鼎新電腦
DataSystems

鼎新 | 行業攻略雲
Industry walkthrough cloud

# 資訊安全白皮書

更新時間：2017 年 4 月

# 目錄

# 一、前言

行業攻略雲是鼎捷集團自主創新，使命是希望能夠打造一個能協助企業高階經理人高效管理的服務，為了達到此目標，確保企業相關資料的安全是我們的首要任務，因此我們將此服務立基於 Microsoft Azure 的平台，為企業資訊安全提供全方位的安全保障！透過以下說明，希望您能更了解我們實踐安全性的做法。

# 二、人員安全

在入職後，所有的員工必須簽署保密協議，確認收到並遵守鼎新電腦的安全政策和保密要求，尤其關於客戶資訊和數據的機密性要求將在入職培訓過程中被重點強調。

此外，鼎新電腦依據員工的工作角色進行額外資訊安全培訓，確保員工管理的用戶數據必須按照安全策略執行。最後，鼎新電腦通過企業價值觀考核的方式檢驗每位員工是否以誠信、敬業的態度來管理每位客戶的雲端數據， 保證其對客戶、合作夥伴的尊重。

# 三、資料安全

資料安全主要目標之一是保護系統和應用程式的基礎安全。行業佔略雲從資料創建、使用至共用，應用資料加密措施，且無任何功能可以直接存取檔案，完整保障了資料保密性、完整性、可用性、真實性、授權、認證和不可抵賴性

## 3.1 資料安全與加密

行業攻略雲採用進階加密標準 AES 128bits 檔案加密，為敏感數據供可持續的保護。且透過 Azure 的防火牆及安全性設定，外部無法直接存取相關資源。

## 3.2 身分驗證及授權

行業攻略雲採用符合業界通訊協定的 OAuth 2，OAuth 2 為一標準規範(RFC-6794)，各大廠雲端服務皆實作採用， 撐起整個雲端平台身份驗證及授權。包含 Facebook、Google、Dropbox、WeChat..等，全面強化安全性及身份驗證機制，依不同情況使用不同驗證模式。Client 端不儲存帳號密碼，以 Token 為認證識別。可調整 Token 有效期限及使用功能範圍(授權)，使用 Redirect URL 進行 Token 回傳的回呼，避免中途被竄改的可能。也為單點登錄 SSO（single sign-on, SSO） Server ，因將驗證及授權層獨立，可降低系統耦合 。

### 3.3 資料安全審計

包含資料活動的詳細跟蹤記錄，從而實現對用戶訪問行為的主動控制。使所有活動詳細可見， 如登錄失敗、權限升級、非法訪問、敏感數據訪問等，這些行為是否合規一覽無餘並做到所有用戶操作有蹤可尋。

## 四、應用程式安全

### 4.1 帳號安全

帳號安全依密碼策略和訪問控制策略，禁用弱密碼，監控非法登錄嘗試，且戶登入使用時間不可過長，定期要求用戶重新以帳號密碼登入(網頁七天需重新登入，行動應用程式會每天會重取 Token) ，以確保用戶帳號安全 。除此之外 ，行業攻略雲服務不使用 session 及 cookie，可避免被攻擊者使用密碼或是冒用身分。

### 4.2 傳輸安全

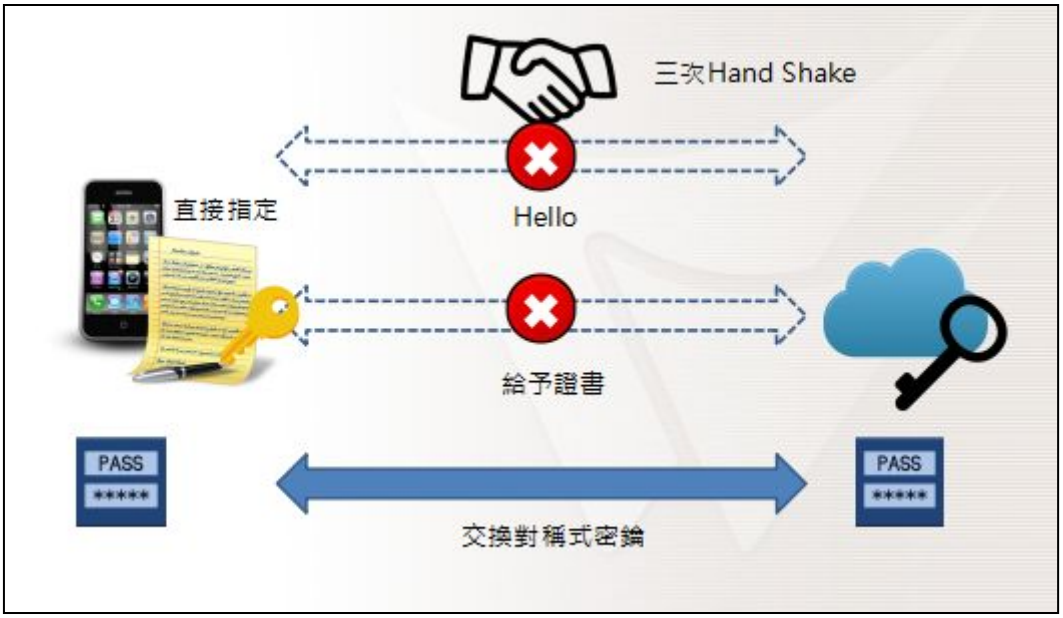
#### 4.2.1 安全協議

為保障用戶資料安全 ，會對所有戶在網路傳輸中的資訊採用 SSL/TLS 加密傳輸功能，通過加密防止篡改/竊聽/截取，以確保用戶的隱私資訊在網路中傳輸安全。此外，行業攻略雲都已經啟用 https 協議來代替 http 協議。

為避免攻擊洩漏程式內部運轉模式，行業攻略雲服務即使出現錯誤，出現 HTTP 錯誤狀態碼，不會直接呈現錯誤，且關閉任何錯誤的自動輸出，無法做進一步分析。

#### 4.2.2 中間人攻擊防禦

為防止行動裝置應用程式，在 SSL/TLS Handshake 時，對傳輸中資料進行篡改的中間人攻擊 ( Man-in-the-middle attack，MITM )。利用以綁定憑證(Certificate Pinning)方式，可直接從特定位置取得，更嚴謹地驗證憑證內容，如此一來，就無須 SSL/TLS 在 Handshake 時，進行公鑰的交換，降低取得非行業攻略雲的公鑰憑證風險。另外，行業攻略雲是由受信任的第三方憑證管理中心 CA 進行簽署，也降低了其他竄改的風險。




### 4.2.3 資料維護歷程自助查詢

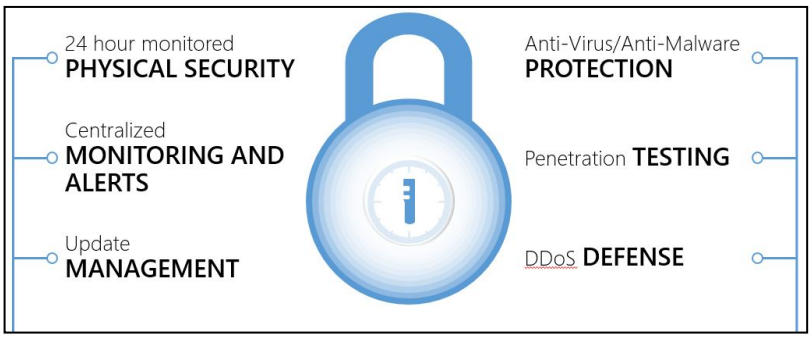
用戶可以方便的自助查詢工作圈的歷史資料維護歷程，如果存在異常維護情況，用戶可以輕易地主動發現。


### 4.2.4 系統登入權限存取

行業攻略雲使用者可依存取權限區分成三種身份：管理者、編輯者、閱覽者，管理者可從工作圈管理後台管理帳單資訊、使用者，管理員亦可以晉升/降級其他用戶的身份。

# 五、基礎設施安全

行業攻略雲服務建置於 Microsoft Azure 上，有完整的方法來保護執行超大規模全域服務所需的雲端基礎結構。Microsoft Azure 雲端基礎結構除實體資料中心之外，還包括硬體、軟體、網路、管理和操作人員每項設備都以 24x7x365 的概念出發，確保免受電源故障、物理入侵和網絡中斷。這些數據中心符合物理安全性和可用性的行業標準（如 ISO 27001)。




## 5.1 災難恢復與業務連續性

行業攻略雲能夠應對各類風險，具有自動調整和快速反應的能力，保障行業攻略雲業務連續運轉。於 Microsoft Azure 上的系統服務一直維持每個資料庫都有三個甚至是更多的副本來保護資料庫，資料異動確認（updates committed）回應前至少已經有兩份資料副本，在高可用性（HA）措施的保護下，要是發生本地端硬體或軟體故障服務中斷的情況，仍可以有效的保護資料庫持續提供服務。並定時進行完整備份，並有完整的異地備援機制，降低資料遺失風險，是能在最短時間恢復在異地恢復運作的災難備援解決方案。