台灣卜蜂企業股份有限公司

壹、資訊安全風險管理架構

針對公司集團內部建立資訊安全制度與資訊管理機制，確保公司營運不中斷為目標，並確保無損害客戶、廠商及員工資料之事件。

壹、資訊安全風險管理架構

建立企業資訊安全風險管理方法，以確保資訊安全事件發生時的處理狀況以及回報機制說明。

一、資訊安全管理組織

本公司資訊安全管理單位，由電腦部門管理，負責監控網路安全運作，部門主管為負責人，下轄一位資訊安全人員及相關資訊人員以負責本公司所有資訊系統，並協同法務及人事部門主管處理相關資安風險處理程序。

資訊安全人員負責以下工作如下:

- 管理網路資訊設備
- 監控網路風險
- 監督DB Server 運作

如遇相關資訊安全風險及事件，並回報電腦部門主管待問題解決後，再回報營運最高主管(CEO)。

有關資訊安全及資訊作業程序監控由本公司稽核部門定期稽核及追踪演練

甲、管理網路資訊設備

A.本公司防護資訊安全架設配備如下：

1、防火牆(Fire Wall)

2、資產軟硬體管理系統(SMART　IT)

3、網路內容管理服務器(SQR)

4、趨勢防毒軟體(APEX 1)

5、微軟安全性更新服務器(WSUS)

6、垃圾郵件阻隔主機(SPAM)

B. 本公司防護資訊機房安全之維運如下：

1、電腦機房配有油電類專用之消防滅火器

2、電腦機房設有專用之發電機以因應機房內之不斷電設備可正常運轉

3、電腦機房內使用獨立的空調系統，以提供機房內設備在適當的溫濕度下能正常運作

4、電腦機房進出應填機房進出管制表

乙、監控網路風險

1、即時更新病毒碼並追蹤更新狀況。

2、監控作業系統安全性性及應用程式安全性更新。

3、監控防火牆及SPAM (垃圾郵件阻隔主機)所產生之異常資訊。

4、監控並記錄所有進出網際網路之電子軌跡。

5、AD及電子郵件密碼定期90天需變更密碼。

6、使用SMART IT軟硬體資產管理系統監控非法軟體安裝並及時通知資訊管理安全人員。

7、透過VPN流量管理器監控各點流量是否正常。

丙、監督 DBServer 運作

1、管理使用者資訊系統權限，避免資訊外流。

2、管理員工資訊系統帳號密碼並定期90天變更密碼(六次內不得重複)。

3、建立ERP資料庫異地備援機制(remote backup)及檔案伺服器備份機制。

4、執行並監控每天之程式原始碼、網頁原始碼、資料庫備份檔之備份作業。

5、定時的進行資料庫備份資料回復演練，以確保備份資料之有效性。

二、資訊安全風險處理架構

資訊安全事件發生標準處理流程如下：

1. 事件發生立即回報資訊安全人員。

2. 資訊安全人員處理事件，並評估資安風險：

重大風險事件：提報管理階層決定對策，並執行資安處理程序。

非重大風險事件：執行資安處理程序。

3. 由資訊安全人員根據事件內容統一指派專責人員處理。

貳、資訊安全作業規範

一、個人資料蒐集及運用

1、依個人工作職掌所提供服務資料，不能任意對其他第三者揭露。

2、使用本公司網路系統時，將自動收集下列資訊：

日期和時間、擷取之網頁網址、存取網路動作。這些資訊可能被用來改善公司網路流量效能。

3、針對以上行為，將監測對公司網路流量所造成重大負荷的上網行為。

二、資訊安全權責及教育訓練

1、對處理機密性資料之人員及因工作需要須賦予系統管理權限之人員，妥適分工，分散權責並建立評估及考核制度，及視需要建立人員相互支援制度。

2、對離職員工應立即通知電腦中心，停止使用各項系統資源之所有權限。

3、依角色及職能為基礎，針對不同層級人員，視實際需要辦理資訊安全教育訓練及宣導，促使員工瞭解資訊安全的重要性，各種可能的安全風險，提高員工資訊安全意識，促其遵守資訊安全規定。

4、資訊安全主管及人員，每年定期參加所需要資安知識的外部教育訓練

三、資訊安全作業及保護

1、建立處理資訊安全事件之作業程序，並授予相關人員必要的責任，以便迅速有效處理資訊安全事件。

2、建立資訊設施及系統的變更管理通報機制，以免造成系統安全上的漏洞。

3、建立系統備份設備，定期執行必要的資料、軟體備份，以便發生災害或儲存媒體失效時，可迅速回復作業。

4、管理員工之工作 PC (帳號密碼、安裝軟體及淘汰 PC 回收)

5、資料主機及網路設備日常維護及監控

6、安排供應商定期檢測設備安全性及妥善程度

四、網路安全管理

1、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。

2、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，機密性文件不得以電子郵件傳送。

3、定期對內部網路主機與個人電腦進行防毒查核，並定期自動更新防毒系統之病毒碼，及各項安全措施。

4、同仁於公司外部要使用公司 ERP 系統，需申請 VPN 帳號後方得連線使用 ERP，並保存連線紀錄以供稽核。員工於離職時，透過人力資源部門通知立即刪除其

外部連線帳號。

五、系統存取管理

1、視作業系統及安全管理需求訂定通行密碼核發及變更程序並作成記錄。

2、登入各作業系統時，依各級人員執行任務所必要之系統存取權限，由電腦部門系統管理人員設定賦予權限之帳號與密碼，並定期更新。

3、針對離(停)職之同仁，人力資源部門通知電腦中心，進行系統帳號的停用。

參、資訊安全宣導內容

一、密碼更換提醒：

1. Windows 系統在開機登入時如果密碼在到期前 7 天，會有提示訊息提示，使用者應在密碼到期前修改密碼。
2. 電子郵件在密碼到期前 10 天會有密碼即將到期郵件通知，使用者應在密碼到期前至網頁郵件變更密碼且需符合密碼原則。
3. 資訊系統在使用登入系統時，密碼到期前 7 天會提示使用者密碼即將在何時到期，使用者應在登入系統後至密碼修改功能程式修改密碼。

二、資安事件宣導：

1. 由資訊安全人員，提供近期與辦公室作業相關的資安事件案例，以郵件通知各部門，提高各部門作業人員的警覺性。
2. 遇有來源不明之郵件，使用者應來電詢問資訊安全人員，由資訊安全人員判斷是否為安全郵件進而採取適當的處理。