

项目名称：档案信息系统支撑平台
(硬件平台) 维护项目

项目编号：310115000250117163037-15189390

磋商文件

投标单位：上海杉木电子科技有限公司

日期：2025 年 9 月



评分索引表

序号	评审内容	对应章节/页码
1	近三年有效类似项目的承接情况	商务标第 16 章节【65-99】
2	供应商的综合履约能力	商务标第 17 章节【104-125】
3	报价得分	商务标第 2、3 章节【12-14】
4	合理建议	技术标第 7 章节【324-328】
5	服务定位和目标（备品备件更换率等）	技术标第 3、4 章节【158-207】
6	维护方案设计	技术标第 5--9 章节【209-337】
7	重点难点分析和应对措施	技术标第 1.2、1.3 章节【147-149】
8	运维实施安排（日、周、月、年计划）	技术标第 3.2.3/3.3 章节【165-170】
9	运维目标实施方案，原厂服务方案等	技术第 5.1、5.4.1 章节【209-213/233-234】
10	运维机构设置、人员驻场安排情况等	技术标 2.1 章节【151-154】
11	培训方案：（如需）	技术标第 9 章节【333-337】
12	安全文明措施（如果有）	技术标第 2.2. 章节【155-156】
13	应急响应方案（包括详细的应急响应过程，响应方式，响应时间，故障修复时间等）	技术标第 5.4.11、5.4.13 章节【253-254/269-283】
14	针对典型安全事件或风险、重大节假日或任务的应急预案以及应急演练等	技术标第 5.4.10、5.4.14 章节【269-296】
15	技术性能及参数指标与采购需求（原系统）的契合程度	技术标第 3.2.1、5.4.12 章节【158、254-267】
16	符合国家标准及采购需求	技术标第 3.2.1、5.4.12 章节【158、254-267】
17	备品备件的日常管理	技术标第 3.2.1、5.4.12 章节【158、254-267】
18	项目维护机构及其运作方法与流程	技术标第 2、5 章节【151-156、209-306】
19	各项管理制度	商务标第 12、13 章节【35-45】
20	运维手册等资料记录、移交计划等	技术标第 9 章节【333-337】
21	拟投入资源综合评价。（人力、设备等）	商务标第 14-17 章节【46-125】
22	负责人经历、能力、实际参与度等	商务标第 14-17 章节【46-125】

目 录

评分索引表	1
第一部分、商务标	10
1. 磋商书	10
2. 磋商报价表	12
3. 分项报价表	13
3.1. 分项报价	13
3.2. 分项服务内容	13
3.3. 运维设备清单	14
4. 商务技术偏离表	20
5. 法定代表人及授权书	21
5.1. 法定代表人证明	21
5.2. 法定代表授权书	22
6. 政府无违纪声明及证明	23
6.1. 无违纪声明	23
6.2. 无违纪证明	24
6.2.1. 信用中国截图	24
6.2.2. 政采网、央采网截图	25
7. 中小企业声明函	27
8. 营业执照等证明文件	28
8.1. 营业执照	28
8.2. ISO 质量体系认证	29
9. 财务状况及社会保障金情况	30
10. 股东情况及管理人员情况	31
10.1. 股东情况及管理人员查询截图	31
10.2. 主要股东和出资情况	32
11. 响应方机基本情况介绍	33
11.1. 基本情况介绍	33
11.2. 基本经济指标（截止上年度 12 月 31 日止）	33
11.3. 其它情况	34
12. 公司保密制度	35
12.1. 保密目的	35
12.2. 保密范围	35
12.3. 保密职责	35
12.4. 保密内容	35
12.4.1. 商业密码的定义	35
12.4.2. 商业秘密的使用	36
12.4.3. 商业密码的公开	36
12.5. 实施细则	37
12.5.1. 员工管理	37
12.5.2. 收购、并购、合作等	37
12.5.3. 处罚机制	37
12.6. 保密与知识产权承诺书	38
13. 服务质量承诺及保障体系和措施	42

13.1. 服务质量承诺说明	42
13.2. 服务质量体系和措施	43
13.2.1. 服务概述	43
13.2.2. 服务目标	43
13.2.2.1. 提供无忧环境	43
13.2.2.2. 应用开拓和发展	43
13.2.2.3. 技术转移	44
13.2.3. 服务质量原则	44
13.2.3.1. 及时响应和处理原则	44
13.2.3.2. 确保可靠性原则	44
13.2.3.3. 主动性预付原则	44
13.2.3.4. 确保专业性原则	44
13.2.4. 服务质量标准	45
13.2.4.1. 标准化	45
13.2.4.2. 电子化	45
13.2.4.3. 周到化	45
13.2.4.4. 主动化	45
14. 投入本项目主要人员表	46
15. 投入本项目人员情况	47
15.1. 项目负责人情况介绍	47
15.2. 工程师介绍	55
15.2.1. 技术工程师一	55
15.2.2. 技术工程师二	61
16. 近三年完成类似项目情况	65
16.1. 类似项目汇总表	65
16.2. 上海哔哩哔哩客户	66
16.3. 上海电信科技发展	76
16.4. 上海期货信息技术	85
16.5. 北京华通安和科技	99
17. 正在进行项目和用户好评	104
17.1. 用户好评及表彰信	104
17.2. 正在承接项目汇总表	106
17.3. 上海中星城置业	107
17.4. 上海哔哩哔哩科技	117
17.5. 常熟哔哩哔哩科技	125
第二部分、技术标	136
1. 投标公司简介及重难点分析与应对	136
1.1. 投标综合说明	138
1.2. 投标公司相关资质	139
1.3. 投标公司针对本项目优势	147
1.4. 针对本项目重难点分析和应对措施	148
1.4.1. 项目重难点分析	148
1.4.2. 针对性应对方法	149
2. 投标公司服务规范及管理	151

2.1. 公司服务规范	151
2.1.1. 项目人员组织	151
2.1.2. 人员情况表	152
2.1.3. 人员行为规范要求	152
2.1.4. 技术支持规范要求	152
2.1.5. 信息保密要求规范	153
2.1.6. 资料归档要求规范	154
2.2. 公司服务管理	155
2.2.1. 安全文明管理	155
2.2.2. 安全文明规范	155
2.2.3. 安全文明检查	155
2.2.4. 施工安全管理	156
2.2.5. 消防安全管理	156
3. 投标公司针对本项目服务	158
3.1. 服务定位	158
3.2. 服务目标	158
3.2.1. 备品备件服务	158
3.2.2. 硬件包修	159
3.2.3. 驻场服务	159
3.2.4. 系统健康检查	162
3.2.5. 机房工程	162
3.2.6. 信息安全保障	164
3.2.7. 系统分析和优化	165
3.3. 服务进度计划	165
3.3.1. 服务计划	166
3.3.2. 计划管理	166
3.3.3. 时间计划及进度表	167
3.3.3.1. 时间周期	167
3.3.3.2. 时间计划表	167
3.3.4. 实施内容	170
4. 信息系统支持平台【硬件平台】现状分析	171
4.1. 系统现状概述	171
4.2. 机房总平面图及区域划分	173
4.3. 硬件基础平台分析	174
4.3.1. 互联网平台	174
4.3.1.1. 概述	174
4.3.1.2. 设备清单	174
4.3.1.3. 拓扑图	175
4.3.2. 政务网平台	175
4.3.2.1. 概述	175
4.3.2.2. 设备清单	176
4.3.2.3. 拓扑图	177
4.3.3. 局域网平台	177
4.3.3.1. 概述	177



4.3.3.2. 设备清单	178
4.3.3.3. 拓扑图	179
4.4. 系统支撑平台分析	180
4.4.1. 互联网系统	180
4.4.1.1. 服务器系统	180
4.4.1.2. 存储系统	181
4.4.1.3. 备份系统	181
4.4.1.4. 数据库系统	181
4.4.1.5. 设备清单	182
4.4.1.6. 机柜图	182
4.4.1.7. 接口互联表	183
4.4.1.8. 设备使用情况	185
4.4.2. 政务网系统	186
4.4.2.1. 服务器系统	186
4.4.2.2. 存储系统	187
4.4.2.3. 备份系统	188
4.4.2.4. 数据库系统	188
4.4.2.5. 设备清单	189
4.4.2.6. 机柜图	190
4.4.2.7. 接口互联表	190
4.4.2.8. 设备使用情况	191
4.4.3. 局域网系统	192
4.4.3.1. 服务器系统	192
4.4.3.2. 存储系统	194
4.4.3.3. 备份系统	194
4.4.3.4. 数据库系统	194
4.4.3.5. 设备清单	195
4.4.3.6. 机柜图	198
4.4.3.7. 接口互联表	200
4.4.3.8. 设备使用情况	203
4.5. 软件系统平台分析	205
4.5.1. 本地系统软件	205
4.5.2. 云端系统平台	207
5. 运维服务方案介绍	209
5.1. 服务方式	209
5.1.1. 现场技术支持服务	209
5.1.2. 现场硬件支持服务	210
5.1.3. 重保服务	211
5.1.4. 重难点分析服务	211
5.1.5. 咨询服务	212
5.1.6. 软件测试、补丁与升级服务	212
5.1.7. 其它综合服务	213
5.2. 服务范围	214
5.2.1. 网络系统	214



5.2.2. 存储硬件	214
5.2.3. 操作系统	215
5.2.4. 数据库及备份	216
5.2.5. 机房工程	217
5.2.6. 网络安全	218
5.2.7. 信息安全	218
5.2.8. 虚拟化平台	219
5.2.9. 系统支持	220
5.3. 运维服务流程介绍	221
5.3.1. 运维流程概述	221
5.3.2. 服务运维职责	222
5.3.3. 服务保障联系方式	222
5.3.4. 故障处理概述	223
5.3.5. 保修处理概述	225
5.3.6. 升级更新处理概述	226
5.3.7. 正常巡检概述	228
5.3.8. 重大保障概述	230
5.3.9. 服务交接概述	232
5.4. 运维服务工作内容	233
5.4.1. 驻场服务和日常工作	233
5.4.1.1. 数据中心机房工程	233
5.4.1.2. 网络安全系统	233
5.4.1.3. Sun 小型机系统	233
5.4.1.4. PC 服务器系统	233
5.4.1.5. 存储备份系统	234
5.4.1.6. 数据库系统	234
5.4.1.7. 备份系统	234
5.4.2. 硬件保修包换服务	235
5.4.2.1. 工作职责	235
5.4.2.2. 工作要求	235
5.4.3. 系统健康监控服务	236
5.4.3.1. 工作职责	236
5.4.3.2. 工作要求	236
5.4.4. 信息安全保障服务	238
5.4.4.1. 工作职责	238
5.4.4.2. 工作要求	239
5.4.5. 机房工程系统服务	240
5.4.5.1. 工作职责	240
5.4.5.2. 工作要求	242
5.4.6. 机房供电系统服务	243
5.4.6.1. 工作职责	243
5.4.6.2. 工作要求	244
5.4.7. 机房制冷系统服务	245
5.4.7.1. 工作职责	245



5.4.7.2. 工作要求	245
5.4.8. 机房配套系统服务	246
5.4.8.1. 门禁系统	246
5.4.8.2. 监控系统	247
5.4.8.3. 环控系统	248
5.4.9. 系统分析及优化	249
5.4.9.1. 工作职责	249
5.4.9.2. 工作要求	250
5.4.10. 重大事项及节假日保障	251
5.4.10.1. 工作职责	251
5.4.10.2. 工作要求	252
5.4.11. 应急故障演练服务	253
5.4.11.1. 演练前准备阶段	253
5.4.11.2. 演练执行阶段	253
5.4.11.3. 演练后总结与评估阶段	254
5.4.11.4. 常态化提升阶段	254
5.4.12. 现场和后端备品备件服务	254
5.4.12.1. 备品备件服务	254
5.4.12.2. 备品备件计划	255
5.4.12.3. 现场备品备件清单	263
5.4.12.4. 保障级备件库	265
5.4.12.5. 备品备件的配置	267
5.4.13. 应急处置方案	269
5.4.13.1. 应急预案概述	269
5.4.13.2. 应急组织及职责	269
5.4.13.3. 突发事件分类	270
5.4.13.4. 应急级别定义	270
5.4.13.5. 突发事件应急方案	271
5.4.13.6. 应急供货及响应	275
5.4.13.7. 故障等级分类及划分	276
5.4.13.8. 应急处理流程	280
5.4.13.9. 应急排错流程	281
5.4.13.10. 应急日志备份	281
5.4.13.11. 故障处理报告	282
5.4.13.12. 应急事件响应	283
5.4.14. 典型事件应急处理方案	285
5.4.14.1. 应急概述	285
5.4.14.2. 一般事故	285
5.4.14.3. 网络故障	286
5.4.14.4. 人为故障	287
5.4.14.5. 紧急事故【断电】	290
5.4.14.6. 紧急事故【数据库】	292
5.4.14.7. 紧急事故【存储】	295
5.4.14.8. 紧急事故【云平台】	295

5.4.14.9. 信息安全事故	296
5.5. 故障恢复方案	297
5.5.1. 恢复方案概述	297
5.5.2. 目标、任务、计划	299
5.5.2.1. 目标	299
5.5.2.2. 任务	300
5.5.2.3. 计划	300
5.5.3. 虚拟化恢复演练	302
5.5.4. 机房制冷系统恢复演练	302
5.5.5. 数据备份恢复演练	304
5.5.6. 数据备份演练测试	305
5.5.7. 恢复演练总结	306
6. 安全支持系统方案介绍	307
6.1. 物理安全介绍	307
6.1.1. 环境安全	308
6.1.2. 设备安全	308
6.1.3. 媒介安全	308
6.2. 网络安全介绍	310
6.2.1. 物理、虚拟控制	310
6.2.2. 通信链路加密	311
6.2.3. 网络入侵检测	313
6.2.4. 漏扫系统	314
6.2.5. 病毒防护	314
6.3. 系统安全介绍	316
6.3.1. 网络系统安全	316
6.3.2. 操作系统安全【Linux 系统】	316
6.3.3. 操作系统安全【Win 及 UI 界面系统】	317
6.4. 应用级安全介绍	319
6.4.1. 系统安全关键技术措施	319
6.4.2. 安全管理体系构建	320
6.4.3. 构建认证体系	320
6.5. 终端统一安全管理	321
6.5.1. 进程检查	322
6.5.2. 外接设备检查	322
6.5.3. 行为审计	322
6.5.4. 通信网卡检查	322
6.5.5. 外置存储检查	323
6.5.6. 重要信息检查	323
7. 系统优化方案介绍	324
7.1. 网络支持平台优化	324
7.2. 系统支持平台	324
7.2.1. 主机系统	324
7.2.2. 虚拟化系统	325
7.3. 安全系统优化	326

7.3.1. 网络安全	326
7.3.2. 系统安全	327
7.4. 存储系统优化	328
8. 项目风险管控	330
8.1. 风控概述	330
8.2. 管理方法	330
8.3. 预测识别与分析	331
8.4. 风险处置	332
9. 文档和培训服务	333
9.1. 文档规范	333
9.2. 文档模版	333
9.3. 培训目的	335
9.4. 培训对象	335
9.4.1. 现场初级培训	335
9.4.2. 集中进阶培训	336
9.5. 培训方式	336
9.5.1. 集中授课培训	337
9.5.2. 现场操作培训	337
9.6. 培训内容	337
10. 验收及考核标准	339
10.1. 运维质量要求	339
10.2. 考核管理要求	339
10.3. 评分办法	339



第一部分、商务标

1. 磋商书

致：上海同济工程咨询有限公司

根据贵方为 档案信息系统支撑平台（硬件平台）维护 项目的磋商邀请（文件编号）项目编号：310115000250117163037-15189390，签字代表 朱千驰、销售经理（全名、职务）经正式授权并代表供应商 上海杉木电子科技有限公司、徐汇区宜山路 333 号汇鑫国际 1204 室（供应商名称、地址）提交下述文件正本一份和副本二份。

1. 磋商书
2. 磋商报价表
3. 报价明细表
4. 商务、技术要求偏离表
5. 法定代表人授权委托书
6. 保密制度及应急预案
7. 中小企业声明函
8. 提供营业执照（三证合一或五证合一）等证明文件
9. 财务状况及税收、社会保障资金缴纳情况声明函
10. 主要股东或出资人信息
11. 正在进行的和承接的项目情况表
12. 提供参加政府采购活动前 3 年内在经营活动中无重大违法记录的书面声明
13. 近 三 年（从 2022 年 01 月 01 日至投标截止前）未被列入“信用中国”网站（www.creditchina.gov.cn）失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单的证明供应商
14. 拟投入本项目的人员表
15. 质量承诺及保证体系、措施、应急方案（有具体响应时间）
16. 响应方基本情况简介

17. 针对本项目的整体服务方案

18. 拟投入本项目的主要人员情况表(附相关证书复印件并加盖公章)

19. 在“国家企业信用信息公示系统”查询的股东情况及主要管理人员信息的截图(加盖公章)

20. 近三年完成的类似项目情况表(附合同复印件，并加盖公章)

21. 其他资料表(磋商文件未要求， 响应方认为应提供的相关资料)据此函，签字代表宣布同意如下：

(1) 所附分项报价表中规定的应提供和交付的项目内容投标总价为即(文字表述)。

(2) 响应方将按磋商文件的规定履行合同责任和义务。

(3) 响应方已详细审查全部磋商文件， 包括修改文件(如有的话)以及全部参考资料和有关附件。

(4) 我们完全理解并同意放弃对这方面有不明及误解的权利。

(5) 自响应文件递交截止时间有效期为 90 个日历日。

(6) 响应方同意提供按照贵方可能要求的与其投标有关的一切数据或资料，完全理解贵方不一定要接受最低价的投标或收到任何投标。

(7) 与本投标有关的一切正式往来通讯请寄：

公司地址： 徐汇区宜山路 333 号汇鑫国际 1204 室

公司电话： 400-816-0504

纳税人识别号： 91310120703380388R

开户银行： 平安银行上海西南支行

银行账号： 11006523950201

响应方代表姓名、职务(印刷体)： 朱千驰、销售经理

响应方名称(加盖企业公章)： 上海杉木电子科技有限公司

日 期： 2025 年 9 月 8 日

响应方代表签字： 朱千驰



2. 磋商报价表

磋商报价表

响应方名称：上海杉木电子科技有限公司
项目编号：310115000250117163037-15189390

货币单位：人民币元

档案信息系统支撑平台（硬件平台）维护项目

供货期/服务项目负责人	备注	最终报价(总价、元)
2025 年 12 月 12 日至 2026 年 12 月 11 日/徐如远		1355000.00 【壹佰叁拾伍万伍仟圆整】

说明：

- 1、所有价格均系用人民币表示，单位为人民币元，精确到元。
- 2、供应商应按照《招标需求》的要求报价。
- 3、“金额”一栏即按包件填写总报价，且各包件总报价不得超过公布的预算金额！
- 4、编制报价明细表（格式自拟）
- 5、项目服务期限，指计划完成本项目的起始日期区间及全部天数（包括中间成果甲方合理的审核天数）。
- 6、如此表中的内容与响应文件其它部分内容不一致的，以此表内容为准。

响应方代表签字：
(加盖企业公章)
日期：2025-9-8



3. 分项报价表

3.1. 分项报价

序号	系统	描述	数量	单价
1	各系统服务	硬件设备维修、备品备件服务、机房工程、系统分析及优化、重大保障、技术培训、文档及知识维护等	1	825000
2	现场技术支持	1 名项目负责人(兼技术工程师)2 名技术工程师 7×8 小时现场驻点运维（周六周日 1 名），关注系统运行状况，预防及处理故障，以及负责机房环境、卫生、安全及设备状态的巡检。	1	530000
合计	壹佰叁拾伍万伍仟圆整		1	1355000

3.2. 分项服务内容

序号	服务项目	服务内容
1	硬件包修服务	对服务范围内的硬件设备及相关功能部件提供包修服务。
2	备品备件服务	针对硬件设备提供完善合理的备品备件清单和解决方案，对于 24 小时内无法修复的硬件故障，必须提供备机服务（备机用于应急使用）。
3	常驻现场	2 名技术工程师 7×8 小时现场驻点运维（周六周日 1 名），关注系统运行状况，预防及处理故障，以及负责机房环境、卫生、安全及设备状态的巡检。
4	系统健康巡检	软硬件系统的健康状况检查。
5	机房工程	负责机房工程所含 6 个子系统的日常维护和定期健康巡检。
6	信息安全保障	信息安全风险评估，每年提供四次安全报告；安全通告、安全整改、安全加固、安全软件和特征库升级等。
7	系统分析及优化	对系统运行状态、运行效率、故障隐患进行评估和分析，提供决策支持数据和解决、优化建议。每年提交四次报告。根据系统分析及优化报告提供软硬件进行设备扩容、大修整治、优化更新等。
8	重大事项现场保障	重大事项期间，增派熟悉该项目的经验丰富的工程师到现场保障，确保系统和应用正常运行。
9	应急处置预案	形成应急处置预案，并定期检验和随时更新。
10	故障恢复演练	每年两次故障恢复演练。

11	技术咨询和培训	提供有针对性的系统知识相关咨询和培训。
12	文档及知识库维护	负责各种有关运维资料的产生、整理和提交。

3.3. 运维设备清单

序号	系统	描述	品牌	数量	单位
机房工程					
1	配电	机房内 2 套 UPS 输出柜, 每个输出柜 44 个 32A 单 P 输出开关, 1 套动力配电柜主要给空调供电	艾默生	2	套
2	UPS	三台 160KVA, 单机运行, 其中两台给机房供电	艾默生	3	套
3	空调	原有风冷、水冷机组各 2 台, 2021 年 10 月新增恒温恒湿机组一台 (内机 SCC12UP, 外机 P-CS016)	艾默生、山特	4	套
4	门禁	机房共 3 个门禁, 单门磁力锁	海康	3	套
5	安防	原有 3 个监控, 分布于机房进出口, 2021 年新增 12 个监控, 其中球机 9 个 DS-2CD3325, 枪机 3 个 DS-2CD3T26WD	海康威视	1	套
6	机柜	服务器机柜		35	套
7	环境监控	主机房环境监控系统, 包含 2 台 UPS、2 个配电柜、8 个温湿度、3 个门禁和漏水检测	计通	1	套
8	集中监控展示平台	业务监控大屏幕展示系统, 包含 4 台 46 寸显示器、1 台图形拼接器、3 个 DVI 信号分配器	王牌	1	套
网络系统					
1	Catalyst 2950G-48	工作组交换机 (48 口)	CISCO	8	台
2	Catalyst 2950G-24	工作组交换机 (24 口)	CISCO	2	台
3	Catalyst 3750X	政务外网核心交换机	CISCO	2	台
4	Catalyst 3750X	因特网核心交换机	CISCO	1	台
5	ECS3	光电转换器 (多模)	Postel	7	台
6	Huawei S5700-24	电脑教室专用交换机	华为	1	台
7	TPLINK-16	政务外网普通交换机	Tplink	1	台

8	Huawei S5700-48	分布式存储网络交换机	华为	2	台
9	Huawei S5700-48	局域网桌面虚拟化接入交换机	华为	1	台
10	Huawei S5700-48	局域网媒资系统网络接入交换机	华为	1	台
11	Huawei S5700-48	政务外网楼层交换机	华为	1	台
12	SNS2124	政务外网光纤交换机	华为	2	台
13	H3C S5130S	政务外网楼层交换机	华三	2	台
14	Huawei USG5150	政务外网防火墙	华为	1	台
15	NISG 5000-IPS	政务外网入侵防御系统	东软	1	台
16	Logbase H530	政务外网安全审计	思福迪	1	台
17	Logbase HS100	政务外网日志收集器探针	思福迪	1	台
18	Huawei USG6650	因特网防火墙	华为	1	台
19	Huawei NIP2050	因特网智能防护系统	华为	1	台
20	H3C S7506E	局域网核心交换机	华三	2	台
21	H3C S5560X	局域网汇聚交换机	华三	2	台
22	H3C S5130S	局域网楼层交换机	华三	10	台
23	H3C S6520X	局域网安全加固区域接入交换机	华三	2	台
24	H3C F1050	局域网防火墙	华三	2	台
25	天清安全隔离与信息交换系统	局域网与政务外网网闸	启明星辰	1	台
26	NIPS NX-CH3330	局域网入侵防御	绿盟	2	台
27	RSAS NX3-X	局域网漏洞扫描	绿盟	1	台
28	SAS NX3-L1000	局域网日志审计	绿盟	1	台
29	SAS NX3-1000C	局域网网络审计	绿盟	1	台
30	AC1000-D600	政务外网上网行为管理	深信服	1	台
31	S5720S-28P	局域网服务器管理交换机	华为	2	台
32	IPSEC/SSL VPN	政务外网跨馆查询加密机	天融信	1	台
33	OSMS NX3-200C	局域网运维安全网关堡垒机	绿盟	1	台

34	SNS2124	局域网光纤交换机	华为	2	台
35	SNS2124	因特网光纤交换机	华为	2	台
36	S5731-S48T4X	政务外网接入交换机	华为	1	台
37	LAS NX3 HD100	因特网日志审计	绿盟	1	台
38	AC-1000-B1300-KL	因特网上网行为管理	深信服	1	台
局域网平台					
1	SUN F4800	局域网文件系统及备份服务器	SUN	1	套
2	SUN F4800	局域网 Oracle 数据库服务器	SUN	1	套
3	DELL 6650	局域网档案利用服务器	DELL	1	套
4	DELL 6650	局域网介质管理服务器	DELL	1	套
5	SUN 3510	局域网数据备份阵列	SUN	4	套
6	TS-439Pro	局域网数据离线备份 NAS	QNAP	1	套
7	DELL R710	局域网虚拟化资源池	DELL	2	套
8	IBM x3650M3	局域网虚拟化资源池	IBM	1	套
9	DELL R510	局域网虚拟化资源池	DELL	2	套
10	DELL MD1200	局域网全文数据备份阵列	DELL	1	套
11	DELL R420	惠南办公点原馆库系统服务器	DELL	1	套
12	DELL MD3200i	惠南办公点原馆库系统磁盘阵列	DELL	1	套
13	DELL R410	局域网全文数据备用服务器	DELL	1	套
14	华为 S5600T	局域网磁盘阵列	华为	1	套
15	华为 S5600T	局域网磁盘阵列	华为	1	套
16	定制阵列	局域网全文数据备份阵列	定制	1	套
17	定制磁盘阵列（SMARTOR I160）	局域网媒资系统二级存储	德拓	1	套
18	CF60	多媒体教室系统服务器	DELL	1	套
19	Huawei RH2288V3	局域网分布式存储服务器	华为	3	套
20	DELL R730	局域网桌面虚拟化服务器	DELL	2	套
21	Huawei RH2288HV3	局域网分布式存储服务器	华为	1	套
22	DELL R730	统一数据支撑平台节点	DELL	1	套
23	DELL R730	媒资系统服务器	DELL	5	套
24	TS-1231XU-RP	NAS 网络存储器	QNAP	1	套
25	Huawei RH2288HV3	局域网分布式存储服务器	华为	2	套

26	DELL R730	门禁系统服务器	DELL	1	套
27	DELL R730	统一数据支撑平台节点	DELL	1	套
28	DELL R730	统一数据支撑平台节点	DELL	2	套
29	DELL R730XD	档案全文数据备份大容量服务器	DELL	1	套
30	Huawei RH2288H V3	局域网分布式存储节点	华为	1	套
31	DELL R730	虚拟化环境备份服务器	DELL	1	套
政务外网平台					
1	SUN V880	政务外网文件系统及备份服务器	SUN	1	套
2	SUN V880	政务外网 Oracle 数据库服务器	SUN	1	套
3	SUN 3510	政务外网备份阵列	SUN	2	套
4	IBM 4700	政务外网磁盘阵列	IBM	1	套
5	IBM 4000 (Exp810)		IBM	1	套
6	IBM 4000 (Exp810)		IBM	2	套
7	DELL R720	政务外网虚拟化资源池	DELL	1	套
8	DELL MD3600f	政务外网磁盘阵列	DELL	1	套
9	华为 S2600T	政务外网磁盘阵列	华为	1	套
10	DELL R730	政务外网虚拟化资源池	DELL	1	套
11	DELL R730	政务外网桌面虚拟化服务器	DELL	1	套
12	TaiShan 200K 2280K (2*32核)	市局民生档案利用系统（跨馆查询）前置机	华为	1	套
因特网平台					
1	SUN 3510	因特网磁盘阵列	SUN	2	套
2	DELL R910	因特网虚拟化资源池	DELL	1	套
3	DELL R720	因特网虚拟化资源池	DELL	1	套
4	DELL R720	因特网桌面虚拟化服务器	DELL	1	套
5	华为 S2600T	因特网磁盘阵列	华为	1	套
软件产品					
1	数据库	Solaris	Solaris	4	套
2	数据库	Oracle Database 9i	Database	1	套
3	系统软件	Windows Server 2003 标准版	Microsoft	13	套
4	系统软件	Windows Server 2003 企业版	Microsoft	1	套
5	数据库	Veritas (包括 Storage Foundation、Cluster Server、NetBackup、HSM)	Veritas	1	套
6	虚拟软件	VMware vCenter Server V5	VMware	1	套
7	虚拟软件	VMware vSphere V5	VMware	1	套

8	数据库	TRS 全文数据库系统 V6.8	TRS	1	套
9	文件软件	TRS 全文检索网关 V4.5	TRS	1	套
10	系统软件	Windows Server 2008 标准版	Microsoft	2	套
11	系统软件	Windows Server 2008 标准版	Microsoft	17	套
12	数据库	SQL Server 2005 标准版	Microsoft	2	套
13	备份软件	SyncBackpro V6	SyncBackpro	1	套
14	虚拟软件	VMware vCenter Server V5	VMware	1	套
15	虚拟软件	VMware vSphere V5	VMware	2CPU	套
16	存储软件	Huawei FusionStorage V100R003 分布式存储许可	Huawei	96TB	套
17	存储软件	Huawei FusionStorage V100R006 分布式存储许可	Huawei	150TB	套
18	数据库	Oracle Database 12c	Oracle	25 用户	套
19	企业办公软件	帆软 Fine BI 5.0+Report 9.0	Fine		套
20	备份软件	联鼎云备份软件	联鼎件	50TB 许可	套
21	杀毒软件	亚信防病毒软件（DS V20.0）	亚信	1 套	套
22	桌面管理	联软桌面管理软件	联软	150 个许可	套
23	数据库	达梦数据库管理系统 V8.1	达梦	1	套
24	服务器软件	东方通应用服务器软件 V7.0	东方	1	套
25	系统软件	统信 UOS V20 服务器操作系统	统信	1	套
26	管理软件	亚信安全端点安全管理系统 ESM V8.0	亚信	1	套
服务器虚拟平台					
1	虚拟机	文档一体化系统数据库服务器	ZW	1	套
2	虚拟机	文档一体化系统应用服务器	ZW	1	套
3	虚拟机	OA 应用服务器	ZW	1	套
4	虚拟机	OA 数据库服务器	ZW	1	套
5	虚拟机	电子签章应用服务器	ZW	1	套
6	虚拟机	分级管理系统数据库服务器	ZW	1	套
7	虚拟机	分级管理系统数据库服务器	ZW	1	套
8	虚拟机	分级管理系统文件服务器	INT	1	套
9	虚拟机	分级管理系统应用服务器	INT	1	套
10	虚拟机	分级管理系统跨馆查询服务器	INT	1	套
11	虚拟机	民生档案智慧服务平台服务器	INT	1	套
12	虚拟机	教育培训管理系统应用服务器	INT	1	套
13	虚拟机	教育培训管理系统视频服务器	ZW	1	套
14	虚拟机	浦东档案 APP 应用服务器	ZW	1	套
15	虚拟机	浦东档案 APP 互联网接口服务器	INT	1	套
16	虚拟机	浦东档案 APP 数据库服务器	INT	1	套

17	虚拟机	浦东档案 APP 政务网接口服务器	ZW	1	套
18	虚拟机	浦东档案 APP 政务网消息队列服务器	ZW	1	套
19	虚拟机	浦东档案微信公众号应用服务器	ZW	1	套
20	虚拟机	浦东开发开放 30 周年档案史料展	ZW	1	套
21	虚拟机	浦东数字档案馆系统应用服务器（数字档案室系统、电子档案接收利用系统）	INT	1	套
22	虚拟机	浦东数字档案馆系统数据库服务器（政务网数据库服务、FTP 服务）	INT	1	套
23	虚拟机	浦东数字档案馆系统应用服务器（全文检索服务和统一认证服务）	INT	1	套
24	虚拟机	浦东数字档案馆系统数据库服务器（政务网数据库）	INT	1	套
25	虚拟机	浦东数字档案馆系统教育培训与监督指导管理	INT	1	套
26	虚拟机	浦东数字档案馆系统互联网信息采集	INT	1	套
27	虚拟机	浦东数字档案馆系统测试服务器	INT	1	套
28	虚拟机	浦东数字档案馆系统云防护服务器	INT	1	套
29	虚拟机	浦东数字档案馆系统微信服务平台后台管理	INT	1	套

5. 法定代表人及授权书

5.1. 法定代表人证明

致：上海市浦东新区档案局

兹证明苗森（姓名），性别：男

年龄：53 身份证号码：210221197208260893，现任我单位 法人 职务，系本公司法定代表人（负责人）。

响应单位名称：（盖章）

日期：2025 年 9 月 8 日



5.2. 法定代表授权书

致：上海市浦东新区档案局

兹委托朱千驰（姓名）全权代表我公司参与 档案信息系统支持平台（硬件平台）维护项目、项目编号：310115000250117163037-15189390 的磋商活动，受委托人由此所出具并签订的一切有关文件，我公司均予承认。

受委托人姓名：朱千驰 性别：男 年龄：25

工作部门：销售部 职务：销售经理 联系电话：17717594816

身份证号码：445281200003013715。

授权期限：2025 年 9 月 1 日至 2025 年 12 月 31 日

代理人无转委托权。

磋商响应单位：上海杉木电子科技有限公司（盖章）

法定代表人：苗森（签字）（盖章）

被授权人签字：朱千驰

日期：2025 年 9 月 8 日



6. 政府无违纪声明及证明

6.1. 无违纪声明

我单位参加 档案信息系统支持平台（硬件平台）维护项目 招标，郑重声明承诺满足以下条件：

- 一、具有独立承担民事责任的能力；
- 二、具有良好的商业信誉和健全的财务会计制度；
- 三、具有履行合同所必需的设备和专业技术能力；
- 四、具有依法缴纳税收和社会保障资金的良好记录；
- 五、参加政府采购活动前 3 年内在经营活动中没有重大违法记录；
- 六、法律、行政法规规定的其他条件；
- 七、在本项目中提供的资料均真实、合法、有效。

我方声明如违反上述承诺，自愿承担相应的法律后果。

特此声明！

响应方法定名称和地址、邮编：上海杉木电子科技有限公司、上海市徐汇区宜山路 333 弄汇鑫国际 1204 室 200030

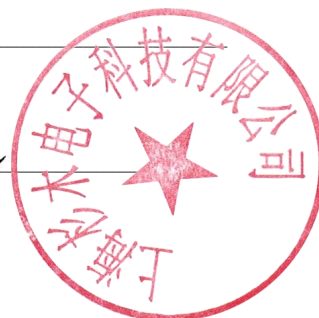
电话：4008160504

传真：_____

响应方法定代表人或授权代表签字或盖章：朱千弛

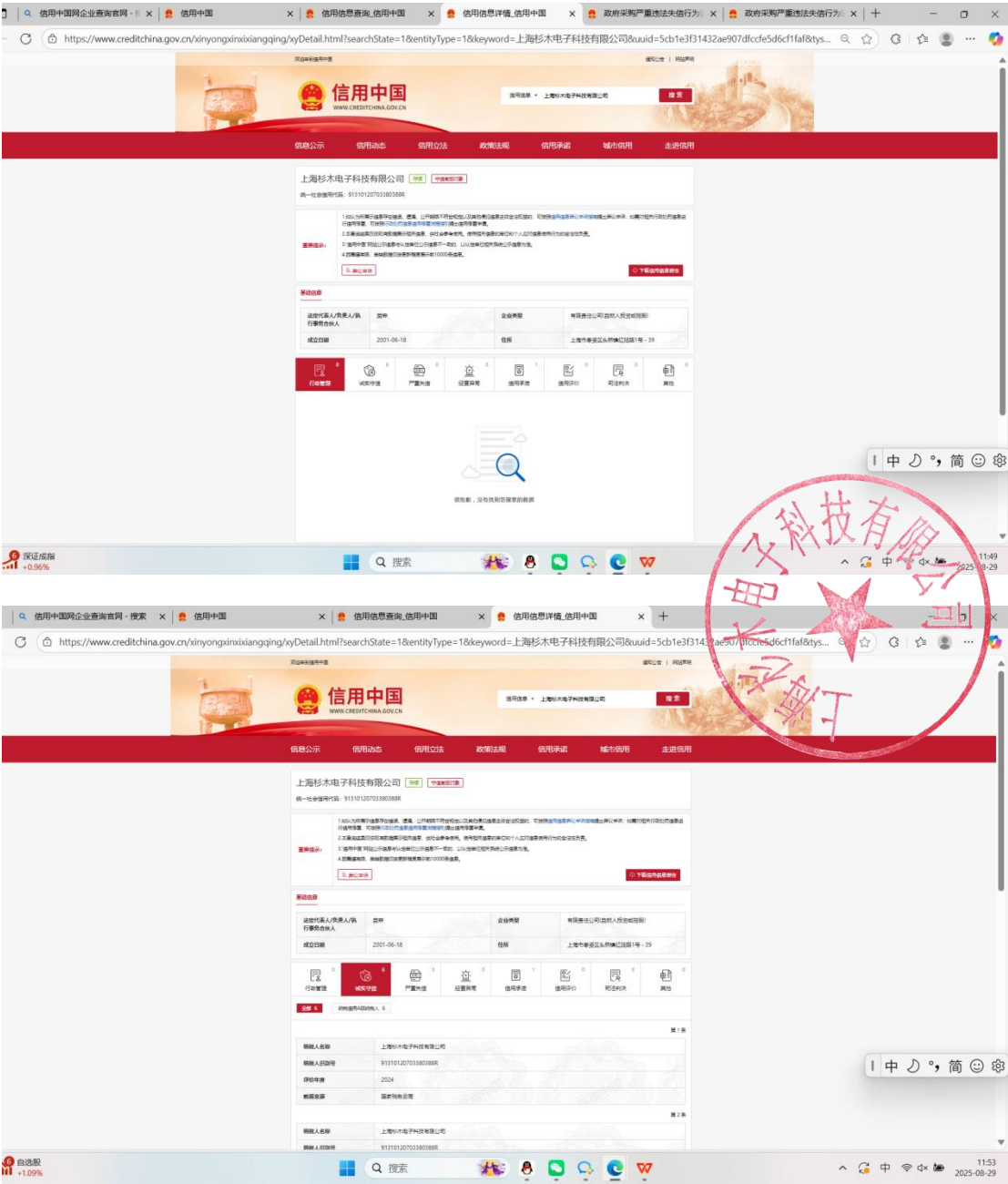
日期：2025 年 9 月 8 日

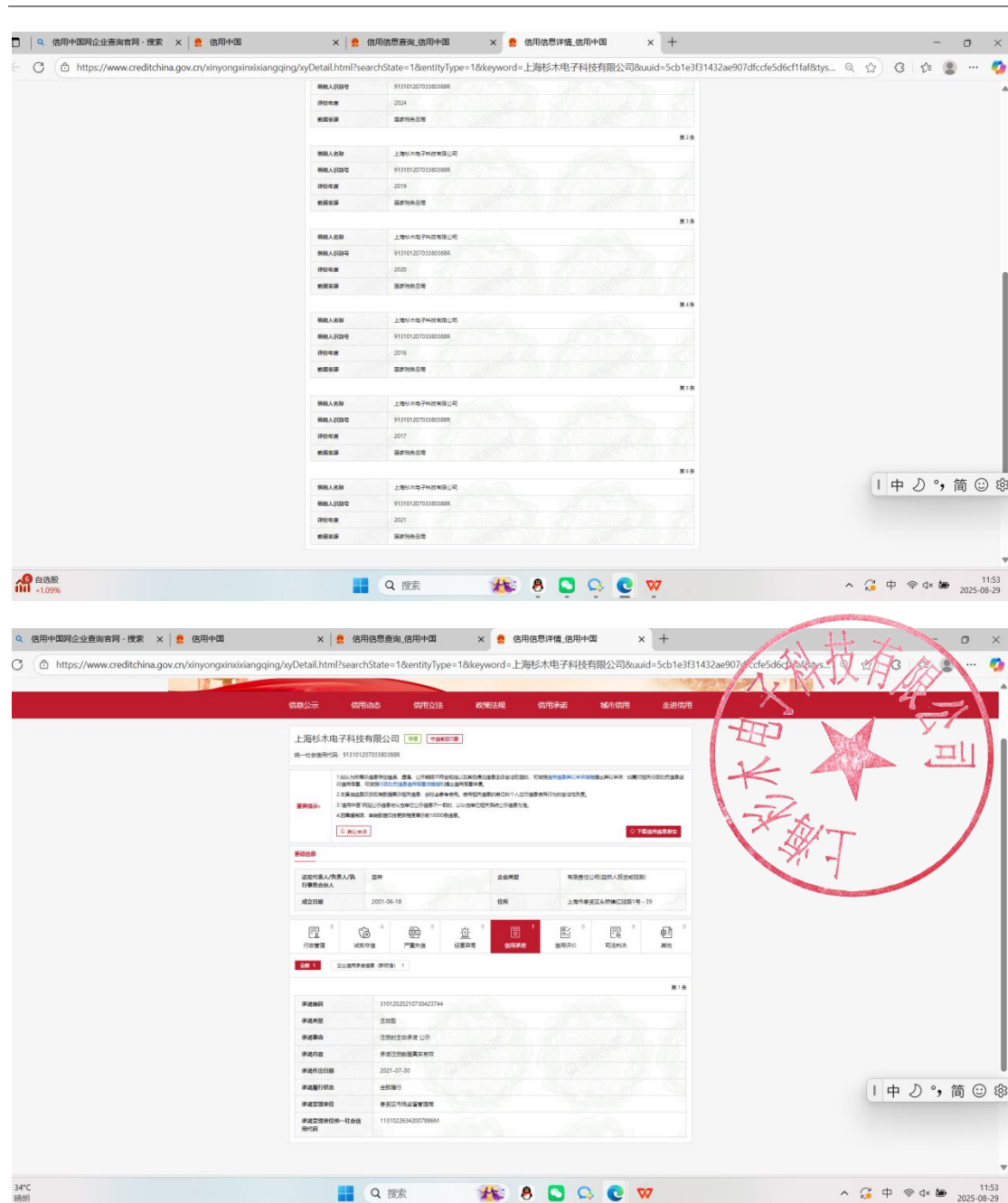
响应方盖章：_____

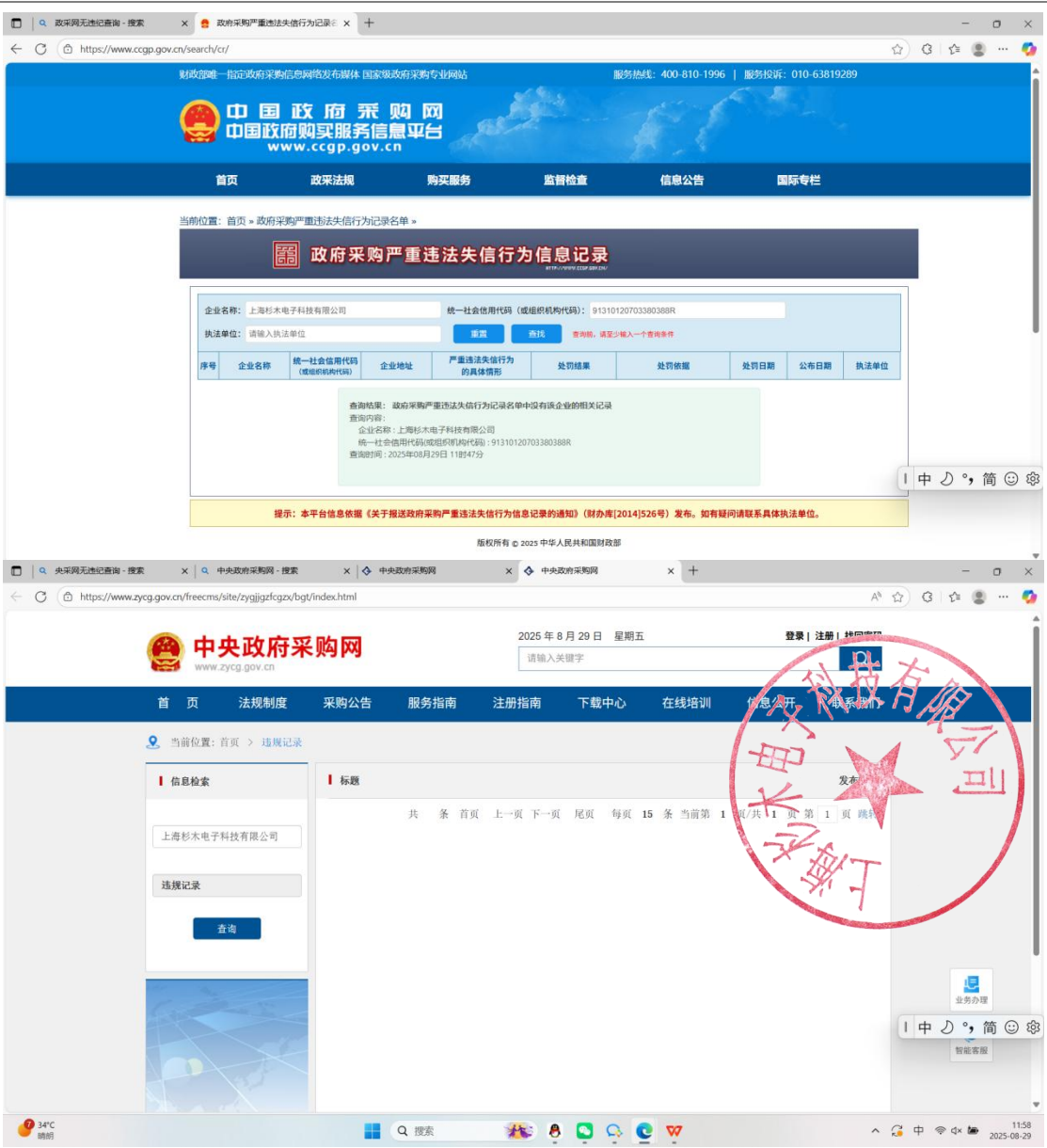


6.2. 无违纪证明

6.2.1. 信用中国截图







7. 中小企业声明函

中小企业声明函(工程、服务)

本公司(联合体)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(联合体)参加(单位名称)的(项目名称)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. 上海杉木电子科技有限公司, 属于 软件和信息技术服务业; 承建(承接)企业为 上海市浦东新区档案局, 从业人员 28 人, 营业收入为 2,944,336.85 万元, 资产总额为 27,585,823.54 万元, 属于(☐ 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:) 上海杉木电子科技有限公司

日期: 2025 年 9 月 8 日

8. 营业执照等证明文件

8.1. 营业执照

统一社会信用代码

91310120703380388R

证照编号:

26000000202009111403

名称

上海杉木电子科技有限公司

类别

有限责任公司(自然人投资或控股)

法定代表人

苗森

经营范围

电子科技领域内的技术开发、技术咨询、技术服务、技术转让，电子设备、仪器仪表、机电设备、通讯设备（除卫星电视广播地面接收设施）、金属材料、机械配件、计算机及配件（除计算机信息系统安全专用产品）、日用百货批发、零售。【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】

注册资本

人民币2000.0000万元整

成立日期

2001年06月18日

营业期限

2001年06月18日至2031年06月17日

住所

上海市奉贤区头桥镇红陆路1号-39

登记机关

奉贤区市场监督管理局

2020年09月11日

扫描二维码登录“国家企业信用信息公示系统”了解更多登记、备案、许可、监管信息。

国家企业信用信息公示系统网址: http://www.gsxt.gov.cn

市场主体应当于每年1月1日至6月30日通过国家企业信用信息公示系统报送公示年度报告。

国家市场监督管理总局监制

营业执照

统一社会信用代码：91310120703380388R

注册号：310120001359160

法定代表人：苗森

登记机关：奉贤区市场监督管理局

成立日期：2001年06月18日

存续（在营、开业、在册）

发送

信息分享

信息打印

基础信息

行政许可信息

行政处罚信息

列入经营异常名录信息

列入严重违法失信名单（黑名单）信息

公告信息

■ 营业执照信息

· 统一社会信用代码：91310120703380388R

· 企业名称：上海杉木电子科技有限公司

· 注册号：310120001359160

· 法定代表人：苗森

· 类型：有限责任公司(自然人投资或控股)

· 成立日期：2001年06月18日

· 核准日期：2020年09月11日

· 注册资本：2000.0000000万人民币

· 登记状态：存续（在营、开业、在册）

· 登记机关：奉贤区市场监督管理局

· 住所：上海市奉贤区头桥镇红陆路1号-39

· 经营范围：电子科技领域内的技术开发、技术咨询、技术服务、技术转让，电子设备、仪器仪表、机电设备、通讯设备（除卫星电视广播地面接收设施）、金属材料、机械配件、计算机及配件（除计算机信息系统安全专用产品）、日用百货批发、零售。【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】

提示：根据《市场主体登记管理条例》及其实施细则，按照《市场监管总局办公厅关于调整营业证照照面事项的通知》要求，国家企业信用信息公示系统将营业证照照面公示内容作相应调整，详见https://www.samr.gov.cn/zw/zfxgk/fdzdgknr/djzcj/art/2023/art_9c67139da37a46fc8955d42d130947b2.html

请登录查看更多信息

8.2. ISO 质量体系认证

管
理
体
系
认
证
证
书

MANAGEMENT SYSTEM CERTIFICATE



质量管理体系认证证书

证书号：30223Q02650R0S

兹证明：

上海杉木电子科技有限公司

统一社会信用代码：91310120703380388R

注册地址：上海市奉贤区头桥镇红陆路1号-39

邮编：201400

办公地址：上海市徐汇区宜山路333号汇鑫国际1204

邮编：200000

经营地址：上海市徐汇区宜山路333号汇鑫国际1204

邮编：200000

质量管理体系符合：

GB/T 19001-2016/ISO9001:2015

证书覆盖业务范围：

网络设备的销售及售后服务



发证日期：2023年06月21日

有效期至：2026年06月20日

本证书在国家规定的行政许可、资质、强制性产品认证有效期内并正常接受年度审核的情况下保持有效。
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。



证书签发人

Certificate issuer

北京中汇恒泰认证有限公司

北京市大兴区天华大街5号院13号楼5层513 总机：010-53606385

第 29 页 共 340 页

9. 财务状况及社会保障金情况

财务状况及税收、社会保障资金

缴纳情况声明函

我方上海杉木电子科技有限公司符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

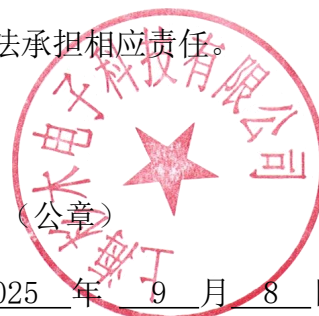
1. 具有健全的财务会计制度；
2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：2025 年 9 月 8 日



10. 股东情况及管理人员情况

10.1. 股东情况及管理人员查询截图

企业详情

天眼查

Q

...

杉木

上海杉木电子科技有限公司

91310120703380388R

发票抬头

评分77

6万+

存续

小微企业

合作风险

司法案件

简介：上海杉木电子科技有限公司，成立于2001年，...更多

法定代表人

苗森

注册资本

2000万人民币

成立日期

2001-06-18

国标行业

工业与专业...

规模

小型

员工

2023年

021-66288311

同电话企业3

邮箱

上海市奉贤区头桥镇红陆路1号 - 39

更多4

股东

2

苗

苗森

受益所有人

持股比例 60%

任职企业 9

张

张彦

受益所有人

持股比例 40%

任职企业 1

高管

2

苗

苗森

执行董事

任职企业 9

张

张彦

监事

任职企业 1

历史股东

查看全部

VIP

买2送1

立即抢购

10.2. 主要股东和出资情况

主要股东或出资人信息

序号	名称 (姓名)	统一社会信用代码 (身份证号)	出资金额 (万元)	占全部股 份比例	备注
1	苗森	210221197208260893	1200	60%	
2	张彦	21022119451128072X	800	40%	

我方承诺，以上信息真实可靠；如填报的股东出资额、出资比例等与实际不符， 视为放弃中标(成交) 资格。

注： 1. 主要股东或出资人为法人的， 填写法人全称及统一社会信用代码(尚未办理三证合一的填写组织机构代码)； 为自然人的，填写自然人姓名和身份证号。

2. 响应方(响应单位)应按照占全部股份比例从大到小依次逐个股东填写， 股东数量多于 10 个的，填写前 10 名，不足 10 个的全部填写。

响应方代表签字：朱千弛

(加盖企业公章)

日期： 2025 年 9 月 8 日

11. 响应方机基本情况介绍

11.1. 基本情况介绍

- 1、单位名称：上海杉木电子科技有限公司
- 2、地址：徐汇区宜山路 333 号汇鑫国际 1204 室
- 3、邮编：200030
- 4、电话/传真：400-816-0504
- 5、成立日期或注册日期： 2001 年 6 月 18 日
- 6、行业类型：电子科技领域内的技术开发、技术咨询、技术服务等

11.2. 基本经济指标（截止上年度12月31日止）

- 1、实收资本： 500 万
- 2、资产总额： 2758 万
- 3、负债总额： 1900 万
- 4、营业收入： 35065 万
- 5、净利润： 294 万
- 6、上交税收： 209 万
- 7、在册人数： 28 人

11.3. 其它情况

- 1、专业人员分类及人数：11 人
- 2、企业资质证书情况：ISO9001
- 3、其他需要说明的情况：公司前身成立于 1993 年。

我方承诺上述情况是真实、准确的， 我方同意根据招标人进一步要求出示有关资料予以证实。

响应方授权代表签字：

朱千弛

响应方(公章)：



日期： 2025 年 9 月 8 日

12. 公司保密制度

12.1. 保密目的

为增加员工的保密意识，保护公司利益和保守商业秘密，特制订以下保密制度。

12.2. 保密范围

本制度适用公司内所有人员，本制度应用于公司各类项目实施及运营、财务管理、行政管理等各类工作。

12.3. 保密职责

- (1) 全体员工根据保密制度，自觉遵守和执行保密协议；
- (2) 各部门领导对本部门员工执行和遵守保密制度负有直接责任，对下属的违反保密制度的行为负全责；
- (3) 公司副总经理、总经理对本公司遵守保密协议和执行保密制度负有直接责任，对下属违反保密制度的行为负全责；
- (4) 总公司副总裁、总裁对恒隆公司遵守保密制度和执行负有间接责任。
- (5) 综合管理部对本公司保密协议遵守和执行负有监督和检查权，并对保密制度的执行和遵守负有连带责任。

12.4. 保密内容

12.4.1. 商业密码的定义

指本公司不为公众所知悉，能为公司带来经济利益、具有实用性并经公司采取保密措施的技术信息、经营信息以及公司根据法律、法规或惯例应当视作商业秘密的其他信息。包括企业在活动中生成、收集、使用的，与现实和未来业务相关的经营信息、财务信息、人力资源信息、客户信息、技术信息、档案信息等。包括但不限于：

- (a) 公司各类会议内容、纪要及管理文件；
- (b) 公司的各种合同书、业务往来文件、业务洽谈情况及投资和业务开

展意向；

(c) 各种合作的计划及材料、业务洽谈备忘录及有关资料；

(d) 各类项目招标(议标)前的各种资料与底价；

(e) 与公司关系密切的合作伙伴和客户的相关资料；

(f) 公司营销策划资料及用户信息；

(g) 驻场人员对用户信息的保密；

(h) 其他属于保密范围内的事项。

(i) 商业秘密的保守：保守秘密是指员工未经授权的情况下，不可以不合理或非法手段获取、透露、使用、允许或协同他人使用商业秘密。

12.4.2. 商业秘密的使用

确需使用商业秘密的，由申请人提出，经部门领导、副总经理、总经理、总裁审批，所有使用商业秘密的由书面批准为依据，否则视为泄密。

12.4.3. 商业密码的公开

商业秘密具有时效性，保密时效过后，由综合管理部根据执行管理层书面签批，方可公布和通报，通报范围为涉及相关工作部门或相应的管理层。未经公开的信息，一律为商业秘密。

12.5. 实施细则

12.5.1. 员工管理

全体员工在签订劳动合同时，签订保密协议，以明确责任和义务。

12.5.2. 收购、并购、合作等

在收购、兼并、合作等过程中，在商谈的前期阶段要求与外部单位签订保密协议，符合上市规则要求，同时保证公司信息不被泄露，保证工作的顺利进行。

12.5.3. 处罚机制

(a) 因过失泄密，视情节分别给予 1000~8000 元的罚款，并予以通报批评，情节严重的解除劳动合同；

(b) 故意泄露机密者，公司将无条件解除劳动合同，并要求其赔偿经济损失，直至追究法律责任；

(c) 触犯国家法律者，移交国家司法部门处理，



12.6. 保密与知识产权承诺书

致：上海市浦东新区档案局：

我方了解国家和上海市浦东新区档案局（以下简称贵司）及其任何关联公司的有关保密和知识产权保护的法律法规和相关制度，知悉应当承担的义务和法律责任。为推进我方与贵司关于的业务合作（以下简称双方业务合作），我方庄重承诺：

一、定义与范围

（一）除了法律规定外，贵司以任何形式（包括但不限于书面、口头、图像、音影、或以样品、范本、计算机程序或其他形式）向我方披露的，所有具有非公知属性的任何信息，均视为保密信息。

1. 前述“保密信息”包括贵司向我方提供的任何技术信息（包括但不限于网络体制、技术标准、技术诀窍、持有技术情况、技术方案、拟申请知识产权的技术成果、未公开的知识产权申请、技术开发方法、技术调研结果、技术数据、技术构想、技术验证过程、技术测试结果等）以及经营信息（包括但不限于业务模式、业务策略、交易手段、定价、原材料价格、劳务报酬、支出费用；财务信息（包括成本、利润和销售）；市场策略；供货商、职员、客户和潜在客户的姓名；与供货商、职员、客户、潜在客户进行的谈判和商业合同；价格组成和内容、提案与合同；内部报告、执行办法等）。

2. 贵司向我方披露的，其从第三方获得并负有保密义务的前述信息亦视为保密信息。贵司与我方相关的合作意向、拟合作事项、合作金额、正在或即将进行的合作商谈内容、已终止合作关系等亦属于保密信息。

3. 前述“保密信息”不包括在披露时或其后已为公众所知晓的信息，但因我方或其雇员过错直接或间接披露的除外。

（二）本承诺书中的知识产权是指技术和知识成果相关的权利或者权益，前述技术果包括但不限于：发明创造、技术方案、技术体制、技术标准、思路、概念、方法、软件（包括代码、程序、文档等）、商业秘密、作品、数据和数据库等。

二、保密信息与知识产权使用

（一）我方承诺仅将保密信息用于双方业务合作，并将促使我方董事、经理、雇员、代理、顾问或其他可能接触上述保密信息的相关人员遵守以下条款：

1. 前述保密信息仅供我方用于双方业务合作，且在任何状况下都不得有损贵司利益。我方承诺不受时间限制地对保密信息执行严格保密（直至相关信息不再属于本承诺书约定的保密信息条件），不得以任何形式（包括任何媒体、宣传渠道等）向任何第三方披露、出售、许可使用等，但我方的雇员和/或顾问为服务双方业务合作而需要了解这些信息的除外；在上述除外情形下我方承诺将告知其雇员和/或顾问保密信息的保密性质，并在他们事先书面承诺接受本承诺书关于不披露义务的约束后方予披露。

2. 我方确有需要，向任何第三方披露保密信息以进行咨询时，应事先向贵司说明情况，并取得贵司的书面同意。

3. 在我方或我方任何雇员和/或顾问被法律强制要求（或类似的法律程序）提供任何保密信息时，我方应当以书面形式于三个工作日（包括第三个工作日）内告知贵司，以便贵司寻求保护令或其他救济或放弃本承诺书保密信息的不披露要求。如未取得保护令或其他救济，或者贵司放弃了保密信息的不披露要求，我方或我方雇员和/或顾问应依法提供要求披露部分的保密信息（客观上我方雇员和/或法律顾问因法律强制程序要求必须立即提供协议保密信息的，不受上述限制，但仍应披露后三个工作日内告知贵司）。

4. 如我方与贵司未达成正式合作，或贵司要求返还保密信息，我方应于15个工作日内（包括第15个工作日），向贵司返还置于我方的所有本承诺书涉及的保密信息，及其复制件、摘要、注解等；我方应销毁并监督我方雇员和/或顾问销毁所有分析文件和他们制备的包含或反映任何保密信息或为之服务的其他文案、计算机文件；不保留任何复制件。销毁行为须以贵司书面方式确认。在遵守前款规定条件下，我方仍须信守保密义务。

（二）对于贵司知识产权，我方已充分知悉以下要求承诺将严格遵守：

1. 如贵司向我方披露的保密信息中包含贵司的知识产权，我方将严格控制该知识产权的知悉范围仅限于为评估双方合作所必要的我方工作人员，且前述人员仅可将该知识产权用于评估双方潜在的合作关系，不得用于反向工

程、内部研发、支撑其他项目等用途。如贵司与我方正式达成合作意向并签署合作协议，我方将严格遵守合作协议中关于保护贵司知识产权的要求。如我方未与贵司正式达成合作意向并签署合作协议，我方承诺不再以任何形式使用该知识产权。

2. 除上述条款外，本承诺书或贵司向我方所披露的保密信息均不构成贵司授予我司任何形式的知识产权转让及许可，亦不构成任何贵司就本承诺书涉及的保密信息向我方提供任何形式的知识产权保证。

三、法律责任

1. 我方承认并同意，本承诺书涉及的保密信息及知识产权是贵司宝贵的专有资产，我方任何违反本承诺书的行为均可能导致贵司不可挽救的损失，且该损失是金钱无法衡量与弥补的。因此，对于我方任何现实的或潜在的违反本承诺书的行为，除金钱补偿之外，贵司还有权寻求临时救济方式，我方将承担贵司因此遭受的全部损失，包括贵司为此支出的包括预期利益、直接损失、诉讼费、合理律师费在内的费用。

2. 我方承诺，若因我方任何现实的或潜在的违反本承诺书的行为导致贵司遭受行政机关、司法机关调查或处罚，我方将尽全力配合贵司澄清事实、消除影响、恢复名誉、赔偿损失，并自觉自愿承担一切相应的法律责任。

三、本承诺书签署、履行、解释和争议解决均适用中华人民共和国法律（不含港澳台地区法律）。凡因执行本承诺书所发生的或与本承诺书有关的一切争议，双方应通过友好协商解决。如果协商不能解决时，任何一方均有权向贵司所在地有管辖权的人民法院提起诉讼。

四、本承诺书条款适用于贵司的任何关联公司所披露的任何符合本承诺书约定的保密信息。“关联公司”是指贵司直接或间接控制的子公司/实体组织、直接或间接控制其的母公司/实体组织、直接或间接被同一母公司/实体组织控制的公司/实体组织。

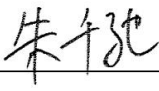
五、我方违反本承诺书约定视为违约，无论赔偿给付与否，贵司均有权不经预告立即解除与我方的合作关系。

六、本承诺书经我方法定代表人或其授权代表签署并加盖公章后生效。本承诺书长期有效，直至该保密信息事实上已合法进入公有领域。

七、无论明示或暗示，本承诺书或向我方所披露的保密信息并不构成双方建立正式合作、签订正式合作协议的承诺。无论双方是否建立正式合作、签订正式合作协议，我方均对保密信息负有保密义务。双方达成正式合作并签署正式合作协议时，本承诺书将作为该合作协议的附件。

（以下无正文）

承诺方（盖章）：上海杉木电子科技有限公司

法定代表人/授权代表（签字）：

承诺日期：2025 年 9 月 8 日

13. 服务质量承诺及保障体系和措施

13.1. 服务质量承诺说明

致：上海市浦东新区档案局：

上海杉木电子本次提供硬件包修服务、备品备件服务、现场服务等。对于 24 小时内无法修复的硬件故障，提供备机服务（备机用于应急使用）。现场服务其中至少安排 1 名项目负责人、2 名技术工程师、若干二线工程师为本项目服务，周一至周五（国定节假日除外）须保证运维现场有 2 名技术工程师（周六周日 1 名技术工程师），负责 7×8 小时现场运维，关注系统运行状况，预防及处理故障，以及负责机房环境、卫生、安全及设备状态的巡检。

针对本项目售后服务响应时间如下表：

地区	响应时间
上海	提供驻场工程师服务，可实时响应 7*8；若有需要，其他工程师可于 4 小时内到达用户现场，提供备品备件；
上海	提供同等规格或同等性能备品备件，保障 24 小时无法修复故障。

公司全称（加盖公章）：上海杉木电子科技有限公司

日期：2025 年 9 月 8 日

13.2. 服务质量体系和措施

13.2.1. 服务概述

为了最大程度的保障浦东新档案局信息系统支持平台维护项目的正常运行，将非计划中断时间降至最低乃至没有，最大限度上保护浦东新区档案局的利益不受损失。杉木电子公司通过诚信、高效、灵活、快捷的综合服务提供商进行现场专业化、技术支持，明确各系统稳定安全可靠的运行、达到最高满意度为最终目的。

13.2.2. 服务目标

我司 IT 服务的基本目标是用户满意，我司向用户承诺提供高效、便捷、专业、个性化的服务，随时听取客户的意见。我司一直以来把用户的利益放在最高标准上，深信用户利益的保障也就是公司无形资产的增长，而用户利益的保障很大程度上取决于服务的支持。为此，我司制定了实施及服务方式，具体即，从项目开始设计、实施、交付运行整个过程中，与用户反复探讨，深入了解要求，尽最大可能在项目完成的同时，为用户在技术上培养起一支过硬队伍，可以由用户自身现场解决实际问题，达到科技的普及化，以适应市场的迅速变化。我司技术支持与服务目标是：

13.2.2.1. 提供无忧环境

我司将集中公司的技术资源，全力解决用户遇到的技术问题和故障。同时以预防为主，负责制定相应的预防保养计划和措施，积极协助用户解决信息系统运行中的隐患，提升系统性能，减少系统停机时间，保障系统正常运行，提高投资回报率。

13.2.2.2. 应用开拓和发展

我司负责向用户传递相关领域的计算机发展方向和产品信息，同时提供系统设计、安装、使用、维护、技术咨询服务等，确保系统处于同行业领先地位。

13.2.2.3. 技术转移

通过对用户系统管理人员和操作人员多层次、多方位的技术培训/咨询和日常操作指导，提高该部分人员的技术水平及工作效率，帮助用户建立一支专业技术队伍。

13.2.3. 服务质量原则

由于本项目对安全性和高效性有较高的要求，为了更好的向用户方提供完善的技术支持和服务，我们的技术支持和服务工作将围绕以上两个要求展开工作并制定了以下原则：

13.2.3.1. 及时响应和处理原则

我司为本项目提供技术支持热线、技术支持网站、现场支持等手段，向用户方提供及时的保修维护服务，对出现故障的设备迅速给予故障排除或更换。在发生故障时，无论出现故障的设备是否属于本工程范围，责任是否在我方，我们都将第一时间响应，以保障用户方系统的安全健壮为第一要务。

13.2.3.2. 确保可靠性原则

我司一支经验丰富、技术过硬的技术服务队伍，并建立了完整的服务体系。本项目中我们将调配优秀并且稳定的技术团队为用户方提供各类技术支持和服务，确保技术支持和服务的质量。

13.2.3.3. 主动性预付原则

在技术支持和服务工作中，我司一贯采取主动原则。通过主动与用户方联系，及时了解本项目系统的运行状况；定期对系统进行例行检查，将隐患消灭在萌芽状态；对发现的问题及时处理，并在检查完成后提供系统检测报告及详尽的分析报告。

13.2.3.4. 确保专业性原则

我司以国际标准为核心理论指导、以人员、流程、工具为主线、以 ISO9001 质量体系为服务标准和保障，建立了以客户为中心的服务交付体系，确保向用户方提供的服务具有安全且专业的水准。

13.2.4. 服务质量标准

13.2.4.1. 标准化

基于符合国际标准的质量控制体系，形成标准化的作业流程，标准化的文档、标准化的服务用语等。

13.2.4.2. 电子化

针对具备上网条件的用户，提供远程登录、WEB 互动、在线支持等电子化服务内容，逐步建立完善的电子化服务渠道。

13.2.4.3. 周到化

倡导基于用户满意度为 100%的个性化关怀；满足用户标准化服务以外的特殊使用需要。

13.2.4.4. 主动化

定期回访制度，针对客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。



14. 投入本项目主要人员表

序号	姓 名	职务	职称及资格证书	主要资历、经验及承担过的项目
1	徐如远	项目负责人	H3CTE、H3CSE-Security、Linuxplus等	上海世博会、公安感知网、庆阳智算、点军人工智能等
2	俞聂敏	服务工程师	H3CIE、H3CSE-Security、麒麟系统工程师等	进口博览会、上海智算、上海期货信息、中芯国际等
3	马运章	服务工程师	H3CIE、麒麟系统工程师等	海关电子口岸、国药集团等

注： 响应方应将表列人员的资历情况填写并附相关资质 证书及证明复印件并加盖公章。

响应方授权代表签字：朱千弛

(加盖企业公章)

日 期：2025 年 9 月 8 日

15. 投入本项目人员情况

15.1. 项目负责人情况介绍

1. 一般情况					
姓 名	徐如远	年 龄	42	技术职务	工程师
职 务	工程师	本合同中拟任职务	项目负责人	为申请人服务时间	17
学 历	本科				
相关职业资格		H3CTE/Linuxplus	取得职业资格时间		2014
2. 经 历					
年 份	负责过的主要项目 (类型、金额)		该项目中任职		备 注
2024年	庆阳智算中心、1.2亿		技术负责人		
2023年	点军人工智能、2950万		服务工程师		
2023年	上海市域铁路城轨云、1900万		服务工程师		

备注： 以上信息均是真实有效的。

响应方授权代表签字：朱千弛

(加盖企业公章)

日 期： 2025 年 9 月 8 日

参保人员城镇职工基本养老保险缴费情况

姓名	徐如远		社会保障号码		342127198312058511		证件号码		342127198312058511		
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	202009	已缴费		21	202205	已缴费		41	202401	已缴费	
2	202010	已缴费		22	202206	已缴费		42	202402	已缴费	
3	202011	已缴费		23	202207	已缴费		43	202403	已缴费	
4	202012	已缴费		24	202208	已缴费		44	202404	已缴费	
5	202101	已缴费		25	202209	已缴费		45	202405	已缴费	
6	202102	已缴费		26	202210	已缴费		46	202406	已缴费	
7	202103	已缴费		27	202211	已缴费		47	202407	已缴费	
8	202104	已缴费		28	202212	已缴费		48	202408	已缴费	
9	202105	已缴费		29	202301	已缴费		49	202409	已缴费	
10	202106	已缴费		30	202302	已缴费		50	202410	已缴费	
11	202107	已缴费		31	202303	已缴费		51	202411	已缴费	
12	202108	已缴费		32	202304	已缴费		52	202412	已缴费	
13	202109	已缴费		33	202305	已缴费		53	202501	已缴费	
14	202110	已缴费		34	202306	已缴费		54	202502	已缴费	
15	202111	已缴费		35	202307	已缴费		55	202503	已缴费	
16	202112	已缴费		36	202308	已缴费		56	202504	已缴费	
17	202201	已缴费		37	202309	已缴费		57	202505	已缴费	
18	202202	已缴费		38	202310	已缴费		58	202506	已缴费	
19	202203	已缴费		39	202311	已缴费		59	202507	已缴费	
20	202204	已缴费		40	202312	已缴费		60	202508	已登记	
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		
上海杉木电子科技有限公司			2020年09月-2021年10月			上海好概信息咨询服务中心			2021年11月-2021年11月		
上海杉木电子科技有限公司			2021年12月-2022年02月			上海网辉电子科技有限公司			2022年03月-2023年01月		
上海杉木电子科技有限公司			2023年02月-2025年07月								
截至2025年08月，累计缴费月数						147					

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。

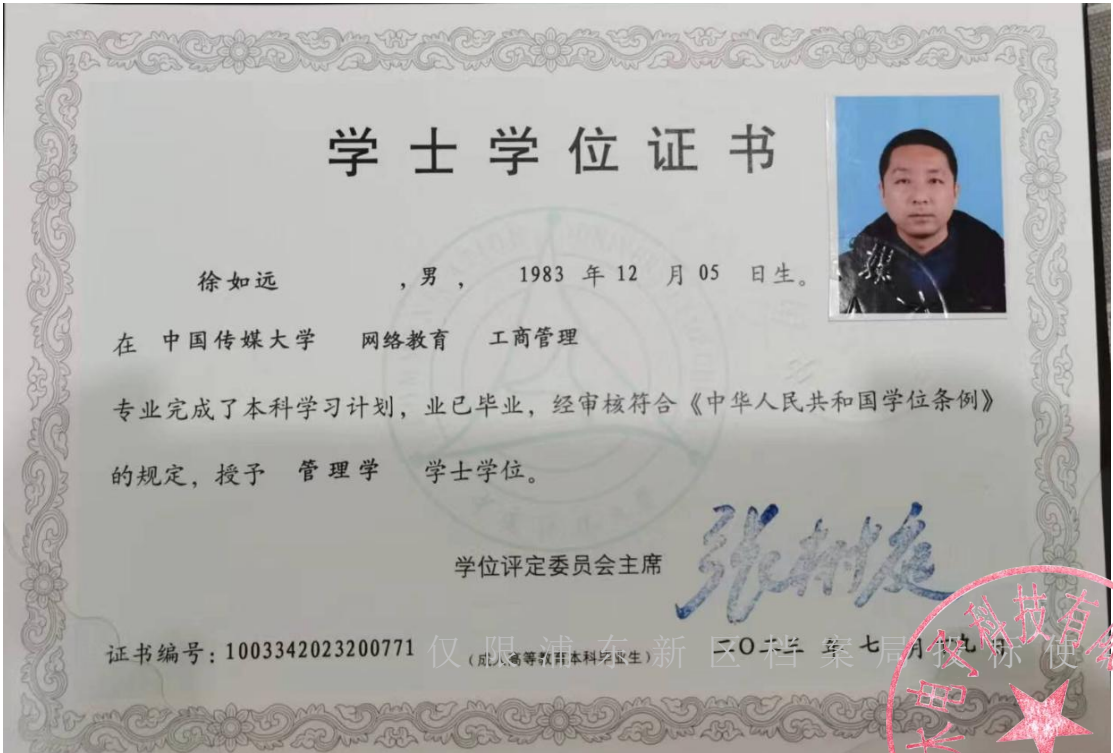
仅限浦东新区档案局投标使用

◆ 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



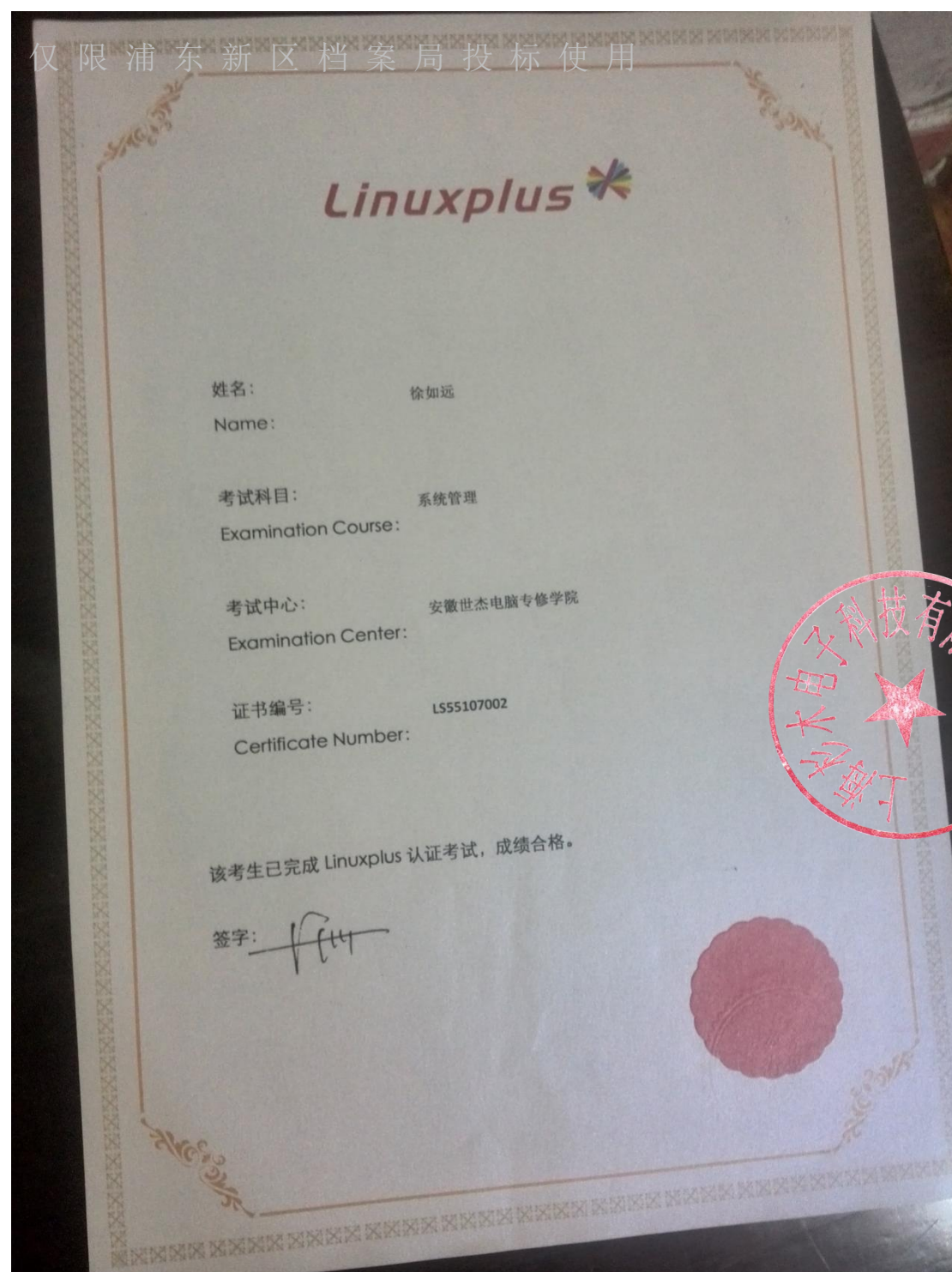
电子印章
验证码：MEQC1F0rbX1H6jJXL27FJwQhp98agbXEa9F65mj0PGz8r041AiBGsHK0vY0SGsLwY7yYjk1u5pUn1PduXrVLihjY1X0AYw==











仅限浦东新区档案局投标使用



15.2. 工程师介绍

15.2.1. 技术工程师一

1. 一般情况					
姓 名	俞聂敏	年 龄	40	技术职务	工程师
职 务	工程师	本合同中拟任职务	服务工程师	为申请人服务时间	16
学 历	大专				
相关职业资格		H3CIE/麒麟系统	取得职业资格时间		2022
2. 经 历					
年 份	负责过的主要项目 (类型、金额)		该项目中任职		备 注
2024年	上海智算中心、7000万		服务工程师		
2023年	上海智算中心、1.3亿		服务工程师		
2022年	哔哩哔哩、4500万		服务工程师		

备注： 以上信息均是真实有效的。

响应方授权代表签字：  朱千弛

(加盖企业公章)

日 期： 2025 年 9 月 8 日

参保人员城镇职工基本养老保险缴费情况

姓名 俞晔敏			社会保障号码				342623198512287716				证件号码		342623198512287716		
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	序号	年 月	缴费情况	补缴退账年月
1	202009	已缴费		21	202205	已缴费		41	202401	已缴费					
2	202010	已缴费		22	202206	已缴费		42	202402	已缴费					
3	202011	已缴费		23	202207	已缴费		43	202403	已缴费					
4	202012	已缴费		24	202208	已缴费		44	202404	已缴费					
5	202101	已缴费		25	202209	已缴费		45	202405	已缴费					
6	202102	已缴费		26	202210	已缴费		46	202406	已缴费					
7	202103	已缴费		27	202211	已缴费		47	202407	已缴费					
8	202104	已缴费		28	202212	已缴费		48	202408	已缴费					
9	202105	已缴费		29	202301	已缴费		49	202409	已缴费					
10	202106	已缴费		30	202302	已缴费		50	202410	已缴费					
11	202107	已缴费		31	202303	已缴费		51	202411	已缴费					
12	202108	已缴费		32	202304	已缴费		52	202412	已缴费					
13	202109	已缴费		33	202305	已缴费		53	202501	已缴费					
14	202110	已缴费		34	202306	已缴费		54	202502	已缴费					
15	202111	已缴费		35	202307	已缴费		55	202503	已缴费					
16	202112	已缴费		36	202308	已缴费		56	202504	已缴费					
17	202201	已缴费		37	202309	已缴费		57	202505	已缴费					
18	202202	已缴费		38	202310	已缴费		58	202506	已缴费					
19	202203	已缴费		39	202311	已缴费		59	202507	已缴费					
20	202204	已缴费		40	202312	已缴费		60	202508	已登记					
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			
上海杉木电子科技有限公司				2020年09月-2025年07月											
截至2025年08月，累计缴费月数												129			

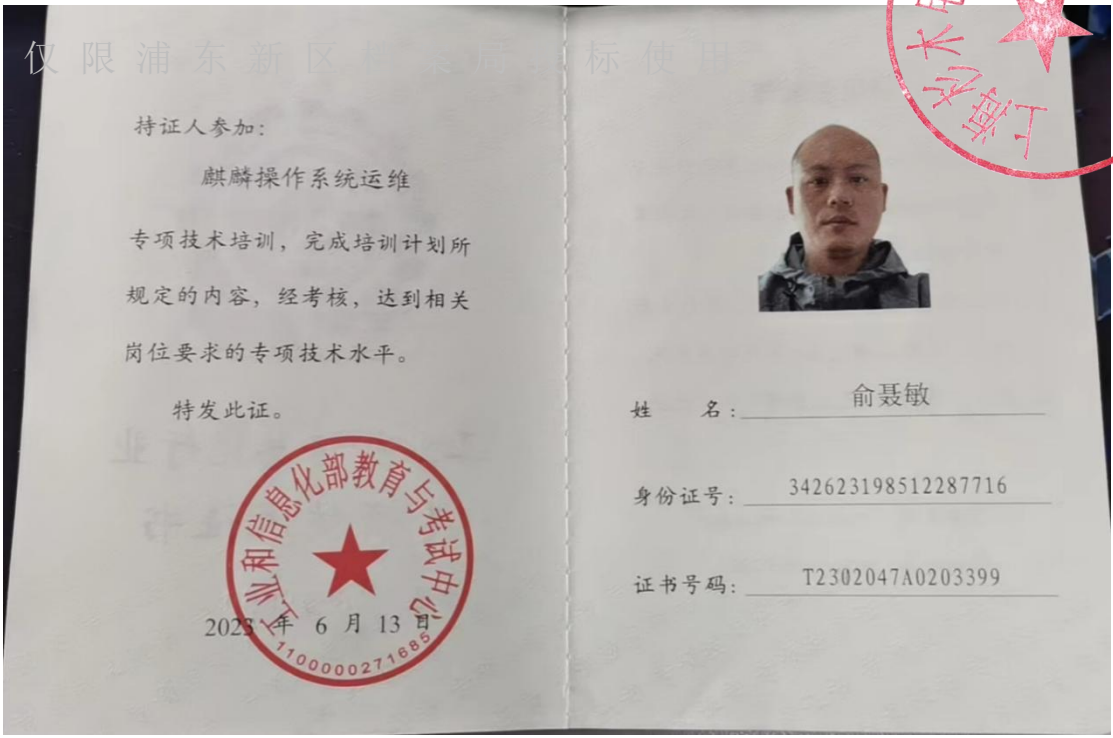
备注：1、本缴费情况的信息以申请打印时点的参保缴费情况为依据，供参考；亦可通过“一网通办”平台、“随申办”APP或线下自助服务终端查询获取。
2、“已登记”表示参保人员属于社会保险参保登记状态；“累计缴费月数”显示的月数为实际记账月数。

◆ 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



电子印章 MEUCIBnb0PxZgVXjQt39ZDCb0k746cwjIzE+y36sXBCFI0DgAiEA25LnymxP/xXzJY21HgCEzwzy49JaYcZ+nrKbuji
验证码：0cjc=



仅限浦东新区档案局投标使用



NSFOCUS Certification

俞聂敏

has successfully completed the NSFOCUS certification requirements and is recognized as a



Certificate No. NSF-SAB101202226416
Valid Through 2024.11.11


NSFOCUS INFORMATION TECHNOLOGY CO.,LTD

仅限浦东新区档案局投标使用



深信服安全资深工程师

俞聂敏

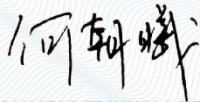
HAS SUCCESSFULLY COMPLETED
THE SANGFOR TECHNOLOGY CERTIFICATION REQUIREMENTS AND IS AUTHORISED AS A

Sangfor Security Technology Professionals

有效日期: Jun.2024
Valid Through

证书编码: SSTP202206302513
Certificate ID




CEO

SANGFOR TECHNOLOGIES INC







15.2.2. 技术工程师二

1. 一般情况					
姓 名	马运章	年 龄	25	技术职务	工程师
职 务	工程师	本合同中拟任职务	服务工程师	为申请人服务时间	4
学 历	本科				
相关职业资格		H3CIE/麒麟系统	取得职业资格时间		2022
2. 经 历					
年 份	负责过的主要项目 (类型、金额)		该项目中任职		备 注
2024年	上海智算中心、7000万		服务工程师		
2023年	上海智算中心、1.3亿		服务工程师		
2022年	哔哩哔哩、4500万		服务工程师		

备注： 以上信息均是真实有效的。

响应方授权代表签字

(加盖企业公章)

朱千弛

日 期： 2025 年 9 月 8 日

参保人员城镇职工基本养老保险缴费情况

姓名			马运章		社会保障号码			340322200010157810		证件号码		340322200010157810	
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	序号	年 月
1	202009	未缴费		21	202205	未缴费		41	202401	已缴费			
2	202010	未缴费		22	202206	未缴费		42	202402	已缴费			
3	202011	未缴费		23	202207	未缴费		43	202403	已缴费			
4	202012	未缴费		24	202208	已缴费		44	202404	已缴费			
5	202101	未缴费		25	202209	已缴费		45	202405	已缴费			
6	202102	未缴费		26	202210	已缴费		46	202406	已缴费			
7	202103	未缴费		27	202211	已缴费		47	202407	已缴费			
8	202104	未缴费		28	202212	已缴费		48	202408	已缴费			
9	202105	未缴费		29	202301	已缴费		49	202409	已缴费			
10	202106	未缴费		30	202302	已缴费		50	202410	已缴费			
11	202107	未缴费		31	202303	已缴费		51	202411	已缴费			
12	202108	未缴费		32	202304	已缴费		52	202412	已缴费			
13	202109	未缴费		33	202305	已缴费		53	202501	已缴费			
14	202110	未缴费		34	202306	已缴费		54	202502	已缴费			
15	202111	未缴费		35	202307	已缴费		55	202503	已缴费			
16	202112	未缴费		36	202308	已缴费		56	202504	已缴费			
17	202201	未缴费		37	202309	已缴费		57	202505	已缴费			
18	202202	未缴费		38	202310	已缴费		58	202506	已缴费			
19	202203	未缴费		39	202311	已缴费		59	202507	已缴费			
20	202204	未缴费		40	202312	已缴费		60	202508	已登记			
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	
上海杉木电子科技有限公司				2022年08月-2025年07月									
截至2025年08月，累计缴费月数												36	

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。

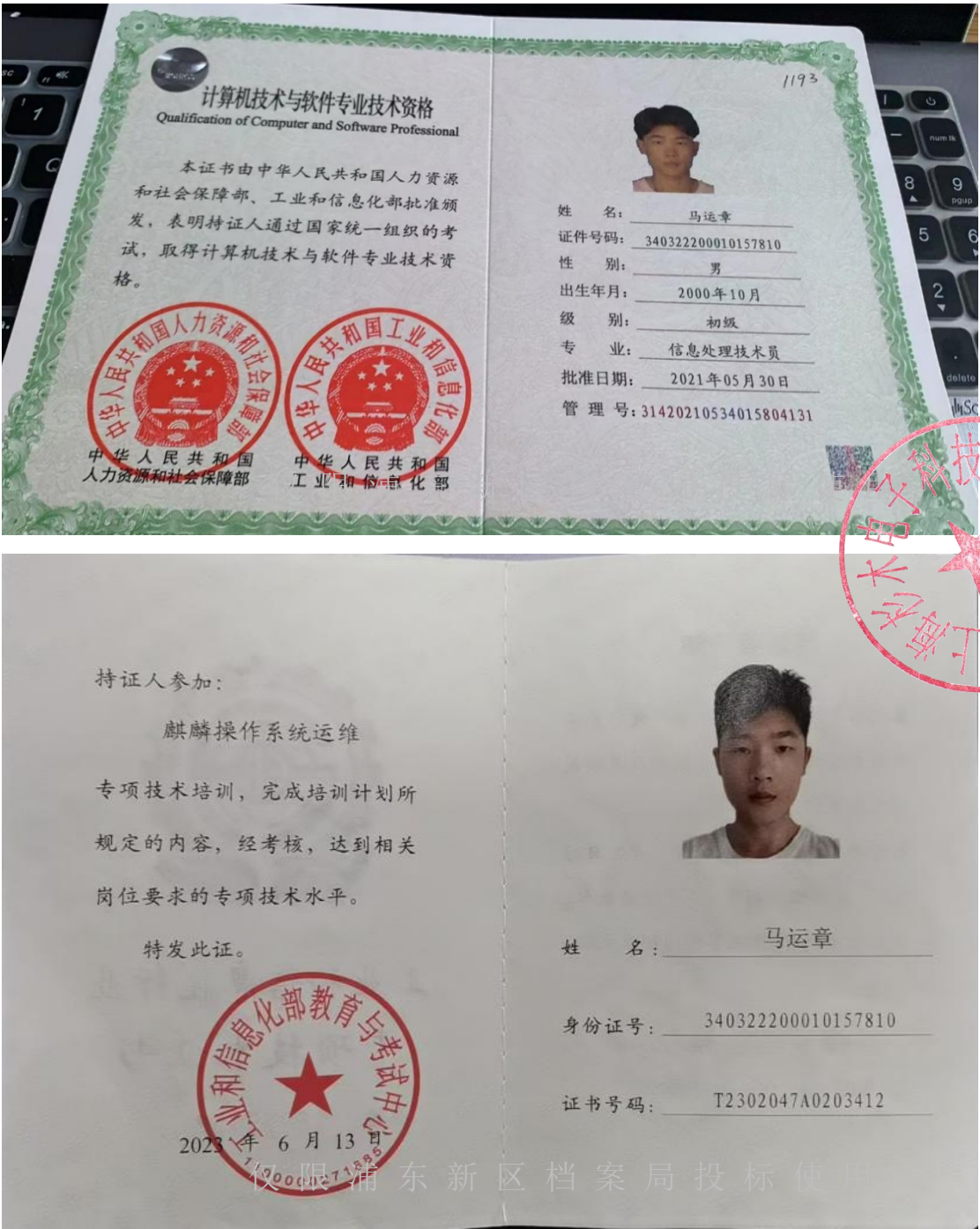
◆ 上海市社会保险事业管理中心业务专用章
已经上海市数字证书认证中心认证，是对外
经办业务指定电子印章，与社保经办机构印
章具有同等效力，不再另行盖章。

经办机构：上海市社会保险事业管理中心
打印日期：2025-9-11
业务专用章

电子印章 MEUCIQD/BLNrPoAF6ftAm8kUrJgEg1nwBqtRJTV2shkLaHE/MQIgJ+I6TtYq2f/5Yga0JMaWY3.j+BGv779LJBVP+at
验证码： fnfY=

仅供上海市档案局投标使用





16. 近三年完成类似项目情况

16.1. 类似项目汇总表

（附合同复印件，并加盖公章）

项目序号	1	2	3	4
项目名称	BILIBILI 网络设备续保	2022年上海电信战略大客户部现场办公业务体验及技术支持服务	2024年度云计算基础实施续保采购项目	新华三产品调试服务项目
项目所在地	常熟	上海	上海	北京
项目采购人名称	上海哔哩哔哩客户有限公司	上海电信科技发展有限公司	上海期货信息技术有限公司	北京华通安和科技有限公司
项目采购人地址	上海	上海	上海	北京
项目采购人电话	15821232173	13761731546	13916845537	010-62603865
合同价格	1747037.00	268550.00	228500.00	3657000.00
开始日期	2021-12-2	2023-1-1	2024-7-15	2023-6-30
完成日期	2023-12-2	2023-12-31	2025-7-14	2023-12-1
项目负责人	刘小芳	宗绪鹏	张仁宝	张仁宝
技术负责人	徐如远	劳开钦	伍明凯	陶勇
项目描述	现场维修支持服务7*24*4	7*24*4技术支持服务	7*24全天候服务	现场维护及调试
备注(用户反映)				

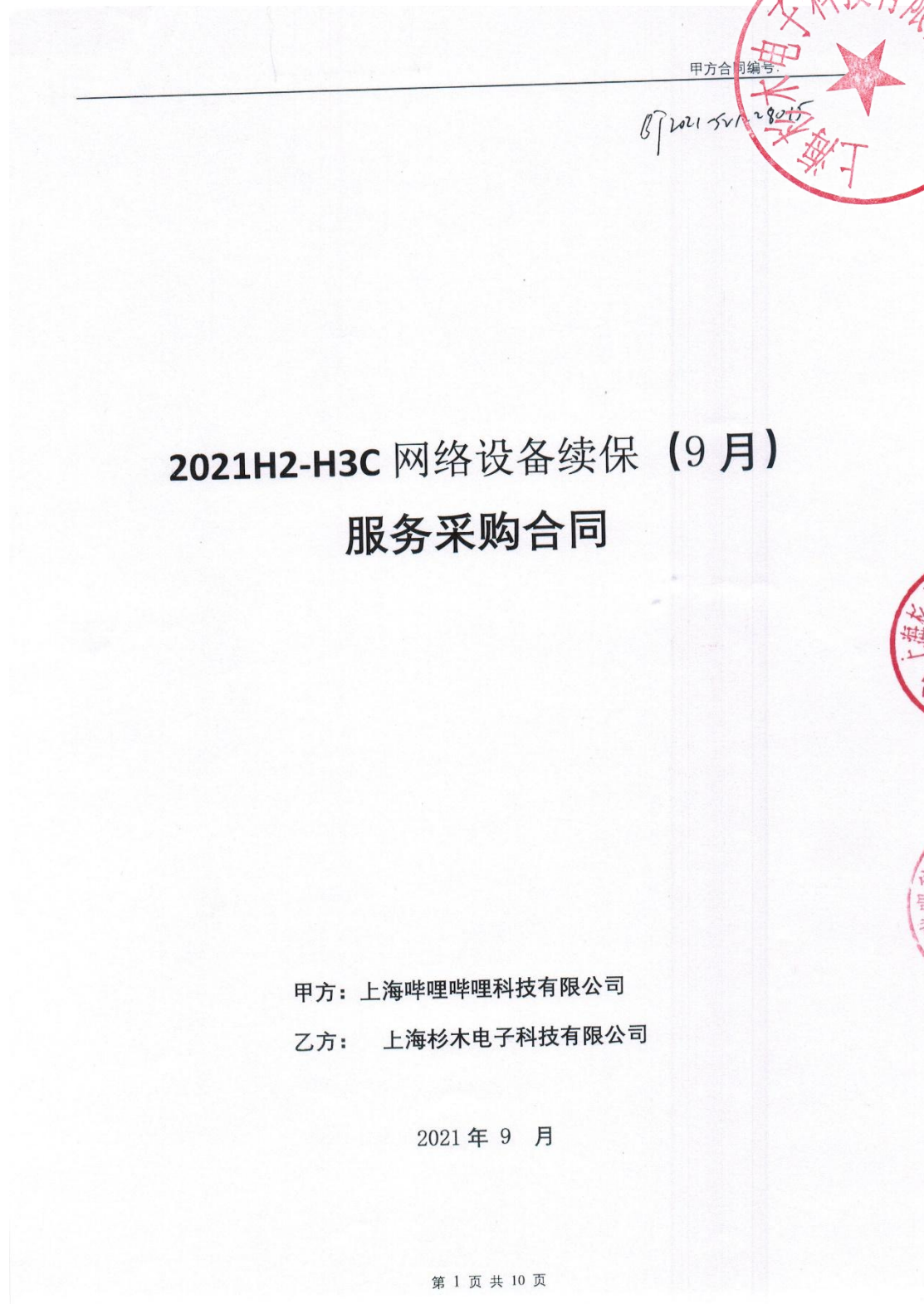
备注：各单位可根据各自的项目数量，调整表单的列数。

响应方授权代表签字：朱千弛

(加盖企业公章)

日期：2025 年 9 月 8 日

16.2. 上海哔哩哔哩客户



甲方合同编号:	
甲方: 上海哔哩哔哩科技有限公司 (以下简称“甲方”)	
联系地址: 上海市杨浦区政立路 485 号国正中心 3 号楼	
乙方: 上海杉木电子科技有限公司 (以下简称“乙方”)	
联系地址: 上海市徐汇区宜山路 333 号汇鑫国际大厦 1204 室	
甲、乙双方根据《中华人民共和国民法典》及相关的法律、行政法规之规定, 就甲方向乙方采购指定产品事宜达成如下条款:	
第一条 产品概况 (详情请见附件)	
1. 甲、乙双方约定, 甲方向乙方采购设备维保服务, 乙方按约定向甲方提供服务, 具体服务涉及设备、服务范围、执行标准、质量检测等内容详见附件约定 (以下简称“服务”)。	
2. 甲、乙双方约定未经甲方书面同意, 乙方不得随意改变服务标准、内容、数量、价格、工艺、时间等, 如需变更服务已确定的内容、参数、数量、时间、地点等内容, 双方应协商达成一致以书面形式确认。	
第二条 费用及付款方式	
1. 本合同服务总金额 (含税): (RMB) ¥ 1,747,037.00 元; 大写: 壹佰柒拾肆万柒仟零叁拾柒元整。	
(1) 上述金额表述两者不符时以中文金额为准 (下同)。	
(2) 上述金额已经包含服务包含的检测、维护、保修、更新升级、部件更换 (含部件费用) 等服务内容的所有费用, 除此外甲方无需向乙方或任何第三方支付额外费用。	
2. 甲、乙双方约定的具体付款方式如下:	
(1) 本合同生效后自甲方确认乙方提供【增值税专用发票】之日起十五个工作日内甲方向乙方汇付首付款, 即 (RMB) ¥ 1,397,629.6 元, 大写: 壹佰叁拾玖万柒仟陆佰贰拾玖元陆角 (以下简称“首付款”)。	
(2) 乙方开始提供服务 (即维保服务期生效) 并经甲方验收确认 30 日后, 自甲方确认乙方提供【增值税专用发票】之日起十五个工作日内甲方向乙方汇付尾款, 即 (RMB) ¥ 349,407.4 元, 大写: 叁拾肆万玖仟肆佰零柒元肆角 (以下简称“尾款”)。	
(3) 乙方未及时出具合格的【增值税专用发票 (13 %)】或未履行甲方支付费用的前置条件时, 甲方有权相应顺延支付费用。	
3. 甲乙双方各自承担应当缴纳的税费, 乙方银行账户信息:	
乙方收款账户信息如下:	
开户行	平安银行上海西南支行

第 2 页 共 10 页

甲方合同编号:

开户人	上海杉木电子科技有限公司
账号	175536-11006523950201

➤

甲乙双方约定若乙方变更收款银行账户信息时，应当及时书面通知甲方，因乙方未及时书面通知甲方所产生的所有额外费用，均由乙方自行承担。

第三条

服务提供

1.

维保服务供货方式：原厂上门提供维护和保修。

2.

维保服务提供地点： 甲方设备所在地

3.

维保服务期： 原设备维保到期时间（2021/10/6、2021/10/8、2021/12/2，以双方系统显示确认为准）至 2023-12-2 止

甲方维保联系人信息：

上海市杨浦区政立路 485 国正中心 3 号楼 祝欣媛 18762315729

4.

如甲方或乙方需要变更上述信息的，需在服务提供前提前叁个工作日书面通知对方。

第四条

服务质量及保修维护

1.

乙方保证具备向甲方提供本合同服务的资质和能力，以原厂标准向甲方提供服务，服务应符合中华人民共和国法律、法规及国家和地方有关服务的质量标准规范以及合同和附件的约定。

2.

乙方提供的服务符合本合同和附件约定、服务说明书及该服务所有技术文件中关于功能、性能、品质及质量的描述，甲方以任何形式确认服务验收合格，并不表明甲方对服务质量的完全认可，乙方对服务承担质量瑕疵担保责任。

3.

乙方承诺在维保服务服务期内，在接到甲方的报修或维护通知之日起 24 小时内赶到现场为甲方提供保修或维护服务（如附件有具体约定，则以附件的约定为准）。

➤

乙方的保修或维护服务联系人为： H3C 原厂官方 ，联系电话为： 400 810 0504 。

4.

服务维保期限届满，乙方应继续为甲方提供相应的保修服务，根据具体服务内容甲方向乙方支付合理的维修服务费用，乙方根据服务内容应事先告知甲方费用标准。

5.

乙方保证若维保服务造成人身、财产等损害，由此产生的责任应由乙方承担。

第五条

权利义务

1.

甲、乙双方均保证具有洽谈、签订、履行本合同的主体资格及相关所需资质，并已获得了洽谈、签订、履行本合同的完全有效且不可撤销的所有授权、同意、批准或许可，且任何一方洽谈、签订、履行本合

甲方合同编号: 

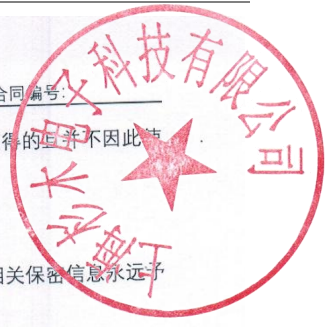
同的行为将不会违反任何在先义务。

2. 乙方应及时向甲方提供乙方加盖公章具备合法经营资质的证明文件及合法提供服务的资质文件, 甲方不得对本合同乙方的任何承诺及保证的审查行为而承担任何责任。
3. 甲、乙双方约定本合同项下乙方完成的全部服务自完成之日所有权属于甲方, 乙方不得在全球范围内申请、注册、登记任何与甲方相同或相近似的商标、专利和著作权等。
4. 甲、乙双方在其自身宣传材料、名片、市场宣传、网站建设以及其他任何方面使用对方授权的名称、域名和网站, 都必须事先通知对方, 并获得对方的许可后方可进行;
5. 除履行本合同所需外, 未经对方书面许可, 任何一方不得擅自使用、复制对方的商标、标识、版权作品、商业信息、技术及其他资料等。在履行本合同期间, 甲乙双方在使用对方授权的企业名称、商标、商号、品牌、域名和网站时, 应当完全单独为甲乙双方在本合同中约定的内容服务, 不得夹带其他业务内容。
6. 甲、乙双方约定若乙方违反诚实信用原则或经营状况严重恶化, 甲方认为乙方难以继续履行本合同时甲方可单方终止本合同。

第六条 保密责任

甲、乙双方均保证对在洽谈本合同约定事项过程中以及签订、执行本合同过程中所获悉的属于对方的且无法自公开渠道获得的文件、资料及信息等予以保密, 具体如下:

1. 接受保密信息的一方 (“接收方”) 应:
 - (1) 对保密信息严格保密;
 - (2) 不向任何第三方披露任何保密信息;
 - (3) 除为履行本合同之目的外, 不为任何其他目的使用保密信息。
2. 保密信息的定义, “保密信息”指:
 - (1) 有关本合同的存在和内容以及有关本合同预期交易的信息;
 - (2) 一方 (“披露方”) 向接收方披露的全部专有、保密、非公开的技术信息和 (或) 商业信息, 包括但不限于 (a) 披露方在本合同签署前或之后披露给接收方或其雇员的任何研发设计、服务或产品设计理念/想法、产品及其规格、数据、模型、样品、草案、产品测试结果等技术类信息;
(b) 营销要求和策略、产品计划及价格、客户名单、公司业务发展的方向、涉及经营管理的制度与流程等的商业信息; (c) 通过签订和履行本合同而获知的对方及对方关联公司的任何信息和因履行本合同而获悉的资料、软件、数据等信息数据内容; 以及 (d) 其它由披露方披露给接收方的且需向第三方承担保密义务的信息 (不论该等信息是以书面、口头、图形、网络还是其他任何形式进行了披露)。
 - (3) “保密信息” 不包括以下信息: (a) 披露方披露之时或之前已为公众所知的信息; (b) 披露之后

甲方合同编号: 

非因接收方的行为或过错而为公众所知的信息；或（c）接收方从第三方处获得的信息并不因此使接收方违反其保密义务的信息。

3. 披露的同意。一方需要对外披露保密信息时应获得另一方的书面确认。
4. 保密期限。在披露方提供给接收方的保密信息被合法地公开之前，接受方应对相关保密信息永远予以保密。
5. 擅自披露的责任。如一方违反其在本合同项下的保密义务，该一方需承担违约赔偿责任（包括但不限于：为追究违约责任支出的律师费、仲裁费、差旅费、鉴定费、文印费、审计费等）。

第七条 不可抗力

1. 本合同所称的不可抗力是指一切不可预见、不可避免并不能克服的客观情况，包括但不限于洪水、地震、飓风、火灾等自然灾害及战争、动乱等情况，以及政府对本合同订立时有效之相关法律、行政法规、政策等进行修订、变更、废止，或颁布新的法律、行政法规、政策以取代原有法律、行政法规、政策或使原有法律、行政法规、政策处于废止状态，从而最终导致本合同无法继续履行。
2. 因不可抗力或者国家政策法律的变化而致使本合同中任何一方或双方部分或全部不能履行本合同的，遭受不可抗力的一方无需向对方承担违约责任，但应及时通知对方不可抗力的发生情况并提交不可抗力的合法证明材料。
3. 如不可抗力情况消失后，本合同仍有必要履行且具备继续履行的条件，双方应继续履行本合同；如因不可抗力导致本合同没有必要或无法继续履行的，则本合同任何一方均有权提出解除本合同，且双方互不承担违约责任。

第八条 违约责任

1. 无论故意或过失，甲、乙双方未履行本合同约定义务或应遵守事项均视为违约。任何一方违约，另一方有权要求违约方停止违约行为，自违约方告知停止违约行为之日起 10 日内，违约方不停止违约行为的，守约方有权单方面解除本合同，解除本合同的通知到达违约方时本合同解除，解除合同不影响守约方要求违约方承担违约赔偿责任（包括但不限于：为追究违约责任支出的律师费、诉讼费、差旅费、鉴定费、文印费、审计费等）。具体提供维保服务的服务方、服务人员违反约定，视为乙方违约。
2. 甲方无正当理由故意未按约定期限向乙方付款时，每逾期一日，甲方须向乙方承担应付而未付款万分之一的滞纳金，逾期超过 30 日仍未付款的，乙方有权解除合同，并要求甲方承担由此给乙方造成的全部损失。
3. 乙方保证取得签署并履行本合同项下内容的合法经营资质、授权资质等，保证有权依法运营其服务，向甲方提供的服务不违反中国法律法规，不侵害任何第三人权益，若发生上述情况或乙方履行本合同过程

甲方合同编号: X

中违反诚实信用原则时，乙方应向甲方承担全部赔偿责任（包括但不限于仲裁费、律师费、赔偿款、差旅费、鉴定费、产品召回费用、罚款等）并向甲方赔偿本合同总金额叁倍的违约金，若甲方的全部损失超过前述违约金时，乙方应赔偿甲方的全部损失并按甲方要求的方式做出公开赔礼道歉。前述约定的违约金，均系双方在签订本合同时已经预见到的违约方因违约方之违约行为将遭受的最低损失。发生违约情形时，守约方在约定的数额范围内主张违约金或损失赔偿金的，违约方放弃主张违约金过高的权利，守约方免于就实际损失举证。但守约方主张其因违约方的违约行为遭受的实际损失大于本合同约定的数额的，守约方应当举证证明其实际发生的损失。

4. 由于乙方提供的服务无法通过甲方的验收或无法满足合同目的导致甲方对乙方做出乙方不具备提供本合同所需能力的判断的；或乙方若单方实质性违约或不能充分履行义务，并在甲方告知后未能进行补救；或未能在甲方要求的期限前提供符合要求的增值税发票；或由于乙方的行为甲方认定乙方不能胜任本合同的履行的；或虽然甲方出于情势所迫不得不使用乙方提供的带有瑕疵的服务开展业务，但甲方仍旧决定追究乙方相关责任的，则甲方在法律允许的前提下有权作出以下一项或多项决定：

- ❖ 甲方有权要求无条件解除/终止本合同，并不再支付任何费用。
- ❖ 甲方有权要求乙方返还已付全额款项。
- ❖ 甲方有权不再支付任何费用。
- ❖ 甲方有权要求乙方向甲方承担损害赔偿。甲方要求乙方承担的损害赔偿的范围包甲方所受的直接损失和间接损失。

5. 因本合同的履行产生的乙方应承担的违约金、赔偿金等，甲方有权从未付款项中预先扣除，不足部分乙方应当补齐。

第九条 禁止转让

乙方未经甲方同意，不得以任何理由将本合同相应权利或义务转让、出借、委托、许可、授权等以任何形式给第三方，同时，不得以本合同中权利对外设立质权及其他担保物权，也不得作其他任何形式的处分，但本合同另有约定的除外。

第十条 通知与送达

双方之间的任何重要通知或书面函件，必须以中文写成，以电子邮件、专人送达（包括特快专递）或挂号信函之形式发送，除非事先以书面通知更改，则双方的沟通工具如下：

双方	合作联系人	电子邮件必要联系人	电子邮箱	手机电话
甲方	杨柳	/	66@bilibili.com	13917930978

第 6 页 共 10 页

甲方合同编号

	/	杨柳	guoyi@bilibili.com	486147847
乙方	刘小芳	/	lxf@sh-shanmu.com	16221235273
	/			

1. 若为电子邮件形式，则邮件进入收件一方指定之电子邮件系统的时间即视为已送达；若为专人派送时（包括特快专递），按收件一方签收之日期为准；若以挂号邮件发送时，以邮局所出具之收据为凭，自寄发日起计五（5）个工作日为准。

2. 鉴于双方未来可能有以电子邮件确认相关合作内容的情况，故设定电子邮件必要联系人，即有关本合同的任何电子邮件内容均需要明示抄送双方指定的电子邮件必要联系人。

第十一条 争议解决

1. 本合同之签署、效力、解释和执行以及本合同项下争议之解决，均应适用中华人民共和国法律法规。

2. 本合同在履行中所产生的争议，或与本合同有关的一切争议，由甲、乙双方协商解决。

3. 甲、乙双方约定协商不成，协商不成则争议各方均一致同意将争议提交广州仲裁委员会根据仲裁规则进行仲裁。仲裁裁决为一裁终局，对各方均有法律约束力。

第十二条 其它

1. 可分割性。除法律、行政法规另有规定外，如果本合同的任何条款违法，该条款将被修改和解释，以在法律允许的最大限度内，最好地实现原条款的目标，同时本合同的其余条款将继续保留其全部效力。

2. 本合同附件为本合同不可分割的组成部分。若本合同附件与合同正文约定不一致的，以附件的约定为准。

3. 本合同未尽事宜，合同各方可另行协商一致签订补充合同、备忘录、订购单等形式予以书面约定，作为本合同的有效补充，具有同等法律效力。

4. 本合同一式肆份，双方各执贰份，经甲、乙双方盖章后生效，具同等法律效力。

附件：服务涉及的设备清单

附件：乙方资质证明文件

甲方：上海哔哩哔哩科技有限公司

(盖章):

签约日期:

乙方：上海杉木电子科技有限公司

(盖章):

以下无正文

第 7 页 共 10 页

甲方合同编号:

附件:

服务价格明细清单

设备大类	设备类型	产品描述	产品数量	服务描述	服务数量	未税单价	含税单价	总价
C2180702113D	PSR2400-54A	交流电源模块-2400W	80	网络产品基本维保服务尊享版(7x24x4到达)	2.167	858.03	969.57	168084.66
C2180702113D	LSXM116XFAN	H3C S12516X-AF 以太网交换机风扇模块	8	网络产品基本维保服务尊享版(7x24x4到达)	2.167	858.03	969.57	16808.47
C2180702113D	LSXM1SUPB1	H3C S12500X-AF 主控制引擎模块	12	网络产品基本维保服务尊享版(7x24x4到达)	2.167	5243.50	5925.15	154077.60
C2180702113D	LSXM108XFAN	H3C S12508X-AF 以太网交换机风扇模块	4	网络产品基本维保服务尊享版(7x24x4到达)	2.167	667.35	754.11	6536.63
C2180702113D	LSXM1SFH08C1	S12508X-AF 交换网板, H型(C类)	12	网络产品基本维保服务尊享版(7x24x4到达)	2.167	5243.50	5925.15	154077.60
C2180702113D	QSFP-40G-D-AOC-7M	40G QSFP+ to 40G QSFP+7m AOC	4	网络产品基本维保服务尊享版(7x24x4到达)	2.167	691.57	781.47	6773.78
C2180702113D	LSXM1QGS48HB1	H3C S12500X-AF 48 端口 40G 以太网光接口模块 (QSFP+) (HB)	10	网络产品基本维保服务尊享版(7x24x4到达)	2.167	17160.53	19391.40	420211.64
C2180702113D	LSXM2SFH16C1	H3C S12516X-AF 交换网板, H型(C类)	24	网络产品基本维保服务尊享版(7x24x4到达)	2.167	8580.27	9695.70	504253.97
C2180702113D	LSXM1TGS48HB1	H3C S12500X-AF 48 端口 万兆以太网光接口模块 (SFP+, LC) (HB)	2	网络产品基本维保服务尊享版(7x24x4到达)	2.167	10486.99	11850.30	51359.20
C2180702113D	LS-12516X-AF	H3C S12516X-AF 以太网交换机主机	4	网络产品基本维保服务尊享版(7x24x4到达)	2.167	8580.27	9695.70	84042.33
C2180702113D	LS-12508X-AF	H3C S12508X-AF 以太网交换机主机	2	网络产品基本维保服务尊享版(7x24x4到达)	2.167	5243.50	5925.15	25679.60
C2180718313K	LSXM1QGS48HB1	H3C S12500X-AF 48 端口 40G 以太网光接口模块 (QSFP+) (HB)	4	网络产品基本维保服务尊享版(7x24x4到达)	2	17160.53	19391.40	155131.20
合计	壹佰柒拾肆万柒仟零叁拾柒元整 ¥: 1747037.00							

甲方合同编号:





16.3. 上海电信科技发展



[2022 年上海电信战略大客户部现场办公业务体验及技术支持服务

项目]技术服务合同

委托方（甲方）：上海电信科技发展有限公司
地址：上海市普陀区江宁路 1306 弄 7 号 19 楼
法定代表人/负责人：夏雷
项目联系人：赵强胜
联系方式：19145546959
通讯地址：普陀区江宁路 1306 弄 7 号 19 楼
电 话：62271800 传 真：
电子邮箱：

受托方（乙方）：上海杉木电子科技有限公司
地址：上海市奉贤区头桥镇红陆路 1 号-39
法定代表人/负责人：苗森
项目联系人：宗绪鹏
联系方式：021-66288311
通讯地址：上海市奉贤区头桥镇红陆路 1 号-39
电 话：021-66288311 传 真：
电子邮箱：

本合同甲方委托乙方就 2022 年上海电信战略大客户部现场办公业务体验及技术支持服务项目（“项目”）进行私有化业务环境体验、办公系统迁移支持、现场技术支持等专项技术服务，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《中华人民共和国合同法》的规定，达成如下合同，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：

- 1.1 技术服务的目标：提供现场技术支持以及试用体验。
- 1.2 技术服务的内容：提供私有化业务环境体验、办公系统迁移支持及现场技术支持。

- 1.3 技术服务的方式：人员派驻现场。

第二条 乙方应按下列要求完成技术服务工作：

- 2.1 技术服务地点：上海。
- 2.2 技术服务期限：合同签订之日起至 60 日。
- 2.3 技术服务进度：7X24 小时响应。

第 1 页 共 9 页



2.4 技术服务质量要求：对技术服务工作的质量进行保证措施、应急保障措施。

2.5 技术服务质量期限要求：按工期要求完成。

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：

3.1 提供技术资料：按需。

3.2 提供工作条件：按需。

3.3 其他配合协作事项：按需。

3.4 甲方提供上述技术资料、工作条件和配合协作事项的时间及方式：实时。

第四条 甲方向乙方支付技术服务报酬及支付方式为：

4.1 本合同费用总额（含税价）：人民币大写贰拾陆万捌仟伍佰伍拾元，小写 268550.00 税率为 6%；其中价款为人民币大写贰拾伍万叁仟叁佰肆拾玖元零角陆分，小写 253349.06，增值税款为人民币大写壹万伍仟贰佰元玖角肆分，小写 15200.94。

本合同费用已包括甲方就乙方履行本合同所应支付的全部报酬、所需的全部费用及税费（包括但不限于营业税、增值税等）。

除另有约定外，甲方无需就本合同项下委托事项向乙方支付上述费用之外的任何其他费用及税费（包括但不限于营业税、增值税等）。

4.2 甲方凭乙方开具的相应金额的、符合国家规定的发票支付技术服务费，并按以下第[1]种方式向乙方付款：

(1) 一次性支付

乙方完成技术服务工作并经甲方验收合格后[30]个工作日内，甲方向乙方支付技术服务费。

(2) 分期支付

甲方分期向乙方支付技术服务费：[/]。

4.3 乙方向甲方开具增值税专用发票的，乙方应派专人或使用挂号信件或特快专递方式在发票开具后 30 日内送达甲方，送达日期以甲方签收日期为准；逾期送达的，每逾期一日，乙方应按逾期送达发票金额的万分之三支付违约金，若因逾期送达造成甲方无法抵扣的，乙方还应赔偿甲方由此遭受的损失，金额相当于逾期送达发票可抵扣金额。

4.4 如乙方提供的增值税专用发票不符合法律法规要求或本合同约定，或不能通过税务认证的，甲方有权拒收或于发现问题后退回，乙方应及时更换，如因此导致未能在第 4.3 条约定时限内送达增值税专用发票的，乙方应当按照第 4.3 条约定承担逾期送达的违约责任。

4.5 本合同费用总额的所有支付由甲方以银行转账（银行转账、电汇、支票等方式）付至乙方。甲乙双方银行账户信息和纳税人信息：

甲方信息如下：



开户行：中国民生银行股份有限公司上海延中支行
银行地址：上海市延安西路 726 号
户名：上海电信科技发展有限公司
账号：0229014140000145
纳税人识别号：91310101132421755T
地址：上海市杨浦区国权北路 1688 弄湾谷科技园 20 号楼
电话：021-63111888
乙方信息如下：
开户行：平安银行上海西南支行
银行地址：上海市徐汇区漕溪北路 1200 号
户名：上海杉木电子科技有限公司
账号：11006523950201
纳税人识别号：91310120703380388R
地址：上海市奉贤区头桥镇红陆路 1 号-39
电话：66288311

4.6 若根据本合同约定乙方应当支付违约金和/或承担赔偿责任，则甲方有权从上述任何一笔付款中直接扣除相应金额。

第五条 保密

5.1 乙方对甲方所提供的所有资料以及在本合同签订、履行过程中所接触到的甲方及其关联公司的商业秘密、技术资料、客户信息等资料和信息（统称“保密资料”）负有保密义务。未经甲方书面许可，乙方不得向任何第三方披露，不得将保密资料的部分或全部用于本合同约定事项以外的其他用途。乙方有义务对保密资料采取不低于对其本身商业秘密所采取的保护手段予以保护。乙方可仅为本合同目的向其内部有知悉保密资料必要的雇员披露保密资料，但同时须指示其雇员遵守本条规定的保密及不披露义务。

5.2 乙方仅为履行本合同之目的对保密资料进行复制。乙方不得以任何方式（如软硬盘、图纸、彩样、照片、菲林、光盘等）留存保密资料。乙方应当在完成委托事项或本合同终止或解除时将保密资料原件全部返还甲方，并销毁所有复制件。乙方应当妥善保管保密资料，并对保密资料在乙方期间发生的被盗、泄露或其他有损保密资料保密性的事件承担全部责任，因此造成甲方损失的，乙方应负责赔偿。

5.3 当出现下述情况时，本条对保密资料的限制不适用。当保密资料：

- (1) 并非乙方的过错而已经进入公有领域的。
- (2) 已通过该方的有关记录证明是由乙方独立开发的。
- (3) 由乙方从没有违反对甲方的保密义务的人合法取得的。或



(4) 法律要求乙方披露的，但乙方应在合理的时间提前通知甲方，使其得以采取其认为必要的保护措施。

5.4 如乙方违反本合同关于保密的约定，乙方应赔偿因此而给甲方造成的一切损失。

5.5 本保密条款自保密资料提供或披露之日起至本合同终止或解除后[2]年内持续有效。

第六条 本合同的变更必须由双方协商一致，并以书面形式确定。但有下列情形之一的，一方可以向另一方提出变更合同权利与义务的书面请求，另一方应当在收到书面请求后 5 个工作日内予以答复；逾期未予答复的，视为同意：

无。

第七条 未经甲方事先书面同意，乙方不得将本合同项目部分或全部服务工作转由第三人承担。

第八条 双方确定以下列标准和方式对乙方的技术服务工作成果进行验收：

8.1 乙方完成技术服务工作的形式：甲方要求的形式。

8.2 技术服务工作成果的验收标准：甲方认可服务质量。

8.3 技术服务工作成果的验收方法：由甲方确定验收方法。

8.4 验收的时间和地点：由甲方决定。

第九条 侵权处理

9.1 乙方应当保证，其依本合同为甲方提供技术服务过程中和/或其为甲方提供的服务成果不侵犯任何第三人的合法权益。如果有人提出法律或行政程序（合称“侵权指控”），声称甲方侵犯了其知识产权等合法权益的，乙方应当负责解决，并赔偿甲方就此所承担的一切损失和费用，包括但不限于上述侵权指控中所产生的诉讼费用、合理的律师费用、调查费用、和解金额或生效法律文书中规定的赔偿金额。

9.2 如果在侵权指控的审理过程中有关机关禁止甲方继续使用技术服务成果的部分或全部，乙方应当采取以下措施之一：

(1) 使甲方重新免费获得使用上述技术服务成果的权利，或

(2) 免费更换或改造上述技术服务成果，使甲方不受上述禁令限制继续使用技术服务成果。

(3) 其它使甲方对技术服务成果拥有合法使用权，或其它弥补甲方受损害、实现合同目的的合理方式。

乙方采取上述措施不能免除乙方就甲方因此遭受的损失进行赔偿的义务。

第十条 项目服务成果的权利归属



10.1 双方确定，乙方所完成的服务成果的所有权利，包括但不限于知识产权、专利申请权和所有权，归甲方所有。

10.2 双方确定，甲方利用乙方的服务成果所完成的新的技术成果的所有权利，包括但不限于知识产权、专利申请权和所有权，归甲方所有。

第十一条 双方确定，乙方在向甲方提供服务过程中，根据甲方要求，为甲方指定的人员提供技术指导和培训。

11.1 技术指导和培训内容：按需。

11.2 地点和方式：按需。

11.3 费用及支付方式：/。

第十二条 违约责任

12.1 双方确定，任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应赔偿因违约给对方造成的一切损失。

12.2 乙方未能按本合同约定按期提供技术服务的，每逾期1日，乙方应当按照本合同费用总额总额的1%向甲方支付违约金。如违约金数额累计达到本合同费用总额总额的30%时，甲方有权终止本合同，乙方仍应支付上述违约金、退还甲方已支付款项并按照同期中国人民银行贷款利率计付利息，同时赔偿甲方的相应损失。

12.3 乙方提供技术服务不符合本合同要求的，乙方应当按照甲方要求更正和修改，并承担由此产生的全部费用。同时，甲方有权终止本合同，乙方应当退还甲方已支付款项并按照同期中国人民银行贷款利率计付利息，并赔偿甲方的相应损失。

第十三条 双方确定，在本合同有效期内，甲方指定赵强胜为甲方项目联系人，乙方指定宗绪鹏为乙方项目联系人。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或造成损失的，应承担相应的责任。

第十四条 双方确定，出现下列情形之一，致使本合同的履行成为不必要或不可能，可以解除本合同：

14.1 发生不可抗力。

14.2 /。

第十五条 法律适用和争议解决

15.1 本合同适用中华人民共和国法律。



15.2 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，则任何一方均可采取下述第2种争议解决方式：

(1) 将该争议提交上海仲裁委员会，按照申请仲裁时该会的仲裁规则进行仲裁。仲裁在上海进行。仲裁语言为中文。仲裁裁决是终局的，对双方均有约束力。仲裁费用由败诉方承担。

(2) 向甲方所在地有管辖权的人民法院起诉。

15.3 仲裁或诉讼进行过程中，双方将继续履行本合同未涉仲裁或诉讼的其它部分。

第十六条 双方确定，本合同及相关附件中所涉及的有关名词和技术术语，其定义和解释如下：

16.1 “不可抗力”：地震、台风、水灾、火灾、战争以及其它本合同各方不能预见，并且对其发生和后果不能防止或不能避免且不可克服的客观情况。

16.2 [/]。

第十七条 与履行本合同有关的下列技术文件，经双方以/方式确认后，为本合同的组成部分：

17.1 技术背景资料：/。

17.2 可行性论证报告：/。

17.3 技术评价报告：/。

17.4 技术标准和规范：/。

17.5 原始设计和工艺文件：/。

17.6 其他：/。

第十八条 双方约定本合同其他相关事项为：

18.1 任何一方未经另一方同意，不得向任何第三方透露本合同的签订及其内容。甲方向其关联公司透露的，不在此限。

18.2 任何与本合同相关但未在本合同中明确规定的事项将由双方另行友好协商解决。对本合同做出的任何修改和补充应为书面形式，由双方签字盖章后成为本合同不可分割的部分。本合同与其补充合同或补充协议冲突时，以补充合同或补充协议为准。

18.3 未得到对方的书面许可，一方均不得以广告或在公共场合使用或摹仿对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写，任何一方均不得声称对对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写拥有所有权。



18.4 本合同的任何内容不应被视为或解释为双方之间具有合资、合伙、代理、劳动关系。

18.5 本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、合同和协议。

18.6 甲乙双方因履行本合同或与本合同有关的一切通知都必须按照本合同中的地址，以书面信函形式或双方确认的传真或类似的通讯方式进行。采用信函形式的应使用挂号信或者具有良好信誉的特快专递送达如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。

第十九条 本合同自双方签字盖章之日起生效。本合同一式肆份，甲方执贰份，乙方执贰份，具有同等法律效力。

第二十条 附件为本合同不可分割的部分。若附件与合同正文有任何冲突，以合同正文为准。

本合同附件为：

附件一：服务清单

附件二：廉洁协议

补充附页

经友好协商，对本合同条款补充、修改如下，本补充附页为合同正文的一部分，与合同正文冲突时，以本补充附页为准：

无



甲方：上海电信科技发展有限公司

法定代表人/负责人

或授权代表：（签字）

2021年12月26日



乙方：上海杉木电子科技有限公司

法定代表人/负责人

或授权代表：（签字）

2022年12月26日





印花税票粘贴处:



(以下由技术合同登记机构填写)

合同登记编号:

[illegible]

1. 申请登记人: _____
2. 登记材料: (1) _____
(2) _____
(3) _____
3. 合同类型: _____
4. 合同交易额: _____
5. 技术交易额: _____

技术合同登记机构 (印章)

经办人：

年 月 日



16.4. 上海期货信息技术

合同编号: SMDZ202405001

合同编号:

维 保 服 务 合 同

所属项目：技术公司金融科技研究中心 2024 年度云计算平台基础设施
施续保服务采购项目

甲 方： 上海期货信息技术有限公司

乙 方： 上海杉木电子科技有限公司

签订日期：2024 年 月



合同编号: SMDZ202405001



本合同由下述双方签订:

甲方: 上海期货信息技术有限公司
地址: 上海市浦东新区乐昌路 399 号
邮编: 201201
联系电话:

乙方: 上海杉木电子科技有限公司
地址: 上海市徐汇区宜山路 333 号汇鑫国际 1204
邮编: 200020
联系电话: 15221235273

甲乙双方根据相关法律法规, 在平等互利的基础上经友好协商, 就甲方向乙方采购云计算平台基础设施续保服务事宜达成如下协议:

一、标的物 and 金额

1、维保服务清单及价格明细详见本合同附件一: 设备续保清单

2、合同总金额: 人民币 228500 元 (大写: 贰拾贰万捌仟伍佰元整)。

其中, 不含税金额 202212.39 元, 增值税税率13%, 增值税 26287.61 元。当国家税收政策发生变化时, 实际结算时按照调整后的税率相应调整本合同相关的价格, 并按调整后的价格开具增值税专用发票。

上述合同金额已包含了维保期间技术支持、维修、保养、配件更换、运输、安装、调试、人工等甲方接受本合同项下服务的所有相关费用以及税金, 为甲方在本合同项下应支付的全部费用。

二、维保期限

本合同项下货物的维保期为一年。如果合同签订之日早于设备原维保到期之日, 设备续保周期自原维保到期之日起一年; 如果合同签订之日等于或晚于

2 / 12

合同编号: SMDZ202405001



设备原维保到期之日，设备续保周期自续保合同签订之日起一年。

三、维保服务

1、本合同项下货物的维保服务由货物原厂承担，乙方负连带责任。维保服务级别及具体内容见本合同附件二。

2、乙方应确保维保方按照合同约定提供维保服务。如维保方或乙方收到甲方通知后未按合同约定响应或解决，甲方可以采取必要的补救措施，但其风险和费用将由乙方承担，甲方根据本合同规定对维保方和乙方行使的其它权利不受影响；如因此致使甲方遭受直接或间接经济损失的，由乙方承担全额赔偿责任。

3、在货物维保期内或应当由乙方负责的其他情况下，若由于维保方更换、修理和续补货物，而造成货物不得不停止使用，货物维保期应依照停止使用的实际时间加以延长。如因此给甲方造成损失，乙方应负责赔偿。

5、联系方式：[厂商联系方式 400-810-0504]。

四、付款和开票

1、本合同签订且验收通过后10个工作日内，甲方将合同总金额的65%，即人民币[148525]元（大写：人民币[壹拾肆万捌仟伍佰贰拾伍]元整）支付给乙方。

2、本合同约定的维保期届满10个工作日内，且维保方和乙方依约履行义务的前提下，甲方将合同总金额的35%，即人民币[79975]元（大写：人民币[柒万玖仟玖佰柒拾伍]元整）支付给乙方。

3、甲方每次付款前，乙方需开具真实有效的相应金额增值税专用发票，否则甲方有权顺延付款时间并不承担任何责任。甲方开票信息内容如下：

名称：上海期货信息技术有限公司

纳税人识别号：91310000761619983T

地址：上海市浦东新区来安路996号7幢

电话：68401039、68401290

账号：310066056018010004121

开户银行：交行上海期货大厦支行

3 / 12

合同编码: SMDZ202405001



若乙方所开发票不符合现行财税政策导致甲方不能抵扣增值税进项税、无法在企业所得税前列支成本费用等造成的损失，由乙方承担赔偿责任。

五、验收

本合同项下维保服务的验收方式为：

乙方续保下单后，经甲方查验原厂官网确认满足采购需求，或由乙方提供满足采购需求的原厂服务书面文件。

六、违约与赔偿

1、除本合同另有约定外，如果任何一方存在违反本合同任何约定的行为，守约方有权书面通知违约方纠正违约行为。如果违约方收到该书面通知后十个工作日内仍未纠正其违约行为，守约方有权立即终止本合同，同时要求违约方赔偿守约方由此遭受的所有损失。

2、在乙方已经完全适当的履行了其在本合同项下相应义务的前提下，如果甲方不按照本合同的约定支付款项，应从收到乙方书面催款通知的次日起，每日向乙方偿付逾期付款部分总值的千分之一的违约金。此项违约金以逾期付款部分总值的百分之二十为限。

3、维保期内，如因乙方和/或维保方未能及时响应并解决甲方的故障报修而导致甲方或任意第三方遭受损失（包括但不限于甲方自行解决问题导致的费用和/或损失等），乙方应对造成的该等损失承担一切赔偿责任。

4、若维保服务验收不合格且给甲方造成损失的，甲方有权单方解除合同，乙方应按照合同总金额百分之二十的标准支付违约金。若违约金不足以弥补甲方因此遭受的损失，则乙方还应予补足。

5、因乙方和/或维保方责任的维保服务造成任何财产毁损、灭失的，乙方应当赔偿所有损失。

6、乙方保证未经甲方书面同意不得委托除货物原厂以外的任何第三人进行维保活动，否则甲方有权单方解除合同，无需支付任何维保费用，且乙方应按照合同总金额百分之二十的标准支付违约金。若违约金不足以弥补甲方因此遭受的损失，则乙方还应予补足。对于第三人的维保活动，乙方应当承担连带担保责任。

4 / 12

合同编码: SMDZ202405001



7、乙方特此确认，甲方有权在应支付给乙方的费用中直接扣除乙方应支付的违约金和/或应给予甲方的赔偿。

七、合同纠纷的解决

因本合同引起的或与本合同有关的任何争议，首先由双方友好协商解决；在协商失败后，任何一方均有权提请上海仲裁委员会在浦东按照该会现时有效的仲裁规则进行仲裁，仲裁裁决是终局的，对双方均有约束力。在仲裁审理过程中，除正在进行审理的有争议部分外，本协议其他不受影响的部分应当继续履行。

八、保密

1、在合同履行期间，乙方和/或维保方可能会获得甲方的机密信息以及任何有关商业、市场、技术、科技及由甲方透露的其他信息，该信息在被告知时，就被指定为机密信息（或类似的指定）、在秘密环境下告知、或能够被乙方和/或维保方通过运用合理的商业判断认为是机密信息（统称“机密信息”）。乙方应对甲方的机密信息保密，并确保维保方亦对甲方的机密信息保密，均只为履行本合同之目的使用该等机密信息；并且不应在合同履行期间和履行后，没有甲方事先的书面同意：（a）泄露或透露甲方的机密信息或其中任何部分给第三方，但因该第三方职责使其有理由获知甲方的机密信息和与乙方有相同保密义务的除外，或者（b）为自身或任何第三方利益使用甲方的机密信息。以上所称保密义务不适用于下列信息：乙方和/或维保方可以证明（通过出示书面记录）其在甲方透露之前已经知道，或者已经被乙方和/或维保方通过其他有合法权利泄露该信息的渠道（除了甲方）合法获得，或者现在或将来不因乙方和/或维保方过错泄露或使用甲方的机密信息而公开可以获得。

2、乙方如违反本条第 1 款的约定，应向甲方支付合同金额的百分之三十的违约金，如该等违约金不足以弥补因此而给甲方造成的损失，乙方还应对不足部分进行补偿。

3、本条项下保密义务在本合同期满或解除/终止后持续有效。

九、合同的生效、变更与终止

1、本合同经双方盖章后立即生效。如本合同在履行过程中有任何变更、补

5/12

合同编码: SMDZ202405001



充或修改，双方应另行签订书面协议。

2、本合同在双方的权利义务履行完毕后自动终止，也可因双方协商一致而提前终止。

3、本合同一式肆份，双方各执贰份，具有同等法律效力。

(以下无正文)

甲方：上海期货信息技术有限公司

盖章：

日期：2024.5.10



乙方：上海杉木电子科技有限公司

盖章：

日期：



合同编码: SMD2202405001



附件一：1.1 设备续保清单

序号	品名	品牌型号规格	数量	资产编号	序列号	维保到期时间	用途
1	交换机	H3C/S12504X-AF	1	0302Y2921	210235A1GFX19B00000C	2024/07/14	网络设备
2	交换机	H3C/S12504X-AF	1	0302Y2922	210235A1GFX19B00000P	2024/07/14	
3	交换机	H3C/S6800-54QF	1	0302Y2923	210235A2BBH19B001844	2024/07/14	
4	交换机	H3C/S6800-54QF	1	0302Y2924	210235A2BBH19B001909	2024/07/14	
5	交换机	H3C/S6800-54QF	1	0302Y2925	210235A2BBH19B002025	2024/07/14	
6	交换机	H3C/S6800-54QF	1	0302Y2926	210235A2BBH19B002065	2024/07/14	
7	交换机	H3C/S6800-54QF	1	0302Y2927	210235A2BBH19B002115	2024/07/14	
8	交换机	H3C/S6800-54QF	1	0302Y2928	210235A2BBH19B002251	2024/07/14	
9	交换机	H3C/5560X-54C-EI/	1	0302Y2929	210235A1XC919CQ00145	2024/07/14	
10	交换机	H3C/5560X-54C-EI/	1	0302Y2930	210235A1XC919CQ00170	2024/07/14	
11	防火墙	H3C/F5030/	1	0302Y2931	210235A1XXB19C000025	2024/07/14	安全设备
12	防火墙	H3C/F5030/	1	0302Y2932	210235A1XXB19C000002	2024/07/14	
13	服务器	H3C/UISC3010G3/	1	0302Y2933	210235A3M4H19C000162	2024/07/14	计算节点服务器
14	服务器	H3C/UISC3010G3/	1	0302Y2934	210235A3M4H19C000163	2024/07/14	
15	服务器	H3C/UISC3010G3/	1	0302Y2935	210235A3M4H19C000164	2024/07/14	
16	服务器	H3C/UISC3010G3/	1	0302Y2936	210235A3M4H19C000165	2024/07/14	
17	服务器	H3C/UISC3010G3/	1	0302Y2937	210235A3M4H19C000166	2024/07/14	
18	服务器	H3C/UISC3010G3/	1	0302Y2938	210235A3M4H19C000167	2024/07/14	
19	服务器	H3C/UISC3010G3/	1	0302Y2939	210235A3M4H19C000168	2024/07/14	

合同编码: SMDZ202405001



20	服务器	H3C/UISC3010G3/	1	0302Y2940	210235A3M4H19C000169	2024/07/14	
21	服务器	H3C/UISC3010G3/	1	0302Y2941	210235A3M4H19C000170	2024/07/14	
22	服务器	H3C/UISC3010G3/	1	0302Y2942	210235A3M4H19C000171	2024/07/14	
23	服务器	H3C/UISC3010G3/	1	0302Y2943	210235A3M4H19C000172	2024/07/14	
24	服务器	H3C/UISC3010G3/	1	0302Y2944	210235A3M4H19C000173	2024/07/14	
25	服务器	H3C/UISC3010G3/	1	0302Y2945	210235A3M4H19C000174	2024/07/14	
26	服务器	H3C/UISC3010G3/	1	0302Y2946	210235A3M4H19C000175	2024/07/14	
27	服务器	H3C/UISC3010G3/	1	0302Y2947	210235A3M4H19C000176	2024/07/14	
28	服务器	H3C/UISC3010G3/	1	0302Y2948	210235A3M4H19C000177	2024/07/14	
29	服务器	H3C/UISC3010G3/	1	0302Y2949	210235A3M4H19C000178	2024/07/14	
30	服务器	H3C/UISC3010G3/	1	0302Y2950	210235A3M4H19C000179	2024/07/14	
31	服务器	H3C/UISC3010G3/	1	0302Y2951	210235A3M4H19C000180	2024/07/14	
32	服务器	H3C/UISC3010G3/	1	0302Y2952	210235A3M4H19C000181	2024/07/14	
33	服务器	H3C/UISC3010G3/	1	0302Y2953	210235A3M4H19C000157	2024/07/14	SDN 控制器服务器
34	服务器	H3C/UISC3010G3/	1	0302Y2954	210235A3M4H19C000158	2024/07/14	
35	服务器	H3C/UISC3010G3/	1	0302Y2955	210235A3M4H19C000159	2024/07/14	
36	服务器	H3C/UISC3030G3/	1	0302Y2956	210235A3M5H19C000033	2024/07/14	分布式存储服务器
37	服务器	H3C/UISC3030G3/	1	0302Y2957	210235A3M5H19C000034	2024/07/14	
38	服务器	H3C/UISC3030G3/	1	0302Y2958	210235A3M5H19C000035	2024/07/14	
39	服务器	H3C/UISC3030G3/	1	0302Y2959	210235A3M5H19C000036	2024/07/14	
合计		39					

合同编号: SMDZ202405001



序号	品名	品牌型号规格	数量	资产编号	序列号	维保到期时间	用途
1	交换机	H3C/S5560X-54C-EI	1	0302Y3208	210235A1XC9204Q0002L	2024/10/29	网络设备
合计		1					

1.2: 设备续保价格明细

序号	名称	数量	未税单价	单价(含税)	小计(含税)	税率
1	交换机 H3C/S12504X-AF	1				
2	交换机 H3C/S12504X-AF	1				
3	交换机 H3C/S6800-54QF	1				
4	交换机 H3C/S6800-54QF	1				
5	交换机 H3C/S6800-54QF	1				
6	交换机 H3C/S6800-54QF	1				
7	交换机 H3C/S6800-54QF	1				
8	交换机 H3C/S6800-54QF	1				
9	交换机 H3C/5560X-54C-EI/	1				
10	交换机 H3C/5560X-54C-EI/	1				
11	防火墙 H3C/F5030/	1				
12	防火墙 H3C/F5030/	1				
13	服务器 H3C/UISC3010G3/	1				
14	服务器 H3C/UISC3010G3/	1				
15	服务器 H3C/UISC3010G3/	1				
16	服务器 H3C/UISC3010G3/	1				
17	服务器 H3C/UISC3010G3/	1				
18	服务器 H3C/UISC3010G3/	1				
19	服务器 H3C/UISC3010G3/	1				
20	服务器 H3C/UISC3010G3/	1				
21	服务器 H3C/UISC3010G3/	1				
22	服务器 H3C/UISC3010G3/	1				
23	服务器 H3C/UISC3010G3/	1				
24	服务器 H3C/UISC3010G3/	1				
25	服务器 H3C/UISC3010G3/	1				

合同编号: SMDZ202405001



26	服务器 H3C/UIISC3010G3/	1		
27	服务器 H3C/UIISC3010G3/	1		
28	服务器 H3C/UIISC3010G3/	1		
29	服务器 H3C/UIISC3010G3/	1		
30	服务器 H3C/UIISC3010G3/	1		
31	服务器 H3C/UIISC3010G3/	1		
32	服务器 H3C/UIISC3010G3/	1		
33	服务器 H3C/UIISC3010G3/	1		
34	服务器 H3C/UIISC3010G3/	1		
35	服务器 H3C/UIISC3010G3/	1		
36	服务器 H3C/UIISC3030G3/	1		
37	服务器 H3C/UIISC3030G3/	1		
38	服务器 H3C/UIISC3030G3/	1		
39	服务器 H3C/UIISC3030G3/	1		
40	交换机 H3C/S5560X-54C-EI	1		
合计含税总价: 228500			小写: 228500.00	
			大写: 贰拾贰万捌仟伍佰元整	

合同编号: SMDZ202405001



附件二：维保服务级别和服务内容

一、原厂承诺维保服务级别

产品类型	服务级别
服务器	基础系统支持 7x24 全天候服务、 缺陷介质保留 DMR 服务（硬盘不返还）
网络设备	7X24X4 备件到达
安全设备	7X24X4 备件到达

二、维保服务内容：（设备共计 40 台）

云计算平台（一期）项目相关设备 39 台，云计算平台（二期）项目相关设备 1 台。

原厂需承诺提供的维保服务及技术支持范围需包含以下内容：

- （1）解答最终用户提出的问题。如出现紧急技术问题，当最终用户提出服务请求后，在 1 小时内以电话、邮件形式做出响应，本地 2 小时内赶到现场（如需要），异地 12 小时内赶到现场（如需要），12 小时内提出解决方案，并持续与最终用户沟通，直至解决问题。
- （2）服务方式：现场服务（地址：金皖路 458 号联通三期），不限次的电话、电子邮件等。
- （3）相关产品和组件等的升级服务，包括：原厂具有知识产权的产品、组件等升级，对任何相关升级将及时通知最终用户。
- （4）无论维保期内外，乙方和原厂须对任何被确认的产品缺陷进行免费修复，确保所有设备的安全可靠。如因产品本身漏洞或缺陷给最终用户造成任何损失，由乙方负责赔偿损失及其他连带责任。
- （5）事后分析报告：在每一次故障排除之后，原厂都须做详细的记载，对每一次故障均做出详细故障原因分析报告，并以此为最终用户提供维护资料和数据，及时给出适当的建议。对未完全解决的问题，服务工程师须至少每周与最终用户方的工程师联系，跟踪问题，分析协商处理方案，直至问题解决。
- （6）原厂定期（每季度至少一次，重大会议等时点需单独进行）对所有设备进行技术巡检，听取最终用户意见，做好预防性工作，并提供现场巡检报告，内容包含系统性能分析、调优建议等。
- （7）免费提供系统优化服务。
- （8）各服务负责人如变更需及时通知最终用户。

合同编号: SMDZ202405001



附件:

保密协议

甲方: 上海期货信息技术有限公司

乙方: 上海杉木电子科技有限公司

根据中华人民共和国有关法律、法规的规定, 为保证____技术公司金融科技研究中心 2024 年度云计算平台基础设施续保服务采购项目__项目的顺利开展, 甲、乙方就双方在业务合作过程中的保密信息事宜达成协议如下:

一、保密信息

1、本协议中的“保密信息”包括以下内容:

(1) 甲方及其股东未经批准公开的重大事项和重要会议内容, 如发展规划、市场调研措施等;

(2) 双方合作过程中, 甲方向乙方(包括乙方工作人员, 下同)披露、或乙方接触到的、或由乙方在合作期间开发的, 所有关于甲方及任何与甲方有关的组织程序、管理程序、市场营销、发展战略、业务伙伴、客户名单等任何商业信息;

(3) 与甲方及其股东财务状况有关的信息, 经审计的或未经审计的帐册、财务记录、文件或其他任何形式的记录, 及其他所有反映甲方财务状况的记录;

(4) 甲方及其股东、客户的应用系统在方案调研、开发阶段中涉及的方案设计细节、程序文件、数据结构, 以及相关业务系统的硬软件、文档、测试和测试产生的数据等;

(5) 甲方及其股东、客户的内部规章制度和有关政策与程序, 内部办公与信息网上非市场公开信息;

(6) 甲方及其股东、客户的数据库资料;

(7) 甲方及其股东的任何形式(包括电子形式)的技术信息, 或者任何形式(包括电子形式)的与技术方法、程序、公式、编排、系统、技术手段、发明创造、机器设备、电脑程序、软件、编码、研究项目有关的各种信息;

合同编号: SMDZ202405001



(8) 甲方从第三方（包括但不限于甲方会员公司、客户）所获得的第三方要求甲方承担保密责任的各类信息；

(9) 甲方披露相关信息时口头或者以任何方式声明该信息应保密的信息；

(10) 一般公众当时不能获得相关信息，以及乙方在特定情况下应合理认为应保密信息。

2、以上保密信息的提供方式包括但不限于：书面形式、电子数据形式、将载有保密信息的物质载体交付给对方、对存储于数据库中的保密信息由甲方向乙方传授开启及存储保密信息的方法、口头说明或以视听方式向乙方展示。

二、保密信息的使用

1、乙方在使用“保密信息”时应履行以下义务：

(1) 保密信息仅可在本合同有效期内用于完成本合同项下的任务，除此之外，乙方不得出于任何目的、通过任何途径使用保密信息。非经甲方书面同意，乙方不得将保密信息透露或复制给任何第三方；

(2) 非经甲方书面同意，乙方不得就本项目的任何相关部分在任何媒体上出版、发表声明、发布任何文件或其他书面或印刷资料；

(3) 妥善保存保密信息载体，应以谨慎态度避免泄漏、公开或传播甲方的保密信息。

(4) 在开发过程中对数据的处理方式应事先得到甲方的许可；

(5) 未经甲方书面许可，不得对有关保密信息进行修改、补充、复制；

(6) 未经甲方书面许可，不得将保密信息以任何方式（如 E-mail）携带出甲方场所；

(7) 乙方保证，保密信息只披露给为管理、执行、或履行本项目而有必要得到该信息的员工，且该员工不会以任何理由、任何方式向任何第三方披露该信息。一旦发生乙方及其员工向任何第三方披露该信息的，由此引发的任何法律责任和甲方损失（包括但不限于：诉讼费、仲裁费、律师费和甲方遭受的任何损失，下同）由乙方承担；

(8) 在保密信息的个别部分或个别要素已被公开，但尚未使保密信息的其他部分或整体成为公开知识，保密信息没有丧失价值的情况下，乙方应承担仍属秘密信息部分的

合同编码: SMDZ202405001



作项目。乙方应向甲方支付合同总额（如无合同总额，则指合同实际已发生的总费用）30%的违约金。如上述违约金不足以弥补乙方给甲方造成的经济、信誉及其他损失，还应赔偿甲方超出违约金部分的损失。

4、乙方未经甲方许可或授权，因过失、故意等其他任何理由将保密信息透露给第三人，应承担违约责任的同时，告知知悉保密信息的第三人负有保密义务，并承担因第三人原因所引起全部责任。

六、保密期限

乙方应当在双方项目合作期间负有上述信息的保密义务。一般情况下，项目结束后六年内，乙方仍然负有保密义务；重大及特殊情况下，根据国家相关法律法规的规定以及具体项目信息的性质需要，如果需要长期保持秘密状态的，乙方在项目合作结束后对此类信息亦负有保密义务。

本协议是为防止甲方的保密信息在协议有效期发生泄漏而制定。因任何理由而导致甲、乙双方的合作项目终止时，乙方应归还甲方所有有关信息资料 and 文件，但并不免除乙方的保密义务。

七、协议文本及效力

1、本协议是合同的一部分，具有同等效力。

2、本协议自甲、乙双方盖章之日起生效，一式【肆】份，由甲方执【贰】份、乙方执【贰】份，各份协议具有同等法律效力。

甲方：上海期货信息技术有限公司

乙方：上海杉木电子科技有限公司

盖章：

盖章：

日期：2024年5月10日

日期： 年 月 日

16.5. 北京华通安和科技



合同编号：_____

新华三产品调试服务采购合同

甲方：北京华通安和科技有限公司

地址：北京市海淀区北清路81号院四区1号楼15层1501A

联系人：孙鹤

电话：010-62603865

传真：010-62603865

乙方：上海杉木电子科技有限公司

地址：上海市徐汇区宜山路333号汇鑫国际1204室

联系人：张仁宝

电话：13916845537

传真：021-66287672

根据《中华人民共和国民法典》及相关法律之规定，就甲方购买乙方（或第三方）提供的硬件或软件（以下简称“产品”）维护服务之事宜，双方经友好协商，达成如下一致：

第一条 维护服务产品范围

甲方需要乙方提供维护服务的产品清单详见本合同附件。

第二条 服务内容及方式

主要的服务内容及方式应列明在本条（具体详见本合同附件）。

第三条 服务品质保证

乙方保证甲方所购买之服务为原厂服务（原厂授权证书作为附件）或达到原厂标准之服务。若甲方发现购买之服务为非原厂服务或未达到原厂标准之服务，则乙方必须退还已收取的全部服务费，并承担由此给甲方造成的全部损失。

第四条 违约责任

1. 乙方应提供符合本协议约定和行业通行的专业化服务，如果达不到甲方和最终用户的



要求，乙方应立即更换人员或改进方法，直至达到甲方和最终用户满意。如因服务错误、失误或不尽职导致设备、软件系统出现故障，甲方有权直接解除合同，乙方除应承担全部责任外，还应退还全部服务费。

2. 乙方如果未按本协议规定的服务内容和方式进行响应并解决问题，则甲方可以采取必要的补救措施，由此产生的风险和费用将由乙方承担。同时，甲方有权决定是否继续履行合同。如果甲方解除合同，则乙方应退还全部服务费并承担由此而给甲方造成的损失。

3. 如甲方迟于合同规定时间付款，自超过付款期限之日起，每天甲方应付给乙方未付款金额万分之一的违约金，违约金总计不超过合同总金额的 5%。

第五条 保密条款

1. 双方对合作及本合同的具体内容负有保密责任。未经对方事先书面同意，任何一方不得将双方的合作及本合同中涉及的商业秘密披露给任何第三方。

本条所指的商业秘密是指以各种有形或无形形式存贮的观点、计划和信息，包括但不限于：技术或商业性质的信息、标语口号、版权物品、计算机软件、源代码、目标代码、技术、技术诀窍、数据、营销企划、摘要、报告及邮件列表等。

2. 本合同如有任何部分被视为无效或不可执行，均不影响保密条款的有效性。

3. 本条规定在本合同终止后两年内仍然有效。

第六条 不可抗力

1. “不可抗力”是指所有超出本合同双方控制范围的事件，该事件应不可预见，或虽然可以预见，但通过合理努力无法阻止或避免其发生，且这类事件发生于本合同签字之后，并且阻止任何一方全部或部分履行本合同。

2. 由于不可抗力事件，致使任何一方不能履行其在本合同下的义务，该方不承担由此给另一方造成的损失；该方应及时通知另一方其不能履行或延迟履行合同义务的原因，并应尽快向另一方提供有关发生不可抗力的证明文件，按事故对本合同的影响程度，双方协商是否终止本合同，或部分免除本合同的义务。

第七条 合同的变更与转让

1. 甲乙双方除非事先得到对方的书面同意或本合同另有规定，任何一方不得将本合同项下的任何权利、义务、责任转让给任何第三方。

2. 未经双方同意，任何一方不得单方面修改本合同，如需变更，由甲乙双方协商一致后签订补充合同予以确认，补充合同与本合同具有同等法律效力。

第八条 争议的解决



1. 因执行本合同所发生的或与本合同有关的一切争议，双方应通过友好协商方式解决。
如双方通过协商不能达成合意时，由原告所在地的法院管辖。
2. 在争议的处理过程中，除正在进行诉讼的部分外，合同的其他部分将继续执行。

第九条 适用法律

本合同的有效性、解释、执行及履行和争议解决应适用中华人民共和国的法律法规。

第十条 其他规定

1. 本合同自双方签字盖章之日起生效。
2. 本合同一式贰份，双方各执壹份。
3. 本合同附件为本合同的组成部分，与本合同具有同等法律效力。

甲 方：北京华通安和科技有限公司
地 址：北京市海淀区北清路81号院四区1号楼15层1501A
税号：91110108MA04EBAU6P
开户行：中国建设银行股份有限公司北京清华园支行
账号：11050163560000002730
电话：010-62603713
盖章：
签署日期：



乙方：上海杉木电子科技有限公司
地址：上海市奉贤区红陆路1号-39
税号：91310120703380388R
开户行：平安银行上海西南支行
账号：11006523950201
电话：021-66288311
盖章：
签署日期：





附件

第一条 维护产品名称、版本、规格、型号、数量、服务价格（维护产品清单）

序号	服务名称	描述	数量	单位	单价（元）	合计（元）
1	集群安装与部署	集群硬件安装（包含计算节点、网络设备等）及系统环境部署服务_1-148 节点	148	节点		
2	GPU 优化服务	为整个精简 GPU 驱动代码、减少 GPU 驱动程序、提高 GPU 驱动程序并发度等	148	节点		
3	软件系统定制开发服务	节点资源管理优化、集群管理软件调优服务	1	套		
4	特定软件安装服务	部署、安装调试最终用户指定软件系统	148	套		
合计（6%）大写：叁佰陆拾伍万柒仟元整						¥3,657,000.00

第二条 维护服务期限和地点

- 1.本合同服务履行期限为5个月，自2023年6月30日起至2023年12月1日止。
- 2.乙方提供服务，驻场地点为履行地点。
- 2.履行地点为 上海市浦东新区两港大道999号

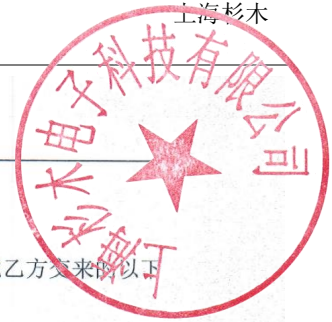
第四条 合同价款及支付

1. 合同价款：¥3,657,000.00 元（人民币大写：叁佰陆拾伍万柒仟元整），其中不含税金额¥3,450,000.00 元（人民币大写：叁佰肆拾伍万元），税率 6%，税额¥ 207,000.00 元（人民币大写：贰拾万零柒仟元）。合同总价是固定的，在服务期限内，乙方为提供本项服务的全部成本费用均包含其中，甲方不再增加任何费用。

注：以上税率按照国家现行有效的税法为准执行，若国家税法规定税率有变化，税额及合同总价将进行相应调整。如开具增值税发票时税金存在尾差，发票金额与本合同所列税额有差异的，以合同金额为准。

- 2.甲乙双方同意按照如下（1）方式进行款项结算：

（1）一次性付款：项目验收合格，甲方向乙方支付合同全部款项。



(2) 分期付款：（可以选择 A 按月付款 B 按季付款 C 按年付款）。

3. 乙方申请付款前，应提前 10 个工作日向甲方提供如下文件，甲方凭乙方交来的以下文件向乙方支付合同款：

- (1) 乙方开出的付款申请书；
- (2) 相应付款金额的服务费发票。

4. 乙方账户信息

户名：上海杉木电子科技有限公司

开户行：平安银行上海西南支行

账号：11006523950201





17. 正在进行项目和用户好评

17.1. 用户好评及表彰信

转发

删除

打印预览

待办事项

企业微信

全文yangxianbo

抄送: 吴昊_Hao <hao.wu@enflame-tech.com>; 林文刚_David <david.lin@enflame-tech.com>; yangxianbo (CHN-集团代表处) <yangxianbo@h3c.com>; wangsijun (上海代表处服务部, CHN-集团代表处) <wangsijun@h3c.com>
主题: 回复: 感谢信-感谢新华三 & 上海杉木

[EXTERNAL EMAIL]
Great work !!

Hi如远、敬缙、欣欣总、张总,
感谢华三和杉木的团队, 为宜昌DJ项目所做的大力支持。我们整个DJ项目组的内部成员都看在眼里!

希望我们在即将到来的24年里, 一起继续共创佳话。

Best Regards,
余雷 Leo YU
MP#: +86 18917562406

发件人: 何进科 Jinke <jinke.he@enflame-tech.com>
发送时间: 2023年12月28日 16:39
收件人: 徐如远 <xry_uan@sh-shanmu.com>; Fengjingmin <feng.jingmin@h3c.com>
抄送: 吴昊_Hao <hao.wu@enflame-tech.com>; 余雷_Lao <leo.yu@enflame-tech.com>; 林文刚_David <david.lin@enflame-tech.com>; yangxianbo@h3c.com; Wangxinbin <wang.xinbin@h3c.com>; wangsijun@h3c.com; renbaoz@sh-shanmu.com
主题: 感谢信

感谢信

致上海杉木电子科技有限公司、新华三上海办:
DJ人工智能算力中心项目自开工以来, 在双方公司的高度重视及现场项目部全体人员共同努力下, 保质保量地完成了业主方的节点目标, 赢得了业主及相关领导的认可。
在施工的关键时期, 面对施工条件复杂、工期紧张、周边环境复杂等诸多不利因素, 积极协调公司各方、解决技术难题、积极组织相关资源。整个项目组迎难而上、发挥攻坚克难的精神, 成功完成了各节点计划。
在此, 燧原科技DJ项目部对上海杉木现场项目管理团队徐如远、陶勇等表示由衷的感谢, 也特别感谢新华三上海办冯敬缙等相关领导、人员的大力支持和有力协调, 希望贵司一如既往的大力支持本项目的后期事宜。
祝贵司事业蒸蒸日上!

转发

删除

打印预览

待办事项

企业微信

搜索邮件

尊敬的 [上海杉木电子科技有限公司] 领导及同事们:

您好!

值此 [中星铂尔曼酒店年度维保] 项目维保服务周期圆满结束之际, 我谨代表 [我方上海中星城际置业有限公司] 向贵公司全体维保团队成员致以最诚挚的感谢和崇高的敬意!

在自 [2023年-11月] 至今的整个维保期内, 贵公司团队展现出了极高的专业素养和负责精神。面对项目中出现的各种技术挑战和突发状况, 贵方工程师总能响应迅速、判断精准、处理高效, 最大限度地保障了系统的稳定运行, 确保了我们的业务连续性。

尤其令我们印象深刻的是, 贵方团队不仅出色完成了合同约定的维保任务, 还主动为我们提供了许多增值服务和宝贵的优化建议, 这种“想客户之所想, 急客户之所急”的服务理念, 让我们深感选择了贵公司是无比正确的决定。

贵公司团队所体现出的严谨的工作作风、卓越的技术能力和以客户为中心的服务精神, 是我们学习的榜样, 也为我们双方未来的长期合作奠定了坚实的基础。

再次对贵公司的鼎力支持与辛勤付出表示衷心感谢! 期待在未来能与贵公司继续携手, 共创辉煌!

顺祝商祺!

Kevin



Kevin Yan 颜云峰
IT Solutions Manager信息技术支持经理
Finance Department财务部

PULLMAN SHANGHAI XUHUI
上海中星铂尔曼大酒店
Address: 1 Pubei Road, Xuhui District
Shanghai 200235, China
地址: 上海市徐汇区浦北路1号
邮编: 200235
T.电话: +86 (21) 24 26 88 88 M.手机: +86 (0)139 0169 1019
F.传真: +86 (21) 24 26 89 99
Kevin.Yan@ACCOR.COM
PULLMANHOTELS.COM - ACCORHOTELS.COM

www.pullmanhotels.com | www.accorhotels.com





17.2. 正在承接项目汇总表

项目序号	1	2	3
项目名称	铂尔曼酒店技术服务维保服务项目	B站接入交换机服务采购合同	B站常熟核心交换机24年Q2服务项目
项目所在地	上海	上海	常熟
项目采购人名称	上海中星城置业有限公司	上海哔哩哔哩科技有限公司	上海哔哩哔哩科技有限公司
项目采购人地址	上海	上海	上海
项目采购人电话	15692101890	15221235273	15221235273
合同价格	214000.00	93659.00	151433.00
开始日期	2023-9-1	2024-6-1	2024-4-23
完成日期	2025-8-31	2026-12-31	2025-4-22
项目负责人	方芳	刘小芳	刘小芳
技术负责人	周海波	伍明凯	伍明凯
项目描述	7*24*4技术支持服务	7*24全天候服务	7*24*4技术支持服务
备注(用户反映)			

备注：各单位可根据各自的项目数量，调整表单的列数。

响应方授权代表签字：朱千弛

(加盖企业公章)

日 期：2025 9 月 8 日

17.3. 上海中星城置业



中星城际置业有限公司 终端设备及网络维护协议

2023-08



甲方：上海中星城际置业有限公司

地址：上海市徐汇区浦北路1号

联系人：颜云峰

电话：021-24268888-61018

乙方：上海杉木电子科技有限公司

地址：上海市中山南二路999弄19号5A

联系人：张仁宝

电话：021-66288337

特别说明：上海中星城际置业有限公司下设分公司“上海中星城际置业有限公司中星大酒店”，经营上海市徐汇区浦北路1号的“上海中星城际置业有限公司中星大酒店”。基于国家和地方财税制度的要求，对于酒店对外业务开展，由上海中星城际置业有限公司签署相关合同（以下简称“甲方”）。

双方经友好协商，就乙方对甲方公司内部网络核心主机、终端设备及其网络提供有偿维护一事达成协议，并共同遵守本协议涉及的全部内容。

一、服务内容

1. 维护人员安排：

- 1) 乙方指派专人为甲方提供网络及硬件服务。（类别见附表）
- 2) 指定主要维护人员名单：宋琦，张金琪
- 3) 乙方如更换工程师，需提前30日书面告知甲方；
- 4) 项目负责人：张仁宝
- 5) 如上述人员有变动，需甲、乙双方协商解决

2. 维护时间：

自2023年09月01日至2025年08月31日止，为期24个月。

3. 维护范围：

- 1) 乙方为甲方提供网络设备维护服务及附件中所列的硬件维保,甲方不承担维保期间任何硬件维修费用。以下出现情况为甲方出资维修：由于酒店内部电压不稳导致设备硬件损坏、由于外界不可抗力力量如：地震、海啸等自然灾害及甲



方人为所致设备损坏。

- 2) 甲方终端的综合布线类维护工作，不在本协议约定的服务范围内。
 - 3) 乙方对所维护网络设备进行故障排查、软件升级。
 - 4) 乙方根据甲方的需求提供相应技术解决方案、软硬件排查服务。
 - 5) 乙方每一年度根据甲方要求免费提供 5000 元等值网络交换机设备，合同期内合计 10000 元。
 - 6) 未尽事宜甲乙双方协商。
4. 技术支持：
- 1) 对于甲方内部网络构架提供整改或优化方案；
 - 2) 通过日常问题，在经过调研后，为甲方提供用于优化解决方案，该方案经甲方认可后，由乙方负责实施。
5. 维护流程：
- 1) 乙方为甲方提供技术支持服务；
 - 2) 当被维护设备发生大规模故障时或甲乙双方共同认定，需要更多技术工程师协助完成工作时，由乙方调配其他工程师参与维护工作；
 - 3) 当被维护范围内的设备出现硬件故障时，乙方工程师必须在接到甲方报修电话后 4 小时到达现场并负责排查故障点并填写《故障报告单》，并在接到甲方报修电话 6 小时内提供甲方所需更换的硬件设备(或相同功能的硬件设备作为临时替代)，乙方技术人员负责调试安装（每天 20:00 至 04:00 发生的硬件故障，硬件更换必须在上午 10:00 前完成）；
 - 4) 本协议中未涉及的维护规范，乙方按以甲、乙双方协商认可的约定标准及时间执行。

二、甲方的权利义务

1. 甲方有权要求乙方工程师按照甲方要求为维护范围内的网络设备设置管理员密码、登录账户、登录密码；
2. 所有与被维护范围内设备相关的密码由甲方统一保管，并可由甲方相关负责人自行更改；
3. 甲方有权要求乙方工程师不得查阅甲方相关业务文件、财务文件及其它甲方认为敏感的任何文件；



4. 当维护范围内设备发生故障需维护时，甲方有义务向乙方工程师提供正确的用户名及密码；
5. 甲方有权要求乙方工程师不得记录相关密码；
6. 甲方承担维护期间新增以及更换软硬件的费用；
7. 甲方有权要求乙方工程师按照甲方的要求时间安排工作；
8. 甲方有权要求乙方技术负责人或行政负责人每月 3-5 号间（若遇国家法定节假日，则该日期顺延）与甲方指定负责人就维护工作中涉及的相关事宜进行直接沟通，以保证维护工作顺利进行。若因其它原因，无法在约定的时间段内进行沟通工作，则本次沟通工作转为邮件形式执行；
9. 在乙方工程师对维护范围内设备进行维护工作时，甲方有义务指派专人进行配合；

三、乙方的权利义务

1. 乙方保证具有签订与履行本合同的权利能力与行为能力，保证提供的服务合法且不侵犯任何第三方合法权益。
2. 乙方工程师不得擅自查阅甲方相关业务、财务文件以及其它甲方认为敏感的文件；
3. 乙方工程师不得擅自记录维护范围内设备的所有密码；
4. 乙方在维护或排除故障时应保证电脑内数据的安全，不得出现因维护而导致的数据丢失、毁损情况；
5. 乙方工程师必须按照甲方的要求时间进行维护工作；
6. 乙方对维护工作中了解到的甲方数据等资料负有保密资料，未经甲方书面许可不得向协议之外的任何第三方泄露、提供、转让等；
7. 乙方工程师在工作中造成甲方财产设备损失的，应当照价赔偿。

四、合同费用

1. 维护协议金额：每一年度人民币壹拾万零柒仟佰元整（RMB107000.00 元），二年共计贰拾壹万肆仟元整（RMB214000.00 元）；
2. 此维护金额针对维护期内的附件所有网络设备；
3. 如甲方在维护期内，设备增加总量不超过 10% 时，乙方将在维护合同期内不再增加维护费用，超过 10% 时，甲、乙双方协商解决维护费用问题。



五、费用支付方式

1. 甲乙双方合同签订后，甲方应在 5 日内支付合同总金额的 50%，共计：人民币壹拾万零柒仟元整（RMB107000.00），2024.9.1 甲方再支付第二年度维护费用人民币壹拾万零柒仟元整（RMB107000.00），乙方应在收到每次款项后 3 个工作日内开出相应金额的增值税专用发票（含 6% 增值税）。
2. 付款方式：现金、支票或者银行汇款
3. 乙方同城汇款帐户信息：
公司名称：上海杉木电子科技有限公司
开户银行：平安银行西南支行
银行帐号：175536-11006523950201
上述汇款信息如有变更，乙方须于甲方付款前至少提前五个工作日书面通知甲方变更，否则因此导致的后果由乙方自行承担。

六、违约责任

1. 乙方如未如实履行本协议所约定的维护项目，所造成损失甲方有权要求乙方赔偿。
2. 双方如发生重大变故，需提前中止协议，必须提前 15 天，并且以书面形式通知并得到对方确认，在协议期内，若单方终止协议，须向另一方支付本合同服务费用总金额的 10% 作为违约金。
3. 若乙方违反本合同的保密条款，应赔偿甲方的一切损失，并支付给甲方相当于本合同全年费用金额的 20% 作为违约金。

七、双方特别约定

1. 如被维护设备中运行某专业软件或硬件，该软件或硬件不在乙方维护范围内，所涉及内容将以《特殊软、硬件列表》形式体现，须经双方签字盖章，并作为本协议附件之一，具有同等效力；
2. 本协议期满前 15 天，乙方会以书面形式（传真或 Email）通知甲方商讨续签事宜，次年的年度服务合同经甲乙双方协商，另行签署。
3. 甲方不得在本协议执行期间及本协议终止后一年内，私下雇佣、聘请（以及其它形式的协议）乙方工程师到甲方内部的相关部门从事专职或兼职网管（或其它类似的合作）。
4. 甲、乙双方协商认可的《IT 运维服务方案》，为乙方为甲方提供运维服务的准，



如乙方未能按照《运维服务方案》内的标准及时间标准执行，甲方有权解除本运维协议，并提前 15 日书面形式通知乙方，并要求退回剩余全部维护费用。

八、保密条款

- 1. 乙方按照甲方提供的内部人员权限表，严格控制甲方内部人员对于内部网络、设备等相关信息的获知权
- 2. 乙方内部对于甲方内部网络、设备等相关信息的获知权仅局限于乙方维护项目负责成员。
- 3. 双方承诺对履行本合同所提供的资料及其它商业秘密负有保密的义务，并采取一切合理的措施以使其所接受的资料免于散发、传播、披露、复制、滥用及被无关人员接触。此保密义务不因本合同的终止而解除。

九、不可抗力

如因不可抗力致使双方不能履行本合同中的部分或全部义务时，双方均不负违约责任。但不能履行义务一方应在合理的时间内，向对方报告所发生的不可抗力并提供有关部门的证明文件。本条所称“不可抗力”是指自然灾害、重大疫情、恶劣天气条件、政府行为、社会异常事件（包括罢工、政变、骚乱、游行等）或新颁布的法律、法规等不能预见、不能避免并不能克服的客观情况。

十、法律适用及争议解决

本合同的解释和执行适用中华人民共和国法律。甲、乙双方在履行本合同中出现的争议首先通过友好协商的方式解决。协商不成时，双方同意到本合同实际履行地人民法院诉讼解决。

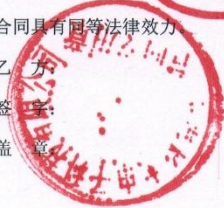
十一、其他

- 1. 本合同经甲、乙双方法定代表人或委托代理人签字并盖章后生效。
- 2. 本合同未尽事宜，双方签订补充协议，补充协议与本协议具有同等法律效力。本合同一式贰份，双方各执壹份，具有同等法律效力；
- 3. 协议附件作为本合同必要组成部分，与本合同具有同等法律效力。

甲方：
签字：
盖章：

乙方：
签字：
盖章：

签约日期：





附件

序号名称	规格	品牌	产地	单位	数量
一、客房网					
核心层					
1 以太网交换机主机	LS-7506E-S	H3C	中国	个	1
2 专用交换路由引擎	LSQM1SRPA0	H3C	中国	个	1
3 交流电源模块, 1400W	LSQM1AC1400	H3C	中国	个	2
4 48端口千兆以太网电接口模块 (PoE, RJ45)	LSQM1GV48SA0	H3C	中国	个	1
5 24端口千兆/百兆以太网光接口模块 (SFP, LC)	LSQM1GP24TSCO	H3C	中国	个	1
6 光模块-SFP-GE-多模模块-(850nm, 0. 55km, LC)	SFP-GE-SX-MM850-A	H3C	中国	个	32
7 主机-双交流电源 (4GE/2Slot)	NS-SecPath F1000-S-AC	H3C	中国	套	1
二、楼层交换机					
8 以太网交换机主机 (48GE+4SFP Combo)	LS-5120-48P-EI-H3	H3C	中国	台	10
9 以太网交换机主机 (24GE+4SFP Combo)	LS-5120-24P-EI-H3	H3C	中国	台	15
10 多模模块-(850nm, 0. 55km, LC)	SFP-GE-SX-MM850-A	H3C	中国	个	20
11 以太网交换机	LS-3100-8TP-PWR-EI-F-H3	H3C	中国	个	15
12 无线局域网AG双模单频可管理型接入点-FIT	EWP-WA2110-AG-FIT	H3C	中国	个	510
13 无线控制器license费用-管理32AP	LIS-WX-32	H3C	中国	个	15
14 H3C WX5004-4端口千兆Combo无线控制器	EWP-WX5004-H3	H3C	中国	个	1
15 150W 交流电源模块	LSKM2150A	H3C	中国	个	2
三、办公网络					
16 cisco核心三层交换机	WS-C3750G-12S-E	cisco	USA	个	2
17 cisco光接口模块	Cisco多模光纤模块	cisco	USA	个	14
18 cisco楼层交换机	WS-C2960-24TC-L	cisco	USA	个	10
19 cisco楼层交换机	WS-C2960S-24TS-S	cisco	USA	个	2
20 cisco光接口模块	Cisco多模光纤模块	cisco	USA	个	14
21 ciscoPOE供电交换机	WS-C2960POE	cisco	USA	台	2
22 Cisco AC控制器	Cisco 2504	Cisco	USA	台	1
23 Cisco AP	1142N-C-K9 AP	Cisco	USA	台	22
24 cisco楼层交换机	Cisco SF302-08	Cisco	USA	台	7
四、员工宿舍					
25 H3C WX3500-4端口千兆Combo无线控制器	EWP-WX3500-H1	H3C	中国	个	1
26 无线局域网AG双模单频可管理型接入点-FIT	EWP-WA2110-AG-FIT	H3C	中国	个	14
27 以太网交换机	LS-3100-8TP-PWR-EI-F-H3	H3C	中国	个	1
四、其他设备					
28 交换机	D-link 16	D-link	中国	个	3
29 光电收发器	D-link	D-link	中国	个	6
30 交换机	D-link 8	D-link	中国	个	1

以下无正文。



附件 1:

1、廉洁条款

乙方承诺，和甲方各级管理人员不存在利益关联。



附件 2: 廉洁协议

甲方：上海中星城际置业有限公司

乙方：上海杉木电子科技有限公司

为规范甲乙双方在经营活动中各项行为，保持廉洁自律的工作作风，防止各种不正当行为的发生，根据国家和上海市有关廉政建设的各项规定，特订立本协议如下：

一、甲乙双方应当自觉遵守国家和上海市有关廉政建设的各项规定。

二、甲方及其工作人员不得以任何形式向乙方索要和收受回扣等好处费。

三、甲方工作人员应当保持与乙方的正常业务交往，不得接受乙方的礼物礼金、有价证券和贵重物品等，不得在乙方报销任何应由个人支付的费用。

四、甲方工作人员不得参加可能对公正执行公务有影响的宴请、健身和娱乐等活动。

五、甲方工作人员不得要求或者接受乙方为其住房装修、婚丧嫁娶、配偶和子女的工作安排以及出国（境）等提供方便。

六、甲方负有管理职权的工作人员不得与乙方发生非正常的借款、委托理财等经济往来；不得介绍配偶、子女、其他特定关系人及其投资经营的企业与乙方发生经济和业务往来。

七、乙方应当通过正常途径开展相对业务工作，不得为获取某些不正当利益而向甲方工作人员赠送礼物礼金、有价证券和贵重物品等。

八、乙方不得为谋取私利擅自与甲方工作人员就项目承包费用结算等进行私下商谈或者达成默契。

九、乙方不得以洽谈业务、签订经济合同为借口，邀请甲方工作人员外出旅游和进入营业性高档娱乐场所。

十、乙方不得为甲方单位和个人购置或者提供通讯工具、交通工具、家电、高档办公用品等物品。

十一、乙方承诺，与甲方各级管理人员不存在利益关联。

十二、乙方如发现甲方工作人员有违反上述协议者，应向甲方领导或者甲方上级单位反映。甲方不得以任何借口对乙方进行报复。甲方对举报属实和严格遵守廉洁协议的乙方，在同等条件下给予承接后续项目的优先邀请投标权。

十三、甲方发现乙方有违反本协议或者采用不正当的手段行贿甲方工作人员，甲方根据具体情节和造成的后果追究乙方合同总价款 1-5% 的违约金。由此给甲方单位造成的损失均由乙方承担，乙方用不正当手段获取的非法所得由甲方单位予以追缴。

十四、本廉洁协议作为上海杉木电子科技有限公司经营合同的附件，与经营合同具有同等法律效力。经协议双方签署后立即生效。

十五、本协议一式贰份，甲、乙双方各执一份。

甲方单位：(盖章)

乙方单位：(盖章)

法定代表人：

法定代表人：

地址：

地址：

电话：

电话：

年 月 日

年

月 日

合同专用章



合同编号: BT2024-SY06110001

甲方合同编号:



甲方合同编号:

甲方: 上海哔哩哔哩科技有限公司 (以下简称“甲方”)
联系地址: 上海市杨浦区政立路485号国正中心3号楼

乙方: 上海杉木电子科技有限公司 (以下简称“乙方”)
联系地址: 上海市徐汇区宜山路333号1204室

甲、乙双方根据《中华人民共和国民法典》及相关的法律、行政法规之规定, 就甲方方向乙方采购指定产品事宜达成如下条款:

B站接入交换机维保

服务采购合同

2024年6月

甲方: 上海哔哩哔哩科技有限公司
乙方: 上海杉木电子科技有限公司

2024年6月

第 1 页 共 15 页

第一条 产品概况 (详情请见附件)

- 甲、乙双方约定, 甲方方向乙方采购设备维保服务, 服务期限自【2024】年【6】月【1】日起至【2026】年【12】月【31】日止, 乙方按约定向甲方提供服务, 具体服务内容及设备、服务范围、执行标准、质量检测等内容详见附件约定 (以下简称“服务”)。
- 甲、乙双方约定未经甲方书面同意, 乙方不得随意改变服务标准、内容、数量、价格、工艺、时间等, 如需变更产品已确定的内容、参数、数量、时间、地点等内容, 双方应协商达成一致以书面形式确认。

第二条 费用及付款方式

- 本合同产品总金额 (含税): (RMB) ¥ 93659.00 元; 大写: 玖万叁仟陆佰伍拾玖元整。
 - 上述金额表述两者不符时以中文金额为准 (下同)。
 - 上述金额已经包含服务包含的质量、维护、保修、更新升级、部件更换 (含部件费用) 等服务内容的费用, 除此外甲方无需向乙方或任何第三方支付额外费用。
- 甲、乙双方约定的具体付款方式如下:
 - 本合同生效后开始提供服务 (即维保服务期生效) 并经甲方验收合格后, 由甲方确认乙方提供【增值税专用发票】之日起30日甲方方向乙方支付尾款, 即(RMB) ¥ 21,141 元, 大写: 贰万壹仟壹佰肆拾壹元整 (以下简称“首付款”)。
 - 乙方于2025年开始提供服务并经甲方确认后 (即2025年维保服务期生效), 自甲方确认乙方提供【增值税专用发票】之日起30日甲方方向乙方支付进度款, 即(RMB) ¥ 36,259 元, 大写: 叁万陆仟贰佰伍拾玖元整 (以下简称“进度款1”)。
 - 乙方于2026年开始提供服务并经甲方确认后 (即2026年维保服务期生效), 自甲方确认乙方提供【增值税专用发票】之日起30日甲方方向乙方支付进度款, 即(RMB) ¥ 36,259 元, 大写: 叁万陆仟贰佰伍拾玖元整 (以下简称“进度款2”)。

第 2 页 共 15 页



甲方合同编号:

乙方未按时出具合格的【增值税专用发票（13%）】或未履行甲方支付费用的前置条件时，甲方有权顺延支付费用。

3. 甲方应承担乙方缴纳的税费：

甲方与收款账户信息如下：

开户行	平安银行上海西南支行
开户人	上海杉木电子科技有限公司
账号	175306-1100652359201
甲方开票信息如下：	
名称	上海野哩哩科技有限公司
纳税人识别号	91310000MA1G8BAXD
地址	上海市杨浦区四平路1945号1641室 021-25099255
开户银行及账号	招商银行股份有限公司上海虹口体育场支行 12193952410103

➤ 甲乙双方约定若乙方变更收款银行账户信息时，应当及时书面通知甲方，因乙方未及时书面通知甲方所产生的所有责任、后果或额外费用，均由乙方自行承担。

第三条 产品交付

1. 维保服务供货方式：原厂上门提供维护和检修。
2. 维保服务提供地点：甲方设备所在地
3. 维保服务期：2024年06月1日起至2026年12月31日止。
4. 甲方维保联系人信息：朱俊宏 17701749253
5. 如甲方或乙方需要变更上述信息的，需在产品交付前提前叁个工作日书面通知乙方。

第四条 服务质量及保修维护

1. 乙方保证具备向甲方提供本合同服务的资质和能力，以原厂标准向甲方提供服务，服务应符合中华人民共和国法律、法规及国家和地方有关服务的质量标准规范以及合同和附件的约定。
2. 乙方提供的服务符合本合同和附件约定、服务说明书及该服务所有技术文件中关于功能、性能、品质及质量的描述，甲方以任何形式确认服务验收合格，并不表明甲方对服务质量的完全认可，乙方对服务承担质量瑕疵担保责任。
3. 乙方承诺在维保服务服务期内，在接到甲方的报修或维护通知之日起24小时内赶到现场为甲方提供保修或维护服务(如附件有具体约定，则以附件的约定为准)。乙方的保修或维护服务联系人：H3C

第 3 页 共 15 页

甲方合同编号:

原厂官方，联系电话为：4008100504

4. 服务维保期限届满后，乙方应继续为甲方提供相应的保修服务，根据具体服务内容甲方应向乙方支付合理的维修服务费用，乙方根据服务内容应事先告知甲方费用标准。
5. 乙方保证若维保服务造成人身、财产等损害，由此产生的责任应由乙方承担。

第五条 权利义务

1. 甲方、乙方均保证具有洽谈、签订、履行本合同的主体资格及相关所需资质，并已获得了洽谈、签订、履行本合同的完全有效且不可撤销的所有授权、同意、批准或许可，且任何一方洽谈、签订、履行本合同的行为将不会违反任何在先义务。
2. 乙方应及时向甲方提供乙方加盖公章具备合法经营资质的证明文件及合法销售产品和提供产品服务的资质文件，甲方不因对乙方提供的任何承诺及保证的审查行为而承担任何责任。
3. 甲、乙双方约定本合同项下乙方交付的全部产品自交付之日起所有权属于甲方，乙方不得在全球范围内申请、注册、登记任何与甲方相同或相近似的商标、专利和著作权等。
4. 甲、乙双方在其自身宣传材料、名片、市场宣传、网站建设以及其他任何方面使用对方的名称、商标、字号、域名和网站等信息，都必须事先通知对方，并获得对方的书面许可后方可进行；
5. 除履行本合同所需外，未经对方书面许可，任何一方不得擅自使用、复制对方的商标、标识、版权作品、商业信息、技术及其他资料等，在履行本合同期间，甲、乙双方在使用对方的企业名称、商标、商号、品牌、域名和网站时，应当完全单独为甲、乙双方在本合同中所约定的内容服务，不得夹带其他业务内容。
6. 甲、乙双方约定若乙方违反诚实信用原则或经营状况严重恶化，甲方认为乙方难以继续履行本合同时甲方可单方终止本合同，且不为甲方违约。

第六条 保密责任

甲、乙双方均保证对在洽谈本合同约定事项过程中以及签订、执行本合同过程中所获悉的属于对方的且无法自公开渠道获得的文件、资料及信息等予以保密，具体如下：

1. 接收保密信息的一方（“接收方”）应：
 - (1) 对保密信息严格保密；
 - (2) 不向任何第三方披露任何保密信息；
 - (3) 除为履行本合同之目的外，不为任何其他目的使用保密信息。
2. 保密信息的定义，“保密信息”指：

第 4 页 共 15 页



甲方合同编号:

(1) 有关本合同的存在和内容以及有关本合同预期交易的信息;

(2) 方(“披露方”)向接收方披露的全部专有、保密、非公知的技术信息和(或)商业信息,包括:

(a) 披露方在本合同签署前或之后披露给接收方或其雇员的任何研发设计、服务或产品;

(b) 营销要求和策略、产品计划及价格、客户名单、公司业务发展的方向、涉及经营管理的制度与流程等的商业信息;

(c) 通过签订和履行本合同而获得的对方及对方关联公司的任何信息;

和因履行本合同而获得的资料、软件、数据等信息数据内容;以及(d) 其它由披露方披露给接收方的且需向第三方承担保密义务的信息(不论该等信息是以书面、口头、图形、网络还是其他任何形式进行了披露)。

(3) “保密信息”不包括以下信息: (a) 披露方披露之前已为公众所知的信息; (b) 披露方后非因接收方的行为或过错而为公众所知的信息; 或 (c) 接收方从第三方处获得且并不因此使第三方违反其保密义务的信息。

3. 披露的同意。一方需要对外披露保密信息时应获得另一方的书面确认。

4. 保密期限。在披露方提供给接收方的保密信息被合法地公开之前,接收方应对相关保密信息永远予以保密。

5. 擅自披露的责任。如一方违反其在本合同项下的保密义务,该一方需承担违约责任(包括但不限于:为追究违约责任支出的律师费、仲裁费、鉴定费、鉴定费、文印费、审计费等)。

第七条 不可抗力

1. 本合同所称的不可抗力是指一切不可预见、不可避免并不能克服的客观情况,包括但不限于洪水、地震、飓风、火灾等自然灾害和战争、动乱等情况,以及政府对本合同订立时有效之相关法律、行政法规、政策等进行修订、变更、废止,或颁布新的法律、行政法规、政策以取代原有法律、行政法规、政策或原有法律、行政法规、政策处于废止状态,从而最终导致本合同无法继续履行。

2. 因不可抗力或者国家政策法规的变化而使本合同中任何一方或双方部分或全部不能履行本合同的,遭受不可抗力的一方无需向对方承担违约责任,但应及时通知对方不可抗力的发生情况并提交不可抗力力的合法证明材料。

3. 如不可抗力情况消失后,本合同仍有必要履行且具备继续履行的条件,双方应继续履行本合同;如因不可抗力导致本合同没有必要或无法继续履行的,则本合同任何一方均有权提出解除本合同,且双方互不承担违约责任。

第 5 页 共 15 页

甲方合同编号:

第八条 违约责任

1. 无论故意或过失,甲、乙双方未履行本合同约定义务或违反守事项均视为违约。任何一方违约,另一方有权要求违约方停止违约行为,自违约方告知停止违约行为之日起10日内,违约方不停止违约行为的,守约方有权单方解除本合同,解除本合同的通知到达违约方时本合同解除,解除本合同不影响守约方要求违约方承担违约责任(包括但不限于:为追究违约责任支出的律师费、诉讼费、鉴定费、鉴定费、文印费、审计费等)。具体提供担保服务的担保方、服务人员违约的,视为乙方违约。

2. 甲方无法正当理由故意未按约定期限向乙方付款时,每逾期一日,甲方须向乙方承担应付而未付款万分之一的滞纳金,逾期超过30日仍未付款的,乙方有权解除本合同,并要求甲方承担由此给乙方造成的全部损失。

3. 乙方保证取得经营并履行本合同项下内容的合法经营资质、授权资质等,保证有依法运营其服务,向甲方提供的服务不违反中国法律法规,不侵害任何第三人权益,且不存在任何侵害人身安全的隐患,若发生上述情况或乙方履行本合同过程中违反诚实信用原则,或未履行合同或本合同项下的任一承诺、保证义务时,乙方应向甲方承担全部赔偿责任(包括但不限于仲裁费、律师费、鉴定费、鉴定费、鉴定费、产品召回费用、罚款等)并向甲方赔偿本合同总金额叁倍的违约金。若甲方的全部损失超过前述违约金时,乙方应赔偿甲方的全部损失并按甲方要求的方式做出公开赔礼道歉。前述约定的违约金,均系双方在签订本合同时已经预见到的违约方违约行为将遭受的最低损失,发生违约情形时,守约方在约定的数据范围内主张违约金或损失赔偿金的,违约方放弃主张违约金过高的权利,守约方免于就实际损失举证,但守约方主张违约金违约方的违约行为遭受的实际损失大于本合同约定的数额的,守约方应当举证证明其实际发生的损失。

4. 由于乙方提供的服务无法通过甲方的验收或无法满足合同目的导致甲方对乙方做出乙方不具备提供本合同所需能力的判断,或乙方若单方实质性违约或不能充分履行义务,并在甲方告知后未能进行补救或不能在甲方要求的期限前提供符合要求的增值服务费;或由于乙方的行为甲方认定乙方不能胜任本合同履行的,或虽然甲方出于情势所迫不得不使用乙方提供的带有瑕疵的服务开展业务,但甲方仍由决定追究乙方相关责任的,则甲方在法律允许的前提下有权作出以下一项或多项决定:

甲方有权要求无条件解除/终止本合同,并不再支付任何费用。

甲方有权要求乙方返还已付全部款项。

甲方有权不再支付任何费用。

甲方有权要求乙方甲方承担本合同总金额的30%作为违约金,并视甲方因此遭受的损失承担赔偿责任。甲方要求乙方承担的损害赔偿的范围包括甲方所受的直接损失和间接损失。

5. 因本合同的履行产生的乙方应承担的违约金、赔偿金等,甲方有权从未付款项中预先扣除,不足部分乙方应当补齐。

第 6 页 共 15 页



甲方合同编号:

第十条 禁止转让

乙方在履行合同过程中，不得以任意理由将本合同相应权利或义务转让、出借、委托、许可、授权等以其他形式转让给第三方，同时，不得以本合同中权利对外设立质权及其他担保物权，也不得作其他任何形式的处分但本合同另有约定的除外。

第十条 通知与送达

双方之间的任何重要通知或书面函件，必须以中文写成，以电子邮件、专人送达（包括特快专递）或挂号信函之形式发送，除非事先以书面通知更改，则双方的沟通工具如下：

双方	合作联系人	电子邮件必要联系人	电子邮箱	手机电话
甲方	张展阳	/	zhangchenyang@11b11.com	18724639879
	/	朱俊宏	zhujuhong@11b11.com	17701749253
乙方	刘小芳	/	lxf@sh-shamu.com	15221235273
	/			

1. 若为电子邮件形式，则邮件进入收件一方指定之电子邮件系统的时间即视为已送达 若为专人派送时（包括特快专递），按收件一方签收之日期为准；若以挂号邮件发送时，以邮局所出具之收据为准，自寄发日起计五（5）个工作日为准。

2. 鉴于双方未来可能难以以电子邮件确认相关合作内容的情况，故设定电子邮件必要联系人，即有关本合同的任何电子邮件内容均需要明示抄送双方指定的电子邮件必要联系人。

第十一条 争议解决

- 本合同之签署、效力、解释和执行以及本合同项下争议之解决，均适用中华人民共和国法律法规。
- 本合同在履行中所产生的争议，或与本合同有关的一切争议，由甲、乙双方协商解决。
- 甲、乙双方约定协商不成，协商不成则争议各方均一致同意将争议提交上海仲裁委员会根据仲裁规则进行仲裁。仲裁裁决为一裁终局，对各方均有法律约束力。

第十二条 其它

- 可分割性。除法律、行政法规另有规定外，如果本合同的任何条款违法，该条款将被修改和解释，以在适用法律的最大限度内，最好地实现原条款的目标，同时本合同的其余条款将继续保留其全部效力。
- 本合同附件为本合同不可分割的组成部分，若本合同附件与合同正文约定不一致的，以附件的约定为准。
- 本合同未尽事宜，合同各方另行协商一致签订补充合同、备忘录、订购单等形式予以书面约定，作为

甲方合同编号:

本合同的有效补充，具有同等法律效力。

4. 本合同一式肆份，双方各执贰份，经甲、乙双方盖章后生效，具同等法律效力。

附件：服务涉及的设备清单

附件：乙方资质证明文件

附件：商业道德承诺书

-----以下无正文-----

甲方：上海申曜哩科技有限公司

乙方：上海杉木电子科技有限公司



签约日期：2024年6月1日

甲方合同编号:

附件：服务产品清单

品牌	型号	条码	服务级别	24 年服务时间	含税 RMB LVA	25 年服务时间	含税 报价	26 年服务时间	含税 报价	合计
H3C	H3C S7503X	210235A1YK320C0000 1Q	网络产品基本维保服务标准 版 (7x24xND 发出)	2024/6/1-2024/12/31		2025/1/1-2025/12/31	1	2026/1/1-2026/12/31		
H3C	H3C S7503X	210235A1YK320C0000 20	网络产品基本维保服务标准 版 (7x24xND 发出)	2024/6/1-2024/12/31		2025/1/1-2025/12/31	1	2026/1/1-2026/12/31		
H3C	LS-5560X-54C-PWR- EI	210235A1X79207Q000 I3	网络产品基本维保服务标准 版 (7x24xND 发出)	2024/6/1-2024/12/31		2025/1/1-2025/12/31	1	2026/1/1-2026/12/31		
H3C	LS-5560X-54C-EI	210235A1X9208Q000 1J	网络产品基本维保服务标准 版 (7x24xND 发出)	2024/6/1-2024/12/31		2025/1/1-2025/12/31	1	2026/1/1-2026/12/31		
H3C	LS-5560X-30C-PWR- C EI	210235A1X9207Q000 DIW	网络产品基本维保服务标准 版 (7x24xND 发出)	2024/6/1-2024/12/31		2025/1/1-2025/12/31	1	2026/1/1-2026/12/31		

第 9 页 共 15 页

甲方合同编号:

附件：代理商资质证书



第 10 页 共 15 页

甲方合同编号：

附件：营业执照副本



第 11 页 共 15 页

甲方合同编号：



甲方合同编号：



附件：商业道德承诺书

商业道德承诺书

致：【上海哔哩哔哩科技有限公司】

我司知悉：贵司或其关联公司为知名的上市公司。根据主协议，双方形成合作关系，贵司为我司的合作方。为配合贵司规范市场交易行为，维护贵我双方各项业务合作的诚信、公平、公正，有效防范双方交易过程中违法或违规违纪行为的发生，特同意签署本《商业道德承诺书》（下称“承诺书”）。

我司理解、支持并保证严格遵守本承诺书的约定，深知下列各项不道德商业行为将给贵司或其关联公司带来严重的商业风险，破坏贵司及其关联公司廉洁的内部环境和良好的公众形象，严重扰乱市场的公平竞争，损害社会道德和行业风气。

我司承诺不会实施任何不道德商业行为，无论该行为发生在协议签订前、协议期间或者协议期满或解除后，上述不道德商业行为包括但不限于：

1. 采取向合作方员工直接给予财物的方式进行贿赂。例如：
 - (1) 假借馈赠、佣金、招待费、宣传费、赞助费、劳务费、科研费、咨询费等名义给付费用；
 - (2) 给予合作方员工不入财务账目的返利、回扣等；
 - (3) 以报销费用等方式给付合作方员工具有价值的物品如礼品、样品、娱乐票券、会员卡及各类有价票券、证券等；
 - (4) 向合作方人员提供持股便利，赠送股票、期权或类似权利，免费给予分红权，提供股票内幕交易信息等；
 - (5) 以租借或其他名义向合作方员工提供不动产供合作方员工免费居住，或免费提供交通工具供合作方员工使用；
 - (6) 以祝贺结婚、生日、乔迁、丧葬等名义向合作方员工提供礼金；
 - (7) 以聘请合作方员工为各类顾问等各种名义给付不正当利益或提供兼职机会；
 - (8) 通过赌博、假诉讼等方式输送不正当利益；
 - (9) 代为支付学费或其他费用等；
 - (10) 给予合作方员工其他任何无需付出对价或明显低于正常对价的财物。

第 13 页 共 15 页

甲方合同编号：

2. 免费或以明显低于正常的价格向合作方员工提供各种有价值的服务，例如：
 - (1) 提供国内外旅游、房屋装修、就业机会、就学安排；
 - (2) 各类宴请或娱乐活动包括 KTV、SPA、足浴、高尔夫、商业演出、旅游、商业体育活动、高档餐饮等。
3. 向合作方员工的近亲属实施前述第 1、2 条的不道德商业行为。
4. 通过向政府官员、政党人员或对双方交易有影响的相关人员实施前述第 1、2 条不道德商业行为，从而影响双方之间的诚信、公平、公正交易。
5. 主动聘用合作方员工（包括关联公司聘用、利用派遣公司聘用），无论系直接聘用或系通过猎头介绍聘用；引诱、怂恿合作方员工离职后至我或我关联公司就职。
6. 聘用合作方员工提供任何兼职、顾问等服务。
7. 与合作方员工或其他第三方恶意串通损害合作方的公司利益，包括：
 - (1) 与合作方员工合伙抬高购买价或压低销售价；
 - (2) 与其他供应商共谋定价，抬高或压低报价；
 - (3) 提交虚假的报价信息及/或其他供应商资质文件；
 - (4) 在接受合作方的调查过程中隐瞒重要信息及/或提供虚假信息。
8. 从事或参与任何有损合作方产品、服务或商业形象的活动；发表或附和任何未经核实或不实的有损合作方产品、服务或商业形象的言论。

我司现承诺，若我司或我司员工实施上述不道德商业行为的：

1. 实施第 1-7 条不道德商业行为的，同意按其提供的不当利益（财物或服务价值）的 10 倍或前一年（非自然年，即从发现实施不道德商业行为之日起的前 12 个月）交易金额的 20% 向我司支付违约金（以较高者为准，但不低于人民币壹拾万元）。
2. 实施第 8 条不道德商业行为给贵司造成损失的，我司同意赔偿贵司全部损失，包括任何有权机构做出的处罚（不限于罚款），以及贵司因前述损失而支出的救济成本如律师费、诉讼仲裁费等。
3. 若贵司有合理依据认为该合作价格明显区别于市场价格，贵司有权对合作项目重新核定价格并按照贵司核定的价格履行支付或收取。
4. 如我司违反本承诺函中任何承诺的，贵司有权即时全部或部分地解除、终止主协议，且不承担任何违约或赔偿责任；此情形视为我司严重违约，协议解除后：
 - (1) 若贵司有未消耗完毕的预付款的，解除通知发出后退还预付款。
 - (2) 若项目已经实际履行，按照上述我司承诺的第 3 项，根据贵司核定的价格，对于实际履行部分重新定价，并且多退少补。
 - (3) 若项目未实际履行，包括但不限于资源包未消耗/IP 未使用/产品未消耗/我司产品未实际交付/服务未提供等任何未实际使用或者履行的情形，我司需要退还贵司

第 14 页 共 15 页

甲方合同编号：

已支付的全部款项，或免于贵司支付应付款项。

- (4) 除上述罗列情形外，我司还应该按照主协议的约定，承担最高违约责任。
5. 本条中约定的违约金不足以弥补贵司损失的，贵司可进一步追索损失，且贵司有权直接从应付给我司的款项中扣除违约金及损失。
6. 上述涉及到我司退款或其他费用支付的，我需要在收到贵方的退款通知或者其他通知后 10 日内向贵司支付。
7. 贵司有权将我列入“合作方黑名单”，进行永久或阶段性的限制交易。

如贵司有合理依据认为贵司人员在与我司的业务合作中发生了不道德商业行为，我司应积极配合并协助贵司进行的相关调查。

我司另同意：若发现贵司人员有上述行为，将及时发送通知邮件至贵司举报邮箱，邮箱地址为：lianzheng@bilibili.com。

我司同意本承诺书不因贵我双方合作交易的终止而终止。

承诺方：【上海杉木电子科技有限公司】



日期：【2024】年【6】月【1】日

17.5. 常熟哔哩哔哩科技

合同编号：BT2024-SV05230006

甲方合同编号



B 站常熟核心交换机 24 年 Q2 维保
服务采购合同

甲方：上海哔哩哔哩科技有限公司

乙方：上海杉木电子科技有限公司

2024 年 4 月

甲方合同编号:

甲方：上海哔哩哔哩科技有限公司（以下简称“甲方”）
联系地址：上海市杨浦区政立路485号国正中心3号楼

乙方：上海杉木电子科技有限公司（以下简称“乙方”）
联系地址：上海市徐汇区宜山路333号1204室

甲、乙双方根据《中华人民共和国民法典》及相关的法律、行政法规之规定，就甲方向乙方采购指定产品事宜达成如下条款：

第一条 产品概况（详情请见附件）

1. 甲、乙双方约定，甲方向乙方采购设备维保服务，乙方按约定向甲方提供服务，具体服务涉及设备、服务范围、执行标准、质量检测等内容详见附件约定（以下简称“服务”）。
2. 甲、乙双方约定未经甲方书面同意，乙方不得随意改变服务标准、内容、数量、价格、工艺、时间等，如需变更产品已确定的内容、参数、数量、时间、地点等内容，双方应协商达成一致以书面形式确认。

第二条 费用及付款方式

1. 本合同产品总金额（含税）：(RMB) ¥ 151433.00 元；大写：壹拾伍万壹仟肆佰叁拾叁元整。
- (1) 上述金额表述两者不符时以中文金额为准（下同）。
- (2) 上述金额已经包含服务包含的质检、维护、保修、更新升级、部件更换（含部件费用）等服务内容的所有费用，除此外甲方无需向乙方或任何第三方支付额外费用。
2. 甲、乙双方约定的具体付款方式如下：
- (1) 本合同生效后自甲方确认乙方提供【增值税专用发票】之日起十五个工作日内甲方向乙方汇付首付款，即(RMB) ¥121146.4 元，大写：壹拾贰万壹仟壹佰肆拾陆元肆角。（以下简称“首付款”）。
- (2) 乙方开始提供服务（即维保服务期生效）并经甲方验收确认 30 日后，自甲方确认乙方提供【增值税专用发票】之日起十五个工作日内甲方向乙方汇付尾款，即(RMB) ¥30286.6 元，大写：叁万零贰佰捌拾陆元陆角（以下简称“尾款”）。
- (3) 乙方未及时出具合格的【增值税专用发票（13%）】或未履行甲方支付费用的前置条件时，甲方有权相应顺延支付费用。
3. 甲乙双方各自承担应当缴纳的税费：

乙方收款账户信息如下：	
开户行	平安银行上海西南支行

甲方合同编号:

开户人	上海杉木电子科技有限公司		
账号	175536-11006523950201		
甲方开票信息如下：			
名称	上海哔哩哔哩科技有限公司		
纳税人识别号	91310000MA1G8B8AXD		
地址	上海市杨浦区四平路 1945 号 1641 室		021-25099255
开户银行及账号	招商银行股份有限公司上海虹口体育场支行		121923952410103

- 甲乙双方约定若乙方变更收款银行账户信息时，应当及时书面通知甲方，因乙方未及时书面通知甲方所产生的所有责任、后果或额外费用，均由乙方自行承担。

第三条 产品交付

1. 维保服务供货方式：原厂上门提供维护和报修。
2. 维保服务提供地点：甲方设备所在地
3. 维保服务期： 2024 年 04 月 23 日起至 2025 年 04 月 22 日止 。

甲方维保联系人信息： 徐韩坤，15542807699，中国江苏省苏州市常熟滨江经济开发区常熟保税区 A 区汪湾北路 1 号

4. 如甲方或乙方需要变更上述信息的，需在产品交付前提前叁个工作日书面通知乙方。

第四条 服务质量及保修维护

1. 乙方保证具备向甲方提供本合同服务的资质和能力，以原厂标准向甲方提供服务，服务应符合中华人民共和国法律、法规及国家和地方有关服务的质量标准规范以及合同和附件的约定。
2. 乙方提供的服务符合本合同和附件约定、服务说明书及该服务所有技术文件中关于功能、性能、品质及质量的描述，甲方以任何形式确认服务验收合格，并不表明甲方对服务质量的完全认可，乙方对服务承担质量瑕疵担保责任。
3. 乙方承诺在维保服务服务期内，在接到甲方的报修或维护通知之日起 24 小时内赶到现场为甲方提供保修或维护服务(如附件有具体约定，则以附件的约定为准)。 乙方的保修或维护服务联系人为： H3C 原厂官方 ，联系电话为： 4008100504 。
4. 服务维保期限届满，乙方应继续为甲方提供相应的保修服务，根据具体服务内容甲方向乙方支付合理的维修服务费用，乙方根据服务内容应事先告知甲方费用标准。
5. 乙方保证若维保服务造成人身、财产等损害，由此产生的责任应由乙方承担。

甲方合同编号:

第五条 权利义务

1. 甲、乙双方均保证具有洽谈、签订、履行本合同的主体资格及相关所需资质，并已获得了洽谈、签订、履行本合同的完全有效且不可撤销的所有授权、同意、批准或许可，且任何一方洽谈、签订、履行本合同的行为将不会违反任何在先义务。
2. 乙方应及时向甲方提供乙方加盖公章具备合法经营资质的证明文件及合法销售产品和提供产品服务的资质文件，甲方不因对本合同乙方的任何承诺及保证的审查行为而承担任何责任。
3. 甲、乙双方约定本合同项下乙方交付的全部产品自交付之日所有权属于甲方，乙方不得在全球范围内申请、注册、登记任何与甲方相同或相近似的商标、专利和著作权等。
4. 甲、乙双方在其自身宣传材料、名片、市场宣传、网站建设以及其他任何方面使用对方的名称、商标、字号、域名和网站等信息，都必须事先通知对方，并获得对方的书面许可后方可进行；
5. 除履行本合同所需外，未经对方书面许可，任何一方不得擅自使用、复制对方的商标、标识、版权作品、商业信息、技术及其他资料等。在履行本合同期间，甲乙双方在使用对方的企业名称、商标、商号、品牌、域名和网站时，应当完全单独为甲乙双方在本合同中约定的内容服务，不得夹带其他业务内容。
6. 甲、乙双方约定若乙方违反诚实信用原则或经营状况严重恶化，甲方认为乙方难以继续履行本合同时甲方单方终止本合同，且不视为甲方违约。

第六条 保密责任

甲、乙双方均保证对在洽谈本合同约定事项过程中以及签订、执行本合同过程中所获悉的属于对方的且无法自公开渠道获得的文件、资料及信息等予以保密，具体如下：

1. 接收保密信息的一方（“接收方”）应：
 - （1）对保密信息严格保密；
 - （2）不向任何第三方披露任何保密信息；
 - （3）除为履行本合同之目的外，不为任何其他目的使用保密信息。
2. 保密信息的定义，“保密信息”指：
 - （1）有关本合同的存在和内容以及有关本合同预期交易的信息；
 - （2）一方（“披露方”）向接收方披露的全部专有、保密、非公开的技术信息和（或）商业信息，包括但不限于（a）披露方在本合同签署前或之后披露给接收方或其雇员的任何研发设计、服务或产品设计理念/想法、产品及其规格、数据、模型、样品、草案、产品测试结果等技术类信息；

甲方合同编号：

(b) 营销要求和策略、产品计划及价格、客户名单、公司业务发展的方向、涉及经营管理的制度与流程等的商业信息；(c) 通过签订和履行本合同而获知的对方及对方关联公司的任何信息

和因履行本合同而获悉的资料、软件、数据等信息数据内容；以及 (d) 其它由披露方披露给接收方的且需向第三方承担保密义务的信息（不论该等信息是以书面、口头、图形、网络还是其他任何形式进行了披露）。

(3) “保密信息”不包括以下信息：(a) 披露方披露之时或之前已为公众所知的信息；(b) 披露之后非因接收方的行为或过错而为公众所知的信息；或 (c) 接收方从第三方处获得的且并不因此使第三方违反其保密义务的信息。

- 3. 披露的同意。一方需要对外披露保密信息时应获得另一方的书面确认。
- 4. 保密期限。在披露方提供给接收方的保密信息被合法地公开之前，接收方应对相关保密信息永远予以保密。
- 5. 擅自披露的责任。如一方违反其在本合同项下的保密义务，该一方需按本合同第八条第 3 款的约定承担违约赔偿责任（包括但不限于：为追究违约责任支出的律师费、仲裁费、差旅费、鉴定费、文印费、审计费等）。

第七条 不可抗力

- 1. 本合同所称的不可抗力是指一切不可预见、不可避免并不能克服的客观情况，包括但不限于洪水、地震、飓风、火灾等自然灾害及战争、动乱等情况，以及政府对本合同订立时有效之相关法律、行政法规、政策等进行修订、变更、废止，或颁布新的法律、行政法规、政策以取代原有法律、行政法规、政策或使原有法律、行政法规、政策处于废止状态，从而最终导致本合同无法继续履行。
- 2. 因不可抗力或者国家政策法律的变化而使本合同中任何一方或双方部分或全部不能履行本合同的，遭受不可抗力的一方无需向对方承担违约责任，但应及时通知对方不可抗力的发生情况并提交不可抗力的合法证明材料。
- 3. 如不可抗力情况消失后，本合同仍有必要履行且具备继续履行的条件，双方应继续履行本合同；如因不可抗力导致本合同没有必要或无法继续履行的，则本合同任何一方均有权提出解除本合同，且双方互不承担违约责任。

第八条 违约责任

- 1. 无论故意或过失，甲、乙双方未履行本合同约定义务或应遵守事项均视为违约。任何一方违约，另一方有权要求违约方停止违约行为，自违约方告知停止违约行为之日起 10 日内，违约方不停止违约行为的，

甲方合同编号:

守约方有权单方解除本合同，解除本合同的通知到达违约方时本合同解除，解除合同不影响守约方要求违约方承担违约赔偿责任（包括但不限于：为追究违约责任支出的律师费、诉讼费、差旅费、鉴定费、文印费、审计费等）。具体提供维保服务的维保方、服务人员违反约定，视为乙方违约。

2. 甲方无正当理由故意未按约定期限向乙方付款时，每逾期一日，甲方须向乙方承担应付而未付款万分之一的滞纳金，逾期超过 30 日仍未付款的，乙方有权解除合同，并要求甲方承担由此给乙方造成的全部损失。
3. 乙方保证取得签署并履行本合同项下内容的合法经营资质、授权资质等，保证有权依法运营其服务，向甲方提供的服务不违反中国法律法规，不侵害任何第三人权益，且不存在任何侵害人身安全的隐患，若发生上述情况或乙方履行本合同过程中违反诚实信用原则，或未履行或未充分履行其与本合同项下的任一承诺、保证义务时，乙方应向甲方承担全部赔偿责任（包括但不限于仲裁费、律师费、赔偿款、差旅费、鉴定费、产品召回费用、罚款等）并向甲方赔偿本合同总金额叁倍的违约金，若甲方的全部损失超过前述违约金时，乙方应赔偿甲方的全部损失并按甲方要求的方式做出公开赔礼道歉。前述约定的违约金，均系双方在签订本合同时已经预见到的守约方因违约方之违约行为将遭受的最低损失，发生违约情形时，守约方在约定的数额范围内主张违约金或损失赔偿金的，违约方放弃主张违约金过高的权利，守约方免于就实际损失举证。但守约方主张其因违约方的违约行为遭受的实际损失大于本合同约定的数额的，守约方应当举证证明其实际发生的损失。
4. 由于乙方提供的服务无法通过甲方的验收或无法满足合同目的导致甲方对乙方做出乙方不具备提供本合同所需能力的判断的；或乙方若单方实质性违约或不能充分履行义务，并在甲方告知后未能进行补救；或未能在甲方要求的期限前提供符合要求的增值税发票；或由于乙方的行为甲方认定乙方不能胜任本合同的履行的；或虽然甲方出于情势所迫不得不使用乙方提供的带有瑕疵的服务开展业务，但甲方仍旧决定追究乙方相关责任的，则甲方在法律允许的前提下有权作出以下一项或多项决定：
甲方有权要求无条件解除/终止本合同，并不再支付任何费用。
甲方有权要求乙方返还已付全额款项。
甲方有权不再支付任何费用。
甲方有权要求乙方向甲方承担本合同总金额的 30%作为违约金，并就甲方因此遭受的损害承担赔偿责任。甲方要求乙方承担的损害赔偿的范围包甲方所受的直接损失和间接损失。
5. 因本合同的履行产生的乙方应承担的违约金、赔偿金等，甲方有权从未付款项中预先扣除，不足部分乙方应当补齐。

第九条 禁止转让

乙方未经甲方书面同意，不得以任何理由将本合同相应权利或义务转让、出借、委托、许可、授权等以

甲方合同编号

任何形式给第三方，同时，不得以本合同中权利对外设立质权及其他担保物权，也不得作其他任何形式的处分，但本合同另有约定的除外。

第十条 通知与送达

双方之间的任何重要通知或书面函件，必须以中文写成，以电子邮件、专人送达（包括特快专递）或挂号信函之形式发送，除非事先以书面通知更改，则双方的沟通工具如下：

双方	合作联系人	电子邮件必要联系人	电子邮箱	手机电话
甲方	周合一	/	zhouheyi@bilibili.com	13552623089
	/			
乙方	刘小芳	/	lxf@sh-shanmu.com	15221235273
	/			

1. 若为电子邮件形式，则邮件进入收件一方指定之电子邮件系统的时间即视为已送达；若为专人派送时（包括特快专递），按收件一方签收之日期为准；若以挂号邮件发送时，以邮局所出具之收据为凭，自寄发日起计五（5）个工作日为准。
2. 鉴于双方未来可能有以电子邮件确认相关合作内容的情况，故设定电子邮件必要联系人，即有关本合同的任何电子邮件内容均需要明示抄送双方指定的电子邮件必要联系人。

第十一条 争议解决

1. 本合同之签署、效力、解释和执行以及本合同项下争议之解决，均应适用中华人民共和国法律法规。
2. 本合同在履行中所产生的争议，或与本合同有关的一切争议，由甲、乙双方协商解决。
3. 甲、乙双方约定协商不成，协商不成则争议各方均一致同意将争议提交上海仲裁委员会根据仲裁规则进行仲裁。仲裁裁决为一裁终局，对各方均有法律约束力。

第十二条 其它

1. 可分割性。除法律、行政法规另有规定外，如果本合同的任何条款违法，该条款将被修改和解释，以在法律允许的最大限度内，最好地实现原条款的目标，同时本合同的其余条款将继续保留其全部效力。
2. 本合同附件为本合同不可分割的组成部分。若本合同附件与合同正文约定不一致的，以附件的约定为准。
3. 本合同未尽事宜，合同各方另行协商一致签订补充合同、备忘录、订购单等形式予以书面约定，作为本合同的有效补充，具有同等法律效力。
4. 本合同一式肆份，双方各执贰份，经甲、乙双方盖章后生效，具同等法律效力。

甲方合同编号:

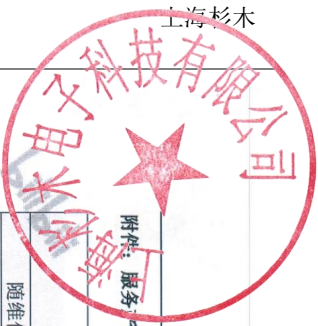
附件：服务涉及的设备清单
附件：乙方资质证明文件
附件：商业道德承诺书

-----以下无正文-----

甲方：上海哔哩哔哩科技有限公司
(盖章):

乙方：上海杉木电子科技有限公司
(盖章):

签约日期：2024 年 4 月 23 日



附件：服务产品清单

甲方合同编号：

产品描述	产品型号	产品数量	服务名称	服务开始时间	服务结束时间
随维保技术支持服务	SV-MA-BTSS	1	随维保技术支持服务	2024-4-23	2025-4-22
交流电源模块-2400W	PSR2400-54A	16	网络产品基本维保服务标准版(7x24xND 发出)	2024-4-23	2025-4-22
S12508X-AF 交换网板, H 型(C 类)	LSXM1SFH08C1	12	网络产品基本维保服务标准版(7x24xND 发出)	2024-4-23	2025-4-22
H3C S12508X-AF 以太网交换机风扇模块	LSXM108XFAN	4	网络产品基本维保服务标准版(7x24xND 发出)	2024-4-23	2025-4-22
H3C S12500X-AF 18 端口 100G 以太网光接口 (QSFP28)/36 端口 40G 以太网光接口模块 (QSFP+) (Hb)	LSXM1CGQ18QGHb1	2	网络产品基本维保服务标准版(7x24xND 发出)	2024-4-23	2025-4-22
H3C S12508X-AF 以太网交换机主机	LS-12508X-AF	2	网络产品基本维保服务标准版(7x24xND 发出)	2024-4-23	2025-4-22
H3C S12500X-AF 主控制引擎模块	LSXM1SUPB1	4	网络产品基本维保服务标准版(7x24xND 发出)	2024-4-23	2025-4-22



附件：代理资质证书



甲方合同编号:



附件：营业执照副本

甲方合同编号：



第二部分、技术标

1. 投标公司简介及重难点分析与应对

上海杉木电子科技有限公司作为 ICT 技术解决方案专家,始终秉持着“合作共赢”的经营理念,以客户需求为核心,为客户提供个性化定制方案。杉木电子致力于为各行业数字化转型贡献全部力量。

杉木电子深耕行业 30 余年,以“满足客户一切需求”为出发点,不断丰富自身产品和服务,为各行业各场景提供智慧办公、智慧校园、智慧医疗、智慧城市、智慧园区、云计算、信息安全、物联网等个性化解解决方案与服务,在金融、教育、互联网、政府、运营商、能源、医疗等行业数字化转型实践经验。

杉木电子目前与国内外知名厂商建立深厚的合作伙伴关系,华为、新华三、麒麟、达梦、深信服、奇安信等国内外知名品牌,并在全国多地建立分公司。





Service process
售前服务流程



Service process
售后服务流程





1.1. 投标综合说明

本文件系上海杉木电子科技有限公司针对“2025 年度浦东新区档案局档案信息系统支撑平台（硬件平台）维护项目”撰写的技术标方案。我司谨向上海市浦东新区档案局全面阐述本次运维服务的各项内容，具体包括服务目标、服务范围、服务方式、响应时效、服务流程、具体服务内容、管理机制、验收标准以及未来系统优化建议等，力求通过清晰、专业的表述，展现出我司对本项目的高度重视与综合服务能力。

能够受邀参与本次运维服务项目的投标，我司深感荣幸。在认真研读招标要求的基础上，我们已组织专业技术团队对用户方的实际需求进行了多轮深入分析与评估，以确保本技术方案内容详实、规划科学，并完全契合贵局对系统稳定性、安全性与持续可用性的要求。

若荣幸中标，我司承诺将投入充足的人力、技术与设备资源，制定周密详实的项目前期工作计划与整体运维服务实施方案。我们将充分发挥在信息技术服务领域积累的丰富经验和技术管理优势，以体系化、标准化和智能化的运维模式，保障贵局档案信息系统支撑平台（硬件部分）的高效、稳定与安全运行。

我司诚挚期望能够藉此机会，与浦东新区档案局建立长期、稳定的战略合作伙伴关系。我们将以高度负责的态度、领先的运维理念和持续改进的服务体系，为贵局提供全方位、专业化、响应迅速且品质可靠的技术支持与服务保障，助力浦东新区档案事业信息化发展迈向新台阶。



1.2. 投标公司相关资质





H3C

数字化解决方案领导者

新华三合作伙伴认证证书

—◀ 安全产品合作伙伴认证 ▶—

上海杉木电子科技有限公司

安全认证合作伙伴

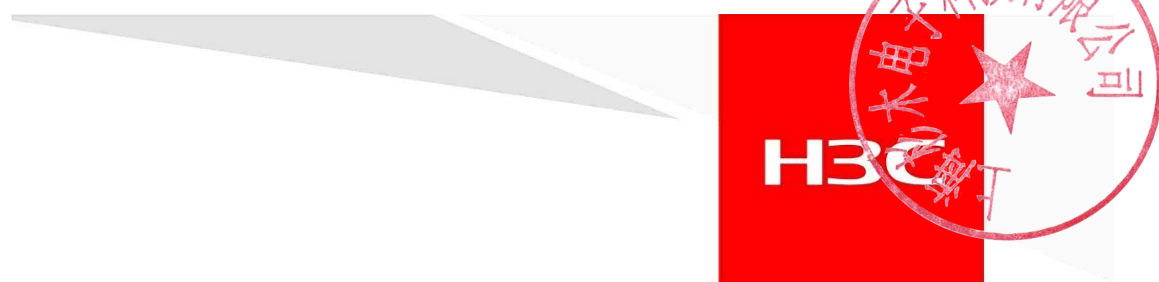
代理商编码：4102

有效期：2025-01-01 至 2025-12-31

本证书不适用于电商平台(包括但不限于京东、淘宝、天猫、拼多多、抖音)授权使用。



首席执行官
新华三集团



服务资质认证证书

上海杉木电子科技有限公司

主网络三星级服务商

证书编码：325021701

有效期：2025年02月17日 - 2026年03月01日

A handwritten signature in black ink, appearing to be "于红枫" (Yu Hongfeng), is written over a horizontal line.

首席执行官
新华三集团











SANGFOR
深信服科技

编号：SI005543

授 权 书

CERTIFICATE OF AUTHORIZATION

兹授予

上海杉木电子科技有限公司

商业金牌经销商

经销本公司SANGFOR系列产品

有效期： 二〇二五年一月至二〇二五年十二月

何朝斌



深信服科技股份有限公司

二〇二五年一月



1.3. 投标公司针对本项目优势

我司自1993年成立以来，近30年深耕IT领域，汇聚资深工程师团队，具备雄厚技术实力与服务经验。公司代理多品牌网络、服务器、安全及软件产品，拥有丰富的产品资源与综合解决方案能力，能精准匹配客户需求，提供稳定、高效、可靠的运维支持，保障系统长期稳定运行，为客户创造持续价值。

我司与去年开始参与档案局信息支撑平台(硬件平台)的整体运维。我们已对本次运维项目的要求做出了深刻解读，更有效的为此次服务范围所涵盖的服务器、网络设备、存储、网络安全、数据库、虚拟化、机房环境、备份恢复等软硬件设备和业务系统提供更为有效的整体运维服务。针对日常运维管理，我司创新设计了多纵多横运维团队体系，确保服务结构清晰、责任到人、响应高效。运维管理团队统筹规划；运维驻场团队提供一线快速响应；二线巡检团队负责主动预防；二线技术专家团队精准定位和解决，三线原厂技术兜底攻坚客难，形成从预防到修复的闭环管理。这种架构确保了所有技术问题都有专人负责，实现了知识的深度积累与问题的精准快速解决，从而全面提升运维服务的质量与效率，保障系统稳定。

针对本项目，我司核心优势在于构建了高效协同的备件保障体系。该体系以档案局现场库为快速响应核心，公司总部库及品牌商在线库提供强大后备支援。通过统一的备件管理系统进行智能调度，此金字塔式结构确保了备件获取的及时性与精准性，能极大缩短平均修复时间（MTTR），显著提升系统可用性。我们凭借近30年的资源积累，能有效整合周边项目资源，为本次运维服务的连续性与稳定性提供坚实可靠的物资保障，最大限度降低停机风险。

针对本项目现场设备系统繁杂、老旧且品牌众多的挑战，我司的核心优势尤为突出。我们凭借近30年的集成、运维服务积淀，与众多设备供应商及技术服务商建立了稳固的合作关系。这对于处理已停产、市面难寻备件的设备故障至关重要。我方工程师不仅能凭借丰富经验快速精准定位故障点，更能高效协同原厂及供应商资源，迅速调动技术力量与稀缺备件，形成解决问题的闭环。



1.4. 针对本项目重难点分析和应对措施

本次档案局运维的项目包含 3 个系统平台（局域网平台、政务外网平台、互联网平台），包括网络、安全、主机、存储、虚拟化、机房工程等众多系统，从招标文件来看，部分系统设备清单可能需要细化更新迭代。本次运维的多个系统关联性强，专业性要求高，对运维团队的专业性，稳定性有很高的要求。各专业均根据招标文件要求选择专业能力优秀的技术人员持证上岗，并对人员职业素养进行确认，人员长期稳定，定期培训考试。根据实际情况，对各类故障应急处理进行规划处理，制定应急处理操作手册，并定期更新。每年定期组织演练，确保小概率事件发生时能快速解决。

1.4.1. 项目重难点分析

1) **系统老旧与复杂性高：**运行20年以上老系统，品牌杂、多代共存，部分设备停产，备件稀缺，兼容性风险极大。

2) **多网络隔离与安全风险：**需同时维护局域网、政务外网、互联网三套逻辑/物理隔离网络，边界安全策略复杂，跨网数据交换存在安全挑战。

3) **架构稳定性挑战：**老旧硬件故障率随年限急剧升高，单一设备故障可能引发系统性风险，保障业务连续性压力巨大。

4) **技术文档与知识缺失：**历经多年，原始技术文档可能遗失，系统架构和配置依赖老员工经验，存在知识断层风险。

5) **现代运维体系融合难：**传统静态运维模式难以满足当前业务需求，如何将自动化、监控预警等现代运维融入老旧环境是一大挑战。

6) **备品备件充分性要求：**信息系统支持平台整体设备情况使用年限较久，并且部分设备仍在运行核心业务系统，对系统的稳定性和对运维时效性有很高的要求。

7) **信息安全的建设：**整体系统环境较为复杂，在信息安全建设方面仍需要进一步针对核心业务系统进行系统建设，保证核心业务系统安全，降低档案信息的泄露风险。



1.4.2. 针对性应对方法

1) 系统性评估与生命周期管理：

进行全面深度巡检，建立精准的资产台账和拓扑图。对核心老旧设备，启动特级保障（现场库为快速响应核心，公司总部库及品牌商在线库提供强大后备支援。通过统一的备件管理系统进行智能调度，确保了备件获取的及时性与精准性，能极大缩短平均修复时间（MTTR），优先保障关键设备备件，制定分阶段的现代化替代迁移计划。

2) 强化安全边界与纵深防御：

严格审核三网间边界安全策略（防火墙、网闸），部署终端准入控制。政务外网严格遵循等级保护要求，互联网区域加强Web应用防护和威胁检测，构建纵深防御体系。

3) 构建高可用与快速响应能力：

优化现有网络架构，尽可能利用现有资源构建冗余。结合“多纵多横”运维团队，驻场团队快速一线响应、二线专家远程支撑、三线原厂攻坚克难，确保故障定位与处理的效率，最大化缩短业务中断时间。

4) 知识管理与标准化：

实施“知识沉淀”计划，由技术专家团队牵头，在巡检和排障中全面更新技术文档。建立标准操作程序（SOP），将个人经验转化为团队资产，降低对个人的依赖。

5) 引入智能运维与渐进式改造：

部署集中监控系统，实现对网络、主机、存储的性能与故障告警。优先在虚拟化、云计算等较新领域推行自动化运维脚本，提升效率，为全局现代化改造积累经验。

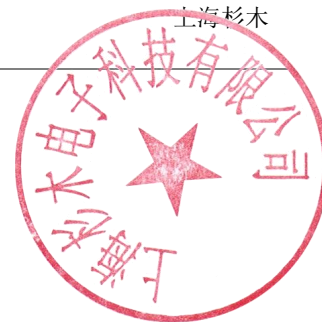
6) 依托成熟的供应商合作生态：

现场设备系统类型较多，设备使用年限较久，涉及的设备品牌及供应商情况复杂，更有部分设备已经停产，市面上已难以找到相关备件，我司通过30多

年的经验积累，依托成熟的供应商合作生态，高效解决老旧复杂设备的故障与备件难题。

7) 成熟的应急管理体系：

杉木电子经过30多年发展积累、已经形成了成熟的应急管理体系，具备大量可操作性强的操作手册、应急预案、演练预案和重保要求，并且每年组织演练，确保小概率事件发生时能快速解决。全面覆盖各应用系统并在突发事件的事前、事发、事中、事后阶段发挥关键支撑作用。



2. 投标公司服务规范及管理

2.1. 公司服务规范

2.1.1. 项目人员组织

为确保本次信息系统运维服务高效、专业地开展，我司严格依据用户方运维需求——包括对网络、安全、主机服务器、存储、备份等硬件设施，以及数据库、中间件等系统软件的日常维护、应急处理，同时覆盖防病毒、日志审计、安全通告及技术培训等服务内容——特成立专项服务项目组。项目组采用角色清晰、责任到位的组织结构，允许符合条件的人员兼任多个角色，具体组成如下：

- 服务工程师：负责网络设备、安全设备、主机服务器、存储及备份系统等硬件和基础软件的日常监控、维护及一般性故障处理，保障系统稳定运行。
- 高级系统工程师：主导项目中出现的重大故障排查与解决，负责系统变更方案的设计与实施，指挥应急响应工作，提供更深层次的技术支持与根因分析。
- 服务经理/项目经理：全面负责项目的组织、协调与进度控制，管理服务交付过程，与客户保持沟通，确保运维工作按既定目标和质量要求推进。
- 质量管理人员：负责运维服务全过程的质量控制，监督各项流程和标准的执行情况，处理客户投诉及改进建议，推动服务质量持续提升。
- 客户服务部经理：负责制定和优化标准化服务流程，组织实施项目组成员的绩效评估与技能培训，不断提升团队整体服务水平和客户满意度。

该项目组结构兼顾技术纵深与管理横向协调，既确保一线运维响应的及时性，也强化高层技术支持和管理的系统性，真正做到责任到人、流程闭环，为信息系统提供可靠、安全、连续的运维保障。

2.1.2. 人员情况表

序号	姓 名	职务	职称及资格证书	主要资历、经验及承担过的项目
1	徐如远	项目负责人	H3CTE、H3CSE-Security、Linuxplus等	上海世博会、公安感知网、庆阳智算、点军人工智能等
2	俞聂敏	服务工程师	H3CIE、H3CSE-Security、麒麟系统工程师等	进口博览会、上海智算、上海期货信息、中芯国际等
3	马云章	服务工程师	H3CIE、麒麟系统工程师等	海关电子口岸、国药集团等

注：详见商务标部分 第 15 章 人员情况表

2.1.3. 人员行为规范要求

- (1) 遵守用户的各项规章制度，严格按照用户相应的规章制度办事。
- (2) 与用户运行维护体系其他部门和环节协同工作，密切配合，共同开展技术支持工作。
- (3) 出现疑难技术、业务问题和重大紧急情况时，及时向负责人报告。
- (4) 现场技术支持时要精神饱满，穿着得体，谈吐文明，举止庄重。接听电话时要文明礼貌，语言清晰明了，语气和善。
- (5) 遵守保密原则。对被支持单位的网络、主机、系统软件、应用软件等的密码、核心参数、业务数据等负有保密责任，不得随意复制和传播。

2.1.4. 技术支持规范要求

运维服务人员应始终秉持耐心、细心和热心的服务态度，以高度的责任心对待每一项运维任务。所有工作须严格执行“事事有记录、事事有反馈”的原则，确保运维过程可追溯、结果可验证。遇到重大问题或异常情况，应立即按

流程上报，并积极配合处理，保障问题及时闭环。同时，必须严格遵守工作作息时间，服从项目安排，并严格遵循既定的服务工作流程和操作规程，专业化、标准化的服务支撑系统稳定运行，提升客户满意度。

(1) 现场支持工程师应着装整洁、言行礼貌大方，技术专业，操作熟练、严谨、规范；现场支持时必须遵守用户单位的相关规章制度。

(2) 现场支持工程师在进行现场支持工作时必须在保证数据和系统安全的前提下开展工作。

(3) 现场支持时出现暂时无法解决的故障或其他新的故障时，应告知用户并及时上报负责人，寻找其他解决途径。

(4) 故障解决后，现场支持工程师要详细记录问题的发生时间、地点、提出人和问题描述，并形成书面文档，必要时应向用户介绍故障出现的原因及预防方法和解决技巧。

2.1.5. 信息保密要求规范

鉴于本次运维服务项目属于政府项目，对日常维护过程中产生的各类文档均有严格的保密管理要求。我司作为长期服务于政府、金融等敏感行业的IT企业，始终将信息安全与保密工作置于首位。公司从高层管理者至一线工程师，均高度重视保密信息的管理，并通过常态化培训与制度约束，确保保密意识深植于每一位员工的日常行为中。

公司领导持续强调保密管理的重要性，并将其作为新员工入职培训的核心内容，系统宣讲保密法规、企业保密政策及实操要求。此外，我司已建立一套专门针对保密项目的档案管理制度，涵盖文档的撰写、整理、归档、存储及传输等全流程，确保各环节均符合保密规范。所有涉密信息均按权限严格控制访问，操作过程全程留痕，实现可追溯、可审计。

我司郑重承诺，未经用户方书面许可，绝不会将运维服务过程中接触的任何信息泄露予任何第三方。具体管理细则详见我司《机房安全管理制度》及《安全保密管理制度》。

2.1.6. 资料归档要求规范

日常运维工作中，工程师在执行系统巡检及各类技术服务时，均须严格按照规范完成相关文档的记录与整理，确保每一项操作均有据可查、所有变更可追溯。服务经理负责对文档进行统一审核、归档与管理，保障维护记录的完整性、一致性和可检索性。通过系统化的配置管理，不仅有效提升了故障排查与变更控制的效率，也为系统持续优化提供了可靠的数据基础，全面增强运维服务的透明性与可靠性。

操作的可追溯与可查询对运维服务的质量保障至关重要。因此，配置管理是我公司运维服务体系中的核心组成部分，其重点在于对各类文档的规范化、全生命周期管理。我们建立了一整套完善的文档管理机制，涵盖从模板制定、内容填写、变更记录到定期备份等各个环节。

在本次运维服务中，我司所提供的所有技术文件将确保全面、完整且内容详实，能够准确反映运维服务的各个环节与成果，切实满足浦东新区档案局档案信息系统支撑平台运维服务项目顺利实施的各项需要。所有交付的文档和资料均同时提供电子文档与纸面文档两种形式，其中电子文档统一采用简体中文版Word格式，以保证文档的通用性、可编辑性与长期可读性，便于归档、查阅及后续管理。



2.2. 公司服务管理

2.2.1. 安全文明管理

项目安全控制必须严格遵循“安全第一、预防为主”的方针。项目经理作为安全生产的总负责人，应建立健全完善的安全管理体系与安全生产责任制，组织制定安全施工组织设计或专项安全技术措施，确保项目安全目标的全面实现。

项目组应围绕项目实施过程中“人的不安全行为、物的不安全状态、环境的不安全因素以及管理缺陷”等各类风险，系统开展安全控制工作。必须建立健全施工安全生产教育制度，定期组织安全培训与考核，增强全员安全意识与风险防范能力，从源头杜绝安全事故发生，保障项目全程处于受控、安全状态。

2.2.2. 安全文明规范

项目现场的管理规范，应建立在施工核定区域内科学合理的空间设计与物料器具定位管理标准化的基础之上，确保现场布局有序、通道畅通、区域功能明确。项目组须紧密结合实际施工条件，严格遵循施工方案与进度计划要求，系统性地施工区域的规划、设计、布置与使用管理，实现施工全过程场地的动态控制与持续优化。

在施工过程中，项目组将严格执行环境保护与原有设施保护措施，对施工区域内及周边环境、原有建筑结构、装饰装修及各类设施实施全面防护，确保其完好无损。通过文明施工和标准化管理，最大限度地减少施工对现场及周边环境的干扰，维持整洁、规范、安全的现场作业环境。

2.2.3. 安全文明检查

项目经理应定期组织项目组对安全控制计划的执行情况进行系统性检查、考核与评估，针对实施中发现的不安全行为与隐患，需深入分析其成因，并制定并落实相应的整改与防范措施，以实现持续改进。

项目组应依据项目实施过程的阶段特点及安全目标的具体要求，科学确定各阶段的安全检查内容与重点，确保检查工作覆盖全面、重点突出。安全检查

应采取随机抽查、现场观察与实地检测相结合的方式，并详细记录检测结果。对项目实施人员的违章行为应及时予以纠正，确保各项安全制度和操作规程在现场得到有效执行，保障项目全程安全受控。



2.2.4. 施工安全管理

在项目实施过程中，我司将积极与施工区域所涉及的各部门进行沟通协调，严格遵循国家、上海市相关法律法规、政策文件及标准规范，并充分参照相关单位的管理要求，全面贯彻落实文明施工与安全生产的各项措施。在确保施工进度同时，我司郑重承诺，施工活动绝不干扰区域内相关部门的正常办公秩序与业务流程。

我司始终将施工安全置于首位，高度重视并切实落实各项安全管理制度与防护措施。如因施工操作造成任何人身伤害、财产损失或由此引发的行政处罚（包括但不限于罚金等），一切责任及经济损失均由我司独立承担，绝不牵连业主单位。

若因施工行为导致任何纠纷或法律诉讼，我司将主动负责处理并承担相应法律后果，确保业主方不因此卷入任何争议或法律程序，切实保障业主权益不受影响。

2.2.5. 消防安全管理

在本项目中，消防安全是项目顺利实施与系统稳定运行的重要保障，主要涵盖设备运行环境的消防安全以及施工作业过程中的消防安全两大方面。我司将严格遵循国家及上海市相关消防法规与技术标准，结合项目实际特点，制定并落实全面、科学的消防管理措施。

一、设备运行环境的消防安全

本项目所涉设备均部署于室内环境中。这些室内运行环境为既有建筑空间，其原有设计及现有设施已包含符合规范的消防安全系统，如烟感报警装置、自动灭火设备、消防栓及应急照明等。鉴于此，本项目不再对基础消防设施进行重复建设，而是将重点放在现有设施的合规使用与增强管理之上。

为确保设备运行环境具备良好的防火能力，我司将严格执行以下措施：
设备安装位置周围严禁堆放易燃易爆物品，保持设备间距符合散热与应急操作要求，并在关键区域设置防火隔离设施，以有效阻隔外部火情对设备造成的损害；

在设备选型与部署阶段，优先选用具备良好散热性能的机箱与组件，对核心设备及高负荷节点加装温度监测与集中报警系统，实时监控设备运行温度，杜绝因设备过热而引发的火灾隐患；

在系统设计与设备安装过程中，将严格依照电气安装规范与技术规程施工，确保所有线缆敷设、接地与负载设计科学合理，坚决防止因短路、过载、接触不良等电气故障诱发的火灾事故。

二、施工作业过程中的消防安全

本项目施工全部在室内进行，作业过程中的消防管理至关重要。我司将建立健全施工现场消防安全责任制，明确各级人员职责，并对所有进场人员进行专项消防安全教育，切实提升防火意识与应急处理能力。

在具体作业中，将严格执行以下规定：

严格禁止在室内施工区域使用明火作业，严禁吸烟，并设置明显禁火标志及专人巡查；

所有临时用电线路须由专业电工敷设，实行审批与巡检制度，确保电缆材质、线径、接口及保护装置符合安全标准，坚决杜绝私拉乱接；

加强接地与防雷管理，对重要施工机具及临时配电系统设置可靠的接地保护，雷雨天气下暂停室外关联作业；

施工现场配备足量灭火器、消防沙箱等应急设备，并保持消防通道畅通，确保一旦发生火情可迅速响应、有效扑救；

我司承诺，在整个项目周期内将持续开展消防隐患自查与整改，积极配合业主及消防管理部门监督检查，全力确保项目实现“零火情”目标。如因我方施工不当引发消防事故，我司将承担全部责任及相关损失。



3. 投标公司针对本项目服务

3.1. 服务定位

浦东新区档案局2025-2026年度档案信息系统支撑平台（硬件平台）维护项目，旨在通过先进、标准化和可控的技术手段，结合科学的运维工具与系统方法，对系统运行状态进行全面监控与智能分析，准确评估运行趋势，精准定位潜在瓶颈，并制定具有针对性的维护策略与操作规程。该项目以实现系统持续稳定运行、保障各项性能指标高效达标为核心目标，确保故障响应与处理流程迅速有效，不断提升系统运行质量。同时，通过系统性优化与潜力挖掘，致力于构建一个良性循环、持续改进的运行生态，为档案信息系统的长期可靠运行提供坚实基础。

基于我司对该支撑平台的深入理解及与用户的充分沟通，本次运维服务的总体目标包括：建立高可用、高可靠的硬件平台运维保障体系，实现从被动响应向主动预防的运维模式转变；通过规范化、精细化的管理流程，显著提升系统整体可用性与业务连续性；依托专业团队与成熟的服务体系，为用户提供及时、专业、可信赖的全生命周期运维支持，全面满足浦东新区档案局在当前与未来业务发展中对信息系统稳定性、安全性与性能的严格要求。

3.2. 服务目标

3.2.1. 备品备件服务

我司将提供全面且科学的备品备件解决方案，并确保该方案中所列的所有产品备件库有对应可替代的产品，以有效保障运维服务的高效性与响应及时性。针对客户运维范围内出现24小时内无法修复的硬件故障，我司将及时提供备机支持，确保业务连续性和系统稳定运行。此外，我司将常态化对备件使用情况进行详细记录与统计分析，并对更换频率较高的设备出具评估与汰换建议，助力客户优化资产配置，提升整体运维管理水平。

3.2.2. 硬件包修

对于服务范围内的设备及所有相关功能部件，我司提供全面的包修服务。如有需要送修至原厂或第三方进行维修，所有由此产生的费用均由我司承担。

3.2.3. 驻场服务

为确保本项目运维服务的连续性与稳定性，我司将组建一支结构合理、职责清晰的专业技术团队。团队配置至少包括1名项目负责人、2名技术工程师及若干二线支持工程师。服务周期内（国定节假日除外），现场均安排工程师值守：周一至周五确保2名技术工程师在现场，周六、周日至少安排1名技术工程师，提供7×8小时的现场运维支持。

现场工程师将全面负责监控系统运行状态，主动预防与及时处理各类故障，并定期执行机房环境、卫生及设备安全检查。此外，还涵盖日常巡检、系统变更、升级操作以及其他客户提出的合理维护需求。通过规范化的流程与专人专岗制度，我司致力于实现运维过程的可控、可追溯，有效保障系统稳定、高效运行。

详细内容如下：

1) 日常维护工作要求

① 事件分析处理：处理系统的日常问题及系统维护管理工作，保障系统可靠平稳运行；

② 及时处理日常系统健康巡检中发现的问题；

③ 对系统故障进行分析和迅速做出处理，保证系统的不间断运行；

④ 故障处理时限要求：核心业务系统故障要求 2 小时内恢复主要业务运行；普通业务系统故障要求 4 小时内恢复业务运行；非业务系统故障要求 8 小时内完成故障处理；

⑤ 数据库系统维护：数据定期检查和整理，数据库的日常维护、故障处理、性能监控及调优等；

⑥ 系统升级与变更：根据需要进行系统升级与变更；

⑦ 系统及软件安全的运行维护。



2) 服务器和系统日常维护要求

根据档案局服务器系统的实际运维需要，我司将提供全面而及时的技术支持服务，主要包括故障诊断与处理、系统配置调整与变更、性能优化及日常维护等。服务范围涵盖各类主流虚拟化平台及多种品牌的物理服务器操作系统，通过规范化的流程和专业的技术手段，保障系统稳定、可靠运行，有效支撑档案局各项业务的顺利开展。

- ① 配合新服务器上架、调试及迁移服务，操作系统、虚拟化平台、数据库安装部署和配置工作；
- ② 配合应用开发商，针对应用系统提供操作系统、虚拟化、数据库等技术支持和变更；
- ③ 升级病毒库，确保所有服务器及时更新到最新版本；
- ④ 定期每月对服务器操作系统升级安全补丁，确保操作系统无高危和中危漏洞，低危漏洞尽可能修补；
- ⑤ 定期每月做好服务器系统备份工作；
- ⑥ 解决服务器和相关系统日常技术故障，保障服务器平台安全稳定运行；
- ⑦ 每日检查小型机 VCS 集群状态，确保集群有效并运行正常。

3) 网络安全日常维护要求

- ① 配合新设备上架、配置、调试等工作；
- ② 定期升级安全设备病毒库，确保系统更新到最新版本；
- ③ 提供相应的交换机端口保护、广播风暴控制、端口快速启动、DHCP 检测、环路检测等系统优化建议；
- ④ 解决网络和安全系统日常技术故障，保障网络安全稳定运行；
- ⑤ 配合应用开发商，针对应用系统调整网络安全策略，包括访问控制，端口开放等；
- ⑥ 针对重点网络和安全设备，定期做好配置备份工作，设备日常日志检查，检查可疑日志并做好安全防护。



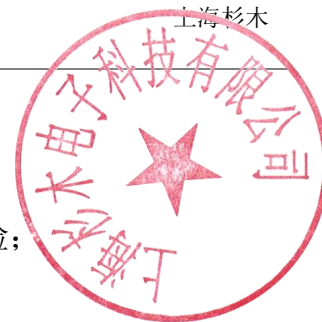
4) 虚拟化平台日常维护

- ① 对虚拟化平台软件提供软件升级服务，提供升级部署及支持服务，包括升级必要性评估、风险评估、升级报告等；
- ② 配合、保障应用开发商针对应用系统的调整和故障处理，为应用开发商提供稳定的虚拟化运行平台；
- ③ 虚拟化软件日常维护管理，包括状态检查、报错信息检查、用户管理、参数配置管理等工作；
- ④ 针对虚拟化软件运行情况，结合虚拟化系统的结构特点和具体应用特性，提供总体设计、规划咨询、系统重新部署服务；
- ⑤ 提供虚拟化平台故障处理、系统变更、系统优化、安全加固、重点保障、应急预案、性能分析等日常维护服务；
- ⑥ 虚拟化运行平台中的服务器、存储、交换机等硬件的日常维护管理，包括硬件配置信息管理、硬件变更调整、报错信息分析、协助硬件报修和 更换备件等；
- ⑦ 虚拟化软件的变更实施，包括新增应用系统虚拟机配置、虚拟机资源调整、参数及配置调整、软件包安装、打补丁和版本升级等；
- ⑧ 虚拟化软件的数据和系统备份、恢复、切换演练；
- ⑨ 配合虚拟化软件平台中应用系统的调整和日常维护；

5) 操作系统日常维护

提供操作系统技术支持服务，内容包括档案局 AD 域控服务器、DNS 服务器等 Windows Server 功能组件技术支持。

- ① 针对 AD、DNS、WSUS 等系统提供技术支持；
- ② 针对 Windows Server 系统漏洞和补丁提供技术支持；
- ③ 针对 Windows Server 系统提供系统修复技术支持。



6) 数据库软件服务

- ① 保障数据库软件的正常运行；
- ② 日常巡检，定期对数据库的运行状态进行现场巡检；
- ③ 对数据库的各个表空间进行监控；
- ④ 对数据的账户安全进行检查和审计；
- ⑤ 对数据库系统进行备份和数据恢复测试，保证备份数据的可用性。
- ⑥ 保障数据库软件的正常运行。

7) 备份服务

- ① 保障备份系统软件的正常运行；
- ② 提供备份策略的优化、更新服务；
- ③ 日常巡检，定期对备份状态进行现场巡检，对备份状态进行监控确认；
- ④ 对备份数据存储空间进行监控；
- ⑤ 提供备份数据恢复测试服务，保证备份数据的可用性；
- ⑥ 根据需求提供备份系统迁移服务，针对数据库提供日常数据备份和数据恢复等服务。

3.2.4. 系统健康检查

①系统日志检查分析：定期检查操作系统、数据库管理系统、中间件服务器等的系统日志记录，并针对错误日志信息、警告日志信息、提醒日志信息以及系统任务执行情况日志信息进行分析及后续处理；

②硬件系统的健康状况检查：针对硬件系统运行日志、运行性能、运行状态、运行错误进行检查及处理。

3.2.5. 机房工程

负责机房工程所含 5 个子系统的日常维护和定期健康巡检。机房运维中各子系统运维或巡检内容要求如下：

- ① 机房环境监控检查和维修：
 - ✓ 检查机房温湿度，根据机房温湿度及时消除机房工作环境存在的隐患。



- ✓ 检查机房门禁系统的运行状况。
- ✓ 检查机房漏水情况，根据报警排除故障隐患。
- ✓ 检查UPS实时监控数据，如发现UPS工作异常及时处理。
- ✓ 检查各个监控开关工作状态，如发现开关工作异常及时处理。
- ✓ 检查环境监控系统软件报警功能，每次巡检检查漏水报警功能，短信报警功能，防止异常报警时短信不能及时发出。

② UPS 检查维护：

- ✓ 现场及其外观检查。
- ✓ 设备显示屏报警信息检查。
- ✓ 风扇运转情况检查。
- ✓ 运行参数检查：输入电压电流、输出电压电流。
- ✓ 发现异常及时处理。
- ✓ 开关外观检查。
- ✓ 检测每路输出开关的电流并与以往数值比较。

③ 门禁设备检查维护：

- ✓ 检查门禁进出记录。
- ✓ 开关门状态。
- ✓ 进门刷卡和出门按钮功能。
- ✓ 发现异常及时处理。

④ 空调设备检查维护：

- ✓ 控制系统：检查显示单元是否正常，各设备参数是否正确，查看历史报警记录对报警内容进行分析消除隐患。
- ✓ 空气过滤器：检查空气过滤器。
- ✓ 加湿器。
- ✓ 发现异常及时处理。



⑤ 空调设备检查：

- ✓ 控制系统：检查显示单元是否正常，各设备参数是否正确，查看历史报警记录对报警内容进行分析消除隐患。
- ✓ 空气过滤器：检查空气过滤器。
- ✓ 加湿器进水。
- ✓ 发现异常及时处理。

3.2.6. 信息安全保障

① 提供保障系统信息安全的解决方案：要求提供有针对性的安全解决方案，对系统的整体环境、业务环节、核心数据环境以及终端安全环境制定一整套安全解决方案；并根据解决方案提供软硬件环境进行现场优化调整；

② 对系统做信息安全风险评估：对物理环境、主机系统、网络与通讯系统、数据库系统、网站系统、日志与统计报表、安全管理制度以及整体的信息安全系统进行全面的安全评估，识别出系统存在的风险，并提出相应的整改措施；我司在运维期内提供每年 4 次安全风险评估，并且每次都提供安全报告；

③ 提供安全通告服务：提供漏洞信息通告、安全威胁通告、安全事件通告，帮助档案局及时了解信息安全热点事件及安全威胁，及时做好安全防护措施；

④ 紧急安全事件的应急响应服务：为档案局提供紧急安全事件应急响应服务，把威胁和风险降到可接受程度；

⑤ 根据相关等级保护/分级保护的规定以及档案局的安全需求，协助档案局进行等级保护的定级、评审、整改、完成，定期对系统进行信息安全测评；

⑥ 负责提供完善的安全评估和安全解决方案，主要包括如下内容，并且依据评估可能存在的风险，进行相对应的安全整改。

⑦ 负责联系第三方安全评测单位，并安排组织相关的安全评测工作；

⑧ 负责根据第三方安全评测报告进行相关的安全加固工作。

3.2.7. 系统分析和优化

①我司将对系统运行状态、效率及潜在故障隐患进行全面评估与深度分析，精准识别系统存在的各类问题，并为决策提供数据支持与可行性解决方案。同时，提出系统性优化建议，以及有关系统配置和变更管理的专业改进措施，助力实现系统持续稳定和性能提升；

②结合操作系统、物理设备等资源，从应用层、中间件层、数据库层、操作系统层和硬件层等各个层面进行分析，定位系统瓶颈，提出性能运维、资源重组计划；

③我司将基于操作系统与物理设备等资源，从应用、中间件、数据库、操作系统及硬件等多个层面开展全面分析，精准定位系统瓶颈，并提出针对性的性能调优方案与资源重组计划，以提升系统整体运行效率和稳定性。

④在运维服务期内，我司将定期开展全面的系统分析与优化工作，每次服务均提供详尽的分析报告、可行优化建议及实施方案，助力系统持续稳定高效运行。

3.3. 服务进度计划

在项目实施阶段，我司项目团队将严格依据既定计划与规范流程，有序推进各项运维服务工作。该阶段的核心任务包括日常运维服务的具体执行以及服务管理体系的落实与持续优化。

日常运维服务将遵循周期性计划安排，按日、周、月、季度为循环单元，系统开展巡检、监控、备份、性能分析及故障处理等操作。每日进行基础状态检查与事件响应，每周执行系统性健康评估与日志审计，每月开展深度巡检与资源优化，每季度实施综合性能评估与总结规划，从而形成闭环、可持续的运维服务机制。

服务管理方面，我司将在项目启动初期即建立完整的服务管理流程和规范，包括事件管理、变更管理、配置管理及服务级别管理（SLA）等。在后续服务过程中，将结合信息系统的实际变更、业务需求变化及绩效反馈，定期对管理体

系进行审查、评估与迭代优化，确保运维服务始终贴合业务发展需要，实现服务质量持续提升。

通过结构化、周期化的服务安排与动态优化的管理机制，我司致力于在项目实施全过程中提供稳定、可靠、高效的运维服务支持。

3.3.1. 服务计划

通过对用户方信息系统提供全面而细致的日常运维服务，我司将致力于高效识别与处理服务范围内的各类安全故障及运行问题。在服务过程中，我们将严格执行故障响应与处理机制，对每一个问题的发现、分析、解决及验证过程实施全程详细跟踪与记录，确保所有操作可追溯、结果可评估。

依托部署成熟的监控工具与运维管理系统，我司将对系统运行状态实施7×24小时不间断监控，实时采集并分析性能数据与日志信息，以及时发现信息系统中的潜在风险与薄弱环节，实现从被动应对向主动预防的运维模式转变。在此基础上，通过不断总结和提炼最佳实践，我司将协助用户方规范系统的日常操作步骤与流程，明确操作权限与变更控制要求，显著降低因操作失误或管理疏漏导致的系统中断。

最终，通过上述系统性、规范化、全周期的运维服务，我司将全力保障用户方信息系统及其上层应用的连续性、稳定性与安全性，为业务开展提供坚实可靠的技术支撑。

3.3.2. 计划管理

为确保本次服务项目的顺利推进与高质量交付，我司项目组在全面梳理当前服务现状的基础上，结合项目实施目标，进行了系统性的分析和规划。我们明确了服务管理全过程中所需生成的各类文档清单，并制定了日常工作必须严格遵循的服务管理流程与规章制度，以形成规范化、标准化、可追溯的服务实施体系。

在文档体系方面，我司将编制并维护包括服务实施方案、日常运维记录、事件报告、变更申请、周期评估总结等在内的全套项目文档，确保每一项运维

活动均有据可查、所有操作过程清晰可追溯。在流程与制度层面，项目组将严格执行事件管理、问题管理、变更管理、配置管理及服务级别管理（SLA）等服务管理流程，同时遵循已在《运维服务管理规范》《安全管理制度》等文件中规定的操作准则，实现对服务过程的精细化控制和持续改进。

通过构建结构清晰、要求明确的文档与流程体系，我司旨在保障运维服务在受控、有序、高效的环境中运行，最终达成项目目标，为客户提供稳定、可靠、专业的技术服务支持。

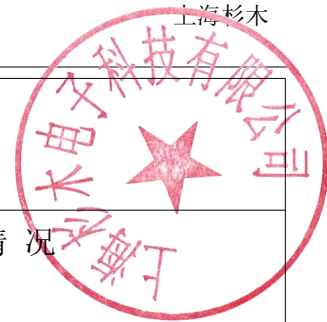
3.3.3. 时间计划及进度表

3.3.3.1. 时间周期

2025-12-12—2026-12-11（暂定，以实际时间为准）

3.3.3.2. 时间计划表

序号	时间	工作内容	阶段成果/完成进度
1	2025-11	项目启动	1、人员进场： 要求驻场工程师、高级运 维技术工程师、服务主管人员进场，召 开项目启动会，明确项目要求、沟通机 制和汇报机制（定期汇报、专题汇报、 应急汇报）等 2、根据合同和招投标要求， 细化工作内 容、落实人员工作职责和详细工作内容
2	2025-12月	系统彻查 系统备	对机房内现有软硬件设备进行整理和统 计，包括备件信息等，并且更新接口对 照表，系统拓扑图等新表单。 对现有所有系统虚拟化平台、数据库平 台、网络和安全设 备配置进行统一的备 份



		份 1	
3	2026-1	完 善 备 品备件	根据系统彻查结果，完善现有备件的情 况
4	2026-2	运 行 分 析 和 优 化 1	收集日常工作中的数据对系统进行评估 分析，并向用户反 馈可优化的空间。
		系 统 升 级 项 目 确 认	根据指定合同期间初步规划，将 2022-2023 系统优化升级的内容进行确 认，并准备相关的 方案
5	2026-3	安 全 评 估 1	根据等保（二级）指标进行安全评估， 并将不符合问题进 行整理，无法整改的 说明情况。
		系 统 升 级 改 造 方 案 制 定	根据年初计划将系统更新的方案进行提 交。
6	2026-4	系 统 备 份 2	对现有系统进行统一的备份
		系 统 健 康 巡 检 1	安排技术团队对档案局系统进行全方位 系统巡检。
7	2026-5	运 行 分 析 和 优 化 2	收集日常工作中的数据对系统进行评估 分析，并向用户反 馈可优化的空间。
		安 全 评 估 2	对日常安全信息进行整理分析。
		故 障 恢 复 演 练	选择演练内容，制定方案和计划对系统 进行故障恢复演练



		1	
		半年度用户满意度回访	进行半年度用户满意度回访，针对用户不满意内容提出整 改建议和措施
8	2026-6	系统更新设备的采购和确认	根据系统运行分析和优化方案、明确针 对本项目需要增加的软硬件配置,制定 详细的深化设计、实施和交付方案
		系统备份 3	对现有系统进行统一的备份
		系统健康巡检 2	安排技术团队对档案局系统进行全方位 系统巡检。
9	2026-7	系统升级改造 实施	严格按照项目流程进行实施,减少对用 户应用系统的影响。
		系统升级改造 实施,并使运行 观察	对系统升级改造后的进行使运行观察, 确保系 统的运行稳定
		运行分析和优化 3	可对新上线设备进行运行分析,并且在 已完成的 项目的前提下,对其他系统进 行优化。
		安全评估 3	
10	2026-8	系统备份 4	对现有系统进行统一的备份
		系统健康巡检 3	安排技术团队对档案局系统进行全方位 系统 巡检。
11	2026-9	安全测评	联系上海安全测评中心对档案局进行安 全评 估工作
		系统备份 5	对现有系统进行统一的备份
		故障恢复演练 2	选择演练内容,制定方案和计划对系统 进行故 障恢复演练
12	2026-10	运行分析和优化 4	

13	2026-11	安全评估 4	对全年的安全整改进行数据整理,并对 整体系统进行评估, 评估其安全性
		系统健康巡检 4	安排技术团队对档案局系统进行全方位 系统巡检。
		年度 kpi 考核	根据全年项目完成情况进行考核, 决定 项目是否进行验收
		年度验收	完成整个年度的运维工作并将验收文档 整理完毕。汇总一年来的故障记录, 并 注明用了多长时间解决。并将全年的工 作内容进行数据分析, 将档案局的整体 情况进行一个有效说明。

3.3.4. 实施内容

- 确定现场服务工程师工作内容、工作职责、工作范围及管理制度;
- 确定服务服务工程师技术要求、现场服务工程师工作流程与日常工作内容（日常机房工程巡检、日常设备巡检等）;
- 确定现场服务工程师与用户方接口与流程;
 - 确定事件管理文档与说明、以及故障的等级、分类、调查、分析、跟踪程;
- 确定故障升级与上报流程;
- 确定日常事件处理流程（按照故障等级进行划分）;
- 现场服务工程师服务内容、服务提交文档目录。



4. 信息系统支持平台【硬件平台】现状分析

4.1. 系统现状概述

浦东新区档案局信息系统支撑平台自2005年3月启动建设，于2007年3月通过专家评审并正式投入运行。该系统至今已持续稳定运行将近二十余年，取得了显著的应用成效，为全区档案信息化工作提供了坚实的底层支持。该平台承担浦东新区档案局所有数据应用系统的运行、计算、存储及备份任务，通过先进的计算机网络技术与系统集成方法，将客户机、应用服务、操作系统、数据库管理系统及前端开发工具等软硬件资源有机整合，构建了一个综合、分层、灵活且安全的信息系统运行环境。

档案局业务系统涵盖全面，主要包括：馆藏档案资源管理系统、接待服务利用平台、电子阅览室系统、档案编研系统、电子数据检测系统、统一认证平台、档案集成管理系统、BIM系统、签章系统、声像档案媒资系统、民生档案智慧服务、分级管理系统、OA系统、电子档案接收利用、数字档案室系统、区块链开放平台、教育培训管理、档案APP、微信公众号、互联网信息采集、监督执法与教育培训系统等。这些系统共同支撑起档案管理、公共服务、内部办公及信息发布的全面业务需求。

以实际应用需求为核心，浦东新区档案局构建了完整的信息化支撑硬件平台，该系统可分为硬件与软件两大部分。硬件系统包括网络设备、安全设备、服务器、监控设备以及存储备份设备等关键基础设施；软件系统则涵盖Solaris操作系统、Windows操作系统、Linux操作系统、VMware虚拟化软件、数据库系统、备份软件、监控平台软件及防病毒软件等重要组成部分。根据档案管理系统特点与信息安全密级要求，整个硬件平台划分为三个物理或逻辑隔离的网络区域：局域网、政务外网和因特网。

局域网作为档案核心业务承载网络，运行馆藏档案资源管理系统、接待服务利用平台、电子阅览室系统、档案编研系统、电子数据检测系统、统一认证平台、档案集成管理系统、BIM系统、签章系统及声像档案媒资系统等关键业务系统，是档案数据管理和利用的核心区域。政务外网作为主要办公网络，部署了民生档案智慧服务、分级管理系统、OA系统、电子档案接收利用、数字档案

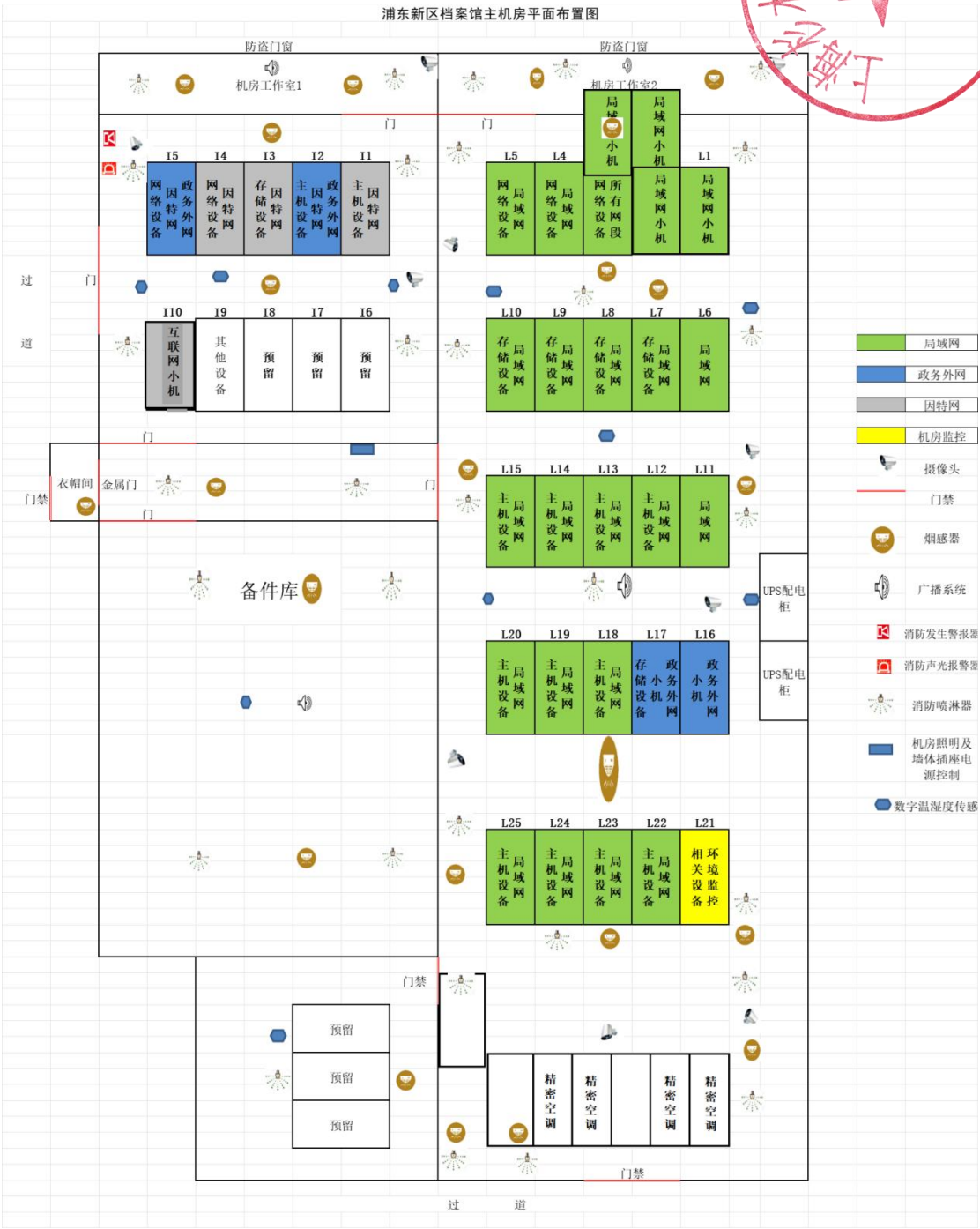
室系统等重要应用，支持日常行政与档案公共服务。因特网区域则主要为办公人员提供互联网接入服务，并运行教育培训管理、档案APP、微信公众号、互联网信息采集、监督执法与教育培训系统等面向公众的服务内容。

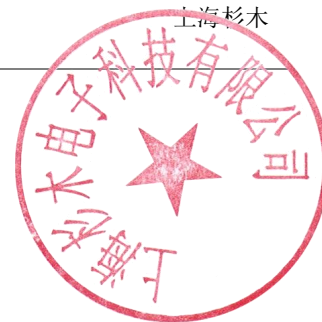
我司对该信息硬件平台具备全面而深入的了解，涵盖系统整体架构、各类设备使用状态、物理与逻辑连接关系以及详细配置信息等多个方面。无论是从全局架构还是局部子系统角度，均积累了丰富的技术认知与运维经验，能够为系统的持续稳定运行提供有力保障。

下文将就本次运维服务所覆盖的系统硬件设备进行详细列举，并对各系统设备的安装与配置情况作进一步说明。



4.2. 机房总平面图及区域划分





4.3. 硬件基础平台分析

4.3.1. 互联网平台

4.3.1.1. 概述

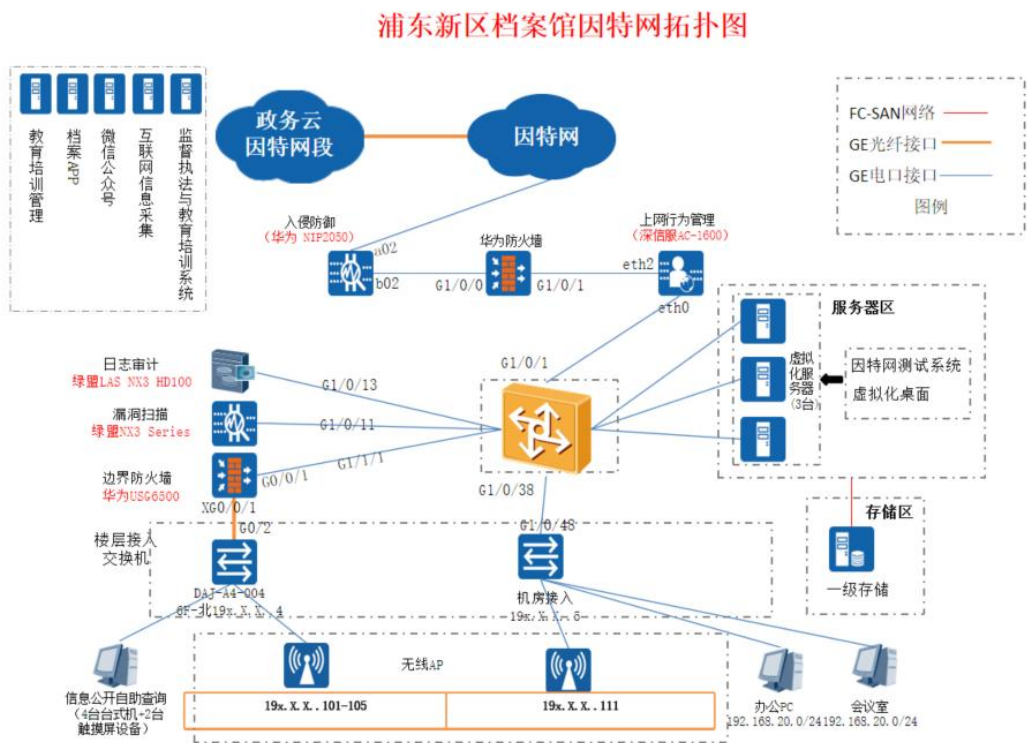
档案局因特网区域采用一台Cisco 3750交换机作为核心交换设备，承担该区域网络流量的汇聚与转发核心职能。上行链路通过专业安全设备链路由电信网络接入，具体依次经上网行为管理系统、智能防护系统及防火墙进行多层级安全过滤与策略控制后，最终与互联网服务提供商连接，出口总带宽为300M，为内部用户提供高速、安全的互联网访问通道。

下行连接则通过Cisco 2950接入层交换机及十多台无线AP设备，共同构建覆盖广泛的办公及公共服务网络。该网络架构有效支撑了档案局培训系统的各类用户、物业管理办公人员以及其他相关合作单位的多样化有线及无线接入需求，为其日常办公、在线学习及业务协同提供了稳定、可靠的网络环境。

4.3.1.2. 设备清单

序号	设备	描述	品牌	数量
1	Catalyst3750X-48	工作组交换机（48 口）	CISCO	1
2	HuaweiNIP2050	智能防护系统	华为	1
3	AC1300	上网行为管理	深信服	1
4	Catalyst2950G-48	工作组交换机（48 口）	CISCO	1
5	HuaweiUSG6650	因特网防火墙	华为	1
6	ECP216B	机架式光电转换器	Postel	1
7	ECS3	光电转换器（多模）	Postel	5
8	AP	无线	H3C	13
9	AC1300	因特网上网行为管理	深信服	1
10	LAS NX3 HD100	因特网日志审计	绿盟	1

4.3.1.3. 拓扑图



4.3.2. 政务网平台

4.3.2.1. 概述

档案局政务外网采用两台H3C S5560X 交换机进行堆叠，共同作为该区域的核心交换设备，在提升整体带宽与可靠性的同时，有效避免了单点故障，保障网络核心的高可用性。上行链路由IPS（入侵防御系统）、防火墙及一台Huawei S5700交换机，安全可靠地连接至浦东新区电子政务中心，建立起符合政务网络安全规范的外部互联通道。

下行通过多台Cisco 2950、H3C 5130S交换机和一台TPLink交换机共同构建接入层，为档案局内部办公电脑及相关终端设备提供稳定、高效的有线网络接入环境，支持日常电子政务、档案信息管理及协同办公等业务的开展。

此外，为确保与上级单位之间的数据传输安全，档案局部署了一台天融信VPN设备，与市档案局建立加密通信隧道。该链路有效保障了跨域档案查询及相关业务系统在与市局进行信息交互过程中的机密性和完整性，全面符合政务网络安全管理的政策与技术要求。

4.3.2.2. 设备清单

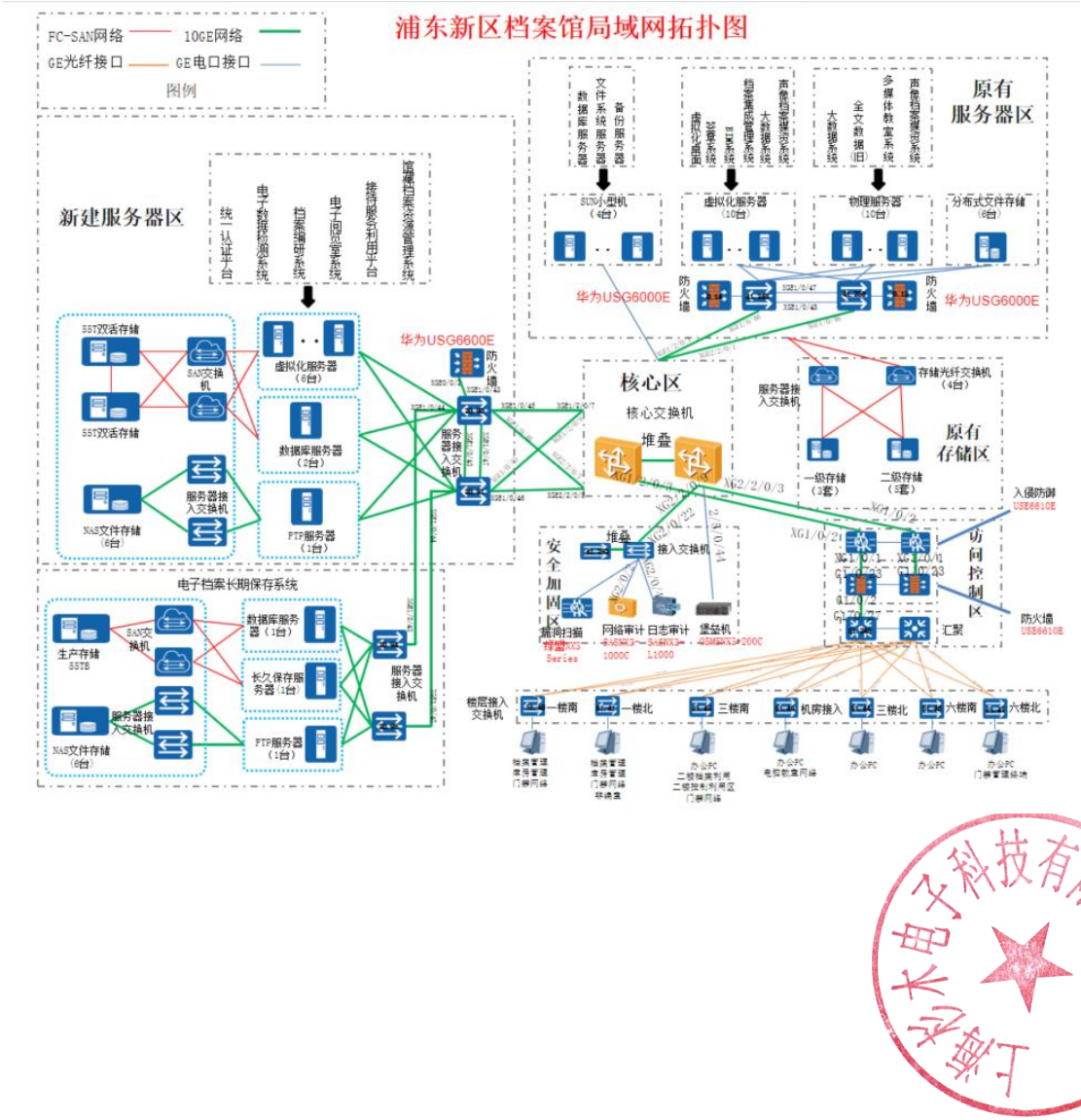
序号	设备	描述	品牌	数量
1	S5560X-52	工作组交换机（48 口）	CISCO	2
2	Catalyst2950G-48	工作组交换机（48 口）	CISCO	2
3	HuaweiS5700-24	华为交换机	华为	1
4	Catalyst2950G-24	工作组交换机（24 口）	CISCO	3
5	HuaweiS5700-48	楼层交换机	华为	1
6	H3CS5130S	楼层交换机	H3C	6
7	IPS	入侵防御设备	东软	1
8	USG5150	防火墙	华为	1
9	TPLINK-16	二层交换机	Tplink	1
10	VPN	跨馆查询加密机	天融信	1
11	LogbaseH530	政务外网安全审计	思福迪	1
12	LogbaseHS100	政务外网日志收集器探针	思福迪	1
13	天清汉马安全隔离	局域网与政务网网闸	启明星辰	1
14	AC1000-D600	政务外网上网行为管理	深信服	1
15	IPSEC/SSL VPN	政务外网跨馆查询加密机	天融信	1
16	S5731-S48T4X	政务外网接入交换机	华为	1

整体网络结构层次清晰、性能匹配合理，核心、汇聚与接入各司其职，共同构建了一个安全、稳定、可扩展的局域网环境，全面支持档案局关键业务的日常运行和数据传输需求。

4.3.3.2. 设备清单

序号	设备	描述	品牌	数量
1	H3C S7506E	局域网核心交换机	华三	2
2	H3C S5560X	局域网汇聚交换机	华三	2
3	H3C S5130S	局域网楼层交换机	华三	10
4	H3C S6520X	局域网安全加固区域接入交换机	华三	2
5	H3C F1050	局域网防火墙	华三	2
6	天清安全隔离与信息交换系统	局域网与政务外网网闸	启明星辰	1
7	NIPS NX-CH3330	局域网入侵防御	绿盟	2
8	RSAS NX3-X	局域网漏洞扫描	绿盟	1
9	SAS NX3 -L1000	局域网日志审计	绿盟	1
10	SAS NX3-1000C	局域网网络审计	绿盟	1
11	S5720S-28P	局域网服务器管理交换机	华为	2
12	OSMS NX3-200C	局域网运维安全网关堡垒机	绿盟	1
13	SNS2124	局域网光纤交换机	华为	2
14	Brocade G610	局域网存储区域光纤交换机	博科	4
15	CE6881-48S	局域网服务器、存储接	华为	10

4.3.3.3. 拓扑图



4.4. 系统支撑平台分析

4.4.1. 互联网系统

4.4.1.1. 服务器系统

服务器系统作为业务应用的承载基础,可进一步划分为小型机系统、x86 物理服务器系统及 x86 虚拟化服务器系统三类,共同支撑各类应用的差异化运行需求。

➤ 小型机系统

该系统包含一台 SUN F4800 小型机,其采用两域 (Domain) 架构设计,通过集群技术实现双机冗余,显著提升了系统的可靠性与业务连续性。该小型机主要用于数据库服务,是培训系统与分级管理系统的核心数据库服务器,为其提供稳定高效的数据处理能力。

➤ x86 物理服务器系统

档案局采用一台 Dell PowerEdge 6650 服务器作为专用的因特网监管平台服务器,用于运行监控及管理类应用,实现对网络状态与业务服务的实时监管。

➤ x86 虚拟化服务器系统

虚拟化集群由一台 Dell R510 与一台 Dell R720 服务器组成,通过 VMware 虚拟化技术整合物理资源,构建资源池化、弹性可扩展的虚拟平台。该环境共承载15台虚拟服务器,广泛支持分级管理系统应用服务器、培训系统应用服务器、市公共档案查询服务、因特网网盘系统、企业档案平台及测试系统等多种业务,在提高设备利用率、节约空间与能耗的同时,依托 VMware 高可用 (HA) 机制有效增强了服务的可靠性。

4.4.1.2. 存储系统

存储系统采用分级存储架构，根据不同业务数据的性能、可用性和备份需求进行合理布局，涵盖生产、近线备份与长期归档等多个层级。

- 一级存储：采用一台华为 S2600T 存储设备，总容量为 7TB，用于存放因特网分级管理系统和培训系统的生产数据库，并为虚拟化平台提供共享存储支持，保障关键业务的高性能访问与数据一致性。
- 二级存储：由四台 SUN ST3510 存储阵列组成，总容量3TB，用于存储两个核心数据库的周期性备份数据，起到近线容灾和快速恢复的作用。
- 三级存储：配备一台 SUN L8 磁带库，总容量3TB，用于实现各大应用系统的长期磁带备份，符合档案数据归档管理的规范要求，支持数据的离线保存和灾难恢复。

4.4.1.3. 备份系统

备份体系与存储架构紧密配合，通过华为S2600T、SUN3510阵列及L8磁带库构建了从在线生产、近线备份到离线归档的全周期数据保护链条，实现了数据的多副本、异质和分级保存策略，极大提升了数据灾害应对能力。

4.4.1.4. 数据库系统

档案局因特网区域核心数据库采用 Oracle9i 数据库系统，该数据库部署于高可用的 SUN F4800 小型机集群环境之上，主要支持因特网分级管理系统与培训系统两大关键业务。其负责所有档案元数据、用户信息及培训资料的结构化存储与管理，完成数据的增、删、改、查等核心操作，是上层应用稳定运行和数据安全的重要基石。

综上所述，该支撑平台通过服务器、存储、备份及数据库四大系统的有机协同，构建了一个结构合理、安全可靠、便于扩展的主机运行环境，为档案局因特网业务的持续稳定开展提供了坚实基础。

4.4.1.5. 设备清单

序号	设备型号	品牌	描述	数量	重要程 度
1	SUN F4800	SUN	因特网 Oracle 数据 库 及 文件服务器	1	关键
2	SUN 3510	SUN	因特网磁盘阵列	2	重要
3	DELL R910	DELL	因特网虚拟化资源 池	1	重要
4	DELL R720	DELL	因特网虚拟化资源 池	1	重要
5	DELL R720	DELL	因特网桌面虚拟化 服 务器	1	重要
6	华 为 S2600T	华为	因特网磁盘阵列	1	关键

4.4.1.6. 机柜图

T1-T5 机柜立面图					
U数	I1	I2	I3	I4	I5
38	24口配线架（背面）	24口配线架（背面）		24口配线架（背面）	3口光纤配架（单模） 24口配线架（背面）
37			华为S2600T 因特网光交换机		
36		华为S5700（背面） 192.168.60.15	华为S2600T 因特网光交换机	华为防火墙（60.90） 24口配线架（背面）	24口光纤配架（多模） 24口配线架（背面）
35					
34		网闸（背面）局域网地址： 192.168.3.242 政务外网地 址：192.68.24.2		因特网电话modem	24口配线架（背面） 3口光纤配线架（多模）
33				因特网华为防火墙	
32				深信服上网行为管理（因特网）	政务外网华为防火墙
31					托 盘
30			TA-DB（FT-B20） 天融信数据库审计	因特网核心交换机	政务外网接入交换机
29	政务网光典灵智平台				政务外网IP2（已使用）
28		托 盘			政务外网核心交换机（新）
27			Huawei S2600T 192.168.20.91	为智能防护系统（作用因特网IPS） 托 盘	政务外网核心交换机（新）
26					政务外网核心交换机（新）
25					政务外网核心交换机（新）
24					政务外网核心交换机（新）
23					政务外网核心交换机（新）
22	因特网虚拟化资源池 I-ESX-R720	市局民生档案利用系统前置 机	SUN-3510-1-JBOD（型号		政务外网核心交换机（新）
21	托 盘		I-SUN-3510-1	托 盘	深信服上网行为管理
20					
19					
18					
17					
16	因特网桌面虚拟化 I-HUAWEI-R720 192.168.70.115（暂时停用）	政务网堡垒机 E-ESX-R730 192.168.60.153	I-SUN-3510-2	因特网绿盟日志审计 LAS NX3	天融信VPN 192.68.16.43
15	托 盘		I-SUN-3510-2-JBOD	政务网绿盟日志审计 LAS NX3	天融信VPN（已不使用）
14		政务外网虚拟化资源池 E-ESX-R730 192.168.60.240	托 盘		
13	因特网虚拟化资源池 I-ESX-R910 192.168.70.242	政务外网虚拟化资源池 E-ESX-R720 192.168.60.241			
12				英特尔网华为防火墙	铜缆配线架
11	托 盘		托 盘		铜缆配线架
10				托 盘	铜缆配线架
9					铜缆配线架
8	配架：6*LC				铜缆配线架
7	托 盘				铜缆配线架
6					铜缆配线架
5					铜缆配线架
4	10口配架：10*10/100 E	10口配架：10*10/100 E			铜缆配线架
3					铜缆配线架
2					铜缆配线架
1			配架：8*LC		铜缆配线架

I6-I10 机柜立面图						
U数	I6	I7	I8	I9	I10	U数
38					I-SUN-D240-B	38
37						37
36					I-SUN-D240-A	36
35						35
34						34
33						33
32						32
31						31
30						30
29						29
28						28
27						27
26					I-SUN-L8-1	26
25						25
24						24
23						23
22				托盘		22
21				IBM 显示器	文件系统及备份服务器 (集群)	21
20			Lenovo x3850 X6		I-FS-F4800-1(域A)	20
19					192.168.20.6	19
18						18
17				IBM X3850 M2	数据库服务器(集群)	17
16					I-ORA-F4800-2(域B)	16
15					192.168.20.7	15
14						14
13				IBM X3850 M2		13
12						12
11						11
10						10
9						9
8						8
7				IBM 外接光驱		7
6				托盘	托盘	6
5					预留	5
4				H3C S1016R	预留	4
3					预留	3
2					预留	2
1				光纤配线架	预留	1

4.4.1.7. 接口互联表

I1						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
I-ESX-R510	51e1	I1-1	I1-1	E-01	Cisco 3750	I4
I-JK-6650-1	66e1	I2-5	I2-5		Cisco 3750	I4
I2						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
I-DATA-2850-1	28e1	I2-4	I2-4		Cisco 3750	I4
I-WEB-6650-1	66e1	I2-2	I2-2	E-04	Cisco 3750	I4
I3						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
I-SUN-3510-1	35d1			35j1	I-SUN-3510-1-JBOD	I3
	35d2			35j2	I-SUN-3510-1-JBOD	I3
	35u1			b1	I-BROCADE-3250-1	I3
	35u2			b1	I-BROCADE-3250-2	I3
	35u3			b2	I-BROCADE-3250-1	I3
I-SUN-3510-1-JBOD	35u4			b2	I-BROCADE-3250-2	I3
	35j1			35d1	I-SUN-3510-1	I3
	35j2			35d2	I-SUN-3510-1	I3
I-SUN-3510-2	35d1			35j1	I-SUN-3510-2-JBOD	I3
	35d2			35j2	I-SUN-3510-2-JBOD	I3
	35u1			b5	I-BROCADE-3250-1	I3
	35u2			b5	I-BROCADE-3250-2	I3
	35u3			b6	I-BROCADE-3250-1	I3
I-SUN-3510-2-JBOD	35u4			b6	I-BROCADE-3250-2	I3
	35j1			35d1	I-SUN-3510-2	I3
	35j2			35d2	I-SUN-3510-2	I3

I-Brocade-3250-11	b0	I3-1, 2	I10-1 I10-2	f1	I-FS-F4800-1 (域A)	I10
	b1			35u1	I-SUN-3510-1	I3
	b2			35u3	I-SUN-3510-1	I3
	b3			1	I-Brocade-3250-21-1	I3
	b4	I3-5, 6	I10-5 I10-6	f1	I-ORA-F4800-2 (域B)	I10
	b5			35u2	I-SUN-3510-2	I3
	b6			35u4	I-SUN-3510-2	I3
I-Brocade-3250-12	b0	I3-3, 4	I10-3 I10-4	f2	I-FS-F4800-1 (域A)	I10
	b1			35u1	I-SUN-3510-1	I3
	b2			35u3	I-SUN-3510-1	I3
	b3			1	I-Brocade-3250-22-1	I3
	b4	I3-7, 8	I10-7 I10-8	f2	I-ORA-F4800-2 (域B)	I10
	b5			35u2	I-SUN-3510-2	I3
	b6			35u4	I-SUN-3510-2	I3
I-Brocade-3250-21	b0			3	I-Brocade-3250-11-3	
	b1					
	b2					
	b3					
	b4					
	b5					
	b6			F1	R720	I1
I-Brocade-3250-22	b0			A0	S2600T	
	b1			3	I-Brocade-3250-12-3	
	b2					
	b3			F2	R720	I1
	b4					
	b5					
	b6					
I-Brocade-3250-22	b7			B0	S2600T	

I10 (SUN SF-CAB)						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
D240 (域B)	SCSI-1			42s1	I-ORA-F4800-2 (域B)	I10
	SCSI-2					
D240 (域A)	SCSI-1			42s1	I-FS-F4800-2 (域A)	I10
	SCSI-2					
I-Sun-L8-1	8L1					
I-FS-F4800 (域A)	x4e1	I10-1	I10-1	E-05	Cisco 3750	I4
	x4e2	I10-2	I10-2	E-06	Cisco 3750	I4
	f1	I10-1 I10-2	I3-1, 2	b0	I-BROCADE-3850-1	I3
	f2	I10-3 I10-4	I3-3, 4	b0	I-BROCADE-3850-2	I3
	(f1和f2冗余)	I10-9 I10-10	I3-9, 10		光纤配架	I5
	(f1和f2冗余)	I10-11 I10-12	I3-11, 12		光纤配架	I5
	42s1				240介网盘	I10
	42s2					
	44e1			44e1	I-ORA-F4800-2 (域B)	I10
	44e2			44e2	I-ORA-F4800-2 (域B)	I10
	44e3					
	44e4					
I10 (SUN SF-CAB)						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
I-ORA-F4800 (域B)	x4e1	I10-1	I10-1	E-05	Cisco 3750	I4
	x4e2	I10-2	I10-2	E-06	Cisco 3750	I4
	f1	I10-1 I10-2	I3-1, 2	b0	I-BROCADE-3850-1	I3
	f2	I10-3 I10-4	I3-3, 4	b0	I-BROCADE-3850-2	I3
	(f1和f2冗余)	I10-9 I10-10	I3-9, 10		光纤配架	I5
	(f1和f2冗余)	I10-11 I10-12	I3-11, 12		光纤配架	I5
	42s1				240介网盘	I10
	42s2					
	44e1			44e1	I-ORA-F4800-2 (域B)	I10
	44e2			44e2	I-ORA-F4800-2 (域B)	I10
	44e3					
	44e4					
	s1			8L1	I-Sun-L8-1	I10
	s2					

4.4.1.8. 设备使用情况

互联网					
序号	设备	服务器名称	IP地址	机柜号	安装配置情况
1	I-FS-F4800-1(域A)	文件系统及备份服务器（集群）	10.1.1.6	I10	Solaris9.0 64 bit 操作系统、Veritas Storage Foundation v4.0、Veritas Cluster Server v4.0、Veritas Cluster Server Oracle Agent v4.0、NBU Master Server、NBU Oracle Agent、NBU Tape Support、oracle9.0数据库
2	I-ORA-F4800-2（域B）	数据库服务器（集群）	10.1.1.7	I10	Solaris9.0 64 bit 操作系统、Veritas Storage Foundation v4.0、Veritas Cluster Server v4.0、Veritas Cluster Server Oracle Agent v4.0、NBU Client、NBU Oracle Agent、oracle9.0数据库
3	I-ESX-R510	虚拟机资源池	10.1.1.8	I1	Vmware 5.1
4	I-ESX-R720	虚拟机资源池	10.1.1.9	I1	Vmware 5.5
		市档案公开查询服务器	10.1.1.2		Windows Server 2003 中文标准版操作系统
		培训管理系统服务器	10.1.1.5		Windows Server 2003 中文标准版操作系统、NBU Client、Weblogic
		分级管理系统应用及数据库	10.1.1.8		Windows Server 2003 中文标准版操作系统
		互联网网盘系统	10.1.1.16		Windows Server 2008 中文标准版操作系统
		互联网企业档案公开系统	10.1.1.17		Windows Server 2008 中文标准版操作系统
5	I-JK-8650	监控服务器	10.1.1.4	I1	Windows Server 2003 中文标准版操作系统、Broadview NCC网络监控、Broadview NCC网络监控



4.4.2. 政务网系统

档案局政务外网主机支撑平台系统作为支撑政务协同与公共服务的关键信息基础设施，整体架构涵盖服务器系统、存储系统、备份系统及数据库系统四大核心组成部分。该系统以高可靠、高可用和数据安全为设计原则，为政务外网多项关键业务提供稳定、高效的运行环境。

4.4.2.1. 服务器系统

服务器系统作为各类政务应用的承载基础，结合不同业务的性能与可靠性需求，划分为小型机系统、x86 物理服务器系统及 x86 虚拟化服务器系统三类，共同构建了层次分明、资源集约的算力支撑体系。

➤ 小型机系统

该系统包括两台 SUN V880 小型机，通过集群技术实现双机热备，显著提升了系统的业务冗余与故障切换能力。该小型机集群作为核心数据库服务器，主要为分级管理系统提供高性能、高可用的数据服务支持。

➤ x86 物理服务器系统

档案局采用一台 Dell PowerEdge R710 服务器作为专用的监管平台服务器，用于实时监控政务外网各项业务的运行状态及网络连通质量，实现对系统健康度的全面感知与管理。

➤ x86 虚拟化服务器系统

虚拟化集群由一台 Dell R730 和一台 Dell R720 服务器共同构建，依托 VMware 虚拟化技术实现计算资源的池化与动态调度，显著提升资源利用率并降低物理设备数量与能耗。通过 VMware 高可用（HA）机制进一步保障业务连续性。

➤ 该平台目前共运行16台虚拟服务器，按功能划分包括：

2台用于电子政务 OA 系统的应用及数据库服务；

2台支撑分级管理系统的应用及全文数据服务；

1台作为档案局域控服务器；1台为签章系统服务器；

1台运行自助查档系统；

1台作为市局公共查询服务器，通过天融信 VPN 实现与市档案局的安全数据交互；

2台面向企业用户提供企业档案系统及网盘服务；

2台用于防病毒管理中心和 WSUS 补丁分发服务；

其余3台为虚拟化基础组件，分别承担数据库、Web Client 管理及 VMware VDP 备份功能。

4.4.2.2. 存储系统

存储系统采用明确的分级策略，根据不同数据的访问频率、性能及保护要求构建了多层次存储架构，实现资源优化与成本效益的平衡。

➤ 一级存储：采用一台华为 S2600T 存储阵列，总容量9TB，用于存放政务外网各大业务系统的生产数据，为关键应用提供高性能、低延迟的数据存取服务。

➤ 二级存储：包括一台 Dell MD3600f 存储阵列（容量6TB）和两台 SUN ST3510 存储阵列（总容量2TB）。Dell 存储主要用于存放分级管理系统的全文备份数据及各虚拟机的备份映像；SUN 存储则专用于存储分级管理系统数据库的备份数据，共同构成近线备份资源池。

➤ 三级存储：配置一台 SUN L8 磁带库，总容量3TB，用于实现政务外网各大系统的长期磁带归档与灾难恢复支持，符合数据长期保留的合规性要求。



4.4.2.3. 备份系统

备份体系与存储架构紧密协同，依托各级存储设备及磁带库构建了从在线生产到近线备份、离线归档的完整数据生命周期管理方案，实现了关键业务数据的多副本、跨介质与异地的保护策略，极大增强了数据的灾难恢复能力。

4.4.2.4. 数据库系统

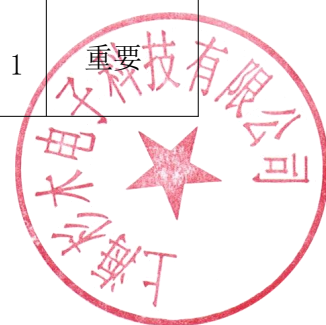
档案局政务外网核心数据库系统采用 Oracle 10g 数据库，该数据库部署于高可用的 SUN V880 小型机集群之上，主要为分级管理系统提供数据服务。其负责档案数据的全面管理，包括数据的写入、更新、查询及事务处理，是保障政务外网核心业务连续性和数据一致性的关键基础。

综上所述，档案局政务外网主机支撑平台通过服务器、存储、备份及数据库四大系统的有机整合与协同工作，构建了一个结构清晰、安全可靠、易于扩展的整体运行环境，有效支撑了政务外网各项业务的稳定、高效运行。



4.4.2.5. 设备清单

序号	设备型号	品牌	描述	数量	重要程度
1	SUN V880	SUN	政务外网文件系统 及备份服务器	1	关键
2	SUN V880	SUN	政务外网 Oracle 数据库服务器	1	关键
3	SUN 3510	SUN	政务外网备份阵列	2	重要
4	IBM 4700	IBM	政务外网磁盘阵列	1	重要
5	IBM 4000 (Exp810)	IBM		1	重要
6	IBM 4000 (Exp810)	IBM		2	重要
7	DELL R720	DELL	政务外网虚拟化资源池	1	重要
8	DELL MD3600f	DELL	政务外网磁盘阵列	1	关键
9	华为 S2600T	华为	政务外网磁盘阵列	1	关键
10	DELL R730	DELL	政务外网虚拟化资源池	1	重要
11	DELL R730	DELL	政务外网桌面虚拟化服务器	1	重要
12	TaiShan 200K 2280K (2*32核)	华为	市局民生档案利用系统（跨馆查询）前置机	1	重要



4.4.2.6. 机柜图

L16-L20 机柜立面图						
U数	L16	L17	L18	L19	L20	U数
38						38
37						37
36					华为防火墙USG6610E	36
35			华为S5720S-28P	Brocade G610光纤交换机	托盘	35
34					华为防火墙USG2601E	34
33				Brocade G610光纤交换机	托盘	33
32			华为CE6881-48S6CQ		华为CE6881-48S6CQ	32
31		E-DELL-MD3600F				31
30			华为CE6881-48S6CQ		华为CE6881-48S6CQ	30
29						29
28						28
27				华为K22K-02		27
26	Huawei 2600T	E-SUN-3510-1-JBOD				26
25		E-SUN-3510-1		华为K22K-02		25
24		托盘				24
23	E-SUN-L8-1 (已报废)		华为K22R-02	华为K22K-02		23
22						22
21			华为K22R-02			21
20						20
19			华为K22R-02			19
18				华为K22K-02		18
17						17
16	Oracle数据库服务器	文件系统及备份服务器	华为K22R-02		华为K22K-02	16
15	E-FS-V880-1	E-ORA-V880-2		华为K22K-02		15
14	192.68.16.6	192.68.16.7	华为K22R-02		华为K22K-02	14
13				华为K22K-02		13
12			华为K22R-02		华为K22K-02	12
11						11
10			华为K22R-02		华为K22K-02	10
9				SPE36C0225		9
8						8
7			华为K22R-02		SPE36C0225	7
6	托盘	托盘				6
5	政务外网光纤交换机			DAE62525U2-10		5
4	(10.77.77.77)					4
3	政务外网光纤交换机	12口铜缆配线架	6口铜缆配线架	12口铜缆配线架	DAE62525U2-10	3
2					预留	2
1				预留	预留	1

4.4.2.7. 接口互联表

L16						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
Huawei2600T	AP0			b4	SNS2124-1	L16
	BP0			b7	SNS2124-2	L16
	MGMT	L17-2	L17-2	E-29	Cisco 3750	L16
E-Sun-L8-1	8L1			s1	E-FS-V880-1	L16
	v1			b0	SNS2124-1	L10
	v2			b0	SNS2124-2	L10
E-FS-V880-1	v3e1	L16-1	L16-1	E-23	Cisco 3750	I5
	v3e2	L16-2	L16-2	E-24	Cisco 3750	I5
	v3e3	L16-2	L16-2	E-24	Cisco 3750	I5
	x4e1			x4e1	E-ORA-V880-2	I7
	x4e2			x4e2	E-ORA-V880-2	I7
	x4e3					
	x4e4					
	s1			8L1	Sun L8	I7
SNS2124-1	b0			v1	E-FS-V880	
	b1			v1	E-ORA-V880	L1
	b2			35u1	E-SUN3510	L17
	b3			35u3	E-SUN3510	L17
	b4			AP0	Huawei2600T	L16
	b5			91f1	E-ESX-R730	L18
	b6			72f1	E-ESX-R720	L19
	b7			36f1	MD3600f	L17
	b8					
	b9					
	b10					
	h11					

4.4.2.8. 设备使用情况

政务外网					
序号	设备	服务器名称	IP地址	机柜号	安装配置情况
1	E-FS-V880-1	文件系统及备份服务器（集群）		L16	Solaris9.0 64 bit 操作系统、Veritas Storage Foundation v4.0、Veritas Cluster Server v4.0、Veritas Cluster Server Oracle Agent v4.0、NBU Master Server、NBU Oracle Agent、NBU Tape Support、oracle9.0数据库
2	E-ORA-V880-2	数据库服务器（集群）		L17	Solaris9.0 64 bit 操作系统、Veritas Storage Foundation v4.0、Veritas Cluster Server v4.0、Veritas Cluster Server Oracle Agent v4.0、NBU Client、NBU Oracle Agent
4	E-ESX-R730	虚拟化资源池		L19	vmware 5.5
5	E-ESX-R720	虚拟化资源池		L19	
		OA系统数据库服务器			Windows Server 2003 中文标准版操作系统、IIS6.0、NBU Client、目录中心系统软件
		OA系统应用服务器			Windows Server 2003 中文标准版操作系统、IIS6.0、NBU Client、目录中心系统软件
		WSUS 补丁服务器			Windows Server 2008 中文标准版操作系统
		域控服务器			Windows Server 2008 中文标准版操作系统
		网盘系统			Windows Server 2008 中文标准版操作系统
		防病毒服务器			Windows Server 2008 中文标准版操作系统
		分级管理系统民生档案服务器			Windows Server 2008 中文标准版操作系统
		市局VPN服务器			Windows Server 2008 中文标准版操作系统
		分级管理系统应用服务器			Windows Server 2003 中文标准版操作系统、IIS6.0
		企业档案服务器			Windows Server 2008 中文标准版操作系统
		政务外网档案服务器			Windows Server 2008 中文标准版操作系统
		自主备份系统			Windows Server 2008 中文标准版操作系统
		VMware vcenter服务器			Windows Server 2008 中文标准版操作系统
		VMware数据库服务器			Windows Server 2008 中文标准版操作系统、SQL 2005
		VMware vdp备份服务器			VMware vdp系统
		VMware web-client服务器			Windows Server 2008 中文标准版操作系统
5	E-JK-R710	监控服务器		I2	Windows Server 2003 中文标准版操作系统、Broadview NCC网络监控、Broadview应用监控



4.4.3. 局域网系统

档案局局域网主机支撑平台系统作为支撑档案核心业务的基础设施，体系完备、技术多元，涵盖服务器系统、存储系统、备份系统及数据库系统四大核心组成部分。该系统基于高可靠、高可用及数据安全的设计目标，构建了层次清晰、资源集约、兼顾传统与创新的技术架构，全面支持档案管理与服务业务的开展。

4.4.3.1. 服务器系统

服务器系统作为各类档案核心应用的运行载体，按技术架构和功能定位，可分为小型机系统、x86 物理服务器系统、x86 虚拟化服务器系统及国产化服务器系统四类，共同构建了灵活可靠、资源可动态调配的计算环境。

➤ 小型机系统

该系统包括两台 SUN F4800 小型机，以集群方式部署，实现系统级冗余与故障自动切换，显著提升核心数据库服务的连续性与处理能力。该集群作为档案信息集成管理系统的核心数据库服务器，承担关键结构化数据的处理与管理任务。

➤ x86 物理服务器系统

档案局采用多台 Dell 服务器承担各类专用物理服务角色，具体包括：

1 台 Dell R410 服务器，作为全文数据服务器；

2 台 Dell PowerEdge 6650 服务器，其中一台运行档案利用系统（为档案信息集成管理系统的子系统），另一台作为局域网 U 盘接入管理服务器，实施外接设备安全管控；

1 台 Dell R710 服务器，作为监管平台服务器，全面监控局域网内业务运行状态与网络连通质量。

➤ x86 虚拟化服务器系统

虚拟化资源池由 5 台物理服务器构建而成，包括 1 台 Dell R510、1 台 IBM x3650、2 台 Dell R710 及 1 台 Dell R730，均采用 VMware 虚拟化



技术进行资源整合，显著提升资源利用率，降低运维复杂度，并通过 VMware 高可用（HA）等技术增强业务弹性与安全性。该平台共运行 43 台虚拟服务器，按业务功能可分为：

10 台服务于档案信息集成管理系统，承担应用及文件服务，支持档案查询、整理与开发利用；

2 台用于分级管理系统的应用及数据库服务；

1 台为电子文件中心系统服务器；

1 台为文档一体化系统服务器；

3 台提供基础架构服务，分别作为域控服务器、防病毒管理中心和 WSUS 补丁服务器；

3 台作为 VMware 平台与华为 FusionStorage 分布式存储的中间服务节点，实现虚拟化平台对分布式存储资源的访问；

其余为 vCenter 及相关管理组件服务器，保障虚拟化环境稳定运行。

➤ 国产化服务器系统

为适应技术自主可控趋势，局域网中新规划两个服务器区及一个 SM 单机区：

➤ 局域网服务器区：包含一组数据库服务器、一组虚拟化服务器、一组 FTP 服务器、一组双活存储及一组文件存储，并通过大缓存数据中心交换机与核心区互联，保障高效数据交换与业务连续性。

➤ 长久保存系统服务器区：包含一组数据库服务器、一组长久保存服务器、一台 FTP 服务器、一组生产存储和一组文件存储。该区域因业务特殊性，侧重内部数据交换，通过数据中心交换机内部互联，暂不与核心区连接，确保数据安全与流程隔离。

4.4.3.2. 存储系统

存储系统采用明确的分级策略，构建了涵盖生产、备份及归档的多层次存储体系，以满足不同业务数据的性能、容量与保护需求。

- 一级存储：采用 4 台 IBM DS4700 存储阵列，总容量 13.6TB，用于存放局域网全文数据等核心生产数据，为高频访问业务提供高性能存储支持。
- 二级存储：包括 3 台华为 S5600T 存储（SAS 盘容量 4.4TB，用于系统生产数据；SATA 盘容量 34TB，用于周期性备份）、5 台 SUN 3510 存储阵列（总容量 2.5TB）及 1 台 Dell MD1200i 存储阵列（容量 9.86TB），共同作为近线备份存储，分别存放数据库及全文数据的定期备份，确保故障时快速恢复。
- 三级存储：配置 1 台 SUN L100 磁带库，总容量 30TB，用于实现各大系统的长期磁带归档与灾难备份，满足数据长期保留和合规性要求。

4.4.3.3. 备份系统

备份体系与存储架构紧密协同，通过多级存储与磁带库结合，构建了从在线生产到近线备份、离线归档的完整数据保护链路，实现了关键业务数据的多副本、跨介质保护与快速恢复机制。

4.4.3.4. 数据库系统

档案局局域网核心数据库采用 Oracle9i 数据库系统，该数据库部署于高可用的 SUN F4800 小型机集群环境之上，是档案信息集成管理系统的核心数据管理平台，负责所有档案数据的增、删、改、查及事务管理，保障了业务系统数据的一致性与完整性。

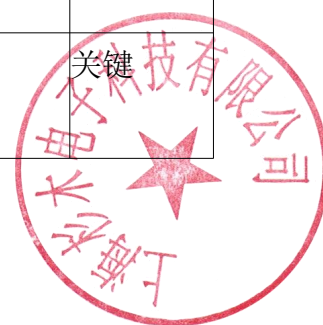
综上所述，档案局局域网主机支撑平台通过有机整合服务器、存储、备份及数据库四大系统，并引入国产化技术路线，构建了一个技术先进、安全可靠、可持续演进的IT基础环境，为档案业务的数字化转型和长期发展提供了坚实支撑。

4.4.3.5. 设备清单

序号	设备型号	品牌	描述	数量	重要程度
1	SUN F4800	SUN	局域网文件系统及备份 服务器	1	关键
2	SUN F4800	SUN	局域网 Oracle 数据库 服务器	1	关键
3	DELL 6650	DELL	局域网档案利用服务器	1	一般
4	DELL 6650	DELL	局域网介质管理服务器	1	一般
5	SUN 3510	SUN	局域网数据备份阵列	4	重要
6	TS-439Pro	QNAP	局域网数据离线备份 NAS	1	一般
7	DELL R710	DELL	局域网虚拟化资源池	2	重要
8	IBM x3650M3	IBM	局域网虚拟化资源池	1	重要
9	DELL R510	DELL	局域网虚拟化资源池	1	重要
10	DELL MD1200	DELL	局域网全文数据备份阵 列	1	重要
11	DELL R420	DELL	惠南办公点馆库系统服 务器	1	关键
12	DELL MD3200i	DELL	惠南办公点馆库系统磁 盘阵 列	1	关键
13	DELL R410	DELL	局域网全文数据备用服 务器	1	重要
14	华为 S5600T	华为	局域网磁盘阵列	1	关键
15	华为 S5600T	华为	局域网磁盘阵列	1	关键
16	定制阵列	定制	局域网全文数据备份阵 列	1	一般

17	定制磁盘阵列 (SMARTOR I160)	德拓	局域网媒资系统二级存储	1	一般
18	CF60	DELL	多媒体教室系统服务器	1	一般
19	Huawei RH2288V3	华为	局域网分布式存储服务 器	3	关键
20	DELL R730	DELL	局域网桌面虚拟化服务 器	2	重要
21	Huawei RH2288HV3	华为	局域网分布式存储服务 器	1	关键
22	DELL R730	DELL	统一数据支撑平台节点	1	重要
23	DELL R730	DELL	媒资服务器	5	重要
24	TS-1231XU-RP	QNAP	NAS 网络存储器	1	一般
25	Huawei RH2288HV3	华为	局域网分布式存储服务 器	2	关键
26	DELL R730	DELL	门禁系统服务器	1	重要
27	DELL R730	DELL	统一数据支撑平台节点	1	重要
28	DELL R730	DELL	统一数据支撑平台节点	2	重要
29	DELL R730XD	DELL	档案全文数据备份大容量服 务器	1	重要
30	Huawei RH2288H V3	华为	局域网分布式存储节点	1	关键
31	DELL R730	DELL	虚拟化环境备份服务器	1	重要
32	TaiShan200K	华为	局域网数字档案馆系统 虚拟6	6	重要

	Model 2280K		化服务器		
33	TaiShan200K Model 2280K	华为	局域网数字档案馆系统 数据 库服务器	2	重要
34	TaiShan200K Model 2280K	华为	局域网数字档案馆系统 FTP 服务器	1	重要
35	TaiShan200K Model 2280K	华为	局域网数字档案馆系统 长久 保存服务器	1	重要
36	TaiShan200K Model 2280K	华为	局域网数字档案馆系统 长久 保存数据库服务器	1	重要
37	TaiShan200K Model 2280K	华为	局域网数字档案馆系统 长久 保存 FTP 服务器	1	重要
38	TaiShan200K Model 2280K	华为	数字档案馆系统保密区 服务 器	1	重要
39	Oceanstor 5210 Enhanced	V5 华为	局域网数字档案馆系统 存储 (阵列+控制柜)	2	关键
40	Oceanstor 5210 Enhanced	V5 华为	局域网数字档案馆系统 长久 保存 (阵列+控制 柜)	1	重要
41	Oceanstor 9000 V5	华为	局域网数字档案馆系统 分布 式 NAS 存储	2	关键



4.4.3.6. 机柜图

L1-L5 机柜立面图					
U数	L1	L2	L3	L4	L5
38	L-SUN-D240-1	L-SUN-D240-2	局域网华为防火墙	汇聚交换机（主） 24口配线架（背面）	24口配线架（背面）
37			局域网华为防火墙	汇聚交换机（备） 24口配线架（背面）	光纤配线架
36					24口配线架（背面）
35			NIPS NX Series	24口配线架（背面）	光纤配线架
34				H3C S7506E交换机 局域网核心交换机	24口配线架（背面）
33			NIPS NX Series		
32					
31					
30					
29					
28					
27	托盘	托盘	TPLink-TLSG-1016DT 交换机		
26			Cisco-2950-48-EI 交换机		
25			Huawei-S5700 交换机		
24					
23			RSAS NX3 Series		
22					
21			SAS NX3 Series	安全接入交换机（主）	安全接入交换机（备）
20				托盘	托盘
19	L-FS-F4800-1	L-ORA-F4800-2	SAS NX3 Series	FC-AS02	FC-AS01
18	Oracle 数据库服务器	文件系统及备份服务器		铜缆配线架	铜缆配线架
17	Sun-F4800 小型机	Sun-F4800 小型机	绿盟运维安全网关	铜缆配线架	铜缆配线架
16	5	7		铜缆配线架	铜缆配线架
15				铜缆配线架	铜缆配线架
14					
13					
12					
11					
10					
9					
8					
7					
6	托盘	托盘	铜缆配线架		
5	预留	预留		托盘	
4	预留	预留			
3	预留	预留	铜缆配线架	托盘	电话配线架
2	PDU-1	PDU-2			
1					

L6-L10 机柜立面图					
U数	L6	L7	L8	L9	L10
38			24口配线架（背面）		
37				华为SNS2124（背面）	
36				华为SNS2124（背面）	
35					
34					
33					
32					
31	QNAP		HuaWei S5600T硬盘柜		
30					
29					QNAP（）
28					托盘
27					
26					
25					
24		IBM DS4700	HuaWei S5600T控制柜		L-SUN-3510-2-JB0D
23					
22					L-SUN-3510-2
21	消磁机				
20	托盘	IBM DS4700扩展柜	HuaWei S5600T硬盘柜		L-SUN-3510-3-JB0D
19					
18					L-SUN-3510-3
17	绝密档案服务器	IBM DS4700扩展柜	托盘		托盘
16	L-DELL-R730-1				
15	托盘				
14					
13	局域网虚拟化桌面	IBM EXP810控制柜			
12	L-DELL-R730-1				
11					
10	局域网虚拟化桌面				
9	L-DELL-R730-2		托盘		
8					
7					
6			6口铜缆配线架	托盘	5口LC光纤配线架
5			预留	预留	24口LC光纤配线架
4			8口LC光纤配线架	预留	预留
3			预留	预留	24口LC光纤配线架
2			预留	预留	预留
1			预留	预留	预留

L11-L15 机柜立面图					
U数	L11	L12	L13	L14	L15
38	24口配线架（背面）	24口配线架（背面）	24口配线架（背面）	24口配线架（背面）	24口配线架（背面）
37			24口配线架（背面）		
36		17寸显示器	17寸显示器	IBM X3650 M3	分布式存储服务器
35				托盘	1
34				KVM	分布式存储服务器
33				托盘	分布式存储服务器
32		托盘	鼠标	托盘	分布式存储服务器
31				分布式存储服务器	托盘
30					
29					
28					
27					
26					
25					
24					
23					
22					
21	中信局域网虚拟化资源	局域网虚拟化资源	局域网服务器虚拟化资源池	分布式存储服务器	电教室服务器
20	L-DELL-R730 192.168.3.97	L-DELL-R730	L-R710-1	1	L-PX-R730
19					
18	oa签章服务器	全文数据服务器备用		分布式存储服务器	
17	L-DELL-R730-1	L-QW-R410-19		192.168.3.198	
16		局域网虚拟化资源池			华为防火墙(USG6610E)
15		L-ESX-R510-19	L-MU-06	分布式存储服务器	托盘
14	L-DELL-R730-2	局域网全文备份	U盘管理服务器		华为防火墙(USG6610E)
13		1			托盘
12	L-DELL-R730-3	托盘	托盘	分布式存储交换机	档案利用服务器
11					L-DA-0650-1
10					
9					
8		托盘	局域网定制存储	托盘	托盘
7			型号：无		
6		L-DELL-R730xd	预留	配架：7*LC	服务器光纤交换机
5			预留	1S	(主)
4	局域网中信大数据		配架：13*10/100 E	配架：8*10/100 E	服务器光纤交换机(备)
3	DELL-R730-4				
2			预留	预留	
1			预留	预留	

L21-L25 机柜立面图					
U数	L21	L22	L23	L24	L25
38	17寸显示器	Brocade G610光纤交换机	CB6881-4836CQ 存储交换机01		
37		Brocade G610光纤交换机	CB6881-4836CQ 存储交换机02	转码服务器	
36				L-DELL-R730-1	
35		CB6881-4836CQ 存储交换机03	华为S5720S-28P		
34					
33		CB6881-4836CQ 存储交换机04		web服务器	
32				L-DELL-R730-2	
31					
30					
29					
28	主机			SQL数据库服务器	
27					
26				KVM	
25	托盘			局域网虚拟化资源	
24				L-DELL-R730-4	
23					
22			华为K22K-02		
21					
20					
19			华为K22K-02	Huawei S5700交换机	
18		华为K22K-02			
17					
16		华为K22K-02		归档服务器	
15				L-DELL-R730-5	
14					
13					
12		华为K22K-02			
11					
10					
9			华为K22K-02	二级存储	
8	环控系统	SPE36C0225			
7	托盘		华为K22K-02		
6		DAE62525U2-10			
5					
4					
3					
2					
1					

4.4.3.7. 接口互联表

L1						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
D240	SCSI-1			SCSI-1	L-FS-F4800-1	L1
	SCSI-2			SCSI-3	D240	L1
	SCSI-3			SCSI-2	D240	L1
L-FS-F4800-1	FC1		L1-1,2	b0	L-BROCADE-3850-1	L10
	FC2		L1-3,4	b0	L-BROCADE-3850-2	L10
	E1	L1-1	L1-1	E-03	Cisco 6509	L5
	E2	L1-2	L1-2	E-03	Cisco 6509	L4
	E3					
	E0(四口千兆卡)			E0	L-ORA-F4800-2	L2
	E1(四口千兆卡)			E1	L-ORA-F4800-2	L2
	E2(四口千兆卡)					
	E3(四口千兆卡)					
	SCSI-1(千兆/SCSI卡)			SCSI-1	D240	L1
	SCSI-2(千兆/SCSI卡)					
	E1(千兆/SCSI卡)					
	E2(千兆/SCSI卡)					
L2						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
D240	SCSI-1			SCSI-1	L-ORA-F4800-2	L2
	SCSI-2			SCSI-3	D240	L2
	SCSI-3			SCSI-2	D240	L2
L-ORA-F4800-2	FC1		L2-1,2	b1	L-BROCADE-3850-1	L10
	FC2		L2-3,4	b1	L-BROCADE-3850-2	L10
	E1	L2-1	L2-1	E-07	Cisco 6509	L5
	E2	L2-2	L2-2	E-07	Cisco 6509	L3
	E3					
	E0(四口千兆卡)			E0	L-FS-F4800-1	L1
	E1(四口千兆卡)			E1	L-FS-F4800-1	L1
	E2(四口千兆卡)					
	E3(四口千兆卡)					
	SCSI-1(千兆/SCSI卡)			SCSI-1	D240	L2
	SCSI-2(千兆/SCSI卡)					
	E1(千兆/SCSI卡)					
	E2(千兆/SCSI卡)					

IBM DS4700	FC1			b15	L-BROCADE-3850-2	L8
	FC3			b15		
	E1			E-09	Cisco 6509	L4
	E2					
IBM EXP810-1	FC2			FC1	IBM EXP810-1	
	FC4			FC4	IBM EXP810-3	
	FC1			FC2	IBM DS4700	
	FC2			FC1	IBM EXP810-2	
IBM EXP810-2	FC3			FC3	IBM EXP810-2	
	FC1			FC2	IBM EXP810-1	
	FC2			FC1	IBM EXP810-3	
	FC3					
IBM EXP810-3	FC4			FC3	IBM EXP810-3	
	FC1			FC2	IBM EXP810-2	
	FC2			FC4	IBM EXP810-2	
	FC3			FC4	IBM DS4700	
L8						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
Huawei5600T控制框	A1-P0			b1	L-BROCADE-3250-2	L8
	A1-P1			b2	L-BROCADE-3250-1	L8
	B1-P1			b2	L-BROCADE-3250-2	L8
	B1-P0			b3	L-BROCADE-3250-1	L8
	A-MGMT	L8-2	L7-小交换机	E-09	Cisco 6509	L4
	B-MGMT	L8-1	L7-小交换机	E-09	Cisco 6509	L4
	SAS1-P0			SAS-11	Huawei5600T硬盘框	L9
	SAS2-P0			SAS-22	Huawei5600T硬盘框	L10
	SAS1-P1			SAS-11	Huawei5600TSAS硬盘框	L11
	SAS2-P1			SAS-21	Huawei5600TSAS硬盘框	L12
	SAS-11			SAS1-P0	Huawei5600T控制框	L9
	SAS-22			SAS2-P0	Huawei5600T控制框	L9
Huawei5600T硬盘框	SAS-11			SAS1-P1	Huawei5600T控制框	L9
Huawei5600TSAS硬盘框	SAS-21			SAS2-P1	Huawei5600T控制框	L9

	FC5			b7	L-BROCADE-3850-2	L10
L-SUN-3510-3-JBOD	LoopA			FC2	L-SUN-3510-3	L10
	LoopB			FC3	L-SUN-3510-3	L10
	FC0			b2	L-BROCADE-3850-1	L10
L-SUN-3510-3	FC1			b2	L-BROCADE-3850-2	L10
	FC2			LoopA	L-SUN-3510-3-JBOD	L10
	FC3			LoopB	L-SUN-3510-3-JBOD	L10
	FC4			b6	L-BROCADE-3850-1	L10
	FC5			b6	L-BROCADE-3850-2	L10
	b0	L1-1,2		FC1	L-FS-F4800-1	L1
L-BROCADE-3850-1	b1	L2-1,2		FC1	L-ORA-F4800-2	L2
	b2			FC0	L-SUN-3510-3	L10
	b3			FC0	L-SUN-3510-2	L10
	b4		L8-5,6	b7	L-BROCADE-3250-1	L8
	b5			FC1	L-SUN-L100	L9
	b6			FC4	L-SUN-3510-3	L10
	b7			FC4	L-SUN-3510-2	L10
	b8					
	b9					
	b10	L14 9-10	L14 9-10	FC1	L-ESX-R510	L12
	b11	L14 3-4	L14 3-4	FC1	L-ESX-R900-1	L13
	b12					
	b13					
	b14	L14 1-2	L14 1-2	FC1	L-QW-R410	L12
	b15			dsf1	IBM DS4700	L7
L-BROCADE-3850-2	b0	L1-3 L1-4	L1-1 3, L1-1 4	f2	L-FS-F4800-1	L1
	b1	L2-3 L2-4	L2-1 3, L2-1 4	f2	L-ORA-F4800-2	L2
	b2			35u2	L-SUN-3510-4	L10
	b3			35u2	L-SUN-3510-3	L10
	b4	L8-7,8	L8-7,8	b7	L-BROCADE-3250-2	L8
	b5					
	b6			35u4	L-SUN-3510-4	L10
	b7			35u4	L-SUN-3510-3	L10
	b8			35u2	L-SUN-3510-2	L10
	b9					
	b10			51f2	L-ESX-R510	L14
	b11			41f2	L-QWSJ-R410	L12
	b12			35u4	L-SUN-3510-2	L10
	b13					
	b14			90f1	L-ESX-R900-2	L13
	b15			dsf2	IBM DS4700	L7
L12						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
L-QWSJ-R410	41f1			b14	L-BROCADE-3850-1	L10
	41f2			b11	L-BROCADE-3850-2	L10
	41e1	L13-1			Cisco 6509	L5
L-ESX-R510	51f1			b10	L-BROCADE-3850-1	L10
	51f2			b10	L-BROCADE-3850-2	L10
	51e1	L13-2			Cisco 6509	L5
	51e2	L13-3			Cisco 6510	L5
	51e3			E13	Huawei S5700-1	L5
	51e4			E14	Huawei S5700-1	L5

L-ESX-X3650	36e1	L13-4			Cisco 6509	L5
L13						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
L-ESX-R900-1	90f1			b11	L-BROCADE-3850-1	L10
	90e1	L13-5			Cisco 6509	L4
	90e2	L13-6			Cisco 6509	L5
L-ESX-R900-2	90f1			b14	L-BROCADE-3850-2	L10
	90e1	L13-7			Cisco 6509	L4
	90e2	L13-8			Cisco 6509	L5
	90e3	L19-6			Cisco 3750	L5
L-USB-6650-1	66e1	L13-9			Cisco 6509	L5
L14						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
L-ESX-R910-1	91e1	L13-10			Cisco 6509	L5
	91e2	L13-11				
	91e3			E15	Huawei S5700-1	L9
	91e4			E16	Huawei S5700-1	L9
L-RH2288V3-1	22e1	L14-1			Cisco 6509	L5
	22e2	L14-2				
	22e3			E1	Huawei S5700-1	L9
	22e4			E2	Huawei S5700-1	L9
	22e5			E1	Huawei S5700-2	L9
	22e6			E2	Huawei S5700-2	L9
L-RH2288V3-2	22e1	L14-3			Cisco 6509	L5
	22e2	L14-4				
	22e3			E3	Huawei S5700-1	L9
	22e4			E4	Huawei S5700-1	L9
	22e5			E3	Huawei S5700-2	L9
	22e6			E4	Huawei S5700-2	L9
L-RH2288V3-3	22e1	L14-5			Cisco 6509	L5
	22e2	L14-6				
	22e3			E5	Huawei S5700-1	L9
	22e4			E6	Huawei S5700-1	L9
	22e5			E5	Huawei S5700-2	L9
	22e6			E6	Huawei S5700-2	L9
L15						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
L-DA-6650-2	66e1	L14-7			Cisco 6509	L5
L19						
设备名	本地接口	本地接口配架接口	对端配架接口	对端接口	对端设备	对端机柜
L-JK-R710	71e1	L19-6	L19-6	E-40	Cisco 6509	L5

4.4.3.8. 设备使用情况

局域网					
序号	设备	服务器名称	IP地址	机柜号	安装配置情况
1	L-FS-F4800-1	文件系统及备份服务器（集群）		L1	Solaris9.0 64 bit 操作系统、Veritas Storage Foundation v4.0、Veritas Cluster Server v4.0、Veritas Cluster Server Oracle Agent v4.0、NBU Master Server、NBU Oracle Agent、NBU Tape Support、NBU SSO、
2	L-ORA-F4800-2	数据库服务器（集群）		L2	Solaris9.0 64 bit 操作系统、Veritas Storage Foundation v4.0、Veritas Cluster Server v4.0、Veritas Cluster Server Oracle Agent v4.0、NBU Media Server、NBU Oracle Agent、oracle9.0数据库
3	L-WDYTH-2850-1	文档一体化服务器		L13	Windows Server 2003 中文标准版操作系统、IIS6.0、NBU Client、档案利用服务器
4	L-ESX-R900	虚拟机系统		L13	VMware 5.5
5	L-ESX-R900	虚拟机系统		L13	VMware 5.5
6	L-ESX-R510	虚拟机系统		L12	VMware 5.5
8	L-ESX-R910	虚拟机系统		L14	VMware 5.5
		分级管理系统应用及数据库			Windows Server 2003 中文企业版操作系统、IIS6.0、oracle
		档案信息集成管理系统			Windows Server 2003 中文企业版操作系统、NBU Client、Weblogic
		档案信息集成管理系统(备用)			Windows Server 2003 中文标准版操作系统、SQL Server 2000 标准版数据库、NBU Client、Helix Server 软件
		网间服务器			Windows Server 2003 中文企业版操作系统
		档案信息集成系统备用			Windows Server 2003 中文企业版操作系统
			192		Windows Server 2008 中文企业版操作系统

				3	Windows Server 2008 中文企业版操作系统
		新增库系统		5	Windows Server 2008 中文标准版操作系统
				4	cent OS 6.4
					Windows Server 2008 中文标准版操作系统
		电子签章系统		8	Windows Server 2008 中文标准版操作系统
		城控服务器		8	Windows Server 2003 中文标准版操作系统
		防病毒服务器		8	Windows Server 2003 中文标准版操作系统、IIS6.0
		WSUS补丁服务器		6	Windows Server 2008 中文标准版操作系统
		电子文件中心服务器		25	Windows Server 2003 中文标准版操作系统、IIS6.0、NBU Client、电子文件中心系统软件
		文档一体化服务器		20	Windows Server 2003 中文标准版操作系统、IIS6.0、NBU Client、电子文件中心系统软件
		vCenter服务器		10	Windows Server 2008 R2 中文标准版操作系统
		vCenter数据库服务器			Windows Server 2008 R2 中文标准版操作系统、SQL 2005
		华为分布式FSA服务器			suse linux定制版
		华为分布式FSA服务器			suse linux定制版
		华为分布式FSM服务器			suse linux定制版
9	L-DA-6650-1	档案利用服务器		22	L14 Windows Server 2003 中文企业版操作系统、IIS6.0、NBU Client、目录中心系统软件
10	L-USB-6650	U盘管理中心		19	L14 Windows Server 2003 中文标准版操作系统
					Windows Server 2003 中文标准
9	L-DA-6650-1	档案利用服务器		22	L14 Windows Server 2003 中文企业版操作系统、IIS6.0、NBU Client、目录中心系统软件
10	L-USB-6650	U盘管理中心		19	L14 Windows Server 2003 中文标准版操作系统
11	L-JK-R710	监控服务器		4	L19 Windows Server 2003 中文标准版操作系统、Broadview NCC网络监控、Broadview应用监控
12	L-PX-2900-1	电脑教室服务器			L15 Windows Server 2003 中文企业版操作系统
13	DELL 2800	文明城区服务器			L15 Windows Server 2003 中文企业版操作系统
14	DELL R410	全文数据服务器		5	L12 Windows Server 2008 中文标准版操作系统

4.5. 软件系统平台分析

4.5.1. 本地系统软件

系统软件构成了浦东新区档案局各项应用稳定运行的基石，为核心业务提供至关重要的底层软件环境与技术支持。其核心组成部分包括稳定可靠的操作系统、高性能的数据库管理系统、完备的存储与备份解决方案，以及高效灵活的虚拟化平台。通过这些系统软件的协同工作，不仅保障了档案信息管理、公共服务及政务协同等关键业务的连续性和可用性，还实现了硬件资源的集约化管理与动态分配，显著提升了整体系统的可维护性、安全性与扩展性，为上层多样化应用提供了统一、规范、安全的软件支撑环境。清单如下：

序号	名称	数量	保修起止日期及原厂质保情况
1	Solaris	4	同 SUN 小型机保修起止日期，厂商不再提供服务，现运行正常
2	Oracle Database 9i	1 套/100 用户	2005/5/28~2006/5/29，厂商不再提供服务，现运行正常
3	SQL Server 2000 标准版	1	2005/8/1~2006/7/31，厂商不再提供服务，现运行正常
4	Windows Server 2003 标准版	13	
5	Windows Server 2003 企业版	1	2006/2/4~2007/2/3，厂商不再提供服务，现运行正常
6	Veritas （包括 Storage Foundation、Cluster Server、NetBackup、HSM）		2005/5/20~2006/5/19，厂商不再提供服务，现运行正常
7	VMware vCenter Server V5	1	2012.10~2013.10，厂商不再提供服务，现运行正常
8	VMware vSphere V5	4CPU	
9	TRS 全文数据库系统 V6.8	1	2012.5~2013.5，厂商不再提供服务，现运行正常
10	TRS 全文检索网关 V4.5	1	

11	Windows Server 2008 标准版	2	2013.4~2014.4, 厂商提供系统补丁更新服务, 现运行正常
12	BroadView BCC V6.0	3	2013.6~2014.6, 厂商不再提供服务, 现运行正常
13	BroadView NCC V6.0	2	2013.10~2014.10, 厂商不再提供服务, 现运行正常
14	Windows Server 2008 标准版	17	2013.9~2014.9, 厂商不再提供服务, 现运行正常
15	SQL Server 2005 标准版	2	
16	SyncBackpro V6	1	2014.3~2015.3, 厂商不再提供服务, 现运行正常
17	BroadView NCC V6.0	1	2014.7~2015.7, 厂商不再提供服务, 现运行正常
18	VMware vCenter Server V5	1	2015.5~2016.5, 厂商提供版本升级服务, 现运行正常
19	VMware vSphere V5	2CPU	
20	Huawei FusionAccess 局域网桌面虚拟化软件	40 个终端	2016.11~2017.10, 厂商不再提供服务, 现运行正常
21	Huawei FusionAccess 政务外网桌面虚拟化软件	20 个终端	
22	Huawei FusionAccess 因特网桌面虚拟化软件	20 个终端	2017.9~2018.8, 厂商不再提供服务, 现运行正常
23	Huawei FusionStorage V100R003 分布式存储许可	96TB	2016.6~2018.5, 厂商不再提供服务, 现运行正常
24	Huawei FusionStorage V100R006 分布式存储许可	150TB	2018.11~2019.11, 厂商不再提供服务, 现运行正常
25	Oracle Database 12c	25 用户	

26	联鼎云备份软件	50TB 许可	
27	亚信防病毒软件（DS V20.0）	1 套	2020.7~2021.7，后每年续保，厂商提供病毒库更新服务，现运行正常
28	联软桌面管理软件	150 个许可	2021.7~2022.7，厂商不再提供服务，现运行正常
29	亚信防病毒软件（ESM V8.0）	1 套	2022.7~2023.8，厂商提供病毒库更新服务，现运行正常
30	达梦数据库管理系统 V8.1	1	2021.12~2022.12，已过保，现运行正常
31	东方通应用服务器软件 V7.0	1	2021.12~2022.12，已过保，现运行正常

4.5.2. 云端系统平台

政务云平台虚拟服务器是基于云计算技术构建的核心计算资源，通过虚拟化技术将物理服务器资源池化，按需为各政务部门提供弹性、可扩展且安全隔离的虚拟化计算环境。其具备高可用性、灵活调度和资源优化等特性，可有效支撑政务应用快速部署、业务连续性保障与集约化运维管理，是现代数字政府建设的重要基础设施。日常维护系统列表如下：

序号	名称	云类型	CPU (核)	内存	操作系统	系统盘 大小	数据盘 大小
1	文档一体化系统数据库服务器	ZW	4	8G	Windows 2008 R2_64	100G	5000G
2	文档一体化系统应用服务器	ZW	4	8G	Windows 2008 R2_64	100G	1100G
3	OA 应用服务器	ZW	4	8G	Windows 2003_32 位	200G	500G
4	OA 数据库服务器	ZW	4	32G	Windows 2003_32 位	200G	2000G

					+SQL2005		
5	电子签章应用服务器	ZW	4	8G	Windows 2008 R2_64	100G	100G
6	分级管理系统数据库服务器	ZW	4	32G	OracleLinux +Oracle12c	200G	3000G
7	分级管理系统数据库服务器	ZW	4	16G	OracleLinux +Oracle12c	200G	3000G
8	分级管理系统文件服务器	ZW	4	16G	Windows 2008 R2_64	200G	20000G
9	分级管理系统应用服务器	ZW	4	8G	Windows 2008 R2_64	200G	500G
10	分级管理系统跨馆查询服务器	ZW	4	16G	Windows 2008 R2_64	200G	100G
11	民生档案智慧服务平台服务器	ZW	4	16G	Windows 2008 R2_64	100G	500G
12	教育培训管理系统应用服务器	INT	4	16G	Windows 2008 R2_64	100G	500G
13	教育培训管理系统视频服务器	INT	4	16G	Windows 2008 R2_64	100G	1000G
14	浦东档案 APP 应用服务器	INT	4	8G	Windows 2008 R2_64	100G	1000G
15	浦东档案 APP 互联网接口服务器	INT	4	8G	Windows 2008 R2_64	100G	100G
16	浦东档案 APP 数据库服务器	INT	4	32G	Windows 2008 R2_64	100G	1000G
17	浦东档案 APP 政务网接口服务器	ZW	4	8G	Windows 2008 R2_64	100G	100G

5. 运维服务方案介绍

5.1. 服务方式

根据上海市浦东新区档案局档案信息系统支撑平台（硬件平台）的复杂功能架构与高标准运维要求，依托我司在多年实践中形成的专业服务模式与成熟管理体系，我们能够更加系统、精准地实现对整体运维质量的有效控制，并全面提升日常维护工作的规范化水平与执行效率。该服务体系以系统化、流程化的管理方法为基础，通过明确岗位职责与分工机制、结合定期系统性健康评估与性能分析，实现对硬件资源从预防性维护、常态化监控到应急响应与持续优化的全生命周期管理。如用户方在实际运行过程中提出额外或更深层次的服务需求，我司具备充分的灵活性与定制能力，可根据具体应用场景与管理目标，针对性设计并实施相匹配的服务内容与深度，确保运维服务始终紧密契合业务发展节奏与信息化管理目标，为系统长期稳定、高效运行提供坚实保障。

5.1.1. 现场技术支持服务

我司提供驻场实施服务，我司能迅速提供现场支持服务，安排经验丰富的技术支持工程师现场分析故障原因，制定故障解决方案，并最终排除故障。

要求如下：

(1) 我司服务人员进行现场支持服务前应作好以下准备：

- ✧ 了解用户设备运行情况及设备以往所发生过的问题及解决办法；
- ✧ 准备技术服务工具、技术服务资料、交通工具、必要的备板备件及软件。

(2) 我司服务人员，首先提交《技术服务申请》给用户负责人签字确认。

(3) 我司了解设备运行情况，核实故障现象，并根据故障现象对设备进行故障分析、测试、诊断，并制定业务恢复和故障解决技术方案。我司须保证优先实施业务恢复，在恢复业务的前提下，再进行彻底的故障修复。

(4) 如果确定为设备硬件故障，我司需免费提供设备硬件为浦东档案局进行更换。如果是软件故障，我司需免费为浦东档案局修复软件故障；如果无法修复，我司需免费提供重新安装服务。

(5) 我司服务人员在处理故障时不能影响到设备的正常运行，并应有浦东档案局用户维护人员在场协同处理；在必须进行系统重装或系统启动等较大操作时，须经浦东档案局用户维护主管部门批准方可实施。若因我司服务人员误操作或擅自行事等主观原因给贵单位带来损失的，贵单位有权向我司提出索赔。

(6) 我司服务人员在处理故障后，要向浦东档案局维护人员解释故障原因和解决方法，以及在日常维护中的预防措施。

(7) 我司服务人员在处理故障时，要认真填写《故障处理报告》，交浦东档案局客户主管部门存档，同时加入我司的用户故障处理数据库。

(8) 现场支持响应时间是指在从用户提出现场支持请求到我司服务人员到达用户故障设备现场所需要的时间，根据浦东档案局设备响应级别的要求不同，服务响应时间要求见下表。

5.1.2. 现场硬件支持服务

我司具有7*24小时的备件更换服务能力，将向客户提供现场硬件支持和快速备件更换服务。

在需要现场备件更换服务时，我司将第一时间向服务接受方提供备机备件更换，即我司的工程师将在服务规定的时效内携带相应的完好替换备件赶赴故障现场进行备件更换服务。所有更换的备件均为与原设备各项性能规格不低于原有设备或模块的备件。

我司将保证备件的充足率，保修设备的备件覆盖率达100%，并在备件消耗后及时补充备件库。对于经常出现故障的硬件，我司为服务接受方在系统安装现场设立专用的备件库，该备件库中的备件将专供该现场的服务接受方的系统维修使用，以便加快系统硬件的修复时间，使故障系统尽快恢复运行。服务接受方可以不定期对专用备件库备件进行清点，发现不符合要求进行相关处理。在服务期限内，所有故障备件的更换均是免费的，即已经包含在总体的服务费用之中，不再另行收取备件费用。当客户认为我司备件或技术能力不能满足实际工作需要时，客户在及时通知我司的同时，可以请第三方公司提供，由此而产生的所有费用应由我司据实支付。

5.1.3. 重保服务

我司将在下面所述所有关键时间节点——包括国家法定节假日、重要系统技术改造、重大版本发布、核心业务系统切换以及其他预先商定的高风险运维窗口——安排经验丰富的驻场技术人员及相应资源，提供专职现场保障支持服务。每次保障服务均确保至少一名专业技术工程师全程在场，负责实时监控系统状态、快速响应并处理突发故障、执行预定应急预案，并与用户方保持密切沟通。通过现场人力与技术的双重保障，我司致力于最大限度降低系统运行风险，确保关键时期业务连续性与稳定性，全力支持各项工作的顺利开展。

5.1.4. 重难点分析服务

针对系统运行中出现的疑难问题，若驻场工程师无法独立或即时解决，该工程师将依照标准流程，通过服务台经理将问题及时升级至更高层级的管理及技术团队，并全程跟踪、协调与推动，确保问题获得快速且有效的处理。

故障升级遵循明确的标准，符合以下任一条件即应启动升级机制：

- （1）在业务高峰期发生的故障，已严重影响核心业务运行，且短期内无法定位或解决；
- （2）重要问题自上报起2小时内仍未能解决，可能对系统稳定性或业务连续性造成进一步风险；
- （3）问题涉及多系统、多技术域耦合或架构级隐患，需协调更多专家资源或第三方支持方可处理。

我司已建立规范的疑难问题升级与协同处理流程，能够系统性地应对复杂系统问题。任何疑难技术问题，均可通过这一机制，获得我司技术中心及第三方合作伙伴（如原厂技术支持、专项服务商等）的联合支持。对于涉及第三方产品的接入与故障排查，我司同样可提供统一的技术协调与对接服务，确保端到端问题闭环解决，最大限度保障系统稳定与业务不受影响。

5.1.5. 咨询服务

我司将提供全面而专业的咨询支持服务，以应对客户在软件产品安装、更新及其他技术环节中可能遇到的各种疑问与挑战。若客户在实施过程中遇到技术障碍或操作疑问，我司将依托资深工程师团队及丰富的合作资源，及时提供清晰、准确的技术指导与可行性建议。

针对服务接受方提出的各类复杂或疑难问题，我司将指派相关工程师主动协助，通过协调内部技术专家、原厂技术团队或授权服务伙伴等多种资源，共同分析并定位问题根源，确保用户获得满意且有效的解决方案。我们致力于通过系统化的咨询与响应机制，为客户提供端到端的专业支持，助力其高效解决问题，提升系统使用体验与运维效能。

5.1.6. 软件测试、补丁与升级服务

我司能够紧密跟踪原厂商发布的系统软件版本更新与补丁升级程序，并深入结合服务接受方的实际业务需求与IT环境现状，定期为其提供系统化的软件版本与补丁管理服务。具体包括在非生产环境中对新版软件及补丁进行全面的兼容性、功能性与稳定性测试，评估其在实际业务场景中的适用性与潜在风险，并据此制定稳妥的升级实施方案。

在测试验证通过的基础上，我司将提供专业的现场或远程支持，协助实施系统软件版本与安全补丁的正式升级部署，涵盖操作系统、中间件、数据库及关键应用软件等范畴。同时，我们也将根据设备运行状态和厂商建议，对服务器、存储等硬件设备的固件进行必要的版本升级，以提升性能、消除已知缺陷并增强系统整体安全性。

通过上述有计划、可控制的软件与固件维护服务，我们致力于帮助服务接受方持续保持系统处于稳定、高效且安全的运行状态，有效规避潜在技术风险，保障业务连续性与数据完整性。

5.1.7. 其它综合服务

我司提供全面、多层次的补充技术服务，涵盖多种支持方式与专业安全及运维保障，旨在构建完善的技术服务生态，提升系统综合管理能力与应急响应水平。具体服务内容包括但不限于以下方面：

在支持响应层面，我司建立多通道、实时化的技术支持体系，用户可通过电话、邮件、即时通讯等多种方式快速触达技术支持团队。我们提供远程问题诊断与解决服务，并结合实际需要提供现场紧急支援，以实现各类故障和需求的敏捷响应与有效处理。

在系统维护与健康管理方面，我司提供系统测查与深度安全评估服务，通过对系统架构、配置、日志及流量进行综合分析，识别潜在运行瓶颈与安全漏洞，并输出优化加固建议，从而提升系统稳健性与安全性。

在安全与合规领域，我司提供专业的等保三级咨询与建设支持服务，协助用户完成定级、备案、测评与整改全流程，确保信息系统符合国家网络安全等级保护制度要求。同时，我们提供专项安全服务，包括漏洞扫描、渗透测试、安全加固、安全事件监测与分析等，体系化增强用户安全防护能力。

在应急管理与业务连续性方面，我司协助制定与优化应急预案，并定期组织恢复演练，模拟真实故障场景，验证预案可行性，提升团队在突发情况下的协同处置能力，最大限度保障业务连续运行。

此外，我司还提供定制化技术培训服务，针对不同角色和需求设计培训课程，涵盖系统操作、日常维护、安全实践等多个维度，助力用户团队提升技术水平和自主运维能力。

通过这些综合服务，我司致力于为用户构建稳定、安全、合规、高效的信息系统运行环境，实现从日常维护到战略保障的全方位技术支撑。

5.2. 服务范围

5.2.1. 网络系统

网络系统巡检是指通过定期、系统性地对网络架构中的各类设备、链路及服务状态进行全面检查与评估，旨在及时发现潜在运行隐患、性能瓶颈及安全风险。巡检范围涵盖路由器、交换机、防火墙等关键设备，包括配置合规性、流量健康状况、日志审计及安全策略有效性等多个维度。通过主动式巡检，可显著提升网络可靠性、优化资源利用率，并为持续的网络优化与安全管理提供数据支撑和决策依据。具体巡检内容如下：

- ① 硬件健康状态检查：检查服务器的硬件组件，如 CPU、内存、硬盘等是否正常工作，是否存在故障或过热等问题。
- ② 软件更新和配置：确保服务器上的操作系统和软件都是最新版本，包括安全补丁和更新，以防止已知漏洞的利用。
- ③ 安全设置和配置：检查服务器的安全设置，包括防火墙、访问控制列表 (ACL)、用户权限等，确保服务器安全性符合最佳实践。
- ④ 日志文件检查：审查服务器的日志文件，包括系统日志、应用程序日志和安全日志，以便及时发现异常活动、攻击尝试或其他异常情况。
- ⑤ 网络连接和带宽使用：检查服务器的网络连接状态和带宽使用情况，确保网络连接正常且带宽利用合理，避免网络拥塞或性能问题。
- ⑥ 数据备份和恢复：确认服务器上的数据备份过程是否正常运行，并测试恢复过程以确保数据可靠性和完整性。
- ⑦ 安全审计和合规性：进行安全审计，确保服务器符合相关的安全标准和合规性要求等。

5.2.2. 存储硬件

我司将为档案局服务器及相关系统提供全面的日常技术支持，重点聚焦于存储硬件及相关子系统的稳定运行与高效管理。服务内容包括存储设备的故障诊断与排除、存储资源配置与策略调整、LUN划分与扩容、磁盘状态监控与预警处理、RAID组管理以及数据迁移与备份协调等。服务范围覆盖连接至多套虚拟

化平台及物理服务器的存储系统，涵盖SAN、NAS及DAS等多种架构，确保不同操作系统环境下存储资源的可靠性、可用性与性能优化，为档案业务数据的安全存储和高效访问提供坚实基础。具体巡检内容如下：

- ① 负责服务器存储设备的硬件安装，包括上架、上电、测试等工作内容；
- ② 查看服务器存储设备的硬件告警灯，发现故障及时维修；
- ③ 查看服务器存储设备电源连接状况，异常时及时报告；
- ④ 查看服务器存储设备网络连接状况，异常时及时报告；
- ⑤ 排除日志中的告警及错误；
- ⑥ 服务器存储设备运行状况例行检测；
- ⑦ 巡检结束后 3 个工作日提交健康检查巡检报告，包括以上检查中任何不正常及错误日志，附上处理意见并联系用户安排时间上门检查且解决问题；

5.2.3. 操作系统

服务器存储设备及操作系统的日常巡检是保障信息系统稳定运行与数据安全的核心环节。该工作通过对服务器硬件状态、存储阵列性能、磁盘健康状况及操作系统运行指标进行定期、系统性的检查与分析，实现对潜在风险的早发现、早预警、早处置。

巡检涵盖物理服务器与存储设备的硬件状态监控，包括但不限于磁盘介质错误、控制器性能、缓存电池健康度、RAID组稳定性及电源与风扇等基础环境指标；同时，针对操作系统层面，重点检查系统日志错误、性能计数器（CPU、内存、I/O负载）、文件系统完整性、补丁状态及关键进程与服务可用性。如涉及虚拟化环境，亦包括对宿主机及虚拟机的存储连接状态、数据存储性能及延迟等指标的监测。

通过建立规范化的日常巡检机制，可显著提升系统可靠性，避免因硬件故障或配置异常引发的服务中断，并为容量规划与性能优化提供决策依据，最终为业务系统持续稳定运行提供坚实基础。具体巡检内容如下：

- ① 负责服务器存储设备操作系统的安装及相关补丁的更新。并对操作系统的运行状态进行查看，确保操作系统运行正常；
- ② 查看并分析应用程序和系统日志，记录警告及错误信息，对可能引起故

障的错误信息认真分析并必要时报修；

- ③ 查看操作系统及其补丁版本，变更时做好记录；
- ④ 查看并登记 CPU 利用率，内存占用情况，占用资源最大的前 5 个进程；
- ⑤ 查看并登记硬盘空间利用情况；
- ⑥ 文件系统利用率情况，根据数据增长量预估决定是否要增加其容量；
- ⑦ 巡检结束后 3 个工作日提交健康检查巡检报告，包括以上检查中任何不正常和错误日志，附上处理意见并联系用户安排时间上门检查且解决问题；

5.2.4. 数据库及备份

数据库日常巡检与备份是保障数据安全、系统稳定与业务连续性的核心运维工作。日常巡检涵盖性能、可用性与安全性等多个维度，包括监控数据库运行状态、空间使用率、会话与锁情况、性能计数器（如缓存命中率、磁盘 I/O、响应延迟等），以及日志中的错误与警告信息。通过定期巡检，可主动识别潜在瓶颈与风险，避免因资源耗尽或配置异常导致的服务中断。

备份工作则需遵循明确的策略与周期，通常包括完整备份、差异备份与事务日志备份等多种类型，以确保数据可恢复性与一致性。备份任务应实现自动化执行，并定期进行恢复演练，验证备份数据的有效性及恢复流程的可靠性。同时，备份数据应实施异质或异地保存，有效防范硬件故障、人为误操作及灾难性事件带来的数据丢失风险。

通过系统化的巡检与备份管理，不仅能够显著提升数据库系统的健壮性与可维护性，也为满足数据合规要求及应对突发故障提供了关键保障。具体巡检内容如下：

- ① 查看数据库文件组文件的大小与分布；
- ② 查看临时数据库文件的大小；
- ③ 查看数据库日志文件组的大小；
- ④ 查看并发数据库进程数；
- ⑤ 查看数据库代理作业运行状况；
- ⑥ 查看数据库资源锁定情况；
- ⑦ 查看数据库运行日志情况；



- ⑧ 作数据库日志备份；
- ⑨ 查看数据库上次备份的日期时间；
- ⑩ 全面巡检数据库运行状况；

5.2.5. 机房工程

机房工程日常巡检是保障数据中心基础设施持续、稳定、安全运行的关键性预防维护工作。该工作通过对机房内各类基础设施进行定期、系统性的检查与测试，旨在及时发现潜在隐患，防范运行风险，确保核心业务环境处于最佳状态。

巡检范围涵盖多个关键子系统：供配电系统（包括市电输入、UPS、蓄电池组、配电柜、PDU等运行状态与参数）、空调与环境系统（精密空调运行模式、温湿度、洁净度、漏水检测状态）、安防系统（门禁权限日志、视频监控画面、消防报警装置及气体灭火系统状态）以及网络物理设施（机柜整洁度、线缆标签与排布、接地可靠性等）。

通过规范化的日常巡检，可有效避免因基础设施故障导致的意外停机，延长设备生命周期，优化能源效率（如PUE值），并为机房容量规划与精细化管理提供决策支持，最终为上层信息系统提供高度可靠的物理环境保障。

具体巡检内容如下：

- ① 温度和湿度：确保机房温度和湿度在正常范围内，避免设备过热或受潮
- ② 除尘：检查机房的除尘工作是否正常，保持环境清洁。
- ③ 供电和照明：检查机房的供电和照明是否正常，确保电力稳定。
- ④ 消防安全：检查机房的消防设备是否齐全，灭火器等是否在有效期内。
- ⑤ 电源设备：检查电源设备，特别是外电引入线路和开关装置是否规范，确保无老化隐患。
- ⑥ 物理安全：检查出入口控制系统和视频监控系統，确保物理安全措施到位。
- ⑦ 检查环境监控系统软件报警功能，每次巡检检查漏水报警功能，短信报警功能，防止异常报警时短信不能及时发出。
- ⑧ 检查机房门禁系统的运行状况及响应记录、进出记录和开关状态。

5.2.6. 网络安全

网络安全日常运维是一项系统性、持续性的安全保障工作，旨在通过常态化的技术与管理措施，确保网络基础设施、信息系统及数据资产免受内外安全威胁。其核心在于构建“监测-防护-响应-恢复”的动态闭环防御体系。

日常工作主要包括：实时监控网络流量与安全事件，分析异常行为与潜在攻击；统一管理防火墙、入侵检测/防御系统（IDS/IPS）、WAF等安全策略；定期更新系统及软件补丁，加固系统配置与访问控制权限；开展漏洞扫描与渗透测试，及时发现并修复安全弱点；组织安全审计与日志分析，满足合规要求并溯源安全事件。

同时，运维团队需制定并演练应急响应预案，确保在安全事件发生时能快速隔离威胁、恢复业务，并持续进行安全意识培训，提升整体防护能力。通过以上闭环管理，有效降低网络安全风险，保障业务连续性 & 数据完整性。

具体巡检内容如下：

- ① 解决网络和安全系统日常技术故障，保障网络安全稳定运行。
- ② 定期升级安全设备病毒库，确保系统更新到最新版本。
- ③ 提供相应的交换机端口保护、广播风暴控制、端口快速启动、DHCP 检测、环路 检测等。
- ④ 针对重点网络和安全设备，定期做好配置备份工作，设备日常日志检查，检查 可疑日志并做好安全防护。
- ⑤ 配合应用开发商，针对应用系统调整网络安全策略，包括访问控制，端口开放等。
- ⑥ 配合新设备上架、配置、调试等工作。



5.2.7. 信息安全

信息安全是一项系统性工程，旨在通过技术、管理和流程的综合措施，保护信息的机密性、完整性和可用性，防范未授权访问、泄露、篡改或破坏。其核心目标在于确保数据在存储、传输和处理过程中的安全，同时保障信息系统的可靠运行与业务连续性。

常见的安全实践包括身份认证与访问控制、数据加密、网络安全防护、漏洞管理、安全审计与入侵检测等。此外，建立符合标准（如ISO 27001、等保2.0）的信息安全管理体系（ISMS），制定应急响应计划并开展员工安全意识培训，也构成信息安全的重要组成部分。

信息安全不仅是技术问题，更涉及组织管理、人员行为与法律法规的多元协作。它服务于组织核心资产保护与合规要求，是数字化时代企业稳健发展的基石。具体巡检内容如下：

- ① 对系统做信息安全风险评估，每年提供年底与 4 次系统安全报告。
- ② 提供安全通告、紧急安全事件的应急响应服务。
- ③ 协助信息系统等级保护的定级、测评、整改工作。
- ④ 根据第三方安全评测报告或安全风险评估报告进行安全加固。
- ⑤ 为档案局现有安全软件提供软件和特征库的升级。

5.2.8. 虚拟化平台

虚拟化及云端虚拟化环境的日常巡检是保障云平台与虚拟基础设施稳定、高效与安全运行的关键运维环节。该工作旨在通过对虚拟化层及其依赖的物理资源进行系统性、周期性的检查与分析，实现对性能瓶颈、配置异常及安全风险的早发现早处理。

巡检内容包括：监控虚拟主机（ESXi、Hyper-V 等）及云平台（如 VMware vSphere、OpenStack 或公有云环境）的计算、存储、网络资源使用情况；检查虚拟机状态、快照管理、高可用与容灾配置是否正常；评估存储性能、磁盘延迟及数据存储兼容性；审视虚拟网络策略、安全组及访问控制规则有效性。同时，也需关注宿主机硬件健康状态及与云平台相关的证书到期时间、API 调用状况等管理项目。

通过建立规范的虚拟化巡检机制，可显著提升资源利用效率，避免因配置错误或资源争用导致的业务中断，增强虚拟环境的安全性与合规性，为混合云与多云架构的可靠运行提供基础保障。

具体巡检内容如下：

- ① 对虚拟化平台软件提供软件升级服务，提供升级部署及支持服务，包括升级必要性评估、风险评估、升级报告等。
- ② 针对虚拟化软件运行情况，结合虚拟化系统的结构特点和具体应用特性，提供总体设计、规划咨询、系统重新部署服务。
- ③ 提供虚拟化平台故障处理、系统变更、系统优化、安全加固、重点保障、应急预案、性能分析等日常维护服务。
- ④ 虚拟化运行平台中的服务器、存储、交换机等硬件的日常维护管理，包括硬件配置信息管理、硬件变更调整、报错信息分析、协助硬件报修和更换备件等。
- ⑤ 配合、保障应用开发商针对应用系统的调整和故障处理，为应用开发商提供稳定的虚拟化运行平台。
- ⑥ 虚拟化软件日常维护管理，包括状态检查、报错信息检查、用户管理、参数配置管理等工作。
- ⑦ 虚拟化软件的变更实施，包括新增应用系统虚拟机配置、虚拟机资源调整、参数及配置调整、软件包安装、打补丁和版本升级等。
- ⑧ 虚拟化软件的数据和系统备份、恢复、切换演练。
- ⑨ 配合虚拟化软件平台中应用系统的调整和日常维护。

5.2.9. 系统支持

系统支持与保护服务为核心IT基础设施提供全面、稳定的技术保障，涵盖Active Directory（AD）、DNS、Windows Server及Linux等多种关键系统平台。该服务致力于确保系统的高可用性、安全性及合规性，贯穿日常运维、主动防护与应急响应全流程。

在AD方面，实施用户权限审计、组策略管理、域控制器健康监测与冗余部署，防止权限滥用或服务中断。DNS服务则通过监控解析状态、记录完整性及防劫持策略，保障网络寻址的准确与安全。针对Windows Server与Linux系统，开展包括系统补丁更新、漏洞修复、身份验证强化、日志审计及恶意代码防范在内的安全加固工作。同时，部署系统级性能监控与资源优化机制，应对高负载及潜在故障场景。

依托规范化运维流程、自动化工具及成熟管理体系，该服务可有效提升系统整体鲁棒性，减少非计划停机，满足等保或行业合规要求，为业务运行提供可靠底座的系统级支撑。

具体巡检内容如下：

- ① 针对 AD、DNS、WSUS 等系统提供技术支持。
- ② 针对 Windows Server 系统漏洞和补丁提供技术支持。
- ③ 针对 Windows Server 系统提供系统修复技术支持。
- ④ 提供统信 UOS 服务器操作系统的日常维护，针对系统漏洞和补丁提供技术支持，协助统信原厂处理操作系统各类问题。

5.3. 运维服务流程介绍

5.3.1. 运维流程概述

服务总流程图涵盖了服务请求的完整处理闭环，主要由三个层级构成：用户层、杉木公司层以及各品牌原厂商层。整个流程始于用户层发出的服务请求，包括故障申报、技术咨询、投诉建议等多种类型。

杉木公司作为服务的协调与调度核心，对接收到的服务请求进行统一分类与初步处理。针对投诉类信息，将直接转交至客户服务部下的质量管理主管；质量管理主管根据投诉内容的严重程度与影响范围，及时向上汇报至公司主管副总经理或服务经理，以推动快速响应与闭环处理。对于用户个人的一般技术咨询电话，则由我司服务台或对应技术方向的工程师直接接洽并提供解答，确保用户问题在第一线得到高效处理。

服务台技术支持人员或现场服务工程师负责对来自邮件、热线电话等服务入口的请求进行记录与初步分析，并统一提交服务经理进行任务分派。服务经理根据服务类型、紧急程度和专业方向，将任务指派至相应的技术服务工程师（若用户现场已有我司常驻工程师，则优先由其直接处理）。工程师在执行服务过程中需详细记录处理步骤与结果，并在维护任务完成后由客服部门对用户进行回访，确认服务效果并收集反馈。

如遇我司工程师无法独立解决的复杂技术问题或硬件设备损坏等情况，服务经理将直接协调相关品牌厂商，申请派遣厂商工程师提供技术支持，或启动设备维修与更换流程，确保用户系统及时恢复运行。整个流程通过杉木公司的枢纽作用，实现对多源服务请求的统一管控、分级处理和有效闭环，保障服务质量与用户满意度。

5.3.2. 服务运维职责

服务运维工程师负责客户现场信息系统的日常运行保障与技术支持工作，主要职责包括对服务器、存储、网络及操作系统等基础设施进行实时监控、定期巡检与性能优化，快速响应和处置系统故障及异常事件。同时，需严格执行变更管理流程，完成系统配置、补丁安装及软件版本更新等操作，并详细记录运维活动。该岗位还承担与客户及后端技术团队的协调沟通，协助开展应急演练与系统恢复工作，确保业务系统持续稳定、安全可靠运行，有效支撑客户业务目标。

- ① 负责服务人员与公司内部部门的接口
- ② 负责对客户、服务人员服务请求的响应
- ③ 负责应急响应人员的调度与调配
- ④ 负责对错误信息进行收集和诊断；
- ⑤ 负责对客户的系统进行远程诊断和故障预判，工作过程将会被记录
- ⑥ 负责给客户提供修复方案，由客户根据现场情况实施这个方案
- ⑦ 负责根据需求和可能，与用户方进行协商，决定是否派工程师去现场，用户方有判断和决定权。
- ⑧ 负责根据具体情况，与用户方协商，决定是否升级至更高级别的技术支持中心，用户方有判断和决定权。

5.3.3. 服务保障联系方式

热线电话：400-816-0504

电子邮件：shanmu1993@sh-shanmu.com

5.3.4. 故障处理概述

当系统故障发生时，我司将立即启动标准化的故障处理服务流程。首先，由具备专业技术基础的服务台人员或现场服务工程师负责接收报修信息，并在第一时间将相关事件详细信息录入《故障接收记录单》，确保所有故障从发生之初即有记录、可追溯。

在完成事件登记的同时，服务台或现场工程师将通过与用户的初步沟通，收集故障现象、发生时间、影响范围等关键信息，并据此进行初步的诊断与故障定级。根据故障级别的不同，我司将立即制定相应的处置任务，并委派具备相关技术能力的服务工程师介入处理。若初步判定为紧急故障，将毫不犹豫地调度工程师赶赴现场，力争在最短时间内定位并解决问题，以最大限度减少对业务的影响。

通常情况下，接到故障处理任务的工程师会优先尝试远程诊断方式。通过电话指导用户配合操作，或利用Telnet、SSH等远程管理工具接入用户设备，从专业视角全面采集故障症状信息，并进行初步修复。如远程手段无法解决问题，或受网络与设备条件限制无法建立远程连接，工程师将迅速转为现场支持，亲赴客户现场进行深度排查与处置，直至故障彻底排除。

针对本项目的特殊要求与服务承诺，我司已在客户现场派驻专职驻点服务工程师，专门用于快速响应频发的小规模故障。该类问题一经上报，驻场工程师将第一时间抵达故障发生地，实施快速诊断与修复，并在处理过程中实时填写《现场服务记录单》，详细记录故障现象、诊断步骤、处理措施及结果等关键信息，确保服务过程透明、可复盘。

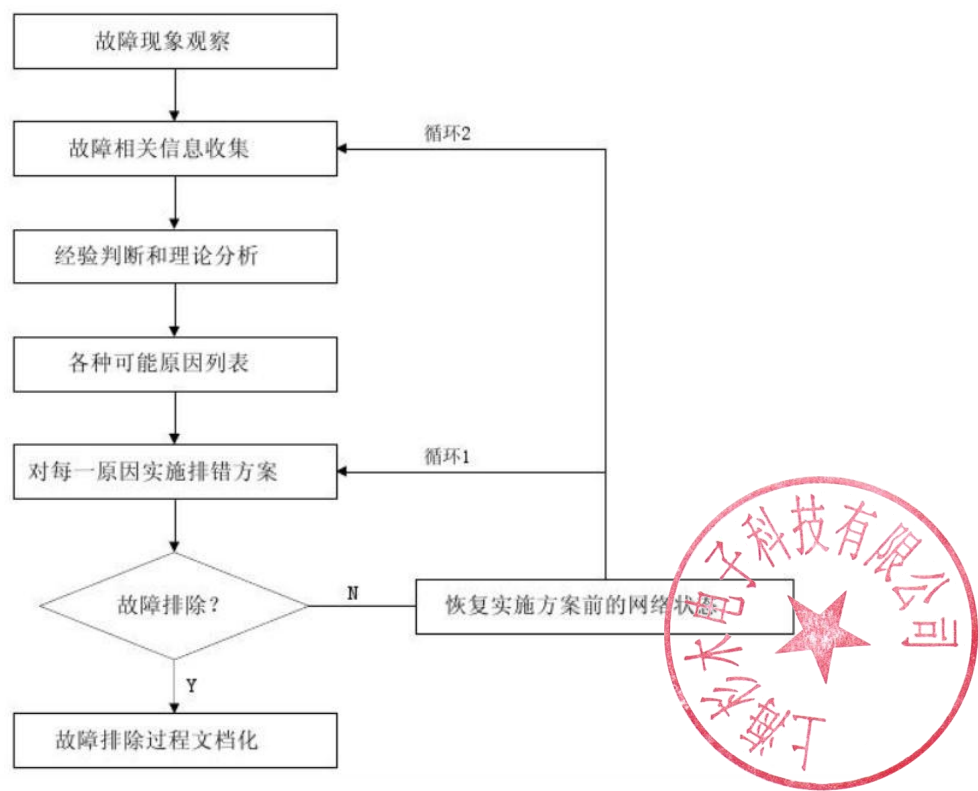
若现场工程师在处理过程中遇到技术难度较高或无法独立解决的问题，将立即启动“多线技术支持”流程，将事件升级至上一级技术专家或二线支持团队，由更资深的工程师协同分析并制定解决方案，确保故障不滞留、问题有闭环。

如经诊断确认故障系由硬件设备本身的缺陷或损坏导致，工程师将严格依照本解决方案中“设备保修”章节所规定的条款与流程，立即启动设备返修或

更换程序，包括联系原厂供应商、协调备件发货、跟踪维修进度等，全力缩短设备故障导致的业务中断时间。

在通过配置调整、部件更换或设备维修最终排除故障，且系统恢复稳定运行后，工程师需系统整理全过程相关文档，完整填写《现场服务记录单》。对于故障原因复杂、处理周期较长或具有典型性的案例，我司还将撰写详细的《故障处理报告》，其中包含故障原因分析、处理过程回顾、后续防范建议等，并向用户进行说明与提交，以便为用户后续的系统优化与预防性维护提供依据。

通过上述层层递进、多方协作的故障处理机制，我司致力于构建一个响应迅速、操作规范、闭环完整的运维服务体系，有效保障用户信息系统的持续稳定运行。流程图如下：



5.3.5. 保修处理概述

本服务针对已在《系统设备及运行情况登记表》中正式登记的设备及其相关功能部件，所提供的专业维修支持。该服务属于事后维护型服务，可能由系统突发故障触发，也可能源于日常巡检中主动发现的设备异常。维修服务所涉及的费用主要包括人工服务费及材料成本费两大类。

在服务模式上，我司为客户提供两种可选维保方案：“保修”与“包修”，以适应不同用户的维护需求与预算安排。

如客户对某设备选择“保修”服务，意味着我司将预先收取一定金额的人工费，该费用主要用于覆盖日后故障诊断过程中所产生的技术服务成本。在实际维修中如需更换部件，材料成本费将根据实际使用情况另行据实收取。

若客户选择“包修”服务，则我司将一次性收取固定费用，该费用已全面涵盖设备后续维修中可能发生的所有人工服务费及材料成本费。在选择“包修”模式后，无论设备在服务期内发生何种故障、需进行多少次诊断与修复，用户均无需再支付任何额外费用。

针对本次用户方的项目特点与实际运维需要，我司郑重承诺为其提供全面的“包修”服务。凡在服务范围内出现的设备故障，涉及需送修至原生产厂商或第三方专业维修机构进行处理的，所有由此产生的维修费、配件费及物流费等，皆由我司承担。我们将依托完善的服务流程与可靠的技术能力，确保故障设备得到及时、专业的处理，最大限度保障系统持续稳定运行，为用户解除后顾之忧之忧。



5.3.6. 升级更新处理概述

当用户业务需求发生变化或提出新的实际要求时，或在日常系统健康巡检过程中识别出优化空间，可能需要对现有系统结构或功能提出升级、变更或改造等调整建议。升级/变更管理旨在系统化地管控此类调整行为，其首要任务是识别并降低与变更相关的各类风险，最大限度减少因变更实施可能引发的服务中断或性能下降。

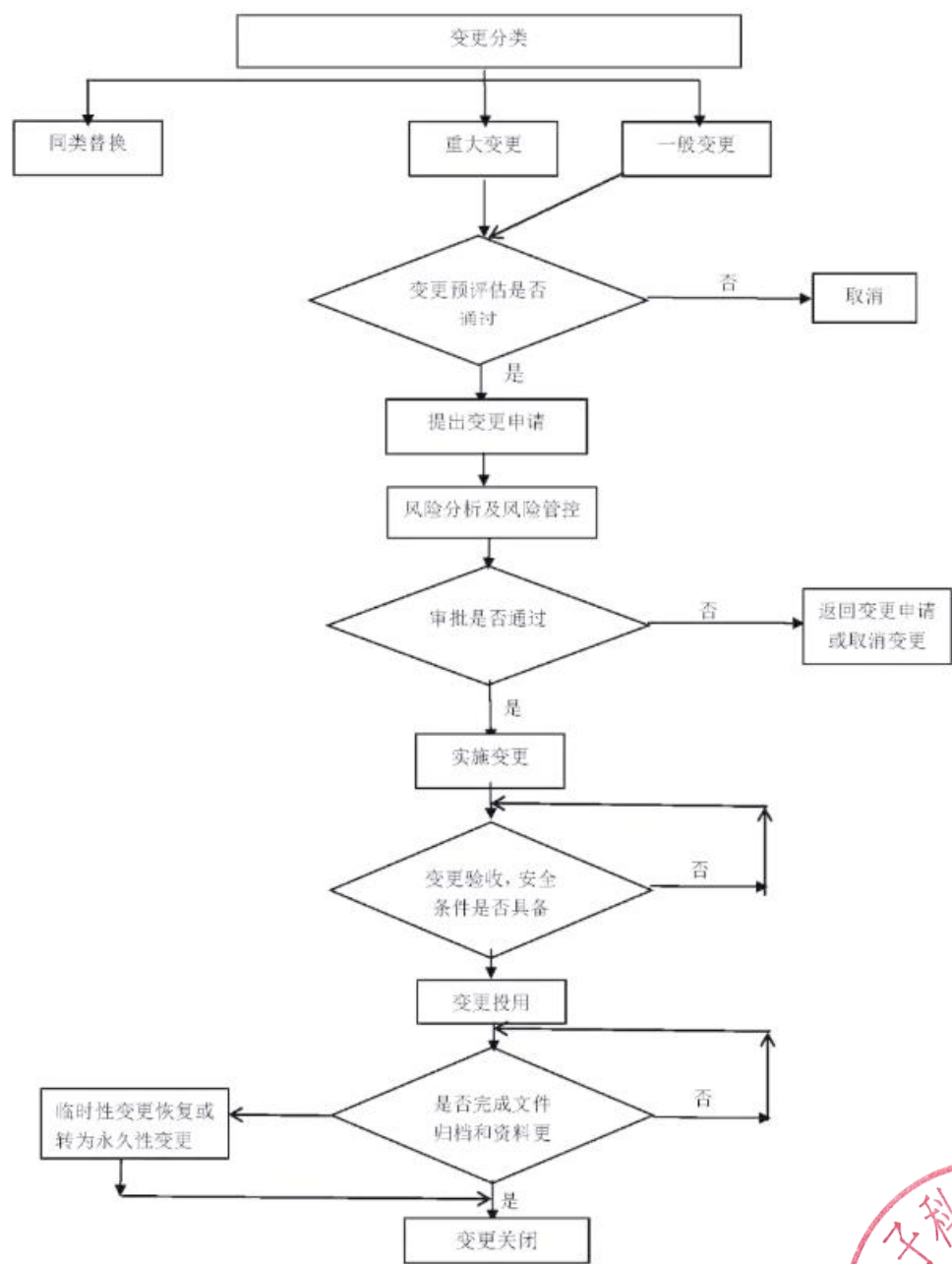
该管理流程涵盖对变更计划的全面审查，包括评估其技术可行性、业务影响及潜在风险。只有在升级/变更方案及实施计划被认定为合理、可控且具备回退策略时，变更管理团队才会予以批准并投入实际执行。需认识到，绝大多数系统突发故障并非偶然发生，而往往是由环境变更所引发——尤其是那些未被充分评估或沟通的变更。因此，有效跟踪配置项的所有变更，确保变更信息能够及时同步至突发事件管理与问题管理流程，对维系系统稳定至关重要。

通过在变更全生命周期中贯彻规范流程，变更管理能够显著减少因非受控变更导致的业务中断，提升系统整体可用性，同时降低运维复杂性与运营成本。

我司所提供的系统升级/变更服务，是指在用户提出合理变更请求且在我司可承接范围内，对已登记系统进行配置层面的适应性调整。典型操作包括但不限于：新增Vlan划分、在防火墙上开放指定端口、创建域用户账户、配置数据库账号与权限、新建及调整表空间等，此类操作属于常规运维服务范畴。

原则上，我司仅对在《系统设备及运行情况登记表》中正式记录的系统或设备提供变更支持。若变更涉及硬件采购，相关设备及物料费用将另行计算；如属软性调整但幅度较大、耗用人力较多，亦将视情况收取相应服务费用。该服务属事前服务，需经评估与审批后方可实施，基本流程如下：





5.3.7. 正常巡检概述

本服务是指以固定周期为单位，定期对在《系统设备及运行情况登记表》中正式记录的设备及相关系统，执行全面、系统性的健康检查与运行状态评估。该服务旨在通过专业、规范的巡检手段，确保整个信息系统持续处于最优运行状态，并最大限度预防潜在故障的发生。

巡检工作不仅包括对硬件设备、操作系统、数据库、中间件及网络配置等关键组件的物理状态与性能指标进行检测，更注重对运行数据的采集与专业分析。通过对历史性能趋势、日志事件、资源利用率等多维数据的综合研判，主动识别系统中存在的异常征兆、性能瓶颈及配置偏差，从而及时提出并实施调整、优化或加固措施。

作为一种日常性、预防性的事前服务，系统性健康巡检致力于将运维模式从“被动响应故障”转变为“主动发现及规避风险”，有效延长设备生命周期，提升系统可靠性与业务连续性。其标准流程如下：



健康巡检



5.3.8. 重大保障概述

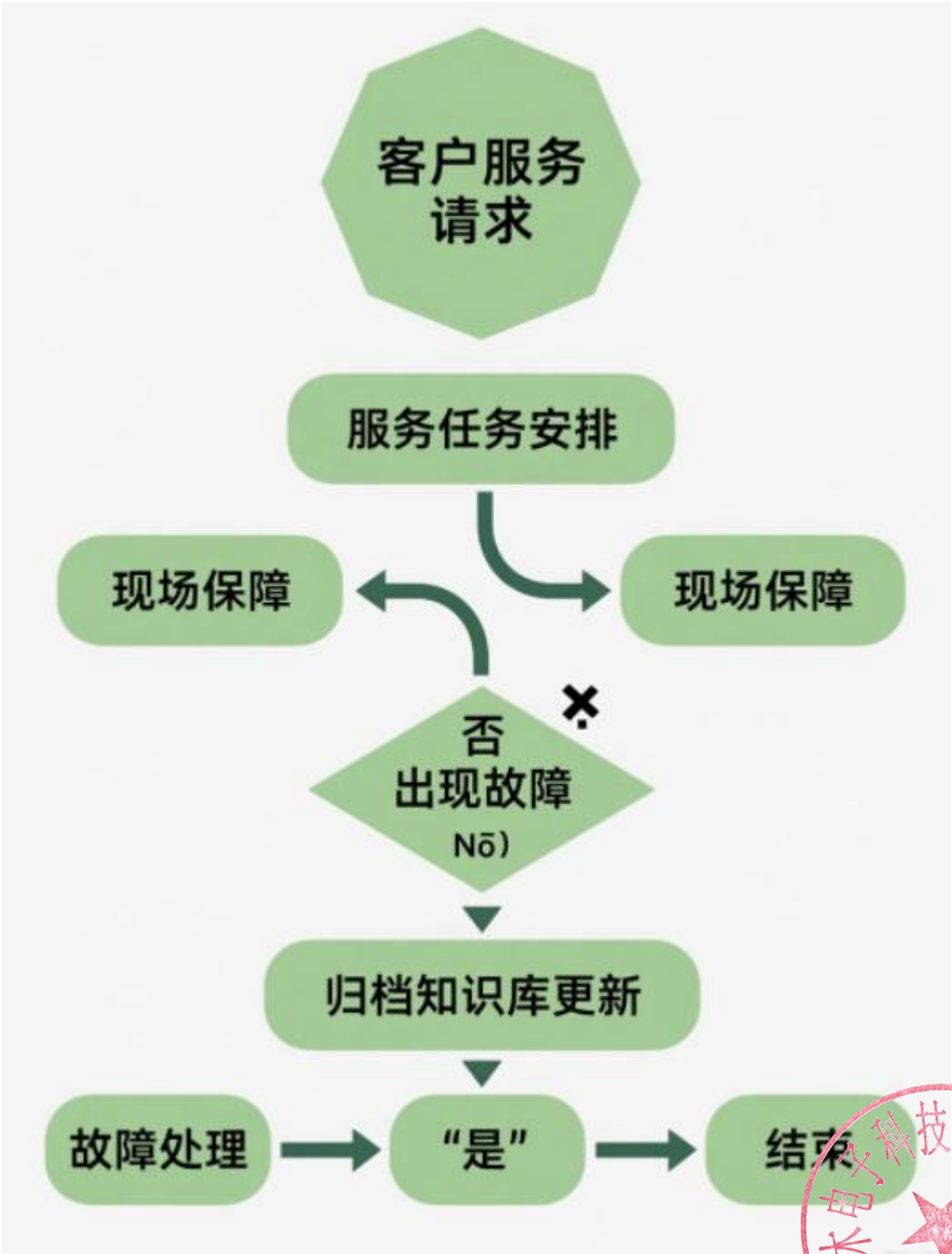
在客户信息系统的全生命周期运行过程中，常会面临诸多关键业务时刻，这些时段对系统的连续性与稳定性提出极高要求。例如，某些核心应用系统在特定重要时间点（如财务月结、业务高峰期或特定关键任务执行期间）绝不允许发生服务中断；又如依托于计算机网络运行的视频会议系统，在客户进行重大跨国会议或高层决策会议时，若网络突发故障，其所造成的业务影响与声誉损失将不可估量；再如电子会议室系统在组织重要发布会、庆典或对外接待期间，常因投影、音响等设备由非专业人员操作，引发误操作、信号中断、设备失灵等问题，进而严重影响会议效果与主办方形象。

针对客户信息系统在上述重大时刻的高保障需求，我司提供“现场服务保障服务”，通过派驻经验丰富的工程师至客户现场，全程值守、实时监控、快速响应，为核心系统与关键业务“保驾护航”，确保其在高风险时段稳定、可靠运行。该项服务旨在以专业的技术支持与及时的现场干预，最大限度规避因系统故障、操作失误或突发异常导致的业务中断，保障关键活动的顺利进行。

原则上，本服务仅针对已在《系统设备及运行情况登记单》中正式记录的系统及设备提供。我们将在保障前与客户共同明确保障时间、范围与目标，制定详细的应急预案与操作流程，并于保障期间严格执行现场值班与故障零延迟响应机制。

该服务属于日常运维体系中的预防性、事前型高端服务，不仅包括重大时刻的现场人力支持，还涵盖事前健康评估、事中实时监控与事后总结优化全流程，致力于为客户关键业务活动提供坚实的技术底座与无声却可靠的安全感。

流程图如下：



5.3.9. 服务交接概述

为确保本次维护项目的顺利启动与后续运维服务的有效开展，我司将首先对项目中涉及的所有子系统进行全面且细致的彻查与清点工作。该过程旨在系统性识别并记录每一设备的运行状态、配置信息及相互依赖关系，并对存在异常或故障的系统及设备立即实施必要的维修或更换，以确保在正式运维服务开始之前，所有子系统均处于稳定、正常的运行状态。

在系统彻查工作正式启动前，我司将向用户方提交《系统彻查申请及用户确认单》，明确列明彻查的范围、计划时间、工作地点、所采用的技术方式及可能的影响等细节，征得用户的书面同意。待用户签署确认后，我司将按约定方案有序开展彻查工作。

彻查实施过程中，我司工程师将在用户方相关人员在场的情况下，逐项检查设备及系统状态，并实时在《系统设备及运行情况登记表》中记录检查结果，包括设备型号、数量、序列号、关键配置参数及当前运行状况等信息。如在彻查期间发现系统或设备存在故障，将立即启动既定的“故障处理”流程，待问题彻底解决后，再行更新登记状态，确保记录与实际状态一致。

彻查工作结束后，双方需共同对《系统设备及运行情况登记表》进行签字确认，并将其作为项目基础文档备案。该登记表后须附上详细的设备硬件清单及当前配置文件的副本（即《设备配置记录》），其具体形式可根据各子系统的实际情况灵活确定，如电子文档、配置导出文件或系统快照等。

在此基础上，我司将根据各系统实际的运行状态与性能指标，建立系统运行基准。该基准主要从安全性、架构合理性、资源利用效率以及系统执行性能等多个维度进行综合评估，形成一套可量化、可比较的初始运行状态参考。在后续运维服务阶段，将以此基准为目标，通过持续的监控、优化与调整，逐步改善系统的整体运行水平，提升可靠性及业务支撑能力。

通过系统化的彻查与基准建立过程，不仅可为后续运维服务奠定坚实的数据基础，更能够显著降低因初始状态不明确或潜在故障引发的运维风险，保障项目目标顺利达成。

5.4. 运维服务工作内容

5.4.1. 驻场服务和日常工作

浦东新区档案局2025年档案信息系统支撑平台（硬件平台）维护项目的服务范围，涵盖了对支撑档案业务稳定运行的关键硬件基础设施及其相关系统的全面、系统性维护保障。本项目旨在通过专业化的技术服务，确保所有硬件设备处于最佳运行状态，有效支撑上层应用与数据服务，并为档案业务的连续性与数据安全提供坚实基础。

安排一名项目经理进行管理协调工作，以及安排两名技术工程师常驻运维现场，负责项目点上 7×8 小时驻点运维工作。

具体需要维护的系统和设备主要包括以下七大类别：

5.4.1.1. 数据中心机房工程

包括但不限于机房供配电系统（市电输入柜、UPS不间断电源、蓄电池组、PDU机柜配电单元）、精密空调与环境监控系统（温湿度、漏水、烟感等传感器）、物理安防系统（门禁、视频监控）及消防报警系统等的日常巡检、状态监控、性能优化与故障处理，确保机房基础环境稳定可靠。

5.4.1.2. 网络安全系统

涵盖防火墙、入侵检测/防御系统（IDS/IPS）、漏洞扫描设备、安全审计系统及网络访问控制设备等安全设施的策略配置优化、日志分析、威胁检测与应急响应，保障网络边界与内部访问的安全性、合规性。

5.4.1.3. Sun 小型机系统

包括Sun系列小型机硬件设备的健康状态监控、诊断分析、高可用集群维护、固件及驱动更新，以及与之相连的外部存储和网络配置管理，确保其作为关键数据库及应用服务器的高性能与高可用性。

5.4.1.4. PC 服务器系统

包括各类品牌x86架构物理服务器（如Dell、HP、华为等）的硬件状态监控、故障排查、部件更换、BIOS及固件升级、性能调优等维护服务，保障服务器资源稳定交付。

5.4.1.5. 存储备份系统

包括磁盘阵列（如SAN、NAS）、光纤交换机、存储控制器及多路径软件等的监控与管理，提供存储资源配置、扩容、性能优化、数据迁移支持，并维护备份设备（如磁带库、虚拟带库及备份服务器）的稳定运行，确保数据存储与备份链路可靠。

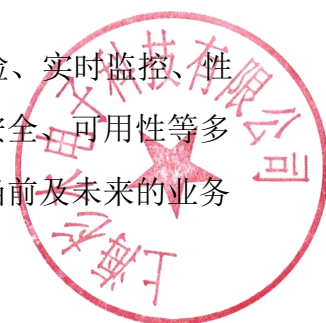
5.4.1.6. 数据库系统

主要指运行于上述硬件平台上的数据库系统环境相关维护，包括数据库运行状态监控、存储空间管理、备份任务验证及与底层硬件兼容性保障等，确保数据库服务高效、稳定。

5.4.1.7. 备份系统

包括备份软件平台、备份策略管理、备份任务监控、介质管理和恢复演练支持，提供从计划制定、执行监控到恢复验证的全流程备份运维服务，保障数据可恢复性与业务连续性。

本项目将基于预防为主、主动运维的原则，通过定期巡检、实时监控、性能分析、故障预警与快速响应机制，为客户提供涵盖性能、安全、可用性等多维度的综合性硬件平台维护服务，全面满足浦东新区档案局当前及未来的业务发展需要。



5.4.2. 硬件保修包换服务

5.4.2.1. 工作职责

- ✓ 负责对在服务范围内的设备及相关功能部件提供包修服务；
- ✓ 负责针对设备故障分析判断原因，及时更换损坏的硬件部件；
- ✓ 负责及时向有关部门反馈设备的维修情况；
- ✓ 负责损坏设备在维修期间提供备件。
- ✓ 流程与文档的管理

5.4.2.2. 工作要求

- ✓ 在发现设备故障后第一时间向用户汇报损坏情况，并提供备件及时更换，避免业务中断；
- ✓ 设备发生故障后，对发生故障的设备进行接收，并填写《故障接收记录单》
- ✓ 对使用备件替换的设备进行验证和交付客户，并填写《故障处理记录单》
- ✓ 设备维修完毕后及时向用户反映情况，并填写《现场服务记录单》
- ✓ 根据客户要求对相关设备的硬件或软件的操作服务，并填写《服务处理记录单》
- ✓ 对设备硬件或软件进行关键性操作，并填写《操作日志》
- ✓ 对设备维修等情况进行记录统计，并填写《设备保修记录单》





5.4.3. 系统健康监控服务

5.4.3.1. 工作职责

- ✓ 负责设备日志的查看，包括网络设备，主机设备，填写《安全设备日志查看》
- ✓ 负责各系统 7×8 小时不间断运行监控和记录；
- ✓ 负责系统运行状态、性能指标及日志信息等事件的收集、反馈和预分析派单；
- ✓ 负责将系统的整体运行情况进行统计，并负责记录填写《日常巡检单》
- ✓ 负责对系统备份情况进行记录，并填写《数据、系统备份记录》
- ✓ 负责每日提供系统监控报告。
- ✓ 流程与文档的管理

5.4.3.2. 工作要求

- ✓ 检查 LOGBASE、绿盟审计系统，发现异常日志信息，检查存在的风险；
- ✓ 检查主机，存储设备的日常日志，检查存在的风险；
- ✓ 检查网络的日常日志，检查存在的风险；
- ✓ 定时收集和统计系统运行状态和性能指标

主机系统

- a. CPU 利用率；
- b. 内存使用情况；
- c. 交换区使用情况；
- d. 磁盘 I/O 情况；
- e. 关键文件系统的状态；
- f. 重要进程的运行情况（例程数量、消耗 CPU、占用内存）；
- g. 操作系统的各类日志文件；
- h. 网络、端口信息；

存储系统

- a. 每日检查系统集群工作状态。
- b. 存储层分配情况；



- c. VG 与 RAID 分配情况；
- d. 逻辑卷配置信息备份策略；
- e. 存储系统的各类日志文件。

数据库系统

- a. 数据库日志文件分布、使用情况；
- b. 数据库数据文件分布、使用情况；
- c. 数据在表空间分布、使用情况；
- d. 数据在数据文件的分布、使用情况；
- e. 数据索引的分布、使用情况；
- f. 数据库对象空间及数据量的增长情况；
- g. 数据库复制工作状态；
- h. standby 数据库工作状态；
- i. 数据库备份策略及实施情况；
- j. Oracle 数据库的系统全局区（SGA）的情况，包括：共享池、Large 池、
- k. 缓冲存储器、记录缓冲区等信息。

中间件及操作系统

- a. 中间件系统日志、运行情况检查；
- b. 中间件处理请求、队列检查。
- c. 操作系统备份策略及实施情况

网络系统及备份系统

- a. 网络吞吐量；
- b. 网络流量；
- c. 网络连通性；
- d. 网络传输质量；
- e. 路由器的路由表；
- f. 网络设备的日志文件；
- g. 网络的安全性；
- h. 数据线路通/断情况。



- i. 每日进行主动式备份系统运行状态检查；
- j. 每日进行备份策略实施及备份介质使用检查，保障数据备份有效执行。

5.4.4. 信息安全保障服务

5.4.4.1. 工作职责

- ✓ 负责提供保障系统信息安全的整体解决方案；
- ✓ 负责加强信息安全评估工作、信息安全策略制定，确保各方面信息资源整体安全性；
- ✓ 负责对系统做信息安全风险评估；
- ✓ 负责识别出各大系统存在的风险，并提出相应的整改措施；
- ✓ 负责收集各大安全网站发布的安全信息通告并整理成文提交给用户，帮助客户了解信息安全热点事件及安全威胁，及时做好安全防护措施；
- ✓ 负责收集各大安全信息网站发布的补丁和安全措施，对系统进行漏洞检查。
- ✓ 负责紧急安全事件的应急响应服务，把威胁和风险降到可接受程度；
- ✓ 负责协助用户进行等级保护的定级、评审、整改、完成，定期对系统进行信息安全测评；
- ✓ 负责网络流量、可疑用户连接检查；
- ✓ 负责系统补丁、漏洞升级维护；
- ✓ 负责病毒防护系统代码更新、病毒检测等安全维护；
- ✓ 负责网络安全策略制定和检查；
- ✓ 负责网络连通性检查；
- ✓ 负责网络及系统的定期安全审计。
- ✓ 负责联系第三方安全评测单位，并安排组织相关的安全评测工作；
- ✓ 负责根据第三方安全评测报告进行相关的安全加固工作。
- ✓ 流程与文档的管理



5.4.4.2. 工作要求

- ✓ 每月定期对安全信息进行收集整理；
- ✓ 及时汇报安全信息通告，并做好防范措施。
- ✓ 发生紧急安全通告必须第一时间通知用户，并做好安全防范。
- ✓ 每日统计分析网络接入的情况，对可疑连接及时上报；
- ✓ 1 小时内定位病毒源并进行隔离；
- ✓ 对于病毒发作的敏感日期进行预警，并提供预防措施；
- ✓ 每季度对系统安全进行评估，优化系统安全设置，消除系统安全隐患；
- ✓ 每季度检查网络拓扑连接；
- ✓ 每季度使用网络侦测工具进行 IP 网络服务、主机操作系统、WEB 服务网站的漏洞扫描；
- ✓ 每季度测试备份网络链路有效性；
- ✓ 每月进行防火墙、路由器、交换机等系统配置的备份；
- ✓ 每季度对 windows 平台服务器系统进行病毒检查；
- ✓ 每日检查网络（防火墙、路由器、交换机）和主机操作系统安全配置；
- ✓ 每日检查网络（防火墙、路由器、交换机）和主机操作系统日志文件；
- ✓ 每日检查入侵检测系统、防病毒系统的系统运行、代码升级和日志信息；
- ✓ 针对本季度各系统的安全巡检结果进行汇总分析后，产生本季度的系统安全评估报告；
- ✓ 每年定期联系第三方安全测评中心对档案局设备进行安全检查和专业的扫描；
- ✓ 根据第三方安全测评中心给出的相关报告，针对未达标的安全漏洞进行整改。



5.4.5. 机房工程系统服务

5.4.5.1. 工作职责

环境监控和管理

- ✓ 温湿度监控：实时监测并调整机房内的温度和湿度，确保其始终处于设备要求的标准范围内。
- ✓ 洁净度控制：定期清洁，防止灰尘堆积影响设备散热和正常运行。
- ✓ 漏水监测：部署并检查漏水检测系统，防止因漏水或冷凝水引发的短路或设备损坏。
- ✓ 环境告警管理：7x24 小时响应环境监控系统的告警，并立即处理。

供配电系统管理

- ✓ 市电输入监控：监测市电电压、电流、频率等参数是否稳定。
- ✓ UPS 系统维护：定期对 UPS 主机及蓄电池组进行测试、充放电维护，确保在市电中断时能无缝切换供电。
- ✓ 配电柜/PDU 巡检：检查各级配电柜、列头柜、机柜 PDU 的开关状态、负载情况、连接紧固度，防止过载。
- ✓ 发电机维护（如有）：定期启动测试，确保油料充足，可在长时间断电时自动启动供电。

空调与制冷系统管理

- ✓ 精密空调运行维护：定期巡检精密空调的运行状态、制冷效率、滤网清洁度、冷媒压力等，并进行预防性维护。
- ✓ 气流组织管理：优化冷热通道布局，防止局部热点产生，提升制冷效率。
- ✓ 冷站/水冷系统维护（如有）：对冷却水泵、冷却塔、水管等部件进行维护，防止漏水或效率下降。

安防系统运维

- ✓ 门禁系统管理：管理人员进出权限，定期审计门禁日志，确保物理访问安全可控。
- ✓ 视频监控系统维护：确保摄像头工作正常，录像功能完好，存储周期符合要求。



- ✓ 防盗措施：检查机柜上锁、防盗报警器等设施是否正常。

消防系统运维

- ✓ 消防设备检查：定期检查气体灭火系统、烟感/温感探测器、手动报警按钮等消防设施的有效性，确保在紧急状态下能正常启动。
- ✓ 消防演练与预案：熟悉消防应急预案，参与定期演练。

网络物理设施与综合布线

- ✓ 机柜管理：保持机柜内部整洁，设备安装规范，标签清晰。
- ✓ 线缆管理：维护光纤、网线、电源线等布线的整齐规范，避免缠绕、挤压，并定期检查线缆完好性。
- ✓ 接地与防雷：检查接地电阻值是否符合要求，确保防雷设施有效。

流程与文档管理

- ✓ 日常巡检记录：按规定周期执行巡检并详细填写记录，形成可追溯的运维日志。
- ✓ 变更管理：严格执行机房内任何物理变更（如设备上下电、进出机柜）的流程审批与操作规范。
- ✓ 应急预案与执行：制定并持续更新停电、空调故障、火灾等应急预案，故障时能迅速按流程响应。
- ✓ 资产与管理文档：维护机房基础设施的资产清单、系统架构图、布线图等文档，确保与实际一致。



5.4.5.2. 工作要求

动力月度柜巡检要求

- ✓ 进线电压、频率、电流
- ✓ 零对地电压
- ✓ 电源指示
- ✓ 各节点运行时温度（开关接线螺丝、铜排连接和连线）
- ✓ 设备温度

输出柜月度巡检要求

- ✓ 主电源总电源空气开关
- ✓ 分路电源开关
- ✓ 电流互感器
- ✓ 指示灯、电压、电流表、按钮开关（用自带设备测试，测试结果与配电柜表记对比）
- ✓ 各节点运行时温度（开关等元器件接线螺丝、铜排连接和连线）
- ✓ 设备温度
- ✓ 铜排、线缆联接状况
- ✓ 零电位和接地系统的电压检测
- ✓ 接地电流

动力季度柜巡检要求

- ✓ 进线电压、频率、电流
- ✓ 零对地电压
- ✓ 电源指示
- ✓ 各节点运行时温度（开关接线螺丝、铜排连接和连线）
- ✓ 设备温度
- ✓ 机柜清洁（每季度）

输出柜季度巡检要求

- ✓ 主电源总电源空气开关
- ✓ 分路电源开关



- ✓ 电流互感器
- ✓ 指示灯、电压、电流表、按钮开关（用自带设备测试，测试结果与配电柜表记对比）
- ✓ 各节点运行时温度（开关等元器件接线螺丝、铜排连接和连线）
- ✓ 设备温度
- ✓ 铜排、线缆联接状况
- ✓ 零电位和接地系统的电压检测
- ✓ 接地电流
- ✓ 机柜清洁（每季度）

5.4.6. 机房供电系统服务

5.4.6.1. 工作职责

UPS 主机检查

- ✓ 现场及其外观检查。
- ✓ 设备显示屏报警信息检查
- ✓ 风扇运转情况检查
- ✓ 运行参数检查：输入电压电流、输出电压电流、直流电压、总谐波失真、频率等参数测量。（用测量仪表测试，测试结果与 UPS 采集的数据对比之间误差）
- ✓ 双母线切换测试。（本测试因为是把两台 UPS 的负载切换到一台 UPS 上，
- ✓ 在切换的过程中，负载的转移，会对 UPS 有一定的冲击，测试存在一定风险）
- ✓ 其它机械组件检查

蓄电池检查

- ✓ 带载的充放电 60--120 分钟测试：浮充状态下电压测量、放电状态下电压测量、放电持续时间、放电过程中的负载电流、放电之前的总直流电压、放电之后的总直流电压、电池后备时间、有无落后电池。
- ✓ 电池外观、电池温度、电池内阻和电池有无泄漏。



常规巡检项目

- ✓ 系统全面检查：每季度 1 次；
- ✓ 重复定期检查的内容；
- ✓ 对 UPS 主机、滤波器、机柜、检查原器件、接线、安装等有无异常，紧固内部线路连接；
- ✓ 校验测量参数的精准；
- ✓ 清洁设备内部；
- ✓ 每个季度对每节电池的浮充电压、内阻做一次测量。
- ✓ 消除设备缺陷，更换不合格元器件；
- ✓ 运行管理软件维护；

5.4.6.2. 工作要求

开关测试

- ✓ 使 UPS 正常运行，并带负载；
- ✓ 关闭逆变器，验证 UPS 将负载从逆变无间断地转移到旁路供电；
- ✓ 重新启动逆变器，验证 UPS 将负载从旁路无间断地转移到逆变供电。

旁路测试

- ✓ 使 UPS 系统正常运行，并带一定的负载；
- ✓ 在 UPS 的输出端监测输出的电压和电流；
- ✓ 操作使 UPS 系统转到旁路供电方式，验证负载无中断；
- ✓ 操作维修旁路开关，验证负载无中断；
- ✓ 试图启动 UPS 的逆变器，验证逆变器由于与维修旁路的互锁而不能启动；
- ✓ 操作 UPS 模块的输出总开关，验证负载没有中断；
- ✓ 反顺序进行上述操作，使系统恢复正常状态。



5.4.7. 机房制冷系统服务

5.4.7.1. 工作职责

负责机房精密空调系统的日常监控、维护与操作，确保温湿度恒定在设定范围；定期巡检压缩机、风机、冷媒管路及滤网，进行预防性维护和故障处理；管理气流组织，消除局部热点，保障服务器等设备在适宜温度下稳定运行，并参与制冷应急演练与能效优化。

5.4.7.2. 工作要求

- ✓ 精密空调进线电压情况，接触器、开关状态情况；
- ✓ 控制显示部分工作情况；
- ✓ 冷凝器运行状态；
- ✓ 室内风机运行情况；
- ✓ 管道保温情况；
- ✓ 加湿及排水情况；
- ✓ 压缩机运行情况；
- ✓ 加湿罐（盘）清洗工作，必要提出更换需求；
- ✓ 对制冷系统进行检测，若发现制冷剂减少，须查出漏点并维修后及时添加；
- ✓ 检查并清洗空调供排水系统的所有部件，包括水过滤器、水管、阀门等等；
- ✓ 检查给排水及水侵系统等线路。



5.4.8. 机房配套系统服务

5.4.8.1. 门禁系统

(1) 工作职责

- ✓ 权限管理：负责机房人员进出权限的分配、变更与注销，确保权限与岗位职责匹配，遵循最小权限原则。
- ✓ 日常监控与审计：实时监控门禁状态，定期审计门禁日志，核查异常出入记录，确保物理访问行为可追溯。
- ✓ 系统维护：对门禁控制器、读卡器、电锁、电源及管理软件等设施进行定期巡检、测试和维护，保障系统稳定运行。
- ✓ 应急处理：处理门禁故障（如打不开门、误报警等），并在紧急情况下（如火警）按预案确保通道畅通。
- ✓ 安全合规：确保门禁系统符合安全规范与审计要求，协助完成安全演练与检查工作。
- ✓ 其核心目标是实现机房物理访问的安全、可控与可审计。

(2) 工作要求

- ✓ 接线使用情况。
- ✓ 16V 交流输入正常。
- ✓ 12V 直流电输入、输出正常。
- ✓ 备用电池充足及充电电压正常。
- ✓ 读卡器、电锁、开门按钮、机械锁
- ✓ 读卡器清洁，加固并在客方在场情况下对读卡器及开门按钮进行模拟测试，检测电锁能否正常灵活开启，并清洁、润滑。
- ✓ 检查门的开关速度。应慢速闭合，不能有快速冲击力现象发生，如有上述现象必须对客方提出并由客方协调装潢公司一起对门进行调整。
- ✓ 供电器
- ✓ 检测供电主板上准确输出 12V 或 24V。
- ✓ 检测充电电压 12V 准确与否，并测试备电充足，如 12V/7AH 电压低于 8V 应更换电池。



- ✓ 目测电压表，电流表工作正常与否。
- ✓ 目测供电设备上 LED 指示灯是否正常。如异常必须及时调整电压使之正常，若无法更正，应告知客方更换主机板。

5.4.8.2. 监控系统

(1) 工作职责

- ✓ 实时监控：对供配电、UPS、空调、温湿度、漏水、消防、门禁、视频等各类子系统状态进行不间断数据采集与监视。
- ✓ 告警管理：设置并管理各类参数的预警和告警阈值，通过声光、短信、电话等多种方式第一时间通知运维人员，并跟踪告警处理闭环。
- ✓ 性能分析：记录并分析历史运行数据（如 PUE、负载趋势、容量使用），为优化运行效率、预防性维护和容量规划提供决策依据。
- ✓ 应急响应：在发生突发故障或紧急事件时，作为指挥中枢，快速提供现场情况，支撑启动应急预案。
- ✓ 系统维护：确保监控系统自身（传感器、软件、网络）的稳定可靠，定期进行校准、备份和功能测试。
- ✓ 报告与审计：生成日常运行报告、合规性报告，并保留完整的操作与告警日志，满足审计要求。

(2) 工作要求

摄像机检查

- ✓ u 硬盘录像机
- ✓ u 检查播放、录象、快进、快倒、暂停等常规功能。
- ✓ u 检查录像、播放效果，若噪声严重应及时向客户反映，并及时送修。
- ✓ u 检查时间、日期显示准确性，若有误差应及时调整。

切换器检查

- ✓ u 检测切换图像，时序切换及常规功能。
- ✓ u 检测视频接插件接触性能良好。
- ✓ u 监视器、操作盘、录象机、报警盘及视频矩阵工作状态检测



其他检查

- ✓ u 线路检查及紧固端子
- ✓ u 蓄电池检测
- ✓ u 主机工作性能检测
- ✓ u 模块性能检测
- ✓ u 线路检测
- ✓ u 检查录象机记录状况
- ✓ u 检查数据库记录状态

5.4.8.3. 环控系统

(1) 工作职责

机房环控系统的工作职责是对机房内所有关键基础设施与环境参数进行7×24小时集中监控、分析与联动控制，确保其持续稳定运行，防范未然。基于您列出的设备，其核心职责包括：

- ✓ 供配电系统监控：实时监测 2 台 UPS 主机的输入/输出电压、电流、频率、负载、电池状态及温度；监控 2 套 UPS 输出配电柜与 1 套动力配电柜的开关状态、负载电流及告警信息，确保供电链路安全。
- ✓ 环境参数监控：通过 8 个温湿度采集器，实时感知机房不同区域的温湿度变化，确保环境恒定，防止局部过热或过湿。
- ✓ 安防与门禁监控：对 3 个门禁点的出入记录、开关状态及异常事件（如强行闯入、门超时未关）进行实时监视与审计，保障物理安全。
- ✓ 漏水监测：对精密空调周边及其他液 risk 区域部署的漏水检测系统进行监控，一旦发生泄漏立即定位并告警，避免电气短路或设备损坏。
- ✓ 告警管理与应急响应：统一管理所有监控告警，通过声光、短信、电话等方式第一时间通知责任人，并跟踪处理闭环，形成故障应急调度的核心枢纽。
- ✓ 数据分析与报告：记录历史运行数据，生成可用性、能耗（PUE）、容量使用等报告，为预防性维护和优化扩容提供决策依据。



(2) 工作要求

检查项目（硬件运行与监测）

- ✓ 通讯卡接线牢固程度
- ✓ 控制箱内电源工作状况
- ✓ 系统通讯状况
- ✓ 声光报警器、短信报警工作
- ✓ 漏水检测绳周边无水源和积灰现象
- ✓ 大平台运行状况

检查项目（软件运行与检测）

- ✓ 远程桌面通讯状况
- ✓ 主机显示界面数据实时变化
- ✓ 系统报警临界点设置与设备参数一致性
- ✓ 报警记录状况
- ✓ 大平台系统链接数据传输情况

系统运行状态参数分析

- ✓ 检查机房门禁系统的运行参数。
- ✓ 检查机房漏水情况，根据报警排除故障隐患。
- ✓ 检查 2 台 UPS 实时监控数据，如发现 UPS 工作异常及时通知用户或物业。
- ✓ 检查各个监控开关工作状态，如发现开关工作异常及时通知用户或物业。

5.4.9. 系统分析及优化

5.4.9.1. 工作职责

系统分析及优化的工作职责是通过对信息系统的全面监测、评估与持续改进，确保其始终在高性能、高可用、高可扩展及安全的状态下运行，并有效支撑业务发展。其主要职责包括：

- ✓ 系统性能监控与分析：建立常态化监控体系，对服务器、数据库、中间件及应用的 CPU、内存、I/O、网络带宽、响应时间等关键指标进行采集与分析，识别性能瓶颈与异常趋势。
- ✓ 容量规划与资源管理：基于业务增长与系统负载历史数据，预测资源需求，制定科学的容量规划，提出硬件扩容、架构调整或资源调度策略，避免资源耗尽导致的系统风险。
- ✓ 瓶颈诊断与根因分析：对系统中出现的性能下降、稳定性问题或故障进行深入诊断，定位根本原因（如代码效率低下、配置不合理、架构缺陷等），并提出切实可行的解决方案。
- ✓ 架构与配置优化：从系统、数据库、应用程序等多个层面提出优化建议并推动实施，包括但不限于查询优化、索引调整、缓存策略优化、线程池调优、负载均衡策略改进等，提升系统吞吐量与响应效率。
- ✓ 成本与能效优化：评估资源使用效率，识别闲置或低效资源，通过资源整合、弹性伸缩或技术升级等手段，降低运营成本，提升整体能效比。
- ✓ 自动化与流程改进：推动自动化工具和脚本的开发与应用，实现常见优化操作（如日志清理、缓存刷新、健康检查）的自动化，减少人工干预，提高运维效率。
- ✓ 撰写分析与优化报告：定期编制系统健康状态、性能趋势及优化效果报告，为技术决策与未来规划提供数据支持和专业建议。

该系统角色的核心价值在于变被动救火为主动预防，通过持续的数据分析与技术改进，不断提升系统的稳定性、效率与业务支撑能力。

5.4.9.2. 工作要求

要求对于系统每个存在的问题、瓶颈、风险，分析其针对性的原因。在进行数据分析时要求涉及应用层、数据库层、操作系统层和硬件层等各个层面，包括以下方面：



- ✓ 根据 CPU/MEMORY 的占用情况，对系统压力及资源的有效利用情况进行分析；
- ✓ 根据磁盘的 I/O 情况，分析系统的磁盘 I/O 瓶颈；
- ✓ 每季度进行数据库配置分析、物理结构分析、逻辑结构分析；
- ✓ 每季度进行数据库性能采样分析，包括：诊断 SharePool 使用效率，诊断 BufferCache 使用效率，诊断 RedoBuffer 使用效率；
- ✓ 确认业务模块最消耗资源的 SQL、所消耗资源的类型，对资源的消耗的合理性分析；对高负载 SQL 语句进行效率分析；
- ✓ 每季度末对整个系统进行综合运行分析，以评估整个系统的运行状态；
- ✓ 每季度进行应用软件各模块资源消耗情况分析、资源使用平衡情况分析、数据分布均衡情况分析，各业务模块间资源冲突情况分析。

5.4.10. 重大事项及节假日保障

5.4.10.1. 工作职责

机房运维重大事项及节假日保障的核心工作职责是通过前置风险排查、强化监控预警和制定应急响应机制，确保关键时期机房基础设施的绝对安全与稳定，实现业务“零中断”目标。其主要职责包括：

保障前准备阶段（事前预防）

- ✓ 风险评估与预案制定：识别重点保障设备（如 UPS、空调、核心网络），制定详细的应急预案（如停电、故障、网络攻击）并组织演练。
- ✓ 全面健康检查：在节假日前或重大事项开始前，完成对供配电系统、精密空调、消防、安防监控、网络等所有关键设施的深度巡检与预防性维护。
- ✓ 备品备件核查：确保关键设备备件（如硬盘、电源模块、蓄电池）库存充足、状态良好，随时可用。
- ✓ 人员安排与沟通：建立明确的 7x24 小时值班表，保障期间专人专岗，责任到人，并建立高效的紧急联络通道。



保障期间执行阶段（事中监控与响应）

- ✓ 强化监控与巡检：提升监控频率，实行 7x24 小时不间断专人值守，不仅依赖动环监控系统，还需增加关键设施的人工现场巡检频次。
- ✓ 严格执行变更冻结：原则上禁止在保障期间进行任何非紧急的配置变更、硬件操作和系统上线，最大限度减少人为误操作风险。
- ✓ 应急响应与处置：一旦发生告警或故障，立即按照预定应急预案启动快速响应流程，协调资源，力争在最短时间内恢复业务。
- ✓ 信息同步与报告：严格执行“零报告”制度，定期向上级汇报系统状态。遇重大故障，及时通报进展，确保信息透明。

保障结束后阶段（事后总结）

保障复盘：对保障期间的系统运行情况、事件处理过程进行全面复盘，总结经验 and 不足。

优化改进：根据复盘结果，优化监控策略、应急预案和运维流程，形成闭环管理，持续提升保障能力。

总而言之，该职责的核心是“主动预防、严防死守、快速响应”，通过一系列严密的组织和技术措施，构建起一道特殊时期的安全防线，为业务的连续性提供坚实基础。

5.4.10.2. 工作要求

- ✓ 根据用户需求，制定针对性的保障服务方案；
- ✓ 根据具体情况，每年三次，每次三人天，安排技术人员对系统进行检查和保障，如遇上海进博会等活动需要加强人员值守，我司将根据用户。
- ✓ 需要增加人员进行重大事项现场保障。



5.4.11. 应急故障演练服务

5.4.11.1. 演练前准备阶段

✓ 方案策划与设计：

根据风险评估和历史故障，确定演练目标与场景（如市电中断、空调故障、网络中断、火灾等）。制定详细的演练方案，包括时间、范围、流程、预期效果、中止条件，确保演练可控、安全。

预案与资源准备：

✓ 检查并更新相应的应急预案（如《供电中断应急预案》、《空调故障应急预案》）。准备演练所需的工具、备件、通讯设备，并确保参与人员熟悉预案流程。

组织与沟通：

✓ 成立演练工作小组，明确总指挥、各角色职责（如操作员、记录员、观察员）。提前发布演练通知，告知相关方（可能受影响的业务部门），避免造成不必要的恐慌。

5.4.11.2. 演练执行阶段

过程控制与引导：

✓ 按照方案触发模拟事件（如手动模拟主路断电），观察并记录运维团队的响应过程。控制演练节奏，在确保安全的前提下，充分暴露问题，必要时根据预案进行干预或中止。

关键项目观察与记录：

- ✓ 响应时效：团队从接警到判断、到初步操作的用时。
- ✓ 操作流程：操作是否规范，是否符合预案步骤。
- ✓ 沟通协作：内部沟通、上报流程是否畅通高效。
- ✓ 系统恢复：故障排除或系统切换的完整耗时与效果。



5.4.11.3. 演练后总结与评估阶段

复盘会议：

- ✓ 组织所有参与人员召开复盘会，回顾演练全过程，基于记录分析优缺点。

编写评估报告：

- ✓ 形成书面报告，详细记录演练过程、达到的目标、发现的问题（如预案缺陷、技能不足、工具缺失等）。

预案优化与改进：

- ✓ 根据演练结论，持续修订和完善应急预案，这是演练最核心的输出成果。
- ✓ 更新运维手册和故障处理流程（SOP）。

5.4.11.4. 常态化提升阶段

培训与宣贯：

- ✓ 针对演练暴露出的知识盲点或技能短板，组织专项培训。

定期循环：

- ✓ 将应急演练纳入年度/季度运维工作计划，形成常态化机制，确保团队持续保持“肌肉记忆”。

应急演练职责的核心不仅是“演”，更是“练”和“改”，其最终目的是将纸面的预案转化为团队本能的、高效的实战能力，并通过每一次演练持续优化整个应急响应体系。

5.4.12. 现场和后端备品备件服务

5.4.12.1. 备品备件服务

根据IT行业的普遍共识，IT硬件设备的典型生命周期通常不超过72个月。浦东新区档案局信息化硬件平台自2006年投入运行以来，目前多数核心设备已

远超该使用年限。随着设备服役时间的延长，硬件故障率呈显著上升趋势，这不仅对关键业务系统的连续运行构成潜在风险，同时也导致维护复杂度及运营成本不断增加。

为有效应对因设备老化所带来的运行风险，我司针对用户现有各类设备类型，科学规划并合理配置了相应的备品备件资源。通过在故障发生时迅速进行部件更换，最大限度缩短业务中断时间，降低对档案信息系统整体运行的影响。

为此，我司专门制定了系统化的《备品备件解决方案》，对各类关键设备的备件实行统一、集中的专业化管理。所有备件在入库前均经过严格的功能与兼容性测试，确保其符合原厂标准及系统运行要求。同时，我司将根据设备现状及故障统计动态更新备件库存，定期评估并优化备件储备策略，从而构建可持续的备件支持体系，切实保障浦东新区档案局在设备高龄运行阶段仍具备快速故障响应与恢复能力。

5.4.12.2. 备品备件计划

为保障档案信息系统支撑平台的持续安全稳定运行，确保业务连续性和数据安全性，并严格满足“24小时内对无法修复的硬件故障提供备机”的服务要求，我司在对客户现有信息系统支撑平台的设备组成、运行状态及历史故障情况进行了全面调研与分析的基础上，系统梳理了当前备品备件的类型、数量及可用性状况，据此科学编制了本《备品备件配置计划》。

本计划严格遵循国家标准GB/T19000-ISO9000《质量管理体系和质量保证》系列标准及相关采购规范，致力于构建一套完整、可靠、响应迅速的备件支持体系。在制定过程中，我们始终坚持运维服务目标与成本效益相结合的原则，优先对客户现场已有的可用备品备件进行整合和利用，减少重复投入；同时，针对现有备件不足或缺失的关键设备与高故障率部件，由我司负责补充配备，确保覆盖主要硬件类别的故障应急替换需求，最大限度降低因硬件故障导致的系统停机风险，为系统整体可靠性提供有力物资保障。



(一) 互联网平台现有设备情况

序号	设备名称	品牌型号	物理位置	备品备件及配置
1	Oracle 数据库及文件服务器	SUN F4800	I10 机柜	SunV440 小型机备份
2	因特网虚拟化资源池	DELL R910	I1 机柜 9-12U	浪潮 NF5270M5、硬盘、内存
3	因特网虚拟化资源池	DELL R720	I1 机柜 21-22U	浪潮 NF5270M5、硬盘、内存
4	因特网桌面虚拟化服务器	DELL R720	I1 机柜 15-16U	浪潮 NF5270M5、硬盘、内存

序号	品名	中文名称	规格描述	数量	备品备件及配置
1	WS-C3750 X-48T-S	交换机	48 端口千兆以太网交换机 Catalyst3750X48PortDataIP	1	H3C S5130S-52S- EI 光纤线 lc-lc
2	ECP-ACD	机架式光电转换器	16 插槽机架式光电转换器	1	光纤收发器
3	1-FE-M1	光电转换模块	100MRJ45，多模 SC 接	10	光纤收发器
4	1-FE-S1	独立光电转换器	100MRJ45，单模 SC 接	1	光纤收发器
5	ECS31-FE -M1	独立光电转换器	100MRJ45，多模 SC 接	2	光纤收发器
6	SANGFORA C1300	上网行为管理设备		1	MA 服务（保险协约服务）
7	H3CWA221 0-AG	无线 AP	1 个 10/100Base-Tx， 7Hz-63Hz，2dBi 双频分集天 线	13	H3C WA6520S-D



(二) 政务外网平台使用情况

序号	设备名称	品牌型号	物理位置	备品备件及配置
1	政务外网文件系 统 及备份服务器	SUN V880	L16 机柜 7-20U	SunV440 小型机备份
2	政务外网 Oracle 数 据库服务器	SUN V880	L17 机柜 7-20U	SunV440 小型机备份
3	政务外网虚拟化 资 源池	DELL R720	I2 机柜 9-10U	浪潮 NF5270M5、硬盘 、内 存
4	政务外网虚拟化 资 源池	DELL R730	I2 机柜 12-13U	浪潮 NF5270M5、硬盘 、内 存
	政务外网桌面虚 拟 化服务器	DELL R730	I2 机柜 15-16U	浪潮 NF5270M5、硬盘 、内 存

序号	品名	中文名称	规格描述	数量	备品备件及配置
1	WS-C3750X-48T-	交换机	48 端口千兆以太网交换机	2	H3C
	S		Catalyst3750X48PortDat aIPBase		S5130S-52S -EI 光纤线 1c-1c
2	WS-C2950G-48-E I	交换机	4810/100MRJ452GBIC 插槽	3	H3C S5130S-52S -EI 光纤线 1c-1c

3	ECS31-FE-M1	独立光电转换器	100MRJ45, 多模 SC 接口	2	光纤收发器
4	WS-C2950G-24-E I	交换机	2410/100MRJ452GBIC 插槽	3	H3C S5130S-52S -EI 光纤线 1c-1c
5	HuaweiS5700-48	交换机	48100/1000MRJ452GBIC 插槽	1	H3C S5130S-52S -EI 光纤线 1c-1c
6	HuaweiS5700-24	交换机	24100/1000MRJ452GBIC 插槽	1	H3C S5130S-52S -EI 光纤线 1c-1c
7	H3CS5310S	交换机	2410/100MRJ452GBIC 插槽	3	H3C S5130S-52S -EI 光纤线 1c-1c

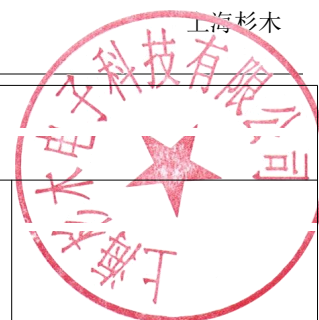


(三) 局域网平台使用情况

局域网服务器设备备品备件配置计划

序号	设备名称	品牌型号	物理位置	备品备件及配置
1	局域网 Oracle 数据库服务器	SUN F4800	L1 机柜	SunV440 小型机备份
序号	设备名称	品牌型号	物理位置	备品备件及配置
2	局域网文件系统及备份服务器	SUN F4800	L2 机柜	SunV440 小型机备份
5	局域网虚拟化资源池	DELL R710	L13 机柜 19-20U	浪潮 NF5270M5、硬盘、内存
6	局域网虚拟化资源池	DELL R710	L13 机柜 23-24U	浪潮 NF5270M5、硬盘、内存
	局域网虚拟化		L12 机柜 15-16U	浪潮 NF5270M5、硬

7	资源池	DELL R510		盘、内存
8	局域网虚拟化资源池	IBM x3650M3	L20 机柜 21-22U	浪潮 NF5270M5、硬盘、内存
9	局域网桌面虚拟化服务器	DELL R730	L6 机柜 9-10U	浪潮 NF5270M5、硬盘、内存
10	局域网桌面虚拟化服务器	DELL R730	L6 机柜 12-13U	浪潮 NF5270M5、硬盘、内存
11	局域网档案利用（电动密集架控制）服务器	DELL 6650	L15 机柜 9-12U	浪潮 NF5270M5、硬盘、内存
12	局域网介质管理服务器	DELL 6650	L13 机柜 13-16U	浪潮 NF5270M5、硬盘、内存
13	媒资系统服务器	DELL R730	L24 机柜 15-16U	浪潮 NF5270M5、硬盘、内存
14	局域网虚拟化资源池、媒资系统服务器	DELL R730	L24 机柜 21-22U	浪潮 NF5270M5、硬盘、内存
15	媒资系统服务器	DELL R730	L24 机柜 27-28U	浪潮 NF5270M5、硬盘、内存
16	媒资系统服务器	DELL R730	L24 机柜 31-32U	浪潮 NF5270M5、硬盘、内存



序号	设备名称	品牌型号	物理位置	备品备件及配置
17	媒资系统服务器	DELL R730	L24 机柜 35-36U	浪潮 NF5270M5、硬盘、内存
18	多媒体教室系统服务器	DELL CF60	L15 机柜 18-19U	浪潮 NF5270M5、硬盘、内存
19	大数据支撑平台节点服务器	DELL R730	L11 机柜 8-9U	浪潮 NF5270M5、硬盘、内存
20	大数据支撑平台节点服务器	DELL R730	L11 机柜 11-12U	浪潮 NF5270M5、硬盘、内存
21	大数据支撑平台节点服务器	DELL R730	L11 机柜 14-15U	浪潮 NF5270M5、硬盘、内存
22	大数据支撑平台节点服务器	DELL R730	L11 机柜 17-18U	浪潮 NF5270M5、硬盘、内存
23	局域网虚拟化资源池、大数据支撑平台节点服务器	DELL R730	L11 机柜 20-21U	浪潮 NF5270M5、硬盘、内存
24	局域网全文数据备用服务器	DELL R410	L12 机柜 18U	浪潮 NF5270M5、硬盘、内存

25	局域网虚拟化资源池、全文数据备份服务器	DELL R730XD	L12 机柜 5-6U	浪潮 NF5270M5、硬盘、内存
26	局域网虚拟化资源池、虚拟化环境备份服务器	DELL R730	L12 机柜 19-20U	浪潮 NF5270M5、硬盘、内存

5.4.12.3. 现场备品备件清单

序号	品名	规格描述	数量	备注
1	H3C R4900	CPU : Intel_6326 (16 核 /2.9GHz) *2 Mem: 32G_DDR4-3200MHz*12 HDD: 4T_SATA_6Gbps_7.2K*6 PowerSupply: 800W_Platinum_220VACor240VDC*2	1	服务器整机
2	H3C S5130S-52S-EI	H3C S5130S-52S-EI L2 以太网交换机主机, 支持 48 个 10/100/1000BASE-T 电口, 4 个 1G/10G BASE-X SFP+端口, 支持 AC	1	交换机整机

3	H3C S5130S-28F-EI	H3C S5130S-28F-EI L2 以太网交换机主机, 支持 24 个 100/1000BASE-X SFP 口(含 8 个 SFP Combo 口), 支持 8 个 10/100/1000BASE-T Combo 电口, 支持 4 个 1/10G BASE-X SFP Plus 光口	1	交换机整机
4	无线 AP	H3C WA5320	1	无线 AP
5	光纤收发器 (多模)	1 个千兆 SFP 口, 1 个 RJ45 电口 (含 1 个多模光模块)	3	
6	光纤收发器 (单模)	1 个千兆 SFP 口, 1 个 RJ45 电口 (含 1 个单模光模块)	1	
7	光纤模块 (多模)	多模千兆	5	
8	光纤模块 (单模)	单模千兆	1	
9	光纤模块 (多模)	多模万兆	3	
10	服务器硬盘 (73G)	SAS 73G	1	
11	服务器硬盘 (300G)	SAS 300G	1	
12	服务器硬盘	SATA, 2TB, 7.2KRPM	1	
13	存储硬盘	73G	1	sun3510, 小机本地硬盘
14	单模光纤跳线	5 米	3	单模
15	多模光纤跳线	5 米	3	多模
16	光纤交换机	8 口 FC 交换机, 8*8G 个端口	4	光 纤 交

		激活	换机
--	--	----	----



5.4.12.4. 保障级备件库

我司提供与最高级别保修服务标准完全统一的备件响应机制，承诺7×24小时全天候响应客户备件需求，确保在任何时间出现硬件故障时，均有专人专线即时受理、快速调度，实现故障件的及时识别与快速匹配。

凭借丰富的多品牌代理资源与完备的备件储备体系，我司能够为各类硬件设备定制完善、合理的备品备件清单与解决方案，涵盖从服务器、存储设备到网络及安全硬件等多个产品门类。依托种类齐全、来源可靠的备件库，可显著提升运维服务响应效率与故障修复及时性，最大限度保障系统持续稳定运行。

针对24小时内无法修复的硬件故障，我司还将及时提供备机服务（限应急使用），通过快速替换保障业务连续性，降低停机对档案信息系统运行的影响。整个备件支持流程严格遵循服务等级协议（SLA），坚持以客户业务恢复为核心，充分发挥我司在多品牌、全品类备件供应链方面的综合优势，为浦东新区档案局硬件平台提供坚实可靠的备件保障。

上海备件库：上海市徐汇区南丹路189弄地下一层

电话： 18516692262

安徽备件库：安徽省芜湖市湾沚区工业大道3999号3号仓库

电话：15155362046





5.4.12.5. 备品备件配置

备品备件根据其性质、用途及在系统中的功能定位，可划分为设备类、材料类和配件类等主要类别。设备类主要指具备独立功能并可部署运行的整机设备，如备用服务器、交换机、存储设备等；材料类包括运维过程中所需的消耗性物料，如线缆、模块、螺丝及标签等；配件类则涵盖用于替换故障部件的组件，例如硬盘、内存、电源、风扇、接口卡等。清晰的分类管理有助于实现备件的规范化存储、快速检索与高效利用，为系统稳定运行提供可靠的物资保障。

备品备件根据其性质、功能及对系统运行的影响程度，通常可分为设备类、材料类和配件类三大类别，每一类在运维保障体系中均扮演不同的角色。

设备类备品备件

主要指关键信息系统中承担核心功能的整机设备，例如服务器、存储阵列、核心交换机等。该类设备一旦发生故障，往往难以在短时间内修复，会直接导致关键业务应用中断，严重影响系统连续性与服务可用性。因此，针对此类设备，通常需根据系统冗余设计和业务容忍度，合理配置应急备机或整机备用方案。

材料类备品备件

包括在日常运维中频繁使用且易损耗的基础材料和连接部件，如各类光纤线、网络跳线、接口转换器、鼠标键盘等。这类材料本身一般不直接影响业务系统功能，但其缺失或损坏仍可能妨碍维护操作的正常开展，因此也需保持适当库存以保证运维效率。

配件类备品备件

涵盖可替换的设备内部组件或模块，例如硬盘、内存、电源模块、风扇、网卡、HBA卡、光纤模块等。该类备件若发生故障，在具备冗余配置的系统中可能不会立即导致业务中断，但仍会显著增加系统运行风险，降低整体可靠性。及时更换故障配件是维持系统健康状态的重要措施。

从资源经济性与管理效率角度出发，盲目储备所有类型备件并不可取。我司基于对本项目所涉及维保设备的故障历史、易损性及供应周期等因素的综合分析，科学制定了备件储备策略，重点配备常用且故障率较高的关键部件，包括但不限于：服务器内存、硬盘、电源和风扇；网络及存储专用配件如网卡、HBA卡、存储硬盘、存储控制器电池、存储电源模块；以及各类关键连接线缆如光纤线等。

通过构建动态可调的备件库存机制，我司将根据实际使用情况定期评估与补充库存，既有效控制成本，又确保在合同约定的修复时间内迅速响应故障，最大限度保障系统稳定运行。



5.4.13. 应急处置方案

5.4.13.1. 应急预案概述

为切实提升浦东新区档案局档案信息系统平台在面对突发网络攻击、设备失效、自然灾害等极端事件时的“自愈力”“免疫力”与“协同力”，形成“预警—处置—恢复—复盘”一体化科学应急机制，确保馆藏数字档案资源、电子文件长期保存平台、档案利用服务系统等核心业务在物理层、系统层、数据层三维安全万无一失，最大限度降低业务中断、数据丢失、声誉受损等风险，保障项目单位合法权益与国家档案信息安全，特制定本专项应急保障方案。

本方案坚持“预防为主、快速反应、以人为本、协同应对”十六字方针。预防为主，即把风险想在前、漏洞补在前、演练做在前；快速反应，即事件发生后15分钟内完成定级、30分钟内完成封控、60分钟内完成业务接管；以人为本，优先保障涉密数据与人员生命安全；协同应对，打通档案局、大数据中心、公安网安、应急管理局、街道及运维厂商的纵向横向联动通道。杉木电子将联合华为、戴尔、VMware、Veritas等原厂商组建“7×24小时联合护航队”，每季度对主机、存储、网络、安全、数据库、中间件、UPS、精密空调、动环监控及灾备体系进行一次深度技术巡检与预防性维护，运用AI日志分析、性能基线比对、固件漏洞扫描、暗网情报监测等手段，做到潜在故障“早预防、早发现、早维护、早解决”，确保档案业务系统始终处于“健康绿码”状态，为浦东新区档案事业数字化转型保驾护航。

5.4.13.2. 应急组织及职责

为了防范和处置各系统突发事件，成立突发事件应急处置小组。

组长：项目单位相关负责人

副组长：现场负责人

成员：杉木技术服务工程师、制造厂技术服务工程师、现场维保技术人员等。

突发事件应急小组职责

负责编制、修订各系统范围内突发事件应急方案。

周期性对各系统进行技术巡检，有预防性的发现设备故障及各种异常情况，做好预防准备。

及时组织专业技术人员对系统内突发事件进行应急处置；负责调查和处置突发事件，及时上报并按照相关规定做好善后工作。

负责组建应急救援队伍并组织培训和演练。

5.4.13.3. 突发事件分类

根据各系统突发事件的发生原因、性质和机理，突发事件主要分为以下四类：

- ✓ 故障类事件：各产品软硬件故障、配置丢失、人为误操作等导致业务中断、系统宕机、瘫痪等情况。
- ✓ 攻击类事件：各产品系统感染计算机病毒、非法入侵导致业务中断、系统宕机、网络瘫痪等情况。
- ✓ 灾害类事件：指因火灾、地震、台风等不可抗力因素导致机器损毁，造成业务中断、系统宕机、业务瘫痪等情况。
- ✓ 供货实施应急类：指在项目设备供货阶段和实施阶段过程中，由于某种原因造成了中断情况。

5.4.13.4. 应急级别定义

我们项目服务支持小组根据用户所突发的事件首先进行业务故障分级，按照不同的应急级别，提供不同的业务服务，我们项目服务支持小组的工程师，会同设备制造厂商，会根据不同的应急故障等级，提供不同的IT解决方案，并且快速解决故障问题。

我们根据系统故障的破坏程度，对系统应急故障级别分为四级，通过四级级别及时发布预警，过渡到应急预案；通过应急预案及时解决突发事件；防止系统突发事件发生或扩散，并及时向用户汇报。并四级故障级别如下所述。

级别	描述现象
蓝色	在系统相关产品功能、安装或配置方面需要信息或支援，很显然对用户的业务运作几乎无影响，或根本没有影响。
黄色	系统的操作性能受损，但业务运作仍可正常工作。
橙色	现有系统的操作能严重降级，或由于系统性能失常严重影响用户业务运作。
红色	现有的系统停机，或对最终用户的业务运作有重大影响。

5.4.13.5. 突发事件应急预案

我司历经三十余年实践沉淀，杉木电子已迭代出一套“预案+算法+专家库”三维融合的故障应急体系：覆盖网络、存储、数据库、虚拟化、安全等八大场景，内置百余条自动化脚本与知识图谱，7×24小时与华为、华三、戴尔、VMware等原厂NOC直通，突发告警10分钟内完成云-边-端协同定位，30分钟内输出可回滚的精密修复方案，为浦东新区档案信息系统提供毫秒级响应、零数据丢失的护航服务。

突发事件类型	突发事件	应急预案处理措施
故障类事件	设备维修应急	杉木电子负责对出现故障的关键设备提供性能相同的替用设备，作为维修阶段的过渡措施，以免贻误用户的应用；并迅速在规定时间内（24小时内）将备品备件送达故障点；设备故障由设备制造商提供及时有效的维修。
	灾难性硬件故障	若出现灾难性故障，我们服务工程师、厂商立即派人将备件送到现场，保证不影响业务运营。现场工程师将损坏设备带回，交由设备制造商提供及时有效的维修。保证项目单位在24小时内得到无故障设备。

	服务器端软件及操作系统崩溃	准备好先前备份数据，同时恢复操作系统及应用环境。
	线路故障	当网络线路发生故障时，首先通过测试确定故障点，然后提出解决方案并指导实施； 当广域网线路发生故障时，具备线路热备份功能的系统自动切换到备份线路，保证系统的不间断运行；项目服务支持小组及时联络杉木电子，并督促按合同时限解决问题。
	配置丢失	项目服务支持小组会将设备的所有硬件型号、嵌入软件版本、参数设置等信息都将记录在标准格式的文档中，服务器设备采取硬盘、光盘等形式，原样备份初始的设备安装状态。使用过程中对设备参数所作的任何修改，都将记录到文档和备份文件中，保持一致性。一旦发生配置丢失情况，项目服务支持小组工程师利用备份文件、备份介质恢复配置。
攻击类事件	不良信息或网络病毒事件	发现不良信息或网络病毒时，信息系统管理员应立即断开网线，终止不良信息或网络病毒传播，并报告信息网络事件应急小组。系统管理员应采取隔离网络等措施，及时杀毒或清除不良信息，并追查不良信息来源。事态或后果严重的，信息网络事件应急小组应及时报告市局信息中心。处置结束后，系统管理员和事发部门应将事发经过、造成影响、处置结果在调查工作结束后一日内书面报告信息网络事件应急小组主任。

	黑客攻击事件	当发现网络被非法入侵、网页内容被篡改，应用服务器产品上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告信息网络事件应急小组和市局信息中心。接报告后，信息网络事件应急小组应立即指令系统管理员核实情况，关闭设备或系统，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。系统管理员应及时清理系统，恢复数据、程序，恢复系统和网络正常；情况严重的，应上报市局信息中心，并请求支援。处置结束后，系统管理员应将事发经过、处置结果等在调查工作结束后一日内报告信息网络事件应急小组。
灾害类事件	中心机房断电	空调停止运行的情况下，立即采取其它措施降温，如开窗通风等。 通知所有应用部门，抓紧完成信息处理工作、停止应用。 实时检测中心机房的室内温度，根据相关情况关闭非重要设备，如机房内温度过高，应立即通知应用部门停止应用并关闭所有设备。 立即向供电部门询问何时恢复供电，并实时检测UPS的储存电能，并有计划地使用，如UPS电能不足以维持所有设备的运转，酌情关闭相关设备，保证关键设备的运作。

	若发生自然灾害、战争、火灾等不可抗力，导致整个系统瘫痪	杉木电子会立即派遣专家小组到用户现场，同用户一起确定解决办法，尽快提出解决方案。通过各级备品/备件库、杉木电子产品中心、厂商支援中心，以最快的速度帮助用户恢复系统运转。在系统恢复后，双方本着友好协商的原则解决其他未尽事宜。
供货实施应急类	由于设备制造周期等原因设备不能按期到货	杉木电子将通过以下方式保证杉木电子快速供货体系： 本项目有限原则全线启动生产、确保供货；设备替代方案。如果通过以上方式仍不能正常供货，杉木电子承诺将暂时提供不低于招标文件要求配置的产品，以保证项目实施的正常进行，投标货物生产完成后再对原设备进行替换，相关费用及成本由杉木电子承担。
	实施过程中计划执行时协调困难，计划可操作性差，造成进度延误。	杉木电子软件将按照项目单位和总集成商要求细化项目实施计划，并与参与项目的各单位共同推敲确认计划，杉木电子软件内部加强计划控制，各项目单位及时协调各部门。保障项目按期完成。

总之，无论发生任何的系统故障，我们都会从“恢复系统运转，减少用户损失”角度出发，及时寻求完善的解决方案。



5.4.13.6. 应急供货及响应

(1) 应急响应

导致系统出现故障的问题是一个庞大的集合，可以分成很多种导致系统出现故障的原因，根据故障出现的状况进行分类，确定故障属于哪一个级别，根据相应的故障级别对故障做对应的处理，确保故障的处理流程是标准化的。

如果没有一套故障处理的标准，工程师只能靠经验去判断，但是依靠经验判断并不是不可以，有时候这种处理方式会很高效率，但是大多数这种处理方式都是不太合理的，如果更换了运维工程师，显然每一个工程师通过经验去判断故障原因的方式都不尽相同，这样的差异将会使故障处理事后不能够得到很好的记录与存档，以供其他工程师以后借鉴故障处理案例。

故障处理标准化的优点：

A. 根据流程可以确定哪些故障应该立即汇报上级，哪些可以自行解决后，再写故障处理报告汇报上级，这样做有助于提高故障处理效率。

B. 对于工程师经验判断，可能出现判断失误的情况，根据故障判断流程，可以不遗漏任何可能的情况对服务器故障进行排除。

C. 有时候工程师处理了故障之后只是简单的做了一下汇报，并没有一些故障处理过程的记录，以及故障处理的详细时间记录，这样对需要追溯以前的具体情况的时候就束手无策了。

(2) 应急供货

杉木公司是中国最早从事各平台代理商之一。杉木公司作为ICT技术解决方案专家，始终秉持着“合作共赢”为企业理念，致力于技术创新和推动计算机技术的应用。杉木电子

作为一个产品和市场领先的公司，把公司代理产品顺利、完好的发送到客户手中，是公司经营很重要的一个环节，杉木电子在这方面积累了丰富的经验和强大的实力。

杉木电子集团公司的大宗货物运输一般有三种方式和途径：航空、铁路、公路（主要是高速公路），下面给予分别说明：

航空运输方式：对于比较紧急的货物发送和采购部件，杉木电子为了减少供货周期和采购周期，会采用航空的运输方式。

铁路运输方式：这是杉木电子长距离运输的主要方式，特点是快捷、准时。每年的铁路运输量非常大，这样即使在运输紧张的时期，杉木电子公司也能保证铁路运输的畅通无阻。

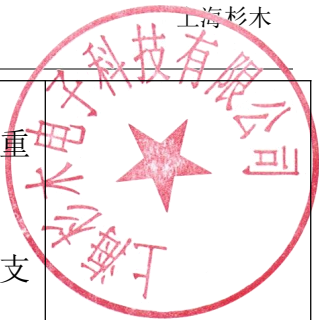
公路运输方式：杉木电子和各家专业的公路运输车队保持紧密合作，针对不同项目，我们主要采取铁路运输和公路运输相结合的方式，对于客户急需的配件产品，我们可以采用航空运输方式以便及时将货物送到客户现场。

杉木电子承诺：在采购人急需设备的情况下，能在用户要求时间之内提供符合性能、配置要求的设备。

5.4.13.7. 故障等级分类及划分

(1) 故障等级划分

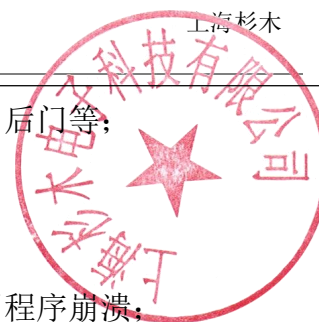
故障级别	故障说明	故障处理第一步
I 级 (紧急)	当系统出现下列相当严重的现象时，属一级故障： 系统整体瘫痪，全部操作失去响应； 系统崩溃，关键硬件或文件系统损坏无法自动修复； 发生间歇性、随机性、重复性的启动或应用退出，无法保障公司业务的正常处理。	立即汇报上级
II 级 (重要)	当系统出现下列比较严重的现象时，属二级故障： 关键部件（含软、硬件）停止工作，导致系统降低运行状态，客户业务受到严重影响； 系统整体性能严重下降，无法自动恢复正常运行状态； 重要数据、参数和配置信息损坏，无恢复，导致客户数据及业务记录严重损失；	立即汇报上级
III 级 (关键)	当系统出现下列现象时，属三级故障： 部分设备或软件异常，局部功能受限，系统整体仍可正常工作，对客户业务影响不大或存在隐患； 关键备用设施因故障离线，主用设施仍能正常工作； 系统运行指标（例如：I/O 效率、CPU 效率）受到直接或间接影响，客户业务处理缓慢；	立即汇报上级
IV 级 (告警)	当系统出现下列情况而不影响客户业务时，属四级故障：	故障排错判断

	不在运行状态的线路、端口损坏； 出于安全考虑并且是受保护的软件降级或应用重启； 因服务器空间不足导致的性能下降； 系统硬件、软件产品功能、安装、或配置方面的支援； 业务仍然可以正常运作，但是服务器报出故障信息的；	
--	---	---



(2) 故障等级分类

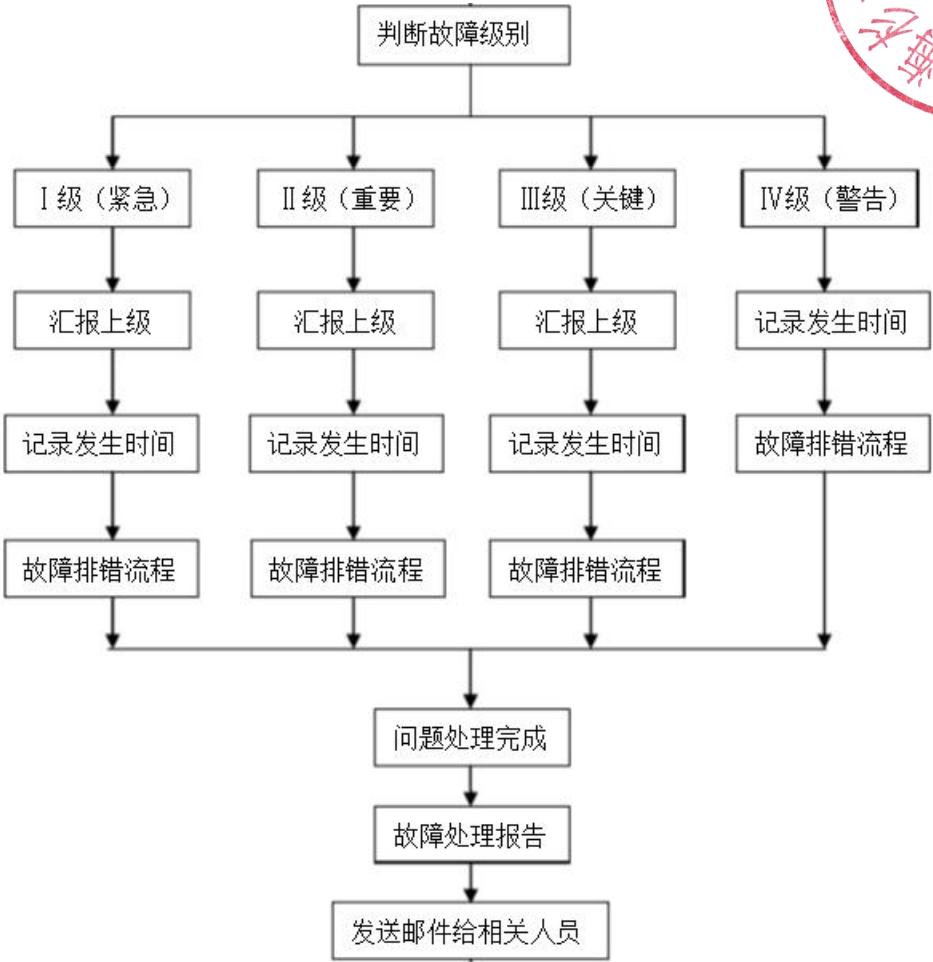
序列	问题种类	详细内容
一	机房网络故障	1、 骨干网光纤切割； 2、 机房网络升级； 3、 机房网络设备调试； 4、 机房网络设备损坏；
二	政府部门封网	1、 服务器没有备案； 2、 域名备案存在问题； 3、 黑客入侵导致服务器违法行为； 4、 违规代理服务器； 5、 服务器转发违禁网站； 6、 服务器放置的网站内容不符合当地的政府法例法规；
三	机房辅助设备故障	1、 机房空调故障问题； 2、 机房灰尘过多问题； 3、 机房电力供应问题；
四	机房机柜迁移	1、 机柜扩容； 2、 机柜移位； 3、 服务器迁移机柜；
五	服务器硬件故障	1、 电源线损坏； 2、 电源损坏； 3、 非人为硬盘损坏； 4、 受黑客入侵攻击时导致硬盘损坏； 5、 CPU 温度过高烧毁； 6、 内存使用中损坏； 7、 主板在电源损坏时容易烧毁；
六	系统故障	1、 黑客攻击导致系统瘫痪； 2、 缓存日志过多没有整理； 3、 人为配置不当导致系统崩溃； 4、 硬盘损坏导致系统崩溃；



七	服务器应用故障	1、 服务器放置的应用程序存在 bug 后门等； 2、 服务器环境配置问题； 3、 黑客攻击导致应用程序崩溃； 4、 硬盘、内存的兼容性差导致应用程序崩溃； 5、 应用程序没有优化占用服务器硬件资源过高导致崩溃； 6、 用户负载过多导致应用程序崩溃；
八	硬件超负荷	1、 数据超过硬盘读写负载能力导致应用程序崩溃； 2、 CPU 使用率跑满导致服务器宕机； 3、 使用内存 cache 占用过多导致宕机； 4、 硬盘空间使用满导致宕机；
九	网络超负荷	1、 用户量过多，服务器带宽不足，导致卡顿，用户访问程序故障； 2、 系统连接数过多造成系统拥堵网络带宽使用不上； 3、 数据库数据读写占用过多服务器连接数，达不到预期的服务器带宽；
十	人为违规操作	1、 人为违规关机； 2、 人为违规操作更改或删除应用； 3、 机房人为关机或断电；
十一	受到攻击	1、 服务拒绝攻击导致系统崩溃，如常见的 UDP 洪水攻击等； 2、 利用型攻击导致黑客入侵系统，如特洛伊木马、口令猜测等； 3、 信息收集型攻击，如体系结构探测、DNS 域转换等 4、 假消息攻击，如 DNS 高速缓存污染、伪造电子邮件等
十二	不可预知因素	1、 机房遭遇火灾事故； 2、 机房遭遇地震事故；

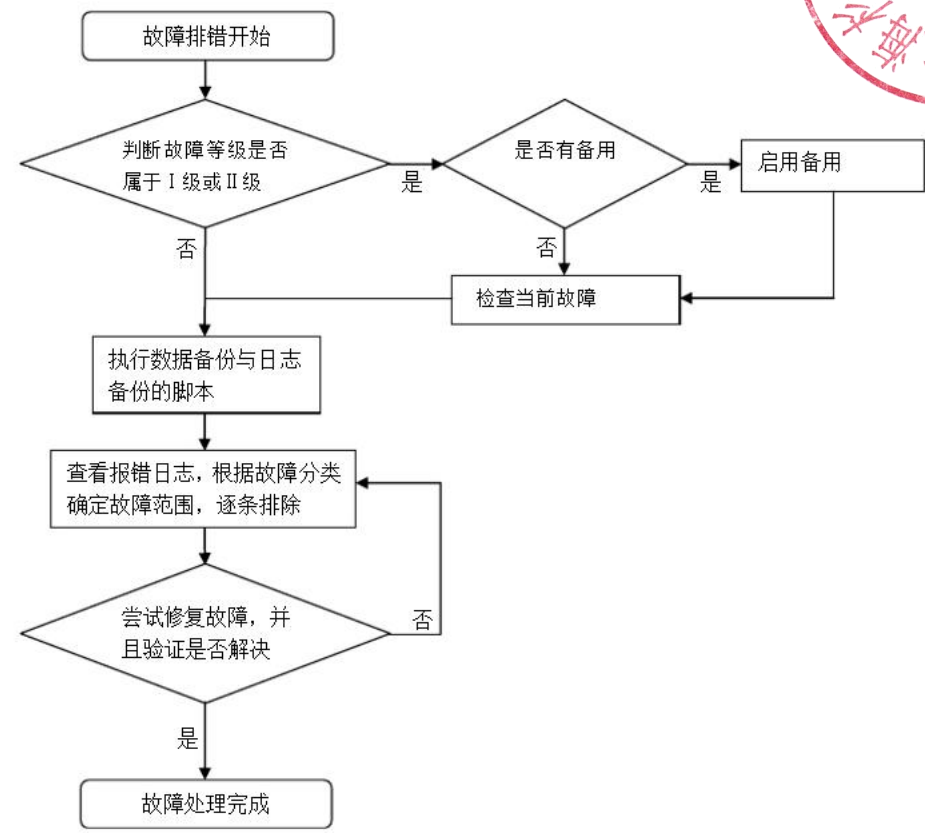


5.4.13.8. 应急处理流程





5.4.13.9. 应急排错流程



5.4.13.10. 应急日志备份

在故障修复过程中，任何一次对系统内核参数、网络策略、数据库监听、应用中间件或档案业务系统配置文件的微调，都可能因版本差异、字符集冲突或权限漂移而引发级联风险，甚至导致业务中断与数据损毁。为此，我们始终坚持“先备份、再动手”的铁律：借助杉木电子自研的 Shell 自动备份脚本，在变更窗口开启前 3 分钟，对 /etc、/opt、/var/log、数据库 spfile、控制文件、归档日志、Web 容器配置、SSL 证书及档案影像文件等关键路径进行一致性快照；脚本内置时间戳、MD5 校验与异地加密推送功能，可在 30 秒内完成全量或增量备份，并自动生成可回溯的清单文件。一旦回退触发，运维人员仅需一条命令即可将系统秒级恢复至变更前状态，确保浦东新区档案信息系统高可用与数据零丢失。



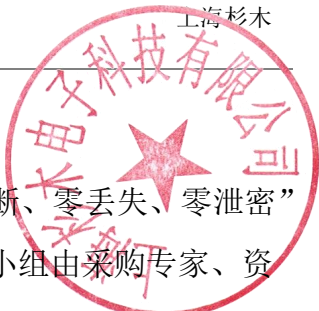
5.4.13.11. 故障处理报告

(1) 故障报告命名规则

文件名前缀	故障级别	名称	故障类型
故障处理报告	I 级—紧急	设备名称	故障分类—详细内容
	II 级—重要		
	III 级—关键		
	IV 级—告警		

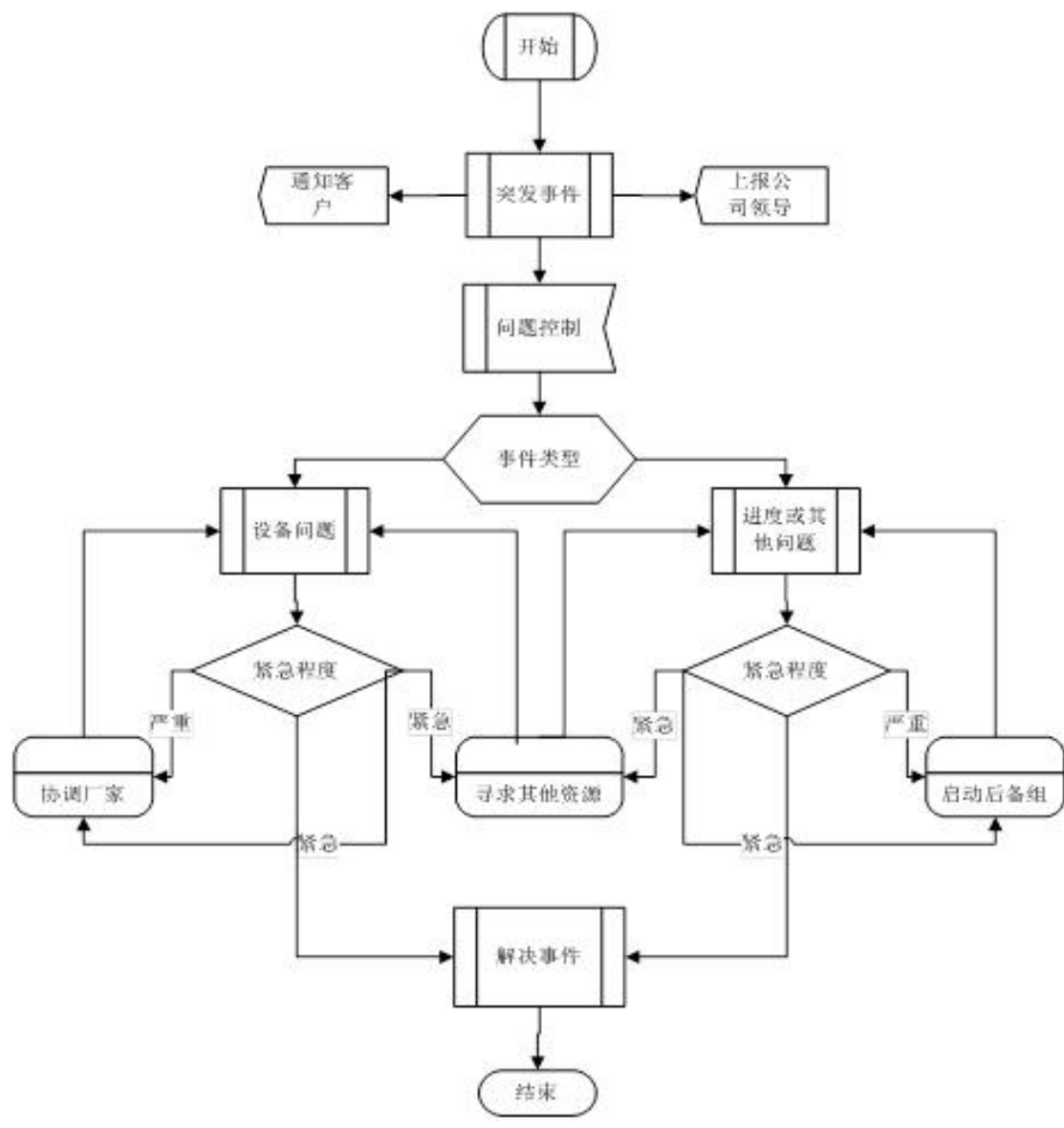
(2) 故障报告内容

故障发现时间	Xxxx 年 xx 月 xx 日 xx:xx (24 小时制)
处理完成时间	如果处理一次就解决的直接写: Xxxx 年 xx 月 xx 日 xx:xx (24 小时制) 如果多次处理后才解决, 按下面格式写: Xxxx 年 xx 月 xx 日 xx:xx (24 小时制) Xxxx 年 xx 月 xx 日 xx:xx (24 小时制) Xxxx 年 xx 月 xx 日 xx:xx (24 小时制)
故障处理人员	
故障描述	根据故障等级划分的说明加上一些详细的内容
故障处理过程	故障排错的详细过程, 可以用图表形式表达
故障原因	导致故障发生的原因
解决方法	写上最终用什么方式解决故障问题



5.4.13.12. 应急事件响应

为在极端情况下仍确保浦东新区档案信息系统“零中断、零丢失、零泄密”，我方已组建跨部门的“档案安全应急技术后备小组”。小组由采购专家、资深技术工程师、质控主管及安全审计员共同构成，实行7×24小时AB角轮值。我们将突发事件精准划分为“严重”与“紧急”两个等级：一旦监测到异常，15分钟内完成事件定级，同步启动后备组三级响应——一级远程会诊、二级现场驰援、三级指挥升级；与此同时，立即触发与华为、华三、深信服、戴尔、Veritas等原厂的联合应急通道，并调用公司备用机房、备机备件库及云灾备资源。依托内部既定应急流程，30分钟内完成应急预案的精准匹配与快速下发，确保在最短时间内恢复核心业务，保障档案数据完整与业务连续。





(1) 通信保障

在本项目中，项目领导小组组长和副组长分别兼任应急总指挥和副总指挥。

应急总指挥、副总指挥和各相关负责人手机24小时开通，随时保持联系。

如需加班处理时，由应急总指挥确认相关人员加班或值班。

(2) 汇报制度

在项目组服务人员已确认风险影响的情况下，应在第一时间向本项目组负责人进行汇报，各级人员均应在第一时间向上级汇报；

如果出现暂时无法联系的情况，可越级汇报或通知可联系到的项目组成员。

(3) 升级制度

在风险影响处理过程中，按照职能、层次分别进行升级。

故障升级管理说明表：

类别	定义
职能升级	当风险解决的时间已经超过解决期限的50%，若处理人员仍未找到相应的解决方案,应立即将故障情况通知上级负责人转给应急副总指挥（由公司相关领导兼任）协调二线支持。
	当风险解决的时间已经超过解决期限的80%，若二线支持仍未找到相应的解决方案,应立即将故障转给应急副总指挥和总指挥（由公司相关领导兼任），协调专家团队等三线支持。
层次升级	若在风险解决期限内，风险未能解决，应通知应急指挥更高一级的管理人员。



5.4.14. 典型事件应急处理方案

5.4.14.1. 应急概述

为了充分保障浦东新区档案局信息化硬件平台的稳定、可靠运行，我司运维团队在强化日常现场人工巡检的基础上，将深度依托已建成的一体化监控管理平台，实现对各类预警与故障信息的实时捕捉与智能分析，从而显著缩短故障排查与处置时间，全面提升应急响应效率。

该监控平台作为一个综合性的监控管理系统，不仅能够对硬件平台中的服务器、存储、网络设备以及关键业务应用进行7×24小时统一监控，还具备强大的数据汇聚与分析能力。系统可对采集的性能指标、日志事件进行多维度关联分析，精准定位故障根源，并依托完善的预警机制与报告功能，实现从“被动救火”到“主动防控”的运维模式转变。

平台已配置系统预警与故障短信即时通知功能。一旦系统检测到异常阈值触发或产生故障告警信息，相关运维责任人将在第一时间通过短信接收详细告警内容，包括设备类型、故障位置、异常指标等，从而迅速启动处理流程，极大提升了故障响应速度与处理时效。

此外，针对机房运行环境的安全保障，我们在机房动环监控系统中同样部署了短信报警功能。一旦出现温湿度越限、漏水、烟感报警等异常情况，系统将立即向运维人员发送告警信息，确保机房环境类故障也能在第一时间被发现和处理，有效避免因环境问题引发的设备宕机或数据丢失风险，全面构建“人防+技防”的双重保障体系。

5.4.14.2. 一般事故

当发生各类突发事故（例如紧急断电、硬件设备故障、网络瘫痪、服务器宕机、数据库异常终止、关键系统服务意外中止等）时，现场运维人员应首先保持冷静，并迅速、准确地判断故障类型与影响范围。

若判定为硬件设备故障（如服务器宕机、存储异常、网络设备失效等），应立即启动相应的硬件应急预案，积极采取隔离、重启或切换等措施，同时第一时间联系硬件维护部门或相关厂商进行紧急抢修。如环境中已部署备用设备，

应毫不犹豫地执行主备切换或设备替换操作，力争在最短时间内恢复系统基本运行能力，最大限度减少业务中断时间。

如属于软件类故障（如数据库异常终止、系统服务崩溃、应用无响应等），须立即组织技术支持人员进行问题排查与调试，收集相关日志、进程状态及错误信息以辅助定位根源。同时，应依据运维协议与服务等级协议（SLA），及时联系相应软件供应商或技术支援团队，寻求远程或现场支持，协同诊断并解决问题，以期尽快恢复正常服务。

综上，清晰的事故判断、有序的应急响应以及高效的团队—厂商协作，是有效控制故障影响、保障系统恢复速度的关键所在。

5.4.14.3. 网络故障

(1) 互联网

在日常运维中，我们坚持在网络运行状态最佳时，定期导出Cisco 3750的最新配置文件，这些配置不仅涵盖了VLAN划分、路由策略、访问控制列表等关键信息，还记录了网络优化的每一个细节。这份配置备份，如同网络的“基因图谱”，是快速恢复网络服务的钥匙。

一旦遭遇Cisco 3750宕机的突发状况，我们将迅速启动应急响应机制，无缝切换至备用的华三（H3C）交换机。通过精确导入事先备份的配置文件，华三交换机能够在最短时间内“克隆”出原网络的核心功能，确保业务连续性不受影响。这一策略不仅体现了我们对网络高可用性的极致追求，也彰显了在复杂网络环境中，多品牌设备协同作战的强大能力，为构建稳定、高效、灵活的网络架构奠定了坚实基础。

(2) 政务外网

政务外网作为数字政府的中枢神经，其稳定性关乎民生服务与公共治理的每一根“毛细血管”。核心区采用两台H3C S5560X做堆叠，双机合一，控制平面与数据平面无缝冗余，任何一台突发故障，另一台可秒级接管，配合预布的光铜缆双上联，现场仅需把关键网线拨到幸存成员端口，业务即可“无感”续

行， $RT0 \approx 0$ 。然而堆叠并非“免死金牌”，极端场景下整机框宕、软件裂脑、配置漂移仍可能发生。为此，我们坚持“配置即资产”理念：每周在业务低峰期通过iMC自动拉取最新running-config，连同堆叠编号、MAD检测、VLAN接口、ACL/QoS策略、OSPF/BGP精细调参一并加密备份，离线存放并做哈希校验，确保一字节不差。

同时，备件库常备一台同型号S5560X冷机，固件版本、堆叠优先级、License预配一致，故障告警一旦升级，值班组立即携备机上架，导入配置后重启堆叠，原拓扑MAC、ARP、FIB表项自动同步，30分钟内即可恢复双机热备。通过“实时冗余+快速替换”的双保险，政务外网真正做到“单点故障不过夜”，让数据多跑路、群众少跑腿的承诺永不掉线。

(3) 局域网

在本单位局域网的主干枢纽，我们部署了一对H3C S7506E作为“双核引擎”。两台设备启用IRF2智能弹性架构，跨框链路聚合成一条逻辑通道，控制与转发平面实时同步，形成真正的“云级”主备。正常运行时，流量被均匀哈希到各业务板，充分利用7.2 Tbps的交换容量；当任一7506E遭遇断电、板卡故障或软件异常时，另一台在毫秒级完成角色升主，MAC、FIB、ARP、ACL状态无缝接管，终端侧仅表现为一次Ping包抖动，RTO趋近于零。

同时，核心到汇聚采用双上行，并运行BFD与OSPF联动，链路失效50 ms内即可触发路由收敛；配合MAD分裂检测与心跳线，彻底杜绝“双主”风险。日常运维中，我们通过iMC定期导出IRF配置、License及补丁基线，冷备一台同版本7506E待命，确保极端灾难下也能30分钟内恢复双核冗余。双机热备加固态存储，让整网稳如磐石，为办公、生产乃至视频会议提供7×24小时不间断的“动脉级”保障。

5.4.14.4. 人为故障

在数字化时代，网络安全关乎国家安全、企业运营和个人隐私，而人为破坏作为网络安全威胁中最不可预测且危害极大的因素，一旦发生，必须迅速、精准、有效地应对。当人为破坏事件发生时，首要任务是冷静判断破坏的来源与性质，明确是内部人员误操作、恶意破坏，还是外部黑客入侵、社会工程攻

击，或是供应链、第三方服务商的违规介入。只有准确识别攻击路径与动机，才能为后续处置提供依据，避免“头痛医头、脚痛医脚”的盲目应对。

在确认破坏来源后，应立即启动应急响应机制，第一时间断开影响系统安全与稳定运行的关键设备，如核心交换机、防火墙、服务器等，防止破坏行为进一步扩散，造成更大范围的数据泄露或服务瘫痪。同时，迅速切断与破坏来源的所有网络连接，关闭相关端口、隔离可疑VLAN或网段，阻断攻击者的持续渗透通道，确保破坏行为被“封控”在最小范围内，避免“二次伤害”。

在此基础上，组织专业力量对破坏行为进行深度溯源，通过日志审计、流量分析、威胁情报比对等手段，精准追踪并锁定破坏来源的IP地址、MAC地址、登录账号、操作轨迹等关键网络信息，形成完整的证据链，为后续的责任追究和法律维权提供坚实依据。同时，对被破坏的信息系统进行全面“体检”，评估数据完整性、配置变更情况及潜在后门风险，采用备份恢复、补丁修复、配置回滚等技术手段，对被破坏的信息进行快速修复，确保系统在最短时间内恢复正常运行，将业务中断损失降至最低。

此外，还需根据事件性质和影响范围，分类制定并实施后续加固方案：对内部人员误操作，强化权限管控与操作审计，推行“双人复核”机制；对外部攻击，升级防火墙策略，部署入侵检测与防御系统，定期开展渗透测试；对供应链风险，建立第三方安全评估与准入制度，签订安全责任协议。通过“应急处置+源头治理+长效防范”的全链条管理，构建“事前预警、事中控制、事后复盘”的闭环安全体系，切实提升网络运维的抗人为破坏能力，筑牢数字空间的“安全堤坝”。

(1) 网络入侵

当病毒警报骤响，运维的第一动作是“定界”：把攻击平面拆成外网、内网两大战场。若源头来自外网，立即锁定首次握手的外层IP，防火墙上秒级关闭被刺探的开放端口，将入侵地址扔进“黑名单”并联动WAF做深度特征过滤；若攻击流量仍呈指数级攀升，果断在边界路由层面临时断开该网段路由，让病毒“呼叫”彻底失联。

一旦溯源指向内网，则迅速切换至“精准清除”模式：通过802.1X日志与DHCP分配表定位中毒终端的真实IP、交换机端口及对应上网账号，即刻

shutdown 该端口，把病毒锁在“单厢”内，防止横向感染文件服务器或域控。随后提取样本流量，回灌至沙箱复盘漏洞利用链，依据回放结果升级 IPS 规则库，补齐杀软无法覆盖的 0-day 检测盲区，实现“发现—隔离—溯源—加固”闭环，确保病毒再无“二次登台”的机会。

(2) 病毒传播

病毒告警一响，分秒必争。先凭流量镜像与EDR日志锁定首台“毒源”主机，即刻shutdown对应交换机端口，物理切断扩散通道；同步抓包判明病毒家族、C2外联特征及所占用高危端口，边界防火墙一键封禁，将TCP/UDP“后门”统统焊死。随后把样本MD5、IP、域名、漏洞利用链写成“战报”，推送至企业微信群、ITSM公告板和官网，附带一键排查脚本、补丁下载与免疫工具，让全员10分钟内完成自查加固，把“单机感染”终结在萌芽，确保网络快速恢复“绿色”运行。

(3) 数据篡改

当监控平台闪现“哈希值异常”红色警报，数据篡改故障被确认瞬间，运维立即启动“熔断”机制：先通过4A审计系统反向追溯会话，锁定可疑账号与终端，一键强制下线并停用其所有VPN、无线及有线接入权限，确保恶意之手无法再触碰任何生产库；同时快照被篡改卷，冻结同步复制链路，防止脏数据继续级联到异地容灾端。随后，应急组依托CDM连续数据保护，在沙箱内比对最后一份可信黄金副本，仅用分钟级即完成差异修复，并触发应用级校验脚本，逐条核对订单、合同、财务凭证等关键表记录，确认零误差后重新开放只读查询，最终在RT0<30分钟之内让业务系统重回“可信”状态，并自动生成篡改溯源报告，为后续司法取证与内控整改提供铁证。

(4) 其它人为事件

面对网络运维中层出不穷的“非典型”故障，我们始终秉持“先阻断、再定位、后复原”的总原则：第一时间把异常模块或网段切换到隔离VZAN，确保生产流量不受牵连；随后结合日志、SNMP 镜像与 AI 基线进行多维交叉分析，判断是协议缺陷、驱动冲突还是供电环境突变，对症下药升级补丁、替换光模块或调整空调风道。

若故障超越现团队技术边界——如芯片级硬件失效、嵌入式系统崩溃、私有协议异常——则在 15 分钟内启动原厂绿色通道，同步上传 Trace、Core Dump 及现场照片，借助厂商实验室的深度诊断与专属 Firmware 修复，实现 7×24 小时联合值守，直至告警彻底消除并输出根因报告，确保每一次“未知”都能被迅速转化为“已知”，让网络重回稳健运行轨道。

5.4.14.5. 紧急事故【断电】

(1) 涉及系统

因电力故障中断供电影响到的系统：

- ✓ 对硬件设备的直接影响
- ✓ 对业务连续性的影响
- ✓ 对数据安全和完整性的影响
- ✓ 对各硬件支撑平台影响
- ✓ 对运维工作的影响

(2) 应急计划

中断前

- ✓ 通知各级领导和科室，包括档案局分管领导和运维服务商相关主管领导和科室；
- ✓ 提前做好各种数据的保存、备份工作，并在时间允许的情况下，有序关闭信息系统设备，一般承载重要数据的设备优先级最高、小型机优先级高于 PC 优先级、价值高的设备的优先级高于价值低的设备的优先级；
- ✓ 向有关部门确定停电的时间长度，做好准备工作；
- ✓ 如果时间允许，则对网络设备和安全设备进行备份和关机操作，按照核心设备→汇聚设备→接入设备的顺序。



中断时

- ✓ 停电期间，确保机房安全，严格控制人员出入；
- ✓ 停电期间，空调系统将停止运行，机房温度会持续升高，陆续关闭已经备份好的相关设备。如果停电时间超过机房 UPS 所能供电的时限，则在备份完毕后关闭所有设备。

电力恢复

- ✓ 在机房温湿度环境适合的情况下，开启机房内相关设备，一般顺序为【有主到次】网络→安全设备→存储设备→主机设备，并检查网络的连通性，如遇硬件故障、无法及时修复的用备件更换；
- ✓ 如数据库服务器发生硬件故障，无法在短时间内恢复应用，由于系统本身采用 vcs 双机热备，oracle 数据库切换至另外一台服务器上，设备则根据“设备保修”流程进行相关处理。

(3) 事后总结

在应急处置的整个过程中，各环节执行人在完成所负责的故障诊断、系统恢复、业务验证等具体操作后，需及时、准确地将处理过程与结果信息进行汇总，并统一提交至应急处置工作小组。该小组对信息进行整合与复核后，将系统、清晰地向上级相关领导汇报事件解决情况，包括事件原因、影响范围、处理措施、恢复结果及后续风险等内容。

事件处置结束后，工作小组须牵头组织针对性的评估与总结工作，重点分析事件根源及处置过程中暴露的流程缺陷、协作短板或技术不足，并据此提出改进措施。同时，应对灾难恢复预案进行相应的复审与维护，更新预案内容，优化响应流程，从而提升未来应对类似事件的效率和能力，形成闭环管理机制。



5.4.14.6. 紧急事故【数据库】

(1) 现状概述

浦东新区档案局目前建立了较为完备的数据备份与灾难恢复体系，采用同城备份中心与本地磁带备份相结合、异地保存重要数据的多重保障模式。当发生灾难性事件时，可依据预定的数据恢复程序，有序开展系统与数据的还原工作。

该备份方案具有成本可控、配置灵活、实施便捷的特点，能够有效应对一般性故障与局部灾难。然而，随着业务数据量的持续增长，磁带备份方式在恢复大量数据时，可能面临恢复窗口过长、时效性难以保证的挑战。

为此，浦东新区档案局制定了清晰的数据恢复优先级策略：在灾难发生后，将优先恢复关键业务数据，确保核心系统与服务快速重新上线；在关键数据恢复完成之后，再逐步恢复非关键数据，从而在有限时间内最大程度保障业务的连续性。

目前，档案局已实施规范化的备份策略，包括每天执行增量备份、每周执行全量备份，确保数据损失风险最小化，并为灾难恢复提供不同时间粒度的数据副本支持。整体而言，该体系在成本与可靠性之间取得了较好平衡，并为未来向实时复制、云备份等更先进模式的演进奠定了基础。

(2) 应急计划

数据库在运行过程中可能发生的故障主要可分为以下三类：磁盘故障或误删文件、系统内部故障，以及用户误操作导致的逻辑故障。针对不同类型的故障，需采取相应的数据恢复策略，其通用恢复步骤概述如下：

首先，需准确判断故障类型及影响范围，并立即确定最适合用于恢复的有效备份集（如全量备份、增量备份或归档日志）。若发生磁盘损坏或文件误删除，需首先从备份中还原受损或丢失的数据文件；若为系统级故障（如实例崩溃、控制文件损坏），则可能需要恢复关键系统文件并利用归档日志执行恢复；若为用户误操作（如误删除重要表或数据），则可结合闪回技术或基于时间点的不完全恢复将数据还原至错误发生前的状态。

在整个恢复过程中，需严格遵循预定的恢复流程，并完成恢复后的数据一致性验证工作，以确保数据库处于可用且正确的状态。

磁盘故障或误删文件

当数据库文件所在的磁盘发生故障，或由于误操作删除了数据库的关键文件（如数据文件、控制文件等），从而导致数据库无法正常访问时，可遵循以下步骤进行恢复操作：

首先，应立即处理底层磁盘故障，例如更换损坏的磁盘或修复存储路径，确保硬件环境恢复正常。随后，建议执行一次冷备份（即关闭数据库后的完整备份），作为恢复过程中的额外保险，防止后续操作中出现意外。在此基础上，利用之前已建立的热备份（如在线备份集及归档日志）开展恢复工作。可针对单个文件、多个文件或整个数据库实施恢复，通过应用归档日志和重做数据，将数据库向前滚动到故障发生前的最后一刻。

由于此类故障一般不涉及逻辑层面的数据错误（如误删除表或记录），因此通常能够将数据库完整恢复至故障前的一致性状态，从而实现几乎零数据丢失的高可靠性恢复。

系统故障

当数据库本身发生内部运算故障，导致整个数据库或关键的SYS表空间不可用时，此类故障在实际生产环境中发生概率极低，但一旦出现则严重影响系统可用性。

若数据库部署于高可用集群环境中，应首先尝试执行集群切换操作，将服务转移至健康节点，往往可通过这一方式快速恢复业务，且通常无需数据恢复。若集群切换无法解决根本问题，则需借助热备份实施基于特定时间点的全库恢复。在此之前，建议先执行一次冷备份，作为重要兜底措施，为后续恢复提供额外保障。随后，利用已有的热备份（包括数据文件、控制文件及连续的归档日志）将数据库还原至故障发生之前最近一个正常状态的时间点。需要注意的是，该时间点之后至故障发生前所有已提交的数据将无法保留，会造成部分数据丢失。

由于此恢复方式需重构整个数据库，其恢复耗时相对较长，应在预案中充分考虑恢复时间目标（RTO）与数据恢复点目标（RPO）之间的平衡。

用户操作故障

当用户对某个表、若干表或其他数据对象（如索引、视图等）执行了错误操作（如误删除、误更新或误截断等），导致这些数据对象不可用或数据异常，但数据库整体服务仍处于正常运行状态时，可按下述步骤进行数据恢复：

首先，为保障恢复过程安全可控，建议立即执行一次冷备份，作为恢复前的状态快照，起到事中保险作用。随后，确定需恢复的数据对象所在的表空间，并据此定位对应的备份文件。接下来，删除当前存在故障或错误的数据对象，进而从事先准备的备份文件中抽取部分或全部相关数据，通过 import 工具（如 Oracle Data Pump 的 impdp）执行导入操作，使该数据对象恢复至备份创建时刻的正常状态。此方法将造成自备份时刻至故障发生前期间内的数据丢失，损失范围可控但需业务方确认。

若该数据对象未包含在常规的“数据库备份操作部署”规划范围内，缺乏可用的逻辑备份，则应转而利用热备份与归档日志，将整个数据库基于时间点恢复（Point-in-Time Recovery, PITR）到错误发生前的某一正常状态。该方法虽恢复时间较长，但可最大程度减少数据损失，恢复对象范围亦覆盖全库。

(3) 事后总结

在数据库崩溃事件成功恢复后，应由应急处置工作小组负责整理和汇总整个恢复过程的关键信息，并形成书面报告，统一向主管领导进行汇报。汇报内容需涵盖事件发生的时间点、故障根本原因、受影响的数据范围、业务中断时长、采取的恢复步骤、数据恢复的完整性与一致性验证结果，以及最终的业务恢复状态。

随后，工作小组需组织专项评估与总结会议，针对本次崩溃事件及处置过程中暴露的薄弱环节，如监控盲点、应急流程缺陷、人员操作失误或预案缺失等，进行深入分析并提出改进措施。此外，应根据总结的经验与教训，对现有的数据库灾难恢复预案进行更新和维护，包括优化恢复流程、明确角色职责、补充常见故障场景的处理方案，并安排后续的应急演练，以提升未来应对类似数据库崩溃事件的响应能力与恢复效率。



5.4.14.7. 紧急事故【存储】

当发生存储故障时，可能导致数据库及全文数据丢失，此时需启动数据恢复流程。恢复操作可通过两种主要途径实施：一是从磁带备份中还原数据，二是利用二级存储中的备份数据进行快速恢复。在存储故障发生时，首先需将二级存储设备 import 至主机，以便接管服务。为实现这一目标，二级存储需依据一级存储原有的挂载结构和参数，完成文件系统的正确挂载，确保其能够被操作系统识别并对外提供服务。

文件系统挂载成功后，即可基于二级存储中预留的备份数据执行恢复操作，逐步将数据库及关联数据还原至可用状态。为提升系统冗余与故障应对能力，当前在政务外网和局域网环境中，均已采用华为存储逐步汰换故障率较高的旧款 SATA 存储设备。新一代存储不仅显著提升可靠性，也同步实现了存储容量的扩展。

此外，原有的 SUN3510 存储阵列经调整后，目前主要用于冷备份及配合 NBU（NetBackup）执行备份任务，成为灾备体系中的重要一环。若发生存储故障，可优先使用 SUN3510 冷备份中的数据快速恢复生产服务，此举将极大缩短业务中断时间，降低故障对业务连续性的影响。待主体存储恢复且业务稳定后，将在非工作时间段内，逐步执行缺失数据的同步与补齐操作，以确保数据的完整性与一致性，最终实现全系统无缝恢复。

5.4.14.8. 紧急事故【云平台】

虚拟化平台的故障根据其影响范围及严重程度，可划分为三个主要层级：虚拟机级故障、宿主机级故障以及VCenter集群级故障。各类故障的表现特征、对业务的影响及应对策略如下：

首先，VCenter集群故障指用于集中管理虚拟化环境的管理平台发生异常。此类故障会导致无法通过VCenter对集群内的主机和虚拟机进行日常管理操作，

例如资源调配、虚拟机迁移或配置修改等。需要注意的是，尽管管理功能受限，绝大多数正在运行的虚拟机业务通常不会受到影响，仍可继续正常提供服务。恢复过程侧重于尽快修复VCenter服务本身，以恢复管理能力。

其次，宿主机故障指单台或多台物理服务器发生硬件或系统级故障。该故障将直接影响运行于该主机之上的所有虚拟机，导致其服务中断。如虚拟化集群中已配置HA（高可用）功能，系统将自动检测宿主机状态，并在检测到故障后，自动将受影响虚拟机迁移至集群中其他健康宿主机上重新启动。该切换过程通常伴随短暂的服务中断（具体时长取决于虚拟机配置及存储性能），但可显著提升业务整体的可用性。

最后，虚拟机故障通常源于客户操作系统内部问题、应用异常或资源配置冲突。此类故障一般仅影响单个虚拟机及其上运行的业务服务（若业务系统自身未配置应用层集群或负载均衡，则会导致服务完全中断）。一旦发生，应首先尝试重启虚拟机或恢复其应用服务。若问题依旧，则需结合备份快照进行快速还原，或从备份中恢复数据，以最大限度地缩短业务中断时间。

综上所述，构建一个具备高可用性、并配备完善监控与应急响应流程的虚拟化平台，是保障云业务连续性的关键基石。

5.4.14.9. 信息安全事故

在数字政府与关键信息基础设施深度融合的当下，任何信息安全事件都可能牵一发而动全身。运维团队的信息入口被严格梳理为“三线并流”：

第一，7×24小时值守的预警平台，通过流量镜像、日志范式化与威胁情报碰撞，实时吐出高、中、低三级告警；

第二，内部OA、电话、即时通讯构成的“人工哨兵”，确保业务处室、开发中心、数据中心发现的异常5分钟内即可抵达值班台；

第三，来自网信办、公安网安、上级主管厅局的通报工单，以加密邮件和传真“双轨”落地，杜绝遗漏。信息一旦汇聚，值班长立即启动“黄金十分钟”先期处置：先依据SLA矩阵评估事件可能造成的影响与损失——是否涉及敏感数据、是否跨域扩散、是否影响实时交易——随后通过语音+工单同步向用户方（

信息化主管部门）进行一事一报。用户在汇总技术侧、业务侧与合规侧信息后，30分钟内完成性质判定：确属网络与信息安全突发事件的，立即对照应急预案分级响应（Ⅰ级断网、Ⅱ级限流、Ⅲ级加固）；经核实为误报的，由二线工程师撰写《误报溯源报告》，优化监测阈值；若判定为供电、空调、线路故障等非安全事件，则转交后勤或运营商团队并全程留痕。

通过“三线收集—快速研判—分类闭环”机制，确保任何异常信号都能被及时消化，实现“小事不过班、大事不过夜”，为用户提供可验证、可追溯、可审计的安全兜底。

5.5. 故障恢复方案

5.5.1. 恢复方案概述

随着信息化建设的日益深入，社会发展对网络与信息系统的依赖程度不断提升，众多重点行业与部门的信息系统已逐步成为国家运行所不可或缺的关键基础设施。对企业而言，信息系统的持续稳定运行更是保障其核心业务正常开展的重要基础。然而，这些承载企业命脉的信息系统自建成之初，便持续面临各类故障与突发事件的威胁。系统可能因硬件失效、软件错误、人为操作失误、外部攻击或自然灾害等原因，出现部分功能异常甚至全面瘫痪，严重影响企业运营与社会服务。因此，如何有效增强信息系统抵御故障及重大事故的能力，最大限度地降低中断时间与经济损失，已成为当前企业信息化建设中的重大挑战。

所谓故障恢复，是指通过一系列事先设计的活动与流程，将信息系统从故障导致的异常或停机状态恢复至可正常运行的状态，并使其所支持的各项业务功能重新达到可接受的服务水平。该过程不仅涉及技术组件的修复与重启，更包括业务连续性管理、数据一致性保障以及用户体验的无感切换等多方面内容。其核心目标在于最大限度减轻故障对企业运营及社会秩序所造成的负面影响，确保关键业务功能在灾难发生之后能够迅速恢复，并继续提供可靠服务。

值得注意的是，故障恢复机制主要针对的是那些发生概率较低但一旦发生即会造成严重影响的高风险事件。在绝大多数情况下，为故障恢复所准备的备

份资源（如冗余设备、灾备中心、备用网络链路等）处于闲置状态，这在带来一定资源闲置成本的同时，也隐藏着“备而不用、用而不灵”的风险。若真发生故障而备份系统未能如期启动或有效接管业务，将可能引发巨大的经济损失与社会信任危机。因此，故障恢复能力不仅是一项技术任务，更是一项需要严格管理、持续验证和高度专业化的系统工程。

这也对负责实施故障恢复的运维服务厂商提出了极高要求。服务提供商必须对客户信息系统的架构、组件及业务依赖关系具有深入的理解，并应配备高水平的技术团队，团队成员须掌握从硬件维护到数据恢复、从应急响应到业务回切等一系列专业技能。此外，为保障在真实故障场景中能够沉着、迅速、有效地采取行动，这些技术人员还需定期参与故障恢复演练，不断积累处理突发问题的实战经验。只有在日常运维中不断验证和优化恢复流程，才能在真正面临危机时有条不紊地执行恢复计划。

为了确保在故障发生时能够顺利启动并执行故障恢复流程，企业必须建立严格的管理规范与组织保障机制。这包括制定详尽的故障恢复预案（Disaster Recovery Plan, DRP）、明确责任分工、设定恢复时间目标（RTO）与恢复点目标（RPO），并建立应急指挥与沟通机制。此外，运维服务团队应具备先进的故障恢复理念，如基于云平台的容灾架构、自动化故障检测与切换机制，以及融合冗余设计和快速重建能力的现代化灾备方案。通过完善的管理模式与持续的技术更新，方能在保障系统日常安全稳定运行的基础上，在真实故障或定期演练中实现信息系统的快速、平滑恢复。

综上所述，故障恢复不仅是企业信息化建设的关键组成部分，更是提升组织韧性和业务连续性的核心手段。它要求技术、流程和人员三方面紧密结合，通过系统化的设计和持续的演练，构建起一道可靠的安全防线，从而在面对不可预知的中断事件时，最大程度地保障企业及社会的信息安全与功能延续。



5.5.2. 目标、任务、计划

5.5.2.1. 目标

故障恢复演练是确保故障备份系统和恢复计划持续有效性的关键环节。通过定期组织演练，用户能够系统性地实现以下几方面的重要目标：

首先，演练的核心目的是全面检验既有的故障恢复计划是否真正满足实际的业务恢复需求。它帮助识别计划中可能存在的漏洞、过时内容或不切实际的假设，从而确保预案在真实故障场景中的可行性与有效性。

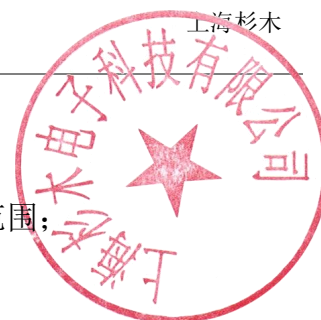
其次，演练致力于验证故障恢复系统的高可用性、高可靠性与高响应度。通过在模拟环境中执行切换、回切等操作，可评估系统在压力下的性能表现及其容错能力，确保技术架构符合设计预期。

演练可用于客观衡量当前的故障恢复水平是否达到用户预先设定的恢复目标，包括恢复时间目标（RTO）、恢复点目标（RPO）和网络恢复目标（NRO）等关键指标。这一过程使恢复能力的评估变得可量化、可追溯。

同时，演练也是对故障备份系统实际处理能力的一次重要检验。包括其数据一致性、负载支持能力、与生产系统之间的同步性能等，确保备份资源在需要时能够顺利接管业务。

最后，演练显著提升恢复团队的技术熟练度与应急协作能力。通过真实场景的模拟操作，团队成员能够积累实战经验、优化沟通流程、增强在紧急状况下的判断与决策能力，从而在真实故障发生时能够迅速、有效地执行恢复任务。

综上所述，故障恢复演练不仅是一次技术验证，更是组织连续性运营管理中不可或缺的管理活动，它从技术、流程和人员三个维度全面提升系统的可靠性与恢复保障能力。



5.5.2.2. 任务

- ✓ 协助用户方制定演练策略，确定演练的目标和范围；
- ✓ 协助用户方建立首次演练组织机构；
- ✓ 协助用户方确定演练的范围、演练参与部门等；
- ✓ 协助用户方制定演练实施方案和演练工作计划；
- ✓ 对用户方演练参与人员进行故障恢复计划和故障演练的培训；
- ✓ 协助用户方制定演练记录模板和演练测试用例；
- ✓ 负责准备演练环境，如 IT 系统环境、工作与生活环境等；
- ✓ 协助用户方组织并实施演练；
- ✓ 负责提供为首次演练提供技术支持；
- ✓ 协助用户方记录演练过程中的各项工作；
- ✓ 协助用户方进行故障演练的总结与评估；
- ✓ 协助用户方对故障恢复计划进行更新。
- ✓ 每年两次故障恢复演练。

5.5.2.3. 计划

在Oracle数据库的运维过程中，有效的备份与恢复策略是保障数据安全与业务连续性的核心环节。Oracle数据库可能发生的故障类型多样，总体上可归纳为三类：磁盘故障或误删文件、Oracle系统内部故障，以及用户操作故障。针对不同类型的故障，需采取相应的恢复手段。以下将详细阐述基于备份的恢复步骤，以系统化地应对各类数据灾难。

首先，针对磁盘故障或误删文件类问题。这类故障通常源于存储硬件损坏，或误删除数据库关键文件（如数据文件、控制文件、重做日志文件等），导致数据库实例无法正常启动或运行。其恢复流程应包括以下几个步骤：第一步，立即处理硬件故障，如更换损坏磁盘，或从操作系统中恢复误删的文件（若仍存在于回收站中）。

第二步，出于保险起见，执行一次冷备份（即关闭数据库后的完全备份），以避免在恢复过程中发生进一步的数据丢失。第三步，依据事先制定的热备份策略，基于具体受损的文件进行恢复。可恢复的范围可以是单个数据文件、控

制文件，也可以是整个数据库。由于此类故障一般不伴随逻辑错误，因此通常能够将数据库完全恢复至故障发生前的最近状态，数据丢失极低，接近零损失。

其次，是Oracle系统自身故障。该类故障概率较低，一般表现为数据库核心进程异常、SYS表空间损坏或集群节点失效等，导致数据库服务不可用。在采用Oracle RAC集群架构的环境中，可首先尝试通过服务切换至健康节点以快速恢复业务。若切换无法解决问题，则需启动基于时间点（Point-in-Time Recovery）的全库恢复机制。恢复前同样建议先执行冷备份以保存当前状态。接着，使用之前制作的热备份将数据库整体回退至某个已知正常的时刻。需要注意的是，这种恢复方式会导致自该时间点以后至故障发生前的所有数据变动丢失，因此需结合业务情况审慎选择恢复时点。此外，全库恢复操作涉及数据重建，耗时较长，对业务连续性有较大影响，需提前制定详细的应急预案。

第三类常见故障是用户操作错误。例如误执行了DELETE、DROP或TRUNCATE等操作，导致部分表或其他数据对象损坏或丢失，但数据库整体仍处于运行状态。这类情况适合使用逻辑备份工具（如Oracle Data Pump中的expdp/impdp）进行恢复。恢复过程包括：首先对当前数据库进行一次冷备份，以保留故障发生后的状态，防止恢复操作中的意外。其次，确定待恢复对象所在的表空间，并定位对应的逻辑备份文件（导出文件）。然后，直接删除或清理故障数据对象，最后通过import操作将逻辑备份文件中相应的数据内容重新导入。该方法可将对象恢复至备份生成时的状态，因此自备份以后至误操作之前的数据将会丢失。如果该数据对象未包含在常规逻辑备份计划中，则需转而采用基于热备份的时间点恢复方式，将整个数据库回退至错误操作之前的状态。

综上所述，Oracle数据库的备份与恢复是一个系统工程，需针对不同故障类型采取差异化策略，并强调日常备份的有效性与可验证性。同时，任何恢复操作前执行冷备份也是一个重要的保护措施，能够为复杂恢复过程增加一重安全保障。定期恢复演练与恢复计划评审，是确保在真实故障中能够快速、有效执行恢复的关键。



5.5.3. 虚拟化恢复演练

针对本次政务外网虚拟化平台故障演练，我们通过强制关闭物理服务器，模拟在实际运行环境中可能发生的硬件设备突发故障场景。具体流程为：在运行过程中主动将主机断电，进而触发其上层虚拟化环境的应急响应机制。

届时，运行于 ESXi 主机IP地址上的所有虚拟机因宿主机意外断电，将出现异常关机状态。同一集群中担任 VMware HA 主控角色的主机会实时监测集群内各节点的状态；一旦检测到主机心跳信号丢失，并同时发现其上的虚拟机非正常停机，HA 机制将自动判断该 ESXi 主机发生故障，随即启动高可用性恢复流程。系统会自动选择集群内另一台正常运行的宿主机，并在其上重新启动受影响的所有虚拟机，以实现业务的快速恢复。

我司工程师在监控界面中确认相关虚拟机已成功在容灾主机上启动，并验证业务系统可正常访问后，立即对发生故障的主机执行紧急现场检修。维护工作包括：恢复 ESXi 系统至稳定状态，重新配置该主机上的网络、存储及虚拟交换机等参数，并对硬件状态（如电源、硬盘、内存等）进行全面检测。

在确认主机硬件及系统功能完全恢复正常之后，运维人员将其重新纳入 vCenter 统一管理平台。具体步骤包括：清理原有无效状态，通过 vCenter 添加主机操作，并重新配置其与共享存储的连接等。待主机正常加入集群后，需进一步针对该节点重新启用 HA 功能，并调整相应的容错策略，确保其再次成为集群中可用的一员，恢复完整的冗余保护能力，为后续可能发生的故障提供自动切换保障。

本次演练有效验证了虚拟化平台高可用机制的可靠性，也体现出运维团队在应急响应与故障恢复过程中的协调与执行能力。

5.5.4. 机房制冷系统恢复演练

机房基础设施的稳定性是保障业务连续性的基石。其中，空调系统的正常运行直接关系到机房的温湿度环境，一旦出现故障，可能导致设备过热、性能下降甚至硬件损坏，进而引发严重的服务中断。因此，定期组织针对空调系统失效的应急恢复演练，具有极其重要的现实意义。本次演练旨在模拟机房空调

发生故障后，运维团队如何通过一系列紧急物理降温措施，有效控制机房温度上升，为设备抢修或备用空调启动争取宝贵时间，最大限度降低业务影响。

演练开始前，应首先明确指挥链与人员分工，通知相关业务方可能的风险，并确认监控系统运行正常，能够实时告警并记录温度变化。当模拟空调故障发生时，运维团队需立即启动应急预案。

首要措施是迅速启用预先储备的应急降温设备，包括工业级备用风扇、移动式空调等。备用风扇应被立即布置于机房热通道出口或机柜间走廊，促进空气流通，避免热空气滞留。同时，可谨慎开启机房的备用门或窗户（若环境安全允许），利用自然通风辅助散热，但必须确保此举不会引入灰尘、湿气或造成安全隐患。

其次，需迅速识别并临时关停非核心的高发热量设备。例如，可对次要的测试服务器、闲置的存储设备或部分可暂时下电的冗余节点执行有序关机，以快速降低整个机房的发热总量。这一操作要求团队非常熟悉业务优先级和设备热负荷，避免对关键业务造成二次影响。

在整个处置过程中，须有专人持续监测核心区域与机柜内的温湿度传感器读数，并每间隔一定时间汇报温度变化趋势，确保降温措施有效。同时，另一组人员应立即排查空调故障原因，模拟联系维保供应商，执行必要的切换或抢修操作。

演练结束后，团队需集合进行复盘，总结物理降温操作的效率、预案的可操作性、团队响应速度以及沟通机制是否存在短板。应特别评估备用风扇的实际效果、开门窗带来的外部风险、以及关停设备策略是否合理。

通过这样贴近实战的机房空调恢复演练，不仅可以验证应急预案的有效性，更能提升运维团队在真实故障下的协同处置能力和冷静应对信心，从而构建起一道应对基础设施风险的可靠防线。



5.5.5. 数据备份恢复演练

故障备份计划的制定要求具备全面而周详的事前准备，尤其需要深入评估故障可能对业务运行造成的冲击程度，并基于分析结果设计相应的备份策略。在结合当前信息技术领域最新可行技术的基础上，提出契合业务连续性要求的最佳恢复方案。系统备份计划初步建立后，还必须通过反复的测试验证其有效性，依据测试结果持续调整与优化，才能最终构建出一套完整、可靠且可执行的系统恢复方案。

首先，需明确浦东新区档案局信息系统在故障恢复体系中所处的等级水平。根据《重要信息系统故障恢复指南》的相关规定，故障恢复能力可依据七个关键要素被划分为六个等级，这些要素包括：数据备份系统、备用基础设施、备用数据处理系统、备用网络系统、技术支持能力、运行维护管理能力以及故障恢复预案。在实际工作中，应立足于风险分析与业务影响分析（BIA）的结论，科学制定与该信息系统关键程度相匹配的恢复策略。

针对浦东新区档案局信息系统目前尚未建立故障备份中心的现状，可将其故障恢复能力定位于第1级。该级别的主要特征为：在本地执行磁带备份，并将重要数据异地保存。具体而言，在本地完成核心数据的备份后，将备份介质转移至异地场所进行安全保管。发生故障时，依据预定的数据恢复程序，对系统及数据进行复原操作。该方案具有实施成本较低、配置相对简便的优点；然而，随着数据量的不断增长，会面临存储介质管理复杂化的挑战，同时在故障发生时，大量数据的恢复效率较低，可能难以满足快速恢复业务的需求。为缓解该问题，应在恢复过程中区分数据优先级，遵循“先恢复关键数据，后恢复非关键数据”的原则，以最大程度压缩业务中断时间。

基于第1级故障恢复能力的特点，我们制定如下备份策略：每周至少执行一次全量数据备份，备份介质需在符合规定的异地场地进行存放。用户方须确保具备适当的物理环境，以满足介质长期保存的要求，包括温湿度控制、防火防盗等基本条件。此外，我方将协助用户方建立完善的介质存取、验证、转储和销毁管理制度，确保备份数据在存储与流转过程中的完整性、可用性与安全性。

同时，为保证备份数据的可恢复性，我方将定期协助用户方进行备份数据的有效性验证，通过模拟恢复操作检测数据是否可正常读取与还原。此外，还

需共同制定详尽的、经过充分测试与实战演练的故障恢复预案。该预案应覆盖故障识别、应急响应、恢复操作、业务回切等全流程，并明确各环节的负责人与具体步骤。通过定期组织恢复演练，不断检验预案的可行性与有效性，增强技术支持团队和运维管理人员的应急处理能力。

最终，通过上述系统性、多层次的措施，可逐步构建一套科学、可靠、适应浦东新区档案局业务发展需要的信息系统故障恢复体系，从而有效应对潜在的运行风险，保障业务连续性和数据安全。

下表为故障恢复的技术和管理支持

序号	要素	要求
1	数据备份系统	1) 完全数据备份至少每周一次； 2) 备份介质场外存放。
2	备用数据处理系统	—
3	备用网络系统	—
4	备用基础设施	1) 有符合介质存放条件的场地。
5	技术支持	—
6	运行维护支持	1) 有介质存取、验证和转储管理制度；2) 按介质特性对备份数据进行定期的有效性验证。
7	故障恢复预案	有相应的经过完整测试和演练的故障恢复预案

5.5.6. 数据备份演练测试

由于数据库系统在线运行使用，数据库恢复拟在某台空闲主机上（测试主机 的主机名为 ylcs-test）进行测试。测试条件：需分配测试主机与原数据库相应的磁 盘存储空间。

- ✓ 划分相同大小的磁盘空间给测试主机 ylcs-test；
- ✓ 在测试主机 ylcs-test 上创建相关卷组；



- ✓ 创建数据库表空间的数据文件所需的相应逻辑卷；
- ✓ 在测试主机 ylcs-test 上创建数据库；
- ✓ 将数据库备份恢复至测试主机 ylcs-test；
- ✓ 将数据库归档日志文件恢复到测试主机 ylcs-test；
- ✓ 使用备份的控制文件启动数据库；
- ✓ 使用归档日志文件进行数据库恢复；
- ✓ 结束恢复操作；
- ✓ 打开数据库，检查数据一致性。

以上为数据库恢复操作全过程，数据库成功恢复并打开。

5.5.7. 恢复演练总结

在相关演练工作结束后，必须系统性地对演练过程中所暴露的薄弱环节与存在的问题进行全面评估与深入总结。这一环节是提升故障恢复能力的核心，旨在识别当前预案与实际操作之间的差距，包括流程衔接、人员操作、系统响应及资源协调等方面的不足。

基于评估结果，应及时对故障恢复预案进行有针对性的维护和更新，例如修订恢复步骤、调整资源配置、优化协同机制或加强人员培训。只有通过持续的复盘与改进，才能确保预案始终贴合实际需求，具备高度的可操作性和有效性，从而在真实故障发生时能够迅速、有序地支撑业务恢复，最大程度保障信息系统连续性和数据安全。



6. 安全支持系统方案介绍

为保障浦东新区档案局业务系统的安全与稳定运行，我司特制定本信息系统安全解决方案。如蒙中标，我司将结合贵单位实际运行环境与安全需求，从物理安全、网络安全、系统安全、应用安全、CA体系、管理安全及终端管理七个层面，系统性地开展安全加固与优化调整工作。通过部署先进的防护设备、强化访问控制机制、定期漏洞扫描与修复、实施统一身份认证与授权管理，并建立健全安全管理规范与应急响应流程，全面提升系统整体安全性、可靠性和抗风险能力，切实保障档案信息资源的保密性、完整性与可用性。

6.1. 物理安全介绍

保证档案局信息系统各类设备的物理安全，是维护整个网络系统安全稳定运行的基石和首要条件。物理安全主要指通过一系列环境控制与访问管理措施，保护计算机、网络设备、设施及相关介质不受地震、水灾、火灾等自然灾害影响，同时防范因人为操作失误、故意破坏或违法犯罪行为所造成的物理损坏或未授权访问。其核心目标在于构建一个可控、可管、可靠的基础运行环境，从实体层面阻断潜在安全威胁。

物理安全体系通常涵盖以下三大方面：

一是环境安全，包括机房选址、建筑防火与防震结构、电力供应保障、温湿度控制、防水与静电防护等基础设施要求；

二是设备安全，涉及关键设备的固定存放、防盗保护、日常维护管理以及报废销毁流程，确保设备在存储、使用及报废全生命周期均处于受控状态；

三是访问控制与监控，通过设置门禁系统、视频监控、人工巡查和日志记录等手段，严格限制人员进出核心区域，实现对物理访问行为的安全审计与追溯。建立健全的物理安全机制，不仅是信息系统整体安全策略的重要组成部分，也是保障档案数据完整性、可用性与保密性的根本前提。



6.1.1. 环境安全

对档案局信息系统所在环境的安全保护，是保障其物理安全的核心环节，主要包括区域保护和灾难保护两个方面。区域保护旨在通过严格的门禁管理、视频监控、周边界防入侵及分区管控等措施，实现对机房及设备存放区域的全方位访问控制与行为监控，防止未经授权人员进入和人为破坏。

灾难保护则侧重于应对地震、火灾、水灾等自然灾害和突发环境事件，需依据国家标准GB50173-93《电子计算机机房设计规范》、GB2887-89《计算站场地技术条件》及GB9361-88《计算站场地安全要求》，在机房选址、建筑结构防火与抗震、防水防潮、供电保障、空调防雷及电磁屏蔽等方面进行系统化设计与建设，形成一个抗灾能力强、稳定性高的物理环境，从而为信息系统及关键设备的持续可靠运行提供基础保障。

6.1.2. 设备安全

设备安全是保障信息系统物理层面可靠运行的关键环节，其内容主要包括对各类服务器、网络及存储设备等的防盗、防毁坏措施，防止因电磁信息辐射而导致的数据泄露，抵御针对传输线路的窃听与截获行为，抑制电磁干扰，并配备稳定可靠的电源保护机制。

此外，还需通过设备级冗余与备份策略，如双机热备、集群部署及冗余电源等，确保关键设施在单点故障时仍能持续提供服务。最终，这些技术手段需辅以严格的管理制度与流程，同时通过系统性的安全培训全面提升相关人员的安全意识与操作规范性，从而构建起技术与管理并重、防护与响应协同的整体设备安全体系。

6.1.3. 媒介安全

设备安全涵盖媒体数据的安全性与媒体本身的安全防护。为确保信息网络系统的物理安全，除需满足网络规划、场地选择及环境控制等基本要求外，还必须有效防范系统信息通过空间途径扩散的风险。现有理论与工程实践表明，敌方能够借助电磁信息辐射还原技术，在数百米至千米之外截取并复原显示设

备信号，这种跨远距离的非侵入式窃取手段，对计算机系统信息的保密性构成了严重威胁。

为抑制此类空间信号泄露，通常需在物理层面采取针对性防护措施，例如采用电磁屏蔽机柜、低辐射设备、信号干扰装置，或对关键区域进行屏蔽室建设，以尽可能减少辐射强度、阻截信息外泄路径，从而切实保障敏感信息在存储、处理及传输过程中的物理安全性。

正常的物理安全防范措施主要涵盖以下三个方面：

一、主机房及重要信息存储、收发部门的屏蔽处理

为保障核心设备的信息安全，应在这些区域建设具有高效屏蔽性能的屏蔽室，用于安装和运行服务器、磁鼓、磁带及高辐射设备等，从而有效防止电磁信号外泄。为提高屏蔽效果，应对所有与外部连接的部位采取隔离措施，包括信号线、电话线、空调、消防控制线路，以及通风口、波导装置和屏蔽门的密封设计，确保电磁屏蔽的整体性和连续性。

二、本地网及局域网传输线路传导辐射的抑制

由于传统电缆在传输过程中不可避免地存在电磁辐射，目前通常采用光缆替代铜缆进行信号传输。普遍做法是在调制解调器（Modem）等设备出口端设置光电转换接口，通过光缆将信号引出屏蔽室外，从而杜绝因线路传导导致的信息泄露风险。

三、终端设备辐射的主动防护

终端设备——尤其是CRT显示器——在工作时会产生较强电磁辐射，容易造成信息外泄。鉴于终端设备分布广泛，难以全部实施屏蔽室防护，除优先选用低辐射设备外，目前主要采用主动干扰技术，通过部署干扰机发射噪声信号，破坏信息窃取企图。对个别特别重要的终端或集中办公区域，也可采用带可视窗的装饰性屏蔽室方案，在适度降低屏蔽效能的同时显著改善使用体验，使人员可在接近普通环境的状态下工作。



6.2. 网络安全介绍

网络安全是保障档案局信息系统安全稳定运行的核心环节。该体系主要涵盖以下五个方面：

一是访问控制，通过部署防火墙、身份认证与权限管理系统，实现对网络边界及内部资源的严格权限管控；

二是通信保密，采用VPN、加密传输等技术确保数据在传输过程中的机密性与完整性；

三是入侵检测，借助IDS/IPS实时监控网络流量，及时发现并阻断恶意行为；

四是网络安全扫描系统，定期对网络设备及服务进行漏洞评估与风险分析，防患于未然；

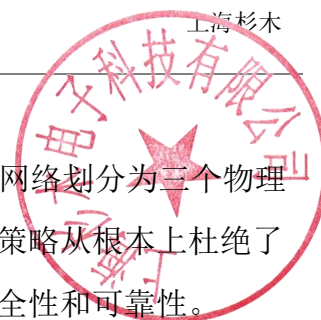
五是全方位防病毒机制，构建覆盖网关、服务器及终端的多层次病毒防护体系，有效遏制恶意代码传播。诸项措施协同运作，共同构筑全面、主动、高效的网络安全防御屏障。

6.2.1. 物理、虚拟控制

(1) 管理制度

为全面完善档案局的信息安全管理体系，我司将协助贵单位系统制定一系列关键的管理规范与制度，具体包括《用户授权实施细则》、《口令字及帐户管理规范》、《权限管理制度》及《安全责任制度》等。这些制度将明确用户身份鉴别、权限分配与审计流程，规范账户生命周期管理，强化口令复杂性要求与定期更换机制，并清晰界定各部门及人员的安全责任，从管理层面系统降低人为操作风险，确保信息系统访问受控、行为可溯、责任到人。

此外，配套管理工具与执行文件，主要包括《机房出入登记表》、《设备操作申请表》、《设备故障报修单》以及《机房管理员规章制度》等。这些文档用于严格管理机房物理访问、设备操作审批、故障处理响应流程，并明确机房管理员的职责与行为规范，从而实现运维操作的标准化、流程化，有效保障核心设施与业务系统的稳定、可靠运行。通过制度与执行文件相结合，可系统构建起一套完整、有效、可持续的信息安全管理机制。



(2) 虚拟子网

档案局依据业务系统的不同特性与安全要求，将整体网络划分为三个物理隔离的部分：局域网、政务外网和因特网。这种物理隔离策略从根本上杜绝了不同网络之间的直接数据交换，有效提高了系统整体的安全性和可靠性。

在档案局内部网络环境中，为进一步细化访问控制，我们基于用户安全级别及不同部门的安全需求，利用三层交换机划分了多个虚拟子网（VLAN）。在不配置路由策略的情况下，各个VLAN之间无法直接通信，从而实现逻辑层面的隔离。通过这种VLAN划分方式，可在网络内部实现初步而有效的访问控制，限制非授权访问，降低内部网络的安全风险，并为后续实施更精细化的安全策略奠定基础。

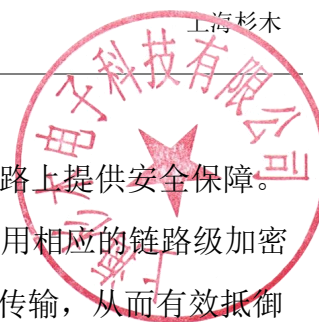
(3) 安全策略

防火墙是构建网络安全体系中最为基础、经济且高效的关键措施之一。它通过预定义的安全策略，有效隔离内外网络或内部网络不同信任域，并实施精细化的访问控制。防火墙不仅支持单向或双向通信管控，还能基于应用层协议实现细粒度的权限管理，从而显著增强网络的整体安全性。

目前，档案局所部署的华为防火墙具备多层控制能力，覆盖从网络层到应用层的全方位安全管控。该设备不仅能够基于IP地址、端口和协议进行传统访问控制，还支持深度包检测（DPI）、应用识别与用户身份绑定等高级功能，从而实现对复杂网络应用和业务流量的精准管理与防护。凭借其高性能与高可靠性，该防火墙为档案局信息系统构建了一道关键防线，有效阻截外部威胁并约束内部越权行为，为整体网络安全提供了坚实保障。

6.2.2. 通信链路加密

为确保浦东新区档案局信息系统中所传输敏感数据的机密性与完整性，有效防止数据在公共或内部网络传输过程中被窃取或篡改，需采用可靠的加密技术对数据进行保护。通过部署加密设备，可将网络上传输的明文数据转换为密文，使得即便数据被截获，非授权用户也无法读取或篡改其内容。当前，主要可采用链路层加密与网络层加密两种技术方式实现该目标。



(1) 链路层加密技术

链路加密主要用于在各保密网络节点之间的广域网线路上提供安全保障。根据实际使用的通信线路类型（如DDN、帧中继等），可选用相应的链路级加密设备，确保保密网内各节点间所交换的数据均以加密形式传输，从而有效抵御数据窃听与篡改风险。

链路加密机的加密机制基于点对点方式运作，即在需要进行加密通信的每一条外线线路上两端均需部署一台加密设备。通过两端加密机的协同工作，实现数据的实时加密与解密。该方式安全性较高，但若网络规模较大、节点众多，则需配备大量加密机，可能导致设备投资成本上升，并在后续的系统维护、扩展及升级中增加复杂度。

(2) 网络层加密与 VPN 技术

面对档案局网络节点分布广泛、通信线路类型多样（如DDN、FR等）的实际情况，若全部采用链路加密方案，将显著增加建设与运维成本。因此，我们建议部署网络层加密设备，即虚拟专用网络（VPN）技术，以实现更灵活、更具扩展性的端到端安全传输。

VPN作为一种符合IPsec标准的新型加密手段，可在网络层面对数据包进行加密处理，实现端到端的通信保护。任一网点仅需配备一台VPN加密机，即可根据安全策略，有选择地对敏感数据进行加密，保障其机密性、真实性与完整性。IPsec作为TCP/IP体系中最主流的网络安全协议之一，为VPN设备提供了标准化的实现基础，使其能够通过建立安全的IP隧道，跨越公共网络进行保密传输。

VPN具备显著的配置灵活性，可实现一对一或一对多的安全通信模式。通过在受保护网络与路由器之间部署VPN设备，并依据实际业务需求制定加密策略，系统可允许部分主机通过加密隧道传输数据，其他主机仍以明文方式通信，从而实现安全性与传输效率的最佳平衡。

此外，由于VPN独立于底层物理链路，不仅能够有效降低多链路加密带来的高额设备投资，还可为上层各类应用提供统一的网络安全基础设施，具备良好的扩展性与适应性。随着未来网络升级或提速，VPN可平滑扩展而不需更改加密架构，尤其适合如档案局这类跨区域、多节点的大型政务网络系统。

因此，我们建议在档案局及各分支单位（如惠南节点）网络与公共网络连接的进出口位置广泛部署VPN设备，构建覆盖全系统的可信传输通道。目前浦东新区档案局与南汇点等单位之间已通过VPN实现通讯保护，为进一步提升系统安全性，建议后续酌情采购专业加密机，在多层级、多范围内实施更严格的安全加固，全面提升数据传输的综合防护能力。

6.2.3. 网络入侵检测

防火墙作为网络安全体系中的基础性防护设施，通过严格、精细的安全策略配置，可有效过滤并阻止各类非安全访问请求，显著降低来自外部及内部非可信区域的网络风险。然而，必须明确指出的是，网络安全防御不能仅依赖防火墙这一单一技术手段。网络安全具有系统性、层次性与整体性，必须通过多种安全技术与产品协同配合，构建纵深防御体系。在防火墙进行访问控制的基础上，还需配备其他专项安全产品作为必要补充，其中入侵检测与防御系统（IDS/IPS）是目前最为关键和有效的配套安全措施之一。

入侵检测系统的主要功能是基于已知攻击特征与行为模式，实时监测网络中的各类操作行为。该系统通过持续获取最新的攻击手段信息与恶意代码特征库，对进出关键网段的所有数据流进行全天候监控与记录，并依据预定义的安全策略进行实时响应。响应机制包括自动阻断可疑连接、生成报警日志、发送邮件通知等，从而有效识别并阻止针对网络系统的攻击与恶意行为，防范信息泄露与犯罪活动。

一套完整的入侵检测系统通常由控制台和探测器（也称为网络引擎）两部分组成。控制台作为系统的管理中枢，负责制定、下发及更新检测策略，管理所有探测器的运行状态，并对警报信息进行汇总与分析。探测器则部署于网络关键节点，以旁路侦听方式捕获流经网络的数据流量，对其进出行为进行深度检测与解析，并执行控制台指令作出相应动作。由于探测器采取监听模式而非直接转发或过滤数据包，其部署不会对原有网络传输性能造成显著影响，也避免了单点故障的风险。

目前，浦东新区档案局根据网络分区及业务特点，已在不同网络区域部署了差异化的入侵检测系统：局域网部分采用了绿盟入侵检测系统，以保障内部

核心业务数据的安全；政务外网区域部署了东软入侵检测系统，有效监控与外部政府机构的数据交互；在因特网边界则部署了华为入侵检测系统，严防来自公共网络的各类攻击行为。通过部署多层次、异构的入侵检测产品，档案局能够进一步提升整体网络的实时监测、精准告警与主动防御能力，形成更加完备的网络安全防护体系。

6.2.4. 漏扫系统

网络扫描系统是主动安全防御体系中的重要组成部分，能够对网络中的各类设备与组件——包括Web站点、防火墙、路由器、交换机以及各类基于TCP/IP协议的服务——进行全面的攻击模拟与安全性扫描。该系统通过主动发送探测数据包，识别和分析目标系统可能存在的安全弱点和漏洞，全面评估当前网络安全状况与潜在风险，并生成详细报告，同时提供具有可操作性的修复建议与补救措施，帮助管理员及时加固系统配置，防范于未然。

系统扫描系统则侧重于对网络中运行的所有应用系统进行深度检测。它通过识别应用层协议、服务及配置中存在的安全缺陷，检测诸如SQL注入、跨站脚本（XSS）、身份验证绕过等常见应用漏洞，并自动生成清晰的风险评估报表，为安全管理与决策提供依据。此外，该系统还会针对每一个已识别的漏洞提出具体修补方案，极大提升了安全运维的针对性和效率。

目前，我司已对档案局绿盟漏洞扫描系统及时更新病毒库，实现了对每个区域资产的定期扫描与风险管控，有效增强了内网安全防护能力。然而，在政务外网和因特网接入区域尚未部署相应漏洞扫描设施，存在一定的安全盲区与隐患。为确保整体网络架构的平稳与安全运行，建议在今后的建设中统筹采购并部署相应漏洞扫描系统，覆盖政务外网及互联网边界，以实现全网级安全风险的可知、可控、可处置，构建闭环的网络安全治理体系。

6.2.5. 病毒防护

由于在网络环境下，计算机病毒具有不可估量的威胁性和破坏力，目前档案局在日常办公中普遍采用Windows操作系统，该系统因其广泛使用性和开放性，较易成为病毒攻击的目标。因此，计算机病毒的防范已成为档案局网络安全建

设中一个至关重要、不可忽视的环节。反病毒技术通常可分为预防病毒、检测病毒和杀毒三大类，通过综合运用这些技术，能够有效降低病毒入侵的风险，保障信息系统安全稳定运行。

预防病毒技术主要通过常驻系统内存，并优先取得系统控制权，实现对系统操作的实时监视与判断，从而在病毒试图进入或破坏系统之前予以阻止。该项技术涵盖多种手段，例如对可执行程序进行加密处理、实施引导区保护、系统监控及读写控制（如传统防病毒卡）等。通过这些方法，能够在病毒激活前识别并拦截其行为，从根本上防止病毒对系统造成损害。

检测病毒技术侧重于依据计算机病毒的典型特征进行识别与判断。常见的检测方式包括自身校验、关键字匹配、文件长度变化监测等。利用这些技术，反病毒系统能够迅速准确地定位可疑对象，并进一步判定病毒的具体类型，为后续处理提供依据。该过程不仅依赖于静态的特征码比对，也越来越多地结合启发式分析、行为监控等动态手段，以应对日趋复杂和隐蔽的病毒变种。

杀毒技术是指在识别病毒后，通过深入分析其代码结构，开发出专用于清除病毒并尽可能恢复受感染文件的程序或功能。该技术强调精准清除恶意代码的同时保障原文件的完整性与可用性。在实际部署中，通常需对服务器、工作站上存储的文件、往来电子邮件及移动存储设备等进行频繁和全面的扫描与监测。一旦发现与病毒代码库中特征匹配的恶意程序，反病毒软件会依据策略采取相应措施，如清除病毒、文件更名或直接删除，从而阻断病毒进一步传播。

为全面提升局域网的安全防护能力，档案局已在网络内部部署了亚信安全服务器版杀毒软件。该软件集成了预防、检测与查杀等多项功能，能够实现对病毒生命周期的全面管控，有效遏制病毒在网络环境中的传播与破坏，确保档案信息数据的完整性、可用性与安全性。通过定期更新病毒库、强化终端防护和制定应急响应机制，档案局进一步巩固了网络安全防线，为日常办公提供了可靠的技术保障。



6.3. 系统安全介绍

6.3.1. 网络系统安全

网络结构系统的安全性是整体信息安全体系的基础，主要指网络拓扑结构的合理性、线路与设备的冗余部署，以及是否存在单点故障风险等关键要素。一个合理且安全的网络架构应能够保证关键节点和链路的可靠性，即使在局部发生故障时，仍可维持整体网络的连通性与服务能力。

档案局在网络规划设计阶段，已充分考虑了上述安全要求，实现了较高水平的架构韧性。具体而言，其在拓扑设计上科学划分功能区域，优化数据流向；在线路层面部署冗余链路，确保某一条物理线路中断时业务仍能通过备用路径传输；在路由层面也实施了冗余策略，通过动态路由协议和设备冗余有效防止单点失效情况的发生。因此，从整体架构角度看，档案局网络具备良好的可靠性与自愈能力，结构设计较为合理和安全，能够满足当前业务运行及未来扩展的需要。

6.3.2. 操作系统安全【Linux 系统】

为确保操作系统安全，可采取以下综合策略：

首先，应优先选用安全性较高的网络操作系统，并完成必要的安全配置。在部署阶段，需关闭那些虽不常用但可能带来安全隐患的应用服务，以减少系统被攻击的面。其次，应对存有用户信息和身份认证相关数据的关键文件实施严格的权限控制。例如，在 UNIX/Linux 环境中，需重点限制如 `/.rhost`、`/etc/host`、`/etc/passwd`、`/etc/shadow`、`/etc/group` 等文件的访问权限；在 Windows 系统中，则需对 `LMHOST`、`SAM` 等文件进行严密保护，防止未经授权访问。

另外，应强化口令策略，要求设置复杂度较高的密码，并避免使用与用户个人相关的易猜解信息。同时，需定期更新口令，并及时安装官方发布的安全补丁，以修复已知漏洞。系统内部之间的调用服务应置于私有环境中，不向外部公开，以减少信息暴露。

最后，建议部署专业的安全扫描系统，定期对操作系统进行全面扫描，主动识别存在的安全漏洞或配置缺陷。根据扫描结果，可有针对性地调整网络设

备的配置，或通过升级系统及应用程序来弥补安全隐患，从而提升整体系统的安全性、抗攻击能力。



6.3.3. 操作系统安全【Win 及 UI 界面系统】

为提升基于Windows及国产化UI界面操作系统（如麒麟等）的信息系统安全性，需从系统底层安全配置、访问控制、漏洞管理、服务优化及持续监控等多方面制定综合防护策略。以下为具体管理方案与建议，涵盖账号安全、补丁管理、自动播放设置、服务与端口控制、注册表安全及账号安全测试等方面：

(1) 账号安全管理

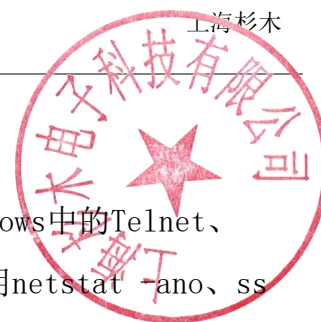
实施严格的账户策略强制使用高复杂度密码，并定期更换（建议90天以内），码长度不少于12位，包含大小写字母、数字及特殊字符。禁用或删除默认账户（如Windows的Guest账户、麒麟系统的测试账户），对管理员账户进行重命名，避免使用常见名称。实行最小权限原则，为不同用户分配所需的最低权限，限制普通用户安装和运行非授权软件。启用账户登录审计与多重认证开启账户登录失败锁定策略，如连续5次失败登录后自动锁定账户30分钟。在支持的环境中部署多因素认证（MFA），如短信验证、USB Key或生物识别，提高关键账户的安全性。

(2) 补丁管理策略

建立系统化的补丁管理机制定期通过官方渠道获取系统及应用程序的安全更新，优先部署高危漏洞补丁。部署内网补丁分发服务器（如WSUS for Windows），或使用国产化系统自带的升级管理工具，实现对终端设备的统一管理和漏洞修复。补丁安装前需在测试环境中进行兼容性和稳定性验证，避免影响业务系统。

(3) 禁用自动播放与外部设备控制

关闭自动运行功能在Windows系统中通过组策略（gpedit.msc）或注册表关闭AutoRun功能，防止U盘、光盘等自动执行恶意程序。在麒麟类系统中通过系统设置或配置文件禁用移动设备的自动挂载与执行。规范外部设备使用管理仅允许授权设备接入，可通过设备管理策略限制未注册USB设备的使用。



(4) 服务与端口管理

最小化系统服务暴露关闭非必需的系统服务（如Windows中的Telnet、Remote Registry服务；麒麟中不必要的网络服务）。使用netstat -ano、ss等命令定期检查活跃端口与关联进程，关闭无用的端口。

部署主机防火墙

配置Windows防火墙或iptables（麒麟系统），仅允许业务必需的端口和协议通信，拒绝所有未经明确的入站请求。

(5) 注册表与系统配置加固

关键注册表项保护在Windows系统中对以下注册表路径设置访问权限限制：

HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

禁止普通用户修改注册表中与系统启动、服务加载相关的键值。

系统安全配置合规化使用安全基线脚本或配置检查工具（如Microsoft Security Compliance Toolkit、开源OpenSCAP）对系统进行加固，并定期审计合规状态。

(6) 账号安全测试与持续监控

定期开展安全渗透与账户审计使用工具（如Hydra、Medusa）模拟暴力破解攻击，检测弱口令账户。开展账户权限提升测试，排查配置错误或权限溢出风险。部署安全审计与行为监控系统开启系统日志记录功能，集中收集和分析账户登录、权限变更等关键事件。

使用EDR类终端检测与响应工具，对异常行为（如异常进程启动、注册表修改）实施实时告警。



6.4. 应用级安全介绍

应用级别安全是信息系统整体安全架构中的关键环节，其核心在于保障软件应用在运行过程中的保密性、完整性与可用性。尤其在当前数字化业务环境中，应用系统直接面向用户、处理关键数据，一旦存在安全漏洞，极易造成数据泄露、越权访问或服务中断等严重后果。因此，构建系统化的应用安全防护机制，并辅以完善的安全管理体系，已成为各类组织在网络安全建设中的重中之重。本文将从系统安全关键技术、安全管理体系框架以及CA认证体系建设三个方面，提出一套完整的应用级安全解决方案。

6.4.1. 系统安全关键技术措施

系统安全是应用安全的基础，主要涵盖身份认证、访问授权、数字签名、操作日志与数据备份等方面，共同构成一道纵深防护屏障。

在身份认证方面，应采用多因素认证（MFA）机制，避免仅依赖用户名和密码的传统方式。推荐整合生物特征识别、硬件令牌或手机动态验证码等多种手段，显著提高账户安全性。对于关键业务系统，应实施强制定期更换密码策略，并对接统一身份管理系统，避免账户信息在不同系统中出现不一致或冗余。

授权机制应遵循“最小权限原则”，基于角色进行访问控制（RBAC）。通过对用户进行分类并明确其可访问资源及操作权限，有效防止越权行为。建议部署权限审计流程，定期审查并调整权限分配情况，确保其与实际业务需求一致。

数字签名技术是保障数据完整性与行为不可否认性的核心措施。在文件传输、合同审批及系统操作等关键环节，应引入基于公钥基础设施（PKI）的数字签名，确保关键数据的来源可信与内容完整。同时，应建立证书生命周期管理机制，包括申请、签发、更新和撤销等全流程管理。

全面、详细的操作日志记录是安全审计与事件追溯的重要依据。应记录用户登录、关键业务操作、系统异常等事件，并集中存储于安全日志服务器，避免本地篡改。利用日志分析工具或安全信息与事件管理系统（SIEM）实现实时监控与异常行为告警，提升安全事件响应速度。

数据备份是系统灾难恢复的最后防线。应制定明确的备份策略，包括备份频率、介质选择和存储地点等，并定期开展恢复演练，验证备份数据的有效性与恢复流程的可行性。对重要数据实施加密备份，防止备份数据被非授权访问。

6.4.2. 安全管理体系构建

建立健全的安全管理体系是实现持续安全运营的保障。该体系应包括明确的安全目标、清晰的架构设计以及可执行的管理规范与技术标准。

安全管理目标应服务于组织的整体战略，致力于降低运营风险，保障业务连续性。典型目标包括：防止敏感数据泄露，确保系统服务高可用，满足国家与行业合规要求（如网络安全法、等级保护制度），以及提升全员安全意识。

在架构设计上，应设立专门的安全管理组织，明确安全团队与开发、运维团队之间的协作关系。推行“安全左移”，将安全要求嵌入系统开发生命周期（SDLC）的各个环节——需求分析、设计、编码、测试和上线运营。同时，构建持续监控与应急响应机制，形成闭环安全管理。

规范与标准是管理体系落地的具体体现。应制定统一的安全管理制度，涵盖账户管理、漏洞响应、数据分类分级及安全运维流程等方面。在技术规范层面，需明确各类应用的安全开发标准（如禁止使用不安全函数、加密算法选型要求）、网络通信安全要求（如强制使用TLS 1.2以上协议）以及安全配置基线（如操作系统、中间件加固规范）。通过定期评审与更新，确保规范的有效性与适用性。

6.4.3. 构建认证体系

公钥基础设施（PKI）及其核心组成部分——认证中心（CA），是现代应用安全的信任基石。构建自有CA体系或合理利用第三方CA，是实现高强度身份认证与数据加密传输的前提。

CA认证体系负责签发和管理数字证书，用于验证通信实体的身份并加密传输数据。部署CA系统时，应首先规划证书策略，明确证书的颁发、使用、更新和注销流程。对于中型及以上组织，建议采用分层结构：设立离线根CA（用于

签发下属CA证书）和在线的中间CA（负责颁发最终用户及设备证书），以提高安全性和灵活性。

在建设过程中，需重点考虑证书生命周期管理的自动化，减少人工操作可能带来的疏漏。可引入证书管理平台，实现证书申请、自动部署、到期提醒和集中撤销等功能。对于对外服务的互联网应用，建议采用全球可信的公共CA所颁发的证书，以确保兼容性与公信力；而对内部系统，则可部署私有CA，便于内部统一管理且降低成本。

此外，应严格保护CA服务器的安全，对根CA实行离线保存、专人管理，并定期进行安全审计与漏洞扫描。只有构建一个可信、可靠和高效的CA认证环境，才能为应用系统提供稳固的身份认证与数据加密能力。

综上所述，应用级安全是一项融合技术、管理与流程的系统工程。组织应从实际风险出发，在关键技术层面强化身份认证与访问控制，在管理层面建立系统化的目标与规范体系，并在基础架构上构建可信的CA认证环境。通过多重措施联动和持续运营改进，方可有效提升应用系统的整体安全水平。

6.5. 终端统一安全管理

在终端网络管理方面，我司推荐使用联软安全网管软件。该软件目前已在单位局域网环境中稳定运行，实践表明其在终端管控、行为审计与安全防护方面表现优异。为进一步提升档案局终端安全管理水平，并适应其不同网络环境中的业务扩展需求，建议将联软网管软件部署范围扩展至政务外网及互联网区域，以实现跨网络环境的统一终端安全管理。

结合档案局实际工作环境与业务特点，现提出包括但不限于以下六个方面的终端安全优化建议：

- 一是强化终端接入控制，确保只有合规设备可接入网络；
- 二是实施精细化权限管理，依据岗位职责严格分配访问权限；
- 三是加强数据防泄漏措施，对重要档案操作行为进行监控与审计；
- 四是定期进行终端漏洞扫描与补丁分发，降低安全风险；

五是构建恶意代码防护体系，实现病毒和木马的有效查杀；

六是建立终端安全状态评估与预警机制，实现对安全事件的快速响应。

通过以上措施，可显著提升终端整体安全防护能力，保障档案数据在各网络环境下的安全性及业务连续性。

6.5.1. 进程检查

通过部署亚信安全终端管理系统，可实现对终端设备上各类应用程序的全面监控，尤其能够精准识别并管控如向日葵、TeamViewer等远程控制及外连软件的使用。该系统可在检测到未经授权的外联行为时，立即向管理员发出实时告警，从而有效防范潜在的数据泄露风险，保障内网资料与敏感信息的安全。

6.5.2. 外接设备检查

该系统能够实时检测计算机是否存在活跃网络连接行为，并识别多类联网方式，如双网卡同时工作、拨号连接及无线网络接入等。同时，它还可对终端访问的网站进行监控与过滤，及时发现并阻断对非法或高风险网站的访问。借助上述功能，可有效防范因终端违规外联可能导致的数据泄露风险，显著提升整体网络与数据安全水平。

6.5.3. 行为审计

通过部署亚信安全终端管理系统，可对终端上的各类操作行为进行全面且细致的审计。该系统提供打印审计、邮件审计、共享审计、进程审计、截屏审计、注册表审计、流量审计及文件审计等多种功能，有效监控终端用户的关键操作与数据流动，帮助管理员及时发现潜在安全风险与违规行为，从而全面掌握终端安全状态，提升整体信息安全防护能力。

6.5.4. 通信网卡检查

通过部署终端安全管理系统，可启用网卡绑定与变动监测功能。一旦检测到终端网卡设置发生未经授权变更，系统将自动发出实时预警通知管理员。管理

员可依据安全策略，及时对该终端执行断网、锁定或强制重启等管控操作，有效阻断潜在违规外联行为，防止敏感数据泄露，切实提升终端安全防护水平。

6.5.5. 外置存储检查

USB接入管理功能提供以下四大核心模块，全面加强对移动存储设备的安全管控：U盘文件审计，可详细记录文件操作行为；U盘安全防护策略，支持读写控制与加密权限设置；USB插拔记录，实时监控设备连接状态并生成审计日志；USB使用控制，基于策略灵活禁用或授权特定设备使用。通过以上功能，有效防范数据通过USB接口泄露的风险，提升终端整体安全性。

6.5.6. 重要信息检查

敏感信息检查功能可对多种文件格式进行深度内容扫描，包括WORD文档、图片、网页文件及压缩包等，精准检测其中是否包含如“机密”、“秘密”、“绝密”等预设或自定义涉敏词汇。一旦识别出含有敏感信息的文件，系统可自动触发预定义响应策略，如立即对终端执行重启、关机、截屏留存现场等操作，及时阻断潜在泄密风险，全面保障档案局核心数据的安全性与保密性。



7. 系统优化方案介绍

7.1. 网络支持平台优化

针对浦东新区档案局当前互联网、政务外网及局域网的多网络运维需求，为实现安全、稳定、高效的一体化运行，特制定以下优化方案：

首先，对三张网络实施精细化分区管理。在互联网出口区域部署新一代防火墙及入侵防御系统（IPS），严格管控访问策略；政务外网严格遵循等级保护要求，强化纵向及横向边界隔离与数据安全交换能力；局域网内部则依据业务部门划分VLAN，抑制广播风暴，提升内部通信效率。

其次，优化网络架构与性能。对核心交换设备进行冗余部署，提升关键路径的可用性。实施流量整形与 QoS 策略，优先保障档案查询、电子文件传输等关键业务的带宽与低延迟。同时，引入网络性能监控平台（如Zabbix、PRTG），实现对全网设备状态、流量及应用的实时可视化监控与主动预警。

最后，建立健全统一的安全运维管理体系。制定覆盖三网的标准化运维流程与应急响应预案，定期开展网络漏洞扫描与渗透测试。加强对运维人员的权限分级与操作审计，确保运维行为可管、可控、可追溯，全面保障档案信息资产在网络环境中的安全性、完整性和可用性。

7.2. 系统支持平台

7.2.1. 主机系统

当前主机系统已持续运行超过多年，随着业务发展和系统更新迭代，操作系统层面逐渐积累了大量临时文件、冗余日志、无效注册表项及废弃缓存等垃圾数据。这些残留内容不仅占据了宝贵的存储空间，更可能引发性能下降、程序响应迟缓及系统稳定性降低等问题。同时，遗留配置偏差、未清理的废弃账户及过期服务也可能构成潜在的安全漏洞，面临被利用的风险。因此，亟需对文件系统进行全面清理与结构优化，包括冗余数据清除、存储空间整理、权限审计与关键目录重构等工作，以提升系统整体健康度和运行效率。

另一方面，当前绝大部分业务服务器已迁移至虚拟化平台，实现了资源的弹性分配和高可用性保障。然而，仍有少量应用系统运行在陈旧实体服务器上。这些物理设备连续运行年限较长，部分组件如硬盘、内存、电源等已进入故障高发期，导致系统中断风险显著增加，维护成本不断上升。此外，老旧硬件平台难以支持现代安全机制，存在难以修补的固件漏洞和兼容性问题，进一步加大了运维风险。为此，迫切需要制定完整的迁移计划，将遗留应用系统从实体服务器平稳迁移至虚拟化环境，并逐步淘汰老旧硬件设备，从而实现资源整合、提升可靠性并强化安全防护体系。

7.2.2. 虚拟化系统

为提升虚拟化平台的稳定性与性能，需制定系统性的硬件更新策略。应有计划地采购新型服务器，逐步替换已超期服役或性能不足的旧设备，以提升整体资源处理能力和能效比。被替换下来的旧设备可经检测与重新配置后，用于构建非核心业务的测试环境、开发环境或灾备节点，从而实现资源的梯次利用，既节约成本，也为关键业务释放出更可靠的主资源池，避免“一刀切”替换带来的资源浪费与业务中断风险。

应根据不同业务系统的性能需求、重要性和负载特征，实施精细化的资源分配策略。对关键业务系统（如数据库服务、档案查询应用等），应在CPU、内存及存储IOPS等方面给予充分且有冗余的资源保障；而对非核心或低负载系统，则可适度控制资源配额，以提高整体资源利用率。通过这种差异化管理，既可避免资源争抢导致的性能瓶颈，也能防止资源闲置，实现虚拟化平台资源分配的合理性、灵活性与经济性。

应全面依托虚拟化管理平台自带的性能监控工具，对集群内所有虚拟机的关键指标（如CPU使用率、内存占用、磁盘I/O和网络流量等）进行持续采集与分析。通过设置性能基线及预警阈值，运维团队可及时发现潜在瓶颈与异常状况，并据此对虚拟机实施动态资源调整——如在线添加vCPU、扩展虚拟内存或迁移至负载较轻的主机，从而以数据驱动的方式优化系统性能，提升服务的响应能力与稳定性。

必须建立定期执行的虚拟机备份与恢复验证机制。除了落实常规的数据备份策略之外，还应周期性地对备份环境执行恢复切换测试，模拟真实故障场景，验证备份数据的完整性、一致性和系统功能的可恢复性。通过此类演练，可确保在发生系统故障、数据损坏或灾难事件时，备份系统能够快速启用并接管业务，最大程度减少停机时间，保障档案信息服务的连续性和可靠性。

应对虚拟化平台的整体配置进行全面梳理与优化，充分发挥高级功能以提升系统效能与可用性。例如，可启用DRS（分布式资源调度）实现负载自动均衡，配置vMotion减少计划内停机时间，调整内存共享与超额分配策略以提升资源利用率。同时，还应定期审视虚拟机的硬件兼容性、虚拟网络拓扑及存储多路径策略等，确保其与当前物理基础设施和业务需求保持最佳匹配，从而提升整个虚拟化环境的管理水平与服务质量。

7.3. 安全系统优化

7.3.1. 网络安全

针对档案局业务特点及多网络环境并存的现状，为全面提升互联网、政务外网及局域网的安全防护水平，制定以下网络安全优化方案：

本方案以“分区管控、纵深防御、持续监测、快速响应”为原则，构建覆盖网络边界、内部区域和核心数据的多层次防护体系。在互联网出口区域部署下一代防火墙（NGFW）、入侵防御系统（IPS）及Web应用防火墙（WAF），严格实施访问控制策略，有效防范外部攻击与恶意访问。政务外网严格遵循等级保护2.0相关要求，强化纵向加密、横向隔离，部署安全网关实现可靠的数据交换。局域网内部依据业务职能划分VLAN，实施最小权限访问策略，防止非授权跨网段访问，抑制内部风险扩散。

同时，构建全域统一的安全监测与运维审计体系。部署网络流量分析（NTA）与安全事件管理系统（SIEM），实现对三网流量的实时异常检测与日志关联分析，及时感知威胁动向。实施终端安全管理，加强对服务器及办公设备的漏洞扫描、补丁更新及外设管控。全面推行运维操作审计与数据库审计，确保运维行为可追溯，敏感数据访问受控。

另外，制定并演练专项应急预案，建立跨网络区域的协同响应机制，提升安全事件的快速处置和业务恢复能力。通过定期对网络架构、安全策略及管理流程进行评审和优化，构建持续演进的安全防护体系，切实保障档案信息资源的真实性、完整性和可用性。

7.3.2. 系统安全

目前档案局局域网终端设备安装有亚信服务器版杀毒软件，政务外网、因特网终端安装 360 杀毒软件，并且病毒库更新到最新版本。

自动播放类病毒防不胜防，为了安全起见最好禁止自动播放功能，我司通过 360 安全卫士的系统防护设置，并且也从开始菜单运行命令“gpedit.msc”，通过左侧菜单栏“计算机配置-管理模板-系统”内，找到“自动播放”项，进行关闭操作。

及时安装最新版本的 SP 和 Hotfixes 补丁程序

针对档案局信息系统现状及安全运行需求，拟制定一套覆盖互联网区、政务外网及局域网的整体安全优化方案，以全面提升网络安全防护能力、系统可靠性和数据保密性。本项目立足于国产化替代与主动防御相结合的原则，通过软硬件升级与架构优化，构建可持续、可信任的内生安全环境。

首先，将全面推进国产化软硬件替代工作。逐步替换现有非自主可控的基础设施，部署国产服务器、网络设备及操作系统，从底层降低供应链安全风险，确保核心环境技术自主可控。尤其在政务外网和内部局域网中，优先采用符合国家认证的国产软硬件产品，增强整体系统的安全基线。

其次，构建覆盖三网的恶意代码防护体系。在所有服务器及终端设备上部署统一管理的国产杀毒软件，确保病毒库实时更新，并定期执行全盘扫描。同时，针对网络边界部署防病毒网关，对流入流出数据包进行深度检测，实现“云-管-端”一体化防护，有效阻断恶意代码传播路径。

此外，实施严格的网络分区与访问控制策略。在不同网络区域之间部署下一代防火墙，配置细粒度的安全策略，仅允许必要的业务流量跨域访问。关键业务系统部署主机加固与入侵防护系统，并对运维行为实施审计与监控，有效防范非授权访问和内外网攻击。

最后，建立持续性的安全运维与应急响应机制。定期开展漏洞扫描与渗透测试，及时修补系统漏洞，同时制定详尽的应急响应预案，并组织演练，确保在安全事件发生时能迅速有效处置，全力保障档案数据安全和业务连续性。

7.4. 存储系统优化

为全面提升档案局信息系统的数据管理能力与服务连续性，现针对存储架构与虚拟化环境提出以下优化方案，以应对当前设备老化、资源分散及高可用性需求不足的挑战：

(1) 整合多平台存储资源，构建统一存储池

当前档案局的业务系统数据分散于多个独立存储平台，存在资源利用率不均衡、管理复杂及扩容困难等问题。需对现有存储资源进行全面梳理与整合，根据业务特点（如电子档案查询频繁、数据增量、保密性要求高等）和数据增长趋势，采用集中化存储管理策略。通过虚拟化存储技术将不同厂商和型号的存储设备整合为统一的资源池，实现存储空间的弹性分配与动态调度。此举不仅可提升存储利用率，减少冗余投资，还能简化日常运维，并为未来数据分级存储和自动化生命周期管理奠定基础。

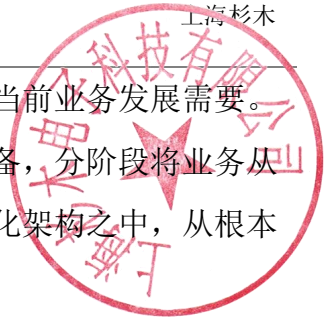
(2) 优化局域网虚拟化环境，部署共享存储以支持高可用机制

目前档案局局域网虚拟化平台因缺乏共享存储架构，无法实现诸如VMware HA（高可用）、vMotion（实时迁移）等关键功能，存在单点故障风险。建议改造现有架构，部署支持光纤通道或iSCSI协议的集中式共享存储系统，使所有虚拟化主机均可访问同一存储资源。在此基础上启用高可用功能后，当单台物理主机发生故障时，其承载的虚拟机可自动在集群内其他主机上重新启动，极大缩短业务中断时间，显著提升档案信息服务的可靠性和连续性。

(3) 新增存储与交换设备，逐步淘汰老旧小型机

现有存储容量已难以应对电子档案规模的持续增长，建议为局域网环境新增一套高性能、高可靠性的集中式存储系统，用于扩展存储空间并提升I/O性能。同时，新增2套共4台光纤交换机，构建冗余 Fabric 网络，消除网络单点瓶颈，确存储网络的高带宽与高可用。目前仍在运行的小型机设备使用年限已远超

出正常生命周期，故障风险高且维护成本巨大，难以满足当前业务发展需要。建议尽快制定迁移与替代计划，采购新的存储与服务器设备，分阶段将业务从小型机迁移至更具扩展性和可靠性的虚拟化平台或现代云化架构之中，从根本上保障档案核心数据的安全性与业务系统的稳定运行。





8. 项目风险管控

8.1. 风控概述

本次运维工作所涉及的档案局档案信息系统支撑平台，是一项结构复杂、功能全面、覆盖广泛的大型信息系统。该系统承载着档案管理与服务的核心业务，其稳定运行直接关系到档案信息资源的安全性、可用性与完整性。为确保本项目达到预期目标，切实发挥系统运维在保障业务连续性、提升服务品质方面的关键作用，必须在项目实施前全面、系统地开展风险预测与评估工作，科学识别各类潜在风险，并制定具有针对性和可操作性的控制与应对措施。

只有通过事前充分的风险研判，建立健全风险管控机制，才能在面临技术、管理、协调及外部环境等多方面不确定性时，做到从容应对、有的放矢，最大程度降低风险对项目推进与系统运行的影响，从而确保本项目顺利实施并最终取得圆满成功。

8.2. 管理方法

为保证项目实施的质量与最终成功率，我们制定并采用了一套严格且系统化的项目风险管理方法。在本项目的全生命周期建设中，将严格依据该方法论对各类潜在风险进行主动识别、科学评估与动态管控。整个风险管理过程构建为一个持续改进的闭环系统，其核心在于实时响应变化、循环反馈与策略优化。

具体而言，在项目推进过程中，随着风险处置计划的逐步落实，原有风险状况可能发生变化，也可能涌现出新风险。这些动态信息将通过预设机制及时反馈至风险管理团队。风险预测与识别人员随后对反馈信息进行汇总与分析，重新评估风险的等级、发生概率和潜在影响，并据此审视现行处置措施的有效性。

基于新一轮评估结果，项目团队可对风险处置计划进行灵活调整与迭代，包括修订应对策略、重新分配资源、增强缓解措施等，并迅速部署和实施更新后的风险处置方案。该过程不断循环运作，形成识别—评估—应对—反馈—调整的闭环管理链条，从而确保风险管理始终与项目实际进展和环境变化保持一致。

通过维持风险管理过程的动态性和自适应性，我们能够显著提升对不确定性的应对能力，最终达到风险管理的预期目标，即最大限度地降低风险对项目目标的负面影响，保障项目按期、按质、按预算成功交付。

8.3. 预测识别与分析

项目风险预测与识别是全面风险管理体系的基础与起点。这一阶段的核心任务在于系统性地发现和判断项目中可能存在的各类不确定因素，并初步厘清其属性、成因及可能造成的影响。具体而言，风险预测与识别需要系统回答以下几个关键问题：项目中究竟存在哪些潜在风险因素？这些风险因素可能诱发何种具体风险事件？这些风险一旦发生，其严重程度如何？概括来说，该过程旨在确定风险源、关键致险因素，并对其后果作出初步的定性评估，从而为后续的风险量化与应对策略制定奠定基础。

在实际操作中，风险预测与识别通常借助多种方法结合实现，包括但不限于专家访谈、德尔菲法、头脑风暴、历史项目文档分析、SWOT 分析及故障树分析等。通过多维度、多轮次的筛查与判断，项目团队能够逐步构建风险清单，并对各类风险进行初步分类与描述，例如技术风险、管理风险、资源风险、外部环境风险等。这一阶段的成果，不仅包括风险登记册的建立，更包括对关键风险发生机制和传导路径的深入理解。

在完成风险识别的基础上，需进一步开展风险评估与分析工作。该阶段致力于将前期识别出的风险从定性认知推向定量衡量，即通过建立系统化的风险模型——如概率影响矩阵、蒙特卡洛模拟、敏感性分析、决策树分析等——对风险事件发生可能性及其潜在损失进行估计。评估过程需综合考虑风险之间的关联性与叠加效应，从而科学估算某一风险或多个风险共同发生时对项目目标（如进度、成本、质量等）造成的具体影响。

风险评估的核心目标在于识别出“关键风险”，即那些发生概率较高、一旦发生会造成较大损失的风险，以及那些可能引发连锁反应、具有系统重要性的风险。这些风险应作为风险应对规划中的重点管理对象。通过量化分析，项目团队能够依据客观数据制定优先级策略，将有限的管理资源投入最关键的风险领域，从而提升风险管理的针对性与经济性。

综上所述，风险预测与识别以及风险评估与分析，共同构成了风险管理的决策依据阶段。两者前后衔接、互为支撑：识别是评估的前提，评估是识别的深化。只有系统、全面、科学地完成这两项工作，才能制定出切实有效的风险应对措施，最大程度降低不确定性对项目的负面影响，最终为项目的顺利实施与成功交付提供保障。

8.4. 风险处置

项目风险管理的精髓，在于把看似混沌的不确定转化为可量化、可比较、可应对的清晰图景。首先，团队需借助历史数据、专家访谈、蒙特卡罗模拟与敏感性分析，对风险发生的概率、影响范围、财务损失、声誉冲击、合规代价等多维指标进行交叉测算，形成“概率-损失”热力图；随后引入行业公认的安全阈值与组织风险承受度，将风险划分为红、橙、黄、蓝四个危险等级，直观回答“风险有多大”“多快必须行动”。在此基础上，进入“风险处置”阶段：对红色高危区，优先采用“风险回避”，通过变更技术路线、压缩高风险功能、终止外包合作等方式，将风险概率直接降为零；

对橙色可控区，实施“风险控制”，以漏洞扫描、双活架构、加密传输、应急演练等手段降低发生概率并削减损失；

对黄色低频低损区，采取“风险自留”，设立应急储备金、购买网络安全保险，用财务手段消化波动；对无法根除且损失巨大的特定风险，则通过“风险转嫁”，以合同条款、SLA罚金、第三方保险或云服务商兜底，把潜在巨灾转移到更专业的承受主体。

最终，针对项目全生命周期的风险清单，编制动态《风险处置路线图》，以“风险回避-控制-自留-转嫁”四位一体的组合拳，实现“成本-效益-安全”的最优平衡，让项目在任何不确定的风浪中都能稳健航行。



9. 文档和培训服务

9.1. 文档规范

在项目全生命周期中，我们将依据项目实际推进情况，协助客户方系统地制定标准规范操作手册，具体涵盖投标产品的日常巡检手册、日常维护手册等一系列关键文档。

整个过程将严格遵循结构化编写流程：

首先明确手册的适用范围与核心内容，依据实际运维场景确定重点；进而设计清晰的手册框架与统一的文档格式，确保逻辑性与可读性；随后编写逐步操作说明，注重细节描述与实际操作对应，必要时附注代码示例以辅助技术人员理解与实施；在此基础上，将积极吸纳档案局技术团队的反馈意见，持续优化手册内容，使其更贴合实际管理需求与使用习惯；

最后通过内部审核与版本迭代机制，保障文档的准确性与时效性，并完成正式发布与共享，确保终端用户能够高效、规范地使用各项产品功能，提升系统整体运维质量与安全管理水平。

9.2. 文档模版

日常巡检

档案局日常巡检

编号：SHSM-JFRCTI-2025-05-001

合同/项目名称：档案信息系统支撑平台运维

日期	局域网				政务外网			
	网络	主机	存储	数据库	网络	主机	存储	数据库
2025/5/1								
2025/5/2								
2025/5/3								
2025/5/4								
2025/5/5	✓	✓	✓	✓	✓	✓	✓	✓
2025/5/6	✓	✓	✓	✓	✓	✓	✓	✓
2025/5/7	✓	✓	✓	✓	✓	✓	✓	✓
2025/5/8	✓	✓	✓	✓	✓	✓	✓	✓
2025/5/9	✓	✓	✓	✓	✓	✓	✓	✓
2025/5/10	✓	✓	✓	✓	✓	✓	✓	✓

机房环境日常巡检记录

上海杉木电子科技有限公司

浦东新区档案局中心机房温湿度记录表

巡检日期：2025 年 4 月 文档编号：SHSM-JFRSD-JL-01

日期	内网机房		外网机房		检查人签名
	温度	湿度	温度	湿度	
4.1	19.6℃	36.7%	19.3℃	36.5%	姜楠
4.2	19.8℃	36.5%	19.4℃	36.7%	姜楠
4.3	20.3℃	35.7%	20.5℃	34.2%	姜楠
4.4	21.5℃	35.5%	21.7℃	36.35%	姜楠

数据系统备份记录2

浦东新区档案局数据、系统备份记录

上海杉木电子科技有限公司

数据系统备份记录 2

浦东新区档案局数据、系统备份记录

上海杉木电子科技有限公司

编号: SHSM-SJAXT-BAK-2025-04-002

合同/项目名称: 档案信息系统支持平台运维

日期

备份时间

备份内容

备份路径

备份大小

备份类型

备注

操作人

2025-4-1	✓	✓	✓	✓	192,188,3,95	每月全备份		
2025-4-2	✓	✓	✓	✓				
2025-4-3	✓	✓	✓	✓				
2025-4-4	✓	✓	✓	✓				
2025-4-5	✓	✓	✓	✓				
2025-4-6	✓	✓	✓	✓				
2025-4-7	✓	✓	✓	✓				
2025-4-8	✓	✓	✓	✓				
2025-4-9	✓	✓	✓	✓				
2025-4-10	✓	✓	✓	✓				
2025-4-11	✓	✓	✓	✓				
2025-4-12	✓	✓	✓	✓				
2025-4-13	✓	✓	✓	✓				
2025-4-14	✓	✓	✓	✓				
2025-4-15	✓	✓	✓	✓				
2025-4-16	✓	✓	✓	✓				
2025-4-17	✓	✓	✓	✓				
2025-4-18	✓	✓	✓	✓				
2025-4-19	✓	✓	✓	✓				
2025-4-20	✓	✓	✓	✓				
2025-4-21	✓	✓	✓	✓				
2025-4-22	✓	✓	✓	✓				
2025-4-23	✓	✓	✓	✓				
2025-4-24	✓	✓	✓	✓				
2025-4-25	✓	✓	✓	✓				
2025-4-26	✓	✓	✓	✓				
2025-4-27	✓	✓	✓	✓				
2025-4-28	✓	✓	✓	✓				
2025-4-29	✓	✓	✓	✓				
2025-4-30	✓	✓	✓	✓				

第 1 页, 共 1 页

编号: SHMJ-SJAXT-BAK-2025-04

合同/项目名称: 档案信息系统支持平台运维

日期

备份时间

备份内容

备份路径

备份大小

备份类型

备注

操作人

2025-4-1	✓	✓	✓	✓				
2025-4-2	✓	✓	✓	✓				
2025-4-3	✓	✓	✓	✓				
2025-4-4	✓	✓	✓	✓				
2025-4-5	✓	✓	✓	✓				
2025-4-6	✓	✓	✓	✓				
2025-4-7	✓	✓	✓	✓				
2025-4-8	✓	✓	✓	✓				
2025-4-9	✓	✓	✓	✓				
2025-4-10	✓	✓	✓	✓				
2025-4-11	✓	✓	✓	✓				
2025-4-12	✓	✓	✓	✓				
2025-4-13	✓	✓	✓	✓				
2025-4-14	✓	✓	✓	✓				
2025-4-15	✓	✓	✓	✓				
2025-4-16	✓	✓	✓	✓				
2025-4-17	✓	✓	✓	✓				
2025-4-18	✓	✓	✓	✓				
2025-4-19	✓	✓	✓	✓				
2025-4-20	✓	✓	✓	✓				
2025-4-21	✓	✓	✓	✓				
2025-4-22	✓	✓	✓	✓				
2025-4-23	✓	✓	✓	✓				
2025-4-24	✓	✓	✓	✓				
2025-4-25	✓	✓	✓	✓				
2025-4-26	✓	✓	✓	✓				
2025-4-27	✓	✓	✓	✓				
2025-4-28	✓	✓	✓	✓				
2025-4-29	✓	✓	✓	✓				
2025-4-30	✓	✓	✓	✓				

第 1 页, 共 1 页

名称	修改日期	类型	大小
杉木电子运维周报 (2025年3月31日-2025年4月7日)	2025/4/7 9:49	XLSX 工作表	
杉木电子运维周报 (2025年4月7日-2025年4月14日)	2025/4/14 10:00	XLSX 工作表	
杉木电子运维周报 (2025年4月14日-2025年4月21日)	2025/4/21 9:48	XLSX 工作表	
杉木电子运维周报 (2025年4月21日-2025年4月28日)	2025/4/28 10:59	XLSX 工作表	
杉木电子运维周报 (2025年4月28日-2025年5月6日)	2025/5/6 14:21	XLSX 工作表	
杉木电子运维周报 (2025年5月6日-2025年5月12日)	2025/5/12 9:40	XLSX 工作表	
杉木电子运维周报 (2025年5月12日-2025年5月19日)	2025/5/19 10:19	XLSX 工作表	
杉木电子运维周报 (2025年5月19日-2025年5月26日)	2025/5/26 9:35	XLSX 工作表	
杉木电子运维周报 (2025年5月26日-2025年6月3日)	2025/6/3 9:41	XLSX 工作表	
杉木电子运维周报 (2025年6月3日-2025年6月9日)	2025/6/9 10:18	XLSX 工作表	
杉木电子运维周报 (2025年6月9日-2025年6月16日)	2025/6/16 10:40	XLSX 工作表	
杉木电子运维周报 (2025年6月16日-2025年6月23日)	2025/6/23 9:40	XLSX 工作表	
杉木电子运维周报 (2025年6月23日-2025年6月30日)	2025/7/1 11:33	XLSX 工作表	
2025年4月度总结	2025/5/10 10:12	文件夹	
2025年5月度总结	2025/6/30 9:56	文件夹	
2025年6月度总结	2025/7/1 10:42	文件夹	
2024年12月份杉木运维服务项目月度总结...	2025/2/5 14:14	DOCX 文档	1,993 KB
2025年1月份杉木运维服务项目月度总结...	2025/2/5 14:11	DOCX 文档	1,469 KB
2025年2月份杉木运维服务项目月度总结...	2025/3/3 13:53	DOCX 文档	1,862 KB
2025年3月份杉木运维服务项目月度总结...	2025/4/8 13:55	DOCX 文档	1,907 KB
2025年6月度总结.zip	2025/7/1 10:43	360压缩 ZIP 文件	3,431 KB

周报和月报记录

- 故障处理记录单-2025年1月份.xlsx
- 故障处理记录单-2025年2月份.xlsx
- 故障处理记录单-2025年3月份.xlsx
- 故障处理记录单-2025年4月份.xlsx
- 故障处理记录单-2025年5月份.xlsx
- 故障处理记录单-2025年6月份.xlsx



9.3. 培训目的

为确保用户能够买得放心、用得舒心、维护安心，杉木公司针对本项目特别成立了专业的培训项目小组。该小组将严格遵循ISO9001质量体系标准，制定系统且详尽的培训计划书，全面负责培训工作的组织、实施与质量保障，以确保项目全程培训内容的规范性、有效性与可持续性。

杉木公司在培训领域投入长期且大量资源，致力于为客户提供高水准、标准化与实用性相结合的培训服务。在课程设计上，涵盖计算机体系架构、服务器与存储平台分析、存储与服务器应用选型分析、服务器数据安全维护、应用系统设计、系统调试与故障排除，以及最新芯片技术和管理技术等关键领域。这些课程内容均基于杉木多年来的项目实践与技术积累不断优化而成，兼具前瞻性与实操性，旨在帮助学员全面提升技术理解与实际操作能力。

基于杉木多年项目经验，技术培训被证明是系统长期稳定运行的重要支撑，能够显著提升用户自主运维能力，有效保障业务连续性与安全性。为此，我方结合贵单位的业务特点与实际需求，精心组建了一支经验丰富的讲师团队，并针对本项目量身编写了专用培训教材，制订了全面而细致的培训计划。

我们高度重视客户的反馈与合作，如贵单位对培训内容、形式或进度有任何意见与建议，杉木将积极听取并根据实际需求迅速对培训方案进行调整与优化，确保培训工作真正贴合贵单位的管理与使用习惯，最终实现知识传递与技能提升的目标。

9.4. 培训对象

9.4.1. 现场初级培训

杉木公司将派资深讲师上门，对用户的技术人员进行随机培训和讲解，并可在保证设备安全和正常安调完成的情况下，指导客户现场操作，加深理解和应用能力。

培训对象：用户的技术人员；

培训内容：讲解产品的结构、安装步骤、调试方法和系统配置等；



培训师资：由杉木公司工程师负责提供

培训日期：现场安装或整改时；

培训地点：实施现场；

培训教材：杉木公示将提供书面或者电子版的培训教材；

培训费用：杉木公司将自行承担授课费、教材费等。

9.4.2. 集中进阶培训

主要是面向有一定计算机管理和维护基础的用户，进行设备使用及应用级别的培训；主要是设备使用、维护、管理、调优和故障排除等方面的内容，并在现有的基础上进行提高。按照用户的要求，我们为贵单位提供进阶级别的培训。

培训对象：用户及与本项目有关的其他人员；

培训内容：设备选型、设备使用、数据安全维护、设备管理和调优、故障排除以及其它高级内容；

培训师资：由杉木公司资深工程师负责培训，使用中文培训；

培训日期：由用户指定；

培训地点：国内（具体地点由用户指定）；

培训教材：杉木公司为每位学员提供标准培训课程需要的原厂中文教材，教材包括纸质版和电子版。

培训费用：杉木公司承担师资及教材费用。

9.5. 培训方式

本次项目培训为境内培训，具体采用“集中基础理论培训”与“现场实践技能培训”相结合的方式，分阶段系统性地提升参训人员的理论认知与实操能力。两种培训形式有机结合、互为补充，旨在帮助学员全面掌握相关设备的架构原理、日常维护及故障处理能力。具体安排如下：



9.5.1. 集中授课培训

集中理论培训以课堂讲授为主要形式，通过系统化的课程设置，重点讲解网络设备与服务器的体系架构、工作原理、服务器平台关键技术、设备应用选型原则以及数据安全维护策略等内容。培训将结合典型应用场景与案例，使学员能够初步建立完整的知识框架，掌握常见故障的初步判断与分析方法，为后续现场实操奠定坚实的理论基础。

9.5.2. 现场操作培训

现场培训将依托实际设备进行演示与动手操作，强化学员对硬件设备的感性认知和实际操作能力。通过实物讲解与指导参训人员完成常规操作、日常维护及典型故障判别与处理，进一步增强其独立运维能力。在实操和模拟故障处理过程中，培训讲师将全程陪同，与学员共同分析所遇问题，并及时提供故障判断、排查与解决方面的现场指导，真正实现“学中做、做中学”，切实提升整体技术素养和应急处理水平。

通过上述两类培训形式的有机结合，本项目旨在全面提升用户对系统设备的理解深度与实战能力，保障今后系统维护工作的规范性、安全性与可靠性。

9.6. 培训内容

在项目实施过程中，为确保用户能够全面掌握系统运维相关知识与实操技能，我方将培训划分为两个主要阶段：集中基础理论培训和现场实践技能培训。两部分内容相辅相成，旨在从理论认知与实际操作两个维度全面提升用户的技术能力。

具体安排如下：

- (1) 在服务期内，我方将根据客户指定的时间安排，组织开展集中理论培训。该阶段以课堂教学为主要形式，系统讲授服务器架构、网络原理、设备功能及安全管理等关键知识，帮助学员建立扎实的理论基础，更好地理解系统组成与运行机制。

(2) 在模拟安装与调试环节，我方将采用现场教学方式，重点培养学员的实际动手与问题解决能力。通过设备实际操作、配置模拟和故障排查等训练，使学员能够熟练掌握日常维护和基本调试技能，并在讲师指导下完成从知识到实践的转化。

通过上述结构化培训安排，既可保障学员对系统整体架构的深入理解，也能显著增强其在真实环境中的操作熟练度和应对能力。



10. 验收及考核标准

10.1. 运维质量要求

对于服务范围内的普通故障，系统各平台业务不可用时长不大于 20 小时/月和100 小时/年，单次恢复时长不超过 2 小时重大故障（业务不可用时长>4 小时）次数不大于 5 次/年。

遵守日常行为规范、人员管理制度，遵守现场考勤管理规定。

遵守系统更新管理规范，按更新流程处理，更新方案按标准提交。

遵守应急管理规定，按应急流程对紧急事件进行处理。

运维文档规范、完整、说明清晰，文档质量符合招标人要求。

10.2. 考核管理要求

详细考核办法详见《浦东新区档案局运维项目管理考评规则》。

10.3. 评分办法

浦东新区档案局用户每月组织运维评估，按照评估考评规则打分，得分 $\geq$ 85 分为合格， <85 分为不合格，当月评估为不合格的必须在 5 个工作日内整改到位。

通过考核指标对应评分细则进行打分，具体方式详见：

《浦东新区档案局运维项目管理考评规则》

以下无正文

