正本

2026年度浦东公交网络安全服务项目

项目编号：GQ31011500026031720025 2（标项1）

资质文件

投标人全称：上海天泰网络技术有限公司

地址：上海市浦东新区盛荣路88弄1号楼9层01室

时间：2026年4月10日

投标文件说明

现就本次项目投标文件的有关内容说明如下：

1、 天泰网络总部在浦东，为浦东公交持续提供网络安全保障服务（提供合同案例），了解浦东公交网络及信息系统的情况，熟悉网络安全需求和管理流程，具备为浦东公交提供安全服务的能力和经验。

2、 天泰网络是浦东新区大数据中心运维保障服务单位（提供合同案例），熟悉浦东政务网络的管理架构、策略和规程，熟悉浦东新区属地化主管部门（网信办、大数据中心、网安）有关网络安全的管理要求，有信心为浦东公交持续做好网络安全相关技术、辅助管理和支撑服务。

3、 自 2016 年起天泰网络参与上海市及浦东新区网络安全、数据安全专项检查的技术支撑，熟悉上海市及浦东新区网络安全检查的内容、要求和流程，能为浦东公交网络安全、数据安全提供高效优质的服务；

4、 天泰网络自主研发的安全防护产品参与了国家标准和行业标准的制定，已成功在浦东新区人大、财政、建交委、科经委、卫健委、教育局等行业应用，作为服务工具可为浦东公交提供安全可靠的安全防护服务；

5、 本次项目天泰网络将安排领导、管理能力强、资源协调调度得力、善于开拓创新的项目负责人参与项目管理协调，保障项目沟通及时、管理高效，同时派遣有经验、有担当的安全服务队伍为用户提供专业服务，天泰网络的专家团队为项目提供高端和紧急支持，以确保项目的服务质量和项目进度达到预期；

6、 天泰网络重视服务的过程管理，及时响应用户的需求，提供贴心的服务，注重用户的评价和满意度，多次获得浦东新区多个党政机关的服务满意表扬，与浦东公交合力追求信息系统无重大网络安全事故、安全治理高成效，天泰网络具有良好的安全服务履约经历，未发生过服务纠纷和投诉。

上海天泰网络技术有限公司

2026 年 4 月 10 日

目录

一、 声明书

致上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）系中华人民共和国合法企业，经营地址上海市浦东新区盛荣路 88 弄 1 号 9 层 01 室 。

我吉训敢（姓名）系上海天泰网络技术有限公司（投标人名称）的法定代表人，我方愿意参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标有关事项郑重声明如下：

1、我方已详细审查全部招标文件，同意招标文件的各项要求。

2、我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3、若中标，我方将按招标文件规定履行合同责任和义务。

4、我方不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。

5、投标文件自开标日起有效期为 90 天。

6、我方参与本项目前 3 年内的经营活动中没有重大违法记录；

7、我方通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询，未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

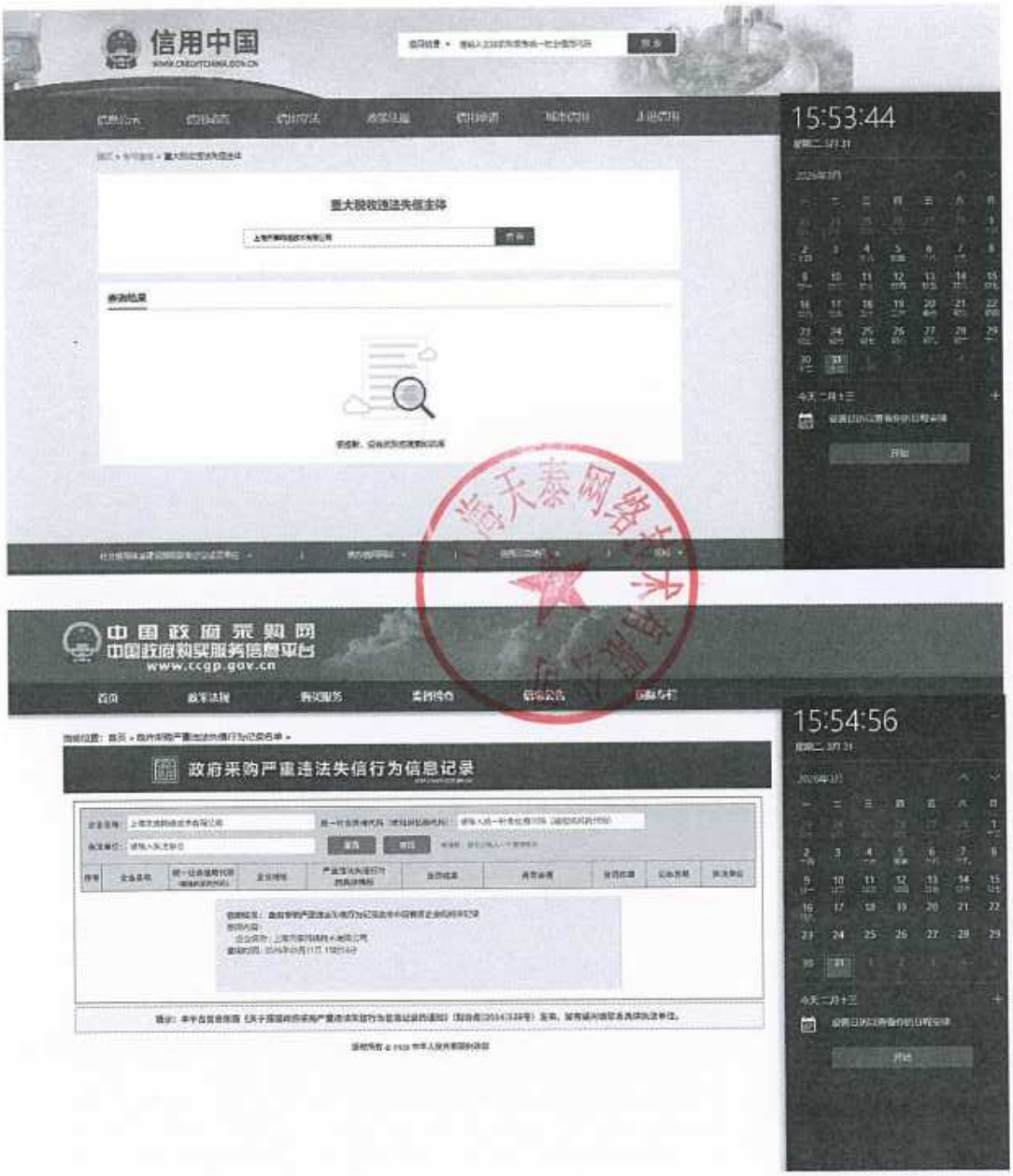
8、以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

法定代表人签名（或签名章）：

日期：2026 年 4 月 10 日

投标人全称（公章）：上海天泰网络技术有限公司

二、 信用查询


信用中国
重大税收违法失信主体
15:53:44
中国政府采购网
中国政府购买服务信息平台
www.ccgp.gov.cn
15:54:56
政府采购严重违法失信行为信息记录


失信被执行人(自然人)公布
失信被执行人(法人或其他组织)公布
15:54:34
查询条件
查询结果
全国法院失信被执行人名单信息公布与查询平台首页
声明

三、 法定代表人授权委托书

上海衷洲管理咨询有限公司：

我吉训敢（姓名）系上海天泰网络技术有限公司（投标人名称）的法定代表人，现授权委托本单位在职职工王鑫（姓名）为授权代表，以我方的名义参加项目编号：GQ31011500026031720025 2项目名称：2026 年度浦东公交网络安全服务项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对授权代表的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。授权代表在授权书有效期内签署的所有文件不因授权的撤销而失效。

授权代表无转委托权，特此委托。

授权代表签名：王鑫 职务：商务

授权代表身份证号码：310225199403254016

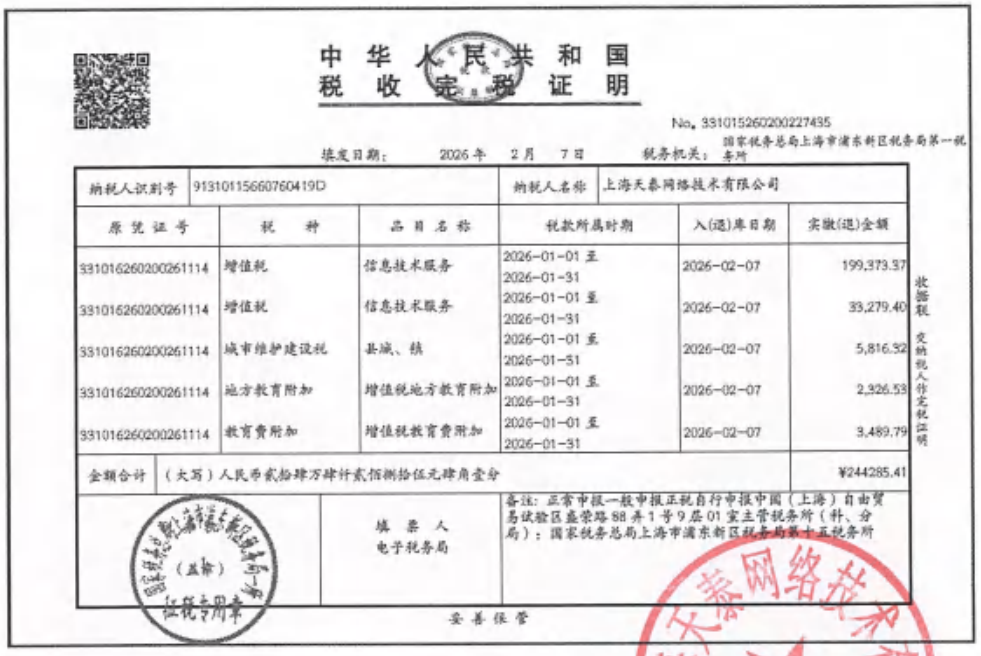
法定代表人签名（或签名章）：吉训敢 职务：董事长

投标人全称（公章）：上海天泰网络技术有限公司 日 期：2026 年 4 月 10 日

四、 营业执照


统一社会信用代码
91310115660760419D
证照编号：41000090202603255125
营业执照
名 称 上海天秦网络技术有限公司
类 型 有限责任公司(自然人投资或控股)
法定代表人 吉训敢
经营范围 依法须经批准的项目，经相关部门批准后方可开展经营活动，具体经营项目以相关部门批准文件或许可证件为准；除依法须经批准的项目外，凭营业执照依法自主开展经营活动。如需查询经营信息公示信息，可扫描营业执照中“二维码”或登录“国家企业信用信息公示系统”
中国（上海）自由贸易试验区
注册资本 人民币3300.0000万元整
成立日期 2007年06月12日
住 所 中国（上海）自由贸易试验区盛荣路88弄1号9层01室
登记机关
2026 年 03月 25日
国家企业信用信息公示系统网址：http://www.gsxt.gov.cn
国家市场监督管理总局监制

五、 纳税、社保缴纳证明



中华人民共和国
税收完税证明

No. 331015260200227435

填发日期：2026年2月7日　　税务机关：国家税务总局上海市浦东新区税务局第一税务所

纳税人识别号	91310115660760419D	纳税人名称	上海天泰网络技术有限公司

原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
331016260200261114	增值税	信息技术服务	2026-01-01至2026-01-31	2026-02-07	199,373.37
331016260200261114	增值税	信息技术服务	2026-01-01至2026-01-31	2026-02-07	33,279.40
331016260200261114	城市维护建设税	县城、镇	2026-01-01至2026-01-31	2026-02-07	5,816.32
331016260200261114	地方教育附加	增值税地方教育附加	2026-01-01至2026-01-31	2026-02-07	2,326.53
331016260200261114	教育费附加	增值税教育费附加	2026-01-01至2026-01-31	2026-02-07	3,489.79

金额合计	（大写）人民币贰拾肆万肆仟贰佰捌拾伍元肆角壹分	¥244285.41

填票人
电子税务局

备注：正常申报一般申报正税自行申报中国（上海）自由贸易试验区盛荣路88弄1号9层01室主管税务所（科、分局）：国家税务总局上海市浦东新区税务局第十五税务所

（盖章）征税专用章

妥善保管

收据联　交纳税人作完税证明

中华人民共和国
税收完税证明

No.431015260200455963

填发日期：2026年2月28日　　税务机关：国家税务总局上海市浦东新区税务局

纳税人识别号	91310115660760419D	纳税人名称	上海天泰网络技术有限公司

原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
431016260200346299	企业职工基本养老保险费	职工基本养老保险(单位缴纳)	2026-01-01至2026-01-31	2026-02-05	77,441.60
431016260200346299	企业职工基本养老保险费	职工基本养老保险(个人缴纳)	2026-01-01至2026-01-31	2026-02-05	38,720.80
431016260200346299	失业保险费	失业保险(单位缴纳)	2026-01-01至2026-01-31	2026-02-05	2,420.11
431016260200346299	失业保险费	失业保险(个人缴纳)	2026-01-01至2026-01-31	2026-02-05	2,420.11
431016260200346299	基本医疗保险费	职工基本医疗保险(单位缴纳)	2026-01-01至2026-01-31	2026-02-05	41,140.91

金额合计	（大写）壹拾陆万贰仟壹佰肆拾叁元伍角叁分	¥162,143.53

税收业务专用章

填票人

备注

妥善保管

收据联　交纳税人作完税证明

中华人民共和国税收完税证明

No.431015260200455964

填发日期：2026年2月28日　　税务机关：国家税务总局上海市浦东新区税务局

纳税人识别号	91310115660760419D	纳税人名称	上海天泰网络技术有限公司

原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
431016260200346299	基本医疗保险费	职工基本医疗保险(个人缴纳)	2026-01-01至2026-01-31	2026-02-05	9,680.20
431016260200346299	基本医疗保险费	地方附加医疗保险	2026-01-01至2026-01-31	2026-02-05	2,420.11
431016260200346299	工伤保险费	工伤保险	2026-01-01至2026-01-31	2026-02-05	968.00
金额合计	(大写)人民币壹万叁仟零陆拾捌元壹角壹分				¥13,068.31

填票人　　备注

收据联　交纳税人作完税证明

妥善保管

单位职工参加城镇基本养老保险情况

参保名称：上海天泰网络技术有限公司　　社会保险码:00294634

序号	姓名	证件号码	上月缴费状态
39	赵建飞	41128119790209405X	参保缴费
58	刘炜	150823198901070346	参保缴费
61	齐健	220202199112292411	参保缴费
70	沈晓勇	411122198707102535	参保缴费
75	曹兴戴	430482198812106525	参保缴费
83	吴纪	341226198502282731	参保缴费
101	叶琦	310115199001251930	参保缴费
102	黄晨瑜	310225199802243023	参保缴费
106	王彩霞	622426199608231581	参保缴费
109	王鑫	310225199403254016	参保缴费
110	吴康	362330200009011633	参保缴费
113	汤金苗	342622199107077318	参保缴费

第 1 页

上海市社会保险事业管理中心

打印日期：2026年04月07日

六、 联合投标协议书（本单位不适用）

甲方：

乙方：

（如果有的话，可按甲、乙、丙、丁…序列增加）

各方经协商，就响应_____组织实施的编号为号的招标活动联合进行投标之事宜，达成如下协议：

一、各方一致决定，以_____为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或授权代理人根据招标文件规定及投标内容而对招标方和采购人所作的任何合法承诺，包括书面澄清及响应等均对联合投标各方产生约束力。如果中标并签订合同，则联合投标各方将共同履行对招标方和采购人所负有的全部义务并就采购合同约定的事项对采购人承担连带责任。

三、联合投标其余各方保证对主办人为响应本次招标而提供的产品和服务提供全部质量保证及售后服务支持。

四、本次联合投标中，甲方承担的工作和义务为：

乙方承担的工作和义务为：

五、有关本次联合投标的其他事宜：

六、本协议提交招标方后，联合投标各方不得以任何形式对上述实质内容进行修改或撤销。

七、本协议签约各方各持一份，并作为投标文件的一部分。

甲方单位：（公章）　　乙方单位：　（公章）

法定代表人：（签章）　　法定代表人：　（签章）

日期：　年　月　日　　日　期：　年　月　日

七、 联合投标授权委托书（本单位不适用）

本授权委托书声明：根据_____与_____签订的《联合投标协议书》的内容，主办人_____的法定代表人____现授权_____为联合投标代理人，代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与这有关的一切事务，联合投标各方均予以认可并遵守。

特此委托。

授权人（签名）：

日期：年 月 日授权代表（签名）；日期： 年 月 日

联合体甲方单位： （公章） 联合体乙方单位： （公章）

法定代表人： （签章） 法定代表人： （签章）

日 期： 年 月 日 日 期： 年 月 日

八、 其他资质材料

8.1 单位服务资质-信息系统安全运维服务资质

信息安全服务资质认证证书

证书编号：CCRC-2019-ISV-SM-158

兹证明

上海天泰网络技术有限公司

统一社会信用代码：91310115660760419D

信息系统安全运维服务资质符合

CCRC-ISV-C01:2021《信息安全服务规范》

CCRC-ISV-R01:2022《信息安全服务资质认证实施规则》

三级服务资质要求

注册地址：中国（上海）自由贸易试验区盛荣路88弄1号9层01室

办公地址：上海市浦东新区盛荣路88弄1号楼901室

发证日期：2025年5月27日　　有效期至：2028年5月26日

首次颁证日期：2019年3月1日

证书有效期内本证书的有效性依据发证机构的定期监督获得保持。

CNAS 中国认可 产品 PRODUCT CNAS C066-P

陈建良 Signed: Chen Jianliang

中国网络安全审查认证和市场监管大数据中心

CHINA CYBERSECURITY REVIEW, CERTIFICATION AND MARKET REGULATION BIG DATA CENTER

中国·北京·朝阳区惠新里241号 100029

No.241 Huixinli Street, Chaoyang District, Beijing, 100029 China

8.2 单位服务资质-信息安全风险评估服务资质

CCRC

信息安全服务资质认证证书

证书编号：CCRC-2019-ISV-RA-557

兹证明

上海天泰网络技术有限公司

统一社会信用代码：91310115660760419D

信息安全风险评估服务资质符合

CCRC-ISV-C01:2021《信息安全服务规范》

CCRC-ISV-R01:2022《信息安全服务资质认证实施规则》

三级服务资质要求

注册地址：中国（上海）自由贸易试验区盛荣路88弄1号9层01室

办公地址：上海市浦东新区盛荣路88弄1号楼901室

发证日期：2025年5月27日　　有效期至：2028年5月26日

首次颁证日期：2019年3月1日

证书有效期内本证书的有效性依据发证机构的定期监督获得保持。

CNAS 中国认可 产品 PRODUCT CNAS C066-P

陳建良

Signed: Chen Jianliang

证书可通过扫描二维码或网站查询 The certificate can be verified through scanning the QR code or the website: cx.cncca.cn or www.isccc.gov.cn

中国网络安全审查认证和市场监管大数据中心

CHINA CYBERSECURITY REVIEW, CERTIFICATION AND MARKET REGULATION BIG DATA CENTER

中国·北京·朝阳区惠新里241号 100029

No.241 Huixinli Street, Chaoyang District, Beijing, 100029 China

8.3 单位服务资质-信息安全应急处理服务资质

CCRC

信息安全服务资质认证证书

证书编号:CCRC-2024-ISV-ER-1036

兹证明

上海天泰网络技术有限公司

统一社会信用代码：91310115660760419D

的**信息安全应急处理**服务资质符合

CCRC-ISV-C01:2021《信息安全服务规范》

CCRC-ISV-R01:2022《信息安全服务资质认证实施规则》

三级服务资质要求。

注册地址:中国（上海）自由贸易试验区盛荣路88弄1号9层01室

办公地址:上海市浦东新区盛荣路88弄1号楼901室

发证日期：2024年2月29日有效期至：2027年2月27日

首次颁证日期：2024年2月29日

证书有效期内本证书的有效性依据发证机构的定期监督获得保持。

CCRC

CNAS 中国认可 产品 PRODUCT CNAS C066-P

魏昊

Signed: Wei Hao

中国网络安全审查技术与认证中心

CHINA CYBERSECURITY REVIEW TECHNOLOGY AND CERTIFICATION CENTER

中国·北京·朝外大街甲10号 100020

A10 Chaowai Street, Beijing, 100020 China

证书可通过网站或扫描二维码查询 cx.cnca.cn www.isccc.gov.cn

The certificate can be verified through scanning the QR code or the website: cx.cnca.cn or www.isccc.gov.cn.

8.4 单位服务资质-信息系统安全集成服务资质

CCRC

信息安全服务资质认证证书

证书编号:CCRC-2024-ISV-SI-4322

兹证明

上海天泰网络技术有限公司

统一社会信用代码：91310115660760419D

的信息系统安全集成服务资质符合

CCRC-ISV-C01:2021《信息安全服务规范》

CCRC-ISV-R01:2022《信息安全服务资质认证实施规则》

三级服务资质要求。

注册地址:中国（上海）自由贸易试验区盛荣路88弄1号9层01室

办公地址:上海市浦东新区盛荣路88弄1号楼901室

发证日期：2024年2月29日有效期至：2027年2月27日

首次颁证日期：2024年2月29日

证书有效期内本证书的有效性依据发证机构的定期监督获得保持。

CCRC

CNAS 中国认可 产品 PRODUCT CNAS C066-P

魏昊

Signed: Wei Hao

中国网络安全审查技术与认证中心

CHINA CYBERSECURITY REVIEW TECHNOLOGY AND CERTIFICATION CENTER

中国·北京·朝外大街甲10号 100020

A10 Chaowai Street, Beijing, 100020 China

证书可通过网站或扫描二维码查询 cx.cnca.cn www.isccc.gov.cn

The certificate can be verified through scanning the QR code or the website: cx.cnca.cn or www.isccc.gov.cn.

8.5 软件企业证书

软件企业认定证书

经审核，上海天泰网络技术有限公司 符合《鼓励软件产业和集成电路产业发展的若干政策》和《软件企业认定标准及管理办法》（试行）的有关规定，认定为软件企业，特发此证。

证书编号：沪R-2008-0109 发证机关：上海市信息化委员会

二〇〇八年 五 月 十 日

8.6 高新技术企业证书

高新技术企业

证书

企业名称：上海天泰网络技术有限公司　　证书编号：GR202231009113

发证时间：2022 年 12 月 14 日　　有 效 期：三年

批准机关：

上海市科学技术委员会　上海市财政局　国家税务总局上海市税务局

关于公示西门子数字医疗科技（上海）有限公司等企业拟认定高新技术企业的通知

发布日期：2025-12-11

沪高企认办〔2025〕017号

各有关单位：

根据科技部、财政部、国家税务总局《高新技术企业认定管理办法》（国科发火〔2016〕32号）、《高新技术企业认定管理工作指引》（国科发火〔2016〕195号）、《上海市高新技术企业认定管理实施办法》（沪科合〔2021〕21号）的有关规定，经审查，现将西门子数字医疗科技（上海）有限公司等1638家符合认定条件的拟认定高新技术企业（名单详见附件）予以公示。

单位和个人对其中企业有异议的，自公布之日起10个工作日内向上海市高新技术企业认定办公室以书面形式提出。提出异议时应当对有异议的企业存在不符合高新技术企业认定条件的具体问题有清楚的表述，并提供相关证据材料。对于收到的任何异议材料，我们将严格按照有关规定办理。异议材料请署名联系人真实姓名及联系方式。

联系地址：钦州路100号1号楼307室

联系人：曹迪新、江淼、吴雪雷

电话：64839009转230、229、236

传真：53088678

邮编：200231

上海市高新技术企业认定办公室

2025年12月11日

附件

拟认定高新技术企业名单

序号	企业名称	主管部门	统一社会信用代码
[illegible]	[illegible]	[illegible]	[illegible]
1300	上海天泰网络技术有限公司	张江园	91310115660760419D

8.7 专精特新中小企业

8.8 质量管理体系认证证书

北京航协认证中心有限责任公司

质量管理体系认证证书

上海天泰网络技术有限公司

注 册 号： 03425Q50780R4M

统一社会信用代码： 91310115660760419D

注册地址： 中国(上海)自由贸易试验区盛荣路88弄1号9层01室

审核地址： 中国(上海)自由贸易试验区盛荣路88弄1号9层01室

管理体系符合： GB/T 19001-2016/ISO 9001:2015

证书覆盖范围： 网络应用安全软件系统的设计开发与服务

颁证日期： 2025年07月23日　　证书有效期至： 2028年08月07日

初次颁证日期： 2013年09月10日

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C034-M

总经理：

北京航协认证中心有限责任公司

本证书颁发后，3年有效期内要至少接受2次监督审核，证书即时有效性可通过网站查询 www.bjhxcc.com.cn

本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询，也可扫描右下角的二维码查询。

地址：北京市朝阳区京顺路七号

8.9 专利证书

证书号第2843439号

发明专利证书

发明名称：一种全自动的WEB客户端人机识别的方法

发明人：叶志强;程胜年

专利号：ZL 2012 1 0557507.8

专利申请日：2012年12月20日

专利权人：上海天泰网络技术有限公司

授权公告日：2018年03月13日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年12月20日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长
申长雨

国家知识产权局

2018年03月13日

第1页(共1页)

证书号第8544138号

专利公告信息

发明专利证书

发明名称：基于主动侦测的网络攻击智能动态防护系统及方法

专利权人：上海天泰网络技术有限公司

地　　址：201203 上海市浦东新区盛荣路88弄1号9层01室

发 明 人：王笑;汤金苗;王彩霞;赵建飞;齐健

专　利　号：ZL 2025 1 1396031.8　　授权公告号：CN 120896782 B

专利申请日：2025年09月28日　　授权公告日：2025年12月05日

申请日时申请人：上海天泰网络技术有限公司

申请日时发明人：王笑;汤金苗;王彩霞;赵建飞;齐健

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，并予以公告。

专利权自授权公告之日起生效。专利权有效性及专利权人变更等法律信息以专利登记簿记载为准。

局长
申长雨

国家知识产权局
2025年12月05日

8.10 中华人民共和国国家标准GA-中小电子商务企业信息安全建设

ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 32906—2016

信息安全技术
中小电子商务企业信息安全建设指南

Information security technology—Guide of construction for information security in small & medium E-commerce enterprises

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本指导性技术文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本指导性技术文件起草单位:浙江省标准化研究院、阿里巴巴(中国)有限公司、浙江工商大学、浙江经济信息中心、厦门标准化研究院、浙江科技学院、浙江飘飘龙网络科技有限公司、浙江富春江通信移动集团有限公司、北京天融信科技有限公司、上海天泰网络技术有限公司、中国计量学院。

本指导性技术文件主要起草人:李宁、刘璇、焦庆春、颜鹰、周广平、马骏、谢俊军、胡蓓姿、邵俊、刘若微、沈锦镭、陈宇、夏祖军、叶志强、范丙华等。

8.11 计算机软件著作权登记证书-天泰 WEB 安全防护软件

计算机软件著作权
登记证书

编号:软著登字第 109942 号

登 记 号:2008SR22763

软件名称:天泰WEB安全防护软件V1.0

著作权人:上海天泰网络技术有限公司

权利取得方式:原始取得

权 利 范 围:全部权利

首次发表日期:2008年06月24日

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定,对以上事项予以登记。

2008 年 10 月 09 日

8.12 中华人民共和国国家标准 GB-WEB 应用防火墙

ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32917—2016

信息安全技术 WEB 应用防火墙安全技术要求与测试评价方法

Information security technology—
Security technique requirements and testing and evaluation approaches for WEB application firewall

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所、上海天臣网络技术有限公司、北京神州绿盟科技有限公司、北京中软华泰信息技术有限责任公司。

本标准主要起草人:邱梓华、张艳、顾健、胡亚兰、叶志强、李从宇、宋万龙、俞优、程胜年、罗宇、任浩、张筑笑、宋好好、吴其聪。

8.13 中华人民共和国公共安全行业标准 GA-WEB 应用防火墙

ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1140—2014

信息安全技术
web 应用防火墙安全技术要求

Information security technology—
Security technical requirements for web application firewall

2014-03-12 发布　　2014-03-12 实施

中华人民共和国公安部　发布

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、杭州安恒信息技术有限公司、神州数码网络(北京)有限公司、北京安氏领信科技发展有限公司、北京神州绿盟信息安全科技股份有限公司、蓝盾信息安全技术股份有限公司、上海天泰网络技术有限公司、公安部第三研究所。

本标准主要起草人：俞优、陆臻、李毅、顾健、张笑笑、张艳、杨元原、范渊、孙小平、黄坚、高继明、秦波、杨青婉、叶志强。

8.14 中华人民共和国公共安全行业标准 GA-WEB 应用安全扫描

ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1107—2013

信息安全技术
web 应用安全扫描产品安全技术要求

Information security technology—
Security technical requirements for web application security scanning products

2013-10-15 发布　　2013-10-15 实施

中华人民共和国公安部　发布

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

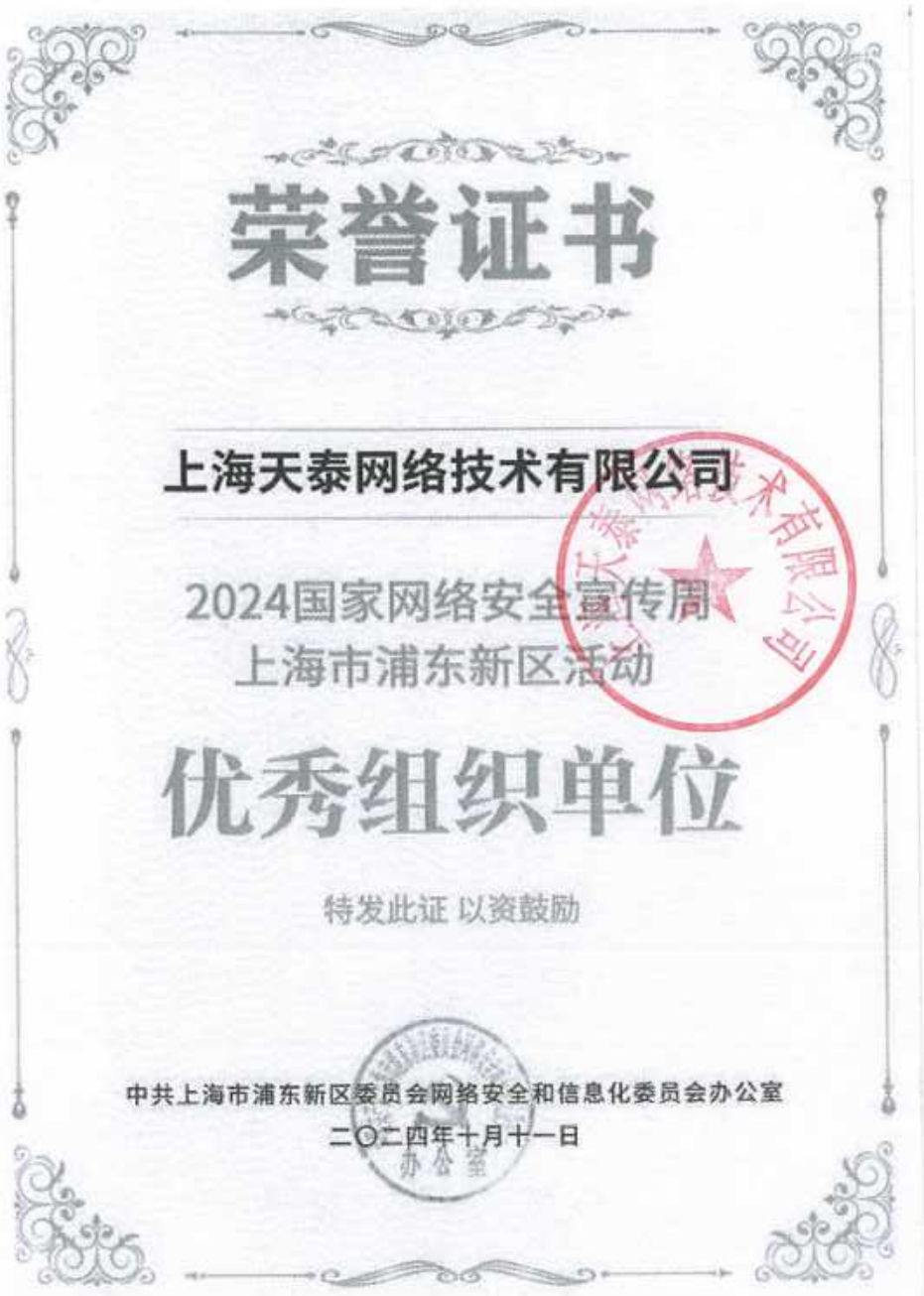
本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、杭州安恒信息技术有限公司、中联绿盟信息技术(北京)有限公司、北京国舜科技有限公司、上海天泰网络技术有限公司。

本标准主要起草人：俞优、张艳、沈亮、顾健、陆辉、杨元原、李毅、苍渊、邹春明、张笑笑、顾建新、宋好好、孙小平、李晟、姜强、程胜年。

8.15获奖情况及社会信用信誉证明

8.15.1 2024 国家网络安全宣传周上海市浦东新区活动-优秀组织单位


荣誉证书

上海天泰网络技术有限公司

2024国家网络安全宣传周
上海市浦东新区活动

优秀组织单位

特发此证 以资鼓励

中共上海市浦东新区委员会网络安全和信息化委员会办公室
二〇二四年十月十一日

8.15.2　上海市信息安全行业协会优秀会员单位

8.15.3 上海市网络与信息安全服务信息推荐单位

8.15.4　上海市信息网络安全管理协会-会员单位

九、 项目资格审查要求响应表

审查要求	应标说明	备注
符合《中华人民共和国政府采购法》第二十二条的规定	天泰符合《中华人民共和国政府采购法》第二十二条的规定	天泰提供承诺函
未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单	天泰未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单	
具有独立承担民事责任的能力；	天泰具有独立承担民事责任的能力；	
具有良好的商业信誉和健全的财务会计制度；	天泰具有良好的商业信誉和健全的财务会计制度；	
具有履行合同所必需的设备和专业技术能力；	天泰具有履行合同所必需的设备和专业技术能力；	
有依法缴纳税收和社会保障资金的良好记录；	天泰有依法缴纳税收和社会保障资金的良好记录；	
参加政府招标活动前三年内，在经营活动中没有重大违法记录；	天泰参加政府招标活动前三年内，在经营活动中没有重大违法记录；	
法律、行政法规规定的其他条件。	天泰遵纪守法，满足法律、行政法规规定的其他条件。	

十、 其他承诺及财务审计报告

10.1 符合《中华人民共和国政府采购法》第二十二条的规定

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ310115000260317200252）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

符合《中华人民共和国政府采购法》第二十二条的规定。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.2 未被“信用中国”、中国政府采购网列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ31011500026031720025 2）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.3 具有独立承担民事责任的能力

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

具有独立承担民事责任的能力。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.4 具有良好的商业信誉和健全的财务会计制度

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

具有良好的商业信誉和健全的财务会计制度。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

上海天泰网络技术有限公司

旭升会审字（2025）第109号

审 计 报 告

上海旭升会计师事务所（普通合伙）

中国.上海

上海旭升会计师事务所（普通合伙）

SHANGHAI XUSHENG CERTIFIED PUBLIC ACCOUNTINGS GP

审计报告

旭升会审字（2025）第 109 号

上海天泰网络技术有限公司全体股东：

一、审计意见

我们审计了上海天泰网络技术有限公司（以下简称贵公司）财务报表，包括 2024 年 12 月 31 日的资产负债表，2024 年度的利润表、现金流量表以及相关财务报表附注。

我们认为，后附的财务报表在所有重大方面按照小企业会计准则的规定编制，公允反映了贵公司 2024 年 12 月 31 日的财务状况以及 2024 年度的经营成果和现金流量。

二、形成审计意见的基础

我们按照中国注册会计师审计准则的规定执行了审计工作。审计报告的"注册会计师对财务报表审计的责任"部分进一步阐述了我们在这些准则下的责任。按照中国注册会计师职业道德守则，我们独立于贵公司，并履行了职业道德方面的其他责任。我们相信，我们获取的审计证据是充分、适当的，为发表审计意见提供了基础。

三、管理层和治理层对财务报表的责任

管理层负责按照小企业会计准则的规定编制财务报表，使其实现公允反映，并设计、执行和维护必要的内部控制，以使财务报表不存在由于舞弊或错误导致的重大错报。

在编制财务报表时，管理层负责评估贵公司的持续经营能力，披露与持续经营相关的事项，并运用持续经营假设，除非管理层计划清算贵公司、终止运营或别无其他现实的选择。

治理层负责监督贵公司的财务报告过程。

四、注册会计师对财务报表审计的责任

我们的目标是对财务报表整体是否不存在由于舞弊或错误导致的重大错报获取合理保证，并出具包含审计意见的审计报告。合理保证是高水平的保证，但并不能保证按照审计准则执行的审计在某一重大错报存在时总能发现。错报可能由于舞弊或错误导致，如果合理预期错报单独或汇总起来可能影响财务报表使用者依据财务报表作出的经济决策，则通常认为错报是重大的。

在按照审计准则执行审计工作的过程中，我们运用职业判断，并保持职业怀疑。同时，

我们也执行以下工作：

（1）识别和评估由于舞弊或错误导致的财务报表重大错报风险，设计和实施审计程序以应对这些风险，并获取充分、适当的审计证据，作为发表审计意见的基础。由于舞弊可能涉及串通、伪造、故意遗漏、虚假陈述或凌驾于内部控制之上，未能发现由于舞弊导致的重大错报的风险高于未能发现由于错误导致的重大错报的风险。

（2）了解与审计相关的内部控制，以设计恰当的审计程序，但目的并非对内部控制的有效性发表意见。

（3）评价管理层选用会计政策的恰当性和作出会计估计及相关披露的合理性。

（4）对管理层使用持续经营假设的恰当性得出结论。同时，根据获取的审计证据，就可能导致对贵公司持续经营能力产生重大疑虑的事项或情况是否存在重大不确定性得出结论。如果我们得出结论认为存在重大不确定性，审计准则要求我们在审计报告中提请报表使用者注意财务报表中的相关披露；如果披露不充分，我们应当发表非无保留意见。我们的结论基于截至审计报告日可获得的信息。然而，未来的事项或情况可能导致贵公司不能持续经营。

（5）评价财务报表的总体列报、结构和内容（包括披露），并评价财务报表是否公允反映相关交易和事项。

我们与治理层就计划的审计范围、时间安排和重大审计发现等事项进行沟通，包括沟通我们在审计中识别出的值得关注的内部控制缺陷。

上海旭升会计师事务所（普通合伙）

中国·上海

中国注册会计师：

中国注册会计师：

二〇二五年四月二日

资产负债表

会小企01表

编制单位：上海天泰网络技术有限公司　　2024年12月31日　　单位：元

资产	行次	期末余额	期初余额	负债和所有者权益	行次	期末余额	期初余额
流动资产：				流动负债：			
货币资金	1	9,718,639.88	8,923,695.65	短期借款	31	5,000,000.00	6,000,000.00
短期投资	2	-		应付票据	32	-	
应收票据	3	-		应付账款	33	37,363.75	1,092,004.98
应收账款	4	8,257,853.75	906,153.63	预收账款	34	51,412.07	51,412.71
预付账款	5	1,869,690.00	8,397,663.75	应付职工薪酬	35	-	374,000.00
应收股利	6	-		应交税费	36	246,991.18	302,498.56
应收利息	7	-		应付利息	37	-	
其他应收款	8	612,993.80	1,891,263.50	应付利润	38	-	
存货	9	611,844.69	1,972,648.24	其他应付款	39	44,803.26	192,000.00
其中：原材料	10	-		其他流动负债	40	-	
在产品	11	-		流动负债合计	41	5,380,570.26	8,011,916.25
库存商品	12	611,844.69	1,972,648.24				
周转材料	13	-		非流动负债：			
其他流动资产	14	-		长期借款	42	-	
流动资产合计	15	21,071,022.12	22,091,424.77	长期应付款	43	-	
非流动资产：				递延收益	44	-	
长期债券投资	16	-		其他非流动负债	45	-	
长期股权投资	17			非流动负债合计	46	-	-
固定资产原价	18	3,321,044.57	2,943,186.19	负债合计	47	5,380,570.26	8,011,916.25
减：累计折旧	19	2,598,523.76	2,511,818.55				
固定资产账面价值	20	722,520.81	431,367.64				
在建工程	21	-					
工程物资	22	-					
固定资产清理	23	-					
生产性生物资产	24	-		所有者权益（或股东权益）：			
无形资产	25	13,979,655.45	15,304,399.17	实收资本（或股本）	48	33,000,000.00	33,000,000.00
开发支出	26			资本公积	49	-	
长期待摊费用	27	-		盈余公积	50	201,396.87	143,661.59
其他非流动资产	28	-		未分配利润	51	-2,808,768.75	-3,328,386.26
非流动资产合计	29	14,702,176.26	15,735,766.81	所有者权益（或股东权益）合计	52	30,392,628.12	29,815,275.33
资产总计	30	35,773,198.38	37,827,191.58	负债和所有者权益（或股东权益）总计	53	35,773,198.38	37,827,191.58

法定代表人：　　主管会计工作负责人：　　会计机构负责人：

利 润 表

会小企 02 表

编制单位：上海天秦网络技术有限公司　　2024年度　　单位：元

项　目	行次	本期金额	上期金额
一、营业收入	1	32,682,588.74	27,339,277.21
减：营业成本	2	15,522,333.81	14,972,723.06
税金及附加	3	66,149.53	46,982.46
其中：	4	-	
消费税	5	-	
城市维护建设税	6	-	
资源税	7	-	
土地增值税	8	-	
城镇土地使用税、房产税、车船税、印花税	9	-	
教育费附加、矿产资源补偿费、排污费	10	-	
销售费用	11	1,107,184.04	1,147,717.60
其中：商品维修费	12	-	
广告费和业务宣传费	13	-	
管理费用	14	12,295,614.42	10,505,222.93
其中：开办费	15		
业务招待费	16		
研究费用	17	7,439,554.36	7,396,552.38
财务费用	18	169,670.65	208,081.85
其中：利息费用（收入以“-”号填列）	19	168,833.25	207,165.35
加：投资收益（损失以“-”号填列）	20	-	
二、营业利润（亏损以“-”号填列）	21	3,521,636.29	458,549.31
加：营业外收入	22	1,195,310.25	201,088.19
其中：政府补助	23	1,107,000.00	
减：营业外支出	24	4,139,593.75	52,518.16
其中：坏账损失	25	4,139,593.75	52,000.01
无法收回的长期债券投资损失	26	-	-
无法收回的长期股权投资损失	27	-	-
自然灾害等不可抗力因素造成的损失	28	-	-
税收滞纳金	29	-	518.15
三、利润总额（亏损总额以“-”号填列）	30	577,352.79	607,119.34
减：所得税费用	31	-	
四、净利润（净亏损以“-”号填列）	32	577,352.79	607,119.34

法定代表人：　　主管会计工作负责人：　　会计机构负责人：

现金流量表

会小企 03 表

编制单位：上海乐泰网络技术有限公司　　2024年度　　单位：元

项　目	行次	本期金额	上期金额
一、经营活动产生的现金流量：	1		
销售产成品、商品、提供劳务收到的现金	2	27,504,069.32	38,571,945.25
收到其他与经营活动有关的现金	3	1,305,825.97	460,508.17
购买原材料、商品、接受劳务支付的现金	4	12,738,663.79	19,258,490.50
支付的职工薪酬	5	8,416,097.72	5,912,532.95
支付的税费	6	1,424,830.99	911,418.85
支付其他与经营活动有关的现金	7	3,835,901.84	5,441,476.11
经营活动产生的现金流量净额	8	2,394,380.95	7,508,535.01
二、投资活动产生的现金流量：	9		
收回短期投资、长期债券投资和长期股权投资收到的现金	10		
取得投资收益收到的现金	11		
处置固定资产、无形资产和其他非流动资产收回的现金净额	12		
短期投资、长期债券投资和长期股权投资支付的现金	13		
购建固定资产、无形资产和其他非流动资产支付的现金	14	377,858.38	91,063.72
投资活动产生的现金流量净额	15	-377,858.38	-91,063.72
三、筹资活动产生的现金流量：	16		
取得借款收到的现金	17	5,000,000.00	6,700,000.00
吸收投资者投资收到的现金	18		
偿还借款本金支付的现金	19	6,000,000.00	7,000,000.00
偿还借款利息支付的现金	20	221,578.34	226,911.66
分配利润支付的现金	21		
筹资活动产生的现金流量净额	22	-1,221,578.34	-526,911.66
四、现金净增加额	23	794,944.23	6,890,559.63
加：期初现金余额	24	8,923,695.65	2,033,136.02
五、期末现金余额	25	9,718,639.88	8,923,695.65

法定代表人：　　主管会计工作负责人：　　会计机构负责人：

财务报表附注

一、公司基本情况

上海天泰网络技术有限公司（以下简称"本公司"）成立于 2007 年 6 月 12 日，于 2018 年 11 月 12 日换取了中国（上海）自由贸易试验区市场监督管理局换发的统一社会信用代码为 91310115660750419D 的《营业执照》，公司类型：有限责任公司(自然人投资或控股)；住所：中国(上海)自由贸易试验区盛荣路 88 弄 1 号 9 层 01 室；法定代表人：吉训敢；注册资本：人民币 3300.0000 万元整；营业期限：2007 年 6 月 12 日至 2057 年 6 月 11 日。公司经营范围为：网络技术的研发，计算机软件的开发、设计、制作、销售；硬件的研发、销售；并提供相关的技术咨询和技术服务，电子产品的销售；网络工程的安装、调试、维护。【依法须经批准的项目，经相关部门批准后方可开展经营活动】

二、财务报表的编制基础

本公司执行财政部颁布的小企业会计准则。

本公司以持续经营为基础编制财务报表。

三、遵循企业会计准则的声明

本财务报表符合小企业会计准则的要求，真实、完整地反映了企业的财务状况、经营成果和现金流量等有关信息。

四、公司主要会计政策、会计估计

1、会计年度

本公司会计年度采用公历年度，即每年自 1 月 1 日起至 12 月 31 日止。

2、记账本位币

本公司以人民币为记账本位币。

3、记账基础和计价原则

本公司会计核算以权责发生制为记账基础，资产按成本计量，不计提资产减值准备。

4、现金流量表的现金确定标准

在编制现金流量表时，现金指本公司的库存现金以及可以随时用于支付的存款和其他货币资金。

5、短期投资核算方法

短期投资核算本公司购入的能随时变现并且持有时间不准备超过 1 年（含 1 年，下同）的投资。

短期投资取得时，按照实际支付的购买价款和相关税费确认初始投资成本。实际支付价款中包含的已宣告但尚未发放的现金股利或已到付息期但尚未领取的债券利息，单独确认为应收股利或应收利息。

在短期投资持有期间，被投资单位宣告分派的现金股利或在债务人应付利息日按照分期付息、一次还本债券投资的票面利率计算的利息收入，计入当期投资收益。

处置短期投资时，出售价款扣除其账面余额、相关税费后净额，计入当期投资收益。

6、坏账核算方法

1. 本公司坏账损失采用直接转销法核算。

2. 本公司应收及预付款项符合下列条件之一的，减除可收回的金额后确认的无法收回的应收及预付款项，作为坏账损失：

（1）债务人依法宣告破产、关闭、解散、被撤销，或者被依法注销、吊销营业执照，其清算财产不足清偿的。

（2）债务人死亡，或者依法被宣告失踪、死亡，其财产或者遗产不足清偿的；

（3）债务人逾期 3 年以上未清偿，且有确凿证据证明已无力清偿债务的；

（4）与债务人达成债务重组协议或法院批准破产重整计划后，无法追偿的；

（5）因自然灾害、战争等不可抗力导致无法收回的；

（6）国务院财政、税务主管部门规定的其他条件。

应收及预付款项的坏账损失于实际发生时计入营业外支出，同时冲减应收及预付款项。

7、存货

存货是指本公司在日常生产经营过程中持有以备出售的产成品或商品、处在生产过程中的在产品、将在生产过程或提供劳务过程中耗用的材料和物料等，包括：商品、周转材料。

本公司取得的存货，按照成本进行计量。

本公司采用加权平均法确定发出存货的实际成本；对于周转材料，采用分次摊销法进行会计处理。

存货发生毁损，处置收入、可收回的责任人赔偿和保险赔款，扣除其成本、相关税费后的净额，计入营业外支出或营业外收入；盘盈存货实现的收益，计入营业外收入；盘亏存货发生的损失，计入营业外支出。

存货数量的盘存方法采用永续盘存制。

8、长期投资核算方法

1. 长期股权投资

（1）以支付现金取得的长期股权投资，应按照购买价款和相关税费作为成本进行计量；实际支付价款中包含的已宣告但尚未发放的现金股利，应当单独确认为应收股利，不计入长期股权投资的成本。通过非货币性资产交换取得的长期股权投资，应当按照换出非货币性资产的评估价值和相关税费作为成本进行计量。

（2）长期股权投资采用成本法进行会计处理。持有期间，被投资单位宣告分派的现金股利或利

润，按照应分得的金额确认为投资收益。

（3）处置长期股权投资时，处置价款扣除其成本、相关税费后的净额，计入投资收益。

（4）长期股权投资符合下列条件之一的，减除可收回的金额后确认的无法收回的长期股权投资，作为长期股权投资损失：①被投资单位依法宣告破产、关闭、解散、被撤销，或者被依法注销、吊销营业执照的；②被投资单位财务状况严重恶化，累计发生巨额亏损，已连续停止经营 3 年以上，且无重新恢复经营改组计划的；③对被投资单位不具有控制权，投资期限届满或者投资期限已超过 10 年，且被投资单位因连续 3 年经营亏损导致资不抵债的；④被投资单位财务状况严重恶化，累计发生巨额亏损，已完成清算或清算期超过 3 年以上的；⑤国务院财政、税务主管部门规定的其他条件。

长期股权投资损失于实际发生时计入营业外支出，同时冲减长期股权投资账面余额。

2. 长期债券投资

长期债券投资按照购买价款和相关税费作为成本进行计量；实际支付价款中包含的已到付息期但尚未领取的债券利息，单独确认为应收利息，不计入长期债券投资的成本。持有期间发生的应收利息确认为投资收益。债券的折价或者溢价在债券存续期间内于确认相关债券利息收入时采用直线法进行摊销。处置长期债券投资，处置价款扣除其账面余额、相关税费后的净额，计入投资收益。

9、固定资产及折旧

（1）确认条件：固定资产是指为生产商品、提供劳务、出租或经营管理而持有的使用寿命超过一个会计年度的有形资产。固定资产在同时满足下列条件时，予以确认：

①与该固定资产有关的经济利益很可能流入企业；

②该固定资产的成本能够可靠地计量。

固定资产发生的后续支出，符合规定的固定资产确认条件的计入固定资产成本；不符合规定的固定资产确认条件的在发生时计入当期损益。

（2）折旧方法：固定资产折旧采用直线法，并按固定资产类别、原价、估计经济使用年限和预计残值确定其折旧率。固定资产的分类及折旧率如下：

资产类别	预计使用年限	净残值率（%）	年折旧率（%）
办公及电子设备	3 -5 年	5	20-33.33

10、无形资产

1. 无形资产按照成本进行计量。外购无形资产的成本包括购买价款、相关税费和相关的其他支出（含相关的借款费用）；投资者投入的无形资产成本，按照评估价值和相关税费确定；自行开发的无形资产的成本，由符合资本化条件后至达到预定用途前发生的支出（含相关的借款费用）构成。

2. 无形资产在其使用寿命内采用年限平均法进行摊销，并根据其受益对象计入相关资产成本或者当期损益。摊销期限自其可供使用时开始至停止使用或出售时止。有关法律规定或合同约定了使

用年限的，按照规定或约定的使用年限分期摊销。不能可靠估计无形资产使用寿命的，摊销期限不低于 10 年。

11、长期待摊费用

本公司长期待摊费用在其受益期限内采用年限平均法进行摊销。

12、职工薪酬

职工薪酬主要包括工资、奖金、津贴和补助；职工福利费；医疗保险费、养老保险费、失业保险费、工伤保险费、生育保险费等社会保险费；住房公积金；工会经费和职工教育经费等其他与获得职工提供的服务相关的支出。于职工提供服务的期间确认职工薪酬，根据职工提供服务的收益对象计入相关的成本费用。支付给职工的解除劳动关系补偿计入当期损益。

13、收入的确认原则

1．商品销售收入

商品销售收入在发出商品且收到货款或取得收款权利时确认，按照从购买方已收或应收的合同或协议价款，确定销售商品收入金额。涉及现金折扣或商业折扣的，按照扣除现金折扣前的金额或扣除商业折扣后的金额确定销售商品收入金额。

2．提供劳务

同一会计年度内开始并完成的劳务，在提供劳务交易完成且收到款项或取得收款权利时，确认提供劳务收入。提供劳务收入的金额为从接受劳务方已收或应收的合同或协议价款。

劳务的开始和完成分属不同会计年度的，按照完工进度确认提供劳务收入。年度资产负债表日，按照提供劳务收入总额乘以完工进度扣除以前会计年度累计已确认提供劳务收入后的金额，确认本年度的提供劳务收入；同时，按照估计的提供劳务成本总额乘以完工进度扣除以前会计年度累计已确认营业成本后的金额，结转本年度营业成本。

14、政府补助

1．收到与资产相关的政府补助，确认为递延收益，并在相关资产的使用寿命内平均分配，计入营业外收入。收到的其他政府补助，用于补偿本企业以后期间的相关费用或亏损的，确认为递延收益，并在确认相关费用或发生亏损的期间，计入营业外收入；用于补偿本企业已发生的相关费用或亏损的，直接计入营业外收入。

2．政府补助为货币性资产的，应当按照收到的金额计量。政府补助为非货币性资产的，政府提供了有关凭据的，应当按照凭据上标明的金额计量；政府没有提供有关凭据的，应当按照同类或类似资产的市场价格或评估价值计量。

3．按照规定实行企业所得税、增值税、消费税、营业税等先征后返的，应当在实际收到返还的企业所得税、增值税（不含出口退税）、消费税、营业税时，计入营业外收入。

15、所得税

当期所得税是按照当期应纳税所得额计算的当期应交所得税金额，应纳税所得额系根据有关税法规定对本年度税前会计利润作相应调整后得出。

五、会计政策、会计估计变更和会计差错更正

本公司会计政策、会计估计变更和会计差错更正采用未来适用法进行会计处理。

1、会计政策、会计估计变更

本报告期内重要会计政策、会计估计未变更。

2、重大会计差错更正说明

本报告期内未有重大会计差错更正。

六、税项

按国家有关税收法律法规规定。

七、财务报表主要项目注释

1、货币资金

项　目	期末余额	期初余额
货币资金	9,718,639.88	8,923,695.65
其中：		
现金	82,569.12	83,341.73
银行存款	9,624,888.61	8,829,191.18
其他货币资金	11,182.15	11,162.74

2、应收账款

账　龄	期末余额	期初余额
应收账款	8,257,853.75	906,153.63
其中：		
1年以内（含1年）	7,837,480.00	878,659.88
1-2年（含2年）	420,373.75	27,493.75

3、预付账款

账　龄	期末余额	期初余额
预付账款	1,869,690.00	8,397,663.75
其中：		
1年以内（含1年）	1,869,690.00	6,532,400.00

1-2 年（含 2 年）		1,865,263.75

4、其他应收款

账　龄	期末余额	期初余额
其他应收款	612,993.80	1,891,263.50
其中：		
1 年以内（含 1 年）	440,488.80	937,328.50
1-2 年（含 2 年）	172,505.00	953,935.00

5、存货

项　目	期末余额	期初余额
存货	611,844.69	1,972,648.24
其中：		
库存商品	611,844.69	1,972,648.24

6、固定资产及累计折旧

项　目	期末余额	期初余额
固定资产原值	3,321,044.57	2,943,186.19
减：累计折旧	2,598,523.76	2,511,818.55
固定资产净值	722,520.81	431,367.64

7、无形资产及累计摊销

项　目	期末余额	期初余额
无形资产原值	29,926,773.88	29,926,773.88
减：累计摊销	15,947,118.43	14,622,374.71
无形资产净值	13,979,655.45	15,304,399.17

8、短期借款

项　目	期末余额	期初余额
保证借款	5,000,000.00	6,000,000.00
合　计	5,000,000.00	6,000,000.00

9、应付账款

账　龄	期末余额	期初余额
应付账款	37,363.75	1,092,004.98

其中：		
1 年以内（含 1 年）	37,363.75	1,092,004.98

10、预收账款

账　龄	期末余额	期初余额
预收账款	51,412.07	51,412.71
其中：		
1 年以内（含 1 年）	51,412.07	51,412.71

11、应付职工薪酬

项　目	期末余额	期初余额
应付职工薪酬		374,000.00
其中：		
应付职工工资		374,000.00

12、应交税费

项　目	期末余额	期初余额
应交税费	246,991.18	302,498.56
其中：		
未交增值税	213,912.20	247,901.8
个人所得税	22,383.38	42,201.68
应交附加税	10,695.60	12,395.08

13、其他应付款

账　龄	期末余额	期初余额
其他应付款	44,803.26	192,000.00
其中：		
1 年以内（含 1 年）	44,803.26	192,000.00

14、实收资本

项　目	期末余额	期初余额
实收资本	33,000,000.00	33,000,000.00

15、盈余公积

项　目	期末余额	期初余额
法定盈余公积	201,396.67	143,661.59

16、未分配利润

项　目	期末余额	期初余额
本期期初余额	-3,328,386.26	1,885,206.33
加：本期净利润	577,352.79	607,119.34
其他转入		-5,760,000.00
可供分配的利润	-2,751,033.47	-3,267,674.33
减：提取盈余公积	57,735.28	60,711.93
本期期末余额	-2,808,768.75	-3,328,386.26

17、营业收入

项　目	本期金额	上期金额
营业收入	32,682,588.74	27,339,277.21
其中：		
主营业务收入	32,682,588.74	27,339,277.21

18、营业成本

项　目	本期金额	上期金额
营业成本	15,522,333.81	14,972,723.06
其中：		
主营业务成本	15,522,333.81	14,972,723.06

19、税金及附加

项　目	本期金额	上期金额
税金及附加	66,149.53	46,982.46

20、销售费用

项　目	本期金额	上期金额
销售费用	1,107,184.04	1,147,717.60
其中：		

工资	494,380.00	669,000.00
五险一金	22,343.49	105,954.32
业务招待费		2,200.00
差旅费		10,311.00
办公费	569.80	3,879.20
租赁费	79,905.60	66,564.40
业务宣传费	252,363.23	67,230.17
招投标费	257,621.92	201,712.26

21、管理费用

项　目	本期金额	上期金额
管理费用	12,295,614.42	10,505,222.93
其中：		
工资	781,547.05	686,721.05
福利费	52,583.15	12,579.37
五险一金	168,004.52	143,992.58
职工教育经费	4,384.62	8,145.00
折旧费	86,705.21	65,243.84
租赁费	177,113.59	324,560.67
办公费	194,876.64	168,257.35
差旅费	82,647.74	66,559.31
水电费	26,976.71	28,045.39
业务招待费	1,669,893.56	1,018,356.51
无形资产摊销	1,324,743.72	364,743.72
研发费用	7,439,554.36	7,396,552.38

22、财务费用

项　目	本期金额	上期金额
财务费用	169,670.65	208,661.85
其中：		

利息支出	221,578.34	226,911.66
减：利息收入	52,745.09	19,746.31
银行手续费	837.40	918.50

23、营业外收入

项　目	本期金额	上期金额
营业外收入	1,195,310.25	201,088.19
其中：		
进项加计税额		57,131.51
增值税退税		3,263.02
政府补贴	1,107,000.00	
其他	88,310.25	140,693.66

24、营业外支出

项　目	本期金额	上期金额
营业外支出	4,139,593.75	52,518.16
其中：		
税收滞纳金		518.15
坏账损失	4,139,593.75	52,000.01

八、或有事项

截至 2024 年 12 月 31 日，本公司不存在应披露的或有事项。

九、承诺事项

截至 2024 年 12 月 31 日，本公司不存在应披露的承诺事项。

十、财务报表的批准

本财务报表及财务报表附注业经本公司管理层批准。

上海天泰网络技术有限公司

统一社会信用代码

91310113068989088

证照编号：150000002024091400032

营业执照

名　　称　上海旭升会计师事务所（普通合伙）

类　　型　普通合伙企业

执行事务合伙人　赵成钢

经营范围　审查企业会计报表、出具审计报告；验证企业资本、出具验资报告、办理企业合并、分立、清算事宜中的审计业务，出具有关报告，基本建设年度财务决算审计；代理记账；会计咨询、税务咨询、管理咨询、会计培训；法律、法规规定的其他业务。【依法须经批准的项目，经相关部门批准后方可开展经营活动】

出　资　额　人民币20.0000万元整

成立日期　2013年01月16日

主要经营场所　上海市浦东新区秀浦路3999弄1号

登记机关

2024 年 09 月 14 日

国家市场监督管理总局监制

会计师事务所

执业证书

名　　称：上海旭升会计师事务所（普通合伙）

首席合伙人：赵成锴

主任会计师：

经 营 场 所：上海市宝山区月浦镇塘湾村[illegible]幢一层3632室

组 织 形 式：普通合伙制

执业证书编号：31000361

批准执业文号：沪财会〔2013〕1号

批准执业日期：2013年1月8日

证书序号：[illegible]

说　明

1、《会计师事务所执业证书》是证明持有人经财政部门依法审批，准予执行注册会计师法定业务的凭证。

2、《会计师事务所执业证书》记载事项发生变动的，应当向财政部门申请换发。

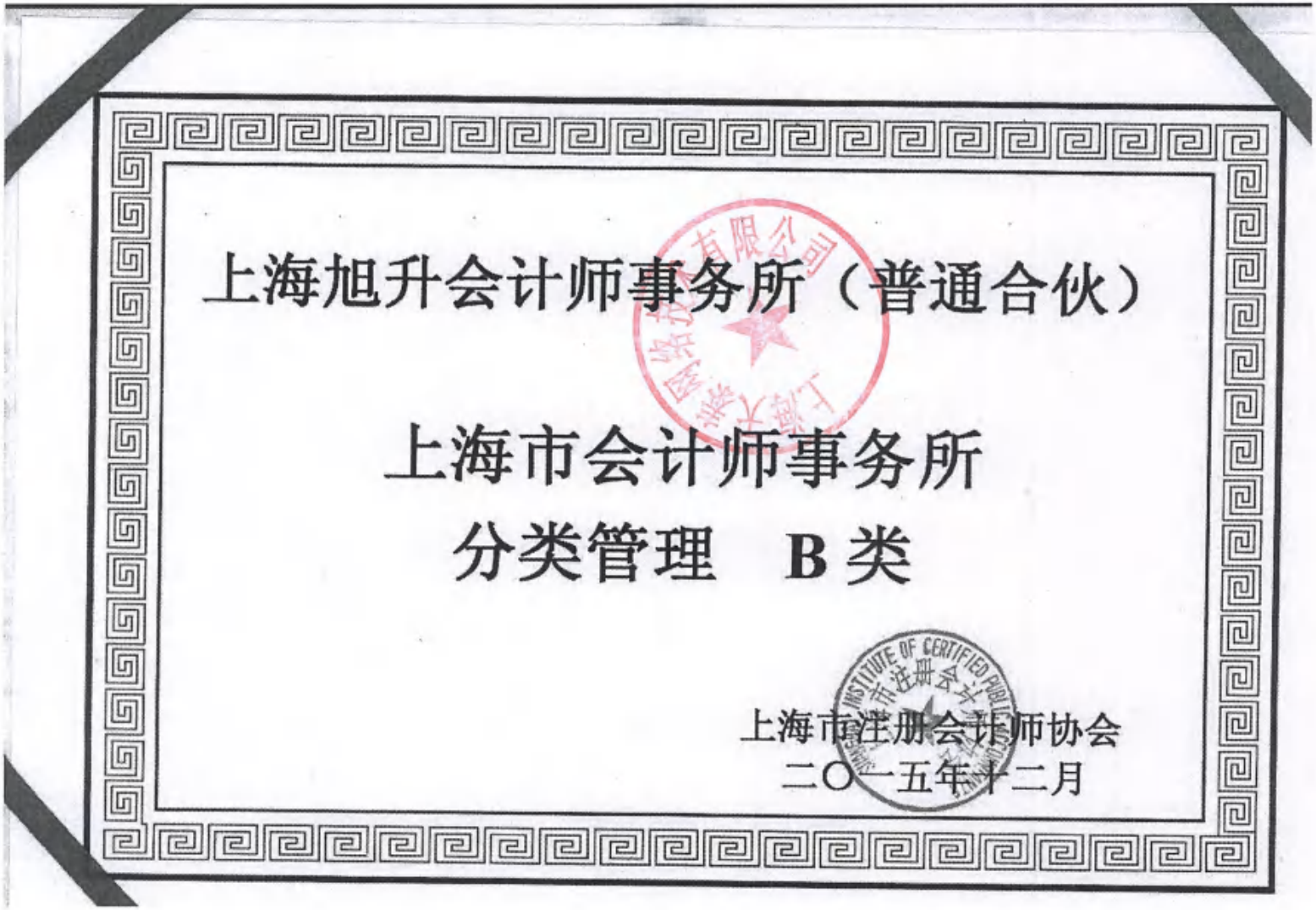
3、《会计师事务所执业证书》不得伪造、涂改、出租、出借、转让。

4、会计师事务所终止或执业许可注销的，应当向财政部门缴销《会计师事务所执业证书》。

发证机关：上海市财政局

二〇二三年八月十一日

中华人民共和国财政部制


上海旭升会计师事务所（普通合伙）
上海市会计师事务所
分类管理 B类
上海市注册会计师协会
二〇一五年十二月

10.5 具有履行合同所必需的设备和专业技术能力

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

具有履行合同所必需的设备和专业技术能力。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.6 有依法缴纳税收和社会保障资金的良好记录

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

有依法缴纳税收和社会保障资金的良好记录。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.7 参加政府招标活动前三年内，在经营活动中没有重大违法记录

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

参加政府招标活动前三年内，在经营活动中没有重大违法记录。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.8 法律、行政法规规定的其他条件

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

符合法律、行政法规规定的其他条件。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.9 按照招标文件规定要求签署、盖章

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

已按照招标文件规定要求签署、盖章。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.10　投标报价未超过投标限价

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002252）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

投标报价未超过投标限价。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.11　投标有效期满足招标文件规定

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

投标有效期满足招标文件规定。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.12　投标文件中未附有采购人不能接受条件

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

投标文件中未附有采购人不能接受条件。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.13 投标文件满足招标文件商务、技术“★”条款要求

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002252）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

投标文件满足招标文件商务、技术“★”条款要求。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.14 投标人未出现招标文件中规定无效投标的其它条款

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

投标人未出现招标文件中规定无效投标的其它条款。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

10.15　投标人未有下列任一情形

致上海浦东新区公共交通有限公司、上海衷洲管理咨询有限公司：

上海天泰网络技术有限公司（投标人名称）参加贵方组织的（2026 年度浦东公交网络安全服务项目）（编号为 GQ3101150002603172002 52）的投标，为此，我方就本次投标其他有关事项郑重承诺如下：

投标人未有下列任一情形：(1)不同投标人的投标文件由同一单位或者个人编制；(2)不同投标人委托同一单位或者个人办理投标事宜；(3)不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；(4)不同投标人的投标文件异常一致或者投标报价呈规律性差异；(5)不同投标人的投标文件相互混装。

投标人全称（公章）：上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

正本

2026年度浦东公交网络安全服务项目

项目编号：GQ31011500026031720025 2（标项1）

技术及商务文件

投标人全称：上海天泰网络技术有限公司

地址：上海市浦东新区盛荣路88弄1号9层01室

时间：2026年4月10日

目录

一、 评分对应表

评分对应表

投标人全称（公章）：上海天泰网络技术有限公司 标项：1

评分项目	投标文件对应资料	投标文件页码
项目需求理解、服务项目定位和目标确定	项目概况、项目需求理解与分析	10-21
项目实施各方案中工作计划、方法流程、时间安排	项目总体方案、项目实施进度安排	22-159 174-177
本项目的重点、难点的分析与措施、应急预案保密措施、质量考核承诺内容以及后期服务保障等方面的考虑	项目重点、难点分析及特色服务 项目管理方案 质量保障措施与承诺 售后服务计划、项目售后服务承诺	13-14 160-176 179-183 177-178
本项目组织机构，人员管理机制，主要管理人员专业配置等人力配置情况，人员数量、任职资格、专业、学历、类似工作经验	本项目组成成员及相关材料 服务组织架构、人员岗位设置及工作职责	189-242 165-172

等等情况满足需求的程度		
合理化建议、特色服务	合理化建议 特色服务	184-187 13-14
技术部分和投标报价之间的相符性、各分项费用报价计取的准确性与合理性等	技术部分和投标报价之间的相符性	188

授权代表签名：_____ 日　期：2026 年 4 月 10 日

二、 投标项目明细清单

投标人全称（公章）：上海天泰网络技术有限公司 标项：1

序号	货物/服务名称	服务频次	服务周期	备注
1	网络安全等保服务	1次	项目服务周期为合同签订生效之日起一年，具体时间以招标人的通知为准	
2	网络安全加固服务	1次		
3	网络安全检测	6次		
4	网络安全应急保障	4次		
5	网络安全培训	5次		
6	网络安全应急演练	1次		
7	网络风险技术性探测	1次		
8	数据安全风险评估	1次		

授权代表签名：[illegible] 日 期：2026年4月10日

三、 技术响应表

技术响应表

投标人全称（公章）：上海天泰网络技术有限公司 标项：1

招标文件要求	投标文件响应	偏离情况
网络安全等保服务	网络安全等保服务	无偏离
网络安全加固服务	网络安全加固服务	无偏离
网络安全检测	网络安全检测	无偏离
网络安全应急保障	网络安全应急保障	无偏离
网络安全培训	网络安全培训	无偏离
网络安全应急演练	网络安全应急演练	无偏离
网络风险技术性探测	网络风险技术性探测	无偏离
数据安全风险评估	数据安全风险评估	无偏离

注：投标人应根据投标设备的性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

授权代表签名：_____ 日 期：2026 年 4 月 10 日

四、 项目概况

4.1 项目名称

项目名称：2026 年度浦东公交网络安全服务项目

项目编号：GQ3101150002603172002 52

采购单位：上海浦东新区公共交通有限公司

地址：成山路 990 号

4.2 项目概况及目标

上海浦东新区公共交通有限公司（下文简称“浦东公交”）是浦东新区国有独资特大型城市公共交通运输企业，现有杨高、金高、上南、南汇 4 家直属公交营运公司，运营浦东新区数百条城市公交线路，管理相关公交基础设施。

随着信息化工作的深入开展，浦东公交及其直属企业的网络安全工作面临着越来越多的挑战，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《网络数据安全管理条例》、《中华人民共和国计算机信息系统安全保护条例》等国家法律法规的要求，结合浦东公交及其直属企业的网络及信息系统实际情况，借助于第三方专业技术服务单位的专业技术支撑，增加浦东公交网络安全整体能力。

本项目目标旨在及时发现浦东公交及其直属企业各类信息系统的网络安全风险，防患于未然；同时，参照上级主管单位的网络安全考核要求，开展细粒度的安全服务，提升网络安全保障能力，切实加强业务系统网络安全管理与防护，避免或降低网络安全事件的发生，保障系统安全可靠运行。

4.3 网络与信息系统总体情况

浦东公交的网络信息系统从地域上分为联通云计算、公司机房、公司本部与各直属企业的办公终端，核心的应用系统部署在联通云计算中心，车载 DVR、机务管理系统等部署在公司机房，公司本部和直属企业的终端根据业务分布分别访问联通云和本地机房的应用，网络信息系统架构如图 4-3-1 所示。

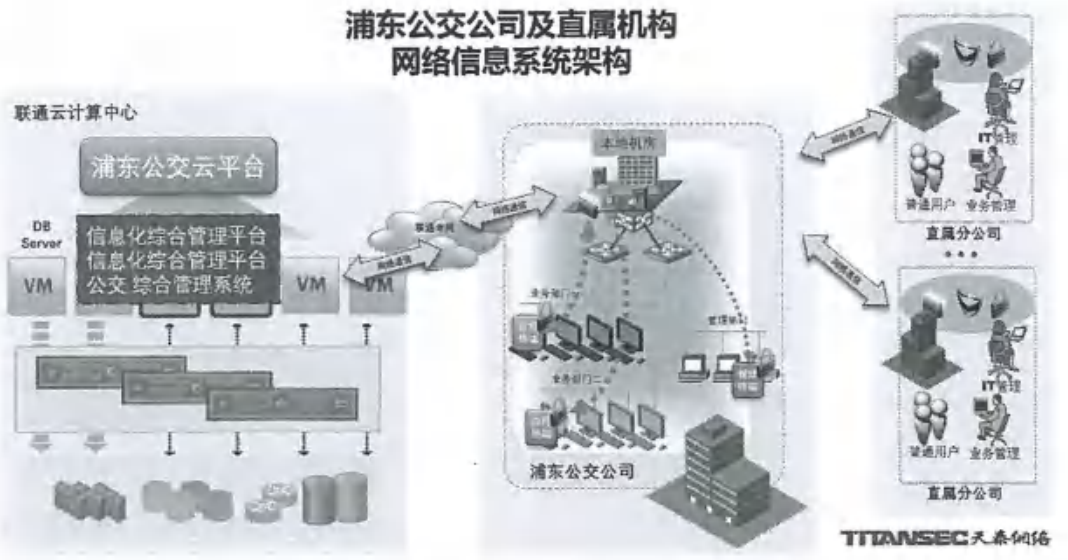


图 4-3-1 浦东公交公司及直属机构网络信息系统架构

4.4 项目方案依据

本项目相关主要依据为网络安全法律法规要求：

《中华人民共和国网络安全法》的颁布实施，强调保障网络安全及维护网络空间主权，要求各单位应采取监测、记录网络运行状态、网络安全事件的技术措施，不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施。第 21 条规定网络运营者（包括关键信息基础设施的运营者）的安全保护义务。

《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》中要求完善网络与信息安全基础设施，加强网络与信息安全专业骨干队伍和应急技术支撑队伍建设，提高风险隐患发现、监测预警和突发事件处置能力。加强信息共享和交流平台建设，健全网络与信息安全信息通报机制。进一步完善监管体制，充实监管力量，加强对基础信息网络安全工作的指导和监督管理。

《网络安全等级保护 2.0》为配合《网络安全法》实施，增加了风险评估、安全监测、通报预警、事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等内容要求。

《中华人民共和国个人信息保护法》规定，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动。该法确立了个

人信息处理应遵循的原则，强调处理个人信息应当采用合法、正当的方式，具有明确、合理的目的，限于实现处理目的的最小范围，公开处理规则，保证信息准确，采取安全保护措施等，并将上述原则贯穿于个人信息处理的全过程、各环节。

《民法典》于 2020 年 5 月 28 日颁布，首次规定了隐私权和个人信息的保护原则，其界定了个人信息的概念，列明了处理个人信息的合法基础，规范了个人信息处理者的义务、自然人对其个人信息的权利以及行政机关的职责。

方案编制的主要依据如下：

《中华人民共和国网络安全法》

《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》

《网络数据安全管理条例》

《中华人民共和国计算机信息系统安全保护条例》

《关键信息基础设施安全保护条例》

《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》

《国家信息化领导小组关于加强信息安全保障工作的意见》

《网络安全等级保护实施指南》（GB/T25058-2019）

《网络安全等级保护定级指南》（GB/T22240-2020）

《网络安全等级保护基本要求》（GB/T22239-2019）

《网络安全等级保护安全设计技术要求》（GB/T25070-2019）

《网络安全等级保护测评要求》（GB/T28448-2019）

《网络安全等级保护测评过程指南》（GB/T28449-2018）

《国家网络安全事件应急预案》

《上海市网络与信息安全事件专项应急预案》

《浦东新区网信工作“1+6”制度体系》

《ISO/IEC 27001 信息系统安全管理体系标准》

《ISO 13335 风险评估方法》

《浦东新区公共交通有限公司网络安全三年规划》

4.5 项目定位与主要内容

2026 年度是浦东公交网络安全三年规划中的第三年度，在上年度网络安全工作的基础上，将继续开展常规网络安全服务，按照浦东公交实际情况，优化网络安全服务内容，完善网络安全管理、防护体系。

2026 年度浦东公交网络安全服务项目的定位是借助第三方专业技术服务单位的专业技术支撑，针对浦东公交及其直属企业的网络及信息系统实际情况，开展各项网络安全服务工作，加强业务系统网络安全管理与防护，增强浦东公交网络安全整体能力，保障系统安全可靠运行。

本项目内容包括以下 8 项：

（1） 网络安全等保服务

（2） 网络安全加固服务

（3） 网络安全检测

（4） 网络安全应急保障

（5） 网络安全培训

（6） 网络安全应急演练

（7） 网络风险技术性探测

（8） 数据安全风险评估

4.6 项目重点、难点分析及特色服务

公交系统承载企业敏感信息，一旦遭受网络攻击或数据泄露，可能导致公共服务瘫痪、社会信任危机甚至国家安全风险。网络安全防护不仅是技术问题，更是维护公众权益的底线要求。随着云服务、大数据平台的普及，攻击面持续扩大，黑客组织、勒索软件等威胁不断升级，需构建覆盖数据全生命周期、系统全架构的安全防线，防范外部入侵与内部违规，确保服务“高效便捷”与“安全可信”的双重目标。

项目重点和难点主要体现在以下几个方面：

- ✧ 技术防护与动态防御：基于等保 2.0 要求，采用安全防护设备，通过持续身份验证、最小权限控制，应对应用系统云化带来的边界模糊问题。
- ✧ 信息资源不充沛：在安全管理过程中，可能存在信息收集不全面、数据

共享不及时不充分的问题，影响安全决策和应急处置的准确性和及时性。

- ✧ 网络隔离不清晰：业务系统之间缺乏有效的网络隔离，可能导致安全风险的扩散，增加了整体安全管理的难度。

针对这些难点和重点问题，需要通过常态化的网络安全工作，系统性地分解和归类安全管理的关键环节，明确浦东公交责任分工，责任到人，确保每个环节都有相应责任人履行好相应职责。通过精细化的管理方式，为浦东公交构建一个高效、可靠的安全管理体系，确保业务系统在复杂的环境中始终保持高水平的安全性，为民生服务提供坚实保障。通过专业的服务和精细化管理的实施，能够有效应对浦东公交在网络安全方面的挑战，为业务系统的稳定运行保驾护航。

我司将针对此项目建立专业的安全服务团队，针对项目整个服务过程中产生的问题进行记录、答疑、沟通、解决和闭环。例如：网络安全加固服务中，我司将不仅提供应用系统防篡改和防病毒服务，还将定期派遣服务人员针对防篡改日志、防病毒日志进行检查和分析，查看是否存在异常情况，并及时通知用户；网络安全检测中应用系统安全检测，不仅仅是安全检测，还将配合用户进行漏洞整改和复核，形成漏洞闭环等其他特色服务。

4.7 项目服务对象

项目服务对象包括浦东公交应用系统、本地机房、浦东公交公司本部和直属企业的网络环境，以及参与网络和信息系统管理使用、管理、运维、保障和服务的管理人员、业务人员、服务人员。

4.8 项目服务周期

项目服务周期为合同签订生效之日起一年，具体时间以招标人的通知为准。

五、 项目需求理解与分析

5.1 浦东公交网络与系统安全现状分析

5.1.1网络与系统安全管理情况

浦东公交采用联通云作为核心系统服务计算环境，云上的应用安全、数据安全、软件系统和虚拟机安全由浦东公交负责，运营商负责云基础设施安全，涉及机房、物理设施、通信网络等安全。浦东公交网络信息系统的网络安全、信息安全不依赖于其他信息系统的安全，并不会对其他信息系统的网络安全、信息安全产生影响，部署办公环境的信息终端，可以通过互联网访问互联网资源。

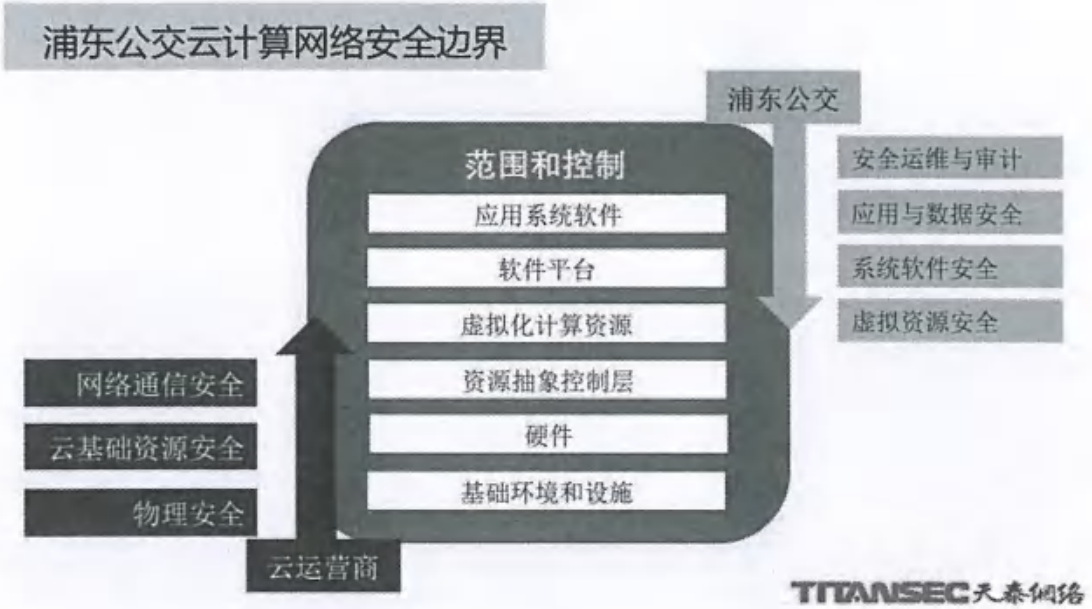


图 5-1-1 浦东公交云计算网络安全边界

浦东公交已落实网络安全管理责任制，企业主要负责人担任网络安全管理委员会的主任，下设网络安全管理小组，具体负责落实网络安全管理委员会制定的网络安全管理策略和工作任务，设立网络安全管理员、系统管理员和安全审计员，明确相关管理人员的岗位职责和工作要求，签订重点岗位人员安全保

密协议，制定人员离岗离职安全管理规定，并建立了外部人员访问机房等重要区域审批制度。

在信息资产管理方面，浦东公交已建立资产清单和信息资产管理制度，已建立设备维修维护和报废管理制度，并保留了一定的信息记录。在账号口令管理方面，浦东公交已建立账号、口令安全管理制度。

5.1.2 网络与系统安全技术设施情况

浦东公交本地存在办公网络等基础设置，已部署防火墙、WEB 应用防火墙、堡垒机、日志审计等网络安全防护设备，并根据需要配置了安全策略，留存了一定数量的网络访问日志。

浦东公交的应用系统部署在云上，已采购云服务商提供的网络和应用层安全服务，具备了一定的网络安全防护基础能力。

5.1.3 应用系统情况

浦东公交业务系统比较多，部分系统部署在联通云上，部分系统部署在本地机房。

5.2 安全风险分析

5.2.1 应用安全风险

应用安全风险是指信息系统在应用层面存在脆弱性，以及受到内外部威胁影响的可能性。

应用安全风险主要包括：病毒蠕虫、木马、口令猜测及暴力破解、拒绝服务攻击、SQL 注入、跨站脚本（XSS）、命令代码注入、图片嵌入恶意代码、本地/远程文件包含、任意代码执行、远程命令执行、请求伪造、任意文件上传下载、任意目录遍历、源代码泄露、调测信息泄露、JSON 挟持、第三方组件漏洞攻击、溢出攻击、变量覆盖、网络监听、会话标志攻击、越权和非授权访问、反序列化、APT 攻击等。研究表明，大多数的安全漏洞来自于软件自身，应用层的漏洞数量已经超过网络、操作系统的漏洞数量。

5.2.2数据安全风险

数据安全风险是指信息系统在数据层面存在脆弱性，以及受到内外部威胁影响的可能性。

最主要的数据安全风险是数据或信息被非授权访问、泄露、修改或删除，具体又可以分为管理风险和技术风险。其中，管理风险主要涉及人员的因素包括：操作失误、故意泄露、人为破坏等；技术层面主要面临：病毒蠕虫、木马、任意文件上传下载、目录遍历、源代码泄露、调测信息泄露、数据库条目暴露、JSON 挟持、网络监听、未授权访问以及 APT 攻击等可能导致数据泄露、篡改或破坏的风险。

近年来，针对基础设施及公共服务信息系统的攻击事件日益增多，归纳起来，系统受到的常见威胁大致包括：第三方人员账号泄露、云服务横向的安全攻击、误操作、错误的安全配置、内部人员泄密、未及时修复的漏洞、高级持续威胁（APT）等。

5.2.3第三方安全风险

第三方是指与浦东公交合作的任何实体。包括集成商、供应商、软件开发商、服务提供商、业务合作伙伴和数据共享单位。

第三方风险管理十分关键，因为使用第三方的产品或服务会直接或间接影响浦东公交的网络信息安全。第三方增加了网络信息安全的复杂性，原因如下：

- ✧ 第三方通常不受浦东公交的完全控制，无法完全了解他们的安全控制情况。一些供应商拥有强大的安全标准和良好的风险管理实践，但还有一些供应商的安全策略并不周密和完善，安全策略和具体要求往往不能落到实处。
- ✧ 每个第三方都是数据泄露或网络攻击的潜在攻击媒介。如果供应商具有易受攻击的攻击面，采购人使用的此类供应商越多，攻击面就越大，面临的潜在风险就越大。
- ✧ 数据安全和个人信息保护等相关法律的实施极大地提高了第三方风险的影响。如果由于第三方导致数据泄露，采购人同样也要面临合规和业务损失的风险。

5.3 网络与信息安全需求分析

5.3.1项目实施需求分析

当前，浦东公交的信息系统部署在云上，已经采取了相应的安全技术措施，保障系统的基础安全，部分在本地的信息系统也已采用安全设备进行保护，需注意要定期更新安全设备的授权，确保各项安全更能处于生效状态；浦东公交的计算设备运维和应用系统开发采用第三方服务，因此须在计算设施运维、软件设计开发阶段加强安全管控，实现覆盖全生命周期的应用安全；浦东公交往年已开展了信息系统网络安全等保工作，还需按照安全主管单位的要求，定期对现有系统开展整改、复测评工作。具体实施过程中应该满足以下几点：

（1） 注重安全规划；

（2） 确保计算环境安全；

（3） 加强软件开发安全管理；

（4） 关注安全设备授权；

（5） 认真对待两高一弱风险；

（6） 提高系统安全检查和整改水平。

5.3.2日常安全管理和保障需求分析

当前，浦东公交需要在服务器可控性、可管理性以及用户自由度的平衡上进行进一步优化，同时应降低服务器管理的复杂性。同时需要从操作系统、应用程序、威胁检测、移动终端四方面加强安全防护。具体实施过程中应该满足以下几点：

（1） 建立操作系统正面清单，选用具有安全组件的操作系统；

（2） 实施服务器的最小安全配置管理，关闭业务作业不用的端口和协议，删除多余的组件；

（3） 采用主流的防病毒系统，有效防范服务器的恶意软件和计算机病毒；

（4） 统一的服务器安全防护策略，对系统补丁、软件升级、系统变更进行统一管理。

5.3.3网络与系统安全服务需求分析

浦东公交网络与系统安全服务包括：

（1） 网络安全等保服务：信息化综合管理平台（等保三级）、集群调度系统（等保三级）、公交综合管理系统（等保二级）3 个信息系统辅助开展网络安全三级、二级等保相关服务，测评过程中，衔接业务系统开发运维单位和测评机构，为测评工作提供协助、整改、反馈、复核等工作，保障系统的等保测评能够顺利通过。

（2） 网络安全加固服务：为应用系统提供 2 个页面防篡改能力，防范应用系统页面被植入非法信息。为 410 台终端设备提供专业级防病毒服务，保护电脑免受恶意病毒威胁。

（3） 网络安全检测：对浦东公交本部的应用系统每 2 月开展一次（服务期内共计开展 6 次）应用系统安全检测，发现应用系统网络安全漏洞隐患，给出漏洞整改建议，并配合采购人指定的开发单位及时落实整改。对下属的四家直属企业各开展一次网络安全检查，发现网络中存在的安全隐患，给出安全建议。

（4） 网络安全应急保障：在重要时期关键节点（如两会、五一、国庆、进博会）或主管单位例行检查时，提供专项保障服务。提供全年的网络安全应急响应保障，发生网络信息安全突发事件，及时响应、介入事件处置，预防和减少网络安全事件造成的损失和危害（一般事件 1 小时内响应，重要事件 30 分钟内响应）。

（5） 网络安全培训：根据需求对浦东公交及其直属企业各开展 1 次网络安全意识培训，宣传最新的网络安全法律法规和政策要求，增强关键岗位应对处置信息安全风险的能力。

（6） 网络安全应急演练：为浦东公交及其直属企业联合开展 1 次网络安全应急演练，模拟突发事件处理过程，验证网络安全应急预案的有效性和可操作性，提升应对网络突发事件的应急处置能力。

（7） 网络风险技术性探测：应对国内外势力发起的网络攻击，开展 1 次技术性探测；利用模拟黑客入侵方式对指定的业务系统开展 1 次渗透测试，测试安全漏洞的存在，验证防护手段的有效性。

（8） 数据安全风险评估：对 1 个指定信息系统开展网络数据安全风险评估，以发现系统数据隐患、防范数据安全风险为目标，围绕数据处理者、数据处理活动开展综合性、全面性的数据安全分析，发现数据资产的威胁性和脆弱性，分析可能存在的安全威胁，促进数据安全管理能力的提升。

5.4 项目建设预期

浦东公交网络安全服务工作围绕公司本部和直属企业的网络和信息系统，开展较为全面的网络安全技术服务工作，按照检查、防护、预警、优化这一链条，从网络安全服务开始，改善和优化网络通信、网络安全条件，保障浦东公交信息化工作的健康高效发展。

本项目需求内容的有效实施，可以显著的降低浦东公交云应用、本地应用的网络安全风险的级别，全面检查网络安全存在的问题、薄弱环节和潜在风险，及时调整网络资源的策略、修补漏洞，强化网络安全薄弱环节的防护，有效提升用户单位的网络安全管理能力和网络安全技术能力。

本项目实现主机和网络应用系统的防护、检查、分析、整改、响应、处理等一系列服务功能，通过技术手段和服务措施可享受到专业、高效的安全保障服务，能够显著提升用户单位业务系统的安全保障效果。

通过安全检测和等保服务能够为应用系统和计算平台提供有效的安全检测手段，及时发现安全警告、黑客入侵、网页篡改、敏感信息泄露等安全事件，并定位入侵路径、篡改页面和敏感信息的位置，使主机和应用系统能够及时发现风险、消除和降低风险，有效降低安全隐患和安全事件的影响。

本项目的应急保障服务是完善安全事件发现与处置的一种主动工作机制。通过应急响应可以让安全团队第一时间控制事件的影响和降低系统损失，同时也可有效识别出当前安全防护系统和处理机制的不足或缺陷。

通过开展安全服务，可大大降低公交公司整体网络安全的事故发生概率，降低系统、设备、数据的损失（包括隐形的损失）。

面对加快推进浦东新区公交系统的数字化转型，全面深化交通行业资源共

享能力，为新区智慧交通事业的发展，本项目将全力保障公交信息系统的网络信息安全，为浦东新区交通行业的深入发展提供信息安全保障，为浦东市民提供安全、快捷、舒适、温馨出行服务提供安全的信息技术支撑。

六、 项目总体方案

6.1 网络安全等保服务

6.1.1服务需求理解

信息化综合管理平台（等保三级）、集群调度系统（等保三级）、公交综合管理系统（等保二级）3个信息系统辅助开展网络安全三级、二级等保相关服务，测评过程中，衔接业务系统开发运维单位和测评机构，为测评工作提供协助、整改、反馈、复核等工作，保障系统的等保测评能够顺利通过。

在网络安全领域，等级保护2.0相关的《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护安全设计技术要求》等国家标准正式发布，根据等保 2.0 的要求，对安全物理环境、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、人员安全管理、系统建设管理、系统运维管理等内容进行安全等级测评，主要要求如下：

1) 安全物理环境：针对目标系统所处的物理环境、物理访问控制、防盗窃和防破坏等对象和内容进行访谈、文档审查；
2) 安全通信网络：针对目标系统的信息资产与安全资源的网络架构、通信传输等内容进行访谈、检查和测试；
3) 安全区域边界：针对目标系统的网络通信设施与安全设备的边界防护、访问控制、安全审计、入侵防范、恶意代码防范、可信验证等内容进行访谈、检查和测试；
4) 安全计算环境：针对目标系统的主机操作系统、数据库管理系统、管理系统的身份鉴别、访问控制、安全审计、入侵防范、防恶意代码、可信验证、数据完整性、个人信息保护等内容进行访谈、检查和测试；
5) 安全管理中心：针对目标系统资源集中的系统管理、审计管理、安全管理、集中管控等内容进行访谈、检查和测试；
6) 安全管理制度：针对网络信息安全管理体系、日常安全管理制度、重要操作规程及相关执行记录等内容进行访谈和检查；

7) 安全管理机构：针对安全管理机构设立文档、网络安全小组名单、岗位说明书等文档及执行记录进行访谈和检查；

8) 人员安全管理：针对人事管理制度、外部人员访问要求等安全管理制度及执行记录进行访谈和检查；

9) 系统建设管理：针对目标系统安全设计方案、网络安全设施报告等文档及软件开发、工程实施等方面的安全管理制度及执行记录等进行访谈和检查；

10) 系统运维管理：针对目标系统运维过程中涉及的安全管理制度及执行记录等进行访谈和检查。

6.1.2服务范围

对浦东公交的三个系统进行测评协助：

- 信息化综合管理平台（等保三级）；
- 集群调度系统（等保三级）；
- 公交综合管理系统（等保二级）。

6.1.3服务流程

（一） 确定测评团队

与专业测评机构确认此次等保测评的测评团队人员（至少三人组成），对测评师的背景和技能提出要求。

（二）确定测评时间和地点

与测评机构确认本次 1 个二级等保测评系统和 2 个三级等保测评系统的测评时间安排，生成相应的系统测评时间表；结合系统测评时间表与浦东公交项目管理人员确认各系统测评的时间和持续天数。在此时间表的基础上分配各个信息系统的测评协助人员进场配合的时间，对应生成一个服务人员配合等保测评的时间表和工作计划表。

（三）确定测评标准和依据

对信息系统安全等级保护进行测评评估，包含两个方面的内容：一是安全控制测评，主要是测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性；其中，

安全控制测评是信息系统整体安全测评的基础。

安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据安全等五个层面上的安全控制测评。

安全管理测评：包括安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全控制测评。

针对测评机构而言，测评机构理应根据《管理办法》、《测评机构管理办法》、《测评要求》、《测评过程指南》等国家标准开展等级测评，并在测评完毕后依照公安部门得出的测评报告模板出示测评报告。天泰网络将根据浦东公交要求挑选符合要求标准的测评机构，根据《测评规定》等技术性标准，按时对目标信息系统安全级别情况进行等级测评。

（四）测评准备阶段

了解项目实施方案或系统运维方案：针对被测评的系统，收集和了解该系统的实施方案和运维方案，对目标系统了解的深度和广度决定了针对该项目的测评计划和测评方案的适配程度。

研讨测评方案：在充分了解系统情况的基础上，可与测评师沟通有关该系统测评方案的相关问题。比如：系统安全设计架构、安全技术标准、安全技术措施和安全运维管理措施等一系列问题。

准备测评环境和资料：根据测评计划和方案的要求，协助测评师准备测试环境，收集整理相关的计划、执行、总结报告或资料，相关的过程文档或配置库等。

（五）收集相关资料和文档

在测评前期，准备测评所需的网络安全管理制度、应用系统的建设方案、运维报告（包含补丁更新、系统升级等）、日常管理留痕记录（检查、整改、小结）、浦东公交应急演练留痕、网络安全培训留痕、领导小组发文文档等其他管理文档。

（六）安排必要的资源和设备

开展测评启动会，主要是由浦东公交网络安全监管部门管理人员、测评师、服务工程师、系统运维与安全服务团队的代表参会。目的是为了协调内部资源，介绍测评方人员及各自职责、后续测评工作计划，为等级测评项目实施做好基

本准备。

在项目启动会后，可安排相关系统运维人员、开发人员配合，提供测评环境进行测评。

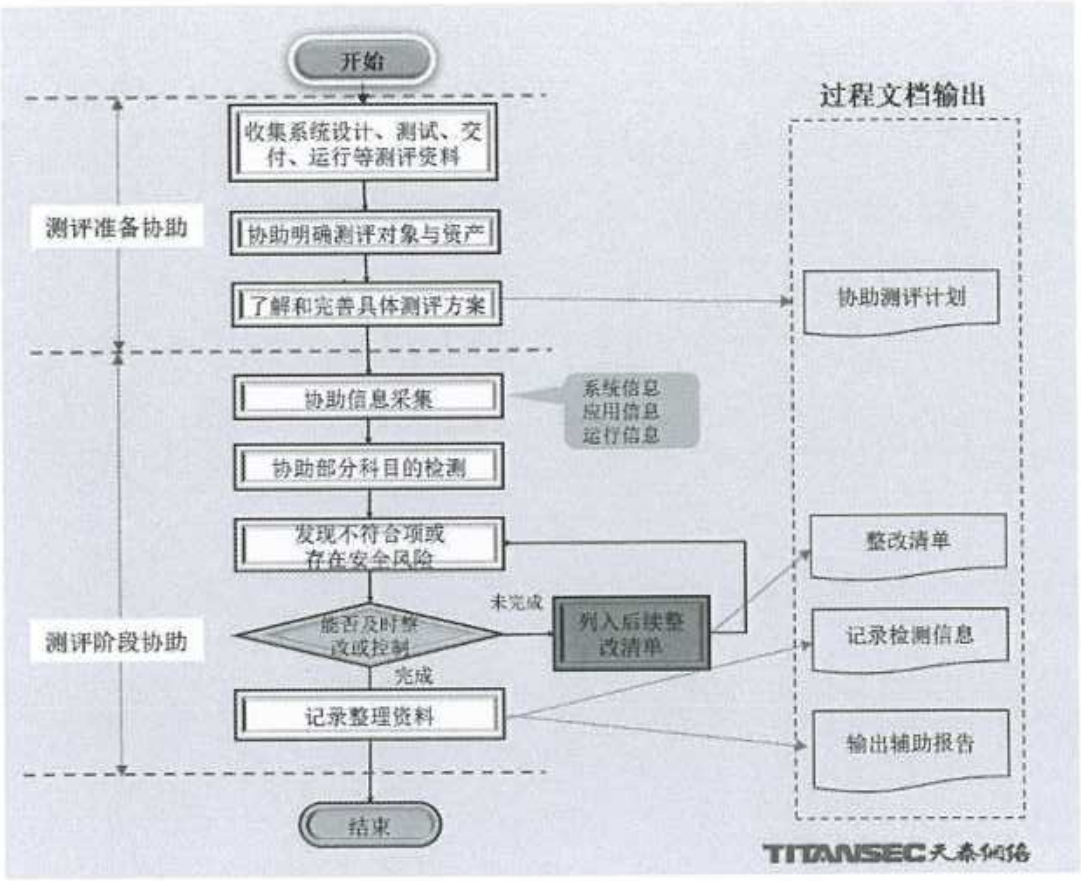


图 6-1-3-1 测评协助流程和过程文档

（七）测评期间协助测评单位

测评期间，配合测评单位的人员提供测评所需的制度材料、技术文档、安全产品信息等。

人员与时间节点安排

等保安全服务根据不同的阶段安排不同的安全服务人员参与项目服务，具体的人员安排与时间节点安排如图所示。

图 6-1-3-2 等保安全服务人员安排和时间节点安排

6.1.4 服务内容

6.1.4.1 等保测评差距项整改

在等级保护测评过程中，由于目标系统运行在联通云租户区和浦东公交公司本地机房，将涉及安全物理环境、安全通讯网络、安全区域边界、安全计算环境和安全管理中心等几个方面。在测评前期对以上涉及的几个方面进行检查，找到差距并进行整改。在测评完成后根据等保机构测评结果的差距分析进行进一步整改，使系统能够满足等保要求。目标系统的等保测评整改要求示例列表如下。

表 6-1-4-1 网络安全等保测评整改要求项列表

等保测评整改要求			整改计划	责任方	配合方	计划完成时间点	整改结果
安全层面	控制点	不符合项					
……	……	……	……	……	……	……	……

6.1.4.2 安全管理方面整改

网络安全管理整改服务主要依据网络安全法和等保要求，主要从包括网络安全管理制度管理、网络安全管理机构、人员安全管理、安全建设管理、安全运维管理等五个方面进行制度建设、开展管理活动和相关活动的记录留档。

对网络安全等级保护二级和三级的要求进行对比分析，相关要求如下：

表 6-1-4-2-1 安全管理制度

序号	名称	具体要求	二级	三级
1	安全策略	a)应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	☑	☑
2	管理制度	a)应对安全管理活动中的主要管理内容建立安全管理制度；	☑	☑
		b)应对管理人员或操作人员执行的日常管理操作建立操作规程。	☑	☑
		c)应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。	☑	☑
3	制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定；	☑	☑
		b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。	☑	☑
4	评审和修订	a)应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	☑	☑

表 6-1-4-2-2 安全管理机构

序号	名称	具体要求	二级	三级
1	岗位设置	a)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	☑	☑
		b)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	☑	☑
		a)应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；		☑
2	人员配备	a)应配备一定数量的系统管理员、审计管理员和安全管理员等。	☑	☑
		b)应配备专职安全管理员，不可兼任。		☑
3	授权和审批	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	☑	☑
		b)应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。	☑	
		b)应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； c)应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。		☑
4	沟通和合作	a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	☑	☑
		b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	☑	☑
		c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	☑	☑

5	审核和检查	a)应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	☑	☑
		b)应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； c)应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。		☑

表 6-1-4-2-3 安全管理人员

序号	名称	具体要求	二级	三级
1	人员录用	a)应指定或授权专门的部门或人员负责人员录用；	☑	☑
		b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查。	☑	☑
		c)应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。		☑
2	人员离岗	a)应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。	☑	☑
		b)应办理严格的调离手续，并承诺调离后的保密义务后方可离开。		☑
3	安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	☑	☑
		b)应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； c)应定期对不同岗位的人员进行技能考核。		☑
4	外部人员访问管理	a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	☑	☑
		b)应在外部人员接入受控网络访问系统前先提	☑	☑

		出书面申请，批准后由专人开设账户、分配权限，并登记备案；		
		c)外部人员离场后应及时清除其所有的访问权限。	☑	☑
		d)获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。		☑

表 6-1-4-2-4 安全建设管理

序号	名称	具体要求	二级	三级
1	定级和备案	a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	☑	☑
		b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	☑	☑
		c)应保证定级结果经过相关部门的批准；	☑	☑
		d)应将备案材料报主管部门和相应公安机关备案。	☑	☑
2	安全方案设计	a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	☑	☑
		b)应根据保护对象的安全保护等级进行安全方案设计；	☑	
		c)应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。	☑	
		d)应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； e)应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证		☑

		和审定，经过批准后才能正式实施。		
3	产品采购和使用	a)应确保网络安全产品采购和使用符合国家的有关规定；	☑	☑
		b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	☑	☑
		c)应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。		☑
4	自行软件开发	a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	☑	☑
		b)应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。	☑	☑
		c)应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； d)应制定代码编写安全规范，要求开发人员参照规范编写代码； e)应具备软件设计的相关文档和使用指南，并对文档使用进行控制； f)应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； g)应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。		☑
5	外包软件开发	a)应在软件交付前检测其中可能存在的恶意代码；	☑	☑
		b)应保证开发单位提供软件设计文档和使用指南。	☑	☑
		c)应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。		☑
6	工程实施	a)应指定或授权专门的部门或人员负责工程实施过程的管理；	☑	☑

		b)应制定安全工程实施方案控制工程实施过程。	☑	☑
		c)应通过第三方工程监理控制项目的实施过程。		☑
7	测试验收	a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	☑	☑
		b)应进行上线前的安全性测试，并出具安全测试报告。*安全测试报告应包含密码应用安全性测试相关内容。*	☑	☑
8	系统交付	a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	☑	☑
		b)应对负责运行维护的技术人员进行相应的技能培训；	☑	☑
		c) 应提供建设过程文档和运行维护文档。	☑	☑
9	等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	☑	☑
		b) 应在发生重大变更或级别发生变化时进行等级测评；	☑	☑
		c)应确保测评机构的选择符合国家有关规定。	☑	☑
10	服务供应商选择	a)应确保服务供应商的选择符合国家的有关规定；	☑	☑
		b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	☑	☑
		c)应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。		☑

表 6-1-4-2-5 安全运维管理

序号	名称	具体要求	二级	三级
1	环境管	a)应指定专门的部门或人员负责机房安全，对	☑	☑

	理	机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；		
		b)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；	☑	
		c)应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；		☑
		d)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	☑	☑
2	资产管理	a)应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	☑	☑
		b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； c)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。		☑
3	介质管理	a)应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，并根据存档介质的目录清单定期盘点；	☑	☑
		b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	☑	☑
4	设备维护管理	a)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	☑	☑
		b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	☑	☑
		c)信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境		☑

		时其中重要数据必须加密； d)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。		
5	漏洞和风险管理	a)应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	☑	☑
		b)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。		☑
6	网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	☑	☑
		b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	☑	☑
		c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	☑	☑
		d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	☑	☑
		e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。	☑	☑
		f)应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； g)应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，操作过程中应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； h)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改		☑

		的审计日志，操作结束后应删除工具中的敏感数据； i)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； j)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。		
7	恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	☑	☑
		b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；	☑	
		c)应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。	☑	
		d)应定期验证防范恶意代码攻击的技术措施的有效性。		☑
8	配置管理	a)应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	☑	☑
		b)应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。		☑
9	密码管理	a)应遵循密码相关国家标准和行业标准；	☑	☑
		b)应使用国家密码管理主管部门认证核准的密码技术和产品。		☑

10	变更管理	a)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	☑	☑
		b)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； c)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	☑	☑
11	备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；	☑	☑
		b)应规定备份信息的备份方式、备份频度、存储介质、保存期等；		☑
		c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	☑	☑
12	安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件；	☑	☑
		b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	☑	☑
		c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	☑	☑
		d)对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。	☑	☑
13	应急预案管理	a)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	☑	☑
		b)应定期对系统相关的人员进行应急预案培		☑

		训，并进行应急预案的演练。		
		c) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；	☑	☑
		d) 应定期对原有的应急预案重新评估，修订完善。	☑	☑
14	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；		☑
		b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。		☑
		c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。	☑	☑

6.1.4.3 安全技术方面差距分析与整改示例

安全技术方面等级保护测评的差距分析与整改建议举例如下：

（1）网络资源、安全模块、虚拟主机、数据库等

1) 身份鉴别

a) 存在弱口令或相同口令

对应要求：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

判例内容：网络资源、安全模块、操作系统、数据库等存在弱口令账户（包括空口令、无身份鉴别机制），并可通过该账户登录；或大量设备管理员账户口令相同，一台设备口令被破解将导致大量设备被控制，可判定为高风险。

补偿措施：由于业务场景需要，使用无法设置口令或口令强度达不到要求

的专用设备，可从设备登录方式、物理访问控制、受限使用情况、其他防护措施、管理制度等角度对其进行综合风险分析，酌情判断风险等级。

整改建议：建议删除或修改账户口令重命名默认账户，制定相关管理制度，规范口令的最小长度、复杂度与生命周期，并根据管理制度要求，合理配置账户口令复杂度和定期更换策略；此外，建议为不同设备配备不同的口令，避免一台设备口令被破解影响所有设备安全。

b) 设备未实现双因素认证

对应要求：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

判例内容：核心设施、操作系统等未采用两种或两种以上鉴别技术对用户身份进行鉴别。例如仅使用用户名/口令方式进行身份验证，削弱了管理员账户的安全性，无法避免账号的未授权窃取或违规使用，可判定为高风险。

补偿措施：

设备通过本地登录方式（非堡垒机方式）维护，本地物理环境可控，可酌情降低风险等级；

采用两重用户名/口令认证措施（两重口令不同），例如身份认证服务器、堡垒机等手段，可酌情降低风险等级；

设备所在物理环境、网络环境安全可控，网络窃听、违规接入等隐患较小，口令策略和复杂度、长度符合要求的情况下，可酌情降低风险等级；

根据被测对象的作用以及重要程度，结合实际情况，酌情判断风险等级。

整改建议：建议核心设备、操作系统等增加除用户名/口令以外的身份鉴别技术，如密码/令牌、生物鉴别方式等，实现双因子身份鉴别，增强身份鉴别的安全力度；对于使用堡垒机或统一身份认证机制实现双因素认证的场景，建议通过绑定等技术措施，确保设备只能通过该机制进行身份认证，无旁路现象存在。

2) 访问控制

a) 设备默认口令未修改

对应要求：应重命名或删除默认账户，修改默认账户的默认口令。

判例内容：网络资源、安全模块、操作系统、数据库等默认账号的默认口

令未修改，使用默认口令进行登录设备，可判定为高风险。

补偿措施：由于业务场景需要，无法修改专用设备的默认口令，可从设备登录方式、物理访问控制、受限使用情况、其他防护措施、管理制度等角度对其进行综合风险分析，酌情判断风险等级。

整改建议：建议网络资源、安全模块、操作系统、数据库等重命名或删除默认管理员账户，修改默认密码，使其具备一定的强度，增强账户安全性。

3) 安全审计

a) 设备无安全审计措施

对应要求：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

判例内容：关键网络资源、安全模块、操作系统、数据库、管理终端等未开启任何审计功能，且未采取其他辅助审计措施，无法对重要的用户行为和重要安全事件进行审计，并对事件进行溯源，可判定为高风险。

补偿措施：

使用堡垒机或其他第三方审计工具进行日志审计（不少于六个月），能有效记录用户行为和重要安全事件，可根据所记录的日志情况、是否存在漏记/旁路等缺陷，综合分析判断风险等级；

核查对象为非核心设备，对整个管理平台影响有限的情况下，可酌情降低风险等级。

整改建议：建议在核心系统、安全模块、操作系统、数据库、运维终端性能允许的前提下，开启用户操作类和安全事件类审计策略或使用第三方日志审计工具，实现对相关设备操作与安全行为的全面审计记录，保证发生安全问题时能够及时溯源。

4) 入侵防范

a)设备开启高危服务端口

对应要求：应关闭不需要的系统服务、默认共享和高危端口。

判例内容：网络资源、安全模块、操作系统等存在多余系统服务/默认共享/高危端口，且存在可被利用的高危漏洞或重大安全隐患，可判定为高风险。

补偿措施：

通过其他技术手段能降低漏洞影响，可酌情降低风险等级；

相关漏洞暴露在可控的网络环境，可根据网络防护程度、漏洞危害情况等，酌情判断风险等级。

整改建议：建议网络资源、安全模块、操作系统等关闭不必要的服务和端口，降低安全隐患；根据自身应用需求，需要开启共享服务的，应合理设置相关配置，如设置账户权限等。

b) 未限制设备管理终端

对应要求：应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

判例内容：通过不可控网络环境远程管理的网络资源、安全设备、操作系统、数据库等，未采取技术手段对管理终端进行限制，可判定为高风险。

补偿措施：管理终端部署在运维区、可控网络或采用多种身份鉴别方式等技术措施，降低终端管控不善所带来的安全风险，可酌情降低风险等级。

整改建议：建议通过技术手段，对管理终端进行限制。

c)系统设施未修补已知重大漏洞

对应要求：应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

判例内容：管理平台可直接访问到的网络资源、安全模块、操作系统、数据库等，如存在外界披露的重大漏洞，未及时修补更新，无需考虑是否有 POC 攻击代码，可判定为高风险。

补偿措施：

相关漏洞暴露在可控的网络环境，可酌情降低风险等级；

网络设备的 WEB 管理界面存在高危漏洞，而该 WEB 管理界面只能通过特定 IP 或特定可控环境下才可访问，可酌情降低风险等级。

整改建议：建议订阅安全厂商漏洞推送或本地安装安全软件，及时了解漏洞动态，在充分测试评估的基础上，修补严重安全漏洞。

5) 恶意代码防范

a) 无恶意代码防范措施

对应要求：（等保二级）应安装防恶意代码软件或配置具有相应功能的软件，

并定期进行升级和更新防恶意代码库。

（等保三级、四级）应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

（2）应用系统及数据

1) 身份鉴别

a) 应用系统口令策略缺失

对应要求：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

判例内容：应用系统无任何用户口令复杂度校验机制，校验机制包括口令的长度、复杂度等，可判定为高风险。

补偿措施：

应用系统采用多种身份鉴别认证技术的，即使有口令也无法直接登录应用系统的，可酌情降低风险等级；

应用系统为内部管理系统，仅内网访问，访问人员相对可控，且实际用户口令有一定的质量，不易被猜测，可酌情降低风险等级；

应用系统口令校验机制不完善，如只有部分校验机制，可根据实际情况，酌情降低风险等级；

特定应用场景中的口令（如 PIN 码等）可根据相关要求和行业特点，酌情判断风险等级；

针对部分专用软件、老旧系统等无法添加口令复杂度校验功能，在管理制度中明确口令复杂度及更换周期要求，并定期检查制度执行情况或采取登录地址限制等控制措施，可酌情降低风险等级

整改建议：建议应用系统对用户的账户口令长度、复杂度进行校验，如要求系统账户口令至少 8 位，由数字、字母或特殊字符中 2 种方式组成；对于如 PIN 码等特殊用途的口令，应设置弱口令库，通过对比方式，提高用户口令质量。

b) 应用系统存在弱口令

对应要求：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

判例内容：应用系统存在易被猜测的常用/弱口令账户（包括空口令或无身

份鉴别机制），可判定为高风险。

补偿措施：

该空口令、弱口令账号为前台注册用户自行修改，被猜测登录后仅影响单个用户，而不会对整个应用系统造成安全影响的，可酌情降低风险等级；

由于业务场景需要，使用无身份鉴别功能或口令强度达不到要求的专用软件，可从软件登录方式、物理访问控制、受限使用情况、其他防护措施、管理制度等角度对其进行综合风险分析，酌情判断风险等级。

整改建议：建议应用系统通过口令长度、复杂度校验、常用/弱口令库比对等方式，提高应用系统口令质量。

c) 应用系统无登录失败处理机制

对应要求：应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

判例内容：可通过互联网登录的应用系统未提供任何登录失败处理措施，攻击者可进行口令猜测，可判定为高风险。

补偿措施：

应用系统采用多种身份鉴别认证技术，可酌情降低风险等级；

登录页面采用图像验证码等技术可在一定程度上提高自动化手段进行口令暴力破解难度，且该技术手段无法被绕过，可视图像验证码的强度，酌情降低风险等级；

根据登录账户的重要程度、影响程度，可酌情判断风险等级。若登录账户涉及到金融行业、个人隐私信息、信息发布、后台管理等，不宜降低风险等级；

针对部分专用软件、老旧系统等无法添加登录失败处理功能，若采取登录地址限制等技术措施，能够限制或降低暴力破解行为，可酌情降低风险等级。

整改建议：建议应用系统提供登录失败处理功能（如账户锁定、多重认证等），防止攻击者进行口令暴力破解。

2) 访问控制

a) 应用系统身份鉴别机制可被旁路

对应要求：应对登录的用户分配账户和权限。

判例内容：应用系统访问控制功能存在缺失，无法按照设计策略控制用户

对系统功能、数据的访问；可通过直接访问 URL 等方式，在不登录系统的情况下，非授权访问系统功能模块，可判定为高风险。

补偿措施：

应用系统部署在可控网络，有其他防护措施能限制、监控用户行为，可酌情降低风险等级；

根据非授权访问模块的重要程度、越权访问的难度，酌情判断风险等级。

整改建议：建议完善访问控制措施，对系统重要页面、功能模块进行访问控制，确保应用系统不存在访问控制失效情况。

b) 应用系统默认口令未修改

对应要求：应重命名或删除默认账户，修改默认账户的默认口令。

判例内容：应用系统默认账号的默认口令未修改，可利用该默认口令登录系统，可判定为高风险。

补偿措施：由于业务场景需要，无法修改专用软件的默认口令，可从设备登录方式、物理访问控制、受限使用情况、其他防护措施、管理制度等角度对其进行综合风险分析，酌情判断风险等级。

整改建议：建议应用系统重命名或删除默认管理员账户，修改默认密码，使其具备一定的强度，增强账户安全性。

c) 应用系统访问控制策略可被旁路

对应要求：

（二级）应对登录的用户分配账户和权限。

（三级、四级）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

判例内容：应用系统访问控制策略存在缺陷，可越权访问系统功能模块或查看、操作其他用户的数据。如存在平行权限漏洞，低权限用户越权访问高权限功能模块等，可判定为高风险。

补偿措施：

应用系统部署在可控网络，有其他防护措施能限制、监控用户行为的，可酌情降低风险等级；

根据非授权访问模块的重要程度、越权访问的难度，酌情判断风险等级。

整改建议：建议完善访问控制措施，对系统重要页面、功能模块进行重新进行身份、权限鉴别，确保应用系统不存在访问控制失效情况。

3) 安全审计

a) 应用系统完全审计措施

对应要求：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

判例内容：应用系统（包括前端系统和后台管理系统）无任何日志审计功能，无法对用户的重要行为进行审计，也无法对事件进行溯源，可判定为高风险。

补偿措施：

采取其他技术手段对重要的用户行为进行审计、溯源，可根据所记录的日志情况、是否存在漏记/旁路等缺陷，综合分析判断风险等级；

审计记录不全或审计记录有记录，但无直观展示，可根据实际情况，酌情降低风险等级。

整改建议：建议应用系统完善审计模块，对重要用户操作、行为进行日志审计，审计范围不仅针对前端用户的操作、行为，也包括后台管理员的重要操作。

b) 应用系统审计记录不满足保护要求

对应要求：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

判例内容：对应用系统的重要业务操作日志、重要安全类日志等保护措施不满足要求，相关日志可被恶意删除、修改或覆盖等情况，日志保存时间不满足法律法规相关要求的，可判定为高风险。

补偿措施：

删除功能只能删除历史日志（超过追溯时效和意义），可根据业务场景及日志信息内容进行综合分析，酌情判断风险等级；

被测系统未上线使用或上线时间不足六个月，应从日志备份策略、日志存储容量等角度进行综合分析当前措施是否能满足日志保存至少六个月的要求，酌情判断风险等级。

整改建议：建议对应用系统重要操作类、安全类等日志进行妥善保存，避免受到未预期的删除、修改或覆盖等，留存时间不少于六个月，符合法律法规的相关要求。

4) 入侵防范

a) 应用系统有效校验功能存在缺陷

对应要求：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

判例内容：由于校验机制缺失导致的应用系统存在如 SQL 注入、跨站脚本、上传漏洞等高危漏洞，可判定为高风险。

补偿措施：

应用系统存在 SQL 注入、跨站脚本等高危漏洞，但系统部署了 WAF、防篡改软件等应用防护产品，在防护体系下无法成功利用，可酌情降低风险等级；

整改建议：建议通过修改代码的方式，对数据有效性进行校验，提交应用系统的安全性，防止相关漏洞的出现。

b) 应用系统存在可被利用的高危漏洞

对应要求：应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

判例内容：应用系统所使用的环境、框架、组件或业务功能等存在可被利用的高危漏洞或严重逻辑缺陷，导致敏感数据泄露、网页篡改、服务器被入侵、绕过安全验证机制非授权访问等安全事件的发生，可能造成严重后果的，可判定为高风险。

补偿措施：可从内网环境管控、访问控制措施、漏洞影响程度、漏洞利用难度、利用可能性等角度进行综合风险分析，酌情判断风险等级。

整改建议：建议定期对应用系统进行漏洞扫描、渗透测试等技术检测，对可能存在的已知漏洞、逻辑漏洞，在重复测试评估后及时进行修补，降低安全隐患。

5) 数据完整性

a) 数据传输无整性保护措施

对应要求：应采用校验技术或密码技术保证重要数据在传输过程中的完整

性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

判例内容参见安全通信网络-通信传输

6) 数据保密性

a) 重要数据明文传输

对应要求：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

b) 重要数据无存储保密性保护

对应要求：应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

判例内容：鉴别信息、个人敏感信息、行业主管部门定义的非明文存储类信息等以明文方式存储，且未采取其他有效保护措施，可判定为高风险。

补偿措施：对存储的敏感信息采取严格的访问限制措施、部署数据库防火墙、数据防泄露产品等安全防护措施的，可通过分析造成信息泄露的难度和影响程度，酌情判断风险等级。

整改建议：采用密码技术保证重要数据在存储过程中的保密性，且相关密码技术符合国家密码管理主管部门的规定。

7) 数据备份恢复

a) 数据备份措施缺失

对应要求：应提供重要数据的本地数据备份与恢复功能。

判例内容：应用系统未提供任何重要数据备份措施，一旦遭受数据破坏，无法进行数据恢复，可判定为高风险。

整改建议：建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。

b) 异地备份措施缺失

对应要求：应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

判例内容：对系统、数据容灾要求较高的系统，如无异地数据灾备措施，或异地备份机制无法满足业务需要，可判定为高风险。

补偿措施：

系统数据备份机制存在一定时间差，若被测单位评估可接受时间差内数据丢失，可酌情降低风险等级；

可根据系统容灾要求及行业主管部门相关要求，根据实际情况酌情判断风险等级。

整改建议：建议设置异地灾备机房，并利用通信网络将重要数据实时备份至备份场地；灾备机房的距离应满足行业主管部门的相关要求。

c) 数据处理系统无冗余措施

对应要求：应提供重要数据处理系统的热冗余，保证系统的高可用性。

判例内容：对数据处理可用性要求较高系统，应采用热冗余技术提高系统的可用性，若核心处理节点（如服务器、数据库等）存在单点故障，可判定为高风险。

补偿措施：当前采取的恢复手段，能确保被测单位评估的 RTO 在可接受范围内，可根据实际情况酌情降低风险等级。

整改建议：建议对重要数据处理系统采用热冗余技术，提高系统的可用性。

8) 剩余信息保护

a) 鉴别信息释放措施失效

对应要求：应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

判例内容：身份鉴别信息释放或清除机制存在缺陷，如在正常进行释放或清除身份鉴别信息操作后，仍可非授权访问系统资源或进行操作，可判定为高风险。

补偿措施：系统采取技术手段，能消除或降低非授权访问系统资源或进行操作所带来的影响，可根据实际情况，酌情判断风险等级。

整改建议：建议完善鉴别信息释放/清除机制，确保在执行释放/清除相关操作后，鉴别信息得到完全释放/清除。

b) 敏感数据释放措施失效

对应要求：应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

判例内容：敏感数据（如个人敏感信息、业务敏感信息等）释放或清除机制存在缺陷，如在正常进行释放或清除操作后，仍可非授权访问这些敏感数据，且可能造成敏感数据泄露的，可判定为高风险。

补偿措施：因特殊业务需要，需要在存储空间保留敏感数据，相关敏感数据进行了有效加密/脱敏处理，且有必要的提示信息，可根据实际情况，酌情降低风险等级。

整改建议：建议完善敏感数据释放/清除机制，确保在执行释放/清除相关操作后，敏感数据得到完全释放/清除。

9) 个人信息保护

a) 违规采集，存储个人信息

对应要求：应仅采集和保存业务必需的用户个人信息。

判例内容：在采集和保存用户个人信息时，应通过正式渠道获得用户同意、授权，如在未授权情况下，采取、存储用户个人隐私信息，可判定为高风险。

补偿措施：在用户同意、授权的情况下，采集和保存与业务有关但非必需的用户个人信息，且用户可根据需要关闭或停止授权的，可根据实际情况，酌情判断风险等级。

整改建议：建议根据国家、行业主管部门以及标准的相关规定，明确向用户表明采集信息的内容、用途以及相关的安全责任，并在用户同意、授权的情况下采集、保存业务必需的用户个人信息。

b) 非授权访问，使用个人信息

对应要求：应禁止未授权访问和非法使用用户个人信息。

判例内容：个人信息可非授权访问或未按国家、行业主管部门以及标准的相关规定使用个人信息，例如在未授权情况下将用户信息提交给第三方处理，未脱敏的情况下用于其他业务用途，未严格控制个人信息查询以及导出权限，非法买卖、泄露用户个人信息等，可判定为高风险。

整改建议：建议根据国家、行业主管部门以及标准的相关规定，通过技术和管理手段，防止未授权访问和非法使用用户个人信息。

10) 数据完整性和保密性

a) 云租户数据，用户个人信息违规出境

对应要求：应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

判例内容：云服务客户数据、用户个人信息等境外存储，且未遵循国家相关规定，可判定为高风险。

整改建议：建议云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

6.1.4.4 等保问题反馈

经过测评机构测评后的 2 周内提供系统的安全问题汇总清单，系统运维单位或开发单位可根据安全问题汇总清单进行整改，秉持杜绝高风险漏洞，中风险漏洞能改尽改的原则。

样表如下：

问题编号	安全要求	安全层面	安全控制点	测评项	资产类型	关联资产	问题描述	问题分析	危害分析	整改建议	关联威胁	原始风险
…												

6.1.4.5 等保问题复核

开发运维单位根据安全问题汇总表的内容进行整改之后，将漏洞整改的结果进行反馈，我司将对相应整改情况进行汇总梳理，并对整改反馈内容进行针对性的复核，确认安全问题是否真正得到整改解决。

6.1.4.6 整改流程与过程文档

网络安全等保整改服务包括准备阶段、整改指导阶段、现场整改阶段、整改报告阶段，并且输出相应的过程文档。

当供应链或第三方产品出现问题时，若整改方案无效，需安排专人跟踪供应链或产品提供方解决问题。

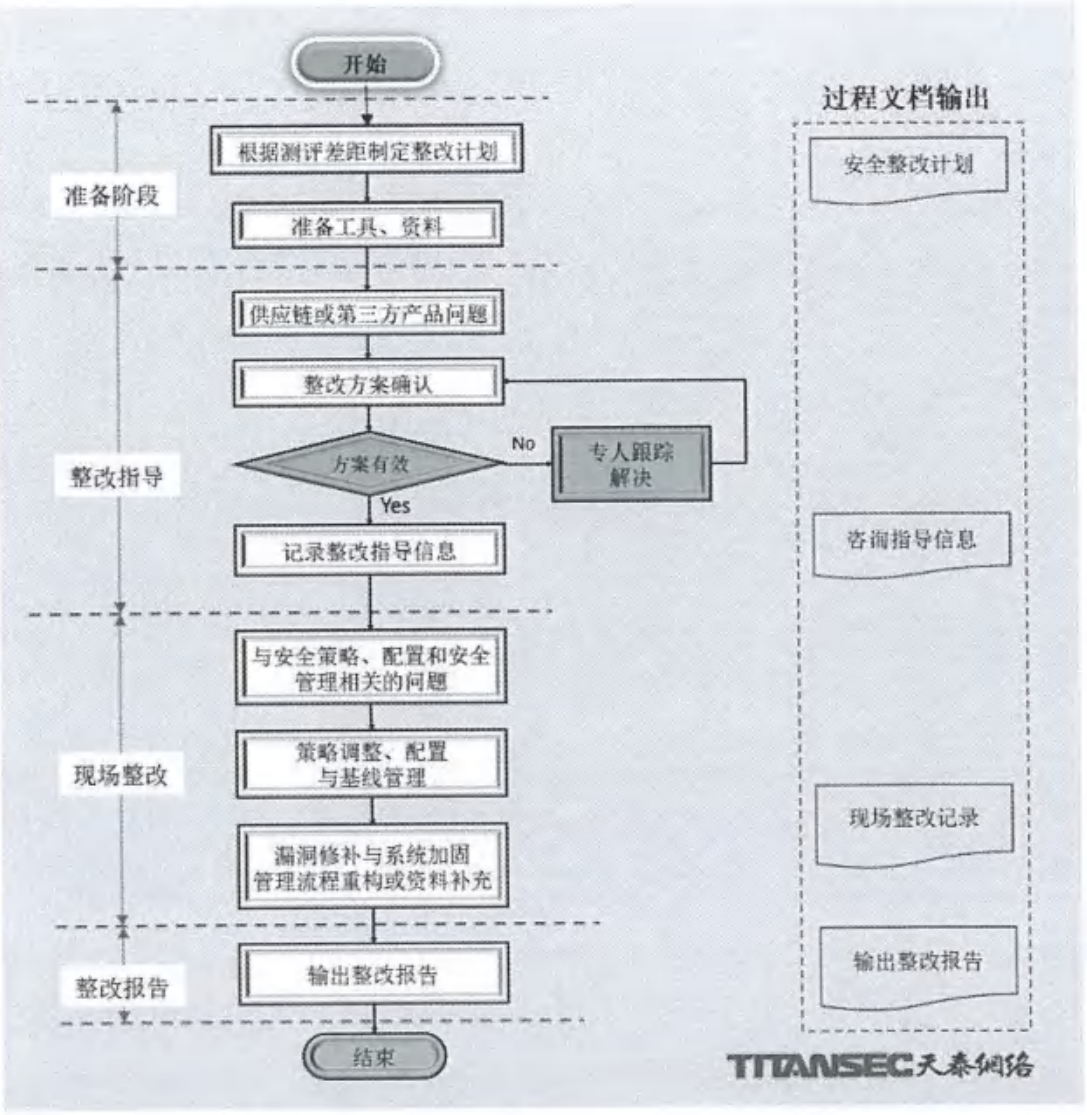


图 6-1-4-6-1 等保测评差距整改流程图

6.1.5服务频次

网络安全等保服务分为现场服务和非现场服务，开展一次，包括两个等保三级和一个等保二级。

对浦东公交公司的等保测评工作将安排在合同签订后的第一个月开始进行，也可根据浦东公交公司的年度网络安全工作计划进行安排。

6.1.6服务成果交付

服务结束后，交付《网络安全测评服务总结报告》。

6.2 网络安全加固服务

6.2.1服务需求

为应用系统 2 个页面防篡改能力，防范应用系统页面被植入非法信息，保障系统正常运行。

为浦东公交使用的 410 台终端提供专业级防病毒服务，保护电脑免受恶意病毒威胁。

6.2.2页面防篡改

在本项目中我司将使用专业的页面防篡改系统为应用系统的页面提供防篡改能力，以达到防范应用系统页面被植入非法信息的目的，保障系统的正常运行。

定期开展页面防篡改运行状态巡检，检查页面防篡改系统保护内容与实际业务的匹配性。及时响应用户业务的变化，根据实际需要，及时调整页面防篡改策略，确保业务系统最新需要保护的页面处于防篡改系统保护范围，

6.2.2.1 防篡改特点

目前，网页被“黑”的现象屡屡发生，尤其是一些重点企事业单位的 WEB 应用，经常成为黑客攻击的目标，为了避免造成经济损失及恶意影响，各 WEB 应用不断加强安全防护。其中，网页防篡改软件最为常见，它能够保护 WEB 应用文件不被篡改。

◆ 有效防护数据安全

通过实施严格的安全措施，如加密技术和访问控制，确保只有授权用户才能访问敏感信息。能够实时监控数据访问和操作行为，一旦检测到异常活动，立即发出警报并采取相应措施。

◆ 维护系统完整性

持续监控文件状态，防止黑客或内部人员对系统文件进行恶意篡改。在检测到文件被篡改时，系统能自动从备份中恢复原始数据，保证数据的一致性和服务的连续性。

◆ 部署简单不影响用户日常使用

网页防篡改软件可以结合当前用户的网站发布模式，或者现有的 CMS 系统进行防篡改软件的部署，部署防篡改之后，通过对发布服务器的操作，通过防篡改的快速同步处理功能，实时将后台更新的网页或者文件同步到监控服务器上面。

1) 网页防篡改的特性

◆ 实时监控响应

a) 持续监测：防篡改软件能够不间断地监控文件和系统的完整性，确保任何未授权的更改都能被即时发现。

b) 警报机制：一旦检测到潜在的篡改行为，软件会立即触发警报，通知管理员采取相应措施。

c) 自动恢复：在很多情况下，防篡改软件不仅能识别问题，还能自动将从备份中恢复数据，保证服务的连续性和数据的一致性。

◆ 多层次安全策略

a) 物理防护：除了软件层面的保护，防篡改解决方案还可能包括物理安全措施，如使用特殊螺丝或封条来防止硬件被非法开启。

b) 逻辑防护：通过加密技术和访问控制来增强安全性，确保只有经过授权的用户才能访问敏感信息。

c) 综合防护：结合多种技术手段，如核心内嵌、外挂轮询等，形成多层次的防护体系，提高整体的安全性。

6.2.2.2 防护功能

页面防篡改防护服务提供如下功能：

类别	具体功能描述
防攻击	采用专利级 Web 入侵检测技术对网站进行多层次的安全检测分析，有效保护网站静态/动态网页及后台数据库信息； 识别、阻止 SQL 注入攻击、跨站攻击、表单绕过、批量挂马等； 识别、阻止其他已知/未知&变形攻击； 基于时间段，源 IP 自动调整防护策略。
防篡改	支持多种保护模式，防止静态和动态网站内容被非法篡改； 新一代内核驱动级文件保护，确保防护功能不被恶意攻击者非法终止； 采用核心内嵌技术，支持大规模连续篡改攻击防护；实时检测与内容恢复，完全杜绝被篡改内容被外界浏览。
平台支持	支持各种主流操作系统：如 Windows2000-2008、RedHat、CentOS、SUSE、Asianux、linux 等； 支持各类 WEB 服务器：如 IIS、Apache、WebLogic、Websphere、Tomcat 等。

6.2.2.3 防篡改服务

天泰网络页面防篡改服务聚焦浦东公交业务系统对外发布网页的安全防护，保障页面内容的真实性、完整性，防范页面被非法篡改、替换内容等安全事件。

（1）实时监测与主动防护

采用文件校验的方式，对网页文件的内容、属性、脚本进行实时监测，识别网页篡改行为，当发现有页面被非法篡改后，快速恢复页面原始内容，确保业务系统页面正常访问。

（2）防篡改页面维护

响应浦东公交业务系统的变化，当业务系统更新时，及时跟进调整防护策略，将最新系统页面纳入防篡改防护范围，确保页面保护与业务系统相匹配。

（3）防护状态巡检

定期对页面防篡改系统开展巡检，查看防篡改系统防护状态，并对防篡改系统防护日志查看和分析，及时发现异常情况并予以处置，最大限度避免安全

事件的发生。

6.2.3 防病毒

在本项目中我司将使用专业的防病毒管理软件，为办公电脑提供防病毒服务，防御办公终端免受病毒等恶意软件威胁；对终端防病毒软件定期进行升级更新，及时更新病毒特征库，确保终端防病毒系统处于最新防护状态；定期开展防病毒状态巡检，确保需要保护的终端都处于防病毒系统保护范围，达到保护电脑免受恶意病毒威胁的目的。

6.2.3.1 防病毒特点

（1）终端安全一体化

◆ 功能一体化：集终端防病毒和安全管控于一体的终端安全管理系统；

◆ 平台一体化：完美兼容 Windows、MacOS、Linux、国产操作系统；

◆ 数据一体化：结合云端大数据和威胁情报，有效感知本地安全态势。

（2）病毒防御多维化

◆ 多引擎技术：拥有领先的 QCE 云安全引擎、QOWL 启发式特征引擎、QDE 机器学习引擎，有效查杀已知和未知病毒；

◆ 立体化主防：具备系统防护、系统加固、入口防护、网络防护等主动防御技术；

◆ 智能自学习：通过海量病毒样本数据自学习，人工智能引擎无需频繁更新特征库、病毒检出率仍远超传统查杀引擎；

（3）安全管控智能化

◆ 资产管理：自动识别全网终端资产信息，实时监控系统状态并告警，保障业务连续性；

◆ 安全策略管理：通过非法外联、外设管理、进程控制、主机防火墙、桌面安全加固等多元化方式，提升终端安全等级；

◆ 漏洞补丁管理：对全网终端漏洞进行扫描并关联，根据终端分组或操作系统类型错峰下发补丁。

（4）满足合规要求

通过一体化的终端管理平台，能够对等级保护等合规要求中的恶意代码防范、访问控制、非法外联管理、资产管理、介质管理、安全审计等控制点进行全面覆盖。

6.2.3.2 防护功能

防病毒提供如下功能：

类别	具体功能描述	
基础功能	控制中心管理	管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定； 支持双因子认证登录方式，提高安全性。
	客户端管理	支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。 支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。
防病毒防护	病毒查杀日志	病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。
	病毒防护报表	病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触、方式统计、趋势图表、按分组、按终端、按病毒名称。
	病毒扫描	支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数。
	主动防御	支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。
	网络防护	支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。

	杀毒引擎	支持不少于两个杀毒引擎混合使用，提高病毒检出率。
补丁管理	漏洞修复设置	支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。
终端管控	外设管理	支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。
	进程管理	支持终端进程红名单、黑名单、白名单功能。可设置核心进程必须运行，也可保护核心进程不被结束，违规并告警。
	违规外联	支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。支持例外白名单添加。
	网络防护	支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建和 IPV6 地址使用等，可自定义提示内容和生效时间。

6.2.3.3 防病毒服务

天泰网络将协助用户完成终端安全管理系统（防病毒）的授权和使用，同浦东公交的网络安全检测、网络安全应急保障等服务协同发力，构建起用户“主动防御+安全检测+应急处置”的全方位安全防护体系。防病毒服务聚焦办公终端病毒、恶意代码、勒索软件等恶意程序的防范与处置，保障办公终端的使用正常，进而保障业务的开展。

（1）防病毒系统部署与适配

深入了解浦东公交终端办公电脑的硬件配置、操作系统类型，选择适配性强、占用资源低、满足政策要求的企业级防病毒软件，确保能够覆盖终端防病毒的需要。

（2）病毒检测与病毒防护

部署防病毒软件管理平台及终端，实时监控终端病毒感染情况，针对病毒、木马、蠕虫等各类恶意程序，采取实时监测、自动拦截的处置方式，最大限度的防范恶意程序扩散。

开启终端病毒安全扫描能力，优化扫描策略、定期对内存、系统关键存储位置、外接设备开展全面病毒查杀，降低病毒感染风险。

（3）病毒库更新与系统优化

建立病毒库定期更新机制，每日同步最新病毒特征库，提升终端病毒防护时效性。定期对防病毒软件进行版本升级、补丁更新，修复防病毒自身安全漏洞，保障防病毒系统稳定运行。

（4）防护状态巡检

定期对终端防病毒防护状态进行巡检，检查终端防病毒软件的运行状态、终端在线情况、病毒库更新情况等，及时发现可能存在的异常情况，并向用户提供整改建议。

6.3 网络安全检测

6.3.1 应用系统安全检测

6.3.1.1 服务需求理解

对浦东公交本部的应用系统每2月开展一次（服务期内共计开展6次）应用系统安全检测，发现应用系统网络安全漏洞隐患，给出漏洞整改建议，并配合浦东公交指定的开发单位及时落实整改，对检测过程中发现的紧急高危漏洞进行人工验证。提供详细的检测分析报告、人工验证报告和漏洞整改建议，协助指导相关应用系统开发单位的技术人员开展漏洞整改，并对整改情况进行复核，确保紧急高危项完成闭环管理。

由于网络协议的开放性、系统软件和应用程序设计上的缺陷、系统管理员的人为疏忽以及网络安全制度的不健全，使得不法分子或者黑客入侵公交网络应用系统成为可能。不管入侵者是从外部还是从内部攻击某一网络应用系统，攻击几乎都是通过不断挖掘操作系统和应用程序的弱点来实现的；这种被利用的操作系统和应用程序的弱点就是所谓的安全漏洞。

漏洞的来源主要分为三类；第一类：是由于操作系统自身设计缺陷带来的安全漏洞，第二类：是应用软件程序的设计 Bug 而引起的漏洞，第三类：是应用服务协议的安全漏洞。为了防止不法分子侵入网络内部，保护网络信息和数

据安全，最有效的方法是确保应用系统没有或者尽量没有缺陷，因此需要对应用系统进行定期的安全检测，以便在非法分子入侵之前找到系统存在的缺陷，从而提前修补漏洞，做到有备无患。

黑客攻击正在从个人向组织化、国家化方向发展，他们目的性强，动机明显，往往有明确的商业、经济利益或政治诉求，攻击手段从传统的随机病毒、木马感染及网络攻击，向高级化、组合化、长期化转变，最明显的一个特点就是能够绕过传统的安全检测和防御体系。

尽管人们在全力以赴发现漏洞，开发人员会快速发布更新或“补丁”，理想情况下，所有用户都会在攻击者有机会利用该漏洞之前安装补丁，但现实情况是，攻击者会迅速发动攻击以利用已知的弱点。此外，即使发布了补丁，由于缺乏漏洞跟踪机制、更新的缓慢实施也意味着攻击者可以在漏洞被发现数年后仍然可以利用漏洞。

面向互联网的应用程序中几乎十分之一的漏洞被认为是高风险或关键风险。

6.3.1.2 应用系统安全漏洞

国际上权威的应用安全漏洞研究与发布机构 OWASP 或 Open Web Security Project 指出，根据漏洞的可利用性、可检测性和对软件的影响，Web 安全漏洞具有优先级。

- ◆ 可利用性　当攻击仅需要 Web 浏览器且最低级别是高级编程和工具时，可攻击性最高。
- ◆ 可检测性　最高可检测性是显示在 URL、表单或错误消息上的信息，最低的是源代码。
- ◆ 影响或破坏　如果安全漏洞暴露或受到攻击，将会造成多大的破坏？最高的是完整的系统崩溃，最低的是什么都没有。

根据 OWASP Top 10 报告，十大应用安全漏洞是：

(1)SQL Injection（SQL 注入）

(2)Cross Site Scripting（XSS 跨站脚本）

(3)Broken Authentication and Session Management（身份验证和会话管理中断）

(4) Insecure Direct Object References（不安全的直接对象引用）

(5) Cross Site Request Forgery（跨站点请求伪造）

(6) Security Misconfiguration（安全配置错误）

(7) Insecure Cryptographic Storage（不安全的加密存储）

(8) Failure to restrict URL Access（无法限制 URL 访问）

(9) Insufficient Transport Layer Protection（传输层保护不足）

(10) Unvalidated Redirects and Forwards（未经验证的重定向和转发）

6.3.1.3 安全服务的计划与方法

扫描评估工具的选用：本方案采用由用户方提供的漏洞扫描工具或由天泰网络提供的应用系统的漏洞扫描工具。

漏洞扫描：通过漏洞扫描和测试分析工具，查找应用系统可能存在的安全漏洞和安全隐患。

人工验证：安排专业技术人员对扫描工具发现的安全漏洞进行人工验证，确认安全漏洞的真实性和可修补性，出具验证报告。

整改加固：采用软件补丁、系统升级、安全加固等方法对存在安全漏洞和安全隐患的系统，进行安全整改指导，指导系统运维、开发单位进行整改加固。

复核验证：对已经整改加固过的应用系统进行漏洞扫描或脆弱性分析，验证确认整改加固的效果，出具复核报告。

图 6-3-1-3 应用系统高风险或关键风险漏洞的闭环管理

漏洞扫描服务方案主要是由安全漏洞方面、安全配置方面检查项构成，这些检查项的覆盖面、有效性成为了安全检查实现的关键。

漏扫工具结合安全管理制度，支持安全风险的检测、管理、评估、预警，并监督安全管理制度各个环节的执行。扫描工具能够高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修复建议，并贴合安全管理流程对修复效果进行审计。

天泰网络可提供自动化的Web应用程序安全测试工具，它可以扫描任何可通过Web浏览器访问的遵循HTTP/HTTPS规则的Web站点和Web应用程序。适用于大型企业的内联网、外延网和面向用户、服务人员、厂商和社会大众的Web网站。

WEB应用程序检测工具的工作方式：

检测工具会扫描整个网站，它通过跟踪站点上的所有链接和robots.txt（如果有的话）而实现扫描，然后就会映射出站点的结构并显示每个文件的细节信息。

在上述的发现阶段或扫描过程之后，检测工具就会自动地对所发现的每一个页面发动一系列的漏洞攻击，这实质上是模拟一个黑客的攻击过程，分析每一个页面中可以输入数据的地方，进而尝试所有的输入组合。这是一个自动扫描阶段。

在它发现漏洞之后，检测工具就会在“警告节点”中报告这些漏洞。每一个警告都包含着漏洞信息和如何修复漏洞的建议。

在扫描完成之后，它会将结果保存为文件以备日后分析以及与以前的扫描相比较。使用报告工具，就可以创建一个专业的报告来总结这次扫描。

6.3.1.4 常见的应用安全漏洞与修补建议

常见的应用安全漏洞类型及整改修补建议：

(1) SQL注入

描述:SQL 注入是一个安全漏洞，允许攻击者通过操纵用户提供的数据来更改后端 SQL 语句。当用户输入作为命令或查询的一部分被发送到解释器并且欺

骗解释器执行非预期的命令并且允许访问未授权的数据时，发生注入攻击。由Web应用程序执行时的SQL命令也可以公开后端数据库。

意义:攻击者可以将恶意内容注入易受攻击的字段。可以从数据库中读取敏感数据，如用户名，密码等。可以修改数据库数据（插入/更新/删除）。管理操作可以在数据库上执行易受攻击的对象:输入字段与数据库交互的URL。

举例：登录页面上的SQL注入

在没有有效凭据的情况下登录应用程序。

有效的UserName可用，密码不可用。

测试网址：http：//demo.testfire.net/default.aspx;

用户名：sjones　密码：1 = 1'或 pass123 创建 SQL 查询并将其发送到Interpreter，如下所示SELECT * FROM Users WHERE User_Name = sjones AND Password = 1 = 1'或pass123;

建议:白名单列出输入字段避免显示对攻击者有用的详细错误消息。

(2) XSS跨站脚本

描述:Cross Site Scripting也简称为XSS。XSS漏洞针对嵌入在客户端（即用户浏览器而不是服务器端）的页面中嵌入的脚本。当应用程序获取不受信任的数据并将其发送到 Web 浏览器而未经适当验证时，可能会出现这些缺陷。在这种情况下攻击者可以使用 XSS 对用户执行恶意脚本，由于浏览器无法知道脚本是否可靠，脚本将被执行，攻击者可以劫持会话 Cookie，破坏网站或将用户重定向到不需要的恶意网站。XSS是一种攻击，允许攻击者在受害者的浏览器上执行脚本。

意义：利用此安全漏洞，攻击者可以将脚本注入应用程序，可以窃取会话Cookie，破坏网站，并可以在受害者的计算机上运行恶意软件。

易受攻击的对象:输入字段网址

例子:

http://www.vulnerablesite.com/home?" < script > alert(" xss") </script >上述脚本在浏览器上运行时，如果站点易受 XSS 攻击，将显示一个消息框。如果攻击者想要显示或存储会话Cookie，则可以进行更严重的攻击。

建议:白名单输入字段输入输出编码

(3) 身份验证和会话管理中断

描述:网站通常为每个有效会话创建会话 Cookie 和会话 ID,这些 Cookie 包含敏感数据，如用户名，密码等。当会话通过注销或浏览器突然关闭结束时，这些 Cookie 应该无效，即每个会话应该有一个新的 Cookie。如果 Cookie 未失效，则敏感数据将存在于系统中。例如，使用公共计算机（Cyber Cafe）的用户，易受攻击的站点的 Cookie 位于系统上并暴露给攻击者。攻击者在一段时间后使用相同的公共计算机，敏感数据会受到损害。以同样的方式，用户使用公共计算机，而不是注销，他突然关闭浏览器。攻击者使用相同的系统，当浏览同一个易受攻击的站点时，受害者的上一个会话将被打开。攻击者可以通过窃取个人资料信息、信用卡信息等任何他想做的事情。应该进行检查以找到身份验证和会话管理的强度。Cookie 应该在不影响密码的情况下正确使用密钥、会话令牌。

易受攻击的对象:在 URL 上公开的会话 ID 可能导致会话固定攻击，注销和登录前后的会话 ID 相同，会话超时未正确管理。应用程序为每个新会话分配相同的会话 ID。应用程序经过身份验证的部分使用 SSL 进行保护，密码以散列或加密格式存储，会话可由低权限用户重用。

意义:利用此漏洞，攻击者可以劫持会话，对系统进行未经授权的访问，从而允许泄露和修改未经授权的信息。使用盗取的 Cookie 或使用 XSS 的会话可以劫持会话。

例子：航空公司预订应用程序支持 URL 重写，将会话 ID 放在 URL 中：http://Examples.com/sale/saleitems;jsessionid=2P0OC2oJM0DPXSNQPLME34SERTBG/dest=Maldives（出售门票）该网站的经过身份验证的用户希望让他的朋友了解该销售并发送电子邮件。朋友收到会话 ID，可用于进行未经授权的修改或滥用保存的信用卡详细信息。应用程序容易受到 XSS 攻击，攻击者可以通过 XSS 访问会话 ID 并可用于劫持会话。应用程序超时未正确设置。用户使用公共计算机并关闭浏览器，而不是注销并离开。攻击者稍后使用相同的浏览器，并对会话进行身份验证。

建议：应根据 OWASP 应用程序安全验证标准定义所有身份验证和会话管理要求。不要在 URL 或日志中公开任何凭据，还应该尽力来避免可用于窃取会话

ID 的 XSS 漏洞。

(4) 不安全的直接对象引用

描述：当开发人员公开对内部实现对象的引用（例如 URL 或 FORM 参数中的文件、目录或数据库键）时，就会发生这种情况。攻击者可以使用此信息访问其他对象，并可以创建将来的攻击来访问未经授权的数据。

意义:使用此漏洞，攻击者可以访问未经授权的内部对象，可以修改数据或破坏应用程序。

易受攻击的对象:在 URL 中。

例子:更改以下 URL 中的“userid”可以使攻击者查看其他用户的信息。http://www.vulnerablesite.com/userid=123 修改为

http://www.vulnerablesite.com/userid=124 攻击者可以通过更改用户标识值来查看其他信息。

建议：实施访问控制检查。避免在 URL 中公开对象引用，验证对所有引用对象的授权。

(5) CSRF 跨站点请求伪造

描述:Cross Site Request Forgery 是来自跨站点的伪造请求。CSRF 攻击是指恶意网站、电子邮件或程序导致用户的浏览器在用户当前已对其进行身份验证的受信任站点上执行不需要的操作时发生的攻击。CSRF 攻击强制登录受害者的浏览器向易受攻击的 Web 应用程序发送伪造的 HTTP 请求，包括受害者的会话 Cookie 和任何其他自动包含的身份验证信息。当用户在登录原始网站时点击 URL 时，攻击者将向受害者发送链接，该数据将从网站上被窃取。

意义:将此漏洞用作攻击者可以更改用户配置文件信息，更改状态，代表管理员创建新用户等。

易受攻击的对象:用户档案页面用户账户表单商业交易页面

例子:受害者使用有效凭据登录银行网站。他收到攻击者的邮件说“请点击此处捐赠 1 元。”当受害者点击它时，将创建一个有效请求以向特账户捐赠 1 元。http://www.vulnerablebank.com/transfer.do?account=cause&amount=1 攻击者捕获此请求并创建以下请求，并嵌入一个按钮，按下按钮“我同意”。http://www.vulnerablebank.com/transfer.do?account=Attacker&amount=10

00 由于会话已通过身份验证并且请求通过银行网站发送，因此服务器将向攻击者转移 1000 元。

建议:在执行敏感操作时强制用户在场。实现 CAPTCHA，重新认证和唯一请求令牌等机制。

(6) 安全配置错误

描述:必须为应用程序、框架、应用程序服务器、Web 服务器、数据库服务器和平台定义和部署安全性配置。如果这些配置正确，攻击者可能会未经授权访问敏感数据或功能。有时这种缺陷会导致系统完全瘫痪。保持软件更新也能提升安全性。

意义:利用此漏洞，攻击者可以枚举底层技术和应用程序服务器版本信息、数据库信息并获取有关应用程序的信息以进行更多攻击。

易受攻击的对象:网址表格字段输入字段

例子:应用程序服务器管理控制台将自动安装，不会被删除。默认账户不会更改。攻击者可以使用默认密码登录，并可以获得未经授权的访问。您的服务器上未禁用目录列表。攻击者发现并可以简单地列出目录以查找任何文件。

建议:强大的应用程序架构，可在组件之间提供良好的分离和安全性。更改默认用户名和密码。禁用目录列表并实施访问控制检查。

(7) 不安全的加密存储

描述:不安全的加密存储是一种常见的漏洞，在敏感数据未安全存储时存在。用户凭据、配置文件信息、健康详细信息、信用卡信息等属于网站上的敏感数据信息。该数据将存储在应用程序数据库中。如果不使用加密或散列函数来正确地存储此数据，则它将容易受到攻击者的攻击。

意义:通过使用此漏洞，攻击者可以窃取，修改此类受弱保护的数据，以进行身份盗用、信用卡欺诈或其他犯罪。

易受攻击的对象:应用数据库。

例子:在其中一个银行应用程序中，密码数据库使用未加保留的哈希函数来存储每个人的密码。SQL 注入漏洞允许攻击者检索密码文件。

建议：确保适当的强标准算法。不要创建自己的加密算法。仅使用经过批准的公共算法，如 AES、RSA 公钥加密和 SHA-256 等。确保异地备份已加密，但

密钥是单独管理和备份的。

(8) 无法限制URL访问

描述：Web应用程序在呈现受保护的链接和按钮之前检查URL访问权限，每次访问这些页面时，应用程序都需要执行类似的访问控制检查。在大多数应用程序中，特权页面、位置和资源不会呈现给特权用户。通过智能猜测，攻击者可以访问权限页面。攻击者可以访问敏感页面、调用函数和查看机密信息。

意义：利用此漏洞攻击者可以访问未经授权的URL，而无需登录应用程序并利用此漏洞。攻击者可以访问敏感页面、调用函数和查看机密信息。

易受攻击的对象：网址

例子:攻击者注意到 URL 表示角色为“/ user / getaccounts”。他修改为“/ admin / getaccounts”。攻击者可以将角色附加到URL。

http://www.vulnerablsite.com 可以修改为

http://www.vulnerablesite.com/admin

建议:实施强大的访问控制检查。身份验证和授权策略应基于角色。限制对不需要的URL的访问。

(9) 传输层保护不足

描述:处理用户（客户端）和服务器（应用程序）之间的信息交换。应用程序经常通过网络传输敏感信息，如身份验证详细信息、信用卡信息和会话令牌。通过使用弱算法或使用过期或无效的证书或不使用SSL，可以允许将通信暴露给不受信任的用户，这可能会危及Web应用程序和/或窃取敏感信息。

意义:利用此Web安全漏洞，攻击者可以嗅探合法用户的凭据并获取对该应用程序的访问权限。可以窃取信用卡信息。

易受攻击的对象:通过网络发送的数据。

建议:启用安全 HTTP 并仅通过 HTTPS 强制执行凭据传输。确保您的证书有效且未过期。

例子：不使用 SSL 的应用程序，攻击者只会监视网络流量并观察经过身份验证的受害者会话 Cookie。攻击者可以窃取该 Cookie 并执行 Man-in-the-Middle 攻击。

(10) 未经验证的重定向和转发

描述:Web 应用程序使用很少的方法将用户重定向并转发到其他页面以实现预期目的。如果在重定向到其他页面时没有正确的验证，攻击者可以利用此功能，并可以将受害者重定向到网络钓鱼或恶意软件站点，或者使用转发来访问未经授权的页面。

意义:攻击者可以向用户发送包含附加编码恶意 URL 的真实 URL 的 URL。用户只需看到攻击者发送的URL 的真实部分就可以浏览它并可能成为受害者。

例子:

http://www.vulnerablesite.com/login.aspx?redirectURL=ownsite.com

修改为

http://www.vulnerablesite.com/login.aspx?redirectURL=evilsite.com

建议:只需避免在应用程序中使用重定向和转发。如果使用，请不要在计算目的地时使用用户参数。如果无法避免目标参数，请确保提供的值有效，并为用户授权。

除了上述 10 类漏洞之外，应用系统的漏洞扫描还要分析系统是否存在以下风险：

- 应用 DDoS 攻击风险
- 弱口令、口令验证风险
- 被注入木马风险
- 后台管理权限泄漏风险
- 目录遍历风险
- HTTP 协议追踪风险
- 敏感信息泄露风险

上述应用安全系统漏洞和风险，应用系统开发人员、网络安全管理人员、网络安全服务与运维人员应了解这些漏洞形成的原因、被利用的方法和防范的措施，以便于从不同的工作角度对应用系统提供安全防护和保障。

6.3.1.5 服务流程

应用系统漏洞检测与整改复核服务包括准备阶段、扫描与漏洞修复阶段、报告阶段，并且输出相应的过程文档。

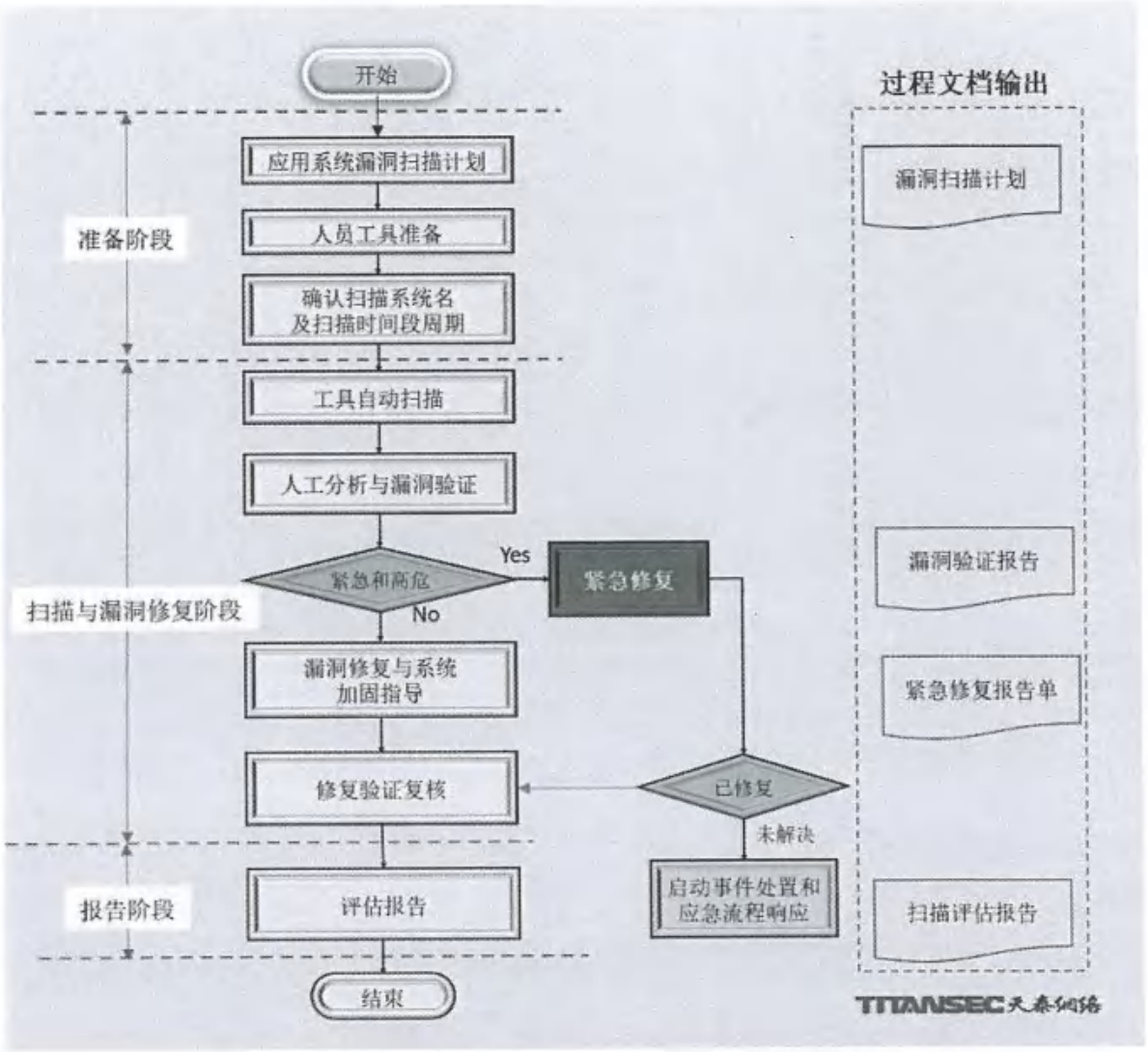


图 6-3-1-5 应用系统漏洞检测与整改修复服务流程

6.3.1.6 服务人员和服务工具

应用系统漏洞检测与整改复核服务根据服务的不同阶段安排不同的服务人员参与，准备阶段由项目经理、检查服务人员和服务支持人员共同制定服务计划和服务检查表单；检查与复核过程中，安排检查小组分别应用系统的安全检查。检查小组由资深的安全检查服务工程师带队，安全服务工程师和安全服务助理参与；检查总结阶段由安全检查服务工程师起草总结报告，安全专家进行

审核。

图 6-3-1-6-1 应用系统漏洞检测与整改复核服务人员

应用系统修复漏洞的最佳方法是更新应用系统软件和相应的组件（中间件），调整应用系统安全配置，强化身份鉴别、授权和访问控制策略。由于应用系统受到系统软件、服务器、软件开发环境的限制，这就需要安全专家、技术支持人员参与进行测试，确保整改修复是安全的和成功的，避免未测试的修复可能导致应用系统严重的安全问题和性能问题。

天泰网络将使用应用系统漏洞扫描工具、弱口令检测工具、病毒查杀类工具及各种服务器检测小程序开展安全检查服务。

表 6-3-1-6-2 应用系统漏洞检测与整改复核服务工具

序号	工具名称	内容描述	版本
一、应用漏洞扫描类			
1.1	天泰安全核查工具	包含主机安全扫描模块，可选配网站安全扫描和基线配置核查模块，集多种安全检测功能于一身，帮助用户发现服务器和 WEB 应用安全缺陷和漏洞。	V2.0
1.2	网御 WEB 安全漏洞扫描平台	含 Web 漏洞扫描模块、网站安全监测模块	TS-WSM-LE3
二、病毒查杀类			
2.1	金山急救箱 3.0	木马查杀软件，可快速诊断系统是否中毒，强力查	3.5.8.18

		杀顽固和未知木马，将系统和上网环境恢复如初	
2.2	天擎终端安全系统	针对需要检查的设备做木马查杀、插件清理、垃圾清理、漏洞修复、电脑体检	10.0

6.3.1.7 服务周期与服务频次

应用系统漏洞检测与整改服务为现场服务，将为浦东公交的应用系统服务期间共6次。

对公交公司应用系统的漏洞检测工作将安排每2月一次。

6.3.1.8 应用系统漏洞扫描报告样例

应用系统漏洞扫描报告（样例）

扫描信息

扫描网址	www.XXXXXX.gov.cn
开始时间	2026年1月02日 00:17:12
结束时间	2026年1月04日 13:57:53
扫描时间	1 天 13 时 40 分

安全风险等级

威胁等级：高危 CVSS分值10.0

发现一个或多个高危漏洞。恶意用户可以利用这些漏洞进行攻击或窃取后端数据库数据或破坏该应用系统。

应用安全情况

在此次扫描中，共发现20类安全问题影响35处，其中高危风险5类影响10处，中危风险5类影响7处，低危风险6类影响8处，提示信息4类影响10处。

安全威胁汇总	**35**	
高危漏洞	**10**	
中危漏洞	**7**	

低危漏洞 8

提示信息 10

应用漏洞类别

漏洞名称	威胁等级	漏洞数量
Blind SQL Injection	高	2
Weak password	高	1
Microsoft IIS tilde directory enumeration	高	1
WebDAV Directory with write permissions	高	3
WebDAV remote code execution	高	3
HTML form without CSRF protection	中	1
PHPinfo page found	中	1
PHP allow_url_fopen enabled	中	1
PHP open_basedir is not set	中	1
WebDAV directory listing	中	3
Clickjacking: X-Frame-Options header missing	低	1
OPTIONS method is enabled	低	1
Login page password-guessing attack	低	1
Possible sensitive directories	低	3
Possible sensitive files	低	1
WebDAV enabled	低	1
Password type input with auto-complete enabled	信息	1
Microsoft IIS version disclosure	信息	1
Possible internal IP address disclosure	信息	5
Broken links	信息	3

6.3.1.9 服务成果交付

网络安全检测中应用系统安全检测服务科目完成后出具服务报告，包含整改复核结果。

6.3.2网络安全检查

6.3.2.1 服务需求理解

对浦东公交下属的四家直属企业各开展一次网络安全检查，发现网络中存在的安全隐患，给出安全建议。

近年来AI的热门兴起，再加上日益严峻的网络安全形式，单位越来越注重网络安，除了本部网络安全需加强之外，下属企业的网络安全也需重视，下属企业存在网络安全资金不足、网络安全人才短缺、员工对网络安全并不是很重视等情况，通过以网络安全检查的形式可**以查促建**（督促补齐短板）、**以查促管**（强化日常管理）、**以查促治**（推动系统治理），完善各单位的网络安全管理制度、网络安全责任制，加强对服务器、终端、应用系统的防护和整改，从而整体增加所有单位的网络安全情况。

6.3.2.2 网络安全检查目的

对下属单位进行网络安全检查，其根本动因已从单纯的“技术合规”升级为“风险治理”，最终目标是保障整个组织体系的安全稳定。具体可从以下四个层面理解：

（1） 法律强制：将顶层设计转化为执法实践

根据《网络安全法》《数据安全法》等，主管单位对下属机构负有指导和监督的法定义务。最新趋势显示，监管逻辑正发生深刻转变：从过去检查“是否买了防火墙、是否制定了制度”（过程合规），转向查验“是否真正防住了攻击、保护好了数据”（结果导向）。这意味着，上级检查不仅是“查作业”，更是“验成效”，下属单位若发生数据泄露，即使制度健全也可能被认定失职。

（2） 履职手段：落实责任制的刚性抓手

网络安全检查是主管单位履行领导责任的直接体现。多地政务部门已明确将网络安全纳入绩效考核和领导干部评价。通过检查，上级单位不仅是在排查漏洞，更是在向下传递压力信号，确保“一把手负责制”不落空。对于自查敷衍、整改造假的下属单位，检查制度通常设置了明确的处罚条款。

（3） 风险管控：从“被动修补”转向“主动清除”

上级检查是发现“灯下黑”最有效的手段。下属单位往往存在弱口令、僵尸系统、供应链后门等自身难以发现或长期忽视的风险。通过上级组织的渗透测试、远程扫描等技术实测，可以像“网络攻防演习”一样，赶在黑客之前挖出深层次漏洞。

（4） 治理升级：构建全链条“生态防御”

随着数字化深入，单一单位的防线已无法应对沿供应链发起的攻击。新修订的《网络安全法》强调从“点状防守”转向“生态治理”。上级检查成为贯穿产业链的“免疫针”：一方面，确保下游单位的脆弱性不会反噬上游核心系统；另一方面，将安全标准作为刚性约束，倒逼整个行业链条提升安全水位。

6.3.2.3 服务范围

浦东公交下属四家直属企业单位。

6.3.2.4 安全服务计划与方法

检查准备：约定检查时间、参与人员、检查内容、相关材料准备。

现场检查：分为制度和技术的检查，制度上检查是否建立网络安全责任制、网络安全管理制度、是否保留制度的相关留痕材料。技术上对应用系统、服务器、终端、大屏等设备进行检查，查看是否存在高风险项。

检查问题反馈：针对本次检查出的问题进行反馈，对制度上以及技术上需整改加强的地方进行反馈。

问题整改：等待下属单位反馈相关整改情况，并进行梳理统计。

复核验证：对已经整改过的问题进行复核验证，形成闭环。

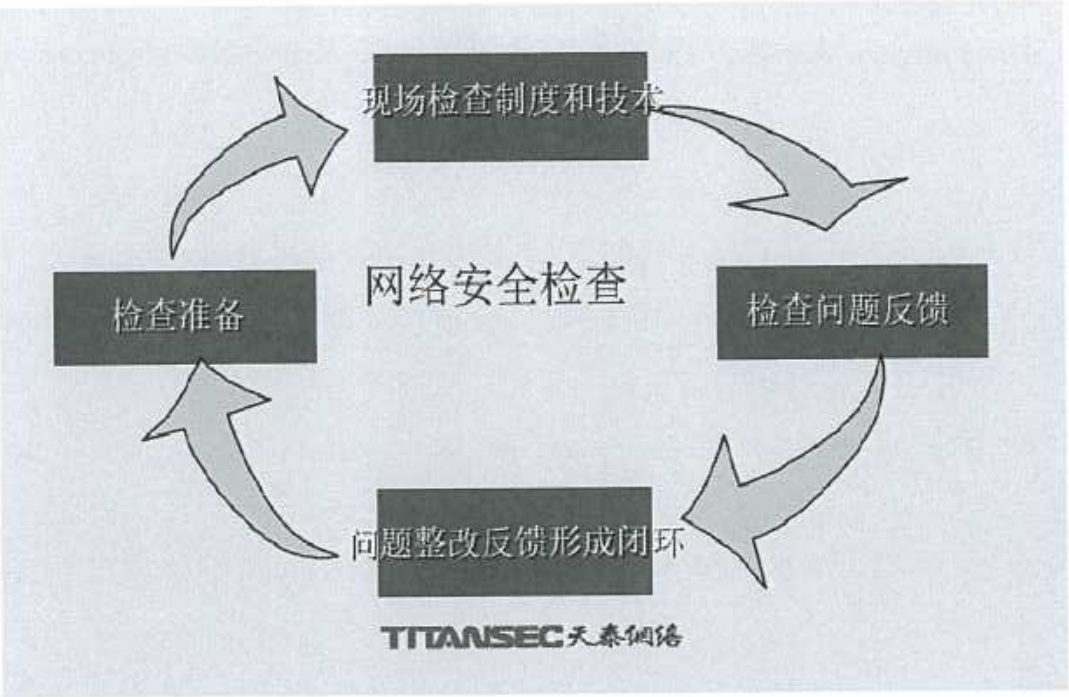


图 6-3-2-4 网络安全检查的闭环管理

6.3.2.5 服务流程

网络安全检查服务包括准备阶段、网络安全检查阶段、检查报告阶段，并且输出相应的过程文档。

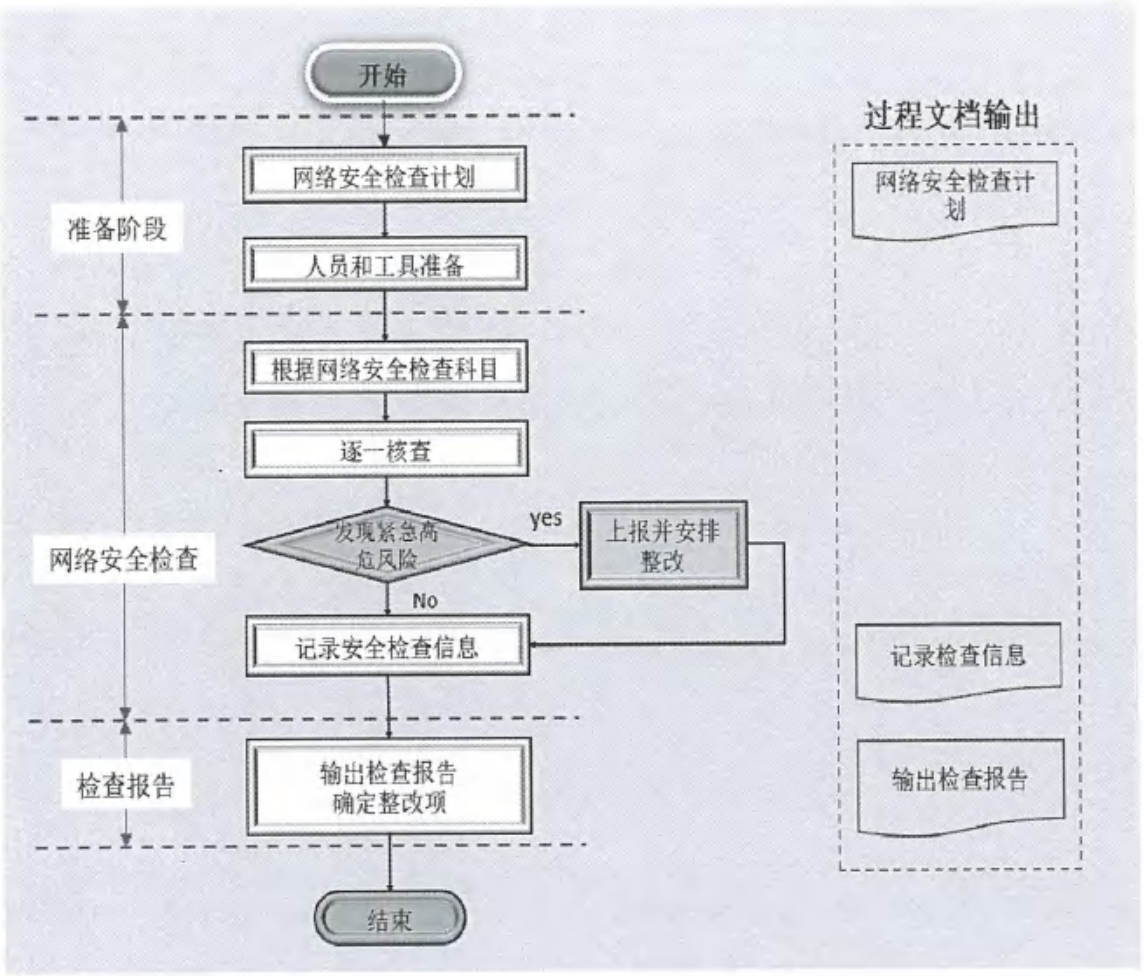


图 6-3-2-5 网络安全检查服务流程

6.3.2.6 服务人员和服务工具

网络安全检查服务根据服务的不同内容安排不同的服务人员参与，准备阶段由项目经理、检查服务人员和服务支持人员共同制定服务计划和服务检查表单；检查过程中，安排检查小组分别应用系统的安全检查、网络安全制度的检查。检查小组由资深的安全检查服务工程师带队，安全服务工程师和安全服务助理参与；检查总结阶段由安全检查服务工程师起草总结报告，安全专家进行审核。

图 6-3-2-6 网络安全检查服务人员

天泰网络将使用应用系统漏洞扫描工具、弱口令检测工具、病毒查杀类工具及各种服务器检测小程序开展安全检查服务，并派遣对于制度方面有丰富经验的服务人员进行制度上的检查。

6.3.2.7 服务周期与服务频次

服务周期一年内共四个季度，计划每季度去一家直属企业进行网络安全检查。

6.3.2.8 服务成果交付

每次直属企业网络安全检查结束，提供《安全检查技术报告》。

6.4 网络安全应急保障

6.4.1服务需求理解

重要时期关键节点（如两会、五一、国庆、进博会等）或主管单位例行检查时，提供网络安全专项保障服务，确保各类重要信息系统的安全可靠运行，并向提供专项保障服务报告。提供全年的网络安全应急响应保障，一般事件 1 小时内响应，重要事件 30 分钟内响应。如采购人发生网络信息安全突发事件，及时响应、介入事件处置，预防和减少网络安全事件造成的损失和危害。

浦东公交网络信息系统可能受到各种已知和未知的威胁而导致有害程序事

件、网络攻击事件、信息破坏事件、数据泄露事件、系统故障和灾害性事件等安全事件的发生。

网络安全应急响应是指浦东公交网络信息系统对于内部监控发现的和外部上报的漏洞和安全事件做出应急处置。内部通过日志收集、安全检查和异常分析检测等手段发现可能的安全事件，并进行告警。外部上报的途径包括应急响应中心、态势感知平台或漏洞扫描服务、开源的第三方组件、对外通报的 CVE 漏洞信息和来自三方的威胁情报信息。

一旦发现安全事件和漏洞，用户管理部门将组织专业人员判断是否进行相应的安全应急响应。应急响应的第一步骤是对上报的漏洞和安全事件的真实性进行排查确认。一旦确认，用户管理部门会启动应急响应流程，并按照标准步骤进行处置。漏洞类事件会先确认漏洞的安全等级和影响范围，并保证安全产品能在对应的 SLA 时间内完成相关漏洞的修复并发布上线。安全事件类的处置则主要包含事件影响范围确认，事件影响消除，和事后复盘改进等主要步骤。同时，应急响应指挥部门也会及时通过线上公告等方式将安全问题第一时间通知相关成员。

以下是发现网络安全事件的方法：

- 特权用户账户的异常行为。控制特权用户账户是网络攻击事件的重要步骤，一旦特权账户出现异常状况，极有可能表明有人在恶意利用该账户试图进入用户的网络和信息系统；
- 未经授权访问服务器和数据。许多内部人员会尝试究竟可以访问哪些系统和数据。危险信号包括未经授权的用户试图访问服务器和数据，请求访问与工作无关的系统或数据，在异常时间从异常位置访问系统，以及在短时间内从多个不同位置登录系统；
- 出站网络流量异常。用户要关注的不仅仅是进入业务网络的流量，还应该监测离开应用边界的流量。这可能包括恶意程序正在外发大量的业务数据；
- 来源或去向异常的网络流量。对于用户来说，其网络应用流量都是有一定规律的，一旦出现来源或去向异常的流量，可能表明是恶意网络活动引发。系统管理员应及时调查发送到未知网络的流量，以确保是合法流

量；

- 资源过度消费。虚拟机内存或存储空间的使用量增加也意味着有攻击者可能在非法访问网络应用系统；
- 系统配置更改。未经批准的配置更改表明可能存在恶意活动，包括重新配置服务、安装启动程序或更改防火墙，添加的额外计划任务也是如此；
- 隐藏的文件。通过文件名、大小或位置的判断，一些突然出现的隐藏文件很可能是可疑的恶意文件，很有可能会导致数据或日志信息泄露；
- 异常浏览行为。这些异常行为包括意外的重定向、浏览器配置变化或重复的弹出窗口等；
- 异常的注册表修改。这种情况主要发生在恶意软件感染操作系统后，这也是恶意软件确保其留在受感染系统中的主要方式之一。

攻击途径是指攻击者用来访问用户虚拟机或应用服务器、投放攻击载荷或实现恶意访问的路径或手段，主要包括病毒、邮件附件、网页、弹出窗口、即时消息、聊天室和欺骗等。这些方法会涉及软件应用、系统软件以及社会工程欺骗等。

在用户网络安全事件响应中，首先应该要妥善处理使用常见攻击途径的事件，包括如下：

- 外部/可移动介质。网络攻击会从磁盘、光驱或 USB 外围设备等可移动介质来执行；
- 暴力消磨。这种攻击使用暴力方法来攻击、削弱或破坏网络、系统或服务；
- Web 攻击。攻击会从网站或基于 Web 的应用程序来执行；
- 电子邮件攻击。攻击通过电子邮件或其附件来发起，攻击者引诱收件人点击恶意链接、进入受感染的网站，或者打开受感染的附件；
- 不当使用。这种类型的事件源于授权的用户违反了用户的可接受使用政策；
- 无意识下载。用户浏览触发恶意软件下载的网站，这可能在用户不知情的情况下发生。无意识下载利用了 Web 浏览器中的漏洞，使用 JavaScript 及其他浏览功能注入恶意代码；

- 基于广告的恶意软件。这种攻击通过嵌入在网站广告中的恶意软件来执行。仅仅查看恶意广告就可能将恶意代码注入到不安全的设备中。此外，恶意广告还可以直接嵌入到受信任的应用程序中，并通过它们来投放；
- 鼠标悬停。这利用了 PowerPoint 等办公软件中的漏洞。当用户将鼠标悬停在链接上而不是点击链接以查看去向时，shell 脚本可以自动启动；
- 恐吓软件。通过恐吓用户来说服用户购买和下载危险的软件，如果用户下载了该软件并允许程序执行，系统就会被感染。

识别网络攻击的方法

虽然用户永远无法确定攻击者会通过哪条路径进入网络，但可以总结了解一些有共性的常用攻击方法，在每个攻击阶段中，攻击者都会有一些特定的实现目标。现代网络攻击通常分为以下几个阶段：

- 侦察（识别目标）。攻击者从用户外面评估目标，以识别可攻击的目标。攻击者的目标是找到那些几乎没有保护措施或存在漏洞的信息系统，进而实现非法的访问；
- 武器化（准备行动）。在这个阶段，攻击者会创建专门设计的恶意软件。攻击者根据在前一阶段收集而来的情报，定制工具，以满足攻击目标网络的特定需求；
- 投放载荷（实施行动）。攻击者会通过多种入侵方法向目标发送恶意软件，比如钓鱼邮件、中间人攻击或水坑攻击；
- 利用（闯入系统）。威胁分子利用漏洞访问目标的网络；一旦黑客侵入了网络，他就会安装持久性的后门植入程序，以便在较长时间内自由访问；
- 指挥和控制（远程控制植入程序）。恶意软件打开一条指挥通道，使攻击者能够通过网络远程操纵目标的系统和设备。然后，黑客可以从管理员手中获取整个系统的控制权；
- 行动（达到任务的目的）。鉴于攻击者已掌握了目标系统的指挥和控制权，接下来发生什么完全取决于攻击者，他们可能破坏或窃取数据、毁坏系统或索要赎金等。

6.4.2 应急响应服务计划和方法

根据用户管理部门的安排，如遇到突发网络安全事件后参与网络安全事件处置和应急响应，除现场服务人员即时响应外，专业服务团队将按响应计划在规定的时间赶到现场，协助风险核查、控制威胁、恢复系统、分析汇报等，参与完成应急处置任务。

应急响应服务，以“服从指挥、快速反应、密切协同、有效处置”为行动指南，在遇到突发网络安全事件后采取专业的安全措施和行动，并对已经发生的安全事件进行监控、分析、协调、处理等工作，保障用户系统的网络安全，最大程度的减少安全事件所带来的经济损失以及恶劣的社会负面影响。

应急响应服务范围为用户网络信息系统可能涉及的有害程序事件（如病毒爆发）、网络攻击事件、信息破坏事件（篡改、泄露、窃取、丢失等）、互联网应用（如网站）漏洞事件、安全系统中断、网络安全设施运行异常等网络安全事件时，由天泰网络应急响应技术人员参与处置现场突发安全事件。

1) 服务方法及服务内容

应急响应服务分为应急准备阶段、监测响应阶段（具体可分为监测阶段、抑制阶段、根除阶段、恢复阶段）和总结阶段。

应急响应的服务团队由管理、业务、技术和行政等人员组成，包括项目管理人员、应急响应专家、应急响应服务实施人员、应急响应日常运行人员及行政后勤人员等。

2) 应急准备阶段

在网络安全事件真正发生前为应急响应做好预备性的工作，安全服务商将与用户沟通应急响应服务的实施方式及内容，制定网络安全事件技术应对表；确定具体角色和职责分工细则；制定应急响应协同调度方案；准备和管理相关技术基础；确定并提交《应急响应实施方案》，并得到开展应急响应实施工作的授权。

应急准备阶段的工作包括：

- 明确用户的应急需求；
- 根据用户提供的网络拓扑图、安全事件报告程序、专项应急预案以及业务系统主管及运维人员介绍，了解用户的各项业务功能及各项业务功能

之间的相关性，确定支持各种业务功能的相应信息系统资源及其它资源，明确相关信息的保密性、完整性和可用性要求。

- 与用户方签订保密协议；
- 制定详细的服务实施方案；
- 做好服务人员和服务工具的准备。

3) 监测阶段

安全服务人员对网络安全事件做出初步的动作和响应，根据获得的初步材料和分析结果，预估事件的类型、范围和影响程度，制定进一步的响应策略，并且保留相关证据。

监测对象及范围确定：

- ✧ 对发生异常的系统进行初步分析，判断是否真正发生了安全事件；
- ✧ 与用户共同确定监测对象及范围；
- ✧ 监测对象及范围需得到用户的授权；
- ✧ 指导并督促运维单位做好系统、数据、配置、核心参数的日常备份管理。

监测方案的确定：

- ✧ 服务人员应和用户共同确定监测方案；
- ✧ 制定的监测方案应明确服务人员所使用的监测规范；
- ✧ 制定的监测方案应明确服务人员的监测范围，其监测范围应仅限于用户已授权的与安全事件相关的数据，对用户的机密性数据信息未经授权不得访问；
- ✧ 制定的监测方案应包含实施方案失败的应变和回退措施；
- ✧ 服务人员将与用户充分沟通，并预测应急处理方案可能造成的影响；
- ✧ 监测阶段过程中，用户需要向服务人员提供必要的配合工作，以完成应急处理工作；
- ✧ 服务人员将在用户的监督下进行，不得脱离用户监督范围进行操作。

监测结果的处理：

- ✧ 确定安全事件的类型

经过监测，判断出网络安全事件类型。网络安全事件分为有害程序事件、网络攻击事件、数据安全事件、信息内容安全事件、系统性故障、其他网络安

全事件。

✧ 评估突发网络安全事件的影响

对于应启动应急预案的安全事件按照应急预案响应机制进行安全事件处置。对未知安全事件的处置，应根据安全事件的等级，制定安全事件处置方案，应根据事件具体情况，采取抑制措施，抑制事件进一步扩散。

4) 抑制阶段

抑制阶段要及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，同时要确保封锁、管控方法对涉及相关业务影响最小。

应急响应服务人员将在监测分析的基础上，初步确定与安全事件相对应的抑制方法。

应急响应服务人员将告知服务对象所面临的首要问题。

应急响应服务人员所确定的抑制方法和相应的措施需得到用户的认可。

在采取抑制措施之前，应急响应服务人员会和服务对象充分沟通，告知可能存在的风险，制定应变和回退措施，并与用户达成协议。

应急响应服务人员将严格按照相关约定实施抑制，不得随意更改抑制的措施的范围，如有必要更改，需获得用户的授权。

抑制效果的判定：

✧ 防止事件继续扩散，限制了潜在的损失和破坏，使目前损失最小化；

✧ 对其它相关业务的影响是否控制在最小范围内。

5) 根除阶段

对事件进行抑制之后，通过对有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

应急响应服务人员应协助服务对象检查所有受影响的系统，在准确判断安全事件原因的基础上，提出方案建议。

由于入侵者一般会安装后门或使用其他的方法以便于在将来有机会继续侵入该被攻陷的系统，因此在确定根除方法时，应急响应服务人员将了解攻击者是如何入侵的，以及与这种入侵方法相同和相似的各种方法。

应急响应服务人员将明确告知用户所采取的根除措施可能带来的风险，制定应变和回退措施，并得到用户的书面授权。

应急响应服务人员将协助服务对象进行根除方法的实施。

应急响应服务人员将使用可信的工具进行安全事件的根除处理，不使用受害系统已有的不可信的文件和工具。

根除效果的判定：

✧ 找出造成事件的原因，备份与造成事件的相关文件和数据；

✧ 对系统中的文件进行清理，根除；

✧ 使系统能够正常工作。

6) 恢复阶段

本阶段将恢复安全事件所涉及的系统还原到正常状态，使业务能够正常进行，恢复工作应避免出现误操作导致数据的丢失。

应急响应服务人员将告知用户一个或多个能从安全事件中恢复系统的方法，及他们可能存在的风险。

应急响应服务实施成员将和用户共同确定系统恢复方案，根据抑制和根除的情况，协助用户选择合适的系统恢复的方案。

应急响应服务人员将按照系统的初始化安全策略恢复系统。恢复系统时，根据系统中各个子系统的重要性，确定系统恢复的顺序。

7) 总结阶段

通过以上各个阶段的记录表格或报告，回顾安全事件处理的全过程，整理与事件相关的各种信息，进行总结，并尽可能的把所有信息记录到文档中。

应急服务小组将及时检查安全事件处理记录是否齐全，是否具备可追溯性，并对事件处理过程进行总结和分析。

进行完整的事件报告：

✧ 项目经理应向用户提供经审核过的网络安全事件处理报告；

✧ 项目经理和应急响应专家向用户提供网络安全方面的措施和建议；

✧ 项目经理和应急响应专家告知用户可能涉及违纪违规或法律诉讼方面的问题或意见。

安全事件上报和共享时，需根据安全状态分析和影响分析的结果，分析可能发生的安全事件，明确安全事件等级、影响程度以及优先级等，形成安全状态分析报告和网络安全事件报送表，按照安全事件等级以及安全事件报告程序

上报，需要共享的按照规定向特定对象共享安全事件。

应急响应时间为：

1）本服务应在浦东公交指定的时间内到达现场，如发生网络安全事件应急响应服务人员应在1小时内到达现场进行安全处置。

2）若网络安全事件发生在特殊时间段，如夜晚、重大节假日，则值班工程师30分钟内响应，应急响应服务工程师1小时内抵达现场参与应急处置。

6.4.3服务流程与过程文档

应急响应服务包括准备阶段、监测阶段、抑制阶段、根除阶段、恢复阶段和总结阶段，并且输出相应的过程文档。

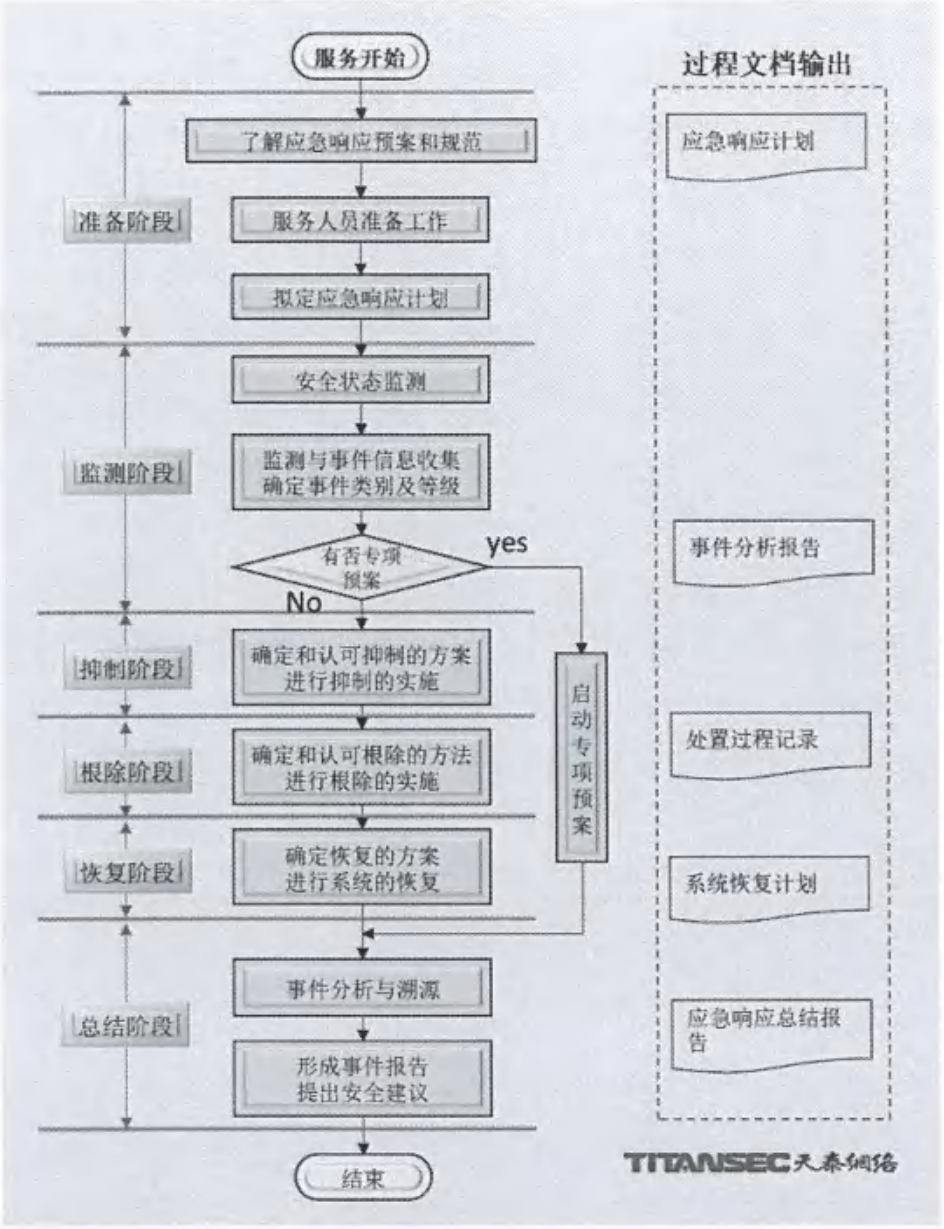


图 6-4-3 应急响应服务流程图

6.4.4 服务人员和服务工具

网络安全应急响应服务根据服务的不同阶段安排不同的服务人员参与，准备阶段由项目经理、应急响应服务人员和应急响应支撑人员共同制定服务计划和监测科目；应急响应过程中，及时调度安全专家、应急响应服务人员赶到现场参与事件分析和应急处置。安全事件处置和应急响应小组由资深的应急响应服务工程师带队，系统安全服务工程师参与；总结阶段由应急响应服务工程师起草总结报告，安全专家进行审核。

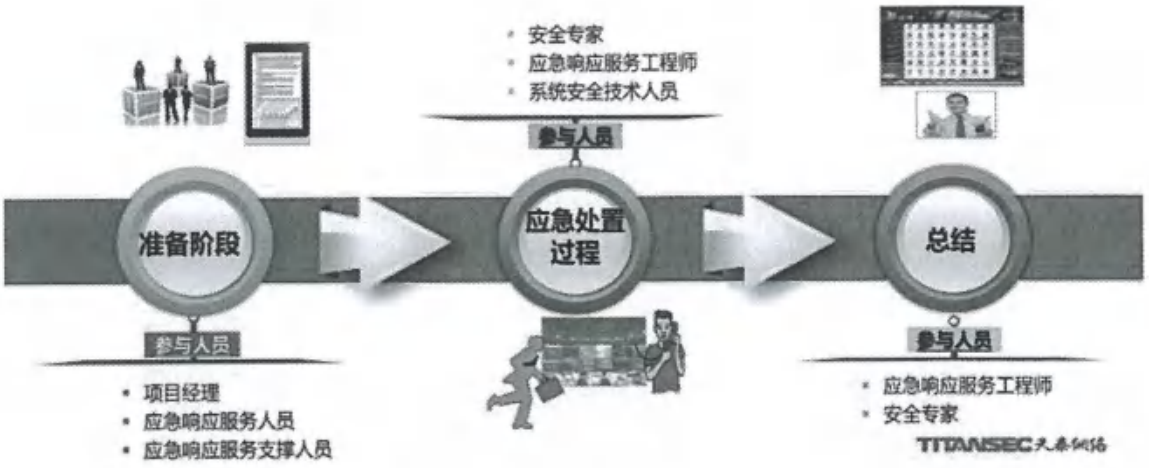


图 6-4-4 网络安全应用保障

6.4.5 服务范围

浦东公交公司突发的网络信息安全事件或上级主管单位检查时的工作协助，安排专业技术人员赶赴现场参与事件处置和技术支援。

6.4.6 服务周期和频次

应急应服务周期为一年，本服务为触发式，全年不限服务频次要求。

6.4.7 服务交付

服务完成后出具《网络安全应急保障服务报告》和《网络安全应急保障专项服务报告》。

6.5 网络安全培训

6.5.1 服务需求理解

根据需求开展网络安全专题培训，宣传最新的网络安全法律法规和政策要求，普及网络安全知识，提升浦东公交办公人员的安全防范意识。

根据需求为相关关键岗位人员提供安全技术培训，通过培训提升网络安全技能，达到网络信息安全相关要求，增强应对处置信息安全风险的能力。

随着国家各项法律法规的颁布，网络安全培训被纳入网络安全工作基本要求。

- 2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》第三十四条要求“定期对从业人员进行网络安全教育、技术培训和技能考核”。
- 2019 年 12 月 1 日起施行的《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）要求“应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；应定期对不同岗位的人员进行技能考核”。
- 2021 年 9 月 1 日实施的《中华人民共和国数据安全法》第二十七条要求“建立健全全流程数据安全管理制度，组织开展数据安全教育培训”。
- 2021 年 9 月 1 日实施的《关键信息基础设施安全保护条例》第十五条要求“组织网络安全教育、培训”。

一系列的法律法规明确了网络安全的培训要求，用户方将根据法律法规的要求，制定技术培训计划，明确培训目标，通过天泰网络开展培训活动，通过考核检验培训效果。

6.5.2 重要的法律法规

近年来全国人大、国务院、国家互联网信息办公室、中央网信办、公安部、工信部陆续发布了有关网络与信息安全的法律法规和管理办法，其中重要的法律法规如下：

表 6-5-2 网络安全法律法规名称与主要内容

名称	颁布单位	主要内容
《网络安全法》	全国人民代表大会常务委员会	为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的法律。主要包括总则，网络安全支持与促进、网络运营安全、网络信息安全、监测预警与应急处置、法律责任、附则等。《网络安全法》规范网络运行安全，特别强调要保障关键信息基础设施的运行安全。网络运行安全是网络安全的重心，关键信息基础设施安全则是重中之重，

		与国家安全和社会公共利益息息相关。强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据强制本地存储等法律措施，确保关键信息基础设施的运行安全。
《网络数据安全管理条例（征求意见稿）》	国家互联网信息办公室	征求意见稿规定，国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。 征求意见稿规定，数据处理者应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关规定从严保护。
《个人信息保护法》	全国人民代表大会常务委员会	规定了个人信息处理的基本原则、与政府信息公开条例的关系、对政府机关与其他个人信息处理者的不同规制方式及其效果、协调个人信息保护与促进信息自由流动的关系、个人信息保护法在特定行业的适用问题、关于敏感个人信息问题、法律的执行机构、行业自律机制、信息主体权利、跨境信息交流问题、刑事责任问题。旨在保护个人信息权益，规范个人信息处理活动，保障个人信息依法有序自由流动，促进个人信息合理利用。
《关键信息基础设施安全保护条例》	国务院	旨在建立专门保护制度，明确各方责任，提出保障促进措施，保障关键信息基础设施安全及维护网络安

		全。
《网络产品安全漏洞管理规定》	工信部、国家网信办、公安部	规定要求任何组织或者个人不得利用网络产品安全漏洞从事危害网络安全的活动，同时，网络产品提供者、网络运营者和网络产品安全漏洞收集平台应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，留存网络产品安全漏洞信息接收日志不少于6个月
《数据安全法》	全国人民代表大会常务委员会	规定了数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放等，旨在保障数据安全，促进数据开发利用
《网络安全审查办法》	国家互联网信息办公室等	规定了关键信息基础设施运营者采购网络产品和服务，应当进行网络安全的审查，旨在确保关键信息基础设施供应链安全，维护国家安全
《网络信息内容生态治理规定》	国家互联网信息办公室	规定了网络信息内容生产者、网络信息内容服务平台、网络信息内容服务使用者、网络行业组织等，旨在营造良好网络生态
《密码法》	全国人民代表大会常务委员会	规定了核心密码、普通密码、商用密码等，旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全
《刑法》（部分）	全国人民代表大会常务委员会	第253、285、286、287、288条违法获取或出售公民个人信息、违法侵入国家事务、国防建设、尖端科技领域信息系统、入侵破坏计算机系统、违法使用无线电台的
《国民经济和社会发展第十四个五年规划和2035年远景目标纲要》	十三届全国人大四次会议	培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业，提升通信设备、核心电子元器件、关键软件等产业水平。健全国家网络安全法律法规和制度标准，加强重要领域数据资源、重要网络和信息系统安全保障。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全风险评估和审查。加强网络安全基础设施建设，

		强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力。加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力。加强网络安全宣传教育和人才培养
《涉密信息系统集成资质管理办法》	国家保密局	涉密集成资质分为甲级和乙级两个等级，甲级资质单位可以从事绝密级、机密级和秘密级涉密集成业务；乙级资质单位可以从事机密级、秘密级涉密集成业务。明确了涉密集成资质的申请、受理、审查、决定、使用和监督管理规定。

6.5.3 服务范围

面向全体工作人员开展网络安全意识培训；

面向浦东公交和直属企业的信息化人员、运维服务人员、安全管理人员、系统管理人员、其他相关人员开展安全技术培训。

6.5.4 培训服务的计划与方法

协助用户开展面向全体工作人员的网络安全意识培训，普及网络安全知识，面向运维服务人员、安全管理人员、系统管理人员、其他相关人员开展安全服务技术培训。

培训主题为：

- ◆ 网络安全意识培训；
- ◆ 网络安全技能培训。

（1）培训服务的具体要求

具体要求包括：

- ✧ 面向全体工作人员开展网络安全意识培训，宣传网络安全法律法规和政策要求，普及网络安全常识，提升浦东公交办公人员的安全防

范意识；

- ✧ 针对与网络安全相关的工作人员和服务人员，开展网络安全设备使用维护的培训，以确保所有工作人员了解网络安全产品的原理和运维管理方法，了解日常安全运维流程与警告、安全事件处置方法，更好地履行网络安全责任和安全工作规范；
- ✧ 用户项目管理部门确定培训的时间、参加培训的人员和培训教师。每次培训前，应提前至少一周发出培训通知；
- ✧ 提供培训的老师可以是服务单位资深的技术或管理人员，或者是外聘的专家和教授，也可邀请安全厂商或服务商的专业人员授课，培训教师应提前准备教材和培训参考资料；
- ✧ 用户项目管理部门了解培训教师的专业性和授课经验，对不合适的培训教师进行调整，并提前审核培训教材和授课内容；
- ✧ 应准备培训记录签到表，培训时所有培训人员应签到；
- ✧ 培训之后，应针对培训内容对培训人员做必要的考核，以检验培训的效果。

（2）安全意识的培训

安全意识的培训内容：

- ✧ 介绍习总书记有关网络安全的讲话；
- ✧ 介绍网络安全法规及违法案例；
- ✧ 介绍数据安全的要求；
- ✧ 钓鱼邮件的防范与应对措施；
- ✧ 网络办公安全的要求。

（3）网络安全技能培训

- ✧ 介绍下一代防火墙、WAF、堡垒机等网关型产品；
- ✧ 介绍日志审计、防病毒软件、防篡改软件等产品；
- ✧ 安全产品的日常管理，包括配置管理、变更、升级、优化和补丁等日常管理。

安全技能培训将根据使用与维护经验，对运维管理、安全管理的人员进行培训。

（4）培训方法

培训方法以老师讲解、答疑、系统演示的方式进行。

6.5.5服务流程

网络安全培训服务包括培训准备阶段、安全培训阶段、总结报告阶段，并且输出相应的过程文档。

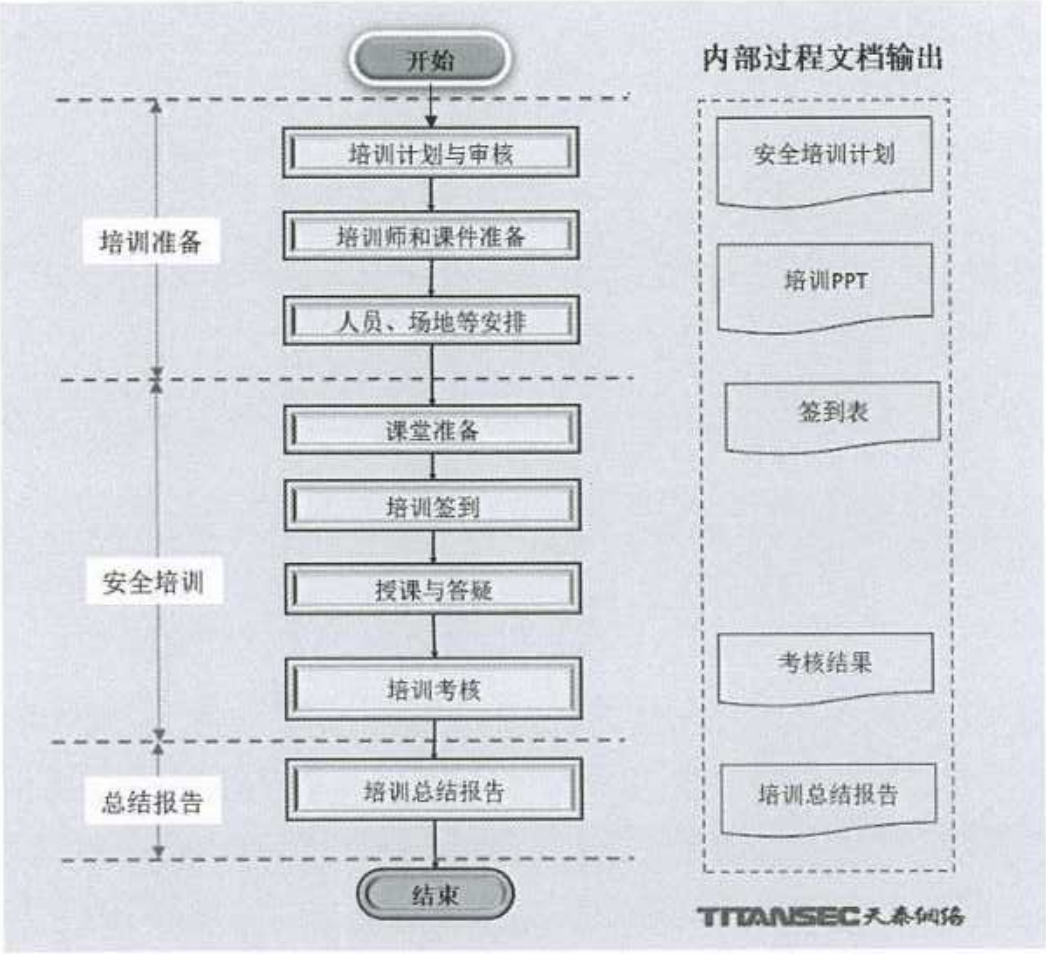
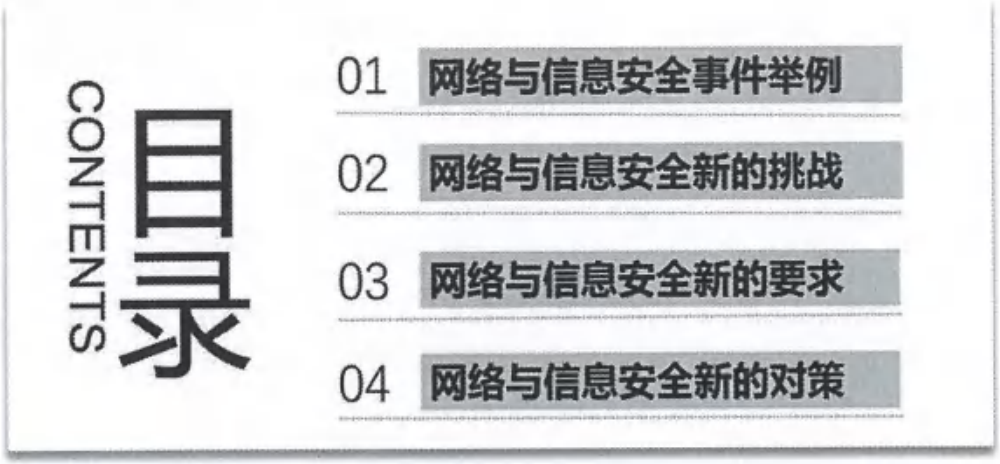
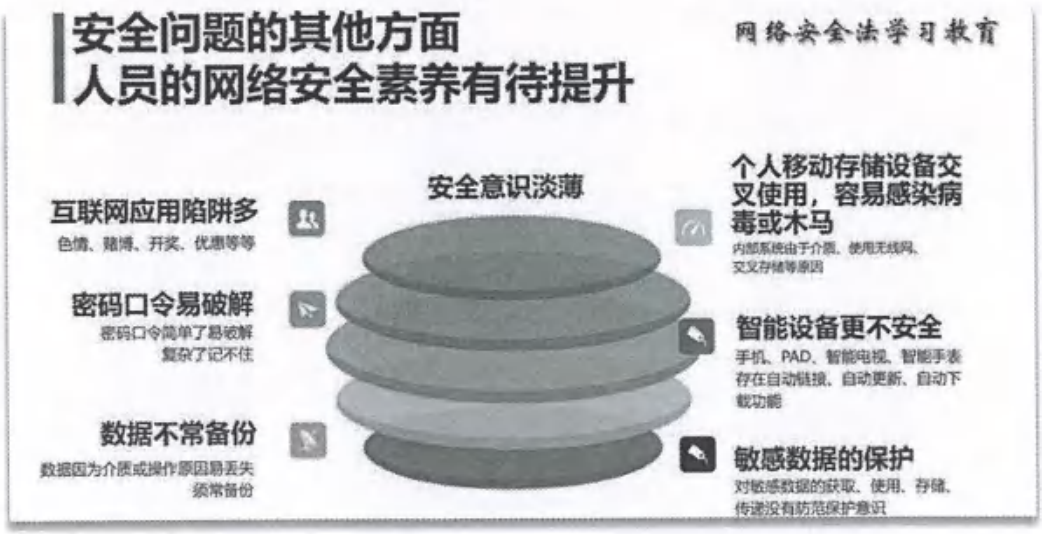


图 6-5-5 网络安全培训服务流程

6.5.6 安全意识教育培训样例





6.5.7 服务人员和服务工具

网络安全培训服务准备阶段由项目经理、培训讲师和服务支持人员共同制定培训计划；培训过程中，由培训讲师讲课；总结阶段由培训讲师撰写总结报告。

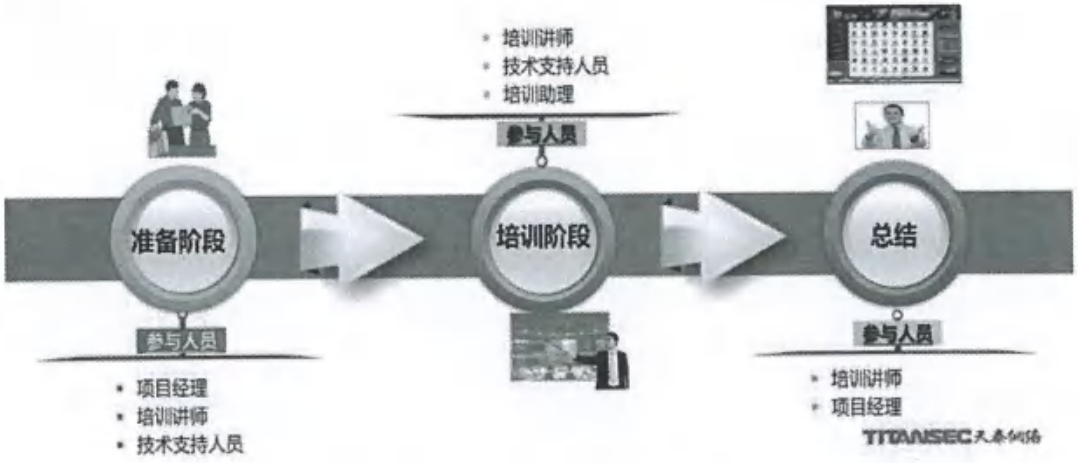


图 6-5-7 安全培训人员

安全培训工具主要使用办公软件 PowerPoint、Visio、Word 等。

6.5.8 服务频次

网络安全培训服务为现场服务，本项目将针对浦东公交本部和直属企业各开展一次。

网络安全培训工作将安排在第三季度的第一个月和第四季度的第一个月，

共需约5周。

6.5.9服务成果交付

培训结束后，交付《网络安全培训总结报告》，包含网络安全培训签到表、网络安全培训考核记录、网络安全培训PPT摘要。

6.6 网络安全应急演练

6.6.1服务需求理解

协助浦东公交组织开展一次网络安全应急演练，模拟突发事件处理过程，验证网络安全应急预案的有效性和可操作性，提升网络安全应急处置能力和效率。

网络安全事故隐患往往“生成”于无形。例如，漏洞或黑客攻击发生之时，被攻击单位可能处于非常危险的境地而无所察觉，不论是内部员工的疏忽还是管理上的大意，都可能给身在“暗处”的网络犯罪分子以可乘之机。

网络安全应急响应和一般意义的突发公共事件应急响应一样，也需要对制定的应急预案“勤加演练”，以巩固能力、检验成果、锻炼队伍。网络攻击等紧急事件的发生，往往会扰乱正常的网络秩序，影响网络信息系统的正常运行，使网络安全受到威胁，造成如网络瘫痪、数据被窃取或丢失等后果，甚至更严重的损失。

因此，在应急预案制定以后，有组织有规划地模拟演练具有至关重要的作用。只有经过网络安全应急预案的扎实培训与演练，才能在遇到网络突发事件时，及时有效地对事件做出响应，切实履行应急响应预案内容，准确给出应急处理方法，将危害降到最低。

协助用户开展面向全公司网络信息系统的年度应急演练，结合网络信息系统的实际情况、贴近实际工作需要，包括演练方案、场景设置、环境准备、演练执行、过程控制和风险管理、演练评价、总结报告和演练宣教视频，通过应急演练，切实达到熟练流程、增强业务人员网络安全意识及提升应急保障能力。

6.6.2应急演练的目标

突发公共事件发生后，需要开展事件应急。在发生网络安全事件时，也需要相关人员加以应对，这就需要提前制定网络安全事件应急预案，并对制定的应急预案加以演练，以巩固应急能力、验证应急效果、锻炼应急队伍、弥补应急不足。

网络攻击等紧急事件的发生，往往会扰乱正常的网络秩序，影响网络办公系统的正常运行，使网络安全受到威胁，造成如网络瘫痪、数据被窃取或丢失等后果，甚至更严重的损失。因此，有组织有规划地开展模拟演练具有至关重要的作用，只有经过网络安全应急预案的扎实培训与演练，检验应急响应小组中每个成员对工作完成的熟练程度和相互配合能力，积累实战练习经验，对应急响应预案内容不断地充实和完善，才能在遇到网络突发事件时，及时有效地对事件做出响应，切实履行应急响应预案内容，准确给出应急处理方法，将危害降到最低。

(1) 应急演练场景的选择

本次演练服务将由浦东公交公司网络安全管理部门牵头，收集 DDOS 攻击、数据泄露、钓鱼邮件、网络攻击、勒索病毒、网络舆情、网页篡改等类型，涉及生产调度、综合管理 2 大场景。结合实际案例与应急管理需求，以钓鱼邮件、网页篡改等为突破口，实战攻防为辅助场景，根据相关法律法规和《信息安全技术信息安全事件分类分级指南》，可将演练可定级为网络安全事件 III 级。

(2) 应急演练的目标

1) 检验应急预案：通过开展应急演练，梳理应急预案处置过程中存在的问题，进而完善应急预案的实用性和操作性。
2) 宣传教育：通过开展应急演练，普及网络安全和应急知识，不断增加网络安全管理的专业化程度，提高全员网络安全风险防范意识。
3) 检验协同机制：通过开展应急演练，进一步明确相关单位和人员的职责任务，理顺工作关系，提高应急处置效率。
4) 煅练队伍：通过开展应急演练，增强演练组织单位、参与单位、观摩单位和人员等对应急预案的熟悉程序，加强配合，提高其应急处置能力。
5) 完善准备：通过开展应急演练，检查应对网络安全事件所需应急队伍、

物资、装备、技术等方面的准备情况，发现不足时予以调整补充，做好应急信息发布工作。

(3) 演练类型

本次应急演练采用“实战演练模拟”模式，在保障演练目标信息系统业务安全提前下，模拟黑客入侵、敏感数据泄露突发事件场景，完成预警、决策、处置等应急响应过程。

6.6.3 服务范围

面向浦东公交公司网络信息系统的应急保障系统和应急预案；用户方参与人员包括从事网络安全领导工作的负责人、网络安全管理人员、应急保障人员、安全运维服务人员和系统管理的人员。

6.6.4 应急演练服务的计划与方法

天泰网络项目经理与用户网络安全管理部门协商演练类型、演练主题和时间地点。

(1) 演练准备工作阶段

为保证攻防演练工作顺利进行，需要成立演练领导小组和工作小组。

1) 指挥部

演练指挥组(指挥部)由组织单位相关部门领导和技术专家共同组成，负责演练工作的总体指挥和点评。

2) 综合协调组

综合协调组负责网络与信息安全事件应急处置过程中的资源协调、信息传达等工作。负责协调网络与信息安全事件的恢复与重建等工作。负责通告应急演练中各小组信息汇总。

3) 技术处置组

技术处置组：负责组织技术力量，收集现场数据，分析事件原因和影响范围，制定具体处置方案，实施具体应急处置，上报处置信息。

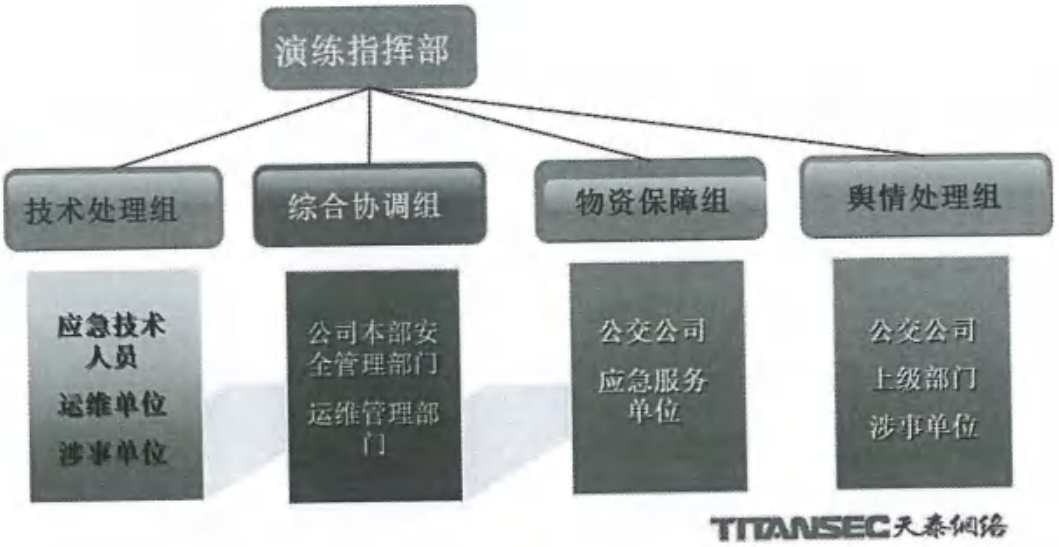


图 6-6-4-1 应急演练的相关组织架构

4) 物资保障组

物资保障组：负责提供网络与信息安全事件应急处置所需求场地、人员、设备等相关物资。

5) 舆情处置组

舆情处置组：负责收集和调控内外部舆论情况，负责向行业单位和社会公众宣传相关网络与信息安全事件预防和处置的基本知识，负责事件处置信息的对外宣传与发布等。

(2) 演练环境搭建及剧本撰写阶段

根据演练方案，对演练目标信息系统或环境，进行备份或创建拟真环境，保障达到演练目的和效果，保障目标信息系统安全稳定的运行。

准备演练过程中攻击方所使用的工具和防守方的防守系统环境。

准备演练方案到剧本的撰写工作。

(3) 演练道具准备阶段

要保证实战攻防演练顺利、高效开展，必须提前做好两项准备工作：一是资源准备，涉及演练场地、演练平台、演练人员专用电脑、视频监控，宣传手册等；二是人员准备，包括攻击队、防守队的人员选拔与审核，队伍组建等。

1) 资源准备

a) 演练场地布置：演练展示大屏、办公桌椅、攻击队网络搭建、演练会场布置等。

b) 演练人员专用电脑：为演练人员配备专用电脑，安装安全监控软件、防病毒软件、录屏软件等，做好事件回溯机制。

c) 视频监控部署：部署攻防演练场地办公环境监控，做好物理环境监控保障。

d) 宣导设计：设计邀请函、KV、宣传手册、导引牌、易拉宝等，做好展示和宣传工作。

e) 演练授权：演练组织方向攻击队和平台提供方进行正式授权，确保演练工作在授权范围内有序进行。

2) 人员准备

- 红队：组建攻击队，确定攻击队数量(2-5 人)，对人员进行技术能力考核，确定组织架构，宣贯攻击规则和演练相关要求。
- 蓝队：组建防守队，确定防守队数量(3-7 人)，对人员进行技术能力考核，确定组织架构，宣贯防守规则和演练相关要求。

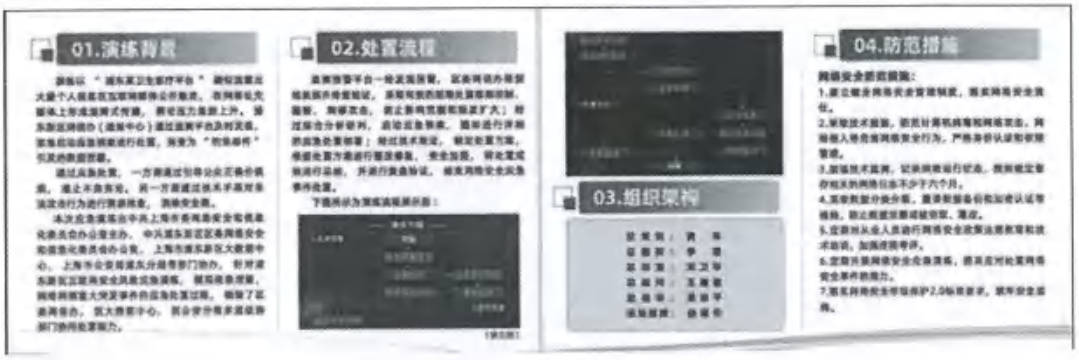


图 6-6-4-2 应急演练的宣传

(4) 演练彩排工作阶段

要保证实战攻防演练顺利、高效开展，必须提前多次进行演练彩排工作。在演练彩排中排练攻防演练流程，对彩排中出现的问题及时处理，排除演练中存在的风险。检查演练中的各项筹备工作重要节点,熟悉整个演练流程,了解场地情况,确保演练过程顺利流畅。

(5) 正式演练阶段

演练组织方组织相关单位召开启动大会，部署实战攻防演练工作，明确演练时间，宣布正式开始演练。

演练过程如下（具体内容略）：

- 舆情预警
- 定位协查
- 初判汇报
- 研判定级、启动
- 任务部署
- 应急处置
- 现场攻防
- 汇报结果
- 验证成效
- 演练复盘

(6) 演练风险和应对

表 6-6-4-1 应急演练风险和应急措施

序号	风险描述	应对措施	备注
1	网站扫描影响服务器性能，如：CPU、内存等产生损耗。	1、实时关注； 2、超出一定阈值及时停止扫描； 3、立即停止演练	随时关注门户网站的可用性
2	扫描 IP 被突然封禁或阻断（如，运营商、FW/IPS/WAF 等主动防护设备）	预留多个扫描 IP 地址；	临时开通部分封禁的协议或端口
2	监管机构对网页篡改进行告警及通报	1、提前向网安/网信报备演练事宜 2、避免被通报的风险	
3	爆破过程中，IP 被封禁或阻断	1、预留多个扫描 IP 地址； 2、FW/IPS/WAF 预先添加白名单	
4	演练过程中，被演练以外的黑客发现开放的端口及弱口令漏洞	1、FW/IPS/WAF 预先添加白名单，只允许白名单 IP 访问和扫描 2、演练中的弱口令漏洞（也可以设置一个强口令），提前告知演练人员，避免真实弱口令被恶	

		意黑客探知	
5	数据库备份数据无法恢复	1、使用数据库测试环境演练 2、预演练验证数据可用性 3、寻找备份数据副本作为备选数据	重要和敏感数据提前做好备份
6	不可预知原因，远程无法修改页面	本地运维人员，将模拟篡改页面替换，并恢复	

(7) 演练结束收尾阶段

演练结束后须做好相关保障工作，如清除后门、恢复临时开放的协议与端口、收回账号及权限、回收设备、回收网络访问权限、清理演练数据等，确保后续业务正常运行。要求如下：

1）依据攻击队报告和监控到的攻击流量，将攻击方上传的后门进行清除；

2）收回账号及权限：演练结束后，收回攻击队所有账号及权限，包括攻击队在目标系统上新建的账号；

3）回收设备：对攻击队电脑（或虚拟终端）进行格式化处理，清除过程数据；

4）收回网络访问权限：收回攻击队的网络访问权限；

5）清理演练数据：对平台的演练数据进行清理。

(8) 演练总结

演练总结主要包括参演单位编写总结报告，领导专家点评总结演练成果，演练全体单位召开总结会议，开展编排演练视频与开展宣传工作。对整个演练进行全面总结，对发现的问题积极整改，开展后期宣传工作，体现演练的实用性。

具体的演练总结内容如下：

1）参演单位进行总结汇报，组织方对演练进行总体评价，攻击队与防守队进行经验分享，对问题提出改进建议和整改计划。

2）视频编排与宣传：制作实战攻防演练视频，方便播放与宣传，提高人员

安全意识。

3）整改建议：实战攻防演练工作完成后，演练组织方组织专业技术人员和专家，汇总、分析所有攻击数据，进行充分、全面的复盘分析，总结经验教训，并对不足之处给出合理整改建议，后续单位内部应不断优化防护工作模式，循序渐进地完善安全防护措施，优化安全策略，强化人员队伍技术能力，整体提升网络安全防护水平。

6.6.5服务流程

应急演练服务包括准备阶段、演练阶段、总结阶段，并且输出相应的过程文档。

通过演练彩排发现存在的问题或不足，对演练方案进行修订，直到领导（小组）对演练彩排满意为止，其后可安排正式演练。

正式演练可邀请体系内的相关机构或单位参与观摩，可以邀请行业或监管单位的领导作为专家观演指导。

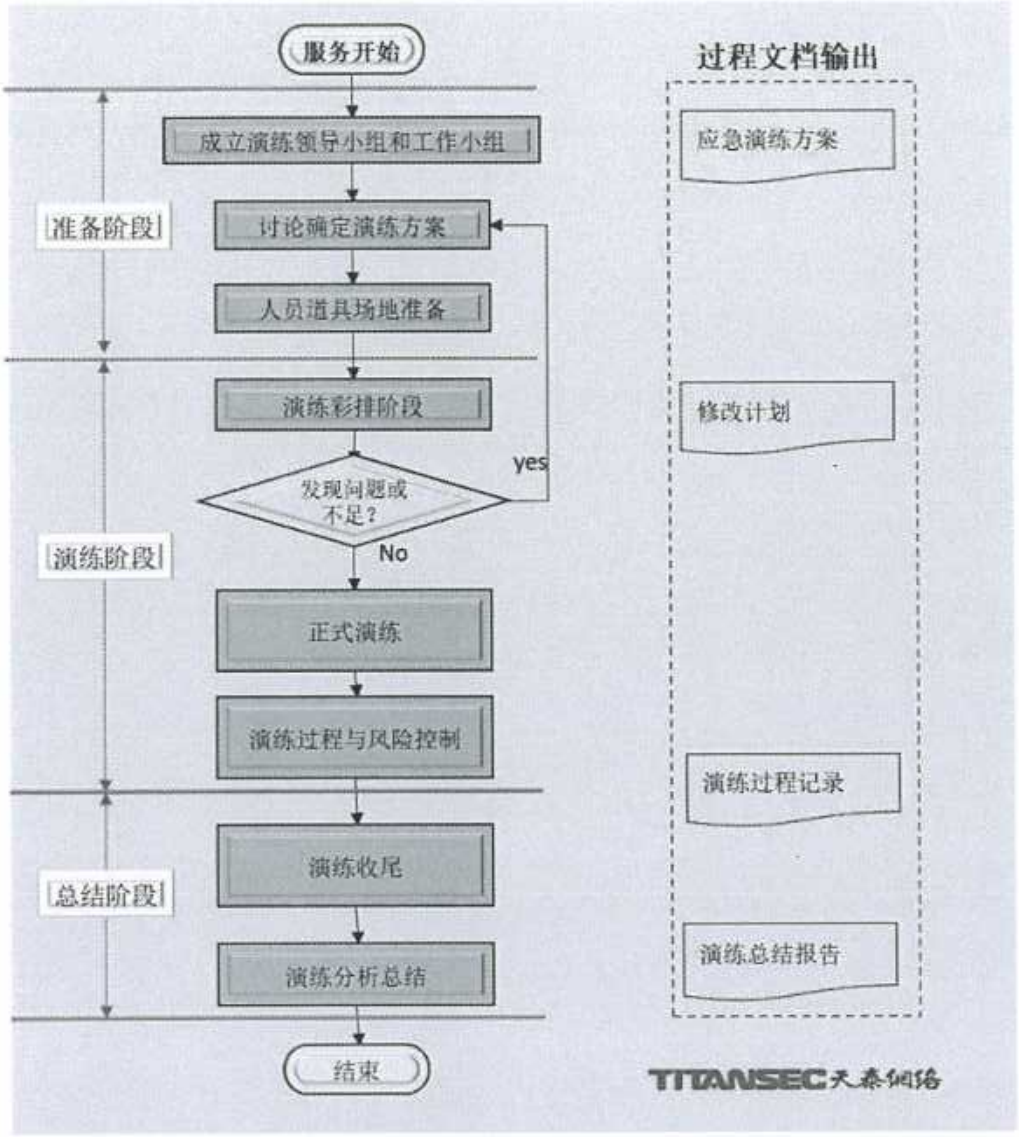


图 6-6-5 应急演练的流程与过程文档

6.6.6 服务人员和服务工具

应急演练服务准备阶段由项目经理、安全专家和技术、协调、保障等人员共同制定演练计划；演练过程包括彩排和正式演练，由主持人、攻防双方、观摩人员、领导专家等组成；总结阶段由项目经理撰写总结报告。

图 6-6-5 网络安全应急演练服务人员

天泰网络将使用漏洞扫描工具、渗透测试工具、弱口令检测工具、病毒查杀类工具及各种攻防小程序开展安全应急演练服务。

应急演练现场主要使用办公软件 PowerPoint、Visio、Word 等，同时需要大屏 2 个，音响一组，无线微型麦克风三个，计算机与网络设备若干。

6.6.7 应急演练的注意事项

应急演练时首先要制定一个适应性计划，在证明应急响应预案有效性的同时，保证网络的安全，避免由于一次演练的失误而造成真正的网络攻击，使重要数据泄露或信息资产遭受损失。

1）应急演练环境

应急演练的环境包括进行应急演练所需的文档、人员和设备。完整的环境不仅保证了演练可以完整实施，也提升了该演练的效果。应急演练的环境应该尽可能与真实场景相同，人员参与尽可能全面，对应急演练事件的记录尽量详细。

通过已有的一些网络安全事件和网络安全应急处置经验，设计与预案相匹配的应急演练环境。

2）应急演练文档

应急演练文档是为了规范和记录应急演练事件，应急演练文档包括应急演练方案、应急通信录以及应急演练记录表。

■ 应急演练方案

应急演练方案是对每次应急演练的部署和指导，该方案应为每个参与应急演练的人员所熟知。应急演练方案应包括以下内容：

（1）应急演练的背景、目的和假设。这一部分应对应急演练进行基本介绍，让全体参与者对演练有初步的了解。

（2）应急演练流程。该部分通过流程图的方式，明确整个事件流程、需要完成的任务、可能出现的情况等。流程图可以对应急演练进行简明扼要的归纳。

（3）网络架构图、应急恢复策略及应急故障处理。这一部分为技术人员提供指引，包括熟知网络拓扑结构以及故障发生时应进行的行动。

（4）事故上报模板、任务分配表以及岗位职责。这一部分明确了应急演练中部门的职责和个人的任务，通过提供模板提高上报速度。

■ 应急通信录

应急通信录保证了当发生事件时，每个涉事人员、部门和领导可以被联络到。应急通信录包括全员通信录、关键电话线、设备供应商通信录和安全厂商通信录。在进行应急演练中，通过全员通信录，可以快速定位到个人；通过关键电话线，可以找到负责某一项工作的部门；如发生意外，通过设备供应商通信录和安全厂商通信录，可以找到设备供应商和有资质的安全厂商，以避免造成不必要的损失。

■ 应急演练记录表

应急演练记录表是指对应急演练过程产生的相关数据进行记录，以备后期查询、分析和总结。应急演练记录表包括响应时间表、损失评估表等，对响应的速度、应急演练每一阶段造成的损失进行记录。这些应急演练记录表是对本次应急演练评估分析的重要依据，因此非常重要。

3）应急演练人员安排

应急演练的参与者可以分为 3 个层次：把握全局的领导层、具体执行演练的实施层以及为演练提供支持的后勤层。

■ 领导层

领导层（如应急指挥长）对应急演练的全局进行把握，确定时间节点、具体方案、应急演练实施的效果以及突发情况下的组织。同时对人员进行调度，对资源进行配置。

■ 实施层

实施层负责具体执行应急演练的任务，包括执行应急演练和后期运维 2 个方面。应急演练执行小组对网络行为、数据行为进行分析，对痕迹进行取证，对涉及的样本进行逆向分析，并且整理应急演练的报告。后期运维小组对应急演练中的行为监控，避免出现越权或破坏行为，应急演练前对设备进行管理，应急演练后对造成的影响进行恢复。

■ 后勤层

后勤层人员对安全事件的影响进行评估。后勤层在出现问题时进行上下级和部门间的沟通，并与外界的厂商、安全机构联络，确保应急演练的实施全程沟通畅通。当出现意外情况时，可以快速寻求帮助，为全员提供支持。

6.6.8 服务频次

网络安全应急演练服务为现场服务，服务周期内开展一次。

对浦东公交公司的应急演练工作将安排在第四季度的第二个月进行，也可根据公交公司的年度网络安全工作计划进行安排。

6.6.9 服务成果交付

演练结束后，交付《网络安全应急演练总结报告》。

6.7 网络风险技术性探测

6.7.1 技术性探测

6.7.1.1 服务需求理解

随着数字化技术的快速发展，企业接入网络的应用与终端数量快速增长，这也意味着企业的风险暴露面随之扩大，并更趋复杂化。同时，网络攻击技术也在持续演进，黑客利用漏洞进行攻击的能力越来越强。因此，互联网风险技术性探测就成为保障企业网络安全的重要手段。

浦东公交的业务系统等信息资产位于互联网上，直接或间接暴露给外部攻击者，这部分包括但不限于互联网上的 IP 资产、域名资产、敏感信息、业务系

统的代码等。这些部分的安全性直接关系到浦东公交整体网络安全，一旦存在漏洞或不当配置，就可能面临外部攻击的风险。

为了更好的应对这种情况的发生，防范可能的外部网络攻击，浦东公交可开展网络风险技术性探测，先于攻击者对自身暴漏在互联网上的已知和未知资产进行全面排摸、深入安全检测，找到潜在的薄弱点，及时进行修补，提升浦东公交的整体网络安全。

包括单位暴露在互联网的已知、未知资产，包括单位的所有互联网 IP 地址，与相关关键词有关的互联网文档信息，业务系统等。

6.7.1.2 网络风险技术性探测的目的

网络风险技术性探测服务的目标是，在互联网上通过技术手段发现浦东公交信息系统、本地网络、服务器等资产的未知的安全风险，进而为网络安全防范措施的制定提供方向，包括：

- ✧ 识别暴露在网上的资产和风险。
- ✧ 评估安全防护水平，量化安全风险。
- ✧ 为收敛资产暴露面提供科学决策依据。

通过开展网络风险技术性探测，可以探测到：

- ✧ 网上未纳入安全管理的信息资产
- ✧ 开放在网上的高危端口
- ✧ 已知的漏洞
- ✧ 不安全的配置
- ✧ 弱密码和默认密码

6.7.1.3 服务范围

浦东公交在互联网上的信息资产，包括云上应用系统、服务器、办公网络接入口等。

6.7.1.4 技术性探测方法

探测方法：

1) 被动检测

通过扫描网络服务、应用程序和系统配置等方式，识别出潜在的漏洞和风险。

2) 主动检测

模拟攻击行为，通过安全测试等方式发现网络系统、应用程序和操作系统的漏洞和安全问题。

6.7.1.5 服务频次

技术性探测服务采用远程服务方式，服务周期内开展一次技术性探测。计划在第一季度的第三个月开展网络安全风险技术性探测，大约需要3周时间。

6.7.1.6 服务成果交付

技术性探测完成后，交付《网络风险探测报告》。

6.7.2渗透测试

6.7.2.1 服务需求理解

对本项目中浦东公交指定的业务系统进行 1 次渗透测试。渗透测试是通过模拟恶意黑客的攻击方法，包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。非破坏渗透测试可以对系统的网络层安全、系统层安全、应用层安全中多项安全指标进行测试和漏洞发现，基于渗透测试报告，可以精准开展安全加固和安全整改工作。

6.7.2.2 渗透测试目的

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。渗透性测试工作是信息系统上线前安全评测工作的重要环节，同时也为风险评估提供重要的参考数据。

渗透测试不同于其他三个评测层面，不是在已知系统上，对已知弱点进行排查，而是测试者模拟黑客，在未知系统中发现弱点，而且还要验证弱点，甚

至还会挖掘出一些未知的弱点。渗透测试是其他三项评测内容的一种最好的补充。

另外，渗透测试的攻击路径及手段不同于常见的安全产品，所以它往往能暴露出一条甚至多条被人们所忽视的威胁路径，从而暴露整个信息系统的威胁所在。最重要的是，渗透测试最终的成功一般不是因为某一个信息系统的某项单一问题所直接引起的，而是由一系列看似没有关联而且又不严重的缺陷组合而导致的。在日常工作中，无论对信息系统进行怎样的传统安全检查工作，对于没有相关经验和技能的人员都无法将这些缺陷进行如此的排列组合从而引发安全漏洞，但安全专家却可以靠其丰富的经验和技能将它们进行串联并展示出来。所以，渗透性测试的结果对信息系统是否符合上线运行条件，可以提供决策支持。

6.7.2.3 服务范围

浦东公交指定的应用系统。

6.7.2.4 渗透测试预期目标

渗透测试是指在取得客户授权的情况下，通过模拟黑客攻击来对客户的整个信息系统进行全面的漏洞查找，分析、利用。最后给出完整的渗透报告和问题解决方案。

渗透测试作为网络安全服务体系中的一种技术，是在实际网络环境下由高素质的渗透人员发起的，经过用户授权的高级安全检测行为。渗透测试过程借鉴了黑客攻击的手法和技巧，可以高度精确的反映用户系统面临的风险。通过渗透测试，可以充分暴露和发掘潜在的漏洞，能直观的让业务系统的管理人员知道自己维护的系统中存在的安全缺陷，从而更好的规避掉这些风险，保障业务系统安全平稳的运行。

本项渗透测试服务将在服务周期内开展 1 轮，通过互联网应用渗透测试，需达到以下目标：

- 了解入侵者可能利用的途径；
- 从黑客攻击的角度发现系统中对外暴露的安全问题；
- 提高信息安全相关人员对漏洞发现和修复的能力；

➢ 对原有安全系统的有效性进行确认，了解系统中的安全短板。

采用技术工具和人工分析结合的方法，发现系统可能存在的 SQL 注入、跨站脚本、弱口令、溢出、文件上传、认证会话管理类、未授权访问类等漏洞，并提出整改建议及协助整改，包含整改后的回归测试，并出具相关报告。

6.7.2.5 渗透测试流程

渗透测试服务通过远程利用目标应用系统等安全弱点，模拟真正的黑客入侵攻击方法，以人工渗透为主，以漏洞扫描工具为辅，在保证整个渗透测试过程都在可以控制和调整的范围之内尽可能的获取目标信息系统的管理权限以及敏感信息。

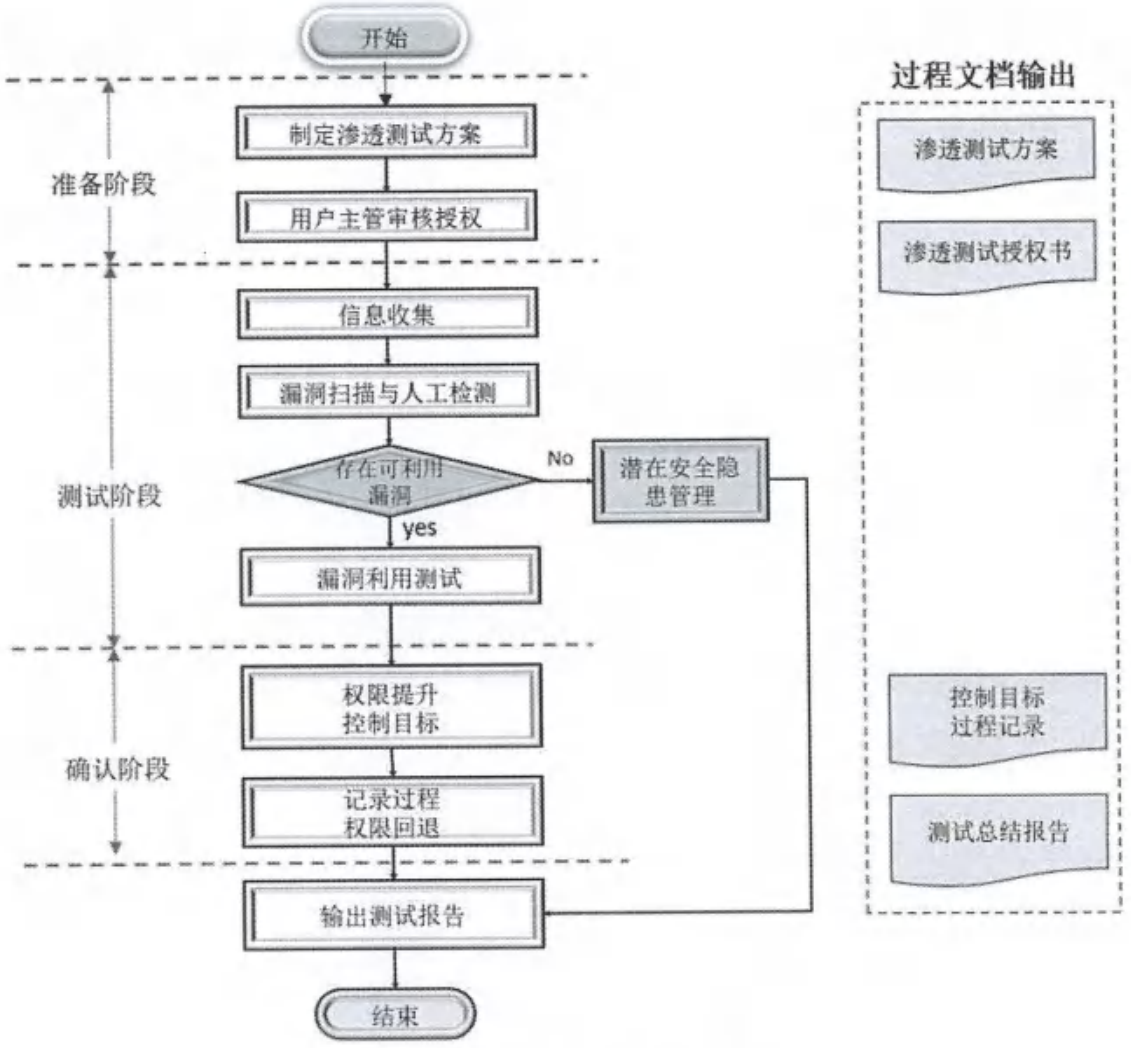


图 6-7-2-5 渗透测试流程图

渗透测试的相关过程：

（1） 信息收集

信息收集是指渗透实施前尽可能多地获取目标信息系统相关信息，例如网站注册信息、共享资源、系统版本信息、已知漏洞及弱口令等。通过对以上信息的收集，发现可利用的安全漏洞，为进一步对目标信息系统进行渗透入侵提供基础。

（2） 漏洞分析及功能分析

对收集到的目标信息系统可能存在的可利用安全漏洞或弱点进行分析，并确定渗透方式和步骤实施渗透测试。

（3） 获取权限

对目标信息系统渗透成功，获取目标信息系统普通权限。

（4） 权限提升

当获取目标信息系统普通管理权限后，利用已知提权类漏洞或特殊渗透方式进行本地提权，获取目标系统远程控制权限

6.7.2.6 渗透测试工具

渗透测试人员模拟黑客入侵攻击的过程中使用的是操作系统自带网络应用、管理和诊断工具、黑客可以在网络上免费下载的扫描器、远程入侵代码和本地提升权限代码以及自主开发的安全测试工具。

这些工具经过全球数以万计的程序员、网络管理员、安全专家以及黑客的测试和实际应用，在技术上已经非常成熟，实现了网络检查和安全测试的高度可控性，能够根据使用者的实际要求进行有针对性的测试。但是安全工具本身也是一把双刃剑，为了做到万无一失，我们也将针对系统可能出现的不稳定现象提出相应对策，以确保服务器和网络设备在进行渗透测试的过程中保持在可信状态。

（1）系统自带工具

以下列出了主要应用到的系统自带网络应用、管理和诊断工具，渗透测试工程师将用到但不限于只使用以下系统命令进行渗透测试。

系统自带的测试工具

工具名称	风险等级	获取途径	主要用途	存在风险描述	风险控制方法
ping	无	系统自带	获取软件部署的信息	无	无
telnet	无	系统自带	登录系统	无	无
ftp	无	系统自带	传输文件	无	无
tracert	无	系统自带	获取网络信息	无	无
net use	无	系统自带	建立连接	无	无
net user	无	系统自带	查看系统用户	无	无
echo	无	系统自带	文件输出	无	无
nslookup	无	系统自带	获取软件部署的主机信息	无	无
IE	无	系统自带	获得 web 信息、进行 SQL 注入	无	无

（2）自有软件和渗透测试工具

以下列出了渗透测试中常用到的网络扫描工具、网络管理软件等工具，这些工具都是网络上的免费软件。渗透测试工程师将可能利用但不限于利用以下工具。远程溢出代码和本地溢出代码需要根据具体系统的版本和漏洞情况来选择，由于种类繁杂并且没有代表性，在这里不会一一列出。

自有软件和渗透工具

工具名称	风险等级	主要用途	存在风险描述	风险控制方法

nc	无	对软件部署的主机扫描端口连接工具	无	无
远程溢出工具	中	通过对软件部署的主机漏洞远程进入系统	溢出程序可能造成服务不稳定	备份数据，服务异常时重启服务。
本地溢出工具	中	通过对软件部署的主机漏洞本地提升权限	溢出程序可能造成服务不稳定	备份数据，服务异常时重启服务。
Arachni	低	高性能安全 Web 扫描程序	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。
XssPy	低	XSS（跨站脚本）漏洞扫描器	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。
w3af	低	Web应用程序进行审计	无	无
Nikto	低	扫描 Web 服务器配置错误、插件和 Web 漏洞	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。
Wfuzz	无	对字段的 HTTP 请求中的数据进行模糊处理，对 Web 应用程序进行审查	无	无
OWASP ZAP	低	在浏览器和 Web 应用程序之间拦截和检查消息	无	无

Wapiti	低	扫描特定的目标网页，寻找能够注入数据的脚本和表单	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。
Vega	低	查找 XSS，SQLi、RFI 和其它的漏洞	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。
SQLmap	低	对后台数据库进行渗透测试和漏洞查找	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。
Grabber	无	管理和运行渗透工具分析器的流行安全工具框架	无	无
OWASP Xenotix XSS	低	用于查找和利用 Web 跨站点脚本的高级框架	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。
Burpsuite	低	用于渗透 Web 应用程序的集成平台	可能造成网络资源的占用	如果软件部署的主机负载过高，停止扫描。

6.7.2.7 渗透测试具体内容

渗透测试主要针对浦东公交指定的信息系统，在以下方面进行渗透测试。

（1）网络层安全

针对该系统所在网络层进行网络拓扑的探测、路由测试、防火墙规则试探、规避测试、入侵检测规则试探、规避测试、无线网安全、不同网段 Vlan 之间的

渗透、端口扫描等存在漏洞的发现和通过漏洞利用来验证此种威胁可能带来的损失或后果，并提供避免或防范此类威胁、风险或漏洞的具体改进或加固措施。

由于服务器系统和网络设备研发生产过程中所固有的安全隐患及系统管理员或网络管理员的疏忽，一般网络层安全漏洞包括以下安全威胁：

- 明文保存密码
- 未配置登录超时
- 未配置 AAA 认证
- 未配置管理 ACL
- 其他配置问题

（2）系统层安全

通过采用适当的测试手段，发现测试目标在系统识别、服务识别、身份认证、数据库接口模块、系统漏洞检测以及验证等方面存在的安全隐患，并给出该种隐患可能带来的损失或后果，并提供避免或防范此类威胁、风险或漏洞的具体改进或加固措施。

- 版本过低
- 远程溢出漏洞
- 本地提权漏洞
- 弱口令
- 权限过大
- 高危服务/端口开放
- 允许匿名 IPC$连接
- 其他配置问题

（3）数据存储安全

- 数据库开放端口访问
- 数据库弱口令/空口令
- 数据库未打补丁

（4）中间件安全

- IIS PUT 漏洞
- IIS 短文件名猜解

- IIS 远程命令执行
- IIS 解析漏洞
- Apache 解析漏洞
- Apache 目录遍历
- Nginx 文件解析
- Nginx 目录遍历
- Nginx CRLF 注入
- Nginx 目录穿越
- Tomcat 远程代码执行
- Tomcat war 后门文件部署
- Jboss 反序列化漏洞
- Jboss war 后门文件部署
- Weblogic 反序列化漏洞
- Weblogic SSRF
- Weblogic 任意文件上传
- Weblogic war 后门文件部署
- FastCGI 未授权访问、任意命令执行
- PHPCGI 远程代码执行

（5）应用层安全

通过采用适当测试手段，发现测试目标在服务系统认证及授权、代码审查、被信任系统的测试、文件接口模块报警响应等方面存在的安全漏洞,并现场演示再现利用该漏洞可能造成的客户资金损失，并提供避免或防范此类威胁、风险或漏洞的具体改进或加固措施。

应用程序及代码在开发过程中，由于开发者缺乏安全意识，疏忽大意极为容易导致应用系统存在可利用的安全漏洞。一般包括 SQL 注入漏洞、跨站脚本漏洞、上传漏洞、CSRF 跨站请求伪造漏洞等。

- SQL 注入
- 跨站脚本
- 表单绕过

- 上传漏洞
- 文件包含
- 已知木马
- 敏感信息泄露
- 源码信息泄露；
- 恶意代码
- 解析漏洞
- 远程代码执行漏洞
- 任意文件读取
- 目录遍历
- 目录列出
- 跨站请求伪造
- 弱口令
- 不安全对象引用
- 安全配置错误
- 链接地址重定向
- 跳转漏洞
- 后台管理
- 会话管理
- 无效验证码

（6）业务场景测试

- 注册场景
- 密码重置
- 界面锁定

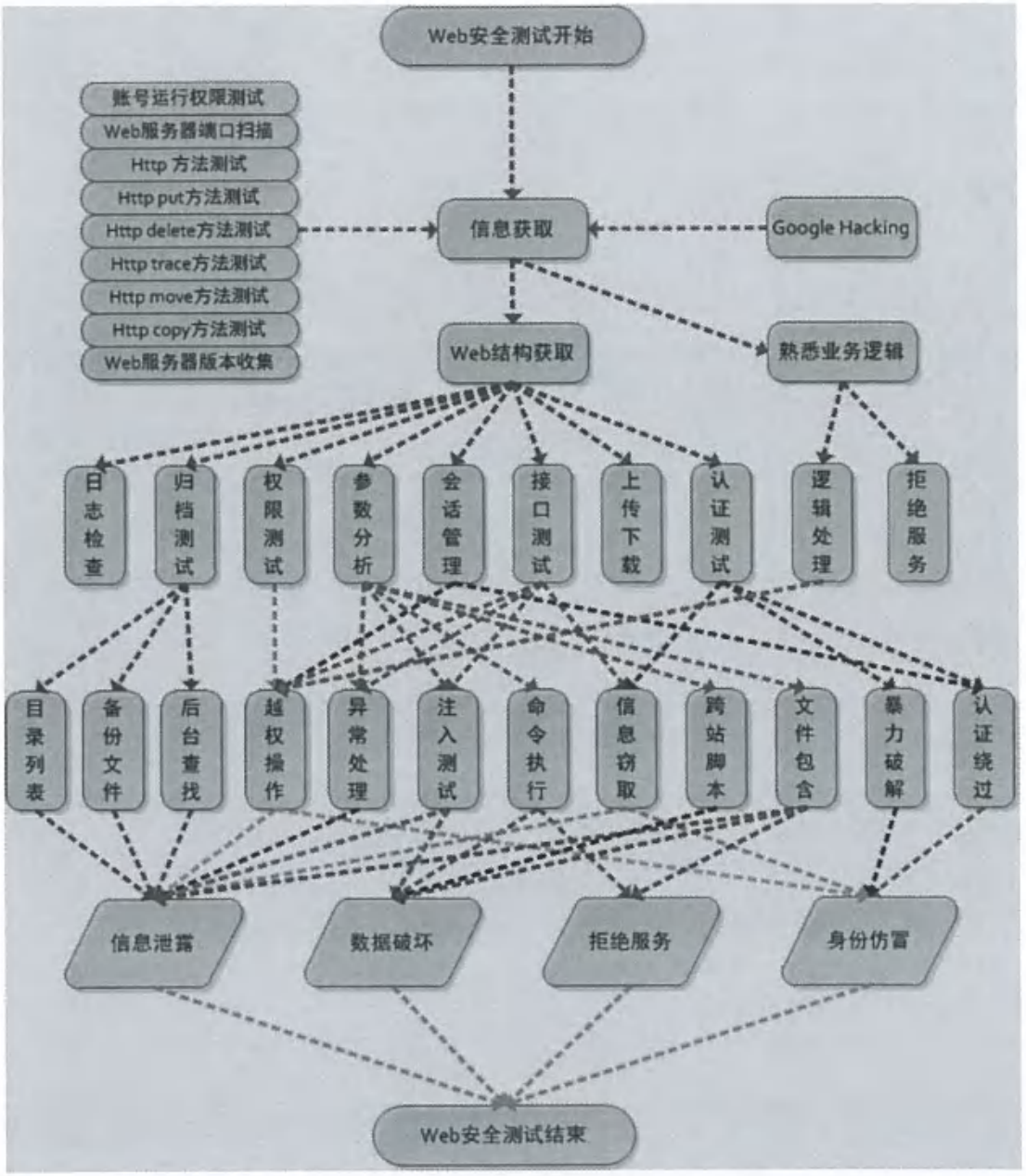


图 6-7-2-7 WEB 应用（网站）渗透测试过程

6.7.2.8 服务频次

服务周期内开展一次渗透测试。计划在第二季度的第三个月开展网络安全风险技术性探测，大约需要 3 周时间。

6.7.2.9 服务成果交付

渗透测试完成后，交付《渗透测试报告》。

6.8 数据安全风险评估

6.8.1服务需求理解

根据上级主管单位要求，对1个指定信息系统开展网络数据安全风险评估，以发现系统数据隐患、防范数据安全风险为目标，围绕数据处理者、数据处理活动开展综合性、全面性的数据安全分析，发现数据资产的威胁性和脆弱性，分析可能存在的安全威胁，促进数据安全管理能力的提升。

6.8.2数据安全风险评估实施依据

- 网络安全标准实践指南-网络数据安全风险评估实施指引（TC260-PG-20231A）
- 《数据安全技术数据安全风险评估方法》（GB/T 45577—2025）

6.8.3数据安全风险评估目的

为落实《数据安全法》《个人信息保护法》等法律法规要求，坚持预防为主、主动发现、积极防范，对数据处理者数据安全保护和数据处理活动进行风险评估，旨在掌握数据安全总体状况，发现数据安全隐患，提出数据安全管理和技术防护措施建议，提升数据安全防攻击、防破坏、防窃取、防泄漏、防滥用能力。

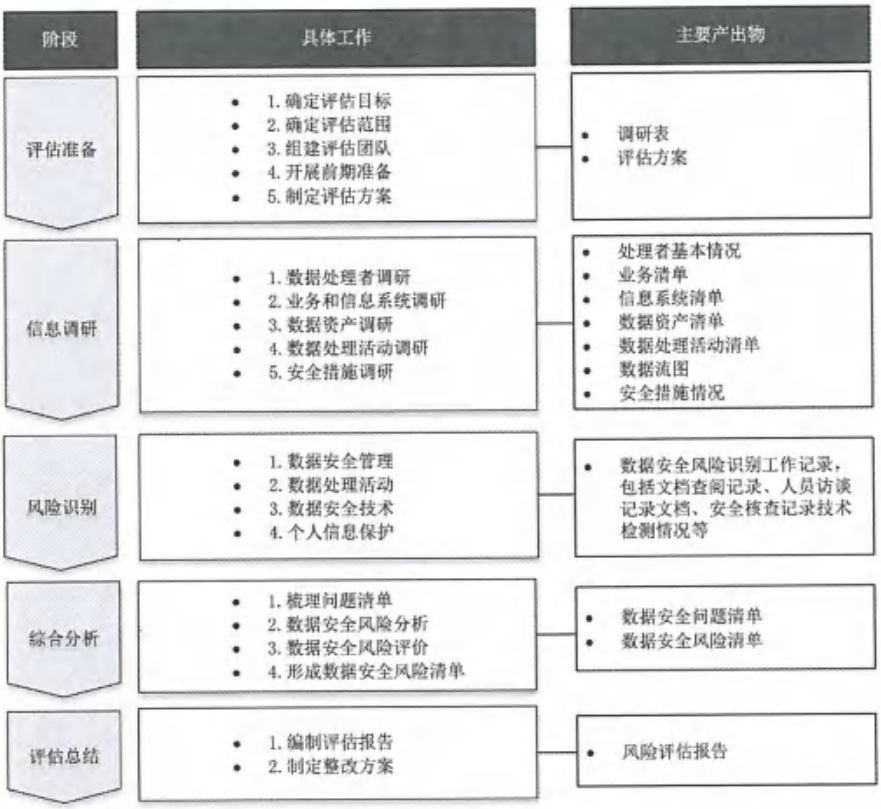
网络数据安全风险评估，主要围绕数据和数据处理活动，聚焦可能影响数据的保密性、完整性、可用性和数据处理合理性的安全风险。首先通过信息调研识别数据处理者、业务和信息系统、数据资产、数据处理活动、安全措施等相关要素，然后从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别风险隐患，最后梳理问题清单，分析数据安全风险、视情评价风险，并给出整改建议；协助数据处理者健全数据安全制度、改进安全措施，规范数据处理活动，保障数据安全。

6.8.4服务范围

浦东公交指定的1个信息系统，可云上系统也可本地机房系统。

6.8.5数据安全风险评估流程

数据安全风险评估流程，主要包括评估准备、信息调研、风险识别、综合分析、评估总结五个阶段。



6.8.6服务内容

6.8.6.1 编制评估方案

网络数据安全风险评估需制定全面的评估方案，确保网络数据安全风险评估工作能够按照评估方案稳步推进，达成预期目标。

6.8.6.1.1 评估目标

网络数据安全风险评估旨在全面贯彻落实《中华人民共和国数据安全法》《网络数据安全管理条例》等法律法规要求，响应上级主管单位的合规与安全监管需求。核心目标是通过开展综合性、全面性评估，主动发现并防范数据安全风险，构建“评估发现风险、报告呈现风险、整改化解风险”的治理闭环。

6.8.6.1.2 评估范围

评估范围包括：

（1） 安全管理制度

（2） 系统网络架构

（3） 信息系统情况

（4） 数据资产情况

（5） 数据处理活动情况

（6） 数据安全技术

（7） 个人信息保护

（8） 人员风险

6.8.6.1.3 评估方法

评估方法包括但不限于：

（1） 文档查阅

（2） 人员访谈

（3） 安全核查

（4） 技术检测

6.8.6.1.4 评估团队

评估团队的组成包括以下几类：

（1） 项目负责人

（2） 技术专家

（3） 数据分析人员

（4） 报告编制人员

6.8.6.1.5 评估步骤

评估步骤分为以下几个阶段：

（1） 评估准备阶段

（2） 信息调研阶段

（3） 风险识别阶段

（4） 风险分析与评价阶段

（5） 评价总结

6.8.6.1.6 评估成果

评估成果包括：

（1） 风险清单

（2） 风险评估报告

（3） 网络数据安全风险评估工作总结报告

6.8.6.2 信息调研

信息调研主要从数据处理者基本情况、业务和信息系统、数据资产、数据处理活动、安全防护措施等方面开展调研。

6.8.6.2.1 数据处理者调研

数据处理者调研主要通过人员访谈和文档审查，了解组织的基本情况、组织架构、在数据安全管理中的角色与职责等。

数据处理者基本情况调研内容如下表：

<table>
<tr><th colspan="5">单位基本概况</th></tr>
<tr><td>单位名称</td><td colspan="2"></td><td>组织机构代码</td><td></td></tr>
<tr><td>单位地址</td><td colspan="2"></td><td>法定代表人</td><td></td></tr>
<tr><td rowspan="2">数据安全负责人和机构</td><td>姓名</td><td></td><td>职务</td><td></td></tr>
<tr><td>联系方式</td><td></td><td>数据安全管理机构名称</td><td></td></tr>
<tr><td>单位类型</td><td colspan="4">☐党政机关 ☐事业单位 ☐国有及国有控股企业
☐民营企业 ☐外商（含港澳台）投资企业
☐其他：</td></tr>
<tr><td>是否属于特定属性数据处理者</td><td colspan="4">☐互联网政务应用管理者 ☐大型网络平台运营者（用户超过五千万）
☐关键信息基础设施运营 ☐重要数据处理者
☐大量个人信息处理者（1000 万人及以上） ☐否：</td></tr>
<tr><td>人员规模</td><td colspan="4">约 人</td></tr>
</table>

单位所属行业	□公共通信和信息服务 □能源 □交通 □水利 □金融 □公共服务 □电子政务 □国防科技工业 □卫生健康 □教育 □科技 □文化 □农业 □其他：
隶属关系	□中央 □省(自治区、直辖市) □地(区、市、州、盟) □县（区、市、旗） □其他：
上级主管部门	主管部门一： 主管部门二： 主管部门二：
业务运营地区，开展数据处理活动所在行政区划	□全球 □全国 □省(自治区、直辖市) □地(区、市、州、盟) □县（区、市、旗） □其他：
主要业务范围、业务规模	XXXX 单位是一家从事 XXXX 工作的企业，其主营业务包括 XXXX、XXXX、XXXX。服务对象为党政机关/事业单位/企业/个人/境外用户，用户规模约为 XXX。
数据处理相关服务行政许可	
开展数据业务的依据文件、监管文件、指导性文件	《中华人民共和国网络安全法》 《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》 《上海市数据条例》
被评估单位的资本组成和实际控制人情况	注册资本：XXX 万 XXXXX 公司： % XXXXX 公司： %

	……
是否境外上市或计划赴境外上市	□是，上市地区和交易所 □计划上市，计划上市地区和交易所 □以协议控制（VIE）架构等方式实质性境外上市 □否

6.8.6.2.2 业务和信息系统调研

业务和信息系统调研主要通过数据使用说明、相关合同协议、测评材料等文档，梳理评估范围内支撑业务运营的信息系统情况，包括业务功能、业务流程、系统架构、网络拓扑、部署环境等，形成业务和信息系统清单。

业务和信息系统调研内容如下表：

业务和信息系统情况	
业务名称	
拓扑结构	
信息系统和系统保护等级（如业务涉及多个信息系统，则填写多个） （可多选）	系统名称 1： 保护等级：□一级 □二级 □三级 □四级 □未定级 □关键信息基础设施 系统名称 2： 保护等级：□一级 □二级 □三级 □四级 □未定级 □关键信息基础设施
业务功能描述	

业务服务对象	□政府部门　□境外用户 □企业用户　□个人信息主体 □其他：_____
业务流程	
业务用户规模	
业务覆盖地域	全国/上海
业务涉及数据类型（可多选）	□个人信息　□个人敏感信息 □重要数据　□核心数据 □一般数据　□其他：_____
业务相关部门信息	
服务入口	□APP：_____【填写 APP 名称及版本】 业务访问 IP 地址：_____ □微信小程序：_____【填写小程序名称及版本】 业务访问 IP 地址：_____ □支付宝小程序：_____ 业务访问 IP 地址：_____ □百度小程序：_____ 业务访问 IP 地址：_____ □其他：_____ 业务访问 IP 地址：_____ 业务访问其他地址：_____
业务系统部署位置（可多选）	□公有云，云服务商：_____ □政务云，云服务商：_____ □自建私有云，技术方案提供方：_____

	□托管机房，运维方：_____ □数据中心：_____ □数据境外地址：_____ □其他：_____
外部来源	□接入的第三方产品，服务商：_____ □接入的第三方服务，服务商：_____ □接入的SDK：_____【填写SDK名称、版本及提供方】

6.8.6.2.3 数据资产调研

数据资产调研主要从数据资产总体情况和数据资产清单进行调研。

➢ 数据资产总体情况调研

数据资产总体情况主要对数据规模、数据范围、数据所属领域、数据分类分级等进行调研，内容如下表：

数据资产概况	
数据规模	截至 XXXX 年 XX 月 XX 日本单位处理*的数据总规模：　　TB，年增长量：　TB ***处理包括：收集、存储、使用、加工、传输、提供、公开、删除等*** 核心数据总规模：　　TB，年增长量：　　TB 重要数据总规模：　　TB，年增长量：　　TB 个人信息总规模：　　MB、　　条，年增长量：　　MB、　　条 公共数据总规模：　　TB，年增长量：　　TB 政务数据总规模：　　TB，年增长量：　　TB 一般数据总规模：　　TB，年增长量：　　TB

数据范围	数据处理范围： □政务数据　　□公共数据　　□个人信息 □核心数据　　□重要数据　　□一般数据
数据所属行业领域	□工业　□电信　□交通　□金融　□自然资源 □卫生健康　□教育　□科技　□政务　□其他：
数据分类分级	1. 是否进行数据分类：□是　　□否 数据分类维度： 主要数据类型： 2. 是否进行数据分级：□是　　□否 数据分为　　级，分别为： 3. 是否制定数据分类分级制度文件： □是，文件名称： □否 4. 是否建立重要数据目录：□是　□否 是否上报重要数据目录：□是，上报部门：　　□否

➢ 数据资产清单内容

数据资产清单内容主要梳理结构化数据资产（如数据库表等）和非结构化数据资产（如图表文件等），摸清数据底数，输出数据资产清单。涉及范围包括但不限于生产环境、测试环境、备份存储环境、云存储环境、个人工作终端、数据采集设备终端等收集和产生的数据。

数据资产清单调研内容如下表：

数据资产清单								
序	数	数据	内容	载体	数据规	存储	重要性描述	是否

号	据资产名称	分类	描述	形式	模	区域/信息系统	用途	级别（如涉及）	存储时效	涉及数据出境
1										
…	*示例：个人信息*	*个人信息*	*姓名，手机号码*	*数据库*	*XXXX人*	*移动政务云*	*用户注册*		*永久*	*否*

6.8.6.2.4 数据处理活动调研

数据处理活动调研主要结合业务场景，梳理数据在“收集、存储、使用、加工、传输、提供、公开、删除”全生命周期中的每一项处理活动，明确各活动的参与主体、操作流程、网络环境及数据流向等。

➢ 数据处理活动总体情况调研

数据处理活动总体情况主要从涉及的数据处理活动类别、关键数据处理、第三方外包机构接触的数据情况及涉及的数据处理活动等进行调研，内容如下表：

涉及的数据处理活动	1.涉及的数据处理活动 □数据收集 □数据存储 □数据使用 □数据加工 □数据传输 □数据提供 □数据公开 □数据删除 □数据出境 □不涉及，说明原因：_____
关键数据处理	1.数据存储位置（多选）：

活动	□自建机房　　□外部租赁 IDC 机房 □租赁云存储服务，品牌为：_____ □涉及数据在境外存储的情况　□其他：_____ 2. 数据使用的目的包括： □向个人/非个人用户提供服务，具体为：_____ □支撑机构内部生产、运营，具体为：_____ □实现统计、分析，具体为：_____ □科学研究，具体为：_____ □其他：_____ 3. 数据加工情况（多选）： □机构内部自行开展数据加工 □委托外部机构进行数据加工，被委托方：_____ □未进行任何形式的数据加工 □其他：_____ 4. 数据提供情况（多选）： □因为本身业务的目的是向外部单位提供数据_ □委托第三方进行数据处理 □数据交易，涉及的数据类型：□个人信息，□重要数据， □其他 □未涉及数据提供 □其他：_____ 5. 数据公开情况： 公开渠道：_____公开数据内容：_____ 6. 数据出境情况： □有数据出境情况，出境数据包含重要数据 □有数据出境情况，出境数据不包含重要数据 □无数据出境情况
第三方外包服	□核心数据　　□重要数据　　□个人信息

务机构接触数据情况	□公共数据　□政务数据　□其他：_____
第三方外包服务机构涉及的数据处理活动	□数据收集　□数据存储　□数据使用　□数据加工 □数据传输　□数据提供　□数据公开　□数据删除 □数据出境　□不涉及，说明原因：_____

➢ 数据收集情况调研

数据收集情况主要从数据收集渠道、收集方式、收集目的、收集频率、数据量等进行调研，内容如下表：

数据收集情况								
序号	数据资产名称	具体内容（简写关键字段）	收集渠道	收集方式	收集目的	收集频率	数据量	日增量
1								
…								

➢ 数据存储情况调研

数据存储情况主要从数据存储方式、存储地点、备份地点、备份方式等进行调研，内容如下表：

数据存储情况	
数据存储方式（可多选）	□集中存储　□分布式存储 □分类分级存储　□其他：_____
数据量	统计截至时间： □数据总量：_____　□日均增量：_____ □用户数据量：_____　□用户数据日均增量：_____ □在线数据量：_____　□离线数据量：_____
存储所在地	【填写包括云环境、数据机房、数据中心等物理地址】

存储系统 （可多选）	□数据库，数据库类型：_____ □大数据平台：_____ □云存储，存储产品类型：_____ □网盘，网盘提供商：_____ □存储介质，介质类型：_____ □外部存储机构：_____ □其他：_____
数据备份所在地	【填写包括同城备份地方、主备份地方、异地备份地方】
数据备份方式 （可多选）	□全量备份 □增量备份 □差异备份 □镜像备份 □实时备份 □定期备份 □冗余备份
安全防护措施 （可多选）	□采取了保密性措施，国产密码技术，加密算法：_____ □采取了完整性措施，国产密码技术，加密算法：_____ □日志审计 □访问控制 □脱敏/去标识化 □身份鉴别 □数据分类分级存储 □其他

➢ 数据传输情况调研

数据传输情况主要从数据传输途径和方式、传输类型、传输协议、传输接口等进行调研，内容如下表：

数据传输情况					
序号	传输数据类型	传输途径和方式	源传输节点	目的传输节点	传输协议
1					
…					

➢ 数据的使用和加工情况调研

数据使用和加工情况调研，主要是对数据使用目的、方式、范围、场景、算法规则、相关系统和部门，数据清洗、转换、标注等加工情况，应用算法推

荐技术提供互联网信息服务的情况，核心数据、重要数据或个人信息委托处理、共同处理的情况等。内容如下表：

数据使用情况							
序号	应用场景	数据资产名称	数据来源	使用目的	使用方式	负责部门	是否对外发布
1							
…							

应用算法推荐技术情况						
序号	算法推荐类型	应用场景	用户特征使用的数据字段	数据来源	调用更新频率	是否上报互联网信息服务算法备案系统
1						
…						

数据加工情况					
序号	加工数据类型	加工目的	加工方式	加工场所	是否委托加工
1					
…					

➢ 数据提供情况调研

数据提供情况调研，主要对数据提供的目的、方式、范围、数据接收方、合同协议，对外提供的个人信息和重要数据的种类、数量、范围、敏感程度、保存期限等进行调研，内容如下表：

数据提供情况									
序号	数据接收方	提供方式	提供目的	提供频率	数据字段	数据量	涉及的业务	用户是否单独	是否签订合同

								同意	协议
1									
…									

➢ 数据公开情况调研

数据公开情况调研主要对数据公开的目的、方式、对象范围、受众数量、行业、组织、地域等进行调研，内容如下表：

数据公开情况								
序号	公开数据类型	目的	方式	对象范围	受众数量	所属行业	公开组织	所处地域
1								
…								

➢ 数据删除情况调研

数据删除情况主要对数据删除情形、删除方式、数据归档、介质销毁等进行调研，内容如下表：

数据删除情况				
数据类型	删除情形	删除方式	能否恢复	数据归档
1				
…				

➢ 数据出境情况调研

数据出境情况主要对是否存在个人信息或重要数据出境，如跨境业务、跨境办公、境外上市、使用境外云服务或数据中心、国际交流合作等场景的数据出境情况进行调研，内容如下表：

数据出境情况						
序号	出境数据类型	数据量	出境目的	出境方式	用户是否单独同意	是否通过出境评估

1						
…						

6.8.6.2.5 安全防护措施调研

安全防护措施主要从已开展的安全测评情况、数据安全现状、网络和数据安全主要措施等方面进行调研。

➢ 已开展的安全测评情况调研

已开展的测评情况主要从等级保护测评、商用密码应用安全性评估、安全检测、风险评估、安全认证、合规审计情况等进行调研，内容如下表：

已开展的安全测评概况	
测评类（可多选）	□网络安全等级保护测评 □关键信息基础设施安全检测评估 □商用密码应用安全性评估 □网络数据安全风险评估 □个人信息保护影响评估 □个人信息安全合规性评估（依据国家标准 GB/T 35273-2020） □移动互联网应用程序个人信息安全测评 □数据出境安全评估 □云计算服务安全评估 □互联网新闻信息服务新技术新应用安全评估 □具有舆论属性或社会动员能力的互联网信息服务安全评估 □互联网信息服务算法评估与备案

	□深度合成类应用程序的安全评估与备案 □其他：
认证类 （可多选）	□数据安全管理认证（DSM） □个人信息保护认证 □APP 安全认证 □其他：_____

已开展的安全测评具体情况				
序号	证书/报告名称	认证/测评单位	认证/测评时间	认证/测评范围
1				
…				

➢ 数据安全现状调研

数据安全现状主要从数据安全管理组织和人配置情况及数据安全管理制度进行调研，内容如下表：

数据安全管理组织和人员配置情况				
数据安全负责人和机构	负责人姓名		负责人职务	
	负责人联系方式		数据安全管理机构名称	
	数据安全管理机构岗位及配备人员数量	岗位 1 名称：XXXXXX ；配备人员： XXXX 人； 岗位 2 名称：XXXXXX ；配备人员： XXXX 人； 岗位 3 名称：XXXXXX ；配备人员： XXXX 人；		

数据安全管理制度情况		
序号	文档名称（下为示例）	主要内容
1	*数据安全总体策略*	
2	*数据安全管理工作规划或方案*	
3	*数据分类分级制度*	
4	*数据分类分级保护制度*	
5	*数据安全管理制度*	
6	*数据安全评估制度*	
7	*数据访问权限管理制度*	
8	*数据安全应急响应制度*	
9	*数据安全应急预案*	
10	*数据安全培训计划与记录*	
11	*数据安全考核及监督问责制度*	
12	*数据安全关键岗位的数据安全操作规程*	
13	*关键岗位人员管理材料*	
14	*个人信息保护内部管理制度*	
15	*个人信息影响评估制度*	
16	*个人信息应急预案*	
17	*外包服务管理制度*	
18	*开发运维管理制度*	

➢ 网络和数据安全主要措施调研

网络和数据安全主要措施从网络架构、网络边界、数据处理活动生命周期

等层面涉及的防护措施进行调研，内容如下表：

网络和数据安全主要措施		
序号	防护措施	措施简述
1	WAF	为应用系统提供网络安全防护
…		

6.8.6.2.6 调研方式

1、人员访谈

（1）访谈对象选择

1) **层级覆盖** 为了确保访谈结果的全面性和代表性，需要选取不同层级的工作人员进行交流。具体包括：

- **高层管理人员：**如单位负责人、主管领导等，了解他们对数据安全的整体战略规划和资源投入情况。
  - **关注点：**企业数据安全政策的方向性决策、资源分配优先级、风险容忍度等。
- **中层管理人员：**如业务主管等，掌握他们在日常管理中的具体实践和挑战。
  - **关注点：**团队内部的安全制度执行情况、技术工具的有效性、跨部门协作的顺畅程度等。
- **一线技术人员：**如系统管理员、数据库管理员、开发人员等，获取他们在实际操作层面的经验和建议。
  - **关注点：**日常工作中遇到的具体问题、技术难点、潜在的安全隐患等。
- **普通员工：**随机抽取部分普通员工，了解他们对信息安全的认识和行为习惯。
  - **关注点：**安全意识水平、培训效果、日常工作中的安全实践等。

2) **角色多样性** 除了按层级划分外，还应考虑不同角色的专业背景和工作职责，确保访谈涵盖各个关键领域：

IT 支持与运维：负责基础设施和技术系统的维护和支持，直接接触硬件设备和网络环境。

数据分析与应用开发：参与数据处理活动的设计和实现，涉及敏感信息的使用和保护。

业务运营与服务提供：在业务流程中使用或生成数据，是数据流转的重要节点。

合规与审计：专注于安全制度的制定和监督，确保组织符合法律法规要求。

（2）访谈记录整理

1) **数据收集方式** 采用多种方式记录访谈过程，确保信息的完整性和准确性：

录音/录像：对于重要访谈，可以事先征得对方同意后进行录音或录像，便于后续回顾和分析。

书面笔记：即时记录关键信息和观点，避免遗漏重要内容。

电子文档：使用笔记本电脑或平板设备实时录入访谈内容，方便后期整理和分类。

2) **结果汇总** 将所有访谈记录进行整理和分类，提炼出有价值的信息和反馈意见：

主题归类：根据访谈大纲中的问题类别，将相似的观点和建议归为同一主题，如“安全管理”、“技术支持”、“员工培训”等。

共性与差异：找出不同层级和角色间存在的共性和差异，分析背后的原因和影响因素。

量化统计：对于一些可量化的反馈（如培训满意度评分），进行简单的统计分析，直观展示整体趋势。

3) **反馈意见形成** 基于汇总的结果，形成有价值的反馈意见，为后续改进提供依据：

问题清单：列出访谈中发现的主要问题，明确其严重程度和紧急性，为整改工作设定优先级。

改进建议：针对每个问题提出具体的改进建议，包括短期应急措施和长期优化方案。

行动计划：制定详细的行动计划，明确责任人、时间节点和预期成果，确保整改措施得到有效落实。

（3）结果呈现

人员访谈最终输出可以包括以下内容：

访谈总结报告：详细记录访谈对象的选择依据、访谈大纲的设计思路以及访谈过程中发现的关键问题和建议。

问题与建议汇总表：以表格形式列出所有识别出的问题及其对应的改进建议，便于快速查阅和跟踪进展。

通过上述方法，可以系统化地开展人员访谈工作，深入了解到站信息发布系统各层级员工对数据安全的看法和经验，识别潜在的风险点，并提出针对性的改进建议，从而有效提升整体数据安全保障水平。

2、文档查验

（1）文档清单编制

1) **确定文档范围** 为了确保文档查验的全面性和系统性，首先需要明确哪些类型的文档是必要的。以下是常见的文档类别及其重要性：

政策与制度类

- **信息安全政策**：涵盖总体安全方针、数据分类标准、加密策略等。
- **访问控制政策**：规定用户认证和授权机制的具体要求。
- **应急响应计划**：详细描述突发事件应对流程和责任分工。

操作指南与流程类

- **系统操作手册**：包括服务器、数据库、网络设备等的操作说明。
- **应用开发规范**：涉及代码编写、测试、部署等方面的最佳实践。
- **变更管理流程**：定义如何处理系统配置或业务逻辑的变更。

技术文档类

- **架构设计文档**：描述 IT 基础设施和技术栈的整体布局。

- **API 接口文档**：提供对外服务接口的详细说明，确保第三方集成的安全性。
- **安全配置指南**：针对防火墙、IDS/IPS 等安全设备的具体设置建议。

合规性文件类

- **法律法规遵从记录**：证明组织符合相关法规要求的证据材料。
- **审计报告**：由内部或外部审计机构出具的安全评估结果。
- **合同协议**：与第三方签订的服务合同中关于数据保护的权利义务条款。

2) **编制清单** 根据上述类别，列出具体需要查阅的所有文档，并为每份文档赋予唯一标识符，方便后续管理和跟踪。示例如下：

文档编号	文档名称	类型	版本号	存放位置
DOC-001	信息安全政策	政策与制度	V1.5	内部知识库
DOC-002	访问控制政策	政策与制度	V2.0	内部知识库
DOC-003	应急响应计划	政策与制度	V1.3	内部知识库
DOC-004	数据中心操作手册	操作指南	V3.1	IT 部门共享文件夹
DOC-005	API 接口文档	技术文档	V2.2	开发团队代码仓库
DOC-006	安全配置指南	技术文档	V1.8	IT 部门共享文件夹
DOC-007	合规性遵从记录	合规性文件	N/A	法务部门档案室

（2）内容准确性核对

1) **真实性验证**

来源确认：检查文档的来源是否可靠，如是否由官方渠道发布、是否有权威签名或印章等。

一致性校验：对比不同版本之间的差异，确保修订过程透明且合理，避免出现矛盾或冲突的内容。

事实核查：对于涉及具体数据或案例的部分，通过实地考察、访谈等方式进行交叉验证，确保信息准确无误。

2） **完整性评估**

结构完整性：审查文档结构是否完整，各章节内容是否连贯，是否存在缺失的关键信息或步骤。

逻辑严密性：分析文档中的逻辑关系，确保其推理过程严谨，结论有据可依。

覆盖范围：确认文档是否涵盖了所有必要的方面，特别是针对新出现的技术或业务场景，是否有相应的补充说明。

3） **外部参照**

法规对照：将文档内容与最新的法律法规（如《中华人民共和国个人信息保护法》）进行对照，确保其符合最新要求。

行业标准：参考国际或国内的相关标准（如 ISO/IEC 27001），评估文档是否达到了最佳实践水平。

（3）结果呈现

文档查验最终输出可以包括以下内容：

文档清单：一份详尽的文档清单，列明所有需要查阅的文档及其基本信息，确保查阅工作的全面性和系统性。

通过上述方法，可以系统化地开展文档查验工作，深入检查到站信息发布系统的各项文档，识别潜在的风险点，并提出针对性的改进建议，从而有效提升整体数据安全保障水平，确保其符合相关法律法规的要求。

3、技术测试

（1）渗透测试

1） **测试目标与范围**

目标设定：明确渗透测试的具体目标，如评估外部网络边界的安全性、检测内部系统漏洞或模拟特定攻击场景。

范围界定：确定测试涵盖的资产范围，包括 IP 地址段、服务器、应用程序、数据库等，并获得必要的授权。

2) **测试方法与工具**

黑盒测试：在不了解内部结构的情况下进行测试，模拟真实的黑客攻击行为，评估系统的整体防御能力。

- **工具选择**：使用 Nmap、Metasploit、Burp Suite 等工具扫描开放端口、发现潜在漏洞并尝试利用。

白盒测试：基于对系统架构和代码的详细了解，进行更深入的漏洞挖掘，重点检查安全配置和编码实践。

- **工具选择**：结合静态分析工具（如 Fortify、SonarQube）和动态分析工具（如 OWASP ZAP），全面审查代码逻辑和运行时行为。

灰盒测试：介于黑盒和白盒之间，提供部分信息给测试人员，既能加快测试进程又能保持一定的挑战性。

3) **测试流程**

前期准备：制定详细的测试计划，包括时间表、参与人员、沟通机制等；确保所有相关方知晓测试安排并同意其影响。

执行阶段：按照预定方案实施攻击模拟，记录每一步操作及其结果，注意遵守法律法规，避免造成实际损害。

报告生成：整理测试过程中发现的所有问题，编写详尽的渗透测试报告，包含漏洞描述、风险等级、修复建议等内容。

4) **后续跟进**

整改验证：根据报告中的建议，督促相关部门采取整改措施，并在规定时间内重新测试以确认问题已解决。

经验总结：定期组织团队讨论会，分享每次渗透测试的经验教训，持续改进测试方法和技术手段。

（2）配置核查

1) **操作系统**

基线配置：对比操作系统厂商提供的安全基线配置（如 CIS Benchmarks），检查是否存在不必要的服务启动项、默认账户未禁用等问题。

更新策略：评估操作系统补丁管理策略的有效性，确保及时安装最新的安全更新，减少暴露于已知漏洞的风险。

访问控制：检查用户权限分配是否合理，遵循最小权限原则，避免过度授权；确保重要的系统文件和目录设置了适当的读写权限。

2) **数据库管理系统**

安全设置：审查数据库的安全配置选项，如 SSL/TLS 加密传输、密码复杂度要求、登录失败锁定策略等，确保其符合最佳实践。

备份恢复：评估备份策略，包括备份频率、保存期限、异地存储等，确保数据可恢复性；测试恢复流程，验证备份数据的有效性。

性能优化：检查数据库性能调优参数，确保其在保障安全的前提下不影响业务效率；监控数据库活动日志，及时发现异常行为。

3) **其他组件**

中间件与应用服务器：审查中间件（如 Apache Tomcat、IBM WebSphere）和应用服务器的安全配置，确保其遵循官方推荐的安全指南。

网络设备：检查路由器、交换机等网络设备的安全设置，如防火墙规则、ACL 访问控制列表等，确保网络环境的安全性。

安全防护工具：评估入侵检测系统（IDS）、防病毒软件等安全防护工具的配置，确保其能够有效识别和阻止潜在威胁。

（3）结果呈现

最终输出可以包括以下内容：

渗透测试报告：详细列出采用不同测试方法识别出的所有漏洞，描述每个漏洞的具体场景和缓解措施。

配置审查报告：全面评估操作系统、数据库管理系统及其他组件的安装配置，指出存在的问题并提出改进建议，确保其安全性和可靠性。

通过上述方法，可以系统化地开展技术测试工作，深入检验到站信息发布系统的技术安全状况，识别潜在的技术缺陷和防护漏洞，估计可能造成的损失，并提出针对性的防护措施和改进建议，从而有效提升整体数据安全保障水平。

6.8.6.3 风险识别

6.8.6.3.1 数据安全管理风险

（1）管理制度审查

1） **安全管理制度的完整性**

政策文件：检查是否制定了全面的信息安全政策，涵盖数据分类、加密、备份、访问控制等方面。确保这些政策明确各级员工的责任，并与最新的法律法规保持一致。

- **数据分类标准**：是否有清晰的数据分类指南，如敏感数据、普通数据等，以确定不同的保护级别。
- **加密策略**：确认是否对静态和传输中的数据进行了适当的加密处理，采用何种加密算法（如 AES-256）。
- **备份管理**：评估备份频率、存储位置以及恢复测试结果，确保数据可恢复性。

2） **流程规范性**

操作流程：审查日常操作流程是否标准化，如用户认证、权限分配、日志记录等。确保所有操作均有书面指南，并定期更新。

- **用户认证流程**：是否采用了多因素认证（MFA），并有详细的登录尝试日志记录。
- **权限管理流程**：是否遵循最小权限原则，权限变更是否有严格的审批程序。
- **日志管理流程**：是否启用了详细的日志记录功能，日志保存期限是否符合法规要求，是否有定期审计机制。

3） **执行力度**

制度执行情况：通过访谈和文档查验，了解安全管理制度在实际工作中的落实情况。检查是否存在执行不到位的问题，如违规操作未被及时纠正。

- **合规性检查**：定期进行内部审计，验证各项制度是否得到有效执行，发现问题及时整改。
- **监督机制**：是否有独立的安全监督部门或岗位，负责监督制度的执行情况，防止形式主义。

（2）人员培训情况

1） **安全意识教育**

培训计划：了解是否有系统化的安全意识培训计划，涵盖不同层级的员工。培训内容应包括但不限于网络安全基础知识、个人信息保护法解读、常见攻击手段防范等。

- **新员工入职培训**：确保每位新员工在入职时都接受了必要的信息安全培训，了解公司安全政策和个人责任。
- **持续教育**：定期组织全体员工参加安全意识提升课程，保持知识更新，增强应对新型威胁的能力。

2） **技能水平评估**

技术技能培训：针对 IT 技术人员和开发人员，提供专业技能提升培训，如漏洞修复、安全编码实践、应急响应演练等。

- **安全编码培训**：确保开发人员掌握安全编码最佳实践，减少代码中潜在的安全漏洞。
- **漏洞修复培训**：培训 IT 人员如何快速识别和修复系统中存在的安全漏洞，提高响应速度。

3） **培训效果评估**

考核机制：建立有效的培训效果评估机制，通过考试、模拟演练等方式检验培训成果。确保每位员工都能将所学知识应用到实际工作中。

- **模拟攻击演练**：定期组织模拟攻击演练，测试员工的实际应对能力，找出薄弱环节并加以改进。

- **反馈收集**：收集员工对培训内容和方式的意见建议，不断优化培训方案，提高参与度和效果。

（3）应急响应机制

1） **应急预案制定**

预案编制：检查是否已编写详细的突发事件应对预案，涵盖从预防、检测、响应到恢复的全过程。

- **事件分级**：根据事件的影响范围和严重程度，制定相应的响应级别和处理流程。
- **职责分工**：明确各部门和人员在应急响应中的具体职责，确保每个环节都有专人负责。
- **资源准备**：确保有足够的资源支持应急响应工作，如备用设备、技术支持团队、外部专家联系名单等。

2） **演练与测试**

演练频率：定期组织应急响应演练，检验预案的有效性和实用性。演练应尽可能贴近实际情况，涵盖不同类型的安全事件。

- **桌面演练**：通过讨论和模拟情景，测试应急预案的逻辑性和可操作性。
- **实战演练**：在受控环境下进行实战演练，验证应急响应团队的实际处理能力和协调配合。

3） **改进与优化**

事后总结：每次演练后进行详细的事后总结，分析存在的问题和不足之处，提出改进建议。

- **经验分享**：将成功的经验和教训整理成文档，供全体员工学习借鉴，提高整体应急响应水平。
- **持续改进**：根据演练结果和实际情况，不断完善应急预案，确保其始终处于最佳状态。

（4）结果呈现

最终输出可以包括以下内容：

管理制度审查报告：详细列出现有安全管理制度的优势和不足，提出改进建议，确保制度的完善性和执行力。

人员培训评估报告：总结培训计划的实施情况和效果，指出需要加强的方面，为后续培训提供依据。

应急响应能力评估报告：全面评估应急响应机制的有效性，提出优化建议，确保在突发事件发生时能够迅速、有效地应对。

通过上述方法，可以全面评估到站信息发布系统的数据安全管理风险，发现潜在问题并提出针对性的改进建议，从而提升整体安全管理水平，确保数据资产的安全性和可靠性。

6.8.6.3.2 数据处理活动风险

（1）威胁建模

1） **采用 STRIDE 模型分析潜在威胁**

定义 STRIDE：STRIDE 是一种广泛应用于软件安全领域的方法论，用于识别和分类可能影响数据处理活动的六种威胁类型：

- Spoofing（**欺骗**）：伪造身份或系统组件，如冒充合法用户或服务器。
- Tampering（**篡改**）：未经授权修改数据或系统配置。
- Repudiation（**抵赖**）：否认执行过某项操作，无法证明其真实性。
- Information Disclosure（**信息泄露**）：敏感信息被非法访问或公开。
- Denial of Service（**拒绝服务**）：使系统或服务不可用，影响正常业务运作。
- Elevation of Privilege（**权限提升**）：未经授权获得更高权限，进行未授权的操作。

2） **威胁建模步骤**

资产识别：明确需要保护的数据资产及其重要性，如居民个人信息、政务数据等。

威胁来源分析：识别可能的攻击者群体，包括内部员工、外部黑客等。

威胁场景构建：基于 STRIDE 模型，为每种威胁类型构建具体的攻击场景，描述可能的攻击路径和手段。

缓解措施规划：针对每个威胁场景，提出相应的缓解措施，如加强身份验证、实施数据加密、启用日志审计等。

3) **其他适用方法论**

DREAD 模型：从损害程度（Damage）、重现频率（Reproducibility）、易利用性（Exploitability）、受影响用户数量（Affected users）、可发现性（Discoverability）五个维度评估威胁的风险等级。

PASTA 框架：通过过程化高级威胁与漏洞分析（Process for Attack Simulation and Threat Analysis），结合业务目标和技术细节，全面评估威胁对组织的影响。

（2）脆弱性扫描

1) **自动化工具选择**

常用工具：使用专业的脆弱性扫描工具（如 Nessus、OpenVAS、Qualys 等）定期查找系统中的漏洞。

- **Nessus**：提供广泛的漏洞库，支持多种操作系统和应用环境，具备强大的报告生成能力。
- **OpenVAS**：开源且免费，适用于中小型企业和个人用户，具有良好的社区支持。
- **Qualys**：提供云服务模式，易于部署和管理，特别适合大型服务平台的需求。

2) **扫描范围与频率**

扫描对象：覆盖所有关键 IT 资产，包括但不限于服务器、数据库、网络设备、应用程序等。

扫描周期：根据系统的敏感性和变更频率，设定合理的扫描周期。建议每月至少进行一次全面扫描，对于高风险区域可以增加到每周一次。

补丁管理：及时修复已知漏洞，确保系统始终保持最新状态。建立快速响应机制，优先处理严重级别的漏洞。

3) **结果分析与处理**

漏洞分类：根据 CVSS 评分标准将漏洞分为低、中、高三个级别，优先处理高危漏洞。

补救措施：针对每个漏洞制定详细的补救计划，包括技术修复、临时缓解措施以及长期改进策略。

跟踪记录：维护完整的漏洞管理台账，记录每次扫描的结果、采取的行动及后续跟进情况，确保问题得到彻底解决。

（3）影响评估

1) **损失估计方法**

直接经济损失：计算因安全事故导致的直接财务损失，如修复成本、法律费用、赔偿金等。

间接经济损失：评估事故对单位声誉、客户信任度、公信力等方面造成的负面影响，量化其带来的长期经济和政治损失。

业务中断损失：估算因系统停机或服务不可用给业务带来的公众损失，考虑恢复时间和替代方案的成本。

2) **风险矩阵分析**

风险概率与影响程度：绘制风险矩阵图，横轴表示事件发生的概率，纵轴表示事件造成的影响程度。将识别出的风险点标示在图上，直观展示其风险等级。

优先级排序：根据风险矩阵结果，确定各项风险的优先处理顺序，集中资源应对高概率、高影响的风险点。

3) **恢复能力评估**

恢复时间目标（RTO）：评估事故发生后恢复正常运营所需的时间，确保关键业务能够在最短时间内恢复。

恢复点目标（RPO）：确定可以容忍的最大数据丢失量，确保数据备份策略能够满足这一要求。

灾难恢复计划：检查是否制定了完善的灾难恢复预案，并定期进行演练，确保其有效性。

（4）结果呈现

最终输出可以包括以下内容：

威胁建模报告：详细列出采用 STRIDE 或其他方法论识别出的所有潜在威胁，描述每个威胁的具体场景和缓解措施。

脆弱性扫描报告：汇总自动化工具扫描结果，分类整理各类漏洞，并提出详细的补救计划和跟踪记录。

影响评估报告：综合分析一旦发生安全事故可能造成的损失，提供量化指标和风险矩阵图，帮助决策层了解风险状况并制定相应对策。

通过上述方法，可以全面评估到站信息发布系统的数据处理活动风险，识别潜在威胁和脆弱性，估计可能造成的损失，并提出针对性的防护措施和改进建议，从而有效提升整体数据安全保障水平。

6.8.6.3.3 数据安全技术风险

（1）技术架构审查

1） **技术基础设施健壮性评估**

网络架构：

- **拓扑结构**：检查现有网络的物理和逻辑拓扑，确保其设计合理、冗余度高，能够应对单点故障。
- **分段隔离**：验证是否采用了虚拟局域网（VLAN）等技术对不同业务单元进行有效隔离，减少横向攻击的风险。
- **边界防护**：确认网络边界处部署了足够的防护设备，如防火墙、入侵检测系统（IDS），并定期更新规则库。

服务器与存储：

- **硬件可靠性**：评估服务器和存储设备的硬件配置，确保其具备足够的计算能力和存储容量，支持业务需求的同时具备良好的容错能力。
- **高可用性设计**：检查是否有集群部署或热备方案，以保证关键应用和服务在发生硬件故障时仍能正常运行。
- **数据备份**：审查备份策略，包括备份频率、保存期限、异地存储等，确保数据可恢复性。

云服务使用情况：

- **供应商选择**：评估云服务提供商的安全认证和合规性，如 ISO/IEC 27001、SOC 2 等。
- **服务级别协议（SLA）**：检查与云服务商签订的 SLA 条款，明确可用性、性能、安全等方面的责任划分。
- **数据主权**：确保数据存储位置符合法律法规要求，特别是涉及跨国传输的数据。

2) **应用程序架构**

开发框架：审查应用程序使用的开发框架和技术栈，确保其安全性，如是否存在已知漏洞或不安全的默认配置。

API 接口：检查所有对外提供的 API 接口，确保采用 HTTPS 加密传输，并有严格的访问控制机制。

第三方组件：评估应用程序中使用的第三方库和插件，确保及时更新至最新版本，避免引入潜在的安全风险。

（2）防护工具效能测试

1) **防火墙**

规则设置：评估防火墙规则是否合理，是否存在不必要的开放端口或宽松的流量允许策略。

日志记录：检查防火墙是否启用了详细的日志记录功能，日志保存期限是否符合法规要求，是否有定期审计机制。

性能监控：通过模拟流量负载测试防火墙的处理能力和响应速度，确保其在高峰期也能稳定工作。

2) **入侵检测系统（IDS）**

检测算法：验证 IDS 采用的检测算法是否先进，能否准确识别已知和未知威胁，如基于特征码、行为分析、机器学习等方法。

响应时间：测试 IDS 从发现威胁到发出警报的时间间隔，确保其能够在最短时间内采取行动。

误报率：评估 IDS 的误报率，确保其不会频繁产生虚假报警，影响日常运维工作。

3) **防病毒软件**

病毒库更新：检查防病毒软件是否定期更新病毒库，确保其能够识别最新的恶意软件。

实时保护：验证防病毒软件是否启用了实时保护功能，能够在文件下载、执行等关键时刻进行扫描。

全盘扫描：定期执行全盘扫描任务，确保系统内不存在隐藏的恶意程序。

4) **端点安全**

终端防护平台（EPP）：评估 EPP 的功能完整性，如反恶意软件、防火墙、应用程序控制等模块是否齐全且有效。

EDR 集成：检查是否集成了终端检测与响应（EDR）功能，以便在事件发生后快速追溯和修复。

移动设备管理（MDM）：对于携带敏感信息的移动设备，确保部署了 MDM 解决方案，实现远程擦除、加密等安全管理措施。

（3）加密策略审查

1) **敏感数据加密状况**

静态数据加密：检查数据库、文件系统中的敏感数据是否进行了适当的加密处理，如采用 AES-256 等强加密算法。

传输数据加密：验证所有内部和外部的数据传输是否使用了 SSL/TLS 等加密协议，确保数据在传输过程中不会被窃听或篡改。

密钥管理：评估密钥管理方案的有效性，包括密钥生成、存储、分发、轮换等环节，确保密钥生命周期的安全性。

2) **加密实施细节**

加密标准：确认所使用的加密算法和协议是否符合国际标准，如 FIPS 140-2 认证，确保其安全性和兼容性。

加密范围：检查加密是否覆盖了所有必要的数据类型和应用场景，避免遗漏重要信息。

性能影响：评估加密措施对系统性能的影响，确保在保障安全的同时不影响用户体验。

3) **密钥管理方案**

密钥生成：确保密钥生成过程遵循随机性和唯一性的原则，采用硬件安全模块（HSM）或其他可信环境。

密钥存储：检查密钥是否存储在安全的地方，如专用密钥管理系统（KMS），并限制访问权限。

密钥轮换：制定并执行密钥轮换计划，定期更换旧密钥，降低长期使用同一密钥带来的风险。

密钥恢复：建立密钥丢失或损坏后的恢复机制，确保在极端情况下仍能解密数据。

（4）结果呈现

最终输出可以包括以下内容：

技术架构审查报告：详细列出当前技术基础设施的优势和不足，提出改进建议，确保其健壮性和可靠性。

防护工具效能测试报告：汇总各类安全设备的测试结果，分类整理各项指标，提供详细的补救计划和优化建议。

加密策略审查报告：全面评估敏感数据的加密状况及其密钥管理方案，指出存在的问题并提出改进措施，确保数据保密性和完整性。

通过上述方法，可以全面评估到站信息发布系统的数据安全技术风险，识别潜在的技术缺陷和防护漏洞，估计可能造成的损失，并提出针对性的防护措施和改进建议，从而有效提升整体数据安全保障水平。

6.8.6.3.4 个人信息保护风险

（1）隐私政策审核

1） **政策清晰度与透明度**

声明内容：确保隐私声明涵盖了所有必要的信息，包括但不限于：

- **数据收集范围**：明确说明收集哪些类型的个人信息（如姓名、身份证号、联系方式等），以及这些信息的用途。
- **使用目的**：详细描述个人信息将如何被使用，是否用于直接营销、数据分析等，并强调不会超出授权范围。
- **共享安排**：列出可能与第三方分享个人信息的情况，说明分享的原因和方式，确保用户知情同意。

- **存储期限**：告知用户个人信息的保存时间及其依据，如法律法规要求或业务需要。

2) **用户友好性**

语言简洁：采用通俗易懂的语言撰写隐私声明，避免使用过于专业的术语，确保普通用户能够轻松理解。

格式规范：遵循国际标准和最佳实践，如 GDPR 中的透明度原则，使隐私声明易于阅读和导航。可以考虑分段落、列表、图表等方式增强可读性。

多语言支持：如果服务对象涉及不同语言背景的用户，提供多种语言版本的隐私声明，确保信息传达无误。

3) **合规性验证**

法规遵从：对照《中华人民共和国个人信息保护法》（PIPL）、《网络安全法》等相关法律法规，逐条核对隐私声明的内容，确保其符合最新的法律要求。

定期更新：随着法律法规和技术环境的变化，及时更新隐私声明，保持其时效性和准确性。每次重大变更都应通知用户，并记录用户的确认情况。

（2）访问控制评估

1) **用户认证机制**

强身份验证：检查是否采用了多因素认证（MFA）等强身份验证方法，如密码+短信验证码、指纹识别、面部识别等，提高账户安全性。

密码策略：评估密码复杂度要求（如长度、字符组合）、过期时间和重试限制，确保密码难以被破解。

单点登录（SSO）：对于多个系统或应用，考虑实施 SSO 解决方案，简化用户登录流程的同时提升整体安全水平。

2) **授权管理**

最小权限原则：根据员工的角色和职责分配最小必要的权限，避免过度授权。确保权限变更经过严格的审批程序，并有详细的日志记录。

角色基础访问控制（RBAC）：通过 RBAC 模型实现细粒度的权限管理，为每个角色定义具体的权限集，简化管理和维护工作。

动态权限调整：针对临时任务或特殊项目，允许灵活调整用户权限，但需确保调整过程可控且可追溯。

3) **审计跟踪**

操作日志：启用详细的日志记录功能，追踪每一次登录尝试、权限更改和敏感操作，便于事后审计和追责。

异常检测：结合机器学习等技术手段，自动分析日志数据，识别异常行为模式，如频繁失败的登录尝试、非工作时间的操作等，及时发出警报。

定期审查：建立周期性的权限审查制度，定期检查现有权限配置是否合理，发现并纠正潜在问题。

（3）传输合规性

1) **法律框架了解**

国内外法规对比：深入研究中国及目标国家/地区的个人信息保护法律法规，如欧盟的《通用数据保护条例》（GDPR）、美国的《加州消费者隐私法案》（CCPA）等，确保数据传输及跨国界的数据流动符合双方的要求。

双边协议：关注中国与其他国家之间签订的数据保护合作协议或谅解备忘录，了解是否存在简化或优化跨境传输的机制。

2) **合规措施实施**

合同保障：在与第三方合作伙伴签订合同时，加入专门的数据保护条款，明确规定双方的责任和义务，如数据处理方式、安全保障措施、违约责任等。

用户同意机制：确保在传输前获得用户的明确同意，特别是当传输可能导致个人信息权益受到影响时，提供充分的信息披露并取得用户的书面或电子形式的同意。

技术手段：采用加密传输、匿名化处理等技术手段，降低传输过程中个人信息泄露的风险，确保数据在传输和存储期间的安全性。

3) **风险评估与监控**

影响评估报告：针对每次传输活动，编写详细的影响评估报告，分析潜在的风险点和应对措施，作为决策参考。

持续监测：建立长期的数据传输监测体系，实时跟踪传输状态和接收方的行为，一旦发现异常立即采取行动。

应急响应计划：制定专门的应急预案，涵盖从事件报告、损失评估到恢复操作的全过程，确保在发生安全事故时能够迅速、有效地应对。

（4）结果呈现

最终输出可以包括以下内容：

隐私政策审核报告：列出现有隐私声明的优势和不足，提出改进建议，确保其清晰、透明且符合法规要求。

访问控制评估报告：总结用户认证和授权机制的评估结果，指出存在的问题并提出改进措施，确保只有授权人员才能访问敏感信息。

通过上述方法，可以全面评估到站信息发布系统的个人信息保护风险，识别潜在的问题和漏洞，估计可能造成的损失，并提出针对性的防护措施和改进建议，从而有效提升个人信息的安全保障水平，确保其符合相关法律法规的要求。

6.8.6.4 整改建议与指导

6.8.6.4.1 管理层面建议与指导

（1）优化组织架构

设立专职岗位：在管理层中设立信息安全主管领导或数据安全主管领导，负责统筹规划和监督整个组织的数据安全工作，确保其主导地位。

组建跨部门团队：建立由IT、法务、业务等部门组成的联合工作组，定期召开会议，协调解决数据安全相关问题，促进信息共享和技术交流。

明确职责分工：细化各部门及员工在数据安全管理中的具体职责，确保每个环节都有专人负责，避免责任不清或推诿现象。

（2）完善规章制度

修订安全政策：根据最新的法律法规（如《中华人民共和国个人信息保护法》,《中华人民共和国数据安全法》）、行业标准（如ISO/IEC 27001）

以及业务需求，全面修订现有的信息安全政策，确保其内容与时俱进且具有可操作性。

制定操作规范：针对日常工作中涉及的数据处理活动（如采集、存储、传输、使用、共享、销毁等），编写详细的操作指南，明确每一步骤的具体要求和注意事项。

加强合规管理：建立专门的合规管理部门或岗位，负责跟踪国内外法律法规的变化，及时调整内部制度以确保符合最新要求；定期开展合规培训，提高全员的法律意识。

（3）加强人员培训

新员工入职培训：为每位新员工提供必要的信息安全培训，内容涵盖基本概念、政策法规和个人责任等方面，帮助他们快速融入企业文化并树立正确的安全观念。

持续教育计划：制定长期的安全意识提升方案，通过线上线下相结合的方式，定期举办讲座、研讨会、实战演练等活动，保持全体员工的知识更新和技术水平提高。

技术技能培训：针对 IT 技术人员和开发人员，提供专业技能提升课程，如漏洞修复、安全编码实践、应急响应演练等，确保他们在面对新型威胁时具备足够的应对能力。

6.8.6.4.2 技术层面建议与指导

（1）增强防护措施

多因素认证（MFA）：推广使用多因素认证机制，如密码+短信验证码、指纹识别、面部识别等，增强用户账户的安全性；对于高敏感区域，考虑采用生物识别技术（如虹膜扫描）进一步提升验证强度。

更强的加密算法：升级现有的加密策略，采用更先进的加密算法（如 AES-256、RSA-4096）对静态和传输中的数据进行保护；引入硬件安全模块（HSM）用于密钥生成和管理，确保密钥生命周期的安全性。

入侵防御系统（IPS）：部署入侵防御系统，不仅能够检测恶意流量，还能主动阻断攻击行为；结合深度包检测（DPI）技术，深入分析网络流量内容，精准拦截已知和未知威胁。

（2）优化数据治理

数据分类分级管理：建立科学合理的数据分类分级体系，根据数据的重要性、敏感性和影响范围将其划分为不同级别，分别采取相应的保护措施；定期审查分类结果，确保其准确性和时效性。

数据生命周期管理：从数据产生到销毁的全过程实施精细化管理，包括但不限于：

- ✧ **采集阶段**：确保数据来源合法，获取必要的同意授权；采用匿名化或假名化技术减少个人身份信息暴露风险。
- ✧ **存储阶段**：选择合适的存储介质和技术手段，如磁盘阵列 RAID、云存储等，保障数据的完整性和可用性；实施严格的访问控制和加密存储策略。
- ✧ **使用阶段**：遵循最小权限原则分配用户权限，限制数据访问范围；启用详细的日志记录功能，追踪每一次操作行为，便于事后审计。
- ✧ **共享阶段**：与外部合作伙伴签订保密协议，明确数据使用的权利义务；采用安全的传输协议（如 TLS 1.3）确保数据在传输过程中的安全性。
- ✧ **销毁阶段**：制定严格的销毁流程，采用物理粉碎或多次覆写等方式彻底清除不再需要的数据，防止残留信息带来风险。

6.8.6.5 评估报告编制

评估完成出具《网络数据安全风险评估报告》。

6.8.6.5.1 报告结构

包括摘要、正文、结论、附录等部分。

6.8.6.5.2 报告主要内容

管理层面评估结果

- ✧ **组织架构分析**：总结现有组织架构在数据安全管理方面的优势和不足，提出优化建议。
- ✧ **规章制度审查**：列出发现的安全政策和操作规范中的问题，并提供改进建议。
- ✧ **人员培训情况**：评估员工安全意识和技术水平，指出培训效果和需要加强的方面。

技术层面评估结果

- ✧ **物理环境考察**：根据需要描述数据中心、机房等关键地点的安全设施检查结果，提出改进意见。
- ✧ **访问权限审计**：根据需要评估门禁系统、视频监控等设置的合理性，指出存在的问题并提供解决方案。
- ✧ **安全测试与漏洞扫描**：根据需要记录渗透测试、配置审查等技术测试的结果，分类整理各类漏洞，并提供详细的修复方案。

合规性验证

- ✧ **法律法规遵从**：对照最新的法律法规（如《中华人民共和国个人信息保护法》）逐条核对现有措施是否达标，提出调整建议。
- ✧ **行业标准符合性**：参考国际或国内的相关标准（如 ISO/IEC 27001），评估现有措施是否达到了最佳实践水平，提供改进建议。

6.8.6.5.3 结论与建议

综合结论：基于前述各项评估结果，给出总体性的结论，明确当前数据安全状况的优势和主要风险点。

整改建议：针对发现的问题，提出具体的整改措施和实施计划，包括短期应急措施和长期优化方案。

后续跟进：说明评估结束后将继续提供的支持和服务，确保整改措施得到有效落实。

6.8.7 服务频次

数据安全风险评估服务的方式为现场服务，服务周期内对选定的一个信息系统开展一次。

对浦东公交公司的数据安全风险评估工作将安排在合同签订后进行，也可根据公交公司的年度网络安全工作计划进行安排。

6.8.8服务成果交付

服务完成后，提交测评系统的《数据安全风险评估报告》。

七、 项目管理方案

浦东公交网络安全项目涉及联通云信息系统和公司本部，为了确保招标要求所涉及的 8 项安全服务的及时性、有效性和服务的品质，天泰网络为安全项目的管理设计了完善的管理架构、组织保障体系、人员安排和进度管理。

7.1 项目管理策略

为了规范和落实本方案所提出的项目服务目标，确保浦东公交网络安全项目的管理工作落到实处，切实提高浦东公交的网络安全保障能力和保障水平，需制定项目管理策略和指导原则，用于总体上规范和指导浦东公交网络安全项目的管理工作。

(1) 项目管理方针

浦东公交网络安全项目管理的总体方针为：面向目标信息资产，坚持“以人为本”，以提升网络安全管理成效为目标，提高天泰网络项目管理人员和服务人员的网络安全风险意识和主动服务意识，强化网络安全服务和安全产品应用的计划、实施和优化调整，完善安全技术措施，管控网络安全风险，持续开展检查、整改、应急保障和培训指导工作，确保用户网络信息系统安全上一个新的台阶。

(2) 项目管理的原则

浦东公交网络安全项目的信息资产包括机房设施、基础网络、管理信息系统、生产调度系统、日常办公系统等，为了确保上述信息资产的安全运营，要求天泰网络项目管理人员和服务小组、技术专家等项目参与人员遵照“目标明确、责任清晰、主角担责、组员参与、密切配合、优质高效、快速响应、风险管控、持续改进”的原则，通过过程管理、风险控制和质量管理等一切可能的措施，加强项目管理。

(3) 项目的管理机构

天泰网络将针对本项目设立浦东公交网络安全项目领导小组（项目领导决策部门），为项目管理提供决策支持；领导小组下设项目部，负责网络安全项目的日常管理协调工作，由项目经理负责；具体服务科目和安全产品支持由各服

务小组具体完成，各小组设组长或服务科目召集人，成员包括服务工程师、技术支持工程师、辅助人员、商务或行政人员，按照计划，安全专家或高级管理人员参与项目服务的，将临时编入服务小组，支持或协助组长开展工作，完成任务。

网络安全服务工程师作为本项目的工作主体，承担本项目各科目的具体的工作内容，具有明确的不可推卸的义务和责任，应签署项目工作责任书，做到任务清晰，职责到人，奖罚分明。

要求参与本项目的所有工作人员应积极参加项目的各种形式的任务交流、培训教育、评估分析活动，遵守相关国家法律、法规、部门规章和行业规范，遵守本单位和用户方的网络安全管理制度，有效履行项目合同约定的各项责任。

(4) 项目管理的策略

1) 项目过程中协助用户分析目标资产及其计算环境，对存在漏洞、缺陷、隐患和使用不当的应优先进行保护和调整。

2) 通过网络安全设施和软件保护信息的机密性、完整性和可用性，以防止未经授权的不当存取、防止未经授权的篡改，确保合法的使用者需求可以得到满足。

3) 要求项目领导小组和项目负责人（项目经理）时刻关注项目的目标责任，通过培训、交流、会议、沟通、督促和奖罚等综合措施，确保项目部门高效优质完成任务。

4) 建议项目负责人与用户方项目管理人员开展周期性的密切的沟通，对项目实施条件不具备、工作环境不充分、相关人员不配合等不利情况进行交流，并采取有效措施推动解决，对于不能在约定的时间内解决的，必须在双方项目管理会上形成决议、意见或备忘录，以便项目管理的有效进行。

5) 项目部将执行目标管理、质量管理、进度管理、效率管理、保密管理等制度或规定，使得全体工作人员清楚工作要求和工作标准。

6) 项目所有工作人员都有责任及时报告在工作中所发现的可疑事件、警告、故障、隐患或错误操作，提醒和协助相关责任人采取措施，防范网络安全事件或故障的发生。

7) 项目所有工作人员的任何危及用户网络安全和系统正常运行的行为，都应给与对应的处罚程序，严重的将付诸法律制裁行动。

(5) 项目管理目标

最大限度保证项目合同的有效执行，完成或超额完成项目规定的安全服务目标和产品应用指标，项目领导得力，项目成员工作成绩达到良好，无安全服务事故，无明显工作失误，无用户正式投诉，用户方的调查满意度的满意率达到 90%以上，服务团队在服务任务完成后争取得到用户方的书面表扬或充分肯定。

(6) 项目管理策略的相关内容

1) 管理范围。它包括本次项目设计的所有信息、系统、设施、程序、数据、网络、所有的服务技术及工具。

2) 文档分类。应当提供特定内容的定义而不是一般化的“公开”或“限制”。

3) 安全信息处理。用户方需要保密的文件和信息，如管理制度、业务数据、个人信息、合同协议等，这些都可以表述为通用的目标，如“用户的私密信息不应当以明文形式授权给除用户代表之外的任何人，并且仅能用于与用户交流的目的。”

4) 其它管理要求和补充文档的策略布置必须与项目管理策略保持一致。

5) 项目文档包括用于参考的各类文件或文档。例如，流程、技术标准、程序、指南、参考文档等。

6) 项目任务书、责任书应指明具体的确切的责任。

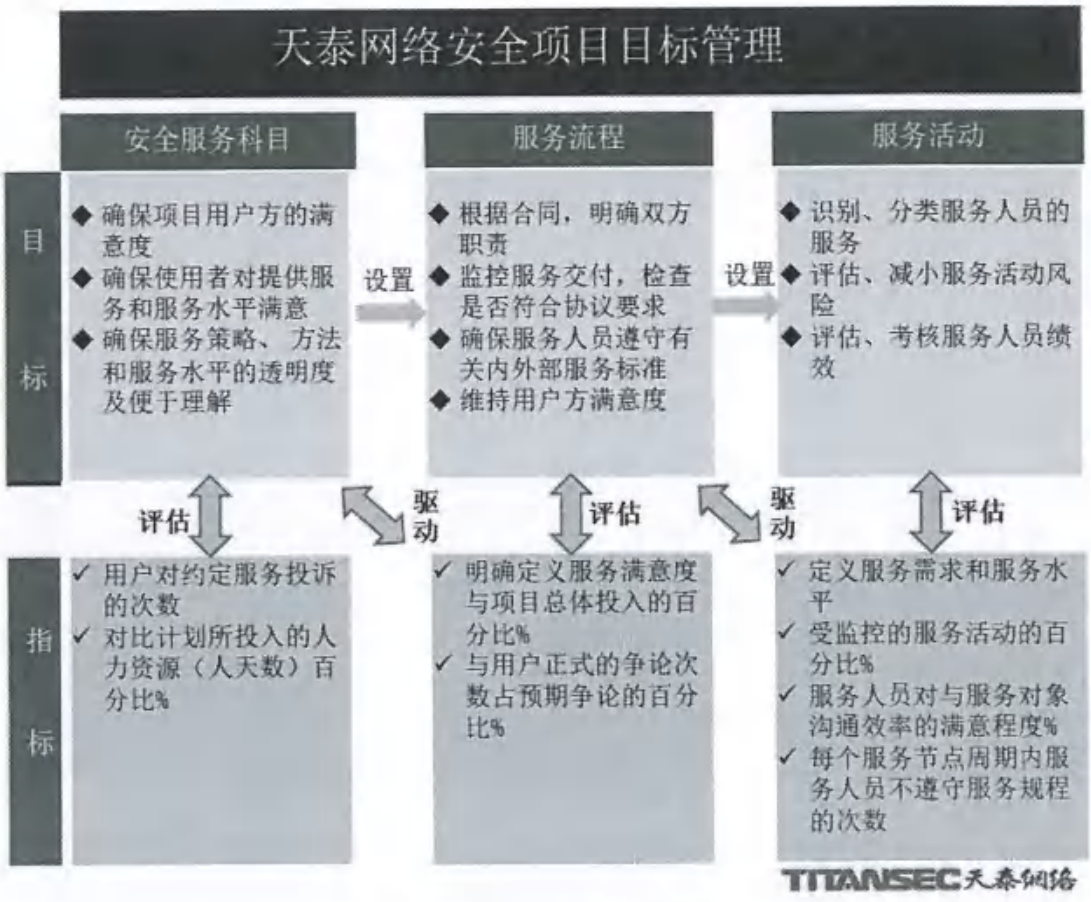
7) 违反规范或制度时所面临的后果（例如：再培训、降级、调离、解聘或合同中止等）。

7.2 项目管理架构

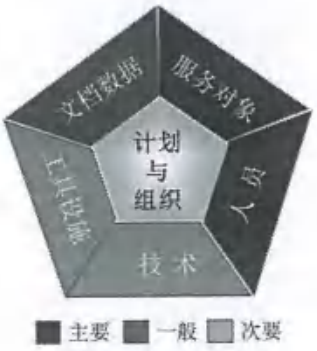
天泰网络安全项目管理采取三层管理模型，项目管理团队由公司负责人、项目经理、专家组成，由项目经理组织开展日常服务工作。项目负责人负责项目决策，审核项目需求与服务计划，确定或修订项目管理制度，明确项目参与人员的岗位与职责。项目经理确认项目任务、时效、质量标准和交付物，制定各服务科目的服务实施计划，给项目组长布置具体工作任务，并明确规范所属下级各组的职责及组间协调关系。

7.3 网络安全项目的目标管理

天泰网络安全项目管理采取目标管理方法，将服务投诉、服务满意度、沟通满意度、受控活动的比例作为管理目标，如下图所示。



天泰网络安全项目目标管理



天泰网络根据项目目标，对项目约定的服务投诉次数、服务满意度、服务争论和沟通效率满意程度进行评估，对评估结果及时反馈到服务人员，以反向激励或约束服务人员更好地开展服务活动。

天泰项目管理计划与组织分为制定服务策略、设计服务架构、制定服务目标、定义组织架构、管理服务投入、沟通目标与方案、人力资源等十一个方面，对项目进行计划管理，管理要素包括高满意度、安全无事故、服务效率、服务功能、系统可用性、服务合规性和系统可靠性等内容，管理的资源包括人员、服务对象、技术、工具设施、

文档数据，对这五种资源按照重要程度分为三类管理。

天泰网络安全项目管理过程与要素

7.4 服务组织架构

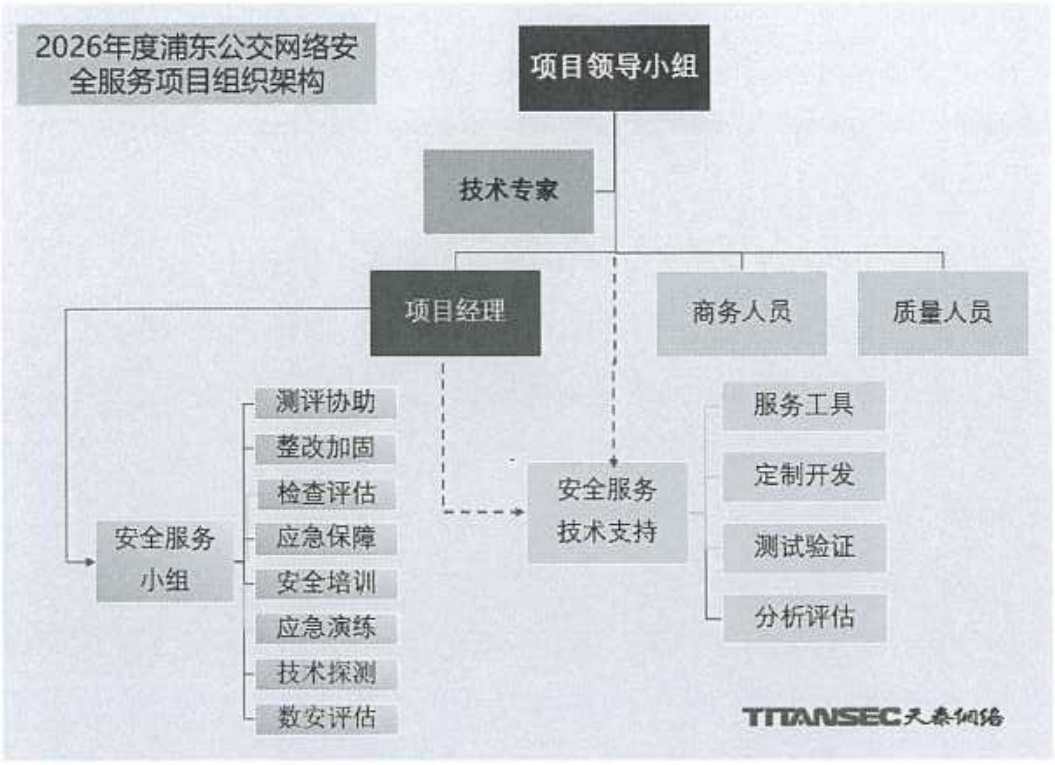
天泰网络将派项目经理参与由用户管理部门牵头的项目管理工作，负责整个服务的进度管理和质量管理，将定期参与项目管理例会，监督服务进度和服务质量，发现并解决出现的问题，并协调各参与单位之间的合作。

服务执行组负责项目的整体执行，实施服务计划；落实服务计划的具体活动内容，按计划推进项目进展，执行项目质量管理要求；配合服务验收工作等。

商务人员负责项目文档、产品、工具等的管理工作，以及专家的协调、会务保障、辅助人员调配等。

质量监督人员根据项目质量管理计划检查项目各科目的进度和质量，以及质量考评、满意度调查、纠纷处理和责任分析，参与项目考评会议和人事考核等。

浦东公交网络安全服务项目组织架构图如下：



浦东公交网络安全服务项目组织架构

7.5 项目组人员岗位设置及工作职责

天泰网络将为本项目成立专项项目服务部，参与整个服务项目的全周期、全过程服务，项目部的主要成员组成如下：

7.5.1 项目经理

项目经理主要工作职责包括：

- 项目组织和决策，并负责与用户方定期沟通项目进展；
- 负责根据项目要求，制定项目方案以及工作计划；
- 负责将服务的成果进行审核并汇总，形成服务总结报告；
- 项目进度与质量控制，对安全检查专项的各项表格、文档进行审核、存档。
- 组织参与重要的服务过程和应急响应处置，协调与项目合作的各方关系。

7.5.2 安全服务小组

安全服务小组的主要工作职责包括：

- 按照网络安全项目计划要求和规范流程，完成各科目的服务任务；
- 组织协调临时工作人员参与安全等保、安全检测、应急保障等现场工作，按时保质完成检查任务，并出具报告；
- 上级专项检查前期开展内部迎检检查配合服务；
- 开展网络安全加固服务；
- 开展应用系统安全检测和 4 次网络安全检查；
- 开展网络安全应急保障服务；
- 开展网络安全应急演练；
- 开展网络风险性技术探测；
- 协助专家、讲师开展网络安全培训工作；
- 开展数据安全风险评估工作；
- 及时报告项目进度和质量，反馈项目服务过程中出现的问题；
- 按要求及时出具服务报告初稿。

7.5.3 安全专家

安全专家的工作职责包括：

- 研究和落实网络安全服务相关的新标准、新方法，设计服务流程和服务规范；
- 对网络安全服务的报告进行审核，并出具审核意见；
- 参与应急响应处置的问题分析，协助解决问题，排查隐患；
- 协助分析安全漏洞，支持系统加固、修补和升级；
- 参与复杂问题的分析和解决，提出安全整改建议；
- 指导安全服务技术相关的工具设计、定制开发和测试验证工作。

7.5.4 商务人员

商务人员的主要工作职责包括：

- 协调项目经理和项目专家的日常沟通工作；

- 负责项目的文档管理，及时提供规格文档，提交并保管核签的文件；
- 参与项目保障和会务安排；
- 安排后勤支持和保障。

7.5.5质量监督

质量监督人员主要工作职责包括：

- 参与项目的日常管理工作；
- 按计划收集项目质量、进度相关的资料、信息；
- 定期开展与质量管理相关的交流、调查、询问、调研工作；
- 开展项目质量管理考核、培训会议；
- 结合项目管理，进行质量分析、评估、考核，参与人事部门的项目考核。

表7-5项目组成员角色与工作任务列表

项目角色	工作任务	拟分配人员
项目领导	确定项目目标 项目整体决策 项目协调与阶段性工作会议	天泰网络总经理担任
项目经理	制定总体方案、服务工作计划及进度控制 报告服务进展情况 向服务相关人员分解并分派项目工作任务 联系并协调客户关系 服务项目质量控制 协调解决项目实施过程中发现的问题 处置服务投诉和纠纷	由具有项目管理资质和经验的项目经理担任
服务小组与安全专家团队	服务小组按照网络安全服务项目计划要求和规范流程，完成各科目的服务任务	服务小组成员由经验丰富、得到用户充分认可的服务工程师担任
	专家参与重要科目和节点的服务工作，把握服务重点，解决疑难为题	专家为从事网络安全工作十年以上在具体专业

	对网络安全服务的报告进行审核，并出具审核意见	上具有造诣的专业人员
商务管理质量监督	协助开展商务支持、质量管理工作，项目人员协调、文档管理、工具管理、质量监督等	质量经理和行政助理担任

7.6 项目服务人员工作要求

7.6.1服务人员的服务目标

天泰网络将根据项目要求安排相应的服务人员为用户提供各项安全服务工作。

针对项目合同确定的服务内容，明确服务需求，天泰网络为用户提供全面、可靠的安全服务，以发现目标系统的安全风险、配合系统等保测评、开展应急演练、安全培训、数据安全风险评估，保障浦东公交公司应用系统、主机和终端的安全性、可靠性和可用性，最大限度降低系统的安全风险，提高网络安全服务保障能力。

根据用户管理部门服务项目的要求，安全服务工程师将遵循网络安全服务规范和流程，结合天泰网络安全服务团队的分工安排，负责或参与或支持安全检测、安全整改、事件处理、应急响应、培训服务等服务活动，配合服务团队有效完成项目的服务任务。

7.6.2服务人员的能力要求

服务人员的能力要求：

(1) 服务人员应具有把握国家网络安全法规政策，理解和掌握相关安全技术标准，熟悉安全服务的方法、流程和工作规范，有依据安全服务规范完成服务任务并出具安全工作报告的能力；

(2) 服务骨干人员应通过指定机构的专业培训并取得相关认证证书；

(3) 服务人员应接受过多种形式的技术培训；

(4) 对服务人员周期性地开展任职经历、履职能力进行审查评估。

7.6.3服务人员的工作要求

服务人员的工作要求：

(1) 根据合同要求，开展网络安全检测、网络安全等保等服务工作；

(2) 开展网络安全事件监控和应急响应处理；

(3) 根据发现的网络安全隐患报请安全管理负责人分析研判，选择合适的方式进行处理；

(4) 以最快的方式响应用户的紧急安全事件，将损失或影响降到最小；

(5) 在网络安全服务科目（如安全整改、配置调整、漏洞修复等）完成之后，监测相关系统或业务的有效性、完整性和稳定性；

(6) 为用户提供安全咨询或安全警告提示，提高安全管理或安全防范能力；

(7) 根据用户方的要求安排工作时间，并参与用户方安排的加班、值班、临时值守等工作，接受天泰网络的日常管理和服务考核。

7.7 人员管理机制

一、总则

为规范公司人员管理，打造高素质、高效率的员工队伍，维护公司与员工的合法权益，依据国家相关法律法规，结合公司实际，特制定本制度。本制度适用于公司全体员工的管理。

二、人员招聘与录用

（一）招聘需求确定

各部门根据业务发展和岗位空缺情况，填写《招聘需求申请表》，详细说明招聘岗位名称、岗位职责、任职要求、招聘人数等信息，经部门负责人和公司管理层审批后，提交至人力资源部。

（二）招聘渠道选择

人力资源部根据招聘岗位特点和需求，选择合适的招聘渠道，如网络招聘平台、校园招聘、人才市场招聘会、内部推荐等，发布招聘信息。

（三）简历筛选与面试

简历筛选：人力资源部对收到的简历进行初步筛选，将符合基本要求的简历推荐给用人部门。用人部门进行二次筛选，确定参加面试的人员名单。

面试组织：人力资源部与用人部门共同组织面试，可采用初试、复试等多轮面试方式。面试过程中，全面考察应聘者的专业知识、工作技能、综合素质等。对于关键岗位，可引入背景调查环节，确保应聘者信息真实可靠。

（四）录用与入职办理

录用：面试结束后，人力资源部和用人部门根据面试结果，综合评估应聘者的能力和素质，确定录用人员名单。经公司管理层审批后，向录用人员发送《录用通知书》。

入职办理：录用人员在规定时间内办理入职手续，提交身份证、学历证书、资格证书等相关资料。人力资源部为新员工办理入职登记，介绍公司基本情况、组织架构、规章制度等，发放办公用品，并安排新员工与用人部门负责人及同事见面。

三、人员培训与发展

（一）培训需求分析

人力资源部每年定期组织各部门进行培训需求调研，通过问卷调查、面谈、绩效评估等方式，了解员工的培训需求和职业发展规划，结合公司战略目标和业务需求，制定年度培训计划。

（二）培训课程设计与实施

内部培训：针对公司内部员工的共性需求，如文化、规章制度、职业素养等，由人力资源部组织内部培训讲师进行授课。对于专业技能培训，可邀请业务骨干或外部专家进行培训。

外部培训：根据员工的职业发展需求和公司业务需要，安排员工参加外部培训机构举办的培训课程、研讨会等。参加外部培训的员工需与公司签订培训协议，明确培训费用的承担方式和服务期限。

（三）培训效果评估

培训结束后，人力资源部通过考试、问卷调查、现场评估等方式，对培训效果进行评估。了解员工对培训内容的掌握程度和对培训组织的满意度，总结培训经验，不断改进培训工作。

四、考勤与休假管理

（一）考勤管理

考勤方式：公司采用打卡考勤对员工进行考勤管理。员工应按时打卡，不得迟到、早退、旷工。

考勤统计：人力资源部每月对员工的考勤情况进行统计，将考勤结果与员工的绩效奖金、工资发放等挂钩。对于迟到、早退、旷工的员工，按照公司规定进行相应的处罚。

（二）休假管理

休假类型：公司员工享有法定节假日、年假、病假、婚假、产假、陪产假、丧假等休假权利。

休假申请与审批：员工申请休假时，需提前填写《休假申请表》，注明休假类型、休假时间、工作交接情况等信息，经部门负责人和公司管理层审批后，交人力资源部备案。

五、绩效管理

（一）绩效指标设定

每年年初，公司根据战略目标和业务计划，将绩效目标分解到各部门和岗位。部门负责人与员工共同制定个人绩效指标，明确工作目标、考核标准、权重等内容，签订《绩效目标责任书》。

（二）绩效评估实施

评估周期：公司采用月度、季度或年度相结合的方式进行绩效评估。月度或季度评估主要用于对员工工作进展的跟踪和反馈，年度评估作为员工绩效奖金发放、晋升、调薪的重要依据。

评估方法：绩效评估采用定量与定性相结合的方法，包括工作业绩、工作能力、工作态度等方面的评估。评估过程中，上级领导、同事、下属和用户等可参与评估，确保评估结果客观公正。

（三）绩效反馈与改进

绩效评估结束后，上级领导应与员工进行绩效反馈面谈，肯定员工的工作成绩，指出存在的问题和不足，共同制定绩效改进计划。员工对绩效评估结果有异议的，可在规定时间内向人力资源部提出申诉。

六、薪酬与福利管理

（一）薪酬管理

薪酬结构：公司实行基本工资 + 绩效工资 + 奖金 + 津贴补贴的薪酬体系，根据员工的岗位价值、工作绩效、市场行情等因素确定员工的薪酬水平。

薪酬调整：公司每年根据员工的绩效表现、市场薪酬水平变化等情况，对员工的薪酬进行调整。薪酬调整包括晋升调薪、绩效调薪、岗位变动调薪等。

（二）福利管理

法定福利：公司按照国家法律法规的规定，为员工缴纳养老保险、医疗保险、失业保险、工伤保险、生育保险和住房公积金等法定福利。

公司福利：公司为员工提供节日福利、生日福利、健康体检、带薪年假、团建活动等公司福利，增强员工的归属感和凝聚力。

七、人员离职管理

（一）离职申请

员工因个人原因申请离职时，需提前向部门负责人提交《离职申请表》，说明离职原因、离职时间等信息。部门负责人应与离职员工进行面谈，了解离职原因，做好挽留工作。

（二）离职审批与交接

离职审批：《离职申请表》经部门负责人、人力资源部和公司管理层审批后，员工方可办理离职手续。

工作交接：离职员工应在规定时间内与接手人进行工作交接，交接内容包括工作资料、用户信息、办公用品等。交接完成后，双方签字确认。

（三）离职结算

人力资源部在员工办理完离职手续后，核算员工的工资、奖金、福利等，进行离职结算。同时，为员工办理社保、公积金等关系转移手续。

八、附则

本制度由公司人力资源部负责解释和修订。本制度自发布之日起施行。公司以往发布的有关人员管理的规定与本制度不一致的，以本制度为准。

7.8 网络安全服务业务流程管理

天泰网络对每个服务科目有针对性的进行服务业务和管理流程设计，根据

项目特点和安全科目的服务流程，关联部门、人员、服务活动、业务流、管理数据、工作职责、过程文档要求在一张流程图上进行规划和描述，服务科目的业务执行人员和管理辅助人员根据服务流程图形成相互合作、相关支撑。

7.9 安全文明措施与承诺

天泰网络针对浦东公交公司安全服务实施安全文明管理措施与承诺：

(1) 天泰网络具备上海市和行业管理部门规定的在本市进行网络安全服务所需的资质、资格，由此引起的所有有关事宜及费用由上海天泰自行负责。

(2) 天泰网络在提供服务期间为确保服务区域及周围环境的整洁和不影响其他活动正常进行，天泰网络严格执行国家与上海市有关安全文明施工管理的法律、法规和政策，积极主动加强和落实安全文明施工及环境保护等有关管理工作，并按规定承担相应的费用。若违反规定而造成的一切损失和责任由天泰承担。

(3) 天泰网络在项目实施期间，将遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度、安全用电、高空作业和网络信息系统设施安全操作等制度，确保杜绝各类事故的发生。

(4) 建立健全安全生产工作责任体系和组织管理网络，建立安全作业监管制度，安排项目经理对施工作业安全进行现场监督；按照“横向到边，纵向到底”责任制要求将安全责任分解，天泰网络的法定代表人与项目管理部、项目经理必须签订安全协议书，明确现场施工安全员，检查汇报安全文明作业的情况，发现问题及时纠正；定期召开安全生产工作会议；组织开展安全作业检查。

7.10项目应急预案管理

(1) 天泰网络根据本项目的突发事件进行应急管理，落实应急预案执行预警和预防机制、应急响应措施、临时设备组织方案、保障措施（包括应急人员、物资、备用设备、资金等）等内容。

(2) 公司分管领导负责项目的应急管理，并落实各部门职责和相关措施。

(3) 与用户管理部门和应急保障支持单位建立联动机制，如过程中发生重特

大网络安全事故、当值服务人员出现意外、服务工具故障、服务系统崩溃等，天泰网络将快速组织专业力量，及时赶到事件现场，实施应急处置，并协同有关单位和部门做好善后处理和系统恢复工作；在人员方面安排 AB 角，可随时替补。

(4) 组建天泰应急保障队伍，一旦紧急事件或重大故障发生，相关的技术专家和核心技术骨干应在最短的时间到达现场进行应急处置。

(5) 定期检查安全服务工具、服务平台、保障物资与设备、器具，确保物资储备数量充足、机具设备完好可用。

7.11 项目实施进度安排

7.11.1 项目实施阶段

本项目实施周期为 1 年时间（将一年分为 4 个季度 12 个月，季度用 4Q 标识，12 个月用 12M 标识），项目实施计划包括服务工作的准备、服务工作的实施、服务工作的总结和验收等。按照项目的要求和时间安排，项目实施总体划分为三个阶段：

（1）服务准备阶段

主要工作内容有：签订服务合同；组建项目部和项目组，建立服务工作场地；服务场地准备；召开项目启动会议；组织施工计划评审，参加项目交底会，进行服务准备；根据服务计划，编制实施性服务组织设计及详细服务进度计划（精确到每个人 P 和每周 W、每天 D）；报送服务科目开工报告，到用户管理部门备案；与其他相关专业机构协调和配合；按照项目总体管理方案，组织项目分项管理队伍，落实针对性的管理流程。

（2）服务实施阶段

本阶段进行的主要工作有：依据服务组织设计及各阶段服务进度计划要求，进行本项目科目的服务实施；按照服务进展情况，实时记录服务过程数据和报告范式数据；制订培训计划并开展培训工作；按服务要求进行服务科目的实施，保证服务达到质量要求；按服务节点进行服务成效的检验，确保服务达到计划要求。

对未达标或未按规范实施的服务科目，及时进行调整、补充和返工。

对服务条件不具备或相关资源未及时配备的，由项目经理与相关方进行协调解决，当项目进入紧迫期或临界点时，项目经理应发起项目进度协调会，在决策层讨论并解决问题，若因协调解决未果，则应将此事作为项目重大问题书面汇报，并通报用户方主管领导。

（3）服务验收及后期阶段

项目初验资料准备，初验审核，按照要求进行服务的验收（阶段性验收和竣工资料）；进行部分服务工作交接。服务后期包括服务业务的交接、质量保证期及质量保证期后的持续服务工作；制订服务回访计划，并按计划回访。

7.11.2 项目服务周期

本项目服务周期为 1 年。项目服务起点以中标后项目合同签订起计算，具体时间以招标人通知为准。

按照服务科目的时间延续特点，将浦东公交网络安全项目的科目分为可计划的安全服务和触发式的安全服务，可计划的安全服务包括单次性服务科目和多次性服务科目，触发式服务是服务时间不可提前安排的具有随机性的服务，如应急响应服务和安全专项检查的迎检服务。

项目总周期为 1 年，项目从合同签署开始到验收通过结束。

7.11.3 服务实施总体进度计划

天泰网络项目部根据项目制定的指导性实施管理计划，依照合同约定组织本项目实施和管理。

项目实施进度总计划见：项目实施进度总计划表 6-10-3。

以项目合同签署后计算项目进展，Q1、Q2、Q3、Q4 分别代表四个季度，M1、M2、M3…分别代表服务的第一个月、第二个月、第三个月……。

表 7-10-3 项目实施进度总计划表

编号	服务名称	服务频次	开始时间	持续周期
P1	网络安全等保服务	1 次	Q1M1	8 周
P2	网络安全加固服务	1 次	Q1M1	1 年
P3	网络安全检测-应用系统整	6 次	每 2 个月 1 次	1 年

	改与复核			
P4	网络安全检测-直属机构检查	4 次	每季度 1 家	1 年
P5	网络安全应急保障	触发式，不限次数	不定	不定
P6	网络安全培训	5 次	Q3M1，Q4M1	4 周
P7	网络安全应急演练	1 次	Q4M2	3 到 4 周
P8	网络风险技术性探测	1 次	Q1M3	3 周
P9	数据安全风险评估	1 次	Q1M3	6 周

7.11.4 项目进度管理

项目进度管理的主要目的是在本次服务项目过程中管理、执行和控制项目进度提供管理依据和方法。

规划进度管理：输入---项目管理计划、项目计划大纲；

输出---项目进度管理计划。

进度管理计划规定：

- 模型。本项目进度模型采用进度临界控制法，并配置相应的动态进度表格。
- 准确度。需要规定服务活动持续时间估算的可接受区间，一级测量时间的人时数、人天数或人周数；用于计量数量的科目点数。
- 组织程序链接。工作分解结构为进度管理计划提供了框架，保证了与估算及资源计划的协调一致。
- 项目进度模型维护。需要规定在项目执行期间，将如何在进度模型中更新项目状态，记录项目进展。
- 控制临界值。可能需要规定偏差临界值，用于监督进度绩效。它是在需要采取某种措施前，允许出现的最大偏差。本项目用偏离基准计划中的参数的某个百分数来标识。
- 绩效测量规则。需要规定用于绩效测量的管理规则或其他测量规则，本

项目以进度基准计算偏差，正偏差考核管理人员，负偏差管理实施人员。

7.12 售后服务计划

天泰网络将为本项目配置高素质的安全服务团队，服务团队核心成员均具备 3 年以上网络安全服务经验，持有 CISAW、CISP、DSO 等专业认证证书，熟悉常见应用系统、操作系统、数据库、中间件的漏洞特性，能够快速响应浦东公交网络安全需求，应对各类突发的安全风险。

配备的安全培训服务支撑团队，具有多年的网络安全意识培训、网络安全技能培训经验，多次为浦东新区党政机关、企事业单位提供网络安全培训，提供的培训内容贴近实际工作需要，既有最新政策法规的解读，也有流行攻击的分析与防御对策介绍，可为按需为浦东公交工作人员提供专业的网络安全知识供给。

配备的安全演练服务支撑团队，深耕网络安全应急演练的各项场景，熟悉各类用户的网络、应用现状，可提供包括桌面推演和实战对抗的多种演练模式，满足从搭建演练环境到保障演练活动开展的全过程支撑。

7.13 项目售后服务承诺

为了高效、高质达成本项目的预期效果，天泰网络对项目售后服务郑重承诺如下：

（1） 服务质量承诺

天泰网络承诺项目服务、售后团队均为具备网络安全专业资质的技术人员，严格遵守浦东公交网络、数据安全各项管理规定，遵守服务现场管理要求，严格保守工作中知悉的信息，包括服务器信息、业务系统信息、漏洞信息及相关数据，服务人员全部签署保密协议，不泄露上述任何信息，所有服务操作均留存记录，形成服务报告。若因服务失误导致业务中断、数据泄露等损失，天泰网络将承担相应责任，并按合同约定进行赔偿。

（2） 响应时效承诺

服务期内，建立 7×12 小时售后服务热线及专属对接群，确保浦东公交的安全诉求能够得到快速响应：针对一般咨询类问题，30 分钟内响应答复；如发生安全事件一般事件 1 小时内响应，重要事件 30 分钟内响应，开展应

急响应处置。

（3） 安全保障承诺

服务期内，不定期提供国内外最新安全态势信息，推送最新流行的网络攻击信息，并提供针对性的安全防护建议；重要时期关键节点（如两会、五一、国庆、进博会等）或主管单位例行检查时，提供网络安全专项保障。

（4） 漏洞跟踪承诺

针对安全检测发现的各类漏洞，服务团队将会全程跟踪紧急高危漏洞整改过程，指导解决漏洞修复过程中遇到的技术问题，跟踪整改进度，漏洞整改修复完成后，及时开展整改有效性验证，确保漏洞得到真实修复。

天泰网络将严格贯彻“持续保障、高效响应、精准处置”的安全服务理念，落实各项服务内容，以高效、优质的服务为浦东公交网络安全保驾护航。

7.14项目的其他要求

项目中标后浦东公交有权要求我司在15日内提供产品、服务工具及相关资质原件，以验证是否满足本项目需求，如我司无法响应或虚假响应的浦东公交可作废中标资格。

八、 质量保障措施与承诺

8.1 质量保证原则

天泰网络确保本项目服务质量的原则有：

- 对问题做出预见性分析，提供预测和完善建议；
- 根据实际情况采取电话、远程诊断和现场服务的方式及时解决各种突发的技术问题；
- 提供用户咨询服务，对用户在服务过程中遇到的问题，提供解决方案或改进的手段；
- 对提供的服务提供完备的支持，并对用户与系统相关的内容提供必要的服务；
- 以服务满意度、服务规范性、服务投诉率为评估指标，衡量服务质量；
- 服务过程可监督、可管理、可追溯，从而保证服务的质量。

8.2 服务策略与质量指标

服务标准化：基于 ISO9001 质量控制体系的技术服务标准，形成标准化的服务流程，标准化的追诉制度，标准化的文挡管理，标准化的能力评估等。

服务体系化：建立全面服务体系，让用户在最短的距离感受到优质的服务。

服务多样化：在计划、执行、总结阶段，倡导基于用户满意度为 100%的个性化服务；满足用户标准化服务以外的特殊需要。

服务主动化：定期交流访问制度，针对用户问题比对历史案例，提出预先解决方案，并保证服务在短时间内到位。

8.3 保密措施

项目保密措施与保密承诺如下：

- 重视项目的安全保密工作，针对具体的项目指派安全保密工作的负责人。

- 依据保密管理制度，定期对工作人员进行保密教育，安全服务人员应当保守在安全服务活动中知晓的国家秘密、工作秘密、商业秘密和个人隐私。
- 明确岗位保密要求，规定其应当履行的安全保密义务和承担的法律责任，并由保密负责人针对性地开展检查工作，杜绝泄密行为。
- 凡是接触到用户方重要信息、敏感信息或个人信息的，在服务过程中接触到的系统数据、管理信息和安全数据的，均要签署保密协议，对保守用户方的信息做出承诺，承担相应的义务。
- 采取技术和管理措施来确保服务过程中相关信息的安全、保密和可控，这些信息包括被原始资料文档、服务活动中生成的数据和记录、以及相应的分析评估报告。

8.4 服务人员与服务资源相关的承诺

天泰网络针对本项目服务人员与服务资源相关的承诺：

(1) 天泰网络具有中国网络安全审查认证和市场监管大数据中心技术颁发的安全评估和安全运维服务资质；

(2) 委派具有 8 年以上网络安全工作经验，具备专有云、交通行业项目管理经验、项目协调能力强的资深项目管理人员担任该项目经理，全权协调和管理本项目的服务业务；

(3) 服务支撑团队不低于 8 人，其中大部分具有 CISP、CISAW、DSO 等专业安全认证工程师等资质证书；

(4) 项目经理和安全骨干人员保持稳定，如有人员变动，将提前一个月通知甲方，接替人员应获得用户管理方的认可；

(5) 服务人员能及时、准确的解决安全服务中遇到的技术问题；

(6) 实行 5×8 小时电话(021-50391981；50391982；4006786569)支持服务；

(7) 7×24 小时在线 400 电话（4006786569）答疑支持服务；

(8) E-mail(support@titansec.com.cn)服务；

(9) 服务质量管理员：熊微，电话：185-1652-3286。

天泰网络在项目服务过程中，承诺为用户提供专业、高效的服务支撑，并

在项目计划的各阶段实行服务监督和公司层面的资源保障，力争为本项目提供最优质的服务。

8.5 服务响应时间承诺

天泰网络针对本项目服务响应时间的承诺：

(1) 针对系统上线、应用系统迁移等业务开通和变更，天泰网络安全服务人员将及时开展安全检查服务；

(2) 重大故障和关键故障、重大和特大安全事件发生时，值守的应急响应服务人员将在 1 小时内到达现场；其他相关的应急处置人员、技术专家队伍应在 2 小时内到达现场。

8.6 质量监控与处罚措施

天泰建立了完备的服务质量监控体系，加强服务项目的管理，从主动监控和被动监控两方面进行服务质量的控制。主动监控为项目质量管理人员主动联系用户项目管理人员和项目合作人员，通过咨询调查，发现问题，及时督促改进。被动监控主要是建立投诉专线，并借助成熟的公司级客户交流体系进行监控。

天泰的服务监督电话是：021－50391982，400-678-6569，当本项目的服务人员在服务过程中接到用户投诉，将根据给用户带来的实际损失和影响对责任人给与惩处。

对在服务过程发现的违反操作规定、泄露用户秘密、工作失误造成损失的，根据管理制度给与处罚或纪律处理，情节严重的依法处置，有关网络安全服务的具体处罚措施参见天泰网络与信息安全服务责任管理制度。

8.7 服务手册及归档资料的记录与移交

8.7.1 服务手册与归档资料

天泰将针对本项目建立专门的安全服务手册、服务归档资料库，并设定 VIP 权限，包括用户对服务支持的要求、服务类别、产品类别型号、工具和系统使

用情况、每次服务支持解决问题的情况、需要进一步研究或解决的疑难问题等信息，都将保存在档案中，以便有针对性地提供深层次的服务与技术研讨。

在每次完成安全检查、安全整改、应急保障等服务后，要求将安全活动记录、安全态势分析、事件处理过程、系统的状况以及由于安全事件而改变的系统参数或对系统做的任何操作都会记录在支持档案中，并同时提交报告给用户作为服务留档保存。

对服务手册和项目文档的管理保存分为电子和纸质两类，原则上应以电子方式保存。电子文件应尽量转换成 PDF 格式，统一设置为“不能修改”模式，并视需要设置为“不能打印”模式；应确保相关电子文档无病毒感染。

文档管理员应按对项目文档进行清点，若发现有关清单和文档不符合归档规范要求的，文档管理员有权要求对文档重新进行编制和完善，直至符合归档规范。

项目组文档管理员对项目文档、服务手册实施统一保管，并负责定期进行刻盘备份，保证归档项目文档的安全可靠。

对可能属于交叉分类的文档，文档管理员应征求文档创建人和项目经理的意见，可对同一文档进行两类管理，但对文档必须进行说明，说明文档属于同一出处，应同步修订更新。

8.7.2 资料移交

服务验收阶段，建立服务工作结束时的移交计划，明确移交的工具、安全服务管理权限（用户名、口令或认证介质）、档案资料、服务数据等，成立移交工作小组，按计划完成移交任务，并以移交工作确认清单签核确认为结束标志。

（1）天泰网络对移交的文档承诺如下：

1) 包含安全检查、安全整改相关的技术方法和甲方需要的过程文档；
2) 分析安全产品故障、安全事件发现的来源，提升故障预警和安全事件预测的能力，提升安全预警预测的能力和覆盖率；
3) 例行操作的意外处置，对例行操作可能出现的意外进行记录，包括渗透测试、应用评估、安全模块变更上线、配置调整等；

4) 权限点，需要进行相关权限的交接和清理工作，尤其是权限的删除需要前置进行，避免系统和权限耦合太深；

5) 风险点，尽可能的将系统存在的各种风险问题进行罗列；

6) 资产盘点，对安全设备、配置、地址、域名、端口、软件版本等资源进行盘点确认；

7) 其他用户方认为需要交接的内容。

（2）交接工作和交接文档的管理协调项如下：

1) 交接期间人员分工明确、责任到人；

2) 交接时间双方商议确定；

3) 交接文档的交付以用户方交接负责人确认为准；

4) 交接效果的验收方法；

5) 上下游交接的约定和规则以及交流和通报机制。

九、 合理化建议

9.1 从攻击方视角看浦东公交服务网的安全弱点

从网络攻防演练对抗中进行分析，攻击方是有组织的攻击队伍，会针对目标系统执行多角度、混合性、对抗性的模拟攻击。以攻击方的视角来看防守方常见的弱点：

1) 系统弱点之：弱口令及同口令

弱口令、同口令历来都是利用难度最低、危害最大、出现频率最高的脆弱点。实战中通过弱口令获得权限的情况占比高达70%以上。另外，有些系统密码复杂度虽然高，但是所有服务器的密码设置相同或者有规律，这种密码也极易被抓取后来进行猜解、爆破。

2) 系统弱点之：漏洞

除常规漏洞外，往往在演练前期所暴露出的“新鲜”漏洞，都会成为攻击方重点关注的方向。例如Weblogic反序列化漏洞、Gmail邮件系统、OA系统等暴露出的漏洞。这些系统和组件在许多党政机关的系统中都有运用。

3) 系统弱点之：集权类系统安全隐患

集权类系统一般会成为攻击者在攻击时所打击的主要目标。拿下集权类系统，可以获取对其所属管辖范围内的所有主机控制权。这些集权系统包括域控服务器、运维管理系统、堡垒机、运维终端、单点登录入口和认证系统等。

4) 攻击手法之：旁路攻击渗透

如果正面攻击有困难，则攻击方可能通过旁路迂回渗透。例如一个国企单位，其业务系统按照行政属性进行三级架构部署，只要敲开任意一个防守薄弱的门，就可以通过内网，逐步访问到企业中心的核心业务系统。

5) 攻击手法之：社工攻击

当攻击方发现系统侧防护严密，通常会把思路转向到对人的攻击。通过钓鱼邮件等攻击方式来对国企职员进行钓鱼，一旦控制了相关员工计算机，攻击方可直接进入到国企单位内网，以终端为跳板向关键业务系统攻击。

6) 攻击手法之：秘密渗透与多点潜伏

攻击方会实施精细化的攻击，甚至编写可以绕过防护设备的代码来实施攻击操作。所以只依靠签名规则告警的监测手段，无法感知到入侵，导致在攻击发生的很长一段时间内，攻击者不仅拿到了系统权限及数据，而且建立多个打通内外网的据点来做权限维持和战果扩大。

9.2 如何进一步做好安全防护工作

首先，最重要的是建立系统的控制力，对于系统的资产情况、安全状态要有明确的认知，并且有针对性的对缺陷或漏洞进行加固和修补。

其次，要有体系化的组织，要全面合理地部署职责明晰、覆盖全面的安全专职队伍，并要有对应能力的人员匹配到相应岗位，技术人员应当具备攻防理论、威胁分析、应急处置等能力。

最后，要解决工具问题，要保证所有流量可见、全量日志可查、有可靠的情报输入，只依靠传统防护设备的被动防护是远远不够的。

建议尝试以下防护方法：

1) 攻击面收敛

“点的突破”会加大以面防守的难度。对外暴露的资产越多，安全工作开展越困难。这就要求用户方必须充分了解自己的资产情况,即使一个不起眼的API 接口都会成为黑客攻击的入口。

要定期梳理网络边界、可能被攻击的路径，尤其是多级网络架构的单位和外联接入的单位。如果正面攻击不成，攻击者往往会选择攻击下级单位、供应商等与目标系统有业务连接的机构，通过这些机构绕至目标系统内网。

2) 防突破和内网横向渗透

一旦外层防线被撕破，攻击者会迅速进行内网横向移动，如果没有纵深防御体系，攻击方将如入无人之境。战争中的纵深防御理论同样适用于网络防护，内外部访问控制（安全域之间，甚至每台服务器之间）、主机层防护、重点集权系统防护、无线网络防护甚至物理层面的防护，都需要考虑。同时要加强内部的监测手段，从网络流量，主机日志、进程、文件等层面进行排查。

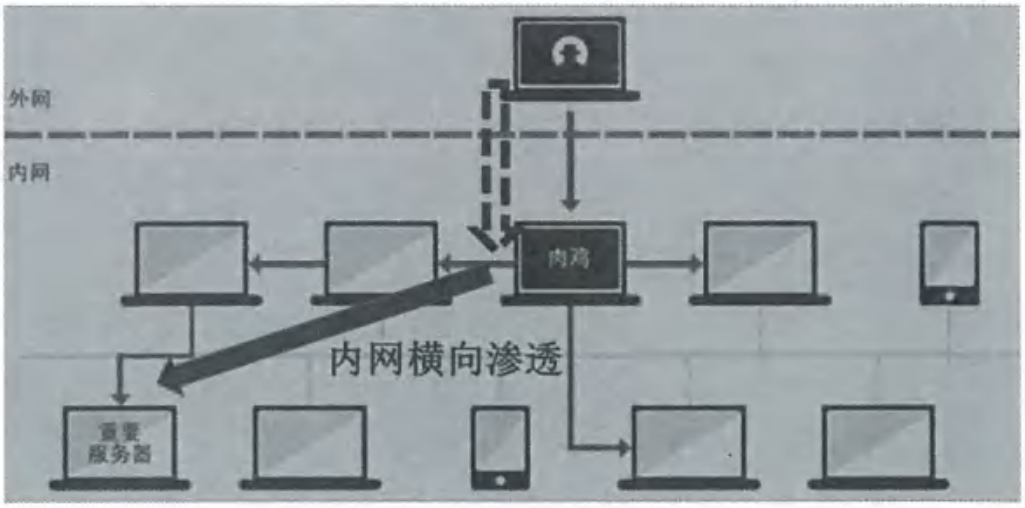


图 9-2 内网横向渗透攻击

3) 目标系统重点把守

核心目标系统是攻击方的最终目标，是整个系统的大本营。对关键系统进行定期的评估检查、渗透测试、整改加固是必要的，同时要保持安全监测工作的常态化开展。

4) 全方位安全监控

攻击者会尽量隐藏痕迹，而防守者恰好相反，需要尽量提前发现攻击痕迹，并通过分析攻击痕迹，调整防护策略、溯源攻击路径，所以建立全方位的安全监控体系是安全防护的最有力武器，监控工作应当从网络层面的全流量监控、主机监控、日志监控、情报监控等多个维度开展。

9.3 重视供应链的安全管理

管理浦东公交供应链中的网络安全风险是一个复杂而多维的任务，建议从多个方面入手：

1）建立全面的供应链安全计划：浦东公交可以制定并实施一个全面的供应链安全计划，涵盖人员、流程和技术三个方面。在人员方面，实施强制性培训计划以增强干部职工的安全意识，并设计桌面演练以确保事件响应协作。在流程方面，调整政策和标准，纳入标准化的安全控制，并对供应商进行风险评估、分级和持续监控。技术方面，开发和实施供应链控制塔，利用实时数据提供网络安全指标，并采用 DevSecOps 将安全整合到软件开发和运营的每个阶段。

2）供应商安全管理：浦东公交可以建立供应商安全管理计划，包括识别关

键供应商、采取基于风险的方法、实施供应商保证过程、评估和监控供应商关系等。此外，浦东公交应定期检查现有供应商，进行网络安全审计、渗透测试和漏洞评估，以确保供应链的完整性和业务的安全性。

3）采用行业标准和最佳实践：企业应遵循如 NIST 800-161、NCSC 原则和 ISO 28000 等标准和最佳实践，以确保供应链的安全性。这些标准提供了从信任到验证的过程，以及如何评估和管理供应链中的风险。

4）加强数据保护和身份验证：在供应链中，数据保护措施和身份验证技术的支持至关重要。浦东公交可加强对供应链的安全管理，评估潜在风险，并采取有效的安全措施，以确保供应链的安全稳定。

5）持续的风险评估与监控：浦东公交应定期进行网络安全风险评估，识别供应链中的潜在风险，并采取科学有效的防护策略。此外，浦东新区建交委应建立多层次防御机制，加密通信，强化身份验证，并进行安全意识培训。

6）承包商的责任：在涉及浦东公交业务合同的情况下，各类承包商需承担网络安全供应链风险管理的责任，定期识别、评估、监控和缓解相关风险，并在浦东公交要求时提供合规文件。

通过以上措施，浦东公交可以有效地管理供应链中的网络安全风险，保护其信息和资产不受威胁，从而实现业务的持续增长和成功。

十、 技术部分和投标报价之间的相符性

本项目投标报价严格对应技术部分的所有服务内容及要求，项目技术方案设计做到真实可落地，服务工作报价与服务价值对等。

1.报价与服务内容相符：投标报价已全面覆盖本项目要求的各项服务内容，包含网络安全等保服务、网络安全加固服务、网络安全检测、网络安全应急保障、网络安全培训、网络安全应急演练、网络风险技术性探测、数据安全风险评估的全部服务成本，无任何服务内容与报价脱节的情况。

2.报价与服务流程相符：报价包含各服务项目全环节成本，涵盖前期筹备、自动化+人工检测、人员值守、培训材料、演练环境等所有步骤，其中工具采购、人工检测、紧急高危漏洞研判、重保值守等核心技术服务的人力成本已足额计入，确保每一步均有对应报价支撑，保障服务质量不打折扣。

3.报价与服务承诺相符：投标报价已包含服务全周期成本，涵盖响应时效保障、漏洞修复跟踪等所有内容，无额外隐形收费，确保服务承诺可兑现，与报价形成完整闭环。

4.报价与服务周期相符：报价严格按照技术部分约定的服务周期（季度、半年度、年度或单次专项服务）制定，区分不同周期的服务频次，报价标准清晰，服务内容与报价精准对应，兼顾合理性与经济性。

十一、 本项目组成成员及相关材料

11.1项目角色及拟派人员

浦东公交公司网络安全项目组成员及拟分配人员如下表：

序号	项目角色	拟分配人员
1	公司项目领导小组	天泰网络执行总经理朱敏担任项目总负责人，赵建飞参与项目管理工作
2	项目经理	曹兴戴
3	安全服务小组	汤金苗、王彩霞、齐健、沈晓勇、刘炜、叶琦、吴康、黄晨瑜、吴纪
4	安全专家	赵建飞
5	质量监督	熊微
6	商务助理	周彩娥
7	安全服务技术支持人员和后备服务工作人员	王玉晴、孙健

11.2项目组人员清单

项目组人员清单

投标人全称（公章）：上海天泰网络技术有限公司 标项：1

姓名	职务	专业技术资格	证书编号	参加本单位工作时间
曹兴戴	项目经理	信息系统项目管理师	信息系统项目管理师：31420201131040102235	11年
汤金苗	安全服务工程师	CISP 国家信息安全测评注册信息安全工程师 CISAW信息安全保障人员（风险评估、安全运维）	CISP：CNITSEC2019CISE10456 信息安全保障人员(CISAW)：2020CISAWOM2994 数据安全风险评估工程师（高级）：325452130231139921	11年
王彩霞	安全服务工程师	CISP 国家信息安全测评注册信息安全工程师	CISP：CNITSEC2023C1SE00727	5年
齐健	安全服务工程师	CISAW信息安全保障人员（应急服务） 数据安全工程师（高级）	信息安全保障人员（CISAW）：2024CISAWES0081 数据安全工程师（高级）：2024BJQY025C013000043	11年
沈晓勇	安全服	CISAW信息	信息安全保障人员(CISAW)：	5年

	务工程师	安全保障人员（应急服务）	2024CISAWES0033	
刘炜	安全服务工程师	信息安全师 CISP 国家信息安全测评注册信息安全工程师	信息安全师：1103000297306968 CISP：CNITSEC2025CISE20591	12 年
叶琦	安全服务工程师	CISP 国家信息安全测评注册信息安全工程师 CISAW 信息安全保障人员（安全运维）	CISP：CNITSEC2022CISE02884 信息安全保障人员(CISAW)：2020CISAWOM3038	10 年
吴康	安全服务工程师	CISP 国家信息安全测评注册信息安全工程师	CISP：CNITSEC2023C1SE-DSG05616	4 年
黄晨瑜	安全服务工程师	CISP 国家信息安全测评注册信息安全工程师	CISP：CNITSEC2023C1SE00728	5 年
吴纪	安全服务工程师	数据安全官（DSO）	CCRC（DSO）：数据安全官 2023DS00144	13 年
赵建飞	安全专家	CISAW 信息安全保障人	信息安全保障人员（CISAW）：	8 年

		员（安全运维） 数据安全工程师（高级） 数据安全风险评估工程师（高级）	2022CISAWRM0432 数据安全工程师（高级）： 2024BJQY025C013000046 数据安全风险评估工程师（高级）： 3254521302311399 29	

授权代表签名：_____ 日 期：2026 年 4 月 10 日

单位职工参加城镇基本养老保险情况

参保名称：上海天秦网络技术有限公司　　社会保险码:00294634

序号	姓名	证件号码	上月缴费状态
39	赵建飞	41128119790209405X	参保缴费
58	刘炜	150823198901070346	参保缴费
61	齐健	220202199112292411	参保缴费
70	沈晓勇	411122198707102535	参保缴费
75	曹兴戴	430482198812106525	参保缴费
83	吴纪	341226198502282731	参保缴费
101	叶琦	310115199001251930	参保缴费
102	黄晨瑜	310225199802243023	参保缴费
106	王彩霞	622426199608231581	参保缴费
109	王鑫	310225199403254016	参保缴费
110	吴康	362330200009011633	参保缴费
113	汤金苗	342622199107077318	参保缴费

第 1 页

上海市社会保险事业管理中心

打印日期：2020 年 04 月 07 日

11.3项目经理与安全服务小组人员情况及证书

本项目将组建个人的安全服务团队，包括参与项目服务的项目经理、安全服务小组等，均承担服务项目的具体任务。

项目经理、安全服务小组每人一表，表后需附相关证书（包括职称/职业资格、执业资格、学历等）和在职证明材料等，所附证书和证明材料均为原件扫描件。

11.3.1 项目经理曹兴戴

项目主要人员基本情况表——曹兴戴

姓名	曹兴戴	年龄	37	从事本专业工作年限	11 年
职称或职业资格	信息系统项目管理师	执业资格（如果有）	信息系统项目管理师	拟在本合同中担任的职务	项目经理
毕业院校和专业	安徽工程大学、计算机科学与技术				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2014 年-2015 年	天泰应用安全产品 WAF、AAP 产品测试		产品测试工程师		
2015 年-2017 年	天泰安全产品（WAF、AAP、ASG、NGFW、ESG）测试经理		产品测试经理		
2018 年-2019 年	浦东教育网络安全在线服务（财政支付系统、教育云应用安全服务）		安全服务工程师 项目经理助理		
2019 年-2025 年	✧ 浦东卫健委网络安全检查服务项目		安全服务工程师		

	✧ 浦东卫健所网络安全巡检服务 ✧ 浦东教育防病毒安全服务 ✧ 浦东卫健所网络安全运维服务		
2022 年至年	浦东新区建交委 WEB 安全系统运行维护 建交委政务云安全系统	项目经理	

普通高等学校

毕业证书

学生 曹兴凯 性别 女，一九八八 年 十二月 十 日生，于 二00七 年 九 月至二0一一年 六 月在本校 计算机科学与技术 专业 四 年制 本 科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校 名：

校（院）长

二0一一 年 六 月二十九日

证书编号：10363120110500154 2

中华人民共和国教育部学历证书查询网址：http://www.chsi.com.cn

计算机技术与软件专业技术资格

Qualification of Computer and Software Professional

本证书由中华人民共和国人力资源和社会保障部、工业和信息化部批准颁发，表明持证人通过国家统一组织的考试，取得计算机技术与软件专业技术资格。

姓　　名：曹兴霞

证件号码：430482198812106525

性　　别：女

出生年月：1988年12月

级　　别：高级

专　　业：信息系统项目管理师

批准日期：2020年11月07日

管 理 号：31420201131040102235

人力资源和社会保障部 人事考试中心 提供查询结果

中华人民共和国 人力资源和社会保障部

中华人民共和国 工业和信息化部

参保人员城镇职工基本养老保险缴费情况

姓名	曹兴戴		社会保障号码		430482198812106525			证件号码		430482198812106525	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		163	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

上海市社会保险事业管理中心 业务专用章

电子印章验证码：MEUCIFy61DMnnF6rcJMiJcI27vd0KYZCBz/UM3IZRYfmC3k0rAiEAz7S+8Qf070goESyVEf7PtjfkzBvb6L1Ydc0+MTkmmIk=

11.3.2 安全服务工程师汤金苗

项目主要人员基本情况表——汤金苗

姓名	汤金苗	年龄	34	从事本专业工作年限	11 年
职称或职业资格	国家信息安全测评注册信息安全专业人员信息安全保障人员 数据安全风险评估工程师（高级）	执业资格（如果有）	CISP 国家信息安全测评注册信息安全工程师 CISAW 信息安全保障人员（安全运维） 数据安全风险评估工程师（高级）	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	安徽农业大学、计算机科学与技术专业				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2013 年-2015 年	安徽省高院安全服务项目		驻场运维工程师		
2016 年	安徽省高院安全服务项目		项目经理		
2016 年-2019 年	✧ 浦东新区卫发院网络安全管理项目 ✧ 浦东新区科经委业务系统云安全保障服务项目等		项目经理		

2019 年-至今	✧ 浦东政务云安全服务项目 ✧ 浦东新区建交委网络安全服务项目 ✧ 浦东新区卫发院网络安全管理项目 ✧ 水利部珠江委安全服务项目等 ✧ 浦东新区世博管委会业务自建系统网络安全保障服务	项目经理 安全服务工程师 安全专家	

成人高等教育

毕业证书

学生 汤金苗 性别 男，一九九一年 七 月 七 日生，于二〇一七年 三 月至 二〇一九年 七月在本校 计算机科学与技术 专业 函授 专升本 科教学计划规定的全部课程，成绩合格，准予毕业。

校 名：

校（院）长

批准文号：教育部[2021]核准字002号

证书编号：10364520190507027 7

二〇一九年 七 月 一日

中国信息安全测评中心
China Information Technology Security Evaluation Center

注册信息安全专业人员 (CISP)
Certified Information Security Professional

首次注册：2019 年 11 月 19 日
Certified Since

发证日期：2023 年 7 月 20 日
Issue Date

有效期：2023 年 7 月 20 日至 2026 年 7 月 19 日
Valid Until

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

证书编号：CNITSEC2019CISE10456
Certificate No.

兹证明
This is to certify that

汤金苗
TANGJINMIAO

证件号：342622199107077518
ID No.

经中国信息安全测评中心的考试和审查，符合《注册信息安全专业人员资质评估准则》的要求，获准 注册信息安全工程师(CISE) 资质。

has successfully fulfilled the requirements prescribed by CNITSEC for certification and is hereby awarded this professional designation.

批准人
Signed by

持证人参加：

数据安全风险评估工程师
（高级）

职业能力培训，完成培训计划所规定的全部课程内容，经考核合格，达到相关岗位要求的专业能力水平。

特发此证

姓　　名：汤金苗

身份证号：342622199107077318

证书号码：325452130231139921

信息安全保障人员认证证书
Information Security Assurance Worker Certification Certificate

兹证明 汤金苗
This is to certify that TANG JINMIAO

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。
has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for information Security Assurance Worker and is hereby awarded the professional-level in security operation and maintenance field.

认证方向/Certification field: 安全运维（专业级）OM/PL
证书编号/Certificate No.: 2020CISAWOM2994 (R)
序列号/Serial No.: 1049815
发证日期/Date of Issue: 2023年12月11日
有效期/Term of Validity: 2026年12月17日

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。
You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书
E-certificate only

参保人员城镇职工基本养老保险缴费情况

姓名	汤金苗		社会保障号码		342622199107077318			证件号码		342622199107077318	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	未缴费		21	202209	未缴费		41	202405	已缴费	
2	202102	未缴费		22	202210	未缴费		42	202406	已缴费	
3	202103	未缴费		23	202211	未缴费		43	202407	已缴费	
4	202104	未缴费		24	202212	未缴费		44	202408	已缴费	
5	202105	未缴费		25	202301	未缴费		45	202409	已缴费	
6	202106	未缴费		26	202302	未缴费		46	202410	已缴费	
7	202107	未缴费		27	202303	未缴费		47	202411	已缴费	
8	202108	未缴费		28	202304	未缴费		48	202412	已缴费	
9	202109	未缴费		29	202305	未缴费		49	202501	已缴费	
10	202110	未缴费		30	202306	未缴费		50	202502	已缴费	
11	202111	未缴费		31	202307	未缴费		51	202503	已缴费	
12	202112	未缴费		32	202308	未缴费		52	202504	已缴费	
13	202201	未缴费		33	202309	未缴费		53	202505	已缴费	
14	202202	未缴费		34	202310	未缴费		54	202506	已缴费	
15	202203	未缴费		35	202311	未缴费		55	202507	已缴费	
16	202204	未缴费		36	202312	未缴费		56	202508	已缴费	
17	202205	未缴费		37	202401	未缴费		57	202509	已缴费	
18	202206	未缴费		38	202402	未缴费		58	202510	已缴费	
19	202207	未缴费		39	202403	未缴费		59	202511	已缴费	
20	202208	未缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2024年04月-2025年12月		
截至2025年12月，累计缴费月数		21	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

上海市社会保险事业管理中心 业务专用章

电子印章验证码：MEUCIQD271MjGDVg3iLKT+IMi+oMhtHIXhGOTbeqM2IHePnijgIgO9H46byWbh/GO2NVLiyj4hmkf0+wWtn51filn+8Q7Z4=

11.3.3 安全服务工程师王彩霞

项目主要人员基本情况表——王彩霞

姓名	王彩霞	年龄	29	从事本专业工作年限	5年
职称或职业资格	国家信息安全测评注册信息安全专业人员	执业资格（如果有）	CISP 国家信息安全测评注册信息安全工程师	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	兰州财经大学陇桥学院、网络工程				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2020年-至今	✧ 浦东人社局安全项目网络安全服务项目 ✧ 浦东新区医疗救助系统等保相关安全服务 ✧ 浦东新区卫发院网络安全服务 ✧ 上海度假区网络安全服务项目 ✧ 浦东新区卫健委网络安全检查服务项目		安全服务工程师		

普通高等学校

毕业证书

学生 王彩霞 性别 女，一九九六年 八 月二十三日生，于 二〇一六年 九 月至 二〇二〇年 六 月在本校 网络工程(网络安全方向) 专业 四 年制 本 科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校 名：兰州财经大学陇桥学院

校(院)长

二〇二〇 年 六 月 二十 日

证书编号：13511120205001583

中国信息安全测评中心
China Information Technology Security Evaluation Center

注册信息安全专业人员 (CISP)
Certified Information Security Professional

首次注册： 2023 年 1 月 26 日
Certified Since

发证日期： 2025 年 12 月 20 日
Issue Date

有效期： 2025 年 12 月 20 日至 2028 年 12 月 19 日
Valid thru

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

（证书编号： CNITSEC2023CISE00727 ）
Certificate No.

兹证明
This is to certify that

王彩霞
WANG CAIXIA

（证件号： 622426199608231581 ）
ID No.

经中国信息安全测评中心的考试和审定，符合
has successfully fulfilled the requirements prescribed by CNITSEC
《注册信息安全专业人员资质评估准则》
for certification and is hereby awarded this professional designation.
的要求，获准 注册信息安全工程师(CISE) 资质。

批准人
Signed by

中国信息安全测评中心 CNITSEC 证书专用章

参保人员城镇职工基本养老保险缴费情况

姓名	王彩霞		社会保障号码		622426199608231581			证件号码		622426199608231581	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		63	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

日期：2026-1-23

电子印章验证码：

MEQCIDJMTeUY98v9WCP2kFj0XeLz7kJiAkviBXTybgLZSfAmAiAl0IEcq1OD93mwI3WUOOOqR35+BhvLmm95opzD//n
Gyw==

11.3.4 安全服务工程师齐健

项目主要人员基本情况表——齐健

姓名	齐健	年龄	35	从事本专业工作年限	11 年
职称或职业资格	信息安全保障人员、数据安全工程师	执业资格	信息安全保障人员、数据安全工程师	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	吉林化工学院、数学与应用数学				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2020 年-2022 年	✧ 上海金桥（集团）有限公司信息系统网络安全保障服务		服务工程师		
2022 年至今	✧ 浦东教育网络安全监管与保障服务项目		安全技术专家		

普通高等学校

毕业证书

学生 齐健 性别 男，一九九一 年 十二月二十九日生，于 二〇一〇 年 九 月至二〇一四年 六 月在本校 数学与应用数学 专业 四 年制 本 科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校 名：吉林化工学院

校（院）长：

二〇一四年 六 月二十三日

证书编号：10192120140500117[illegible]

中华人民共和国教育部学历证书查询网址：http://www.chsi.com.cn

信息安全保障人员认证证书
Information Security Assurance Worker Certification Certificate

兹证明 齐健
This is to certify that QI JIAN

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。
has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for Information Security Assurance Worker and is hereby awarded the professional-level in emergency service field.

认证方向/Certification field: 应急服务（专业级）ES/PL
证书编号/Certificate No.: 2024CISAWES0081
序列号/Serial No.: 1052783
发证日期/Date of Issue: 2024年04月19日
有效期/Term of Validity: 2027年04月18日

魏昊

请登www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。
You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书
E-certificate only

持证人参加：

数据安全工程师（高级）

职业能力培训，完成培训计划所规定的全部课程内容，经考核合格，达到相关职位要求的专业能力水平。

特发此证。

2024 年 06 月 26 日

姓　　名：齐健

身份证号：220202199112292411

证书号码：2024BJQY025C013000043

参保人员城镇职工基本养老保险缴费情况

姓名	齐陡		社会保障号码	220202199112292411			证件号码	220202199112292411		
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		22	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		23	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		24	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		25	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		26	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		27	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		28	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		29	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		30	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		31	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		32	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		33	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		34	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		35	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		36	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		37	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		38	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		39	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		40	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		134	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

电子印章验证码：MEUCIQDfZrZYy7HOCG/jF7k3IulkiksRz7UAZYqdQyhMeFJSgQIgd2pxNQU6pzE1xVoXcfgDAUONWV/okRdqAg5Ru7B NTPQ=

11.3.5 安全服务工程师沈晓勇

项目主要人员基本情况表——沈晓勇

姓名	沈晓勇	年龄	38	从事本专业工作年限	14 年
职称或职业资格	信息安全保障人员	执业资格（如果有）	信息安全保障人员	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	郑州大学、计算机科学与技术				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2020 年-2021 年	✧ 市经信委工业安全综合管理平台项目		项目经理		
2022 年-2023 年	✧ 上海市浦东新区建设和交通委员会 ✧ 浦东新区建交委 WEB 安全系统运行维护		服务工程师		
2022 年-至今	✧ 浦东新区大数据中心政务网络安全管理技术服务费_1		服务工程师		

普通高等学校

毕业证书

学生 沈晓勇 性别男 ,一九八七 年七 月十 日生，于二〇〇六 年 九 月至二〇一〇 年 七 月在本校 计算机科学与技术(软件工程) 专业 四 年制 本 科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校 长：申长雨

证书编号：10459120100500313

二〇一〇 年 七 月 一 日

信息安全保障人员认证证书

Information Security Assurance Worker Certification Certificate

兹证明 沈晓勇

This is to certify that SHEN XIAOYONG

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。

has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for information Security Assurance Worker and is hereby awarded the professional-level in emergency service field.

认证方向/Certification field：应急服务（专业级）ES/PL

证书编号/Certificate No.：2024CISAWES0033

序列号/Serial No.：1052256

发证日期/Date of Issue：2024年04月03日

有效期/Term of Validity：2027年04月02日

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。

You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书

E-certificate only

参保人员城镇职工基本养老保险缴费情况

姓名	沈晓勇		社会保障号码		411122198707102535			证件号码		411122198707102535	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		174	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

电子印章验证码：MEUCIAmpSWe35nVC7tpyLzw6WD7SDeG/vBM2U610GufHBRVBzAiEAjwrJq4RPBOmWgKkCRnAw9yYoO8DWx+WM+UBZ11I1KGo=

11.3.6 安全服务工程师刘炜

项目主要人员基本情况表——刘炜

姓名	刘炜	年龄	36	从事本专业工作年限	12 年
职称或职业资格	国家信息安全测评注册信息安全专业人员 信息安全师	执业资格（如果有）	CISP 国家信息安全测评注册信息安全工程师 信息安全师	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	上海第二工业大学、网络工程				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2012 年-2017 年	✧ 上海互联网金融安全在线服务项目 ✧ 云 WEB 应用安全防护系统		产品工程师 软件工程师		
2018 年至今	✧ 浦东应急局网络安全服务项目 ✧ 浦东卫健委网络安全检查服务项目 ✧ 浦东新区医疗救助系统等保相关安全服务项目 ✧ 浦东新区建交委网络安全服务项目		安全服务工程师 安全培训讲师		

普通高等学校

毕业证书

学生 刘婷 性别 女，

学号 084833144，一九八九年

一月 七日生，于 二〇〇八年

九月至 二〇一二年 七月在本校

网络工程 专业

四年制本科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校（院）长：胡青松

上海大学网络技术学院公司印

校名：上海第二工业大学

二〇一二年 七月 一日

证书序列号：NO.10548444

证书编号：120441201205001047

职业名称： 信息安全师
等级： 高级/三级
评定成绩： 优秀
证书号码： 1103000297306968

鉴定内容：
1 维护操作系统安全
2 防治计算机病毒
3 使用防火墙产品
4 使用扫描技术产品
5 使用入侵检测技术产品
6 配置网络应用服务安全
7 使用安全审计技术产品
8 使用安全策略管理技术产品
9 处理计算机应急事件

姓 名：刘炜
性 别：女
出生日期：1989 年 01 月 07 日
身份证号：150823198901070346

证书
专用章

职业技能鉴定（指导）中心（印）
2011年12月08日
鉴定专用章

中国信息安全测评中心
China Information Technology Security Evaluation Center

注册信息安全专业人员 (CISP)
Certified Information Security Professional

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

证书编号 Certificate No.: CNITSEC2025CISE20591

兹证明 This is to certify that

刘炜
LIU WEI

证件号 ID No.: 150823198901070346

经中国信息安全测评中心的考试和审定，符合
has successfully fulfilled the requirements prescribed by CNITSEC
《注册信息安全专业人员资质评估准则》
for certification and is hereby awarded this professional designation,
的要求，获准 注册信息安全工程师(CISE) 资质。

发证日期 Issue Date: 2025 年 10 月 26 日
有效期 Valid thru: 2025 年 10 月 26 日至 2028 年 10 月 25 日

批准人 Signed by

中国信息安全测评中心 证书专用章

参保人员城镇职工基本养老保险缴费情况

姓名	刘炜		社会保障号码		150823198901070346			证件号码		150823198901070346	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		162	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

日期：2026-1-19

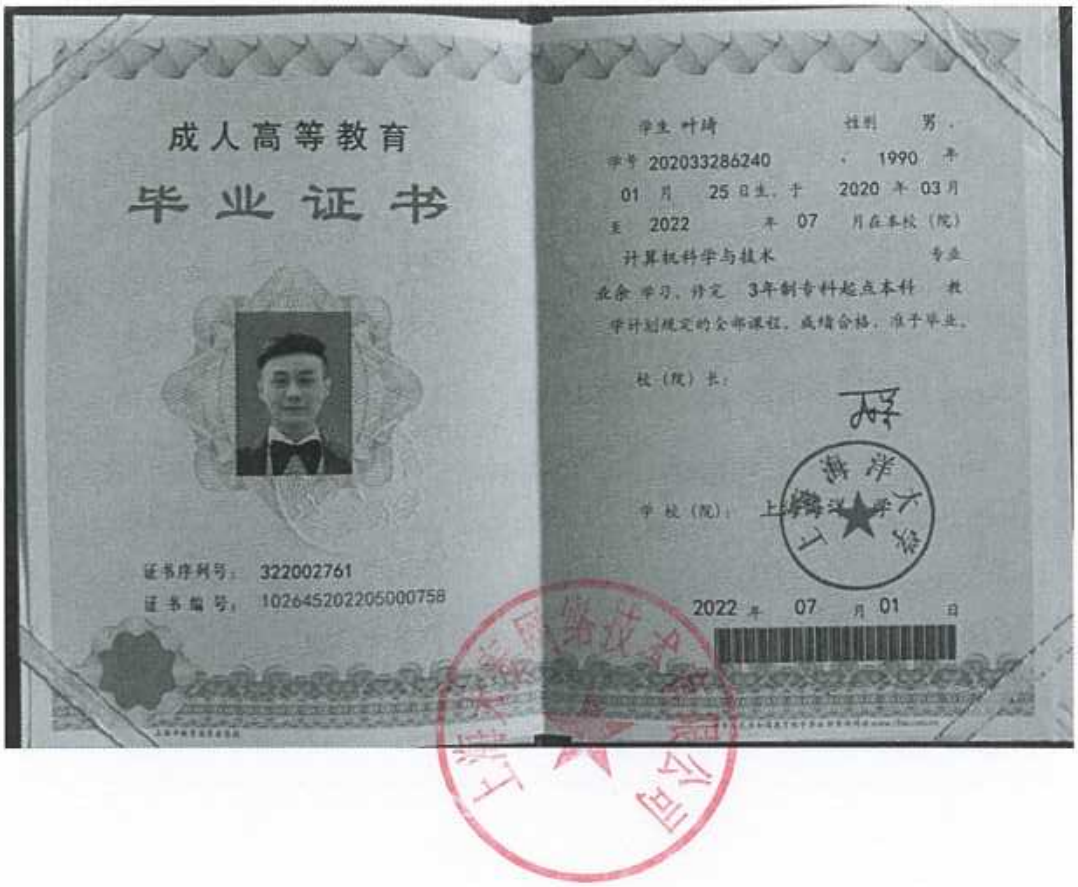
上海市社会保险事业管理中心 业务专用章

电子印章验证码：MEQCIAHiVL+ZaJGIM7jZvGo8YrqFrW/+o8a6+FBsBHwSFHRKAiBaZENInKDajO8qGmDy9H/jbjLIOGpmaFnB7F4F8BQ==

11.3.7 安全服务工程师叶琦

项目主要人员基本情况表——叶琦

姓名	叶琦	年龄	35	从事本专业工作年限	11年
职称或职业资格	信息安全保障人员、国家信息安全测评注册信息安全专业人员	执业资格（如果有）	CISP 国家信息安全测评注册信息安全工程师 CISAW信息安全保障人员（安全运维）	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	上海海洋大学、计算机科学与技术				
主要工作经历					
年~年	参加过的项目		担任何职	备注	
2015年-2018年	浦东教育发展研究院教育网网络安全设备项目		安全运维工程师		
2018年至今	✧ 浦东大数据中心网络安全管理日常服务项目 ✧ 浦东新区政务云网络安全运维服务等项目 ✧ 浦东新区规划和自然资源管理局网络安全服务项目 ✧ 浦东新区财政局网络安全服务项目		安全服务工程师		



成人高等教育

毕业证书

证书序列号：322002761

证书编号：102645202205000758

学生 叶琦 性别 男，

学号 202033286240 ，1990 年

01 月 25 日生，于 2020 年 03 月

至 2022 年 07 月在本校（院）

计算机科学与技术 专业

业余 学习，修完 3年制专科起点本科 教

学计划规定的全部课程，成绩合格，准予毕业。

校（院）长：

学校（院）：上海海洋大学

2022 年 07 月 01 日

信息安全保障人员认证证书
Information Security Assurance Worker Certification Certificate

兹证明 叶琦
This is to certify that YE Qi

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。
has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for information Security Assurance Worker and is hereby awarded the professional-level in security operation and maintenance field.

认证方向/Certification field：安全运维（专业级）OM/PL
证书编号/Certificate No.：2020CISAWOM3038（R）
序列号/Serial No.：1050284
发证日期/Date of Issue：2023年12月19日
有效期/Term of Validity：2026年12月24日

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。
You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书
E-certificate only

中国信息安全测评中心
China Information Technology Security Evaluation Center

注册信息安全专业人员 (CISP)
Certified Information Security Professional

首次注册：2022 年 2 月 28 日
Certified Since

发证日期：2025 年 5 月 20 日
Issue Date

有效期：2025 年 5 月 20 日至 2028 年 5 月 19 日
Valid thru

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

（证书编号：CNITSEC2022CISE02884）
Certificate No.

兹证明
This is to certify that

叶琦

（证件号：310115199001251930）
ID No.

经中国信息安全测评中心的考试和审定，符合
has successfully fulfilled the requirements prescribed by CNITSEC
《注册信息安全专业人员资质评估准则》
for certification and is hereby awarded this professional designation.
的要求，获准 注册信息安全工程师(CISE) 资质。

签署人
Signed by

参保人员城镇职工基本养老保险缴费情况

姓名	叶琦		社会保障号码		310115199001251930			证件号码		310115199001251930	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		132	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

电子印章验证码：MEUCIFg9SaS+N0k1H/7IX8obd6xpoxkWb+IKGLzwnhTLzfFFAiEA3g8dglnWLrFgvymYvCmboiggnJvWhgnq/wSFbNLkJ50=

11.3.8 安全服务工程师吴康

项目主要人员基本情况表——吴康

姓名	吴康	年龄	25	从事本专业工作年限	4年
职称或职业资格	国家信息安全测评注册信息安全专业人员	执业资格（如果有）	CISP 国家信息安全测评注册信息安全工程师	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	上海科学技术职业学院、信息安全与管理				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2022年-至今	浦东新区政务云网络安全运维服务项目		安全运维工程师		

中国信息安全测评中心
China Information Technology Security Evaluation Center

注册信息安全专业人员 (CISP)
Certified Information Security Professional

发证日期：2023 年 3 月 26 日
Issue Date

有效期：2023 年 3 月 26 日至 2026 年 3 月 25 日
Valid thru

技术支持单位：北京关键信网络安全技术有限公司
Technical Support Units: Beijing Topsec Network Security Technology Co.,Ltd

注册数据安全治理专业人员
CERTIFIED
DATA SECURITY GOVERNANCE
PROFESSIONAL

（证书编号：CNITSEC2023CISP-DSG05616）
Certificate No.

兹证明
This is to certify that

吴康

（证件号：362330200009011433）
ID No.

经中国信息安全测评中心的考试和审定，符合
has successfully fulfilled the requirements prescribed by CNITSEC
《注册信息安全专业人员资质评估准则》
for certification and is hereby awarded this professional designation.
的要求，获准注册数据安全治理专业人员 (CISP-DSG) 资质。

批准人
Signed by

普通高等学校

毕业证书

学生 吴康 性别 男，
学号 18171022，2000 年
09 月 01 日生，于 2018 年
09 月至 2021 年 06 月在本校
信息安全与管理 专业
3年制专科 学习，修完教学计划规定的
全部课程，成绩合格，准予毕业。

校（院）长：周胜

校 名：上海[illegible]学院

2021 年 06 月 28 日

证书序列号：121094856
证书编号：128011202106000189

参保人员城镇职工基本养老保险缴费情况

姓名	吴康		社会保障号码		362330200009011633			证件号码		362330200009011633	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	未缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	未缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	未缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	未缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	未缴费		25	202301	补缴	202302	45	202409	已缴费	
6	202106	未缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	未缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	未缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	未缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	未缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	未缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	未缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海骊豆信息技术有限公司	2022年01月-2022年12月	上海天泰科技术有限公司	2023年01月-2025年12月
截至2025年12月，累计缴费月数		48	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

日期：2026-1-8

业务专用章

电子印章验证码：MEQCIPW/FSUe/wEZxIhuMkOfEOj+Rrxnm2rP81hICwqM8OPAAiAWs0CeLpXfgvz9zWJEw3hdfUP4KtIyOdmt/hkW205 7Nw==

11.3.9 安全服务工程师黄晨瑜

项目主要人员基本情况表——黄晨瑜

姓名	黄晨瑜	年龄	27	从事本专业工作年限	5 年
职称或职业资格	安全服务工程师	执业资格（如果有）	CISP 国家信息安全测评注册信息安全工程师	拟在本合同中担任的职务	安全服务工程师 安全运维 安全检查
毕业院校和专业	河南大学 计算机科学与技术				
主要工作经历					
年~年	参加过的项目		担任何职		备注
2020 年-2021 年	公司项目管理		项目管理员		
2021 年-至今	✧ 浦东政务云安全运维服务项目 ✧ 浦东新区卫健委网络安全管理服务项目 ✧ 浦东建交委网络安全服务项目 ✧ 浦东城运中心网络安全服务项目		驻场工程师 安全服务工程师		

河南大學
HENAN UNIVERSITY

毕业证书

黄晨瑜，女，一九九八年二月二十四日生，于二〇一六年九月至二〇二〇年六月在本校 计算机科学与技术 专业 四 年制本科学习，修完培养方案规定的全部课程，成绩合格，准予毕业。

校长：宋鹏印纯

证书编号：104751202005601534

（普通高等教育本科毕业生）

河南大学

二〇二〇年六月二十日

中华人民共和国教育部学历证书查询网站：http://www.chsi.com.cn

中国信息安全测评中心
China Information Technology Security Evaluation Center

注册信息安全专业人员 (CISP)
Certified Information Security Professional

首次注册：2023 年 1 月 26 日
Certified Since

发证日期：2025 年 12 月 20 日
Issue Date

有效期：2025 年 12 月 20 日至 2028 年 12 月 19 日
Valid thru

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

（证书编号：CNITSEC2023CISE00728）
Certificate No.

兹证明
This is to certify that

黄晨瑜
HUANG CHENYU

（证件号：310225199802243023）
ID No.

经中国信息安全测评中心的考试和审定，符合
has successfully fulfilled the requirements prescribed by CNITSEC
《注册信息安全专业人员资质评估准则》
for certification and is hereby awarded this professional designation.
的要求，获准 注册信息安全工程师(CISE) 资质。

批准人
Signed by

中国信息安全测评中心 证书专用章

参保人员城镇职工基本养老保险缴费情况

姓名	黄晨瑜		社会保险号码		310225199802243023			证件号码		310225199802243023	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		60	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

上海市社会保险事业管理中心 业务专用章

电子印章验证码：

MEQCIBTYASAxTYkqH+g+kcKZxIK6hZB3GKVk1sWXoi/Sh4b1AiA2SHwWzK2JSQ1NDJz0pqbtmFBhsRjlPd4N6B2nKYK

YnA==

11.3.10 安全服务工程师吴纪

项目主要人员基本情况表——吴纪

姓名	吴纪	年龄	40	从事本专业工作年限	17 年
职称或职业资格	数据安全官（DSO）	执业资格（如果有）	数据安全官（DSO）	拟在本合同中担任的职务	安全服务工程师
毕业院校和专业	华东师范大学、网络教育工商管理				
主要工作经历					
年~年	参加过的项目	担任何职			备注
2023 年-至今	上海国际旅游度假区管理委员会网络安全相关服务	服务工程师			
2022 年-2024 年	上海市浦东新区医疗保险事务中心浦东新区医疗救助系统等保服务	服务工程师			

毕业证书

学生 吴杞 性别 男
学号 11162838003047 ，1985 年
02 月 28 日生，于 2016 年
09 月至 2019 年 01 月在本校
工商管理 专业网络教育
专科起点本科 学习，修完教学计划规定的
全部课程，成绩合格，准予毕业。

校（院）长：

校 名：华东师范大学

证书序列号：418021617
证书编号：10269720190500289I

2019 年 01 月 15 日

CCRC

数据安全官证书
Data Security Officer Certificate

兹证明 吴纪
This is to certify that WU JI

参加了数据安全官考试，考试合格，特发此证。
has passed the examination of Data Security Officer and is hereby presented the certificate.

证书编号/Certificate No.: 2023DSO0144
发证日期/Date of Issue: 2023年05月25日
有效期/Term of Validity: 2026年05月24日

中国网络安全审查技术与认证中心

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性
You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code

本证书仅发放电子证书
E-certificate only

参保人员城镇职工基本养老保险缴费情况

姓名	吴纪		社会保障号码		341226198502282731			证件号码		341226198502282731	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		174	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考，亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

业务专用章

电子印章验证码：MEQCIGpiZ/XRmHZZfx27JxgU/A7xJ142FwJLVz105MaLdzJxAiAWQ4AXz1ECTisOG+LMvOERMzJ2QDyRqMt65EWa2dBtqA==

11.3.11 安全专家赵建飞

姓名	赵建飞	年龄	46	从事本专业工作年限	12 年
职称或职业资格	信息安全保障人员、数据安全工程师	执业资格（如果有）	信息安全保障人员、数据安全工程师	拟在本合同中担任的职务	网络安全专家
毕业院校和专业	上海海洋大学、计算机科学与技术专业				
主要工作经历					
年~ 年	参加过的项目		担任何职		备注
2012 年-2018 年	上海互联网金融安全在线服务项目 上海区块链安全服务项目		项目经理		
2018 年至今	浦东应急局安全服务项目 浦东建交委网络安全服务项目 浦东新区卫健委安全服务项目		项目专家 高级网络安全服务工程师		

成人高等教育

毕业证书

证书序列号：

证书编号：

学生 赵建飞 性别 男，

学号 200901562316，一九七九 年

二月 九日生，于二〇〇九 年 三 月

至 二〇一二 年 一 月在本校（院）

计算机科学与技术 专业

业余学习，修完 专科起点三年制本科 教

学计划规定的全部课程，成绩合格，准予毕业。

校（院）长：

学校（院）：上海海洋大学

二〇一二 年 一 月 十五 日

CISAW

信息安全保障人员认证证书

Certificate of Information Security Assurance Workforce Certification

兹证明 This is to certify that

赵建飞
ZHAOJIANFEI

考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，具备下述认证方向和级别所需的知识和技能，特颁此证。

has passed the examination and certification assessment, successfully fulfilled the requirements of Cisaw Criteria, and obtained the knowledge and skills required for the following field and level. This certificate is hereby issued.

认证方向 / Certification Field: 风险管理 / Risk Management

认证级别 / Certification Level: 专业级 / Professional Level

证书编号 / Certificate No.: 2022CISAWRM0432 (R)

发证日期 / Date of Issue: 2025年10月13日 / October 13, 2025

有效期至 / Date of Expiry: 2028年10月09日 / October 9, 2028

CCRC

陳建良

Signed: Chen Jianliang

中国网络安全审查认证和市场监管大数据中心

CHINA CYBERSECURITY REVIEW,CERTIFICATION AND MARKET REGULATION BIG DATA CENTER

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。

You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书

E-certificate only

持证人参加：

数据安全工程师（高级）

职业能力培训，完成培训计划所规定的全部课程内容，经考核合格，达到相关职位要求的专业能力水平。

特发此证

2024 年 06 月 26 日

姓　　名：赵建飞

身份证号：41128119790209405X

证书号码：2024BJQY025C013000046

参保人员城镇职工基本养老保险缴费情况

姓名	赵建飞		社会保障号码		41128119790209405X			证件号码		41128119790209405X	
序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月	序号	年 月	缴费情况	补缴退账年月
1	202101	已缴费		21	202209	已缴费		41	202405	已缴费	
2	202102	已缴费		22	202210	已缴费		42	202406	已缴费	
3	202103	已缴费		23	202211	已缴费		43	202407	已缴费	
4	202104	已缴费		24	202212	已缴费		44	202408	已缴费	
5	202105	已缴费		25	202301	已缴费		45	202409	已缴费	
6	202106	已缴费		26	202302	已缴费		46	202410	已缴费	
7	202107	已缴费		27	202303	已缴费		47	202411	已缴费	
8	202108	已缴费		28	202304	已缴费		48	202412	已缴费	
9	202109	已缴费		29	202305	已缴费		49	202501	已缴费	
10	202110	已缴费		30	202306	已缴费		50	202502	已缴费	
11	202111	已缴费		31	202307	已缴费		51	202503	已缴费	
12	202112	已缴费		32	202308	已缴费		52	202504	已缴费	
13	202201	已缴费		33	202309	已缴费		53	202505	已缴费	
14	202202	已缴费		34	202310	已缴费		54	202506	已缴费	
15	202203	已缴费		35	202311	已缴费		55	202507	已缴费	
16	202204	已缴费		36	202312	已缴费		56	202508	已缴费	
17	202205	已缴费		37	202401	已缴费		57	202509	已缴费	
18	202206	已缴费		38	202402	已缴费		58	202510	已缴费	
19	202207	已缴费		39	202403	已缴费		59	202511	已缴费	
20	202208	已缴费		40	202404	已缴费		60	202512	已缴费	

近60个月缴费单位信息

缴费单位名称	缴费起止时间	缴费单位名称	缴费起止时间
上海天泰网络技术有限公司	2021年01月-2025年12月		
截至2025年12月，累计缴费月数		174	

备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。

2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 上海市社会保险事业管理中心业务专用章已经上海市数字证书认证中心认证，是对外经办业务指定电子印章，与社保经办机构印章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心

打印日期：2026-1-23

上海市社会保险事业管理中心 业务专用章

电子印章验证码：MEUCIQCGY6T95aB1+iGq441aIWIqBQ1jgG7+ahhQGNstZ+vJCQIgHjTL6XHHC8tE9G57ffgtXuiqDuXD+HYsXZbBS1Cs8CM=

十二、 技术服务方案小结

12.1天泰网络应标技术能力和方案的符合性

天泰网络技术服务方案的符合性和高可行性如下：

1) 本技术服务方案根据招标要求，从 8 个服务科目的需求理解、业务分析、服务内容、流程设计、过程文档、服务人员和工具、服务周期与频次、服务成果提交等方面，对每个服务科目进行了全面细致的描述，与招标服务要求和目标完全一致。

2) 通过服务管理方案，从项目管理策略、管理结构、服务组织架构、项目组人员岗位设置及工作职责、网络安全服务业务流程管理、安全文明措施与承诺、项目应急预案管理、项目实施进度安排、售后服务承诺等方面，描述了项目组织实施的具体方式方法，有效的展示了完成安全服务任务的管理措施和资源保障能力。

3) 技术服务方案提供了 10 人组成的服务团队参与项目的服务，从团队的人员项目履历、服务经验、认证资历，以及各自专业特长的搭配组合，是一个完全可以覆盖项目服务要求的高效的团队。针对日常检查运维和使用指导服务，服务团队将及时予以响应，有关故障、安全事件的响应和恢复均满足招标文件的要求。

4) 本方案提出了三个方面的合理化建议，具有很强的操作性，合理性；建议开展的顶层设计和安全防护工作有很强的有效性及针对性。

十三、 商务响应表

投标人全称（公章）：上海天泰网络技术有限公司　　标项：1

项目	招标文件要求	是否响应	投标人的承诺或说明
服务期限	合同签订生效之日起一年，具体时间以招标人通知为准	完全响应	完全响应招标文件要求的服务期限
付款条件	（1）合同签订后的一个月内支付合同价款的40%； （2）服务满半年，开展阶段性工作评估，通过后的十五个工作日内支付合同价款的30%； （3）服务期满，项目通过第三方专家验收后的十五个工作日内支付合同价款的25%； （4）项目通过第三方审价后，根据审价结果，支付剩余5%尾款。	完全响应	完全响应招标文件要求的付款条件
违约责任及争议解决方式	（1）如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。 （2）如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。 （3）合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。 （4）调解不成则提交提交上海市浦东新区人民法院诉讼解决。 （5）如诉讼事项不影响	完全响应	完全响应合同要求的违约责任及争议解决方式

	合同其它部分的履行，则在诉讼期间，除正在进行诉讼的部分外，本合同的其它部分应继续执行。		
响应情况	综合评审对项目需求的理解、服务项目定位和目标确定，以及项目实施各方案中工作计划、方法流程、时间安排等方面的考虑。评价方案的合理性、针对性、具体性、操作性	完全响应	详细描述对项目的理解及服务实施的方案计划等内容
本地化服务要求	采购单位地址：成山路990 号	完全响应	天泰网络总部位于浦东新区，具备提供本地化服务的能力
公司技术力量情况	投标人企业和服务的各类证书情况	完全响应	提供满足本项目服务所需的资质材料，包括信息系统安全运维服务资质、信息安全风险评估服务资质、信息安全应急处理服务资质、信息系统安全集成服务资质、质量管理体系认证证书。提供证明公司技术实力的相关证书，如高新技术企业证书、专精特新中小企业、专利证书、获社会信用证明的相关证书
经验或业绩要求	投标人应具有同类项目经验，具有较好的用户口碑、并提供相关证明文件的优先	完全响应	提供 7 个类似业绩

授权代表签名：_____ 日期：2026 年 4 月 10 日

十四、 投标人业绩情况一览表

投标人全称（公章）：上海天泰网络技术有限公司

采购单位名称	设备或项目名称	采购数量	单价	合同金额（万元）	附件页码		采购单位联系人及联系电话
					合同	用户评价	
上海浦东新区公共交通有限公司	浦东公交网络安全服务采购	1	98.12万元	98.12	249	本项目含保等测评、安全防护、安全检查、急应演练、安全培训等服务，获得用户感谢信	陶老师 021-50186155
上海市浦东新区大数据中心	政务网络安全管理技术服务项目	1	170.35万元	170.35	254	本项目为管单位向区政务网络安全监管服务，主面新目含渗透测试、应急演练、数	吴老师 021-20742666

						安风评、安培等务，得户谢信 据全险估全训服获用感	
上海市浦东新区人力资源和社会保障局	2024年浦东人社局重要信息系统安全保障服务	1	97.8万元	97.8	260	项为户供全服及保服务，获用感信 本目用提安类务等类务，得户谢	傅老师 021-20742824
上海市浦东新区城市运行综合管理中心	信息系统网络安全服务费	1	92.75万元	92.75	267	项提类安服用感信 本目供似全务，获得户谢	洪老师 021-38939761
上海市浦东新区应急管理局	信息系统网络安全服务项目	1	69.8万元	69.8	272	项为户供全固改、扫安检服 本目用提安加整漏与全查	唐老师 021-38939911

						务及急障务，得户谢信	
上海市浦东新区建设和交通委员会	2025年浦东新区建交委网络安全等保建设项目	1	168.34万元	168.34	276	本项为户供全服，获用感信	张老师 021-65548029
上海市浦东新区卫生健康委员会	网络安全管理项目	1	89.75万元	89.75	281	本项提安整技支、应演和用统全护务，获用感信	王老师 021-38583172
备注	提供投标人同类项目合同复印件、用户评价（如有）。						

授权代表签名：_____ 时 间：2026年4月10日

14.1浦东公交网络安全服务采购项目

14.1.1 项目合同

说明：本项目为浦东公交及下属单位提供等保测评、安全防护、安全检查、应急演练、安全培训等服务。

合同编号：

浦东公交网络安全服务采购项目合同

1

甲方：上海浦东新区公共交通有限公司

地址：上海市浦东新区成山路 990 号 16 楼-17 楼

乙方：上海天泰网络技术有限公司

地址：上海市浦东新区盛荣路 88 弄 1 号楼 9 楼

甲方和乙方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》《中华人民共和国网络安全法》等相关法律法规的规定，达成如下协议（以下简称“本合同”），并由甲乙双方共同恪守。

第一条 项目内容

1. 项目目标

2. 网络安全服务

（一）网络安全测评服务

（二）网络安全防护服务

（三）网络安全检测服务

（四）网络安全应急保障

（五）网络安全培训

（六）网络安全应急演练

（七）网络风险技术性探测

（八）乙方应当按下列要求完成技术服务工作：

① 技术服务地点：甲方指定地点。

② 技术服务期限：自合同签订之日起一年内，运维服务期限为12个月。

③ 技术服务质量要求

④ 技术服务工作报告：

第二条 为保证乙方有效开展项目工作，甲方应当向乙方提供下列工作条件和协作事项：

1. 提供技术资料：本合同范围内系统的相关技术资料。

2. 提供工作条件：乙方提供安全服务时，甲方提供必要的配合支持。

3. 甲方提供上述工作条件和协作事项的时间：本合同有效期内。

第三条 项目金额和付款方式

1. 项目总额（含税）：人民币玖拾捌万壹仟贰佰圆整（小写：¥981,200.00元），税率为6%，不含增值税价款为¥925,660.38元，增值税为¥55,539.62元。（价格明细表详见附件一）

2. 项目付款方式

注：费用由甲方及其四家直属企业分摊支付

3. 本合同中的费用由甲方及指定的4家直属企业（使用单位）向乙方支付，每次付款前，乙方需向甲方及四家直属企业分别开具平均金额(当次支付总金额的五分之一)的增值税普通发票(6%)。

（本页无正文，为《浦东公交网络安全服务采购项目合同》之签署页）

甲方（盖章）：上海浦东新区公共交通有限公司

法定代表人/授权代表（签字）：[redacted]

日期：2024 年 12 月 30 日

地点：浦东新区

乙方（盖章）：[illegible]

法定代表人/授权代表（签字）：

日期：2024 年 12 月 30 日

地点：浦东新区

14.1.2 用户评价-感谢信

感谢信

致：上海天泰网络技术有限公司

上海浦东新区公共交通有限公司谨以此信，对贵公司在2025年度“浦东公交网络安全服务采购项目”中提供的全方位、高质量网络安全服务表示高度认可与衷心感谢，并对项目团队的专业精神与突出贡献提出表扬。

2025年度，我公司网络安全工作面临保障范围广、实时性要求高、潜在风险点多等挑战。贵公司组建了以孙健、黄晨瑜、陈杰等同志为核心的专业服务团队，为我司提供了涵盖等保测评咨询、常态化安全检测、应急响应保障、实战化演练及人员培训等系列服务。服务期间，团队展现出了卓越的技术素养与高度的责任感，为浦东公交的日常运营与公众服务提供了坚实可靠的安全屏障。

本次合作充分证明贵公司是一家值得信赖的网络安全服务提供商。我们诚挚感谢贵公司及项目团队全年的辛勤付出与卓越贡献，并期待在未来能与贵公司继续深化合作，携手提升浦东公交网络安全整体防护水平。

特此致信表扬，谨表谢忱！

上海浦东新区公共交通有限公司

2026年1月29日

14.2政务网络安全管理技术服务项目

14.2.1 项目合同

说明:本项目为上海市浦东新区大数据中心提供协助开展全区党政机关网络安全等级保护工作管理、渗透测试、应急演练、数据安全风险评估、安全培训等工作提供安全服务。

政务网络安全管理技术服务项目合同

合同编码：11NM82P0407620241602

甲方：上海市浦东新区大数据中心

乙方：上海天玺网络技术有限公司

双方同意按下述条款和条件签署本合同（以下简称"合同"）：

1. 合同文件

本合同所附的下列文件是本合同不可分割的组成部分（解释顺序按排列序号）：

（1） 成交通知书；

（2） 供应商提交的响应文件；

（3） 竞争性磋商文件及其附件。

2. 合同范围和条件

本合同的范围和条件应与上述合同文件的规定相一致。

3. 服务范围及内容

本合同所提供服务范围及内容详见"竞争性磋商文件与响应文件"。服务标准以竞争性磋商文件采购需求书中的内容为基础。服务范围及内容应至少满足并涵盖竞争性磋商文件中要求的内容。

4. 合同价格

根据上述合同文件的规定，本合同的合同价格为人民币 1703500 元（大写：壹佰柒拾万零叁仟伍佰元整），分项价格在分项报价表中有明确说明。

5. 支付条件

本项目合同金额采用分期付款方式，在采购人和成交供应商合同签订后，按下款要求支付相

1

应的合同款项。

分期付款，时间进度要求和支付比例具体如下：

（1）合[redacted]司

[redacted]

（2）[redacted]

[redacted]

注：对于满足合同约定支付条件的，甲方应当自收到发票后将资金支付到合同约定的乙方账户，不得以机构变动、人员更替、政策调整等为由延迟付款，不得将采购文件和合同中未规定的义务作为向乙方付款的条件。若甲方逾期支付资金，乙方可依法追究甲方相应的违约责任。

6. 服务时间

自合同签订之日起1年。

7. 履约延误

7.1 乙方应按照合同规定的时间、地点提供服务。

7.2 如乙方无正当理由而拖延服务，甲方有权解除合同并追究乙方的违约责任。

7.3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

8. 误期赔偿除合同第10条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以从应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每周赔偿延期服务的服务费用的百分之零点五（0.5%）计收（一周按七天计算，不足七天按一周计算），直至提供服务为止，但误期赔偿费的最高限额不超过合同价的百分之五（5%）。

乙方通讯地址：上海上海市浦东新区张江高科技园

乙方收件人：吉训敬

18. 补充条款

（1）本合同为中小企业预留合同.

（以下无正文）

甲方（加盖公章或合同章）：上海市浦东新区大数据中心

地点：上海市浦东新区大数据中心

法定代表人或授权代表（签字或盖章）：[illegible]

日期：2024-05-06

乙方（加盖公章或合同章）：上海[illegible]网络技术有限公司

地点：上海上海市浦东新区张江高科技园

法定代表人或授权代表（签字或盖章）：吉训敬

日期：2024-05-06

第三章 采购需求书

一、项目概况

本项目主要服务内容是对浦东新区党政机关重要信息网络系统设施开展网络安全防护、安全评估、渗透测试、应急演练、应急响应和重保等技术服务，完善网络数据安全应急处置机制，支撑新区大数据中心全天候网络安全日常管理，协助网络安全制度体系建设、网络安全绩效管理，协助等保工作推进、数据安全工作推进、漏洞管理和咨询培训等。

二、工作内容

1. 浦东新区网络安全制度体系建设

[redacted]

2. 网络安全绩效管理

[redacted]

3. 威胁情报和漏洞管理

[redacted]

4. 协助开展全区党政机关网络安全等级保护工作管理

[redacted]

5. 数据安全推进工作

[redacted]

6. 重要网站（系统）动态防护服务

[redacted]

7. 区级核心应用系统数据安全风险评估

[redacted]

8. 互联网应用系统渗透测试

协助定期开展全区党政机关互联网系统安全渗透，利用模拟黑客入侵方式对业务进行渗透测试，验证安全漏洞的存在以及防护手段的有效性，服务期内不低于 200 个（次）信息系统并提供整改指导和技术支持。

9. 应急演练

[redacted]

10. 应急响应支撑服务

[redacted]

11. 网络安全保障工作（重保）

[redacted]

12. 网络（数据）安全培训

[redacted]

13. 网络安全咨询服务

[redacted]

14. 采购人安排的其他管理工作

[redacted]

14.2.2 用户评价-感谢信

感 谢 信

上海天泰网络技术有限公司：

2024年是中华人民共和国成立75周年，也是浦东新区数字化转型全面加速之年。为护航浦东数字政府建设，赋能全区安全管理体系建设，天泰团队有效发挥了技术支撑与保障作用，全年全区安全事故“0”发生。在支撑中心网络数据安全日常管理工作中，天泰团队充分展现了卓越的技术能力和专业素养，特别是团队成员朱敏、叶琦等同志更是以高度的责任感和敬业精神，为各项工作任务的圆满完成付出了辛勤努力，特此表扬和感谢。

当前，浦东新区正全力投入社会主义引领区建设，加速推进城市数字化转型，希望贵公司能够继续发挥本地化优势，以一流的专业水准提供一流的服务，进一步助力中心提升网络数据安全绩效管理能力和水平！

上海市浦东新区大数据中心

2024年12月30日

14.3浦东人社局重要信息系统安全保障服务项目

14.3.1 项目合同

说明：本项目为浦东人社局部署在浦东政务云上的业务系统提供等保测评、安全咨询服务、安全培训服务、服务器风险评估、漏扫服务、应急演练、应急响应服务等服务。

合同编号：

技术服务合同

项目名称：2024年浦东人社局重要信息系统安全保障服务项目

委托方（甲方）：上海市浦东新区人力资源和社会保障局

受托方（乙方）：上海天泰网络技术有限公司

签订地点：上海市浦东新区

本合同系由 上海市浦东新区人力资源和社会保障局（以下简称“甲方”）委托 上海天泰网络技术有限公司（以下简称“乙方”） 就 2024 年浦东人社局重要信息系统安全保障服务项目 提供 技术服务工作，并支付相应的技术服务报酬而订立。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》等相关法律、法规的规定，达成如下协议（以下简称“本合同”），并由双方共同恪守。

第一条 甲方委托乙方进行技术服务的内容如下：

1、技术服务的目标：对

2．技术服务的内容：

（1）等保服务：根

（2）网络安全培训：组

（3）应急演练服务：

（4）网络安全检查：对

（5）服务器风险评估服务：对

（6）应用系统漏洞扫描服务：对

[redacted]

(7) 服务器安全核查服务：[redacted]

(8) 应用系统安全防护服务：[redacted]

(9) 资产统计服务：[redacted]

(10) 特权账号管理服务：[redacted]

(11) 网络安全应急保障服务：[redacted]

(12) 网络安全咨询服务：[redacted]

(13) HTTPS 证书：[redacted]

的信息进行加密，确保传输数据不被泄露或篡改。

第二条 乙方应当按下列要求完成技术服务工作：

1．技术服务地点：甲方政务云平台或甲方指定地点。

2．技术服务期限：自合同签订之日起至 2024 年 12 月 5 日。

3．技术服务质量要求：按照甲方要求完成本合同第一条所约定的全部服务，及时完成等保测评工作。

第三条 为保证乙方有效进行技术服务工作，甲方应当向乙方提供下列工作条件和协作事项：

1．提供技术资料：本合同范围内系统的相关技术资料。

2．提供工作条件：乙方提供安全服务时，甲方提供必要的配合支持。

3．甲方提供上述工作条件和协作事项的时间：自合同签订之日起至 2024 年 12 月 5 日。

第四条 甲方向乙方支付技术服务报酬及支付方式为：

1．技术服务费总额为：人民币玖拾柒万捌仟元整（小写：￥978,000.00）。

2．技术服务费由甲方 分期 （一次或分期）支付乙方。

具体支付方式和时间为 [redacted]

乙方开户银行名称、地址和账号为：

开户银行：兴业银行上海张江支行

开户名称：上海天泰网络技术有限公司

银行账号：2165 1010 0100 0086 97

第五条 保密条款

1．乙方安全服务人员不得对甲方/用户的业务系统和数据进行任何违反相关业务制度的增删或修改。在未经甲方书面许可的情况下，不得对甲方业务系统相关数据进行任何形式的复制工作。

2．乙方对于甲方/用户在安全服务过程中提供的有关技术数据或与合同相关

的，受不可抗力影响的一方应及时书面通知对方，并自不可抗力事件发生之日起3日内提供有关机构出具的证明后可以解除本合同，无需向对方承担责任。

第十一条 所有因本合同引起的或与本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议的，则任何一方均有权向本合同签订地有管辖权的人民法院起诉。

第十二条 本合同一式 肆 份，甲方持 叁 份乙方持 壹 份，具有同等法律效力。

第十三条 本合同经双方法定代表人或授权代表签字并盖章后成立。

（以下无正文）

甲方：上海市浦东新区人力资源和社会保障局（盖章）

法定代表人/授权代表：_____（签名）

2024年3月22日

乙方：上海天秦网络技术有限公司（盖章）

法定代表人/授权代表：_____（签名）

2024年3月22日

14.3.2 用户评价-表扬信

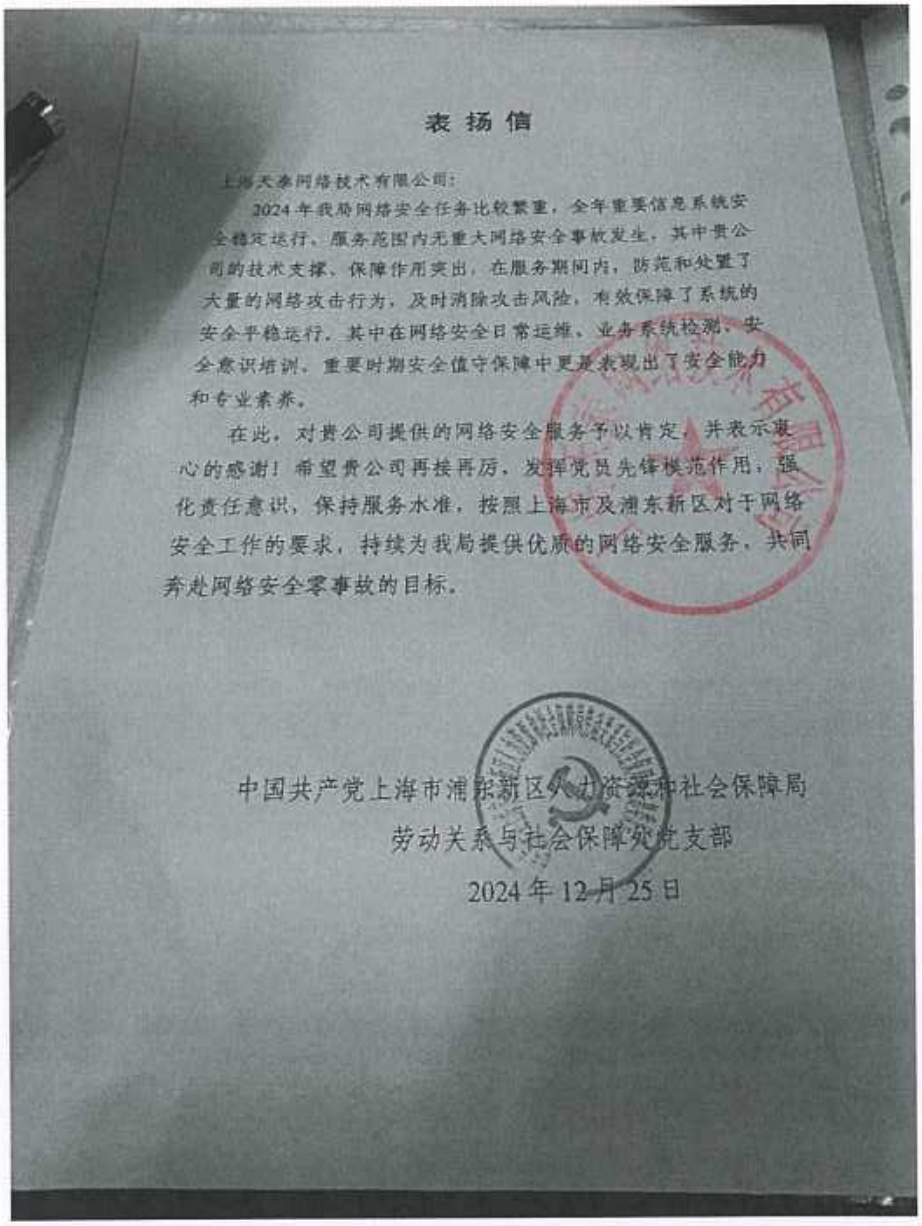


表 扬 信

上海天泰网络技术有限公司：

2024年我局网络安全任务比较繁重，全年重要信息系统安全稳定运行，服务范围内无重大网络安全事故发生，其中贵公司的技术支撑、保障作用突出，在服务期间内，防范和处置了大量的网络攻击行为，及时消除攻击风险，有效保障了系统的安全平稳运行。其中在网络安全日常运维、业务系统检测、安全意识培训、重要时期安全值守保障中更是表现出了安全能力和专业素养。

在此，对贵公司提供的网络安全服务予以肯定，并表示衷心的感谢！希望贵公司再接再厉，发挥党员先锋模范作用，强化责任意识，保持服务水准，按照上海市及浦东新区对于网络安全工作的要求，持续为我局提供优质的网络安全服务，共同奔赴网络安全零事故的目标。

中国共产党上海市浦东新区人力资源和社会保障局

劳动关系与社会保障处党支部

2024年12月25日

14.4浦东城运中心信息系统网络安全服务项目

14.4.1 项目合同

说明：本项目受上海市浦东新区城市运行综合管理中心委托提供网络安全建设与日常管理工作咨询服务、漏洞扫描服务、安全配置管理服务、安全加固服务、重保及应急响应服务、安全整改服务、应急演练、安全培训等服务。

信息系统网络安全服务费项目合同

甲　　方：上海市浦东新区城市运行综合管理中心

乙　　方：上海天泰网络技术有限公司

本合同甲方委托乙方就 信息系统网络安全服务费项目 提供安全服务工作，并支付相应的技术服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下协议，并由双方共同恪守。

第一条 甲方委托乙方进行技术服务的内容如下：

1. 安全建设与日常管理工作咨询：为

2. 漏洞扫描与安全检查服务：

3. 安全配置管理与日常保障服务：

4. 安全加固服务：

5. 重保与应急响应服务：

6. 应急演练服务：

7. 安全培训服务：

宣传政策法规，提高网络安全意识，提升网络安全相关技能；针对城运分中心开展1场网络安全意识培训。

第二条　乙方应当按下列要求完成技术服务工作：

1. 技术服务地点：浦东新区城市运行综合管理中心或甲方指定的地点；

2. 技术服务期限：2024年4月1日至2025年3月31日；

3. 技术服务进度：根据约定的服务周期开展安全服务并出具服务报告，并结合实际运行情况适时调整安全服务频次；

4. 技术服务质量要求：甲方应用系统运行中发生的安全突发事件，乙方给予7*24小时响应和处理。

第三条　为保证乙方有效进行技术服务工作，甲方应当向乙方提供下列工作条件和协作事项：

1. 提供技术资料：本合同范围内系统的相关技术资料。

2. 提供工作条件：在乙方技术人员提供安全服务时，甲方提供必要的配合支持。

第四条　甲方向乙方支付技术服务报酬及支付方式为：

1. 技术服务费总额（含税价）为：人民币玖拾贰万柒仟伍佰元整（小写：￥927,500.00）；

2. 技术服务费由甲方分期（一次或分期）支付乙方。

具体支付方式和时间为（以下各项均以甲方收到乙方等额有效发票为付款前提）：

[redacted]

表签字后生效。

（以下无正文）

甲方（盖章）：

单位名称：上海市浦东新区城市运行综合管理中心

乙方（盖章）：

单位名称：上海大泰网络技术有限公司

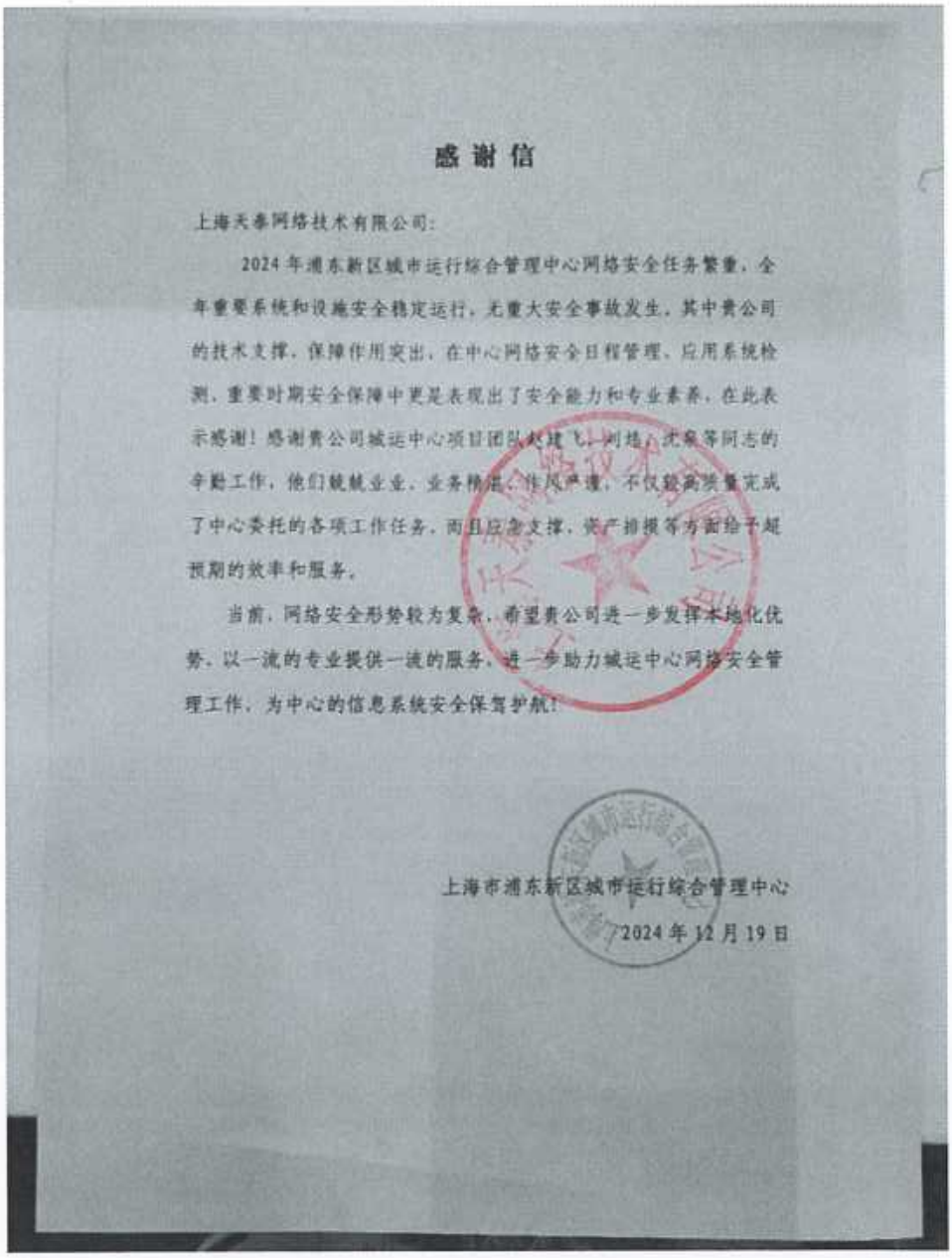
法定代表人或授权代表人：

日期：2024年3月29日

法定代表人或授权代表人：

日期：2024年3月29日

14.4.2 用户评价-感谢信



感谢信

上海天泰网络技术有限公司：

2024年浦东新区城市运行综合管理中心网络安全任务繁重，全年重要系统和设施安全稳定运行，无重大安全事故发生，其中贵公司的技术支撑，保障作用突出，在中心网络安全日程管理、应用系统检测，重要时期安全保障中更是表现出了安全能力和专业素养，在此表示感谢！感谢贵公司城运中心项目团队赵建飞、刘旭、尤泉等同志的辛勤工作，他们敬业业，业务精湛，作风严谨，不仅能高质量完成了中心委托的各项工作任务，而且应急支撑，资产排摸等方面给予超预期的效率和服务。

当前，网络安全形势较为复杂，希望贵公司进一步发挥本地化优势，以一流的专业提供一流的服务，进一步助力城运中心网络安全管理工作，为中心的信息系统安全保驾护航！

上海市浦东新区城市运行综合管理中心

2024年12月19日

14.5信息系统网络安全服务项目

说明：本项目为浦东应急局测评前提供安全加固整改、安全建设与日常管理工作、漏扫与安全检查服务。

信息系统网络安全服务项目合同

甲方：上海市浦东新区应急管理局

乙方：上海天泰网络技术有限公司

根据《中华人民共和国民法典》等法律、法规之有关规定，为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，就有关事宜达成如下协议：

第一条：项目内容

1.安全建设与日常管理工作咨询服务

2.漏洞扫描与安全检查服务

3. 安全加固整改指导服务

4. 重保与应急响应服务

[redacted]

第二条：项目要求及进度

合同服务期限：2024 年 4 月 1 日 至 2025 年 3 月 31 日

1. 根据甲方的要求及时开展服务，在服务完成后出具相应的报告；

2. 甲方服务范围内的安全技术问题和安全管理问题，乙方给予 5*8 小时响应和处理。

第三条：项目经费使用及支付方式

1. 项目经费确保专款专用。

2. 合同价款总额为：（大写）人民币陆拾玖万捌仟元整（小写：￥698,000.00）

3. 支付方式为分期支付，具体支付方式和时间如下：

[redacted]

甲方（公章）

法定代表人/授权代

地址：浦东新区迎[illegible]

电话：38939771

签约日期：　　年　月　日

乙方（公章）

法定代表人/授权代表人：

地址：浦东新区[illegible]路88弄1号楼901

电话：50391981

签约日期：2024年 3月 29日

14.62025 年浦东新区建交委网络安全等保建设项目

说明：本项目为浦东建交委部署在浦东新区政务云上的信息系统提供安全防护服务、等保整改等服务。

14.6.1 项目合同

2025年浦东新区建交委网络安全等保建设项目的合同

合同统一编号： 11N00245642320251202

合同内部编号：

合同各方：

甲方：上海市浦东新区建设和交通委员会

地址：世纪大道2001号

邮政编码：

电话

传真：

联系人：

乙方：上海天泰网络技术有限公司

法定代表人：吉训敢（男）

地址：中国（上海）自由贸易试验区盛荣路88弄1号9层01室

邮政编码：201203

电话：

传真：

联系人：

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1 乙方根据本合同的规定向甲方提供以下服务：

1.1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见招标文件和投标文件。

2 合同价格、服务地点和服务期限

2.1 合同价格

本合同价格为1683377.52元整（大写：壹佰陆拾捌万叁仟叁佰柒拾柒元伍角贰分）。

20.3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21 合同修改

21.1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）：

法定代表人或授权委托人（签章）：

日期：

乙方（盖章）：

法定代表人或授权委托人（签章）：

日期：2025年05月30日

合同签订点：网上签约

9 招标内容与质量要求

9.1 工作目标与总体要求

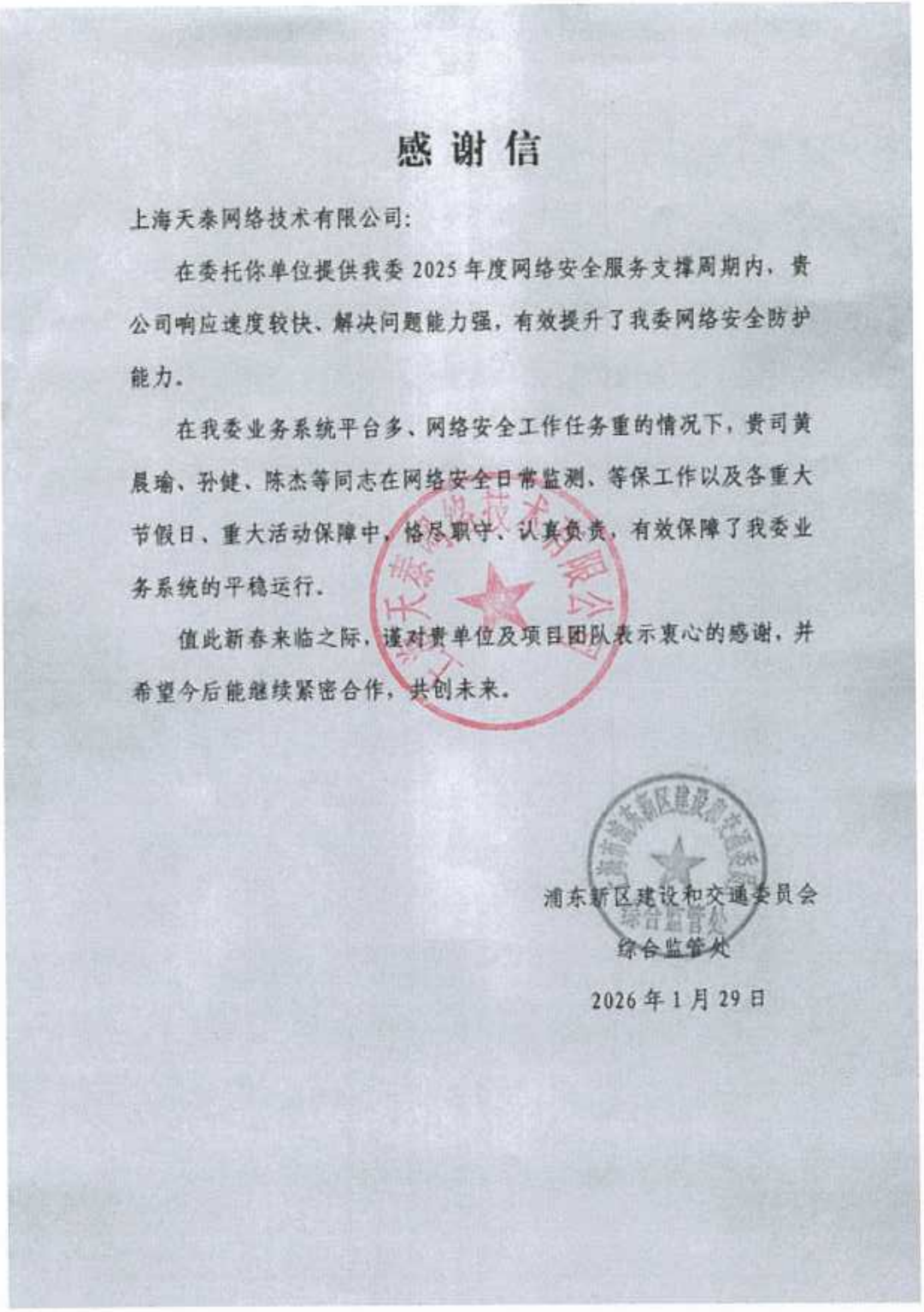
依据国家信息安全等级保护制度，遵循国家及上海市相关标准规范，明确信息安全保障重点，建立信息安全等级保护工作机制，切实提高医院的信息安全防护能力、隐患发现能力、应急处置能力，进一步加强核心系统数据的安全管理，有效满足系统的可靠性、安全性、稳定性和先进性要求，为单位信息化健康发展提供可靠保障，全面维护患者利益、公共利益和社会秩序。

9.2 本项目招标内容与具体质量要求（但不仅限于）详见下表。

服务内容一览表（工作量清单）

序号	服务内容	分项内容	数量	服务要求	备注
1	等保安全服务	等保二级差距评估服务	1		
		等保二级整改服务	1		
		等保二级级测评协助	1		
		等保三级差距评估服务	1		
		等保三级整改服务	1		
		等保三级级测评协助	1		
2	等保测评服务	等保二级测评	1		
		等保三级测评	1		
3	渗透测试服务	渗透测试服务	1		
4	安全防护服务	云上系统安全防护-防篡改服务	24		
		云上系统安全防护-日志审计服务	4		
		云上系统安全防护-运维审计服务	4		
		云上系统安全防护-数据库审计服务	2		

14.6.2 用户评价-感谢信



感谢信

上海天泰网络技术有限公司:

在委托你单位提供我委2025年度网络安全服务支撑周期内，贵公司响应速度较快、解决问题能力强，有效提升了我委网络安全防护能力。

在我委业务系统平台多、网络安全工作任务重的情况下，贵司黄晨瑜、孙健、陈杰等同志在网络安全日常监测、等保工作以及各重大节假日、重大活动保障中，恪尽职守、认真负责，有效保障了我委业务系统的平稳运行。

值此新春来临之际，谨对贵单位及项目团队表示衷心的感谢，并希望今后能继续紧密合作，共创未来。

浦东新区建设和交通委员会

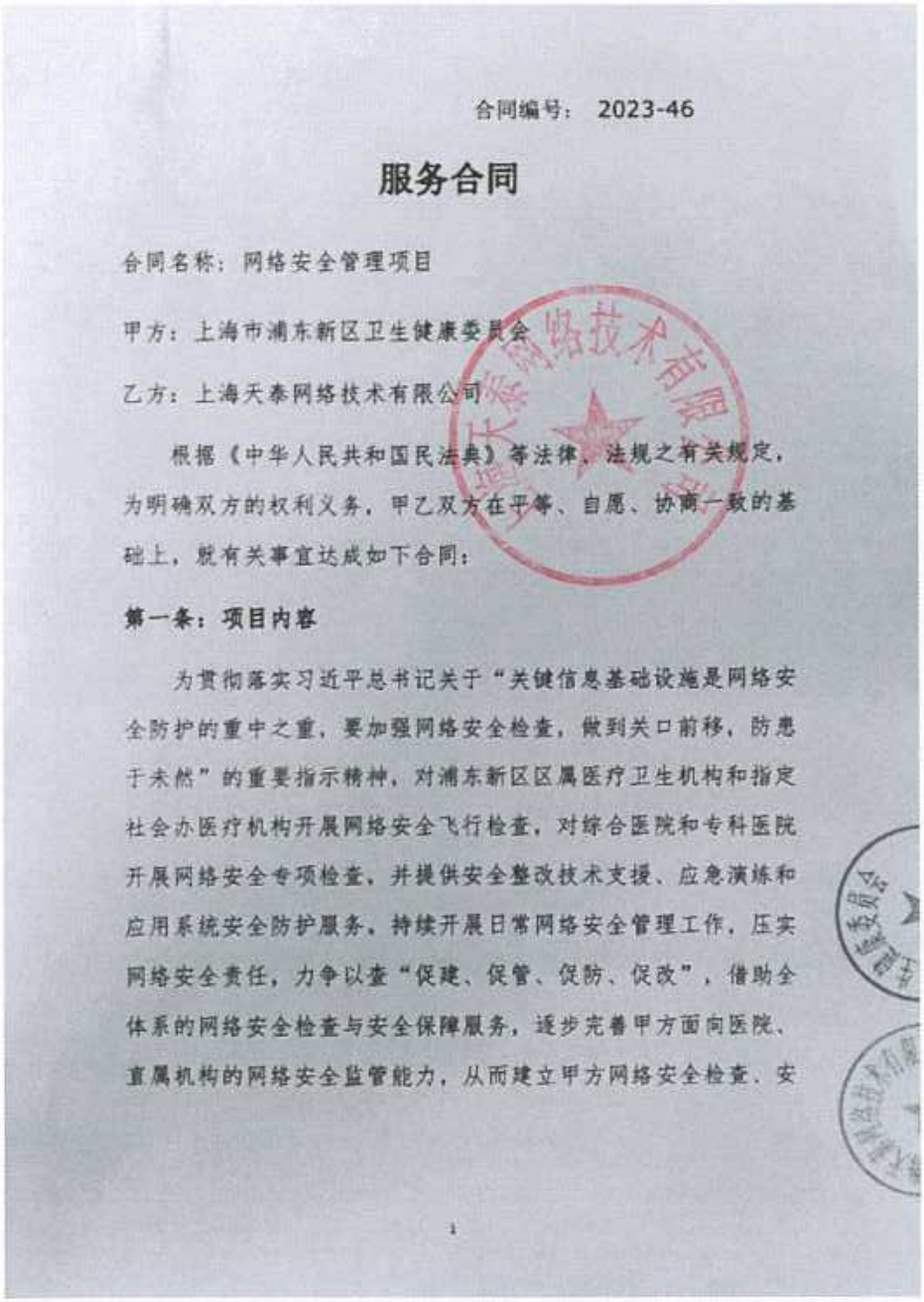
综合监管处

2026年1月29日

14.7浦东卫健委网络安全管理服务项目

14.7.1 项目合同

说明：本项目为浦东卫健委部署在浦东新区政务云上的信息系统提供安全整改技术支援、应急演练和应用系统安全防护服务等服务。



合同编号： 2023-46

服务合同

合同名称：网络安全管理项目

甲方：上海市浦东新区卫生健康委员会

乙方：上海天奉网络技术有限公司

根据《中华人民共和国民法典》等法律、法规之有关规定，为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，就有关事宜达成如下合同：

第一条：项目内容

为贯彻落实习近平总书记关于“关键信息基础设施是网络安全防护的重中之重，要加强网络安全检查，做到关口前移，防患于未然”的重要指示精神，对浦东新区区属医疗卫生机构和指定社会办医疗机构开展网络安全飞行检查，对综合医院和专科医院开展网络安全专项检查，并提供安全整改技术支援、应急演练和应用系统安全防护服务，持续开展日常网络安全管理工作，压实网络安全责任，力争以查“促建、促管、促防、促改”，借助全体系的网络安全检查与安全保障服务，逐步完善甲方面向医院、直属机构的网络安全监管能力，从而建立甲方网络安全检查、安

1

全通报和安全整改等环环相扣的网络安全监管和服务的管理闭环。

第二条：项目内容

1、网络安全飞行检查：依[redacted]

2、网络安全专项检查：[redacted]

3、安全整改技术支援：针[redacted]

4、应急演练：开[redacted]

5、应用系统安全防护服务：[redacted]

6、服务期限：自合同签订之日起至2023年12月31日前完成。

第三条：项目经费使用及支付方式

1.项目经费确保专款专用。

2.合同价款总额为：897500元(大写：捌拾玖万柒仟伍佰圆整)。

[redacted]

第四条：双方权利和义务

(一)甲方权利、义务

1.甲方有权在项目实施过程中，随时了解掌握项目工作进度及资金使用情况，乙方应予配合。

2.协调乙方在提供服务过程所需的相关信息。

(二)乙方权利、义务

1.乙方应定期向甲方汇报项目进展情况。

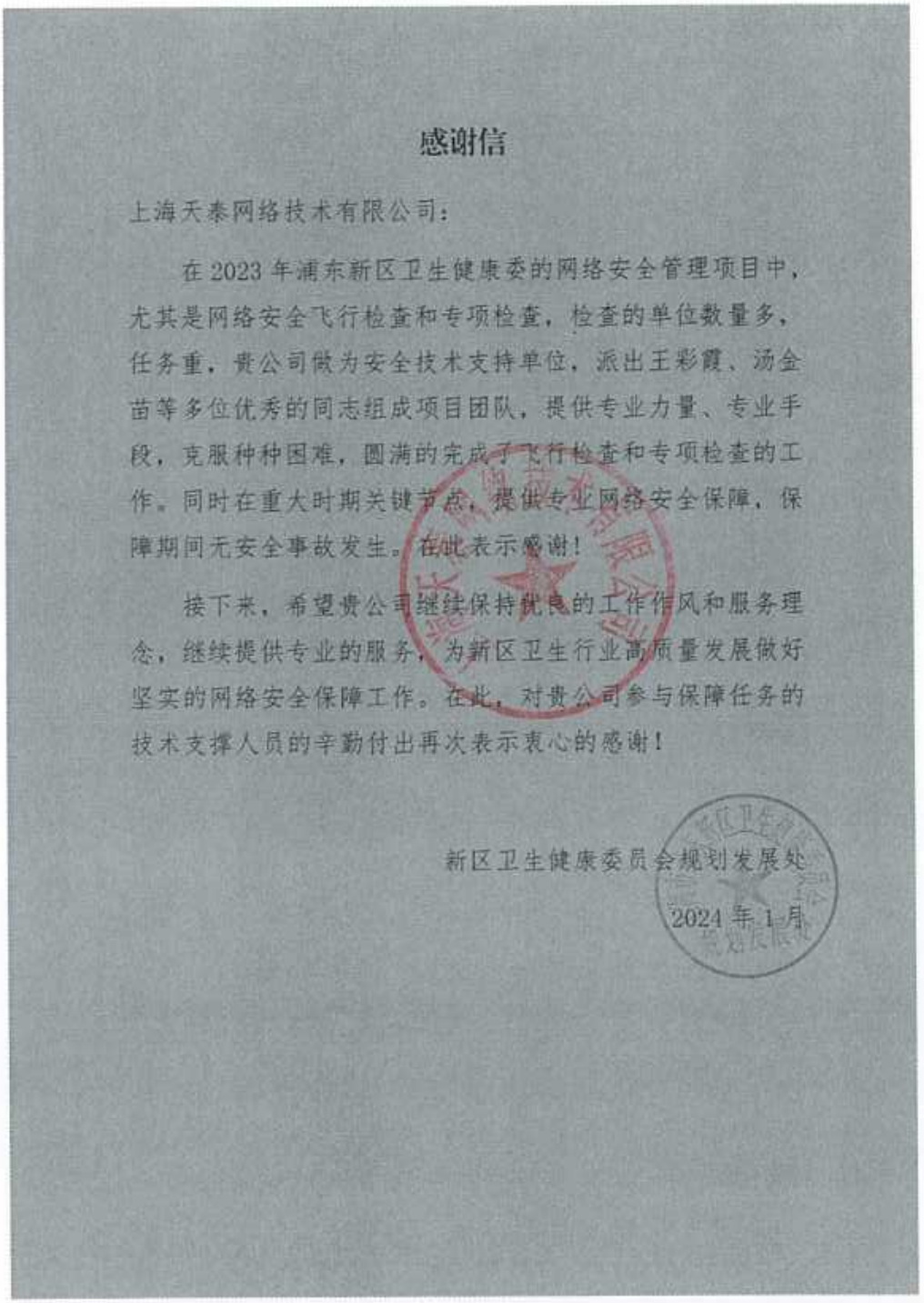
2.乙方在履行合同过程中，不得将服务项目委托给第三人，应按时、按标准完成项目任务。

第五条：完成项目的形式和验收标准

（以下为签字页，无正文）

甲方（公章）	乙方（公章）
授权代表或法定代表人：	授权代表或法定代表人：
地址：上海市浦东新区成山路990号	地址：浦东盛荣路88弄1号901室
电话：38583226	电话：50391981
签约日期：2023.5.6	签约日期：2023.5.6

14.7.2 用户评价-感谢信



感谢信

上海天泰网络技术有限公司：

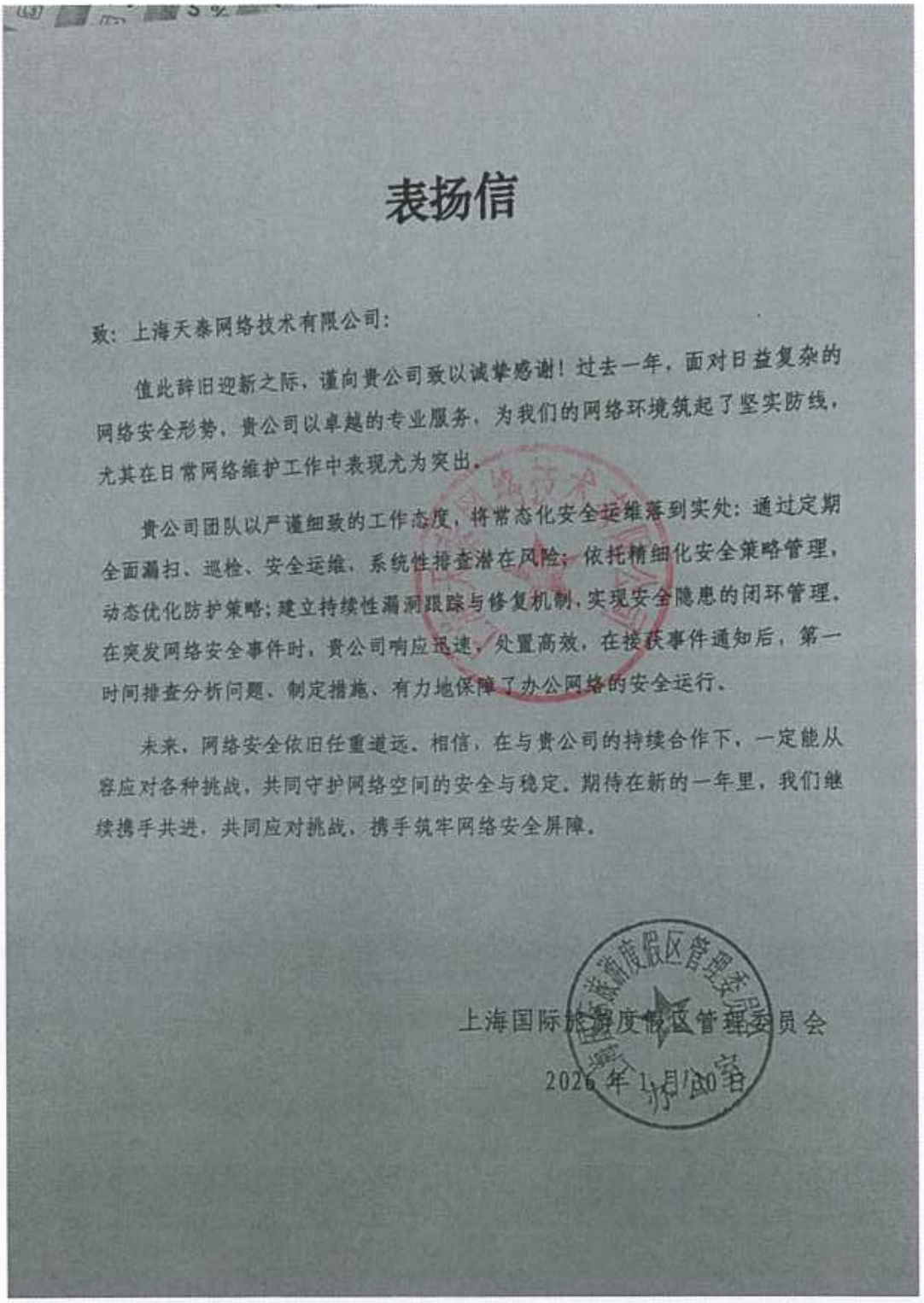
在2023年浦东新区卫生健康委的网络安全管理项目中，尤其是网络安全飞行检查和专项检查，检查的单位数量多，任务重，贵公司做为安全技术支持单位，派出王彩霞、汤金苗等多位优秀的同志组成项目团队，提供专业力量、专业手段，克服种种困难，圆满的完成了飞行检查和专项检查的工作。同时在重大时期关键节点，提供专业网络安全保障，保障期间无安全事故发生。在此表示感谢！

接下来，希望贵公司继续保持优良的工作作风和服务理念，继续提供专业的服务，为新区卫生行业高质量发展做好坚实的网络安全保障工作。在此，对贵公司参与保障任务的技术支撑人员的辛勤付出再次表示衷心的感谢！

新区卫生健康委员会规划发展处

2024年1月

14.8获得用户认可的证明材料



表扬信

致：上海天泰网络技术有限公司：

值此辞旧迎新之际，谨向贵公司致以诚挚感谢！过去一年，面对日益复杂的网络安全形势，贵公司以卓越的专业服务，为我们的网络环境筑起了坚实防线，尤其在日常网络维护工作中表现尤为突出。

贵公司团队以严谨细致的工作态度，将常态化安全运维落到实处：通过定期全面漏扫、巡检、安全运维，系统性排查潜在风险；依托精细化安全策略管理，动态优化防护策略；建立持续性漏洞跟踪与修复机制，实现安全隐患的闭环管理。在突发网络安全事件时，贵公司响应迅速，处置高效，在接获事件通知后，第一时间排查分析问题、制定措施、有力地保障了办公网络的安全运行。

未来，网络安全依旧任重道远。相信，在与贵公司的持续合作下，一定能从容应对各种挑战，共同守护网络空间的安全与稳定。期待在新的一年里，我们继续携手共进，共同应对挑战，携手筑牢网络安全屏障。

上海国际旅游度假区管理委员会

2026年1月30日

感谢信

致：上海天泰网络技术有限公司

上海市浦东新区规划管理事务中心（上海市浦东新区城市规划和公共艺术中心）谨此致信，对贵公司在2025年度为我中心“公众号项目”提供的专业网络安全服务表示高度认可与衷心感谢。

为保障我中心浦东新区城市规划和公共艺术中心公众移动综合服务平台的安全稳定与合规运营，在服务期间贵公司团队围绕网络安全等级保护测评、云平台安全防护、渗透测试、漏洞扫描及人员培训等核心内容，提供了全面、有效的技术支持。通过专业的服务，有力保障了平台对外服务的连续性与数据安全性。

贵公司项目团队，特别是黄晨瑜、孙健、陈杰等主要成员，在整个服务过程中展现出严谨负责的工作态度、扎实精湛的专业水准以及高效的协同精神，其工作成果获得了我中心的一致好评。我们对此表示诚挚谢意，并期待未来能继续携手，深化合作。

特此表扬，顺致谢忱！

上海市浦东新区规划管理事务中心

（上海市浦东新区城市规划和公共艺术中心）

2026年1月29日

感 谢 信

上海天泰网络技术有限公司：

上海市浦东新区医疗急救中心向天泰团队表示最诚挚的感谢。在2025年度网络安全技术服务工作开展过程中，天泰团队以高度的专业能力和严谨的工作作风，为我单位提供了全面、系统、高质量的安全保障支持。围绕网络安全管理服务、网络安全技术服务及应急保障服务三大方向，天泰团队在安全制度建设、风险排查与整改、安全加固实施、技术支撑以及应急响应处置等方面持续发力，有效提升了我单位整体安全防护水平。

在服务实施过程中，天泰团队娄向医、汤金苗、王彩霞等同志始终坚持规范化、专业化的工作要求，积极沟通协作，响应迅速、处置得当，高标准推进各项服务任务落实，充分展现了扎实的技术实力和良好的服务意识，为我单位网络与信息安全运行提供了有力支撑。

通过双方密切配合，我单位网络与信息安全管理体系更加规范，安全运行保障能力显著增强，为业务系统稳定运行和数据安全提供了坚实基础。

在此，我单位对天泰团队的辛勤付出和专业贡献表示衷心感谢！期待未来继续深化合作，共同推进网络安全建设水平不断提升。

上海市浦东新区医疗急救中心

2026年1月29日

感谢信

致上海天泰网络技术有限公司：

值此辞旧迎新之际，谨向贵公司致以诚挚感谢！过去一年，面对日益复杂的网络安全形势，贵公司以卓越的专业服务，为我们的网络环境筑起了坚实防线，尤其在日常网络维护工作中表现尤为突出。

贵公司团队以严谨细致的工作态度，将常态化安全运维落到实处：通过定期全面巡检、安全运维，系统性排查潜在风险；依托精细化安全策略管理，动态优化防护策略；建立持续性漏洞跟踪与修复机制，实现安全隐患的闭环管理。在突发网络故障时，贵公司响应迅速、处置高效：在接获故障通知后，第一时间选派经验丰富、技术精湛的工程师火速奔赴现场，指查分析问题、制定措施、高效有序地开展网络故障修复工作，有力地保障了办公网络的持续稳定运行。

尤其值得肯定的是，贵团队定期协助我方开展信息资产的系统化梳理与动态更新，使我们能够清晰掌握资产状况，为精准防护奠定了坚实基础。在此，特别感谢项目经理曹兴戴及其团队展现的高度责任心、卓越专业能力和始终如一的辛勤付出，这已成为我方网络安全工作稳步推进的重要支撑与保障。

未来，网络安全依旧任重道远。我们坚信，在与贵公司的持续合作下，一定能从容应对各种挑战，共同守护网络空间的安全与稳定。期待在新的一年里，我们继续携手共进，共同应对挑战，携手筑牢网络安全屏障。

上海市浦东新区疾病预防控制中心

（上海市浦东新区卫生健康监督所）

2026年1月22日

感谢信

致：上海天泰网络技术有限公司

上海市浦东新区建设市场管理事务中心谨以此信，对贵公司在 2025 年度为我中心提供的全面、专业的网络安全服务表示高度赞许与衷心感谢。

2025 年，为确保我中心业务系统稳定运行与数据安全，在服务期内，贵公司团队展现出高度的专业性与责任心，围绕服务器安全配置核查与加固、定期漏洞扫描、网络设备深度巡检等核心工作，提供了系统化的技术保障。贵公司组织开展的网络安全意识培训与实战化应急演练，显著提升了我中心全员的防护意识与协同处置能力。

尤为值得肯定的是，以黄晨瑜、孙健、陈杰等同志为主要成员的服务团队，工作作风严谨扎实，服务响应及时高效。他们不仅技术功底深厚，更具备良好的沟通能力与服务意识，贵公司团队全年不懈的努力，为我中心构建主动、可控的网络安全防御体系提供了有力支撑，有效提升了整体安全防护水平。我们对本次合作深感满意，并对贵公司团队的专业付出表示诚挚的谢意。期待未来能继续与贵公司携手，共同筑牢网络安全的坚固防线。

特此致信表扬，以表谢忱！

上海市浦东新区建设市场管理事务中心

2025 年 1 月 29 日

感谢信

致：上海天泰网络技术有限公司

上海浦东新区公共交通有限公司谨以此信，对贵公司在2025年度“浦东公交网络安全服务采购项目”中提供的全方位、高质量网络安全服务表示高度认可与衷心感谢，并对项目团队的专业精神与突出贡献提出表扬。

2025年度，我公司网络安全工作面临保障范围广、实时性要求高、潜在风险点多等挑战。贵公司组建了以孙健、黄晨瑜、陈杰等同志为核心的专业服务团队，为我司提供了涵盖等保测评咨询、常态化安全检测、应急响应保障、实战化演练及人员培训等系列服务。服务期间，团队展现出了卓越的技术素养与高度的责任感，为浦东公交的日常运营与公众服务提供了坚实可靠的安全屏障。

本次合作充分证明贵公司是一家值得信赖的网络安全服务提供商。我们诚挚感谢贵公司及项目团队全年的辛勤付出与卓越贡献，并期待在未来能与贵公司继续深化合作，携手提升浦东公交网络安全整体防护水平。

特此致信表扬，谨表谢忱！

上海浦东新区公共交通有限公司

2026年1月29日

信息管理部

感 谢 信

上海天泰网络技术有限公司：

2025 年贵公司的安全服务团队在保障网络安全、防范网络攻击和应急保障等方面展现出了卓越的专业素养、技术实力和响应速度。

在今年的各项重保工作期间，服务团队恪尽职守、兢兢业业，全程在线，包括安全检查、漏洞扫描、安全设备巡检，并及时汇报当天工作内容，发现漏洞在第一时间内通知并协助进行整改，在保障期间，每日对平台进行安全巡检，7*24 响应和值守，防范和处置了大量的网络攻击行为，及时消除攻击风险，有效保障了系统的安全平稳运行，最终圆满完成了各项重保工作，在各方共同努力之下，年度服务范围内无重大网络安全事件发生。

基于以上，我委对贵公司提供的网络安全服务予以肯定，并对贵公司参与重保任务的技术支撑人员的辛勤付出表示衷心的感谢！希望贵公司再接再厉，强化责任意识，保持服务水准，按照上海市及浦东新区对于网络安全工作的要求，持续为我委提供优质的网络安全服务，共同奔赴网络安全零事故的目标。

上海市浦东新区科技和经济委员会办公室

2026 年 1 月 29 日

表扬信

上海天泰网络技术有限公司：

在 2025 年度浦东新区政务服务中心信息化及网络安全防护保障服务项目实施过程中，贵团队以高度的专业素养和高效协作能力，出色完成了各项任务，展现了务实担当、精益求精的工作作风，为中心信息化系统的稳定运行与安全防护提供了全方位保障。

项目期间，贵团队刘炜、沈晓勇同志恪尽职守、兢兢业业，始终以严谨细致的态度落实各项任务，确保工作高效、稳定推进。尤其在 2025 年度护网行动期间，贵团队凭借专业的技术支撑筑牢网络安全防线，实现网络安全“零事件”。

在此，谨向贵团队全体成员表示衷心感谢！同时，对刘炜、沈晓勇同志的专业表现提出特别表扬！

希望在未来的工作中，贵团队再接再厉，继续发扬专业精神，为中心信息化及网络安全防护提供更加坚实、可靠的支持。

再次感谢贵团队的辛勤努力与突出贡献！

上海市浦东新区政务服务中心

2026 年 2 月

十五、 合同模板

[合同中心-合同名称]

合同统一编号：[合同中心-合同编码]

合同内部编号：

合同各方：

甲方：[合同中心-采购单位名称]

地址：[合同中心-采购单位所在地]

电话：[合同中心-采购单位联系人电话]

联系人：[合同中心-采购单位联系人]

[供应商信息-联合体]

根据《中华人民共和国政府采购法》《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1. 乙方根据本合同的规定向甲方提供以下服务：

1.1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见合同附件。

2. 合同价格、服务地点和服务期限

2.1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2.2 服务地点

2.3 服务期限

本服务的服务期限：[合同中心-合同有效期]。

3. 质量标准和要求

3.1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准

确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的， 按照通常标准或者符合合同目的的特定标准确定。
3.2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4. 权利瑕疵担保
4.1 乙方保证对其交付的服务享有合法的权利。
4.2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。
4.3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权利。
4.4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5. 验收
5.1 项目考核指标：在服务周期内，如因乙方网络安全服务范围内原因导致甲方发生各级网络安全通报事件，每发生一起，将对乙方处以人民币 10000 元的考核扣款。

5.2 项目成果：项目验收前，乙方需提供所有网络安全服务，并提交《阶段性服务报告》和《项目总结报告》。

5.3 验收的地点：现场。

6. 保密
6.1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7. 付款
7.1 本合同以人民币付款（单位：元）。
7.2 本合同款项按照以下方式支付。

7.2.1 付款内容：（分期付款）
7.2.2 付款条件：

[合同中心-支付方式名称]
（1） 合同签订后的一个月内支付合同价款的 40%；
（2） 服务满半年，开展阶段性工作评估，通过后的十五个工作日内支付合同价款的 30%；
（3） 服务期满，验收通过后的十五个工作日内支付合同价款的 25%；
（4） 项目通过第三方审价后，根据审价结果，支付剩余 5%尾款。

7.2.3 本合同中的费用由甲方指定的 4 家直属企业（使用单位）向乙方支付，每次付款前，乙方需向甲方的四家直属企业分别开具该次支付总金额四分之一的增值税专用发票(税率为 6%)。

使用单位名称 1：上海浦东新区杨高公共交通有限公司
地址：上海市浦东新区邹平路 191 号
统一社会信用代码：91310115630867864Q
开户银行：工商银行浦东分行
账号：1001182609004653427

使用单位名称 2：上海浦东新区上南公共交通有限公司
地址：上海市浦东新区高科西路 1758 号
统一社会信用代码：91310115741193735Y
开户银行：工行陆家嘴支行
账号：1001182609004656532

使用单位名称 3：上海浦东新区金高公共交通有限公司
地址：上海市浦东新区金高路 1500 号
统一社会信用代码：91310115630479685E
开户银行：工商银行浦东分行
账号：1001280909004636869

使用单位名称 4：上海浦东新区南汇公共交通有限公司
地址：上海市浦东新区下盐路 7300 号
统一社会信用代码：913101156309092359
开户银行：交通银行上海南汇支行
账号：310069105018003622738

8. 甲方（甲方）的权利义务
8.1 甲方有权在合同规定的范围内享受，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。
8.2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。
8.3 由于乙方服务质量或延误服务的原因，使甲方有关或设备损坏造成经济损失的， 甲方有权要求乙方进行经济赔偿。
8.4 甲方在合同规定的服务期限内有义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。
8.5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。
8.6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知

乙方涉及合同服务范围调整的，应与乙方协商解决。

9. 乙方的权利与义务

9.1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9.2 乙方为了更好地进行服务，满足甲方对服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时，可以要求甲方进行合作配合。

9.3 如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。

9.4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9.5 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9.6 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9.7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供服务的费用。

9.8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10. 补救措施和索赔

10.1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10.2 在服务期限内，如果乙方对提供服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1） 根据服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低服务的价格。

（2） 乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3） 如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11. 履约延误

11.1 乙方应按照合同规定的时间、地点提供服务。

11.2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11.3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后， 应尽快对情况进行评价，并确定是否同意延期提供服务。

12. 误期赔偿

12.1　除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期服务的服务费用的百分之零点五（0.5%）计收，直至提供服务为止。 但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足 七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13. 不可抗力

13.1　如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13.2　本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件， 但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13.3　在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受 不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行 合同的协议。

14. 争端的解决

14.1　合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调 解。

14.2　调解不成则提交提交上海市浦东新区人民法院诉讼解决。

14.3　如诉讼事项不影响合同其它部分的履行，则在诉讼期间，除正在进行诉讼的部分外，本合同的其它部分应继续执行。

15. 违约终止合同

15.1　在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）　如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

（2）　如果乙方未能履行合同规定的其它义务。

15.2　如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

16. 破产终止合同

16.1　如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

17. 合同转让和分包

17.1　除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

18. 合同生效
18.1　本合同在合同各方签字盖章后生效。
18.2　本合同一式三份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

19. 合同附件
19. 1 本合同附件包括：　招标(采购)文件、投标（响应）文件
19. 2 本合同附件与合同具有同等效力。
19. 3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

20. 合同修改
20.1　除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）：

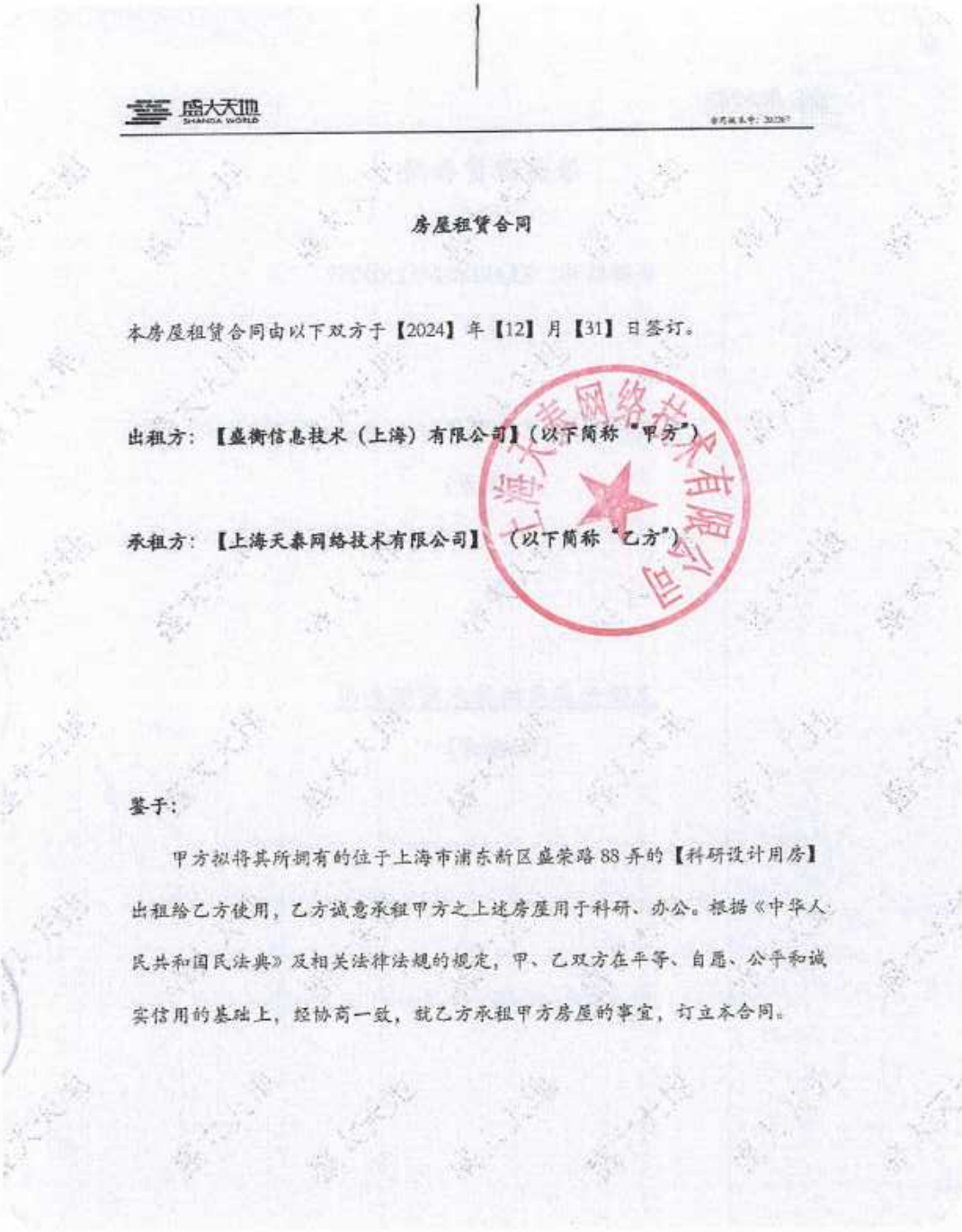
法定代表人或授权委托人（签章）：

[供应商法定代表人-联合体]

合同签订点：网上签约

十六、 本地化服务证明

天泰网络注册及经营地为上海市浦东新盛荣路 88 弄 1 号楼 901 室，具备本地化服务的能力。



盛大天地 SHANDA WORLD

房屋租赁合同

本房屋租赁合同由以下双方于【2024】年【12】月【31】日签订。

出租方：【盛衡信息技术（上海）有限公司】（以下简称"甲方"）

承租方：【上海天泰网络技术有限公司】（以下简称"乙方"）

鉴于：

甲方拟将其所拥有的位于上海市浦东新区盛荣路 88 弄的【科研设计用房】出租给乙方使用，乙方诚意承租甲方之上述房屋用于科研、办公。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、公平和诚实信用的基础上，经协商一致，就乙方承租甲方房屋的事宜，订立本合同。

第一条 租赁房屋的基本情况

1. 甲方出租给乙方的房屋位于上海市浦东新区盛荣路88弄（以下简称“本项目”）的1号-901室（以下简称“租赁房屋”、“该房屋”），该房屋建筑面积[redacted]乙方明确，本合同本条所述之房屋位于的楼栋号及/或楼层及/或室号实为甲方自行编排，如不同于实际楼栋号及/或楼层及/或室号，乙方不会因为该编排之楼栋号及/或楼层及/或室号与政府部门登记备案的楼层及/或室号之间有差异，而单方面向甲方提出解除本合同及/或向甲方提出任何索赔要求或任何其他形式的权利主张。本合同签署前，乙方已对该房屋进行了实地勘测，对房屋建筑面积确认无误，并确认该房屋的租金、物业管理费或其他根据该房屋面积计算的款项均以本款规定的建筑面积为计算基数。该房屋的平面图见本合同附件一标记的位置及范围。
2. 乙方租赁该房屋的用途仅限于【科研、办公】。在租赁期限内，非经甲方事先书面同意并按规定经政府有关部门审批、核准通过前，乙方不得擅自改变该房屋的用途。否则，乙方应自行承担由此产生的全部法律后果。
3. 本合同签署前，乙方已现场查看租赁房屋并对该房屋权属、土地性质、房屋现状、附属设施设备、市政规划、园区配套设施、周边环境、交通流量、交通状况、噪音污染及相关其他情况作了充分了解及评估，并对因此给日后房屋装修（若需）、后续使用行为的影响承担全部责任。
4. 租赁房屋的公用或合用部位的使用范围、条件和要求，以及现有装修、附属设施设备状况和其他有关事宜，由甲、乙双方在本合同附件二中加以列明。甲、乙双方同意该附件作为甲方向乙方交付租赁房屋和本合同终止/解除时乙方向甲方返还租赁房屋的验收依据。
5. 在签订本合同前，甲方已告知乙方：该租赁房屋已设定抵押。

第二条 房屋的租赁期限与免租期

十七、 供应商认为需加以说明的其他内容

17.1天泰网络基本情况

上海天泰网络技术有限公司（以下简称：天泰或天泰网络或天泰公司或上海天泰）成立于 2007 年，注册资本 3300 万元，天泰在信息加密、身份认证、传输管理、协议分析、应用攻防等技术方面有深厚的积累和独到的创新。自研的 WEB 应用防火墙已保护着上千家政府机构、企业和事业单位的 WEB 信息系统，作为 WAF 产品国家标准和行业标准的制定单位之一，应用安全能力赢得行业和用户的广泛认可。

天泰网络将网络安全产品服务化的理念与用户需求相结合，开创了全新的网络和数据安全服务模式，全力确保用户核心应用网络合规、安全、可用、可视。

天泰重视企业文化建设，将建设一流网络安全企业作为企业的经营目标，以“包容、诚信、效率和优质”作为天泰研究、开发和营销工作的精髓和公司的文化核心，在应用安全与保障领域建立国内一流的技术、产品和服务能力，用可靠的队伍、先进的技术和优异的服务报效国家、贡献社会、服务人民。

天泰用户群体：

- 党政行业
- 教育行业
- 卫生行业
- 旅游行业
- 水利行业
- 司法行业
- 国有企业

天泰参与的国家部委行业的安全项目：

- 公安部等级保护中心核心应用系统安全防护项目

- 质检总局特种设备管理系统安全保障项目
- 食药监总局综合门户系统安全防护项目
- 文化部文化交流中心门户网站安全系统
- 国家人力资源和社会保障部教育考试系统安全项目
- 解放军后勤保障部卫生信息系统安全项目
- 民政部福彩中心网络应用安全项目
- 水利部珠江水利中心网络安全保障服务项目
- 上海世博会应用安全项目
- 杭州 G20 峰会应用安全防护项目

天泰参与的上海市网络安全建设项目：

- 市直属部门的 WAF 集采项目（公安、教委、口岸办、工商等）
- 应用安全保障平台 AAP
- 中小企业安全服务平台
- 区块链安全服务平台
- 安全混合云项目
- 关键信息基础设施安全申报系统
- 工业控制信息安全管理系统
- 网络安全管理绩效考核系统

天泰参与的浦东新区网络安全项目：

- 浦东新区大数据中心政务网络安全管理技术服务项目
- 浦东教育学校与数据中心应用安全系统
- 浦东卫健委网络安全管理服务项目
- 浦东政务云网络安全运维项目
- 浦东应急局网络安全服务项目
- 浦东城运中心网络安全保障服务
- 浦东发改委信用管理系统安全检查与整改项目
- 浦东建交委应用系统安全服务
- 浦东规化资源局信息系统安全服务保障
- 人大、科经委、财政局、人社局、知识产权局、度假区管委会、世博管理局等单位安全服务保障项目

- 新区国有企业网站安全检查评估项目（陆家嘴集团、浦发集团、张江集团等）
- 浦东区属医疗机构（卫发院、卫监所、急救中心、牙防所、北蔡/上钢/航头/老港等社区医院）单位的安全服务与保障

17.2公司发展历程

天泰公司的发展历程如下：

2007 年 6 月 12 日注册成立，注册地浦东张江。

2008 年天泰被认定为“软件企业”，企业向市场推出 WEB 应用防火墙产品。

2009 年天泰 WAF 产品获得公安部、工信部、保密局和军队的安全产品认证。

2010 年天泰 WAF 产品被上海世博会选用，顺利保障上海世博会应用系统运行 184 天。

2011 年 11 月天泰作为 WAF 产品国家标准的制定组长单位，参与 WAF 产品的国家标准的制定。

2012 年 11 月受公安部第三研究所邀请，天泰参与 Web 安全评估和 Web 安全防护产品行业标准的制定。

2013 年天泰 AAP 项目立项上海市软件和集成电路产业发展专项资金，项目已与 2015 年 10 月顺利通过验收。

2013 年天泰被认定为“高新技术企业”，天泰产品在军队、卫生、教育、国土、检察院、政府门户等行业得到广泛应用。

2014 年天泰 WEB 安全监测系统 V1.0 获批创新基金专项资金，获得专项资助；项目已于 2016 年 4 月顺利通过验收。

2015 年起，天泰向云应用服务平台进军，推出云应用相关解决方案，并率先入驻阿里云、华为云、腾讯云，促使天泰的安全产品虚拟化、服务化。

2016 年到 2018 年，天泰分别在政务云、教育云和工业云进行了应用安全服务方案的建设，在浦东政务云、浦东教育云、舟山工业云等取得了明显的成效。

2019 年的混合云安全解决方案通过上海市经信委的验收，标志着天泰公司在混合云安全方面取得了重大突破。

2018 年到 2021 年，天泰在党政机关、公共服务行业、国有企业开展规模化的网络安全检查、网络安全整改和网络安全应急保障服务，相关业务规范化、体系化，成为公司新的增长点。

2020 年到 2021 年，天泰参与了解放军某单位的某型国产化安全产品研发工作，选用了国产化计算平台和开发工具，产品研发取得了成功。

2018 年到 2021 年，天泰受邀参与上海市某主管单位网络安全绩效管理软件

的开发和支持工作，相关软件和平台在全市得到应用，受到主管单位的好评。

2020 年，天泰研究并开发了在线安全检测服务平台，首次将人工智能和机器自动化服务运用到项目中，该平台在金融行业、中小企业得到了应用。

2021 年起，天泰在物联网、大数据、人工智能、移动计算、工控安全、5G 通信等技术方面进行了研究，相关研究成果融入了天泰的 SGFW、vWAF、ESG、FWaaS、tCloud 等安全产品或解决方案。

2022 年起，天泰在数据安全方面与国内专业机构联合开展实践研究，尤其是数据安全管理和技术措施实践方面积累了成功的经验。

2023 年，天泰参与市级数据安全风险评估试点项目，辅助支撑的项目获得市级主管单位评优。

2024 年，天泰成为浦东教育云（传统云和信创云）现场安全保障技术公司，实现为浦东三朵云（政务云、政务云卫生城、教育云）提供现场保障的安全服务目标。

17.3天泰网络产品技术积累情况

天泰网络在网络安全技术和网络安全管理方面持续开展技术研究和产品开发，获得的产品著作权如下表：

表 天泰网络安全产品列表

天泰网络产品列表（著作权）（截止 2026 年 2 月）
天泰 VPN 安全软件 V1.0
天泰 WEB 安全防护软件 V1.0
天泰应用监控管理系统 V1.0
天泰 WEB 安全监测系统 V1.0
分布式网上交易监测软件 V1.0
分布式 WEB 访问日志采集分析软件 V1.0
WEB 应用安全审计软件 V1.0
WEB 应用安全测试软件 V1.0
WEB 服务器防篡改软件 V1.0
天泰 WEB 应用交付软件 V1.0
天泰 WEB 应用审计软件 V1.0
天泰下一代防火墙软件 V1.0
天泰应用安全综合防护平台软件 V1.0
天泰 WEB 应用监测管理软件 V3.0
天泰 WEB 安全监测系统 V3.0
天泰下一代防火墙软件 V3.0
天泰 WEB 应用交付软件 V3.0
天泰 WEB 应用审计软件 V3.0
天泰大数据环境下的云应用安全服务软件 V1.0
天泰 WEB 安全防护软件 V2.0
天泰 WEB 应用交付软件 V4.0
天泰下一代防火墙软件 V4.0
天泰 WEB 应用防火墙软件 V1.0

天泰 WEB 安全监测系统 V4.0
天泰大数据环境下的云应用安全服务软件 V2.0
天泰应用安全综合防护平台软件 V2.0
天泰安全混合云安全可视化软件 V1.0
天泰安全混合云安全控制软件 V1.0
天泰安全混合云安全知识库管理软件 V1.0
天泰安全混合云应用安全网关软件 V1.0
天泰安全混合云安全控制软件 V2.0
天泰泰云安全防护平台软件 V1.0
天泰混合计算环境安全防护平台软件 V1.0
天泰安全混合云应用安全网关软件 V2.0
天泰安全混合云 API 安全网关软件 V1.0
天泰安全混合云应用安全网关软件 V3.0
天泰网络安全工作绩效评估软件 V1.0
天泰网络安全管理绩效软件 V1.0
天泰 IP 阻断网络防火墙软件 V1.0
天泰 WEB 服务器边缘防护软件 V1.0
天泰下一代防火墙软件 V5.0
天泰安全混合云安全知识库管理软件 V2.0
天泰泰云安全防护平台软件 V2.0
天泰边缘安全网关软件 V1.0 天泰 IP 阻断网络防火墙软件 V2.0
天泰 WEB 安全防护软件 V3.0
天泰网络安全工作绩效评估软件 V3.0
天泰项目信息系统管理软件 V1.0
天泰云网边缘安全软件 V1.0

天泰网络从成立之初就在 WEB 应用安全方面开展研究、研发、应用和创新，结合后来研发的泰云安全管理平台，天泰网络在这一领域具有独到技术特色和

大规模应用保障能力。

17.4天泰网络参与的研究性项目

天泰网络参与的上海市、国家部委的相关研究性项目如下表：

天泰网络的网络安全研究项目列表

研发项目名称	情况描述
新一代 WEB 应用安全综合防护平台	2013 年 4 月上海市软件和信息服务业领域产业专项资金项目，项目规模 670 万。
安全混合云解决方案研究与部署项目	2017 年 7 月该项目投资 699 万元，得到了上海市软件和集成电路产业发展专项资金资助。
上海市市直单位 WEB 安全系统	2014 年 7 月全市 16 家市直单位委托开发 WEB 应用防护系统，成为上海本地企业首家网络安全直采的供货单位。
互联网金融信息安全公共服务平台	2015 年 12 月上海市信息安全测评认证中心代表市经信委采购天泰网络研发的互联网金融信息安全公共服务平台。
上海市网络安全信息集中采集系统	2018 年 2 月上海市信息安全测评认证中心代表市网信办采购天泰网络研发的网络安全信息集中采集系统。
上海市工控安全管理系统	2018 年 5 月上海市经信委采购天泰开发的上海市工控安全管理系统。
天泰 SaaSP 安全服务平台	2017 年 11 月浦东新区软件和信息服务业发展专项资金项目天泰 SaaSP 安全服务平台。
上海市网络安全管理绩效考核系统	2019 年 3 月上海市信息安全测评认证中心采购天泰网络研发的上海市网络安全管理绩效考核系统。
工信部信创项目——某应用安全防护系统	2020 年 9 月参与工信部信创项目——某应用安全防护系统的研发，项目通过验收。
解放军某部信创项目——某系统安全防护系统	2021 年 6 月参与解放军某部信创项目——某应用安全防护系统的研发，通过阶段性验收。
浦东社会领域信息化项目——天泰云网边缘安全系统	2023 年天泰云网边缘安全系统在浦东科经委立项，2025 年 8 通过项目验收。

17.5 天泰在云网边缘安全领域的创新能力

近两年来，天泰网络在云网边缘安全服务能力方面进行了架构建设、产品研发和服务流程重构，为远程安全办公和业务安全访问提供高效的解决方案，特别适用于应急场所、分布式办公、异地大量访问等情况下的安全访问和应用安全保障。

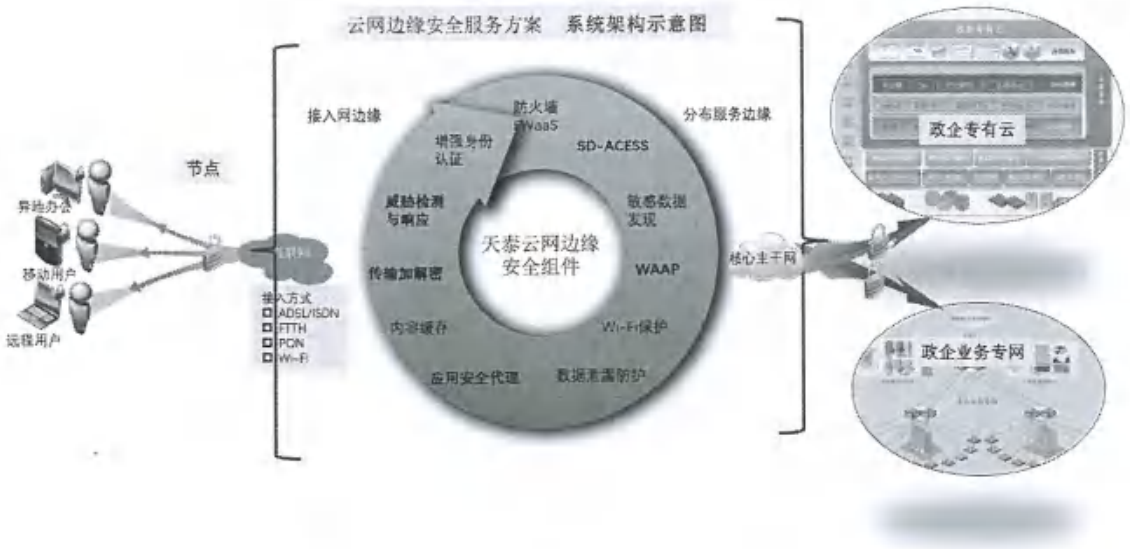
云网边缘安全服务体系采用全新的安全理念，推出的智能安全访问服务，基于云原生部署计算能力、运用软件定义的远程接入能力、分布式边缘安全防护能力，统一解决了远程用户访问应用的安全问题、效率难题，并对用户账号和行为动态授权，实现用户终端、访问身份、广域网络、安全防护集群、检测响应服务等综合安全防护策略，实现客户应用层的安全访问和有效管理。

云网边缘安全服务方案在应用端和用户端之间部署边缘安全云。

分支机构或远程用户通过边缘安全云访问目标云资源或数据中心，边缘安全云赋予用户访问所需的安全能力。在业务流程上，将原来的直接访问变为间接访问，边缘安全云提供与访问用户相匹配的网络接入和安全要素。

云网边缘安全服务方案克服了分散集成和地理位置约束解决方案的成本、复杂性和刚性，可以更好地解决广域网接入、互联网办公、业务异地协同方面的安全性和效率问题。

云网边缘安全服务方案可以支持整个 WAN 访问过程，它使政府和企业的 IT 资源能够以敏捷、安全和经济有效的方式提供业务所需的网络联通和安全功能。



天泰云网边缘安全服务方案架构

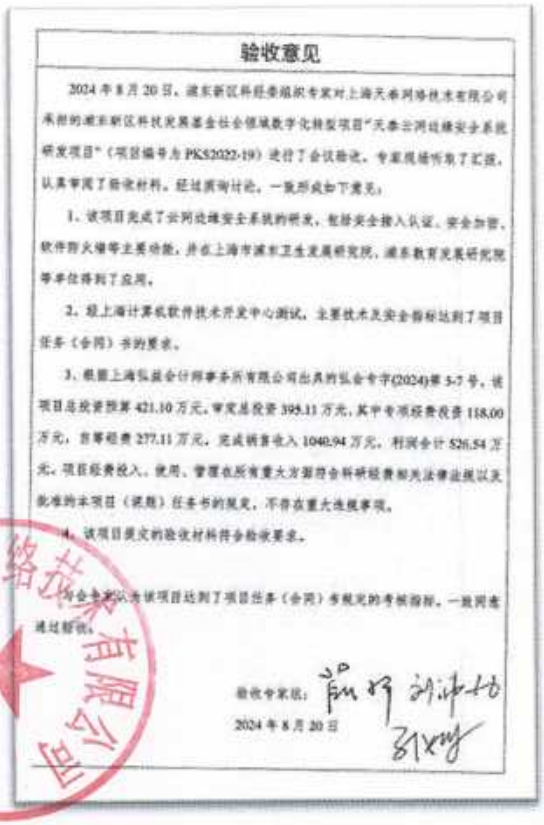
云网边缘安全服务方案提供包括认证、解密、防火墙、URL 过滤、应用防护、反恶意软件和动态威胁管理等服务功能，并且对所有连接的云网边缘都可用。

云网边缘安全服务方案有利于促进新一代云网安全业务的高质量发展，进一步提升新技术新资源的服务广度和深度，促进云网与互联网、广域网的安全融合和数字产业化的发展，是云产品、安全技术、在线风险控制等相关技术的融合式发展和创新突破。

天泰云网边缘安全服务具有以下创新点：

- 在网络和安全能力上进行有机融合和深度融合，对目标服务对象进行评估，有效利用云资源的弹性，规划安全组件的网络接入能力和网络安全能力，进行准确的组合和配置，并引入软件定义安全（SDS）和软件定义性能（SDP）的概念。
- 保护接入端的人员和设备：服务方案将提供在线安全检测组件，对接入设备的主机和软件系统进行安全评估和威胁管理服务，提醒终端用户修补漏洞、升级软件、安装防护产品。
- 管理远程安全接入：服务方案能支持众多使用移动设备的外部员工，将提供统一的远程访问架构和简单的接入配置，方案将提供工具以检验服务方案的接入终端或软件是否能够正常且有效管理。

- 服务方案的合作生态：服务方案的安全组件供应链是否拥有足够强大的合作体系来简化、聚焦网络、安全和管理方面的能力，该能力全面支持安全服务化、定制化和目录化，匹配目标客户的业务规模和业务模式，支持功能定制并提供多租户模式。
- 健壮的商业模式：服务方案服务要有良好的商业模式和生存能力，能够快速灵活地适应产品服务化的市场需求、技术要求、管理要求，坚持专业、灵活、方便、廉价的特点，不断成长壮大。



验收意见

2024 年 8 月 20 日，浦东新区科经委组织专家对上海天泰网络技术有限公司承担的浦东新区科技发展基金社会领域数字化转型项目"天泰云网边缘安全系统研发项目"（项目编号为 PKS2022-19）进行了会议验收。专家现场听取了汇报，认真审阅了验收材料，经过质询讨论，一致形成如下意见：

1、该项目完成了云网边缘安全系统的研发，包括安全接入认证、安全加密、软件防火墙等主要功能，并在上海市浦东卫生发展研究院、浦东教育发展研究院等单位得到了应用。

2、经上海计算机软件技术开发中心测试，主要技术及安全指标达到了项目任务（合同）书的要求。

3、根据上海弘盛会计师事务所有限公司出具的弘会专字(2024)第 5-7 号，该项目总投资预算 421.10 万元，审定总投资 395.11 万元，其中专项经费投资 118.00 万元，自筹经费 277.11 万元，完成销售收入 1040.94 万元，利润合计 526.54 万元。项目经费投入、使用、管理在所有重大方面符合科研经费相关法律法规以及批准的本项目（课题）任务书的规定，不存在重大违规事项。

4、该项目提交的验收材料符合验收要求。

专家组一致认为该项目达到了项目任务（合同）书规定的考核指标，一致同意通过验收。

验收专家组：

2024 年 8 月 20 日

天泰云网边缘安全系统验收意见

正本

2026年度浦东公交网络安全服务项目

项目编号：GQ31011500026031720025 2（标项1）

报

价

文

件

投标人全称：上海天泰网络技术有限公司

地址：上海市浦东新区盛荣路88弄1号楼9层01室

时间：2026年4月10日

目录

一、 投标报价明细表

投标人全称（公章）： 上海天泰网络技术有限公司

招标编号及标项：GQ31011500026031720025 2（标项 1）

2026 年度浦东公交网络安全服务项目包 1

服务期限	其他优惠承诺	最终报价(总价、元)
合同签订生效之日起一年，具体时间以招标人通知为准	无	1,201,800.00 元

授权代表签名： 日期：2026 年 4 月 10 日

二、 投标人针对报价需要说明的其他文件和说明

分项报价明细表

序号	服务项	数量	单价	总价	备注
1	网络安全等保服务	1	450,000.00	450,000.00	2个三级复测，1个二级复测，协助、整改、反馈、复核
2	网络安全加固服务	1	86,200.00	86,200.00	2个防篡改、410个终端防病毒
3	网络安全检测	1	75,200.00	75,200.00	本部6次应用检测，下属单位各1次安全检查
4	网络安全应急保障	1	106,000.00	106,000.00	重保、应急响应
5	网络安全培训	5	6,000.00	30,000.00	每家1次网络安全意识培训
6	网络安全应急演练	1	20,000.00	20,000.00	1次应急演练
7	网络风险技术性探测	1	232,400.00	232,400.00	1次技术性探测，1次渗透测试
8	数据安全风险评估	1	202,000.00	202,000.00	1个系统数据安全风险评估
合计				1,201,800.00	

三、 中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司参加上海浦东新区公共交通有限公司的 2026 年度浦东公交网络安全服务项目采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策 要求的中小企业承接）。相关企业（含联合 体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. 2026 年度浦东公交网络安全服务项目，属于（软件和信息技术服务业）；承建（承接）企业为上海天泰网络技术有限公司（企业名称），从业人员 46 人，营业收入为 3268 万元，资产总额为 3577 万元， 属于小型企业（中型企业、小型企业、微型企业）；

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大 企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）： 上海天泰网络技术有限公司

日期：2026 年 4 月 10 日

注：从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报

各行业划型标准：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

四、 残疾人福利性单位声明函（本单位不适用）

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加____单位的____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　期：