

我是一份机密档案。

从诞生起，我就由专人照料，生活在恒温恒湿的舒适环境中，任何人想见我都必须经过严格审批。就在我以为生活会一直这样平静美好下去时，一场突如其来的变故打破了这份宁静。我被列入了档案数字化清单，我很高兴能有这样难得的机会实现新的蜕变，却不知一场泄密危机悄然而至……



AI 生成

一天，管理员把我交给几个陌生人后，便匆匆离去。而后我和其他小伙伴被带到了一处陌生的房间。我悄悄打量周围，发现这个房间都是陌生的面孔，既没有平时的监控设施，也没有层层保密防护，这一切都让我陷入了深深的恐惧。不久，这群陌生人便对我进行了拍照、扫描，甚至将我的照片通过网络传输了出去。一套流程之后

他们将我和其他小伙伴们随意扔到了角落。

几日之后，这群陌生人离开了，我和小伙伴们也被打包带离了房间，我以为这惊悚的一切终于要结束了。没想到，我和小伙伴们竟然被送到了废品回收站！我被扔上了分拣传送带，正当我痛苦地闭上双眼准备认命的时候，一名细心的分拣员发现了我身上的“机密”印

一份机密档案的『历险记』

章！他连忙叫停了传输清理工作，拨打了 12339，国家安全机关的警察叔叔闻讯赶到现场，第一时间把我保护起来。

经过勘验，像我一样标有密级的小伙伴还有几百个！一旦被流散出去，这后果将不堪设想！后来，在警察叔叔们的交谈中，我才得知，负责此次档案数字化的公司根本就没有取得国家秘密载体印制资质，工作人员也未接受过正式的保密教育和资格审查便匆匆上岗。而负责保管我的部门对此次档案数字化工作疏于管理，既没有严格审查，也没有落实保密规定。

种种漏洞让我和小伙伴们险些落入泄密的深渊，还好有分拣员敏锐的安全意识和国家安全机关警察叔叔的迅速出击，才有力阻断了这场悲剧。

我想用这段惊险的经历告诉大家，我和我的小伙伴们不仅承载着国家过去的记忆，更是维护国家安全、保障国家发展的重要基石。对于我们的安全请大家务必慎之又慎，妥善管理，做到万无一失。

国家安全机关提示

一份机密档案的故事来自于真实案件，为我们敲响了警钟。档案数字化工作对档案管理部门提升管理效率、保障信息安全、促进资源共享具有重要意义。但在档案数字化过程中的泄密隐患不容忽视，需要严格落实保密规定，牢牢守住安全底线。

强化保密监管

对于涉密档案的数字化工作，应慎重选择具有涉密资质的外包企业开展工作，同时对外包企业进行严格审查，签订保密协议，明确保密责任。对参与数字化的工作人员要做好保密身份审核、登记工作。数字化加工场所须实行物理隔离、配备屏蔽设施、禁用无线设备，并安装无死角视频监控系统，确保档案数字化工作全过程可追溯。

规范成果管理

档案数字化工作中要做好交接手续，严格清点相关文件资料，确保不丢件、不错件。加工完成的数字化档案要认真整理、登记，采用符合安全管理要求的存储介质进行储存、备份。要建立系统完善的后台管理机制，对数字化资料的使用和流转进行严格限制，做到有据可查，防止因管理不善导致泄密。

开展教育培训

必须加强对档案数字化工作人员的安全保密教育和技能培训，通过案例剖析、法规解读、实操演练等，让工作人员深知泄密危害与防范要点，并定期开展考核与复训，促使相关单位及个人树牢国家安全意识，守住保密防范底线。

守护“随身而行”的安全

在数字化时代的今天，智能手表、智能手环、智能眼镜等智能穿戴设备，以其便捷性、功能多样性在社会面迅速普及，它们不仅可以记录健康数据、提供导航服务，还能实现远程通信和信息推送。但这些便利功能的背后，却存有一定的泄密风险，需要我们加以防范。

多维记录的泄密隐患

智能穿戴设备通常内置了摄像头和麦克风并自带定位功能等，可获取用户的指纹、虹膜、面部信息等生物特征，能实时记录用户脉搏、血压等健康数据和用户的行为状态与活动轨迹，对用户进行精准人物画像，若此类数据不慎泄露，可能引发安全问题。

数据关联的云端黑洞

智能穿戴设备在使用中可能会与社交软件、支付软件等各类应用

程序关联，相关数据会自动同步到云端服务器。但云存储在安全保密领域存在一定局限性，一旦账号被破解或服务商自身存在系统漏洞，又或者遭受境外间谍情报机关的攻击，则可能导致存储在云端的信息泄露或被恶意利用。

不易察觉的“特洛伊木马”

相较于其他智能终端，部分智能穿戴设备系统相对不够完善。有报道指出，部分智能穿戴设备存在第三方程序违规获取权限、系统更新滞后等情况，若黑客利用此类安全漏洞植入木马程序，可能导致数据被违规收集、个人隐私泄露、设备被远程控制等安全问题。

跨越物理隔离的“数据虫洞”

智能穿戴设备通常通过蓝牙、Wi-Fi等方式与手机或其他设备连接，有的设备具备“自组网”特性，可

在无基站情况下实现多终端互联，形成独立通信网络，可绕过涉密网络的物理隔离屏障。若黑客通过植入木马的智能穿戴设备组建临时局域网，将其他设备的信息数据经蓝牙逐级跳传至外部设备，可能会造成失泄密隐患。

国家安全机关提示

一块手表、一枚手环，或许就是守护国家安全的“第一道闸门”，我们在享受科技便利的同时，更要守护好个人隐私和国家秘密，谨防智能穿戴设备失泄密，共同守护智能时代的国家安全。

规划使用禁区

严禁在涉密场所使用智能穿戴设备，禁止将智能穿戴设备与涉密信息系统连接。涉密场所的入口处、办公区域等显著位置建议设置警示标识，

并配备专门的电磁隔离保管箱，对进入涉密场所人员的电子设备进行集中保管，从源头上避免失泄密隐患。

加强自用管理

用户应选择正规渠道购买产品，及时更新设备的系统和应用程序；合理设置设备权限，谨慎授权第三方应用，关闭位置定位分享、麦克风等非必要功能；不存储敏感信息，警惕陌生链接和可疑应用程序，尽量避免连接公共网络，定期对设备进行杀毒和数据清查。国家安全，人人有责。广大公民在购买、使用智能穿戴设备中如发现疑似网络间谍行为，请及时通过 12339 国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或直接向当地国家安全机关进行举报。

（均转自国家安全部微信公号）