不承担违约责任。但若一方违约在先，不得以此后发生不可抗力为由免除其违约责任。

2. 受不可抗力影响的一方应在事件发生后，立即通知对方，并在十日内以书面方式向对方提供该不可抗力事件的证明文件（如政府公告、新闻报道等），并应于不可抗力事件结束后，立即恢复对本合同的履行。

3. 如果不可抗力事件后果影响合同执行超过 90 天，双方则就未来合同的履行另行商议。

十三、争议的解决

1. 本合同按中华人民共和国相关法律、法规进行解决。

2. 因履行合同所发生的一切争议，双方应友好协商解决，协商不成的按下列第（1）种方式解决：

（1）提交北京仲裁委员会仲裁，仲裁裁决为终局裁决；

（2）依法向甲方所在地有管辖权的人民法院起诉。

3. 发生争议期间，乙方有义务继续按照服务内容条款中的要求提供服务，不得中断。

十四、合同的终止与解除

1. 到期

合同期限届满，且双方未就续约事宜达成一致的，合同到期终止。

2. 违约的解除

甲方违反合同的约定未及时支付乙方合同款，甲方在乙方发出要求甲方纠正违约行为的书面通知之日起30天内未能纠正违约行为并赔偿损失的，乙方有权书面通知违约方立即解除本合同。

乙方在连续1个月的运维服务质量考核中不合格的，乙方在甲方发出要求乙方纠正违约行为的书面通知之日起30天内未能纠正违约行为的，甲方有权解除合同。

乙方在提供运维服务过程中，出现重大安全事件的，甲方有权解除合同。

根据本合同约定、甲方解除合同的，双方的合同款按日计算（每日的合同款＝年度合同款÷365天），乙方应按日返还其已经收取的、解除合同之日以后的合同款。乙方应在收到甲方解除通知的30日内完成返还义务。

十五、其它条款

1. 在合同履行过程中，甲、乙双方均不得任意修改合同内容，一方如需修改合同某项条款，需向另一方出具变更内容及理由的申请书，经对方同意并修改相应内容后方可实施，在达成新的协议之前，双方仍按原合同条款进行，否则，后果由自行修改条款一方负责。

2. 本合同的附件为本合同不可分割的部分，与合同正文具有同等效力。

3. 如本合同附件中的条款或本合同签署之前所签署的任何文件与本合同的条款相冲突或不一致，以本合同为准。

十六、附则

鉴于安全应用维护服务合同款由财政拨款的特殊性，下一年度此项目运维合同生效之前，乙方应按本合同继续提供系统的运维、服务保障，确保系统的稳定、安全、可靠运行。

由于合同中所涉及的服务内容具有连续性、不间断性的特点，在本合同服务到期后至甲方与新服务商签署服务合同前，乙方将根据本合同服务条款内容继续提供运维服务，服务时间至甲方与新服务商签署服务合同时为止，费用按照乙方服务时间占全年服务时间的比例乘以本合同总金额计算，由新服务商提供。

十七、合同的生效

1. 本合同自双方加盖单位合同章或公章后生效。

2. 本合同一式陆份，甲、乙双方各执叁份。具有同等法律效力。

3. 本合同未尽事宜，应经双方协商后以补充协议方式明确。补充协议自双方加盖单位合同章或公章后生效，且补充合同内容不得背离本合同实质性内容。

合同特殊条款

无。

附件一：中标/成交通知书

中信国际招标有限公司

中标通知书

北京国信博飞科技发展有限公司：

在我公司组织的安全应用维护服务（0733-22182237）招标活动中，经评标委员会推荐和采购人确认，确定你单位为上述项目的中标人。中标金额：大写：陆佰零捌万伍仟柒佰元整，小写：¥6,085,700.00。

请你方在本通知书发出之日起30日内与采购人签订本项目合同。

特此通知。

中信国际招标有限公司

二〇二二年十一月十五日

【中信国际招标有限公司】

附件二：《服务内容》

1 身份认证服务

身份认证由用户认证、应用认证、设备认证组成、利用数字证书和智能密码钥匙，采用统一的身份认证协议和身份认证票据传递机制为用户、业务应用系统、设备等提供身份认证、信任传递、访问控制服务。统一为市人力社保局信息系统提供身份认证服务，包括基于实体数字证书、移动证书和社保卡等形式的用户身份鉴别，确保信息系统的应用安全。

服务名称	服务内容	数量
身份认证服务	为市人力社保局用户的证书提供有效期验证、随机数验证、黑名单列表验证、证书链列表验证等维护服务。对用户证书与业务系统绑定进行维护服务。提供对用户认证的统计分析，并提供安全预警配置服务。 服务频率：服务期限内全年提供服务。每日监控认证接口运行情况、黑名单下载情况、异常登录情况。每月对登录日志进行处理及认证数据的整理。每年一次服务器证书更换。 提交成果：每月提交用户登录情况与安全分析报告，每日检查安全接口及服务器状态运行情况并生成检查运维单。	1 项

2. 数据加解密及密码管理服务

统一为市人力社保局信息系统提供数据加解密服务，通过数据加密保障数据防泄露，通过数据签名保障数据完整性，为信息系统中重要数据提供加密、解密、签名、验签等措施，确保数据应用的安全可靠。统一为市人力社保局信息系统提供密码管理服务，包括提供密码安全管理、密码配置、密钥备份和密码应用等，根据用户需求完善密码安全体系建设，配合开展密码评估等工作。

服务名称	服务内容	数量
数据加解密服务	为业务数据提供数据加解密、数据签名验签服务，以及与其它委办局进行数据交换提供加解密维护服务，对业务系统的重要数据进行安全分析制定防护措施。 服务频率：服务期限内全年提供服务。每日监控加解密接口、签名验签接口及日志处理服务运行情况。每月对加解密、签名验签日志进行处理及安全数据的整理。每年对加解密密钥进行更新。	1 项

	提交成果：每月提交业务数据加解密、签名验签情况与安全分析报告，每日检查接口及服务器状态运行情况并生成检查运维单。	
密码管理服务	进行密码的综合管理，提供数据查询统计、系统配置等运行维护。为信息系统的加解密、签名验签及数据交换接口提供密码服务的安全配置维护服务。为每个信息系统提供不同的密钥，为管理人员提供密钥制作、生成、导出等维护服务。 服务频率：服务期限内全年提供服务。每日监控系统及加密机服务运行情况。每日对加密池的缓存进行清理。每月对检查密钥的使用情况以及对密钥的备份。 提交成果：每月提交密钥使用情况与安全分析报告，每日检查接口及服务器状态运行情况并生成检查运维单。	1 项
安全验证服务	对安全接口服务调用的验证服务、安全配置进行维护服务。对服务调用和调用结果的安全验证进行维护服务。提供安全接口应用的统计分析及安全配置服务。 服务频率：服务期限内全年提供服务。每日监控验证接口运行情况。每月对安全接口访问情况进行统计。 提交成果：每月提交安全验证接口使用情况与分析报告。	1 项

3 安全审计及操作日志分析服务

统一为市人力社保局信息系统提供安全审计服务，包括提供用户操作业务的审计行为、用户操作信息系统的日志采集、用户操作行为追溯以及安全配置等服务。

服务名称	服务内容	数量
安全审计及操作日志分析服务	精确地记录用户的日志，可按日期、地址、用户、资源等信息对日志进行查询、统计和分析。审计结果通过 Web 界面以图表的形式展现给管理员。 负责对用户的访问日志进行实时监控、访问操作行为进行合规监管。日志监控主要包括三部分： （1）系统管理员分配权限的日志。（2）上传下载保密文件的日志记录。（3）上机日志。 对用户操作信息系统的日志采集、用户操作行为追溯以及数据安全配置进行维护服务。对用户所有操作及数据行为进行统计和分析，提供安全监控服务能力。 服务频率：服务期限内全年提供服务。每日监控系统及接口运行情况，每月对审计日志进行处理及日志数据备份。	1 项

	提交成果：每月提交用户登录、操作行为情况与安全分析报告，每日检查数据处理接口运行情况并生成检查运维单。	

4 数字证书服务

统一为市人力社保局信息系统提供用户管理、数字证书管理和权限管理，包括实体证书和移动证书等，进行证书申请、发放、更新、吊销、补办及技术支持等服务。

服务名称	服务内容	数量
数字证书服务	1、用户生成、用户校验、用户初复审状态、用户吊销等管理。 服务频率：每日对用户的生成、验证等服务进行监控；每日查看需要新增、吊销的用户信息并进行新增和吊销操作；每月对用户信息进行梳理。 提交成果：每月提交用户系统使用情况与分析报告。 2、市人社局 22500 张数字证书更新服务，包括申请、发放、吊销补办等技术支持。 服务频率：服务期限内全年提供服务。 提交成果：每月提交用户证书使用情况与分析报告。 3、资源、角色及其关系维护、权限申请、审批员审批、管理员授权等维护工作。 服务频率：每日对权限验证、权限同步等服务进行监控、每日对权限申请的数据进行梳理和整合；每月对权限信息进行整理分析。 提交成果：每月提交权限验证接口使用情况与分析报告。	1 项

5 应急演练

针对市人社局网络安全环境协助编制应急预案并修订完善，根据应急预案规定的流程，进行相应的模拟演练，使得相关人员了解应急流程和自己的责任，在安全时间发生时，能够有条不紊开展应急工作，最大程度降低安全事件带来的负面影响和损失。

服务名称	服务内容	数量
应急演练	根据应急预案规定的流程协助市人社局每年进行 1 次网络安全预案的模拟演练工作，使相关方熟悉流程，提高对安全时间的响应能力，根据实际情况对应急预案进行修订。 服务频次：每年 1 次 提交成果：《网络与信息安全应急预案》、《应急演练方案》、《应急演练报告》	1 项

6 网络安全服务及安全软硬件设备维护

服务内容包括日常网络安全服务保障；银行、代办、保险公司等专线的安全接入和维护保障；区人力社保局、社保所和社区等接入访问的安全维护与保障；各专线和网络接入的安全软硬件设备维护等。

服务项目	服务名称	服务内容	数量
网络安全日常服务保障	网络流量监控	监控人员每日监控办公楼互联网、政务外网等网络的运行状态和网络流量，及时评估网络运行状况，对异常网络流量进行分析。 服务频率：服务期限内每日对网络流量进行监控。 提交成果：每月提交网络流量监控与分析报告。	1 项
	网络安全监控	监控人员每日对办公楼安全防护设备网络攻击防御、应用攻击防御、入侵检测等进行监控。 服务频率：服务期限内每日进行网络安全监控。 提交成果：每月提交网络安全分析报告。	1 项
	配置核查	根据当前的网络安全形势对办公楼安全设备的安全策略进行调整，防止被攻击和利用，调整内容包括访问控制策略，隔离不同安全区域策略，关闭易受攻击的端口策略等。 服务频率：服务期限内每季度提供一次配置核查服务。 提交成果：配置核查报告。	1 项
	日志分析	运维人员每月对办公楼安全防护设备产生的日志进行分析，包括网络攻击日志、防病毒日志等，可及时发现异常攻击行为，并对攻击源进行封堵，防止恶意流量进入内部网络，确保办公楼网络正常运行。 服务频率：服务期限内每月提供一次日志分析服务。 提交成果：日志分析报告。	1 项
	应急响应	针对日常和重要时期发生的应急事件按照应急预案进行应急响应。保证事件的损失降到最小，清除安全事件产生的影响，并开展相应的事后分析。	1 项

		服务频率：日常和重要时期发生的应急事件后第一时间进行应急响应。 提交成果：应急响应事件报告。	
	安全预警	了解网络安全信息，提供网络安全预警通报，提供防范与保障建议。 提交成果：安全预警报告。	1 项
	安全隐患事件通报预警情况	针对北京市政务信息安全保障中心、市网络与信息安全信息通报中心、人社部等部门推送的安全漏洞和预警，配合开展排查和整改，并形成整改报告。 提交成果：安全隐患事件排查报告。	1 项
	网络安全及正版化工作检查	配合用户开展人社部、市网信办、市经信局、市公安局、市密码管理局等单位的各项安全排查、现场检查、攻防演练等工作，以及按照市使用正版软件工作联席会议办公室的工作要求，配合正版软件检查工作。 服务频率：服务期限内根据用户需求提供服务。 提交成果：根据检查要求提供文档。	1 项
	配合信息系统等保测评和密评	配合用户和第三方测评单位开展信息系统网络安全等级保护测评工作，协助用户保障系统安全合规。 服务频率：每年至少开展一次信息系统等保测评及密评工作。 提交成果：安全加固和安全整改报告。	1 项
	系统上线前安全检查	对于新上线系统和模块开展安全检查评估，通过“远程安全扫描”、“本地安全检查”等方式对新上线系统和模块进行上线前的安全配置核查及安全扫描评估。 服务频率：新上线系统和模块上线前进行安全检查。 提交成果：系统上线安全检测报告。	1 项
安全软硬件设备维护	针对各接入单位进行安全监控、策略管理调试和设备维护保障等	银行、代办、保险公司等专线的安全接入和维护保障；区人力社保局、社保所和社区等接入访问的安全维护与保障；涉及的安全软硬件维护保障。包括对防火墙、网闸等安全设备运行状况、资源利用情况、网络连接情况等进行检查。维护安全设备登录用户名及口令，备份设备配置，并做好版本管理。对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	1 项

		订、配置策略备份、配置策略分析、配置优化等 服务频率：服务期限内全年提供服务。 提交成果：每月软硬件维护报告与记录。	

7. 人员要求

序号	岗位名称	人数	职能要求	主要职责
1	项目经理	1	具备5年以上系统集成项目管理经验。	负责整体项目计划，协调项目资源，分配及调整工作内容、把控项目整体进度。
2	安全需求分析及安全系统运维人员	4	了解用户业务范围，并对业务系统有初步了解，具备较强的沟通、理解能力，能够准确把握用户提出安全需求的核心要点。	负责对业务系统的整体安全进行需求分析。负责安全应用的性能调优、数据接口服务的安全配置。
3	数据安全分析处理人员	1	对国家关于数据安全相关的法律法规有一定理解，在数据安全方面能够针对问题提出合理建议，熟练使用主流数据挖掘及分析工具，并且具备较强的数据分析与治理能力。	负责对业务系统的重要数据进行数据安全分析和处理。
4	技术支持服务保障人员	2	了解各类安全软件、安全应用系统的功能并熟练使用，具备较强的学习能力和沟通能力，能够对用户提出的各类技术支持需求迅速理解并解决。	负责对市、区、街道和社区用户的安全应用和安全客户端等提供技术支持。要求至少1人在通州城市副中心办公区提供5（天/周）×8（小时/天）小时驻场技术服务。
5	数字证书服务人员	3	熟悉用户生成、用户校验、用户初复审状态、用户吊销等用户管理工作；熟悉证书申请、发放、更新、吊销、补办及技术支持等数字证书工作；熟悉权限资源、角色及其关系维护、权限申请、审批员审批、管理员授权等维护工作。	负责每日对用户的生成、验证等服务进行监控；每日查看需要新增、吊销的用户信息并进行新增和吊销操作，每月对用户信息进行梳理；负责对市、区、街道和社区用户的数字证书提供申请、发放、更新、吊销补办及技术支持等服务；每日对权限验证、权限同步等服务进行监控、每日对权限申请的数据进行梳理和整合，每月对权限信息进行整理分析。要

				求至少1人在通州城市副中心办公区提供5（天/周）×8（小时/天）小时驻场技术服务。
6	网络安全维护工程师	2	具备5年以上网络安全服务工作经验，熟悉网络安全设备调试和网络安全法律法规要求。	负责对安全应用进行日常的监控和日志查看工作，负责安全评估，日志分析，安全策略调整，安全设备的日常维护等工作。要求至少1人在通州城市副中心办公区提供5（天/周）×8（小时/天）小时驻场技术服务。
7	技术支持和证书权限机动人员	2	了解各类安全软件、安全应用系统的功能并熟练使用，熟悉用户、权限的基本的申请、管理流程。熟悉数字证书的使用流程及安装环境。	负责我局各办公地点安全应用和安全客户端等提供技术支持，负责对用户证书、用户权限的技术支持和维护工作。

附件三：《安全应用维护服务方案》

1. 项目运维实施方案

1.1. 身份认证服务方案

为市人力社保局提供身份认证服务，主要包括对证书的有效期验证、随机数验证、黑名单列表验证、证书链列表验证等维护服务。对用户证书与业务系统绑定进行维护服务。提供对用户认证的统计分析，并提供安全预警配置服务。

1.1.1. 日常维护

（一）每日维护

（1） 服务内容

日常维护工程师每日对身份认证系统的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1）检查证书有效期验证服务是否正常运行；

2）检查证书随机数验证服务是否正常运行；

3）检查证书黑名单列表验证服务是否正常运行；

4）检查证书链列表验证服务是否正常运行；

5）检查证书黑名单列表每日晚上更新是否成功；

6）检查身份认证票据生成、验证服务是否正常运行；

7）检查身份认证日志生成服务是否正常；

8）检查移动证书二维码生成及扫码登录接口是否正常；

9）检查社保卡二维码生成及扫码登录接口是否正常；

10）检查身份认证的数据库运行情况是否正常；

11）检查身份认证日志中是否有用户登录的异常情况；

12）检查 IIS 中间件运行是否正常、系统日志是否有异常情况；

13）检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件。

（2） 服务频率

每日对身份认证所有服务的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

（二）每周维护

（1） 服务内容

每周对身份认证服务器的运行情况进行监控和分析，使系统和接口最大程度为用户和业务系统提供安全，全面的服务，确保系统快速稳定运行，需要提供的服务如下：

1）每周检查安全系统所有应用服务器的运行情况，主要包括服务器 CPU、内存、磁盘的使用情况；

2）每周检查安全服务器中登录日志目录空间是否能正常使用；

3）每周对数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4）每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对身份认证服务器使用情况进行检查。

（3） 服务成果

定期维护需要形成相关的记录单。

（三）每月维护

（1） 服务内容

对身份认证服务的运行情况进行统计分析，通过对用户登录的认证情况进行月统计，监控每月的用户登录峰值，确保系统快速稳定运行，需要提供的服务如下：

1）每月对身份认证的用户登录进行分析，检查是否存在异常登录的情况，发现异常登录按异常流程进行处理；

2）每月对身份认证服务生成的登录日志进行处理，对登录认证数据进行整理和统计。

3）每月对数据库自动备份的日志文件进行人工备份；

（2） 服务频率

每月对身份认证登录日志进行统计分析及备份处理。

（3） 服务成果

维护服务需要形成相关的记录单。

（四）特殊时期维护

（1） 服务内容

在特殊时期对身份认证服务的运行情况进行监控和分析，为业务系统的用户登录提供安全、全面、精准的服务，确保系统快速稳定运行，需要提供的服务如下：

1）针对业务系统重要时间段，由于业务系统期间用户量多、认证数据量大，安全系统需要针对这种情况，加强身份认证系统相关接口及服务的检查频率；

2) 重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率。

（3） 服务成果

系统维护需要形成相关的巡检记录单。

1.1.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.1.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括各种认证服务接口问题、安全服务器的问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.1.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后登录系统对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作如下：

1）对用户证书与业务系统绑定进行维护服务，根据用户证书的使用需求，为用户操作业务系统的权限进行绑定或解绑服务。

2）身份认证系统可根据业务系统实际的使用情况，对具有风险的操作时间段、IP 使用地址等进行访问控制。

3）根据用户证书身份认证的数据统计分析，提供安全预警配置服务。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.1.5. 数据备份

（1） 服务内容

数据备份方式一般采取三种方式进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1） 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。程序对日志文件数据进行自动备份，保存到备份目录。

2） 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3） 介质备份

原始数据是以 mdf 方式存储的，数据管理人员接收到 mdf 数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.1.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询、现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求做到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

身份认证系统主要提供的技术服务如下：

1） 客户端技术支持

主要为局用户提供用户证书的终端等方面的技术支持，主要包括证书工具读取问题、安全终端读取问题、浏览器证书识别问题、浏览器版本及兼容等各种用户使用过程中的问题。

2） 认证服务技术支持

主要为局用户提供用户证书的登录认证方面的技术问题，主要包括证书过期、密码错误、登录失败等方面的技术问题。

（2） 服务频率

根据用户实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.2. 数据加解密及密码管理服务

统一为市人力社保局信息系统提供数据加解密服务，通过数据加密保障数据防泄露，通过数据签名保障数据完整性，为信息系统中重要数据提供加密、解密、签名、验签等措

施，确保数据应用的安全可靠。统一为市人力社保局信息系统提供密码管理服务，包括提供密码安全管理、密码配置、密钥备份和密码应用等。

1.2.1. 数据加解密服务

1.2.1.1. 日常维护

- **每日维护**

（1） 服务内容

日常维护工程师每日对数据加解密系统的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1) 检查数据加解密服务是否正常运行；
2) 检查数据签名验签服务是否正常运行；
3) 检查批量数据加解密服务是否正常运行；
4) 检查批量数据签名验签服务是否正常运行；
5) 检查数据交换接口的服务是否正常运行；
6) 检查加密机的服务接口是否正常运行；
7) 检查数据日志生成服务是否正常；
8) 检查数据加解密的数据库运行情况是否正常；
9) 检查数据加解密接口的日志，是否有数据加解密失败的情况；
10) 检查数据签名验签接口的日志，是否有签名或验签失败的情况；
11) 检查 IIS 中间件运行是否正常、系统日志是否有异常情况；
12) 检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件；
13) 每日对加密机服务器的缓存进行清理。

（2） 服务频率

每日对数据加解密所有服务的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

- **每周维护**

（1） 服务内容

对数据加解密服务的运行情况进行统计分析，使系统和接口最大程度为用户和业务系统提供安全，全面的服务，确保系统快速稳定运行，需要提供的服务如下：

1) 每周检查安全系统应用服务器及加密机的运行情况，主要包括服务器CPU、内存、磁盘的使用情况；

2) 每周检查安全服务器中加解密、签名验签日志目录空间是否能正常使用；

3) 每周对加解密数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4) 每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对数据加解密服务器使用情况进行检查。

（3） 服务成果

系统维护需要形成相关的记录单。

- **每月维护**

（1） 服务内容

对数据加解密服务的运行情况进行统计分析，通过对业务数据加解密、签名验签的数据量进行安全分析，确保安全系统快速稳定运行，需要提供的服务如下：

1) 每月对数据加解密接口调用的情况进行统计分析，根据查询统计的数据进行安全分析，如发现异常数据按异常流程进行预警和处理；

2) 每月对数据加解密接口生成的数据日志进行处理，对数据日志进行整理和统计。

3) 每月对数据库自动备份的日志文件进行人工备份；

（2） 服务频率

每月对数据加解密服务的日志进行统计分析及备份处理。

（3） 服务成果

维护服务需要形成相关的记录单。

- **特殊时期维护**

（1） 服务内容

在特殊时期对加解密服务的运行情况进行监控和分析，为业务系统的重要数据处理提供安全、全面、精准的服务，确保系统快速稳定运行，需要提供的服务如下：

1) 针对业务系统重要时间段，由于业务系统期间用户量多、重要数据解密数据大，安全系统需要针对这种情况，加强对数据加解密相关接口及服务的检查频率；

2) 根据业务系统调用数据加解密接口的实际访问量，如果发现加密机压力过大，则对加密机缓存进行清理，保证加密机接口的性能；

3) 重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率及处理频率。

（3） 服务成果

系统维护需要形成相关的巡检记录单。

1.2.1.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.2.1.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括各种数据加解密、签名验签服务接口问题，安全服务器、加密机相关的故障问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.2.1.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后登录系统对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作如下：

1）为业务系统使用的数据加解密、签名验签的密钥进行更新配置，并可对主密钥进行定期的更新。

2）可根据业务系统实际的使用情况，对业务系统服务器访问加解密服务器的IP地址进行接口访问控制。

3）可根据业务系统数据解密统计分析，制定符合业务系统的安全配置。

4）对业务系统的重要数据进行安全分析制定防护措施的配置。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.2.1.5.数据备份

（1） 服务内容

数据备份方式一般采取三种进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1） 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。

程序对日志文件数据进行自动备份，保存到备份目录。

2） 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3） 介质备份

原始数据是以mdf方式存储的，数据管理人员接到mdf数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.2.1.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询，现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求作到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

数据加解密系统主要提供的技术服务如下：

1） 业务数据技术支持

主要为业务系统解决数据加解密、签名验签接口访问相关的技术问题。

（2） 服务频率

根据用户实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.2.2. 密码管理服务

1.2.2.1. 日常维护

- **每日维护**

（1） 服务内容

日常维护工程师每日对密码管理系统的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1）检查密码管理系统登录、统计分析、系统配置等是否正常运行；

2）检查数据加解密、签名验签的密钥是否正常运行；

3）检查身份认证的随机数签名密钥是否正常运行；

4）检查数据交换使用的密钥是否正常运行；

5) 检查密钥管理系统的密钥自动备份是否正常备份；

6) 检查密钥管理系统的密钥生成、导出服务是否正常；

7) 检查密钥管理系统的数据库运行情况是否正常。

8) 检查密钥管理系统是否有系统异常日志；

9) 检查 IIS 中间件运行是否正常、系统日志是否有异常情况；

10) 检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件。

（2） 服务频率

每日对密码管理所有服务的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

➢ **每周维护**

（1） 服务内容

每周对密钥管理系统的应用服务器运行情况进行统计分析，使应用服务器最大程度为安全接口提供稳定，全面的服务，确保系统快速稳定运行，需要提供的服务如下：

1) 每周检查安全系统所有应用服务器的运行情况，主要包括服务器 CPU、内存、磁盘的使用情况；

2) 每周检查安全服务器中日志目录空间是否能正常使用；

3) 每周对密钥管理数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4) 每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对服务器使用情况进行检查。

（3） 服务成果

系统维护需要形成相关的记录单。

➢ **每月维护**

（1） 服务内容

对密钥管理系统的运行情况进行统计分析，检查密钥使用情况，确保系统快速稳定运行，需要提供的服务如下：

1) 每月对身份认证、数据加解、数据交换等使用的密钥情况进行分析，检查是否存在密钥异常的情况，发现异常按异常流程进行处理；

2) 每月对密钥管理系统生成的登录日志进行处理，对业务系统及安全系统的密钥数据

进行整理和统计。

3) 每月对数据库自动备份的日志文件进行人工备份；

（2） 服务频率

每月对密钥日志进行统计分析及备份处理。

（3） 服务成果

系统维护需要形成相关的记录单。

➢ **特殊时期维护**

（1） 服务内容

在特殊时期对密钥管理系统的运行情况进行统计分析，使系统和接口最大程度为用户和业务系统提供安全，全面的服务，确保系统特殊时期的稳定运行，需要提供的服务如下：

1) 针对业务系统重要时间段，加强对业务系统、安全系统密钥的检查频率；

2) 重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率。

（3） 服务成果

系统维护需要形成相关的巡检记录单。

1.2.2.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.2.2.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括各种密钥生成、制作、自动备份等问题、服务器系统的问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.2.2.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后登录系统对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作如下：

1) 对密钥管理系统的密钥备份路径、备份周期进行安全配置。

2) 对业务系统使用数据加解密密钥、数据交换密钥进行 IP 访问控制。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.2.2.5. 数据备份

（1） 服务内容

数据备份方式一般采取三种进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1) 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。

程序对日志文件数据进行自动备份，保存到备份目录。

2） 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3） 介质备份

原始数据是以 mdf 方式存储的，数据管理人员接到 mdf 数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.2.2.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询，现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求作到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

密钥管理系统主要提供的技术服务如下：

1） 系统技术支持

主要为局业务系统提供安全密钥的生成、使用、备份等相关问题的技术支持。

（2） 服务频率

根据用户实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.2.3. 安全验证服务

1.2.3.1. 日常维护

- **每日维护**

（1） 服务内容

日常维护工程师每日对安全验证服务的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1) 检查加解密、签名验签接口的验证服务是否正常运行；

2) 检查数据交换接口的验证服务是否正常运行；

3) 检查身份认证的验证服务是否正常运行；

4) 检查安全验证的数据统计、安全配置是否正常运行；

5) 检查 IIS 中间件运行是否正常、系统日志是否有异常情况；

6) 检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件。

（2） 服务频率

每日对安全验证所有服务的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

- **每周维护**

（1） 服务内容

每周对安全验证服务的应用服务器运行情况进行统计分析，使应用服务器最大程度为验证服务提供稳定，全面的服务，确保系统快速稳定运行，需要提供的服务如下：

1) 每周检查安全系统所有应用服务器的运行情况，主要包括服务器 CPU、内存、磁盘的使用情况；

2) 每周检查安全服务器中日志目录空间是否能正常使用；

3) 每周对安全验证数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4) 每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对服务器使用情况进行检查。

（3） 服务成果

系统维护需要形成相关的记录单。

➢ 每月维护

（1） 服务内容

对安全验证服务的运行情况进行统计分析，检查安全规则使用情况，确保系统快速稳定运行，需要提供的服务如下：

1) 每月对身份认证、数据加解、数据交换等使用的安全规则情况进行分析，检查是否存在异常访问的情况，发现异常按异常流程进行处理；
2) 每月对安全验证服务生成的访问控制日志进行处理，对业务系统及安全系统的数据处理规则进行整理和统计。
3) 每月对数据库自动备份的日志文件进行人工备份；

（2） 服务频率

每月对验证日志进行统计分析及备份处理。

（3） 服务成果

系统维护需要形成相关的记录单。

➢ 特殊时期维护

（1） 服务内容

在特殊时期对安全验证服务的运行情况进行统计分析，使系统和接口最大程度为用户和业务系统提供安全，全面的服务，确保系统特殊时期的稳定运行，需要提供的服务如下：

1) 针对业务系统重要时间段，加强对业务系统、安全系统安全验证服务的检查频率；
2) 重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率。

（3） 服务成果

系统维护需要形成相关的巡检记录单。

1.2.3.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.2.3.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括各种安全验证规则生成、验证服务等问题、服务器系统的问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.2.3.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后安全验证服务对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作有：

1) 对安全验证服务业务系统访问权限的控制、访问规则等进行安全配置。

2) 对业务系统使用安全验证服务进行 IP 访问控制。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.2.3.5. 数据备份

（1） 服务内容

数据备份方式一般采取三种进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1） 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。

程序对日志文件数据进行自动备份，保存到备份目录。

2） 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3）介质备份

原始数据是以 mdf 方式存储的，数据管理人员接到 mdf 数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.2.3.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询，现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求作到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

安全验证服务主要提供的技术服务如下：

1） 系统技术支持

主要为局业务系统提供安全验证接口访问、安全规则配置等相关问题的技术支持。

（2） 服务频率

根据用户实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.3. 安全审计及操作日志分析服务

统一为市人力社保局信息系统提供安全审计服务，包括提供用户操作业务的审计行为、用户操作信息系统的日志采集、用户操作行为追溯以及安全配置等服务。

1.3.1.1. 日常维护

（一）每日维护

（1） 服务内容

日常维护工程师每日对安全审计系统的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1) 检查安全审计系统图表统计分析是否正常运行；

2) 检查安全审计用户操作行为追溯服务是否正常运行；

3) 检查系统管理员分配权限的日志是否正常运行；

4) 检查上传下载保密文件的日志记录是否正常运行；

5) 检查用户上机操作行为日志是否正常运行；

6) 检查登录行为日志采集服务是否正常；

7) 检查操作行为日志采集服务是否正常；

8) 检查业务敏感数据操作日志采集服务是否正常；

9) 检查审计数据清洗、处理服务是否正常；

10) 检查 IIS 中间件运行是否正常、系统日志是否有异常情况；

11) 检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件。

（2） 服务频率

每日对安全审计及操作日志分析的所有服务的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

（二）每周维护

（1） 服务内容

对数据安全审计系统及操作日志的分析服务的服务器运行情况进行监控和分析，保障服务器的稳定运行，使系统和接口最大程度为用户和业务系统提供稳定的服务，确保系统快速稳定运行，需要提供的服务如下：

1）每周检查安全系统应用服务器及加密机的运行情况，主要包括服务器 CPU、内存、磁盘的使用情况；

2）每周检查安全服务器中安全审计及操作日志的目录空间是否能正常使用；

3）每周对数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4）每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对服务器使用情况进行检查。

（3） 服务成果

系统维护需要形成相关的记录单。

（三）每月维护

（1） 服务内容

对数据安全审计数据处理服务及用户操作行为进行统计分析，通过对用户行为进行全方位的安全分析，确保安全系统稳定运行，需要提供的服务如下：

1）每月对用户登录日志、操作日志、客户端上机日志、敏感数据日志进行统计分析，分析用户行为是否存在异常行为，如发现异常按异常流程进行预警和处理。

2）每月对数据清洗、数据处理服务的日志进行处理，对日志进行整理和统计。

3）每月对数据库自动备份的日志文件进行人工备份。

（2） 服务频率

每月进行统计分析及备份处理。

（3） 服务成果

维护服务需要形成相关的记录单。

（四）特殊时期维护

（1） 服务内容

在特殊时期对安全审计数据处理及安全分析服务的运行情况进行监控，为业务系统安全提供全面的保障服务，确保系统快速稳定运行，需要提供的服务如下：

1）针对业务系统重要时间段，由于业务系统期间用户量多、用户操作行为数据量大，安全系统需要针对这种情况，加强对数据统计分析、用户行为追溯服务的检查频率；

2）重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率及处理频率。

（3） 服务成果

系统维护需要形成相关的巡检记录单。

1.3.1.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.3.1.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括各种用户登录异常行为、操作异常行为、数据异常行为的问题，安全审计及操作日志服务器的故障问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.3.1.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后登录系统对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作如下：

1) 可根据用户登录、操作业务系统模块的行为分析，制定符合业务系统的安全配置；

2) 可根据用户登录业务系统敏感的行为分析，制定符合业务系统的安全规则配置；

3) 可根据安全审计及操作行为的数据规则，配置各种安全指标的预警值。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.3.1.5. 数据备份

（1） 服务内容

数据备份方式一般采取三种进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1) 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。

程序对日志文件数据进行自动备份，保存到备份目录。

2) 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3) 介质备份

原始数据是以 mdf 方式存储的，数据管理人员接到 mdf 数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.3.1.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询，现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求作到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

安全审计系统主要提供的技术服务如下：

1） 业务数据技术支持

主要为安全管理员解决操作行为数据统计、安全行为分析等技术问题。

（2） 服务频率

根据用户实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.4. 数字证书服务

统一为市人力社保局信息系统提供用户管理、数字证书管理和权限管理，包括实体证书和移动证书等，进行证书申请、发放、更新、吊销、补办及技术支持等服务。

1.4.1. 证书管理服务

1.4.1.1. 日常维护

- **每日维护**

（1） 服务内容

日常维护工程师每日对数字证书系统的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1）检查数据数字证书申请服务是否正常运行；

2）检查数据数字证书发放服务是否正常运行；

3）检查数字证书吊销服务是否正常运行；

4）检查数字证书补办服务是否正常运行；

5）检查与用户接口数据交换服务是否正常运行；

6）检查系统日志生成服务是否正常；

7）检查 IIS 中间件运行是否正常、系统日志是否有异常情况；

8）检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件。

（2） 服务频率

每日对系统所有服务的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

➢ 每周维护

（1） 服务内容

对数据数字证书服务的运行情况进行统计分析，使系统和接口最大程度为用户和业务系统提供安全，全面的服务，确保系统快速稳定运行，需要提供的服务如下：

1）每周检查安全系统应用服务器的运行情况，主要包括服务器 CPU、内存、磁盘的使用情况；

2）每周检查安全服务器中服务日志目录空间是否能正常使用；

3）每周对数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4）每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对证书服务器使用情况进行检查。

（3） 服务成果

系统维护需要形成相关的记录单。

➢ 每月维护

（1） 服务内容

对数字证书服务的运行情况进行统计分析，通过对用户对证书操作的数据量进行分析，确保证书系统快速稳定运行，需要提供的服务如下：

（2） 每月对数字证书服务申请、使用情况进行统计分析，根据查询统计的数据进行安全分析，如发现异常数据按异常流程进行预警和处理；

（3） 每月对数字证书服务生成的数据日志进行处理，对数据日志进行整理和统计。

（4） 每月对数据库自动备份的日志文件进行人工备份；

（5） 服务频率

每月对证书服务日志进行统计分析及备份处理。

（6） 服务成果

维护服务需要形成相关的记录单。

- **特殊时期维护**

（1） 服务内容

在特殊时期对数字证书服务的运行情况进行监控和分析，为业务系统重要时期提供安全、全面的数字证书发放服务，确保系统快速稳定运行，需要提供的服务如下：

1）针对业务系统重要时间段，由于业务系统期间用户申请量多，证书制作量大，针对这种情况，安全增加数字证书制作人员、证书技术支持人员，保障业务系统稳定运行。

2）重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率及人员数量。

（3） 服务成果

证书服务需要形成相关的申请记录单。

1.4.1.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.4.1.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括各种数字证书服务问题，证书客户端的技术问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.4.1.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后登录系统对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作如下：

1）对用户申请数字证书的相关流程，可根据实际情况进行审核流程的修改和配置，满足用户使用需求。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.4.1.5. 数据备份

（1） 服务内容

数据备份方式一般采取三种进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1） 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。

程序对日志文件数据进行自动备份，保存到备份目录。

2） 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3） 介质备份

原始数据是以 mdf 方式存储的，数据管理人员接到 mdf 数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.4.1.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询，现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求作到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

数字证书服务主要提供的技术服务如下：

1） 证书使用技术支持

主要为用户提供数字证书的使用过程中的问题，主要包括数字证书工具的读取、密码修改等。

2） 证书申请流程技术支持

主要为用户提供数字证书申请、审批流程相关的问题解答。

（2） 服务频率

根据用户实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.4.2. 用户管理服务

1.4.2.1. 日常维护

- **每日维护**

（1） 服务内容

日常维护工程师每日对用户管理系统的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1）检查用户生成服务是否正常运行；

2）检查用户校验服务是否正常运行；

3）检查用户初复审服务是否正常运行；

4）检查用户吊销服务是否正常运行；

5）检查移动证书解析用户信息是否正常运行；

6）检查实体证书解析用户信息是否正常运行；

7）检查用户管理系统日志生成服务是否正常；

8）检查用户管理系统的数据库运行情况是否正常。

9）查看需要新增、吊销的用户信息并进行新增和吊销操作；

10）检查 IIS 中间件运行是否正常、系统日志是否有异常情况；

11）检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件。

（2） 服务频率

每日对所有服务及管理系统的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

- **每周维护**

（1） 服务内容

对用户管理系统的服务器使用情况进行监控和分析，使系统和接口最大程度为用户和业务系统提供安全，全面的服务，确保系统快速稳定运行，需要提供的服务如下：

1）每周检查安全系统应用服务器及加密机的运行情况，主要包括服务器 CPU、内存、磁盘的使用情况；

2）每周检查安全服务器中用户管理系统日志、用户解析接口日志目录空间是否能正常使用；

3）每周对用户管理数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4）每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对用户管理服务器使用情况进行检查。

（3） 服务成果

系统维护需要形成相关的记录单。

- **每月维护**

（1） 服务内容

对用户管理系统及服务接口运行情况进行统计分析，确保安全系统快速稳定运行，需要提供的服务如下：

1）每月对用户管理系统中用户数据申请、吊销情况进行统计分析，根据统计数据进行安全分析，如发现异常用户按异常流程进行预警和处理；

2）每月对解析用户信息相关的接口及服务生成的数据日志进行处理，对数据日志进行整理和统计。

3）每月对数据库自动备份的日志文件进行人工备份；

（2） 服务频率

每月对用户管理系统进行统计分析及备份处理。

（3） 服务成果

维护服务需要形成相关的记录单。

- **特殊时期维护**

（1） 服务内容

在特殊时期对用户管理系统的运行情况进行监控和分析，为业务系统的重要数据处理提供安全、全面、精准的服务，确保系统快速稳定运行，需要提供的服务如下：

1）针对业务系统重要时间段，由于业务系统期间用户使用量多，安全系统需要针对这

种情况，加强对用户解析、用户验证相关接口及服务的检查频率；

2）针对业务系统期间证书申请量多，生成用户信息量大，针对这种情况，安全增加操作用户管理系统人员，保障业务系统稳定运行；

3）重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率及处理频率。

（3） 服务成果

系统维护需要形成相关的巡检记录单。

1.4.2.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.4.2.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括各种用户管理系统及用户解析等问题，用户管理服务器的故障问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.4.2.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后登录系统对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作如下：

1) 对用户生成、审核的相关流程，可根据实际情况进行审核流程的修改和配置，满足用户管理需求。

2) 可根据业务系统实际的使用情况，对业务系统服务器访问用户解析信息等接口 IP 地址进行接口访问控制。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.4.2.5. 数据备份

（1） 服务内容

数据备份方式一般采取三种进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1） 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。

程序对日志文件数据进行自动备份，保存到备份目录。

2） 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3） 介质备份

原始数据是以 mdf 方式存储的，数据管理人员接到 mdf 数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.4.2.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询，现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求作到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

用户管理系统主要提供的技术服务如下：

1） 业务数据技术支持

主要为业务系统解决用户解析接口、用户信息验证接口访问相关的技术问题。

（2） 服务频率

根据用户实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.4.3. 权限管理服务

1.4.3.1. 日常维护

- **每日维护**

（1） 服务内容

日常维护工程师每日对权限管理系统及接口的运行情况进行监测，发现问题立即报告故障排查人员进行故障排查，具体工作如下：

1）检查用户权限申请服务是否正常运行；

2）检查审批员审批服务是否正常运行；

3）检查管理员授权服务是否正常运行；

4）对业务系统的资源、角色及其关系进行维护；

5）检查为业务系统提供的权限信息同步接口是否正常运行；

6）检查权限管理系统日志生成服务是否正常；

7）检查权限管理系统的数据库运行情况是否正常；

8）检查数据权限接口服务的异常日志，查看异常记录的生成原因；

9）检查 IIS 中间件运行是否正常、系统日志是否有异常情况；

10）检查事件查看器中的 windows 日志，检查应用程序、安全、系统项中是否存在异常的事件。

（2） 服务频率

每日对权限管理系统及所有服务的运行状态进行巡检。

（3） 服务成果

日常维护需要形成相关的巡检记录单。

➢ **每周维护**

（1） 服务内容

对权限管理系统服务器的运行情况进行监控和分析，使系统和接口最大程度为用户和业务系统提供安全，全面的服务，确保系统快速稳定运行，需要提供的服务如下：

1）每周检查系统应用服务器的运行情况，主要包括服务器 CPU、内存、磁盘的使用情况；

2）每周检查服务器中权限接口日志目录空间是否能正常使用；

3）每周对权限管理数据库的运行情况进行检查、并对数据库的文件进行收缩等；

4）每周对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

每周对服务器使用情况进行检查。

（3） 服务成果

系统维护需要形成相关的记录单。

➢ **每月维护**

（1） 服务内容

对权限管理系统用户权限申请、审核及验证的使用情况进行统计分析，确保安全系统快速稳定运行，需要提供的服务如下：

1）每月对用户申请权限角色、资源的情况进行数据统计，根据查询统计的数据进行安全分析，如发现异常数据按异常流程进行预警和处理；

2）每月对业务系统调用权限验证接口进行统计，对并统计数据进行安全分析。

3）每月对所有接口及服务生成的数据日志进行处理，对数据日志进行整理和统计。

4）每月对数据库自动备份的日志文件进行人工备份；

（2） 服务频率

每月对数据进行统计分析及备份处理。

（3） 服务成果

维护服务需要形成相关的记录单。

- **特殊时期维护**

（1） 服务内容

在特殊时期对权限系统验证服务的运行情况进行监控和分析，为业务系统的权限验证提供安全、全面、精准的服务，确保系统快速稳定运行，需要提供的服务如下：

1）针对业务系统重要时间段，由于业务系统访问量增大，权限验证访问也随之增大，安全系统需要针对这种情况，加强对权限相关接口及服务的检查频率；

2）重大节假日前后，对系统的运行环境进行巡检（如：服务器、软件配置、应用容器、系统日志等），如发现问题及时解决并上报。

（2） 服务频率

根据实际情况，加强检查频率及处理频率。

（3） 服务成果

系统维护需要形成相关的巡检记录单。

1.4.3.2. 需求分析

（1） 服务内容

针对用户和业务系统运行过程中新的需求，或者各安全系统本身的安全相关需求，需对安全系统或接口进行升级更新等情况发生时。由需求工程师向用户及业务系统开发公司进行需求调研，生成功能需求文档，结合用户需求对安全系统、应用系统可行性进行分析评估，并生成系统需求可行性分析报告提交用户，并签字确认。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

需求分析需要形成相关的记录单。

1.4.3.3. 故障处理

（1） 服务内容

对系统的突发性故障进行维护，包括权限管理系统、权限验证接口问题，权限服务器的故障问题，各种日志数据存储问题等进行故障处理。对系统突发性故障立即发现，立刻上报相关领导，按系统的应急方案进行处理，并做好事后记录工作。

（2） 服务频率

根据系统运行的实际运行情况提供运维服务。

（3） 服务成果

故障处理需要形成相关的记录单。

1.4.3.4. 系统配置

（1） 服务内容

遵循项目总体要求，结合用户对系统功能、数据、安全等方面调整需求进行可行性分析并汇报用户，用户确认后对系统进行功能调整、参数设置等操作，调整完成后通知相关使用部门对调整内容进行确认，并签署调整数据单。

主要的运维工作如下：

1) 可根据业务系统实际的使用情况，对业务系统服务器访问权限服务器的 IP 地址进行接口访问控制。

2) 可根据业务系统权限验证的统计分析，制定符合业务系统的安全配置。

（2） 服务频率

根据业务系统实际情况提供运维服务。

（3） 服务成果

系统调整需要形成相关的记录单。

1.4.3.5. 数据备份

（1） 服务内容

数据备份方式一般采取三种进行备份，备份数据有日志数据、配置数据库、服务器的发布站点等。

1） 本地备份

数据在进入展现库之前，首先会在清洗库进行流程的清洗和数据的过滤。数据管理人员会在每次清洗完数据后，手动对清洗库进行本地备份。

程序对日志文件数据进行自动备份，保存到备份目录。

2） 异地备份

展现库的备份方式采取每天备份的形式，于每天的零点进行自动备份，但由于数据库数据量过大，现在正式数据库的服务器已经没有充足的存储空间，现采取异地备份的方式，将展现库于每周六备份到另一台服务器上。缓解了现有服务器的压力。

定期对日志文件数据人工进行异地备份，防止服务器上的日志数据丢失。

3） 介质备份

原始数据是以 mdf 方式存储的，数据管理人员接到 mdf 数据后，会将数据转化为数据库的形式进行存储，而这部分数据现采取移动硬盘备份的方式。

（2） 服务频率

每月或数据库实际使用情况提供运维服务。

（3） 服务成果

数据备份需要形成相关的记录单。

1.4.3.6. 技术支持

（1） 服务内容

日常维护中，为用户解决问题的方式有很多种，包括电话咨询，现场技术支持等。

配备专人接听用户电话，了解用户疑难。维护人员根据不同用户的各种情况进行分析并一一解答，电话无法解答前往现场进行现场排查解决。提供工作时间 5（天/周）×9（小时/天）小时驻场技术服务，以及 7 X 24 小时响应服务，现场服务的场地由用户指定，这样时刻保证随时响应；所有非工作时间将安排专职响应工程师。对用户提出的技术支持要求作到接到用户的报修请求后的 1 小时内安排专人与用户电话具体联系，时间最长 2 小时（郊区 4 小时）内上门检查、修复故障。

主要为权限管理系统及业务系统访问的接口提供技术服务：

1） 权限管理系统技术支持

主要为用户使用权限管理系统进行权限分配时的相关操作问题。

2） 接口服务技术支持

主要为业务系统提供资源、角色、模块的访问控制提供技术支持。

（2） 服务频率

根据用户及系统实际情况随时提供服务。

（3） 服务成果

技术支持需要形成相关的记录单。

1.5. 应急演练服务方案

1.5.1. 应急演练的需求

近年来安全事件频繁发生，但应对突发事件的能力参差不齐，导致对单位蒙受了巨大的经济损失和社会影响。《网络安全法》中明确规定：“关键信息基础设施的运营者应当制定网络安全事件应急预案，并定期进行演练”，“国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。”应急演练提升到国家安全高度。

1.5.2. 应急预案解决方案

针对应急预案中全部或大部分应急响应功能，搭建模拟测试环境，演练过程采取交互方式进行，要求尽量真实，以测试应急响应的功能。例如，指挥和控制功能的演练，检测、评价多个部门在紧急状态下实现集权式的运行和响应处置能力等。

1.6. 网络安全服务及安全软硬件设备维护

服务内容包括日常网络安全服务保障；银行、代办、保险公司等专线的安全接入和维护保障；区人力社保局、社保所和社区等接入访问的安全维护与保障；各专线和网络接入的安全软硬件设备维护等。

1.6.1. 网络流量监控

(1) 服务人员

技术支持服务保障人员 2 人，至少 1 人在通州城市副中心办公地驻场。

(2) 运维范围

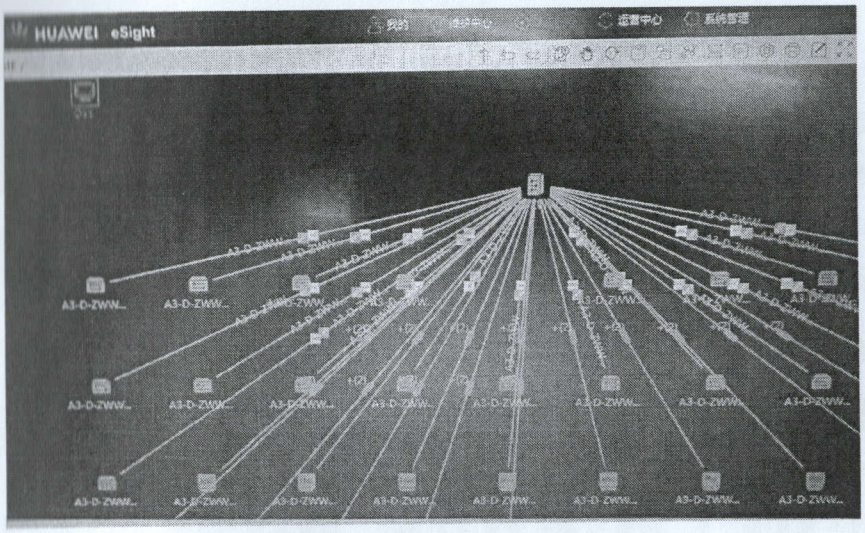
市人社局办公楼互联网、政务外网网络的运行状态和网络流量进行分析；

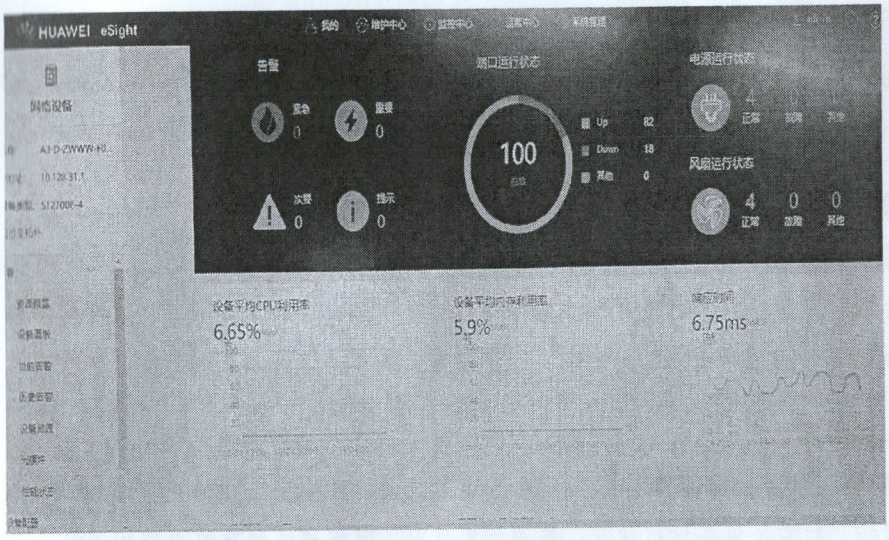
(3) 服务频次

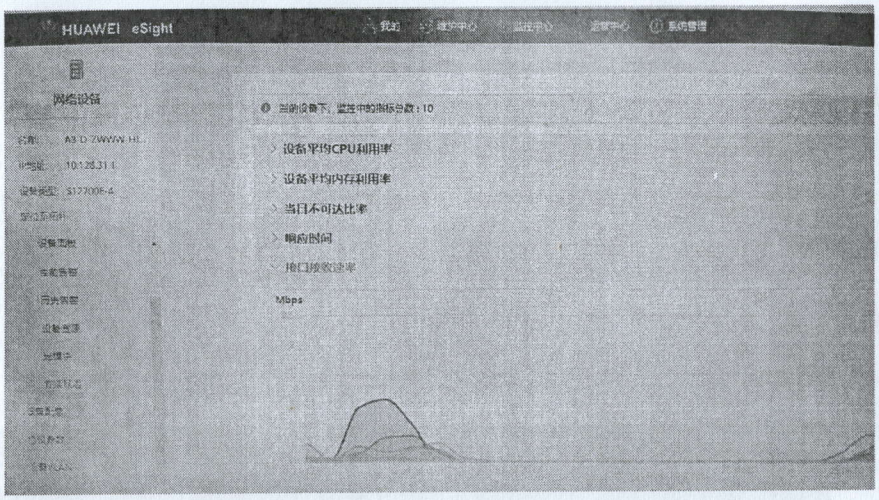
服务期限内每日进行网络流量监控，提供工作时间5（天/周）×8（小时/天）小时技术服务。特殊时期和重要节假日技术保障（在每年的元旦、春节、五一、十一等国家法定节假日和重大活动期间），按照甲方的要求完成特殊的应急服务工作。

(4) 监控工具

Hawei eSight







(5) 运维内容

通过安排具有丰富经验并且经过专业系统化培训的安全工程师开展5×9小时现场安全值守工作，监控办公楼互联网、政务外网等网络的运行状态和网络流量，及时评估网络运行状况，对异常网络流量进行分析。

(6) 提交材料

每月提交《网络流量监控与分析报告》。

1.6.2. 网络安全监控

(1) 服务人员

网络安全维护工程师2人，至少1人在通州城市副中心办公地驻场。

(2) 运维范围

市人社局办公楼安全防护设备网络攻击防御、应用攻击防御、入侵检测；

(3) 服务频次

服务期限内每日进行网络安全监控，技术人员提供工作时间5（天/周）×8（小时/天）小时技术服务。特殊时期和重要节假日技术保障（在每年的元旦、春节、五一、十一等国家法定节假日和重大活动期间），按照甲方的要求完成特殊的应急服务工作。

(4) 运维内容

通过安排具有丰富经验并且经过专业系统化培训的安全工程师开展5×9小时现场安全值守工作，对安全设备运行状况、资源利用情况、网络连接情况等进行检查并提交巡检报告。定期维护安全设备登录用户名及口令，定期备份设备配置，并做好版本管理。如发现问题及时与用户进行沟通，并提出解决方案，得到用户确认后对出现的问题进行解决，做到及时、准确保证无差错。同时将实时跟踪、搜集相关安全设备的漏洞及补丁信息，第一

时间获得公开的设备漏洞及补丁资料，及时联系并协调厂家进行版本的升级，保证安全措施的有效性。同时，实时升级特征库、规则库等动态库，确保动态库是最新的版本，提高信息系统安全防护效果。

(5) 提交材料

每月提交《网络安全分析报告》。

1.6.3. 配置核查

(1) 服务人员

网络安全维护工程师 2 人，至少 1 人在通州城市副中心办公地驻场。

(2) 运维范围

对办公楼安全设备的安全策略进行调整。

(3) 服务频次

服务期限内每季度提供一次配置核查服务。

(4) 运维内容

根据当前的网络安全形势，调整、完善安全设备的配置，包括删除无用策略、设置相应的访问控制、关闭易受攻击的服务端口等，并做好安全设备的配置管理工作，每月备份一次设备的配置文件，当设备发生故障，影响信息系统正常运行时，及时恢复设备的配置文件。当设备的配置文件发生变化时，做好备份工作。在因业务变化导致策略变更时，网络安全工程师对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、配置检查优化等，并形成维护记录提交用户。

(5) 提交材料

每季度提交《配置核查报告》。

1.6.4. 日志分析

(1) 服务人员

网络安全维护工程师 2 人，至少 1 人在通州城市副中心办公地驻场。

(2) 运维范围

对办公楼安全防护设备产生的日志进行分析。

(3) 服务频次

服务期限内每月度提供一次日志分析。

(4) 运维内容

办公楼安全防护设备会产生大量的网络访问日志、设备运行记录等信息，这些信息中可能隐含着潜在的网络攻击行为或已经发生但未发现的攻击行为、设备故障等。为此，网络安全维护工程师将利用工具并结合资产信息等实际情况，每月对设备的日志进行分析，找出有价值的网络攻击、运行故障等信息，从而确保在网络出现异常时能够做到提前预警，安全事件发生时能够及时有效处理。

(5) 提交材料

每月提交《日志分析报告》。

1.6.5. 应急响应

(1) 运维范围

针对日常和重要时期发生的应急事件按照应急预案进行应急响应。保证事件的损失降到最小，清除安全事件产生的影响，并开展相应的事后分析。

(2) 服务频次

日常和重要时期发生的应急事件后第一时间进行应急响应。

(3) 提交材料

提交《应急响应事件报告》。

1.6.6. 安全预警

(1) 工作内容

根据目前的信息安全形势，通过收集和整理最新安全漏洞、安全事件、安全资讯等信息，定期向用户发送安全预警通告，遇紧急高危漏洞或重大信息安全事件即时通告。

通告内容包含但不限于以下内容：

- 系统漏洞信息：定期将各操作系统、应用系统等最新安全漏洞编制成册，包括漏洞威胁、影响平台及修补方法等；
- 病毒信息：将一段时期内，将最具威胁性的病毒信息编制成册，包括病毒危害、感染原理及防护措施等；
- 安全预警：一旦出现将可能造成大规模网络攻击事件的安全漏洞或病毒木马，及时通知用户进行安全预警，积极进行补丁修复和安全防护工作；
- 信息安全事件：定期将相关信息安全事件编制成册，避免信息系统遭遇同样安全攻

击，造成严重损失。

(2) 提交材料

提交《安全预警报告》。

1.6.7. 安全隐患事件通报预警情况

(1) 工作内容

针对北京市政务信息安全保障中心、市网络与信息安全信息通报中心、人社部等部门推送的安全漏洞和预警，配合开展排查和整改，并形成整改报告。

(2) 提交材料

提交《安全隐患事件排查报告》。

1.6.8. 网络安全及正版化工作检查

(1) 工作内容

配合用户开展人社部、市网信办、市经信局、市公安局、市密码管理局等单位的各项安全排查、现场检查、攻防演练等工作，以及按照市使用正版软件工作联席会议办公室的工作要求，配合正版软件检查工作。

(2) 提交成果

根据各项检查要求提供相应文档

1.6.9. 配合信息系统等保测评和密评

(1) 工作内容

1) 协助定级、备案

依据等级保护管理办法和定级指南，按照“用户初步定级、专家评审、主管部门审批、公安机关审核”的定级步骤，协助用户通过确定定级对象、系统初步定级、填写定级备案材料、提交定级备案材料完成被测评系统的定级工作，取得定级备案证明。

2) 等保测评

依据《信息安全技术 网络安全等级保护基本要求》及规范，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理层面配合测评机构进行安全测评。

依据初测结果及测评中《安全漏洞扫描报告》、《渗透测试报告》，做好整改建议评估及技术规避风险措施，形成《安全加固和安全整改报告》，最终确保信息系统通过等级保护测评工作。

(2) 提交成果

《安全加固和安全整改报告》

1.6.10. 系统上线前安全检查

(1) 工作内容

新上线系统及模块在上线前通过“远程安全扫描”、“本地安全检查”的方式进行安全检查的评估，主要手段是渗透测试及安全配置核查。

渗透性测试是一种整体防御层面的评测手段，根据已掌握的安全漏洞，模拟黑客攻击方法，对信息系统进行非破坏性的攻击性测试，用来发现信息系统防御体系漏洞的一种常用方法。渗透性测试的目的在于充分挖掘和暴露信息系统的弱点，从而了解信息系统所面临的威胁。渗透测试的目的在于发现分析并验证信息系统存在的主机安全漏洞、敏感信息泄露、SQL 注入漏洞、权限漏洞、跨站脚本漏洞及弱口令等安全隐患，评估系统抗攻击能力，提出安全加固建议。通过为应用系统相关的主机、数据库、中间件等常见应用的安全策略配置进行科学、全面、认真的检查，进一步完善配置管理体系、满足合规需求、降低安全风险，提供强有力的支撑和依据。

(2) 提交成果

《信息系统上线安全检测申请表》

《安全加固和安全整改报告》

1.6.11. 安全软硬件设备维护

(1) 工作内容

银行、代办、保险公司等专线的安全接入和维护保障；区人力社保局、社保所和社区等接入访问的安全维护与保障；涉及的安全软硬件维护保障。包括对防火墙、网闸等安全设备运行状况、资源利用情况、网络连接情况等进行检查。维护安全设备登录用户名及口令，备份设备配置，并做好版本管理。对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、配置优化等。

(2) 维护内容

（1） 日常运行值守

通过安排具有丰富经验并且经过专业系统化培训的网络工程师开展5×9小时现场值守工作，对银行、代办、保险公司等专线所使用的相关安全软硬件设备运行状况、资源利用情况、网络连接情况等进行监控。如发现问题及时与用户进行沟通，并提出解决方案，得到用户确认后对出现的问题进行解决，做到及时、准确保证无差错。同时将实时跟踪、搜集相关网络设备的漏洞及补丁信息，第一时间获得公开的设备漏洞及补丁资料，及时联系并协调厂家进行版本的升级，保证安全措施的有效性。

（2） 设备巡检

驻场工程师定期对纳入运维的安全设备进行设备检测、定期巡检的目的在于及时发现和预防可能出现的硬件问题，从而在最大程度上为设备的连续稳定运行提供保证。

（3） 故障处理

当驻场工程师发现网络设备出现技术故障，如CPU使用率过高、通信异常、配置文件错误、设备宕机以及电源故障等问题，将立即进行故障原因定位和故障排除工作。

（4） 配置管理

根据网络安全设备运行情况，完成防火墙、网闸等安全设备的配置管理工作，每月备份一次设备的配置文件，当设备发生故障，影响信息系统正常运行时，及时恢复设备的配置文件。当设备的配置文件发生变化时，做好备份工作，同时做好安全设备登录用户名及口令的定期更换工作。对于安全策略管理工作，则做好定制安全配置策略，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、配置优化等。

附件四：《安全保密协议》

安 全 保 密 协 议

甲　方：北京市人力资源和社会保障局

乙　方：北京国信博飞科技发展有限公司

一、目的

北京市人力资源和社会保障局与北京国信博飞科技发展有限公司就“安全应用维护服务”事宜达成一致，并签订了委托服务合同。为确保本项目的安全保密，经双方协商，特制定本协议。

二、保密范围（包括但不限于以下内容）

1. 相关工作合同、方案、系统数据，以及有关会议文件、会议纪要和领导批示。

2. 相关工作人员之间往来的传真、信函、电子邮件等。

3. 相关工作实施过程中涉及的信息和资料以及可能产生的新的信息和资料。

4. 相关工作实施过程中各方拥有的知识产权信息，已经公开的知识产权信息除外。

5. 经甲乙双方在该工作实施过程中确认的需要保密的其他信息。

6. 保密义务在双方的服务合同结束后仍然有效。

三、乙方责任

1. 乙方为保密资料接受方，负有保密义务，承担保密责任。

2. 乙方未经甲方书面同意不得向第三方（包括新闻界人士）公开和披露任何保密资料或以其他方式使用保密资料。

3. 乙方须把保密资料的接触范围严格限制在因本协议规定目的而需接触保密资料的负责任的雇员的范围内。

4. 除经过甲方书面同意而必要进行披露外，乙方不得将含有甲方或其雇员披露的保密资料复印或复制或者有意无意地提供给他人。

5. 如果甲乙双方合作不再继续进行，经甲方在任何时候提出书面要求，乙方应当、并应促使其代表在五（5）个工作日内销毁或向甲方返还其占有的或控制的全部保密资料以及包含或体现了保密资料的全部文件和其它材料并连同全部副本。

6. 乙方将以并应促使其雇员以不低于其对自己拥有的类似资料的照料程度来对待甲方向其披露的保密资料，但在任何情况下，对保密资料的照料都不能低于合理程度。

7. 乙方违反保密义务，参照主合同第十条承担违约责任。

四、双方共同遵守的条款

1. 双方确认，任何一方接触并知悉本协议保密信息的人员对保密信息均负有保密义务，任何一方人员违反保密协议，将由该方承担泄密责任。

2. 双方确认，任何一方不能利用获悉的对方保密信息为自己或其他方开发信息、技术和产品。

五、其他

1. 本协议履行期间，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协议的组成部分，签字盖章后与本协议具有同等法律效力。

2. 本协议，自甲乙双方法定代表人或授权代表人签字并盖章之日起生效。

甲方：北京市人力资源和社会保障局

法定代表人或授权代表人：

签约日期：2022年12月13日

乙方：北京国信博飞科技发展有限公司

法定代表人或授权代表人：

签约日期：2022年12月13日