vivo安全与隐私保护透明白皮书

vivo

目录

01

vivo安全与隐私保护的战略与原则

1 vivo安全与隐私保护的战略与原则

近年来，随着人们工作和生活的数字化进程不断加快，海量个人信息以数字化形式传输、存储和使用，但保护不足的问题日益凸显，数据安全与隐私保护已经成为社会关注的热点议题。近些年来，中国相继颁布和实施了《网络安全法》、《数据安全法》和《个人信息保护法》，以法律条文形式向社会、企业等层面明确提出数据安全与隐私保护的要求，并提供了必要的指导措施。从用户角度来说，移动智能终端涉及大量用户个人数据的采集和使用，其数据安全与隐私保护能力成为用户选择智能手机品牌时优先考虑的重要因素之一。

对此，vivo一直致力于打造安全可信的数字化产品与服务，让用户在享受便捷数字生活的同时，保护好自身隐私。vivo构建了涵盖安全与隐私保护战略、隐私保护原则、安全与隐私组织、管理流程、安全与隐私技术工程、安全与隐私文化和培训等各方面完善的安全与隐私保护管理体系。本白皮书，将对该体系进行透明展示。

1.1 公司安全与隐私保护战略

vivo创始人、总裁兼CEO沈炜先生曾说过：

“……数据安全与隐私保护是消费者的基本权利，是企业获得消费者信任的基石，我们要把数据安全、隐私保护与守法合规作为企业研发经营活动中绝对不可以触碰的红线和基本底线，来指导各项工作的开展……”

上述这段话，表明vivo公司对于安全与隐私保护策略的重视态度，提出了vivo整体的安全战略：**隐私是用户的基本权利，vivo必须全力保障**。

vivo将安全与隐私保护提升到公司战略层面，保证vivo在安全与隐私保护上的长期投入，使能最优的科技手段为用户数据与隐私护航。在2022年7月发布的《vivo可持续发展报告》中，vivo正式将信息安全和用户隐私保护作为公司可持续发展的重点投入方向。

图1：《vivo可持续发展报告》中展示，信息安全与用户隐私保护成为重要性最高的两个课题

此外，vivo率先在业界提出人文安全的理念，即在用户隐私保护层面，在以科技能力为前提的基础上，还通过更透明可控的安全设计、更优雅易用的安全体验、更符合特殊人群的隐私保护需求的安全服务，将更科技转变为更人文更有温度的安全守护，让所有用户均可简单安心地保护好自己的隐私。

1.2 公司隐私保护原则

为践行公司安全与隐私保护战略，vivo通过对行业的深入洞察和分析，结合内部最佳实践，总结出vivo隐私保护三原则，并融入到vivo相关产品服务的需求、设计、开发、测试、发布、运维各个环节，在数据流动的全链路、用户体验的全场景，全面守护用户隐私。

原则1 透明可控

在提供各类服务时，确保用户明确知悉设备上数据的分享和使用情况，并且可进行管控；

原则2 端侧处理

在提供各类服务时，数据尽可能在设备本地处理，减少数据流出设备；

原则3 数据最小化

在提供各类服务时，仅采集和使用服务必需数据，减少数据收集。

02

vivo安全与隐私保护体系

2 vivo安全与隐私保护体系

随着互联网时代的大潮和大数据技术相继出现，用户的数据安全与隐私保护受到越来越多的关切，全球各地不断发布和更新相关的法律法规。vivo以法律法规为指引，借鉴业界标准，洞察监管要求以及行业动态趋势，结合vivo公司自身实践，建立了一套完善的安全与隐私保护体系，用于指导数据安全与隐私保护工作的有效开展。

2.1 体系架构

vivo的安全与隐私保护体系架构如图2所示，其组成部分为：

图2：vivo安全与隐私保护体系架构

公司安全战略

如前章节所述，vivo在公司战略层面明确了数据安全与隐私保护是消费者的基本权利，数据安全、隐私保护与守法合规作为企业研发经营活动中绝对不可以触碰的红线和基本底线。

隐私保护三原则

隐私保护三原则是vivo根据自身经验以及业界实践汇总的公司级的指导方针。隐私保护三原则体现在公司对于安全技术点的研究和部署、自研产品流程的卡点与检测、数据全生命周期的保护中，是vivo对于隐私保护的最终目标。

PROTECT安全与隐私保护技术战略

vivo结合行业优秀实践以及公司现状，拆解对于安全与隐私保护的需求，在隐私保护三原则的指导下，针对每个需求点提供对应技术解决思路，制定了PROTECT安全与隐私保护技术战略，为承接公司安全战略，指出聚焦主攻的技术方向。其中P代表隐私（Privacy）、R代表数据风险（data Risk）、O代表产品对象安全（product Object security）、T代表关键安全技术（security Technologies）、E代表安全工程（security Engineering）、C代表合规管理（Compliance management）、后一个T代表安全攻防（security penTesting）。在PROTECT技术战略的指导下，安全技术的研究重点投入在对应的技术点，有的放矢，提升能力，满足公司安全与隐私战略和隐私保护三原则的要求。

安全与隐私组织

vivo成立了网络信息安全和用户隐私保护委员会、安全与隐私专业部门，并配备了业务部门安全合规负责人、内部认证安全/合规工程师等职位分别履行安全与隐私工作，确保公司安全与隐私保护战略的执行。

相关方规范和需求

vivo按法律法规要求，以及利益相关方，包括用户、客户、员工、监管和合作伙伴等的安全需求，经过洞察和解析后，转换为内部流程和内部需求进行管理，包括形成内部的数据安全与隐私保护的制度、规范与要求等。

产品开发流程安全与隐私保护

vivo采用嵌入式方式，把安全与隐私相关要求端到端地融入到产品需求、设计、开发、测试、发布和运维的全生命周期中，提升产品的安全性及合规遵从性。

数据全生命周期安全与隐私保护

vivo在数据采集、传输、存储、处理、交换和销毁的全生命周期中，制定了相关安全保障措施，满足合规要求的同时，严格保护用户的数据和隐私。

工具能力建设

为提高安全与隐私保护工作的效率和有效性，vivo构建出一整套安全与隐私保护检测工具，并融入到日常开发活动和业务流程中。

生态与用户沟通

vivo积极参与行业生态建设并与用户保持透明沟通，利用隐私中心窗口，向用户展示vivo所具备的安全与隐私保护能力和相应工作，并构建部分数据主体权利自动化处理。

数据安全与隐私保护标准

vivo将公司遵循的安全理念与具体实践输出给业界，共同提升业界安全与隐私保护水平。vivo积极参与国内外标准化工作，贡献自身的经验和最佳实践，参与相关标准的制定。

数据安全与隐私保护认证

vivo积极与国内外公认的权威安全标准对齐，提升整体安全水平。vivo积极开展认证工作，并在数据安全与隐私保护方面获得多项国际和国内权威认证。

2.2 组织架构

vivo公司的安全与隐私保护管理组织架构如图3所示，其组成分别为：

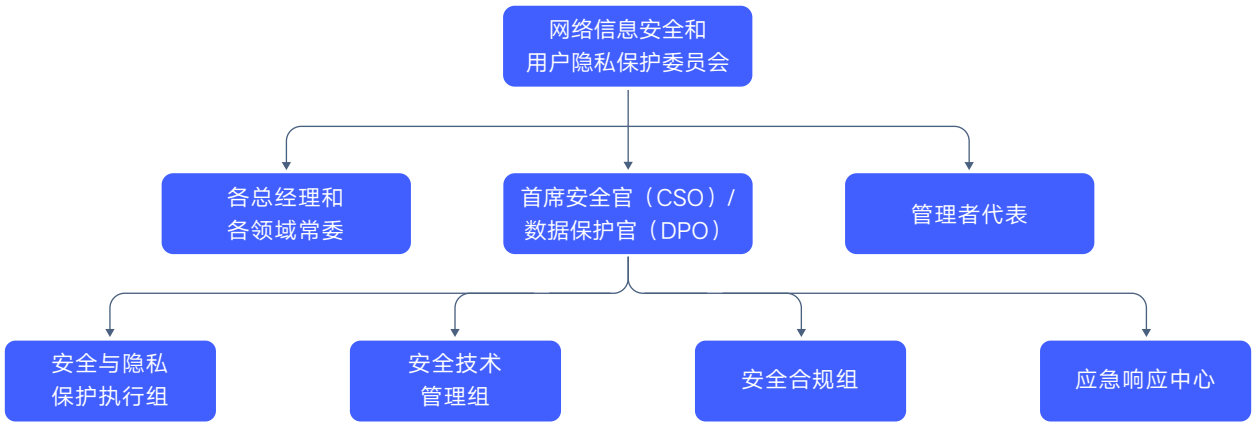


图3：vivo安全与隐私保护管理组织架构

- **网络信息安全和用户隐私保护委员会**

作为vivo数据安全与隐私保护最高管理机构，直接向公司经营最高决策机构—公司管理委员会汇报，负责决策和批准公司总体安全与隐私保护战略和执行落实。

- **首席安全官（CSO）/数据保护官（DPO）**

对技术和管理执行的推动和落实提供支持，确定数据安全与隐私保护管理工作的方向和目标；建立跨组织的数据保护横向团队，形成管理合力。

- **各总经理和各领域常委**

作为该领域和部门安全的最高负责人，为安全工作的落实提供决策和支持。

- **管理者代表**

从公司管理者角度，综合各类信息，开展评估和决策，给出管理改进方案。

- **安全与隐私保护执行组**

作为安全与隐私保护的业务部门，推进和落实安全与隐私保护相关事项，并同步执行情况。

- **安全技术管理组**

持续关注行业发展趋势，并结合公司现状，支撑安全与隐私保护的整体技术架构和规划，制定未来的路标和策略。

- **安全合规组**

根据公司发展方向策略，建立预防和改善机制，制定、维护数据安全与隐私保护政策和相关规程，组织开展相关培训，确保平台、系统、产品、服务符合安全合规要求。

- **应急响应中心**

统一处理外部安全与隐私事件，向网络信息安全和用户隐私保护委员会、CSO/DPO汇报。

2.3 赋能培训

vivo深知员工的安全意识培养与技能培训的重要性，为此，vivo构建了一套完整的安全培训体系，不断提升公司全员的安全与隐私保护认知，形成人人重视安全与隐私保护的文化，为公司安全与隐私保护工作提供保障，进一步提高vivo面向用户的产品服务的质量水平。

通过vivo网络安全与隐私保护活动月和主题周、安全与隐私保护轮训、专家讲座、知识竞赛、安全攻防大赛等活动，以及不断完善的配套激励制度，vivo持续提升全员安全意识，践行公司安全文化。

例如，vivo举行新员工入职安全与隐私保护相关课程的培训；针对在职员工开展安全与隐私轮训；结合业务部门实际情况，持续总结并发布安全与隐私典型案例和FAQ；每周例行推送安全与隐私-每周早报：V资讯-热点事件、V学习-重要法律法规、V事件-重大事件；通过授课、考试以及实践等方式为业务部门培训一线认证合规工程师和认证安全工程师；举办数据安全主题周活动为全员提供了更加全面的数据安全和隐私保护的相关知识。

2021年，vivo举办的数据安全主题周活动以“数据安全，护航未来”为主题，在线上和线下同步进行，包括安全技术分享、案例讲解、游戏互动等环节，通过此类互动体验，让vivo员工直观地感受数据安全与隐私保护的重要性，在工作中养成将安全与隐私放在首位的意识。

03

安全与隐私保护融入集成产品开发流程

3 安全与隐私保护融入集成产品开发流程

产品的安全与隐私保护需要依赖流程和制度进行保障，因此在产品的全生命周期中，vivo通过在项目集成开发产品（Integrated Product Development，IPD）流程的各个环节融入安全与隐私保护要求和活动，包含有安全、隐私、合规对应的工作，来保障最终交付产品和服务的质量。

图4：vivo产品开发生命周期的安全隐私保障

3.1 需求阶段

作为产品开发周期的第一个环节，每个项目在明确需求集合后均会对可能涉及的安全、隐私、合规等相关风险的需求点进行拆解和识别。经过安全与合规专家评审后，制定风险缓控措施和开发设计要点，并将结论纳入后续详细设计方案中，同时发起其它必要的评估流程。

1. 需求安全合规评审

vivo根据国内外法律法规及行业标准、客户安全需求、业界最佳实践等制定了《vivo安全需求基线》，对涉及到数据全生命周期、云端API、账号认证、端口开放、WebView使用等多种需求场景提出明确要求，为业务需求分解提供指导。在需求阶段，安全和合规专家会协助产品经理依照安全基线对需求集合进行拆解和分析，确定潜在安全与隐私需求并随项目功能需求同步跟进，确保项目需求落地的安全性和合规的遵从性。

2. 引入能力安全及合规评估

对于将要引入并集成到代码的外部能力，vivo以《vivo外部引入安全准入要求》为标准，建立了完备的评估流程。通过资料收集建档、基础安全合规扫描、人工渗透分析以及迭代情况平台留存等节点保证引入技术能力的安全性与合规遵从性。当集成组件发现风险时，vivo档案化的管理方式，能够及时溯源并通知所有的集成模块进行升级修复，从而有效地将影响降到最低。

3. 供应商引入数据保护与隐私合规风险评估

引入新供应商时，vivo首先判断供应商是否涉及接收、访问、处理、共享vivo用户的个人信息。在与供应商签约前，vivo对供应商数据保护与隐私合规风险进行评估，确保所选的供应商具备必要的隐私保护能力*。通过评估后，vivo与供应商签署含数据保护内容的合同或数据处理协议。

注：隐私保护能力，即根据业务所在地的个人信息保护相关法律法规要求处理个人数据，并采取了合理及适当的管理、技术和物理措施保护个人数据免受丢失、滥用和未经授权的访问、披露、更改和破坏，且没有发生过重大安全与隐私事件。

3.2 设计阶段

vivo遵循设计驱动的企业文化，践行隐私设计（Privacy by Design，PbD）原则。在项目架构设计阶段，架构师会根据《vivo安全设计规范》对产品开展安全架构设计和业务安全需求设计，出具包含保障架构安全性和合规性的设计方案后，需通过项目安全与合规专家评审。同时对判定为高风险功能场景的方案开展威胁建模，确保架构设计的风险最小化。经过建模分析及评审产生的设计方案形成后续验收阶段的测试用例，用以对安全设计及风险保护能力的验证。

1. 隐私设计

隐私设计是保障产品安全隐私体验的重要方法论和实践指引。隐私设计的 7个最佳实践原则包括：

① 主动应对（预防）而非被动响应（补救）：需要先预测潜在的威胁、识别出弱点，从而减轻和消除隐私风险，做到提前预防，而不是事后补救；

② 隐私作为默认设置：将数据最小化、限制数据访问等作为产品的基础能力，为用户提供默认的隐私保护；

③ 隐私设计驱动：隐私保护不是产品和服务的附加能力，而是需要将隐私保护的理念嵌入到产品开发流程中的各个阶段 ；

④ 功能正和，而不是零和：采用“双赢”的方法来实现产品中所有合法利益方的目标，从而使得不同的合法利益各方，都能相互共存；

⑤ 端到端安全和全生命周期保护：在数据的收集、存储、使用、转发等各个阶段，都需要采取最充分的保护措施，以实现数据全生命周期的保护；

⑥ 可见性、透明度、保持开放：数据主体及相关方，能获得用户数据的收集和使用的详细情况；

⑦ 尊重用户隐私，以用户为中心：在收集和处理用户数据时，需要及时通知用户，并得到用户的友好支持，保证用户的权利和自由。

实践中，需要将隐私设计的7个原则，贯穿整个产品的生命周期。隐私设计落地的全流程涵盖：隐私设计原则、隐私设计策略、隐私设计模式、隐私保护技术、隐私设计案例等部分。其目标是从产品设计原则开始，即充分考虑安全与隐私保护风险，并具有风险消减措施。vivo在其产品的打造过程中已实践隐私设计多年，这是保障vivo产品安全与隐私保护体验达到较高水平的重要基础。

2. 数据保护影响评估

在设计阶段，通过系统化方法，对vivo的业务流程、产品、系统中涉及的个人信息采集、传输、存储、处理、交换和销毁活动开展风险识别、分析和评估。其中包含评估个人信息活动过程中的安全管控弱点程度、面临的威胁种类与影响程度。数据保护影响评估内容包含但不限于：功能特性、数据清单、敏感权限、数据流程图、第三方供应商、初评、风险评估项。

3. 方案安全评估及威胁建模

为将《vivo安全设计规范》更好地融入流程，vivo将规范的核心部分拆解后纳入设计方案模版中的安全设计章节。该章节要求项目从威胁建模，基础安全设计两方面对架构进行分析，其中包括加解密算法、日志打印、数据生命周期保障、权限、外部引入、各国安全要求等共计11大安全设计风险面，有效协助架构设计工程师进行全面的威胁分析。另外，vivo遵循业界最佳实践对高风险场景开展威胁建模活动，将架构设计存在的安全风险尽量全面的在设计阶段暴露出来，并对发现的风险制定相应的缓解措施。此部分案例同时也应用于建立设计风险库和缓解措施库，并不断迭代，成为后续业务设计的指导和参考。

3.3 开发阶段

项目进入开发阶段后，为了持续推进编码工作的高标准和高质量，vivo对内定制了针对业务源代码的批量自动化扫描能力，集成成熟的商业化扫描工具以及自研的代码安全扫描插件。在编码基本完成时，业务需要依照列表对代码整体做提测前的最后一道检查，确保每个风险项都已经消减，最后结果将会由项目中的品质工程师进行验收。

1. 代码安全扫描插件

vivo针对内部开发人员常用的Android Studio、IDEA定制研发了代码安全扫描工具。该工具以插件的形式集成，会在开发人员编码过程中实时检测，以及在分支合并，编译构建和持续集成/持续交付（Continuous Integration/Continuous Delivery，CI/CD）流程中进行代码扫描。扫描规则覆盖主流安全漏洞和《vivo移动应用安全编码规范》中的内容，同时具备代码质量、性能和稳定性方面的检测能力。

2. 源代码安全扫描

源代码静态扫描是指在软件工程中，使用扫描工具对项目源代码进行扫描，并找出代码中存在的语义缺陷、安全漏洞等问题的解决方案。在vivo，产品项目的源代码扫描运行在CI/CD流水线扫描模块，与依赖包扫描、敏感文件等扫描作为平行扫描任务。目前扫描引擎支持Java、Python、Go、NodeJS、C++五种编程语言和二十种主流安全漏洞类型的检测，并能够生成从入口参数到触发点的漏洞利用链扫描报告。

在CI/CD流水线执行构建时，源代码扫描模块异步提交扫描任务给DevSecOps安全度量系统，由DevSecOps系统总体负责任务调度下发和报告回传的工作。DevSecOps系统下发具体扫描任务给作业平台，并由作业平台调度扫描引擎，进行扫描并上传报告至报告服务器。最后DevSecOps系统获取报告内容，并将报告内容连同扫描状态等信息返回至CI/CD流水线。总体流程架构如下图所示：

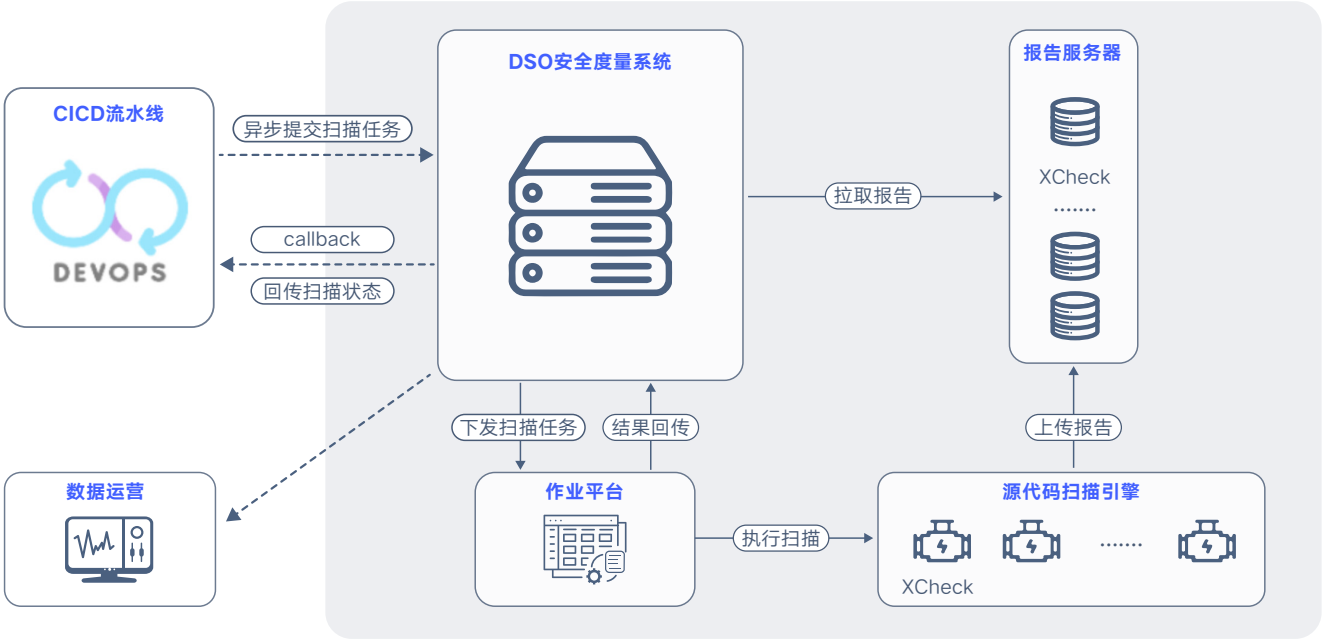


图5：源代码安全扫描流程

3.依赖包安全扫描

随着公司项目业务不断扩增，版本频繁发布，开发项目经常引用二方或三方依赖包进行开发。当依赖包存在漏洞时，易受外部针对性攻击，使业务遭受损害。

现阶段vivo大部分项目都是基于Java实现的，而围绕Java构建的开发生态普遍依赖第三方组件来完成开发。同样的，除了Java以外，Python、Golang、Nodejs都有大量的三方组件，而这些三方组件可能会引入大量的漏洞，需要软件成分分析（Software Composition Analysis，SCA）进行检测。为规避以上由依赖包安全漏洞带来的业务安全影响，vivo开发了一套针对依赖包管理的系统，提供项目依赖包的分类、版本及安全基线的管理。

目前，vivo针对不同的场景需求，分别设计了定时扫描与CI上线扫描两种流程。

① 定时扫描：每日凌晨零点对已经部署预发环境和生产环境的制品进行扫描。根据部署记录，服务器从制品仓库中下载对应的制品进行扫描。如果触发设定的阈值，就会创建漏洞工单，同时通知对应的安全工程师和业务人员。

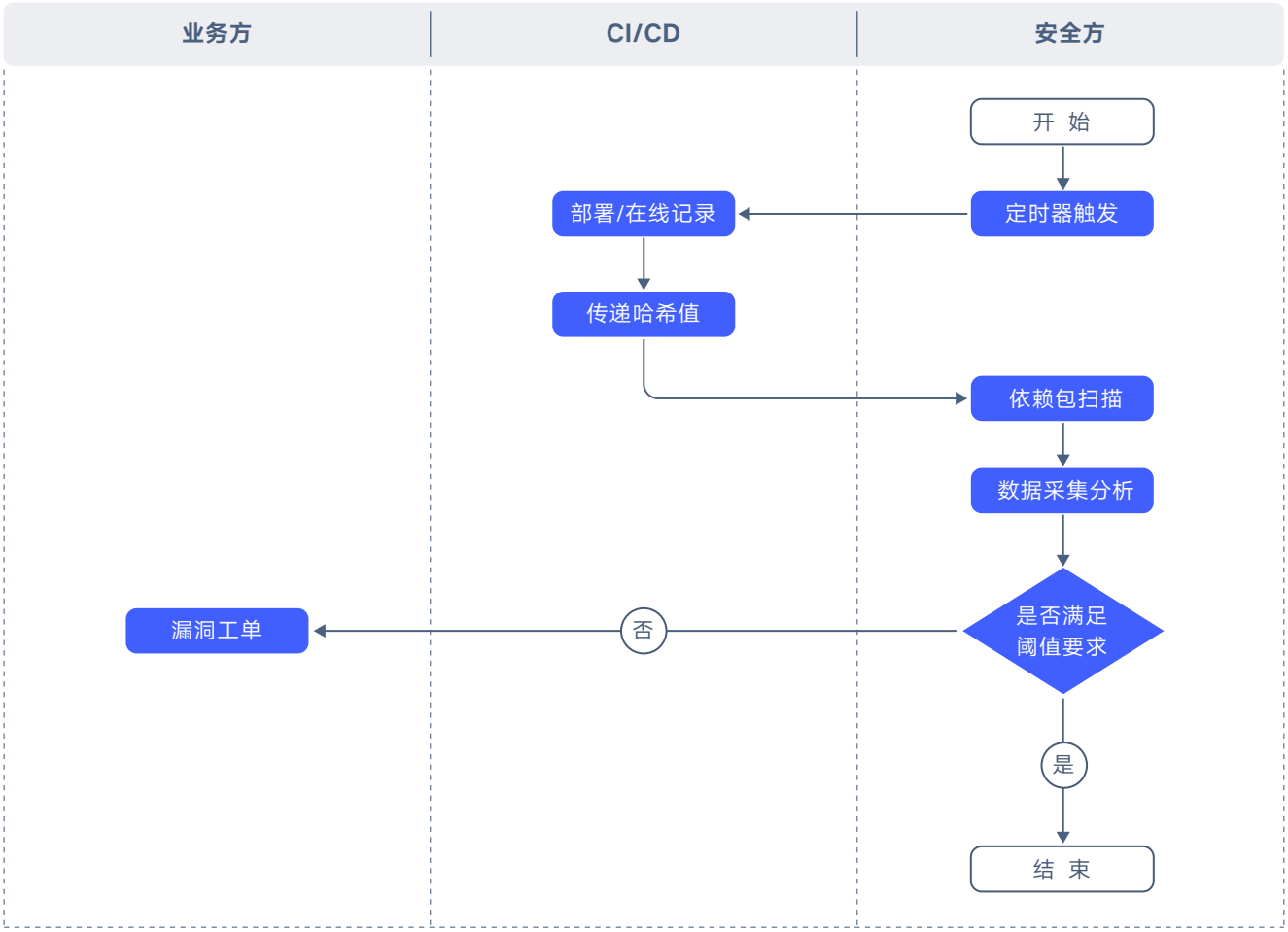


图6：定时扫描流程

② CI上线扫描：在业务流水线构建之后，获取构建制品的哈希值，实时对制品进行依赖包安全扫描。扫描结果展示在流水线CI/CD平台，并通知相关业务人员，提醒在业务上线时，需要进行卡点检测。

通过这两种依赖包扫描流程，在开发阶段以及部署阶段实现常规化运营，及时有效的发现监控到相关制品的依赖组件，并且为后续预警处置提供数据支持。

4. 敏感文件扫描

在实际场景中，可能会出现由于配置不当造成敏感日志和项目配置文件的泄露的问题，这使得攻击者可以更全面地收集信息，进而导致应用面临信息泄漏的风险。常见的原因是运维人员疏忽、存放敏感信息的文件泄露或网站运行出错等。例如，如果Web应用程序显示了某些文件名称，此信息能帮助攻击者对站点进行进一步的攻击，攻击者可能猜测文件的内容、其它的文件名或目录名，并尝试访问它们。

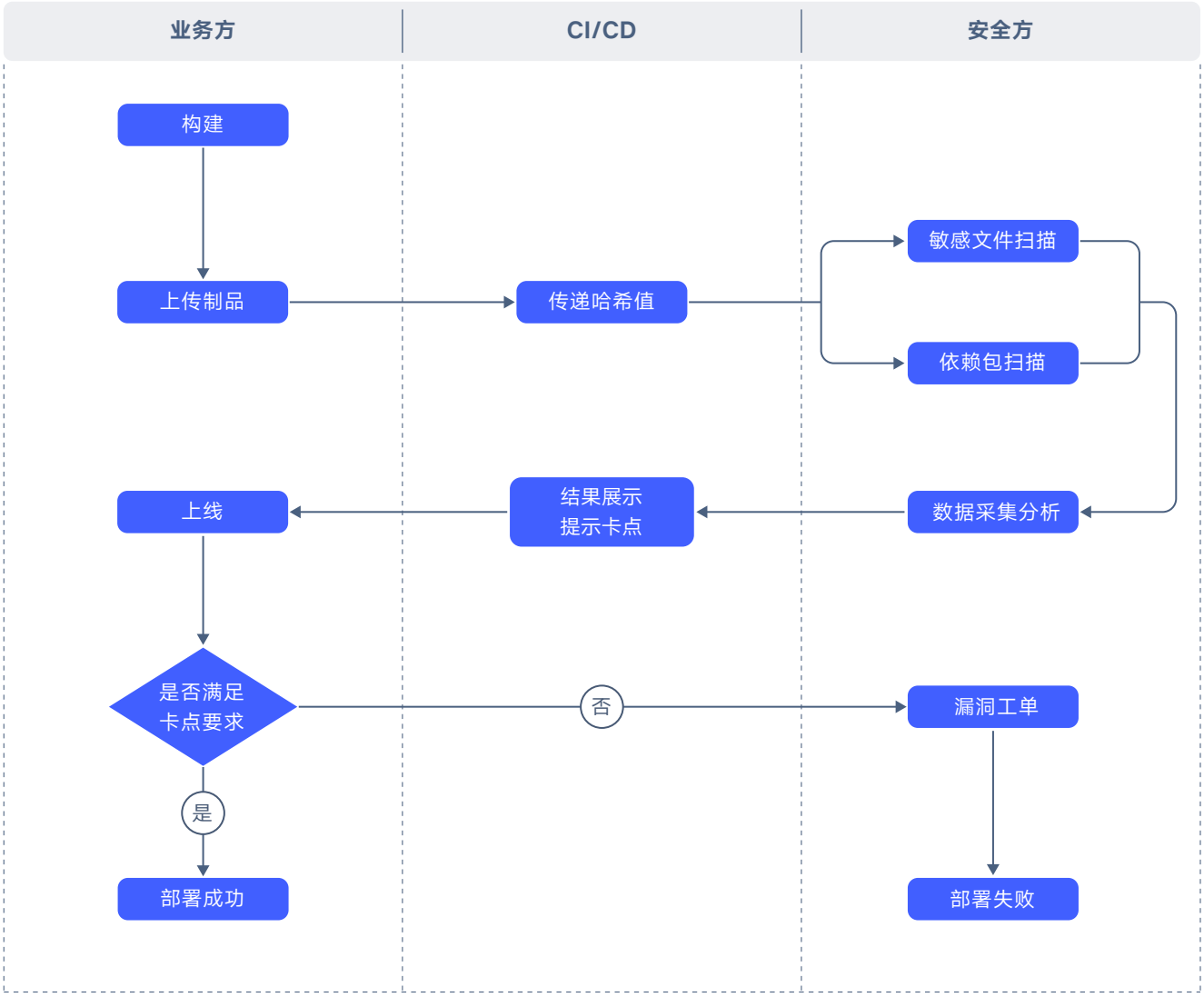


图7：CI上线扫描和敏感文件扫描流程

考虑到上述风险，vivo在CI/CD安全扫描上建设敏感文件扫描能力，在特定的扫描机器上执行扫描脚本，使用本地服务获取远程DevSecOps平台中配置的规则，再对构建好的制品包解压后进行匹配扫描。扫描完成后会将结果上传到DevSecOps平台中，最后由DevSecOps平台同步结果至CI/CD的安全扫描界面。

5. 镜像安全扫描

随着业务容器化进程加速，容器资产成为重要的基础设施。为保障业务在容器环境下安全运行，vivo开展容器安全相关能力建设。首先，限制线上容器对第三方源镜像的使用。如果业务方必须使用第三方源镜像，需要将镜像下载后上传至互联网容器仓库中，业务部署仅使用来自互联网仓库的容器镜像。其次，建设镜像扫描能力。对仓库的存量镜像开展周期性安全扫描检测，发现容器操作系统层面的风险，并根据风险情况，对镜像赋予不同等级的标签。最后，建设容器CD部署前扫描能力，对新构建的容器镜像提供系统漏洞扫描并告警。

6. 安全与隐私自检

在编码工作基本结束后，产品开发人员将进行人工代码走读，并对项目代码按照《安全隐私点检表》进行自检，点检项从数据安全、组件安全、权限管理、服务器和端口管理、隐私保护技术等11个方面对代码设计和编写给出检查要求，自检完成后将由各项目安全工程师和品质工程师验收，确保代码质量符合安全与隐私保护要求。

3.4 测试阶段

在测试验收阶段，vivo对于自研业务均配备了安全合规测试团队和安全合规检测工具。工具检测可覆盖公司安全与合规基础测试用例，而在方案设计阶段识别出的安全及合规风险形成的定制测试用例，则会由人工进行测试。通过工具扫描和人工检查，可对安全及合规问题早发现早处理，不让其有机会流入市场。

1. 应用安全检测平台

vivo自研应用主要使用应用安全检测平台进行业务自检和安全验收，该工具基于权限、组件、SDK、加固、签名、二进制、敏感行为等风险视角，从应用代码、配置、组件、数据、加密、通信等多个维度，进行自动化安全检测。

平台不仅支持通用编码安全问题检测，还支持特殊地区安全要求相关问题的检测（如特殊安全标准、特殊认证等）。目前平台已对公司内重点应用进行持续的安全检测，最大程度提前发现安全问题，保障产品的质量。后续会输出能力至vivo生态，促进生态的蓬勃发展。

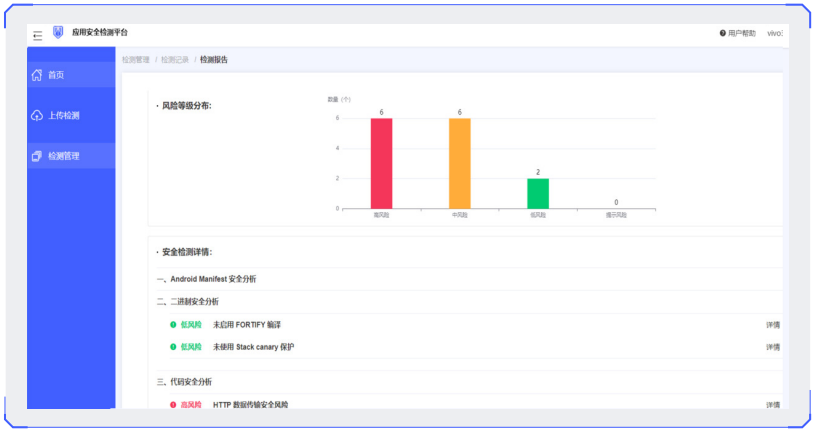


图8：应用安全检测平台

2. 隐私与合规检测平台

隐私与合规检测平台是一款检测移动应用隐私与和合规风险的SaaS平台。依据监管机构的法律法规，平台基于专家解读的规则，结合动态检测、静态分析、AI检测等技术，可自动、高效、准确地检测移动应用中存在的隐私与合规风险。目前该平台已通过vivo开发者社区发布，帮助开发者自检自纠，降低应用合规风险。

3. 自动化漏洞扫描平台

vivo自动化漏洞扫描平台通过自动化扫描的方式，能够发现三方组件安全风险、端口开放风险、Web安全漏洞风险等风险类型。该平台同时支持对线上环境和资产的周期性安全扫描监控。在DevSecOps流程中充当动态应用程序安全测试（Dynamic Application Security Testing，DAST）角色，结合交互式应用安全测试（Interactive Application Security Testing，IAST）、静态应用安全扫描（Static Application Security Testing，SAST）等产品，实现从多角度对业务系统的安全风险识别。

图9：自动化漏洞扫描平台

4. 交互式应用安全测试

交互式应用安全测试(IAST)，是一种对应用和API进行自动化识别和诊断软件漏洞的技术。IAST不仅是一个扫描器，它能够持续地从内部监控应用中的漏洞。在整个开发生命周期中，IAST可以通过在开发阶段和测试阶段使用的工具，实时地提供告警，vivo通过利用IAST agent监控应用程序运行时的函数执行情况，采集相关数据，与服务端进行实时交互，从而高效、准确地识别出应用程序中的漏洞。同时，IAST agent可准确定位到漏洞所在的文件、行数、方法及参数，方便开发团队及时修复漏洞。

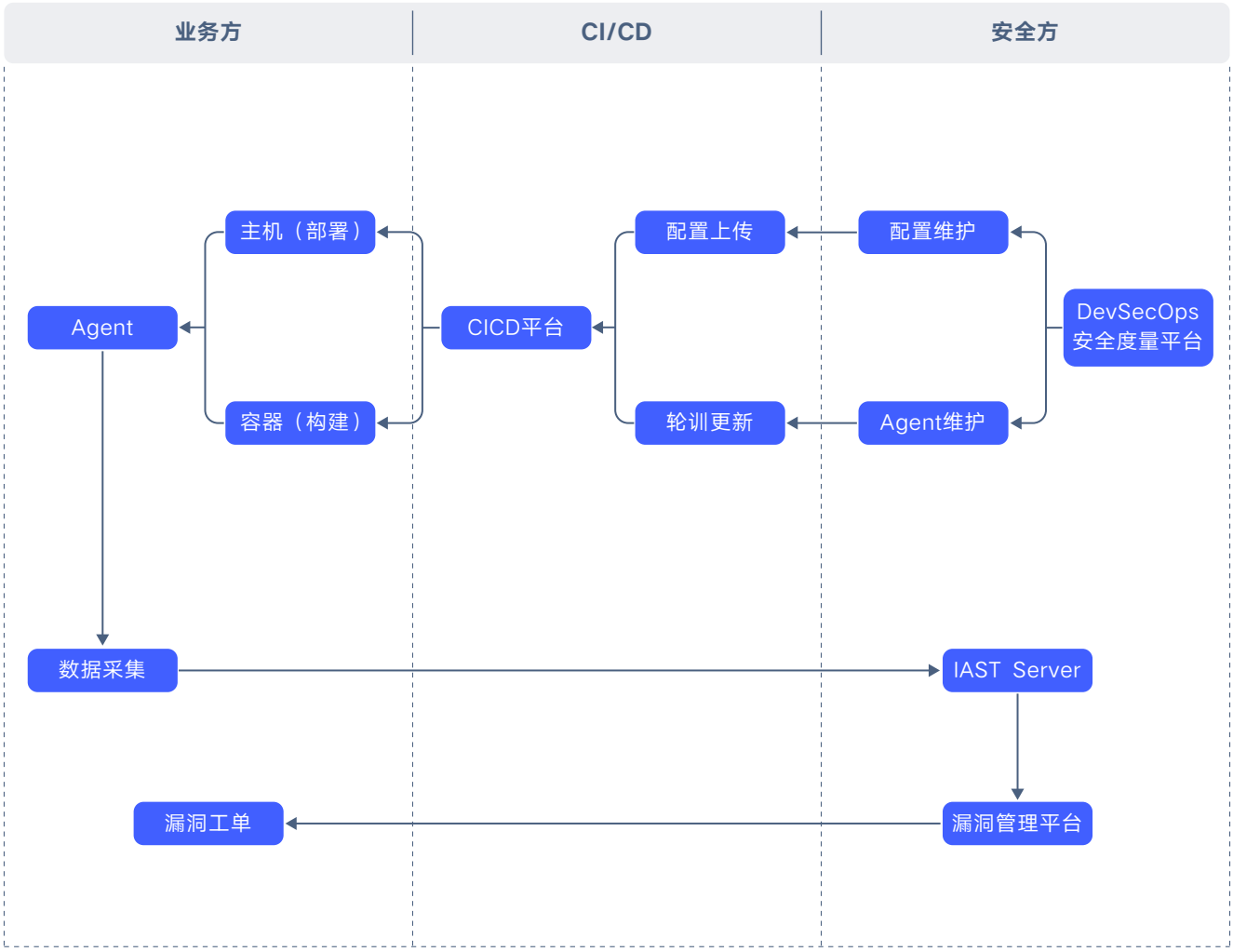


图10：vivo IAST流程

5. 周期性人工渗透测试

当vivo产品和服务的大版本迭代时，进入测试阶段后，vivo千镜安全实验室攻防团队将开展专项渗透测试，识别产品中的安全与隐私保护风险。同时，攻防团队会每月对产品进行稽核，人工挖掘零日或长攻击链的安全漏洞，进一步缩小产品攻击面和风险。

3.5 发布阶段

发布阶段作为vivo产品上市前的最后一环，安全检查的重要性不言而喻。vivo自研软件在发布前，首先需通过模块安全合规测试。合格后，软件才会跟随ROM版本集成在终端设备上。之后，软件还会在整机维度上经过多轮安全及合规检查，检查均合格后才会对外发布上市。

互联网业务的敏捷性导致业务不能遵照传统的安全管控方式进行发布，即要求业务完成安全标准评估后才能进行下一步动作。因而，vivo配合互联网业务研发生命周期流程，建立了自动化管控能力，自动化识别扫描结果是否符合安全与合规的上线要求，提高整体工作效率。

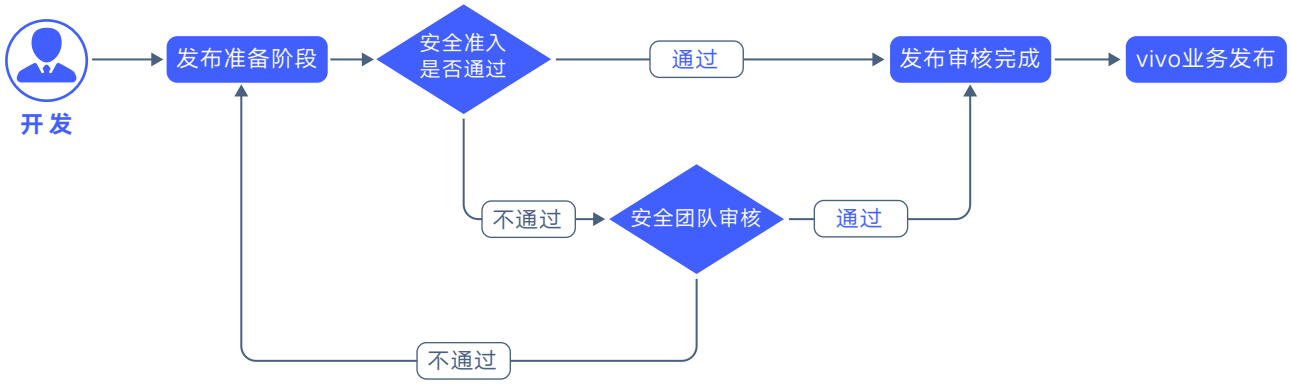


图11：端侧软件和互联网业务发布阶段流程

最后，移动端软件和互联网业务发布前由品质代表组织相关负责人输出专项合格结论，测试代表输出安全与合规测试结论，只有均通过审批的版本才能发布。

3.6 运维阶段

vivo针对自研产品上市后的安全与隐私持续运维，建立了内部组织：vivo安全事件响应团队（vivo Security Incident Response Team，vSIRT），vivo安全响应中心（vivo Security Response Center，vivoSRC）及数据主体权利（Data Subject Right，DSR）需求处理团队，及时对严重安全与隐私保护漏洞响应并修复和对用户的数据主体权利需求进行响应，与外部研究者和用户合作，共同建设更安全的vivo产品。

1. vSIRT

vivo安全事件响应团队从组织架构、流程、工具等方面来协同配合，通过对外部事件进行定级、分析溯源、协调处理、复盘追责、迭代流程等多个方面，实现控制风险和快速处理外部安全事件。

图12：vSIRT安全事件处理流程

同时，vivo也鼓励漏洞研究人员、行业组织、政府机构或供应商主动将与vivo产品相关的安全漏洞报告给vivo，即将漏洞文档发送邮件至security@vivo.com。同时，作为CVE编号颁发机构（CNA），vivo可以为vivo产品漏洞分配CVE编号。

2. vivoSRC

vivo致力于维护互联网健康安全生态环境，促进与业界个人、组织及公司密切合作与交流，建立安全、隐私保护合规问题收集的应急响应平台vivoSRC。

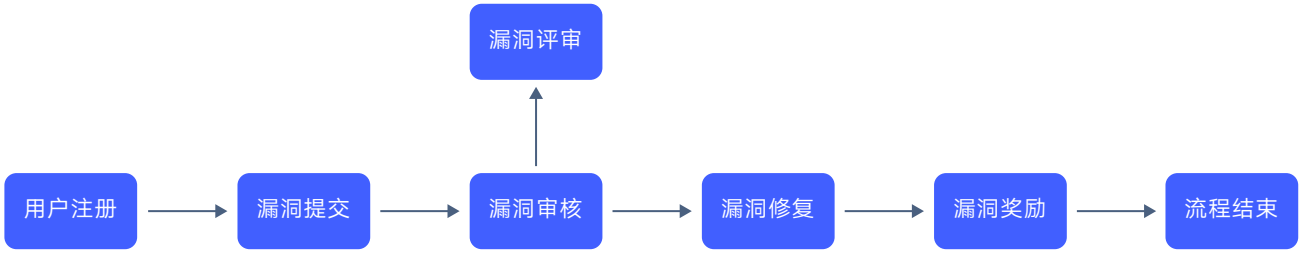


图13：vivoSRC漏洞提交流程

3. DSR需求处理

vivo十分重视保障用户数据主体权利，用户可以通过拨打vivo的客服电话、登录vivo官网通过在线客服、发送电子邮件或登陆隐私中心发起请求的方式与vivo联系，vivo将在验证您的主体身份后，在规定时间内作出合理的解释与答复。为保障高效处理用户的问题并及时反馈，部分情况下vivo可能会要求用户提交身份证明、有效联系方式和书面请求及相关证据，vivo会在验证您的身份后处理您的请求。

04

数据生命周期安全合规保障

4 数据生命周期安全合规保障

vivo始终将守护用户数据安全与隐私保护放在首位，vivo内部规范《vivo用户数据分类分级规范》指导vivo产品与服务对用户数据进行分类分级管理。该规范将用户数据分为14大类，并针对不同安全等级的用户数据确立对应的安全策略和控制措施要求。与规范相匹配的，vivo定制了各阶段保证数据安全的组件能力，共同守护用户数据安全。

图14：数据全生命周期及安全保障技术工具

4.1 数据采集

数据的采集是数据生命周期的第一步，通常发生在用户的端侧。在数据采集阶段，最重要的两件事是：1.定义哪些数据可以采集；2. 如何与用户沟通采集数据。

1. 数据分类分级

以《vivo用户数据分类分级规范》为指引，vivo对用户数据实施分类分级治理：对主要业务进行用户敏感资产梳理，将数据分成14大类，68小类，300+明细类别，并采用“数据新增时人工分类分级、落库后人机协同纠偏”的方式对全量的在线业务数据及大数据进行分类分级，以及通过数据安全专家定期抽检审核分类分级结果，不达标进入优化流程、达标后进入常态化运营管理，以确保数据分类分级的结果不断进步，为用户敏感数据在后续环节得到有效的管控和保障提供基础。

2. 收集个人信息的合规保障流程

① 评估收集的合法性及收集目的：个人信息收集目的必须特定、明确且合法，不得进行超过数据收集目的以外的处理；

② 评估数据收集是否最小化：个人信息数据收集应满足最小化原则，即仅收集和处理与实现特定目的相关的、最小数量的个人信息，且仅向第三方披露或共享合理、必要且最小数量的个人信息；

③ 对当事人进行告知；通过隐私政策解释收集个人信息的类型、目的和处理过程；

④ 授权同意：基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出；而法律、行政法规规定处理个人信息不需取得个人单独同意或者书面同意的，应遵从其规定；

⑤ 告知与同意的记录：无论使用何种形式进行告知并取得当事人同意，vivo相关业务团队均应保存告知与同意的相关记录。

3. 差分隐私

差分隐私是借助统计学工具对数据引入无偏噪声以保护个体隐私的隐私保护机制。其可以在进行数据查询或本地数据发布时，保护个体隐私且尽可能保证数据可用性或整体统计学特征。基于差分隐私技术，vivo能够在保护个人隐私的同时，通过人工智能能力，在设备可靠性、性能、功耗等方面进行持续改进和优化，为用户提供更好的使用体验。

4.2 数据传输

当数据在端侧采集完成后，很多场景下需要将部分数据发送回服务器端进行存储与分析。其中最重要的基础能力是：数据加密传输的密钥生成和管理系统和数据加密传输所使用的协议。

1. 密钥生成和管理系统（Key Management System，KMS）

数据的传输场景中，最关键的操作是对于数据的加解密。加解密过程中用来完成加密、解密、完整性验证的关键信息被称为“密钥”。密钥就如开锁的钥匙，需要进行安全生成和管理。

KMS密钥管理系统底层使用的是金融级数据硬件加密机(Hardware Security Module，HSM)。HSM是一类具有物理安全保护措施的硬件设备，其以现代密码技术为核心，使用专业密码芯片生成和存储密钥。KMS密钥管理系统的产品特点如下：扩展SM1、SM2、SM3、SM4国产密码算法，支持三层密钥体系，提供完善的密钥管理功能，提供硬件冗余设计，用专业安全芯片硬件实现高质量真随机数、多种密码算法。

在端侧，通过安卓底层密钥生成和管理模块，包括vivo提供的加解密SDK，能够提供对于本地密钥的有效管控。

KMS密钥管理系统作为vivo数据加密体系的底层核心，支撑了数据传输加密、数据存储加密、文件加密、证书管理等多个场景的密钥托管，并且提供安全高效的密钥接口，有效地避免密钥泄漏的风险。

2. 数据传输加密

为保障数据在传输中的机密性和完整性，在手机端到服务端传输场景中，vivo基于可信执行环境（Trusted Execution Environment，TEE）建设了一套硬件级别的安全传输方案。结合HTTPS协议，可实现传输通道和内容的双重加密、身份认证、防止传输线路上的窃听、泄漏、篡改等攻击行为。同时，在WEB端，vivo参考行业最佳实践，实现了基于密码学的加密传输方案，解决HTML5、小程序、快应用等场景中数据加密传输的问题。

目前数据加密传输能力已经在vivo钱包、vivo浏览器、游戏中心等核心业务落地，为用户数据安全传输建立起一道强有力的安全屏障。

4.3 数据存储

当数据流转至服务端，并进入数据库存储时，vivo使用数据加密系统对敏感数据，如手机号、身份信息等，进行加密存储。vivo数据加密系统使用KMS密钥管理系统对密钥进行管理，并使用国家密钥局认证的硬件加密机和符合国家和行业标准的多种数据加密算法。数据加密系统通过对用户敏感数据进行可靠的加密运算和密文存储，极大地减少用户敏感数据泄露、恶意破坏的风险。而且通过信封加密、三级密钥机制、上下文加密等技术，有效地保障了加密数据的机密性、完整性。

目前vivo数据加密系统已在MySQL、MongoDB、ElasticSearch等各类数据库及大数据场景中落地，充分保障了用户数据的存储安全。

4.4 数据交换

为了保证数据交换场景中数据的可审计可追溯，vivo建立了覆盖自有产品的操作审计体系，可实现：

① 可评估：vivo每个数据交换场景均需经过安全与隐私保护团队的数据保护影响评估，消减所有存量风险后方可进行数据交换，vivo会定期对供应商的隐私保护的措施和实践进行评估；

② 可管控：为了保证重要数据操作的有效管理，如批量的导入导出、修改、拷贝、下载等，每次操作前需获得相应数据管理部门的审批通过后方可执行；

③ 可追溯：相关操作的人员、操作行为、时间、数据范围等均记入日志系统，以备后续追溯。为了方便数据追溯，vivo通过数据水印技术，将水印标记注入携带数据的EXCEL、PDF等类型的电子文档和各类图片文件中。文件外发后，可通过水印提取技术，提取隐藏在文件中肉眼不可见的水印内容，进行数据溯源，降低由于内部人员文件外发导致的数据泄露风险。

4.5 数据处理

当数据被处理时，即数据被使用产生价值时，最为关注两个问题：1. 数据是否可以追溯到某个特定的用户；2. 数据是否可以在端侧进行处理，无需将数据上传。

1. 数据脱敏

在数据处理的各类场景，如数据查询、展示、分析等场景，为了满足数据隐私保护方面的合规要求并保障数据的机密性、防止数据泄露，vivo针对用户敏感数据，采用哈希、屏蔽、变形、伪码、掩码、格式保留加密、强加密算法等多种脱敏算法对用户数据进行处理，使得用户敏感数据在使用过程中，去除敏感信息，有效防止敏感数据被滥用和泄露，极大地实现了敏感数据的安全保护。

2. 联合学习

为满足vivo隐私保护三原则中端侧处理的要求，借助联合学习技术，vivo业务无需用户上传原始数据，而是通过服务器下发的基础模型在用户终端进行训练，完善学习模型。用户数据保留在设备本地，仅将训练后的模型更新匿名化后上报到服务器，避免泄露用户隐私。同时，云端汇集大量用户终端设备的模型更新数据，并不断完善，提升AI模型能力。

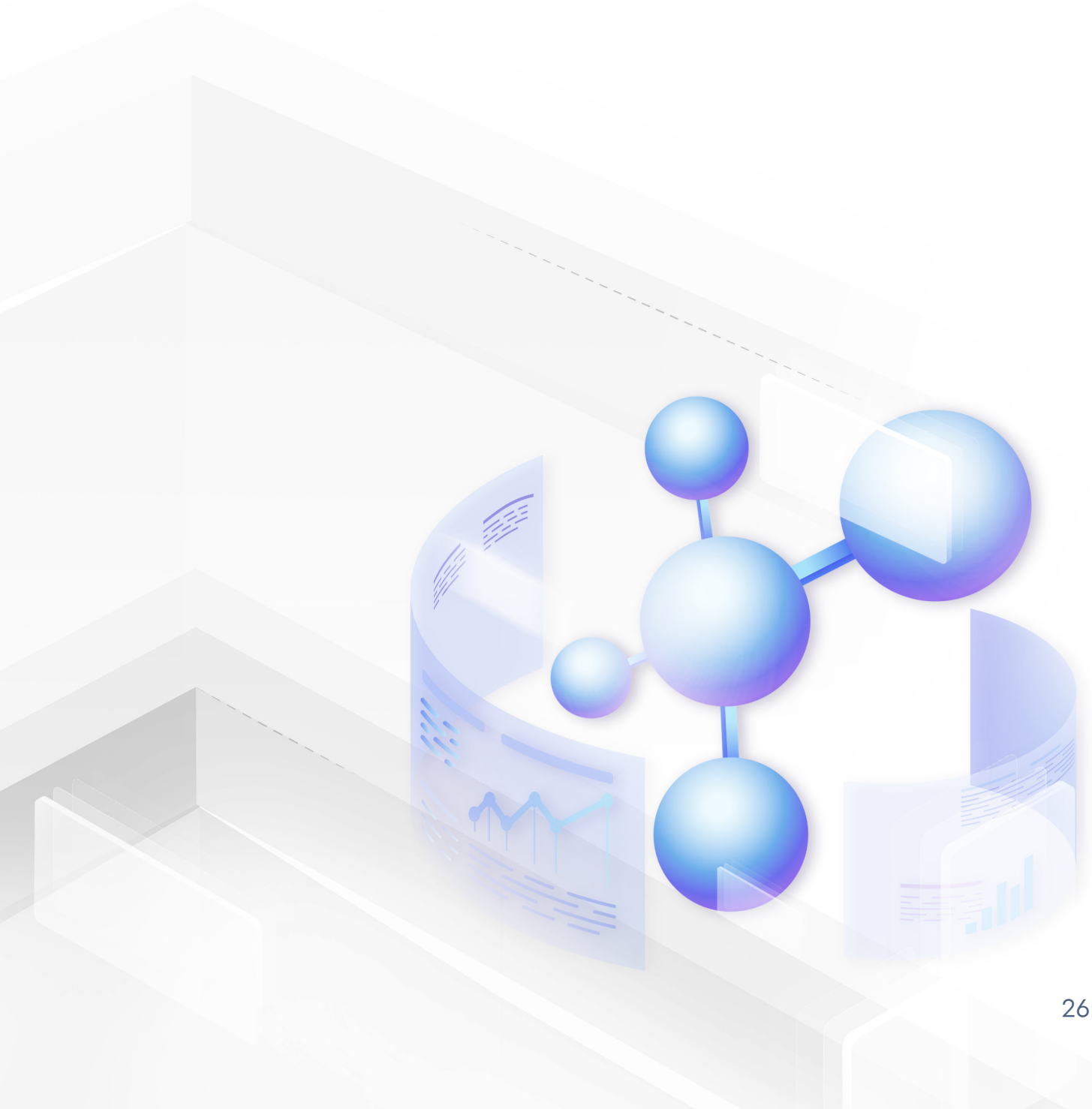
4.6 数据销毁

各场景下的数据销毁依据《vivo用户数据分类分级标准》执行，对于每种数据采集制定相应的销毁策略并由需求发起人监督执行，并由对接项目的安全及合规专家定期检查。

为了满足业务数据存储最短必要期限的要求，当数据不再必要、超出与用户约定的存储期限或用户请求删除时，vivo采用逻辑销毁或物理销毁的方式对数据进行删除。对于数据存储介质进行报废处理时，vivo采用物理销毁的方式对数据存储介质进行销毁，确保数据不能被恢复。其中，当用户请求删除数据时，vivo通过DSR流程进行处置和闭环销毁。

05

业界生态建设



5 业界生态建设

网络安全体系需社会多方共建。除了加强自身内部安全体系，vivo秉持开放式创新态度，积极探索安全生态建设，与行业伙伴共同推动安全产业发展，携手共创更安全的用户产品体验。

5.1 安全生态联盟

2020年，为构建更加坚实、健康、高效的软硬件技术环境，vivo作为创始成员单位，联合百度、腾讯等等生态软硬件企业，联合发起成立移动智能终端生态联盟（Intelligent Terminal Alliance，简称“金标联盟”）。该联盟旨在通过强化移动互联网生态内各大企业间的密切联系与沟通，形成统一的行业标准，维护开放生态，对行业赋能，共同提升用户体验效果以及安全能力。在金标联盟中，vivo作为安全标准组代表，负责该联盟隐私保护和安全相关的工作，和联盟成员一起推动联盟生态建设，共同打造一个开放、共享、合作、共建的安全生态链。

5.2 安全行业交流

vivo通过自办峰会或参与安全领域各类学术及产业会议，开放共享技术研究成果及最新安全实践，不断促进行业内安全与隐私保护相关工作的交流与合作。

vivo每年定期举办vivo开发者大会（VDC），积极与开发者共享前沿技术，期望为业界带来更优秀的创新成果。2021年，vivo开发者大会设立安全专场，并在会上明确了vivo公司隐私保护三原则，推出了增强安卓生态安全与隐私保护能力的千镜安全架构，公布了PROTECT安全技术战略，并且面向全球发布了《OriginOS安全白皮书》。同时，vivo率先提出了“安全守护也应该更人文更有温度”的人文安全理念。

2022年4月，vivo作为博鳌亚洲论坛战略合作伙伴出席开幕式，同各国政要、学术领袖、企业代表们一起见证盛会的召开，并分享科技领域的最新观点。在“数字经济：向阳而生”分论坛上，vivo首席安全官与参会伙伴共同探讨数字经济与数字安全的问题，并发布由vivo和中国信息通信研究院联合编撰的《数据保护合规趋势白皮书》，分享vivo在数据保护与合规上的思考与实践。

5.3 安全标准制定

vivo积极参加国内外安全与隐私保护标准化工作，致力于在安全能力保障和隐私保护方面，与行业达成共识，分享自身优秀标准化实践，共同为个人隐私信息保护与终端安全贡献一份力量。

vivo积极参加全国信息安全标准化技术委员会、中国通信标准化协会和电信终端产业协会等标准组织，在其中参与个人信息保护、AI应用安全、基础安全技术、软件及系统安全、数据安全、应用商店生态管理、通信互联安全、供应链安全、反电信网络诈骗等众多专题领域的标准讨论会议，与众多专家讨论并提出建设性意见，持续研究并探索如何使标准价值最大化。截止2022年7月，vivo累计主导或参与制定近130项标准，部分标准如下：

1. 国家标准

GB/T 41388-2022 《信息安全技术 可信执行环境 基本安全规范》

GB/T 39720—2020 《信息安全技术 移动智能终端安全技术要求及测试评价方法》

2. 行业标准

YD/T 4177.11-2022 《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第11部分：短信信息》

YD/T 2407-2021 《移动智能终端安全能力技术要求》

YD/T 2408-2021 《移动智能终端安全能力测试方法》

3. 团体标准

T/TAF 050-2019 《移动智能终端及应用软件用户个人信息保护实施指南 第2部分：个人信息分类分级》

T/TAF 077.9-2022 《APP收集使用个人信息最小必要评估规范 第9部分：短信信息》

T/TAF 014-2020 《移动智能终端应用软件分类与可卸载实施指南》

T/TAF 109-2022 《移动应用分发平台 APP开发者信用评价体系》

T/TAF 104-2021 《移动应用程序（APP）下载安装升级测评规范》

5.4 开放平台生态建设

vivo开放平台致力于为广大用户营造更加安全、健康、和谐的APP生态环境，同时也积极响应相关部门对APP隐私安全的要求，在2022年上半年，累计发起90次合规检查、排查应用超9万余次、通知整改应用超1.3万余次、处理应用下架超9000余款。为进一步加强用户个人信息保护，切实履行企业主体责任，vivo开放平台开展APP隐私合规问题专项整治行动：

- **存量APP巡检**

平台将不定期开展大规模的存量APP巡检行动，重点针对用户隐私信息保护问题开展复查复测，对违规应用采取通知整改、下架、冻结账号等处罚措施。

- **提倡开发者主动排查、整改旗下应用**

平台提供《APP常见隐私问题合规指引》供开发者参考重点排查。

- **开发者保持联络通道畅通**

开发者需及时更新在vivo开放平台的联系信息，确保可以及时接收到平台的通知，并积极协助平台对APP进行整改。

vivo应用商店联动开发者共建和谐健康的网络生态环境，通过合规解读、审核标准升版、自动化检测能力升级、APP巡检排查、合规宣导、协助开发者整改、APP违规处罚、用户反馈等进行APP全链路管理。采取以下有效保障措施：

- **建立长效的开发者账号实名注册和信用体系**

严格审查开发者资料信息，确保开发者信息真实性；针对账号违规行为，制定了详细的《vivo开放平台账号处罚规则》。

- **构建严谨的入库审测流程，保证入库合规**

vivo应用商店拥有一套完善和严格的入库审测流程，每个APP需经过病毒和风险代码扫描、自动化测试、人工深度测试、人工资质和信息审核共四道审测程序，方能上架。

- **建立完善的上下架管控标准，保证问题产品的高效识别和违规处罚**

vivo应用商店在APP上架、巡检下架处罚全路径都制定了详细的规则规范，包括：《APP审核规范》、《APP巡检处理流程及规则》、《嫌疑风险APP识别规则》、《特殊行业类资质要求》、《账号处罚规则》、《APP违规处罚规则》等，从而实现对问题APP的高效识别和违规处罚。

- **针对应用上架后的篡改和违规行为，采用全库和精准打击的巡检机制**

针对上架应用通过云控开关或者APP内部推送更新版本的方式进行篡改和违规的行为，vivo应用商店启动了全库和精准打击高危类型的巡检清理专项。

- **自动化检测能力强化，持续提升攻守效率**

自主打造了兼容性测试实验室，含遍历测试、安全漏洞、恶意行为、隐私检测、木马病毒等5大自动化检测能力，覆盖vivo最热最新的机型，24小时不间断提供测试服务，保障开发者的产品在真实环境下，快速进行测试。

- **推动开发者自我排查整改，助力行业隐私合规建设**

vivo应用商店将常见的侵害用户权益的问题、识别方法、整改方法等梳理成合规指引文档，成为行业内首个推出《APP常见隐私问题合规指引文档》的手机厂商平台，有效地帮助了开发者在开发、运营过程中更好地解读规则和优化APP。同时，vivo应用商店号召广大开发者对旗下APP开展排查和整改，助力行业整体隐私合规建设。

- **联动开发者、用户共推合规建设**

持续投入巡检排查，帮助开发者进行应用隐私问题的整改和合规上架。健全APP投诉举报路径和处理机制。提升用户安全心智，不定期发布应用商店安全报告。

- **针对应用开发过程中常见的安全与隐私保护问题**

vivo发布代码安全扫描插件，应用安全检测平台，隐私与合规检测平台，帮助开发者在应用代码开发阶段发现安全、隐私和合规问题，提早引入解决方案，降低解决问题成本。

5.5 监管合作

vivo公司作为一家以手机终端产品为主的高科技公司，兼具着移动智能终端生产企业、APP开发运营者、APP分发平台、APP第三方服务提供者四重身份，在数据安全与隐私保护管理工作中责任重大。vivo公司深知这份责任的重要性，一直以来都在利用自身的技术能力优势，参与监管体系建设工作，积极配合工信部和网信办等部委的数据安全与隐私保护工作，包括与工信部合作共建全国 APP 技术检测平台、全国 SDK 管理服务平台、工信反诈大平台，参与工信部164/165号文 APP/互联网整治行动等。同时，vivo公司作为头部手机终端厂商，始终站在提升用户体验、完善行业生态的角度，参与到多项工信部与网信办发布的数据安全合规和个人隐私保护的管理规定的制定项目中，包括：《移动互联网应用程序个人信息保护管理暂行规定》、《关于开展信息通信服务感知提升行动的通知》、《移动互联网应用程序信息服务管理规定(征求意见稿)》、《互联网信息服务算法推荐管理规定(征求意见稿)》等。

5.6 安全技术研究

vivo先后同国内顶尖高校在安全技术研究、安全竞赛等方面开展合作，充分发挥自身与用户直接沟通，以及安全攻防的优势，与科研界合作攻关网络安全技术领域重大前沿课题，并为业界高等网络安全人才的培养贡献力量。

06

用户透明沟通

6 用户透明沟通

6.1 vivo隐私中心

vivo隐私中心是vivo基于“透明可控”原则建立的安全隐私门户网站，其目标主要用于展示vivo安全与隐私保护技术能力，并提供用户对于其数据处理的通道。

基于“透明”原则，vivo隐私中心从隐私保护原则、安全隐私功能、数据安全技术、安全认证等多维度方面出发，立体化展现了vivo专业可信的安全与隐私保护能力，建设安全品牌心智，并公开透明呈现了vivo数据处理的原则与目的，传递隐私保护理念。

基于“可控”原则，vivo隐私中心组建出集成多数据类型、多数据控制方式、多端的用户数据处理中心。用户可以便捷地控制和管理自身数据，并且给予用户自动化处理数据主体权利，满足监管合规要求。

vivo隐私中心覆盖海内外多个国家和地区，通过隐私中心，用户可全面洞悉vivo的安全与隐私保护理念、成果及实践，形成具有vivo特色的“透明可控”用户沟通窗口。

图15：vivo隐私中心门户网站

6.2 vivo安全与隐私保护白皮书

为展示vivo端侧安全技术能力，和对于用户数据及隐私保护合规的实践和经验，vivo在2021年VDC发布了《OriginOS安全白皮书》，并于次年博鳌亚洲论坛发布了《数据保护合规趋势白皮书》。2022年发布的《vivo可持续发展报告》中也提出，信息安全与用户隐私保护是vivo企业可持续发展中最重要的课题。

《OriginOS安全白皮书》从底层的芯片硬件层、中间层的系统内核、以及到上层的应用，尽可能详尽地向用户展示vivo端侧所使用的安全技术和能力，从端侧安全能力出发，由浅入深地向用户介绍各安全能力背后所使用的技术，并分析技术的优势。

《数据保护合规趋势白皮书》通过总结全球各区域和国家近两年数据保护立法和执法情况，发现其中的合规风险点，并提出相应应对措施。该白皮书中的案例为vivo业务方的数据安全和隐私合规工作提供借鉴，帮助业务方更好地选择方案，保障用户的数据安全和隐私。

6.3 vivo安全与隐私保护认证

作为一家以用户为导向的公司，vivo持续洞察消费者需求，始终将消费者安全与隐私保护放在首位，自成立以来坚持以国际最权威的安全合规标准要求自己，目前已获得多项国际和国内权威认证。

1. 移动智能终端安全能力5级证书

泰尔实验室“移动智能终端安全能力分级测试”从硬件安全、操作系统安全、应用层安全、外围接口安全和用户数据保护5个层面共84项对移动智能终端的安全能力提出了要求，vivo X Fold和X Note两款手机通过并获得了最高等级5级。

五级

2. 移动智能终端操作系统个人信息保护能力5星证书

“移动智能终端操作系统个人信息保护能力”证书是国内首个针对移动智能终端操作系统个人信息保护能力的权威证书。OriginOS获得了中国泰尔实验室首张移动智能终端操作系统个人信息保护能力五星产品的证书。

3. 欧洲隐私保护认证ePrivacySeal

由欧洲隐私认证权威机构 ePrivacy 颁发，涵盖了数字产品的《通用数据保护条例》（General Data Protection Regulation，GDPR）的要求，从法律和技术两个维度对认证对象进行评估，确保覆盖 GDPR法律要求。“i 管家”与“vivo 相册”欧洲版本通过审查并取得认证。

4. TRUSTe企业隐私保护认证

基于各国公认的法律和法规标准，由国际权威隐私合规评估机构TrustArc颁布。通过认证表明企业满足国际级隐私保护的认证标准，相关技术和管理能力获得美国隐私认证权威机构TrustArc的认可。

5. ISO/IEC27001信息安全认证

ISO/IEC27001 由国际标准化组织和国际电工委员会联合发布的信息安全管理体系（ISMS）标准，通过认证表明企业已经建立并有效运行信息安全管理体系，满足内外部信息安全管控要求。

6. ISO/IEC27701隐私信息管理体系认证

ISO/IEC27701 由国际标准化组织和国际电工委员会联合发布，为建立、实施、维护和持续改进隐私信息管理系统提供具体要求和指南。通过认证表明企业隐私信息管理体系和隐私保护能力满足国际标准。

7. 网络安全等级保护三级

vivo互联网服务遵循网络安全等保保护要求，已经通过网络安全等级保护三级。

7 总结

vivo深刻认识到，安全与隐私保护对用户至关重要，同时其又是一个集管理、技术、流程和生态等多方面于一体的系统化工程，需要不断地努力，长期的、潜移默化的将安全与隐私保护的心智融入到产品的生命周期和用户数据生命周期的不同阶段。为此，vivo把安全与隐私保护提升到公司可持续发展的最高位置，保障对安全与隐私保护赛道的坚定投入，坚持长期主义，让用户安全便捷地享受手机等终端带来的数字化生活。

vivo也认识到，没有任何一家公司可以独自解决所有安全与隐私保护问题、满足用户所有的安全与隐私保护需求。因此，vivo积极与上下游伙伴、监管部门、标准组织等携手，加强自律和律他，加速最新安全与隐私保护方案的落地，构建安全隐私新生态。同时通过隐私中心等通道，积极与用户透明沟通，增强用户数据安全与隐私保护感知。

vivo希望通过在数据安全与隐私保护上的不懈努力，让用户放心、安心，成为用户首选的可信赖的终端品牌。

8 术语表

术语	英文全称	中文全称
AI	Artificial Intelligence	人工智能
API	Application Programming Interface	应用程序接口
APP	Application	应用程序
CD	Continuous Delivery	持续交付
CEO	Chief Executive Officer	首席执行官
CI	Continuous Integration	持续集成
CSO	Chief Security Officer	首席安全官
CNA	CVE Numbering Authority	CVE编号机构
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
DAST	Dynamic Application Security Testing	动态应用程序安全测试
DevSecOps	Development, Security, and Operations	开发、安全和运营
DPO	Data Protection Officer	数据保护官
DSR	Data Subject Right	数据主体权利
FAQ	Frequently Asked Questions	常见问题集
GDPR	General Data Protection Regulation	数据通用保护条例
HSM	Hardware Security Module	硬件安全模块
HTML	HyperText Markup Language	超文本标记语言
HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
IAST	Interactive Application Security Testing	交互式应用安全测试
IEC	International Electrotechnical Commission	国际电工委员会
IPD	Integrated Product Development	集成产品开发

术语	英文全称	中文全称
ISMS	Information Security Management System	信息安全管理体系
ISO	International Organization for Standardization	国际标准化组织
KMS	Key Management System	密钥生成和管理系统
OriginOS	OriginOS	vivo OriginOS系统
PbD	Privacy by Design	隐私设计原则
ROM	Read-only memory	只读存储器
SaaS	Software as a Service	软件即服务
SAST	Static Application Security Testing	静态应用安全扫描
SCA	Software Composition Analysis	软件成分分析
SDK	Software Development Kit	软件开发工具包
TEE	Trusted Execution Environment	可信执行环境
VDC	vivo Developers Conference	vivo开发者大会
vivoSRC	vivo Security Response Center	vivo安全响应中心
vSIRT	vivo Security Incident Response Team	vivo安全事件响应团队