文件名稱	資訊安全規範			頁次/頁數	1 / 35
文件編號				制/修訂單位	資訊部
制定日期	96/12 /1	修訂日期	107/ 12 /11	版本/版次	

洋華光電股份有限公司

資訊安全規範

目錄

壹、資訊安全規範概要

一、前言

為確保洋華光電股份有限公司(以下簡稱本公司)有關資料、資訊系統、設備及網路之安全，特訂定本規範，作為本公司有關資訊安全管理組織權責分工、人員教育訓練、電腦硬軟體、網路環境管理之準則。

二、目標

本公司資訊安全管理目標如下:

（一）維持資訊系統持續運作

（二）防止駭客、病毒等入侵及破壞

（三）防止人為意圖不當及不法使用

（四）避免人為疏失造成系統意外問題

三、範圍

本規範管理之範圍包括人員、應用系統、硬體設備及網路設施等四部分。

（一）人員

涵概本公司正式人員、約聘雇人員及使用本公司資訊資源之委外廠商人員。

（二）應用系統

1.ERP 系統

2.郵件伺服器

3.檔案伺服器

4.Windows 帳號管理伺服器(AD)

5.網際網路應用：

6.內部網路 AP 應用

（三）硬體設備

各式主機、伺服器及個人電腦。

（四）網路及其設施

本公司台北辦公室、觀音廠、越南河內廠三地辦公室、網際網路之數據專線及相關網路設施。

四、內容

本規範內容包括如下：

壹. 人員管理及教育訓練
貳. 電腦系統安全管理
參. 網路安全管理
肆. 系統存取安全管理
伍. 系統發展及維護安全管理
陸. 資訊設備實體及環境安全管理
柒. 備援回復作業計畫

貳、人員管理及教育訓練

一、員工資訊訓練

(一) 新進人員需於新人訓練時，由人資部協助進行資訊安全規範 簽名與人事資料統一歸檔。

(二)本公司各級主管應負責督導屬員之資訊作業安全，防範不法及不當行為；對可存取機密性、敏感性資訊或系統者及配賦系統存取特別權限之人員，應妥適分工，分散權責，並視需要建立制衡機制。

(三) 離職、退休人員，應立即取消其所有電腦系統帳號與密碼，取消系統使用權限。

二、員工維護資訊安全及公務機密責任

(一)本公司資訊安全規範應以書面、電子或其他方式告知員工，員工應遵守本計畫所訂定之規範及其他相關資訊安全規定。員工若違反資訊安全相關規定，得依情節輕重予以處分。

三、資訊安全教育訓練

(一) 依員工角色及職務層級，進行適當的資訊安全宣導(如：資訊安全、病毒介紹及其防範作業等)，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

(二) 隨時公告資訊安全如病毒等相關訊息。

參、電腦系統安全管理

一、電腦系統作業程序及責任

(一) 資訊安全事件之管理

1、應建立處理資訊安全事件之作業程序及權責分工。

2、應訂定下列資訊安全事件之處理程序

(1)資訊電腦緊急應變計畫

當資訊系統當機後經處理並恢復正常時，應確認安全控制系統是否完整及正確。

(2)災難復原計畫

發生資訊安全事件時，依影響程度向主管報告處理情形。

(3)系統異常報告

緊急事件處理的過程，應予記錄以備日後查考。

3、除災難復原計畫與緊急應變計畫外，系統異常報告尚應納入下列事項：

(1)導致資訊安全事件之原因分析。

(2)防止類似事件再發生之補救措施的規劃及執行。

4、處理資訊安全及電腦當機事件，依下列原則辦理：

(1)系統恢復正常時，應確認安全控制系統是否完整及正確。
(2)發生資訊安全事件時，依影響程度向主管報告處理情形。
(3)緊急處理的過程，應予記錄，以備日後查考。

（二）資訊安全責任之分散

1、對關鍵性的資訊工作項目，應將資訊安全管理及執行的責任分散，分別賦與相關人員必要之責任。

2、下列工作項目視作業需要與執行人力資源狀況，儘可能授權分由不同的人員執行：

（1）應用系統之使用。

（2）資料建檔。

（3）電腦作業。

（4）網路管理。

（5）系統行政管理。

（6）系統發展及維護。

（7）變更管理。

（8）安全管理。

（三）系統開發及正式作業之區隔

1、為降低風險，應將系統開發及正式作業分開處理，以減少作業軟體或資料遭意外竄改，或遭未經授權的存取。

2、系統開發及正式作業分開處理，應考量下列安控措施：

（1）儘可能在不同的伺服器、不同的系統環境以區隔作業。
（2）維護正式作業系統時，應依安全控管程序處理。
（3）系統開發及正式作業使用不同的登入帳號，以減少風險。
（4）不直接以正式作業之資料做測試用途。

（四）資訊作業委外服務之安全管理

1、資訊作業委外時，應於事前評估潛在風險（如帳號或密碼遭破解、系統被破壞或資料被竊取等），與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款

2、資訊委外服務契約應註明事項如下：

（1）業者應遵守的資訊保密協議書。

（2）業者處理及通報事件的責任及程序。

（3）業者應配合事項。

二、系統管理規劃

（一）備援作業之規劃

1、應規劃資訊系統設備損害或電腦當機時，可維持本公司業務繼續正常作業的備援方案。

2、應定期演練備援作業程序。

（二）系統變更之管理

1、資訊設施及系統的變更，應建立控制及管理機制，以免造成系統安全上的漏洞。

2、系統變更之管理，應填寫”系統修改記錄表”,包括下列事項：

（1）界定及記錄重大變更的事項。

（2）評估系統變更之可能衝擊。

（3）建立系統變更之程序。

（4）與相關使用者事前溝通系統變更之細節。

（5）系統變更不能順利執行時之回復作業程序及責任，或放棄執行系統變更之作業程序及責任。

三、電腦病毒及惡意軟體之防範

(一)電腦病毒及惡意軟體之控制

本公司伺服器及個人電腦應採行必要的事前預防及保護措施,防制及偵測電腦病毒及惡意軟體等的侵入;促使員工正確認知電腦病毒的威脅,提升員工的資訊安全警覺,健全系統之存取控制機制。

(二)電腦病毒防範應考量的重要原則

1、各單位及使用者應遵守軟體授權規定,禁止使用未取得授權的軟體。

2、不定期公告重大危害病毒將發作之日期、相關資訊。

3、使用電腦病毒防制軟體,應依下列原則:

(1)電腦病毒防治軟體及病毒碼應每日更新版本。

(2)應提供即時掃瞄電腦系統及資料儲存媒體功能。

(3)使用可掃除電腦病毒及回復系統功能的解毒軟體。

四、軟體版權之控管

(一)本公司有關軟體之使用,應遵守相關法令及契約規定。

(二)軟體版權管理應考量下列事項:

1、禁止員工保有或使用未取得授權的軟體。

2、禁止員工在未取得授權同意前,將軟體安裝到電腦設備上。

3、須在原授權許可之外的電腦設備上使用軟體時,應取得正式的授權或另行採購。

4、應不定期稽核軟體使用情形。

五、日常作業之安全管理

（一）資料備份

1、應定期執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

2、系統資料備份及備援作業，應符合本公司業務持續運作之需求。

3、資料備份作業原則如下：

（1）備份資料應另異地存放，異地存放時，有專人負責運送，並填寫 ”檔案系統備份記錄表”，紀錄運送時間及內容、人員姓名。以降低發生災害時可能帶來的傷害；存放處所環境應儘可能不低於電腦機房的安全標準。

（2）重要資料的備份，應至少保留三個循環以上。

（3）依災難復原辦法每半年執行測試備份資料，以確保備份資料之可用性。

（4）資料的保存時間應由使用單位訂定。

（二）系統錯誤事項之處理

1、系統發生錯誤時，應迅速報告權責主管人員，並採取必要的更正行動。

2、使用者對電腦及通信網路系統錯誤的報告，應於系統異常處理表詳實記錄，以供日後查考。

3、緊急應變處理程序的作業規定如下：

（1）應檢查錯誤處理的紀錄，確保系統作業已經恢復正常。

（2）應檢查更正作業是否妥適，確保更正作業未破壞系統原有的安控措施，及確保更正作業係依正當的授權程序辦理。

（三）電腦機房環境之監控

1. 電腦機房環境如溫度、溼度及電源供應之品質等，應依據設備規格建置；並建立監控系統，隨時監控電腦作業環境狀況。

六、電腦媒體之管理

（一）電腦媒體之使用管理

1、應納入管理之電腦媒體包括可攜帶移動的磁帶、磁碟、光碟、電腦列印報表、作業程序目錄及系統文件等。

2、電腦媒體儲存環境應建置下列安全控管措施：

（1）儘量使用代碼標示媒體儲存的資料內容。
（2）儲存媒體報廢時，不再繼續使用時，應將儲存的內容消除。
（3）儲存媒體應依保存規格要求，存放在安全的環境。

（二）媒體處理之安全

內含機密性或敏感性資料的媒體報廢時，應由專人以安全的方式處理，例如：燒毀、以碎紙機處理，或將資料從媒體中完全清除。

電腦媒體報廢時之流程如下：

1、使用單位填寫“資訊服務申請單”，並由資訊部協助判斷。

2、資訊部門人員親臨現場並了解問題癥結或是接收需報廢資訊媒體。

3、經判定需廠商維修之設備需移除”資料儲存”設備，如硬碟；由資訊部人員
4、報廢時應有兩人以上在場，並留下相片等相關紀錄。

電腦媒體報廢方式如下：

1、硬碟、軟碟、可抹除式光碟 ： 將其重新格式化後可重複使用

2、一次性寫入光碟 ： 直接將光碟片銷燬

3、紙本文件 ： 統一送至碎紙機銷燬

肆、網路安全管理

一、網路安全規劃與管理

（一）網路安全規劃作業

1、建立電腦網路系統的安全標準、程序及準則之控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取。

2、定期檢討電腦網路安全事項之執行。

3、引進具網路監控能力的防火牆(Fire Wall)，以控管外界與本公司內部網路之間的資料傳輸與資源存取。

4、得邀請網路安全專家診斷本公司網路運作環境之安全性漏洞。

5、隨時公告有關電腦網路安全之各項事宜。

6、利用公眾網路傳送敏感性資訊，須採取資料加密之保護措施如 VPN 連線之管理方式。

（二）網路服務之管理

1、網路服務系統的最高使用權限，應經由權責主管指派相關人員管理。

2、網路管理工作之職權可分由不同人員負責，並明定職務代理人。

3、網路系統管理人員負責執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性。

4、本公司員工之使用者帳號由資訊部系統人員負責建立；新進人員於報到時填寫申請表格，並交由資訊部人員處理；人員離職時，系統人員應於離職生效日起，撤銷其使用者帳號。

5、非經總經理或副總(含)以上單位主管許可，網路系統管理人員不得私自閱覽他人之檔案或資料。

6、對任何網路安全事件，網路系統管理人員應循資訊電腦緊急應變計畫向資訊主管反應。

7、管理人員不得新增、刪除、修改系統日誌檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。

8、建立電腦網路系統之防毒機制，以確保資料之安全性及正確性。

（三）網域使用者之管理

1、本公司員工經申請網域帳號後成為合法授權的網域使用者（以下簡稱網域使用者）,並在授權範圍內存取網路資源。
2、本公司網域使用者應遵循以下規定：

(1) 禁止不當取得公司機密資料以及洩露公司機密性資料給未經授權之他人。

(2) 未經副總（含）以上單位主管簽核同意，不得將其他電腦設備或廠商的電腦

連接上本公司電腦網路。

(3) 除經審核發給之隨身碟、光碟機、燒錄機外，禁止將電腦私自外接隨身碟、光碟機、燒錄機、數據機等具有儲存、複製、通訊功能之週邊設備，以保障公司智慧產權。

(4) 未經允許，不得使用他人或未經授權之電腦。離開電腦十分鐘以上時間，電腦啟動螢幕保護程式。

(5) 不得將自己的登入帳號與密碼交付他人使用。

(6) 未經資訊單位授權，不得擅自搬移資訊設備，人員離職或到任，需填寫固定資產增置異動單，將該員保管之資訊設備進行轉入或轉出。

(7) 禁止安裝使用未授權軟體，若在工作上確有使用需要，應循正常請購程序，經資訊相關單位會簽後彙整購置。

(8) 禁止將色情檔案建置在本公司網路，亦不得在網路上散播不法、不當或違反善良風俗習慣的資料。

(9) 禁止利用本公司網路從事不法、不當得利之情事。

(10) 網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。

（四）主機之安全防護

1、不直接提供遠端登入，以避免資料經由電話線路或網際網路傳送時，被偷窺或截取(如一般網路服務 Telnet、FTP 等的登入密碼)。

2、防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

（五）防火牆之安全管理

1、本公司網路之節點，依作業需求與安全等級，設置防火牆區隔內、外網路，以控管外界與內部網路之間的資料傳輸與資源存取。

2、本公司網路防火牆設置防禦區域(Military Zone)與非戰區域(De Military Zone)，以區隔內外網路服務的使用層級；提供本公司內部服務與使用之資源設置於防禦區域，提供對外服務性質之伺服器(如 Web Server、DNS 等)設置於非戰區域。

3、外界網路需經申請始可使用[防禦區域]提供的服務。

4、網路防火牆應由專人執行控管設定，並隨時檢核日誌。

5、防火牆設置完成時，由系統管理人員負責測試，直到符合既定的安全目標。

6、網路系統管理人員應配合本公司資訊安全規範及規定的異動，檢討及調整防火牆系統設定及取存權限，並填寫資訊系統修改申請表並經簽核通過後執行，以保持安全的防禦狀況。

7、網路系統管理人員應負責網路安全問題，並維持正確的版本，以因應各種網路攻擊。

8、對於與本公司往來之廠商與客戶，由接洽單位填寫管制類資訊作業需求申請表經由部處主管核准後，由資訊部開放使用 VPN(Virtual Private Network)，以確保資料傳遞的保密與安全。

（六）資訊、軟體下載之管制

1、禁止下載未經授權使用的檔案或軟體。

2、禁止下載、放置或傳遞與工作內容無相關的檔案資料，如電動玩具程式與音樂檔案。

3、不得瀏覽與工作內容無關之網站。

（七）網路資訊之管理

1、對外開放的資訊系統，應儘可能安裝在一部專用的主機上，並以防火牆與本公司內部網路區隔，提高內部網路的安全性。

2、對外開放的資訊系統，應針對蓄意破壞者可能以發送作業系統指令或傳送大量

資料(如電子郵件、註冊或申請資料)導致系統作業癱瘓等情事，預作有效的防範，以免影響本公司的服務品質。

3、機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

4、網路系統管理人員得監督網路資料使用情形，檢查有無違反資訊安全規定之事件發生視需要通報其主管。

5、對外開放的資訊系統所提供之網路服務(FTP、HTTP 等)，應做適當的存取控管，以維護系統正常運作。

二、電子郵件之安全管理

本公司電子郵件的安全管理規定如下：

1、電子郵件接收後應自行保管，並立即自郵件系統信箱中刪除。

2、不得以電子郵件等方式洩漏公司機密資料。

3、未經總經理簽核同意，不得直接將 E-mail 傳送給全體同仁。

4、對來路不明的電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞；並應通知電子郵件系統管理者處理。

5、禁止發送電子郵件騷擾他人，導致其他使用者之不安與不便。

6、單一郵件寄送人數上限設定為 30 人，若有特別需求需各別提出經由總經理簽核後執行。

7、單一郵件寄送容量限制為 10MB，若有特別需求需各別提出經由單位主管簽核後執行。

8、 公司內部禁止使用網際網路所提供之”免費/收費郵件信箱”，以防止公司機密資訊洩漏。

三、網際網路應用之安全管理

(一）網路設備與系統之備援

1、為維持本公司網路的持續正常運作，各重要網路設備應有備援。

2、對必要之網路硬體設備使用不斷電系統(UPS)。

3、為確保內部網路與外界的服務持續暢通，內部網路與外界網路的連接，視實際需要建制一個以上的替代路徑。

4、網路系統中之各網路設備應不定期(系統架構設定變更時)將系統設定檔做備份。

（二）網路入侵之處理

1、若發現網路被入侵或疑似被入侵時(如：網頁遭竄改、分散式攻擊、資料非法存取、密碼被破解等)，應依照緊急應變程序處理，並採取必要的通知。

四、網路安全稽核

（一）網路安全稽核事項

1、操作紀錄及作業紀錄應至少保存二星期以上。

2、對於通過防火牆之各項連線資訊，均應予詳細記錄。

3、各服務伺服主機應詳細紀載各項連結服務的作業紀錄(system log) 。

4、對網路系統管理人員或資訊安全主管的操作，應建立資訊系統修改申請表，經

核准後執行。

（二）警示系統

1、視需要建立警示系統，讓網路系統管理人員在特定的網路安全事件發生時(例如:當有不明的使用者連續嘗試侵入時)，及時獲得警示性的訊號，俾利採取有效的防範措施，減少網路安全事件的發生。

2、警示系統的功能包括下列事項：

（1）記錄警示事件於警示檔。

（2）發送電子郵件給網路系統管理者。

（3）啟動管理控制台的警示功能，自動發出警示訊號。

（4）執行一特定應用程式(如自動復歸程式)。

（三）網路入侵之追查

1、對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並聯合相關單位(如網路服務公司)，追蹤入侵者。

2、入侵者之行為若觸犯法律規定，構成犯罪事實，應立即通知有關單位，請其處理入侵者之犯罪事實調查。

3、對可疑之入侵者列入追蹤名冊，依安全需求做反制與監管處理。

伍、系統存取安全管理

一、資訊系統存取控制規定

（一）應用系統負責人，應將系統之存取控制需求，明確告知系統管理者，以利其執行及維持有效的存取控制機制。

（二）應用系統負責人，應依業務需求、特性，訂定系統存取控制規範，並明定使用單位及使用人員的系統存取權限，非相關主管單位人員，如需存取該應用系統需填寫管制類資訊作業需求申請單，並經該主管單位核可後放其權限。

（三）資訊系統存取控制規定之研擬，應考量事項如下：

（1）個別應用系統之安全需求。

（2）資訊傳佈及資料應用之名義及授權規定。

二、使用者之存取管理

（一）使用者帳號管理

1、對於多人使用的資訊系統，必須建立使用者帳號管理程序。

2、使用者帳號管理程序，必須考量的事項如下：

（1）使用者是否已經取得使用該資訊系統之授權。

（2）使用者被授權的程度是否與其業務目的相稱，是否符合資訊安全規範及規定。

（3）告知使用者之系統存取權限。

（4）使用者調整職務及離（休）職時，必須註銷其系統存取權限。

（5）必須定期檢查及取銷閒置不用的識別碼及帳號。

（二）通行密碼之管理

本公司通行密碼管理，依下列規定處理：

1、為維持通行密碼的機密性，必須先配賦使用者臨時通行密碼，並強迫使用者於首次使用時，立即更改通行密碼的方式處理。

2、使用者忘記通行密碼時，必須提供臨時的通行密碼，並強制使用者立即更改其密碼。

（三）系統存取權限之檢討評估

1、為有效控管資料及系統存取，應定期檢討及評估使用者之存取權限，ERP 系統每半年檢討一次。

2、系統存取權限之評估，應考量其工作實際需求並定期評估系統存取權限。

三、系統存取之責任

（一）通行密碼之使用管理

使用者選擇及使用通行密碼時，必須遵守本公司資訊安全規定；並依下列原則配賦、管理及使用通行密碼：

1、以嚴謹的程序核發通行密碼，明確規定使用者應負的責任。

2、個人必須負責保護通行密碼，以維持其機密性。

3、避免將通行密碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。

4、當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。

5、使用者密碼的長度最少應由四位長度組成(不得為空白)。

6、避免使用下列事項作為通行密碼：

(1) 年、月、日等時間資訊。

(2) 個人姓名、出生日、身分證字號或汽機車牌照號碼。

(3) 電話號碼。

(4) 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

(5) 重複出現兩個字以上的識別字碼。

(6) 以全部數字或是全部字母組成密碼。

(7) 英文或是其他外文字典的字。

(8) 電腦上使用者的名字。

(9) 電腦主機名稱、作業系統名稱。

(10) 地方名稱。

(11) 專有名詞。

(12) 任何人的名字。

7、必須定期更換通行密碼，原則上以每兩個月至少需更新一次為原則；且避免重複或循環使用舊的通行密碼。

（二）暫時不使用電腦設備之安全管理

人員暫時離開或不使用電腦設備時，應注意下列事項：

1、當作業結束時，必須完全登出電腦系統或離線。

2、當電腦設備不使用時(超過十分鐘)，應使用鍵盤鎖或其他控管措施保護電腦畫面資料。

四、網路存取之安全控制

（一）維修廠商以遠端登入方式進入本公司電腦網路系統進行維修的通信作業埠，應經申請管制類資訊申請表經核准才可使用；於申請時間後，需將該系統之遠端登入帳號停用。

五、電腦系統之存取控制

（一）電腦系統登入程序

1、使用者進入電腦系統，應經由安全的系統登入程序。

2、安全之登入程序應具備下列的功能：

(1)限制系統登入不成功時可以再嘗試的次數，原則上以三次為原則，系統並應：

• 記錄系統登入不成功的事件。

• 在使用者嘗試登入系統失敗後，應強迫必須間隔三十分鐘之後才能再次登入。

• 於登入失敗三次後應中斷資料連結作業。

(2)在系統登入被拒絕後，應立即中斷登入程序。

(3)系統應記錄下列的資訊：

• 上一次成功登入系統的日期及時間。

• 上一次成功登入系統之後，有無被系統拒絕登入的詳細資料。

（二）使用者身分辨識

1、使用者識別碼不應有足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。

2、只有在例外的情況下，經權責主管人員之同意，核發群組內人員共用同一使用者帳號。

（三）使用者通行密碼之管理

本公司各應用系統的使用者通行密碼，應依下列規定管理：

1、任何帳號皆必須設定通行密碼。

2、允許使用者自行選擇及更改通行密碼。

3、使用最少四位長度的通行密碼。

4、使用者每兩個月更改通行密碼。

5、使用者自行選擇密碼時，應在第一次登入系統時強迫使用者更改臨時性的密碼。

6、使用者密碼的歷史紀錄，應保留二~五組使用紀錄，並避免使用者重複使用相同的密碼。

7、在登入系統程序中，系統不應顯示使用者的密碼資料。

8、應使用單向加密演算法儲存使用者密碼。

9、在軟體完成安裝作業後，應立即更改廠商預設的使用者密碼。

10、使用者自行考量通行密碼是否安全可靠，參考基準如下：

(1) 避免使用與日期有關的年、月、日。

(2) 避免使用單位名稱、識別碼或是其他參考性資訊作為通行密碼。

(3) 避免以使用者識別碼，團體識別碼或其他系統識別碼作為使用者通行密碼。

六、應用系統之存取控制

(一)資訊存取之限制

1、系統進入時應提供畫面供使用者鍵入代號以辨識其身分。

2、依據使用者身分控制資料的存取範圍及授權（例如限定使用者僅能執行唯讀、寫入、刪除或執行等功能。）

(二)原始程式資源之存取控制

本公司原始程式及相關文件之管理，應考量下列事項：

1、應用程式原始程式碼、資料庫及執行檔應分別存放。

2、應用程式原始程式碼、資料庫及執行檔之管理、更新及核發，應由作業負責人指定專人管理。

3、開發中及正式作業之應用程式及資料庫應各自存放。

4、各系統應保有各版本之更新紀錄。

(三)機密及敏感性系統之獨立作業

對機密及敏感性資料的處理,由該單位自行於獨立的或是專屬的電腦作業環境中執行。

七、系統存取及應用之監督

（一）事件之記錄

1、資訊安全事件發生時應建立記錄，並保存至結案查出原因為止，以作為日後調

查及監督之用。

2、事件之記錄應包括下列事項：

（1）使用者帳號。

（2）登入及登出系統之日期及時間。

（3）電腦的識別資料或其網路位址。

（二）電腦作業時間校正

由系統管理人員定期校正電腦系統作業時間，以維持系統稽核紀錄的正確性及一致性。

陸、系統發展及維護之安全管理

一、系統安全需求規劃

本公司各應用系統之安全需求視各業務單位之要求而定，有關各項控管、權限、使用範圍等概由業務主管單位提出，並確認後納入系統規劃設計規範中。規劃時應注意下列事項：

（一）應用系統在規劃分析時，應納入安全需求考量，以確保資料安全性。

（二）資訊系統安全需求分析應考量：

1、應訂定安全控制措施，定期備份及錯誤發生時之立即回復處理程序。

2、資訊安全需求分析，應特包括：

(1) 系統及資料之存取控制方式。

(2) 應保護系統避免未經授權的竄改或是修改。

(3) 系統應經由使用者帳號及密碼授權管制方式，確保處理的有效性及資料的真實性。

(4) 系統及資料應定期複製備份。

(5) 除了定期複製備份外，對於版本更新、重大處理及大量資料異動等情形，均應先行備份再予處理，以確保資料安全。

(6) 應訂定錯誤發生時之立即回復作業程序。

二、應用系統之安全管理

（一）資料輸入之驗證

1、輸入資料前應由該業務負責單位進行資料檢核，以確保資料的正確性。
2、資料輸入應考量的安控措施如下：

（1）應檢查是否有以下的錯誤：

• 是否有超出設定範圍的數值。

• 資料檔案是否有錯誤的文、數字。

• 是否有超出設定數值的上限或是下限。

三、應用系統檔案之安全

（一）程式版本之控制

應用系統執行時，應嚴格控制程式版本，減少可能危害作業系統的風險：

1、應用程式執行碼更新作業，應限定只能由授權的管理人員才可執行。

2、應建立應用程式執行碼的更新稽核紀錄。

3、版本更新應保留舊版的軟體。

（二）系統測試資料之保護

1、應保護及控制測試資料，避免以含有個人資料的真實資料庫進行測試；如須以真實的資料，應於事前將足以辨識個人的資料去除。

2、在使用真實的資料進行測試時，應採行下列的保護措施：

（1）適用在實際作業系統的存取控制措施，亦應適用在測試用的系統。

（2）真實資料被複製到測試系統時，應取得授權後始能進行。

（3）測試完畢後，真實資料應立即從測試系統中刪除。

（4）真實資料的複製情形應予以記錄，以備日後稽核之用。

四、系統變更之安全管理

為確保系統安全控制不被破壞，應建立變更控制程序；任何的系統變更，皆應獲得權責管理人員的同意；建立變更控制程序，應考量的事項如下：

(一) 依事前訂定的授權規定，執行變更作業。

(二) 系統完成變更作業後，應獲得系統使用者之認可。

(三) 檢視系統安全控制及正確性的程序，以確保系統變更作業不致影響或破壞系統原有的安全控制措施。

(四) 系統文件在每次完成變更作業後，應立即更新，舊版的系統文件亦應妥善保管及處理。

(五)應建立軟體更新的版本控制機制。

柒、資訊設備實體及環境安全管理

一、設備安全管理

(一)設備安置地點之保護

1、設備應安置在適當地點，以減少環境不安全引發之危險及未經授權存取系統的機會。

2、設備安置應遵循的原則如下：

（1）設備應儘量安置在人員不需經常進出之地點。處理機密性資料工作站，應放置在管理人員可注意及可就近照顧之地點。

（2）需特別保護之設備，應考量與一般設備區隔。

（3）應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等加諸於設備之危害。

（4）電腦作業區應禁止抽煙及飲用食物。

（5）應考量其他可能導致之危險因素。

(二)電源供應

1、電腦設備之設置，依據製造廠商提供之規格設置電源，以防止斷電或其他電力不正常導致之傷害。

2、應謹慎使用電源延長線，以免電力無法負荷導致火災等危害安全情事。

(三)電纜線安全

1、電力及通信用電纜線，應予適當之安全防護，以防止被破壞或資料被截取。

2、電力及通信纜線保護原則如下：

（1）應採取保護網路通信線路措施，以防止遭截取或是受到破壞。

（2）對於特別敏感性或是特別重要之系統，應採取加強之安全措施。

(四)設備維護

1、應妥善維護設備，以確保其完整性及持續使用。

2、設備維護原則如下：

（1） 應依據設備特性定期進行檢測，並紀錄電腦主機定期維護表。

（2） 設備之維護應由授權之維護人員執行。

（3） 應明確記錄所有的錯誤或認為有疑問之處。

(五)設備報廢處理之安全措施

資訊設備報廢應依照”參、電腦系統安全管理”中的“六、電腦媒體之管理”處理

(六)資訊設備濫用之防止

1、如發現資訊設備有不當使用情形，應通知該設備保管人單位主管督導與改善。

2、若屬累犯得累次提高通知層級。

二、機房安全管理

(一)機房之安全與管理

本公司電腦機房安全與環境維護由操作人員負責，為確保機房安全，進出人員應遵守下列規定：

1、機房採門禁系統管制，人員進出應使用核發之通行卡刷卡後進入，禁止未被授權的人員進出。

2、電腦維修廠商或其他廠商人員，應由資訊部相關人員陪同，始得進入機房工作。

3、機房內嚴禁吸煙、飲食。

4、機房內嚴禁存放易燃物及未經核准之電器或其他物品。

5、操作人員應隨時注意環境監控系統，掌握機房溫度及溼度狀況，若發現異常狀況應即刻通知廠務處理。

6、操作人員熟悉自動滅火系統操作方法及滅火機位置，如遇預警系統發生警報時，應查明真正原因，並做適當之處置，且迅速報告主管及工安，以便及時支援處理。

7、作業中遇緊急事故時，值班人員請依應緊急應變程序處理。

8、機房設備應由操作人員負責執行啟動及操作，除系統管理人員基於業務需要外，其他人員不得擅自操作機器。

9、值班人員應將所發生之異常狀況填寫於「值班人員定期例行檢核表」內，並轉知相關人員。

10、各項安全設備應依廠商的使用說明書定期檢查；員工應施予適當的安全設備使用訓練。

11、資訊部緊急應變處理程序應不定期演練及測試，每年至少一次。

(二)資訊財產攜出之安全管理

電腦設備、資料及軟體，未有核准之放行條，不得攜離辦公處所。

捌、緊急應變計畫及災難復原計畫

相關程序請參照”資訊部緊急應變計畫”及”資訊部災難復原計畫”

附註一: 洋華光電股份有限公司資訊安全施行規範

目的 : 為有效使用公司電腦資源以及維護公司資訊安全， 依據"洋華光電股份有限公司資訊安全規範"，訂定施行規範如下

一、一般資訊設備使用規範

1、未經副總（含）以上單位主管簽核同意，不得將其他電腦設備或廠商的電腦連接上本公司電腦網路。
2、除經審核發給之隨身碟、光碟機、燒錄機外，不得將電腦私自外接隨身碟、光碟機、燒錄機、數據機等具有儲存、複製、通訊功能之週邊設備，以保障公司智慧產權。
3、除經審核發給或經副總（含）以上單位主管簽核同意並貼有許可證之筆記型電腦外，不得攜帶個人筆記型電腦進入公司。
4、離開電腦超過十分鐘以上，自動啟動螢幕保護程式。
5、未經資訊單位授權，不得擅自搬移資訊設備，人員離職或到任，需填寫固定資產增置異動單，將該員保管之資訊設備進行轉入或轉出。
6、不得安裝使用未授權之非法軟體，若業務上有使用需要，應循正常請購程序，經資訊部會簽後彙整購置。
7、不得將色情檔案建置在本公司網路，亦不得在網路上散播不法、不當或違反善良風俗習慣的資料。
8、不得利用本公司網路從事不法、不當得利或個人營利活動。

二、網際網路之使用規範

1、不得下載未經授權使用的檔案或軟體。
2、不得下載、放置或傳遞與工作內容無相關的檔案資料，如電動玩具程式與音樂檔案。
3、網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。

三、電子郵件安全管理規範

1、電子郵件接收後應自行保管，並立即自郵件系統信箱中刪除。
2、不得以電子郵件等方式洩漏公司機密資料。
3、未經總經理簽核同意，不得直接將 E-mail 傳送給全體同仁。
4、對來路不明的電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞；並應通知電子郵件系統管理者處理。
5、不得發送電子郵件騷擾他人，導致其他使用者之不安與不便。
6、單一郵件寄送人數上限設定為 30 人，若有特別需求需各別提出經由總經理簽核後執行。
7、單一郵件寄送容量限制為 10MB，若有特別需求需各別提出經由單位主管簽核後執行。
8、 公司內部不得使用網際網路所提供之”免費/收費郵件信箱”，以防止公司機密資訊洩漏。

四、本公司電腦密碼之安全管理規範

1、使用最少四位長度的通行密碼。
2、使用者每二個月更改通行密碼。
3、使用者密碼的歷史紀錄，應保留二~五組使用紀錄，並避免使用者重複使用相同的密碼。