防止機關洩密事件預警作為小叮嚀

	態樣	風險違失	策進建議
1	監視器影像之管理、調閱流程、保密措施。	1.管理權責不清，多人同時知悉帳號、密碼。 2.管理、調閱流程、保密措施等，皆無具體因應措施。	1.訂定監錄系統資料之調閱流程、保密措施等規管措施。 2.建置監錄系統資料調閱申請單。 3.定期召開監視器影像管理檢討會議。
2	知悉本市確診者足跡及消毒資訊。	於本府公布前洩漏確診者足跡及消毒資訊。	1.有關疫情相關資訊，請以指揮中心公布為主，切勿以訛傳訛。 2.接獲來源不明的訊息時，可透過疾管署全球資訊網、疾管家Line官方帳號、疾管署臉書專頁等管道查證最新疫情資訊。
3	以即時通訊軟體（如 LINE、Facebook、Messenger、WeChat 等）處理公務。	1.即時通訊軟體帳號被盜、洩密、誤傳訊息。 2.即時通訊軟體無法加密訊息。	1.應盡量避免使用即時通訊軟體傳送隱私、機敏資料。 2.加裝及定時更新防毒防駭軟體。
4	受理民眾陳情、檢舉、申請等，可能因此取得民眾之陳情書及相關個人資料。	未妥善保管並洩露民眾之陳情書或個人資料。	1.訂定相關個人資料管理機制，以符合個人資料保護法。 2.必要時，民眾之個人資料予以去識別化。
5	考績委員知悉機關同仁之考績。	考績委員洩漏機關同仁之考績	提醒考績委員嚴守保密規定。

	態樣	風險違失	小叮嚀
6	將可攜式設備或媒體（如筆記型電腦、行動硬碟、隨身碟等）攜出辦公室處理公務。	公務機密外洩。	非因公務需要並經主管核准，不得攜出辦公處所，攜回時應進行掃毒或系統還原
7	使用公務電腦處理公務。	1. 個人電腦之使用者識別碼及密碼，未妥善保存、交付他人使用、未定期更換。 2. 非經核准擅自下載軟體或變更硬體規格。 3. 機敏資料存放於對外開放之資訊系統中。	1. 避免開啟來路不明的電子郵件及檔案，或瀏覽非法或機關所限制之網站。 2. 重要機敏檔案之備份媒體，嚴密管制或由專人管制。 3. 禁止下載安裝或使用未經授權來路不明之軟體。 4. 遇有資安異常事件發生，即時向資訊單位反映處理。 5. 落實機關資訊安全稽核。
8	列印或傳真機敏文件。	機敏資料外洩。	1. 立即領取列印出之機敏文件。 2. 廢棄之機敏文件應立即以碎紙機銷毀，並達到無法辨識之程度。 3. 傳真機敏文件時，傳真人及接收人應全程在場、核對張數，嚴禁使用自動傳真。
9	機關辦理採購。	1. 洩漏應保密之廠商投標文件。 2. 機關於決標前公布底價。 3. 於宣布保留決標前先行公布底價。	遵守政府採購法第 34 條之規定。