

資通安全責任：

1. 廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。此外機關保有對廠商以派員稽核或其他適當方式執行相關查核的權利。
2. 廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道（covert channel），提出安全性檢測證明，涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。廠商於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。
- 本案金額達新臺幣一千萬元以上，廠商交付之軟硬體及文件，應接受委託機關或其所委託之第三方進行安全性檢測：.....
.....（其項目由機關於招標時載明）。
3. 契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還或移交之，並保留執行紀錄。
4. 廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
5. 廠商提供服務，如違反資通安全相關法令或知悉發生資安事件時，必須立即通報機關，提出緊急應變處置，並配合機關做後續處理。
6. 廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合機關對系統品質及資通安全的要求。
7. 廠商如違反第 1 目至第 6 目規定，應~~適用第 15 條之違約責任~~，並就機關所受損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。