

hicloud CaaS/CVPC 資訊安全暨隱私權政策

當您使用 hicloud 的 CaaS/CVPC 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。

您於本政策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、瞭解並同意遵守本政策之修改或變更。

若您未滿二十歲，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、瞭解並同意遵守本政策之所有內容，您方得使用或繼續使用本服務；當您於本政策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、瞭解並同意遵守本政策之修改或變更。

一、 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)的服務，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)。

二、 客戶資訊及數據資料定義：

1. 數據資料：您使用本服務時，本服務所提供的數據資料，如：虛擬主機等。
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。

三、 資訊安全角色與責任：

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、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。

四、 資訊安全作為：

我們提供本服務的資訊安全皆遵守 ISO 27001、NCC 27011、ISO 27017、ISO 27018 與 CSA STAR 的規範，並定期請公正第三方審視。

本服務開發委由中華電信研究院，過程皆遵守 CMMI-DEV ML3 的規範，並依據 OWASP 所釋出的資安風險或弱點，持續性地進行修正與補強。

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。

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，如維運人員需透過雙因子的身分認證、維運網路環境與 Internet 隔離等措施。

我們有提供您自行管理您的數據資料的存取權限，以及數據資料自行備份或復原等(如虛擬主機的快照與還原)功能。

我們有提供您可透過 log 紀錄查詢您的數據資料操作日誌，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。

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。

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。

當您不再使用我們的 hicloud CaaS 雲伺服器時，應辦理終止作業，如於 3 天之內系統尚未進行清除作業時，您得於上班時間(9:00~18:00)提出申請復裝(需支付費用)，此復裝即為重啟申請作業，恢復您的租用權利。我們將在第 4~11 天內逐步清除您的數據資料，第 12 天起我們完全沒有您的數據資料。

當您不再使用 hicloud CVPC 雲伺服器時，應辦理終止作業，我們不再保留任何資料。

如果您需要保留您的數據資料，您應在退租終止本服務前將其轉為範本檔案，並使用 S3 服務匯出。

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。

五、 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。

1. 蒐集、處理與您的權利

我們會蒐集您的以下資訊：

- (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)
- (2) 聯繫資訊：電話、手機、帳單地址、email
- (3) 網路識別碼，如 IP、cookie 等。
- (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。

上述客戶資訊保存時間為法令規定之期間或您提出終止後二年紙本資訊或十五年電子資訊。

2. 上述客戶資訊因為以下目的會被使用：

- (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。
- (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) 網路位址註冊，如您有使用到網路位址(IP)，依據法規規定，需登錄使用人。
- (4) 其他依法令規定(如檢警調需求等)、與本服務有契約關係者等。

3. 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、利用及刪除等權利，行使前揭權利時，需撥免付費客服電話 0800-080-365。

4. 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。

六、 資料自我保護措施：

1. 數據資料：依據中華電信 hicloud 服務租用契約第四十五條，您的數據資料我們負有保密的義務，我們會定期於網站上公布統計資料，內容為前述四十五條所稱機關要求與我們提供的次數。
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。在您使用完成本服務後，務必記得登出帳戶，若您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，以防止他人讀取您的資訊。

七、 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，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。

八、 數據資料加密

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。

九、 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。

十、 資訊安全事件通報

如您發現租用之本服務有可疑活動，請依據中華電信 hicloud 服務租用契約或網站上的連繫方式通知我們，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。

前項經我們確認可疑活動確實存在，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。

依前述資訊安全政策說明，我們會盡力保護您的數據與客戶資訊，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重大服務異常或不可控的天然災害情形。

十一、 附則

前述各項未說明之事項，您同意遵守相關法令規定、及中華電信 hicloud 服務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如有歧異時，應以中文版之文義為主。

hicloud CaaS/CVPC Information Security & Privacy Policy

When you use hicloud CaaS/CVPC service (hereinafter referred to as the Service), you entrust valuable information to us for safekeeping. We care about your data security and privacy, so when you use this Service, we follow the regulations (such as the Taiwan Personal Information Protection Act) and use your data in a legal manner, and comply with internal procedures and security regulations. It is our goal to protect the privacy and security of your data.

When you continue to use this Service following any modification or change to this Policy, it will be deemed that you have read, understood and agreed to comply with the modifications or changes to this policy.

If you are under the age of 20, you may use or continue to use the Service, provided that not only should you comply with the above requirements but you should also request your parent (or guardian) to read, understand and agree to abide by all the contents of this policy at the same time; Your continued use of the Service after any modification or change has been made to this Policy means that your parent (or guardian) has actually read, understood and agreed to abide by the modifications or changes to this policy.

1 Information Security Policy:

This Service provides you with on-demand, flexible resource configuration, including click-to-deploy high convenience CaaS, external (Internet) and internal network isolation high security CVPC, access to private network (VPN) services, and identity and access management (IAM).

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. Should there be any security incident, we will provide records (such as log) according to the process.

2 Definition:

2.1 Digital Data: The data provided by the Service when you use the Service, such as virtual machine.

2.2 Customer Information: Customer information required for this Service, such as: name, English name, phone number, address, certificate number (ID card number, or passport number, or uniform number, etc.), email, member account, payment instrument card number, equipment Number (such as HNXXXXXXXX, mobile phone number), credit card number, year and month of expiration date, card security code, network identification code (such as IP, cookie).

3 Information Security Roles and Responsibilities:

This Service is responsible for the infrastructure, such as the hypervisor, the physical host device that maintains the virtualized environment, the related network infrastructure, the storage device, the user operating platform and the physical security of the cloud room.

The services you rent through the user operating platform such as virtual machine or firewalls, updates or vulnerability fixes in operating system layer, other installers/data, or your own data and installed programs, information security of the above is your responsibility.

4 Information Security Action

4.1 The information security of our Services complies with ISO 27001, NCC 27011, ISO 27017, ISO 27018 and CSA STAR specifications, and is regularly reviewed by a fair third party.

4.2 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.

4.3 As to infrastructure and user operation platform of the Service, we have anti-virus protection measures and regular backup, and continue to correct and strengthen weaknesses.

4.4 In terms of access management, the management backend of the Service will be maintained and operated through high-security methods. For example, the maintenance personnel are required to pass two-factor identity authentication, and the maintained network environment and the Internet are isolated.

4.5 We provide features such as access authority to manage your Digital Data, and to back up or restore your Digital Data (such as snapshots and restores of virtual machine).

4.6 We provide you with a log record to query your Digital Data operation log, such as virtual machine power on/off, copy, etc.; log retention period is according to the Taiwan Personal Information Protection Act, and we perform security protection and preservation accordingly.

4.7 We have strict security controls to manage IDC room for the cloud service to protect your data integrity, security and confidentiality.

4.8 The NTP calibration standard for our infrastructure is subject to national standard time, but the time displayed may be different from national standard time due to transmission delay in the Internet.

4.9 When you no longer use our hicloud CaaS cloud server, you shall make termination process. During 3-day period in which clearance of the system has

not been made, you can apply for reinstatement (A fee is required) during working hours (9:00~18:00). This reinstatement is to reopen the previous application and reactivate your rental rights. We will gradually clear your Digital Data from the 4th day to 11th day, and we will not have your Digital Data at all from the 12th day.

4.10 When you no longer use the hicloud CVPC cloud server, you shall make terminate process and we will not retain any data.

4.11 If you need to retain your Digital Data, you shall transfer it to the template file before you terminate the Service, and export it by using S3 service.

4.12 In order to provide you with a better service, the user operating platform of the Service uses cookies to record user behavior. The record can identify users. For example, it may 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 on this website.

5 Privacy Policy

Thank you for using this Service. As to your personal privacy, we absolutely respect and protect. To help you understand how we collect and process the Customer Information you provide, please read the following carefully.

5.1 Collect, Process and Your Rights

We will collect the following information from you:

5.1.1 Personal information: name, English name, certificate number (ID card number, passport number or uniform number)

5.1.2 Contact information: phone, mobile phone, billing address, email

5.1.3 Network identification codes, such as IP, cookies, etc.

5.1.4 Payment instrument number or credit card information used for payment: credit card number, year and month of expiration date, CVV three digital verification code.

The above Customer Information is kept for the period specified in the law, or for two years after you terminate regarding paper information or fifteen years regarding electronic information.

5.2 The above Customer Information will be used for the following purposes:

5.2.1 Customer service, such as handling abnormal service , processing paper application, knowing performance of service, etc.

5.2.2 Accounting services, such as fee collection, credit card certification, arrears, suspension, settlement, or collection of accounts.

5.2.3 Network address registration, if you use network address (IP), according to the regulations, it is required to enroll the users.

5.2.4 Complying with other laws and orders (such as request by prosecutors, police, investigation bureau, etc.), sharing with entities who have contractual relationship in connection with the service, etc.

5.3 You may, in accordance with the relevant laws and regulations, request to inquire, review, make duplications, supplement or correction, discontinue collection, processing, utilizing, and delete the above-mentioned Customer Information. When exercising the above rights, you shall dial the customer service phone number 0800-080-365.

5.4 The method of providing information, processing deadline, inquiry fee and payment deadline for the exercise of the rights mentioned above are subject to laws and the relevant provisions of the service contract, and we may charge necessary cost and fee. We may decide whether to accept the application based on the necessity for performance of business, legal retention period, etc.

6 Self-Protection Measures:

6.1 Digital Data: According to Article 45 of Chunghwa Telecom's hicloud service lease contract, we have obligation to keep confidential of your data. We will publish statistical data on the website periodically, regarding the number of times requested by the Government, specified in the above-mentioned Article 45, and provided by us.

6.2 Customer Information: We are obligated to keep your Customer Information confidential. Please carefully keep your password or any information. Do not provide any information, especially the password, to anyone. After you use this Service, be sure to log out of your account. If you are sharing a computer with anyone or using a public computer, remember to close the browser to prevent others from reading your data.

7 Storage Location

All customers' Digital Data and Customer Information of this Service are stored in the territory of the Republic of China. We will not move or copy your data outside the country without your consent.

8 Digital Data Encryption

We provide guidance on data encryption, so that you can decide whether your data needs to be encrypted. Please refer to the operating system file and disk encryption SOP file on the official website.

9 Delete Physical Storage Device Data

When our infrastructure storage equipment has malfunction or is being replaced, the data on the equipment will be safely erased or destroyed to ensure that the data cannot be recovered in any way.

10 Information Security Incident Notification

If you find that the Service you are renting has suspicious activities, please notify us according to the Chunghwa Telecom hicloud service rental contract or the link on the website. We will understand and analyze the possible conditions according to the procedure and try our best to reduce the impact on you. You may be asked to provide information and will be notified of the results.

In the preceding paragraph, after we confirm that suspicious activities do exist and will affect our other customers, we will notify by announcement or email.

In accordance with the above Information Security Policy, we will try our best to protect your Digital Data and Customer Information, but if we find that your information has suspicious activities (such as lost, leaked or tampering), and the cause of the problem is attributed to us, we will notify you within 72 hours. The aforementioned notice period does not include a major abnormal service or an uncontrollable natural disaster situation.

11 Supplementary

For matters not covered in the preceding terms, you agree to abide by the relevant laws and regulations, and the relevant provisions of Chunghwa Telecom's hicloud service lease contract.

In the event of any discrepancy between the preceding terms or the Service Contract in the Chinese and English versions, the Chinese version shall prevail.