著作權集體管理團體個人資料檔案安全維護管理辦法草案

條　　文	說　　明
第一條　本辦法依個人資料保護法(以下簡稱本法)第二十七條第三項規定訂定之。	明定本辦法訂定之授權依據。
第二條　著作權集體管理團體(以下簡稱集管團體)保有個人資料檔案者，應依其業務規模，配置管理之人員，規劃、訂定、修正與執行其個人資料檔案安全維護計畫(以下簡稱本計畫)。 集管團體應於本辦法發布施行之日起六個月內完成本計畫之訂定。	一、配合個人資料保護法(以下簡稱本法)第二十七條及其施行細則第十二條規定，集管團體為防止所管理之個人資料被竊取、竄改、毀損、滅失或洩漏，應考量業務規模，配置管理之人員，規劃、訂定、修正與執行個人資料檔案安全維護計畫，爰於第一項明定。 二、考量集管團體訂定個人資料檔案安全維護計畫需一定時間，爰於第二項規定集管團體應完成個人資料檔案安全維護計畫之期限，使集管團體於本辦法發布後有時間因應訂定。 三、本辦法所稱個人資料係指依本法第二條第一款、第二款所稱個人資料及個人資料檔案。
第三條　本計畫應納入符合第四條至第十條規定之具體內容，適時清查其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及處理個人資料作業流程說明文件。 集管團體應訂定本計畫之稽核機制，定期或不定期檢查本計畫執行狀況，以確保本計畫之落實。 集管團體應隨時檢視所適用之個人資料保護法令及社會環境之變動，以持續改善本計畫。	一、配合本法施行細則第十二條第二項規定，應定期清查所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，並作為建立個人資料檔案清冊及處理個人資料作業流程之依據，爰於第一項規定。 二、配合本法施行細則第十二條第二項第九款規定，集管團體應於本計畫中，訂定稽核機制，定期或不定期檢查本計畫執行狀況，以確保本計畫之落實，爰於第二項規定。 三、配合本法施行細則第十二條第二項第十一款規定，集管團體應於本計畫中，訂定個人資料安全維護之整體持續改善機制，另配合應適用之

	各種法令的調整及社會環境的變動，應適時改善本計畫，爰於第三項規定。
第四條　集管團體應適時評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定個人資料被竊取、竄改、毀損、滅失或洩漏等事故發生後之應變機制，其內容應對下列事項為具體規定： 一、採取之應變措施，包括降低及控制當事人損害之方式。 二、查明事故發生原因及損害狀況，以適當方式通知當事人，並通報相關機關。 三、研議其改善措施之機制。 集管團體遇有個人資料安全事故，將危及其正常營運或大量當事人權益者，應於發現事故後七十二小時內填列個人資料侵害事故通報與紀錄表(如附件)通報著作權專責機關。 著作權專責機關接受前項通報後，得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。	一、配合本法施行細則第十二條第二項第三款及第四款規定，集管團體應以所管理之個人資料範圍及其相關業務流程為依據，評估個人資料可能面臨之風險及其發生可能性，並根據風險評估結果，訂定相關因應機制及其必要作為，以降低或控制因個人資料被竊取、竄改、毀損、滅失或洩漏等事故發生後造成財產及非財產上之損害，爰於第一項規定。 二、集管團體遇有個人資料安全事故，將危及其正常營運或大量當事人權益者，應於發現事故後七十二小時內填列個人資料侵害事故通報與紀錄表通報著作權專責機關，通報項目包括團體名稱、事件發生時間、事件發生種類、發生原因及事件摘要、損害狀況、個資侵害可能結果、擬採取之應變措施、擬採通知當事人之時間及方式、是否於發現個資外洩後七十二小時內通報等事項，爰於第二項規定。 三、著作權專責機關於接獲集管團體個資侵害事故通報後，為瞭解該事故狀況及集管團體相關因應措施，得依本法第二十二條至第二十五條規定為後續之行政檢查，包括派員檢查、命為提供資料或說明、扣留或複製得沒入或可為證據之個資或其檔案；集管團體若有違反本法者，得命其禁止蒐集、處理、利用個資、刪除經處理之個資檔案、沒入或銷燬違法蒐集之個資、公布集管團體違法情形及董事長等相關監督管理措施，爰於第三項規定。
第五條　除法律另有規定外，集管團體應就下列個人資料蒐集、處理或利用事項	配合本法施行細則第十二條第二項第五款規定，集管團體應於本計畫中，訂定個人

訂定具體程序或機制： 一、檢視個人資料之蒐集、處理、利用與本法第五條、第六條、第八條、第九條、第十九條第一項及第二十條第一項之規定相符；依當事人同意而為特定目的外利用者，應確認已符合本法第七條第二項規定。 二、檢視個人資料是否正確，正確性有爭議者，應視情形分別依本法第十一條第一項、第二項及第五項之規定辦理。 三、對個人資料進行國際傳輸前，應檢視著作權專責機關有無依本法第二十一條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方為預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象、方式及當事人行使本法第三條所定權利之相關事項等事項之監督。 四、於特定目的消失、期限屆滿或有違反本法其他規定而為個人資料之蒐集、處理或利用時，應主動或依當事人之請求，刪除或停止蒐集、處理、利用個人資料。 五、委託他人蒐集、處理或利用個人資料之全部或一部時，應有選任受託人之標準及評估機制，且應於委託契約或相關文件明確約定適當之監督方式，並確實執行。 六、當事人行使本法第三條所定之權利，應注意之相關事項： (一)當事人身分之確認。 (二)提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。	資料蒐集、處理及利用之內部管理程序，以確保個人資料之蒐集、處理或利用，符合個人資料保護相關法令之規定： 一、於第一款明定集管團體就個人資料之蒐集、處理或利用，須符合本法第五條規定之目的、第六條特種個資之規定、第八條與第九條規定之告知義務、第十九條第一項規定之特定目的利用、第二十條第一項但書規定之特定目的外利用及第七條規定之同意。 二、集管團體應確保所蒐集之個人資料之正確性，如正確性有爭議時，爰於第二款明定須依本法第十一條第一項、第二項及第五項之規定處理，以維護當事人之權益。 三、按本法第二十一條規定:「非公務機關為國際傳輸個人資料，有涉及國家重大利益、國際條約或協定有特別規定、接受國對於個人資料之保護未有完善法規致有損害當事人權益之虞及以迂迴方法向第三國(地區)傳輸個人資料規避本法者，中央目的事業主管機關得限制之。」準此，集管團體將個人資料作跨國(境)之處理或利用時，應不得對於我國人民隱私產生重大影響，或有危及國家安全之疑慮，爰於第三款明定集管團體應遵守著作權專責機關依本法第二十一條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方為預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象、方式及當事人行使本法第三條所定權利之相關事項等事項之監督，以保障當事人權益。 四、於第四款明定集管團體應依本法第十一條第三項及第四項規定，應主動或依當事人之請求，刪除或停止蒐集、

（三）對當事人請求之審查方式，並遵守本法第十三條有關處理期限之規定。 （四）有本法第十條及第十一條所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。	處理、利用個人資料之事由，以維護當事人之權益。 五、集管團體如須委託他人蒐集、處理或利用個人資料之全部或一部者，因涉及當事人之權益，爰於第五款明定相關之標準、機制及監督方式，據以執行之。 六、按本法第三條規定，當事人就其個人資料得行使之權利包括查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及請求刪除等，爰於第六款明定當事人行使上述權利時應注意之相關事項。
第六條　集管團體應考量業務性質、個人資料存取環境、個人資料傳輸之工具與方法及個人資料之種類、數量等因素，採取適當之資訊安全、作業安全及設備安全之管理措施。	配合本法施行細則第十二條第二項第六款至第八款規定，集管團體保有個人資料檔案者，應於本計畫中，訂定適當之資訊安全、作業安全及設備安全管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
第七條　前條所定資訊安全管理措施之執行，應包括下列事項： 一、個人資料有加密之必要者，應於蒐集、處理時，採取適當之加密措施。 二、個人資料有備份之必要者，應對備份資料採取適當之保護措施。 三、傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。 四、設定個人資料之存取權限，建立蒐集、處理或利用個人資料之電腦、相關設備或系統必要之控管機制，並定期確認其有效性。 五、建立因應惡意程式及系統漏洞所造成威脅之安全機制，並定期確認蒐集、處理或利用個人資料之電腦、相關設備或系統安全機制之有效性。 六、進行軟硬體測試時，應建立個人	集管團體保有個人資料檔案者，應於本計畫中，訂定適當之資訊安全管理措施，說明如下： 一、個人資料檔案經風險評估有加密之必要時，集管團體應依蒐集、處理或利用等各種行為態樣，採取適當之加密措施，爰於第一款規定。 二、依本法施行細則第十二條第二項第五款規定，本法第二條第二款所定個人資料檔案，包括備份檔案。準此，個人資料檔案經風險評估有備份之必要時，集管團體亦應針對複製、備份之個人資料檔案，採取適當之保護措施，爰於第二款規定。 三、集管團體傳輸個人資料時，應依不同傳輸方式及其風險評估結果，採取適當之安全措施，爰於第三款規定。 四、集管團體於蒐集、處理或利用個人資料時，應採取適當的安全機制，例如

資料防護機制，如確有使用個人資料之必要時，應明確規定其使用之程序及安全管理方式。 七、定期檢視處理個人資料之資訊系統，檢查其使用狀況及存取個人資料之情形。	何人可接觸所管理的個人資料，以防止該等電腦、相關設備或系統遭受無權限人之存取，爰於第四款規定。 五、集管團體應定期確認蒐集、處理或利用個人資料之電腦、相關設備或系統已具備必要之安全性，例如防火牆、防毒程式與作業系統是否已更新至最新或修補相關程式，以防止惡意程式及系統漏洞所造成之威脅，爰於第五款規定。 六、集管團體於測試軟硬體之功能時，為確保個人資料不因該等功能而致被竊取、竄改、毀損、滅失或洩漏，應避免使用真實之資料，如須使用真實資料者，亦應明確訂定使用的程序與安全管理方式，爰於第六款規定。 七、集管團體為避免所管理之個人資料被竊取、竄改、毀損、滅失或洩漏，應定期檢查處理個人資料資訊系統之使用狀況及存取個人資料之情形，爰於第七款規定。
第八條　第六條所定作業安全管理措施之執行，應包括下列事項： 一、與所屬人員約定保密義務。 二、對業務內容涉及個人資料蒐集、處理或利用之所屬人員，定期實施個人資料保護與管理認知宣導及教育訓練。 三、依業務特性、內容及需求，設定所屬人員接觸個人資料之權限。 四、所屬人員離職後，應將其執行業務所持有之個人資料辦理交接，不得私自持有或繼續使用，並取消其存取權限。	集管團體保有個人資料檔案者，應於本計畫中，訂定適當之作業安全管理措施，說明如下： 一、為確保所屬人員履行人員管理相關措施，約定其保密義務，爰於第一款規定。 二、實施認知宣導及教育訓練，使所屬人員均能明瞭個人資料保護相關法令之要求、其所負擔之責任範圍及個人資料檔案安全維護計畫中各項管理程序、機制及措施之要求，爰於第二款規定。 三、為控管所屬人員接觸個人資料之權限，集管團體應檢視業務內容涉及個人資料蒐集、處理或利用人員，考量其業務之特性、內容及需求，應設定所屬人員接觸個人資料之權限，爰於第

	三款規定。 四、為防止因所屬人員離職而導致個人資料被竊取、竄改、毀損、滅失或洩漏，集管團體應要求該人員交接個人資料之載體，並不得私自持有因執行業務而持有之個人資料，及取消該離職人員存取個人資料之權限，爰於第四款規定。
第九條　第六條所定設備安全管理措施之執行，應包括下列事項： 一、依電腦、自動化機器或其他儲存媒介物之特性及使用方式，建置適當之保護設備或技術。 二、所屬人員應妥善保管個人資料之媒介物。 三、針對存放儲存媒介物之環境，施以適當之進出管制措施。	集管團體保有個人資料檔案者，應於本計畫中，訂定適當之設備安全管理措施，說明如下： 一、於第一款明定依儲存媒介物之特性及使用方法，建置適當的保護設備或技術，例如建置防火牆、安裝防毒軟體及定期安裝作業系統之修補程式等。 二、於第二款明定所屬人員應妥善保管個人資料之媒介物，例如將其放置於可上鎖之抽屜或其他存放場所。 三、於第三款明定針對存放儲存媒介物之環境，施以適當之進出管制措施，例如有權進出該等存放儲存媒介物場所人員，須以帳號密碼等管控措施，進出該等場所。
第十條　集管團體執行本計畫時，應評估其必要性，保存下列紀錄： 一、個人資料之蒐集、處理及利用紀錄。 二、自動化機器設備之軌跡資料。 三、其他落實執行本計畫之證據。 集管團體於業務終止後，其保有之個人資料應依下列方式處理及記錄： 一、刪除、停止處理或利用個人資料者，記錄其方法、時間、地點及證明方式。 二、移轉者，記錄其原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。	一、集管團體執行本計畫時或業務終止後，應保存相關紀錄，以避免不必要之爭議。 二、配合本法施行細則第十二條第二項第十款規定，集管團體應於本計畫中，訂定相關使用紀錄、軌跡資料及證據保存機制，妥善保存個人資料之蒐集、處理及利用紀錄、自動化機器設備之軌跡資料及落實本計畫之證據等，爰於第一項規定。 三、集管團體業務終止後，其個人資料如因此刪除、停止處理或利用者，應留存相關紀錄;如移轉予他人者，應記錄其原因、對象、方法、時間、地點及受移轉對象得蒐集該個人資料之合

	法依據，爰於第二項規定。本項所稱業務終止，係指著作權專責機關依著作權集體管理團體條例第四十八條規定命令集管團體解散，或集管團體依其章程規定關於解散之決定，併此說明。
第十一條　本辦法自發布日施行。	本辦法之施行日期。

附件：

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>集管團體名稱：

通報機關：</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　簽名(蓋章)
職稱：
電話：
Emial：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個資_____筆
□特種個資_____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採取通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後 72 小時內通報</td><td colspan="2">□是
□否，理由：</td></tr>
</table>