VEILORA 安全终端使用指南

目录

0. 前言 4

0.1 关于本手册 4

0.2 安全与合规声明 4

1. 快速入门 6

1.1 认识您的手机 6

1.2 首次开机引导 7

1.3 系统账号管理 10

1.4 快捷安装应用 13

2.如何创建与设置隐私空间 15

2.1 全系统多层级隔离加密存储 15

2.2 初始化隐私空间 15

2.3 设置“双 PIN 码”实现空间切换 16

2.4 跨空间文件同步指南（主空间 ➔ 隐私空间） 18

3.如何防止被外界网络画像 20

3.1 防追踪画像、主动网络攻击防护 20

3.2 智能流量异常管控 20

4.如何防止 APP 窃取隐私 22

4.1 应用权限管控与风险审计 22

4.2 一键超级隐私防护模式 23

5.如何防止在即时通信中被第三方留存导致泄密 24

5.1 开启密写转换工具 24

5.2 如何进行加密消息通讯 26

5.3 如何发送加密文件 28

5.4 如何查看与浏览加密文件 33

5.5 如何进行加密语音通讯 34

6.如何使用私有云进行加密备份与恢复 36

6.1 WebDAV 云空间配置 36
6.2 设置自动/手动备份计划 38
6.3 本地数据恢复流程 40
7.如何强化系统安全 43
8.如何进行应急还原 46
8.1 如何还原整个手机 46
8.2 如何还原隐私空间 47
8.3 如何远程锁定与还原 51

0. 前言

感谢您选择 VEILORA（隐御）安全手机。在数字化高度发展的今天，数据泄漏、网络监听与隐私追踪等数字威胁无处不在。VEILORA 并非一台普通的智能终端，而是一座为您精心打造的“移动数字堡垒”。

VEILORA 是一款专注于数字终端隐私保护与数字安全防护的专业操作系统，其服务对象为军队、警察、政府要员及高价值商务人士、科学家等需要极高数字安全防护的人士。产品依托自研具身安全内核，整合网络安全、隐私管控、加密通信、隔离存储、应急防护、数据防提取、安全云备份、智能防御八大核心能力，构建覆盖数据采集、传输、存储、使用全生命周期的闭环安全防护体系，从底层筑牢终端设备与敏感数据的安全壁垒。

0.1 关于本手册

本手册旨在帮助您快速了解并熟练掌握 VEILORA 安全手机的各项专属安全功能及日常使用规范。由于本设备包含了诸多独特的底层加密与隔离机制，即使您已非常熟悉普通智能手机，我们仍强烈建议您在首次使用前仔细阅读本手册的所有章节。

0.2 安全与合规声明

在享受 VEILORA 带来的极致安全体验前，请您仔细阅读并知悉以下声明与合规条款：

1. 免责声明：您的核心秘钥（如账号恢复密语、隐私空间密码、手机还原密码）仅保存在设备本地的硬件安全模块中，由您自行离线保管。官方服务器绝对不备份、不存储您的任何解密凭证。因用户个人原因遗失密语、遗忘密码导致的数据无法解密或设备彻底锁定，VEILORA 官方及授权服务方将无法为您提供强制破解或数据恢复服务，亦不对由此产生的任何直接或间接数据损失承担连带责任。

2. 安全使用责任界定：本设备提供的“即时通讯加密”、“一键还原”、“网络隐身”等高级安全功能，旨在保护用户的合法通信隐私与正当数字资产。用户作为设备的唯一所有者，应妥善保管设备及其安全凭证，并自行承担使用该设备产生的一切法律后果。严禁将本设备用于任何违反所在地国家或地区法律法规的非法活动。

3. 系统完整性声明：请勿尝试对本设备进行非官方授权的提权破解（Root）、Bootloader 解锁或刷入第三方固件。此类高危操作导致设备不可逆转地锁定或清除所有数据，并使您的设备丧失保修资格。

1. 快速入门

欢迎使用 VEILORA 安全终端。首次开机时，系统内置的专属安全引导程序将协助您完成基础设置，并建立设备与您个人账号的唯一信任绑定关系。请保持网络通畅，并按照以下步骤耐心完成配置。

1.1 认识您的手机

Pixel 9 Pro XL 硬件外观介绍、实体按键功能说明、各类接口参数与使用注意事项，帮助用户快速熟悉设备硬件。



① 电源键（侧边键）：

常规操作：短按可点亮/息灭屏幕；长按可唤出关机或重启菜单。

② 音量键：用于调节通话、媒体及系统通知的音量。同时按下“电源键 + 音量减”可进行屏幕截图。

③ 前置摄像头：用于日常拍摄与加密视频通话。

④ 后置影像系统：包含超高像素主摄、超广角及长焦镜头，用于日常记录或扫描账号安全绑定等私密二维码。

⑤ SIM 卡槽：位于机身底部边框，使用顶针弹出卡托后，用于放置您的实体通讯 SIM 卡。

⑥ USB-C 数据/充电接口：

常规操作：支持高速快充。

⑦ 麦克风矩阵：分布于机身顶部与底部，用于清晰拾音与语音加密通话。与摄像头类似，麦克风被调用时屏幕右上角会有专属的绿色警示标识。

⑧ 立体声扬声器：顶部听筒与底部扬声器组成，提供优质的语音通话与媒体播放音质。

1.2 首次开机引导

① 欢迎界面

如图 1-1 所示，这是开机后的首屏画面。您可以在此选择系统语言（如“中文”），或根据需要设置无障碍选项。确认后，点击右下角的“下一步”正式开始配置流程。

② 连接 Wi-Fi 网络

如图 1-2 所示，为了确保后续的账号注册与硬件指纹校验顺利完成，请开启“WLAN”开关并连接至一个可靠的无线网络。连接成功后，点击“下一步”继续。

③ 登录 VEILORA OS 账号

如图 1-3 所示，此步骤是实现设备所有权绑定的核心。若您已有账号，请输入绑定的手机号与密码并点击“下一步”进行登录；若您是新用户，请点击下方的“立即注册”跳转至图 1-4。

④ 创建 VEILORA OS 账号

如图 1-4 所示，在注册界面，请输入您的手机号并设置一个高强度的登录密码（需输入两次以确认）。点击“立即注册”后，系统将在底层为您生成专属安全凭据，并与当前硬件进行唯一性强绑定。



图 1-1



图 1-2



图 1-3



图 1-4

⑤ 备份核心凭证（恢复密语）

如图 1-5 所示，账号绑定成功后，系统会生成唯一的“恢复密语”。

⚠ 重要： 密语是您重置密码、解除设备绑定及恢复数据的唯一离线凭证，系统云端不予留存。请务必将其准确抄写在纸质介质上并妥善存放于安全处。

确认保存： 抄写完成后，勾选下方的“我已安全保存恢复密语”，此时右下角的“完成并返回登录”按钮将解锁。点击该按钮即可返回登录界面完成首次身份激活。

⑥ 核对日期与时间

如图 1-6 所示，系统通常会自动同步网络时间，但请您在此界面再次仔细核对时区、日期与时间是否准确。准确的时间参数是系统校验各类安全加密证书、确保网络通信合规的重要基准。确认无误后，点击“下一步”。

⑦ 位置服务隐私设置

如图 1-7 所示，您可以根据个人隐私需求，在此统一预设底层的位置权限。您可以自主决定是否开启“使用位置信息”、“网络定位”、“始终允许 Wi-Fi 扫描”以及“地理编码”等开关。

💡 提示： 彻底关闭这些选项能最大程度实现地理位置隐身，但可能会影

响地图导航等应用的精准度。配置完成后，点击“下一步”。



图 1-5



图 1-6



图 1-7

设置系统锁屏密码（PIN 码）

完成上述隐私设置后，系统将引导您进入锁屏密码设置界面。请按照屏幕指引设置您的系统解锁 PIN 码。该密码将作为您进入系统主空间、解锁屏幕以及加密本地存储的核心密钥。

⑧ 安全预览版补丁设置

如图 1-8 所示，勾选界面中的选项后，您的设备将能够绕过常规更新通道，第一时间获取并应用最新的底层安全补丁。建议您开启此项。配置完成后，点击右下角的“Next”。

⑨ 恢复应用与数据

如图 1-9 所示，如果您之前使用的是另一台 VEILORA 安全手机，并拥有基于该账号的安全备份，可点击右下角的“恢复”按钮进行数据无缝迁移。若您是初次使用本系列产品，或希望作为一台没有任何冗余数据的全新设备启动，请点击左下角的“跳过”。

⑩ 手势导航学习与配置完成

如图 1-10 所示，在向导的最后，系统将引导您熟悉全局滑动操作（如侧滑

返回、上滑回到主屏幕等）。您可以点击右下角的“试试看”进行交互演练，也可以点击左下角的“跳过”直接结束全部引导。至此，您的设备已准备就绪，欢迎开启纯净、安全的 VEILORA 系统体验。

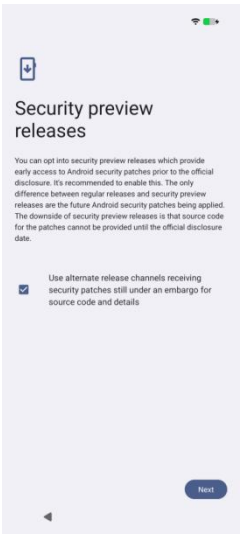


图 1-8

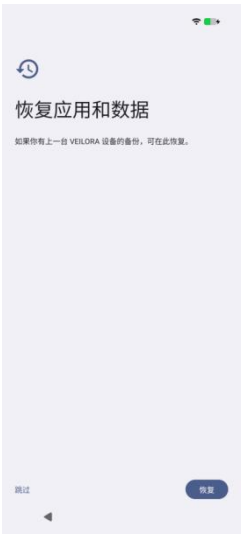


图 1-9



图 1-10

1.3 系统账号管理

VEILORA 安全账户是开启设备唯一绑定、加密云备份及远程防护能力的钥匙。请按照以下步骤完成账户的登录与维护：

① 进入账户管理入口

打开手机原生“设置”应用。如图 1-11 所示，在设置列表的最顶部，点击带有蓝色头像图标的“未登录（点击登录您的账户）”项，即可跳转进入专属的个人账户管理系统。

② 账号登录与功能导航

如图 1-12 所示，在欢迎登录界面：

登录：若已有账号，请输入绑定的手机号及密码，点击“登录”。

注册：若您是初次使用本设备，请点击右下角的“立即注册”，跳转至图 1-13。

重置：若您忘记了现有账号的密码，请点击左下角的“忘记密码？”，跳转至图 1-14。

③ 建立新账号（注册）

如图 1-13 所示，在注册账号界面，请输入您计划绑定的手机号码，并设置符合安全强度要求的登录密码（需输入两次以确认）。点击“注册”后，系统将引导您生成极度重要的“恢复密语”（详见后续密语管理章节）。

④ 找回账号权限（重置密码）

如图 1-14 所示，若需找回账号，请在重置密码界面输入绑定的手机号，并填入您在初次注册时离线备份的“安全密语”。密语校验成功后，您即可直接设置并确认新的登录密码。



图 1-11



图 1-12



图 1-13



图 1-14

登录成功后，您可以在个人信息页面对账户资料、安全绑定及核心凭证进行全面管理。

⑤ 个人信息主页

如图 1-15 所示，此界面为您展示了账户基本信息（头像、昵称、唯一账号 ID）及安全绑定状态。您可以在此发起修改密码、查看密语或退出登录等操作。

⑥ 修改账户昵称

如图 1-16 所示，点击“昵称”栏可弹出修改窗口。输入新的名称并点击“确定”，即可完成账户对外显示名称的更新。

⑦ 手机号解绑（设备释放）

若需更换账号或转让设备，请点击“手机号”栏。如图 1-17 所示，系统将弹出确认弹窗。点击“确定”并完成随后的身份验证，即可解除当前设备与账号的强绑定关系并自动登出。

⑧ 关键操作身份验证

如图 1-18 所示，当您执行“查看密语”、“修改密码”或“解绑设备”等高敏感操作时，系统会强制要求输入登录密码。您可以点击“眼睛”图标核对明文，确认无误后点击“确定”通过验证。

⑨ 专属密语查阅与备份

如图 1-19 所示，通过验证后即可查看您的“安全密语”及二维码。

⚠ 重要：密语是找回权限的最高凭证。若您同时遗忘了登录密码且丢失了安全密语，官方将无法通过后台为您重置账号，请务必妥善保管您的核心凭证。

安全限制：界面将显示“剩余查看次数”，请务必在次数耗尽前将其离线妥善备份。点击“复制并关闭”可一键存入剪贴板。

⑩ 修改登录密码

如图 1-20 所示，点击“修改密码”后，请依次输入您的旧密码及两次新密码。点击“确定”即可完成更改。若忘记原密码，请参考前文“重置密码”流程。

⑪ 安全退出登录

如图 1-21 所示，点击页面底部的“退出登录”并确认。为了极致的隐私防护，登出操作将同步永久清除本设备上的所有本地账号缓存数据，请在操作前确认重要信息已完成同步。



图 1-15



图 1-16



图 1-17



图 1-18



图 1-19



图 1-20



图 1-21

温馨提示：

密语是您重置密码的唯一凭据。请务必在初次登录后，将您的密语抄写在纸上或保存在离线的安全硬件中，切勿将其截图保存在手机相册或发送给他人，以免造成不可逆的账号丢失或数据泄露。

“退出登录”仅清除本地账号缓存；而“解除绑定”不仅会登出，还会清除该设备与云端的所有记录，使其失去远程定位和远程还原的保护，请谨慎操作。

1.4 快捷安装应用

为了保障系统环境的纯净与安全，VEILORA 手机提供了“精选应用”快捷安装功能。您可以从中一键获取经过安全兼容性测试的常用办公与社交软件。

① 进入精选应用入口

如图 1-22 所示，在手机桌面打开 【设备管理】 应用。在主界面的控制中心面板最下方，找到并点击 【精选应用（一键安装）】 选项。

② 选择并执行批量安装

如图 1-23 所示，进入“精选应用”列表页面，系统为您罗列了主流的社交（微信）、支付（支付宝）、购物（淘宝、京东）及地图（高德地图）等必备软件。

单项安装：点击目标应用右侧的 【安装】 按钮，系统将自动从安全源下载并执行安装。

批量安装：您可以勾选多个应用左侧的选择框，或者点击左下角的“全选”，随后点击底部的蓝色按钮 【立即安装 (X)】，系统将按顺序为您自动完成所有选定应用的部署。



图 1-22

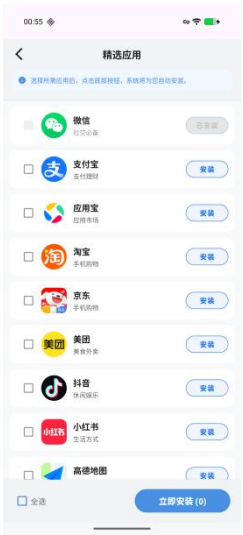


图 1-23

2.如何创建与设置隐私空间

2.1 全系统多层级隔离加密存储

VEILORA 安全终端具备全系统多层级隔离加密存储能力。一是物理级多空间隔离，各空间拥有独立 UID、独立运行应用、独立存储分区、独立加密密钥，相互隔离、互不干扰；二是应用沙箱隔离，应用间相互隔离，降低应用间恶意数据窃取和数据泄露风险；三是文件级精细化加密，不同用户、不同存储空间配备独立密钥，实现单文件、单空间精准加密防护。

2.2 初始化隐私空间

本系统支持通过不同的锁屏密码直接进入对应的存储空间，实现主空间（日常使用）与隐私空间（高度机密）的瞬间无感切换。

① 进入系统设置界面

如图 2-1 所示，在主屏幕点击“设置”图标。在菜单列表中向下滚动，找到并点击 【系统】。这里是管理语言、时间以及多用户隔离环境的核心配置入口。



图 2-1

② 管理用户账户空间

如图 2-2 所示，在系统设置列表中，点击 【用户】 选项。在此页面，您可以直观地查看到设备当前分配的所有存储空间状态。

③ 访问隐私空间入口

如图 2-3 所示，在用户列表中找到 【隐私空间】（首次使用时，下方会标注为“未设置”）。点击进入隐私空间的详细功能配置页面。

④ 空间功能配置与权限管理

如图 2-4 所示，在此页面您可以开启“允许在后台运行”、“开启通话和短信功能”等高级权限。配置完成后，点击首项【切换到隐私空间】即可触发环境转换。

⑤ 启动隐私空间初始化

如图 2-5 所示，系统会弹出对话框询问“要现在设置该用户吗？”，请点击【立即设置】。随后系统将引导您进入一个完全隔离的全新桌面环境，按照系统提示完成引导即可。



图 2-2



图 2-3



图 2-4



图 2-5

2.3 设置“双 PIN 码”实现空间切换

为了达到极致的隐蔽性与操作效率，VEILORA 支持不同密码进入不同空间的机制。您为主空间和隐私空间设置不同的 PIN 码后，在锁屏界面输入对应的密码，系统将自动识别并跳转至相应空间。

① 进入安全和隐私设置

如图 2-6 所示，在系统主界面打开“设置”，向下滚动并点击【安全和隐私】选项。

② 选择设备解锁

如图 2-7 所示，在安全和隐私管理页面中，点击【设备解锁】栏目。、

③ 开启屏幕锁定配置

如图 2-8 所示，点击【屏幕锁定】（下方通常会显示当前已设置的锁类型，如 PIN 码）。

④ 设置 PIN 码与自动确认解锁

如图 2-9 所示，在“选择新的屏锁”界面点击【PIN 码】：

设置密码：请输入一组 6 位以上的数字。

建议策略： 为主空间设置一个日常密码（如：111111），为隐私空间设置一个完全不同的保密密码（如：888888）。

开启自动确认（核心操作）：在设置密码后，请务必勾选下方的【自动确认解锁】开关。

优势： 开启后，当您在锁屏界面输入完最后一位正确数字时，系统将无需点击确认键即可直接进入对应空间。



图 2-6



图 2-7

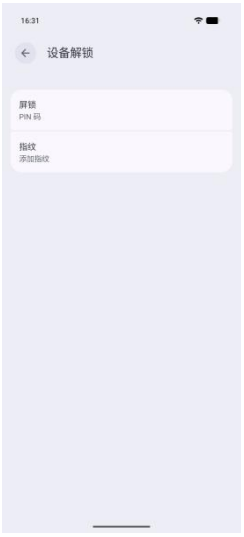


图 2-8



图 2-9

2.4 跨空间文件同步指南（主空间 ➔ 隐私空间）

本系统的主空间与隐私空间在物理和逻辑上实现了严格的数据隔离。当您需要将主空间的敏感文件转移至隐私空间妥善保管时，无需借助外部存储设备，可通过系统内置的“一键同步”功能安全直达。

【第一阶段：在主空间发起同步】

① 选中目标文件

如图 2-10 所示，在主空间中打开系统自带的“文件”或图库应用。浏览并找到您需要转移的敏感文件（例如图中展示的两张照片），长按并勾选它们。

② 唤出同步选项

选中文件后，点击屏幕右上角的“⋮”（三个垂直点）图标打开更多操作菜单。如图 2-11 所示，在弹出的下拉列表中，选择专门定制的 “同步到隐私空间” 选项。

③ 确认同步指令

如图 2-12 所示，屏幕中央会弹出安全确认窗口。此步骤旨在防止因误触导致的跨空间数据流转。核对无误后，点击 【同步】 按钮。

④ 查看同步反馈

如图 2-13 所示，系统将在底层加密通道中执行数据复制。传输完成后，屏幕下方会弹出“同步完成 X 个项目”的提示浮窗，表明文件已安全抵达隐私空间。

【第二阶段：在隐私空间查阅文件】

⑤ 进入隐私空间文件系统

请先切换至“隐私空间”状态。如图 2-14 所示，打开隐私空间内的“文件”应用，点击左上角的“═”菜单唤出侧边栏，并选择您的设备名称（如“Pixel

9 Pro XL”）进入内部存储根目录。

⑥ 定位同步接收目录

如图 2-15 所示，在根目录列表中找到名为 “Sync” 的系统文件夹。该文件夹是隐私空间接收主空间同步数据的专属归档区域。

⑦ 进入深层同步目录

如图 2-16 所示，点击进入 Sync 文件夹，并继续点击内部的 Sync 子目录。

⑧ 按原始路径查看文件

进入深层目录后，如图 2-17 所示，您会发现系统保留了文件在主空间时的原始目录结构（如 Sync > Sync > DCIM > Camera）。这种设计方便您在转移大量数据后，仍能按照原有的组织逻辑快速精准地找回照片或文件。



图 2-10



图 2-11



图 2-12



图 2-13



图 2-14

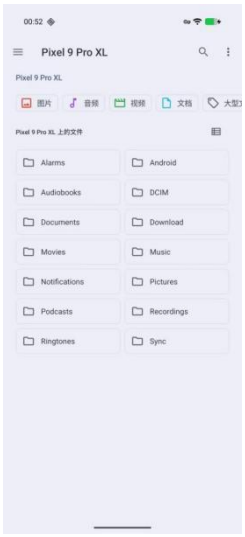


图 2-15

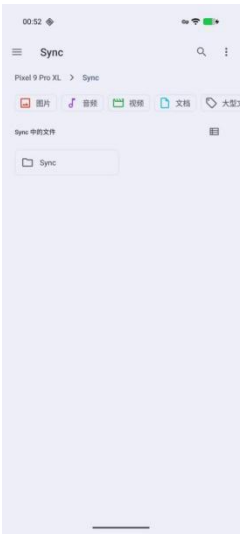


图 2-16



图 2-17

3.如何防止被外界网络画像

针对终端网络探测、画像、攻击、流量入侵等风险，VEILORA 通过网络隐身、反追踪定位、攻击防护、智能流量管控四大机制，动态收敛设备网络攻击面，显著降低终端网络暴露风险，打造低可视、高安全的网络运行环境。

3.1 防追踪画像、主动网络攻击防护

有效规避设备在局域网、互联网环境下被嗅探、端口扫描、资产特征抓取的风险；支持手动关闭 GPS 定位、基站连接功能，动态缩减设备网络暴露范围，大幅降低设备被发现、被定向攻击的概率。



图 3-1

如图 3-1 所示，在“隐私与安全”APP 主页的“违规网络访问”面板中，找到 【设备隐身】 开关。

默认配置： 为了您的最高隐私安全，本功能建议始终保持默认开启状态。

3.2 智能流量异常管控

① 开启网络通信管控

如图 3-2 所示，在主页“违规网络访问”面板中，点击开启 【网络通信管控】 开关。开启后，系统流量防火墙将全面接管所有数据包请求。若需查看异常联网详情，点击该区域上方的“违规网络访问”卡片，进入风险审计列表。

② 查看网络风险列表

进入“网络风险”界面后（如图 3-3 所示），系统会按联网异常频次自动排列应用名单。您可以直观地看到各应用在近期尝试连接外部服务器的总次数以及目标 IP 地址。通过此列表，您可以快速锁定那些在非活跃状态下频繁“偷跑”流量的可疑软件，点击卡片进入详情。

③ 执行应用级精准阻断

在特定应用的“网络活动详情”页中（如图 3-4 所示），您可以精确查阅该应用每一次联网的时间戳、目标域名/IP 及触发状态。

精准管控： 针对非必要联网的应用，您可以在“权限控制”栏根据需求开启 “禁止访问”、“禁止后台访问” 或 “禁止锁屏访问”。一旦开启拦截，系统将从底层网络驱动级强制断开该应用对外网络通信。



图 3-2

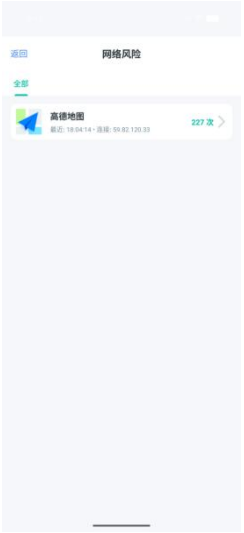


图 3-3



图 3-4

4.如何防止 APP 窃取隐私

突破传统静态权限授权模式，构建“实时审计、全程监控、主动拦截、一键防护”的动态隐私防护体系，提升终端隐私权限在多场景、多状态下的管控能力，降低 APP 恶意获取权限、后台窃取数据及越权访问等安全风险。

4.1 应用权限管控与风险审计

在线实时监控系统及所有第三方 APP，在前台运行、后台驻留、锁屏待机全状态下，对通讯录、相册、短信、剪贴板、麦克风、扬声器、定位、WiFi、基站、各类传感器等隐私资源的调用请求与操作行为，实现提升监控覆盖范围，生成权限审计日志，便于追溯相关隐私操作行为。

设备锁屏、应用后台驻留状态下，根据安全策略限制 APP 的隐私权限调用请求，降低恶意应用在用户无感知情况下后台获取隐私数据的风险，增强待机状态下的隐私防护能力。

① 开启全局权限管控

如图 4-1 所示，在“隐私与安全”APP 的首屏“安全管控中心”，找到【应用权限管控】全局开关并将其开启（默认开启状态）如图 4-2。此操作将全面激活系统底层的权限管控能力，开始实时接管并监控设备内所有应用的行为，防止隐私被静默窃取。

② 查看越权访问风险列表

点击该区域上方的“越权访问请求”卡片，进入如图 4-3 所示的“权限风险”列表。在此界面，系统会清晰罗列近期尝试调用敏感权限的应用及其频次。您可以通过顶部的“位置”、“相机”、“麦克风”等标签进行分类筛选，快速识别存在隐私侵犯嫌疑的软件。

③ 执行应用级精准阻断

点击特定应用卡片进入详情页。如图 4-4 所示，您可以在“权限控制”区域执行细粒度阻断，包括 “禁止访问”、“禁止后台访问” 以及 “禁止锁屏

访问”。开启拦截后，系统将从底层静默阻断该应用的越权请求，并在下方的“近期风险记录”中实时生成拦截日志。



图 4-1



图 4-2

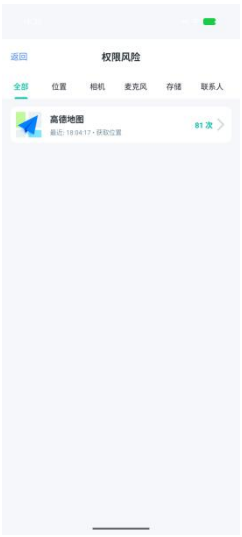


图 4-3



图 4-4

4.2 一键超级隐私防护模式

针对涉密会议、商务谈判、私密场景等高频高隐私需求场景，支持一键开启超级隐私模式，临时限制整机 APP 的敏感权限调用能力，从源头降低设备隐私泄露风险。

① 触发超级隐私模式

如图 4-5 所示，在主页“越权访问请求”卡片区域内，点击开启 【超级隐私模式】 开关。该功能具有最高优先级的保护权限。

② 确认底层熔断预警

如图 4-6 所示，系统会弹出红色预警窗口。开启此模式后，系统将在驱动层强制禁用相机、麦克风及 GPS 位置定位模块，彻底切断所有数据交互。提示： 开启后常规电话、视频通话及导航将受限。确认后点击 【开启】 即可进入绝对隐私状态。

③ 退出超级隐私模式

如图 4-7 所示，当您离开敏感环境需要恢复手机正常功能时，只需返回此界面并关闭【超级隐私模式】开关。系统将重新加载底层硬件驱动，设备随即回归常规工作状态。



图 4-5



图 4-6



图 4-7

5. 如何防止在即时通信中被第三方留存导致泄密

针对即时通讯、文件传输、语音通话、网络会议等高频信息交互场景，系统内核支持端到端加密能力，在适配场景下减少对第三方应用改造的依赖，降低第三方服务器明文留存、窃取和泄密风险，提升各类通信数据传输过程中的安全性。详细操作步骤如下：（仅有在隐私空间内才能使用即时通信安全功能）

5.1 开启密写转换工具

为了在第三方应用中实现文字、语音和文件的即时加解密，您需要首先开启系统的“密写转换工具”并授予必要的底层权限。：

① 启动密写转换工具

如图 5-1 所示，进入隐私空间并打开“隐私与安全”APP。在主页底部找到【密写转换工具】选项并点击开启。由于该功能需要全局悬浮显示并接管输入法流量，首次开启时系统会自动跳转至“无障碍权限”设置页面。



图 5-1

② 选择服务项

如图 5-2 所示，在自动弹出的“无障碍功能”列表中，找到并点击【隐私与安全】这一项。



图 5-2

③ 开启服务开关

如图 5-3 所示，进入详情页后，点击“使用隐私与安全”右侧的开关。

④ 确认系统授权

如图 5-4 所示，由于该权限涉及屏幕内容读取与全局操作，系统会弹出高级别安全提示。请阅读说明后点击【允许】，以授权“隐私与安全”服务运行底层加密引擎。

⑤ 校验权限开启状态

如图 5-5 所示，开关变为蓝色激活状态，表示系统已成功授予该工具所需的底层运行权限。

⑥ 确认开启并激活悬浮锁

如图 5-6 所示，返回“隐私与安全”APP 界面，此时【密写转换工具】开关已处于开启状态。同时，屏幕左侧边缘会同步出现“金色悬浮安全锁”图标。至此，您已完成通讯加密的所有前置准备，可在任何第三方通讯软件中通过该“悬浮锁”进行加密操作。



图 5-3



图 5-4



图 5-5



图 5-6

5.2 如何进行加密消息通讯

通过密写转换工具，将您的原始聊天信息（明文）转换为无意义的乱码（密文）。即使通讯软件的服务器被劫持或聊天记录泄露，攻击者也只能看到无法破解的乱码字符。只有拥有该安全手机的授权用户，才能在终端通过专用工具还原真实信息。

① 激活密写工具入口

如图 5-7 所示，打开任意即时通讯应用进入对话界面。长按屏幕左侧的“金色悬浮锁”图标，即可在当前界面上方唤出密写转换工具。

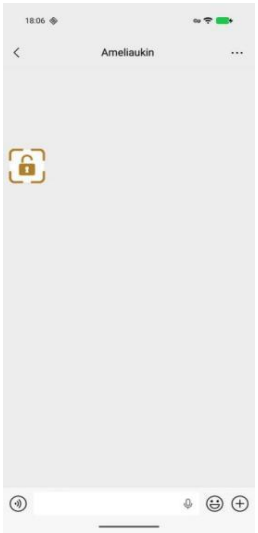


图 5-7

② 编辑原始明文并生成密文

如图 5-8 所示，在弹出的【密写转换工具】对话框内，输入您想要发送的真实原始信息（例如“你好”）。输入完成后，点击底部的 【复制密文】 按钮。此时，系统已自动完成高强度加密，并将生成的加密字符串存入您的系统剪贴板。

③ 准备执行密文粘贴

如图 5-9 所示，点击右上角的“×”关闭工具窗口返回聊天界面。长按通讯软件原生的文字输入框，唤出系统的功能菜单。

④ 将密文粘贴至发送框

如图 5-10 所示，点击菜单中的 【粘贴】。此时，刚才生成的乱码字符串（密文）会填入输入框。

⑤ 执行安全发送

如图 5-11 所示，点击通讯软件的发送按钮。该密文消息将通过网络发出。在此过程中，任何尝试拦截数据的第三方或通讯平台服务器，仅能获取到这组加密乱码，无法获知真实的沟通意图。

⑥ 消息实时还原与查看

如图 5-12 所示，当您或对方收到密文消息时，安全手机的底层解密引擎会自动识别并处理这些特定格式的密文。借助系统级实时渲染技术，真实的明文内容（如“你好”）将以半透明浮层的方式覆盖在原有密文之上。这种“即看即显”的模式既保障了安全性，又确保了沟通的流畅性。

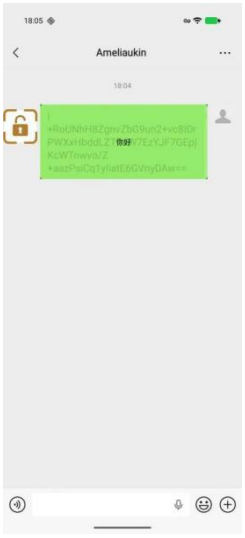


图 5-12



图 5-8

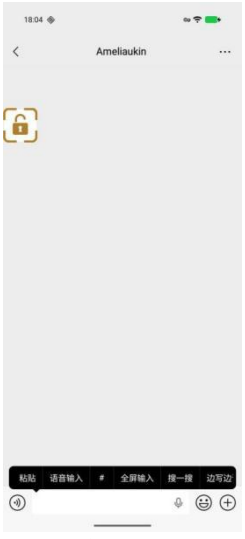


图 5-9

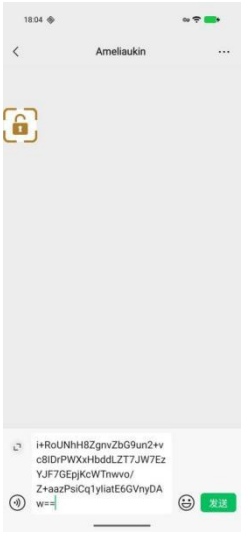


图 5-10



图 5-11

温馨提示：当前密文实时渲染解密支持的软件包括微信、手机短信；更多软件适配尽请期待。

5.3 如何发送加密文件

传输文件可支持本地前置加密处理，加密文件传输至接收方后自动解密，降低明文文件流转以及传输过程中被截留、泄密的风险。

5.3.1 第三方 APP 选择本地文件进行密/明发

5.3.1.1 发送明文图片/文件

① 准备发送文件

如图 5-13 所示，进入微信对话界面，点击“+”号并选择“文件”功能。核心提示：请观察屏幕右侧的“金色悬浮安全锁”，此时锁头处于开启状态，代表系统当前处于明文传输模式。

② 浏览明文相册

如图 5-14 所示，在微信内置的“手机相册”页签下，您可以正常看到手机内所有图片的原始缩略图，方便您快速预览和筛选。

③ 勾选明文图片

如图 5-15 所示，直接勾选您想要发送的一张或多张图片，点击右下角的“发送”按钮，图片将以常规原图形式发出。

④ 选取手机本地文件

如图 5-16 所示，若需发送文档或其他类型文件，请切换至“手机文件”页签，并点击下方的“选取”按钮。

⑤ 在系统目录中检索

如图 5-17 所示，系统将调用底层文件管理器。在这里，您可以根据目录结构浏览并选中您需要发送的原始明文文件。

⑥ 确认并完成明文发送

如图 5-18 所示，选中文件后返回微信确认界面。此时文件显示为正常的 .png 或相关格式。点击右下角的“发送”按钮，文件将以不加密的形式直接发送给对方。

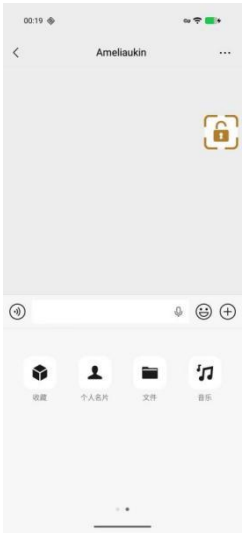


图 5-13



图 5-14

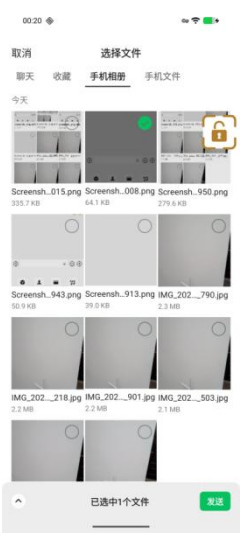


图 5-15



图 5-16



图 5-17



图 5-18

5.3.1.2 发送密文图片/文件

① 激活加密模式（上锁）

如图 5-19 所示，在聊天界面点击右侧悬浮锁，使其切换为闭合状态。代表系统底层加密引擎已接管数据接口。

② 自动转换密文格式

如图 5-20 所示，再次进入微信“手机相册”页签。您会发现系统已自动对所有文件进行了底层加密处理，并通过专用手段在页面上能够明文查看，方便选择；图片名称后缀统一变更为.xefc（本系统专属加密格式）。

③ 勾选密文图片发送

如图 5-21 所示，勾选带有.xefc 后缀的目标文件，点击右下角的“发送”按钮。该文件将以高强度密文形式传输。

④ 选取加密文件入口

如图 5-22 所示，若发送非相册文件，请在“手机文件”页签下点击“选取”。

⑤ 系统底层实时加密

如图 5-23 所示，在弹出的系统底层文件管理器中选中目标文件。

⑥ 确认密文发送状态

如图 5-24 所示，返回微信确认界面。此时您可以清晰地看到即将发送的文件后缀名已自动变更为 .xefc。确认无误后点击“发送”。

⑦ 发送结果直观对比

如图 5-25 所示，返回对话主界面可查看到发送结果：

上方消息：明文发送，显示正常缩略图及原文件名。

下方消息：密文发送，显示为 .xefc 格式，平台无法直获取文件内容，仅有具备权限的接收方方可解密查阅。



图 5-19



图 5-20

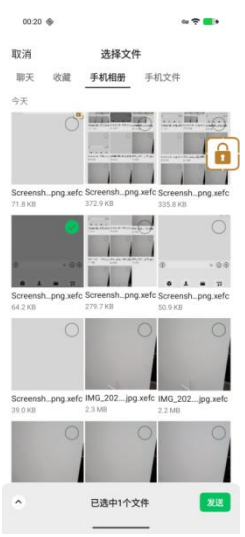


图 5-21



图 5-22



图 5-23



图 5-24

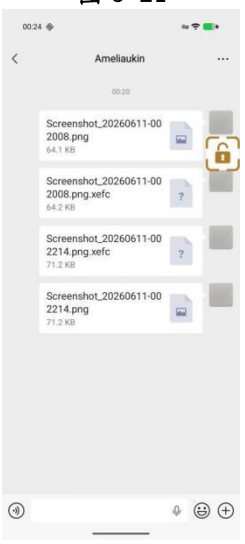


图 5-25

5.3.2 使用文件管理 APP 进行文件密/明发

5.3.2.1 发送明文图片/文件

如果您需要快速分享非敏感照片或文档，请使用常规分享通道。

① 路径导航与准备

如图 5-26 所示，打开“文件”（Files）应用，点击左上角菜单，导航至目标文件所在路径（例如：Pixel 9 Pro XL > DCIM > Camera）。

② 选中文件并识别明发图标

如图 5-27 所示，长按选中目标照片（出现蓝色勾选框）。此时屏幕右上角会亮起两个分享图标：

灰色分享图标代表明文分享通道。点击该图标，系统将以原始格式和文件名调起分享面板，后续操作与常规手机一致。

5.3.2.2 发送密文图片/文件

如果您需要外发的资料涉及核心机密，请务必调用红色的安全加密分享通道。

① 选中目标并调起加密通道

如图 5-27 所示，长按选中照片。点击右上角特设的红色加密分享图标。这是触发 VEILORA 底层加密引擎的专属入口。

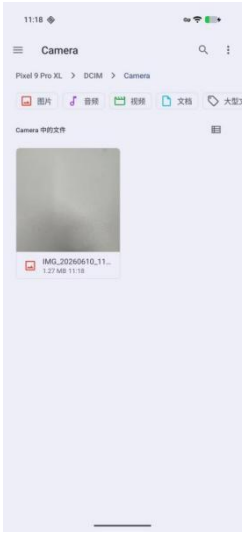


图 5-26

② 核对密文状态并选择渠道

如图 5-28 所示，在弹出的分享面板中，请核对待分享的文件名后缀是否确已变为 .xefc（本系统专属加密后缀）。确认已自动加密后，在下方应用列表中选择您需要使用的通讯工具（如“微信发送给朋友”）。

③ 确认接收人与加密信息

如图 5-29 所示，在跳转出的第三方软件界面中选择接收对象。在最后的发送预览框中，再次确认文件名带有 .xefc 标识。核对无误后，点击“发送”。

④ 密文成功发送

如图 5-30 所示，返回聊天界面，您可以看到加密文件已成功发出。该文件在传输全路径及第三方平台服务器中均以加密形态存在，只有具备权限的接收方使用同款安全手机方可解密。

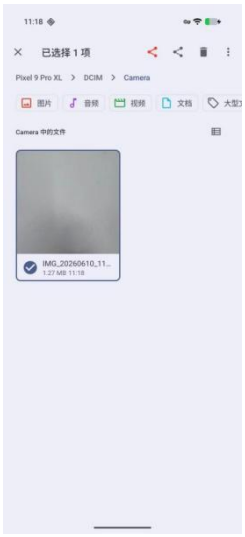


图 5-27



图 5-28



图 5-29

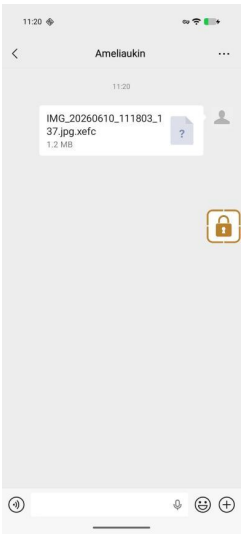


图 5-30

5.4 如何查看与浏览加密文件

若要查看专用的加密文件，请按照以下步骤规范操作：

① 触发加密文件预览

如图 5-31 所示，在聊天界面点击收到的加密文件（文件名后缀为 .xefc）。此时通讯软件会进入系统预检界面，由于文件处于高强度加密状态，屏幕将显示无法预览。

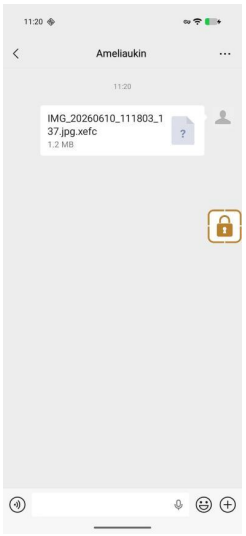


图 5-31

② 调用外部安全打开方式

如图 5-32 所示，点击屏幕底部的【用其他应用打开】按钮。此时系统底层会拦截该请求，并弹起可供选择的安全处理工具列表。

③ 选中专属密件查看器

如图 5-33 所示，在弹出的“用其他应用打开”面板中找到并点击【VEILORA 密件查看】。这是系统内置的唯一具备解密权限的安全沙箱入口。



图 5-32

④ 确认安全环境跳转

如图 5-34 所示，系统会弹出二次确认窗口，提示即将

离开第三方应用并打开安全工具。点击【允许】，系统将即刻切断与第三方应用的直接关联，并将加密文件流导入受保护的隔离安全沙箱进行解密处理。

⑤ 选择解密后文件的浏览软件

如图 5-35 所示，密件查看工具在沙箱内完成实时解密后，会询问您使用何种软件查看解密后的明文内容。

软件选择：图片或视频类建议选择“图库”；文档类请选择“WPS”或“Office”等。

推荐操作：选中对应软件后点击【始终】。系统将建立永久关联，后续打开同类加密文件时，将自动唤起安全查看器并调用对应软件，实现“秒开”体验。

⑥ 成功查阅密件内容

如图 5-36 所示，经过系统底层安全引擎的实时处理，加密文件的真实内容将完美呈现。查阅过程完全在隔离的内存沙箱中进行，确保文件解密后的明文内容不会被第三方应用非法抓取或留存。



图 5-33



图 5-34



图 5-35


图 5-36

5.5 如何进行加密语音通讯

依托系统原生内核能力，实现语音采集自动加密、语音播放自动解密，支

持覆盖多类网络语音通话、线上会议场景，降低通话窃听、会议内容抓取、明文留存等安全风险，提升语音通信安全性。

① 切换至普通语音通话模式（明文）

如图 5-37 所示，当“悬浮安全锁”图标处于解开状态时，代表当前处于常规非加密模式。

状态确认：点击图标切换至解锁状态。在此模式下，您的通话将通过通讯软件的标准通道发出，适用于日常普通沟通。

② 切换至安全加密通话模式（密文）

如图 5-38 所示，点击“悬浮安全锁”图标使其变为锁闭状态。此时，系统底层的全局语音加密引擎已激活。

状态确认：当锁头闭合时。在此模式下，系统将接管通讯软件的音频流并进行高强度实时加密。

开启后直接正常使用第三方软件进行加密语音通话即可；

③ 通过隐私与安全软件打开语音加密功能

如图 5-39、图 5-40 所示，在隐私空间中，进入隐私与安全软件，可在软件首页底部看到全局语音加密开关，可通过在这里切换开关状态来切换语音加解密模式。



图 5-37



图 5-38



图 5-39



图 5-40

温馨提示：该模式能有效防止通话内容在网络传输链路中被非法窃听或录音。请注意，为了达到最佳加密效果，建议通话双方均使用本款安全手机并同时开启该模式。

6.如何使用私有云进行加密备份与恢复

6.1 WebDAV 云空间配置

VEILORA 安全手机的“云空间管理”不同于传统手机强制使用厂商自带云服务，我们支持通用的 WebDAV 协议。您可以自由选择自建 NAS、个人服务器或第三方支持 WebDAV 的网盘作为备份基座。通过加密隧道，系统可自动将相册、联系人、短信等应用数据同步至您的私密空间，实现数据的高度自主与安全备份。

① 进入云空间管理入口

如图 6-1 所示，在手机桌面打开 【设备管理】 APP。在下方的控制中心面板中，点击 【云空间管理】 选项。该模块是您管理远程存储节点与自动化备份策略的统一中枢。

② 云空间状态概览与应用配置

如图 6-2 所示，进入主页后，您可以在顶部查看到当前正在使用的空间名称（如默认的“VEILORA”）及连接状态。在该页面，您可以根据需求通过开关自主勾选需要备份的数据类别（如：相册、联系人、信息、通话记录等）。点击 【管理】 按钮可进入深层节点配置。

③ 管理云空间列表

如图 6-3 所示，在此界面您可以查看到所有已绑定的云存储节点。若需添

加新的私有存储空间，请点击右侧蓝色的 【+】 图标。

④ 选择云空间通信协议

如图 6-4 所示，系统将弹出协议选择菜单。请点击选择 【WebDAV】。这是一种通用的标准网络存储协议，能够完美支持大多数自建 NAS（如群晖、威联通）或支持 WebDAV 的第三方网盘服务。

⑤ 配置服务器连接参数

如图 6-5 所示，在添加界面准确输入您的云存储信息：

空间名称：自定义一个易于识别的备注名。

服务器 URL：输入 WebDAV 地址（需包含协议头及端口号，如 http://ip:port/dav）。

账户/密码：输入对应的登录凭证。

填写完成后，点击 【验证并添加】，系统将自动进行握手连接测试。

⑥ 设置默认存储节点

如图 6-6 所示，在已绑定的空间列表中，点击目标空间卡片。在弹出的菜单中选择 【设为默认云空间】。设置成功后，系统后续所有的自动化加密备份指令都将定向发送至该空间。您也可以在此处执行【删除云空间】操作。

⑦ 指定远程备份根目录

如图 6-7 所示，进入特定空间的目录树界面，浏览并进入您预设的备份文件夹（如 backup 目录）。确认路径无误后，点击右上角的 【设为备份目录】。至此，您的私有加密备份通道已正式搭建完成，本地重要数据将按照策略自动同步至该安全区域。



图 6-1

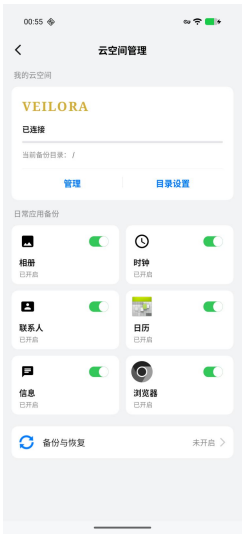


图 6-2

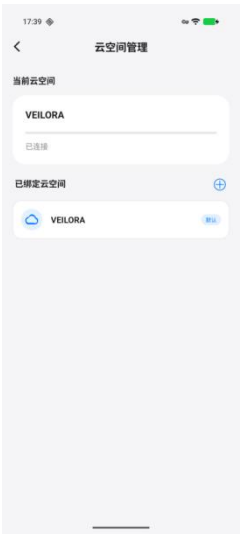


图 6-3

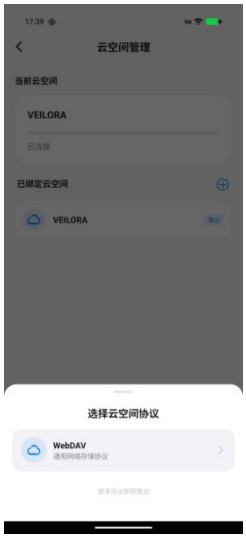


图 6-4



图 6-5



图 6-6

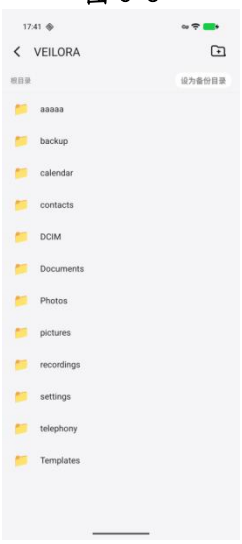


图 6-7

端到端加密：所有上传至私有云的数据在离屏瞬间均已完成本地加密。即使您的 WebDAV 服务器本身被入侵，攻击者无法在没有本机密钥的情况下解析备份文件的内容。

6.2 设置自动/手动备份计划

“备份与恢复”功能为您提供自动与手动两种数据备份模式。系统支持“静默备份”逻辑，即在设备接入电源、锁定屏幕并连接 WLAN 时，自动执行指定应用的备份，确保备份过程不干扰您的正常使用。同时，您也可以随时发起“立即备份”，为当下的重要数据留存快照。

在配置好私有云存储节点后，您可以设定自动化备份计划，确保在设备丢失或损毁时，能够通过云端加密快照完整恢复数据。

① 进入云空间管理入口

如图 6-8 所示，启动系统内置的 【设备管理】 应用。在主页控制中心点击 【云空间管理】。该模块是您管理所有远程存储路径与执行数据同步任务的统一中枢。

② 配置基础备份项

如图 6-9 所示，首先请确认顶部云空间处于“已连接”状态。

快捷同步：在“日常应用备份”列表中，您可以一键勾选相册、联系人、短信、通话记录等核心基础数据。

进阶设置：完成基础项勾选后，点击页面最下方的 【备份与恢复】 项，进入自动执行计划配置页。

③ 设定备份计划与手动执行

如图 6-10 所示，在此界面您可以全方位掌控备份行为：

激活自动备份：开启 【备份此设备】 开关。系统将在设备接入电源且连接 Wi-Fi 的空闲状态下，静默执行后台备份。

频率控制与手动备份：通过“备份频率”设定周期（如 7 天一次）；也可点击 【立即备份】 文字即刻手动触发上传。

跨设备版本管理：在“所有设备备份”列表中，您可以直观查看本台设备以及账号下其他关联设备在云端存储的备份大小与时间戳。

④ 精细化内容选择

如图 6-11 所示，点击上一页的“备份选项”可进入精细化配置页面。

定制内容：您可以针对系统设置、日历、录音、甚至特定的第三方应用数据进行个性化勾选。

存储优化：通过精细化配置，您可以优先保障核心机密业务数据的备份，从而更有效地管理您的私有 WebDAV 空间的存储容量。



图 6-8

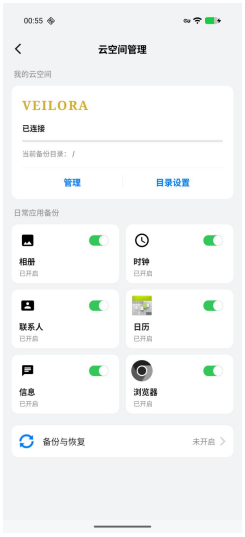


图 6-9



图 6-10



图 6-11

温馨提示：所有的备份数据在传输过程中均经过系统底层的高强度加密，确保云端存储的内容即便被非法获取也无法被解密。

6.3 本地数据恢复流程

设备重置、换设备场景下的云端数据恢复步骤、恢复范围、恢复进度查看与异常处理。

① 进入云空间管理入口

如图 6-12 所示，打开【设备管理】应用，在主界面点击【云空间管理】。该模块是连接您私有云端资产的唯一通道。

② 进入备份与恢复设置

如图 6-13 所示，首先确认页面顶部显示云空间为“已连接”状态。随后点击底部的 【备份与恢复】 选项，进入数据还原的决策界面。

③ 选择备份源设备

系统支持多设备备份共用同一空间。如图 6-14 所示，在“所有设备备份”区域，系统会列出当前 WebDAV 空间内存储的所有终端记录。请点击您需要提取数据的目标设备名称（例如：Pixel 9 Pro XL）。

④ 选择历史时间点（快照）

如图 6-15 所示，进入该设备的备份管理页面，您可以查看到所有的历史快照。请根据您的需求，在“其他备份”列表中点击选择对应时间点的备份项。

⑤ 勾选需要还原的数据项

如图 6-16 所示，在数据选择界面，您可以进行按需恢复：

精细化勾选：选择想要还原的应用数据（如：图库、联系人、系统设置等）。

执行还原：核对勾选的项目数量及总大小，确认无误后点击底部的蓝色按钮 【恢复所选数据】。

⑥ 恢复风险二次确认

如图 6-17 所示，系统会弹出“要恢复数据吗？”的红色预警提示框。

⚠ 覆盖逻辑说明：请知悉，恢复操作将使用云端数据覆盖本机现有的同类数据，且此过程不可逆。请确保环境安全且电量充足，点击 【继续】。

⑦ 输入安全密语完成验证

为防止备份数据被非法提取，系统将触发最高级别的身份验证。

验证身份：如图 6-18 所示，请输入该备份数据所属设备的唯一安全密语（即开机引导阶段您备份的密语）。

开始还原：点击 【验证】。验证通过后，系统将即刻启动云端下载并进行实时流解密，自动完成本地数据的覆盖恢复。



图 6-12

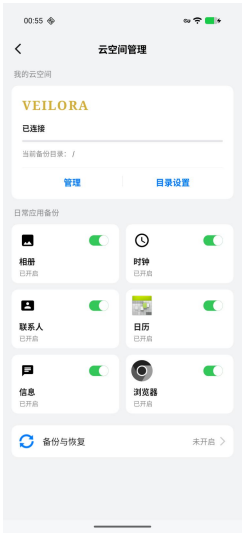


图 6-13



图 6-14



图 6-15

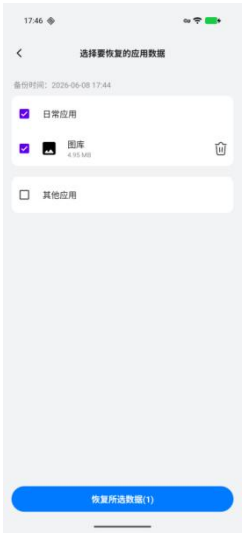


图 6-16

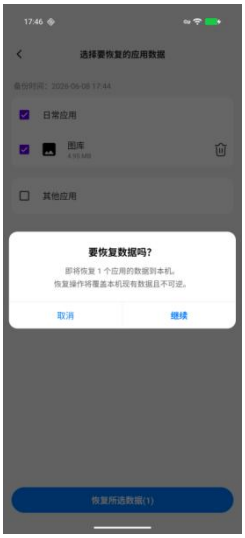


图 6-17

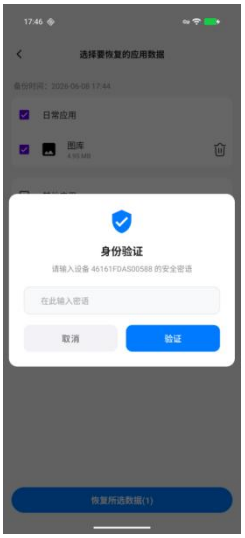


图 6-18

7.如何强化系统安全

依托系统具身安全智能内核，打破传统被动防御模式，提升系统安全自学习、异常行为识别与拦截能力，有助于应对未知风险和新型攻击，并持续迭代升级安全防护能力。

① 启用具身安全智能体（AI 主动防御）

如图 7-1 所示，打开“隐私与安全”APP，在主页“系统安全风险”卡片中，找到 【启用安全智能体】 开关（默认启用）。开启后，本地 AI 模型将实时分析系统的指令流与应用行为，智能识别并拦截零日漏洞攻击，实现无人值守的主动防御。

② 开启系统级禁止远控

如图 7-2 所示，在同一面板中，点击开启 【禁止远控】 开关（默认开启）。该功能会从底层驱动级切断所有的远程协助协议、屏幕共享流、ADB 调试接口以及模拟触控行为，确保您的设备无法通过网络被他人隐蔽操控。

③ 进入系统风险管理界面

如图 7-3 所示，点击“系统安全风险”卡片的任意位置，即可跳转进入深层的系统安全风险列表。通过此入口，您可以对设备底层的各类安全事件进行审计与追溯。

④ 实时扫描与多维度风险审计

如图 7-4 所示，进入详情页后，顶部的导航栏将威胁细分为“高危命令”、“文件风险”、“网络风险”、“进程风险”等专业维度。

健康状态：通常情况下列表为空白，表示系统处于安全稳定状态。

自动拦截：一旦检测到恶意软件尝试提权、调用高危指令或非法进程，系

统会立即在此处发出报警并自动执行阻断操作，保护系统基线不被破坏。

本地化运行：具身安全智能体完全在设备本地运行，不会将您的任何行为数据上传至云端，兼顾了智能化防御与极速隐私保护。



图 7-1



图 7-2



图 7-3

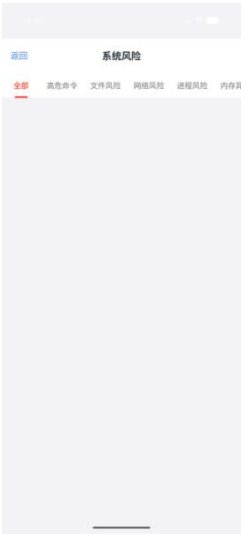


图 7-4

除了主动监控外，VEILORA 还提供了系统级的漏洞利用防护策略，通过硬化硬件接口和底层内存管理，为设备打造防御 0-day 攻击的坚实底座。

① 进入系统安全与隐私设置

打开手机原生“设置”应用，在列表中找到并点击【安全和隐私】，如图 7-5。此页面是系统原生安全能力的聚合中心，为您展示设备当前的整体合规状态及基础防护选项。

② 访问漏洞利用防护入口

如图 7-6 所示，在“安全和隐私”页面中滑动至底部，在“其他设置”栏目下点击【漏洞利用保护】。该模块包含了针对硬件端口、无线连接以及应用执行环境的多项高级加固开关。

③ 硬件接口与系统级安全配置

如图 7-7 所示，进入详情页后，您可以针对物理和网络连接进行深度策略定义：

USB-C 端口防护：建议保持“锁定时仅充电”。此功能在底层切断了锁屏状态下的 USB 数据链路，防止攻击者通过外部物理设备提取手机数据。

自动重启：预设固定的重启周期（如 18 小时）。定期重启可以强制清除内存中的非持久性恶意脚本，并使系统秘钥重新进入冷加密状态。

无线连接管控：您可以设置 Wi-Fi 或蓝牙在闲置时自动关闭，以减小设备的无线攻击面。

④ 应用级内存与动态代码防护

如图 7-8 所示，在页面下方的“应用级漏洞利用防护”区域，您可以配置更深层次的沙箱防御（保持默认配置即可）：

加固内存分配器：通过内存标记（Memory Tagging）等技术，实时拦截缓冲区溢出等针对应用漏洞的利用企图。

动态代码加载防护：严格管控第三方应用在内存中动态运行未授权指令的行为，有效封堵木马病毒的隐蔽注入路径。

安全进程启动：开启后，系统将对每一个新启动的应用进程执行完整性校验，确保其核心代码未被篡改。



图 7-5



图 7-6



图 7-7



图 7-8

8.如何进行应急还原

针对设备丢失等极端特殊场景，搭建三级密钥应急体系+快捷应急操作能力，支持快速升级设备安全等级，降低核心隐私数据被非法获取的风险。

日常解锁密钥：用于设备常规解锁、双域空间自由切换，保障日常正常使用；隐私空间还原密钥：输入后可正常进入日常开放域，同时执行隐私安全域不可逆还原至出厂状态；手机还原密钥：触发设备恢复出厂设置，实现更高等级的数据防护。

8.1 如何还原整个手机

8.1.1 手机还原密码设置

“手机还原密码”是针对极端安全场景设计的应急功能。当用户面临胁迫或紧急情况时，输入该预设密码，系统将重置所有数据，恢复出厂设置，确保核心敏感信息不被非法获取。具体设置步骤如下：

① 进入安全和隐私设置

如图 8-1 所示，在手机主屏幕中点击“设置”图标，进入系统设置主菜单。在列表中找到并点击【安全和隐私】选项。该模块是管理设备锁定、生物识别及隐私权限的核心入口。

② 展开高级安全选项

如图 8-2 所示，进入【安全和隐私】页面后，滑动至页面底部，在“其他设置”栏目下点击【更多安全和隐私设置】，以进入更深层次的系统加固选项。

③ 进入应急保护入口

如图 8-3 所示，在【更多安全和隐私设置】页面中向下滑动，在“安全”类别下点击【应急保护】。该功能专为极端紧急情况设计，为您提供最后的数据防护屏障。

④ 配置手机还原密码

如图 8-4 所示，在应急保护页面点击【手机还原密码】。

身份验证：系统会首先验证您当前的锁屏 PIN 码，以确保是本人操作。

设置还原密码：验证通过后，请按照屏幕提示设置专属的“还原密码”。



图 8-1



图 8-2



图 8-3

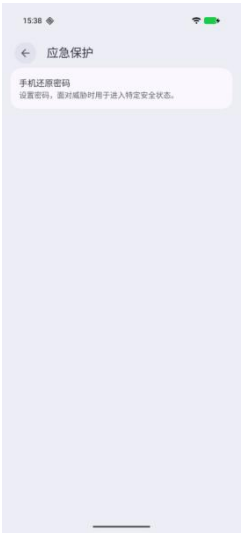


图 8-4

温馨提示：请确保该密码与您的日常开机解锁密码不同。设置成功后，在面对安全威胁的特殊时刻，通过输入此“手机还原密码”，将触发设备恢复出厂设置，实现更高等级的数据防护。

8.2 如何还原隐私空间

8.2.1 隐私空间一键还原设置

隐私空间“一键还原”是专为应对突发威胁设计的“数字还原”开关。开启后，用户无需进入复杂菜单，只需通过长按电源键唤出的电源菜单，即可立即执行隐私空间的数据擦除指令。具体设置步骤如下：

① 进入安全和隐私设置

如图 8-5 所示，在系统主界面打开“设置”，在列表下方找到并点击【安全和隐私】选项。



图 8-5

② 进入更多安全设置

如图 8-6 所示，在【安全和隐私】页面滑动至最底部，点击“其他设置”栏目下的【更多安全和隐私设置】。

③ 开启应急保护入口

如图 8-7 所示，向下滑动至“安全”栏目，点击【应急保护】选项。该功能是设备在极端情况下保护核心数据的最后防线。

④ 激活“一键还原”开关

如图 8-8 所示，在应急保护页面，点击打开【一键还原】右侧的开关。

功能原理：开启后，系统会在底层的电源管理菜单中新增一个名为“一键还原”的快捷指令，以便您在不解锁屏幕的情况下也能触发防护。

⑤ 呼出电源菜单并执行还原

如图 8-9 所示，当您需要执行紧急隐私空间还原时：

呼出菜单：在设备任何状态下（包含锁屏、黑屏或亮屏状态），长按电源键。

执行还原：在弹出的电源菜单中，点击并长按右下角的【一键还原】图标。

运行效果：执行后，系统将立即静默还原隐私空间内的所有机密数据与设置，确保核心隐私不被第三方获取。



图 8-6



图 8-7

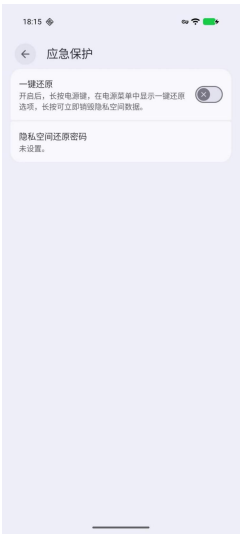


图 8-8



图 8-9

操作警告：在紧急情况下，长按该按钮，系统将立即按照预设逻辑抹除隐私空间的所有数据。此操作不可逆，请在确保数据已备份或确实面临安全威胁时谨慎使用。

8.2.2 隐私空间还原密码设置

“隐私空间还原密码”是一组特殊的 6 位数字密码。不同于常规的解锁密码，当您在锁屏界面输入此密码时，系统将在确保您使用该密码正常进入主空间的同时，立即执行预设的隐私空间数据擦除等指令，且整个过程无需二次确认，具有极高的隐蔽性和响应速度。请按以下步骤完成配置：

① 进入安全和隐私设置

如图 8-10 所示，在系统主界面点击“设置”图标。在列表下方找到并点击【安全和隐私】选项，进入系统的安全综合管理页面。

② 进入更多设置选项

如图 8-11 所示，在【安全和隐私】页面滑动至页面最底部，在“其他设置”栏目下点击【更多安全和隐私设置】。

③ 找到应急保护入口

如图 8-12 所示，在【更多安全和隐私设置】页面中向下滑动。在“安全”

栏目下找到并点击【应急保护】项，这是管理应急还原功能的入口。

④ 开启还原密码设置

如图 8-13 所示，在应急保护页面中，【隐私空间还原密码】默认显示为“未设置”。点击该选项，正式启动还原密码（静默口令）的创建向导。

⑤ 设置 6 位静默口令

如图 8-14 所示，系统跳转至“设置静默口令”界面。请在此输入一组唯一的 6 位数字。

⚠ 安全建议：为确保应急触发的隐蔽性与准确性，此密码必须与您的手机锁屏密码、隐私空间进入密码完全不同，严禁使用过于简单的连续数字。

⑥ 再次输入确认

如图 8-15 所示，根据屏幕提示重新输入刚才设定的 6 位数字以进行校验。核对无误后，点击底部的【确认】按钮。

⑦ 校验设置状态

如图 8-16 所示，配置成功后，屏幕下方会弹出“设置成功”的浮窗。返回应急保护主页面，您可以看到该选项已更新为“已设置还原密码”。



图 8-10



图 8-11



图 8-12

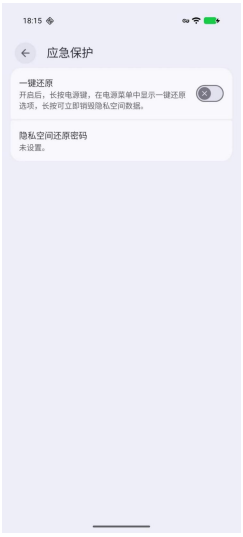


图 8-13

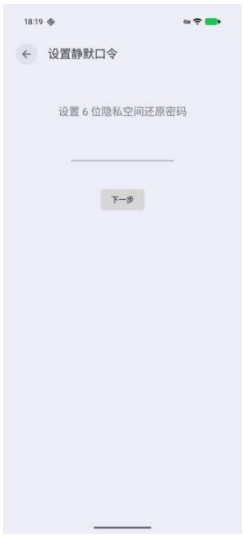


图 8-14

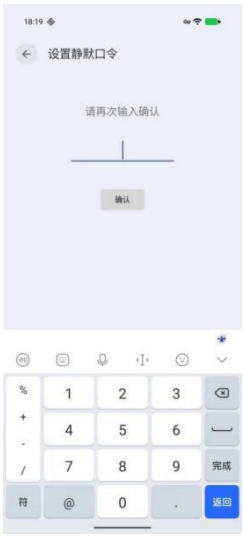


图 8-15



图 8-16

温馨提示：请确保该密码与您的主空间、隐私空间解锁密码不同。

注意：手机触发隐私空间还原操作后。如需再次启用隐私空间进行使用，需要重启一次手机后再进行隐私空间的创建与切换。

8.3 如何远程锁定与还原

8.3.1 远程锁定与追踪

“远程定位追踪”为您提供失联设备的高精度坐标。配合“丢失模式”，您可以远程对设备下达锁定指令，防止他人非法进入系统，并开启轨迹追踪功能，实时记录设备的移动路径，为找回设备提供关键线索。

① 进入设备管理入口

如图 8-17 所示，打开【设备管理】应用。在主页控制中心，点击【我的设备】项，进入账号下所有关联终端的管理列表。

② 锁定目标遗失终端

如图 8-18 所示，在设备列表中找到并点击您需要管控的遗失设备（例如：Pixel 9 Pro XL）。系统将尝试与该设备建立远程安全连接。

③ 开启丢失模式选项

成功连接后，界面将显示设备的实时（或最后已知）地理位置。如图 8-19 所示，在下方功能菜单中点击【丢失模式】。

④ 丢失模式初始配置

如图 8-20 所示，进入设置页面：

启用丢失模式：点击开启首项开关，准备锁定远程设备。

丢失轨迹追踪：同步开启此项。系统将记录设备在锁定期间的所有移动路径，而非仅仅是单一坐标点。

⑤ 设置锁屏留言与执行下发

如图 8-21 所示，您可以进一步强化保护：

锁屏信息自定义：开启【设置锁屏信息】开关。在文本框内输入联系方式或归还酬谢说明。

下发指令：确认所有配置后，点击底部的蓝色按钮【启用丢失模式】。

轨迹查看：开启后，您可点击“丢失轨迹追踪”旁的【查看】链接，回溯设备的移动历史。

⑥ 身份安全校验（第一重验证）

如图 8-22 所示，为了防止他人恶意操作，系统会触发身份验证。请在弹出的对话框中输入您 VEILORA OS 管理账号的登录密码，点击“确定”。

⑦ 目标设备锁屏密码二次验证（第二重验证）

为了确保指令的合法性与强制性，如图 8-23 所示，系统要求验证目标设备的底层锁屏密码：

双空间校验：在“主空间锁屏密码”栏输入该设备的解锁 PIN 码。若该设备设有隐私空间，需同时在下方输入对应的“隐私空间锁屏密码”。

指令生效：点击【验证】。验证通过后，远程指令将瞬间送达遗失终端，使其立即强制进入锁定状态，并显示您预设的留言信息。



图 8-17



图 8-18

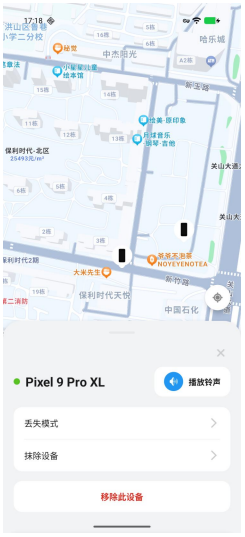


图 8-19

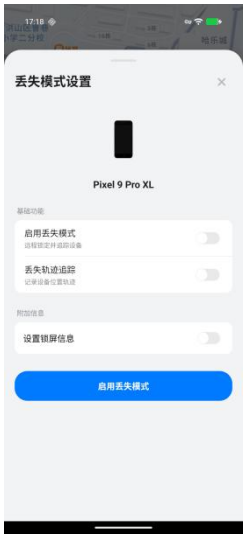


图 8-20



图 8-21

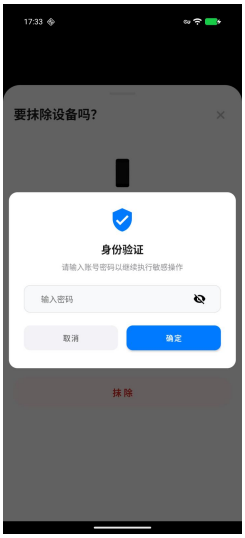


图 8-22



图 8-23

操作提示：一旦远程锁定成功，除非通过您预设的正确密码解锁，否则该设备将无法通过任何方式绕过锁定。如需解除锁定，在找回设备后输入新的本地锁屏密码即可。

8.3.2 远程还原

当您确认丢失的设备已无法取回，且其中含有极度敏感的数据时，通过此功能可以远程触发隐私空间的格式化指令。系统将强制还原隐私空间数据，保护您的隐私及数字资产不被非法获取、恶意利用。

① 进入设备管理入口

如图 8-24 所示，在另一台受信任的 VEILORA 设备上打开【设备管理】应用。在主界面的控制中心点击【我的设备】，查看当前账号关联的资产列表。



图 8-24

② 选择需要还原的目标终端

如图 8-25 所示，在设备列表中精准点击需要执行隐私空间还原的终端名称（例如：Pixel 9 Pro XL）。系统将进入该设备的远程实时监控界面。

③ 开启抹除操作选项

如图 8-26 所示，在设备详情页下方的操作菜单中，找到并点击【抹除设备】。此时系统会预先进行环境扫描，准备建立高权限的加密指令通道。

④ 确认抹除详情与风险告知

如图 8-27 所示，系统将弹出“要抹除设备吗？”的关键确认界面。在执行前，请务必知悉：

数据删除：指令一旦生效，远程设备将立即执行物理级的全盘擦除并恢复出厂设置，所有数据将永久消失，不可找回。

持续定位：抹除后，系统仍会尝试保留最后的定位上报能力，但由于应用环境已被重置，您将无法再次发起任何抹除指令。

执行操作：确认无误后，点击底部的红色文字【抹除】。

⑤ 身份与凭证安全双重校验

为确保该最高权限指令由机主本人发起，系统会执行多重身份核验（如图 8-28 所示）：

第一重： 输入您的 VEILORA OS 管理账号密码。

第二重： 根据系统提示验证本机的安全密语或锁屏密码。

指令下发： 验证通过后，点击【确定】。隐私空间还原指令将立即通过加

密隧道下发。一旦远程设备连接至任何网络，将无视一切状态，瞬间启动隐私空间及系统全盘数据的静默擦除流程。



图 8-25



图 8-26



图 8-27

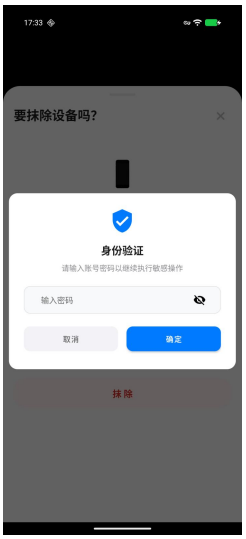


图 8-28

安全提醒：远程抹除操作是不可逆的。一旦执行，设备未备份的数据将无法恢复。建议您在日常使用中通过“云空间管理”功能定期备份重要数据到您的 WebDAV 空间，以便在更换新设备后快速恢复。