一、適用範圍

有關資訊安全之事項，除另有規定外，悉依本辦法辦理。

二、資訊安全政策

維護公司整體資訊安全，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性與適法性，避免發生人為疏忽、蓄意攻擊及天然災害時影響公司作業或損及公司權益，確保業務持續營運。

三、 資訊安全組織

（一） 本公司配置適當人力資源及設備，進行資訊安全之規劃、監控及執行資訊安全管理作業，並應指派綜理資訊安全政策推動及資源調度事務之人擔任資訊安全專責主管及至少 1 名資訊安全專責人。

（二） 資訊安全組織職權如下：

1. 制定企業資訊安全政策、目標與管理制度。
2. 企業資訊安全相關工作之規劃、執行與檢討。
3. 企業資訊安全各方案執行成效之追蹤、檢視與修訂。
4. 企業資訊安全報告書之編製發行。

四、資安事件通報流程

為有效預防及處理資訊安全事件，特制定資訊安全通報流程，以快速應變資安事故發生之相關處理。資訊單位於收到通知後，將依是否為資訊安全事件。資安事件通報流程如附件（一）

五、帳號生命週期管理

（一）資訊系統均需有帳號及密碼登入管理功能。

（二）使用者須妥善保管個人帳號、密碼，密碼至少十個字元及應三個月更換乙次。

（三）同仁異動經權責主管核定後，應依其異動狀況停用或刪除其帳號及許可權。

六、資料存取

（一）系統資料庫由資料庫管理者依使用者群組訂定不同使用權限，無權限者不得直接存取資料庫內容。

（二）系統應依資料之重要性設定安全機制，並應可追蹤資料流及使用者操作記錄。

（三）系統資料儲存異常時，應有自動警報或回復功能。

（四）資料依重要性區分，設定不同的保存或銷毀期限，除另有規定外，保存期限至少為五年以上。

（五）使用單位經由系統所取得之機密性資料均應嚴加管制，限制傳閱、影印、複製、攝影、轉出或以其他方式記錄。

（六）系統資料轉出應填寫資訊服務單，經權責主管核定後始得辦理。

（七）系統存取及應用之監督

1.應建立及製作異常事件及資訊安全事項的稽核軌跡，並妥善保存，以作為日後調查及監督之用。
2.系統稽核軌跡應包括下列事項：
（1）使用者識別碼。
（2）登入及登出系統之日期及時間。
（3）儘可能記錄端末機的識別資料或其位址。

七、網路安全管理
(一)網路應安裝監控系統，監控通訊線路、通訊協定、資料流量、資料內容及使用物件，由資訊部門指定專人辦理。
(二)重要伺服器均應裝置於公司受到保護的網路內，內、外網路須安裝安全防護設備(防火牆)區隔，並依業務所需設定安全存取權限。
(三)防火牆安全權限之異動申請，經資訊部門核定後，由專責人員修改，並紀錄異動歷程。
(四)資訊部門應定期檢討防火牆安全權限及電腦網路安全事項，並應建立網路入侵偵測系統，以有效偵測惡意入侵事件。
(五)經由公眾網路傳輸機密資料時，應採取資料加密機制。
(六)防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。
(七)憑證安全管理
1.資訊平台與外部連結時，須建置憑證金鑰。
2.憑證金鑰之產生、儲存、使用、備份、銷毀、更新及復原作業等，應建立嚴格的安全管理機制。

八、系統原始碼管理
(一)資訊系統之相關原始碼，應依機密等級給予適當安全屬性，不同安全屬性之文件應分開，並以相對應的安全措施加以保存。
(二)調閱相關原始碼須經資訊部門主管核定並記錄。
(三)資訊系統原始碼須通過資安原始碼檢測。

九、備份作業管理
(一)為確保集團資訊系統之資料完整與正確，應設有三層備份資料保護機制，確保災害發生時，能根據不同等級的損害進行資訊資料的重建工作。
1.本機資料備份：存放於運行中的主機上。
2.異機資料備份：存放於同機房的其他主機上。
3.異地資料備份：存放於異地機房。
(二)資訊部門應依業務及重要性設定系統完整之備份計劃，且須設定密碼後方能執行，並詳細記錄主機名稱、日期、起迄時間、內容、編號、狀態、保存位置及操作人員。
(三)備份軟體須確保備份資料的完整性及安全性。

（四）備份以磁帶為主，其他媒體為輔，並須存放於隔熱防火、防潮整潔之場所，且應與主機異地安全保存。

（五）重要資料的新舊備份，均應依政府法令規範時效保存。

（六）備份資料應依系統特性及重要性安排回復測試作業，並詳細記錄主機名稱、日期、起迄時間、內容、編號、步驟、狀態、結果及操作人員。

（七）資訊部門應定期演練備援作業程序，以便發生災害或儲存媒體失效時，可迅速回復正常作業。

十、資訊系統可用性管理

（一）監控機制

1.需設有監控平台，可隨時監看當下系統妥善狀態。

2.每月定期提供系統可用性報表。

（二）異地備援

1.應訂定異地備援計劃。

2.備援地點不可與運作中的機房為同一棟大樓。

3.備援地點須具備運行系統服務的硬體設備。

（三）災害復原

1.應訂定災害復原計劃。

2.每年執行災害復原演練，過程需有文件和紀錄備查。

十一、病毒防治

（一）公司所有伺服器主機、個人電腦、筆記型電腦均應安裝規定之防毒軟體，掃毒紀錄應由專人每日檢視，並採取必要之措施；所有伺服器亦應按月執行掃毒作業，並將紀錄留存備查，以防制及偵測電腦病毒與惡意軟體等的侵入。

（二）使用防毒軟體，應依下列原則辦理：

1.定期更新版本及病毒碼。

2.定期或即時掃描電腦系統及資料儲存媒體。

3.使用之防毒軟體由資訊部門審核後，方可使用。

4.對來路不明及內容不確定的資訊媒體，應在使用前詳加檢查是否感染電腦病毒。

5.定期將必要的資料及軟體予以備份。

（三）電腦設備如遭病毒感染，應立即離線（拔除網路線連結），並通知資訊人員處理，直到確認病毒已消除後，方可重新連線。

十二、機敏資料的保護措施

（一）辦公室環境不貼密碼便條，畫面設定自動螢幕保護。

（二）對公司使用的資訊系統資料嚴加保密，不論下載或是列印資料，在系統上均有詳記紀錄，禁止複製、攜出、傳送到外部平台等相關行為。

十三、個人資料保護

資訊系統之運作功能及資料存取應符合個人資料保護規範，依據「個人資料保護作業要點」相關規定辦理。

十四、實體及環境安全管理

資料中心及機房之安全管理，依「資訊機房管理辦法」相關規定辦理。

十五、其他資安規範

同仁應遵守上述資安條文外，並應遵守下列規定：

(一)不得傳輸、發送、散播電腦病毒、等任何干擾集團無線系統服務正常運作使用之行為，加重集團無線系統負擔或消耗網路頻寬之程式使用或資訊傳輸者。

(二)不得擅自重製、散布、刊載、傳輸、下載、發送或儲存等侵害他人之智慧財產權或其他權益之資料。

(三)不得發表恐嚇、誹謗、詐欺、侮辱、猥褻色情、侵犯他人個資隱私、散布傳播不實新聞消息損害公共利益、違背公序良俗等違法之言論文字、圖片或影音。

(四)濫發廣告商業電子郵件，寄發垃圾訊息，或其他未經收件人同意收受之訊息郵件。

(五)利用集團網路系統傳遞、販賣、推銷、仲介等本國法令所禁止之各項商品或服務。

十六、資安遵守

(一)同仁應遵守公司資訊安全政策之相關規定，違者按情節輕重依「同仁獎懲辦法」相關規定予以處分。

(二)同仁應遵守業務機密之相關法令規定，在職及離退職後均不得洩漏所知悉之資訊機密，或為不當之使用，違者按情節輕重依「同仁獎懲辦法」相關規定予以處分，必要時並得追究相關法律責任。

十七、施行日期

(一)本辦法於二〇一〇年四月一日整合制定。

(二)本辦法於二〇一九年十一月一日第一次修正。

(三)本辦法於二〇二四年二月一日第二次修正。