# 網路通訊安全管理作業辦法

1. 目的：

為強化資訊安全管理，建立安全及可信賴之電子化作業環境及保障公司權益，制定本準則。

2. 適用範圍：

作業辦法適用於公司電腦資料傳輸，網路安全、電子郵件、電子監控系統(註一)等之管理。

3. 內容：

3.1. 資料及軟體輸出之安全管理：

3.1.1. 公司對其他企業或非公司組織內的員工進行電子資料（註二）的輸出時,除日常例行工作事項外，其餘應經直屬主管同意，始可輸出資料，單位主管具有監管業務範圍內電子資料的責任。啟用電子監控系統前必須公告，調閱監控資料時需提出申請，並依控管方式進行完整授權後方可進行。

3.1.2. USB 磁碟儲存裝置接入時都應執行掃毒，以確保資料安全性。並嚴禁使用未經認可的裝置，初次使用時需提出申請，方可使用特定的隨身碟。

3.1.3. 網路安全規劃與管理：

3.1.3.1. 主機安全防護。

3.1.3.2. 為提升大型主機或伺服器主機連線作業之安全性，公司內主要資訊作業系統一律只設定為內部 IP，除與委外廠商連線外，不和其它外界連接。

3.1.3.2.1. 公司與外界網路連接的網點，有加裝防火牆，以控管外界與機關內部網路之間的資料傳輸與資源存取。

3.1.3.2.2. 網路系統管理人員應配合公司政策及規定的更新，以及網路設備的變動，隨時檢討及調整防火牆系統的設定或升級設備，以反應最新的狀況。

3.1.3.3. 網路資訊之管理：

3.1.3.3.1. 本公司的資訊系統，基於安全性原則，除委外廠商須連線處理系統外，不對外開放。

3.1.4. 電子郵件安全管理：

3.1.4.1. 公司的電子郵件未經直屬主管許可，不可傳送公司內部的機密資料。

3.1.4.2. 電子郵件的附件安全管理：

3.1.4.2.1. 附件禁止傳送可執行檔案(如*.bat *.exe *.com……)。

3.1.4.2.2. 附加檔案禁止傳送超越 20MB 的檔案。

3.1.4.2.3. 嚴禁利用公司的 e-mail 散發或轉寄與公司業務無關的郵件，若違反本項規定，其相關法律責任由 e-mail 使用者自行負責，且公司有權停止其 e-mail 使用。

3.1.5. 網際網路資通安全之管理：

3.1.5.1. 個人掃毒軟體：

3.1.5.1.1. 公司內每一部個人電腦皆有加裝個人式掃毒軟體，會針對下載的每一檔案做電腦病毒或惡意內容的掃描，嚴禁自行移除防毒軟體。

3.1.5.1.2. 每台個人電腦應定期更新病毒碼及個人電腦作業系統。

3.1.5.1.3. 每台個人電腦每週應至少對個人電腦掃毒一次。

3.1.5.2. 網路入侵之處理-網路如發現有被入侵或疑似被入侵應採取下列防範步驟：

3.1.5.2.1. 第一時間通知相關主管。

3.1.5.2.2. 第一時間將對外的接點切斷。

3.1.5.2.3. 檢查被入侵的主機是否有異狀，快速進行搶救。

3.1.5.2.4. 檢查主機漏洞，並針對主機漏洞予以修復或修補。

3.1.5.2.5. 當事件發生時，迅速依通報程序進行通報，提出資安事件通報單(FM-CC000021)，並採取必要之應變措施，降低事件可能帶來之衝擊，並建立事件學習機制，降低事件造成的損害。

3.1.5.2.6. 資安管理單位依「資安事件通報單」發現人員通報之資料，進行記錄及分類。

3.1.5.2.7. 資安管理單位在收到通知後，會進行研判以確定是否涉及資訊安全事件；若判定為非資訊安全事件，會向通知人員做出回饋，而若判定為資安事件，則會根據事件影響程度通知相關權責單位主管，待事件處置完成並一切回復正常運作後，須將處置之結果，記錄於「資安事件通報單」中。

3.1.5.2.8. 根據涉及利害關係人（包括主管機關和情報共用機構）的情況，執行相應的通報機制，並在通知利害關係人後記錄通報過程，同時根據與利害關係人的合約評估事件等級，必要時召開雙方資安防護會議

3.1.6. 電子監控資料調閱之管理：

3.1.6.1. 人員電腦操作歷程與瀏覽記錄、電子郵件往來與通訊軟體訊息記錄與電話錄音之管理：

3.1.6.1.1. 電子監控資料需定期或自動備份存放於特定儲存裝置或媒體。人員操作歷程與瀏覽記錄、電子郵件往來與通訊軟體訊息記錄至少保留二年之記錄，電話錄音部份至少保留一年之記錄。

3.1.6.1.2. 電子監控資料當有調閱需求時，需提出電子監控資料調閱申請表(FM-CC000018)，經申請單位主管、部門主管、系統管理員、財務資訊管理處、稽核室、總經理、執行長核准後，方可進行調閱。若涉及公共利益或基於防止造成他人權益重大危害，可不需告知和取得當事人之同意，即可進行調閱申請。電子監控資料調閱申請單須保存二年以

供備查。

3.1.6.1.3. 已核准之調閱申請，於進行調閱時，需系統管理員、稽核人員同時在場方可進行調閱，完成調閱後，系統管理員準備調閱報告，並將其呈報給經營層代表。

3.1.6.1.4. 若為管理統計與異常分析所進行非特定當事人的記錄利用，分析與揭露之數據無法辨別特定當事人時，不需提出申請即可進行利用，惟異常分析後，若明確指向特定人員，於揭露前需先告知當事人，除涉及重大公共利益時可不需告知避免造成利益損失。

3.1.6.1.5. 公務機關若有執行法定職務需求時，確認合法性後，應提供相關資訊給公務機關人員，以滿足法定職務需求，此後由系統管理員提出電子監控資料調閱申請表(FM-CC000018)，並在單據中詳細注明公務機關所屬部門和姓名及需求，經申請單位主管、部門主管、財務資訊管理處、稽核室、總經理核准。

3.1.6.2. 監視器錄影檔之管理：

3.1.6.2.1. 監視器錄影檔指監視期間自動備份之檔案，檔案保留期限依監視設備主機設定為主。

3.1.6.2.2. 當有存取調閱需求時，需提出電子監控資料調閱申請單(FM-CC000018)。需經過申請單位主管、部門主管、財務資訊管理處、稽核室、總經理的核准，方可正式進行存取調閱程序，惟調閱需求牽涉到影響公司重大利益或個人安全問題時，稽核單位主管在審核後可立即請求資訊單位提供緊急的調閱資料。

3.1.6.2.3. 公務機關若有執行法定職務需求時，確認合法性後，應提供相關資訊給公務機關人員，以滿足法定職務需求，此後由系統管理員提出電子監控資料調閱申請表(FM-CC000018)，並在單據中詳細注明公務機關所屬部門和姓名及需求，經申請單位主管、部門主管、財務資訊管理處、稽核室、總經理核准。

3.1.7. 公司內部電話、手機使用管理規範：

3.1.7.1. 桌上型話機之管理：

3.1.7.1.1. 接聽電話需保持電話禮儀。

3.1.7.1.2. 當人員暫時不在座位時，應協助代接與記錄來電者資訊，並於人員回座位時留言提醒與告知。

3.1.7.1.3. 轉接電話前，應先確認轉接對象是否方便接聽，確認可接聽後再進行轉接，避免轉接後無人接聽。

3.1.7.1.4. 桌上型話機為單位固資，需維持清潔並愛護使用。

3.1.7.1.5. 公司電話即代表耀億公司，通話時避免洩漏公司內部機密或劣化公司形象。

3.1.7.2. 員工私人手機使用之管理：

3.1.7.2.1. 私人手機使用需提出員工權限異動申請表，待核准後方可使用。

3.1.7.2.2. 當申請使用私人手機，即同意公司內部使用該號碼進行聯繫，惟當需提供給公司外部人員時，需先告知該員與取得同意，公司其他人員方告知予外部人員。

3.1.7.2.3. 私人手機於該員離職時該員可要求取消此號碼紀錄,取消後未經同意，公司不得將號碼進行內部公佈或提供第三方。

3.1.7.2.4. 使用私人手機因公務需求所產生之通話費，可於帳單產生後提出通話明細並標示公務需求通話，核實後進行費用申請。

3.1.7.2.5. 上班時間私人手機應以公事使用為主，避免影響公事為原則。

3.1.7.3. 公司手機使用之管理：

3.1.7.3.1. 公司手機使用、申請、續約、取消，皆需提出「員工權限申請/異動申請表」(FM-CC000006)，資訊人員憑單至電子簽核系統提出印鑑申請暨合約審查單處理。

3.1.7.3.2. 公司手機門號統一以公司名義進行申請，不可自行申請門號後再轉入公司使用。

3.1.7.3.3. 當申請使用公司手機，該號碼屬於公司所有，公司內部皆可依需求直接提供相關對象以便於聯繫。

3.1.7.3.4. 公司手機於該員離職時須繳回號碼。

3.1.7.3.5. 公司手機不得要求提前續約，但可依使用狀況提出申請與核准後調整月租費率。

3.1.7.3.6. 除該公司手機門號使用人員本人外，其他人員不得以非個人使用之手機門號要求續約與申請優惠方案。

3.1.7.3.7. 公司手機可續約時，使用人員可提出續約需求，並由管理人員調閱歷史使用情形，重新調整月租費率經核准後進行續約，不得為優惠方案而調高月租費率。

3.1.7.3.8. 公司手機簽約、續約若為人員要求特定方案，申請後須支付追加金額時，由使用申請人員自行支付差額。

3.1.7.3.9. 公司手機所有通話費由公司負擔，但其餘私人購買之手機軟體、配件等私人消費行為，其金額合併於當月帳單時，使用人員需繳交此部分之費用予公司。

3.1.7.3.10. 公司手機於使用期間損壞或遺失，其費用由使用人員自行負擔。

3.1.7.3.11. 使用公司手機應以公事使用為主，避免造成公司不必要之支出。

3.1.7.4. 電信相關費用衍生紅利積點之管理：

3.1.7.4.1. 公司支付電信相關費用衍生贈品或兌換點數，填具簽呈經核准後，統一由經營層確認後進行使用與兌換。

3.2. 資訊安全發生通報之層級：

3.2.1. 依資訊安全發生等級來判定通報之層級訂定如下：

3.2.1.1. 等級：4 級

通報層級：執行長

發生內容：

(1) 機密等級資料洩漏。

(2) 核心業務系統或資料遭受嚴重竄改或毀損。

(3) 嚴重衝擊多個業務、系統運作，影響企業聲譽，無法於 8 小時內復原。

3.2.1.2. 等級：3 級

通報層級：執行長

發生內容：

(1) 內部限閱等級資料洩漏。

(2) 影響核心業務運作或相關系統中斷服務。影響之重要業務、系統運作，可於 8 小時內復原。

3.2.1.3. 等級：2 級

通報層級：部門主管

發生內容：

(1) 一般等級，非核心業務系統。

(2) 只是資料遭輕微竄改，業務運作遭影響或系統效率降低。不影響重要業務、系統運作。

3.2.1.4. 等級：1 級

通報層級：單位主管

發生內容：

(1) 非核心業務之資產。

(2) 受到衝擊的損失程度很低，不影響業務、系統運作。

3.2.2. 資安事件應變處理

3.2.2.1. 4 至 3 級事件，指揮由指揮官（召集人）擔任；2 至 1 級事件，指揮由副指揮官擔任。(指揮應視狀況完成緊急應變小組配置，進行異常事件排除及控制。)

3.2.2.2. 4 至 3 級資安事件須於 36 小時內；2 至 1 級資安事件須於 72 小時內。(完成復原或損害管制) 。

3.2.2.3. 資訊安全事件通報對象、通報方式及處置期限如下表所示。

| 資訊安全事件等級 | 指揮統籌 | 通報方式 | 通報對象 | 處置期限 |
|---|---|---|---|---|
| 第 4 級(嚴重) | 指揮官 | 電話<br>(或任何可通訊手法) | 臺灣證券交易所 | 接獲通報後 36 小時以內 |
| 第 3 級(重大) | 指揮官 | | TWCERT/CC | 接獲通報後 36 小時以內 |

| | | | | |
|---|---|---|---|---|
| 第 2 級(注意) | 副指揮官 | | 內部受影響單位 | 接獲通報後 72 小時以內 |
| 第 1 級(輕微) | 副指揮官 | | 內部受影響單位 | 接獲通報後 72 小時以內 |

3.2.2.4. 當資安事件無法在預定的修復時間內完全解決時，需要重新評估以下方面：事件的範圍、損失評估、事件等級、事故分類、資源需求、緊急應變措施以及涉及的利害關系人，這些重新評估的結果應補充到「資安事件通報單」中。

3.2.2.5. 視事故類型採取應變程序因應，必要時得經權責主管同意後，進行備援或緊急應變作業。

3.2.2.6. 資安事件等級為 4 級，指揮官應成立重大資安事件緊急應變小組，應符合上市上櫃公司資通安全管控指引「第三十四條」，啟動重大資安事件通報，並依相關規定辦理重訊發布。

3.2.2.7. 為確保資訊安全，應檢討並分析相關資訊，以釐清資訊安全事件的根本原因和責任歸屬，同時評估是否存在潛在的重複發生風險，並積極修補現有資訊環境中的漏洞。其次，對於資訊安全事件，必須保留事件發生的關鍵線索，以實現有效的追蹤和深入檢討事件的根本原因。當資訊安全事件達到重大等級或以上時，應在成功控制事件後召集相關單位，由事件指揮官或副指揮官主持資安事件檢討會議，以深入分析問題發生的根本原因，以確保預防類似資安事件的再次發生。

3.2.2.8. 應審視現有環境的漏洞，細節記錄於「資安事件通報單」。

3.3. 成立資訊安全委員會組織，討論公司內部資訊安全相關議題。

3.3.1. 目的：規劃公司資訊工作目標設定，確立資訊安全政策執行與落實。

3.3.2. 成員：

主席：集團執行長

委員：事業群總經理、各部門主管

列席人員：各廠資訊/資安主管、稽核主管

3.3.3. 討論範疇：

3.3.3.1. 機房設備軟/硬體升級。

3.3.3.2. 資訊安全政策修訂。

3.3.4. 行政單位：

資訊安全委員會會議聯絡、書面資料蒐集及其他行政事項，由資安專責主管依資訊安全委員會主席之指示，在時程內辦理。

3.3.5. 會議召開：定期每半年召開一次。

3.4. 成立資訊安全推動委員會組織，執行項目推動監督。

3.4.1. 目的：該委員會將負責監督和推動公司資訊安全相關活動的執行。

3.4.2. 成員：

召集人：集團執行長

副召集人：財務資訊管理處主管
資安稽核單位：稽核室主管
資安推動單位：事業群總經理、各部門主管
資安文件管制單位：人資課主管
資安管理單位：資訊課主管、資安主管
列席人員：由主席指派相關人員

3.4.3. 討論範疇：

3.4.3.1. 強化公司的資訊安全管理以及確保資訊安全政策的有效執行。

3.4.4. 會議召開：委員會會議將在需要時召開，以確保有效的協調和監督公司的資訊安全活動。

註一：電子監控系統的資料範圍如下

1. 網路瀏覽記錄。
2. E-mail 往來記錄。
3. 人員電腦操作歷程。
4. 電話錄音等影音記錄。
5. 監視器保存之歷史記錄。

註二：電子資料的範圍如下

1. 由印表機印出的書面資料。
2. 存在儲存媒體(註三)的資料。
3. E-mail 的附加檔案。
4. BPM 的文件管理資料。
5. 網路硬碟。

註三：儲存媒體範圍如下

MO、磁帶、磁片、光碟、行動碟、記憶卡、硬碟、行動硬碟。

4. 表單：

4.1. 資安事件通報單 FM-CC000021

4.2. 電子監控資料調閱申請表 FM-CC000018

4.3. 員工權限異動申請表 FM-CC000006