



通信业务合作协议

甲方: 白山市浑江区退役军人事务局 (以下简称甲方)

(公章或合同专用章)

法定代表人或授权代表:

注册地址: 白山市浑江区浑江大街 1651 号

联系人: 沙虹宇

联系电话: 18843929576

签署日期: 2025 年 6 月 17 日

乙方: 中国联合网络通信有限公司白山市分公司 (以下简称乙方)

(公章或合同专用章)

负责人或授权代表:

注册地址: 白山市浑江大街 1842 号

联系人: 潘勇鹏

联系电话: 18643995801

签署日期: 2025 年 6 月 16 日

鉴于甲乙双方彼此长期友好的战略合作伙伴关系, 现就双方进一步合作事宜, 本着平等互利、共同发展的原则, 经过甲、乙双方协商, 达成如下协议。

第一条 声明和保证

1.1 甲方拥有独立法人资格, 具备签署本协议所需要的相应权利。

1.2 乙方是国家基础电信运营商。

第二条 合作内容

2.1 鉴于甲乙双方长期友好合作关系, 乙方针对甲方现有办公固定电话, 一条 50M 政务外网电路, 一条 50M 互联网专线, 一条财政 vpn 专线, 乙方给予优惠, 其中固定电话费用 2400 元/年、政务外网电路费用 3600 元/年、互联网专线费用 8160 元/年, 财政 vpn 专线费用 840 元/年; 固话费用包含: 来显、国内语音、悦铃、其他, 400 元/月折扣优惠为 200 元/月, 不足 200 元/月时按 200 元/月收取; 超出 400 元/月时除收取 200 元外, 还要收取超出部分的 60%。合同总价款为人民币【15000】元 (大写:【壹万伍仟元整】), 其中固话、电路增值税税率 9%, 互联网专线、财政 VPN 增值税税率 6%, 合同总价下不含税的价款为人民币【13995.16】元 (大写:【壹万叁仟玖佰玖拾伍元壹角陆分】), 增值税税款为人民币【1004.84】元 (大写:【壹仟零肆元捌角肆分】)。

2.2 收款信息



账户名称: 中国联合网络通信有限公司白山市分公司

开户银行: 中国工商银行八道江支行

银行账号: 0807210329000672195

第三条 甲方的权利和义务

3.1 甲方不得使用乙方提供的用户号码(普通固话号码、手机号码)用于呼叫中心呼出服务,不得使用固话号码开展商业性营销、违规催收、贷款理财、股票推荐、房地产营销等,如出现违规行为,乙方有权关停业务。

3.2 甲方需按时足额向乙方交纳所使用的各项通信费用,如出现欠费,乙方有权按规定停止通信服务,直到补交齐欠费为止。

第四条 乙方的权利和义务

4.1 乙方按照国家规定的通信业务资费标准以及本协议相关约定,有权向甲方收取本协议项下各项费用。

4.2 乙方要主动为甲方做好服务工作,及时协调、解决甲方的各种通信需求。

第五条 质量保障和故障处理

5.1 乙方提供的服务具体标准满足信息产业部颁布的《电信服务标准》,保证甲方使用通信业务安全畅通。

5.2 乙方向甲方提供故障申告电话 10010,每天 24 小时受理甲方的故障申告,在承诺时限内进行修复,甲方应积极予以协助配合。

第六条 违约责任

6.1 任何一方未履行本协议项中的任何一项条款均被视为违约。任何一方在收到对方的具体说明违约的书面通知后,如确认违约行为实际存在,则应在 10 日内对违约行为予以纠正并书面通知对方;如认为违约行为不存在,则应在 10 日内向对方提出书面异议或说明,在此情形下,甲乙双方可就此问题进行协商,协商不成的,按本协议争议条款解决。违约方应承担因自己的违约行为而给守约方造成的实际损失。

6.2 乙方基于甲方承诺使用期限(即协议服务期)给予甲方优惠折扣,因此,如甲方提前停止服务的,甲方还应向乙方补缴该项服务实际使用期间,该项服务按正常资费标准结算与按乙方提供的优惠标准结算之间的差额。前述补缴费用应与该项服务最后一期账款一并向乙方付清。

6.3 如甲方逾期 30 日不交纳费用,乙方有权暂停为甲方提供服务,同时在甲方欠费期间不办理任何业务,并遵照《中华人民共和国电信条例》第三章第三十四条规定,自甲方欠费之日起至甲方付清欠费之日止每日按全部欠费金额的 3%向甲方加收违约金。若甲方在乙方暂停服务 60 日内仍未足额支付欠费及违约金的,则乙方有权单方解除本协议,终止为甲方提供服务,并有权继续追索甲方所欠的全部费用及其违约金,由此导致的责任和后果由甲方承担。

第七条 保密

双方对彼此之间提供的信息、资料以及本协议的具体内容负有保密责任。

第八条 免责条款

因不可抗力导致甲乙双方或一方不能履行或不能完全履行本协议项下有关



义务时,双方相互不承担违约责任。但遇有不可抗力的一方或双方应于不可抗力发生后 15 日内将情况告知对方,并提供有关部门的证明。在不可抗力影响消除后的合理时间内,一方或双方应当继续履行协议。不可抗力事件包括严重自然灾害、政府行为、第三方服务故障等不可抗拒的事件。

第九条 争议的解决

9.1 本协议的成立、效力、解释、履行、签署、变更和终止以及争议的解决均应适用中华人民共和国法律。

9.2 因履行本协议所产生的争议,任何一方有权向乙方所在地的法院提起诉讼。

9.3 除正在诉讼的争议事项外,双方应继续行使其本协议项中的其余权利,并履行本协议项中的其它义务。

第十条 通知

一方向另一方发出的书面信息,应按本协议列明的地址以邮寄、邮件或图文传真的方式发送。任何一方对其联系方式的变更应及时书面通知对方。

第十一条 协议期限

11.1 本协议服务 一 年,自 2025 年 6 月 1 日至 2026 年 5 月 30 日。

11.2 本协议自双方法定代表人(负责人)或授权代表签字并加盖公章(合同专用章)之日起生效,并追溯至上述服务期起始日。

第十二条 产权归属

凡由乙方投资建设的线路及相关设备,其产权归乙方所有。

第十三条 附则

13.1 如遇国家调整有关资费标准,或双方主管部门下达有关政策文件,双方本着真诚合作、友好协商的原则另行商定收费方法。

13.2 本协议未尽事宜,按照《中华人民共和国电信条例》及国家有关规定执行。

13.3 未经甲乙双方书面确认,任何一方不得自行变更或修改本协议。

13.4 本协议一式四份,甲、乙双方各执二份。

13.5 本协议所有附件作为协议不可分割的组成部分,与协议正文具有同等法律效力。



附件 1. 网络安全协议

针对合作中涉及的网络安全、信息安全、数据安全工作,明确双方责任与义务,遵守相关法律法规,双方共同达成本协议,以资共同信守。

1. 甲方责任

1.1 甲方承诺提供的设备、系统、服务等均严格履行国家《网络安全法》及其相关法律法规、行业标准及国家标准有关内容及要求,并按要求取得相应授权或资质证明。提供的设备、系统要进行风险评估,确保安全。甲方要自行对提供的设备进行安全隐患排查,对照国家相关权威单位发布的漏洞预警,定期排查、整改安全隐患。

1.2 甲方承诺合作服务期间,严格按照电信管理机构的规定开展网络安全防护工作,并严格遵守《中国联通合作方网络与信息安全管理办法》。

1.3 甲方承诺签订《信息安全保密协议》和《网络与信息安全和保密承诺书》等文件以备查。

1.4 甲方承诺每年至少开展一次网络安全风险评估,包括网络安全、信息安全、数据安全范畴,并按需向乙方提交评估报告和整改报告。

1.5 甲方承诺主协议服务期间,根据乙方要求配合完成乙方开展或第三方开展的攻防实战演练、应急演练、安全评测和安全检查工作,并针对发现的问题及时完成整改。

1.6 甲方承诺针对主协议服务,制定网络与信息安全事故应急预案,并定期(至少每年一次)组织内部相关人员进行应急响应培训和应急演练,使其掌握岗位职责和应急处理策略和规程。

1.7 甲方要建立完善的信息安全情报获取和响应体系。当有业界情报发现供应链相关的漏洞时,第一时间告知乙方,并对自身产品进行排查,并根据相关信息对产品进行加固。

1.8 甲方设备、系统或软件的安全策略更新时,要进行充分评估和测试后再执行,避免因策略更新导致的业务中断。

1.9 甲方承诺加强甲方所辖参与合作服务的个人终端及设备必须安装乙方指定的终端安全管控软件。甲方更换服务人员前,应书面通知乙方,经乙方同意后,甲方配合做好相关人员操作账号、终端敏感信息的清理工作。

1.10 对于乙方向甲方提供的系统登录用户名和密码,甲方仅用于维护使用不得擅自做其他用途或泄露给第三方。禁止甲方人员掌握相关系统管理员权限,禁止为甲方人员分配具备创建系统账号或者其他超出工作范围权限的高权限账号;甲方账号应实人实名,账号不得转让、转借;甲方应定期对全量账号进行严格审核,控制甲方涉及敏感信息人员的范围。



1.11 甲方不得利用乙方提供的电脑和网络系统,私自连接外网,发送垃圾邮件、攻击网络和计算机系统,不得私自使用外来移动硬盘、U 盘、光盘等移动存储介质,防止计算机病毒传播,危害网络信息安全。

1.12 甲方不得在运行的信息系统上私自开发、挂靠与业务工作无关的软件或系统,不得发布通知或广告。

1.13 如甲方有系统接入吉林联通内部网络时,应进行严格接入认证,需具备双因素认证能力,接入内部网络的设备应做白名单访问限制,不允许使用无线连接方式,并安装符合要求的防病毒软件。

1.14 如合作业务涉及新建系统,必须明确新建系统的安全责任归属,如归属甲方,新建系统不可以带有联通标志、联通相关信息等内容,IP 地址备案、ICP 备案均不得以联通公司名义备案,安全责任要在合同中进行明确。如归属联通公司,由安全责任归属部门按照《吉林联通自有网站、APP 管理办法》进行上线审批。无论系统责任归属,系统日志,应至少保留 6 个月。

1.15 当甲方系统被检测出漏洞时,要在 3 个工作日内完成整改,否则将暂停接入;当涉及严重漏洞时,视情况,乙方有权立即暂停接入,待整改并验证后,方可再次接入。

1.16 甲方承诺做好自有人员及合作相关人员的安全意识培训和宣贯工作(一年不少于四次),确保相关人员严格遵循乙方各项网络信息安全和数据安全管理规定,严格履行“十三不准”:

(1) 不准设置弱口令。

(2) 不准使用非工作邮箱代收工作邮件。

(3) 不准点击来路不明邮件中的链接或打开附件。

(4) 不准将账号和口令明文保存在终端上。

(5) 不准将系统设计文档、网络拓扑等敏感信息存放于服务器上。

(6) 不准将本人使用的账号与口令告知他人。

(7) 不准在互联网上的外部网站或应用(如论坛、微博、即时通信软件等)上使用与乙方设备、系统上相同的账号或口令。

(8) 不准允许来路不明的人员远程控制乙方各类设备或执行其告知的各项指令。

(9) 不准将网站或系统源代码上传至互联网上。

(10) 不准设置乙方业务系统为自动登录。

(11) 不准私自在办公网络及其他内网中搭建无线热点。

(12) 不准将未进行自我检查和安全加固的终端接入内网。

(13) 不准未经审批开通乙方内部系统的互联网出口。

1.17 甲方在出现违反《中国联通合作方网络与信息安全管理办法》的情况或出现网络信息安全事故时,要在发生 12 小时内书面通知乙方,并积极有效的开展应急处置,有效控制风险影响范围,有效压降双方损失。在事件处置完毕后,要提供书面详细真实的事件报告。



2. 乙方责任

2.1 甲方与乙方在签订主协议时,乙方提供并与甲方确认共同遵守《中国联通合作方网络与信息安全管理办法》,同时签订本协议。

3. 违约责任

3.1 甲方违反本协议项中任何约定、陈述或保证的,甲方要承担违约和处罚责任:

(1) 甲方违反了国家法律法规的要求或违反了本协议的约定;

(2) 甲方未能有效履行网络信息安全和数据安全保护责任或该方安全能力未满足国家法律法规的要求;

(3) 甲方在发生安全事件时未能按照本协议的约定通知乙方或未采取相应合理、恰当、有效的补救措施和处置;

(4) 甲方无正当理由拒绝配合乙方进行攻防实战演练、应急演练、安全评测或安全检查和;

(5) 甲方向乙方提供的证明材料、信息等存在虚假、遗漏或误导等情况;

(6) 因甲方原因,乙方出现运营事故,或导致乙方与任何第三方产生任何纠纷,或遭受监管部门通报处罚的;

3.2 乙方有权采取下述一种或多种方式,追究甲方的违约和处罚责任:

(1) 要求甲方立即停止违约行为、予以纠正或采取补救措施;

(2) 采取或要求甲方采取有效补救措施(包括但不限于更改口令、回收权限、断开网络连接等)控制或消除安全风险;

(3) 收回甲方涉事人员所有账号权限,并在相关安全事件处置完毕之前禁止该人员继续参与乙方相关项目;

(4) 要求甲方赔偿乙方因此遭受的全部损失;

(5) 要求甲方按主协议合同含税总价的【10】%支付违约金;

(6) 解除本协议和/或终止双方基于主协议的合作关系;

(7) 若发现甲方行为涉嫌违法犯罪等情节较严重的网络信息安全、数据安全事件,乙方有权依据《中国联通供应商黑名单管理办法》相关规定,将甲方列入中国联通黑名单供应商,采取禁入等措施。

(8) 无论本协议是否终止或解除,乙方有权要求甲方删除、销毁或归还其已提供的数据,并提供其已删除、销毁相关数据的证明。

(9) 因甲方违反本协议项下任何约定、陈述或保证,导致乙方与任何第三方产生任何纠纷,或遭受监管部门处罚的,甲方应当协助乙方进行处理并妥善解决。由此导致乙方遭受任何损失(包括但不限于乙方因此支付的罚款、向第三方支付赔偿金的、和解金、律师费、鉴定费、诉讼费、差旅费以及其他合理开支),甲方应当予以全额赔偿。

3.3 除本协议另有约定外,任何一方违约,造成守约方损失的,违约方应当赔偿守约方遭受的直接损失。



4. 协议的生效与终止

4.1 本协议自双方法定代表人/负责人或授权代表签字并盖章之日起生效，本协议的效力不因《业务协议》的终止或无效而有任何减损。

4.2 本协议在下列情况之一发生时终止：

4.2.1 本协议约定的各项权利义务已履行完毕；

4.2.2 任何一方行使本协议约定的单方解除权，解除通知到达对方时；

4.2.3 双方协商一致终止本协议。

4.3 除本协议或双方另有约定外，本协议终止或解除不能免除各方在履行本协议过程中已产生的权利、义务与责任。

4.4 双方合同解除权行使期限：自任一方知道解除事由之日起至该方书面放弃合同解除权。

5. 其他

5.1 本协议为双方就本协议约定事宜达成的唯一的完整的协议和约定，并取代和废除双方在此之前口头或书面所做出的关于同一事宜的协议、商谈、承诺或声明。

5.2 本协议中所有标题仅为方便阅读所列，并不影响本协议任何部分的含义或解释。



附件 2 信息安全保密协议

鉴于:

- 1、甲乙双方(“双方”)正在进行[通信业务合作]项目(“项目”)。
- 2、在项目合作过程中,乙方已经或将要向甲方提供平台/系统的数据使用权限。
- 3、本协议所述的数据指吉林联通管理、控制的 用户相关数据和企业自身数据,以及反诈法相关法律法规规定的 数据。
- 4、双方均希望对本协议所述数据予以有效保护。

经双方协商,达成本协议。

第一条 保密原则

1.1 遵循《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》《中华人民共和国电信管理条例》《中国联通网络与信息安全管理 办法》《中国联通数据安全管理办法》《中国联通合作方数据安全管理办法》《吉林联通数据安全管理办法》《吉林联通数据安全 管理实施细则》以及其他相关法律法规、国家标准和公司数据安全 管理相关规定。

1.2 保密数据包括但不限于以下内容,如:用户相关数据(姓名、证件号码、手机号码、固定电话号码、宽带账号等及使用情况)、企业自身数据(平台技术数据、网络拓扑数据、合作协议数据等)。

1.3 上述保密数据按照“数据不出门”原则,并对用户相关数据进行加密存储,原则上不将数据带出系统。

1.4 参与项目的员工可以接触到的数据处理相关平台系统,及其数据使用权限、内容、范围及用途,应符合最小化原则。

1.5 涉及个人信息收集、存储、使用、加工、传输、提供等处理行为的,遵循合法、正当、必要原则,征得个人信息主体同意。

第二条 双方权利和义务

2.1 甲方保证对于乙方提供的数据履行保护责任,仅用于与项目有关的如数据分析、挖掘等用途。甲方不得未经同意改变数据使用的目的、方式和范围。甲方不得将数据用于项目以外的任何用途。除为执行项目目的外,甲方不得缓存、窃取、泄露、滥用、非法向他人提供数据、不得对数据进行加工后还原原始数据。未经乙方同意,甲方也不得利用数据进行新的挖掘和使用。甲方应遵守中国联通相关管理办法,并接受必要的安全监控和审计等。

2.2 甲方保证对用户数据予以妥善保管,并对用户数据在甲方期间发生的用户数据被盗、泄露等项承担全部责任,因此造成乙方和乙方用户损失的,甲方应负责赔偿。

2.3 甲方保证对数据和系统账号按本协议约定予以保密,对于具有乙方系统账号的甲方工作人员,须将身份信息提供乙方报备,甲方如发生相关工作人员岗位或职责调整,应及时将变更情况向乙方报备。



2.4甲方保证仅为双方合作项目,将数据提供给确有知悉必要的甲方工作人员。在甲方上述人员知悉该数据前,应向其说明数据的保密性及其应承担的义务,保证上述人员同意接受本协议条款的约束,并对上述人员的保密行为进行有效的监督管理。甲方如发现数据泄露,应采取有效措施防止泄密进一步扩大,并及时告知乙方。

2.5针对合作事项涉及的数据安全风险,甲方需配备的安全保护措施,包括但不限于数据加密传输、数据加密存储、敏感数据脱敏、操作权限控制、批量操作审计等。

2.6如合作过程中,甲方未保护乙方客户利益,影响客户体验,乙方将对涉嫌损害用户权益的数据合作予以关停。

2.7对于工作中可接触吉林联通用户个人信息数据或企业重要数据的甲方工作人员,应签订个人安全保密承诺书,明确数据安全保护责任,确保上述人员承担保密责任的程度不低于乙方与甲方数据安全保密协议规定程度。

2.8合作结束后,甲方及时返还相关资料、销毁保密数据,甲方提供销毁记录承诺书报乙方备案,明确数据未按要求销毁的法律责任。

2.9在技术服务中涉及采集外部数据的,甲方应说明数据来源,并对数据来源的合法性承担保证责任,确保外部数据采集渠道的合法合规且不存在侵权事项。

2.10甲方不得向境外传输、存储数据。

2.11甲方每年就合作内容至少开展一次数据安全合规性评估并提交评估报告。(依据法律法规、公司制度规定及具体业务情况需约定的其他事项。)

2.12甲方在合作范围内开发的系统、网站、app等接入吉林联通网络前必须做好源代码检查、漏洞扫描、web扫描、弱口令检查、基线核查、风险评估等安全保护措施。甲方对运行中的业务系统进行的任何改动,针对增量部分也需要采取上述安全保护措施。

2.13甲方事前进行的安全保护措施需提供证明材料给相关部门审核,合格后方允许接入网络,未采取事前安全保护措施或安全保护措施经检查不满足要求的不允许接入乙方公司网络。

2.14甲方在合作范围内开发的系统、网站、app等接入吉林联通网络前必须向相关部门报备资产清单,资产清单包括:设备名称、操作系统版本号、IP地址、物理机柜位置等基础信息,对于有互联网出口的系统、服务,同时须包含网站域名、公网IP地址及端口号等信息。运行中的系统进行增删改操作时,须要及时将更新的资产清单进行报备。

2.15甲方使用数据违反有关保密规定的,依照《中华人民共和国保密法》等有关法律法规的规定处理;因甲方使用或保管数据不当,导致知识产权纠纷或失密事件,由甲方负全部法律责任。

2.16甲方违反本协议规定未及时上报相关资产信息或上报信息有误的,乙方有权对因此造成的损失要求赔偿;构成犯罪的,由司法机关追究其刑事责任。

第三条 违约责任

3.1甲方未履行或未完全履行本协议项下的条款均构成违约,甲方应赔偿因此而给乙方造成的一切损失,包括但不限于乙方因调查违约行为而支付的合理费



用,因甲方违约而导致用户与乙方发生纠纷时,甲方应赔偿乙方及乙方用户全部损失(含直接、间接损失)。如涉嫌违法的,将移交司法机关处理。

第四条 协议生效及其他

4.1 本协议有效期与主协议保持一致。本协议签署前,乙方已经向甲方提供的本协议范围内的保密数据也受本协议约束。

4.2 如果本协议的任何条款在任何时候变成不合法、无效或不可强制执行而不从根本上影响本协议的效力时,本协议的其它条款不受影响。

4.3 对协议内容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协议不可分割的部分。

4.4 双方因履行本协议或与本协议有关的一切通知都必须按照本协议中的地址,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。采用信函方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。



附件 3 网络与信息安全、数据安全及个人信息保护承诺书

中国联合网络通信有限公司白山市分公司:

我方与贵方已就通信业务合作事宜签署白山市浑江区退役军人事务局通信业务合作协议(以下简称“项目合同”),现我方就该合作事宜涉及的网络与信息安全、数据安全及个人信息保护事项承诺如下:

第一条 本单位承诺遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》《中华人民共和国电信条例》《关键信息基础设施保护条例》《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《电信和互联网用户个人信息保护规定》及网络与信息安全、数据安全、个人信息保护有关法律、法规、规章、有权监管机构规范性文件、强制适用的国家及行业标准(以下简称“相关法律规定”),依法合规使用网络,建立健全网络安全、数据安全、个人信息保护与反电信网络诈骗等安全体系,依法设置风险防控管理机构及人员,制定内部控制机制和安全责任等管理制度,落实安全等级保护、安全技术措施和评估、报告、信息共享、监测预警等安全保护机制,加强风险防控管理,保障网络安全、稳定运行,有效应对网络安全事件,防范网络违法犯罪活动,维护网络数据的完整性、保密性和可用性,全面履行网络与信息安全、数据安全、个人信息保护、反电信网络诈骗及保密义务。

第二条 本单位承诺本单位及本单位履行项目合同的人员、为履行项目合同本单位必须合作的第三方及其人员(以下简称“己方及己方相关人员”)了解并遵守中国联通合作方网络与信息安全、数据安全、个人信息保护、反电信网络诈骗及保密等相关管理制度和规定,不违法违规使用联通方所辖资产及品牌、业务名称、商标、标识或 LOGO 等信息。遵守“十三不准”要求。

“十三不准”要求包括:

- (一) 不准设置弱口令;
- (二) 不准使用非工作邮箱代收工作邮件;
- (三) 不准点击来路不明邮件中的链接或打开附件;
- (四) 不准将账号和口令明文保存在终端上;
- (五) 不准将系统设计文档、网络拓扑等敏感信息存放于服务器上或上传至互联网的百科、文库等平台;
- (六) 不准将本人使用的账号与口令告知他人;
- (七) 不准在互联网上的外部网站或应用(如论坛、微博、即时通信软件等)上使用与中国联通设备、系统上相同的账号或口令;
- (八) 不准允许未授权人员远程控制中国联通各类设备或执行其告知的各项指令;
- (九) 不准将网站或系统源代码上传至互联网上;



- (十) 不准设置中国联通业务系统为自动登录;
- (十一) 不准私自在办公网络及其他内网中搭建无线热点;
- (十二) 不准将未进行自我检查和安全加固的终端接入内网;
- (十三) 不准未经审批开通内部系统的互联网出口。

第三条 本单位承诺不利用网络（包括但不限于固定通信网、移动通信网、互联网，下同）及计算机信息系统从事危害国家、社会、集体利益和公民合法权益的活动；不利用网络危害国家安全、网络与信息安全、数据安全以及计算机信息系统安全；不开展为他人实施电信网络诈骗活动提供支持或帮助等违法犯罪活动；不侵害自然人的个人信息权益；不侵害他人名誉、隐私、知识产权和其他合法权益。

第四条 本单位承诺己方及己方相关人员具备相关法律规定及联通方（“联通方”指中国联合网络通信集团有限公司及其分公司和全资、控股子公司，中国联合网络通信有限公司及其分公司和全资、控股子公司，下同）要求的开展项目合同所涉业务需要的网络与信息安全、数据安全、个人信息保护、反电信网络诈骗、保密等业务资质及相应授权。

本单位承诺同意、接受并配合联通方根据相关法律规定和项目合同业务事项需要开展的网络与信息安全、数据安全和个人信息保护、反电信网络诈骗、保密相关准入评测、接入认证、安全能力及资质核验、评估及审查、产品及服务安全检测、安全风险评估、安全监控和审计、安全检查及整改、安全事件应急预案制定及处置、攻防实战演练、应急演练等工作，对发现的问题及时按照相关法律规定及要求处理并解决，全面落实合作事项涉及的本单位网络与信息安全、数据安全、个人信息保护、反电信网络诈骗和保密责任。

第五条 本单位承诺不从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不为其提供技术支持、广告推广、支付结算等帮助。

本单位承诺向联通方提供及对接联通方的设备、系统等软硬件产品及服务等均符合相关法律规定、国家及行业标准以及联通方要求，并按相关法律规定要求取得合法授权及资质证明。本单位承诺配合联通方开展内外部网络信息安全相关攻防演练、各类检查工作，并对发现的网络与信息安全问题按照要求时限完成整改。

本单位承诺接入联通方的系统、平台和终端，不开启对外网口，不安装远程控制软件，不进行非授权接入和操作。入网终端安装符合要求的防病毒软件，符合联通方统一终端安全管理平台的纳管要求。本单位承诺符合联通方的安全及保密要求。

本单位承诺己方人员不通过远程方式接入联通方内部网络环境进行系统维护和数据操作。

第六条 本单位承诺履行数据安全保护责任，对接触及获取的数据履行保密义务；未经联通方同意不改



变数据使用的目的、方式和范围,不将联通方提供或委托处理的数据提供给第三方;不缓存、复制、窃取、泄露、损毁、篡改、滥用、非法向他人提供联通方数据、联通方用户数据、保密信息、敏感信息和个人信息;不对数据进行加工后还原成原始数据。不违法违规使用、编制、复制与联通方有关的测试数据。联通方有权要求本单位删除、销毁或归还已提供的数据,本单位及时处理并出具已删除、销毁相关数据的证明。每年就合作内容至少开展一次数据安全合规性评估并提交评估报告;合作结束后,及时返还数据、销毁保密数据、不留存相关的数据副本。

本单位承诺不在互联网存储、传输重要数据和核心数据;承诺已配备安全保护技术措施和其他必要措施,包括但不限于数据加密传输、数据加密存储、敏感数据脱敏、操作权限控制、批量操作审计等,防止数据泄露、损毁、丢失、窃取、篡改。

本单位承诺涉及采集外部数据的,提供并说明数据来源,对数据来源的合法合规性承担责任,确保外部数据采集渠道的合法合规,且不存在侵权事项;本单位承诺在中华人民共和国境内收集和产生的数据,在境内储存;本单位承诺不向境外传输、存储本合作涉及的数据。如因业务等需要确需向境外提供,须经联通方同意,并遵守相关法律规定。

第七条 本单位承诺收集、存储、使用、加工、传输、提供等处理个人信息行为遵循合法、正当、必要和诚信原则,不通过误导、欺诈、胁迫等方式处理个人信息。处理个人信息具有明确、合理的目的,并与处理目的直接相关,采取对个人权益影响最小的方式。收集个人信息,限于实现处理目的的最小范围,不过度收集个人信息。处理个人信息遵循公开、透明原则,公开个人信息处理规则,明示处理的目的、方式和范围。

本单位承诺在处理个人信息前,已依法向个人信息主体(“个人”)履行法定告知义务并取得个人的同意,并已明确个人信息处理的目的、期限、处理方式、个人信息的种类、保护措施以及权利和义务等。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的,本单位已依法取得个人单独同意或书面同意。在个人信息主体授权同意的范围内开展业务合作,不超出合同约定的目的和范围处理个人信息,或使用匿名化处理之后的数据。处理满十四周岁未成年人个人信息的,本单位已依法取得未成年人的父母或者其他监护人的同意。处理不满十四周岁未成年人个人信息的,本单位已制定专门的个人信息处理规则。

本单位向联通方提供个人信息或委托联通方处理个人信息的,本单位承诺已向个人履行法定告知义务,并取得个人单独同意。本单位向联通方提供或委托联通方处理的个人信息和数据的,本单位承诺该等个人信息和数据来源合法合规,不存在违反相关法律规定的情况。

本单位受联通方委托处理个人信息的,或本单位与联通方共同处理个人信息的,本单位按照与联通方的合同约定处理个人信息,不得超出约定的处理目的、处理方式等处理个人信息。



本单位承诺遵守用户真实身份信息制度（“实名制”）的各项要求，提供身份证件号码、统一社会信用代码等真实身份信息进行认证并开展合作业务，不冒用组织机构、他人身份信息进行虚假注册，保证所提供信息、资料的真实、完整、准确和有效。

本单位承诺己方及己方人员对收集、使用的个人信息严格保密，不泄露、篡改或者毁损，不出售或者非法向他人提供。

第八条 本单位承诺不利用联通方提供的产品和服务从事制作、查阅、复制和传播国家法律法规或公共道德所禁止的以及损害联通方利益的信息内容，包括但不限于：

- (一) 反对宪法所确定的基本原则的；
- (二) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- (三) 损害国家荣誉和利益的；
- (四) 歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；
- (五) 宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；
- (六) 煽动民族仇恨、民族歧视，破坏民族团结的；
- (七) 破坏国家宗教政策，宣扬邪教和封建迷信的；
- (八) 散布谣言，扰乱经济秩序和社会秩序的；
- (九) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- (十) 侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；
- (十一) 法律、行政法规禁止的其他内容。

第九条 本单位承诺使用联通方提供的账号时做到实名实人、分级管理、岗位互斥、职责分离、最小授权、限期授权、定期审计，并且执行一人一账号管理要求，账号不得转让、转借、共用，不泄露给第三方，不持有 root、DBA 等超级权限账号、不持有敏感信息权限账号。

本单位承诺配合联通方做好合作账号的申请、新增、变更、授权、网络设置调整、有效期设置、回收、数据清理等管理，业务合作期满或己方人员离职或岗位变动时，提前通知联通方联系人，配合联通方及时回收账号权限、调整网络配置、销毁相关数据、防范安全风险。

第十条 本单位承诺己方及己方相关人员均已向联通方备案并签署与业务相关的网络与信息安全、数据安全、个人信息保护、保密等承诺书（承诺范围和程度不低于本承诺书标准），全面遵守相关法律规定及联通方各项网络与信息安全、数据安全及个人信息保护、反电信网络诈骗、保密管理制度、规定及要求。

本单位承诺按照相关法律规定和联通方管理要求，开展己方及己方相关人员的网络与信息安全、数据安全、个人信息保护、反电信网络诈骗、保密相关知识、技能和安全责任的培训工作（一年不少于【1】



次), 培训记录包括但不限于培训时间、培训内容、培训考试、培训反馈等, 相关材料应以书面形式留存。

第十一条 本单位承诺根据相关法律规定及联通方要求, 对本单位提供的服务和产品制定网络信息安全事件应急预案, 开展安全应急演练和应急响应培训(每年不少于【1】次)。在发生安全事件时, 第一时间启动应急预案, 组织有效应急处置, 最大程度减少损失和危害, 并按照“边处置边上报”原则, 依法依规履行向有权监管机关的报告义务。

本单位承诺出现违反《中国联通合作方网络与信息安全管理办法》《中国联通合作方数据安全管理办法》的情况或出现网络与信息安全、数据安全、个人信息保护安全事件/事故或涉嫌为他人实施电信网络诈骗活动提供支持或帮助时, 将在发生【24】小时内书面通知联通方, 并积极有效的开展应急处置, 有效控制风险影响范围, 有效压降双方损失。在事件处置完毕后, 提供书面详细真实的事件报告。

本单位承诺应及时响应、处置联通方安排的安全工作, 对本单位管理的系统、组件、云资源等的安全事件、隐患及时阻断、排查、处置、溯源(包括但不限于攻防演练等相关活动中发现的安全隐患或漏洞)。

第十二条 本单位承诺所接入联通方的网络或系统均已通过安全评估和准入测试, 接入期间每年至少开展一次网络与信息安全、数据安全、电信网络诈骗风险防控相关的安全合规性评估及风险评估, 并向联通方提交评估报告和整改报告。

第十三条 本单位承诺配合联通方为公安机关、国家安全机关等政府部门依法维护国家安全和侦查犯罪的活动提供协助, 如实提供有关安全保护的信息、资料及数据文件, 积极协助查处信息网络违法犯罪行为。

第十四条 本单位承诺, 如发生重大安全事故或其他影响网络与信息安全、数据安全和个人信息保护、涉嫌为他人实施电信网络诈骗活动提供支持或帮助的突发事件, 联通方有权采取包括但不限于停止业务等紧急措施, 以保证网络与信息安全、数据安全和个人信息保护, 及时阻断电信网络诈骗风险。

第十五条 己方及己方相关人员有任何违反本承诺书的行为即构成违约, 本单位应立即停止违约行为, 予以纠正或采取补救措施; 给联通方造成损失或不良影响的, 或因给第三方造成损失导致联通方被追偿的, 本单位负责消除不良影响并赔偿联通方全部损失(包括但不限于联通方因此支付的罚款、向第三方支付赔偿金、和解金、律师费、鉴定费、诉讼费、差旅费以及其他合理开支, 下同)。

如因本单位原因导致联通方发生网络与信息安全、数据安全、个人信息保护、电信网络诈骗、泄密相关安全事件/事故, 包括但不限于网络攻击、网络瘫痪、网络安全事件/事故、数据泄露、个人信息泄露等, 受到监管机构通报处罚或法律责任追究的, 联通方有权在不通知本单位的情况下暂停、停止业务直至解除项目合同且不承担任何责任。

若发现本单位行为涉嫌违法犯罪等情节较严重的网络信息安全、数据安全事件, 联通方有权依据《中国联通供应商黑名单管理办法》相关规定, 将本单位列入中国联通黑名单供应商, 采取禁入, 向行业联盟通报本单位黑名单事件等措施。



承诺单位（公章）：

法定代表人或授权签约人（签字）：

沙晓亭

日期：2025年6月17日