裕山環境工程股份有限公司	編號	N2-CE-002
	版本	第一版
資通安全管理辦法	制/修訂日期	112.04.21
	制/修訂單位	資訊組

第一條　總則

一、目的：建立公司之資通安全檢查作業，避免資訊不當洩漏，並確保系統與資料的安全性與完整性，特制定本管理辦法，以資遵循。

二、範圍：包括系統安全、分工權限及資料備份維護方式等。

三、權責：資訊組為本文件之權責單位，負責本文件之管制，並確保依據本文件之規範作業。

第二條　作業程序

一、系統安全監控

(一)公司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)公司對外之網路系統，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。

二、分工及權限

(一)網路申報系統的最高使用權限，應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。

三、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，應每日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另存備份，同時為便於管理，資料應以日期、檔案、部門別分類儲存。

第三條　控制重點

一、公司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。

二、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。

三、公司對外之網路系統，是否對內安裝防毒軟體，對外設置網路防火牆。

四、是否教育員工正確使用合法軟體之概念。

五、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。

六、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。

七、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。

八、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。

九、個人電腦及網路系統伺服器，是否具備電腦病毒掃瞄工具。

十、個人電腦及網路系統之資料，是否每日定期備份重要檔案及資料。

十一、　申報之資料是否儲存於電腦內並另存備份。

第四條　附則

一、本辦法呈總經理核准後實施，修改時亦同。

二、本辦法訂定於民國 112 年 4 月 21 日。