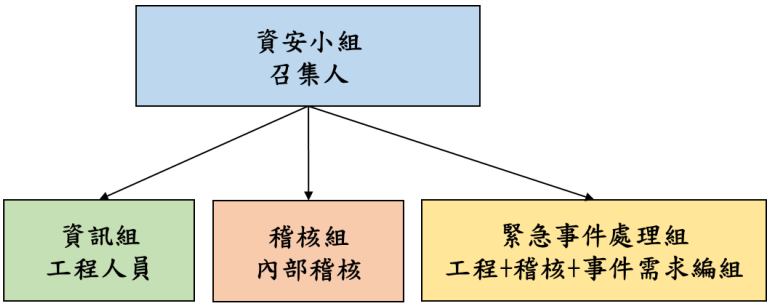
利機企業股份有限公司
114 年度資通安全管理執行報告

一、 資通安全管理策略與架構：

（一）資通安全風險管理架構

1. 本公司成立資通安全小組，落實資通安全管理，成員包含高階主管(經理級以上)、資訊組工程人員、稽核組稽核人員，負責督導、維運與稽核，資安管理事項請參閱下列 6 項說明，資通安全小組架構請參閱圖一。
2. 資通安全小組執行事項:
   [1] 資通安全規範建立與督導。
   [2] 資通安全作業執行與協調。
   [3] 資安緊急事件處置與監督。
   [4] 資通安全事件檢討與改善。
   [5] 相關資訊安全事項執行與稽核。
   [6] 定期召開資訊安全會議。



召　集　人　：高階主管
工 程 人 員 ：由資訊部門成員組成
內 部 稽 核 ：由公司稽核人員組成
事件需求編組: 依事件需要進行臨時編組

圖一、資通安全小組架構圖

3. 本公司稽核組為資訊安全監理之查核單位，若查核發現缺失，隨即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。
4. 資訊安全工作-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。

（二）資通安全政策

為確保本公司資通訊作業安全與穩定之運作，提供可信賴之資通訊服務，並順利推展本公司各項業務，符合資通安全管理作業，本公司資通安全政策將落實下列政策原則。

1. 兼顧資訊安全與便利使用。
2. 避免內外部的資安風險。
3. 確保服務穩定可用。
4. 達成企業永續經營。

（三）具體管理方案

因應近年資安事件頻傳，本公司針對各項資訊系統與規則強化管理機制，具體方案如下:

1. 制定使用者設備的使用規則，區隔並限制私人設備與公司設備的使用環境與上網權限，嚴禁非允許設備使用內部網路，並針對隨身碟等外部儲存裝置需經過檢測方可於公司電腦使用。
2. 個人電腦與資訊主機定期執行病毒掃描，安全性更新，並每年針對公司重大資訊系統執行弱點掃瞄，修補安全漏洞。
3. 強化資料備份頻率與異地資料保存。
4. 加強員工資安觀念，定期透過會議、公告、企業內部網站等，向同仁宣導資安觀念與個案分享，如有可疑之資料及電子郵件請勿輕易開啟，避免遭到社交工程攻擊。
5. 加入資安聯防組織與定期參與資安相關研討會，透過資安訊息分享隨時提升資安資訊與防護知識，避免訊息孤島，衍生防護漏洞。

（四）投入資通安全管理之資源

本公司持續投入資訊安全與資料保護，個資保護等相關作業，資源投入事項包含完善治理面及技術面之安全基礎架構、強化資安防禦設備、與教育訓練等，每年檢討公司資安防護狀況，適時更新資安防護設備，防護效果最佳化。

二、 資通安全管理執行報告：

(一)114 年度資安推行成果:

1. 資訊系統災難復原模擬演練，每年 1 次演練，完成率 100%。
2. 每季資安宣導暨重要資安宣導，每年 4 次，完成率 100%。
3. 資安同仁參與資安相關研討會或訓練，每年二次，完成率 100%。
4. 委外廠商進行主機弱點掃描與修補，完成率 100%。
5. 重點主機導入 MDR 資安防護機制，完成率 100%。
6. IST 監控管理系統持續部署至新版主機並建置管理報表。
7. SCM 系統升級至新版 SQL 2022 系統、完成漏洞修補並切斷 VPN 專線，有效減少駭客侵入管道。
8. 展開 ERP 更換暨相關系統導入，利於系統升級改版，提升資安效能。

(二)115 年度預計推廣項目:

1. 資訊系統災難復原模擬演練，每年 1 次演練。
2. 每季資安宣導暨重要資安宣導，每年 4 次。
3. 資安同仁參與資安相關研討會或訓練，每年二次。
4. 委外廠商進行主機弱點掃描與修補。
5. 委外廠商實施社交工程暨資安防護演練。
6. 持續進行 ERP 暨相關系統之導入，強化資安效能。

三、 資通安全風險與因應措施：

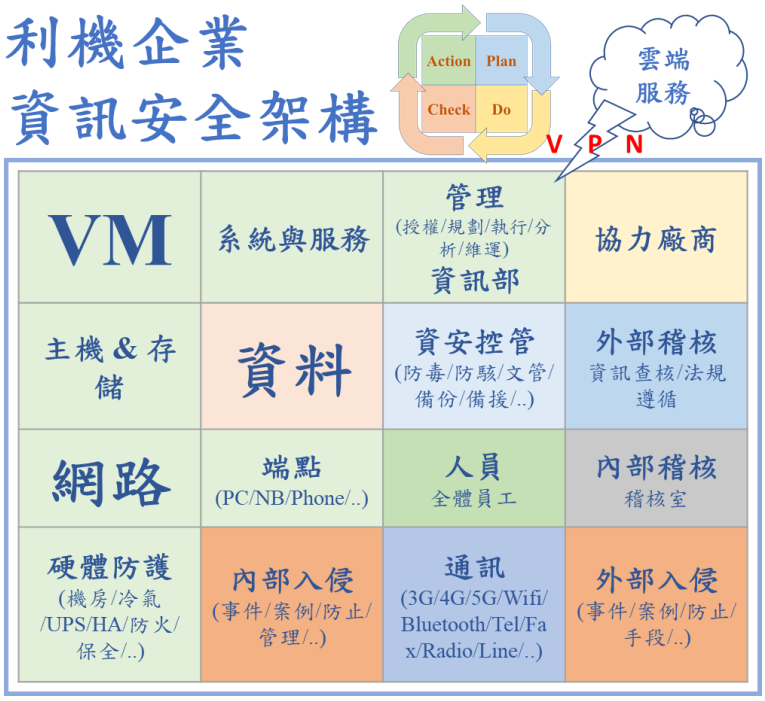
1. 資通安全風險說明與因應原則:

本公司依據所處產業特性，建立合適且完整的資訊管理系統，確保在半導體與科技產業中，能夠隨時面對產業與技術的世代更迭，並滿足不同的業務與營運型態，隨時保持最佳的資訊處理與整合能力，因此針對資訊安全面，公司建構完整的網路與電腦系統管理機制以符合利害關係人與相關法規之要求，並透過持續每年配合稽核機構的風險評鑑與定期資安風險評估，運用系統升級與資安強化，有效維持公司資訊安全與長期競爭力之目的。

利機公司過去網頁曾經遭受駭客攻擊，並植入惡意跳板程式，未來也可能面臨類似的攻擊。為了預防及降低此類攻擊所造成的傷害，利機公司落實相關改進措施並持續更新，並制定資訊安全執行措施。

2. 資訊安全執行措施:

針對近年資安事件頻傳，除上述說明與因應原則外，實務上強化建置網路防火牆與網路權限管理以防止駭客攻擊，並建置主機與端點防毒與掃毒系統，針對內含惡意附件的信件或病毒軟體有效防護，避免滲透進入公司，防止電腦病毒跨機台及跨廠區擴散，加強釣魚郵件偵測與資安宣導，此外利機公司因應專案需求需要分享高度敏感及機密的資訊給部分第三方廠商，以使其能提供相關服務，利機公司在和第三方服務廠商簽訂之服務合約中，要求其遵守保密與網路安全規定。每年委外專業廠商進行系統漏洞偵測與防護補強措施，搭配不定期資安宣導並執行員工警覺性測試，建構多層嚴密防護機制，實施嚴格資安控管，除上述做法外，仍針對各項資訊服務建構完整的資訊安全架構(參閱圖二)，並擬定相關作業措施(參閱表一)。



圖二、資訊安全管理架構圖

表一、資訊安全具體作業措施

架構區塊	說明	相關配置措施及作業
VM	虛擬主機系統的資安控管措施	建立 HA 架構, 減少停機損失。
		系統服務區隔避免相互影響，提高系統服務可用度。
主機&存儲	主機與存儲系統的資安控管措施	各分點配置 2 部以上主機以達成即時備援作業。
		一線存儲均使用 RAID5 以上的保護架構，並適當規劃備份作業。
網路	網路連線層的控制措施	各分點配置防火牆進行資安管控。

架構區塊	說明	相關配置措施及作業
		分點及端點連線使用 VPN 連線。
硬體防護	機房內的防護措施	獨立 2 組以上空調確保主機作業溫溼度正常。
		使用 ON-LINE UPS 確保電源穩定及短時間斷電不受影響。
		配置機房專用二氧化碳滅火器。
		保全連線確保災害發生時可第一時間通知處理。
系統與服務	各資訊系統的控制及防護措施	系統各模組操作均設定權限，登入均需通過 AD 帳號安控驗證。
		存取資料均留下 LOG 軌跡以供稽查。
資料	電子資料的控制及防護措施	操作需通過 AD 帳號安控驗證。
		存取資料均留下 LOG 軌跡以供稽查。
		資料依重要性進行多層備份機制（含異地備份）。
		定期災害復原演練。
端點	端點的控制及防護措施	操作需通過 AD 帳號安控驗證。
		PC 筆電均安裝防毒軟體。
		重要電腦安裝文件加密系統。
資安控管	資訊部的資安控管及防護作業	配置防毒主機中央管控，確保更新成功及異常管理。
		防火牆管理，確保連線有依企業安全政策。
		配置文管系統主機管理，確保機密文件存取安全及發現異常存取記錄。
		備份管理，檢查備份均確實完成並可被驗證復原。
		主機/電腦弱點檢測及更新措施。
		病毒防護與惡意程式檢測。
		BI 分析 LOG，異常監控處理。
		定期災害復原演練。

架構區塊	說明	相關配置措施及作業
管理	資訊系統管理維運的控制及防護措施	系統的權限規劃［授權、操作、執行、設定］均使用 AD 帳號密碼驗證 確保作業均被核准且有跡可查。
		資訊部依［主管命令，稽核建議，內部優化，使用者申請經主管核准］進行資安控管及設定。
		規劃制訂災害復原計劃並定期檢查備份作業記錄。
		監控系統服務及網路可用狀態並建立通報機制。
人員	企業內部人員的資安控管及防護作業	內部員工接受資訊安全宣導及法規遵循宣導。
		有資訊系統作業的使用者均配發 AD 帳號並定期更換密碼，所有系統操作及權限均需使用 AD 驗證並留下登入軌跡。
通訊	對於其他通訊管道的資安控管及防護作業	企業內網與個人用網路區隔管控。
		內部電腦系統除特殊授權外禁止連接 Gmail、Line、Skype 等通訊軟體，以管控資通管道。
協力廠商	廠商協助作業的控制及保護措施	廠商維護合約均有簽訂保密條款。
		廠商連線作業事前需電話申請並使用 VPN 連線。
		連線作業均留下 LOG 記錄以供稽查。
內部入侵	對於內部入侵的資安控管及防護作業	參考其他企業發生案例或內部事件，調控內部資安規則避免資安風險。
外部入侵	對於外部入侵的資安控管及防護作業	參考其他企業發生案例或外部事件，調控外部資安規則避免資安風險。
內部稽核	內部資安稽核作業	稽核室定期進行資訊安全稽核作業，確保資安防控作業確實有效。
外部稽核	外部資訊稽核作業	外部定期進行資訊安全稽核作業，以供會計師簽查核，並提供完善資安管理規劃建議。
雲端	雲端系統的資安控管及防護作業	內部與雲端系統的資料連線均採加密驗證通道進行。
		連線通訊經防火牆並留下 LOG 記錄以供稽查。
		設定系統異常主動通報，並定期監看服務報告。
備註: 因資訊系統會不斷進行完善更新作業，資安控管防護作業並非一成不變，會因應現實狀況進行優化及調整安控方式及作法。		

四、重大資通安全事件：

本公司近四年(2022-2025)並無資通安全風險對公司財務業務造成影響(請參閱表二)。

表二、近四年資通安全事件統計表

資安事件件數/年度	2022	2023	2024	2025
違反資安或網路安全事件數	0	0	0	0
商業資訊洩漏事件數	0	0	0	0
個資洩漏事件數(含員工與客戶資訊)	0	0	0	0
因資訊洩漏受影響事件數	0	0	0	0
因資安事件遭受損失件數	0	0	0	0