機密等級：□一般 ■限閱 □密 □機密	文件編號：IS-04-021	保存年限：3年
日　　期：　　年　　月　　日	紀錄編號：	版本：1.0

Gramm Tek Inc.
安全要求事項表

□專案起始要求設定(是否符合免填)　□專案執行定期安全查核

項目名稱				
控制措施	類別	安全事項	說明	是否符合
存取控制	帳號管理	使用者的會談階段，設定該帳號在合理的時間(至多30分鐘)內未活動即自動失效		
	最小權限	對使用者/角色，僅賦予所需要的最低權限		
		軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限		
稽核與可歸責性	稽核事件	針對身分鑑別失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行日誌記錄		
	稽核紀錄內容	日誌紀錄包含以下項目 1.識別使用者之ID(不可為個資類型)。 2.經系統校時後的時間戳記。 3.執行的功能或存取的資源。 4.事件類型或等級(priority)。 5.事件描述		
	稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量		
	稽核處理失	資訊系統應在稽核處理失效(如儲存容量不足)之情況下，採取適當之行動，例如：關閉資訊系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。		

機密等級：□一般 ■限閱 □密 □機密	文件編號：IS-04-021	保存年限：3年
日　　期：　　年　　月　　日	紀錄編號：	版本：1.0

Gramm Tek Inc.
安全要求事項表

□專案起始要求設定(是否符合免填)　□專案執行定期安全查核

項目名稱				
控制措施	類別	安全事項	說明	是否符合
	效之回應	當公司規定需要即時通報的稽核失效事件發生時，資訊系統應在公司規定之時效內，對公司特定之人員、角色提出告警(適用於高等級)		
稽核與可歸責性	時戳	系統內部時鐘應具備定期同步機制		
	稽核資訊之保護	對日誌紀錄進行適當保護及備份，避免未經授權存取		
		定期備份稽核紀錄到與原稽核系統不同之實體系統(如Log伺服器)		
營運持續計畫	資訊系統備援	採用「高可用性」(High Availability)架構(分散式或叢集伺服器架構)		
識別與鑑別	身分鑑別管理	確實規範使用者密碼強度(密碼長度8個字元以上、包含英文大小寫、數字，以及特殊字元)		
		身分鑑別相關資訊不以明文傳輸		
	鑑別資訊回饋	資訊系統應遮蔽在鑑別過程中之資訊(如密碼)，以防止未授權之使用者可能之窺探/使用		

機密等級：□一般 ■限閱 □密 □機密	文件編號：IS-04-021	保存年限：3年
日　　期：　　年　　月　　日	紀錄編號：	版本：1.0

Gramm Tek Inc.
安全要求事項表

□專案起始要求設定(是否符合免填)　□專案執行定期安全查核

項目名稱				
控制措施	類別	安全事項	說明	是否符合
系統與服務獲得	安全系統發展生命週期需求階段	針對系統安全需求，以檢核表方式進行確認		
	安全系統發展生命週期設計階段	應根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估		
	安全系統發展生命週期開發階段	具有防範SQL命令注入攻擊(SQL Injection)之措施		
		發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息		
		具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)		
系統與服務獲得	安全系統發展生命週期測試階段	執行「弱點掃描」安全檢測		
		執行「滲透測試」安全檢測		
	安全系統發展生命週期部署與維運階段	作業平台定期更新並關閉不必要服務及埠口(Port)		
		針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新		
	獲得程序	開發、測試以及正式作業環境應作區隔		
	資訊系統文件	應儲存與管理系統發展生命週期之相關文件		

機密等級：□一般 ■限閱 □密 □機密	文件編號：IS-04-021	保存年限：3年
日　　期：　　年　　月　　日	紀錄編號：	版本：1.0

Gramm Tek Inc.
安全要求事項表

□專案起始要求設定(是否符合免填)　□專案執行定期安全查核

項目名稱				
控制措施	類別	安全事項	說明	是否符合
系統與通訊保護	傳輸之機密性與完整性	機敏資料傳輸時，採用加密機制		
		使用公開、國際機構驗證且未遭破解的演算法		
	資料儲存之安全	參數設定或系統設定存放處，限制存取或進行適當保護		
		機敏資料儲存時，採用加密機制		
系統與資訊完整性	資訊系統監控	發現資訊系統有被入侵跡象時，應通報管理人員		