# 資享「資料保全銀行」安全考量 無可挑剔

為了確保貴公司存放於「資料保全銀行」的備份資料安全，資享科技在各個安全層面上所做的考量均遵循相關法令規定的嚴格審核標準。以下將分項詳細說明我們在各方面的努力：資料備份傳輸安全、遠端備份系統安全、IDC/RBC遠端備份中心機房環境安全。

## 資料備份傳輸安全機制

### 透過HiTrust/VeriSign第三方數位憑證機制之128位元的SSL通訊渠道

介於「資料保全銀行」的RBC遠端備份中心之備份伺服器與用戶Client端電腦之間的溝通與資料的傳遞，都是透過第三方(HiTrust/ Verisign)的數位憑證確認過後而建立連線的128位元的SSL (Secure Socket Layer)安全且封閉的渠道。因此，即使當用戶的備份資料傳送至「資料保全銀行」的遠端備份中心(Remote Backup Center,RBC)時是經由Internet的公衆網域，網路駭客也無法從中獲取任何資訊。

HiTrust/VeriSign 所提供的第三方數位憑證機制完全符合中華民國財政部所規範的128位元加密機制標準。VeriSign 在全世界伺服器數位憑證市場佔有率超過90%，全球財星500大及全球前40家知名電子商務網站皆使用 VeriSign 伺服器數位憑證，同時已有超過41萬個全球資訊網站使用 VeriSign 伺服器數位憑證來提高其網站的安全性、競爭力及網站用戶信任度。 Verisign 的數位憑證從申請、核驗到簽發的全部作業流程均需通過 KPMG SAS.70(Statement on Auditing Standards)稽核作業及WebTrust 稽核，嚴謹的作業在於達到各環節點上得到有效的安全控管目標。

### 資料保全銀行工作人員不會持有用戶的加密鑰

本服務重視客戶備份資料的機密性(Confidentiality)，具備資訊不被未經授權的個人、實體或過程取得或者揭露的特性；ISO/IEC 13335-1:2004。

備份檔案均先經過壓縮、加密後，再由戶自行輸入設定的加密鑰匙(密碼)，才會將備份檔案傳輸至遠端的備援中心。這些處理過後的資料，只有對用戶本身有使用的價值；其他人，包括資享的「資料保全銀行」RBC工作人員，即使獲取這些機密資料檔案，也頂多是一些儲存於RBC上的亂碼。用戶自行設立的加密鑰匙，除了用戶自己知道之外，也只存放在用戶的電腦中。在備份資料的傳輸過程中，此加密鑰匙並不會隨著資料傳送至網際網路。請注意！如果忘記加密鑰匙的密碼，所有的備份檔案將永遠都不能打開、更改、或還原。因此，就算「資料保全銀行」RBC專屬特定工作人員能接觸到用戶儲存在RBC的備份檔案，但是我們對用戶儲存的檔案內容，有別於一般公司的內部MIS人員，仍是一無所知。

### 需要8.77x1017年才能破解的128位元加密鑰匙

我們用於加密用戶備份檔案的演算法之一是128 位元的Twofish。這是由Counterpane實驗室所設計的一種塊狀密碼，也是目前透過美國國家技術標準局(NIST)所選出之世界上五種最先進的加密標準(Advanced Encryption Standard, AES)之一。此加密演算法經常被公開提出檢閱，但截至目前為止，還未聽聞過任何被外界攻擊而破解的案例。

### 備份資料完整性檢測確保用戶資料完整無誤

用戶資料在本地端待異地傳輸之前，會啓動備份資料量的檢測工作，並由用戶端發出總備份資料量通知遠端的異地備份中心RBC，才開始備份資料的傳輸動作。待備份工作完成後，位於遠端的備份主機系統會自動檢視所上傳的備份資料是否符合用戶端所發出的總資料量數據。如果不符合，則系統會發出備份失敗之警訊，並於亦日再啓備份工作，以確保用戶的備份資料完整無誤。

### 備份資料的取得可以以IP位址為依據

用戶也可以預設一組IP 位址來限制備份資料的取得。如果不是來自於用戶設定下的IP位址，想進入存取您的線上備份資料，將會被系統拒絕進入。這項安全機制可以保證(經鑑別進而顯示可能有違反資訊安全政策或保護措施失效;ISO/IEC TR 18044:20)，即使在知道用戶ID和密碼的情況下，備份檔案的存取不是開放於所有地點。

### 備份帳戶凍結防護機制

用戶可由「資料保全銀行」所發出的備份報告（透過 Email 及 Attachment 方式）得知每日資料備份狀況。如客戶發現並告知備份帳戶發生不正常資料存取行為，「資料保全銀行」RBC專屬特定工作人員可協助客戶將帳戶設定凍結，以避免資料繼續外洩。

## 遠端備份系統安全機制

### 叢集式(Cluster)備份主機/負載平衡運算(Load Balance)

雙迴路電源、雙HBA卡、使用最新 64 位元四核心 Intel Xeon 處理器的效能比前代雙核心處理器產品高出 63%。32GB /64 位元的記憶體定址能力為記憶體密集型應用程式提供了可擴充性。搭配國際知名大廠 Radware AppDirector 負載平衡器 (Load Balancer)有效均衡IP 應用負載並優化網路服務品質。

### SAN Fibre Channel 光纖儲存陣列系統/RAID防護機制

雙迴路電源系統、雙RAID控制器；此整套系統媲美國內外大型及跨國企業之後端儲存設備。儲存之備份資料安全 、完整性、擴充性、及持續性皆有完善的保護規劃。

### Juniper Networks 安全服務閘道器5XX系列(SSG)防火牆

專屬的安全防護軟、硬體平台，以及完整的統合威脅管理 (UTM) 安全防護功能，包括狀態防火牆、IPSec VPN、IPS、防毒 (包括防間諜軟體、防廣告軟體、防釣魚攻擊)、防垃圾郵件和 Web 過濾功能。

### Intrusion Prevention System, IPS 入侵偵測預防系統

提供超過 2500 種預先定義好的攻擊特徵檔，並定期從原廠網站下載更新，防禦最新攻擊，並提供政策範本，隨時依據攻擊特徵檔能力，修改防火牆與政策。整體管理系統以營運風險方案為基礎來建立、實施、操作、監督、審查、維持及改進資訊安全;ISO/IEC 17799:2005。

## IDC/RBC遠端備份中心機房環境安全機制

### 99.999% 的電力及備援系統

雙迴路電源供應與N+1設計以達成五個九(99.999%)之穩定性，全年累積中斷時間不超過 5.26 分鐘。 除此之外，當電力中斷時，第一線防護為具備20分鐘以上續航能力的電池電力備援。 30 秒內即由1500KW, N+1 之可24小時連續運轉發電機自動加入運轉； 備有36小時的燃料備用油槽 (與中油簽訂制式契約，於接到電話4小時內補給燃油)，來確保在電源供應回復前仍保有不間斷的電力供應。

### N+2 雙迴路空調系統

雙迴路設計水冷式獨立型微電腦恆溫濕空調機，搭配 N+1空調水塔、N+2的空調主機及7天的儲水量水塔。具液漏偵測功能及最佳的工作環境：空調機溫度維持在22° C +/- 1° C,溼度維持在 50+/- 5%。

### 火災預警偵測及抑制系統護機制

大樓的環控系統和早期偵煙系統連結：多重偵測、預防假警告及動作發生，並備有緊急作業程序防止事故發生。使用FM200潛艦級消防系統做為滅火工具：地下室使用 CO2及乾粉滅火器。

### 芮氏七級防震建築結構

機房本身的設置地點為非斷層帶經過，建築物耐震度亦通過芮氏七級耐震測試，可保障建築物不易受一般地震的影響。機房內置機櫃皆以角鋼相互連結以增強其堅固度；每座機櫃亦均以U型槽固定，以避免機櫃倒塌。

### 24x7x365 全年無休保全暨維運中心

24 小時的網管監控中心(Network Operation Center, NOC)全年無休的監控網路安全，並使用指紋辨器及讀卡機來做人員進出入管制。除了包含機電維護人員待命及大樓環境管理之外，大樓警衛巡查與車道管控搭配使用 360度全方位的監控攝影及移動偵測系統隨時監控。

eSTORAGE 資享科技股份有限公司
總公司：台北市114內湖區新湖二路221號2樓 TEL：(02)2790-5928 FAX：(02)2790-5972
南部辦事處：高雄市804鼓山區明華路345號4樓 TEL：(07)550-0590 FAX：(07)550-0591
http://www.estorage-isb.com 免付費服務專線：0800-28-9988