本合同为中小企业预留合同

政府采购合同

合同编号：BYH-2022-241

项目名称：信息系统运维类项目—
北运河闸站自动化监控系统信息化运维项目

采购人：北京市北运河管理处

供应商：北京大恒软件技术有限公司

签署日期：2022年 6 月27日

信息系统运维类项目—

北运河闸站自动化监控系统信息化运维项目

合同协议书

发包人（甲方）：北京市北运河管理处

承包人（乙方）：北京大恒软件技术有限公司

合同编号：BYH-2022-241

签订地点：北京通州

签订时间：2022 年 6 月 27 日

北京市北运河管理处为了进行信息系统运维类项目—北运河闸站自动化监控系统信息化运维项目（合同编号：BYH-2022-241），通过公开招标方式，确定北京大恒软件技术有限公司为该项目承包人。合同总价为人民币（大写）**壹拾玖万贰仟圆整**（小写） 192000.00 元。本着平等自愿原则，双方就下列问题达成一致协议，并于2022年 6 月 27 日签订本合同。

1、下列文件为本合同文件的组成部分，具有经济合同的法律效力：

（1）本合同书；

（2）中标通知书；

（3）采购需求；

（4）合同实施过程中双方共同签署的补充文件；

（5）招标文件及修改/补遗文件；

（6）投标文件及澄清文件；

（7）经双方确认的会议纪要及相关文件。

上述文件间有矛盾时，以日期在后的文件为准。

2、承包人保证按合同文件的一切规定提供相关服务，并承担合同文件规定承包人的全部义务和责任。

3、发包人保证按合同文件的规定付款，并承担合同文件规定发包人的全部义务和责任。

4、本合同书须经双方法定代表人或授权委托人签名、盖章，并提供履约保证金后生效。

5、本合同书一式 捌 份，甲方执 肆 份，乙方执 肆 份，具有同等法律效力。

6、本合同书在服务期限结束后合同款结清并完成理赔事宜后失效。

（本页无正文）

发包人：北京市北运河管理处（盖章）　　承包人：北京大恒软件技术有限公司（盖章）

法定代表人：＿＿＿＿＿＿（签章）　　法定代表人：＿＿＿＿＿＿（签章）

（或委托代理人）：＿＿＿＿＿＿　　（或委托代理人）：＿＿＿＿＿＿

联系人：＿＿＿＿＿＿　　联系人：邓峰

联系人电话：＿＿＿＿＿＿　　联系人电话：18600245418

邮　　编：＿＿＿＿＿＿　　邮　　编：100080

电　　话：＿＿＿＿＿＿　　电　　话：010-82828800

传　　真：＿＿＿＿＿＿　　传　　真：010-82827961

开户银行：＿＿＿＿＿＿　　开户银行：北京银行双榆树支行

帐　　号：＿＿＿＿＿＿　　帐　　号：0109 0321 0001 2010 9325 735

合 同 条 款

根据《中华人民共和国民法典》及相关法律法规的规定，甲乙双方在平等、自愿、协商一致的基础上达成如下协议：

一、维护对象

对杨洼闸、北关分洪枢纽、辛堡闸、榆林庄闸的通信系统、计算机网络及软件系统及北运河综合信息平台进行维护。

二、服务期限与服务地点

1.服务期限：2022 年 7 月 1 日至 2022 年 12 月 31 日。

2.服务地点：北京市。

三、服务内容和要求

详见采购需求。

四、维护确认与验收

1.维护人员

甲乙双方指派专人组成本合同维护项目的管理小组管理和实施本项目。双方可以根据具体情况更换本方管理小组的成员，但应当以书面方式通知另一方；如乙方重新指定的小组成员涉及到本项目的重要方面，应当事先通知甲方管理小组人员，并征得甲方的同意。双方应当在合理和维护双方利益的基础上讨论人员更换事宜。参与项目的所有人员都应当受本合同第八条各条款的约束。

2.维护确认

（1）重大维护内容发生后，乙方可以及时以书面方式提交甲方进行确认。提请对应用软件维护项目进行维护确认的，乙方还应当提交相应的软件维护文档，所提交的文档应当包括纸质版和电子版各一份。

（2）甲方应当在接到乙方书面材料的3个工作日内进行维护确认。如甲方无正当理由而不进行维护确认，则视为甲方已经确认。双方对此另有约定的除外。维护确认的内容包括系统故障现象、原因、故障排除过程、更换配件情况、恢复状况等。

3.验收详见附件1“履约验收方案”。

五、价格与付款方式

1.本维护项目总价为人民币（大写）**壹拾玖万贰仟圆整**（小写）192000.00元。

2.合同定价方式：固定单价。

3. 履约保证金

（1）履约保证金金额为合同价的 10%，即人民币大写壹万玖仟贰佰圆整（小写：19200.00）。

（2）履约保证金用于补偿甲方因乙方不能完成其合同义务而蒙受的损失。

（3）履约保证金采用下述方式第③方式提交：

①银行保函：由甲方可接受的在中华人民共和国注册和营业的银行出具，其格式采用发包人可接受的格式

②担保机构保函

③支票

④汇票

（4） 在乙方根据合同进行服务，合同终止之前，履约保证金将一直有效。若乙方未发生违约行为，且未给甲方造成任何损失，考核合格，约定延长服务期满且完成验收及档案移交工作后 30 个工作日内无息退还，如在退还履约保证金时发生银行费用，则将扣减银行费用后的余款退回。履约保证金采用支票、汇票形式的，以支票或汇票方式退还；采用保函形式的，合同期满自行作废，不再退还。

（5）因乙方原因导致合同无法部分或全部履行的，履约保证金将不予退还。

（6）甲方逾期退还履约保证金，按照中国人民银行的同期贷款利率按逾期天数计算并支付补偿金。

4. 付款方式

预付款：甲方于合同签订后 20 个工作日内向乙方支付合同价款的 50%作为预付款；

进度款：剩余项目款在预付款用尽后按照项目进度按月支付。

根据运行服务需要，在服务期中，甲方如有停止运行维护的项目，以合同单价按日平均为标准，按实际运维天数予以支付。

在实际支付时，如遇财政部门国库结账、北京市水务局文件调整等特殊要求，具体支付将根据财政部门、北京市水务局相关规定要求调整执行。

中标人在收到中标通知书后，并在签订合同前向采购人提交合同签约价10%的履约保证金。

六、义务与责任

1. 甲方

（1）甲方应当向乙方提供必要的工作条件，包括必要的技术资料、技术准备，协

助乙方做好维护服务。

（2）甲方应当保证其要求乙方维护的软件、硬件以及相关的文档未侵犯第三方知识产权。

（3）由项目管理小组成员依据本合同对乙方的工作进行检查。

2. 乙方

（1）乙方保证维护工作的过程未侵犯第三方合法权益。

（2）经乙方维护更新后的软件，其任何部分如被依法认定为侵犯第三方合法权利，或者任何由乙方授予的权利被认定为侵权，乙方应当承担相应的责任，并尽力用相等功能的合法软件替换该软件，或者取得相关授权，以使甲方能够继续享有本合同所规定的各项权利，并且乙方应当赔偿甲方由此而造成的损失。

（3）乙方所承担的维护项目的质量标准应当符合国家标准、行业标准或者制造企业的标准。若无国家标准、行业标准或者制造企业的标准的，以符合合同目的的其他标准作为质量标准。

（4）未经甲方同意，乙方不得将本合同项目的部分或者全部维护工作转包给第三方承担。

（5）运行维护工作过程中所更换设备及元器件单件设备 1000 元（含）以内的由乙方承担。

（6）乙方应认真执行项目管理单位发出的与合同有关的任何指示，按合同规定的内容和时间正常有序地开展开发工作和相关服务，完成本合同所约定的任务，并承担相应的责任。

七、所有权、知识产权和使用权

1. 所有权

本合同中所列硬件设备，不论维护前还是维护后，其所有权均归甲方所有。

2. 知识产权

合同中所列应用软件的知识产权归甲方所有，另一方非经对方同意，不得以任何方式向第三方披露、转让，除本项目维护需要外，不得以任何方式进行商业性利用。

3. 使用权

甲方拥有合同中所列产品软件的正版使用权，乙方仅可在与项目有关的维护工作中使用，任何情况下不得以复制或者其他方法供自己使用或者提供给第三方。

甲方使用乙方提供的第三方软件，应当依照乙方与第三方对该软件使用的约定进行。

乙方应当将该约定的书面文件的原件交甲方核对，复印件交甲方存档。

八、保密

1. 信息传递

在本合同的履行期内，任何一方可以获得与本项目相关的对方的保密信息，对此双方皆应谨慎接受并不得向第三方披露。

2. 信息披露

获取对方保密信息的一方仅可将该信息用于履行其在本合同项下的义务，且只能由相关的工程技术人员使用。获取对方保密信息的一方应当采取适当有效的方式保护所获取的信息，未经授权不得使用、传播或者公开。除非有对方的书面许可，或者该信息已被拥有方认为不再是保密信息，或者已在社会上公开，该信息在不得对外披露。

3. 保密措施

甲乙双方同意采取相应的安全措施，遵守和履行上述约定。经双方协商，一方可以检查对方所采取的安全措施是否符合上述约定。

4. 竞争限制

甲乙双方承诺，在本合同履行过程中以及本合同履行完毕后，双方均不得使用在履行本项目过程中得到的对方保密信息，从事与对方有竞争性的业务，也不得采取任何方式聘用本项目中的对方相关技术或者管理人员。

九、服务变更

1. 甲方如提出部分维护项目的变更建议，应当以书面形式提交给乙方。乙方应当3个工作日内，对该变更后合同价格、服务内容、系统性能、技术参数等可能发生的变化作出预估，并书面回复甲方。

2. 甲方在收到乙方回复后，应当在3个工作日内，以书面方式通知乙方是否接受乙方回复。如甲方接受乙方回复，则双方可对该变更以书面形式予以确认，并按变更后的约定继续履行本合同。

3. 乙方如提出部分维护项目的变更建议，应当对该变更后合同价格、服务内容、系统性能、技术参数等可能发生的变化作出预估，并以书面形式提交给甲方。

4. 甲方在收到乙方的变更建议后，应当在3个工作日内，以书面方式通知乙方是否接受乙方的变更建议。如甲方接受乙方的变更建议，则双方可对该变更以书面形式予以确认，并按变更后的约定继续履行本合同。如甲方不同意乙方的变更建议，则乙方应当按原合同执行，但由此产生的信息系统的风险以及其他相关风险由甲方承担。

十、不可抗力

1. 由于台风、水灾、火灾、地震等不可抗力因素，直接影响本合同的履行或者不能按照合同的约定履行时，可以免除遇有不可抗力的一方的相关合同责任。但遇有不可抗力的一方应当及时通知对方，并在7日之内提供不可抗力的详细情况及合同不能履行或者部分不能履行或者需要延期履行的理由和有效的证明文件。甲乙双方根据不可抗力因素对合同履行的影响程度，协商决定是否解除合同，或者部分免除履行合同的义务，或者延期履行合同。

2. 遇有不可抗力的一方，应当尽可能地采取必要的措施减轻不可抗力对本合同的履行所造成的影响。由于未采取适当措施致使另一方损失扩大的，不得就扩大损失的部分要求免除本方责任；由于未采取适当措施致使本方损失扩大的，也不得向对方要求赔偿。

十一、违约责任

1. 如乙方未按合同约定完成维护项目，除依照以下约定支付违约金外，甲方有权要求乙方赔偿损失。

（1）乙方在两周内不能做到熟悉项目内容，解决系统运行中发生的各种问题，甲方有权解除合同，选择能够胜任的运维单位。

（2）因乙方自身原因造成的工作延期，每延期1日，乙方应当向甲方支付合同总价0.3‰的违约金，但违约金的总数不超过合同总价的 10%；

（3）因乙方自身原因造成的工作延期，如延期超过10日或者延误维护确认3次，甲方有权解除合同，并要求乙方赔偿损失。

2. 任何一方违反合同约定的保密义务，违约方应当支付合同总价10%的违约金。如包括利润在内的实际损失超过违约金的，受损失一方有权要求对方赔偿超过部分。

3. 任何一方违反合同约定的知识产权保护条款，除立即停止违约行为外，还应当支付违约金 不超过合同总价的 10% 元。

4. 甲方未能按合同约定支付预付款或合同价款，乙方可向甲方发出通知，要求甲方采取有效措施纠正违约行为。甲方收到乙方通知后的28天内仍不履行合同义务，乙方有权暂停履行合同，并通知甲方，甲方每逾期一日按合同价款的0.5%向乙方支付违约金，但最多不超过合同总价款的 / %。甲方承担由此增加的费用和（或）服务期延误，并支付乙方合理利润。

5. 因甲方原因导致项目变更、中止的、终止合同的，乙方有权要求甲方赔偿相应损失。

6. 如发生违约事件，履约方要求违约方支付违约金时，应当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，应当于3日内答复对方，并支付违约金。

十二、争议解决

本合同发生争议的，由双方协商解决，也可按下列第2种方式解决。

1. 提交北京仲裁委员会仲裁。

2. 依法向通州区人民法院提起诉讼。

十三、合同的生效

1. 本合同经双方各自指定的代表签字并盖章后生效。

2. 本合同一经签署，未经双方同意，任何一方不得随意更改。本合同所列的附件经双方代表签字并盖章后成为本合同的组成部分。

3. 未尽事宜双方协商签订补充协议，补充协议与本合同具有同等法律效力。

4. 本合同书一式捌份，甲方执肆份，乙方执肆份，具有同等法律效力。

十四、名词解释

1. 维护

维护是指为保障信息系统的正常运行和使用，对其中软件、硬件等进行的检查、维修、备份以及改正错误、提高性能等相关工作。

2. 维护确认

维护确认是指甲方对乙方依照合同对维护工作内容进行确认的行为。

3. 业务应用系统

业务应用系统是指按甲方业务需求，由乙方或者第三方定制开发的计算机应用软件系统。

4. 产品软件

产品软件是指甲方向乙方或者第三方购置的成熟的商品化软件，包括操作系统、数据库、开发工具、中间件软件、安全软件、办公自动化软件、专业应用软件等。

5. 保密信息

保密信息是指甲乙双方各自所拥有的不为公众所知的管理信息、方式方法、产品信息、计算机源代码、技术文档和技术资料等，或者由甲乙双方在履行本合同过程中明确指明为保密的合法信息。

6. 规格

规格是指在技术或者有关维护服务任务上所设定的关于硬件和软件的技术标准、规范。

十五、其他

1. 如一方改变通讯地址，应当提前以书面方式通知另一方。

附件 1：履约验收方案

履约验收方案

一、履约验收主体：甲方。

二、验收方式：甲方有权委托第三方机构进行验收，对此乙方应当配合。

三、验收时间：维护项目按合同规定完成后，甲方应当及时进行验收。乙方应当以书面方式向甲方递交维护项目验收通知书，甲方在收到验收通知书后的 5 个工作日内，确定具体日期。

四、验收条件：1）完成项目实施方案和合同约定的各项内容；2）有完整的技术档案和管理资料。

五、验收程序：乙方按照合同约定，完成维护、配件更换、现场服务等项目的服务，同时提交完整的验收资料。甲方按照招标文件、投标文件要求完成验收，验收合格后双方签署验收书。如属于乙方原因致使维护项目未能通过验收，乙方应当排除故障，并自行承担相关费用，同时延长 1 个工作日，直至符合验收标准由乙方按要求弥补缺陷后再次组织验收，直至验收合格。如由于甲方的原因致使维护项目未能通过验收，甲方应当在 1 个工作日内排除故障，5 日内再次进行验收，直至验收合格。

六、验收内容及标准：

序号	验收内容	验收标准	备注
一	技术要求		
1	项目执行的标准和规范	项目实施过程中执行的标准和规范符合采购需求规定的各项标准和规范要求。	由甲方组织验收小组成员核查乙方提交的记录文件及其他验收资料，以及日常检查考核记录，验收小组成员全部认为符合要求后签认。
2	维护标准	维护标准及要求不得低于《计算机网络及通信设备运行管理规定(BYH-YXJC-12-2020)》和《网络信息系统运行管理办法（BYH-YXGL-39-2020）》相关要求。	
3	维护内容	项目维护实施要求符合采购需求。	
4	保障要求	项目保障要求符合采购需求。	
5	组织方案或解决方案	按承诺方案组织完成项目。	
二	商务要求		
1	项目实施期限	按合同约定期限。	
2	项目实施地点	北京市。	
3	合同价款支付	付款进度比例符合合同约定，付	

		款条件满足合同约定。	
4	备品备件包装材料环保要求	项目实施中备品备件涉及商品包装的，满足采购需求环保标准要求。	乙方提供商品包装材料环保检测报告，涉及重金属和VOCs检测的，需符合采购需求规定的检测方法。

附件 2：计算机网络及通信设备运行管理规定(BYH-YXJC-12-2020)

计算机网络及通讯设备运行管理规定
(BYH-YXJC-12-2020)

1 总则

为了加强计算机网络及通讯设备运行管理，保护网络系统的安全运行，保障全处各项工作的顺利进行，根据《中华人民共和国计算机信息系统安全保护办法》、《计算机信息网络国际联网安全保护管理办法》、《互联网安全保护技术措施规定》、《北京市信息化促进条例》和《信息安全技术网络安全等级保护基本要求》等相关法律规定，结合实际，制定本制度。

涉及有关固定资产管理和信息安全的内容执行处其他相关规章制度。

2 适用范围

本制度所称计算机网络及通讯设备是指：电脑软硬件，网络设备、服务器设备、操作系统和应用系统（如 OA、办公软件等）。

本制度适用于在管理处范围内使用计算机设备及网络的人员、监控室操作人员、信息网络及机房管理人员、计算机设备及网络代维人员。其中，“使用计算机设备及网络的人员”为各计算机及其它可接入网络设备的操作使用人员，以下简称“设备使用人员”；“监控室操作人员”为各单位自动化监控室的实际操作人员，简称“操作人员”；“信息网络及机房管理人员”为各相关单位指定的对所属信息网络设备及机房的负责人员，简称“管理人员”；“计算机设备及网络代维人员”为受委托对计算机网络和设备进行检修和维护的人员，简称“代维人员”。

3 职责与分工

3.1 工程科科负责全处信息网络及设备的统一管理，负责对管理处内各主要网络设备、计算机服务器、工控机等进行操作配置，计算机及其它网络设备（如无线路由等）加入我处信息网络网，必须由科教科安排接入网络，分配设备名称、IP 地址和使用权限，并记录归档，具体执行处《有线网络接入安全管理规定》、《无线网络接入安全管理规定》、《互联网使用管理规定》和《账号与口令使用安全规定规定》。

3.2 各基层单位应确定至少一名计算机信息网络管理人员。

4 管理内容和要求

4.1 设备使用人员要求

机房。

3）机房内物品应摆放有序，网线、电源线、数据线及设备等标签铺设整齐。

4）机房内禁止存放易燃、易爆、易腐蚀物品及强磁性物体，配备气体灭火器及做好防盗、防潮、防尘、防鼠咬、防静电、防雷击等措施。

5）机房内温度应控制在摄氏22±5℃；湿度应控制在45%~65%；温度变化率小于5℃/h，不得结露。

6）机房内所有设备系统要妥善保管和使用，机房内的电源插座、开关及有关设施固定使用，不得变更用途，不得随意接入其它设备，不得随意开关电源；增加设备时，要考虑电源负荷，机房内布信号线时，要尽可能远离电源线及避免并排敷设。

7）管理人员每天要对机房所有设备工作情况进行细致的检查，发现问题及时处理；下班时，要对所有设备的电源进行检查，该关的要切断电源，并检查门窗是否关好。

8）机房内所有设备系统要妥善保管、维护，不得随意操作、搬动、拆装、外借。

4.4 网络与信息管理

4.4.1 管理处网络接入具体执行处《有线网络接入安全管理规定》、《无线网络接入安全管理规定》、《互联网使用管理规定》和《账号与口令使用安全规定规定》。

1）管理处网络接入由处工程科统一规划。处机关由工程科负责执行，其他各基础单位自行管理本单位网络接入，处工程科提供统一规划及技术支持。

2）管理处网络接入需进行必要的身份鉴定，公用设备应明确当班管理人员，临时接入设备应记录设备所有者信息，信息记录应包含接入设备识别码及授权人信息。

3）由无线网络方式接入网络的应妥善保管接入账户及密码等信息，不得借予他人，如发现非授权接入应立即通知网络接入管理部门，变更登陆信息。

4）处工程科随时可因网络安全问题及其他上级部门要求关闭网络接入，当处工程科要求关闭网络接入时，所有部门应主动配合。

5）工程科有权对全处的互联网访问内容进行监管，对与业务不相关的网站

4.1.1 设备使用人员应遵循以下相关规定:

1）设备使用人员应负责该计算机及其附属设备的管理使用，严格落实计算机管理责任制，谁使用谁负责。

2）设备使用人员应熟知管理处信息网络管理相关规章制度，明确操作注意事项，确保计算机及其附属设备得到规范、合理使用;

3）设备使用人员负责所辖计算机及配套设备的日常使用、清洗、保养、管理工作，确保完好无损，并保持设备及其所在环境的清洁，出现故障及时上报处科教科，下班时，务必关机，切断电源。

4）设备使用人员必须使用由工程科设定的IP地址，未经许可，禁止更改设备IP地址、软硬件配置、参数（如：设备名称、组件等）。

5）设备使用人员须对个人上传至服务器（ftp）中的文件负责，并及时清理过期文件。

6）所有接入处信息网络的设备都应安装由公安部认证的杀毒软件或处统一部署的杀毒软件，并定期升级病毒库及杀毒引擎，保证设备及网络安全，具体执行处《防病毒安全管理规定》。

7）任何人员不得故意输入计算机病毒；不得向他人提供含有计算机病毒的文件、软件、媒体；对在互联网上接收到来历不明的电子邮件，不要打开其附件，防止受到计算机病毒的攻击；从互联网上直接下载的软件和浏览器插件要有可靠来源，因其可能有破坏性程序，必须对此严加防范；及时检测、清除计算机信息系统中的病毒，无法清除的，应当迅速采取隔离、控制措施，保护相关数据，并及时向处工程科汇报，等待专业人员处理。

8）终端设备上不安装和使用未经授权的软件。

4.1.2 设备使用人员接入互联网必须自觉遵守国家有关法规，不得泄露国家秘密；严禁上网流传、处理、储存涉密文件、资料、数据；严禁将与涉密文件、资料、数据相关的计算机、工控机联网运行。

4.1.3 设备使用人员不得利用互联网制作、复制、查阅和传播下列信息:

1）煽动抗拒、破坏宪法和法律、行政法规实施;

2）煽动颠覆国家政权，推翻社会主义制度;

3）煽动分裂国家、破坏国家统一;

4）煽动民族仇恨、民族歧视、破坏民族团结；

5）捏造或者歪曲事实，散布谣言，扰乱社会秩序；

6）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪；

7）公然侮辱他人或者捏造事实诽谤他人；

8）损害国家机关信誉的；

9）其他违反宪法和法律、行政法规和制度的。

4.1.4 设备使用人员不得从事下列危害信息网络安全的活动：

1）未经允许，进入计算机信息网络或者使用计算机信息网络资源；对计算机信息网络功能进行删除、修改或者增加；对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加。

2）故意制作、传播计算机病毒等破坏性程序；

3）其他危害信息网络安全的活动。

4.2 代维人员管理

处应与代维单位签订信息安全和保密有关协议，并监督代维人员遵守。

代维人员要及时排查硬件设备的故障，又要防范和减少故障，确保不影响业务系统影响。未经处相关人员许可，不得改变原有设备、软件平台及集成系统，运维管理和维修应保证全部资产的完整、安全并处于良好状态。必须服从处对网络与信息安全和保密的各项管理规定和要求，并严格执行处《服务器日常维护安全管理规定》、《网络安全设备管理规定》和《自动化系统故障处置管理规定》。

4.3 计算机及机房管理

4.3.1 监控室及专门设备操作人员应严格按照设备使用说明进行操作，发现问题及故障应逐级向所属单位领导及处工程科汇报，不得擅自对所属设备进行拆装、修改等操作，具体执行处《机房监控安全管理规定》和《终端设备管理规定》。

4.3.2 信息网络及机房管理应执行处《计算机房安全管理规定》、《服务器日常维护安全管理规定》和《网络安全设备管理规定》，管理人员须遵循以下规定：

1）管理人员要保证计算机软、硬件运行正常，满足工作需要。

2）管理人员负责机房的管理工作，保持室内清洁卫生，无关人员不得进入

（网购、视频等）进行一定程度的限制。

6）工程科负责对全处的网络带宽进行按需分配，对有线、无线网络的开放时间进行按需调整，以保证全处工作的高效运转。

4.4.2 管理处网络储存管理规定

1）处工程科统一管理处网络储存设备上的文件。

2）当文件过期或丧失价值时，文件上传人应主动清理。

3）处工程科定期检查处FTP的文件，对检查发现的有害信息可立刻清除，并向上级报告。

4）处工程科将定期对服务器里的文件进行筛查和清理工作。

5）任何要上传文件至FTP的文件必须先进行病毒检测，确保无毒后方可上传。

6）任何使用管理处网络的人员若发现有害信息应即时上报工程科。

4.4.3 与管理处业务相关的微信群、QQ群统一由工程科进行管理，群主需在工程科处登记备案，群成员必须严格遵守国家发布的《互联网群组信息服务管理规定》，并遵守以下内容：

1）在微信、QQ上发布信息应严格审核，未经审核的信息不得发布。

2）发布、转载有关信息必须遵守国家有关规定，涉密信息不得发布。

3）群交流必须遵守国家法律法规及相关网络信息管理规定，禁止出现不良政治倾向、色情、暴力等内容。

4）严格保守管理处秘密，对业务通报、群内信息、工作内容等敏感信息严禁转发给非相关人员。

5）交流中，禁止诋毁管理处各部门和员工形象，禁止出现有违社会公德、不文明、侮辱性及涉人身攻击性语言。

4.4.4 工程科协助相关部门做好舆情管控工作，在网络端准确把握、快速反应，做好突发事件的应急处理。

5 附则

5.1 本制度由工程部门负责解释。

5.2 本制度自发布之日起执行。

附件 3：网络信息系统运行管理办法(BYH-YXGL-39-2020)

网络信息系统运行管理办法
（BYH-YXGL-39-2020）

1 总则

1.1 为规范信息系统的运行维护与监控管理工作，明确网络安全管理人员职责、分工及问题的处理，确保信息系统的安全可靠运行，使信息系统更好的服务于工程运行管理，特制订本办法。

1.2 本办法适用于北京市北运河管理处管理范围内的所有办公设备、网络接入设备、信息系统等。外单位派遣人员或工作人员自有设备，如接入北运河管理处各级办公机构的网络系统内，同样受本办法管理。

2 引用文件

《中华人民共和国计算机信息系统安全保护办法》

《计算机信息网络国际联网安全保护管理办法》

《互联网安全保护技术措施规定》

《北京市信息化促进条例》

3 职责与分工

3.1 工程管理科负责信息化及办公自动化管理工作和办公电子设备的计划、管理工作。

3.2 处其他科室负责与其职责范围内信息系统的运行管理。

4 管理内容和方法

4.1 有线网络接入安全管理办法

4.1.1 角色与职责

（1）网络管理人员的职责：负责评估、制定与搭建本单位的网络环境。

（2)网络与信息安全工作小组的职责:负责审批与授权本单位的网络环境。

（3）网络使用人员的职责：遵守本办法。

4.1.2 网络接入安全管理流程

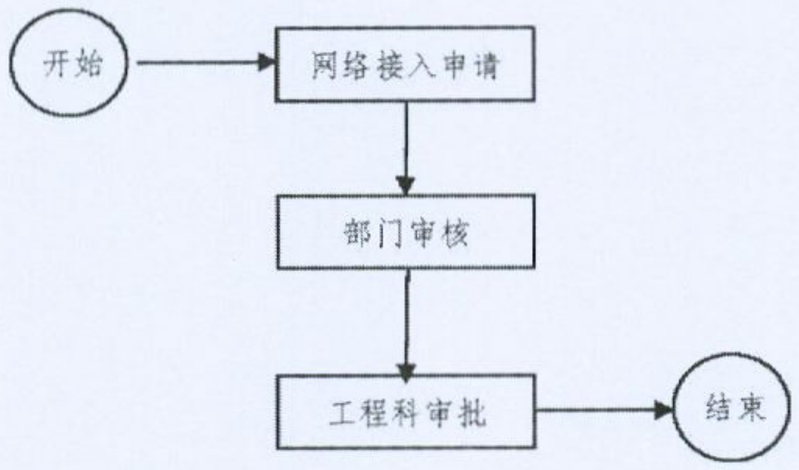


图 38-1 网络接入安全管理流程

4.1.3 有线网络使用管理规定

（1）网络办公环境，经工程管理科评估无敏感信息传输需求的情况下，由网络管理人员制定网络接入方案；网络接入方案由工程科审批，经审批与授权后，由工程管理科网络管理人员负责有线局域网络环境搭建；涉密计算机及涉密网络环境搭另行管理。

（2）有线网络（以太网）接入以设备识别码为主要技术手段，其他安全配置要求视具体网络接入权限而定。

（3）对于非本单位的访客访问无线局域网络，需要向相关科室负责人进行申请，申请后填写相关申请，送工程科审核实施；访客网络仅提供最小访问权限。

4.1.4 相关记录

《网络接入申请表》

表 39-1　网络接入申请表

编号:

申请人姓名		申请部门		申请日期	
申请类型	□职员接入　　□访客（访客担保人签字:　　）				
接入类型	□有线局域网网络接入		□无线网络接入* （*无线网接入全部带有互联网访问权限）		
	□有线互联网接入				
操作类型	□申请用户　　□用户权限变更　　□注销用户				
系统、设备名称					
接入设备识别码（MAC 地址）					
申请人承诺	未经授权不在网上发布我单位涉密信息。不通过网络查阅或发布黄色及反动内容。不利用网络从事违法、违规活动。不在连接网络的计算机上运行非法软件。从无线网上下载的任何信息资源，未经检测、查杀计算机病毒等处理不得使用。 承诺人签字:				
部门或科室负责人审批意见	签字:		日期:		
分配（变更、注销）的用户 ID					
信息化主管部门负责人审批意见	签字:		日期:		

4.2 无线网络使用安全管理办法

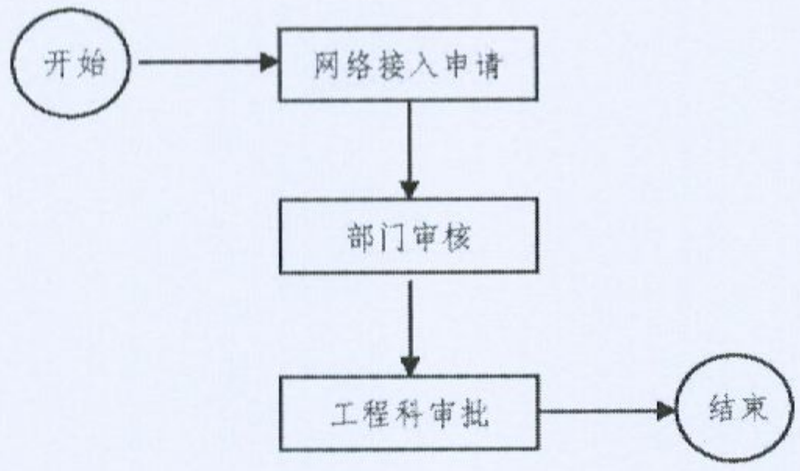
4.2.1 角色与职责

（1）网络管理人员的职责：负责评估、制定与搭建本单位的网络环境。

（2）网络与信息安全工作小组的职责：负责审批与授权本单位的网络环境。

（3）无线网使用人员的职责：遵守本规定。

4.2.2 无线网络安全管理流程



4.2.3 有线网络使用管理规定

（1）网络办公环境，经工程管理科评估无敏感信息传输需求的情况下，由网络管理人员制定网络方案；网络接入方案由工程科审批，经审批与授权后，由工程管理科网络管理人员提供账号密码和配置方式等信息；

（2）对于非本单位的访客访问无线局域网络，需要向相关科室负责人进行申请，审批与授权后方可访问网络，且只能开通必要访问权限；对于短期访客，可由部分负责人与工程科沟通后，获得临时授权方式，自行对访客进行授权并记录相关情况，无需填写《网络接入申请表》。

（3）无线网络账户及密码 应由本人保管，不得借与他人使用，发现异常情况应立刻联系工程科对账号进行冻结，详细要求参见《账号与口令使用安全管理规定》。

4.2.4 相关记录

《网络接入申请表》

表 39-2　网络接入申请表

编号:

申请人姓名		申请部门		申请日期	
申请类型	□职员接入　　□访客（访客担保人签字:　　）				
接入类型	□有线局域网网络接入 □有线互联网接入		□无线网络接入* （*无线网接入全部带有互联网访问权限）		
操作类型	□申请用户　　□用户权限变更　　□注销用户				
系统、设备名称					
接入设备识别码（MAC 地址）					
申请人承诺	未经授权不在网上发布我单位涉密信息。不通过网络查阅或发布黄色及反动内容。不利用网络从事违法、违规活动。不在连接网络的计算机上运行非法软件。从无线网上下载的任何信息资源，未经检测、查杀计算机病毒等处理不得使用。 承诺人签字:				
部门或科室负责人审批意见	签字:		日期:		
分配（变更、注销）的用户 ID					
信息化主管部门负责人审批意见	签字:		日期:		

4.3 互联网使用安全管理办法

4.3.1 角色与职责

（1）网络与信息安全工作小组的职责：负责制定本单位职工访问国际互联网的策略和管理规范；负责定期牵头组织对本单位职工上网行为进行监督、检查。

（2）科室负责人的职责：负责对本科室职工访问国际互联网申请进行审核。

（3）工程管理科的职责：负责对本单位职工访问国际互联网申请进行审核。

（4）互联网申请人的职责：遵守本办法。

4.3.2 互联网使用安全管理办法

（1）接入审查及身份认证管理

1）互联网申请人员均需填写书面的《网接入申请表》，经所在科室领导审核确认后，由申请人员提交至工程管理科；

2）工程管理科网络管理人员在接到《网接入申请表》后，对拟申请上网的计算机防病毒软件、操作系统补丁、网络资源的接入分配等进行审查，审查完毕提交工程管理科负责人审批同意后，实施网络接入工作；

3）工程管理科须建立本单位上网职工的管理台账，并由专人记录上网职工的姓名、所属科室、主机名称、设备地址（IP、MAC）、申请事由、联系方式等信息。

（2）访问互联网安全管理

1）职工访问国际互联网必须遵守国家法律、法规和北京市水务局互联网使用安全管理制度，严禁制作、复制、发布、传播下列信息：

① 违反宪法所确定的基本原则的；

② 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

③ 损害国家荣誉和利益的；

④ 煽动民族仇恨、民族歧视，破坏民族团结的；

⑤ 破坏国家宗教政策，宣扬邪教和封建迷信的；

⑥ 散布谣言，扰乱社会秩序，破坏社会稳定的；

⑦ 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

⑧ 侮辱或者诽谤他人，侵害他人合法权益的；

⑨ 含有法律、行政法规禁止的其他内容的。

2）上班时间仅允许使用单位内部许可的即时通讯工具，严禁以下行为：

① 严禁使用即时通讯工具传递敏感信息，存有涉密数据信息的介质，不得在接入国际互联网的计算机上使用；

② 严禁盗用他人 IP 地址，影响他人使用互联网；

③ 严禁对网络及联网计算机进行网络地址扫描或端口扫描、干扰网络正常运行；

④ 严禁使用可能影响单位网络正常运行的已经感染病毒的电脑；

⑤ 严禁将互联网上下载的任何信息资源，未经检测、查杀计算机病毒等在内部网络上使用；

⑥ 严禁在网络上私设服务器，提供代理、DHCP、Email、下载、P2P 等服务。

3）联网监督管理

① 应充分利用已部署的上网行为管理系统，对职工的上网内容进行记录和控制；

② 应指派专人负责维护网络防火墙及代理服务器，对互联网使用过程中存在的问题快速反应、及时解决，确保正常使用互联网；

③ 网络与信息安全工作小组负责定期牵头组织对本单位职工上网行为进行监督、检查，权限开通必须严格审核把关；

④ 工程管理科负责对职工上网情况进行动态监控，发现上网违规行为将提出通报并进行处罚。

4.3.3 相关记录

《网络接入申请表》

表 39-3　网络接入申请表

编号:

申请人姓名		申请部门		申请日期	
申请类型	□职员接入　　□访客（访客担保人签字:　　）				
接入类型	□有线局域网网络接入		□无线网络接入* （*无线网接入全部带有互联网访问权限）		
	□有线互联网接入				
操作类型	□申请用户　　□用户权限变更　　□注销用户				
系统、设备名称					
接入设备识别码（MAC地址）					
申请人承诺	未经授权不在网上发布我单位涉密信息。不通过网络查阅或发布黄色及反动内容。不利用网络从事违法、违规活动。不在连接网络的计算机上运行非法软件。从无线网上下载的任何信息资源，未经检测、查杀计算机病毒等处理不得使用。 承诺人签字:				
部门或科室负责人审批意见	签字:		日期:		
分配（变更、注销）的用户 ID					
信息化主管部门负责人审批意见	签字:		日期:		

4.4 账号与口令使用安全管理办法

4.4.1 角色与职责

1）系统管理人员的职责：负责对各系统中的用户进行开通、变更、撤销及复查等过程。

2）系统使用人员的职责：遵守本办法。

4.4.2 账号与口令使用安全管理流程

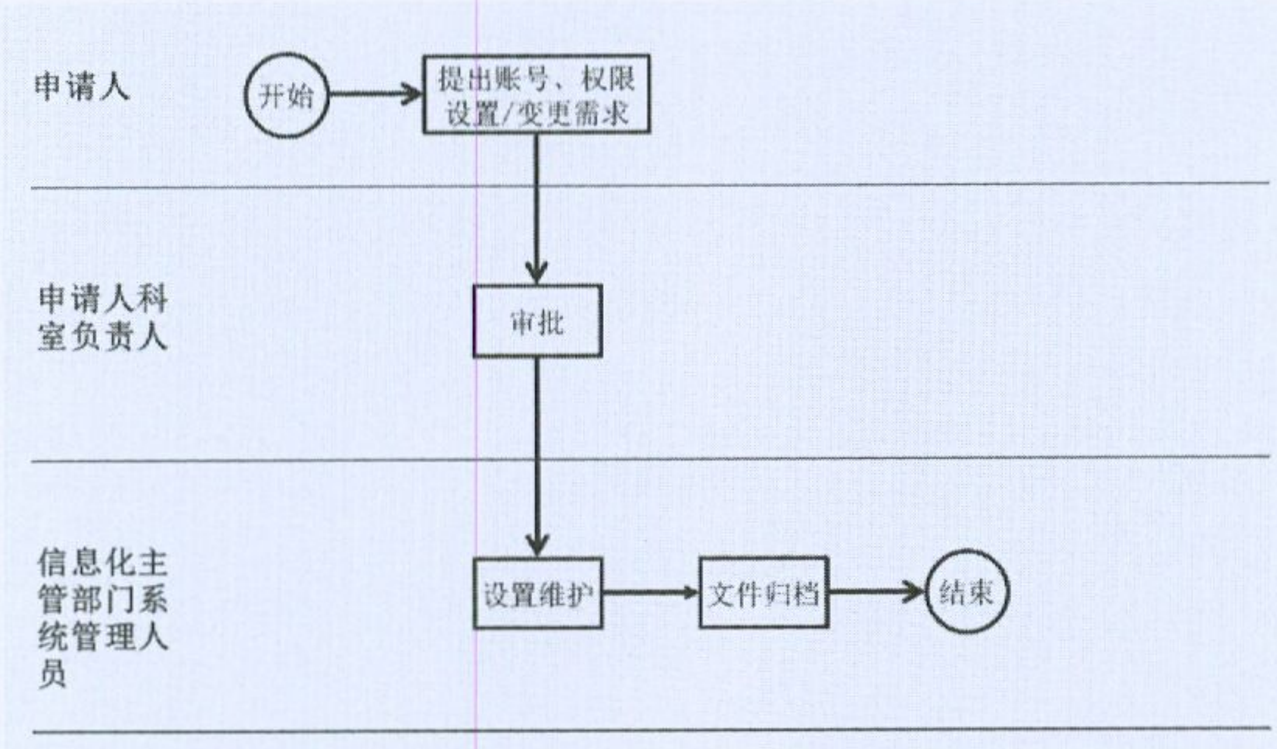


图 39-1 账号与口令使用安全管理流程

4.4.3 账号与口令使用安全管理办法

（1）账号权限申请

1）所有用户账号的开通应通过正式的账号申请审批过程，由账号使用者提出申请，并根据本单位审批流程进行审批。

2)非本单位内部人员需要使用账号时，应由内部人员作为担保人代为申请，担保人对其账号负责。

3）在对系统账号管理的过程中，应做到账号与拥有人一一对应，确保每个账号都有人负责，对于外部人员申请使用的系统账号，必须指定一名内部人员作为担保人。

4）在系统权限的申请过程中，须遵守最小授权原则，即只开通职工业务范围内所必须的账号及权限。

5）系统管理人员在开通账号前，应检查申请人是否在该系统中拥有其它账号，若没有，方可为用户创建账号并分配相应的权限。每个用户只能拥有唯一的账号，不得重复申请账号（特殊系统账号除外）。

（2）账号使用规则

1）用户在获得账号后，应当立即修改账户默认口令。

2）用户账号口令的选择和使用应当与口令保护策略相符合。

3）用户账号是用户的唯一标识，只能由本人使用，不得交由他人使用。

4）不得多人共用一个账号（特殊系统账号除外）。

5）服务器本地管理员账号由信息化主管部门系统管理人员保管，并禁用匿名账号（Guest 账号）。

（3）账号权限变更

1）在系统账号使用过程中，如果账号权限发生变化，应进行重新申请。如需要增加系统权限，在申请的过程中，应对增加权限的原因进行详细描述并由申请人员所在部门签字确认。

2）在进行系统权限的变更时，工程科系统管理人员应检查申请人员是否存有不再需要的其它账号或权限，如果存有不需要的账号或权限，应及时进行撤销。

3）在系统账号权限变更授权过程中，权限变更内容以及变更原因应由工程科系统管理员进行详细记录，以备以后查看。

（4）账号权限消除

当系统使用人员由于离职、调职等原因或临时访问人员不需要使用原有的账号或者权限时，应消除其系统账号权限。消除申请自人员离职日起 15 日内由使用人员所属部门负责人向系统管理部门递交，系统管理部门管理员审核确认相关变更后消除相关账号。

（5）口令保护策略

1）普通用户账号口令选取长度在 8 位以上，并且包含大小写字母、数字、特殊符号其中的两种以上。

2）特权用户账号口令选取长度在 10 位以上，并且包含大小写、数字、特殊符号其中的三种以上。

3）所有账户不得使用系统默认口令，不得使用账号创建时的初始口令，用

户首次使用账号时，应当立即更改默认口令。

4）用户不能将口令包含在任何自动登录程序上，不得将写有口令的纸条贴在显示器或者座位上。

5）用户要保护口令的保密性，不得多人共用口令；不允许在计算机系统上以无保护的形式存储口令。

6）信息化主管部门系统管理员应对特权账号的口令进行适当的保护，如为方便记忆将口令存储于电子文件中，应对文件进行加密操作，并以纸质形式存在，则需要密封。

7）用户只要发现任何表明口令或系统遭到滥用的迹象，应立即更改口令。

8）用户应当每三个月更换一次口令，要避免重复使用前两次使用的口令。

9）如果用户忘记口令，需要向系统管理员提出申请，由管理员确认后再进行重置默认口令。

10）对于泄漏口令而造成的损失，由用户本人负责。

4.4.4 相关记录

《用户权限设置/变更申请单》

《转岗检查单》

《IT 权限管理记录表》

表 39-4　用户权限设置变更申请单

编号:

申请人姓名		申请部门		申请日期	
操作类型	□申请用户　　□用户权限变更　　□注销用户				
系统、设备名称					
权限说明					
部门或科室负责人审批意见	签字:		日期:		
分配（变更、注销）的用户 ID					
信息化主管部门系统管理人员	签字:		日期:		

表 39-5　转岗检查单

转岗日期：　　检查日期：

<table>
<tr><td>姓名</td><td></td><td>现部门或科室</td><td colspan="2"></td></tr>
<tr><td>新部门或科室</td><td></td><td>职务</td><td colspan="2"></td></tr>
<tr><td>工作交接</td><td colspan="4">交接情况描述：

交接人：</td></tr>
<tr><td>部门确认</td><td colspan="3">现部门或科室主管负责人签字</td><td></td></tr>
<tr><td rowspan="4">系统管理部门</td><td>现所在部门或科室资源的归还：
归 还 □</td><td rowspan="4">责任人</td><td rowspan="4"></td></tr>
<tr><td>新部门或科室资源的申请：
已发放 □</td></tr>
<tr><td>现所在部门或科室系统权限的删除
注销 □</td></tr>
<tr><td>新部门或科室系统权限的申请
已注销 □</td></tr>
<tr><td>备注说明</td><td colspan="4"></td></tr>
<tr><td rowspan="2">部门确认</td><td colspan="2">新部门或科室主管负责人签字</td><td></td></tr>
<tr><td colspan="2">人事科相关人员签字</td><td></td></tr>
</table>

表 39-6　IT 权限管理记录表

序号	职工姓名	入职时间	部门或科室	岗位	内部系统			离职日期
					系统名称	用户名	权限描述	

4.5 终端设备管理办法

4.5.1 角色与职责

工程管理科的职责:

1）负责制定本单位统一的设备编码规则;

2）负责组织建立和管理本单位统一的终端设备台帐;

3）负责统计和更新本单位终端设备信息;

4）负责定期组织终端设备清查核对工作。

5）提出本单位终端配置规划和要求;

6）负责终端设备维护以及报废的技术鉴定工作;

7）定期组织对本单位终端设备的使用情况进行评估;

8）组织协调、监督检查本单位终端设备的使用及维护工作。

9）设备使用部门的职责:

10）负责监督保管本部门内的设备

11)负责确保本部门内设备处于可用状态，对即将发生问题的设备进行申报。

4.5.2 终端设备管理流程图

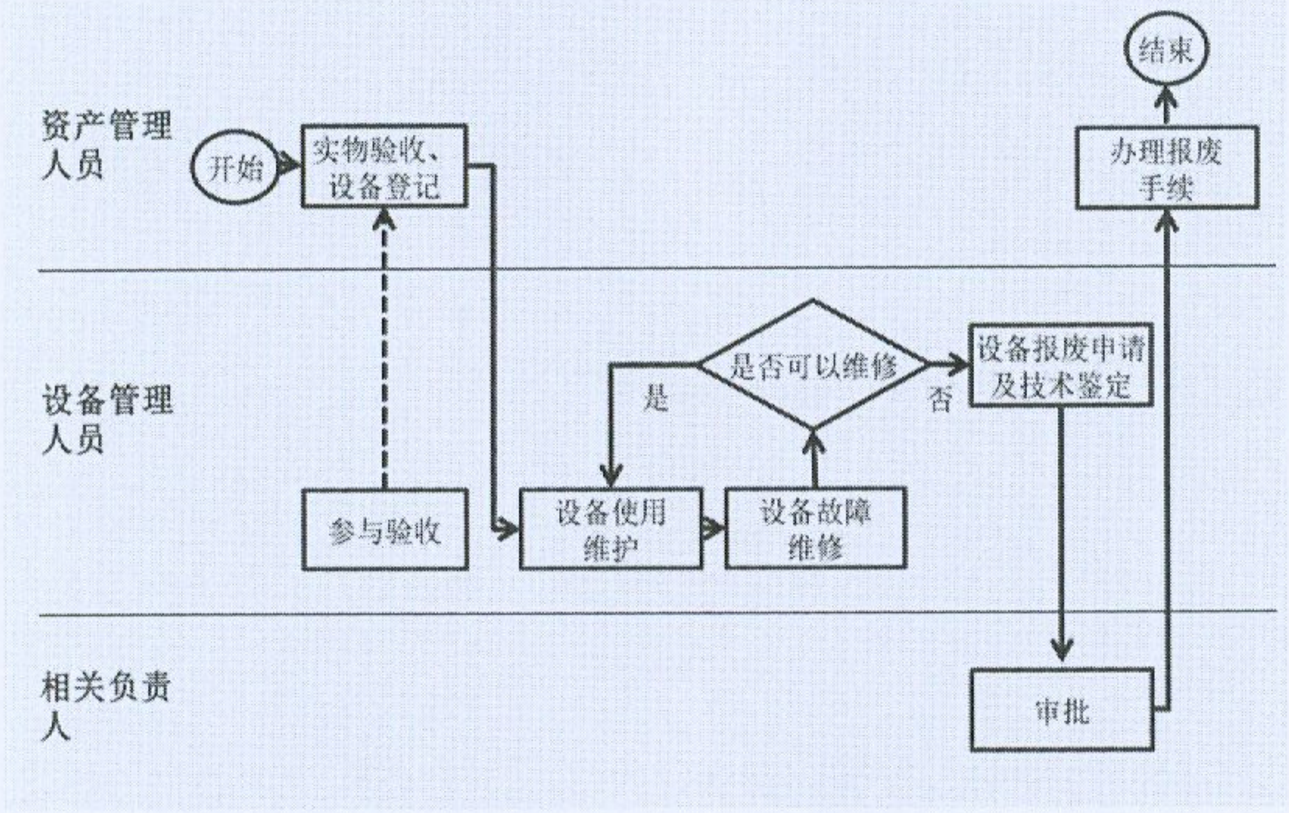


图 39-2 终端设备管理流程图

4.5.3 终端设备管理办法

（1）终端设备入库及配置管理

1）终端设备入库均须由本单位固定资产管理人员进行实物登记。

2）终端设备到货后由设备管理人员配合固定资产管理人员验收，并由固定资产管理人员办理固定资产编号、建卡、建账等工作。

3）如遇终端设备调拨、迁移等变化内容，应由本单位固定资产管理人员按设备台帐的要求，及时调整和更改有关终端设备信息。

4)设备原保管人如调整岗位的，设备处置由原保管人所在部门负责人负责，负责人应依处置结果填写《固定资产变更表》并主动上报工程科。对因退休等原因离职的，部分负责人应在员工离职前将《固定资产变更表》上报工程科。

（2）终端设备的使用及维护管理

1）终端设备领用时，固定资产管理人员应及时更新设备配置信息，所有在用的终端设备必须指定终端管理人员。

2）已经使用过的终端设备改作它用时，若涉及到保密信息，应由终端管理人员按照保密管理的有关办法妥善处理。

3）终端设备使用人员应爱护设备，做好防尘、防水、防磁、防震等工作。禁止在设备上运行违规程序，未经终端管理员允许不得随意更改系统和网络设置。

4）终端设备所涉及的系统软件应使用合法渠道获得的正版软件。

5）工程管理科终端管理人员负责本单位终端设备的维护工作，并建立严格的《设备故障维修登记表》。终端使用人员未经允许不得私自移交、交换、拆卸所使用终端。

4.5.4 相关记录

《固定资产验收移交单》

《设备故障维修登记表》

《单位固定资产处置申请表》

《固定资产变更表》

表 39-7　固定资产验收移交单

金额单位：元

<table>
<tr><td colspan="4">入帐单位:</td><td colspan="2">验收日期:</td><td></td></tr>
<tr><td>资产名称</td><td></td><td>规格型号</td><td></td><td colspan="2">计量单位</td><td></td></tr>
<tr><td>单价</td><td></td><td>数量</td><td></td><td colspan="2">总金额</td><td></td></tr>
<tr><td>生产厂家</td><td colspan="3"></td><td colspan="2">资产编号</td><td></td></tr>
<tr><td colspan="7">1、采购部门验收移交说明

采购负责人签字:</td></tr>
<tr><td colspan="7">2、使用部门实物使用人签收</td></tr>
<tr><td colspan="7">3、归口管理人员登记台帐后签字</td></tr>
<tr><td colspan="7">4、资料接收人签字</td></tr>
<tr><td colspan="3">（1）装箱单　　份</td><td colspan="4">（4）质量合格证　　份</td></tr>
<tr><td colspan="3">（2）保修卡　　份</td><td colspan="4">（5）其他</td></tr>
<tr><td colspan="3">（3）使用说明书　　份</td><td colspan="4"></td></tr>
<tr><td colspan="7">5、使用部门负责人签字</td></tr>
<tr><td colspan="7">6、财务部门登记台帐后签字</td></tr>
</table>

编制说明：

本表由采购部门负责填制，在经使用单位签收及登记台帐后，交财务部门存档，作为资产入帐和结算付款的依据。

表 39-8　设备故障维修登记表

设备编号：　　设备管理员：　　年　　月　　日

<table>
<tr><td>设备名称</td><td></td><td>型号规格</td><td></td><td>设备使用科室</td><td></td></tr>
<tr><td rowspan="2">故障日期</td><td rowspan="2"></td><td rowspan="2">报修时间</td><td rowspan="2"></td><td>修理时间</td><td></td></tr>
<tr><td>修理完成时间</td><td></td></tr>
<tr><td colspan="2">1. 现象</td><td colspan="2">2. 原因</td><td colspan="2">3. 处理</td></tr>
<tr><td>故障部位</td><td>现象编号</td><td colspan="2" rowspan="2"></td><td colspan="2" rowspan="2"></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">故障现象编号</td><td colspan="2">故障原因编号</td><td colspan="2">处理方法编号</td></tr>
<tr><td>1.磨损</td><td>11.杂音</td><td>1.设计不良</td><td>10.润滑不良</td><td colspan="2">1.检查</td></tr>
<tr><td>2.腐蚀</td><td>12.裂纹</td><td>2.装配不良</td><td>11.老化</td><td colspan="2">2.调整</td></tr>
<tr><td>3.泄漏</td><td>13.精度不良</td><td>3.制造不良</td><td>12.灾害</td><td colspan="2">3.更换</td></tr>
<tr><td>4.松动</td><td>14.短路</td><td>4.安装不良</td><td>13.事故</td><td colspan="2">4.改装</td></tr>
<tr><td>5.破损</td><td>15.接触不良</td><td>5.调整不良</td><td rowspan="2">14.原因不明</td><td colspan="2">5.清扫</td></tr>
<tr><td>6.烧伤</td><td>16.温度异常</td><td>6.保养不良</td><td colspan="2">6.应急措施</td></tr>
<tr><td>7.污染</td><td>17.压力异常</td><td>7.使用不良</td><td></td><td colspan="2">7.修复</td></tr>
<tr><td>8.脱落</td><td>18.断线</td><td>8.修理不良</td><td></td><td colspan="2"></td></tr>
<tr><td>9.变形</td><td>19.啮合不良</td><td>9.超负荷</td><td></td><td colspan="2"></td></tr>
<tr><td>10.振动</td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="4">更 换 零 件 清 单</td><td colspan="2">修理科室</td></tr>
<tr><td>名称</td><td>型号规格</td><td>数量</td><td>修理人</td><td colspan="2">备注</td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2" rowspan="3"></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

验收人：

表 39-9　单位固定资产处置申请表

单位：元

资产名称	账面原值	购建时间	
规格型号	已提折旧	计划使用年限	
单价	净值	已使用年限	
数量	估计残值	处置形式	
处置方向			
申报原因：			
申报单位技术鉴定：	申报单位资产管理部门意见：	申报单位财会部门意见：	
负责人：	负责人：	负责人：	
申报单位盖章：	主管部门审核意见： （章）	财政部门审批意见： （章）	
年　月　日	年　月　日	年　月　日	

4.6 防病毒安全管理办法

4.6.1 日常管理职责

（1）贯彻执行北京市水务局相关防病毒管理规定，负责本单位防病毒策略部署、规划；

（2）负责本单位防病毒系统安装、升级、维护和技术支持，定期检查防病毒系统软件安装及正版化使用、策略配置、软件升级情况；

（3）负责检查本单位防病毒软件的正版化安装情况，不允许私自安装非正版的防病毒软件；

（4）负责检查本单位防病毒软件的安装及防病毒引擎、恶意代码库升级情况；

（5）负责本单位范围防病毒工作宣传报道和防病毒知识普及教育；

（6）负责解答本单位防病毒系统客户端使用人员通过电话、FTP 等形式提交的关于防病毒的问题。

（7）负责定期对病毒防范相关知识进行培训，培训方式可以是现场，也可以是以 FTP 等形式将病毒防范相关知识发送给相关人员。

4.6.2 病毒爆发应急处理职责

（1）负责在本单位查找病毒源、隔离感染病毒的主机；

（2）负责将病毒爆发方式、处理方法、杀毒工具和注意事项通知到本单位所有职工；

（3）在接到北京市水务局紧急病毒查杀通知后及时传达到本单位防病毒系统客户端使用人员，并监督执行本单位病毒检查及系统补丁安装；

（4）负责统计汇总本单位计算机系统受病毒感染的情况并上报北京市水务局；

（5）遇到重大问题（比如，威胁生产系统运行），应及时向北京市水务局网络与信息安全工作小组汇报；

（6）负责事后将病毒造成的影响以及处理方式、处理结果上报北京市水务局网络与信息安全工作小组，并存档备案。

4.7 移动设备和远程办公安全管理办法

4.7.1 角色与职责

工程管理科相关人员的职责：

（1）负责本单位移动设备的安全检查；

（2）负责本单位远程接入的实施；

（3）负责本单位远程接入的安全策略的制定及更新。

（4）申请部门或科室负责人的职责：

（5）负责本部门远程接入的申请及批复。

4.7.2 移动设备和远程办公安全管理流程图

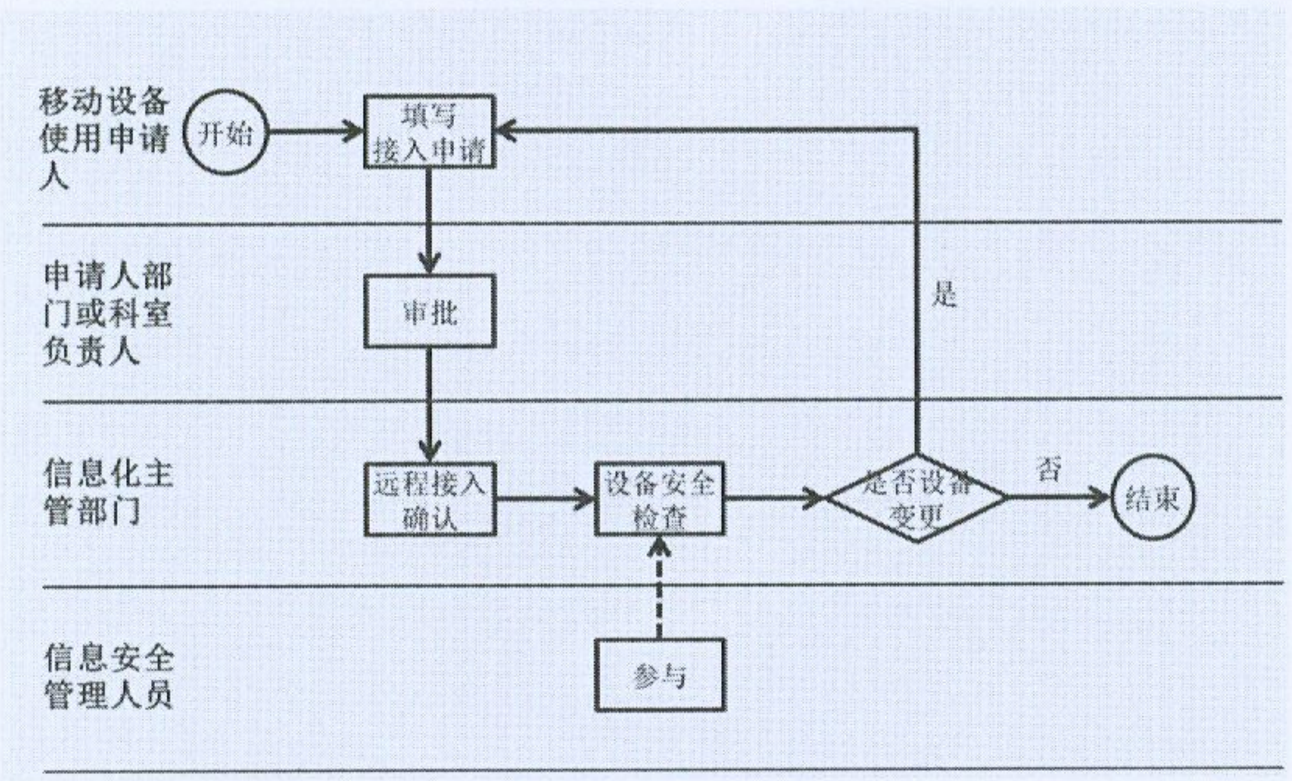


图 39-3 移动设备和远程办公安全管理流程图

4.7.3 移动设备安全管理办法

（1）移动设备日常安全管理

1）任何人员不得利用本单位移动设备进行违法、违规活动或为违法、违规活动提供条件。

2）移动设备持有人员应妥善保管该设备，严禁故意损毁、破坏。

3）移动设备持有人员应及时对移动设备的操作系统安全补丁进行升级，保证系统安全运行。

4）移动设备持有人员应设置登录口令（登录口令应不少于 8 位，密码复杂

度应满足字母+数字+符号的构成要求），并负责口令保密，设置带有密码的屏幕保护功能。

5）严禁在移动设备上安装、运行与工作无关的应用软件等应用程序，严禁使用移动设备从事与工作无关的活动。

6）通过移动设备使用、传输的单位生产数据，应由信息化主管部门相关人员对移动设备的安全性进行检查，并在数据的使用、传输过程中应用加密措施，禁止进行明文传输。

（2）移动设备网络接入安全管理

1）移动设备接入办公网应经信息化主管部门批准。

2）未经信息化主管部门同意，严禁把移动设备或其他任何设备接入办公网或从网络上拆除。

3）遵循“涉密不上网，上网不涉密”的原则，严禁将包含涉密信息的移动设备接入互联网。

4）接入办公网的移动设备因工作原因带离，再次接入办公网，履行以下手续:

① 使用人员提交接入办公网的相关申请;

② 信息化主管部门指派相关人员查杀病毒，确认移动设备安装了最新系统补丁、防病毒程序和最新病毒特征代码，并设置为定期进行系统补丁和病毒特征码更新的管理模式。

（3）移动设备防病毒管理

① 移动设备使用前必须事先安装防病毒软件。

② 按照“谁使用，谁负责”的原则，明确移动设备管理人员，并实现专机专用，保证防病毒软件的及时升级和病毒特征码的最新下载。若发现防病毒软件无法正常使用，应及时向信息化主管部门反映情况。

③ 应对移动设备下载、安装或使用的软件和数据文件进行病毒检测，禁止安装使用未经检测的软件或数据文件。

④ 禁止访问与工作无关或来历不明的互联网站点。

（4）移动设备带离及丢失管理

① 因工作需要将移动设备带离本单位工作场所时，设备使用人员需向本部

门或科室负责人请示并得到批准，将移动设备带离本单位的职工负有管理、保证信息安全的责任，不得擅自将该移动设备借予他人使用。

② 严禁擅自携带涉密移动设备外出，因工作携带时，应当按照有关保密办法办理批准和携带出国（境）手续。

③ 当移动设备出现遗失，设备使用人员须即时上报本单位行政管理部门及信息化主管部门，并提交事件报告。安全管理部门跟进事件报告后，明确责任，提出处理意见，并进行相关备案。具体请参见《移动设备丢失报备流程申请》及《移动设备丢失报备流程申请单》

④ 因移动设备出现遗失，信息化主管部门负责将相关信息、账号等内容与权限即时进行清理并对评估资产损失的金额；如需赔偿或者处罚，由相关部门根据行政管理部门处理结果提供协助。

4.7.4 远程接入安全管理办法

（1）远程接入的计算机、远程终端需安装操作系统补丁、防病毒软件等。

（2）在发现安全隐患的情况下，信息化主管部门将采取必要技术手段隔离网络中的计算机及远程接入设备，以保障本单位网络系统安全。

4.7.5 相关记录

《移动设备和远程办公接入申请表》

《移动设备丢失报备申请表》

《移动设备接入记录表》

《外部人员内网访问接入申请表》*注 1

*注 1：本表与《网接入申请表》区别在于，是否需要访问处属信息系统及政务外网相关系统，如通过我处网络访问互联网资源等开发资源，只填写《网接入申请表》即可，如需要访问政务信息系统资源，则需同时填写《外部人员内网访问接入申请表》。

表 39-10　移动设备和远程办公接入申请表

编号：

申请人姓名		申请部门		申请日期	
申请类型	□移动设备接入　　□远程办公接入				
操作类型	□申请用户　　□用户权限变更　　□注销用户				
系统、设备名称					
权限说明					
部门或科室负责人审批意见	签字：		日期：		
分配（变更、注销）的用户 ID					
信息化主管部门负责人审批意见	签字：		日期：		

表 39-11　移动设备丢失报备申请表

申请人姓名		申请部门		申请日期	
申请类型	□移动设备接入　　□远程办公接入				
操作类型	□申请用户　　□用户权限变更　　□注销用户				
系统、设备名称					
权限说明					
科室负责人审批意见	签字:		日期:		
分配（变更、注销）的用户 ID					
信息化主管部门系统管理人员	签字:		日期:		

表 39-12　外部人员内网访问接入申请表

接入科室		日期	年　月　日	
申请人	使用人		主机名称	
	IP 地址		MAC 地址	
	操作系统及补丁包版本	（如 Windows 7 SP1，Window10）		
	最新病毒定义文件时间			
	楼层、房间、工位		联系电话	
申请事由（含申请访问的主要业务名称、网址等）				
访问时段				
申请人承诺	未经授权不在无线网上发布我单位涉密信息。不通过无线网查阅或发布黄色及反动内容。不利用无线网从事违法、违规活动。不在连接无线网计算机上运行非法软件。从无线网上下载的任何信息资源，未经检测、查杀计算机病毒等处理不得使用。 承诺人签字：			
（以上内容由申请人如实填写）				
科室负责人意见		工程管理科审批意见		

表 39-13　移动设备接入记录表

序号	姓名	部门或科室	移动设备标识	接入时间	接入目的	设备 IP	申请人	申请人部门或科室负责人

4.8 服务器日常维护安全管理办法

4.8.1 角色与职责

服务器管理员的职责:

（1）负责本单位服务器系统或特权账号的开通、关闭与审核;

（2）负责本单位服务器操作系统的安全配置;

（3）负责本单位服务器的重启、重装与补丁管理;

（4）负责本单位服务器的日志、监测与备份管理。

4.8.2 服务器重启与安装管理流程

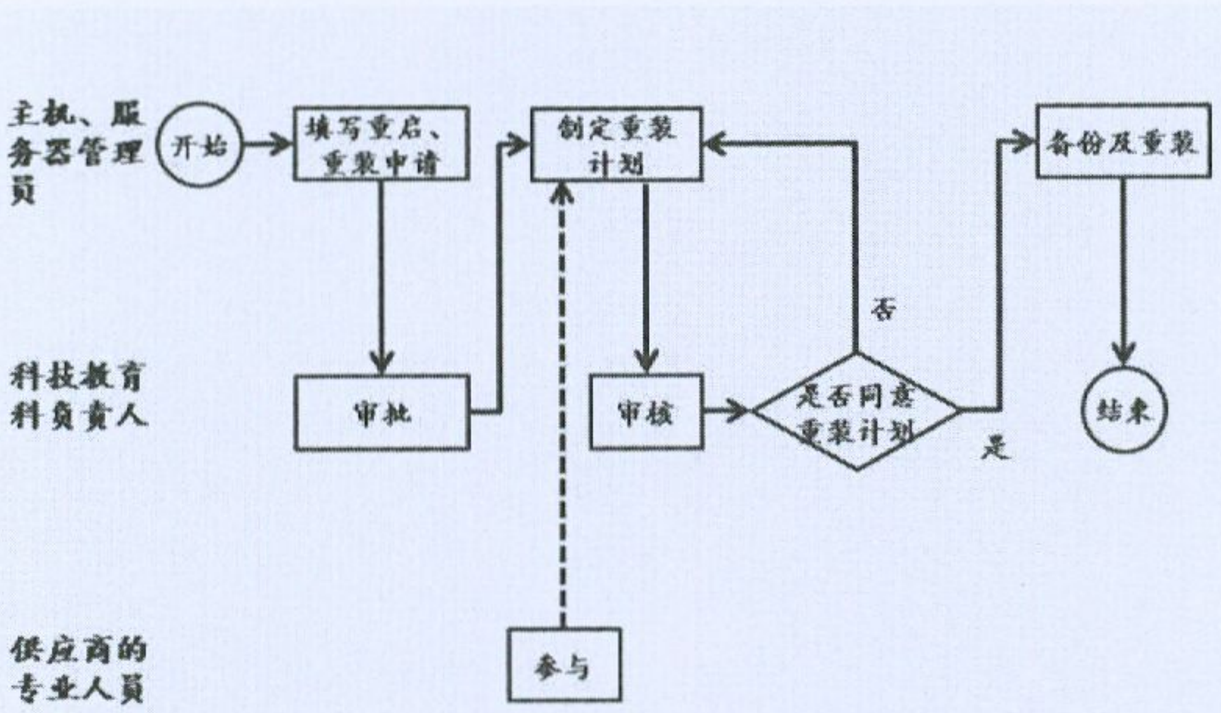


图 39- 4 服务器重启与安装管理流程

4.8.3 服务器日常维护安全管理流程

（1）权限和账号管理

1）操作系统仅开设满足业务或运行需要的账号，不得开设与业务系统运行无关的账号。

2）除了指定的服务器管理员可开设特权账号之外，其他人在未得到明确授权的情况下不得开设特权账号。

3）账号和密码禁止共享使用，如业务运行需要使用系统账号或特权账号，应在得到授权的情况下由服务器管理员开设仅对授权人使用的账号，并对账号使用进行登记。

4）服务器管理员定期对账号信息进行审核，确保系统中不存在同业务运行无关的账号以及过期的账号。

（2）安全配置管理

服务器管理员对服务器操作系统进行安全配置，保证服务器提供的安全机制的有效性，安全配置应至少包括：

① 关闭不必要的服务和端口；

② 在未经授权的情况下，不得在服务器上安装同业务运行和维护无关的软件；

③ 新安装系统遵循最小化安装原则。

（3）访问控制管理

1）除了授权的业务和运维访问外，任何人不得以任何方式非法访问本单位服务器。

2）授权业务或运维访问使用加密的传输协议连接服务器，例如通过 SSH 来登录服务器，禁止使用 Telnet 等明文方式登录服务器，并保留访问记录。

3）服务器管理员应开启服务器屏幕保护功能，防止未授权的访问。

（4）系统重启和重装

1）任何人不得随意重启有业务运行的服务器。服务器管理员在例行维护或特殊情况下需重启业务运行的服务器时，须事先提交服务器重启申请，经工程管理科负责人审批后方可执行。

2)如服务器需要重新安装，服务器管理员须向工程管理科负责人提交申请，并制定重装计划，在得到明确的批准后执行重装计划，计划中要包含：

3）需要重装的服务器的基本信息，包括操作系统以及其上运行的应用和服务等。

4）需要配合的科室和人员列表。

5）对业务系统正常运行的影响分析。

6）安装完毕对服务器进行安全配置。

7）业务系统服务器重启和重装申请记录应归档保存。

（5）日志管理

1）服务器管理员应启用服务器的日志记录功能，保证重要的事件能够记录

到服务器日志中，例如人员登录信息和操作信息。

2）服务器管理员应定期对服务器日志进行检查，以便发现可疑的登录信息或操作信息，对于日志的检查可以借助日志管理技术手段，日志检查应保留检查记录，未经授权不得删除日志信息。

（6）检测和监控

1)服务器管理员应针对服务器制定定期的系统检查计划，检查内容应包括：硬件有无报错、系统存储空间、CPU 和内存利用率、中间件状态、数据库状态等。

2）若发现系统异常，应立即进行异常分析和处理，并保留异常分析和处理记录。

（7）冗余备份

1）服务器管理员协同各业务科室相关人员识别需要备份的数据信息，并维护数据备份的列表。备份的信息应当包含但不限于操作系统、数据库系统、中间件、应用系统、应用系统数据、系统软件、设备配置、网站内容等。

2）应根据不同的数据信息，确定适合的备份手段，备份手段包括但不限于硬盘备份、冗余主机备份、磁带备份、光盘备份、存储局域网备份等。

3)应按照计划实施备份，并确保备份实施成功，并保留备份记录以备审查。

4.8.4 相关记录

无。

4.9 网络安全设备管理办法

4.9.1 角色与职责

工程管理科的职责：

（1）负责制定本单位统一的设备编码规则；

（2）负责组织建立和管理本单位统一的安全设备台帐；

（3）负责统计和更新本单位安全设备信息；

（4）负责定期组织安全设备清查核对工作。

（5）提出本单位安全设备配置规划和要求；

（6）负责安全设备日常巡查、维护以及报废的技术鉴定工作；

（7）定期组织对本单位安全设备的使用情况进行评估；

（8）组织协调、监督检查本单位安全设备的使用及维护工作；

4.9.2 网络安全设备管理流程图

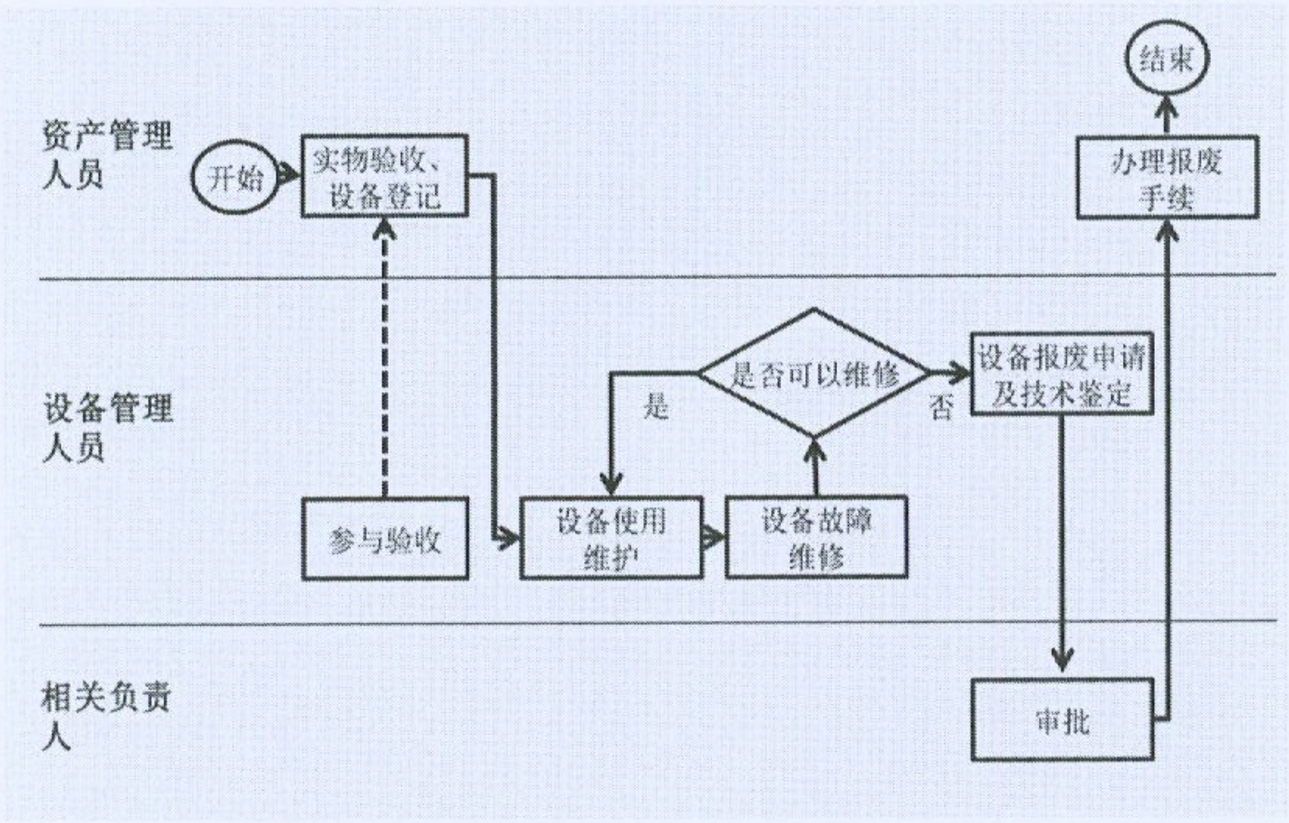


图 39-5 网络安全设备管理流程图

4.9.3 网络安全设备管理办法

（1）安全设备入库及配置管理

1）安全设备入库均须由本单位固定资产管理人员进行实物登记。

2）安全设备到货后由设备管理人员配合固定资产管理人员验收，并由固定资产管理人员办理固定资产编号、建卡、建账等工作。

3)《设备信息登记表》须反映安全设备的基本状况，主要包括设备编码、序列号、名称、型号、配置、价格、合同编号、购置日期、设备位置、维护责任和相关厂商情况等信息。固定资产管理人员应按照《设备信息登记表》要求认真填写设备信息的相关内容。

4）如遇安全设备系统变更或设备升级、改造、维修、调拨、迁移等变化内容，应由本单位固定资产管理人员按设备台帐的要求，及时调整和更改有关安全设备信息。

（2）安全设备的使用及维护管理

1）安全设备领用时，固定资产管理人员应及时更新设备配置信息，所有在用的安全设备必须指定设备管理人员；

2）安全设备管理人员在使用前应掌握安全设备的使用方法；

3）已经使用过的安全设备改作它用时，若涉及到保密信息，应由设备管理人员按照保密管理的有关办法妥善处理；

4）安全设备管理人员应爱护设备，做好防尘、防水、防磁、防震等工作。禁止在设备上运行与业务无关的程序，未经系统管理员允许不得随意更改系统和网络设置、变更网线、加装设备等。

5）安全设备所涉及的系统软件应使用合法渠道获得的正版软件，在免费服务期后，应通过适当的采购方式获得原厂商或其授权服务提供商的有偿维护和必要的升级服务。

6）工程管理科设备管理人员负责本单位安全设备的日常巡查和维护工作，并建立严格的《设备故障维修登记表》。

（3）安全设备的日志管理

1）设备管理人员应定期登录负责的安全设备日志系统，检查系统运行状态是否正常；

2）所有重要信息系统的访问行为均应在相应的安全设备中留有日志记录，且针对保存在安全设备中不同级别的日志信息，应定制不同的保存时间以备审计；

3）设备管理人员收到报警信息后，应及时登录报警设备，诊断故障、分析原因，提出解决方案，实施解决措施，并跟踪询问故障处理结果；

4）安全设备报警信息在处理的过程中，应按照本单位相关信息系统突发事

件应急管理的相关办法及流程执行。

4.9.4 网络安全设备运维管理办法

（1）防火墙设备运维

1）定期维护工作。

① 为保证防火墙设备正常运行，防火墙设备管理员需要定期对设备进行例行检查，包括查看系统CPU、内存使用率及网络接口等工作状态是否正常；如果出现异常，在判断不是网络攻击事件后，可重启防火墙。如仍存在问题，请及时联系厂商，并通知相关负责人。

② 为确保防火墙异常事件及时发现，防火墙设备管理员应定时查看系统中高级别的告警日志，并分情况进行处理:

③ 若为设备本身造成的中高级别告警，立即通知厂商达到现场进行处理。处理完毕后，形成报告，并发送相关负责人。

④ 若为网络故障造成的中高级别的告警日志，协调网络管理员共同分析处置。处理完毕后，形成报告，并发送相关负责人。

⑤ 若为网络攻击行为造成的中高级别的告警日志，协调网络管理员、系统管理员共同分析处置。处理完毕后，形成报告，并发送相关负责人。

2）不定期维护工作。

如需要增添防护对象或更改配置信息，防火墙设备管理员应填写《设备配置变更申请单》，相关负责人审批通过后，才能执行相关操作。

（2）入侵检测设备运维

1）定期维护工作。

① 为保证入侵检测设备正常运行，入侵检测设备管理员需要定期对设备进行例行检查，包括查看系统CPU、内存使用率及网络引擎等工作状态是否正常；如果出现异常，在判断不是网络攻击事件后，可重启入侵检测引擎或设备。如仍存在问题，请及时联系厂商，并通知相关负责人。

② 为确保入侵检测设备异常事件及时发现，入侵检测设备管理员应定期查看系统中高级别的告警日志，如出现高风险事件，按照以下步骤进行处理:

③ 通知防火墙设备管理员，查看防火墙日志，是否对该攻击行为已自动阻断。

④ 如已进行了阻断，协同网络管理员、系统管理员，定位攻击源 IP。

⑤ 源攻击 IP 定位后，安排相关技术人员分析内网存在漏洞的原因，并对该漏洞进行修补。

⑥ 高风险事件处理完毕后，形成相关报告，提及相关负责人。

⑦ 入侵检测设备管理员应根据厂商发布的版本升级情况，定期完成入侵检测设备相关版本的升级工作。

2）不定期维护工作。

如需对入侵检测设备的配置信息进行更改，入侵检测设备管理员应填写《设备配置变更申请单》，相关负责人审批通过后，才能执行相关操作。

（3）上网行为管理设备运维

1）定期维护工作。

为① 保证上网行为设备正常运行，上网行为设备管理员需要定期对设备进行例行检查，包括查看系统 CPU、内存使用率及存储等工作状态是否正常；如果出现异常，可通过重启设备进行恢复。如仍存在问题，请及时联系厂商，并通知相关负责人。

② 为确保上网行为设备异常事件及时发现，上网行为设备管理员应定期查看系统中高级别的告警日志，并分情况进行处理:

③ 如发现职工在工作时间，因使用 P2P 软件、视频软件等造成网络流量激增，网络带宽下降，影响正常业务时，应采取策略限制访问行为。同时，通知相关负责人并进行事件处理。

④ 如发现职工通过互联网渠道，发布不当内容，应及时通知相关负责人并进行事件处理。

⑤ 对于上网行为设备监测到的任何信息，上网行为设备管理员不应随意散布，只能知会相关事件负责人。

⑥ 上网行为设备管理员应根据厂商发布的版本升级情况，定期完成入相关版本的升级工作。

2）不定期维护工作。

如需对上网行为设备的相关配置信息进行更改，上网行为设备管理员应填写《设备配置变更申请单》，相关负责人审批通过后，才能执行相关操作。

4.9.5 相关记录

《设备信息登记表》

《设备故障维修登记表》

《设备报废、销毁记录表》

《设备配置变更申请单》

表 39-14　设备信息登记表

年　月　日　　入库单号:

设备编号	设备名称	规格型号	资产类别	供应商	单位	数量	单　价（元）	金额（元）	备注
合计									
验收意见:　　验收人员（签字）:									
工程管理科设备管理员（签字）:　　采 购 员（签字）:									

表 39-15　设备故障维修登记表

设备编号：　　设备管理员：　　年　月　日

<table>
<tr><td>设备名称</td><td></td><td>型号规格</td><td></td><td>设备使用科室</td><td></td></tr>
<tr><td rowspan="2">故障日期</td><td rowspan="2"></td><td rowspan="2">报修时间</td><td rowspan="2"></td><td>修理时间</td><td></td></tr>
<tr><td>修理完成时间</td><td></td></tr>
<tr><td colspan="2">1.　现象</td><td colspan="2">2. 原因</td><td colspan="2">3. 处理</td></tr>
<tr><td>故障部位</td><td>现象编号</td><td colspan="2" rowspan="2"></td><td colspan="2" rowspan="2"></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">故障现象编号</td><td colspan="2">故障原因编号</td><td colspan="2">处理方法编号</td></tr>
<tr><td>1.磨损</td><td>11.杂音</td><td>1.设计不良</td><td>10.润滑不良</td><td colspan="2">1.检查</td></tr>
<tr><td>2.腐蚀</td><td>12.裂纹</td><td>2.装配不良</td><td>11.老化</td><td colspan="2">2.调整</td></tr>
<tr><td>3.泄漏</td><td>13.精度不良</td><td>3.制造不良</td><td>12.灾害</td><td colspan="2">3.更换</td></tr>
<tr><td>4.松动</td><td>14.短路</td><td>4.安装不良</td><td>13.事故</td><td colspan="2">4.改装</td></tr>
<tr><td>5.破损</td><td>15.接触不良</td><td>5.调整不良</td><td rowspan="2">14.原因不明</td><td colspan="2">5.清扫</td></tr>
<tr><td>6.烧伤</td><td>16.温度异常</td><td>6.保养不良</td><td colspan="2">6.应急措施</td></tr>
<tr><td>7.污染</td><td>17.压力异常</td><td>7.使用不良</td><td></td><td colspan="2">7.修复</td></tr>
<tr><td>8.脱落</td><td>18.断线</td><td>8.修理不良</td><td></td><td colspan="2"></td></tr>
<tr><td>9.变形</td><td>19.啮合不良</td><td>9.超负荷</td><td></td><td colspan="2"></td></tr>
<tr><td>10.振动</td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="3">更 换 零 件 清 单</td><td></td><td colspan="2">修理科室</td></tr>
<tr><td>名称</td><td>型号规格</td><td>数量</td><td>修理人</td><td colspan="2">备注</td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2" rowspan="3"></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

验收人：

表 39-16 设备报废、销毁记录表

序号	登记日期	设备保管或管理人	设备类型	信息检查	报废、销毁审批人	报废、销毁执行人	备注

二、廉政责任书

廉政责任书

项目名称：信息系统运维类项目—北运河闸站自动化监控系统信息化运维项目

建设地点：北京市

发包人（甲方）：北京市北运河管理处

承包人（乙方）：北京大恒软件技术有限公司

为加强项目建设中的廉政建设，规范甲乙双方的各项活动，防止发生各种谋取不正当利益的违法违纪行为，保护国家、集体和当事人的合法权益，根据国家有关法律法规和廉政建设责任制规定，甲乙双方特订立本廉政责任书。

第一条甲乙双方的责任

（一）应严格遵守国家关于市场准入、项目招标投标、项目建设和市场活动的有关法律、法规，相关政策，以及廉政建设的各项规定。

（二）严格执行建设合同文件，自觉按合同办事。

（三）业务活动必须坚持公开、公平、公正、诚信、透明的原则（除法律法规另有规定者外），不得为获取不正当的利益，损害国家、集体和对方利益，不得违反第三方安全测评管理的规章制度。

（四）发现对方在业务活动中有违规、违纪、违法行为的，应及时提醒对方，情节严重的，应向其上级主管部门或纪检监察、司法等有关机关举报。

第二条甲方责任

甲方的领导和从事该建设项目的工作人员，在事前、事中、事后应遵守以下规定：

（一）不准向乙方和相关单位索要或接受回扣、礼金、有价证券、贵重物品和好处费、感谢费等。

（二）不准在乙方和相关单位报销任何应由甲方或个人支付的费用。

（三）不准要求、暗示或接受乙方和相关单位为个人装修住房、婚丧嫁娶、配偶子女的工作安排以及出国（境）、旅游等提供方便。

（四）不准参加有可能影响公正执行公务的乙方和相关单位的宴请、健身、娱乐等活动。

（五）不准向乙方和相关单位介绍或为配偶、子女、亲属参与同甲方项目建设合同有关的设备、材料、分包等经济活动。不得以任何理由要求乙方购买项目建设合同规定以外的材料、设备、服务等。

第三条乙方的责任

应与甲方保持正常的业务交往，按照有关法律法规和程序开展业务工作，严格执行项目有关方针、政策，尤其是有关的强制性标准和规范，并遵守以下规定：

（一）不准以任何理由向甲方及其工作人员索要、接受或赠送礼金、有价证券、贵重物品及回扣、好处费、感谢费等。

（二）不准以任何理由为甲方和相关单位报销应由对方或个人支付的费用。

（三）不准接受或暗示为甲方、相关单位或个人装修住房、婚丧嫁娶、配偶子女的工作安排以及出国（境）旅游等提供方便。

（四）不准以任何理由为甲方、相关单位或个人组织有可能影响公正执行公务的宴请、健身、娱乐等活动。

第四条违约责任

（一）甲方工作人员有违反本责任书第一、二条责任行为的，按照管理权限，依据有关法律法规和规定给与党纪、政纪处分或组织处理；涉嫌犯罪的，移交司法机关追究刑事责任。

（二）乙方工作人员有违反本责任书第一、三条责任行为的，按照管理权限，依据有关法律法规和规定给与党纪、政纪处分或组织处理；涉嫌犯罪的，移交司法机关追究刑事责任。

第五条其它

（一）本责任书作为政府采购合同的附件，与政府采购合同具有同等法律效力。经双方签署后立即生效。

（二）本责任书的有效期为双方签署之日起至该项目最终验收合格时止。

（三）本责任书一式捌份，甲方执肆份，乙方执肆份，具有同等法律效力。

甲方单位：（盖章）

法定代表人

或授权代理人签字：

甲方监督单位（盖章）

签订时间：2022年6月27日

乙方单位：（盖章）

法定代表人

或委托代理人签字：

乙方监督单位（盖章）

签订时间：2022年6月27日

三、安全及保密协议

安全及保密协议

甲方：北京市北运河管理处

联系地址：通州区潞苑大街99号

邮编：101100

电话：80593800

乙方：北京大恒软件技术有限公司

联系地址：北京市海淀区苏州街3号大恒科技大厦北座1101室

邮编：100080

电话：010-82828800

甲方委托乙方承担**信息系统运维类项目—北运河闸站自动化监控系统信息化运维**项目，为落实运维安全管理，保护双方在合同执行期间维护服务所需的有关信息的保密性，双方在平等、自愿、协商一致的基础上签订此安全保密协议，订立以下条款并共同遵守。

1. 运维安全管理责任

1.1 乙方对合同内的运维服务承担安全责任，乙方（包括乙方所有参与该维护服务的维护人员）对甲方的业务秘密和系统安全与风险信息负有保密责任。

1.2 乙方应遵照《信息安全等级保护管理办法》（公通字[2007]43号）和《北京市开展信息安全等级保护工作实施方案》（京公网监字[2007]788号）等有关规定执行，并遵守甲方的有关运维安全管理制度和工作规范。

1.3 乙方在维护过程中，应针对项目的特点编制维护计划和落实相应的安全措施，服从北京市水务局安全运维公司在安全方面的统一管理。

1.4 乙方在运维过程中如发生重大信息安全事件，其处置应按照《关于印发<北京市国家机关重大信息安全事件报告制度>的通知》（京信息办函 [2004]73号）和《北京市国家机关重大信息安全事件调查处理办法》(京信息办函 [2004]227号)等文件执行。

1.5 乙方应配合甲方建立运行监控管理机制，动态掌握网络及信息系统的运行状况，针对可能出现的重大故障和灾难，制定相关应急预案。应根据《信息系统灾难恢复规范》

(GB/T20988-2007)和《关于加强我市电子政务信息系统灾难恢复工作的意见》（京信安协[2006]3 号）等有关规定，对本公司承担的维护项目进行风险分析和业务影响分析，衡量确定灾难恢复目标，制定灾难恢复相关预案。并适时提出应急演练申请，对各种异常情况做出快速响应。

1.6 乙方应对运维服务有关数据的备份、恢复、加工、访问、清除和销毁等制定控制流程。涉及保密的数据，依照国家、北京市有关数据安全的规定及本协议第二条的要求执行。

1.7 乙方在维护过程中所带的电脑及其它存储设备必须是经过严格病毒查杀的，不得将病毒等恶意程序带入服务器中。

1.8 在调试服务器等相关设备时，应严格按照相关程序及规范，否则造成的所有后果由乙方承担。

1.9 对于软件维护，乙方在每次对系统代码进行更新之前，必须先对服务中的文件、数据及相关日志进行备份。

1.10 未经甲方书面许可，乙方维护人员不得私自对市水务局业务系统、网络、数据库等进行操作，否则因此造成的损失由乙方承担。

2. 保密管理责任

2.1 本协议指的保密内容，包括（但不限于）：维护对象的有关信息（如信息系统中的数据和信息，所提供的书面资料和电子文档包括相关的方案、设计文档、配置和参数等），以及为满足维护服务而涉及的技术秘密、商业秘密，无论是书面的、口头的、图形的、电磁的或其它任何形式的信息。

2.2 双方承诺在获得对方书面同意之前，不将对方的保密内容泄漏、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。

2.3 一方可以在任何时候，以书面形式要求对方返还或销毁任何依该项目而提供的可记载在任何有形介质上的保密信息及其复制件，另一方应予以执行，并保证没有直接或间接地故意保留或控制任何保密信息及其复制件。

2.4 一方依据法律或政府部门的有效指令而使用对方提供的信息时，应及时通知对方。

2.5 乙方在参加国内外学术会议或交流活动中需要公开发表与保密内容有关资料，必须事先向甲方提出申请；未经甲方同意，乙方不得擅自就保密内容或资料情报向外公开。

2.6 除直接参与本项工作的人员之外，乙方不得将保密信息透露给其它任何人。

2.7 双方不能将此专有信息的全部或部分进行复制或仿造。

2.8 乙方应当告知并以适当方式要求其参与本项工作之雇员遵守本协议规定，若参与本项工作之雇员违反本协议规定，乙方应承担连带责任。

2.9 没有甲方的书面许可，乙方不得丢弃和处理任何书面的或其他有形的专有信息。

2.10 严禁乙方将软件系统中的涉密资料外漏，不得擅自拷贝软件系统中的涉密文件。对于涉及甲方信息的服务，乙方只能实施现场服务，不得将信息或携带信息的产品带离甲方工作现场。

3. 人员管理责任

3.1 乙方应强化维护人员安全意识，加强人员管理，重视人员教育，约束人员的行为，每年组织不少于 2 次的人员保密意识培训。

3.2 乙方应在员工入职前进行政治审查和安全保密培训，并与员工签订保密协议，以高度的责任心及使命感，做好水务信息系统信息安全工作。

3.3 乙方应根据甲方要求及保密政策变化，及时组织安全保密意识培训。

3.4 乙方人员在调离岗位或离职时，要履行保密协议，承诺保密事项，并上交有关资料、证件。

3.5 乙方离职人员工作交接由乙方负责人具体负责，并统一协调。在工作交接中，离职人员管理及办理的一切事务均应移交。工作交接要注明工作职责、工作内容、工作重点等履行情况和办理情况，对于正在办理和未办理事项要进行详细移交。要认真进行原工作资料的移交。

3.6 乙方离职人员办公物品交接由项目负责人负责办理。离职人员因原工作关系所保管、使用、配发、借用等非个人用品应一并进行移交。涉密文件或设备不得个人保存。

3.7 乙方员工应加强学习与工作相关的专业知识和技能，积极参加公司和甲方组织的各项保密相关培训。

3.8 乙方员工应在工作时间全身心的投入，保持高效率的工作，确保不因工作疏忽造成失密事件发生。

3.9 乙方员工在任何时间均不得利用甲方的场所、设备及其他资源从事私人活动。

3.10 乙方员工必须保管好个人的文件资料和办公用品，未经同意不可挪用他人的资料和办公用品。

3.11 乙方员工要保管好个人电脑，按甲方规定进行文档存储、杀毒及日常维护。

3.12 乙方员工必须服从甲方的整体管理，包括职务的分配及工作内容的安排。

3.13 乙方员工有相关业务方面的问题须及时向上级领导反映，听取意见。

3.14 涉及超出乙方员工权限的决定必须报经甲方同意。

3.15 乙方驻场人员应严格遵守甲方制订的《人员安全管理程序》、《外包驻场人员的管理办法》、《人员离职和换岗管理制度》、《项目人员离职交接》等管理办法和流程。

4. 疫情防控责任

4.1 为认真贯彻落实市委市政府、市水务局关于新型冠状病毒疫情防控工作要求，以政治要求和法律责任的高度，坚决防范和控制疫情传播和蔓延，坚决确保北运河管理处防疫工作落到实处，坚决打赢新冠肺炎病毒疫情“阻击战”、“攻坚战”，乙方需落实以下防疫责任：

（1）负责市水务局及北运河管理处防疫政策、措施的具体落实工作；

（2）组织开展有关防控新冠肺炎病毒的知识教育，普及疫情预防知识，提升职工自我防范意识；

（3）督促责任范围内人员的疫苗接种工作；

（4）了解掌握并及时上报疫情期间职工个人及共同居住成员健康状况及节假日期间主要出行情况，引导职工尽量保持“两点一线”工作生活模式；

（5）督促职工存在进返京、出现弹窗或短信提示信息、与阳性患者有时空交集等情况的要落实相应防控要求，并将有关情况及时上报，报告内容真实有效，不得迟报、漏报、谎报、瞒报；

（6）负责派驻北运河管理处的运维人员疫情防控的现地管理工作，包括防疫信息查验、行程动态管理、个人健康状况监测、情况上报及防疫措施落实（包含但不限于办公区域、设备设施、工器具的清洁消毒工作）等工作。

5. 协议生效与终止期限

5.1 本协议对合约双方具有同等约束力。

5.2 本协议所确定的安全保密业务在双方合作终止后仍然有效，不因为双方合作及合作项目的中止、终止而解除。

6. 违约责任

6.1 任何一方如违反本协议规定给对方造成损失的，应承担相应的法律责任和赔偿责任，无论造成损失的当事人与合同执行单位是否存续雇佣关系。

7. 其他

7.1 本协议自双方签字盖章之日起生效。本协议书一式捌份，甲方执肆份，乙方执肆份，具有同等法律效力。

7.2 本合同发生争议的，由双方协商解决，也可按以下方式解决：提交北京仲裁委员会仲裁、依法向人民法院提起诉讼。

7.3 本合同未尽事宜，双方可以另行协商，商定内容经双方代表签字并盖章后与本合同具有同等效力。

甲　方：北京市北运河管理处

（盖章）

法定代表人

或授权委托人：

日　期：2022年6月27日

乙　方：北京大恒软件技术有限公司

（盖章）

法定代表人

或授权委托人：

日　期：2022年6月27日