茂訊電腦資通安全管理委員會成員及分工表

製表日期：112年10月18日

單位職級	人員權責	名稱	職掌事項	分機	備註 （代理人）
總經理	召集人	沈頤同	負責資安政策、目標相關辦法核定、公告、發布 並於董事會中提報資安事項執行情形	201	周詠翔
執行副總	資安專責主管	周詠翔	「資通安全推動小組」執行狀態確認與回報 若接獲內外部資安管控相關事件，聯繫相關處理單位進行控管與處理	501	簡逸華
資訊室-資深 MIS 資訊工程師	資安專責人員	簡逸華	擬定規劃並推動資安項目，判別資安風險及等級，執行應變程序 依應變程序處置復原作業或系統重建	272	林怡君
稽核專員	資安稽核人員	陳俞璇	參與「資通安全推動小組」審查，並執行資安稽核	306	
執行副總	發言人	周詠翔	企業對外發布新聞或發言，負責事件綜整，擬定媒體溝通計畫	501	

茂訊電腦股份有限公司

資通安全管理辦法

資訊安全管理辦法

修改版本條文與內容概要紀錄

版本增修	增修日期	修訂條文與內容概要	資訊安全專責主管	執行長
Ver 1.0	112/10/18	建立資通安全管理辦法		

目錄

前言:

此**資通安全管理辦法**,為符合相關資通安全法令,所另外重點列出的管理條文,以補足現有的資訊管理辦法,使其符合現有資安法令相關辦法,以達到”資通安全管理”的完整性!

壹、管理辦法依據

本管理辦法依據「依金管證審字第 11003656544 號法令及公開發行公司建立內部控制制度處理準則」所訂定。

貳、適用範圍

涉及本公司資訊作業或資料使用之全體員工、承包商、顧問、臨時雇員、客戶、第三方人員，皆應遵循本政策。

凡委外廠商、系統商顧問等，接觸到本公司機敏資料人員，皆須簽結資訊保密暨資通安全規範切結書。(附件表格二)

參、核心業務及重要性

核心業務確認，鑑別可能造成營運中斷事件之發生影響程度，設置適當之備份機制及備援計畫。

一、 核心業務及重要性:

(一)本公司之核心業務及重要性如下表:

核心業務	核心資通業務	重要性說明	業務失效影響說明	最大可容忍中斷時間
流程導向企業資源規劃	Workflow ERP GP(鼎新電腦)	各部門流程資源規劃	中斷會導致各部門無法執行工作任務	12Hr
電子郵件	硬體式郵件伺服器(眾至資訊)	內部及外部業務通信	失效會導致即時性資訊無法送達	12Hr
圖文管理系統	DOC System(公司自建)	研發處產品圖文管理系統	中斷會導致研發產品資訊無法查詢(舊資料)	24Hr
人事薪資管理系統	人事薪資管理系統(日城資訊)	人事考勤管理系統	中斷會造成考勤失效，無法有效計算薪資	12Hr
智能現場執行系統	sMES(鼎新電腦)	生產線生產產品流程、序號蒐集	無法有效派工製造，及紀錄半成品、成品序號	12Hr
產品生命週期管理系統	Open PLM(博威顧問)	研發處研發資料圖文、BOM 表管理簽核	無法對產品資料做有效登載控管	12Hr
客戶關係管理系統	CRM(鼎新電腦)	對客戶報價、關係管理	無法有效並完整對客戶報價	24Hr
檔案伺服器	Synology RS1221+(NAS)	各部門文件資料存放空間	無法有效取用重要文件及資訊	24Hr

通路事業處內網系統	.net 平台(自建)	進銷存、人員出缺勤	無法有效掌握商品銷售資訊、人員出缺勤	12Hr

(二)各欄位定義：

1.核心業務：公司內部維運、提供關鍵基礎設施所必要之業務。

2.核心資通系統:該項核心業務所必須使用之資通系統名稱。

3.重要性說明:說明該業務對公司營運之重要性。

4.業務失效影響說明:該項業務使用之系統失效後，公司業務運作有何影響。

5.最大可容忍中斷時間單位以小時計算。

二、非核心業務及說明:

(一)本公司之非核心業務及說明如下表:

非核心業務	業務失效影響說明	最大可容忍中斷時間
公司官方網站	無法有效宣傳公司當前業務及讓顧客下載驅動程式等資源	48Hr
端點防護軟體系統	失效後端點依然有基本保護能力(Windows 內建安全軟體)	48Hr
備份系統	備份有留存安全天數份數，損失為該失效時間內備份	48Hr

(二)各欄位定義:

1.非核心業務系統:相關業務之資通系統，例如資訊傳遞、用戶端服務、端點安全等。(依實際狀況列出)

2.業務失效影響說明:該項業務使用之系統失效後，對公司內部運作有何影響。

3.最大可容忍中斷時間單位以小時計算。

肆、資通安全政策

一、目的

為使本公司業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality)、完整性（Integrity）及可用性（Availability)，特制訂本政策如下，以供全體同仁共同遵循：確保公司業務資訊之機密性、完整性與可用性。

二、管理原則

(一)應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

(二)因應資通安全威脅情勢變化，提高本公司同仁之資通安全意識，同仁應確實參與資通安全教育訓練，本公司不定時進行資通安全宣導。

(三)勿開啟來路不明或無法明確辨識寄件人之電子郵件。

(四)可攜式媒體依各該資訊系統管理規定使用。

(五)系統及資料之使用須經授權,且存取權限之授予應以業務所需之最小範圍為原則。

(六)建立資訊安全組織並明訂其權責,以推動及維持資安管理、執行與查核等工作。

(七)訂定資安管理相關辦法及程序,以保護人員、資料、資訊系統、設備及網路等之機密性、完整性及可用性。

(八)不定期召開資安管理會議,檢視內外部風險、科技及業務需求等最新發展,以採取因應措施。

(九)資訊系統建置適當之備援及備份機制並進行應變演練,強化資訊服務在面對威脅時之韌性。

(十)辦理員工資安教育訓練,持續提升同仁資安意識。

(十一)依照資安、個資保護相關法規之規定,謹慎處理與保護資料及系統的安全性。

三、目標

(一)量化型目標:

(1)知悉資安事件發生,能於規定的時間完成通報、應變及復原作業。

(2)核心資通系統可用性達 99.99%以上。(中斷時數/總運作時數≤ 0.1%)

(3)禁止帳號共用,禁止使用弱密碼。

(二)質化型目標:

(1)適時因應法令與技術之變動,調整資通安全維護之內容,以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害,以確保其機密性、完整性及可用性。

(2)達成本公司資通安全責任等級分級之要求,並降低遭受資通安全風險之威脅。

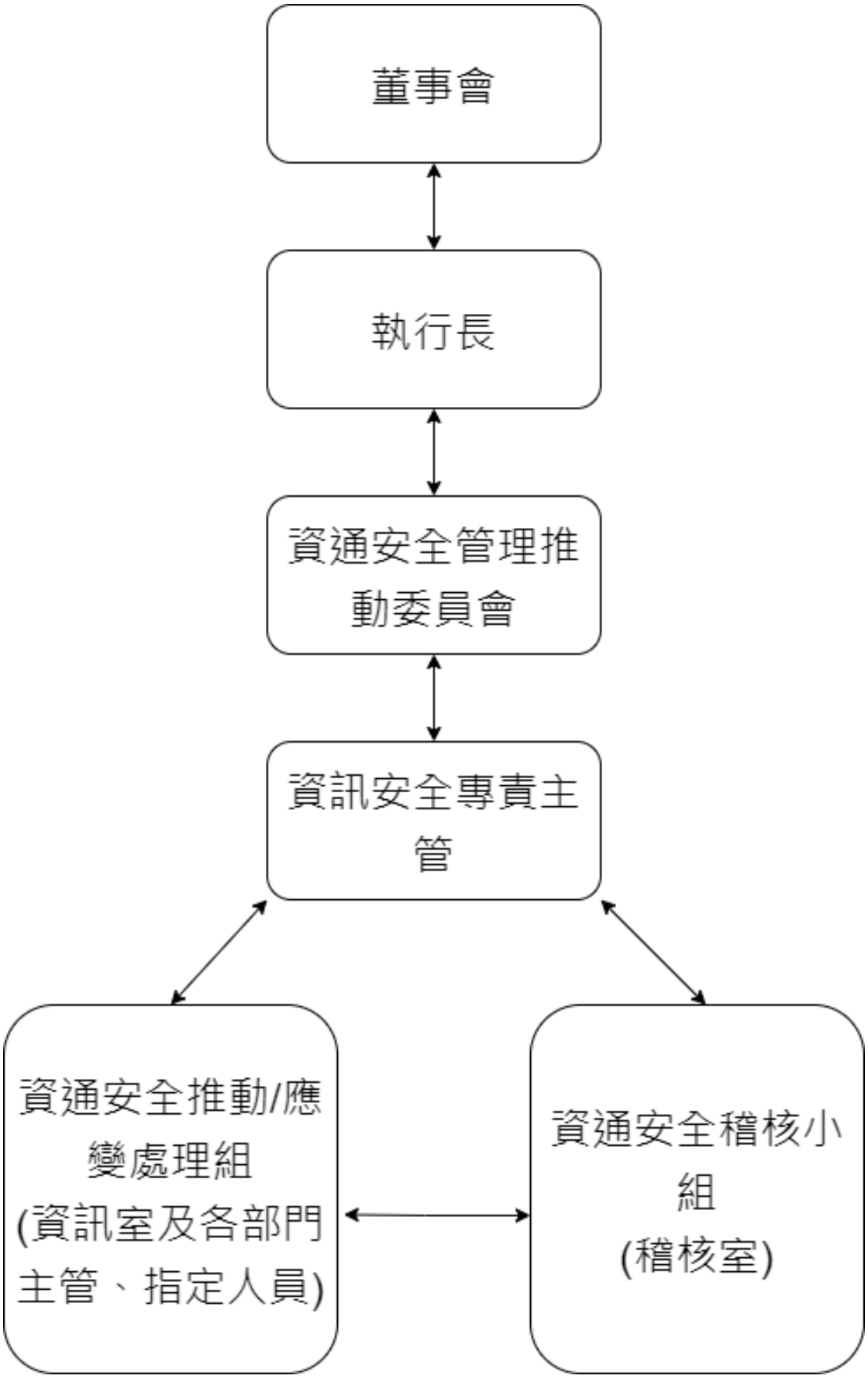
(3)提升人員資安防護意識、有效偵測與預防外部攻擊等。

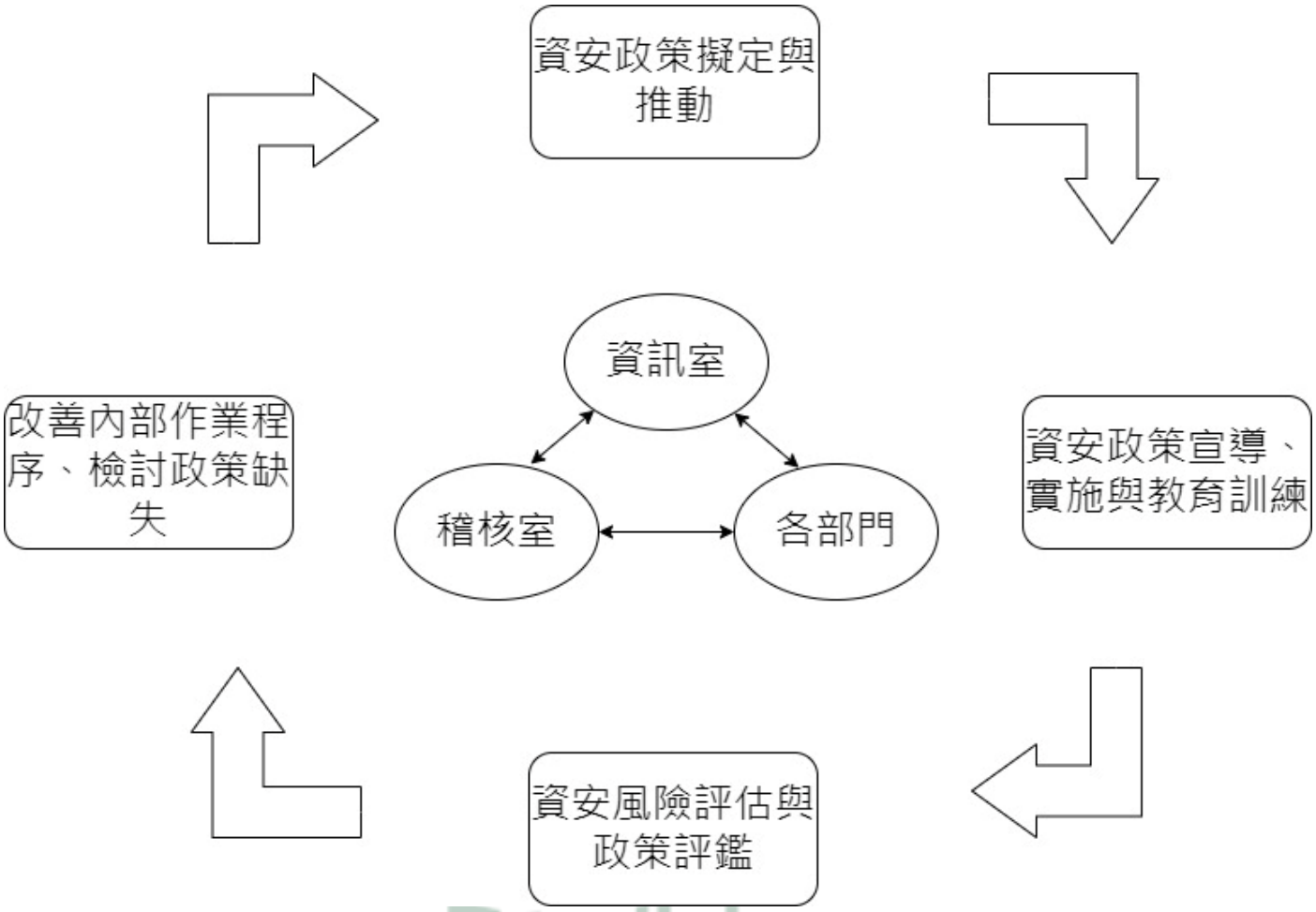
四、審查:

(一)本政策應至少每年審查一次,以反應相關法令、及本公司業務等最新發展,並予以適當修訂。

(二)本政策修訂由總經理(執行長)核定後,於公告日施行。且應以公告、書面、電子郵件或其他方式告知利害關係人,如:全體員工、合作廠商、供應商等。

伍、資通安全推動組織


董事會
執行長
資通安全管理推動委員會
資訊安全專責主管
資通安全推動/應變處理組
(資訊室及各部門主管、指定人員)
資通安全稽核小組
(稽核室)



一、目的：

旨為強化本公司之資訊安全管理、確保資料、系統及網路安全，並設立資訊安全管理推動委員會，擬定、推動並執行資安業務，防止因資安問題導致企業秘密、財物的損失。

由本公司執行長擔任管理委員會召集人，成立資通安全管理委員會，並向董事會報告。

下設資訊安全專責主管(以下簡稱資安主管)，負責委員會執行狀態確認與回報。

二、分工與權責:

(一)資安主管:

(1)資通安全管理政策及目標之核定、督導。

(2)資通安全責任分配及協調。

(3)資通安全資源分配。

(4)資通安全事件檢討及監督。

(5)其他資通安全事項核定。

(二)資通安全推動組織:

(1)跨部門資通安全事項權責分工及協調。

(2)整體資通安全措施之研議

(3)其他重要資通安全事項之研議

(三)資訊室為資安專責單位，由資訊室資安人員，負責資訊安全事務的規劃、推動與執行，並由資安主管核可。各部門最高級幹部，負責協助資訊安全管理事務發佈後的政策執行。

(四)資安稽核單位:

(1)參與「資通安全管理委員會」審查。

(2)稽核資訊安全管理辦法的施行。

(五)事件通報與應變單位:

(1)公司發言人

(2)資安主管

(3)資訊室

本公司所有員工，皆須遵從發佈之政策。

三、教育訓練：

(一)填寫並提報年度資通安全教育訓練計畫(附件表單一)

(二)教育訓練

(1)資安人員專業教育訓練:

每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。

(2)資安教育訓練:

資通安全專責人員以外之資訊人員，每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。

一般使用者及主管，每人每年訂定須接受三小時資安教育訓練。

陸、資訊資通系統盤點

一、本公司每年辦理資訊資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產等。

二、資訊及資通系統資產如下:

(一)資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。

(二)軟體資訊：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

(三)實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

柒、資安資訊情資共享平台

本公司為上櫃公司，為加強資安，已主動加入 TWCERT/CC 機構資安聯盟，成為該聯盟資安聯防體系中的一員！

共享國內外最新的資安資訊、企業資安事件通報協處、產品資安漏洞通報、惡意檔案檢測。

該機構並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享。

捌、資安事件通報及應變作業程序

一、目的：

為使公司資安事件之處理有明確的相關規範，當事件發生，能迅速依通報程序進行通報，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。

二、適用範圍：

公司各項資訊資產之管理，均適用之。

三、名詞定義：

(一)資訊安全事件：凡於作業環境中，資訊或資通系統之機密性、完整性、可用性，遭受影響導致異常之事件。

(二)發現人員：指企業所有人，含正式或非正式人員（臨時員工或派駐人員），發現疑似資安事件時，皆負有即時通報之責任。

四、資安事件通報及應變：

(一)若發現或疑似資訊安全事項時，由發現人員依事件之人、事、時、地、物，迅速通報資安管理權責人員，並由資安管理人員告知資安主管。

(二)資安管理單位、依發現人員通報資料，紀錄於「資通安全事件通報單」，進行通報流程處理並留存處理紀錄。

(三)資安管理單位於收到通報後，需初步研判是否為資通安全事件。

(1)若判斷為非資安事件時，將判斷結果回覆通報人。

(2)若判斷為資安事件，則啟動通報流程，紀錄後並報知資安主管。

五、資安事件分類

類別	事件狀況
天然災害	火災、水災、地震等
機房設施失效	UPS、電力、冷卻空調等失效

系統異常	硬體設備故障(電腦主機及其零組件)、軟體異常(資料庫或 ERP 等服務系統)
網路異常	網路中斷
駭客入侵	攻擊導致系統損壞、中斷(病毒、勒索軟體、DDOS 等攻擊)
人員操作失誤	執行人員未遵守相關作業程序。 廠商維修及維護人員未依規定執行評估及風險控管作業。 人為蓄意破壞、無意疏失、洩漏機敏資料或違反資安規範之行為。
設備失竊	設備遭竊取
其他	無法分類之項目

六、資安事件分級

(一)〔資安管理單位〕接獲資安事件通報時,應先研判該事件為資安或非資安事件,若為資安事件,依列表分級定義該資安事件等級。

(二)資安事件等級

事件衝擊 等級	評估內容
4 級	機密等級資料洩漏。 核心業務系統或資料遭受嚴重竄改或毀損。 嚴重衝擊多個業務、系統運作,影響企業聲譽
3 級	內部限閱等級資料洩漏。 影響核心業務運作或相關系統中斷服務。 影響重要業務、系統運作
2 級	一般等級,非核心業務系統。 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。
1 級	非核心業務之資產。 受到衝擊的損失程度很低,不影響業務、系統運作。

七、資安事件通報

(一)資訊安全事件發現後,發現人員應通知資安管理單位,並由資安管理單位填寫「資通安全事件通報單」並啟動處置程序。

(二)資安管理單位,應視情況尋求維護廠商或公司相關人員協助判斷,並填入「資通安全事件通報單」中。

(三)需持續向資安主管報告事件處理狀況，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「資通安事件通報單」中，呈與資安主管簽審。

(四)資安事件若 涉及利害關係人（或主管機關/情資共享機關）

(1)應依與各利害關系人，制定或要求之通報機制執行通報。

(2)通知利害關係人接獲本公司通報過程，應予留存軌跡記錄。

(3)應依據與利害關係人之合約/契約進行事件等級評估。

(4)應視利害關係人要求或依情況召開雙方資安防護會議

八、資安事件應變處理

(一) 4、3 級事件指揮官由資安主管擔任，指揮官視狀況完成緊急應變小組配置，進行異常事件排除及控制。2、1 級事件指揮官由資安管理單位主管人員擔任。

(二)資安事件等級，4、3 級事件須於 36 小時內，完成復原或損害管制；2、1 級事件須於 72 小時內復原或損害管制。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	通報對象	通報方式	處置期限
第 4 級（嚴重）	資安主管	電話（或任何可通訊手段）	接獲通報後 36 小時以內
第 3 級（重大）	資安主管		接獲通報後 36 小時以內
第 2 級（注意）	資安管理單位主管		接獲通報後 72 小時以內
第 1 級（輕微）	資安管理單位主管		接獲通報後 72 小時以內

(三)資安事件無法於評估修復完成之時間內修復

(1)通知資安主管，並需於一小時內釐清，發生事實、可能影響，並重新核定等級。

(2)重新核定之範圍、損失評估與事件等級、事故分類、判斷資源申請、採取之緊急應變措施與利害關係人，補充於【資通安全事件通報單】，並評估是否聯繫相關維護廠商協助事件處理。

(四)視事件類型採取應變程序因應，必要時得經資安主管同意後，進行備援或緊急應變作業。

(五)資安事件等級為 4 級，指揮官需成立「重大資安事件緊急應變小組」，依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，並依相關規定辦理 重訊通報。

九、資安事件追蹤調查

(一)檢討分析相關資訊以釐清事件發生的原因與責任，並分析是否會重複發生，並審視現有資訊環境的漏洞，加以修補。

(二)為有效追蹤，檢討事件原因，應審視現有環境的漏洞，細節記錄於「資通安全事件通報單」。

十、檢討改善會議

(一)若為重大等級以上資訊安全事件，於處理完畢且獲得控制後，為預防資安事件不再重複發生，須由指揮官或副指揮官召集相關單位召開資安事件檢討會議，研析問題發生之原因。

(二)依據資安事件檢討會議之結果，由系統負責人執行矯正措施，進行問題矯正的作業，以降低事件再發生的可能性。

玖、附件表單

一、年度資通安全教育訓練計畫

二、資訊保密暨資通安全規範切結書

三、資通安全事件通報單

四、資通安全管理委員會成員及分工表

茂訊電腦股份有限公司____年度資通安全教育訓練計畫

壹、依據

茂訊電腦股份有限公司之資通安全管理辦法辦理。

貳、目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行（本公司）之資通安全管理辦法，以強化（本公司）之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

叁、實施範圍（茂訊電腦股份有限公司）

本機關所屬人員：

人員類別	人數
資通安全專責人員	
一般人員	
主管人員	
共計	

肆、訓練項目

人員類別	訓練課程[1]	時數
資通安全專責人員	電子郵件安全 ○○	○○
資訊人員	資訊系統風險管理 ○○	
一般人員	資訊安全通識 ○○	○○
主管人員	○○	○○

伍、訓練課程名稱

_____

陆、訓練方式

_____

教育訓練方式(實體課程、線上課程…)。

資訊保密暨資通安全規範切結書

版次：01

為確保**茂訊電腦股份有限公司**（以下稱甲方）資訊工作之資訊通訊安全與維護公司隱私及公司業務資料等保密資訊，立切結書人（以下稱乙方）願嚴格遵守本切結書之內容，且保密義務之存續於任何期間均為有效。如有違背以致影響甲方權益遭受損害者，乙方願負擔相關法律責任：

一、資訊保密責任 乙方同意因從事甲方受託專案相關工作而經手或取得之任何形式資料（含文件、媒體、電 子檔、照片等）及業務機密與個人資料，非甲方授權不得對外提供，亦不得將獲得之全部

（或部份）資料內容以各種型式媒體重製發行，並遵守「資通安全管理法」與「個人資料保護法」等相關法令規範。

二、資通安全規範

1. 乙方因受託專案使用甲方之所有資訊系統與電腦設備（包含軟體、硬體、服務、有線或無線網路）須符合受託專案業務之需要或性質相關，不得使用於任何個人用途，亦不得妨害公務。甲方應適時執行監控管理作業，乙方應配合資通安全稽核作業。
3. 乙方應遵循智慧財產權之規範，禁止任意安裝或下載非公務需要、非經合法授權或有安全性疑慮之軟體或資料，或利用從事惡意之破壞行為，或傳送散佈具恐嚇性、暴力性、違背善良風俗之資料，或謾罵侮辱他人等不當言論。
4. 乙方為避免資訊通訊系統遭受駭客入侵、病毒攻擊或植入木馬程式致衝擊甲方營運，嚴禁連結與受託專案無關之網站，並嚴禁使用來路不明之磁片、光碟片及隨身碟。
5. 乙方應提升自我資訊通訊安全意識並遵循甲方「資通安全政策」。

三、違反責任 乙方如有違反切結書之情事或有損害甲方權益之行為時，應依法負民、刑事及行政責任。 乙方得要求接觸資訊保密責任之第三人簽署本切結書，如發現交付資訊保密責任之第三 人有違反本切結書之行為，應立即通報甲方進行緊急處置。

四、準據法與管轄法院 乙方同意以中華民國法律為準據法，並以案件分配地方法院為主。

<u>本人已詳細閱讀，並確知且接受上述切結內容。</u>

此致　　茂訊電腦股份有限公司

立切結書人	職　　稱	
電子郵件信箱	※ 建檔列管，請填具公務電子郵件信箱	
受託專案名稱		
公 司 名 稱	公司電話	
公 司 地 址		
□ 身分確認與驗證，由本公司資通安全人員簽名		

西　　元　　年　　月　　日

茂訊電腦股份有限公司

資通安全事件通報單

<table>
<tr><td colspan="4">一、通報單位聯絡資料：</td></tr>
<tr><td colspan="2">通報單位名稱：</td><td>通報人：</td><td>電話：</td></tr>
<tr><td colspan="2">通報時間：　年　月　日　時　分</td><td colspan="2">事件發生時間：　年　月　日　時　分</td></tr>
<tr><td rowspan="3">設備資料</td><td colspan="2">IP 位址：</td><td>外部 IP/Web URL：</td></tr>
<tr><td colspan="2">名稱：</td><td>安全防護機制：</td></tr>
<tr><td colspan="3">作業系統及版本：</td></tr>
<tr><td colspan="4">二、事件通報及處理事項：</td></tr>
<tr><td>事件分類</td><td colspan="3">□天然災害 □機房設施失效 □系統異常 □網路異常 □駭客入侵 □人員操作失當 □電腦或週邊失效 □設備失竊 □中毒 □其他_____</td></tr>
<tr><td colspan="4">事件狀況說明：</td></tr>
<tr><td colspan="4">可能影響及範圍評估：</td></tr>
<tr><td colspan="2">資安管理單位人員：</td><td colspan="2">通報單編號：</td></tr>
<tr><td colspan="4">三、事件分級及應變措施：</td></tr>
<tr><td colspan="4">資安事件等級：
□非資訊安全事件；□一般資訊安全事件；□1級；□2級；□3級；□4級</td></tr>
<tr><td colspan="4">應變/處置措施說明：</td></tr>
<tr><td colspan="4">事件追蹤調查：</td></tr>
<tr><td colspan="4">是否符合利害關係人通報要求 □是□否</td></tr>
<tr><td>契約客戶：</td><td></td><td>通知客戶時間：</td><td>年　月　日　時　分</td></tr>
<tr><td>主管機關：</td><td></td><td>通知機關時間：</td><td>年　月　日　時　分</td></tr>
<tr><td>情資共享機關：</td><td></td><td>通知共享時間：</td><td>年　月　日　時　分</td></tr>
<tr><td>關係通報執行人</td><td></td><td>覆核主管/人員</td><td></td></tr>
<tr><td>事件處理人員</td><td></td><td>權責主管審核</td><td></td></tr>
</table>

1. 資通安全推動小組成員及分工表

茂訊電腦資通安全推動小組成員及分工表

製表日期：___年___月___日

單位職級	名稱	職掌事項	分機	備註 （代理人）