供应商产品及服务安全协议

（适用于生产物料采购业务场景）

协议编号:

买方：武汉光迅科技股份有限公司

供方：

重要提示

1. 本模板中所有“【】”中的内容均为变量，应当根据签约时的具体情况进行填写或修改。
2. 本合同中涉及到“适用语言”、“法律适用”、“争议解决”等条款，合同拟制人应当充分考虑与同一签约对方当事人签署的一系列合同在相关条款上的一致性和统一性。
3. 海外子公司、分支机构在使用本模板前，应当先交财务、法务人员进行评审，如果有修改，应当在修改的基础上通过PDMC发布适用于本国或本地区部的区域模板。

1. 前言

1.1. 协议双方

【武汉光迅科技股份有限公司】是一家根据【中华人民共和国】法律成立的公司，公司位于【中国湖北省武汉市江夏区藏龙岛开发区潭湖路 1 号】，邮编：【430205】（以下简称为“买方”）

【　　】是一家根据【　　】法律成立的公司，公司位于【　　】，邮编：【　　】（以下简称为“供方”）

根据具体情况，买方及供方可统称为“双方”或分别称为“一方”、“另一方”。

1.2. 生效日期

本《供应商产品及服务安全协议》（简称为“本协议”）经双方签署后，自【　　】年【　　】月【　　】日（“生效日期”）起生效。

1.3. 鉴于

鉴于买方有意向供方采购且供方同意向买方提供采购协议（含相关附件）中所述的产品及/或与产品配套的服务，为明确双方在产品及/或与产品配套的服务安全方面的权利义务，双方经自愿、平

等协商达成本协议内容如下。

2. 定义（按英文首字母的顺序排列）

2.1. “暴力破解”(Bruteforce attack)：指一种口令被破译的方法，即通过逐个尝试找到真正的口令。

2.2. “客户（Customer）”：指买方的直接的或间接的客户。

2.3. “数据外传”（Data Disclosure）：指除了系统正常运行所必须的数据交互之外的数据转移。

2.4. “加密”(Encryption)：指对明文的数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，只有在输入相应的密钥之后才能显示出原来内容，确保数据不被非法窃取。

2.5. “隐秘访问方式”(Hidden Access Methods)：指未向买方公开说明的访问方式，如隐藏账号、隐藏组合键访问、隐藏的端口等。

2.6. “关键安全岗位”（Key Security Positions）：指可能直接或间接产生产品及/或服务的安全问题的岗位，包括但不限于研发、生产制造（芯片烧录、软件加载、组装、测试等）、仓储、物流和采购等相关环节的岗位。

2.7. “物流服务”(Logistics services)：指将产品从供应地运送到买方指定的接收地的服务过程，包括产品运输、储存、装卸、搬运等环节。

2.8. “开源软件”(Open Source Software)：指任何受“开源许可证”约束的源代码或者目标码。开源许可证（Open Source License）是指满足下列任一条件的许可证：（i）要求许可人允许任何人对被许可软件或其修改部分、或集成被许可软件的软件进行反向工程；（ii）要求以源代码形式分发或者免费分发被许可软件或其修改部分、或集成被许可软件的软件。“开源许可证”包括但不限于下列许可证：(a) GNU General Public License (GPL) or Lesser/Library GPL (LGPL), (b) The Artistic License (e.g., PERL), (c) the Mozilla Public License, (d) the Netscape Public License, (e) the Sun Community Source License (SCSL), (f) the Sun Industry Standards Source License (SISL), (g) the Apache Server license, (h) QT Free Edition License, and (i) IBM Public License。

2.9. “端口”(Ports)：指可通过软硬件接入设备的通道，包括但不限于物理端口（如串口、网口等）和软件端口（如 TCP 端口等）等。

2.10. “产品（Product）”：指供方依采购协议（含相关附件）向买方交付的所有设备、软件及

技术文件。

2.11. “服务（Service）”：指供方依采购协议（含相关附件）向买方提供的与产品有关的包括但不限于【安装、调试、交付、仓储、维修、验收】在内各项服务。

2.12. “安全问题”(Security problems)：指导致买方客户产品、解决方案或服务的可用性、完整性、机密性、抗攻击性和可追溯性遭受或可能遭受损害的问题。

3. 安全要求

3.1. 产品安全要求

(1) 供方提供的产品应满足买方安全要求，不得含有任何形式的木马、后门、蠕虫、病毒、恶意代码、未知功能及未知权限。

(2) 供方提供的产品的所有功能特性须向买方说明，特别是任何可能侵犯个人隐私和通信自由的功能，包括但不限于 DPI 深度报文检测、干扰业务流量等。

(3) 供方提供的产品的所有端口须向买方说明，不得存在隐藏端口。开启的端口应是系统运行和维护所必需的，无用的端口应关闭。开启/关闭端口须有权限控制，且开启/关闭的方法应向买方说明。

(4) 供方提供的产品中，所有能对系统进行管理或控制的通信端口（包括但不限于能对系统进行管理或控制的物理端口），均须有接入认证机制（无认证机制的标准协议除外）；认证机制须具备防暴力破解、防仿冒等内容；供方须提供所有认证的初始账号和口令清单。

(5) 供方提供的产品若对系统或数据进行访问时，不得采用绕过系统安全机制（包括但不限于认证、权限控制、日志记录）的隐秘或不可管理的认证或访问方式（如不可管理的账号、口令）。

(6) 供方提供的产品若具有存储或传送数据的功能，则供方须对产品的口令、敏感个人数据（如银行帐号等）的存储和传送过程进行加密。传输的口令不得含有硬编码，若无须还原口令，则须使用不可逆算法存储口令。

(7) 供方提供的产品若含有加密算法，则此算法不得使用私有或已知不安全的加密算法，且供方须提供加密算法清单。

(8) 供方提供的产品若含有采集或转移客户/最终用户数据（含个人数据）的功能，须向买方进行说明，且客户/最终用户有权决定是否使用或关闭此功能。

(9) 供方提供的产品若含有软件（包括但不限于供方自研软件、第三方商用软件、开源软件等）升级的功能，须向买方说明，且客户/最终用户有权决定是否使用或关闭此功能。

(10) 供方须向买方说明产品数据外传的目的、数据格式和内容、实现和管理机制，并保证数据收

集或传送遵守所适用的关于保护个人数据和隐私、通信自由及保障网络安全运行等方面的法律、法规。

(11) 供方提供的产品若含有软件（包括但不限于供方自研软件、第三方商用软件、开源软件等）或芯片，须在交付前进行安全检测，检测项目包括但不限于：病毒扫描、端口扫描、漏洞扫描和 Web 安全检测，并对存在的安全问题进行修复，或升级到无安全问题的新版本。

(12) 供方提供产品时应同时提供安全测试报告，软件（含软件包/补丁包）须提供完整性校验机制（如数字签名等）。

(13) 供方依双方的约定提供物流服务的，供方须遵守所在国相关的法律法规以及 C-TPAT 或 TAPA 标准和买方的安全要求，并对服务过程进行安全管控，确保物流服务过程不存在安全隐患或问题（包括但不限于货损货差、改变性状等）。

3.2. 服务安全要求

供方在提供与产品相关的【工程实施、安装、调试、维护、升级等】服务过程中，应遵守如下要求：

(1) 遵守所在国相关法律法规以及买方及/或客户的安全要求，确保服务过程不存在安全隐患或问题。

(2) 遵守所适用的关于保护个人数据和隐私、通信自由及保障网络安全运行等方面的法律法规。严格遵从双方的约定、买方及/或客户的指示进行个人数据处理、转移及其他相关业务。

(3) 不得攻击、破坏买方或客户的网络、不得窃取买方或客户网络中的任何数据或信息、不得破解买方或客户的账户密码。

(4) 不得在买方及/或客户的设备或系统中植入非法代码、恶意软件或后门，不得预留任何未公开接口或账号。

(5) 未经买方及/或客户书面授权，不得使用非授权账号或他人账号登录设备进行操作或账号和密码与他人共享。在产品进入商用或转入维护阶段后，不得保留或使用管理员账号或其它非授权账号。

(6) 未经客户书面许可，不得使用个人便携设备、存储介质接入客户网络。

(7) 未经买方及/或客户书面授权，不得访问买方及/或客户系统或收集、持有、处理、修改、泄漏、传播客户网络中的任何数据和信息。

(8) 对在提供服务期间获悉的买方及/或客户的任何信息或数据应承担严格的保密义务，直至相关信息或数据被合法披露为止，并不得利用该信息或数据谋取个人利益或用于其它非法目

的。

(9) 须使用买方及/或客户提供的或指示渠道获得的软件版本、补丁及许可，不得使用非法软件在买方及/或客户的网络上运行。

(10) 未经买方及或客户的许可或授权，提供买方指定的服务之外的任何服务。

(11) 确保供方服务人员在服务过程中使用的电脑不含有非法软件或病毒。

3.3. 体系安全要求

(1) 供方应建立安全保障体系，实施产品及或服务的安全管理并定期进行安全自检，同时提供自检报告给买方。买方及/或客户有权对供方的安全保障体系及执行情况进行审核。

(2) 供方须建立安全应急响应机制，对产品及/或服务的安全问题（含安全漏洞）及问题的解决方案（含安全补丁），通过邮件、传真或其他书面方式向买方进行通报。

(3) 当供方对外发布产品及/或服务的安全问题（含安全漏洞）时，须提前 72 小时通过邮件、传真或其他书面方式通知买方，并将问题的解决方案（含安全补丁）通过正式版本发布渠道通知买方。

(4) 供方应对关键安全岗位员工进行安全管理，包括但不限于与员工安全协议签署、进行安全培训、对员工遵守安全规范的情况进行审核及改善通过审核发现的问题。

(5) 供方应在研发、生产制造（芯片烧录、软件加载、组装、测试等）、物流和采购等环节建立详细的安全过程记录，以确保过程的可追溯性。若供方的产品及/或服务含有日志，则日志应有访问控制，任何情况下不得更改或删除日志。

4. 责任

任何对本协议条款的违约都是对本协议的实质违约。在无损买方依据双方签署的采购协议及或相关附件享有的各项救济措施的前提下，若供方违反本协议约定，则买方有权单方采取以下措施之部分或全部：

(1) 要求供方在买方指定的合理期限内以费用自担的方式纠正其与本协议约定不符的行为，直至符合本协议要求。

(2) 要求供方赔偿买方因此遭受的全部损失，包括但不限于为消除供方不符合本协议约定行为的影响所支付的费用、诉讼费、律师费，以及客户主张的赔偿金等。

(3) 要求供方就买方由于供方违反本协议遭到的如下索赔、损失、费用及开支做出赔偿：

i 由于供方或供方人员的故意或过失导致的任何第三方（包括但不限于客户、最终用户）的实际损失；

ii 最终用户根据相关的法律法规，如：《消费者权益保护法》、《产品质量法》、《侵权法》、《中华人民共和国电信条例》等（包括其修订、替换、编撰或重新发布的版本）提出的索赔。

iii 终止与供方的采购关系，单方解除相关《【采购协议】》及/或相关的《【采购订单】》等。

5. 法律适用及争议解决

5.1. 法律适用

本协议应受【中华人民共和国】法律约束并按其解释，而不参考冲突法规范。

5.2. 争议解决

因本协议引起的或与本协议有关的任何争议，均应通过友好协商解决。如协商不成，则应提请【武汉仲裁委员会】按照该会仲裁规则进行仲裁。仲裁裁决是终局的，对双方均有约束力。

6. 期限

本协议自生效之日起【二（2）】年内有效。若协议双方均未在本协议终止前【六十（60）】日发出终止本协议的书面通知，则该协议自动延续【一（1）】年，自动延续的次数不限。

7. 复本

本协议一式【贰】份，双方各执【壹】份，均具有相同法律效力。

买方（盖公章）：武汉光迅科技股份有限公司	供方（全称，盖公章）：
授权代表签名：	授权代表签名：
授权代表职务: 采购中心总经理	授权代表职务:
日期：	日期：

[本页以下空白]