米斯特國際企業(股)公司 Life	資訊安全管理辦法	編　號 FD-043

歷次文件修訂紀錄

項目	修訂日期	版本	內容摘要	備　註
1	111.01.01	01	新增訂	

米斯特國際企業股份有限公司 文管中心 發行 2022-01-01 日期 文件發行章

核 准	審 核	製 表
林瑞豪		盧錡鋒

一、 目的：

公司為推動及強化資訊安全管理，建立安全及可信賴之電子化企業，確保資料、系統、設備及網路安全，保障公司權益，特訂定本辦法。

二、 適用情形：

2.1 公司應依有關規範，考量營運目標，進行資訊安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施，確保資訊蒐集、處理、傳送、儲存及流通安全。

2.2 本辦法所稱適當及充足之資訊安全措施，應綜合考量各項資訊資產之重要性及價值，以及因人為疏失、蓄意或自然災害等風險，致資訊資產遭不當使用、洩漏、竄改、破壞等情事，影響及危害公司業務之程度，採行與資訊資產價值相稱及具成本效益之管理、作業及技術等安全措施。

2.3 資訊單位應就下列事項，定期評估資訊安全實施成效：

2.3.1 資訊安全政策訂定。

2.3.2 資訊安全權責分工。

2.3.3 人員管理及資訊安全教育訓練。

2.3.4 電腦系統安全管理。

2.3.5 網路安全管理。

2.3.6 系統存取控制管理。

2.3.7 系統發展及維護安全管理。

2.3.8 業務永續運作規劃。

三、 名詞定義：

無。

四、 相關權責單位：

4.1 資訊單位：負責規劃、監督及執行資訊安全管理作業，列示如下

4.1.1 定期評估資訊安全實施成效。

4.1.2 資訊安全政策、計畫及技術規範之研議、建置及評估。

4.1.3 資訊安全管理事項之協調及推動。

4.1.4 其他資訊安全相關事宜。

4.2 各單位：

4.2.1 資料及資訊系統之安全需求研議、使用管理及保護。

4.2.2 辦理與配合資訊安全相關事宜。

4.3 資訊安全專責人員：

負責規劃、監督及執行資訊安全管理作業。

五、 作業程序：

5.1 資訊安全政策

5.1.1 說明：確保公司資訊的機密性、完整性、可用性，所訂定之資訊安全管理

作業規定、措施、標準、規範及行為準則等，以符合永續營運。

5.1.2 定義：將安全保護措施應用於資訊系統，並使資訊系統可正常無誤的運作。

5.1.3 目標：建立資訊安全管理，確保資訊系統持續運作，保障公司權益。

5.1.4 應定期進行資訊安全之評估，以確保資訊安全實務作業之可行性及有效性。

5.1.5 資訊安全政策及規定之宣達應以書面、電子或其它方式通知員工共同遵守。

5.2 資訊安全權責分工

5.2.1 公司應依下列分工原則，配賦有關單位及人員之權責：

5.2.2 資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。

5.2.3 資料及資訊系統之安全需求研議、使用管理及保護等事項，由使用部門負責辦理。

5.2.4 資訊機密維護及稽核使用管理事項，由資訊單位會同稽核單位負責辦理。

5.2.5 公司對所屬各單位資訊作業，應進行定期或不定期之資訊安全稽核。

5.2.6 資訊單位應負責資訊安全管理事項之協調及推動。

5.2.7 各單位應視資訊安全管理需要，指定適當人員負責辦理與配合資訊安全相關事宜。

5.3 人員管理及資訊安全教育訓練

5.3.1 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務

指派時，審慎評估人員之適任性，並進行必要的考核。

5.3.2 應定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升資訊安全水準。

5.3.3 應加強資訊安全管理人力之培訓，提升資訊安全管理能力。若資訊安全人力或經驗如有不足，得洽請公司資訊單位門或專業廠商提供顧問諮詢服務。

5.3.4 負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工、分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。

5.3.5 各部門主管應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

5.4 電腦系統安全管理

5.4.1 辦理資訊業務委外作業，應於事前提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守。

5.4.2 對系統變更作業，應建立控管機制，以備查考。

5.4.3 應依相關法規或契約規定，複製及使用軟體，並建立軟體使用控管機制。

5.4.4 應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

5.5 網路安全管理

5.5.1 利用公眾網路傳送資訊或進行交易處理，應評估可能之安全風險，確定資

料傳輸具完整性、機密性、可用性等安全需求。

5.5.2 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用安全技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

5.5.3 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。

5.5.4 開放外界連線作業之資訊系統，必要時應以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

5.5.5 利用網際網路及全球資訊網公佈及流通資訊，應實施資料安全評估，機密性、敏感性及未經當事人同意之個人隱私資料及檔案，不得上網公佈。

5.5.6 機密性資料及檔案，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及檔案，如有電子傳送之需要，應視需要以適當的安全技術處理。

5.6 系統存取控制

5.6.1 應依資訊安全政策，賦予各級人員必要的系統存取權限，人員之系統存取權限， 應以執行法定任務所必要者為限。

5.6.2 離(休)職人員，應立即取消使用公司內各項資訊資源之所有權限，並列入公司人員離(休)職之必要手續。

5.6.3 應建立系統使用者註冊管理機制，加強使用者通行密碼管理，並要求使用者定期更新。

5.6.4 開放外界連線作業，應明定其應遵守之資訊安全規定、標準及應負之責任。

5.6.5 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立相關安全保密責任。

5.6.6 重要資料之委外建檔，不論在公司內外執行，均應採取適當及足夠之安全管制措施，以防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

5.6.7 應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，系統中之稽核紀錄檔案，應禁止任意刪除及修改。

5.7 系統發展及維護安全管理

5.7.1 自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量，系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

5.7.2 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍。若基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即取消其使用權限。

5.7.3 委託廠商建置及維護重要之軟硬體設施，應在相關人員監督及陪同下始得為之。

5.8 業務永續運作之規劃

5.8.1 應要求委外廠商訂定系統備援及回復計畫，以確保業務持續營運。

5.8.2 應建立災害緊急召集處理機制，在發生資訊安全事件時，應依資安事件通報相關作業流程之規定，採取應變措施，將損壞減至最低程度。

六、 注意事項：

無。

七、 使用表單：

無。