機密等級：■一般□敏感□機密

達盛機械工程股份有限公司
DarSheng Mechanical Enginnering

資訊安全政策與承諾

一、資訊安全是公司全體員工的共同責任，各級員工必須充分理解並貫徹所負職責。

二、為維護整體資訊資產安全，有關資訊安全之目標和認知、行動準則之建立必須考慮到：

1.建立完整的資訊安全性組織。	9.確保資訊安全事件之完善處理。
2.資產管理。	10.密碼學安全執行。
3.確保人力資源安全。	11.確保資訊設施安全運作。
4.確保實體及環境之安全管理。	12.確保供應者的資安管理。
5.確保資訊資產的風險管理。	13.確保資訊安全法規的遵循與審查。
6.確保通訊及作業管理安全。	14.確保商業營運持續管理。
7.確保建立安全存取控制管理機制。	15.確保資訊安全供應鏈滿足資安要求。
8.確保資訊系統之獲得、發展和維修管理安全性。	16.滿足相關於資訊安全之適用要求事項的承諾。

三、資訊安全管理系統的建立和維持，完全依據法律法規的要求及合約的安全責任，並和公司的企業風險管理背景相結合。

四、為有效管控資訊安全風險，必須建立包括風險評估方法、資訊安全法律法規要求、接受風險的標準、及風險之可接受程度等之風險評估暨作業管理程式，並落實執行。

五、訂定資訊安全之營運持續計畫並實際演練，確保資訊業務持續運作。

六、明確規範資訊系統及網路服務之使用權限，防止未經授權之存取行為。

七、建立機房實體及環境安全防護措施，並定期施以相關保養。

八、實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

九、建立資訊硬體設施及軟體之管理機制，以統籌分配、有效運用資源。

十、新資訊系統應於建置前將資訊安全因素納入，防範危害系統安全之情況發生。

十一、資訊安全政策應定期進行評估，以反映資訊安全管理、法令、技術及本公司業務之最新狀況，並確保本公司資訊安全實務作業之可行性及有效性。

十二、確保行動裝置及遠距使用的資訊安全措施，以管理使用行動裝置所導致之風險。包含保護存取、處理或儲存於遠距工作場所之資訊。

十三、提供設定資訊安全目標使用之依據方向。

■ **資訊安全目標**

1. 工作站中毒事件，每年≦ 2件以下。
2. 工作站設備非計劃維修事件，每月應≦2 件以下。
3. 未經授權之存取訊號事件，應達到每月≦1 件事件。
4. 主機系統服務可用性，每月系統非計劃中斷時間累計應≦12 小時以下。
5. 系統遭外部入侵與資訊外洩等資安事件，應每年≦1 次。
6. 資安事件發生後，在規定的時間完成通報、應變及復原作業的比率為 100%。

總經理：何義雄　　日期：113、1、1