运维服务外包合同

项目名称：北京市智慧交通发展中心网络系统与网络安全运维服务政府采购项目

甲方：北京市智慧交通发展中心（北京市机动车调控管理事务中心）

乙方：北京云椤网安信息技术有限公司

合同编号：

签约地点：北京市通州区

签约日期：2015.8.12

甲方：北京市智慧交通发展中心（北京市机动车调控管理事务中心）

法定代表人：王炯

住所：北京市通州区通济路 8 号北投大厦

联系人：李伟

联系方式：010-80818335

乙方：北京云楒网安信息技术有限公司

法定代表人：马翔宇

住所：北京市通州区西集镇企业发展服务中心 4103 号

联系人：马翔宇

联系方式：010-51255233

甲、乙双方根据《中华人民共和国民法典》和北京市相关法律法规的规定，本着诚实守信、合作互利的原则，经过友好协商，就乙方提供“北京市智慧交通发展中心网络系统与网络安全运维服务”事宜签订本合同。

第一章 合同说明条款

一、 甲、乙双方之间任何与本合同有关的信函、电子邮件、电话，均使用并且只能使用下列双方确认的地址、传真号码、电话号码、电子邮件地址名。

	甲方	乙方
法定代表人	王炯	马翔宇
联系人	李伟	马翔宇
地址	北京市通州区通济路 8 号北投大厦	北京市通州区西集镇企业发展服务中心 4103 号
邮编	101117	101108
电话	010-80818335	010-51255233
传真	010-80818388	010-51255233
电子邮件	liwei@jtw.beijing.gov.cn	maxiangyu@cloudyunsi.com

二、甲、乙双方之间有关合同的财务往来及结算，应通过下列甲方与乙方共同确认的银行及账号进行。本合同存续期间，乙方若遇结算银行及账号变化，应

在变化之日起3日内书面告知甲方。若因乙方未及时提供变更后的银行账号导致甲方付款延迟的，甲方不承担任何违约责任。

乙方账户信息：

账户名称	北京云椤网安信息技术有限公司
开户行	中国工商银行股份有限公司北京菜市口支行
账号	0200001809200472332

三、本合同的有效组成部分包括：本合同、合同附件和补充协议（如有）。

第二章 服务内容

一、服务内容

乙方为甲方提供“北京市智慧交通发展中心网络系统与网络安全运维服务政府采购”项目运行维护服务，保证政府数据安全和信息交换安全；服务内容详细描述见附件1。

乙方提供本项目服务过程中，因硬件发生质量问题需要更换时，新的硬件产品由乙方免费提供，不得再向甲方另行收取硬件费用，且乙方对更换后的硬件产品的质量承担保证责任。

二、服务承诺

乙方在本合同约定期限内选派的专业技术运维人员应满足甲方的服务需求。

乙方不得随意更换选派的专业技术运维人员，如有特殊原因需要更换人员的，须事先向甲方书面提出申请并提交拟更换人员的详细资料，更换后的人员在水平、经验、资历等方面不得低于原有人员，经甲方审查书面同意后方可更换，否则将视为乙方违约，并承担1万元/人次的违约金。若乙方擅自更换人员达到3人次的，甲方有权解除合同，于此情形下，乙方应当支付本合同运维服务费20%的违约金，违约金不足以弥补甲方因此遭受的全部损失的，乙方承担补足责任。

如果甲方认为乙方选派的运维人员不能胜任工作，有权要求乙方予以更换，乙方应当在甲方通知后3日内更换为资格资质更高且能胜任工作的运维人员。乙方在提供本项目服务过程中应采用已有的国家标准、行业标准和主流国际标准。服务质量考核标准详细描述见附件2。

未经甲方事先书面同意，乙方不得将本合同项下的权利义务转让或者分包给任何第三方。否则甲方有权解除合同，于此情形下，乙方应当支付本合同运维服务费20%的违约金，违约金不足以弥补甲方因此遭受的全部损失的，乙方承担补足责任。

三、服务期间

乙方为甲方提供本合同项下运行维护服务的期间为 2025 年 8 月 13 日至 2026 年 8 月 12 日。

第三章 合同价款

本合同项下甲方应当支付给乙方的运维服务费即合同价款（含税）为：人民币 1,032,000.00 元，大写：人民币壹佰零叁万贰仟元整。该价款为乙方完成本合同项下服务内容应得的全部报酬和费用。除此之外，甲方不再向乙方支付其他任何款项。

运维服务费清单详见附件1。

第四章 支付条款

一、支付依据

乙方应定期向甲方汇报运维的工作情况，甲方根据乙方提交的季度运维服务工作报告以及年度运维服务工作报告及相关服务要求和约定，支付运维服务费。

二、支付方式

本合同给项下项目报酬分两期支付：

1.第一期支付：本合同生效且市财政拨付本项目运维经费后 20 个工作日内，甲方应向乙方支付运维服务费的 50 %，即人民币 516,000.00 元，大写：人民币 伍拾壹万陆仟元整 。

2.第二期支付：在2025年 12月 9 日前 ，甲方支付乙方运维服务费的剩余部分，即人民币 516,000.00 元，大写：人民币伍拾壹万陆仟元整 。

每期付款前，乙方应向甲方出具符合甲方要求的与应付款总额等额的合法有效发票。若乙方未及时出具发票，甲方有权不予付款且不承担任何违约责任。

在甲方支付第二期运维服务费之前，乙方应当以支票、电汇或银行保函等非现金的方式向甲方提交运维服务费总金额5%即人民币 51,600.00 元（大写：伍万壹仟陆佰元整）的履约保证金，履约保证金期限应覆盖至合同履约期满后的30个自然日。如乙方未按时支付履约保证金，甲方有权不予支付第二期运维付费或者有权从第二期运维服务费中直接扣除等额款项作为乙方的履约保证金。如在履约过程中乙方存在违约情形，甲方有权从乙方的履约保证金中扣除乙方应支付的违约金、赔偿金。本合同质量保证期届满后，甲方将剩余的履约保证金无息退还乙方。

若因财政拨付的原因不能及时支付款项的，甲方有权顺延付款且不承担任何责任。

第五章　违约条款

一、乙方未按约定提供服务

乙方未按本合同约定的服务条款提供服务或者提供的服务质量不符合本合同约定或者甲方要求的，但甲方认为乙方提供的服务具有一定的补救价值，可以给予乙方一定的宽限期，乙方在甲方指定的宽限期内仍未按合同约定提供服务或者提供的服务不符合质量要求的，乙方应按本合同运维服务费的20%向甲方支付违约金。给甲方造成损失的（损失包括但不限于因索赔或者被索赔发生的诉讼费、律师费、鉴定费、保全费、差旅费、被有权机关处以的罚款以及向第三方支付的赔偿金，下同），乙方还须承担赔偿责任。违约金和赔偿金的支付并没有解除乙方继续履行合同规定之内容。如果甲方认为本合同已没有继续履行的必要，甲方还有权解除本合同，乙方在接到甲方通知之日起3日内返还甲方已支付的全部款项，并按照本合同约定的运维服务费总额的20%向甲方支付违约金，违约金不足以支付因此给甲方造成的全部损失的，乙方应予赔偿。

若乙方未按合同约定提供服务的或者提供的服务质量不符合本合同约定或甲方要求的，且甲方认为乙方提供的服务不具有补救价值，乙方应按本合同运维服务费的20%向甲方支付违约金。给甲方造成损失的，乙方还须承担赔偿责任。同时，甲方还有权解除本合同，并要求乙方在接到甲方通知之日起3日内返还甲方已支付的全部款项。

第六章　移交条款

一、合同的履行地点和方式

本合同履行地点为甲方指定地点，具体地点以甲方通知的为准。乙方须向甲方提供季度运维服务工作报告以及项目总结报告，每次提交的报告应包括装订成册的纸质版一式贰份，电子版壹份。

二、运维服务验收

（一）验收依据

1. 国家有关规定，国家或行业标准；

2. 甲乙双方签订的本合同；

3. 甲乙双方关于运维服务工作安排的记录、洽商文件，乙方运维服务工作记录，乙方日常工作报告及总结。

4. 法律法规以及其他相关文件另有规定的按其规定。

（二）验收方式

1. 本合同服务期届满前 30 个工作日内，由乙方提出验收申请，经由甲方审核后 10 个工作日内，甲方组织对乙方的服务工作进行验收。因验收而发生的全部费用由乙方承担，包括但不限于专家费、会议费等。乙方应在验收前，按甲方要求提交总结报告、工作记录、项目管理等文档；

2. 经甲方验收合格书面确认后，视为验收合格。

三、质量保证

本合同服务项目的质量保证期为 1 年，自乙方提交年度运维服务工作报告且经甲方最终验收合格之日起计算。在质量保证期内发现服务质量缺陷的，乙方应当负责返工或者采取补救措施，直至符合本合同约定或者甲方的要求，期间发生的费用由乙方自行承担。但因甲方使用、保管不当或其他非乙方原因引起的问题除外。

四、联络点

甲方和乙方双方同意以下人员作为各自的外包联络员。他们负责双方之间的日常联络工作。任何一方在以书面通知通告对方的前提下，可以更换其联络人员。甲方同意由甲方的联络人员接受本合同所规定的乙方提供的产品和服务，乙方同

意由乙方的联络人员承担本合同所规定的所有相关的义务。

甲方的联络员为：李伟，联系电话：80818335

乙方的联络员为：马翔宇，联系电话：51255233

第七章　服务质量考核条款

一、甲方依据服务质量标准（见附件 2），对乙方提供的服务进行考核。

二、如果乙方没有满足服务质量考核标准，双方应按照本合同第五章第 1 条的内容执行。

三、乙方应当按时向甲方提交相关的书面运维服务工作报告(含季报及年报)，接受甲方的评审；甲方有权对乙方的服务提出评审意见和建议，乙方应当根据该意见和建议进行修正和完善，直至得到甲方的满意。

第八章　安全保密条款

一、本合同生效之日起，乙方应当对甲方本项目中形成和取得的各项数据、资料、报告等成果、甲方提供的各种技术文件（软件、咨询报告、服务内容）与信息以及乙方在履行本合同过程中知悉的甲方各种信息资料（统称保密信息）承担保密责任，未经甲方事先书面批准不得提供给任何第三方或者用于非本合同用途。乙方的该等保密义务持续有效，并不随着本合同被认定为无效、被撤销、解除或终止而免除。

乙方未按照上述约定履行保密义务的，应当向甲方支付运本合同维服务费用 20%的违约金（违约金不足以弥补甲方损失的，乙方还应当补足甲方的损失），并且，甲方有权解除本合同。

二、乙方必须与甲方签订《安全保密协议》，见附件 3。

三、乙方及乙方安排在甲方现场的工作人员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，生产安全及甲方系统数据安全。

四、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。

五、乙方如违反《安全保密协议》，乙方必须承担全部责任并赔偿甲方的一切损失，甲方有权按照本合同第八章第 1 条追究乙方的责任并终止本合同。

六、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。

第九章　知识产权条款

一、乙方保证甲方在使用乙方提供的任何产品、服务时，不受任何第三方提出侵犯知识产权或者其他合法权益的指控。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，同时还应按照本合同约定的运维服务费总额20%向甲方支付违约金，违约金不足以弥补甲方的全部损失的，乙方还应当补足甲方的损失，于此情形下，甲方有权解除本合同。

二、本项目实施所产生的信息资源及完成的所有技术成果（包括但不限于软件、源代码及技术资料）的所有权和知识产权（包括但不限于著作权、专利权、商标权、专有技术等权利）及由此衍生的一切权利均由甲方所有。

三、对在运维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。

四、本条款约定义务不因合同终止而免除。

第十章　不可抗力

一、如果合同任一方因战争、火灾、洪水、台风、地震、政府行为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，并可根据情况部分或全部免予承担违约责任。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。

二、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。

三、如果不可抗力事件后果影响合同执行超过180天，双方则就未来合同的履行另行商议。

第十一章　争议解决条款

一、 争议的解决

因履行本合同所发生的和与本合同有关的一切争议，甲、乙双方应首先通过

协商方式解决。若协商不成，任何一方均可向合同签订地有管辖权的人民法院提起诉讼。

二、 争议期间服务的连续性

如果甲方或者甲方的用户和乙方之间发生争议，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。如果争议的内容是有关甲方应支付的费用，乙方能且只能在做出书面通知 3 个月之后，终止合同并停止服务。

第十二章 其他条款

一、 在本合同履行过程中，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。

二、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。

三、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，以本合同条款为准。

第十三章 合同的终止

一、到期

本合同到期的服务终止，乙方应至少在合同到期日前 30 天以明确的书面形式通知甲方。

二、续约

乙方在本合同到期日前 30 天提前通知甲方且甲方同意的情况下，双方可以商议续约。

三、违约的终止

任何一方违反合同的约定并在接到非违约方书面的违约通知 15 天内补救失败，非违约方在提前 15 天给予书面通知的情况下有权终止合同。一旦合同以这种方式终止，各方应按照约定履行。

第十四章 合同的生效

一、本合同履行期限为 2025 年 8 月 13 日至 2026 年 8 月 12 日，合

同自双方法定代表人或者授权代表签字并加盖单位合同章或公章后生效。

二、本合同一式肆份，甲、乙双方各执贰份，具有同等法律效力。

（以下无正文）

甲方：北京智慧交通发展中心
（北京机动车调控管理事务中心）

法定代表人：

或授权代表：

签约日期：2025.8.12

乙方：北京云楚网安信息技术有限公司

法定代表人：

或授权代表：

签约日期：2025.8.11

附件1　运维外包服务水平条款

一、运维服务内容及水平

（一）脆弱性检测

（1）服务内容

乙方应针对甲方当前部署的信息系统所涉及的服务器及网络安全设备进行脆弱性检测，通过两种漏扫设备进行安全检查。通过专业化的技术分析，识别存在的脆弱点和安全风险隐患。

（2）服务频次

本项目服务周期内，提供4次脆弱性检测服务。

（3）服务成果

乙方应提交以下成果文档

《脆弱性检测报告》

（二）安全加固

（1）服务内容

根据脆弱性检测等工作结果，结合甲方的业务需求，对甲方存在的各类脆弱性问题提出合理的安全整改建议和切实可行的安全加固方案。

（2）服务频次

本项目服务周期内，提供4次安全加固服务。

（3）服务成果

乙方应提交以下成果文档

《安全加固报告》

（三）网站安全监测

（1）服务内容

乙方应按照甲方的网站监控需求及监控范围，采用远程监控系统提供不少于20个网站可用性监测、实时告警、网站防篡改服务，及时发现问题并提供改进建议。监测内容包含但不限于：

1. 挂马检测

2. 网页敏感词检测

3. 网站漏洞检测

4. 网站可用性检测

（2）服务频率

在本项目服务周期内，提供全年7*24小时监测。

（3）服务成果

乙方应提交以下成果文档

《网站安全监测服务报告》

（四）信息安全应急响应

（1）服务内容

乙方应在服务期间内提供应急响应支撑服务，在服务期内，一旦重要信息系统及网络出现突发安全事件，根据应急响应要求，提供应急响应服务并能够及时进行有效的应急处理。当发生重大、紧急的信息安全事件时，现场值守人员无法解决，派遣资深安全工程师在30分钟内给予响应，1小时内到达现场，4小时内予以解决。乙方应在服务期内能够针对病毒类安全事件、网络类安全事件和系统类安全事件开展应急响应工作。在信息安全事件发生时，能够保证网络与信息系统的正常运行。

（2）服务频率

本项服务按需提供

（3）服务成果

乙方应提交以下成果文档

《信息安全响应报告》

（五）应急演练

（1）服务内容

乙方应根据应急预案规定的应急处理流程协助甲方编制应急演练方案，并组织信息系统的主管部门、应用系统维护服务商等相关人员开展信息系统应急演练工作，使唤得相关人员了解应急流程和自己的责任，在安全事件发生时，能有条不紊开展工作，最大程度降低安全事件带来的负面影响和损失。

（2）服务频率

在本项目服务周期内，开展 1 次应急演练工作

（3）服务成果

乙方应提交以下成果文档

《信息系统应急演练报告》

（六）安全驻场服务

（1）服务内容

乙方应派驻 3 名安全工程师，提供 5*8 小时的现场安全值守服务，在现场值守期间负责监控网络、信息系统运行状态，及时反馈和处理各类故障问题，对于信息安全事件有效预警、上报、反馈；设备日常运维服务内容包括运行值守与故障处置、网络设备巡检、网络架构维护、网络设备事件应急响应、设备配置管理、张贴设备标签、技术支持服务。

（2）服务频率

本项服务在服务期内持续提供

（3）服务成果

乙方应提交以下成果文档

《安全服务报告》、《运维工作日报》

（七）特殊时期值守

（1）服务内容

乙方应在五一、国庆、全国两会等特殊时期和春节等重要节日，安排 1 名高级工程师，提供 7*24 现场值守服务，值班结束后提交值班服务记录。以保障甲方信息系统安全运行为主要目标，及时发现安全隐患并协助处置、排队信息系统安全隐患，提高信息安全事件发生和处置能力，提高信息安全水平。

（2）服务频率

本项服务按需开展

（3）服务成果

乙方应提交以下成果文档

提交《特殊时期安全值守报告》

（八）网络设备巡检

（1）服务内容

乙方人对纳入运维的网络设备定期进行设备检测、日志分析、故障预警、性能评估、网络调优、策略配置管理和维护等工作，并提交巡检报告。定期巡检的目的在于及时发现和预防可能出现的硬件和系统问题，从而在最大程度上为系统的连续稳定运行提供保证。

（2）服务频率

在本项目服务周期内，开展 12 次/年本项服务

（3）服务成果

乙方应提交以下成果文档

《网络设备巡检报告》

（九）设备配置管理

（1）服务内容

乙方应根据采购人网络系统运行情况，完成网络、防火墙等设备的配置管理工作，每月全部备份一次设备的配置文件，当设备发生故障，影响网络系统正常运行时，及时恢复设备的配置文件。当设备的配置文件发生变化时，随时做好备份工作。

（2）服务频率

在本项目服务周期内，开展 12 次/年本项服务

（3）服务成果

乙方应提交以下成果文档

《设备配置台账》

（十）网络和信息报告

（1）服务内容

网络和信息安全报告服务是为了跟踪最新的系统、网络和应用相关的安全问题，为采购人提供安全预警而设置的，投标人的安全专家应关注新的漏洞的出现，同时与国际和国家权威安全机构保持紧密联系，并根据采购人的资产情况、人员情况以及业务情况，在提供标准的安全通告的基础上，提供定制的安全通告，提高采购人的安全防范意识，确保网络安全。

（2）服务频率

在本项目服务周期内，开展 1 次/周，共 52 次服务

（3）服务成果

在本项服务完成时，将提交但（不限于）如下文档：

《网络和信息安全通告》

（十一）网络设备维保

（1）服务内容

自签订合同起，乙方应提供网络设备维保，服务内容包括对网络设备提供维保服务、原厂售后及维修服务以有及备机备件服务。详细服务内容如下：

- **设备硬件维保、维修及备品备件**

在甲方要求的服务期限内，须对网络设备（参见“网络设备列表”）提供原厂级别的硬件维保服务(设备维保过程中所维修的硬件及人工费用均包含于投标总价，所有故障备件免回收)，乙方应对所列网络设备提供一年的保修服务，并负责维修和更换网络设备包含的各项备件。

网络设备列表

序号	设备名称	设备品牌	设备型号	单位	数量
1	楼层汇聚交换机	H3C	LS-9505E	台	1
2	交通委楼层接入交换机	H3C	LS-5500-52C	台	23
3	考试中心机房交换机	H3C	H3C 5500	台	1

乙方需提供包括（但不限于）设备日常巡检、备品备件服务和设备故障维保等服务。

乙方需负责维修和更换设备维保汇总表中所包含的各项备件，保修服务响应级别全部为7*24小时；当故障需要现场诊断、处理时，要求维护工程师在1小时内赶至现场；影响用户应用的故障备件应在4小时内完成维修、排除故障或提供同等级别的备品备机等手段保障网络畅通。设备故障需要返厂维修时，乙方应提供维修期间的原厂备件与服务，并在5个工作日内完成设备更换。

备品备件服务作为应急响应故障处理过程的一项辅助性服务，对于加快故障处理时间，及时恢复系统运行起到不可替代的作用。乙方必须设有同城备件库，准备充足的设备备件，并对备品备件的更换制定相关的预案，在发生设备更换的时候将依据预案进行更换流程，避免造成更换过程中发生的风险。所有更换的备件均为与原设备或模块的型号相同，或各项性能规格不低于原有设备或模块的备件。服务提供的备件必须是来自设备原厂商，必须是经合法渠道采购的备件。不得使用非法渠道获得的备件或用其他方式进行替代。乙方在维护服务过程中提供的软硬件产品，必须保证该产品拥有合法的使用权。维护更换的备件，均提供自更换之日起1年的保修期。在发生硬件故障时，乙方确定故障必须采取备件更换方式才可解决的情况下，首先通知甲方相关负责人。乙方提供的备件更换服务必须按不同的设备故障影响范围，结合甲方的实际情况制定相应的备件快速响应流程。在系统正常运行期间，若属于设备自然损坏、老化等故障，或自然灾害与不可抗力（如雷击、电压不稳等）引起的损坏，经甲乙双方技术人员现场检测确认后，则直接用备品备件替换，换回的损坏设备由乙方协助甲方负责维修，修好后补充回备件库。

（2）服务频率

1年

（3）服务成果

在本项服务完成时，将提交如下文档：

《设备故障处理报告》

二、运维地点

北京市智慧交通发展中心（北京市机动车调控管理事务中心）指定地点

三、运维服务实施内容

（一）脆弱性检测

乙方应针对甲方当前部署的信息系统所涉及的服务器、网络设备进行脆弱性检测，通过两种漏扫设备进行安全检查。通过专业化的技术分析，帮助甲方了解自身信息系统。

（二）安全加固

根据前期脆弱性检测的结果，结合甲方的业务需求，对甲方相关的设备进行安全策略加强、调优等，提出合理加固方案并指导相应的实施，加强系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。

（三）网站安全监测

乙方应通过远程监控系统为甲方 20 个网站站点提供远程安全监测、实时告警服务，及时发现问题并提供改进建议。以便快速定位安全风险隐患，并协助团队迅速分析、防范及处置各类风险隐患和安全事件，从而确保网站的安全稳定运行。

（四）信息安全应急响应

乙方应在服务期间内提供应急响应支撑服务，在服务期内，一旦重要信息系统及网络出现突发安全事件，根据应急响应要求，提供应急响应服务并能够及时进行有效的应急处理。当发生重大、紧急的信息安全事件时，现场值守人员无法解决，派遣资深安全工程师在 30 分钟内给予响应，1 小时内到达现场，4 小时内予以解决。乙方应在服务期内能够针对病毒类安全事件、网络类安全事件和系统类安全事件开展应急响应工作。在信息安全事件发生时，能够保证网络与信息系统的正常运行。

（五）应急演练

乙方应根据应急预案规定的应急处理流程协助甲方编制应急演练方案，并组

织信息系统主管部门、应用系统维护服务商等相关人员开展信息系统应急演练工作。使得相关人员了解应急流程和责任，在安全事件发生时，能有条不紊开展工作，最大程度降低安全事件带来的负面影响和损失。

（六）安全驻场服务

驻场安全工程师应具备信息安全事件有效预警、上报、反馈的能力，能够通过监控工具、日志分析等手段，主动发现潜在或已发生的安全威胁与异常行为，进行初步研判，遵循既定的信息安全事件报告流程，及时、准确地将预警或确认的事件信息上报，对事件处置进展及最终结果进行及时跟踪与反馈，确保信息传递畅通，形成闭环管理。还需提供设备日常运维服务包括运行值守与故障处置、网络设备巡检、网络架构维护、网络设备事件应急响应、设备配置管理、张贴设备标签、技术支持等服务。

（七）特殊时期值守

乙方应在五一、国庆、全国两会等特殊时期和春节等重要节日，安排 1 名高级工程师，提供 7*24 现场值守服务，值班结束后提交值班服务记录。以保障甲方信息系统安全运行为主要目标，确保在关键时期，能够高效、专业地提供系统安全保障，包括实时监控、快速响应、风险预警及应急处置等，以保障信息系统的稳定运行和数据安全，有效应对各类网络安全威胁，确保重要时期的网络安全无虞。

（八）网络设备巡检

乙方应对纳入运维的网络设备定期进行设备检测、日志分析、预警、性能评估、网络调优、策略配置管理和维护等工作，并提交巡检报告。定期巡检的目的在于及时发现和预防可能出现的硬件和系统问题，从而在最大程度上为系统的连续稳定运行提供保证。

（九）设备配置管理

乙方根据甲方网络系统运行情况，完成网络、防火墙等设备的配置管理工作，每月全部备份一次所有设备的配置文件，当设备发生故障，影响网络系统正常运行时，及时恢复设备的配置文件。当设备的配置文件发生变化时，随时做好备份工作。

（十）网络和信息报告

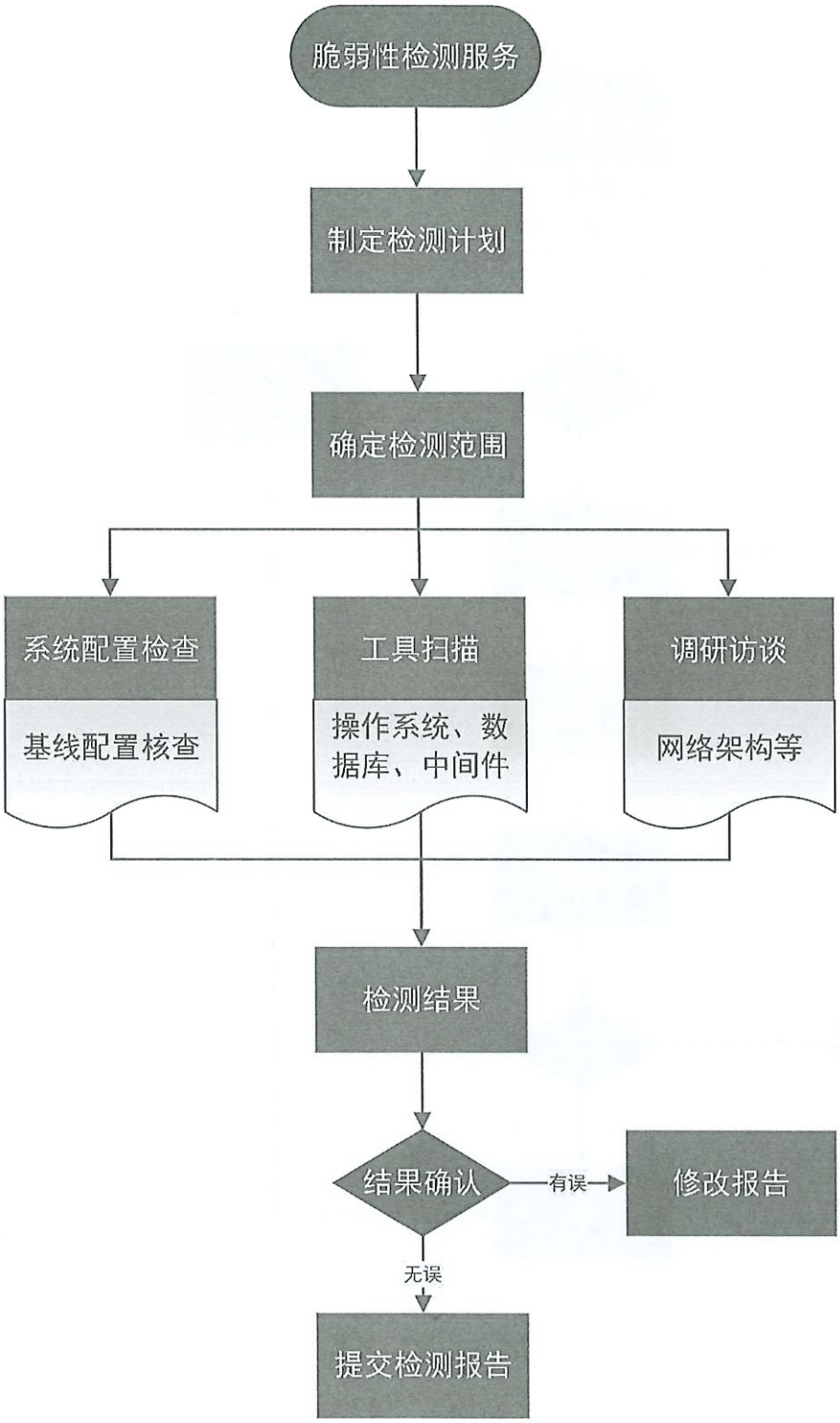
通过专业的网络和信息安全报告服务，并紧密跟踪网络安全行业的最新发展态势，结合信息系统的实际安全运行情况，编制出详尽的信息系统安全运行态势报告。通过这份报告，能够及时、全面地掌握信息系统的安全状态，识别潜在的安全风险，为制定有效的安全策略和改进措施提供数据支持和决策依据，确保信息系统的持续稳定运行。

（十一）网络设备维保

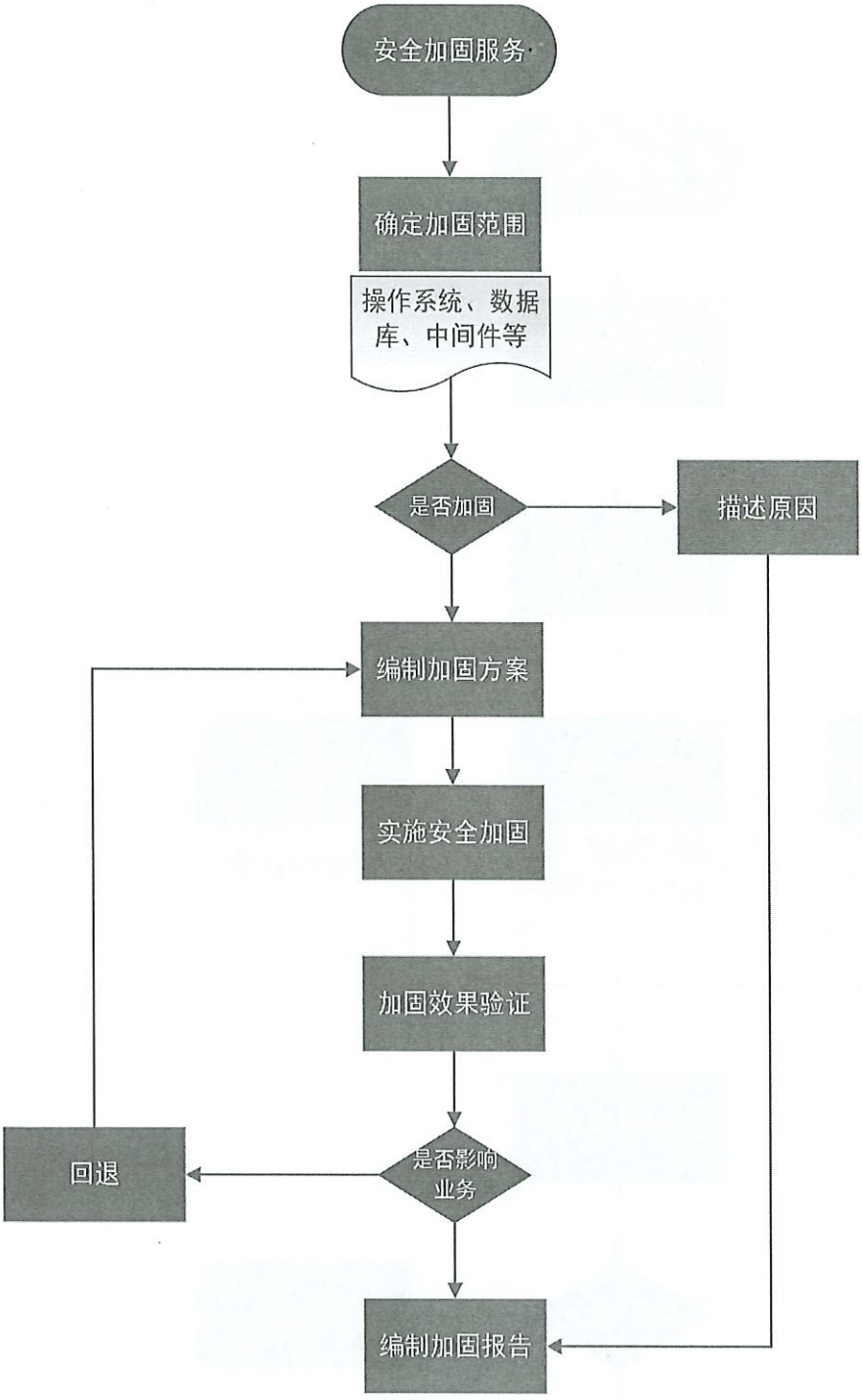
自签订合同起，乙应提供网络设备维保、服务内容包括对网络设备提供维保服务、原厂售后及维修服务以及备机备件服务。

四、服务流程

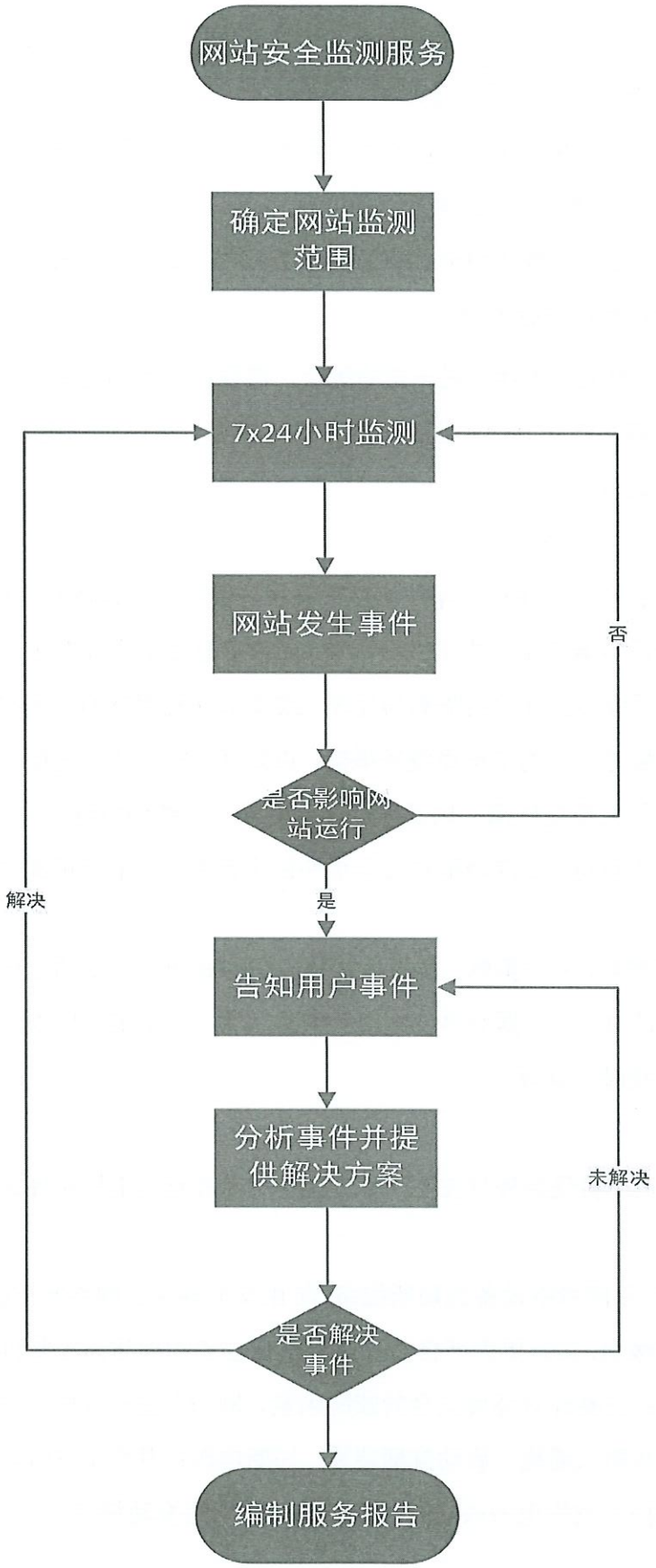
（一）脆弱性检查



（二）安全加固


安全加固服务
确定加固范围
操作系统、数据库、中间件等
是否加固
描述原因
编制加固方案
实施安全加固
加固效果验证
是否影响业务
回退
编制加固报告

（三）网站安全监测


网站安全监测服务
确定网站监测范围
7x24小时监测
网站发生事件
是否影响网站运行
否
是
解决
告知用户事件
分析事件并提供解决方案
未解决
是否解决事件
编制服务报告

（四）信息安全应急响应

事件响应

建立三级应急响应体系，设定为三级到一级，一级最低，三级最高，根据不同事件等级逐步提高应急响应和服务支持力度。

(1) 一级响应：当网络系统突发事件较小，现场值守人员能够处理时，由值班安全工程师直接进行处理，并填写相应的处理记录；

(2) 二级响应：当网络系统突发事件超出了值班安全工程师的处理能力时，由行公司应急响应小组赶赴现场，进行处理；

(3) 三级响应：当网络系统突发事件超过一定的等级，需要更深入的处理时，将求助于网信办、公安局等网络安全行业监管机构，请求资深专家提供在线指导，必要时赶赴现场，共同处置。

事件抑制

事件抑制的目标是限制安全事件对受保护信息系统所造成影响的范围与程度。事件抑制作为信息安全应急响应工作中的关键环节，需在信息安全事件发生的第一时间，对故障系统或区域实施有效的隔离与处理；或者依据所拥有的资源状况以及事件的等级，采取临时切换到备份系统等举措，以降低事件损失，避免安全事件的扩散（例如蠕虫的大规模传播）以及安全事件对受害系统的持续性破坏，这有助于应急响应工作人员迅速、准确地对安全事件做出判断，并采取正确的应对策略。

应急抑制涵盖物理抑制、网络抑制、主机抑制和应用抑制四个层次的工作内容。当发生信息安全事件时，应根据对事件定级的结果，综合运用多个层次的抑制措施，确保抑制工作及时、有效。

1. 物理抑制

(1) 关闭主机：防止主机受到外界安全事件的影响，或者避免主机对外部环境产生影响。

(2) 切断网络连接：关闭网络设备或切断线路，防止安全事件在网络间扩散。

(3) 提升物理安全级别：实施更为严格的人员身份认证和物理访问控制机制。

(4) 环境安全抑制：主要针对环境安全的威胁因素，例如发生火灾时，关闭防火门、启用消防设备和防火通道、启动排烟装置、切断电源；发生水灾时，启用排水设备、关闭密封门；发生电力故障时，启用 UPS 和备用发动机等。

2. 网络抑制

(1) 网络边界过滤：对路由器等网络边界设备的过滤规则进行动态配置，过滤包含恶意代码、攻击行为或有害信息的数据流，切断安全事件在网络间的传播途径。

(2) 网关过滤：对防火墙等网关设备的过滤规则进行动态配置，阻断包含恶意代码、攻击行为或有害信息的数据流进入网关设备所保护的网络区域，有效实现针对信息安全事件的网络隔离。

(3) 网络延迟：采用蠕虫延迟和识别技术，限制恶意代码在单位时间内的网络连接，有效降低蠕虫等恶意代码在网内和网间的传播速度，减小蠕虫事件对受保护网络系统的影响范围。

(4) 网络监测：提高网络入侵检测系统、安全监测系统的敏感度和监测范围，收集更为细致的网络监测数据。启用网络监测与网络边界过滤及网关过滤的联动机制，提高网络对攻击行为或恶意代码的响应速度。

3. 主机抑制

(1) 系统账号维护：禁用或删除主机中被攻破的系统账号以及攻击者生成的系统账号，防止攻击者利用这些账号登录主机系统，进行后续的破坏行为。

(2) 提升主机安全级别：实施更为严格的身份认证和访问控制机制，启用主机防火墙或提高防火墙的安全级别，过滤可疑的访问请求。

(3) 提升主机监测级别：提高主机入侵检测系统、主机监测系统的敏感度和监测范围，收集更为细致的主机监测数据。启用主机监测与主机防火墙、网络边界过滤及网关过滤的联动机制，提高主机对攻击行为或恶意代码的响应速度。

4. 应用抑制

(1) 应用账号维护：禁用或删除被攻破的应用账号以及攻击者生成的应用账号，防止攻击者利用这些账号登录应用服务，进行后续的破坏行为。

(2) 提升应用安全级别：针对应用服务，实施更为严格的身份认证和访问控制机制，增加攻击者攻击应用服务的难度。

(3) 提升应用监测级别：提高应用入侵检测和监测系统的敏感度和监测范围，收集更为细致的应用服务监测数据。启用应用监测与主机防火墙、网络边界过滤及网关过滤的联动机制，提高应用服务对攻击行为或恶意代码的响应速度。

(4) 关闭应用服务：避免应用服务受到来自网络的安全事件影响，或者防止

应用服务对外部网络环境产生影响。

(5) 启用陷阱：针对恶意的攻击行为，启用蜜罐陷阱系统，将攻击者转移到陷阱系统，以收集更为详细、准确的信息，用于后续的应急处理和证据保留工作。

事件根除

在信息安全事件得到有效抑制之后，这仅仅是解决问题的第一步。接下来，我们需进一步深入、全面地剖析该事件。不能留下任何隐患，防止类似的安全事件再次发生。

事件根除工作可分为物理根除、单机根除和网络根除三个层面。

物理根除层面，主要是针对与信息系统相关的物理设备进行检查和处理。例如，要仔细检查服务器、存储设备等硬件是否存在被破坏、被植入恶意装置的情况。若发现有异常的硬件设备，要及时进行更换或修复，以确保物理层面的安全。

单机根除层面，则聚焦于每一台独立的计算机设备。需要对单机系统进行全面的病毒查杀、漏洞修复等操作。要检查系统中的各类软件程序，看是否存在被篡改、被植入恶意代码的情况。对于那些可能存在安全风险的软件，要及时进行更新或卸载，保障单机系统的纯净和安全。

网络根除层面，重点在于对整个网络环境进行梳理和优化。要检查网络拓扑结构是否合理，网络访问权限是否设置得当。还要对网络中的数据流进行监控和分析，查看是否存在异常的网络流量，是否有黑客通过网络进行入侵的迹象。对于发现的网络安全漏洞，要及时进行封堵，防止外部的恶意攻击。

为确保从受保护网络系统中彻底清除安全威胁，针对不同类型的安全事件，应综合运用不同层面的根除措施。

不同的安全事件具有不同的特点和成因，单一的根除措施往往难以达到理想的效果。因此，我们需要根据具体情况，灵活组合物理根除、单机根除和网络根除这三个层面的措施，形成一套全方位、多层次的安全防护体系，为网络系统的安全稳定运行保驾护航。

1. 物理根除

(1) 统一施行严格的物理安全举措：例如，针对关键物理区域，统一实施基于双因素或多因素的身份认证与物理访问控制机制，要求智慧交通发展中心提供正确的口令和 IC 卡，并通过指纹识别完成精准的身份鉴别。

(2) 环境安全保障：主要针对环境安全的威胁因素采取行动，如使用消防设

施灭火，更换故障电力设备以恢复正常电力供应，修复网络通信线路，修复被水浸湿的服务器等。

(3) 物理安全保障：强化视频监测、人员排查等措施，最大程度减少可能对受保护信息系统造成威胁的人员和物理因素。

2. 单机根除（包括服务器、客户机、网络设备及其他计算设备）

(1) 清除恶意代码：清除感染计算设备的各类恶意代码，如文件型病毒、引导型病毒、网络蠕虫、恶意脚本等，同时清除恶意代码在感染和发作过程中产生的数据。

(2) 清除后门：清除攻击者安装的后门，防止攻击者利用该后门登录受害计算设备。

(3) 安装补丁和升级：安装安全补丁和升级程序，涵盖硬件补丁与升级、操作系统补丁与升级、应用系统补丁与升级、安全产品补丁与升级（如病毒升级库）。所安装内容由各厂商提供，但须事先经信息安全应急支援中心严格审查和测试，并统一发布。

(4) 系统修复：修复因黑客入侵、网络攻击、恶意代码等信息安全事件对计算设备的文件、数据、配置信息等造成的破坏，如被非法篡改的系统注册表、信任主机列表、用户账号数据库、应用配置文件等。

(5) 修复安全机制：修复并重新启用计算设备原有的访问控制、日志、审计等安全机制。

3. 网络根除

(1) 全面进行单机根除：对受保护网络系统中的所有服务器、客户机、网络设备和其他计算设备开展上述单机根除工作。

(2) 评估排查：对受保护网络系统中的所有计算设备进行评估排查，测试是否仍存在受同种信息安全事件影响的单机。

(3) 网络安全保障升级：对网络中的安全工具进行升级，使其具备对该安全事件的报警、过滤和自动清除功能，例如为防火墙添加新的过滤规则，为入侵检测系统增添新的检测规则，升级网络病毒防御系统等。

应急恢复

当成功完成安全事件的根除工作之后，还需全面恢复系统的运行流程。系统的正常运行与否直接关系到整个业务的开展。我们需要将受影响的系统、设备、软件以及应用服务逐一仔细地还原到正常工作状态。这里的受影响范围可能涵盖了各个层面，比如服务器系统可能因为遭受攻击而出现数据混乱，网络设备可能出现连接中断，软件可能存在功能异常，应用服务可能无法正常响应客户请求等，都需要我们按照严谨的流程和规范的操作来进行恢复

恢复工作共分为五个阶段：系统恢复阶段、网络恢复阶段、用户恢复阶段、抢救阶段和重新部署/重入阶段。

1. 系统恢复阶段

协助应用开发商和基础设施运维人员恢复关键业务所需的服务器及应用程序。系统恢复过程完成的标志为数据库可用、用户的数据通讯链路重新建立、系统操作用户开始工作。网络和用户恢复任务与系统恢复同步进行。

2. 网络恢复阶段

协助网络运维人员安装通信设备和网络软件，配置路由及远程访问系统，恢复语音通信和数据通信，部署设置网络管理软件和网络安全软件等，恢复受灾系统的网络通信能力。

3. 用户恢复阶段

协助开展用户恢复工作。用户恢复任务与系统恢复任务和网络恢复任务同步进行，包括取回恢复工作所需资料并分发，联系预先指定的供应商和服务商，协调工作站、外围设备、传真和其他办公设备的运输，修复办公局域网和语音通信能力，协助安装和测试硬件，恢复用户相关的日常事务工作，如邮政业务、交通运输、后勤保障等。当系统和网络就绪后，利用抢救出来的记录以及备份存储的数据和信息，尽快恢复数据库。

4. 抢救阶段

与系统运维人员和数据库管理员共同开展抢救工作。抢救行动与其他灾难恢复工作同步进行，包括收集和保存证据，评估数据中心和用户操作区环境的恢复可行性和成本，抢救数据、信息和设备并转移至备份区域。

5. 重新部署/重入阶段

协助用户依据灾难恢复计划中定义的工作职能，将系统、网络和用户重新部署到原有的或新的设施中，并将应急状态下的服务级别逐步切换回正常服务级别。

事件分析

事后分析工作的意义，不仅体现在本次信息安全事件的处理之中，更重要的是，它有助于探寻安全问题的深层次原因，总结应对紧急安全问题的经验和教训，评估并改进现有安全机制的不足之处，从而为后续可能发生的信息安全事件的响应过程提供参考。

事后分析工作的目标是回顾并梳理发生信息安全事件的各类相关信息，尽可能将所有情况记录到文档中，研究事件发生的整个过程，剖析导致事件发生的根本原因，评估系统遭受的损失，并依据分析和评估结果对现有的工作方案进行调整。对多次发生的事件或同一时期的多个事件进行事后联合分析，意义更为重大。

针对信息安全事件的事后分析工作包括损失评估、审计分析以及对应急预案的评估修正。

1.损失评估

评估信息安全事件给受保护信息系统在各个方面造成的损失。鉴于受保护系统自身特性和安全需求存在差异，如功能定位、服务需求、网络状况、系统状况、人员状况等，损失评估必须全面考量信息安全事件带来的直接和间接影响。需考虑的因素如下：

- 受损设备和设施：涵盖因信息安全事件而遭受破坏或影响的服务器、客户机、输入输出设备、网络设备、通信线路、办公设备、安全设施、建筑物以及其他所有相关的设备设施。

- 受损数据：包含受保护系统中因信息安全事件而被窃取、篡改或删除的数据，如人事档案、公文、安全日志等。

- 受损服务：由于受到信息安全事件的影响，无法向用户或公众提供相应服务。例如，某单位的Web服务器因遭受拒绝服务攻击，无法为公众提供信息查询和电子政务功能。

- 人力耗费：信息安全事件发生后，应急响应体系为完成事件分析、事件处理、灾难恢复等工作所消耗的人力资源。

- 公众形象：信息安全事件的发生会对单位公众形象产生影响，进而导致无形资产损失。某些敌对组织正是出于此目的，对信息系统进行恶意攻击和破坏。

- 重建资源：信息安全事件发生后，为完成系统的重建恢复工作所消耗的各类资源，包括硬件、软件、人员、经费、通讯、能源、运输等。

2. 审计分析

对发生的信息安全事件展开审计分析，确定受保护信息系统中被安全事件利用的漏洞，查明事件发生的原因，并提出相应的整改措施。综合运用技术、人员、管理等多方面手段，避免相同或类似信息安全事件再次发生。该项工作内容包含以下三个方面：

- 漏洞定位：安全威胁对系统产生影响的根本原因在于受保护系统本身存在可被攻击的脆弱性（漏洞），如软硬件漏洞、人员失误、管理制度缺陷等。为从已发生的信息安全事件中及时汲取经验教训，避免同类安全事件再次发生，必须确定导致本次安全事件发生的漏洞，以便有针对性地确定整改措施，弥补系统漏洞。

- 查明原因：信息安全工作应遵循责任到人的原则，信息安全规划的首要任务是明确信息系统中的安全角色及对应的职责。信息安全事件发生后，应依据事先确定的角色和职责，结合审计分析结果，确定对安全事件发生负有相关责任的人员，以便对信息安全事件进行调查处理。

- 确定整改措施：根据上述漏洞定位和责任定位的分析结果，确定用于弥补系统漏洞的整改措施，如更换存在缺陷的硬件设备、对软件系统进行升级、安装系统补丁、修改系统配置、购置安全和监测设备、加强人员安全培训、制定并实施更为严格的安全管理制度等。

（五）应急演练

演练前期准备

(1)组建应急演练团队

应急演练应在依据应急预案所明确的应急领导机构或指挥机构的统一领导下有序组织开展。设立专门负责演练过程组织的工作机构，有助于切实加强对演练实际效果的监督与评估工作，并以第三方的客观视角，助力智慧交通发展中心精准识别演练过程中所暴露的实际问题，进而提出具有针对性的对应急预案内容的优化与调整建议。

(2)制定应急演练计划

为推动应急演练工作更加科学、高效地开展，我公司安全服务人员将全力协助智慧交通发展中心做好应急演练过程的组织以及评估记录等工作，并在关键环节给予专业指导。为此，在开展演练之前，需对智慧交通发展中心进行全面、系统的评估，准确确定应急演练科目内容、演练的最佳时段以及参与演练人员的专业技能等情况。

应急演练计划需对上述情况进行详细汇总、深入整理和全面总结，为演练指挥小组在决策演练发起条件、演练范围、演练时间进度安排、演练程序设置、人员角色分配以及通信联系方式等方面提供科学依据，并在实际演练计划中予以明确和落实。

(3)演练计划确认

演练指挥领导机构应针对已形成的应急演练计划召开专题讨论会，对计划中涉及的相关问题进行深入研究和分析，明确演练工作各阶段组织人员的具体职责和详细工作方案。只有当演练计划经演练指挥领导机构审核通过后，方可作为下一步启动演练的必要条件之一；若未通过审核，需严格按照领导机构的意见进行相应的修改和调整。

(4)演练计划培训

演练计划确定之后，我公司安全服务人员将组织智慧交通发展中心参与应急演练的相关人员进行集中培训。通过培训，确保所有参与人员充分了解自身工作内容，熟练掌握应急演练的实施流程和各环节工作步骤，为应急演练的顺利开展提供坚实保障。

(5)落实演练措施

应急预案中通常会明确为贯彻落实应急响应预案而制定的一系列应急保障措施。这些措施旨在确保在实际应急工作中能够有效应对各类问题，为应急工作提供必要的物质、技术和人员等方面的有力支持。

在应急演练过程中，将应用这些保障措施。因此，在演练前，我公司将协助智慧交通发展中心切实落实演练所需的各项保障措施，具体包括以下三类：

1）应急人力保障：协助智慧交通发展中心加大信息安全人才培养力度，强化信息安全宣传教育工作，打造一支政治素质高、业务能力强的信息安全核心人才与管理队伍，全面提升信息安全防御意识。

2）物质条件保障：协助智慧交通发展中心在资金安排上合理预留一定资金，用于预防和应对信息安全突发事件，进一步优化信息安全应急处理工作的物资保障条件。

3）技术支撑保障：协助智慧交通发展中心设立信息安全应急响应中心，搭建预警与应急处理的技术平台，不断提升安全事件的发现和分析能力。从技术层面逐步构建发现、预警、处置、通报等多个环节以及不同网络、系统、部门之间应急处理的联动机制。

开展演练工作

(1)演练的启动

应急演练作为对应急预案进行检验的一种重要形式，其意义深远且重大。它并非仅仅局限于集中在特殊时间段前开展，在日常的工作环境和条件下，应急演练要充分凸显应急事件所具有的突发性特点。各类应急事件并不会按照我们的预期时间和场景发生，它们往往在不经意间突然降临，所以日常演练对于提升应对能力至关重要。

(2)协助现场指挥

围绕着精心制定的演练计划和详细周全的应急预案，在我公司专业的安全服务人员全方位、全过程的协助之下，演练现场指挥部以严谨、规范的指令形式，正式启动演练过程。

我公司作为此次演练的支持单位，始终秉持严谨负责的态度。我们将根据智慧交通发展中心当前的信息安全现状，开展全面且深入的分析与研究。针对可能对智慧交通发展中心正常运行造成严重影响的典型信息安全事件，如网络攻击、数据泄露、系统故障等，制定应急预案并开展一场严谨、规范且具有实际意义的

应急演练。

应急演练启动后，智慧交通发展中心的演练人员会严格按照演练计划中预先精心设定的目标、逼真的场景和详细的脚本，有序推进演练进程。在演练过程中，充分运用通信手段及时、准确地传达演练指挥部下达的各项指令。

同时，我公司演练成员将对演练过程进行全程、全方位的记录与评判。过程记录在后续的应急演练汇报中起着不可替代的重要作用，它可作为场景再现的关键证据，用于验证应急预案存在的主要问题。记录人员会使用专业且先进的工具，对演练中使用的 IT 工具进行全面、细致的检测，包括硬件设备的性能检测、软件系统的稳定性检测等。他们还会认真提取日志操作文件，详细记录每一个操作步骤和相关数据。这些记录信息设有专门且安全可靠的备份保存机制，以防止数据丢失或损坏，确保能供智慧交通发展中心日后观摩使用，为其总结经验、改进预案提供有力支持。

(3)演练的终止

按照演练程序的终止条件，当演练过程达成既定的演练目标要求时，这意味着本次演练在各个方面均已取得预期效果。此时，演练现场指挥部会发布演练终止指令。该指令将通过多种渠道迅速传达给智慧交通发展中心的各参与人员，通知他们有序、安全地撤离演练场所。

我公司应急演练评估人员将针对演练的最终结果以及各项演练指标，开展全面、深入的现场取证和记录工作。评估工作不仅包含工具化的采样，借助先进技术手段采集和分析演练过程中的各类数据；还包括对参与演练人员的访谈，通过与他们面对面交流，深入了解其在演练过程中的实际感受、遇到的问题以及对预案实施过程的看法和建议。通过这些工作，获取预案实施过程中需要改进的意见，为进一步完善应急预案、提升应急处置能力提供有力依据。

演练报告与预案评估

(1)演练报告

我公司安全服务人员在演练结束后，组织专人对演练的全程效果进行总结，总结材料将包括以下内容：

1) 演练方案；

2) 演练过程、结果；

3) 演练效果评价、改进建议。

除了上述客观反映演练情况的内容以外，报告还专门对演练组织情况进行评价，反映在演练 过程中演练组织者，在演练组织和指挥能力的情况的评价。

(2)预案评估

通过演练，让相关各方熟悉流程，提升对安全事件的响应能力；同时验证预案的正确性与适用性，开展总结分析，并按需对应急预案进行修订。以此建立起验证和评价预案效果的评价体系，达成以下评估目标：

1）预案效果评估：应急预案是在信息安全事件发生时，用于指导应急操作的文件。为使应急预案能最大程度契合应急响应的实际需求，保障应急响应工作的准确与高效，每次启动应急预案并完成事件处理后，都必须对预案的实际效果展开评估，例如评估其是否符合单位的应急响应需求、预案的实际操作效率，以及在解决信息安全事件方面的实际成效等。

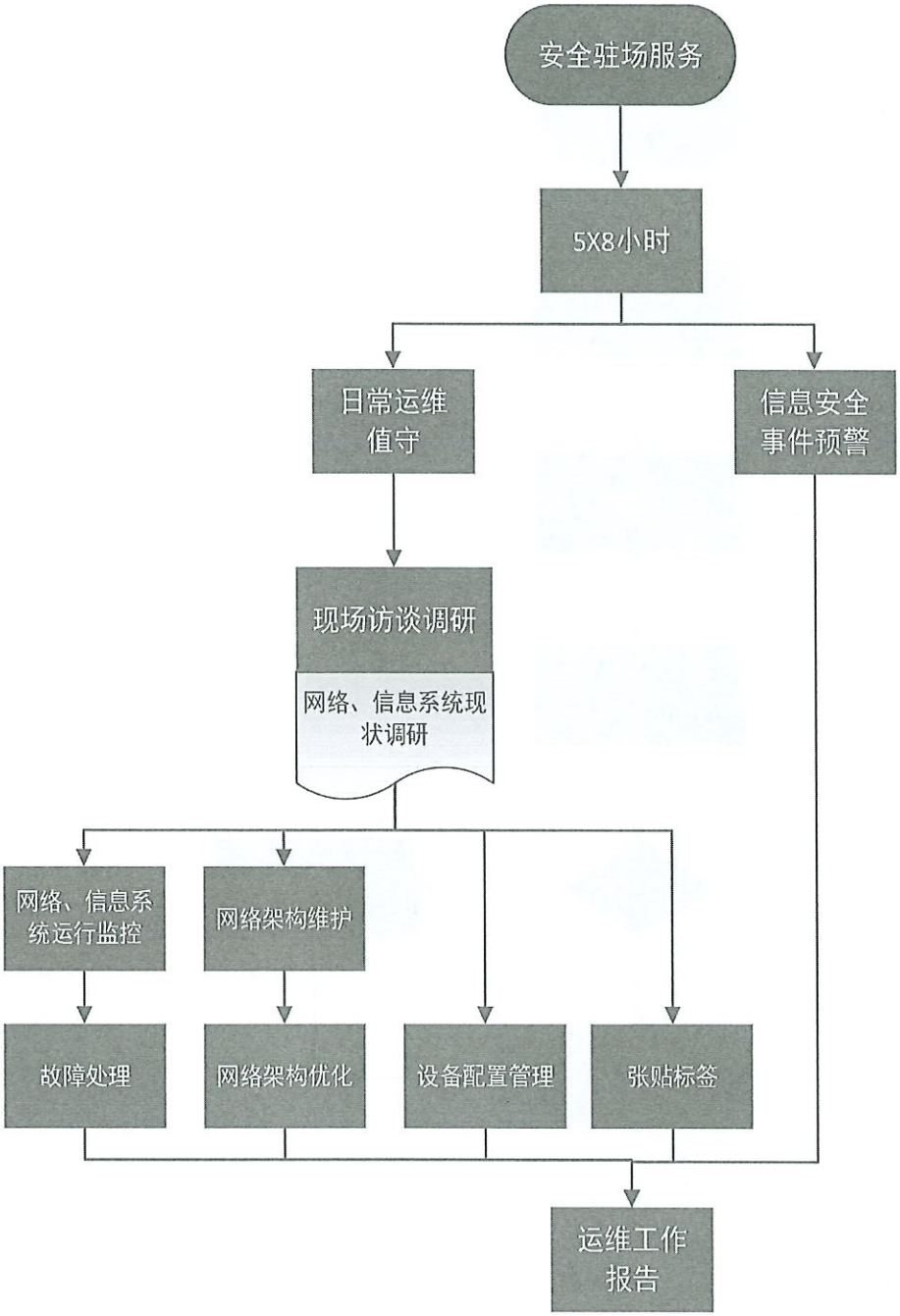
2）预案不足分析：鉴于预案是依据事先设想的各类信息安全事件所制定的操作文件，受多种因素制约，难免存在一些设计与实施上的缺陷。本阶段工作旨在找出预案制定和执行过程中的问题与不足，为预案的整改和修正提供依据。必要时，还需分析应急响应演练过程中未发现预案缺陷的原因。

3）预案更新：根据上述对预案效果和预案缺陷的分析结果，提出针对信息安全事件应急预案的更新方案，经批准后，在规定时间内完成预案的更新和审查工作，并予以发布施行。

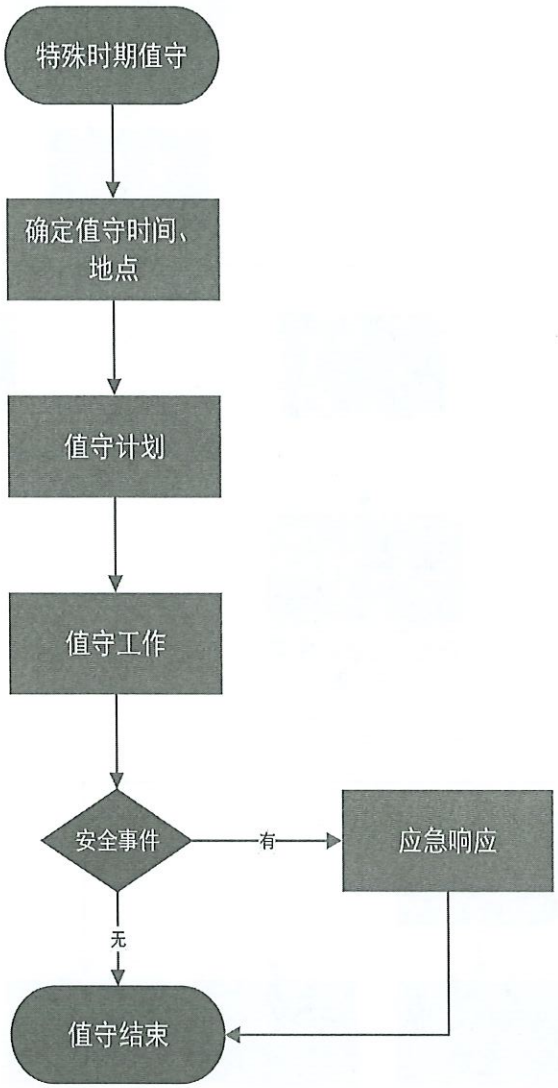
(3）预案整改建议

经过前期的演练报告和预案评估，对应急预案从人员、技术、流程等方面进行归类、整理。针对某些遗留问题，我公司安全服务人员将组织智慧交通发展中心应急工作相关负责人进行会商，最终形成预案修改意见。其中，对于某些关键问题，需各相关部门共同确认。

（六）安全驻场服务


安全驻场服务
5X8小时
日常运维值守
信息安全事件预警
现场访谈调研
网络、信息系统现状调研
网络、信息系统运行监控
网络架构维护
故障处理
网络架构优化
设备配置管理
张贴标签
运维工作报告

（七）特殊时期值守

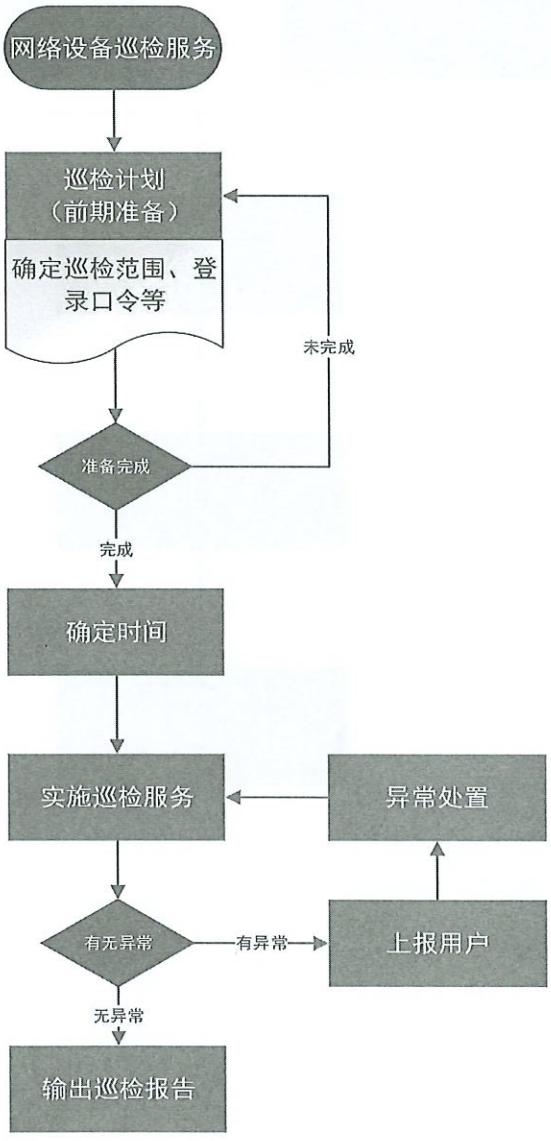


（八）网络设备巡检

在充分理解和掌握智慧交通发展中心信息系统的网络设备资产情况、网络部署情况、核心业务信息系统实际运行状况的前提下，对本项目所属的网络和安全设备的安全状况进行检查和判断，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。

网络设备巡检服务将按照如下流程进行：

1. 设备运行情况检查；
2. 设备配置情况检查；
3. 设备性能检查；
4. 编写设备巡检报告，智慧交通发展中心相关负责人签字。

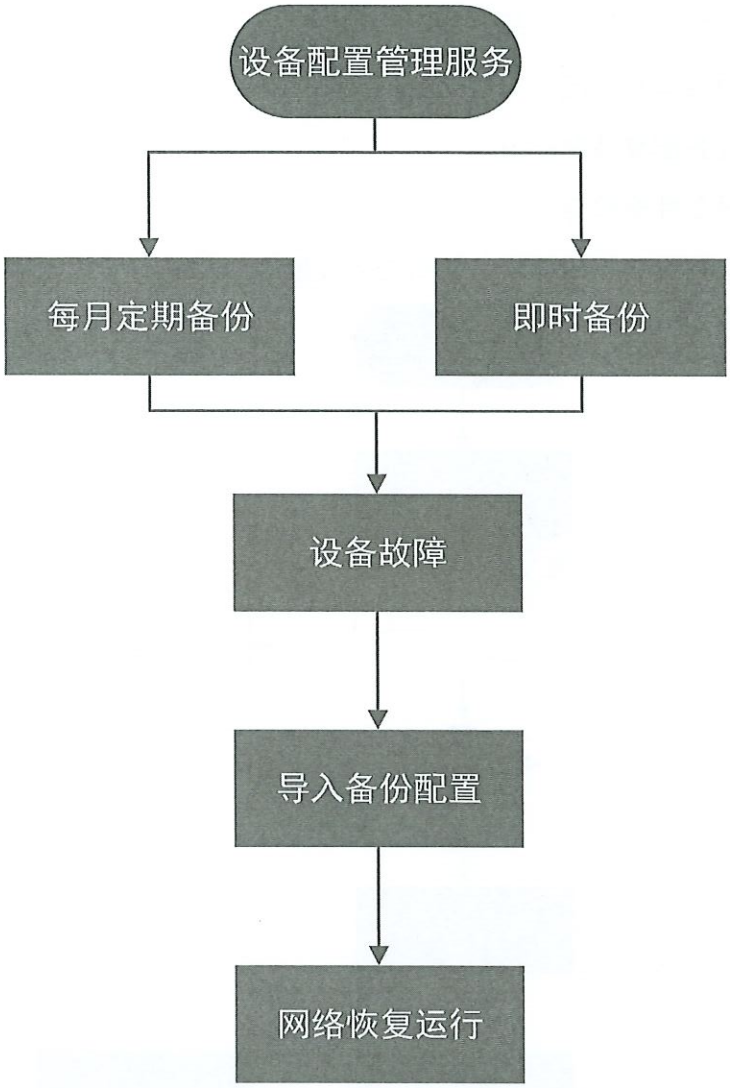


（九）设备配置

1. 每月进行 1 次网络设备、安全设备配置的备份。

2. 设备配置发送变化时，随时进行备份。

3. 3 设备发生故障时，通过备份配置使用备机及时恢复网络运行，保障业务连续性。



（十）网络和信息报告

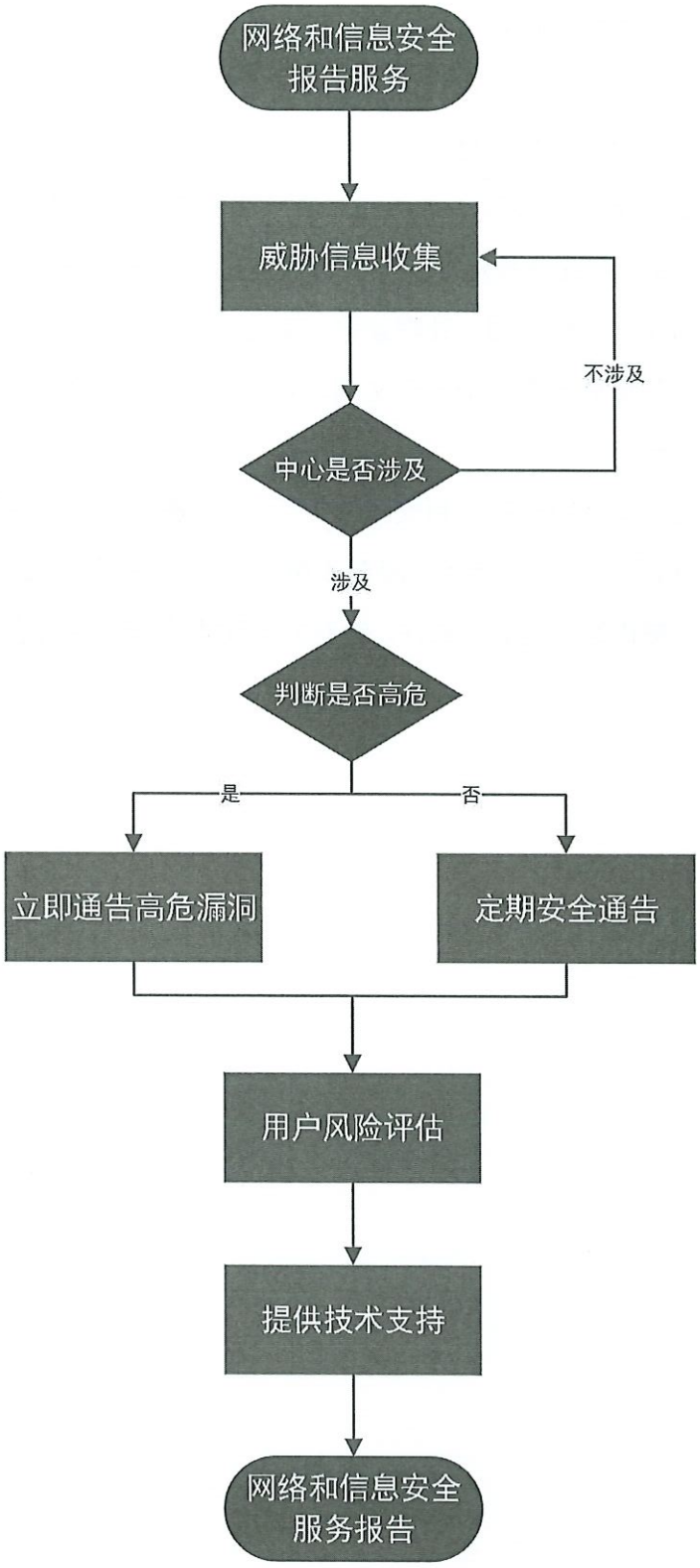
1.我公司安全服务人员每天对互联网发布的相关安全资讯、漏洞等信息进行收集，形成安全通告编写素材。

2.在发生严重安全漏洞并有可能对智慧交通发展中心的网站及业务系统等造成影响时，我公司在掌握漏洞的第一时间编写并发布紧急安全通告。发布内容要包括漏洞描述、影响范围、处理建议三部分。

3.安全团队每周形成安全通告文档，并以邮件形式向智慧交通发展中心指定的邮箱进行发布。

4.智慧交通发展中心在收到安全通告后，可根据自身信息系统及其资产相关情况，自行评估安全通告中涉及的漏洞或事件，是否会对自身信息系统产生影响。

5.我公司提供远程电话、邮件，针对安全通告中涉及的内容进行解释，临时处置方案建议


网络和信息安全
报告服务
威胁信息收集
不涉及
中心是否涉及
涉及
判断是否高危
是
否
立即通告高危漏洞
定期安全通告
用户风险评估
提供技术支持
网络和信息安全
服务报告

（十一）网络设备维保

在发生硬件故障时，我公司确定故障情况，必须采取备件更换方式才可解决的情况下，首先通知智慧交通发展中心相关负责人。备件更换服务必须按不同的设备故障影响范围，我公司将根据用户的实际情况制定相应的备件快速响应流程，其中城区抵达现场的时间应不超过 1 个小时，郊区抵达现场的时间应不超过 4 个小时。

在系统正常运行期间，若属于设备自然损坏、老化等故障，或自然灾害与不可抗力(如雷击、 电压不稳等)引起的损坏，经北京市智慧交通发展中心(北京市机动车调控管理事务中心)及我公司双方技术人员现场检测确认后，则直接用备品备件替换，换回的损坏设备由我公司协助北京市智慧交通发展中心(北京市机动车调控管理事务中心)负责维修，修好后补充回备件库。

五、专业技术运维人员配备

项目经理—邓冬花

姓　名	邓冬花	性　别	女	出生日期	1993.11
在本项目中拟任职务		项目经理			
网络安全相关从业经验年限		7 年			
技术能力		具备丰富的网络安全与运维服务项目的实施与管理经验，能够熟练掌握并高效执行各项服务交付流程，包括但不限于漏洞扫描、基线核查、重保值守、攻防演练、风险评估以及渗透测试等多个环节。在实际工作中，能够根据项目需求制定详细的实施计划，确保各项服务按时、按质完成，同时具备应对突发事件的应急处理能力，保障网络安全服务的稳定性和可靠性。 拥有广泛的网络安全知识储备，对网络安全运营、数据安全、密码测评、等级保护等多个领域均有了解和实际操作经验。不仅熟悉各类网络安全产品和部分工具的使用，还能结合实际业务需求，提供网络安全解决方案，确保信息系统在各个环节的安全性和合规性。		
证书获取情况		CISP-CISE CISP-DSG CCSK	职　称	无	
主　要　经　历					
时　　间		参加过的网络安全相关项目名称		该项目中任职	
2021.9		菏泽人社数据中心建设及维保服务项目（2021）		项目经理	
2021.10		济南市人力资源社会保障智慧服务中心		项目经理	

2022.5	山东省药品监督管理局信息网络安全服务	项目经理
2023.10	集团公司网络安全团队值守及网络安全能力提升技术服务	咨询经理
2024.12.25	移动应用APP安全检测及加固	咨询经理
2024.12.30	北京市交通运行监测调度中心2025年网络安全运维服务合同	项目经理

特殊时期值守人员—李豪

姓　名	李豪	性　别	男	出生日期	2001.07.06
在本项目中拟任职务	特殊时期值守人员（高级工程师）				
网络安全相关从业经验年限	5				
技术能力	熟悉《网络安全法》《数据安全法》《个人信息保护法》等国家法律法规，了解网络安全等级保护2.0等相关国家技术标准； 具备丰富的网络安全运维服务经验，多次参与政府/金融/环境等多个网络安全项目，并担任项目经理，负责驻场服务管理和实施工作，对网络安全运维项目相关服务实施和交付流程熟练把控。				

	具备全栈渗透测试能力，精通 Web 安全领域中 OWASP 漏洞的挖掘与利用，熟悉二进制漏洞剖析、域渗透突破以及云安全。 熟悉常见攻击技术及防御手段，具备安全日志及网络流量协议分析能力，拥有木马、病毒、后门等方面的分析技能。 具备应急响应与溯源反制能力，可对各类网络攻击事件进行研判分析，还原攻击路径，实现溯源与反制。 熟悉主流品牌的网络设备(如华为、 H3C、锐捷等)网络设备厂商的安装、配置、调试及运维。		
证书获取情况	CISP（注册信息安全专业人员） CCSK(云计算安全认证) 信息安全工程师（信息技术应用创新考试评价证书）	职　称	无
主　要　经　历			
时　　间	参加过的网络安全相关项目名称	该项目中任职	
2019.9-2020.10	中国环境监测总站网络安全运维项目	项目经理	
2020.10-2022.2	泰康养老保险集团网络安全运维项目	高级工程师	
2022.5-2022.8	文化和旅游部网络安全实战化攻防演练项目	高级工程师	

2022.10-2025.7	北京市政务云（太极）安全技术服务运维项目	高级工程师

项目驻场工程师—庞宇

姓　名	庞宇	性　别	男	出生日期	1999.10.10
在本项目中拟任职务	项目驻场工程师				
网络安全相关从业经验年限	5				
技术能力	熟悉《网络安全法》《数据安全法》《个人信息保护法》《密码法》和《关键信息基础设施安全保护条例》等国家法律法规；熟悉网络安全等级保护 2.0、商用密码应用安全保护等相关国家技术标准； 拥有丰富的网络安全运维服务经验，具备网络安全等级保护、数据安全、商用密码应用安全方案的规划能力，同时具备网络建设方案规划以及网络与安全设备的运维能力。 持有 CISP（注册信息安全专业人员）、HCIE-Security（华为认证 ICT 专家-安全方向）、CCSK（云安全知识认证）、信息安全工程师（信息技术应用创新考试评价证书）、HCIP-Datacom（华为认证 ICT 专家-数据通信方向）认证证书。			
证书获取情况	CISP HCIE-Security CCSK 信息安全工程师（信创）		职　称	无	

	HCIP-Datacom		
主 要 经 历			
时 间	参加过的网络安全相关项目名称	该项目中任职	
2023.11	2023 年北京市交通领域节能减排统计与监测平台建设（二期）运维(第四包：机房环境及网络安全）	技术支持工程师	
2024.1	北京市交通安全应急指挥中心搬迁项目（副中心）	项目经理	
2024.3	北京市交通委员会行政审批系统商用密码应用安全性评估测评服务项目	技术支持工程师	
2024.12	北京市交通运行监测调度中心 2025 年网络安全运维服务项目	技术支持工程师	
、 2025.3	北京市交通运行监测调度中心 2025 年网络安全等级保护技术服务项目	项目经理	
2025.4	北京市交通行业数据中心风险评估及测评安全服务项目	项目经理	

项目驻场工程师—张皓

姓　名	张皓	性　别	男	出生日期	1996.7.5
在本项目中拟任职务		项目驻场工程师			
网络安全相关从业经验年限		9年			
技术能力		多年网络安全从业经历，具备安全服务项目实施和管理经验。多次参与策划和管理北京市区县级网络安全攻防演练项目，参与1年国护主防，3年国护协防。主导部委和监管行业客户项目服务。多个北京市监管行业和国家部委级单位项目实施与管理经验，在安全运维、应急响应及项目管理方面有自己的见解和经验。			
证书获取情况		CCSK 信息安全工程师（信创）		职　称	
主　要　经　历					
时　　间		参加过的网络安全相关项目名称		该项目中任职	
2019.3		区卫健委信息系统安全等级保护建设项目		项目经理	
2020.5		区卫生健康委员会网络安全保障项目		项目经理	
2021.12		北京市通信管理局应急演练服务项目		项目经理	
2022.6		人社部安全服务项目		项目经理	
2024.5		北京市交通委员会大兴公路分局网络安全服务项目		项目经理	

项目驻场工程师—贾驰昊

姓　名	贾驰昊	性　别	男	出生日期	2002.5.12
在本项目中拟任职务		项目驻场工程师			
网络安全相关从业经验年限		2			
技术能力		持有信息安全工程师（信息技术应用创新考试评价证书）证书，具备网络设备、安全设备运维能力。			
证书获取情况		信息安全工程师（信息技术应用创新考试评价证书）		职　称	无
主　要　经　历					
时　　间		参加过的网络安全相关项目名称		该项目中任职	
2023.11		2023年北京市交通领域节能减排统计与监测平台建设（二期）运维(第四包：机房环境及网络安全）		驻场工程师	
2024.12		北京市交通运行监测调度中心2025年网络安全运维服务项目		驻场工程师	

六、设备运维服务清单

网络设备清单

序号	设备名称	设备品牌	设备型号	单位	数量
1	楼层汇聚交换机	H3C	LS-9505E	台	1
2	交通委楼层接入交换机	H3C	LS-5500-52C	台	23
3	考试中心机房交换机	H3C	H3C 5500	台	1

七、运维外包服务费清单

序号	分项名称	单价(元)	数量	合价（元）	备注/说明
1	脆弱性检测	20000	4	80000	服务频率：4次/年
2	安全加固	20000	4	80000	服务频率：4次/年
3	网站安全检测	5000	20	100000	全年20个网站
4	信息安全应急响应	100000	1	100000	全年
5	应急演练	57000	1	57000	服务频率：1次/年
6	安全驻场服务	420000	1	420000	在服务期内持续提供：派驻3名安全工程师
7	特殊时期值守	45000	1	45000	按需开展，提供7*24现场值守服务，派驻1名高级工程师
8	网络设备巡检	1500	12	18000	服务频率：12次/年
9	设备配置管理	1500	12	18000	服务频率：12次/年
10	网络和信息安全报告	1000	52	52000	服务频率：1次/周，共52次
11	网络设备维保	62000	1	62000	1年
总价（元）				1,032,000.00	自合同签订之日起一年

附件2　服务质量考核标准

一、考核原则

本着“以甲方为中心，质量至上，公平合理”原则。

二、考核方式

1.半年考核

●满意度调查

●统计系统的性能参数达标情况。统计参数如下：

（1）响应时间

（2）处理时间

（3）故障率

2、年度考核

●满意度调查

●统计系统的性能参数达标情况。统计参数如下：

（1）响应时间

（2）处理时间

（3）故障率

三、考核内容与标准

1.人员管理

检查乙方是否按合同要求的服务内容及服务周期，组建稳定、专业、独立的服务团队，专门负责本项目的安全服务工作。派遣专业安全工程师完成各项服务。

服务实施过程中出现的问题是否有相应的人员在规定的时间内进行响应，并提出有效的解决方案

乙方应急事件响应小组是否在遇到需要现场解决的故障和事件时，派遣专人到达现场，并进行处理。

2.服务质量

（1）响应时间

乙方要提供包括电话、传真、邮件和网络方式的7*24小时响应服务，并且接受到请求后10分钟内做出响应。

（2）处理时间

要有快速响应流程，高端技术人员随时参与响应现场要求，如果 2 个小时内不能定位问题时，乙方需派出高端咨询师以最短时间抵达客户现场。危机发生时，在最短的时间内调集全公司的技术力量来协同响应。

（3）安全保密

包括当事人各方情报和资料保密义务的内容、期限和泄露技术秘密应承担的责任。

（4）客户满意度

客户满意度>=95%，分别从以下指标考核客户满意度：

产品质量

服务态度

维修效率

技术支持

（5）故障率

保证故障率远远小于甲方原来的故障率

（6）绩效加分

如果客户满意度>=95%，投诉率是 0，考核表是优，并使得客户的系统到达到了顾客的满意程度，会给与绩效加分。

3.其他

（1）乙方应及时响应甲方现场发生的故障和事件，若乙方未能及时响应并处理相关问题，影响甲方工作时，甲方有权聘请第三方予以处理，因此发生的费用由乙方承担，并且乙方应当赔偿甲方因此遭受的损失。

（2）乙方自行负担其工作人员在甲方指定地点工作的通告费、餐饮费。

乙方的工作人员应遵守甲方的规章制度，不得利用为甲方提供服务的便利条件，从事危害甲方信息系统安全、侵犯甲方财产利益及声誉的行为。

附件3　安全保密协议

甲　　方：北京市智慧交通发展中心（北京市机动车调控管理事务中心）

住　　所：北京市通州区通济路 8 号北投大厦

法定代表人：王炯

乙　　方：　北京云椤网安信息技术有限公司

住　　所：北京市通州区西集镇企业发展服务中心 4103 号

法定代表人：马翔宇

在 “北京市智慧交通发展中心网络系统与网络安全”项目运维过程中，乙方已经或将要知悉甲方的相关保密信息。为了保护上述合作中涉及的保密信息，明确双方的权利义务，甲、乙双方在平等自愿、协商一致的基础上达成以下协议：

一、安全要求

1. 乙方在甲方现场或甲方指定地点工作时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。

2. 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。

3. 如乙方人员在甲方指定地点工作时发生人身财产损害，由乙方负责承担责任，甲方对此不承担任何责任。

4. 如乙方人员在甲方指定地点工作时给甲方或者第三方造成人身财产损害，乙方及乙方人员应当负责及时承担赔偿责任。

二、保密信息范围

本协议所称的“保密信息”是指，乙方在本合同履行过程中获得的下列信息：

1. 工作秘密：一切与甲方及甲方关联单位有关的信息资料或其他性质的资料，包括但不限于：政府业务数据、人员机构信息、财务资料等；

2. 技术秘密：包括但不限于甲方的计算机信息系统、网络架构、信息安全体系结构、软件、数据库系统、系统数据、文档及技术指标等；

3. 其他保密信息：包括但不限于运维过程中获取的有关数据、流程、分析成

果；甲方的内部管理资料、财务资料、人员资料；甲方其他项目的信息及有关政府行政机关规划、调整等尚未公开的资料。

上述保密信息的表现形式不限，无论是书面的、口头的、图形的或其他任何形式的信息。

三、安全保密期限

无论在主合同履行期限内还是主合同终止后，乙方均应遵守本协议约定的保密义务。本协议项下约定的保密义务持续有效，直至相应信息成为社会公众可通过公开途径查询到的信息为止，并不随着主合同被认定为无效、撤销、解除或终止而免除。

四、保密义务人

本协议项下保密义务人为乙方单位及乙方可能涉及保密信息的员工。

五、保密义务

（一）乙方保证对所获悉的甲方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，应至少采取适用于对自己的保密信息同样的保护措施和审慎程度进行保密：

1．仅将本协议项下保密信息使用于与运维工作有关的用途。

2．除直接参与运维工作的人员之外，不得将保密信息透露给其他无关人员或任何第三方。

3．不能将甲方保密信息的全部或部分进行发布、传播、复制或仿造。

4．乙方应告知并以适当的方式要求其直接参与运维工作的人员，按照本协议规定保守保密信息。如乙方工作人员违反本协议约定，泄露甲方保密信息的，乙方应承担违约责任。

5．乙方不能利用获悉信息为自己或其他方开发信息、技术和产品，或与甲方的产品进行竞争。

（二）乙方的其他保密义务

1．未经甲方事先书面许可并采取加密措施，不得擅自将载有保密信息的任何文档、图纸、资料、磁盘、胶片等介质，带离甲方工作场所。

2．对于用户数据和服务结果数据的保管、访问，乙方无关人员不能访问；必需访问的人员，乙方要进行严格的访问控制；管理用户数据的人员应由乙方严

格筛选。

3. 对于甲方提供给乙方使用的任何资源，如网络、NOTES 等，乙方都只能将其用于主合同项下的工作，而不能用于其他目的。

六、保密信息的交回

1. 运维工作终止后，乙方应按照甲方的要求对相关保密信息做相应处理，比如销毁或其他处理方式。

2. 当甲方以书面形式要求乙方交回保密信息时，乙方应当立即交回所有的书面或其他有形的保密信息以及所有描述和概括保密信息的文件。

3. 未经甲方事先书面许可，乙方不得丢弃和自行处理保密信息。

七、违约责任

乙方未履行本协议项下的任一条款均视为违约，应按照甲方要求采取有效的补救措施，以防止泄密范围继续扩大，同时还应按照主合同约定承担违约责任。

八、争议的解决

因履行本合同而发生的或与本合同有关的一切争议，双方应协商解决，协商不成的，任何一方均可向主合同签订地有管辖权的人民法院提起诉讼。

九、其他

1. 本协议未尽事宜，甲、乙双方另行签订书面补充协议。

2. 本协议一式肆份，甲、乙双方各执贰份，具有同等法律效力。

3. 本协议自甲、乙双方法定代表人或者授权代表签字并加盖公章或合同专用章之日起生效。

甲方：（盖章）北京市智慧交通发展中心（北京市机动车调控管理事务中心）

法定代表人：（签字）

或授权代表：

乙方：（盖章）北京云楔网安信息技术有限公司

法定代表人：（签字）

或授权代表：

签订时间：2015.6.12

签订地点：北京市通州区