潤弘精密工程事業(股)公司資安應變計畫

一、依據及目的

（一）依上市上櫃公司資通安全管制指引（110.12.23）及公開發行公司建立內部控制制度處理準則（110.12.28）辦理。

（二）目的：為利潤弘精密工程事業股份有限公司於遭遇資通安全事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保潤弘精密工程事業股份有限公司各項業務之正常運作，特訂定本計畫。

二、適用對象及時機

（一）適用對象：潤弘精密工程事業股份有限公司(以下稱本公司)及所屬單位。

（二）適用時機：本公司於發生重大資通安全事件或其他災害涉及資通安全事件時，應立即依本計畫辦理。

三、資通安全危機處理組織

為落實本公司資通安全預防及危機通報、緊急應變處理等相關工作，即由本公司「資訊安全室」負責執行資通安全預防及危機通報、緊急應變處理等相關工作。

四、安全防護機制

（一）本公司依「資通安全管理法施行細則」及「上市上櫃公司資通安全管控指引」，規劃建置資通系統及網路安全，整體防護環境含系統存取控管機制、連線紀錄資料庫、建構防火牆軟硬體、虛擬私人網路（VPN)、病毒掃描機制、入侵偵測系統 IDS IPS、外部弱點掃描、頻寬管理、系統內部安全漏洞檢測(更新、補強)、儲備必要之備份資料、程式或異地備援、重要文件資料檔案採取加密方式儲存等防護工具或措施。

（二）本公司「資訊安全室」執行即時偵防、監測預警工作，藉由二十四小時之監測工具（如入侵偵測系統 IDS IPS 等）掌握最新的預警訊息，並適時對公司總部、楊梅工廠、全國各工地發布告警及因應處理措施，以控制及降低資通安全事件受損程度。

（三）本公司應依「資通安全管理法施行細則」及「上市上櫃公司資通安全管控指引」制訂資訊安全政策等各項規定以執行資通安全管理工作。

（四）本公司依資通安全防護需要，經呈報總經理同意後，可協調外部資安公司協助支援執行入侵偵測、安全掃瞄、漏洞檢測修復等安全體檢工作，以做好事前防禦準備。

五、資通安全事件定義及分類

（一）內部危安事件：發現或疑似遭人為惡意變更、破壞、毀損、作業不慎等危安事件。

（二）外力入侵事件：

1. 病毒感染事件。
2. 駭客攻擊或非法入侵事件。

（三）天然災害或重大突發事件：

1. 天然災害：颱風、水災、地震或其他天然災害。
2. 重大突發事件：火災、爆炸、核子事故或其他重大突發事件。

六、資通安全事件等級

IT 資通安全事件			
等級	資料與資料庫	伺服器/ 個人電腦	網路設備
第 4 級	屬公司全面性資安事件，業務停頓或機密資料外洩，造成公司損失及信譽影響		
第 3 級	公司端重要資料或資料遭嚴重竄改毀損、系統停頓、無法於可容忍中斷時間內復原		
第 2 級	工廠、工地端資料或非核心業務資料受損，於可容忍中斷時間內恢復正常作業		
第 1 級	單一電腦或多台電腦中毒，且有擴散跡象，作業短暫停頓可快速修復		

潤弘精密工程事業(股)公司資安應變計畫

七、危機通報作業處理程序

（一）本公司所屬各單位於發現異常資安事件時，應向「資訊安全室」反應，資訊安全室應立即（最遲不得超過一個小時）研判影響等級，如嚴重程度超過含三級以上，填報「潤弘精密工程資通安全事件通報單」傳真（以下簡稱通報應變網站）臺灣電腦網路危機處理暨協調中心(TWCERT/CC)。通報登錄資通安全事件細節、影響等級及支援申請等資訊。

（二）本公司通報資通安全事件時，如因網路或電力中斷等事由，致使無法上網填報資通安全事件，與(TWCERT/CC)聯繫，先行提供事件細節，並於網路通訊恢復正常後至通報應變網站補登錄通報。(TWCERT/CC)連繫資訊如下：

1. 聯絡電話：(02) 2733-9922 (24 小時專線電話)。
2. 傳真：(02) 2733-1655。
3. 電子郵件：service@icst.org.tw。

（三）本公司所屬各單位發現疑似資通安全事件，但無法確認是否屬資通安全事件時，可填具「潤弘精密工程資通安全事件通報」請求協助研判，本公司「資訊安全室」於接獲通報後，立即研判並進行標準程序作業。

（四）本公司進行資通安全事件處理，時效性及損害管制分類如下:

3 級、4 級事件須於三十六小時內復原或完成損害管制；

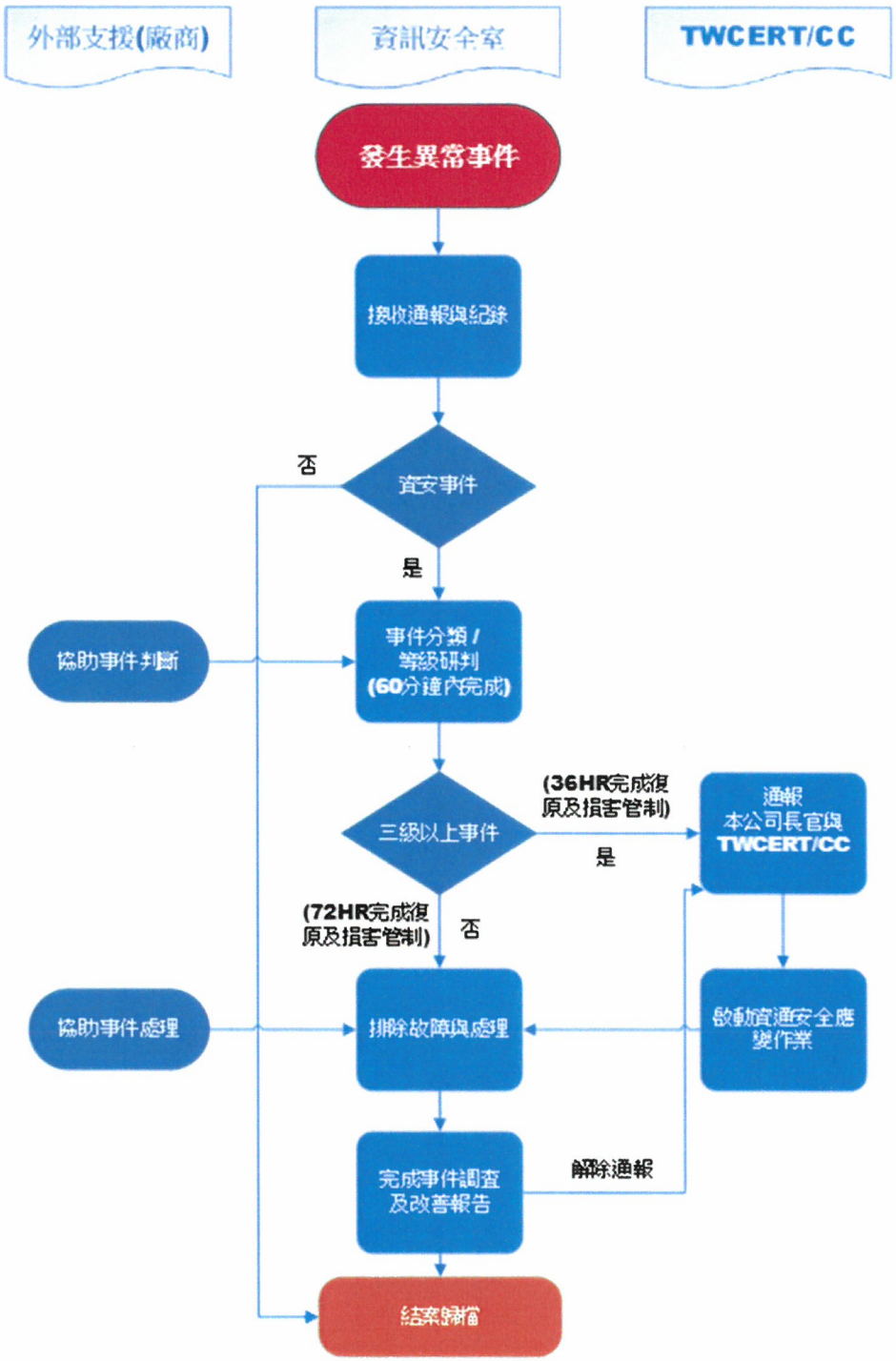
1 級、2 級事件應於七十二小時內復原或完成損害管制。

（五）本公司資通安全事件處理完畢，系統恢復正常運作時，應透過「潤弘精密工程資通安全事件通報單」以傳真、電話、電子郵件方式或上網將處理情形通報至行政院國家資通安全會報通報應變組解除事件列管，並將事件紀錄於資訊安全室以作經驗存查。

（六）本公司所屬各單位如遇資通安全事件，危及人員生命或設備遭到破壞等涉及民、刑事案件時，由資訊安全室立即通報檢調單位請求處理。如引發重大災害時，應向災害防救體系提報，請求支援處理。

（七）如發生災損，有關通報單之災害損失評估內容包括如下：作業影響情況、設備或系統損害情況、作業延誤情況、資料受損項目、估算資通訊系統作業及資料回復所需時間、備援中心設備及人員支援狀況等。

潤弘精密工程事業(股)公司資安應變計畫



附件一 潤弘精密工程資通安全事件通報單

八、緊急應變作業處理程序

（一）緊急應變優先順序：本公司所屬各單位如遇發生重大資通安全事件或其他災害涉及資通安全事件時，有關緊急應變優先順序處理原則。參照「潤弘精密工程資通安全應變作業」。

（二）資通安全事件分類緊急應變程序

1. 內部危安事件：發現或疑似遭人為惡意破壞毀損、作業不慎等危安事件時，應迅速查明事件影響狀況、受損程度等，啟用備份資料、程式或啟動備援計畫相關措施，期儘速回復正常運作。

2. 病毒感染事件：病毒入侵後，立即聯絡防毒維護廠商協助掌握電腦病毒感染最新動態，隔離病毒，避免疫情擴散；同時儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。

3. 駭客攻擊或非法入侵事件

（1）發現攻擊或被入侵時，立即隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並迅速啟動備援系統或程序。

（2）全面檢討網路安全措施、修補安全漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情事再度發生。

（3）紀錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考，並向主管機關或檢警單位反映。

4. 天然災害或重大突發事件應變程序

（1）如遇颱風、水災、地震等天然災害或火災、爆炸、核子事故、重大建築災害等重大意外事件，應迅速攜帶重要資料及程式等離開現場，以利爾後系統重置復原。

（2）如遇資通網路系統骨幹（主幹頻寬）中斷事件，應立即聯繫線路租用及網路維護廠商查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶修作業。

九、復原追蹤鑑識

（一）本公司所屬各單位因資通安全事件受損應盡速依資訊系統回復作業計畫之災難損害回復處理步驟，實施災後復原重建工作。

（二）受損部門或工地執行災後復原工作，應先檢驗資通安全環境及硬體設備是否可以正常運作，並執行環境重建、系統復原及掃描作業，其步驟包含軟硬體設備重新取得建置、重置作業系統及應用

系統，以及運轉測試等；並俟運作正常後即進行安全備份檔案下載、資料回復、資料重置等相關事宜。

（三）當危機解除後，資訊安全室將災害應變處置復原過程之完整紀錄（如事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料）建檔管制，以利爾後查考使用。

（四）資訊資產受損部門或單位如有需要，應保留事件發生之線索，經洽公司「資訊安全室」同意後，向臺灣電腦網路危機處理暨協調中心(TWCERT/CC)單位申請追蹤鑑識、偵查支援，藉研析稽核紀錄或入侵活動偵測等相關資料，釐清事件發生的原因與責任並找出防護系統之漏洞，尋求補強保護方法以避免事件再度發生。

十、獎懲標準

（一）有下列情事之一者，應為獎勵：

1. 通報之資安事件資料具時效性，足以提醒本公司所屬各單位，及早防範，防止資安事件之擴大。
2. 於資安事件通報後，積極辦理相關回復工作，降低對本公司所屬各單位內影響程度，績效顯著者。
3. 提供資訊安全室分析之紀錄，具事先預防公司及所屬單位內資安事件發生及預防效益者，應從優獎勵。
4. 公司及各單位積極推動資通安全防護及通報作業，績效卓著應從優獎勵。

（二）有下列情事之一者，應為懲處：

1. 本公司所屬各單位通報之資安事件資料，經查明如有不實之處，將依法處置。
2. 未遵循本計畫進行資安事件通報、應變作業，致使公司及投資人權益損失情形嚴重者，除公司內部依相關辦法懲處外，若遭金管會懲處亦須依相關法令規章進行人事處分。

(三)上述相關標準依公司獎懲辦法相關規定辦理。

附件一 潤弘精密工程資通安全事件通報單
附件二 潤弘精密工程資通安全保密同意書
附件三 潤弘精密工程委外廠商執行人員保密切結同意書
附件四 潤弘精密工程年度資通安全教育訓練計畫
附件五 潤弘精密工程資通安全認知宣導及教育訓練簽到表
附件六 潤弘精密工程資通安全應變作業
附件七 潤弘精密工程資訊安全人員負責設備表
附件八 潤弘精密工程資通安全維護計畫實施情形
附件九 潤弘精密工程資通事件調查及改善報告

附件一

潤弘精密工程事業股份有限公司
資安事件通報應變標準作業程序單

通報時間：_____年_____月_____日_____時_____分

一、發生資安事件單位資料：

部門：_____ 聯絡人：_____ 分機：_____

二、資安事件通報事項：

1. 事件發生時間：_____年_____月_____日_____時_____分

2. 事件說明:

◎事件分類：□非法入侵 □感染病毒 □服務中斷 □其他 _____

◎破壞程度：□系統當機 □資料庫毀損 □網頁遭篡改 □其他_____

◎影響範圍及損失評估：_____

_____

3. 設備資料：

◎IP 位址(IP Address)：內部 IP：_____外部 IP：_____

◎網際網路位置(Web-URL)：_____

◎設備廠牌、機型：_____

◎作業系統名稱、版本：_____

◎已裝置之安全機制：□防火牆□防毒軟體□其他_____

◎維護廠商：□無□有：_____

4. 解決方式：□自行解決□請求資訊安全室支援□其他_____

5. 改善情況及因應措施 ：

通報單位人員	
承辦人	單位主管或其職務代理人

以下資料，由資訊安全室填寫

本次資安事件處理方式：

☐通報國家資通安全通報應變網站

☐通報決策高層及集團資訊處

☐通報證交所/櫃買中心

☐更新防毒軟體病毒碼、修補作業系統及應用程式漏洞，並進行掃描以清除病毒、漏洞

☐更新入侵偵測系統攻擊碼與防火牆規則

☐通報單位已自行處理完畢，所內結案

☐彙整資安事件相關資料，供交易所備查

☐其他：

解決時間：_____年_____月_____日_____時_____分

資訊安全室	資訊安全長或其職務代理人

附件二

潤弘精密工程事業股份有限公司
資通安全保密同意書

立同意書人　　於民國　　年　　月　　日起於　　任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。

二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：　　(簽章)

身份證字號：

服務單位：

中　華　民　國　　年　　月　　日

附件三

潤弘精密工程事業股份有限公司
委外廠商執行人員保密切結書

立切結書人.....（簽署人姓名）等，至潤弘精密工程事業股份有限公司(以下稱本公司)處理資訊業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經本公司資訊安全室人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將本公司之資訊設備、檔案及簽呈文件、文書攜出。

二、 未經本公司資訊安全室確認並代為申請核准，不得任意將攜入之資訊設備連接網路。

三、 本公司得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

四、 本保密切結書不因立切結書人離職而失效。

五、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章

身分證字號

聯絡電話及戶籍地址

中　華　民　國　　年　　月　　日

附件四

潤弘精密工程事業股份有限公司
年度資通安全教育訓練計畫

潤弘精密工程事業(股)有限公司年度資通安全教育訓練計畫

壹、依據

潤弘精密工程事業(股)有限公司之資通安全應變計畫辦理。

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（本公司之資通安全應變計畫，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。

參、實施範圍

本公司所屬人員：

肆、訓練項目

※可參考行政院國家資通安全會報技術服務中心之資安職能課程項目，網址：https://www.nccst.nat.gov.tw/Capacity?lang=zh

伍、訓練期程

由本公司自行排定教育訓練期程。

陸、訓練方式

由本公司自行決定教育訓練方式(實體課程、線上課程…)。

附件五

潤弘精密工程事業股份有限公司

資通安全認知宣導及教育訓練 簽到表

課程名稱：資安宣導課程-案例分享、資安防護重點及社交工程等

時　間：112年　月　日 8：00－9：00

地　點：

簽　到：

部　門	姓　名	部　門	姓　名

附件六

潤弘精密工程事業股份有限公司
資通安全應變作業

本公司之資訊、通訊系統因影響公司營運經營甚鉅，依資通安全應變計畫提出資通安全應變作業，針對資通安全可能遭受的危及狀況，進行以下應變作業以維持正常營運運作：

資安應變作業執行項目

- ☐ 資通環境復原建置 (天災或破壞)
- ☐ 電力線斷線復原
- ☐ 電力跳電復原
- ☐ UPS故障復原
- ☐ 網路通訊斷線復原
- ☐ 網路通訊設備故障復原
- ☐ 主機設備故障復原
- ☐ 中斷對外網路，封鎖入侵管道 (駭客入侵)
- ☐ 清除病毒 (病毒感染)
- ☐ Veeam還原 (台北、楊梅)
- ☐ RHFILE還原
- ☐ ERNAS還原
- ☐ Windows VSS還原
- ☐ PURE STORAGE快照還原
- ☐ 龍潭端DR備份還原
- ☐ 龍潭主機攜回總公司開機
- ☐ 工地NAS備份還原
- ☐ 研發NAS備份還原
- ☐ 其他或說明

附件七

潤弘精密工程事業（股）資訊事件應變計畫

TPE HQ 資訊安全人員負責設備表

負責人 / 設備項目	林明毅	洪以昇	謝易勳	姚長宇	資訊處 資安支援
資訊安全監控項目	■	■	■		
防火牆防護項目（CP+Forti80）			■		■
網頁應用程式防火牆		■			
入侵偵測/防禦系統(IDS+IPS)工地端	■	■	■	■	
入侵偵測/防禦系統(IDS+IPS)HQ 總部			■		■
防毒中心主機(RTC Apex one)				■	
AD Server (rtc.ruentex.corp)	■	■			
Network Device 監控				■	
Mail SPAM(郵件防護系統)					■
End User 電腦及相關設備	■	■	■	■	

潤弘精密工程事業（股）資訊事件應變計畫

楊梅工廠　資訊安全人員負責設備表

負責人 / 設備項目	林明毅	曾采葳	謝易勳	姚長宇	資訊處 資安支援
資訊安全監控項目	■	■	■		
防火牆防護項目（CP+Forti80）			■		■
網頁應用程式防火牆		■			
入侵偵測/防禦系統(IDS+IPS)HQ 總部			■		■
防毒中心主機(RTC Apex one)				■	
AD Server (rtc.ruentex.corp)		■		■	
Network Device 監控		■			
Mail SPAM(郵件防護系統)					■
End User 電腦及相關設備		■			

附件八

潤弘精密工程事業股份有限公司
資通安全維護計畫實施情形

本公司之主機系統資料因影響公司營運經營甚鉅，依資通安全應變計畫，提出本（112）年度資通安全維護計畫實施情形、執行成果及相關說明如下所示：

一. 備份情形

是 □ 否 □ Windows VSS
是 □ 否 □ Veeam備份 (台北、楊梅)
是 □ 否 □ PURE STORAGE快照
是 □ 否 □ ERNAS BACKUP (磁帶)
是 □ 否 □ RHFILE備份(磁帶)
是 □ 否 □ 研發NAS備份
是 □ 否 □ 工地NAS備份
其他

二. 異地備份情形

是 □ 否 □ 台北公司系統於龍潭端備份
是 □ 否 □ 楊梅工廠重要資料備份於台北公司
其他

三. 災害演練

是 □ 否 □ 龍潭端備援回台北公司開機
其他

附件九

潤弘精密工程事業股份有限公司
潤弘精密工程資通事件調查及改善報告

本公司針對資通安全事件的發生，依資通安全應變計畫，提出事件調查並進行改善措施報告，以供備查及回饋。

一. 資通事件日期時間

二. 資通事件發生原因

三. 資通事件處理過程

四. 資通事件改善說明