得物安全白皮书

前言

得物 App，是全球领先的新一代潮流网购社区，集正品潮流电商和潮流生活社区于一体，专注于帮助年轻人得到美好事物。得物在坚持严格的选品标准、专业的查验鉴别、统一的履约交付等服务的同时，不断完善得物安全团队，致力于建设安全可靠的网络环境，让用户获得新潮又放心的购物体验。

一.安全团队及资质

1.1 安全团队职责范围

得物安全，负责得物安全管理、安全运营、标准制定等工作，包括 SDL 评估、数据全生命周期管理、隐私合规检测、安全攻防等。已纳入众多专业人员参与平台的安全治理，致力于保障数据安全、网络安全、隐私合规等多项安全领域。

1.2 安全资质

得物安全在保障信息安全的专业性和成熟度上处于业内较高水准，保障信息安全的能力符合多项标准。

得物 App 连续多年获得信息系统安全等级保护三级认证、通信网络安全防护认证、ISO/IEC 27001 信息安全管理体系与 ISO/IEC 27701 隐私信息管理体系认证，这意味着，得物 App 在保障网络安全、数据安全、个人信息保护上持续获得权威机构肯定，为年轻人带来可信赖的潮流体验。

网络安全等级保护三级：《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》简称网络安全等级保护，是中国国家标准化管理委员会发布的信息安全标准，也是目前互联网信息安全管理行业的重要标准。等级根据信息系统的重要程度，从低到高分为一至五个等级，不同安全等级实施不同的保护策略和要求。得物已通过三级信息系统的认证，即非银行机构的最高等级保护认证。

通信网络安全防护认证：根据《通信网络安全防护管理办法》要求的一项认证工作。得物于 2022 年已获得通信网络安全防护定级备案证明，展现了完备的通信网络安全防护能力。

ISO/IEC 27001 信息安全管理体系：作为全球应用最广泛、最权威的信息安全管理标准之一，其对企业隐私保护、数据处理和信息管理等均提出多项高规格的技术和管理标准，是企业安全管理与技术服务先进性、现代化与合规的权威指标。得物已通过此项认证，体现了其在网络基础安全能力和信息安全保障能力上均达到国际高标准。

ISO/IEC 27701 隐私信息管理体系：该标准建立在 ISO/IEC27001 要求的基础之上，规定了建立、实施、维护和持续改进隐私相关所特定的信息安全管理体系的要求。得物已通过此项认证，建立起保护个人信息的管理体系（PIMS），将处理个人可识别信息 （PII）所需的隐私保护措施纳入考量。

二.物理基础设施

得物安全制定安全管理制度，明确规定了机房访问管理、机房环境安全等要求，并采取了完善的管理和技术措施保障基础设施安全。

得物的配套数据中心位于浙江杭州，合作了国内头部服务提供商支持相关服务，得物与其签订协议明确双方的责任和义务，明确服务范围和数据中心的服务可用性水平，保障系统物理安全和基础设施安全。

在安全通信网络方面上，互联网边界处已设置访问控制策略，通过部署防火墙等方式对网络入侵、DDOS 攻击等网络攻击事件进行识别、报警和分析，并及时检测和清除恶意代码。

三.安全管理

3.1 人力资源管理流程

得物为各项人力资源活动提供了安全保障，在保证信息便捷共享的同时，也搭建了严密的防护网，有效避免信息泄露。

新员工的聘任须经过相关部门和岗位需求部门的审批，新员工招聘流程与结果记录在人力资源系统中；

经员工授权，人力资源部会在国家法律法规允许的情况下对部分岗位进行背景调查，确保该岗位上的员工录用符合公司的各项规章制度；

新员工入职时将接受信息安全相关的培训，强化安全意识、践行信息保密规范；

新员工须签订劳动合同和保密协议，其中对员工在信息安全方面所应承担的责任和义务进行了规范；

员工的各项权限启用严格遵守工作相关原则和最小授权原则，满足日常分享协作的要求同时保证其他用户个人隐私安全；

员工离职须由本人或部门领导在人力资源系统中发起申请，经过人力资源部、相关职能部门进行审核后方可正式离职，离职前注销其所有账号并需归还所有硬件和软件资产（如电脑、工作文档等）。

3.2 安全制度

得物安全联合法务团队统筹安全制度的建设工作，已制定一套完整的安全管理制度，特别是数据安全和个人信息保护制度，规范了得物个人信息处理流程，覆盖了数据的全生命周期。

3.3 安全培训与学习

得物安全长期组织各类安全培训活动，并通过线上/线下多种渠道进行信息安全宣导，有效覆盖得物全部员工职业生命全周期，积极营造正向安全氛围，提升整体信息安全意识。

3.4 终端安全管控

得物安全通过网络准入控制验证内部网络访问者身份，可有效拦截非法外部访问、无身份异常访问、部分黑客攻击等请求。

得物所有员工办公终端均部署有防病毒软件，可及时查杀各渠道病毒，将病毒威胁防患于未然。办公终端的防病毒软件都默认安装、后台自动升级病毒库和防病毒扫描策略，无需人工干预，员工无法主动卸载防病毒终端。员工离职后，将针对办公终端磁盘进行全面格式化，清除其携带的数据，并重新安装操作系统。

3.5 安全审计

得物安全长期开展审计专项，通过梳理系统清单、厘清个人信息流转情况等手段审计数据存储、数据加密、数据脱敏、数据共享等个人信息处理情况，有效识别用户个人信息管理风险，提出整改建议并推进整改方案落地，满足监管层面合规，同时提升内部管理水平，降低用户数据泄露风险。

四.网络安全

针对互联网行业普遍面临的 DDOS 攻击、网络钓鱼、网络黑灰产等威胁，得物安全一贯保持演练状态，通过“安全监控大屏”7*24 小时密切监控网络异常。同时联合国内多家头部云厂商、安全厂商，针对公司网络边界及纵深，从舆情监控、策略配置、风险识别、防御控制、事件响应、安全恢复等各阶段建立了一套完整的联动机制。

五.服务器安全

得物安全采取了一系列安全管控措施，保障服务器生产安全，有效防范网络恶意攻击行为。

5.1 服务器访问控制

得物安全定期扫描服务器资产，及时关闭非标服务器开放端口及服务，减少对外安全敞口。同时，定期进行弱口令检测，督促服务器运维人员提升密码复杂度，防范暴力破解。另外，限制服务器访问路径并规范留存操作日志，通过安

全组、防火墙、白名单等手段控制业务服务的访问来源，保证仅授信来源可以访问。

5.2 漏洞扫描

得物安全采用自动化的漏洞扫描工具，定期进行服务器系统漏洞检测，检测结果经确认后及时推动处理，并定期督促运维人员进行系统补丁更新，有效保障服务器稳定运行。

5.3 入侵检测

得物服务器全面部署了入侵检测系统，可以支持自动化实时入侵威胁检测、病毒查杀、漏洞智能修复、基线一键检查、网页防篡改等功能。外部通过 WAF（应用防火墙）攻击检测并验证客户端流量，对恶意请求予以实时阻断。内部通过 NIDS 检测潜在入侵流量，确保服务器安全性与合法性。

六.应用安全

得物安全结合自身的业务模式，用更高标准建设平台的底层安全，研发出“原生免疫系统“和“原生防护系统”，打造具备安全基因的安全基础设施，成为支撑平台安全的坚实基础。

面对不断升级的攻击手法，得物安全结合云服务商原生服务能力，以及天然的电商基因，通过融入天然一体的云基础设施，把碎片化的安全能力打造成系统性、可全局联动的原生免疫系统，把复杂的安全问题归纳成极简且智能的原生防护系统，让上层应用得到有效保护。

同时，得物安全根据自身业务特点，结合公有云打造基于得物安全需求的一体化网络安全基础底层，为用户应用保驾护航。

6.1 安全开发流程

得物安全追求从源头解决安全漏洞，定期开展安全意识培训，安全评分考核。

所有产研人员均须完成安全培训，了解安全漏洞成因及编码知识。得物开发流

程严格遵循 SDL(安全开发生命周期)，从需求、设计到发布产品的各个阶段均配置相应的安全活动，以减少漏洞数量并将安全缺陷降低到最小程度。

6.2 漏洞与安全事件管理

得物安全拥有完善的漏洞生命周期管理策略，通过多种自动化检测工具，对内部服务进行安全检查，一经确认会根据漏洞等级第一时间推送至相关应用负责人进行修复处理。

得物安全开放了 SRC 平台，积极鼓励外部白帽子提交漏洞。同时，与业界顶尖的第三方公司签订合作协议，邀请其对公司内外网进行渗透测试，以求提升安全能力。

得物安全已制定完善的应急响应预案，针对突发安全事件，严格执行 7*24 小时应急响应策略，当安全事件发生后第一时间遵照信息安全事件处理流程做出响应。

七.隐私合规安全

7.1 运行环境

得物安全通过 root/越狱检测、hook 框架检测 、模拟器环境检测、多开环境检测、代理环境检测、调试检测 、二次打包检测等手段对得物 App 运行环境进行检测，以保证环境安全可信，防止被非法利用。

7.2 隐私合规

得物安全重点关注其所持有个人可识别信息（PII）的隐私保护工作，从数据生命周期入手，对 PII 收集、传输、使用、共享和披露等过程均实施了严格要求。得物安全定期进行 App 隐私合规自检，同时委托第三方测试单位对 App 进行隐私安全检测并出具检测报告。

7.2.1 全生命周期个人信息保护

对于收集的用户个人信息，得物建立起了全生命周期保护，从收集使用个人信息的事前、事中、事后，全方位落实保护措施，保障数据的全流程管控能力。

（1）隐私政策的制定、发布与更新

基于公司实际业务开展的需求以及具体的业务场景，得物数据合规法务与安全合规部门协作配合，制订简明、易懂、全面、透明、易获取的《隐私权政策》。同时，得物要求，各业务部门的个人信息收集、处理活动与《隐私权政策》文本内容相一致，业务实质性变更与《隐私权政策》更新相一致。此外，对于处理用户的敏感个人信息；向第三方提供或委托第三方处理用户的个人信息；公开用户本人的个人信息；向境外提供用户个人信息的，得物皆会在对应页面植入文本以履行单独告知并获得用户单独同意的义务。

（2）个人信息保护影响评估

在具体业务场景之下，得物要求将数据保护措施融入到产品设计的理念中；同时，新服务、产品、信息系统等上线前，会评估其处理个人信息的安全风险，以防止更新服务功能、产品或信息系统可能会对个人信息主体权益产生的影响。个人信息保护影响评估记录也作为得物已落实相关合规义务的证据。

（3）个人信息分类分级管理

得物从个人信息分类分级管理和个人信息清单方面提供了隐私合规指引。在隐私合规要求的指引下，规范数据处理流程，保障公司的数据资产安全，避免数据处理不当引发的数据安全风险。

（4）用户同意

除法律存在特殊性规定的情形外，一般而言，获得个人信息主体的同意是收集、处理其个人信息的必要前提。在具体的业务场景下，得物会在获取个人信息主体的同意后对其个人信息进行收集、处理，并记录个人信息主体的同意，并保障个人信息主体撤回同意的权利。

（5）收集

得物坚持收集个人信息的最小必要性原则，并通过采取假名化、匿名化和传输加密等隐私增强技术，保障个人信息收集、传输过程中的安全。

（6）使用

得物各部门坚持在向个人信息主体叙明并获得同意的处理目的范围内使用个人信息，并采取适当的技术和组织措施，保障个人信息的使用安全。同时，得物亦对用户数据的访问权限进行严格的限制，通过《数据权限审批及访问控制管理办法》，明确公司对信息、数据的权限设置、安全控制要求。

（7）存储和处置

得物通过制定和维护操作规范明确了业务处理活动中涉及的个人信息的留存期限，规范个人信息的存储与删除行为，加强对个人信息的保护。个人信息留存期结束后，公司技术部门会对个人信息采取删除、匿名化或销毁等处置措施。

（8）跨境传输

确保个人信息跨境转移的合规性是得物安全中心的工作重点之一。在个人信息跨境转移前，得物数据合规法务与安全合规部门会首先对目的地的法律环境进行评估，选择合法合规、适当的跨境转移机制，并对可能存在的风险提出适当的整改措施，并保留数据出境安全评估和数据转移协议等相关记录。同时，对于需要履行数据出境安全评估的情形，得物积极开展落实自评估工作。

7.2.2 第三方 SDK 管理

得物坚持在合法、正当、必要的原则下接入 SDK，并在事前、事中、事后采取全方位措施，以保障用户隐私安全。得物《隐私权政策》向用户明确了由第三方 SDK 提供的产品或服务，并提醒用户关注第三方 SDK 用户个人信息处理规则。同时，得物要求第三方 SDK 告知自身所收集的个人信息字段，并要求第三方 SDK 作出承诺，其应在自身隐私政策的范围内收集个人信息，不得超出用户授权范围收集、使用、处理个人信息，或私自向其他应用或服务器发送、共享用户个人信息等。同时，得物安全会不定时对第三方产品或服务进行安全监测，在发现其未落实安全管理责任和要求时，及时督促其整改，必要时会停止接入。

八.数据安全

得物安全对数据全生命周期进行管理，对各阶段均制定了明确的规范和流程，配置了技术保障措施，并搭建了一系列平台系统确保技术保障措施的覆盖和落实。

8.1 数据传输

得物安全为用户提供了基于强加密协议的加密链路，支持从用户端到服务端的

全链路加密传输。同时，得物自研并部署独有的加密签名算法，确保得物 App 在数据传输过程中不被破解，保障数据传输安全。

8.2 数据使用

得物安全已建立完备的权限治理策略，系统、数据库等数据访问权限均须单独授权，且权限管理系统已对接员工管理系统，实现异常场景下的系统权限自动回收。安全团队定期对权限分配及使用等情况开展审计。

8.3 数据存储

得物安全自研敏感数据加密网关（融合数据加密和密钥管理功能），采用国际领先的强加密算法对敏感数据进行数据库加密存储。同时，网关对接数据库管理系统，及时审核数据库表的变更操作，确保新增敏感数据加密存储落库，不会遗漏。

得物安全已制定数据分类分级标准，通过数据资产地图实现自动化数据分析和分类分级，并对不同类别、级别的数据实施不同的安全管控策略。

8.4 数据销毁

用户可通过得物客户端进行账号注销或提出个人信息删除需求，接收到账号注销或个人信息删除的申请后，得物将对注销账号的数据及文档等进行删除或匿名化处理。

所有数据删除或匿名化处理技术手段均符合法律法规要求、行业通行标准。

8.5 合作方数据安全

针对合作方数据交互，得物安全联合法务团队制定合作方安全准入基线。合作方接入前，得物将对合作方的安全资质、内部安全能力等开展评估，符合要求后方允许接入。

得物自建安全网关，合作方统一使用安全网关接入。安全网关对数据加密、数据流量进行统一管理。

九.灾难恢复与业务连续性

9.1 备份与灾难恢复

得物已建立完善的数据备份机制，对信息系统的数据备份、运行维护与管理、灾难恢复与演练进行了规范。基于现有的云服务商以及自建存储系统，实现了多云、多区域备份，同时具备快速恢复现有数据的能力。

9.2 业务连续性保障

得物业务系统接入层均采用高可用方式接入，保证服务的可靠性。对流量和故障做细致监控，在发生流量突发等故障时，采用降级运行方式保障业务可用性。

得物针对可能导致业务中断的场景进行了严格梳理，并制定了相应的应急响应和恢复措施。得物定期评估最大可容忍中断时间、恢复时间目标和最小服务水平等指标，执行业务影响分析和风险评估，识别重要业务流程和可能造成公司业务与资源中断的威胁，并针对不同业务的中断场景制定应对策略。

9.3 应急演练

得物具有完备的应急演练机制，通过引入随机和不可预知行为的受控实验来识别威胁，定期进行故障演练，保证得物全站全年数据的可用性。

十.变更控制

10.1 程序变更

得物已制定完善的程序变更管理规定，明确了变更管理要求及流程，包括变更方案制定、变更评审、变更审批及变更实施等。得物产研人员所有变更操作，经批准后方可执行，以防影响服务的稳定性。公司各应用均部署有独立的开发、测试及生产环境，变更经测试后方可上线。

10.2 源代码控制

得物已制定严格的源代码管理流程，研发人员仅可访问和管理其所属团队对应的代码仓库。代码仓库中各项目代码仓设置了代码仓负责人，研发人员如需申请其团队以外的代码仓库访问权限，须在代码仓库中提交申请，经其部门主管和所申请的代码仓库负责人严格审批后，才可添加相应权限。

10.3 基础架构变更

得物在公网边界部署访问控制列表对网络访问进行控制。若需对 ACL 配置基线及网络访问控制列表进行变更，运维人员通过平台提交申请，由专业工程师对变更合理性进行判断后执行操作。仅授权的工程师拥有执行网络访问配置的变更操作权限。

10.4 变更监控

得物定期执行内部审计以检查公司内部控制体系的运行情况，其中涵盖对变更管理相关控制的执行有效性检查。若发现异常，由内审部门和相关负责团队沟通并跟进整改结果。