

## hicloud CaaS/CVPC/S3 資訊安全暨隱私權聲明

當您使用 hicloud 的 CaaS/CVPC/S3 服務(以下簡稱本服務)時，您將寶貴的資料委託給我們保管，我們非常在乎您的資料安全與隱私權，故您使用本服務時，我們遵循法規(如個資法)且以合法的方式使用，並遵照內部程序與資安規定執行，保護您資料的隱私權及資料安全是我們的目標。

您於本文為任何修改或變更後仍繼續使用本服務時，視為您已確實閱讀、瞭解並同意遵守本文之修改或變更。

若您尚未成年，除您本人應遵守上述規定外，並請您的家長（或監護人）同時確實閱讀、瞭解並同意遵守本文之所有內容，您方得使用或繼續使用本服務；當您於本文為修改或變更後仍繼續使用本服務時，即表示您的家長（或監護人）亦已確實閱讀、瞭解並同意遵守本文之修改或變更。

### 1 資訊安全政策

本服務為您提供隨選、彈性的資源配置，包含隨點即用便利性高的 CaaS、外部 (Internet)與內部網路隔離高安全性的 CVPC、接取私有網路(VPN)、hicloud S3 雲儲存及帳號權限管理(IAM 管理)。

為確保雲端網路的安全，雲端服務中心全年無休的持續觀察訊務，盡力減少異常訊務對於您的影響，而供給您多樣選擇的資訊安全服務，包含防火牆、IPS、DDoS 防護等，倘若不幸發生事故，我們亦會依據流程提供紀錄(如 log)。

### 2 客戶資訊及數據資料定義

- 2.1 數據資料：您使用本服務時，所申租之特定資源，如：虛擬主機、虛擬主機範本、雲儲存。
- 2.2 客戶資訊：本服務所需的客戶資訊，如：姓名、英文姓名、電話號碼、地址、證號(身分證號、或護照號碼、或統一編號等)、email、會員帳號、支付工具卡號、設備號碼(如 HNXXXXXXXXX、行動電話號碼)、信用卡卡號、有效年月、卡片後三碼、網路識別碼(如 IP、cookie)等。
- 2.3 數據資料之控制者：使用本服務時，本服務所提供的數據資料之擁有者，如：虛擬主機擁有人等。
- 2.4 數據資料之處理者：依數據資料之控制者的操作或指示處理該數據資料。
- 2.5 客戶資訊之控制者：使用本服務時，中華電信 hicloud 為您所提供的客戶資訊控制者；依法規定註冊 IP 需提供 TWNIC 使用者資訊，因此 TWNIC 為控制者，而中華電信為處理者。

### 3 隱私權政策

感謝您使用本服務，您個人的隱私權，我們絕對尊重並予以保護。為了幫助您瞭解，我們如何蒐集及處理保護您所提供的客戶資訊，請您詳細閱讀以下內容。

### 3.1 蒐集、處理與您的權利

我們會蒐集您的以下資訊：

3.1.1 個人資訊：姓名、英文姓名、證號(身分證字號、護照號碼或統一編號)

3.1.2 聯繫資訊：電話、手機、帳單地址、戶籍地址(僅限紙本)、email

3.1.3 網路識別碼，如 IP、cookie 等

3.1.4 付款使用的支付工具號碼或信用卡資訊：信用卡卡號、有效年月、CVV 三碼驗證碼。

上述客戶資訊您得自由選擇填寫，但若資料不足時將影響服務申請或其完整性；上述客戶資訊在您提出終止後，紙本資訊保留二年及電子資訊則依稅務法規定年限。

### 3.2 中華電信 hicloud 作為客戶資訊的控制者，我們基於以下目的而處理您的客戶資料：

3.2.1 客戶服務，如服務異常處理、紙本申請作業、使用情形關懷等作為。

3.2.2 帳務服務，如費用收取、信用卡認證、欠費、停止、拆除、或催收帳務等作為。

3.2.3 其他依法令規定(如個資法等)、與本服務有合作關係的供應商(鏈)等。

### 3.3 中華電信 hicloud 作為數據資料的處理者，客戶的數據資料會因為以下目的被處理：

3.3.1 hicloud 將根據書面指示處理客戶數據資料，如虛擬主機資源異動、S3 數據資料異動。書面指示範圍之外的其他指示需要 hicloud 和客戶之間的事先書面協議。書面指示包括租用契約、客戶透過 hicloud 管理控制台或 hicloud 為服務提供的 API 指示。

3.3.2 您使用網路位址(IP)相關事宜，依規定應登錄之使用人名稱、email、電話與地址。

### 3.4 您得依相關法律規定，就上述客戶資訊請求查詢、閱覽、製給複製本、補充更正、請求停止蒐集、處理、利用、刪除、以及資料可攜、反對等權利，行使前揭權利時，需撥免付費客服電話 0800-080-365。

### 3.5 您行使上開權利之資訊提供方式、處理期限、查詢費用及繳費期限等事項，均依法令及服務契約相關規定辦理，並得酌收必要成本費用。我們得依執行業務所必需及法定保存期間等考量，決定是否接受申請。

### 3.6 中華電信 hicloud 服務之客戶資訊與數據資料必須事前取得您的同意才會用於

行銷或廣告目的。

#### 4 資訊安全暨隱私權雙方角色與責任

本服務係由我們負責基礎設施，如虛擬化環境(hypervisor)、維持虛擬化環境的實體主機設備、相關網路基礎設施、儲存設備、雲儲存服務、使用者操作平台與雲端機房實體安全等。

而您透過使用者操作平台所申租的服務，如虛擬主機、防火牆等、或作業系統層的更新、弱點修補、或其他安裝程式/資料等、或您自行放置的資料與安裝的程式，前述的資訊安全由您負責；上述您所負責的內容，如您需要我們的協助，請透過撥打客服專線或障礙申告等方式通知我們，我們會盡力協助您，但部分的協助或許需支付費用。

您為數據資料之控制者或處理者，而中華電信 hicloud 為此資料之處理者，中華電信 hicloud 擔任數據資料之處理者時，將僅依客戶的操作或指示處理。

#### 5 資訊安全與隱私權作為

- 5.1 我們提供本服務的資訊安全與隱私權皆遵守 ISO 27001、NCC 27011、ISO 27017、ISO 27018、ISO27701 與 CSA STAR 的規範，並定期請公正第三方審視。
- 5.2 本服務的使用者操作平台委由中華電信研究院開發，開發過程皆遵守 CMMI-DEV ML3 的規範，並依據 OWASP 所釋出的風險或弱點，持續性地進行修正與補強。
- 5.3 本服務的基礎設施與使用者操作平台，我們有防毒保護措施與定期備份，且持續修正與補強弱點。
- 5.4 存取管理方面，本服務的管理後台會透過高安全性的管道維運，如維運作業需透過雙因子的身分認證、維運網路環境與 Internet 隔離等措施。
- 5.5 我們有提供您自行管理您的數據資料的存取權限，以及虛擬主機自行備份或復原等(如快照與還原)功能。
- 5.6 我們有提供您可透過 log 紀錄查詢您的 CaaS/CVPC 虛擬主機操作日誌，如虛擬主機的開關機、複製等，log 保留期限比照個資法規定，並執行安全的保護與保存。
- 5.7 我們有提供您可透過啟用 S3 bucket logging 功能查詢您的 S3 上的資料操作日誌，如檔案查詢、刪除、新增等，保留期限為用戶自訂，並執行安全的保護與保存。
- 5.8 我們會有嚴格的安全管制措施管理雲端服務機房，以保障您的資料完整性、安全性與機密性。
- 5.9 我們的基礎設施的 NTP 校正標準來自於國家標準時間，但可能因為 Internet

傳輸延遲因素，所顯示的時間可能與國家標準時間有所差異。

- 5.10 為提供您更完善之服務，本服務的使用者操作平台會使用 Cookie 以記錄使用者行為，此記錄能夠辨識使用者，例如依您偏好的特定種類資料執行不同動作。如果您不希望接受 Cookie，請自行利用瀏覽器之設定加以排除；但您將可能無法使用本網站所提供的部分服務。

## 6 供應商(鏈)

- 6.1 本服務的 24 小時雲端機房、免付費客服中心的客戶和帳戶服務業務，以及基礎設施的設備提供，我們委託供應商(鏈)負責並簽訂契約，其內容包含資通安全要求，如您有供應商(鏈)的相關問題，請和我們聯繫。
- 6.2 如有您使用 hicloud 服務時，您將同意授權我們的供應商(鏈)宏華國際股份有限公司，根據您的要求進行數據資料的處理及必要處置。hicloud 在變更供應商(鏈)前至少 30 天，會公告於網站，若您反對此供應商(鏈)，您可以辦理終止服務。

## 7 資料自我保護措施

- 7.1 數據資料：依據租用契約第四十六條，您的數據資料我們負有保密的義務，中華電信 hicloud 接獲具法律約束力的客戶數據(強制性)揭露要求，hicloud 將合理通知客戶該要求，以便客戶尋求保護令或其他適當救濟措施，除非 hicloud 在法律上被禁止這樣做。我們會定期於網站上公布統計資料，內容為前述四十六條所稱機關要求與我們提供的次數。中華電信 hicloud 將拒絕任何不具法律約束力的數據資料揭露要求。
- 7.2 客戶資訊：您的客戶資訊我們負有保密的義務，亦請妥善保管您的密碼或任何資訊，不要將任何資訊，尤其是密碼提供給任何人，如想提高安全，我們建議您啟用雙因子認證。在使用完成本服務後，務必記得登出帳戶，若是與他人共享電腦或使用公共電腦，切記要關閉瀏覽器視窗或清除 cookie 和紀錄，以防止他人讀取您的資訊。

## 8 法律

- 8.1 中華電信 hicloud 謹遵守資訊技術服務提供者所適用之法令規定 (即中華民國法律)，包括個資保護法及主管機關行政命令之規定，惟中華電信 hicloud 若認知到您指示操作個資的方式有違反法律的疑慮(情形)時，將透過適當方式告知您。
- 8.2 中華電信 hicloud 並無任何義務遵守您或其產業相關可能適用之該國法令，也不會決定您之資料是否受任何特定法律或規定所拘束之資訊，相關安全性事件係受安全性事件通知條款之拘束。



- 8.3 當您使用本產品與服務時，需自行遵守一切相關之法令規定，包括個資保護法及您所應該適用的主管機關行政命令之規定。您應自行決定產品與服務是否適合儲存和處理等措施，您應瞭解本產品與服務之使用方式，是否符合您與您的客戶之相關法律義務；您應自行負責決定所有資訊，是否受您所應適用之任何法律或特定規範所拘束。

## 9 儲存位置

本服務所有客戶數據資料與客戶資訊均存放於中華民國境內，謹遵守中華民國法律。未經您同意，我們不會將您的資料移出或複製到本國以外的地方，如有變更請參考官網公告，如您反對變更可終止服務。

## 10 數據資料加密

- 10.1 數據資料加密：如您需加密數據資料，虛擬主機我們提供資料加密的指引，讓您自行決定您的資料是否需加密，請參考官方網站的作業系統檔案與磁碟加密 SOP 文件；hicloud S3 請參考官方網站文件進行資料加密功能啟用。
- 10.2 數據資料傳輸過程加密：中華電信 hicloud 虛擬主機與虛擬主機範本傳輸通道皆加密，例如虛擬主機轉存為範本與範本轉存到 S3 等，hicloud S3 服務也提供傳輸過程加密功能，讓您自行決定資料是否於傳輸過程需加密。

## 11 刪除實體儲存設備資料

我們基礎設施的儲存設備故障或汰換，設備上的資料會被安全抹除或銷毀，以確保無法透過任何方式恢復數據資料。

## 12 資訊安全與隱私權事件處理

- 12.1 通知：如您發現租用之本服務有可疑活動，或其他客戶的可疑活動影響到您，請依據租用契約或網站上的聯繫方式通知我們；但若我們發現您的資料有可疑活動(如遺失、洩漏或遭竄改)，且發生問題原因歸責於我們時，我們會在 72 小時內通知您，前述通知時間不包含不可控因素(如:風災、水災、地震、政治、戰爭、國際傳染疫情等)。
- 12.2 回應：事件發生時，我們會依程序了解並分析可能的狀況，並盡力降低對您的影響，過程中可能會請您提供資訊，並將處理結果通知您。
- 12.3 回覆方式與內容：經我們確認可疑活動確實存在(不論由我們或您發現)，且會影響到我們的其他客戶時，我們將會以公告或 email 個別通知；其內容在不影響其他客戶的隱私原則下，會包含事件的影響範圍。
- 12.4 建議措施：資訊安全或隱私權事件發生時，建議您使用我們提供的備份或還原功能恢復虛擬主機，同時洽詢您的資訊安全或資料保護人員或廠商，如您沒有

資安或資料保護人員，可洽詢本公司業務，為您建議並規劃服務。

## 13 終止服務

- 13.1 當您不再使用 hicloud CaaS、CVPC 雲伺服器與 S3 雲儲存時，應辦理終止作業，我們不再保留任何資料，如果您需要保留虛擬主機，應在退租終止本服務前自行將虛擬主機轉為範本，並匯出至 hicloud S3，然而 hicloud S3 的資料，由您選擇要刪除或載回本地或其他雲儲存空間。
- 13.2 hicloud CaaS、CVPC 與 S3 如於您的電信帳單繳納期限截止日或信用卡扣款失敗之日起，17 天內您將無法使用 hicloud CaaS、CVPC 與 S3，第 17 天起系統自動終止您的 hicloud CaaS、CVPC 與 S3，我們不再保留任何資料。您得於前述期間內提出申請復裝，但增值服務(如防火牆服務、負載平衡、監控等)仍需重新申請。
- 13.3 除依據中華電信股份有限公司雲端服務租用契約(下稱租用契約)所列不法行為外，如您超過 24 個月未登入本服務使用者操作平台(登入紀錄以本公司使用者平台為主)，且未使用任何 hicloud 服務，則本公司得不經通知終止您的帳號。

## 14 附則

前述各項未說明之事項，您同意遵守相關法令規定、及租用契約等之有關規定。

前述各項或本服務契約如有中英文版本之文義，英文翻譯僅供參考，應以中文版之文義為主。

## hicloud CaaS/CVPC/S3 Information Security & Privacy Policy

When you use hicloud CaaS/CVPC/S3 service (henceforth referred to as the Service), you entrust valuable data to us. We care about your data security and privacy. When you use the Service, we follow the regulations (such as the Personal Information Protection Act), the internal procedures and security policy. It is our goal to protect the privacy and data security of your data.

When you continue to use the Service after any modifications or changes of this policy, we consider that you have read, understood, agreed and complied with the modifications or changes of this policy.

If you are not adult, not only you should comply with above policy but also your parent (or guardian) should read, understand, agree and comply with all the contents of this policy at the same time in order to use or continue to use the Service. When you continue to use the Service after any modifications or changes of this policy, we consider that your parent (or guardian) have read, understood, agreed and complied with the modifications or changes of this policy.

### 1 Information Security Policy

The Service provides you with on-demand and flexible resource configuration including CaaS which is easy-to-use, CVPC which is high security, private network (VPN) services, S3 which is cloud storage service and account management (IAM management).

In order to ensure the security of the cloud network, the cloud service center continuously observes the traffic all the year round, tries to reduce the impact of abnormal traffic on you, and provides you with various choices of information security services including firewall, IPS, DDoS protection, etc. If necessary, we can also provide records (such as log) according to the process.

### 2 Customer information and data definition

2.1 PII: When you use this service, specific resources you subscribe, such as virtual machines, virtual machine templates, cloud storage.

2.2 Customer Information: Customer information required for the Service, such as name, English name, phone number, address, certificate number (identity number, passport number, or uniform number, etc.), email, member account, payment instrument card number, equipment number (such as HNXXXXXXXX and mobile phone number), credit card number, valid year and month, Card Validation Code (CVC), network identification code (such as IP, cookie).

2.3 PII Controller: The owner of the data provided by the service when using the service, e.g., a virtual host owner is the controller.

- 2.4 PII Processor: Process the data as per the operations or instructions of the PII controller.
- 2.5 Customer Information Controller: When using this service, Chunghwa Telecom hicloud is the controller of the customer information provided to you. According to legal regulations, to register the IP we must provide user information, so TWNIC is the controller and Chunghwa Telecom is the processor.

### 3 Privacy Policy

Thank you for subscribing the Service. We absolutely respect and protect your personal privacy. For better understanding how we collect and process the customer information you provide, please read the following carefully.

#### 3.1 Collect, process and your rights

We will collect the following information:

- 3.1.1 Personal information: name, English name, certificate number (identity certificate number, passport number or uniform number)
- 3.1.2 Contact information: phone, mobile phone, billing address, Registered permanent residence(only paper), email
- 3.1.3 Network identification codes, such as IP, cookies, etc.
- 3.1.4 Payment instrument number or credit card information used for payment: credit card number, valid year and month, CVV verification code.

After the termination of the above customer information, the paper information is retained for two years and the electronic information is kept for the period specified in the law.

#### 3.2 Chunghwa Telecom hicloud is the PII controller for the aforementioned collection of customer data, and this information will be used for the following purposes.

- 3.2.1 Customer service, such as service exception handling, paper application process, user experience, etc.
- 3.2.2 Accounting services, such as fee collection, credit card certification, arrears, suspension, dismantling, or collection of accounts.
- 3.2.3 Other legal regulations (such as the Personal Information Protection Act, etc.), and supply chain.

#### 3.3 As the data processor of PII hicloud, Chunghwa Telecom will process customers data for the following purposes:

- 3.3.1 hicloud will only process PII customers data based on written instructions, such as modifications to virtual machine resources or modifications to S3 data. Any instructions beyond the scope of written instructions require prior written agreement between hicloud and the customer. Written instructions include instructions provided by lease contracts, the hicloud management console, or the



APIs provided by hicloud for the service.

3.3.2 For matters related to the use of Internet addresses (IP), the user's name, email, phone number and address should be logged in according to regulations.

3.4 You can request to inquire, read, make copies, make supplementary corrections, and request the right to stop collecting, processing, utilizing, deleting and also the right to data portability, objection for the above-mentioned customer information, in accordance with relevant laws and regulations. When enforcing rights mentioned above, you need to dial the customer service phone number 0800-080-365.

3.5 The rights you exercise as described in the Previous. We deal with mentioned in comply with the relevant law and service contract. We will charge the necessary cost and decide whether to accept the application based on considerations such as the necessary and legal preservation period for the execution of the business.

3.6 Customer information and data provided by Chunghwa Telecom hicloud services must obtain your prior consent before being used for marketing or advertising purposes.

#### 4 The roles and responsibilities of both side in information security and privacy

The Service is responsible for the infrastructure, such as the hypervisor, the physical host device for the virtualized environment, the related network infrastructure, the storage device, the cloud storage service, the user operating platform and the physical security of the cloud data center.

The services you subscribe through the user operation platform, such as virtual machines, firewalls, operating system updates, vulnerability patches, or other installed programs/data, or the data and programs you deploy on your own, is your responsibility. If you require our assistance for the responsibilities mentioned above, please notify us through methods such as calling our customer service hotline or reporting issues. We will make every effort to assist you, although some assistance may be subject to charges.

You are the PII controller or processor, while Chunghwa Telecom hicloud is the PII processor for this data. When Chunghwa Telecom hicloud acts as the PII processor for personal data, it will process the data only in accordance with the customer's operations or instructions.

#### 5 Information security and privacy action

5.1 The information security and privacy of our services is following ISO 27001, NCC 27011, ISO 27017, ISO 27018, ISO27701 and CSA STAR specifications, and is regularly reviewed by a fair third party.

5.2 This Service is developed by Chunghwa Telecom Research Institute. The process complies with the specifications of CMMI-DEV ML3 and is continuously revised and reinforced according to the security risks or weaknesses released by OWASP.

5.3 The infrastructure of the Service and user portal have anti-virus protection, regular backup, and continue to correct and strengthen weaknesses.

5.4 In terms of access management, the management background of the Service will be operated by high-security environment. For example, the maintenance work requires to be verified by two-factor authentication and the network environment isolates from the Internet.

5.5 We provide access authentication for you to manage your data and snapshot or restore function to virtual machine.

5.6 We provide you with a log record to query your CaaS/CVPC operation log of data, such as power on, power-off and copy of virtual machine, etc. The period of Log retention is based on the Personal Information Protection Act and perform protection and preservation of security.

5.7 We provide you with the ability to query your S3 data operation logs, such as file searches, deletions, additions, and more, through enabling the S3 bucket logging feature. The retention period is user-defined, and we ensure secure protection and preservation of these logs.

5.8 We have rigorous security controls to manage the cloud service data center in order to protect your data integrity, security and confidentiality.

5.9 The NTP standard of our infrastructure comes from National Standard Time, but displayed time may differ from the National Standard Time (NST) due to Internet transmission.

5.10 In order to provide you with a better service, the user portal of the Service uses cookies to record user behavior. This record can identify users, for example, perform different actions according to the specific kind of data you prefer. If you do not wish to accept cookies, please use your browser settings to exclude them. However, you may not be able to use some of the services offered by this website.

## 6 Suppliers chain

6.1 The customer and account services of the 24-hour data center and the free customer service center, and the equipment supply of infrastructure are entrusted to the supplier (chain) to be responsible, all of which are in accordance with the company's regulations, signing a contract and including information security terms, if you have any questions about suppliers (chains), please contact us.

6.2 If you use the hicloud service, you agree to authorize our supplier (chain), Hong Hua International Co., Ltd. to process the data and necessary dispositions according to your request. hicloud will announce on the website at least 30 days prior to the change of our supplier (chain), and if you object to this provider, you have to apply for the termination of the service.

## 7 Data self-protection measures

- 7.1 Data: According to Article 46 of Chunghwa Telecom's hicloud service lease contract, we have the obligation to keep your data confidential. If Chunghwa Telecom hicloud receives a legally binding (mandatory) disclosure request for customer data, hicloud will reasonably notify the customer of the request. , so that Customer may seek a protective order or other appropriate relief, unless hicloud is legally prohibited from doing so. We will regularly publish statistical information on our website, which contains the number of times the agencies requested and provided by us as mentioned in the forty-sixth article above. Chunghwa Telecom hicloud will reject any non-legally binding PII disclosure request.
- 7.2 Customer Information: We are obligated to keep your customer information confidential. Please keep your password or any information safely. Do not provide any information especially the password to anyone, if you would to increase security we suggest you using two-factor authentication. After you use the Service, be sure to log out of your account. If you are sharing a computer with another person or using a public computer, remember to close the browser window or clear cookie and record to prevent others from reading your information.

## 8 Law

- 8.1 Chunghwa Telecom hicloud only complies with all applicable laws and regulations applicable to the service provider in our country (i.e., the laws of the Republic of China), including the provisions of the Personal Information Protection Law and the administrative orders of the competent authorities. However, if Chunghwa Telecom hicloud recognizes that there is any suspicion that the manner in which you have instructed the operation of your data information is in violation of any law, Chunghwa Telecom hicloud will notify you in an appropriate manner.
- 8.2 Chunghwa Telecom hicloud is not under any obligation to comply with the laws and regulations of your country that may be applicable to your customer or its industry, and Chunghwa Telecom hicloud only complies with the laws or regulations generally applicable to information technology service providers. The relevant security events was restrained to the terms of the security event notification action.
- 8.3 When you use the Service, you are responsible for complying with all relevant laws and regulations, including personal information protection laws and administrative orders of the competent authorities to which you should apply. You shall decide for yourself whether the Service is suitable for storage and processing measures, and you shall understand whether the use of the Service complies with the relevant legal obligations of you and your customers; you shall be responsible for deciding for yourself whether all information is subject to any law or specific regulation that you

shall apply.

## 9 Storage location

All customer data and information are stored in the Republic of China (Taiwan) and are subject to the laws of the R.O.C. We will not transfer or copy your information outside of the R.O.C. (Taiwan). We will not move or copy your information outside of this country.

## 10 Data encryption

We provide data encryption guidelines so that you can decide whether your data needs to be encrypted. Please refer to the operating system files and disk encryption SOP documents on the official website. For S3 services, please refer to the official website documents to enable the data encryption function.

10.1 Data encryption: if you need encryption data, we provide data encryption guidelines for virtual machine, allowing you to decide by yourself. Whether the data needs to be encrypted. Please refer to the operating system files and disk encryption SOP documents on the official website. For hicloud S3, please refer to the official website documents to enable the data encryption function.

10.2 Encryption of data transmission process: Chunghwa Telecom's hicloud transmission channels are encrypted include virtual machine and virtual machine template were transmission. For example, the virtual machine is transferred to a template and the template is transferred to S3 bucket. The hicloud S3 service also provides the transmission process encryption function, allowing you to decide by yourself. Whether the data needs to be encrypted during transmission.

## 11 Delete information of physical storage device

The failure or replacement of our infrastructure storage equipment ensure that the data on the equipment will be safely erased or destroyed and cannot be recovered in any way.

## 12 Information security and privacy incident handling

12.1 Notification: Notification: If you find suspicious activity of the service rented, or suspicious activity of other customers affects you, please notify us according to Chunghwa Telecom's hicloud service lease contract or the contact method on the website; but if we find that your When suspicious activities (such as loss, leakage or tampering) are attributed to us, we will notify you within 72 hours. The aforementioned notification time does not contain uncontrollable factors (such as: politics, wind disasters, floods, wars, International infectious diseases, etc.).

12.2 Response: When an event occurs, we will follow the procedure to understand and analyze the possible conditions, and try our best to reduce the impact on you. During the process, you may be asked to provide information and notify you of the

processing results.

- 12.3 Response methods and content: When we confirm that suspicious activity does exist (whether discovered by us or you) and will affect our other customers, we will notify you individually by announcement or email; its content will include the scope of the incident, without violating the privacy principles of other customers.
- 12.4 Recommended measures: When an information security and privacy incident occurs, it is recommended that you use the backup or restore function provided by us to recover virtual machine, and at the same time contact your information security (or data protect) personnel or manufacturer. If you do not have security (or data protect) personnel, you can contact the company's business for you suggest and plan security services.

### 13 Terminate service

- 13.1 When you would not use the hicloud CaaS, CPVC and S3 service, you should terminate the subscription and we will not retain any data. If you need to retain your virtual machine, you should convert it to a template file and export it to the hicloud S3 service before terminating the service. However, it is up to you to delete or load back the hicloud S3 data to local or other cloud storage spaces.
- 13.2 If you are unable to use hicloud CaaS, CVPC and S3 for 17 days after the due date of your telecommunication bill or the date of your credit card debit failure, your hicloud CaaS, CVPC and S3 will be automatically terminated from the 17th day onwards and we will no longer retain any of your data. You may apply for reinstallation within the above period and value-added services (e.g. firewall services, load balancing, monitoring, etc.) still need to be re-applied.
- 13.3 In addition to Illegal behavior in Chunghwa Telecom's hicloud service lease contract, if you have not logged in to the user operation platform of this service for more than 24 months (login records are mainly based on the user operating platform), and no any hicloud resource (such as VM etc.). The Company would terminate your account without notice.

### 14 Supplementary

With regard to the matters not specified above, you agree to abide by the relevant laws, regulations, and the relevant provisions of Chunghwa Telecom's hicloud service contract.

The English translation is for reference only and should not be construed as binding on the terms; The Agreement and Policy shall be construed and enforced in Chinese language.