网络安全专业化服务第2包：网络安全保障及监控服务合同

甲方：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心

乙方：北京安信天行科技有限公司

北京市科学技术委员会、中关村科技园区管理委员会
综合事务中心

甲方：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心

法定代表人：崔彦民

地址：北京市通州区运河东大街57号院

联系电话：55578031

乙方：北京安信天行科技有限公司

法定代表人：翟建军

地址：北京市海淀区北四环西路68号10层1001号

联系电话：58045858

根据《中华人民共和国民法典》等法律法规的有关规定，结合《市科委、中关村管委会综合事务中心信息化运维管理规定》要求，就网络安全专业化服务第2包：网络安全保障及监控项目，甲乙双方友好协商，达成一致，签订本服务合同，以资共同遵守。

一、服务内容

乙方为和甲方签订的网络安全专业化服务项目—第2包：网络安全保障及监控项目提供如下安全服务（参照招标技术需求及投标响应文件）：

该项目技术服务内容包括安全风险识别与处置、安全监控预警与防护、安全保障与支撑等服务内容。具体内容如下：

1.安全风险识别与处置服务。安全风险识别与处置服务服务内容，包括安全基线检查及处置、脆弱性检测及处置、WEB远程安全性测试及处置、弱口令检查、木马查杀、数据安全检查、数据安全评估等工作。

2.安全监控预警与防护服务。安全监控预警与防护服务内容，包括网络安全态势感知服务和安全防护服务工作，其中网络安全态势感知服务涉及网络安全态

势感知、网络流量回溯及分析、安全态势预警通告服务、威胁分析服务、互联网网站域名监控服务、本地高级可持续威胁及研判服务、OA 展示服务等工作；安全防护服务涉及网页防篡改服务、主机日志管理服务等工作。

3. 安全保障与支撑。安全保障与支撑服务内容，包括应急保障服务（攻防对抗应急演练及预案、安全事件应急响应）、重要时期信息安全保障、软件正版化检查协助等工作。

二、服务期限

自签订合同之日起一年。

三、服务费用

1. 服务费用：人民币：叁佰捌拾柒万叁仟元（大写：3,873,000.00），即《中标通知书》中确认的金额。该费用为乙方完成本合同项下工作的全部费用，除本合同另有约定外，甲方无需向乙方支付任何其他费用。如市财政资金未能及时到位，乙方保证不影响合同执行，且不追究甲方延迟付款的责任。

资金支付条件及时间：

合同签订后三十个工作日内乙方向甲方提供合同金额 80%的增值税普通发票，甲方收到发票后十个工作日内向乙方支付合同金额的 80%，即¥3,098,400.00 元（大写：叁佰零玖万捌仟肆佰元整）。

年底前，乙方向甲方提交已完成工作的总结报告和服务成果，提供合同金额 20%的增值税普通发票，甲方收到发票后十个工作日内向乙方支付合同尾款。即¥774,600.00 元（大写：柒拾柒万肆仟陆佰元整）。

2. 乙方指定收款账户信息如下：

开户名称：北京安信天行科技有限公司

开户银行：北京银行双清苑支行

银行账号：0109 0327 8001 2010 2315 974

乙方保证上述信息真实、准确。乙方的上述账户信息发生变化的，应在发生变化后三日内书面通知甲方，否则由此导致的错付、无法支付等所有法律后果均由乙方自行承担。

甲方开票信息如下：

单位名称：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心

纳税人识别号：12110000MB1M157146

地址电话：北京市通州区宏安街 9 号

开户行及账号：招商银行北京通州分行 110949251810588

四、甲方权利义务

1. 掌握项目执行进度，监督乙方完成工作的权利。

2. 按照约定支付报酬的义务。

3. 为乙方履行义务提供必要的协助或便利的义务。

4. 甲方负责主导技术需求，有权对乙方工作提出意见和建议，乙方应在甲方要求的时间内按照甲方的建议和意见进行整改，甲方有权进行验收。

5. 根据市科委、中关村管委会综合事务中心信息化运维管理规定，甲方有权对乙方工作开展绩效考核，并进行考核结果通知。如发生严重违反合作原则、伤害甲方利益、影响服务质量等行为，甲方有权随时提出人员撤换要求。

6. 甲方有权对乙方参与本项目的核心人员的确定和变更进行审查。

五、乙方权利义务

1. 根据甲方需求处理项目工作的义务。特殊情况下乙方不限于在服务期限内协助甲方处理项目工作，经甲方确认后符合约定要求的工作成果给予经费支持。

2. 亲自处理项目工作的义务，未经甲方书面同意，不得将本合同项下全部或部分工作转包、分包给任何第三方。

3. 处理项目工作事务应尽忠诚与勤勉义务。

4. 按照甲方要求报告项目工作处理情况的义务。

5. 处理项目工作取得的成果与利益转交给甲方的义务。

6. 处理项目工作时接受甲方监督的义务。乙方应按照甲方要求对工作成果进行补充、修改，直至通过甲方验收，工期不予顺延，否则，乙方应承担延期交付的违约责任。

7. 乙方保证其人员具备完成本合同项下工作所需的相应资格和能力，并保证服务期限内乙方人员的稳定性，未经甲方事先同意，乙方不得更换本项目中的工作人员。乙方人员的工作能力及表现不符合本合同约定和甲方要求的，甲方有权要求乙方在甲方指定的期限内更换。

8. 在履行本合同义务时，乙方应采取相应措施保证乙方人员的人身、财产安全。因乙方未采取适当保护措施而造成人身或财产损害的，由乙方承担相应责任和费用。

9. 乙方保证在履行本合同过程中，不得侵犯任何第三方的合法权益，否则乙方应负责解决由此产生的一切纠纷，承担相应法律责任，并赔偿甲方因此遭受的所有损失。

10. 如有需要，乙方应配合甲方进行项目费用审计等工作，接受甲方或其委托的第三方机构及有关部门的监督检查和绩效评价等工作。

11. 特殊情况下乙方不限于在服务期限内协助甲方处理项目工作，经甲方确认后符合约定要求的工作成果给予经费支持。

12. 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给其他任何第三方。

13. 乙方在服务的全过程，应始终坚持正确的政治导向、价值导向、舆论导向，不得违背国家方针政策。

14. 自本合同服务期满至下一年度服务商进驻之前，乙方应继续做好合同项下各项服务直至新服务商进驻，并配合做好与新服务商的交接。

六、项目管理人员及技术人员要求

1. 项目管理人员

双方各指派代表作为本项目负责人，项目职责人职责范围包括：网络安全保障及监控安全服务。

甲方项目负责人：陈龙；联系方式：010-55578029。

乙方项目负责人：司晓宾；联系方式:17732589591。

2. 项目技术人员

乙方需根据项目要求安排具备相应资质的专业技术人员，并确保项目实施团队的稳定（项目技术人员名单作为附件附后）。项目实施过程中，乙方如因正当理由需要调整项目技术人员的，驻场人员应当提前一个月通知甲方（非驻场人员需提前一周），由乙方做好岗前培训并组织岗前考核，做好人员交接，交接单经甲方确认后执行，更换人员不得影响正常工作开展。

七、成果验收条款

1. 验收时间及主体：乙方完成全部工作并向甲方提出验收申请后 10 日后由甲方组织验收。

2. 考核指标：（参照招标技术需求及投标响应文件）

详见附件 4：信息化绩效考核指标及评分标准

3. 验收标准：

（1）完成全部合同约定的技术服务内容；

（2）提交齐备的验收材料；

（3）提交项目审计报告；

（4）提交信息化绩效考核结果；

（5）通过专家验收会。

4.验收方法：甲、乙方共同参与验收，验收完成后由甲方出具书面的验收报告或在验收清单上签字。

5.验收结果：经甲方验收，乙方全部履行本合同约定的义务且提供的技术服务完全满足采购文件中的技术服务需求，视为验收合格。若乙方未完全通过验收，甲方有权视情况追回已拨付费用并要求乙方赔偿相应损失，同时甲方可视情况按绩效考核等级标准追回相应已拨付费用，根据《市科委、中关村管委会综合事务中心信息化运维管理规定》的考核等级退回尾款的 20%、40%、60%。

八、知识产权条款

1.乙方处理项目工作形成工作成果的知识产权归甲方所有。

2.乙方保证其向甲方提供的服务属于自有合法权利，不存在任何侵犯第三方著作权、商标权、专利权等合法权益的情形。任何第三方以本合同项下的成果侵权为由向甲方主张权利的，乙方应按照甲方要求处理，赔偿因此给甲方造成的全部损失，并按照合同的有关约定承担违约赔偿责任。

3.乙方不得侵犯甲方对服务成果的知识产权，否则应赔偿给甲方造成的一切经济损失及承担全部法律责任。

4.本合同因履行完毕、解除或不可抗力等原因导致终止的，自终止之日起三十日内，乙方应将甲方提供的所有信息和资料以及乙方的阶段性成果移交甲方，并且不得继续以任何目的、任何形式使用或擅自许可任何第三方使用，亦不得向任何第三方泄露。

九、保密条款

1.乙方及其人员对于工作过程中接触到的有关信息及本合同各阶段形成的工作成果等不为公知的信息严格保密，不得泄露给第三方，不得用于本合同外的其他目的。此保密条款持续有效，不因本合同的终止而终止。

2. 乙方保证不向承担本合同项下工作人员以外的其他人员披露本合同项下的保密信息。乙方应告知并采取必要的有效措施保证其参与本项目之人员无论是在职中或离职后都能够履行本合同项下的保密义务。若乙方人员违反本条规定，乙方应对本方侵权人承担连带责任。

3. 本合同解除或者终止时，乙方应当立即停止使用甲方提供的一切相关资料，同时应当按照甲方的要求，将资料给予返还或销毁。

十、合同变更或解除

经甲、乙双方协商一致，可以变更或解除本合同。对本合同的变更或解除必须以书面协议进行。双方未签署书面变更或解除协议的，应认定为没有对本合同进行变更或解除。

十一、违约责任

1. 乙方若未履行或未完全履行本合同约定，甲方有权要求乙方继续履行、采取补救措施并赔偿损失。

2. 若乙方不按照本合同约定履行义务或提供的服务及工作成果未通过甲方验收，甲方有权解除本合同，视情况追回已拨付费用并要求乙方赔偿相应损失。乙方提供服务无法实现合同目的的，甲方有权解除合同，视情况追回已拨付费用并要求乙方赔偿相应损失。

3. 乙方未按照本合同约定的时间交付阶段性/最终工作成果，每延期交付一日，乙方应向甲方支付合同总金额 1%的违约金，延期交付超过 30 日，甲方有权解除合同并要求乙方支付合同总金额 30%的违约金。

4. 乙方未经甲方批准，擅自将事项全部或部分转委托给其他人实施的，甲方有权解除合同，并要求乙方支付合同总金额 10%的违约金。由此造成的经济损失由乙方承担。

5. 如违约金不足以弥补甲方因此遭受的经济损失，包括甲方为签约付出的

合理费用以及在合同履行后可以获得的利益（包括但不限于实际损失、预期损失和甲方为此支付的律师费、交通费和差旅费等），则乙方还应承担赔偿责任。

十二、不可抗力

1.因不可抗力导致本合同不能全部或部分履行，双方互不承担违约责任，但一方迟延履行合同的除外。

2.在不可抗力发生后，发生不可抗力一方应及时通知另一方，并在合理时间内提供相关部门证明，同时采取积极措施避免损失的扩大。

十三、解决争议的方法

1.凡与本合同有关的争议，双方应协商解决。

2.协商不成或协商不能解决，任何一方均应向甲方所在地有管辖权的人民法院提起诉讼。

3.诉讼进行过程中，除双方有争议的部分外，本合同其他部分仍然有效，各方应继续履行。

十四、其他事项

1.本合同一式陆份，甲乙双方各执贰份，招标代理机构执贰份具有同等法律效力。

2.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。

3.本合同未尽事宜，甲乙双方可另行协商签订补充协议。补充协议与本合同具有同等的法律效力。补充协议与本合同有冲突的，以补充协议为准。

4.下列材料构成本合同不可分割部分，与本合同具有同等法律效力：

（1）中标通知书

（2）招标文件

（3）投标文件

5.本合同附件构成本合同不可分割的部分，与本合同具有同等的法律效力。

附件 1：网络安全保障及监控项目保密协议

----------以下无正文，供各方签署----------

甲方：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心（盖章）

代表人：_____（签字）

日期：2024.6.3

乙方：北京安信天行科技有限公司（盖章）

代表人：_____（签字）

日期：2024.6.3

附件1

网络安全专业化服务项目第2包：网络安全保障及监控项目

保密协议

甲方：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心

乙方：北京安信天行科技有限公司

由于乙方与甲方签订了网络安全专业化服务项目第2包:网络安全保障及监控项目，并承担相关的网络安全保障及监控工作，在实施过程中可能涉及国家秘密、工作秘密（相关内部敏感信息），为了维护国家利益和双方的合法权益，明确保密责任和义务，根据国家的有关法律、法规，甲、乙双方本着自愿、公平、诚实信用的原则，订立本保密协议。

一、保密信息的内容和范围

（一）项目实施过程中涉及到的工作秘密包括但不限于以下内容：

1、任何涉及甲方的实施计划、规章制度、操作规程、处理手段、财务信息；

2、甲方向乙方提供的所有信息和资料，包括：系统需求、计算机设施的配置、网络结构、数据库结构、业务流程、业务软件，及其文件和数据，信息资源、安全保密技术措施、技术路线、数据资源、研究成果等等。

3、双方就该项目进行合作的重要商务文件、业务函电等。

4、双方依照法律规定或者有关协议的约定，对外承担保密义务的事项。

（二）双方如对国家秘密和工作秘密的界定有异议，则申请由市科委、中关村管委会保密主管部门认定，或由市科委、中关村管委会保密主管部门向上级单位申请处理。

二、保密期限

甲、乙双方确认的保密期限为各项秘密被其合法拥有者公开时止：

1、严格遵守国家秘密的保密期限。

2、工作秘密的保密期限由甲方确定，本项目为项目期间及项目验收后2年。

三、保密责任和义务

（一）甲、乙双方其他保密责任和义务：

1、甲、乙双方明确保密责任和义务责任人。

2、在项目规划、研发、建设过程中，甲乙双方均应承担对国家秘密、工作秘密的保密责任，如发现保密内容因自身的过失泄露或被对方泄露，应当采取有效措施防止泄密的进一步扩大，并及时向主管部门报告，否则应承担由此引起的一切法律和纪律责任。

（二）乙方应当承担的保密责任和义务：

1、乙方对于从甲方处获得的国家秘密和工作秘密，在未经甲方事先书面允可的情况下，不得以任何方式提供给合同之外的第三方，不得以任何方式对保密信息进行任何形式的改动。

2、未经甲方的书面同意，不得查询、复制、下载、传播系统中的业务数据，不得向任何第三方泄露甲方的保密内容；未经甲方的书面同意，不得允许或协助任何第三方使用本协议所述的保密内容。

3、不利用工作之便在甲方办公室查阅国家秘密和工作秘密，不利用工程建设机会了解、泄露甲方的其他涉密及内部情况。

4、不泄露甲方的内部管理制度、安全保密制度、安全保卫制度。

5、乙方应严格保证，所收到的信息在乙方企业内部能得到谨慎的使用，只能透露给乙方企业内部参与该项目的雇员，并且该雇员在知晓保密信息之前已经充分了解了本协议的内容。该雇员如不在乙方继续工作，当其泄露保密信息时，仍应由乙方承担责任。

6、在未经甲方事先书面允许的情况下，乙方不得使用甲方取得的经验、材料、产品以及其他甲方所有的信息，作为案例、模型或其他任何形式的材料，在

任何场合演示和推广。

7、乙方不能利用甲方保密信息为自己或第三方进行信息、技术和产品等开发，项目所产生的研究成果仅在市科委、中关村管委会系统内使用，不得以商业目的对外传播。

四、违约责任

1、如乙方未履行本协议项下的任一条款均视为违约，乙方应停止违约行为，并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。

2、任何保密信息的泄漏或任何其它违反本协议的行为给甲方造成损失，乙方应向甲方支付合同金额30%的违约金，或赔偿包括但不限于甲方所受直接损失、丧失相关权利的损失、调查违约行为而支出的费用及仲裁费、律师费等，违约金和损失赔偿以高者为准；情节严重的，可以依法追究乙方及相关人员的法律责任。

五、争议的解决办法

因项目执行过程中发生纠纷的，可以由双方协商解决，或双方共同信任委托的第三方调解，经协商无法解决争议时，可以向甲方所在地的人民法院提起诉讼，通过法律程序予以解决。

六、特殊条款

无。

七、协议的效力和变更

本协议一式贰份，双方各持壹份，具有同等法律效力。

本协议自双方签字盖章后生效。

本协议如有未尽事宜，甲方可以根据工作需要对保密内容、范围、期限、乙方责任和义务等进行修改和补充，乙方须同意遵守并履行。

----------以下无正文，供各方签署----------

甲方：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心（盖章）

代表人：_____（签字）

日期：2024.6.3

乙方：北京安信天行科技有限公司（盖章）

代表人：_____（签字）

日期：2024.6.3

附件2

个人保密协议

甲方：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心

乙方：司晓宾　　性别：男

身份证号：130523199804020819　　住址：北京市通州区中仓街道富力运河十号 B01 号楼 3 单元 722

甲方与乙方于2024年 6月3 日就网络安全专业化服务—第 2 包：网络安全保障及监控项目达成协议并签署了《保密协议》。乙方承诺对在该项目中获悉的市科委、中关村管委会的内部工作秘密信息承担如下保密义务：

一、保密内容

本协议所涉及的工作秘密，包括：市科委、中关村管委会计算机信息系统中的数据和信息，市科委、中关村管委会的内部业务内容，市科委、中关村管委会提供的所有书面资料，其他经市科委、中关村管委会确定应当保密的事项。具体内容如下表所示：

级别		内容
工作秘密	非常敏感的信息	■ 应用系统业务数据、备份数据； ■ 各类身份鉴别信息等。
	比较敏感的信息	■ 资产清单； ■ 网络拓扑图、VLan 划分及 IP 地址分配情况、网络设备与安全设备配置策略； ■ 应用系统配置、程序源代码； ■ 系统运行日志； ■ 安全性评估报告； ■ 市科委、中关村管委会的红头文件、资料信息等。

	最小敏感性信息	项目相关文档：包括合同、协议、可行性研究报告、需求规格说明书、工程实施方案、测试验收报告、操作手册、培训资料、运维工作记录、工作总结报告、主要会议记录等。

二、保密义务

1. 乙方在市科委、中关村管委会工作期间，必须遵守市科委、中关村管委会制定的《信息系统网络安全管理办法》《介质管理规定》《口令管理制度》等各项安全管理制度，保守市科委、中关村管委会的保密信息，不损害市科委、中关村管委会利益和不以市科委、中关村管委会保密信息谋取私利。市科委、中关村管委会安全管理制度没有规定的，乙方应本着谨慎、诚实的态度，采取任何必要、合理的措施，维护其知悉或者持有的保密信息。

2. 乙方承诺对在该项目过程中接触到的涉及市科委、中关村管委会工作秘密的资料、文件、数据等承担保密义务。

3. 乙方承诺只在该项目需要时使用上述工作秘密。

4. 乙方承诺在该项目过程中不去刺探或者以其他不正当手段获取市科委、中关村管委会的工作秘密。

5. 乙方承诺不将市科委、中关村管委会的工作秘密泄漏、告知、公布、发布、出版、传授、转让给任何第三方或以其他任何方式予以披露。

6. 乙方承诺在没有获得市科委、中关村管委会事先书面同意之前，不得在任何时候以任何形式为本项目以外的目的使用工作秘密。

7. 乙方因该项目需要所持有或保管的一切记录着上述工作秘密的文件、资料、报告、信件、传真、磁带、磁盘以及其他任何形式的载体，须在市科委、中关村管委会要求下的任何时候予以交还；未经市科委、中关村管委会授权，乙方不得留有这些文件的复制文件。

8. 乙方如发现上述工作秘密被泄露或者因自己过失泄露，应当采取有效措

施防止工作秘密进一步扩散，并及时告知市科委、中关村管委会。

9. 乙方保证，项目完成后仍对其在该项目期间接触、知悉的属于市科委、中关村管委会的工作秘密承担与项目期间相同的保密义务。

10. 乙方保证，离职之后仍对其在该项目期间接触、知悉的属于市科委、中关村管委会的工作秘密承担与任职期间相同的保密义务，而无论乙方因何种原因离职。

三、保密期限

甲、乙双方确认，双方的保密义务从本协议签署之日起生效。保密义务不受本合同终止或届满之影响。如果本协议所列保密内容因甲乙方之外的其他人员泄漏，乙方不承担泄密责任，但仍继续承担保密义务。

四、违约责任

乙方如违反本协议规定的保密义务，给甲方造成了损失，甲方有权向乙方追偿（包括但不限于直接损失、间接损失、甲方因此支出的调查费、律师费、诉讼费等），并保留追究乙方其他责任的权利。

五、争议的解决

因本保密协议产生的任何纠纷应向甲方所在地人民法院提起诉讼。

六、其他

乙方确认，在签署本协议前已仔细审阅过协议的内容，并完全了解协议各条款的法律含义。

本协议自双方签字盖章之日起生效。本协议一式二份，甲乙双方各执一份，具有同等法律效力。

甲方：北京市科学技术委员会、中关村科技园区管理委员会综合事务中心　乙方：

日期：2024年 6月 3日　　日期：2024年 6 月 3日

附件3

项目主要人员名单

序号	姓名	学历	职称	职务	项目角色	承担工作	服务类型
1	司晓宾	本科	PMP 证书	项目经理	安全项目经理	统筹项目整体工作	驻场服务
2	武天祺	本科	无	项目成员	项目成员	安全监控预警与防护服务	驻场服务
3	邹鹏	本科	CISP 证书	项目成员	项目成员	安全保障与支撑	驻场服务
4	王永亮	本科	CISP	项目成员	项目成员	数据安全评估等	二线支持
5	戴群	本科	CISP-PTE	项目成员	项目成员	WEB 远程安全性测试及处置等	二线支持

附件4

信息化绩效考核指标及评分标准

考核分类	考核事项	考核内容	考核标准	考核说明
日常管理	人员管理	驻场人员出勤管理	迟到早退每人次扣 0.5 分， 每月病事假超过 3 天的，每增加 1 天，每人次扣 0.5 分， 无故离岗、串岗、闲聊、大声喧哗每人次扣 0.5 分， 旷工每人次扣 2 分。	比规定到岗时间晚 1 小时以内算迟到 比规定离岗时间早 1 小时以内算早退 比规定到岗时间晚 1 小时以上算旷工 比规定离岗时间早 1 小时以上算旷工 闲聊、大声喧哗以被其他部门投诉为准
		驻场人员变动管理	人员变动未及时沟通每次扣 0.5 分 岗位空缺，每天扣 0.5 分	人员变动提前 1 个月提交申请
		人员着装	每人次扣 0.5 分	工作日着装正式，仪表整洁，不可穿拖鞋、背心、吊带装，男生不可染非黑色发
	运维规范管理	运维制度执行	运维操作不按制度执行，每次扣 0.5 分	是否按照相关制度执行相关规范
		执行完成率	工作任务未完成、未反馈的，每次扣 0.5 分	是否按时完成相关制度、规范及领导交办的任务
	文档管理	文档完整性	不完整每缺失一项扣 0.5 分	考核文档内容是否与要求内容一致，无缺项。每缺失 1 项扣 0.5 分。
		文档准确性	不准确每次扣 0.5 分	1. 考核文档中相关数据的准确性，发现

				与实际不符为不准确，每发生一次扣0.5分；2.文档中错别字，错别字每5个扣0.5分，不足5个按5个算。
		文档及时性	不及时每次扣0.5分	考核文档是否及时提交，周报为每周1个工作日内提交，月报为每月第一周3个工作日内提交，季报、半年报为每季度或每半年第一周5个工作日内提交；故障报告或事件记录报告为故障解除完成后3个工作日内提交；其他报告双方共同约定合理时间。
		分类保管	未分类扣0.5分	
	资产管理	规范落实	不规范扣0.5分	是否按相关要求执行
		资产盘点完成情况	未完成扣0.5分	是否按相关要求执行，对未明确保管的资产不做考核
		资产损失	每损失一件，扣1分	人为原因造成资产的损坏，损失，除赔偿外，考核需扣分
		资产表更新及时性	每发现一次扣0.5分	确认的变更是否在一周内及时更新
重点保障	应急保障	重要保障	可用性90%-99%扣0.5分 低于90%扣1分 考核期内达到100%加0.5分	可用性=正常运行时长/总使用时长 非可控因素造成的中断时长不计入考核 会议保障参考会议相关制度扣分
		一般保障	可用性80%--90%扣0.5分， 低于80%扣1分， 考核期内达到100%加0.5分。	

		较大故障	每次扣 20-30 分	由于运维人员失误，影响重大进程，造成不良影响，导致中心领导、处室处级领导点名批评的。
		重大故障	每次扣 40-50 分	由于运维人员失误，造成重大工作无法进行，重大会议无法召开，委领导以上点名批评的。
	特殊时段保障	制定保障计划	没有计划扣 1 分	是否制定
		事故数	每出现一次人为事故扣 1 分， 保障时期内未出现事故加 1 分。	
		发现隐患	发现隐患并及时汇报处理并解决，加 1 分	日常应发现的隐患不可加分，每个考核期最多加 5 分
应急响应及处置	巡检情况	巡检完成情况	每漏检一次，扣 0.5 分	
	巡检质量	巡检反馈及时性	发现运维范围内问题后，未在 15 分钟内反馈的，扣 0.5 分	巡检结果当日反馈
		主动发现问题并反馈	发现运维范围外问题，加 0.5 分	发现问题当日反馈
	服务响应管理	来电未接、需求未响应	每次扣 0.5 分	通过查询通话记录、微信语音记录
	工作成果考核	派工及时性	不及时扣 0.5 分	驻场人员收到相关咨询或问题，无法处理的，超过半小时未反馈或分配给二线技术支持的，需扣分
	应急预案管	制定应急	没有预案扣 1 分	

	理	预案		
		制定演练计划，按计划演练	没有计划或有计划不演练扣 1 分	是否有演练计划和报告
	应急事件处置	应急响应情况	不响应扣 1 分， 响应不及时扣 0.5 分， 考核周期内，无扣分项，加 1 分。	是否符合专项应急预案分级规范
		应急处置时间	未完成、无反馈扣 1 分， 未能在规定时间内完成扣 0.5 分， 规定时间内完成不扣分。	是否符专项应急预案分级规范
		应急处置意见建议	每被采纳加 1 分	事件处置中是否口头或书面提出建设性意见，对事件解决的效率或效果产生直接的正面影响。
	故障处置情况	响应时间	超时扣 0.5 分	是否符合故障处置分级规范
		故障处置时间	超时扣 0.5 分	是否符合故障处置分级规范
		意见建议	被采纳加 0.5 分	是否有利提高效率
信息系统可用性	信息系统可用性、故障率	信息系统可用性	可用性达到 99%加 1 分， 可用性 90%-99%扣 0.5 分， 可用低于 90% 扣 1 分。	可用性=（总体工作时间-故障时间）/总体工作时间

		信息系统故障率	考核周期内，云应用监管统计系统 4 级及以上故障数量， 数最少的排名前三名加 1 分， 第四名至故障率平均值不扣分， 不到平均值的，扣 0.5 分， 最后三名，加扣 0.5 分。 此外， 出现一级故障的，每次扣 10 分， 出现二级故障的，每次扣 5 分。	云应用监管平台统计各系统考核周期内故障数量，并进行排名
	网络、安全设备可用性	网络、安全设备可用性	可用性达到 99% 加 1 分， 可用性 90%-99% 扣 0.5 分， 可用低于 90% 扣 1 分。	网络可用性=（总体工作时间*总设备数-故障时间*故障设备数）/（总体工作时间*总设备数）
	云上主机效率	信息系统云效率	考核周期内，对信息系统政务云效率进行排名， 排名前三名加 5 分， 第四名至平均值不扣分， 不到平均值的，扣 1 分， 最后三名，扣 5 分。	
	终端设备可用性	终端设备维护后可用性	同一设备相同问题第一次维护后，每再产生一次扣 0.5 分。	

用户满意度	日常满意度	服务态度	重要人员投诉每次扣 1 分， 一般人员投诉每次扣 0.5 分， 重要人员表扬每次加 1 分， 一般人员表扬每次加 0.5 分。	重要人员：处级及以上领导 一般人员：其他工作人员
	整体满意度	信息系统责任部门及服务部门满意度	非常满意加 5 分， 满意加 1 分， 基本满意不加分， 不满意扣 5 分， 无满意度调查反馈的，扣 1 分。	以考核时满意度调查表打分情况统计

附件5：

网络安全专业化服务项目第 2 包：网络安全保障及监控项目实施方案

一、安全风险识别与处置服务

（一）安全基线检查及处置

（1）信息系统安全基线检查

通过完善安全基线内容，建立周期性安全基线检测机制，每季度对对市科委、中关村管委会信息系统涉及到的云主机操作系统数据库、中间件进行安全基线配置检查，及时发现信息系统运行风险。

（2）信息系统安全基线检查处置

根据安全检测工作结果，通过技术手段对信息系统相关的安全设备等进行安全策略加强、调优，加强操作系统、数据库和中间件抵御网络攻击和威胁的能力，整体提高网络安全防护水平；

针对安全基线检测阶段发现的脆弱点，进行安全风险分析，并针对各安全风险提出风险控制建议；

依据安全风险分析的结果和风险控制建议，由市科委、中关村管委会综合事务中心主导，信息安全运维服务商协助其他运维服务商对信息系统开展整改工作，指导其他运维服务商落实安全风险控制和安全加固优化措施，查验信息系统安全风险的整改控制情况，确保各项安全措施落实到位，保障信息系统的安全稳定运行。

（二）脆弱性检测及处置

（1）脆弱性检测

采用专业化检测工具（极光、天镜等）和人工分析的方式，对市科委、中关村管委会重要信息系统服务器操作系统、数据库、中间件等进行脆弱性检测，及

时广泛地了解设备脆弱性情况。

（2）脆弱性检测处置

针对脆弱性检测阶段发现的脆弱点，进行安全风险分析，并针对各安全风险提出风险控制建议；

依据安全风险分析的结果和风险控制建议，由市科委、中关村管委会综合中心主导，信息安全运维服务商协助其他运维服务商对信息系统开展整改工作，指导其他运维服务商落实安全风险控制和安全加固优化措施，并根据漏洞整改结果进行复测工作，查验信息系统安全风险的整改控制情况，确保各项安全措施落实到位，保障信息系统的安全稳定运行。

（三） WEB 远程安全性测试及处置

(1) WEB 远程安全性测试

采用 IBM Rational AppScan Standard Edition/WebRavor4.0/Netsparker 等工具和人工分析方式，对市科委、中关村管委会重要信息系统进行深层次受控的、非破坏性的 WEB 用远程安全性测试和分析，查找存在的安全隐患，检查发现问题，核查问题，配合整改问题，复查问题，并督促相关应用开发责任单位限期对漏洞进行整改，切实保证信息系统安全。

(2) WEB 远程安全性测试处置

针对 WEB 远程安全性测试阶段发现的脆弱点，进行安全风险分析，并针对各安全风险提出风险控制建议；

依据安全风险分析的结果和风险控制建议，由市科委、中关村管委会综合中心主导，信息安全运维服务商协助其他运维服务商对信息系统开展整改工作，指导其他运维服务商落实安全风险控制和安全加固优化措施，根据根据整改结果并进行复测检查工作，查验信息系统安全风险的整改控制情况，确保各项安全措施落实到位，保障信息系统的安全稳定运行。

（四）弱口令检查

采用人工检查形式，对信息系统口令复杂度、口令长度、管理后台访问方式等进行专项检查，对发现的不合规项进行分类统计，形成检测报告，并督促各运维单位在指定时间内完成不合规项整改工作，提升各信息系统安全系数。

弱口令检测技术是指通过一定的技术手段来检测用户账号和密码是否符合安全标准。 在网络攻击中，弱口令攻击是一种非常普遍的破解方式。 当用户使用弱口令时，黑客可以通源自文库暴力破解或字典攻击等方式获取用户的账号和密码，从而入侵用户设备，偷取敏感信息等。

（五）木马查杀

采用 D 盾 WebShell 专杀工具，针对信息系统各类文件中包含的 shell 语句进行深入检测，对发现的 shell 文件进行危险级别分类，并进行详细信息展示，准确定位危险点。

（六）数据安全检查

针对网信办、经信局等的数据安全检查，协助准备材料，对发现的问题协助进行整改，形成数据安全检查报告。

（七）数据安全评估

围绕关键业务系统，明确对应数据处理活动，基于合规要求，运用人工访谈、文档核查、技术工具等手段，根据数据资产梳理结果和已有安全防护措施，分析数据安全防护措施与国家相关标准规范的差距，识别安全风险以及风险等级，形成数据安全评估报告，并给出整改建议。

二、安全监控预警与防护

（一）网络安全态势感知服务

（1）网络安全态势感知

全面感知市科委、中关村管委会的网络安全状态、及时处置重大安全事件。

对安全隐患、安全事件进行通报预警。

由市科委、中关村管委会综合中心主导，信息安全运维服务商协助其他运维服务商对网络安全开展整改工作，指导其他运维服务商落实整改，查验整改控制情况，确保各项安全措施落实到位，保障信息系统的安全稳定运行。提升关键信息基础设施的安全防护能力。实现威胁与事件的通报预警，提升响应速度和应急处置效率。

（2）网络流量回溯及分析

通过对网络流量的捕获，可以对其进行 PCAP 级数据回溯分析，整体网络流量使用情况监测，异常网络行为预警，会话关系多维度展现，安全类故障问题分析，领导决策数据来源，多方责任界定等。

（3）网络安全态势预警通告服务

市科委、中关村管委会网络安全预警通报及安全月报工作机制，为了更及时掌握信息安全态势，每周一次有针对性地向委内提供安全漏洞信息、病毒信息等各种安全信息，并确保在第一时间内得到相关的网络安全信息，提高安全防范意识。并不断关注安全技术的发展和新的漏洞的出现，根据信息资产情况提供相应的安全信息通告，提高客户的安全防范意识。

（4）威胁情报分析

威胁情报分析：对客户关键操作系统进行定期扫描，扫描内容包括威胁 IP、威胁文件、威胁木马等；

高级持续性威胁感知：针对目标网络内流量进行深度分析，识别出网络流量中的攻击、病毒、木马等信息，并进行关联分析、展示；

综合安全关联分析：通过对安全巡检、日志分析、流量信息等功能进行数据的关联，从而分析出资产威胁现状。

针对威胁分析阶段发现的脆弱点，进行安全风险分析，并针对各安全风险提

出风险控制建议。

依据安全风险分析的结果和风险控制建议，由市科委、中关村管委会综合中心主导，信息安全运维服务商协助其他运维服务商对信息系统开展整改工作，指导其他运维服务商落实安全风险控制和安全加固优化措施，查验信息系统安全风险的整改控制情况，确保各项安全措施落实到位，保障信息系统的安全稳定运行。

（5）互联网网站域名监控

对市科委、中关村管委会重要信息系统开展安全监控工作，重点对外网门户网站等互联网系统进行 7*24 小时安全监控，通过网络安全监控、事件分析、事件预警、应急响应，确保门户网站等重要信息系统安全稳定运行。应能够检测到重要信息系统的可用性、网页篡改、网站挂马等安全风险。

由市科委、中关村管委会综合中心主导，信息安全运维服务商协助其他运维服务商对信息系统开展安全风险整改工作，指导其他运维服务商落实安全风险控制，查验信息系统安全风险的整改控制情况，确保各项安全措施落实到位，保障信息系统的安全稳定运行。

（6）本地高级可持续威胁及研判服务

针对惠裕大厦的各类网络安全攻击事件进行每日监测，并通过安全设备日志等信息对攻击行为进行分析，找到攻击者的源 IP 地址、攻击服务器 IP 地址、邮件地址等信息，并对攻击方法、攻击方式、攻击路径和工具等进行分析研判，对产生的日志进行实时分析，重大安全事件进行综合性研判、溯源、反制。利用安全防护设备如（APT 攻击监测系统）开展实时监测到的数据，对攻击行为进行确认，记录相关攻击数据，梳理主要攻击对象及攻击来源，结合分析结果，进行上报处置，充分保障楼体内网络稳定、持续、安全运行。

（7）OA 展示服务

OA 平台展示云上安全态势感知动态及分析研判服务。

（二）安全防护服务

（1）网页防篡改服务

保证系统平台完整性得到保护，对 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、电子文档、图片等任何类型的文件进行非法篡改和破坏，与现有安全防护软件可以纳入统一管理。

（2）主机日志管理服务

针对市科委、中关村管委会基于提供服务的业务系统，提供招标人登录、退出操作系统、应用系统分析服务，记录高危的招标人权限的变更行为，分析日志中的攻击行为，包括 SQL 注入、跨站脚本攻击等安全事件，保障信息系统平稳运行，所提供的软件能够纳入统一管理。

三、安全保障与支撑

（一）应急保障服务

（1）攻防对抗应急演练及预案

攻防对抗应急演练：根据应急预案规定的流程，协助市科委、中关村管委会进行信息系统应急演练工作，使各相关部门熟悉流程，提高对信息系统突发事件的响应能力。应对第三方进行的攻方攻击，验证我方作为防御方的安全防护能力。

协助完善和优化综合预案，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。在预案修订与完善的咨询服务过程中，将与招标人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）安全事件应急响应

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后，能够及时处理和恢复，保证网络与系统的正常运行。

（二）重要时期信息安全保障

在春节、北京两会、全国两会、五一、七一、国庆等重要时期之前，做好网络安全保障准备和检测工作，确保重要时期市科委、中关村管委会网络和信息系统安全稳定运行。提高网络安全事件防范和处置能力，提高网络安全保障水平。

（三）软件正版化检查协助

根据正版化相关工作要求，配合协助市科委、中关村管委会综合中心开展机关及直属单位软件正版化现场检查，协助进行软件正版化巡检工作，形成全委软件使用详细情况。

四、服务成果

服务期内各项安全服务内容全部完成，并提交相关成果和过程材料。具体如下：

1．完成 4 次信息系统安全基线检查及处置，提交 4 份《信息系统安全基线检查及处置报告》。

2．完成 4 次信息系统脆弱性检测及处置，提交 4 份《信息系统脆弱性检测及处置报告》。

3．完成 4 次信息系统 WEB 远程安全性测试及处置，提交 4 份《信息系统远程安全性测试授权书》、《信息系统远程安全性测试报告》。

4．完成 4 次信息系统弱口令检查，提交 4 份《信息系统账户安全检查表》。

5．完成 4 次信息系统木马查杀，提交 4 份《木马查杀记录》。

6．完成 1 次数据安全检查，提交 4 份《数据安全检查报告》。

7．完成 1 次数据安全评估，提交 5 份《数据安全评估报告》。

8．提供 7*24 小时网络安全态势感知服务，提交 12 份《网络安全态势月度分析报告》。

9．提供 7*24 小时网络流量回溯及分析，提交 12 份《网络流量分析服务报

告》。

10. 提供 7*24 小时网络安全态势预警通告服务，提交 12 份《信息系统安全预警通告》。

11. 提供 7*24 小时威胁情报分析，提供 12 份《网络威胁月度分析报告》和 1 份《年度安全分析及运营报告》。

12. 提供 7*24 小时互联网网站域名监控，提供 12 份《互联网信息系统安全监控报告》。

13. 提供 7*24 小时本地高级可持续威胁及研判服务，提供 12 份《本地高级可持续威胁报告》。

14. 提供 7*24 小时 OA 展示服务，提供 12 份《月度平台分析报告》。

15. 完成网页防篡改服务，按需提交《网页防篡改服务报告》。

16. 完成云主机日志管理服务，按需提交《云主机日志管理服务报告》。

17. 完成 4 次基础设施安全信息库，提交 4 份《基础设施安全配置信息库》。

18. 完成攻防对抗应急演练及预案，提交 2 份《信息系统应急演练工作总结》、《信息系统综合预案》。

19. 完成安全事件应急响应，按需提交《信息安全事件应急响应报告》。

20. 完成一年不少于 40 天的重要时期安全保障，提交 1 份《特殊时期安全保障方案》。

21. 完成 1 次正版化检查协助服务，提交 1 份《软件正版化资产清单》。

22. 电话、远程支持响应时间≤30 分钟，现场服务响应时间≤1 小时。