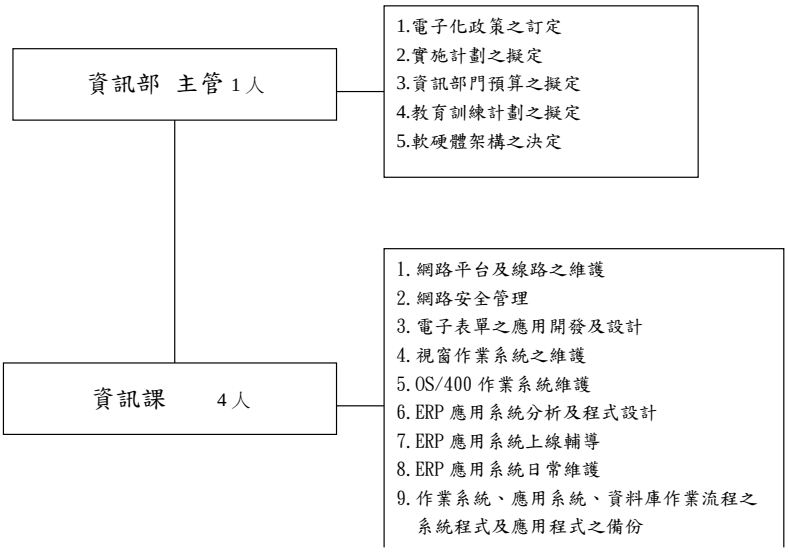
本公司為強化資通安全管理，建立安全及可信賴之電子化企業，確保資料、系統、設備及網路安全，成立專責資訊部依有關法令，進行資通安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資通安全措施，確保公司內外部資訊蒐集、處理、傳送、儲存及流通之安全。

資訊部就下列事項，訂定資訊安全計畫實施，並定期評估實施成效：

（一）資通安全管理辦法訂定。
（二）資訊安全權責分工。
（三）人員管理及資訊安全教育訓練。
（四）電腦系統安全管理。
（五）網路安全管理。
（六）系統存取控制管理。
（七）系統發展及維護安全管理。
（八）資訊資產安全管理。
（九）實體及環境安全管理。
（十）業務永續運作計畫管理。
（十一）其他資訊安全管理事項。

資訊部組織圖及職責說明



單位	資訊部	資訊安全
職責說明	1.MAIL:收發管制、異常處理。	
	2.防駭、防毒:防止電腦被入侵&資料外洩、系統異常無法運作。	
	3.帳號管理:人員新進、離職與系統權限應用變更。	
	4.網路管理:資料分享、上網管制、流量異常管理。	
職責	任務	
MAIL	1.收發管制	不定期
	2.垃圾郵件過濾	每日
	3.帳號被入侵、盜用偵測排除	不定期
	4.異常郵件處理	不定期
防駭、防毒	1.防毒軟體安裝與更新	不定期
	2.資訊安全通報與宣傳	不定期
	3.使用者電腦異常排除	不定期
	4.作業系統補丁更新處理	不定期
帳號管理	1.MAIL 帳號管理	不定期
	2.AD 帳號管理	不定期
	3.AS400 帳號管理	不定期
	4.網頁帳號管理	不定期
	5.條碼系統帳號管理	不定期
網路管理	1.資源分享管理	不定期
	2.上網管制	不定期
	3.入侵防禦偵測、流量異常處理	不定期
	4.防火牆設定	不定期

遭勒索病毒攻擊之資訊安全措施:

WannaCry 勒索病毒/勒索蠕蟲在全球範圍持續擴散，蠕蟲會主動攻擊電腦安全性漏洞，只要聯網就有被感染機會，資訊部立即執行及建議以下操作避免病毒攻擊！

1.使用隨身碟、外接硬碟或者雲端空間，備份您的重要資料。

2.關閉網路共用資料夾。

3.不要點擊來路不明的網站和檔案等。

4.修補電腦作業系統相關漏洞。可以上微軟安全性修補程式(勒索病毒/勒索蠕蟲 WannaCry/Wcry(想哭))，下載安裝修補程式。

5.開啟電腦作業系統的 Windows Update，隨時升級系統與修補漏洞。