附錄五、網站安全政策範例

「○○網站」(以下簡稱本網站）為保障您及本網站的資料安全，特別依照「個人資料保護法」之精神，擬定以下網站安全政策，以說明本網站在資訊安全方面的作法。

一、 政策適用範圍：

以下的網站安全政策，適用於您在本網站瀏覽時，所涉及的個人資料蒐集、運用與保護，但不適用於在本網站置設之其他網站之連結，當您點選連結至其他網站時，適用各該網站的網站安全政策。

二、 資訊存取控制

- 訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。
- 離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
- 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過六個月為原則。
- 對系統服務廠商以遠端登入方式進行系統維修者，加強安全控管，並建立人員名冊，課其相關安全保密責任。
- 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

三、 網站安全措施與規範

任何未經授權而企圖上載或更改本單位所提供的各項服務及相關資訊的行為，都是嚴厲禁止而且可能觸犯法律。為了網站安全的目的和確保這項服務能夠繼續服務所有的網路使用者，本網站提供了以下的安全保護措施：

- 與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。
- 使用網路入侵偵測系統，監控網路流量，以確認未經授權而企圖上載或更改、網頁資訊或蓄意破壞者。
- 裝設掃毒軟體，定期掃毒，以提供使用者更安全的網頁瀏覽環

境。

- 建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以備發生災害或儲存媒體失效時，可迅速回復正常作業。
- 不定期摹擬駭客攻擊，演練發生安全事件時的系統回復程序，並提供適當的安全防禦等級。
- 機密性及敏感性的資料或文件，不存放在對外開放的資訊系統中，機密性文件不以電子郵件傳送。
- 自動接收所有來自相關作業系統廠商或應用程式廠商所寄發的安全維護電子信通知，並依照電子信的建議，安裝適當的修補程式（Patch）。
- 網際網路資料的傳輸不能保證百分之百的安全，本網站將努力保護本網站及您個人資料的安全，部分情況下會使用通行標準的 SSL 保全系統，保障資料傳送的安全性。但由於資料傳輸過程牽涉您上網環境保全之良窳，我們並無法確保您傳送或接收本網站資料的安全，您須注意並承擔網路資料傳輸之風險。請您諒解此部份所造成的後果均非本網站所能控制範圍。

四、 防火牆之安全管理

- 防火牆具備網路服務的轉送伺服器（如代理伺服器（Proxy Server）等）以提供 Telnet、FTP、 WWW 等網路服務的轉送與控管。
- 防火牆係本單位整個網路之樞紐，對於防火牆主機及軟體，均應預留一套備份，以備不時之需。
- 本單位防火牆系統平時記錄整個網路之活動事件，記錄檔之資料至少應包括事件之日期、時間、起訖 IP、通訊協定等項目，以便於平時之管理及日後之稽核作業。
- 本單位防火牆之記錄檔（log）由防火牆管理人員檢視分析有無異常狀況；記錄檔並應保存一年以上。
- 本單位防火牆主機只能由系統終端機登入，不得以其他任何方式登入，以確保防火牆主機安全。
- 本單位防火牆之安全控管設定應經常檢討，並作必要之調整，以確定發揮應有的安全控管目標。
- 本單位防火牆系統定期作好資料備份，且只能做單機備份，不

可採用網路等其他方式備份資料。

- 本單位防火牆系統軟體，經常更新版本，以因應各種網路攻擊。

五、 資料備份作業原則

- 重要資料的備份，以維持至少三代為原則。
- 備份資料有適當的實體及環境保護，其安全標準應儘可能與主要作業場所的安全標準相同；主要作業場所對電腦媒體的安控措施，應儘可能適用到備援作業場所。
- 定期測試備份資料，以確保備份資料之可用性。

六、 資料回復作業原則

- 資料回復作業時，先檢查資料之一致性與完整性。
- 網站資料回復，除突發重大事件，主機機房或網路運作無法回復等因素外，資料能於 24 小時內回復正常，並保障備份資料能保持兩日以內之最新完整資料，資料回復後，程式及資料庫均能立刻正常啟用運作。
- 應定期測試備份資料，以確保備份資料之可用性。
- 資料回復作業完成後，相關單位人員應持續觀察三日，以確保系統運作正常，新增之資料正確無誤。

七、 本網站資安政策的修改由於科技發展的迅速，相關法規訂定未臻完備前，以及未來可能難以預見的環境變遷等因素，本網站將會視需要修改網站上所提供的資安政策的說明，以落實保障網路安全的立意。當本網站完成資安政策的修改時，我們會立即將其刊登於本網站上，並以醒目標示提醒您前往點選閱讀。

八、 如果您對以上條款有任何疑問或意見，歡迎透過本網站所示之聯絡方式與我們聯絡。