版 本 号： V1.0
受控状态： 受控

京东集团
三方合作伙伴信息安全管理细则

文档信息

文档名称：京东集团三方合作伙伴信息安全管理细则	制度编号：JD-ISMS-03-011
拟文人：王宁	审核人： 侯建龙、赵波、徐迪
审批人：冯娜	生效日期：2023 年 11 月 22 日
收文人：京东全体	抄送人：//
附件：//	

版本记录

版本号	版本日期	修改人	修改章节	修改记录
V1.0	2023.8.6	王宁	-	新建
V1.1	2024.2.26	王宁	4.4.1	修改安全测试报告接收地址

目 录

京东集团三方合作伙伴信息安全管理细则

1 编写目的/背景

为营造规范、有序、安全的京东开放、生态环境，为了更好的保障用户信息的安全、提升三方应用对于用户个人信息的保护及应用自身的安全防护能力，根据国家相关法律法规，以及依据《京东开放平台规则总则》《商家信息安全管理规范》等内容，特制定此规范。

此规范对系统的使用、数据的获取、数据的存储、数据的传输、数据的使用、软件产品的提供、SaaS 服务的提供都有对应的安全要求，三方合作伙伴需要遵对应的安全要求，执行相关的安全要求，进行账号和权限安全管理、数据脱敏、数据加密、数据入鼎、账号登录体系统一接入京东账号风控等安全措施，并对企业自身员工开展数据安全保护意识宣传，提升业务安全性，遵守平台规则实行安全运营及对应业务的开展。

2 适用范围

本规范适用于所有与京东有数据交互的第三方合作伙伴，包括商家、商品供应商、软硬件产品供应商、分销商、第三方开发者、服务商以及自研应用的商家。所有与京东有数据交互的三方合作伙伴必须严格遵守该安全管理规范，以保证用户数据、商家数据及平台数据的安全。

为了更好的指导合作伙伴开展安全管理活动，请您基于自身的业务场景，参考以下对应场景的安全管理要求，执行相关安全管理动作：

- **京东系统使用者**

如果您通过使用京东提供的系统开展相关业务，包括商家、供应商、分销商等，请您参考第四节安全要求>4.1 系统使用要求的内容进行安全管理。

- **SaaS 服务提供者**

如果您通过为京东提供 SaaS 服务与京东开展相关业务，请您参考第四节安全要求>4.2 SaaS 系统安全要求的内容进行安全管理。

- **服务市场 ISV 提供者**

如果您是开发者，在京东开放平台、各服务市场发布供商家、供应商及其它合作伙伴使用的软件类产品，请您参考第四节安全要求>4.3 开发者安全要求的内容进行安全管理。

- **与京东对外业务接口进行对接**

如果您是自研应用的商家、承运商广告商或其它需要与京东服务接口进行对接的服务商，通过与京东开放接口进行对接以获取必要的业务数据开展业务时，请您参考第四节安全要求>4.3 开发者安全要求的内容进行安全管理。

- **软硬件产品供应商**

如果您是软硬件产品供应商，为京东提供软件开发服务、软件产品或提供的产品服务包含软件系统，需将产品部署在京东的网络环境中，请您参考第四节安全要求>4.4 软件产品安全要求的内容进行安全管理。

- **外包服务人员**

如果您是外包服务人员，通过与京东签订合作协议的第三方合作伙伴公司为京东提供服务，请您参考第四节安全要求>4.5 第三方人员安全要求的内容进行安全管理。

3 术语和定义

术语	定义
开发者	指京东开放、生态应用中通过有效申请并通过验证的可以基于开放平台进行应用开发的单位或者个人，在开放平台开发者也可称为“京东合作伙伴”。
应用	指开发者基于开放平台所开发的软件或服务，包括自用型应用和他用型应用两种类型。 供应商为京东提供的软件系统。
云鼎、入鼎	云鼎是京东云推出的电商应用云计算平台，为商家、ISV 以及其他合作伙伴提供计算、存储和电商数据开放服务，实现基础资源的弹性伸缩，保证应用运行稳定安全。 云鼎平台提供完全由用户掌握的私有网络空间，并且集成了一系列基础运维服务，采用直接可用的方式提供服务，用户随时购买随时可用，无需考虑一系列繁琐的底层运维和安全性问题，您可以更加专注于业务上的研发。

	入鼎即应用接入京东云鼎平台。 **使用京东提供敏感数据接口、API 的应用必须入鼎。**
信息安全	保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。
安全策略	用于治理组织及其应用内在安全上如何管理、保护和分发资产（包括敏感信息）的一组规则、指导和实践，特别是那些对应用安全及相关元素具有影响的资产。
用户	使用京东合作伙伴所提供应用的机构或自然人，以注册的 ID 与用户信息为判断依据。
商家	租用电子商务平台进行经营活动的法人、法人委派的行为主体、其它组织机构或自然人。
网络交易	发生在企业（或其他组织机构）之间、企业（或其他组织机构）与消费者之间、消费者之间通过网络手段缔结的商品或服务交易。
二次验证	在用户注册或登录后进行一些重要或敏感业务操作时,通过除密码之外的如验证码、手机短信、安全问题、数字证书等对用户进行第二次校验的方式。
加密	加密是将明文的文件或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"）。
安全事件	特指电子商务安全事件,不仅包括网络上攻击或入侵行为造成的安全事件，也包括电子商务业务应用中出现的欺诈、盗号、违禁等恶意行为。
敏感数据	依据《京东集团数据分类分级指南》的规定，敏感数据的范围包括 L3 级别（保密数据）、L4 级别（机密数据），包括但不限于用户姓名、身份证号、收货地址、发货地址、手机号等，因此或涉及到相关的订单、发货等接口。
信息安全风险	人为或自然的威胁利用信息应用及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。
软件供应链	软件供应链是从软件开始加工,直到生产出最终产品并实施运营过程的全流程链条，包括第三方组件、开发工具和开发环境等要素。
制品	制品是指由源码编译打包生成的二进制文件,不同的开发语言对应着不同格式的二进制文件,这些文件通常可以直接运行在服务器上，用以支撑应用运行。
第三方组件	由京东和开发者以外的其他软件开发组织或人员开发的独立可用或可调用的软件组件,通常是由二进制程序文件或者源代码程序文件构成。
软件物料清单	软件采用的所有组件、许可协议、组件依赖关系和层次关系的清单

软件构成图谱	软件物料清单、软件供应关系、知识产权、安全风险、软件供应链基础设施等信息的表示形式,支撑实现软件供应链的安全保护目标。

4 安全要求

4.1 系统使用安全要求

如果您通过使用京东提供的系统开展相关业务，包括商家、供应商、分销商等，请您参考本章节的内容进行安全管理。

4.1.1 安全意识教育

1. 合作伙伴务必要在开始使用系统前在内部进行员工安全意识教育,强调网络安全的重要性；保管好自身及客户的账号信息、个人信息等，防止被内部员工私自收集、泄露。
2. 定期开展培训活动和学习计划，为员工进行案例分析讲解，加强员工的安全意识，避免被不法分子利用，造成信息安全事件；制定网络安全事件应急预案，明确反馈及处理流程，并定期进行演练。
3. 合作伙伴应从自身做起抵制打击电信诈骗黑色产业链，坚持“正道成功”，拒绝刷单、恶意好评返现等非正当途径，建设更加安全的网络环境。

4.1.2 权限安全管理

1. 京东为合作伙伴提供的系统设置了严格的账号及权限管理机制,在使用系统时，结合业务需要，在保证一个人对应只使用一个账号的前提下，仅创建适当数量的子账号。每个账号按最小权限原则，根据使用人员的业务需要，仅分配需要使用的权限。严禁大量账号同时具有查看订单等敏感操作的权限，禁止多人共用一个账号的情况。
2. 针对新入职的员工，建议为其新建专用账号，供其熟悉业务；短期避免其接触可操作敏感数据（订单、售后等）的账号；针对已离职员工，在其离职后，须立即删除或停用其账号及权限。

4.1.3 账号及密码安全管理

1. 正常情况下，严禁以任何形式将账号共享给内部/外部人员。若相关人员有使用账号需要，可结合其需求为其单独创建账号，并分配所需的权限。
2. 任何情况下，严禁将系统的账号、密码、验证码告知他人，切勿随意点击不明链接，更不要扫描来历不明的二维码。如非.jd.com 作为域名结尾但宣称为京东网站的，都属于虚假网页，请商家一定要认清，避免中招钓鱼诈骗。
3. 密码设置应具有安全性、保密性，密码是保护系统和数据安全的控制代码，也是保护用户自身权益的控制代码。切勿使用明显有规律性的密码，如“123”、“abc”、“qwert”等；密码不能包含具有特殊意义的字符串，切勿使用用户名/店铺名/生日/姓名等作为密码的全部或一部分；密码应尽量同时包含大小写字母、数字、特殊符号等。各应用系统密码应定期进行更换，如至少 3 个月更换一次密码，降低密码泄露的风险，如发现或怀疑密码遗失或泄露应立即修改。
4. 避免因为便利,将账号及密码存储于 word 或文本文档,放置于公用电脑中。

4.1.4 敏感数据安全管理

1. 非必要业务需求，避免导出敏感数据，且避免将包含数据的 excel 等文档直接存在办公电脑上。对已导出的不需要再使用的数据，需及时删除。
2. 如有业务需要，需将携带敏感信息（订单、售后）的文档或 EXCEL 表格等数据传输至他人，需将文档使用压缩包加密后，再进行发送传输。压缩包使用的密码应尽量复杂，避免如 123456…admin…等弱密码。
3. 在任何情形下，严禁将用户的订单信息，联系方式等通过 QQ 群、微信群发送给物流或其他人。且合作伙伴内部使用的 QQ 群、微信群等，需要有严格的加群审核与管控，避免除工作人员以外的人员加群。

4.1.5 计算机设备安全管理

1. 员工需使用公司提供的计算机设备（特殊情况需经过上级审批），不得私自调换及拆卸，并保持清洁、安全、良好的计算机设备工作环境；
2. 应指定专人进行计算机病毒和网络攻击的防范工作，安装安全防护类软件，

定期进行计算机病毒检查和漏洞扫描,发现病毒和数据安全隐患等安全问题要及时处理和上报;

3. 办公用途的计算机未经允许不准安装与各自业务无关的软件、严禁安装各种游戏软件,不准使用未经查毒处理的存储介质,如光盘、U 盘、软盘、移动硬盘等。员工禁止使用办公电脑访问不良网站。登陆系统的电脑,严禁用于其他用途,不得轻易点击任何人发来的不明信息或链接;
4. 员工对所使用计算机及相关设备的安全负责,如暂时离开座位时须锁定系统,移动介质自行安全保管。未经许可,不得私自使用他人设备。

4.2 SaaS 系统安全要求

如果您通过为京东提供 SaaS 服务与京东开展相关业务,请您请您参考本章节安全要求进行安全管理。

4.2.1 平台资质要求

为京东提供 SaaS 服务的平台须满足《网络安全等级保护基本要求 2.0》中第三级安全要求所明确的条目,供应商须提供以下其中一个证明文件:

1. SaaS 平台通过等级保护三级的等级测评报告;
2. 具备信息安全服务资质的安全服务机构出具的可覆盖《网络安全等级保护基本要求 2.0》中第三级安全要求所明确条目的安全评估报告。

4.2.2 平台基础安全要求

1. SaaS 平台须支持租户间的安全隔离,租户只能访问和操作自己的 SaaS 服务资源;
2. SaaS 平台须支持租户间的数据安全隔离,租户只能访问和操作自己的数据;
3. 未经京东授权,SaaS 系统管理员禁止访问京东在 SaaS 平台上的应用资源;
4. 未经京东授权,SaaS 系统管理员禁止访问京东在 SaaS 平台上的数据;
5. 须支持京东自行定义和设置数据备份和数据导出权限的能力;

6. 须支持京东自行定义和设置数据重置权限的能力；
7. 须支持京东的应用和数据存储资源回收时删除相关数据的能力；
8. 须支持京东退租后删除相关数据，包括删除备份和归档数据的能力；
9. 须支持用户故障安全隔离的能力，其它 Saas 租户业务故障，不影响京东在平台的使用；
10. 须支持用户身份和访问管理，支持密码策略管理，包括密码长度、复杂度及多因素认证；
11. 须支持用户权限控制的能力，支持限制用户功能权限和数据访问权限；
12. 须支持记录 SaaS 应用系统的登录日志的能力，包括记录用户成功/失败的认证/登录、用户注销.超时退出等活动；
13. 须支持记录对用户信息管理日志的能力,包括记录用户和用户权限的增删改以及密码的修改和重置等活动；
14. 须支持记录数据操作日志的能力包括记录应用系统中存放的业务数据进行操作(查询、修改、删除等)的活动；
15. SaaS 资源管理平台须在必要时支持向京东提供审计日志。

4.2.3 平台数据安全要求

如为京东提供服务的 SaaS 平台涉及处理京东敏感数据，平台须满足以下数据安全要求：

1. 须支持数据的高可用性,支持数据所在系统故障时不会导致数据丢失的能力；
2. 须按照国家法律法规要求支持数据隐私保护,禁止未授权访问和使用用户隐私信息；
3. 京东的敏感数据在平台的传输和存储须使用加密算法进行加密,数据加密算法须满足国家对于加密的合规性要求；
4. SaaS 平台为京东提供的服务如涉及采集和处理个人信息,平台须遵守以下安全要求：

   a) 平台须按照国家监管要求进行隐私政策的制定和告知，并采取对应的技

术措施对个人隐私信息进行技术保护；

b) 平台采集的个人信息须严格按照合同约定的使用场景进行数据使用，禁止在合同外的业务场景使用。

5. SaaS 平台如因技术保护措施落实不到位、运行维护人员操作疏忽、遭受恶意攻击等情况下造成数据泄露，平台须承担对应的安全责任，同时京东将保留对平台的审查及诉讼的权利，以备在必要时发起相关的行动。

4.3 开发者安全要求

本章节安全要求主要针对京东合作伙伴的应用开发者，包括第三方服务商以及自研应用的商家。所有的应用开发者必须严格遵守该安全管理规范，以保证商家数据及平台数据的安全。

应用开发者为京东提供服务前，须与京东相关的主体签署服务协议（合同），同时，必须签署安全保密协议。

4.3.1 账号认证和权限

4.3.1.1 认证

安全项	具体要求
用户登陆、授权	1）用户通过三方应用软件，登陆京东平台，需要用户对应用进行授权（京东平台支持 OAUTH2.0 协议来进行用户授权认证）。应用不能自行登录用户账号来获取数据。 2）三方接入的应采用集团统一的用户体系，不可自建用户账号体系。个人用户登录验证采用集团用户登录页，商家用户登录验证采用生态服务部登录页。
用户登陆态验证	三方应用要验证用户登录状态的有效期。过期后，第三方应用必须重新获取用户授权才能继续访问平台。不能出现登录状态长期有效的情况。
黑白名单	三方应用应具备身份黑名单机制。黑名单可以是企业名称、账号、IP 等。黑名单企业、账号、IP 的应限制其接入开放平台。

4.3.1.2 权限

安全项	具体要求
最小化授	1）应用应按业务接口的不同属性、安全级别、风险状况，合理控制用

权	户账号、商家账号、管理预案的访问权限。防止低安全级别账号访问高级别接口、防止账号跨类别属性访问接口，以及出现安全风险时快速进行止损。 2）应用必须实现防越权逻辑，防止水平或垂直越权，避免出现 意外的非授权数据获取。
权限回收	应用要验证用户账号的登陆态、权限有效期。过期后，第三方应用必须重新获取用户授权才能继续访问平台。不能出现账号敏感权限长期有效的情况。

4.3.2 账号管理要求

安全项	具体要求
账号唯一性	应用应该为每个用户独立分配一个账号，严禁多个用户共享一个账号。
账号风控	应用应该可以识别账号异常登录（被盗、撞库、异地登录），并采取手机验证码等方式确保账号登录安全。 如果发生过异常登录，应用应该以合适的方式提示用户。
账号锁定	账号密码输错达一定次数时，应该将账号锁定，一定时间内不能登录账号，以防止暴力破解。
账号回收	账号超过一定时间不用、多余账号等情况，应用应及时回收。
账号有效期	应用应对用户账号和应用管理员的账号设置有效期。
无用账号删除	应用应及时删除或禁止多余的、过期的用户账号，避免共享账号的存在。
账号权限回收	应用应及时清理和回收应用相关的开发账号、测试账号和后台管理账号及权限，如：相关账号使用者离职或转岗时。
口令更换	应用应定期提醒用户对口令进行修改，建议口令至少每六个月更换一次。
口令强度	应用、应用、数据库账号口令要求满足一定的长度和复杂度，确保口令强度（口令不能为空、不能为默认、不能少于 8 位、应该有字母大小写、数字、特殊符号，不能与身份信息关联）。
口令重置	应用应提供给用户口令重置功能。 口令重置应该有较强的身份校验机制，避免被轻易更改口令导致账号丢失。 重置后的口令必须通过短信、邮件等用户绑定的可信任的渠道告知用户。
超时退出	所有会话应该具备超时退出机制，当会话空闲超过一定时间，应用应要求用户重新验证或重新激活会话。

多因素认证	1、应用应支持对同一用户采用两种或两种以上组合的鉴别技术（口令验证、邮箱验证、短信验证等）实现用户身份鉴别。 2、在执行敏感操作（口令修改或重置）或账号行为异常的情况下，应用应采用两种或两种以上的组合鉴别方式。

4.3.3 安全审计

安全项	具体要求
审计用户的行为和操作	应用应记录用户的行为日志，包括帐号、appkey、源 IP、访问时间、行为类型、行为内容等。
日志存储保护	应用应保护用户行为日志的完整性，避免其受到未预期的删除、修改或覆盖等。
日志保存期限	所有日志留存时间不低于 6 个月，敏感数据访问的日志保留时间不少于 1 年。
服务端上报日志	应用需严格遵循京东日志规范，对整个应用中涉及敏感操作的功能点（包括但不限于订单明细的查询、导出。订单收货手机号、姓名地址的查询/导出），需保证全部接入安全日志。三方应用侧在日志接入的开发完成后，为保证日志接入的质量节约沟通时间，需由三方侧研发/运维对日志内容进行主动验收，提交《三方服务日志上报自检报告回收》验收报告。

4.3.4 数据获取

安全项	具体要求
获取途径	1）禁止应用从京东平台外部的服务器上发起 API 的数据请求，应用类型包含但不限于服务商后台应用、商家后台应用、客户关系管理、促销管理、订单管理、订单付费、商品管理、在线订购应用、电商财务、全渠道 ERP、行业/店铺分析、客户服务、营销工具、图片/视频工具、分销应用等。 2）禁止应用通过其他应用代理发起发起 API 的数据请求。

4.3.5 数据存储

安全项	具体要求
口令存储	应用对用户口令应使用安全的不可逆的加密算法进行加密保存，防止特权用户获取用户口令。
Access Token 存储	a) 应用对其获取访问用户数据的 Access Token（授权令牌，即原来的 Session Key），应按照平台认可的安全方案进行加密存储；

	b) 如该 Access Token 涉及访问用户的隐私数据，该 Access Token（授权令牌，即原来的 Session Key）应存储在云鼎。
数据储存	应用中的数据应存储在京东平台、云鼎内，通过平台提供的解密接口获得涉及用户个人敏感信息的订单数据，禁止任何形式保存，包含不限于本地服务器或数据库等。

4.3.6 数据传输

安全项	具体要求
传输加密	应用中涉及敏感数据的传输应按照平台安全相关方案对涉及消费者个人敏感信息采取加密、去标识化等安全技术措施进行加密传输。
应用间的数据交互	a) 京东平台、云鼎内部的应用涉及敏感数据（如订单数据等）与其它应用（包括同一个开发者的不同应用和不同开发者的应用）的数据传输（包括云鼎内部应用之间的数据传输、云鼎内部应用与京东平台外部应用之间的数据传输），应符合京东安全标准进行传输； b) 云鼎内部的应用涉及非敏感数据与其它应用的数据传输，应符合京东安全标准进行传输；

4.3.7 数据使用

安全项	具体要求
数据处理	1）应用在对其敏感数据（如订单数据等）进行后台的处理或计算时，其相关功能的组件和模块应部署在云鼎内部的应用里； 2）开发者应用调用解密接口须选择使用场景及使用数据具体用途回传至平台，并且保证回传数据的真实性； 3）数据处理应根据业务场景处理业务实现所必须的最小量数据。
数据展示	1）应用应按照平台安全要求对涉及用户个人敏感信息（如姓名、电话号码、地址等）的展示，进行去标示化处理（模糊化、匿名处理等）； 2）数据展示需设置权限控制。
数据导出	应用禁止提供涉及用户敏感信息的导出功能，包括但不限于姓名、联系方式、地址等。应用涉及非用户敏感信息的导出须具备二次验证的能力，如短信验证等。

4.3.8 数据加固

安全项	具体要求
数据脱敏	对不适合对外输出敏感数据的场景，平台具备敏感数据脱敏的能力，将敏感数据进 行加工脱敏且符合不能还原的安全要求后再进行输出。

数据加密	1）敏感数据输出采用加密的方式，禁止敏感数据明文对外输出，禁止敏感数据在第三 方应用中存储明文数据。 2）提供数据解密机制，确保第三方应用仅能通过开放平台提供的解密机制来使用数据， 包括解密、密文查询等功能。 3）开放平台加解密机制应符合信息安全部安全要求。如密钥管理分配逻辑,加密算法， 密钥长度等。推荐采用集团信息安全部的加解密服务。
数据入鼎	1）京东数据要在京东授权的环境中存储和使用。未获得授权情况下，不能进行数据转移。京东授权的最佳环境为京东为第三方业务专门建立的云鼎。 2）开放平台 API 只能在云鼎中进行调用。 3）第三方应用应使用京东云数据库存储数据。 4）不同应用间交换数据要通过虎符进行，不得私自进行数据交换。被禁止的数据交换 方式包含但不限于直接写数据库、RPC、接口、消息等。

4.3.9 供应链安全要求

4.3.9.1 外部组件使用

安全项	具体要求
确保无已知风险	开发者所使用的开源软件和第三方组件不存在已公开漏洞未修复的情况。若漏洞尚处于刚公开未有官方修复措施的情况，则确保有经过评估后的补救措施。
黑名单和使用登记	开发者应当如实向京东登记其采用的开源和第三方的代码、组件和软件的名称、版本号和哈希值。禁止使用位于京东黑名单上的相关代码、组件和软件。
可靠仓库	开发者应当使用官方的仓库或经过反复验证的仓库，不得随意使用网络上公开的仓库地址。

4.3.9.2 应用自身安全

安全项	具体要求
无后门	禁止应用内设置后门或利用软件产品的便利条件非法获取用户数据、控制和操纵用户系统和设备,不会利用软件产品的依赖性谋取不正当利益，不得在用户未授权情况下对软件产品进行升级或更新换代。
禁止非关联功能	禁止应用设置与应用或自身主营业务无关的功能，例如捆绑其他软件、利用用户设备挖矿等。
默认安全	开发者应当合理配置应用的默认值,确保在默认情况下应用的配置即为安全可靠的。例如不得设置默认不哈希存储密码、对敏感信息默认

	不脱敏等配置。
安全测试	开发者应当在每次发布应用前组织安全测试，确保无已知的软件供应链漏洞存在。同时不可撤销地授权京东对发布前、发布中和发布后的应用执行对应安全测试、安全扫描。

4.3.9.3 事件响应和持续运维

安全项	具体要求
安全风险监测	1）开发者应当具备自主的安全风险监测能力，对软件构成图谱或自身应用中已经发生的风险能够主动识别、感知。 2）开发者不得忽略/拒绝或消极对待来自京东方面的安全风险监测通知，收到通知后，需按照通知所载明内容在规定时间内执行对应排查/补救动作。
应急响应	开发者具备对风险事件的应急响应能力，在发生安全事件后，根据事件不同严重性在不同的时间内完成对事件的分析、处置。
持续稳定	开发者应保证应用的持续稳定，确保有专人对尚在使用的应用提供对应的运维，不得出现无人维护的僵尸应用。

4.4 软件产品安全要求

如果您是软硬件产品供应商，为京东提供软件开发服务、软件产品或提供的产品服务包含软件系统，包括基础服务提供商、网络服务提供商、设备采购与维护服务商、软件采购与维护服务商、软件开发商、技术服务提供商、技术测评和咨询服务提供商等，需将产品部署在京东的网络环境中，请您参考本章节的内容进行安全管理。

本节内容适用于京东集团各业务单元信息科技外包及采购类项目。信息科技类外包项目在服务商交付最终验收之前，交付的信息科技产品须满足本节规范的技术管控要求，确保信息科技产品满足监管合规要求、无中高风险安全漏洞。

4.4.1 安全管控流程

项目阶段	安全动作
合同阶段	1.合同阶段需与外包服务商定义安全交付标准，项目验收时须按照交付标准执行。 2.安全管理要求： 服务商须按照合同约定参考本规范完成相关安全功能开发及交付工作。

	服务商应确保交付系统开发过程中的开发测试环境与实际运行环境隔离。 禁止服务商将交付系统源代码上传至甲方外部第三方平台，如：上传到 github、gitlab、百度网盘等。 当交付系统接受国家监管机构或测评机构检查时，服务商应积极配合做好迎检准备、应答解释及整改等工作。 服务商应在合同期间配合甲方做好信息安全审计、信息安全风险评估、个人信息影响评估、个人信息监督审计及安全功能评估验收等安全工作，对不符合项应在规定时间内配合做好整改工作。 服务商信息安全评估的结果将作为合同执行期间服务交付的考核依据，用以保证供应商服务及交付的质量和安全性。
验收阶段	1.验收阶段，需服务商提供具备安全服务资质的第三方公司实施的安全测试报告，确保系统中不能存在中危及以上安全风险及漏洞。（安全评估报告发送地址：wangjinhua25@jd.com） 2.若服务商可提供源代码，须对服务商提交的应用进行源代码安全扫描，防止系统留有后门程序，确保系统安全性。 3.基于安全交付标准，完成 ISV 安全验收。

4.4.2 安全技术要求

安全控制点	要求详情
身份鉴别	1)原则上 ISV 提供的系统/应用须接入集团统一账号体系，接入集团账号安全能力
	2)系统应具备身份鉴别功能，对登录用户进行身份标识和鉴别，身份标识具有唯一性，如使用用户 ID 做为唯一标识，ID 应是以数字组成的唯一标识。
	3）身份鉴别信息应满足密码复杂度要求，密码长度应不低于 8 位，至少由大写字母、小写字母、数字、 特殊符号中的三种组成，系统中不可存在空口令用户，密码不能与用户名相同。
	4）身份鉴别应提供校验码或验证码机制，防止暴力破解。
	5)若系统用户涉及企业账号时，企业账号基础信息由工商信息组成，其中企业名称为必选项，其他信息为可选项。
	6)当涉及重要系统或者重要操作时，建议采用两种或两种以上组合的鉴别技术(如密码、短信验证码、邮箱、Token、二维码、人脸、指纹等)对用户进行身份鉴别，其中手机和邮箱二者必须有一项为必选，其余为可选。
	7)当用户输入密码进行登录时，密码应不可见。
	8)系统密码默认有效期不低于 3 个月,更换的密码不可与前 5 次的历史密码重复。

	9)系统应具有登录失败处理功能，登录失败提示信息应模糊处理，不可将详细错误信息返回给用户；5 次登录失败直接锁定账号，锁定时间不低于 30 分钟。
	10)系统应具备连接超时登出功能，超时时间建议设置在 30 分钟内，若因业务需要可根据业务情况自行设计超时时间。
	11)账号登录后系统应显示上一次用户成功或者失败时登录时间、IP、地点、设备指纹等信息，用户可发现账号被盗用的情况，及时采取措施。
	12)如系统涉及自然人实名要求时，系统应具备实名认证功能。个人实名认证方式包含但不限于公安网校验、银行卡四要素鉴权、人脸识别、运营商校验等方式实现；
	13)如系统涉及企业实名要求时，系统应具备实名认证功能。企业实名认证包含但不限于统一社会信用代码、普通五证、多证合一、国和企业证件。统一社会信用代码为必选类型，其他为可选类型。企业实名认证须提供人工审核，通过后台对接工商数据，人工比对、工商数据实时监控和设置实名有效期。
账号安全	系统应为用户账号提供基于异常环境的安全识别功能，在异常环境中登录，需要做二次验证。比如 IP 地址异常、APP 客户端 ROOT 环境等需要做二次验证。
访问控制	1)系统应具有访问控制机制，应对主体以用户/用户组定义并控制其对客体的访问，并禁止非授权用户对客体的访问。
	2)系统应支持角色及权限的创建，针对不同角色分配系统访问权限。 权限管理应不少于三级：一级权限：应用访问权限、二级权限：功能访问权限、三级权限：数据访问权限。
	3)管理员账户，普通账户，审计账户等系统用户需职责分明，每个账户只能具有上述一种职能。
	4)权限控制应对角色访问的数据类型，访问数据的范围，单次可访问的数量都进行限制。
	5)用户首次登陆系统后应提示用户修改默认账号密码。
	6)用户账号超过 3 个月未使用时应自动锁定。
安全审计	1)系统应具有用户操作行为审计记录(日志)功能，能够记录并覆盖所有账户的操作行为，并提供检索功能。
	2)日志应至少包括操作时间，账号，真实 IP 地址，操作类型，事件详情，是否操作成功及其他审计相关的信息。不应该在日志中存储认证敏感信息。
	3)系统在没有业务需求的情况下不应提供审计记录日志的删除和修改功能。
	4)日志应单独搭建服务器系统存储，定期进行归档和备份，保存时

	间至少 6 个月。
	5)日志记录事件应通过统一的 NTP 服务获取，保证时间准确一致。
软件容错	1)系统应对所有的用户输入进行校验，确保通过人机交互或者接口输入的内容符合系统设定要求。包括 a)具备 OS 命令注入、SQL 注入、XML 注入、XPATH 注入、链接/框架注入攻击、跨站脚本攻击、路径遍历及文件包含攻击、恶意文件上传及敏感文件下载的防护能力； b)身份证号、电话号码，银行卡等个人实名数据应接入相应平台进行真实校验; c)需要本人校验数据，如指纹信息，人像数据应提供人机校验接口; d)金额、数量、交易、订单等数据在跨平台/接口流转时应进行多次认证，保证数据一致性；
	2)发生故障后具有一定程度的自保护，能够记录一部分状态信息和数据日志，并能自动恢复。
	3)不可将详细错误信息反馈给用户，应制定统一的报错页面或提示。
数据收集	1)系统应遵循合法性及最小必要原则。收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该等信息的参与，产品或服务的功能无法实现;
	2)系统应遵循用户授权同意原则。收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则(例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等)，并获得个人信息主体的授权同意。相关隐私政策及协议须经过法务部门的审核;
	3)隐私政策调整审核及公示原则。系统如有功能的增加、更改、删减涉及到对个人信息收集的变化时，应及时更新隐私政策条款内容。同时更新后的隐私政策条款应通过法务部门的审核后再发布;
数据传输及存储	1)应采用校验码技术或密码技术保证通信过程中重要数据的完整性;
	2)应采用密码技术保证通信过程中重要数据的保密性;
	3)重要数据须进行加密存储;
	4)存储个人生物识别信息，密码等认证信息时，应处理后再进行存储，例如仅存储摘要信息。如人脸信息，应该进行数据处理后保存，避免通过存储的数据还原个人人脸;
数据使用及展示	1)系统内对重要数据（L3 级/L4 级）的批量操作应设置审批流程，如批量修改、拷贝、下载等;
	2)系统内对重要数据（L3 级/L4 级）的访问、修改、下载等行为，

	应进行权限控制，且遵循最小授权原则，同时针对操作行为进行日志记录;
	3)重要数据须去标识后再进行使用;
	4)使用重要数据时应尽量保持在本系统范围内进行处理;
	5)涉及页面展示个人信息时，应对需展示的个人信息采取去标识化处理等措施;
	6)涉及重要数据的展示应在系统展示页面添加水印功能;
备份与恢复	1)应提供重要数据的数据备份与恢复功能;
个人隐私合规	系统如涉及对自然人数据的处理及重要数据处理，在产品开发需求阶段应进行隐私影响评估，开发过程中须进行自查工作，以最大限度降低隐私合规风险;
系统源代码安全管理	1)源代码开发过程中，对关键模块采取程序集强命名、混淆、加密、权限控制等各种有效方法进行保护。
	2)服务商提供的系统若涉及开源组件，须服务商做好开源组件商业化管理，避免知识产权法律纠纷。
	3）应对系统的源代码进行统一和有效的管理，建立代码库由专人进行管理和授权。
系统安全上线	1）系统正式上线前应删除所有测试页面、测试接口、私钥、密码等保密信息和代码片段。
系统安全交付	1）服务商开展服务或提供信息系统中若涉及需要使用或处理京东数据，须遵循合同中约定的数据的安全相关条款并承担数据泄露对京东造成的所有损失。
确保无已知风险	开发者所使用的开源软件和第三方组件不存在已公开漏洞未修复的情况。若漏洞尚处于刚公开未有官方修复措施的情况，则确保有经过评估后的补救措施。
黑名单和使用登记	开发者应当如实向京东登记其采用的开源和第三方的代码、组件和软件的名称、版本号和哈希值。禁止使用位于京东黑名单上的相关代码、组件和软件。
可靠仓库	开发者应当使用官方的仓库或经过反复验证的仓库，不得随意使用网络上公开的仓库地址。
安全测试	开发者应当在每次发布应用前组织安全测试，确保无已知的软件供应链漏洞存在。同时不可撤销地授权京东对发布前、发布中和发布后的应用执行对应安全测试、安全扫描。
无后门	禁止应用内设置后门或利用软件产品的便利条件非法获取用户数据、控制和操纵用户系统和设备，不会利用软件产品的依赖性谋取不正当利益，不得在用户未授权情况下对软件产品进行升级或更新换代。
禁止非关联	禁止应用设置与应用或自身主营业务无关的功能，例如捆绑其他软

功能	件、利用用户设备挖矿等。
默认安全	开发者应当合理配置应用的默认值，确保在默认情况下应用的配置即为安全可靠的。例如不得设置默认不哈希存储密码、对敏感信息默认不脱敏等配置。
安全风险监测	1）开发者应当具备自主的安全风险监测能力，对软件构成图谱或自身应用中已经发生的风险能够主动识别、感知。 2）开发者不得忽略/拒绝或消极对待来自京东方面的安全风险监测通知，收到通知后，需按照通知所载明内容在规定时间内执行对应排查/补救动作。
应急响应	开发者具备对风险事件的应急响应能力，在发生安全事件后，根据事件不同严重性在不同的时间内完成对事件的分析、处置。
持续稳定	开发者应保证应用的持续稳定，确保有专人对尚在使用的应用提供对应的运维，不得出现无人维护的僵尸应用。

4.5 第三方人员安全要求

如果您是外包服务人员，通过与京东签订合作协议的第三方合作伙伴公司为京东提供服务，请您参考本章节的内容进行安全管理。

4.5.1 安全协议签订

外包服务人员开始为京东服务前，按照京东的项目管理需求签订个人版《安全保密协议》，严格遵守京东各项保密和安全要求。

4.5.2 人员安全管理

外包服务人员开始为京东服务时，须遵守京东集团对于服务商及外包人员管理的相关规范和要求，严格按照规范要求进行入场、培训考核、账号申请、权限开通、网络接入及转岗离场等操作。