# 雲計算平臺

# 資安白皮書

**Sep 2024**

# 目錄

**1. 概述 ..... 3**

**2. 責任劃分 ..... 4**

2.1. 客戶義務和責任 ..... 4
2.2. 泰富國際的義務和責任 ..... 4

**3. 數據中心安全 ..... 5**

3.1. 設施及人員訪問安全 ..... 5
3.2. 環境安全 ..... 6

**4. 雲平臺安全 ..... 6**

4.1. 雲平臺整體架構安全 ..... 6
4.2. 虛擬主機的安全 ..... 7
4.3. 雲平臺數據存儲安全 ..... 7
4.4. 雲平台數據傳輸安全 ..... 7
4.5. 雲平台數據使用安全 ..... 8
4.6. 雲平臺的可用性 ..... 9

**5. 通訊與網路安全 ..... 9**

5.1. 雲端網路架構設計原則 ..... 9
5.2. 網路及通訊埠安全 ..... 10
5.3. 網路安全建議 ..... 10

**6. 雲平臺運維安全 ..... 11**

6.1. 員工安全教育訓練 ..... 11
6.2. 員工權限控制 ..... 11
6.3. 稽核軌跡追蹤 ..... 12
6.4. 用戶憑證 ..... 12

**7. 服務變更管理 ..... 12**

7.1. 服務客服流程 ..... 12

**8. 數據銷毀 ..... 13**

8.1. 數據銷毀 ..... 13
8.2. 客户資源池回收 ..... 14
8.3. 虛擬機數據銷毀 ..... 14
8.4. 儲存數據銷毀 ..... 15

**9. 數據保護策略 ..... 15**

9.1. 數據備份及快速恢復服務 ..... 15
9.2. 數據複製及災難恢復服務 ..... 15

**10. 安全事故處理及報告 ..... 16**

10.1. 資訊安全管理 ..... 16
10.2. 安全事故處理 ..... 16

**11. 漏洞管理 ..... 17**

11.1. 漏洞管理方法 ..... 17

**12. 漏洞報告 ..... 17**

12.1. 漏洞報告方法 ..... 17
12.2. 漏洞評估 ..... 18
12.3. 漏洞公佈 ..... 18

**13. 可接受的使用政策 ..... 18**

13.1. 禁止非法、有害或冒犯性的使用或內容 ..... 18
13.2. 禁止危害網路安全的違規活動 ..... 19
13.3. 禁止網路濫用 ..... 19
13.4. 監控及執行 ..... 19

# 1. 概述

泰富國際網絡股份有限公司（以下簡稱“泰富國際”）SmartCLOUD 服務提供了一個基於 VMware 虛擬化平臺，並且具備高性能、高可靠性以及安全保障的 IT 基礎設施服務。

使用 SmartCLOUD 服務的客戶，可以根據自身的需求，靈活調整中央處理器(CPU)、記憶體(Memory)和儲存(Storage)等 IT 資源。 服務平臺具備完善的容錯能力和可靠性，能夠避免因為硬體故障等原因導致的業務中斷，進而最大限度的保障客戶利益。

作為領先的雲計算服務商，泰富國際不僅連續多年通過 ISO 9001、ISO 20000 和 ISO 27001 認證，而且實施了從基礎設施到頂級應用的各種安全策略，確保客戶數據在 SmartCLOUD 服務平臺上的安全。本文件描述了每個安全策略的詳細過程，包括：

- 責任劃分
- 數據中心安全
- 雲平臺安全
- 通訊與網路安全
- 雲平臺維運安全
- 服務變更管理
- 數據銷毀與硬體報廢
- 數據保護策略
- 安全事故處理及報告
- 漏洞管理
- 漏洞報告
- 可接受的使用政策

# 2. 責任劃分

## 2.1. 客戶義務和責任

客戶應負責：

- 在 SmartCLOUD Director 平臺中管理自己的操作系統、應用程式和數據（包括備份數據）;
- 虛擬機內部的操作系統管理（包括操作系統修補程式、安全修補程式和安全控制等）;
- 虛擬機器內部的應用程式和用戶;
- 在 SmartCLOUD Director 平臺中設定虛擬機的網路參數;
- 虛擬機器內部操作系統和應用程式的紀錄;
- 泰富國際強烈建議客戶在虛擬機上安裝 VMware Tools，以保證客戶虛擬機內部的操作系統時間能與底層 VMware 主機（ESXi Host）同步。

## 2.2. 泰富國際的義務和責任

泰富國際應負責：

- 確保為使用 SmartCLOUD 服務的客戶提供安全可靠的基礎機構，包括任何與服務有關的硬體、軟體、網路及基礎設施等;
- 為客戶提供虛擬機管理介面，包括任何與虛擬機層面相關的日誌、事件及使用者操作記錄;
- 建立完善的數據分類分級標準，所有數據在建立時均按照《安全策略手冊》(Security Policy Manual）標準進行統一的分類分級。 客戶數據在泰富國際內部屬於 “Company Confidential Level 2”，即商密安全等級的數據。 泰富國際對客戶數據高度重視，在人員、流程、技術上等層面嚴格把關控制與防範，確保客戶數據的機密性、可用性和完整性。
- 持續建設內部整體的資訊安全管理體系，為客戶的個人資訊提供安全可靠的保護能力。泰富國際的隱私政策可在官網上查詢，詳細資訊請參見隱私政策。 泰富國際將對客戶任何隱私相關的問題進行及時回覆。
- 確保客戶使用服務時的安全性和隔離性，包括：

  i. 不同客戶之間的環境完全隔離;

ii. 客戶環境與泰富國際管理環境完全隔離;

iii. 客戶環境與其他未受信任的環境（如網際網路）完全隔離。

- 與客戶溝通任何功能上的更改或更新（如有且適合）
- 確保高效的維運與安全管理，包括並不限於從數據中心安全、雲平臺安全、通訊與網路、雲平臺維運安全、服務變更管理、數據銷毀、數據保護策略、安全事故處理與報告、漏洞管理與報告等層面實施管控（請參考安全白皮書第 3 至第 12 章節）。

# 3. 數據中心安全

## 3.1. 設施及人員訪問安全

3.1.1. 為 SmartCLOUD 服務平臺的基礎設施提供 7x24 小時的監控並具有嚴格的進入訪問控制。

3.1.2. 任何人員（包括泰富國際的工作人員、客戶或數據中心訪客）需要進入數據中心時，必須在登記系統中登記其相關資訊。 僅當數據中心安全營運經理核准其進入訪問請求後，該人員才可進入數據中心，且進入訪問全程均須有泰富國際工作人員的陪同並確實掌握其所有行為。

3.1.3. 泰富國際為客戶提供在多個區域放置資源池和儲存數據的靈活性。 客戶數據位於他們選擇的服務位置當地， 對應提供 SmartCLOUD 服務的數據中心如下：

| **SmartCLOUD Compute 站點** | **位址（國家及地區）** |
|---|---|
| HK-ALC | 香港島，香港 |
| HK-CTT | 新界區，香港 |
| SG-DRT | 新加坡 |
| TW-TPEASP | 臺北，臺灣 |
| TW-TPEYUD | 臺北，臺灣 |
| TW-TCH | 台中，臺灣 |
| JP | 日本，東京 |
| CN-GZYUJ | 廣州，中國 |
| CN-GZKXC | 廣州，中國 |
| CN-SHWGQ | 上海，中國 |
| CN-SHBAO | 上海，中國 |

| | |
|---|---|
| CN-BJJXQ | 北京， 中國 |
| CN-BJKC | 北京， 中國 |
| DE-FRA | 法蘭克福，德國 |
| US-LAX | 洛杉磯，美國 |
| US-NYC | 紐約，美國 |
| US-NY11 | 紐約，美國 |
| ZA-CPT | 開普敦，南非 |
| GB-LND | 倫敦，英國 |
| EE-TTLSOL | 塔林，愛沙尼亞 |

## 3.2. 環境安全

3.2.1. 具有備用的數據中心交流電電源系統，一旦主電源發生中斷，備用的不斷電系統（UPS）和發電機會立即開始運作，以確保連續的電源供應。

3.2.2. 溫度控制系統將為數據中心的所有設施保持一個恆定的運行溫度，任何異常情況（如過熱），都會觸發警報，數據中心營運人員會立即採取適當的措施。

3.2.3. 數據中心安裝了自動火災檢測和滅火系統。 所有數據中心機房、機械和電力設施、製冷機房和發電機房中的火災探測系統均採用煙霧探測感應器。

# 4. 雲平臺安全

## 4.1. 雲平臺整體架構安全

4.1.1. 服務平臺內所有的基礎設施均位於 Tier III+ 企業級數據中心的專用安全機櫃內，與數據中心內其他設施實體隔離。

4.1.2. 泰富國際的雲計算營運團隊將 24x7x365 不間斷對服務平臺內的設施進行監控，當有任何硬體故障發生時，雲計算營運團隊的工程師將第一時間聯繫廠商進行硬體更換。

4.1.3. 如需要進入數據中心，必須得到數據中心安全營運經理的核准，並詳細記錄其個人資料。

## 4.2. 虛擬主機的安全

4.2.1. 服務平臺建立在安全穩定的 VMware 虛擬化平臺上。

4.2.2. VMware 是完全封閉原始程式碼的專用軟體，由 VMware 合規性的參考架構框架和安全合規性的平臺獨立驗證。

4.2.3. 泰富國際通過以下方式確保及強化服務平臺虛擬主機的安全性：

- 限制 SSH 訪問;
- 使用指定使用者和最小特權;
- 儘可能減少打開的 ESXi 防火牆通訊埠數;
- 在 ESXi 主機使用鎖定模式;
- 檢查 VIB 軟體包完整性;
- 管理 ESXi 證書;
- ESXi 帳戶鎖定;
- 設定雲服務平臺從 NTP 伺服器自動同步時間，NTP 伺服器從香港天文臺自動同步時間。

## 4.3. 雲平臺數據存儲安全

4.3.1. 服務平臺中的所有數據均儲存在具有 RAID 保護的集中式 SAN（儲存區域網路）中，該 SAN 儲存與服務平臺的基礎設施位於同一機櫃，並受到 24x7x365 監控。

4.3.2. 泰富國際向客戶提供數據容器的標識，例如根據 vCLOUD Director 中的資源池分配相關的虛擬私有機構或虛擬數據中心組織。

## 4.4. 雲平台數據傳輸安全

4.4.1. 每位使用服務的客戶均有專用的 vLAN 號碼，確保其數據在傳輸過程中與其他客戶完全隔離。

4.4.2. 每位使用服務的客戶均有專用的網路連接實體通訊埠，在實體上實現與其他客戶數據隔離。

4.4.3. 客戶應先登錄 MC Portal，然後按兩下 SmartCLOUD Compute Director 選項以建立雙因子身份驗證連接，然後再連接存取 SmartCLOUD Compute Director，其中數據傳輸均使用國際知名廠商的 TLS 加密，非對稱加密至少 RSA-2048，對稱加密至少 AES-256 和簽名演算法至少 SHA-256 進行加密。

## 4.5. 雲平台數據使用安全

4.5.1. 當客戶需要登入服務管理平臺對虛擬機或數據進行管理時，必須首先經過雙因子驗證。雙因子採用動態密碼驗證方式，客戶必須在接收到動態密碼（可通過手機簡訊或電子郵件接收）後的 300 秒內登入平臺，否則密碼將作廢，客戶需重新操作。

4.5.2. 泰富國際為每位客戶提供專用的數據儲存、網路和資源池，以確保每位客戶的資料都是完全隔離。

4.5.3. 客戶可以使用 VM 加密，進而可以建立加密的 VM 或者加密現有的 VM。 由於所有包含敏感資訊的 VM 檔都被加密，因此整個 VM 受到了保護。 與其他任何儲存策略一樣，加密實質上是一種應用於 VM 的儲存策略。 應用加密儲存策略後，VM 將自動加密。

4.5.4. VM 加密支援對以下類型的檔案進行加密：

- VM 檔
- 虛擬磁碟文件
- 主機核心轉存文件

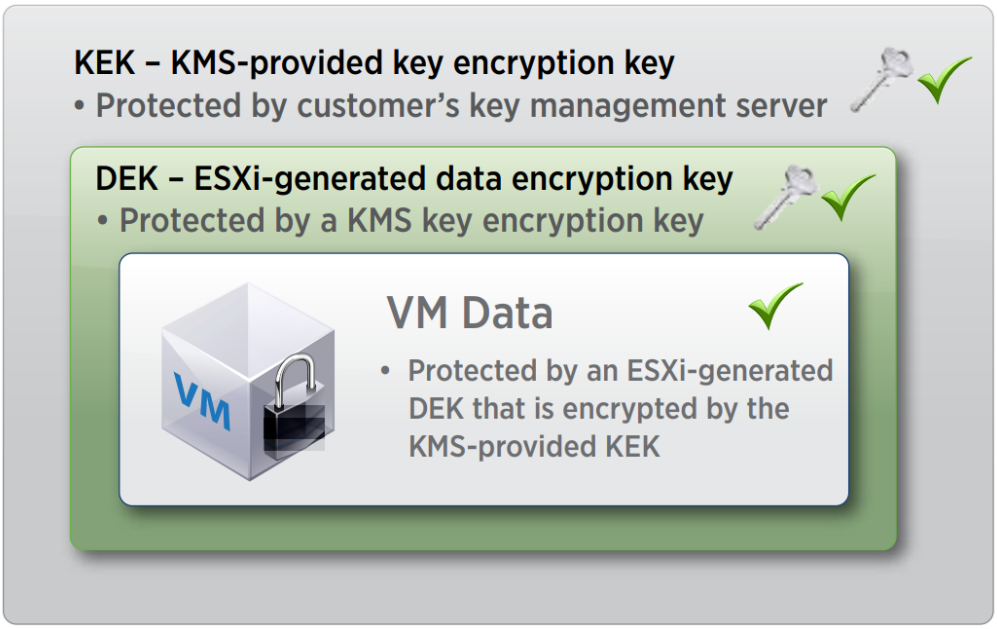
與 VM 關聯的某些檔未加密或部分加密，因為它們不包含敏感資訊：

- 日誌文件
- VM 設定文件
- 虛擬磁碟描述器文件

4.5.5. VM 加密使用兩種類型的密鑰：

- 數據加密密鑰（DEK）：ESXi 主機生成並使用內部密鑰對 VM 和磁碟進行加密。這些 XTS-AES-256 密鑰用作 DEK。
- 密鑰加密密鑰（KEK）：vCenter Server 實例從 KMS 請求 AES-256 密鑰。 vCenter Server 僅存儲每個 KEK 的 ID，但不儲存密鑰本身。

當主機需要密鑰時，vCenter Server 系統將需要加密 VM 的 KEK 轉移到 ESXi 主機。 ESXi 主機使用 KEK 加密 DEK，並把此已加密的 DEK 儲存到已加密的磁碟上。 ESXi 主機不會在磁碟上儲存 KEK。 下圖說明了 KEK 和 DEK 的作用。




## 4.6. 雲平臺的可用性

4.6.1. 服務平臺內的所有核心設備均採用備用設計，任何單一硬體的故障均不會對客戶的業務系統造成中斷。

4.6.2. 服務平臺建立在安全穩定的 VMware 虛擬化平臺上。 泰富國際定期更新 VMware 軟體版本，並對關鍵 VMware 組件（如 vCenter）應用安全修補程式，以確保雲平臺的安全和穩定。

4.6.3. SmartCLOUD 的服務等級協定（SLA）如下：

- SmartCLOUD 資源池：99.99%
- SmartCLOUD 通訊埠：99.9%

有關 SmartCLOUD 服務等級協定的詳細規定，請參考《SmartCLOUD 服務等級協定》。

# 5. 通訊與網路安全

## 5.1. 雲端網路架構設計原則

5.1.1. 區域層次防護

相比傳統的 IDC，雲計算數據中心的網路架構同樣需要多層設計原則，通過劃分區域及層次進而確認各自負責的安全防禦任務。 泰富國際根據內外部分流原則，再

按照關聯性、管理及安全防護等方面的不同需求，將數據中心網路劃分為不同的區域：

- vSphere 基礎架構區（用於 vMotion、儲存等功能）
- 管理區
- 虛擬機區
- 外部網路區（例如網際網路、MPLS 及點對點連接）

5.1.2. 以上的某些安全功能可能需要額外收費，具體情況請諮詢泰富國際銷售人員。

## 5.2. 網路及通訊埠安全

5.2.1. 在 SmartCLOUD 服務中，泰富國際使用 VMware vCloud Director（SmartCLOUD Compute Director）為每位客戶分配專用且獨一的 vLAN 號碼，並由實體及虛擬轉換器（vDS）執行。 vLAN 建立一組交換機連接埠的邏輯群組，虛擬機透過該邏輯群組進行專屬通訊，讓它們在實體上與其他交換機連接埠上的機器分開，確保其數據在傳輸過程中與其他客戶完全隔離。

## 5.3. 網路安全建議

5.3.1. 部署防火牆

為虛擬網路增加防火牆保護，方法是在其中的部分或所有虛擬機上安裝和設定以主機為基礎的防火牆。 為提高效率，可設置專用虛擬機乙太網或虛擬網路。 有了虛擬網路，可在網路最前面的虛擬機上安裝以主機為基礎的防火牆，此防火牆可以充當實體網路轉接器和虛擬網路中剩餘虛擬機之間的保護性快取記憶體。 由於以主機為基礎的防火牆會降低性能，因此請先根據性能目標對安全需求進行權衡，然後再決定在虛擬網路中的其他虛擬機上安裝以主機為基礎的防火牆。

5.3.2. 網路分段

把每個虛擬機區域隔離在自己的網段中，可以大大降低虛擬機區域間洩漏數據的風險。 網路分段可防止多種威脅，包括：

- 位址解析協定（ARP）欺騙：攻擊者操作 ARP 表格以重新映射 MAC 和 IP 位址，進而接入進出主機的網路流量。 達到劫持目標系統、執行阻斷服務 （DoS） 攻擊或以其他方式破壞虛擬網路的目的;
- 中間人攻擊（MITM）：攻擊者通過攔截正常的網路通訊數據，並對數據進行篡改而通訊的雙方卻毫不知情;
- 監聽攻擊：此類攻擊監聽網路上流經的數據封包，進而竊取數據封包內的重要隱

私資訊。

5.3.3. 阻止未授權的存取

泰富國際防護網路安全的首要原則是只允許系統執行必要的連接和網路通訊，所有其他通訊埠、協定，以及連接都會被阻止。 具體安全措施舉例：

- 在路由器上使用分層式訪問控制列表（ ACLs）;
- 在主機上應用 IPsec 策略;
- 在網路中使用防火牆規則和以主機為基礎的防火牆規則對網路通訊、協定，以及通訊埠號進行限制。

# 6. 雲平臺運維安全

## 6.1. 員工安全教育訓練

6.1.1. 泰富國際所有新員工均須參加資訊安全教育訓練，並簽署協定，保證不洩露泰富國際及其客戶的任何機密資訊。

6.1.2. 每位雲計算營運團隊的新員工必須參加產品教育訓練並通過考試。 每位員工根據其工作性質和職務，將參加不同等級的產品教育訓練。

## 6.2. 員工權限控制

6.2.1. 每位泰富國際員工均有一個唯一的登入帳號，此帳號可存取泰富國際內部網路和系統。如員工離職，其登入帳號會被立即停用。

6.2.2. 在管理方面泰富國際遵循「最低權限」的原則，每一位雲計算工程師只賦予能夠完成他日常維運工作所需要的最低權限，進而最大限度的保障客戶數據或資訊的安全性和隱私性。 一般來說，泰富國際的雲計算工程師在管理和維運時只能讀取以下有限的客戶資訊：

- 客戶資源池名稱、類型、大小;
- 客戶數據量名稱、類型、大小;
- 客戶網路編號（vLAN ID）、預設定的 IP 範圍;
- 客戶虛擬機的資源設定、資源的使用率;
- 其他與客戶數據無關的必要維運資訊。

## 6.3. 稽核追蹤

6.3.1. 對於泰富國際內部網路和系統（包括 SmartCLOUD 服務平臺）的重要操作（如用户 ID、時間戳、操作詳細資訊等）的日誌都會被詳細記錄並安全保存，以便在需要的時候隨時進行查看。

6.3.2. 重要的系統操作日誌都會進行保存處理，確保可進行查詢。 客戶可以透過 SmartCLOUD Director 平臺查看相關日誌。

6.3.3. 泰富國際對活動中的任何操作都進行相應的記錄並根據《安全策略手冊》對日誌資訊採取嚴格的保護措施，所有日誌記錄至少保留 180 天。

## 6.4. 用戶憑證

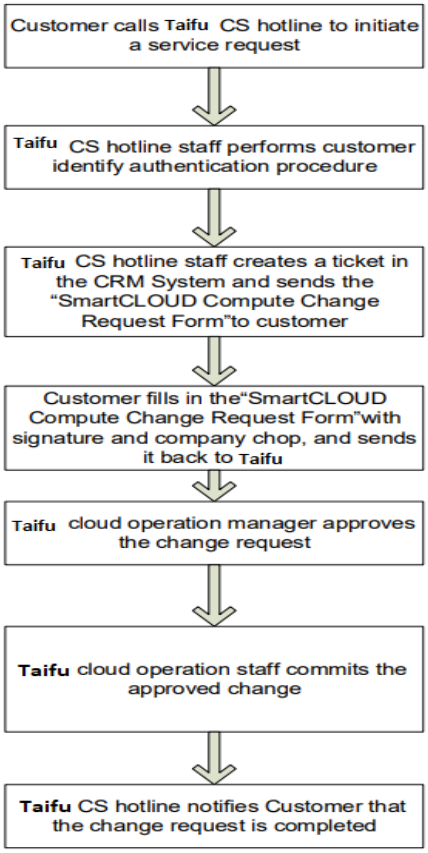
6.4.1. SmartCLOUD 平臺帳號受密碼保護。客戶首次登入平臺後需修改密碼，該密碼長度至少為 10 個字元，由大小寫字母、數位和符號混合組成。泰富國際鼓勵用戶設置較難被猜到的高強度密碼。

6.4.2. 雙因子身份驗證是登入 SmartCLOUD 平臺帳號的附加安全保護層。 客戶除了需要輸入用户名及密碼外，還需要輸入發送至指定電子郵件信箱或手機的六位一次性密碼。

# 7. 服務變更管理

## 7.1. 服務客服流程

7.1.1. 未經客戶許可，雲營運員工不得存取客戶的虛擬機或數據。 僅當客戶發出服務請求時，雲營運員工將嚴格按照流程來處理變更。工作流程如下：

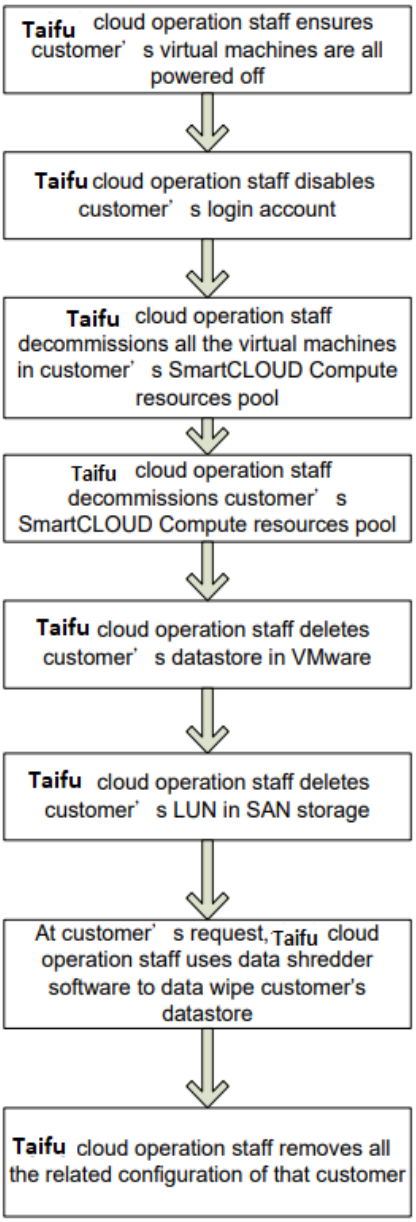



# 8. 數據銷毀

## 8.1. 數據銷毀

### 8.1.1. 客戶數據銷毀

當客戶的《SmartCLOUD 服務合約》終止後，客戶的相關設置會在約定服務結束的 7 天內停用，約定服務結束後 30 天內刪除客戶數據。雲計算營運團隊的員工會徹底刪除該客戶於服務平臺上的所有數據（包括虛擬機/資源池/ datastore / LUN 等）並確認在任何情況下均不可恢復，以保障客戶數據的隱私性。 資料刪除流程如下：




## 8.2. 客户資源池回收

8.2.1. 泰富國際維運工程師確認客户所有的虛擬機都已關閉;

8.2.2. 泰富國際維運工程師凍結客户所有的 SmartCLOUD 服務登入帳號（SmartCLOUD Compute Director / SmartCLOUD Compute Reporter）。

## 8.3. 虛擬機數據銷毀

8.3.1. 泰富國際維運工程師刪除客户所有的虛擬機檔案。

## 8.4. 儲存數據銷毀

8.4.1. 泰富國際維運工程師在 VMware 管理介面中刪除客戶的數據儲存（Datastore）;

8.4.2. 泰富國際維運工程師在 SAN 儲存管理介面中刪除客戶的邏輯單元號（LUN）;

8.4.3. 基於客戶特別要求（需額外付費），泰富國際維運工程師使用數據銷毀軟體徹底銷毀客戶數據（符合 DoD 5220.22-M 標準）;

8.4.4. 泰富國際維運工程師刪除全部與客戶服務相關的設定（包括網路、通訊埠、備份及複製任務等）。

# 9. 數據保護策略

## 9.1. 數據備份及快速恢復服務

9.1.1. 泰富國際在提供雲計算服務的同時，也為客戶提供全面的數據保護服務，防止客戶因技術故障、人為錯誤、自然災害、病毒和特洛伊木馬等原因造成的數據遺失。 泰富國際提供的數據備份服務包括以下範圍：

- 為客戶運行於專屬雲服務平臺上的虛擬機提供本地備份和異地備份的服務。
- 為客戶定期建立備份任務和修改備份設定。
- 24x7x365 不間斷監控備份任務及提供技術支援服務。
- 為客戶提供虛擬機還原，資料夾還原或文件等級的還原服務。

## 9.2. 數據複製及災難恢復服務

9.2.1. 泰富國際也為客戶提供全面的數據複製和災難恢復服務; 當正式環境站點出現重大災難時客戶的虛擬機可以立即在災備站點啟動，進而最大限度的縮短了客戶業務中斷的時間。 當客戶的正式環境站點恢復後，泰富國際可提供災難還原服務，將客戶的虛擬機從災備站點切換回正式環境站點。 泰富國際提供的災難恢復服務包括以下範圍：

- 客戶可以自定虛擬機定期複製至異地數據中心的間隔和相關選項，以滿足客戶要求。
- 24x7x365 不間斷監控複製任務，並在災難演習及真實災難發生時，提供災難恢復和災難還原等技術支援服務。

# 10. 安全事故處理及報告

## 10.1. 資訊安全管理

10.1.1. 安全事故是指不利於客戶利益的資訊洩露或資訊系統和/或網路中的不利事件，對計算機或網路的機密性、完整性和可用性構成威脅。

10.1.2. 安全事故的例子包括：未經授權的存取、未經授權的服務使用、拒絕服務、受保護數據/程序網路系統特權的損害、電子形式的機密數據洩露、惡意破壞或修改數據、滲透和入侵、濫用系統資源、病毒和惡作劇，以及影響網路系統的惡意代碼。

## 10.2. 安全事故處理

10.2.1. 當檢測到安全事故時，由負責方按照預定程序進行反應。 安全事故反應是指處理事故和恢復系統正常運行而執行的行動，這些行動會基於 10.2.2 的安全事故處理的嚴重性，向客戶提供最新更新或訊息。

10.2.2. 泰富國際把每個安全事故主要分為嚴重和受影響等級，對應處理服務如下：

| 等級 | 初步確認 | 第一次<br>反應時間 | 持續定期<br>反應時間 | 描述 |
|---|---|---|---|---|
| 嚴重 | 三十分鐘 | 一小時 | 一小時 | 客戶伺服器/服務中斷<br>( 服務已終止 ) |
| 受影響 | 三十分鐘 | 兩小時 | 兩小時 | 客戶伺服器/服務降級<br>( 備用下降/性能緩慢或不佳/<br>服務不穩定 ) |

10.2.3. 客戶也可以通過電話或電子郵件報告問題/故障以提升程序等級：

| | | |
|---|---|---|
| Level 0 (0 ~ 2 hours): | 第一線客戶服務專線<br>Email: help@taifu.net.tw | Tel: 852-2811-8187 (香港)<br>Tel: 400-880-1222 (中國)<br>Tel: 1800-226-8888 (新加坡)<br>Tel: 0800-606-966 (臺灣)<br>Tel: 60-3-2280-1488 (馬來西亞) |
| Level 1 (2 ~ 4 hours): | 第二線客戶服務 | Tel: 852-2811-8187 (香港) |

| | | |
|---|---|---|
| Level 2 (4 ~ 6 hours): | 客服服務值班工程師 | Tel: 852-2811-8550 (香港) |
| Level 3 (> 6 hours): | 客戶服務支援經理 | Tel: 852-2811-8552 (香港) |

10.2.4. 在安全事故處理後，將採取後續追蹤，對事件進行評估，加強安全防護，防止再次發生。

# 11. 漏洞管理

## 11.1. 漏洞管理方法

11.1.1. 泰富國際將定期對所有的操作流程進行審核和優化，並完成風險評估。審查程式從設計階段已開始，持續至啟動，甚至到正式營運。

11.1.2. 泰富國際保護專屬雲服務平臺免受攻擊，以保證有效率地控制新威脅和漏洞。

11.1.3. 泰富國際將對專屬雲服務平臺及其組件進行評估，驗證現有管制。

# 12. 漏洞報告

## 12.1. 漏洞報告方法

12.1.1. 泰富國際十分重視安全問題，並會調查所有報告漏洞。泰富國際歡迎任何員工、客戶或承辦商報告雲服務在任何方面的漏洞。

12.1.2. 如果要報告漏洞，或有任何關於服務安全方面的問題，請發送郵件至 help@taifu.net.tw。

12.1.3. 請盡可能提供有助於我們了解漏洞性質和嚴重程度的相關資訊（如概念驗證代碼、工具輸出等）。 未經過報告人的允許，泰富國際不會將該資訊透露予第三方。

12.1.4. 泰富國際會審查已提交的報告後，向每個漏洞報告分配一個指定的追蹤編號，並定期通知報告人後續進展。

## 12.2. 漏洞評估

12.2.1. 泰富國際會對所有收到的漏洞報告進行驗證。 如果需要更多資訊才能驗證或重現該問題，泰富國際將會聯繫報告人。

12.2.2. 如果該漏洞涉及第三方產品，泰富國際將通知第三方供應商。 泰富國際會負責報告人和第三方之間的協調。未經過報告人的允許，泰富國際不會將報告人的身份透露予第三方。

12.2.3. 泰富國際使用風險評估工具來評估潛在漏洞。 泰富國際將根據風險評估工具生成的分數評估潛在漏洞的嚴重性以及決定回應的優先順序。

## 12.3. 漏洞公佈

12.3.1. 在確認漏洞之後，泰富國際將向報告人及客戶公佈漏洞的具體情況。

12.3.2. 為保障客戶的資訊安全，泰富國際要求報告人在漏洞未得到泰富國際確認及解決之前，不得向外界透露與該漏洞有關的任何資訊。

# 13. 可接受的使用政策

## 13.1. 禁止非法、有害或冒犯性的使用或內容

13.1.1. 客戶不得利用泰富國際提供的 SmartCLOUD 服務用於任何非法、有害、欺詐、侵權或冒犯性用途， 包括傳輸、儲存、展示、分發或以其他方式提供相關內容。 禁止的活動或內容，包括但不限於：

- 非法、有害或欺詐活動：任何非法、侵犯他人權利或可能損害他人、影響泰富國際營運或聲譽的活動，包括傳播、宣傳或協助製作兒童色情製品、提供或傳播欺詐性商品、服務、計劃或促銷活動，賺取快錢、進行龐氏騙局和層壓式推銷，及網路釣魚或域名欺騙等;
- 侵權內容：侵犯或盜用他人智慧財產權或專有權利的內容;
- 攻擊性內容：誹謗、淫穢、辱罵、侵犯隱私或其他令人反感的內容，包括構成兒童色情、與獸交相關或描繪未經同意的性行為的內容。

## 13.2. 禁止危害網路安全的違規活動

13.2.1. 客戶不得使用泰富國際提供的 SmartCLOUD 服務來破壞任何網路、計算機或通訊系統、軟體應用程式，或網路設備的安全性及完整性。 禁止的活動包括但不限於：

- 未經允許的存取：未經允許存取或使用任何系統，包括試圖探測、掃描或測試系統的漏洞、破壞系統使用的任何安全或身份驗證措施;
- 攔截：未經允許監控系統上的數據或流量;
- 偽造來源：偽造 TCP-IP 表頭、電子郵件表頭或描述其來源或路由任何部分的消息。本條款不禁止合法使用別名和匿名轉發器。

## 13.3. 禁止網路濫用

13.3.1. 除非客戶授權與其他用戶進行通訊，否則客戶不得進行以下但不限於與任何使用者、主機或網路建立網路連接的活動：

- 監控或爬取：會損害或破壞正在監控或爬取的系統;
- 阻斷服務攻擊 （DoS）: 用通訊請求淹沒目標，導致目標無法回應合法流量或速度太慢以至服務中斷;
- 故意干擾：干擾任何系統的正常運行，包括通過郵件轟炸、新聞轟炸、廣播攻擊等，故意使系統超過負荷;
- 某些網路服務的操作：營運開放代理、開放郵件轉遞或開放遞回 DNS 等網路服務;和
- 避免系統限制：使用手動或電子方式避免對系統施加的任何使用限制，例如存取和儲存限制。

## 13.4. 監控及執行

- 泰富國際保留調查任何違反本政策或濫用 SmartCLOUD 服務的權利，但不承擔義務。任何阻斷服務攻擊、通訊埠掃描和探測、釋放病毒或蠕蟲、其他惡意活動（不論是是故意或無意），或任何未經授權嘗試存取任何其他帳戶、主機或網路來破壞身份驗證或安全措施的行為，該客戶的雲服務將被立即終止並不作另行通知。