网络与信息安全承诺书

为进一步明确网络与信息安全责任，确保天津港（集团）有限公司网络安全和天津港信息技术发展有限公司数据中心网络与信息系统安全、稳定运行，按照《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）和《信息安全等级保护管理办法》（公通字[2007]43号）等规定，在承接天津港信息技术发展有限公司《信息公司人员车辆进出管理系统》技术开发（委托）合同项目过程中，我单位郑重承诺严格落实以下工作并承担相关责任：

一、按照“谁主管，谁负责；谁运营，谁负责”的原则，法定代表人为第一责任人，逐级落实信息网络安全责任制，并提供必要的人员和经费保障。

二、明确本单位网络与信息安全工作职责和任务，加强组织领导，明确职责任务，将网络与信息安全职责层层分解、落实到具体部门、具体岗位和具体人员。加强网络与信息安全工作的组织领导，建立健全网络与信息安全工作机构和工作机制，保证网络与信息安全工作渠道的畅通。

三、主动配合公安机关的监督、检查和指导，对本单位运营、使用的网络与信息系统开展定级、备案、安全建设整改及等级测评工作。

四、承诺遵守《中华人民共和国网络安全法》、《关键信息基础设施保护条例》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《天津港（集团）有限公司网络安全管理办法》等其他国家法律法规和行政规章制度，落实信息安全等级保护管理制度和技术防护措施，及时查找本单位安全隐患和漏洞，对薄弱环节和潜在威胁采取措施进行整改，确保网络与信息系统运行安全、数据安全。

五、按照天津市政府相关要求，与公安机关建立信息网络安全事件（事故）发现、报告、处置等工作机制，开展对本单位网络与信息系统的实时监测工作，留存相关日志，及时向公安机关上报本单位出现的网络与信息安全事件。

六、制定本单位信息安全应急预案，明确应急处置流程，加强应急队伍建设、物资储备、人员培训和应急值守工作，定期组织开展应急演练，发生网络与信息安全事件后立即启动应急预案进行快速妥善处置。在重大活动、节日等

重保期间，制定本单位信息安全保障方案，加强对重要信息系统的安全检测，加强值班，严防死守，随时应对各类突发事件。应急值守人员24小时保持电话畅通。

七、本单位可根据实际需要，申请开放特定的网络和主机端口，在利用开放的端口进行信息传播和自我服务期间，应严格遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国公用计算机互联网国际联网管理办法》和《中国互联网络域名注册暂行管理办法》等相关规定。保证服务器对外发布的信息不违反中华人民共和国有关法律、法规和行政规章制度规定，不能制作、复制、传播下列内容：

1)煽动抗拒、破坏宪法和法律、行政法规实施的；

2)煽动颠覆国家政权，推翻社会主义制度的；

3)煽动分裂国家、破坏国家统一的；

4)煽动民族仇恨、民族歧视，破坏民族团结的；

5)捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

6)宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

7)公然侮辱他人或者捏造事实毁谤他人的；

8)损害国家机关信誉的；

9)其它违反宪法和法律、行政法规的。

八、申请开放端口的主机要做好安全防护，防止被他人攻击后影响天津港（集团）有限公司网络环境和天津港信息技术发展有限公司数据中心网络安全及稳定运行。天津港信息技术发展有限公司将协助集团公司网络安全领导小组办公室不定期检查已申请开放端口的主机所提供的服务以及采取的安全措施，若不符合本承诺书的要求，将随时中断其网络服务。

九、认真执行国家和天津市网络与信息安全工作要求的工作事项，如发生网络与信息系统安全问题，造成损失和影响的，自愿承担相关责任。

十、合规性要求。

10.1 本单位承诺遵守《中华人民共和国网络安全法》、《关键信息基础设施保护条例》、《天津港（集团）有限公司网络安全管理办法》等其他国家法律法规和行政规章制度。

10.2 产品应具备检测合格凭证。

10.3 产品若为计算机信息系统安全专用产品，应具备销售许可证。

提供密码产品或服务，应具有国家密码管理局相关产品或服务的认证证书。

十一、安全性要求。本单位承诺对本单位产品实行全生命周期的安全防护，确保产品自身的安全性，及时进行版本迭代更新、补丁安装，对于安全负责人员的权限进行严格管控，审计操作日志等。

11.1 产品设计规划阶段，应充分考虑安全性要求，采取必要的防护措施，防止产品信息泄露或被破坏。

11.2 产品研发测试阶段，本单位承诺对本单位开发产品的源代码库采取管控措施，防止第三方人员违规访问其开发维护项目之外的源代码等违规行为。

11.3 产品试运行及维护阶段，应记录产品操作维护行为，留存产品维护记录。

11.4 产品应能够保证自身安全性，无法删除自身的审计日志。

11.5 未经天津港信息技术发展有限公司事先书面同意，产品不得进行版本变更。

11.6 严格控制产品调试和使用操作权限。产品正式交付后，未经天津港信息技术发展有限公司事先书面同意，不得随意进行查看和操作。

十二、产品交付要求。本单位承诺采用可信、可控的产品分发、交付和仓储手段，保证产品在运输、存储及交付等过程中的安全。

12.1 产品分发条件。除本订单另有规定，我单位承担包装、装载、将货物交付给天津港信息技术发展有限公司并将货物装上天津港信息技术发展有限公司的运输工具的所有有关费用。

12.2 产品交付。应按照天津港信息技术发展有限公司指定的交付日发货或提供服务，如果由于我单位未能及时发货，而导致其无法按照约定的运输方式在交付日发货，则这些产品应采用航空运输或其它天津港信息技术发展有限公司所能接受的最快捷方式发送。由此增加的任何相应的运输费用应由我单位支付。

12.3 部分履行的服务。如果我单位在交付日只能履行部分服务内容，我单位必须立刻通知天津港信息技术发展有限公司。除非天津港信息技术发展有限公司要求重新安排履行服务的时间，否则我单位在交付日履行这些服务。

12.4 能够提供部分货物。我单位如果在交付日只能发送部分货物，应立刻通知天津港信息技术发展有限公司。除非天津港信息技术发展有限公司要求重

新安排发货时间，否则我单位应发送该部分货物。如果通过订单规定以外的方式发货，则我单位支付由此增加的相应的运输成本。

12.5 产品存储。应按照良好商业惯例、天津港信息技术发展有限公司的规格、政府规定及其它有关要求，对货物加以保存、搬运和包装，以防止货物的损失或损坏。无论货物的所有权及/或灭失风险何时由卖方转移至天津港信息技术发展有限公司，对于因我单位未适当保存、包装和搬运货物所导致的任何损失或损坏，我单位承担责任。天津港信息技术发展有限公司无需向我单位提出该损失或损坏的任何索赔。

12.6 产品签收。每次向天津港信息技术发展有限公司交付货物时，都必须包含一份装箱单，其中至少应包括：订单号、部件号、发货量、发货日期。装箱单上的信息须与商业合同中的信息一致。

十三、供应链断供的应对措施。针对意外地未能交付货物或服务的事件，应保持合理的库存，采用多方采购、准备后备供应商、分散供应地点等措施，同时备用多种不同的物流路线/渠道，核心业务的供应链具有异地多活措施，具有紧急替换能力。

十四、第三方服务人员操作要求。

14.1 设备上架替换。设备上架或替换时，应将设备或主要部件进行固定，并设置明显的不易除去的标识。

14.2 产品更新升级。对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中保留不可更改的审计日志，操作结束后应同步更新配置信息库。

14.3 产品运行维护。对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视。

14.4 介质管理。将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理。

14.5 服务人员操作管理。建立第三方服务人员操作记录，并定期审查。采取视频监控、运维管理系统等必要的技术防护手段，发现第三方服务人员违规行为，包括接触非其项目之外的代码、接触敏感信息、直接进行生产操作，第三方设备违规接入网络等。

14.6 服务人员保证不利用网络危害国家安全、泄漏天津港信息技术发展有限公司机密、损害天津港信息技术发展有限公司的合法权益，不从事违法犯罪活动。

十五、本单位承诺对天津港信息技术发展有限公司数据在收集、存储、使用、加工、传输、销毁等环节采取安全管控措施，保证数据安全有效，不私自使用、泄漏天津港信息技术发展有限公司数据，否则将依照相关法律承担相应责任。

十六、离职人员要求。当本单位或第三方服务人员离职时，应立即进行账号注销、系统权限撤销等操作，并在指定的日期内，完成项目交接等工作。

十七、网络安全违约责任承诺。

17.1 产品质量保证期或运维服务期条款

在产品质量保证期或运维服务期内本单位提供 7*24 小时应急响应服务，包括但不限于配合安全隐患排查、定期安全漏洞修复、安全策略调优、系统代码逻辑缺陷调优、网络安全事件应急处置等，本单位负责在组件提供商、应用提供商发布漏洞补丁后，进行对应系统已公布漏洞修复。在接到天津港信息技术发展有限公司通知 2 小时内确认疑似漏洞的有效性和影响范围，并启动应急响应，安全漏洞需在发现后 5 天内对安全漏洞制定并落实漏洞修补方案进行修复或完成抑制措施，并对应用系统或服务器上的安全漏洞修复进行验证，确保漏洞已修复且应用系统或服务器没有出现异常情况，形成漏洞修复或抑制报告，并将相关文档提供天津港信息技术发展有限公司留档。每超过 1 天按照合同价款的 0.5%支付违约金，按天累计计算。超过 3 天后天津港信息技术发展有限公司有权委托第三方进行处理，产生的费用均由本单位承担。

说明：此项适用于软件开发、软件运维、信息化设备采购、信息化设备运维等相关合同。违约金比例供各部门参考，由业务部门自行商定，原则上违约金应覆盖公司可能造成的损失。

17.2 重大活动和敏感时期条款

在重大活动和敏感时期（包括但不限于春节、国庆、攻防演习等，具体视天津港信息技术发展有限公司要求而定）提供 7*24 小时应急响应服务，包括但不限于配合安全隐患排查、安全漏洞修复、安全策略调优、系统代码逻辑缺陷调优、网络安全事件应急处置等，视天津港信息技术发展有限公司要求提供现

场值守；配合天津港信息技术发展有限公司进行网络安全防护，在确认网络产品存在安全漏洞后，应当立即对安全漏洞进行评估与处置；因系统安全漏洞问题导致系统被攻击而不得不对业务系统下线的，每下线一次需按照合同价款的1%支付违约金，按次累计计算。4小时内未完成修复上线的，还需按照合同价款的2%支付违约金。超过4小时后天津港信息技术发展有限公司有权委托第三方进行处理，产生的费用均由本单位承担。

说明：此项适用于软件开发、软件运维、信息化设备采购、信息化设备运维等相关合同。违约金比例供各部门参考，由业务部门自行商定，原则上违约金应覆盖公司可能造成的损失。

17.3 应用系统及源代码安全条款

本单位应保证天津港信息技术发展有限公司应用系统源代码安全，建立严格管控机制，确保最少人员接触，且不暴露在互联网，未经授权不得使用天津港信息技术发展有限公司标识标牌进行页面和代码嵌入。本单位应保证交付天津港信息技术发展有限公司应用系统已进行安全漏洞扫描和截止交付日期前的已发布安全漏洞都已修复完毕，经过处理后以确保修复的漏洞不会给天津港信息技术发展有限公司业务造成影响。由于本单位原因造成源代码泄露，漏洞攻击失陷及上级监管部门通报，每发生一次按照合同价款的1%支付违约金，按次累计计算；由于本单位原因造成源代码泄露并导致网络安全事件发生，每发生一次按照合同价款的2%支付违约金，按次累计计算。此外，天津港信息技术发展有限公司负责组织评估和控制所造成的影响，产生的相关费用由本单位承担。

说明：此项适用于软件开发、软件运维（如涉及该单位开发）等相关合同。违约金比例供各部门参考，由业务部门自行商定，原则上违约金应覆盖公司可能造成的损失。

17.4 网络安全防护应用条款

本单位应加强网络与信息核心技术的使用，实现安全监测、安全预警、灾难恢复、安全防护等安全保障，构建可信、可控、可查、可溯的网络与信息安全防护体系，全面保障天津港信息技术发展有限公司网络业务安全，确保业务连续性，需确保不影响天津港信息技术发展有限公司现有网络架构，业务访问方式，不得改变现有业务系统运行模式，所提供安全类软件应具备防护及阻断简单有效，业务系统稳定运行。由于本单位原因造成业务中断小于5分钟，每

发生一次按照合同价款的 1%支付违约金，按次累计计算；由于本单位原因造成业务中断 5 分钟以上或网络安全事件发生，每发生一次按照合同价款的 2%支付违约金，按次累计计算。此外，天津港信息技术发展有限公司负责组织评估和控制所造成的影响，产生的相关费用由本单位承担。

说明：此项适用于网站云防护、网络阻断设备类相关服务或采购合同。违约金比例供各部门参考，由业务部门自行商定，原则上违约金应覆盖公司可能造成的损失。

17.5 网络安全漏扫设备条款

天津港信息技术发展有限公司接到上级监管部门安全漏洞通报后，明确为本单位责任的单个高危漏洞单次扣除 2000 元违约金，单个中危漏洞单次扣除 1000 元违约金，多个漏洞进行累加计算。

说明：此项适用于漏洞扫描设备相关服务或采购合同。违约金金额供相关部门参考，由业务部门自行商定，原则上违约金应覆盖公司可能造成的损失。

本承诺书一式两份，双方各执一份，自承诺单位签字盖章之日起生效，于项目结束后终止。

承诺单位（盖章）：

法定代表人或负责人（签字）：

日期：2023.7.12