台灣金山電子工業股份有限公司
資訊安全風險管理辦法

壹、目的

為保護集團公司營運所使用的各類資訊資產安全,使資訊資產在遭受外在威脅或內部作業以及人員不當的管理下仍能維持在正常運作,並確保資訊資產的機密性、完整性及可用性。

貳、適用範圍

以與集團公司營運所使用的相關資訊資產為主要保護的對象,包括人員、資料、資訊實體環境和軟硬體設施。

參、作業權責單位

資訊處（IT）及所屬各部成員。

肆、作業辦法

1、 人員管理及資訊安全教育訓練

1-1、對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。各業務主管人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

1-2、針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升資訊安全水準。

2、 系統發展及維護安全管理

2-1、自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本 異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

2-2、對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

2-3、委託廠商建置及維護重要之軟硬體設施，應在本公司相關人員監督及陪同下始得為之。

3、 資料異地備份管理

3-1、為了公司的數據安全，通過資料異地備份管理機制可以實現對系統異常，資料庫異常的一種容災方案。當異常或者災難發生後能及時恢復到正常狀態，使公司的損失降到最低。

3-2、備份方法

3-2-1、數據備份平台操作。公司內部在備份服務器部署了賽門鐵克公司的 NBU 備份平台。NBU 備份系統的所有操作均需要在 netbackup 管理控制台上完成。首先打開管理控制台,然後新建備份項目的策略，但在新建策略前，需要先規劃 NBU 客戶機的名稱，備份策略名，對備份日期/時間和保留做合理安排（避

免沖突）。方法：在 netbackup 管理控制台上点击 netbackup manager—policy，在出现的 all polices 框中的空白处点击右键，选择 new policy（也可通过复制一个已存在的 policy 来创建一个新的 policy）。

一個新的備份項目按照下列參數的順序進行配置。

Attributes
Schedules
Clients
Backup selections

另外對 NBU 服務器上還需要編輯/etc/hosts 文件，確定 NBU 客戶機名—ip 相對應。

3-2-2、備份客戶端操作。對客戶機需要進行備份的檔案以及資料，都需要通過安裝 NBU agent 實行備份作業。並在客戶機添加 NBU 服務端的 hosts 文件添加主機名—IP 對應關系。

3-2-3、在公司外部設置異地存儲服務器，每天定時複製公司內部備份服務器上的備份數據透過網路傳輸存放於異地存儲服務器，以達資料異地備份保存管理。

3-3、備份數據管理

3-3-1、對於需要備份的數據如（ERP、條碼、SPC、流程簽核、電子郵件、用戶資料）等都是通過 NBU 平台備份策略自動實現異機備份。並且備份內容都存放在非系統盤內，並有明顯的備份標識以及明確的備份位置。

3-3-2、備份的文件以及備份日志在每天都有信息管理人員進行檢查維護。發生異常情況時及時向資訊主管報告並妥善處理解決。

3-4、備份數據恢復

3-4-1、系統管理員對 NBU 平台備份的數據進行核查。當系統發生故障，檔案數據被破壞、遺失的情況，及時努力進行數據恢復以減小損失。

3-4-2、根據需要做數據恢復的，都需部門主管、資訊主管或上級主管領導簽字確認後，才能開始做恢復工作。同時需確保恢復數據的有效性。如遇恢復錯誤或技術無法實現，必須保護好數據源，及時上報提出數據恢復方案，絕對不允許人為原因造成數據二次污染。

3-5、權限與職責

3-5-1、系統管理員負責公司數據備份的管理，包括數據備份檢查、故障處理以及數據恢復等。

3-5-2、因可控的人為原因造成重要檔案資料數據丟失的，公司將對當事人進行嚴厲處罰。

4、 所有集團公司所屬的電腦相關設備均需加入網域，並且均需安裝公司指定之防毒軟體，若有特殊需求則需專案申請處理。

5、 未經資訊單位同意或是不明的資訊相關設備，不得私自接入公司內部網路

環境，包含有線和無線的資訊設備。

6、 私人資訊設備欲攜帶至集團公司使用，除需經過總經理核准外，並且需比照公司電腦設備管理規範設置。

7、 在公司外部需連線回集團公司處理相關事務時，必須提前申請 VPN 帳號密碼後，才能在公司外部以 VPN 進行連線，進而使用集團公司的資訊系統資源。

8、 資訊硬體設備之管控：

8-1、隨身碟(U 盤)、移動硬碟之管控：

8-1-1、在集團公司區域使用的隨身碟(U 盤)或移動硬碟存儲設備統一由資訊單位進行保管和管理，而經過申請使用之隨身碟(U 盤)或移動硬碟存儲設備，則依申請主管之管制方式進行管控。

8-1-2、當需求單位需使用隨身碟(U 盤)或移動硬碟存儲設備時，需向資訊單位提出需求，經資訊單位最高主管同意後方可領用，使用後須按時歸還給資訊單位保管。

8-1-3、在使用部門歸還隨身碟(U 盤)或移動硬碟存儲設備時，資訊單位管理人員必須先進行查殺病毒操作，並且刪除隨身碟(U 盤)或移動硬碟存儲設備內之所有儲存資訊，以確保隨身碟(U 盤)和移動硬碟存儲設備無任何資訊內容。

8-1-4、隨身碟(U 盤)和移動硬碟設備由資訊單位保管，使用範圍以集團公司區域內使用，借用人若有特殊事由需帶出集團公司以外使用，需經借用單位主管以及資訊單位主管核準後，才可攜帶出集團公司使用，如違反規定將按照人事制度進行懲處。

8-1-5、集團公司相關單位因工作關係需長期使用隨身碟(U 盤)或移動硬碟時，需經該單位最高主管和資訊單位最高主管同意後，由資訊單位編號列管後發給使用單位使用。

8-1-6、使用隨身碟(U 盤)或移動硬碟設備應善盡保管義務，若因個人使用因素出現故障異常，則應負起維修或賠償之責任。

8-2、數碼相機或 DV 以及記憶卡之管控：

8-2-1、使用數碼相機或 DV 或記憶卡之存儲內容應以集團公司公務需求為原則，若因私人借用則需經該部門最高主管同意，才可因私使用。

8-2-2、各部門購置之數碼相機或 DV 或記憶卡，由各部門主管指定專職管理人員進行管控，若需攜出集團公司外部使用，則需經該部門最高主管和資訊最高單位主管同意，才可攜出廠外使用。

8-2-3、由於數碼相機或 DV 都是公司高單價之資產，應以共用為原則。

8-3、筆記型電腦之管控：

8-3-1、在集團公司使用之筆記型電腦必需經由資訊單位依照辦公電腦標準安裝相關辦公軟體，不得私自安裝未經授權之軟體，如違反規定將按照人事制度進行懲處，並且自負侵害授權軟體之賠償責任。

8-3-2、各部門保管之共用筆記型電腦，需由各部門主管指定專職管理人員進行管控，若需攜出集團公司外部使用，則需經該部門最高主管和資訊單位最高主管同意，才可攜出集團公司外部使用。

8-3-3、資訊單位應準備公用筆記型電腦，並安裝辦公電腦常用之應用軟體，以供各相關部門因公務需求時短期借用。

8-3-4、各部門借用筆記型電腦之順序以提前預約和先到先借用為原則。

8-3-5、各部門因公務工作之原因而需使用筆記型電腦時，可到資訊單位登記後領用，借用人應善盡設備保管責任，若因個人使用因素出現故障異常，則應負起維修或賠償之責任。

9、 資訊軟體之管控：

9-1、隨身碟(U 盤)、移動硬碟之管控：

9-1-1、一般使用人員設定無任何 USB 之使用權限。

9-1-2、各部門助理和課級以上人員之權限設定為唯讀權限，僅可讀取 USB 設備之檔案，如從數位相機等設備下載資訊。

9-1-3、處級以上人員則設定為完整存取權。

9-1-4、當需求單位對 USB 設備有長期存取需求時，需經該部門主管同意後，再向資訊單位提出申請，經資訊單位最高主管核準設定後才可正常使用。

9-2、Line 、Wechat 等 IM 軟體之管控：

9-2-1、一般使用人員設定無任何使用權限。

9-2-2、課級以上人員設定為可使用文字訊息，但不能直接在 IM 相關軟體中傳輸檔案。

9-2-3、處級以上人員設定為完整存取權，包含可上傳資料到網頁。

9-2-4、因專案或特殊需求需在電腦使用 IM 等相關軟體時，需經該部門主管同意後，再向資訊單位提出申請，經資訊單位最高主管核準設定後才可正常使用。

9-3、外部網頁瀏覽之管控：

9-3-1、一般使用人員設定無任何使用權限。

9-3-2、課級以上人員設定為網頁瀏覽權限，但不能直接在網頁相關軟體中傳輸檔案。

9-3-3、處級以上人員設定為完整存取權，包含可上傳資料到雲端。

9-3-4、因專案或特殊需求需在電腦使用外部網頁等相關軟體時，需經該部門主管同意後，再向資訊單位提出申請，經資訊單位最高主管核準設定後才可正常使用。

9-4、外部網頁 Mail 之管控：

9-4-1、一般使用人員設定無任何使用權限。

9-4-2、處級以上人員設定為完整存取，可使用公司以外之網頁郵件系統。

9-4-3、因專案或特殊需求需在電腦使用外部網頁 Mail 等相關軟體

時，需經該部門主管同意後，再向資訊單位提出申請，經資訊單位最高主管核準設定後才可正常使用。