金雨企業股份有限公司

資通安全檢查之控制

1、目的：

俾確保本公司員工有資訊系統安全預防與網路傳輸資料安全之遵循，及危機處理相關事宜之能力。

2、範圍：

凡本公司資訊系統安全之網路認證程序、系統維護及管理均適用此作業程序。

3、內容：

3.1.程序說明：

3.1.1.系統安全監控

（一）公司內部應有專業人員負責處理有關資訊系統安全預防及危機處理相關事宜，以防範電腦網路犯罪與危機，維護資訊系統安全。

（二）應建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取，造成機密資料之外洩。

（三）對於跨公司之電腦網路系統，應特別加強網路安全管理，並且對內安裝防毒軟體，設置對外之網路防火牆，以防止電腦病毒、攻擊性之惡意軟體入侵，而造成公司網路系統癱瘓。

（四）應教育員工正確使用合法軟體之概念，促使員工正確認知電腦病毒的威脅，進一步提昇員工的資訊安全警覺。

3.1.2.分工及權限

（一）網路申報系統的最高使用權限，須經權責主管人員審慎評估後，交付可信賴的人員管理，防止非相關人員存取系統資訊。

（二）最高使用權限人員，應依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，應立即撤銷該使用者之帳號及權限。

（三）使用者之帳號及密碼，應避免使用容易被識破及猜測的密碼，並且應定期更改密碼。

3.1.3.資料備份及維護方式

（一）網路系統管理人員應負責網路安全規範的擬訂，執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性。

（二）個人電腦及網路系統伺服器，應具備電腦病毒掃瞄工具，並且定

期掃瞄電腦病毒與更新病毒碼。

（三）個人電腦及網路系統之資料，應每週定期備份重要檔案及資料，以備不時之需。

（四）申報之資料應儲存於電腦內，並以磁碟片、磁帶儲存備份，同時為便於管理方便，資料應加以分類儲存。

3.2.控制重點：

3.2.1.公司內部是否有專業人員負責處理有關資訊系統安全預防及危機處理相關事宜。

3.2.2.是否建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，防止未經授權的系統存取。

3.2.3.對於跨公司之電腦網路系統，是否對內安裝防毒軟體，對外設置網路防火牆。

3.2.4.是否教育員工正確使用合法軟體之概念。

3.2.5.網路申報系統的最高使用權限，是否經權責主管人員審慎評估。

3.2.6.公司是否依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，是否立即撤銷該使用者之帳號及權限。

3.2.7.使用者之帳號及密碼，是否避免使用容易被識破及猜測的密碼，並且是否定期更改密碼。

3.2.8.網路系統管理人員是否負責網路安全規範的擬訂，執行網路管理工具之設定與操作。

3.2.9.個人電腦及網路系統伺服器，是否具備電腦病毒掃瞄工具。

3.2.10.個人電腦及網路系統之資料，是否每週定期備份重要檔案及資料。

3.2.11.申報之資料是否儲存於電腦內，並以磁碟片、磁帶儲存備份。

4、附表：

無。