

幸福水泥股份有限公司

網路安全明文政策

一、資訊安全權責與教育訓練

- 對處理敏感性、機密性資料之人員及因工作需要須賦於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。
- 對離（休、停）職人員，依據人員離（休、停）職之處理程序辦理，並立即取消使用各項系統資源所有權限
- 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，以提高員工資訊安全意識，促其遵守資訊安全規定。

二、資訊安全作業及保護

- 建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理資訊安全事件。
- 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。
- 依據電腦處理個人資料保護法之相關規定，審慎處理及保護個人資訊。
- 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，以便發生災害或儲存媒體失效時，可迅速回復正常作業。

三、網路安全管理

- 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。
- 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。
- 定期對內部網路資訊安全設施與防毒進行查核，並更新防毒系統之病毒碼，及各項安全措施。

四、系統存取控制管理

- 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。
- 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，由資訊部系統管理人員設定賦予權限之帳號與密碼，並定期更新。
- 增設 USB 控管軟體，登記並控管各部門可使用外接存取裝置之使用，資訊部認證後的儲存裝置始得存取資料。

五、資訊安全政策呈核董事長後公佈實施，修正時亦同。