微信泄密又出新案例：赶紧筛查工作群

2022-02-22保密服务

近年来，因微信办公而导致的失泄密案件多发，特别是一些涉密信息在工作群、同学群、老乡群等微信群内发送引发的泄密案件，导致涉密信息迅速传播，给国家秘密安全带来极大危害。
机关、单位虽然采取了一些保密措施，但微信群发泄密案件依然频发，屡禁不止，需要引起高度重视。
**典型案例**
**1.工作群下达紧急任务**
某市市委组织部工作人员曾某，收到上级单位下发的一份秘密级文件，要求紧急传达落实。因需要阅办的领导外出不在，曾某为尽快将文件传达到位，遮盖文件密级标志进行扫描，将电子版发送至单位微信工作群，造成泄密。



“保密观”有话说：100-1=0

任何情况下，以泄露国家秘密为代价推进业务工作都是万万要不得的。如果业务工作是100分，保密工作是1分，那么100减1并不等于99，而只能是0。
**2.同学群炫耀政策密件**
某市市委办公厅领导许某因家中有事，将收到的一份秘密级、一份机密级密码电报放在办公桌上离开。工作人员安某给领导报件时看到桌上的涉密文件，翻阅后发现其中内容涉及某行业领域重大调整，出于炫耀心理，安某用手机拍摄发送到自己的微信大学同学群，造成泄密。


“保密观”有话说：严控泄密源头，筑牢保密防线

涉密文件在传递、收发、保管、阅办、销毁等任何环节，保密管理松一分，泄密风险隐患就会增十分。
**3.老乡群扩散密码电报**
某自治区某县金某在工作中私自拍摄一份机密级密码电报复印件，并存储在手机中，后发送给邹某，并特别叮嘱“密电不得外传”，但邹某却将图片制成文档格式，转发给了马某，马某又发送到自己的微信老乡群，造成泄密。



“保密观”有话说：一粒泄密种子，一片灾难森林

“口头叮嘱”往往是给自己的心理安慰，起不到保护涉密文件的作用，更无法阻止涉密文件不被外传。保密这件事，不能把责任和信任寄托在他人身上，最稳妥的做法是自己不违规，关紧泄密的闸门。
**对策建议**
针对这些典型的微信群发泄密案例，机关、单位应从以下三个方面加强保密管理，防范微信办公泄密情况的发生。
1.开展专项保密教育
机关、单位要开展专项保密教育，普及信息与网络管理保密知识技能，让干部职工普遍认识到微信办公的风险隐患，不仅做到自己不使用微信传密，发现此类情况还要及时报告。



2.严格落实管理要求
微信工作群应指定专人作为管理员，做好保密管理，交流内容严格限定为周知性的一般信息，禁止传播国家秘密、工作秘密、商业秘密以及个人信息。此外，机关、单位要将涉密载体流程管理与智能手机使用管理结合起来，从源头上消除涉密文件数字化的隐患。
3.强化保密检查监督
机关、单位应对微信工作群进行重点筛查，发现问题及时纠正并立刻向本单位保密工作机构报告。保密工作机构要采取措施防止信息扩散，并立即向同级保密行政管理部门报告。