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。

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)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)。

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，本服務所提供的數據資料，如：虛擬主機等。

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 HNXXXXXXXX、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。

3 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；上述您所負責的內容，如您需要我們的協助，請通知我們，我們會盡力協助您，但部分的協助或許需支付費用。

本文件未經中華電信許可禁止引用或翻印。

4 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 hicloud CaaS 與 CVPC 雲伺服器時，應辦理終止作業，我們不再保留任何資料。

hicloud CaaS 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，第 17 天系統自動終止您的 hicloud CaaS，您得於前述期間內提出申請復裝，但加值服務(如防火牆服務、負載平衡、監控等)仍需重新申請。

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。

5 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。

5.1 蒐集、處理與您的權利

我們會蒐集您的以下資訊：

本文件未經中華電信許可禁止引用或翻印。

5.1.1 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)

5.1.2 聯繫資訊：電話、手機、帳單地址、email

5.1.3 網路識別碼，如 IP、cookie 等。

5.1.4 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。

5.2 客戶資訊因為以下目的會被使用：

5.2.1 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。

5.2.2 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。

5.2.3 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。

5.2.4 其他依法令規定(如個資法等)、與本服務有合作關係者等。

5.3 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、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。

5.4 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。

6 資料自我保護措施：

6.1 數據資料：依據中華電信 hicloud 服務租用契約第四十六條，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，內容為前述四十六條所稱機關要求與我們提供的次數。

6.2 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。

7 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。

8 數據資料加密

本文件未經中華電信許可禁止引用或翻印。

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。

9 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。

10 資訊安全事件處理

10.1 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，請依據中華電信 hicloud 服務租用契約或網站上的連繫方式通知我們；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)。

10.2 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。

10.3 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。

10.4 建議措施：資訊安全事件發生時，建議您使用我們提供的備份或還原功能恢復數據資料，同時洽詢您的資訊安全人員或廠商，如您沒有資安人員，可洽詢本公司業務，為您建議並規劃資安服務。

11 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。

本文件未經中華電信許可禁止引用或翻印。

hicloud CaaS/CVPC Information Security & Privacy Policy

When you use hicloud CaaS/CVPC 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 under the age of 20, 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 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 Data: When you subscribe the Service, the data provided by the Service such as virtual machine.

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).

3 Information Security Roles and Responsibilities:

本文件未經中華電信許可禁止引用或翻印。

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 user operating platform and the physical security of the cloud data center.

The services you subscribe with user portal, such as virtual machine, firewalls, etc., operating system layer updates, vulnerability fixes, other installers/data, or your own data and installed programs. Information security of all mentioned above is your responsibility. As noted above content you are responsible, if you need your assistance. Please tell us. We will try our best to help you, but some may have to be paid.

4 Information security action

4.1 The information security of our services is following 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 The infrastructure of the Service and user portal have anti-virus protection, regular backup, and continue to correct and strengthen weaknesses.

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

4.5 We provide access authentication for you to manage your data, and to back up or restore your data, such as snapshot and restore of virtual machine.

4.6 We provide you with a log record to query your 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.

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

4.8 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.

4.9 When you cancel subscription of the hicloud CaaS and CPVC cloud server, you should terminate the subscription and we will not retain any data.

4.10 As From hicloud CaaS is on the date which telecommunication bill or credit card deduction failure, you couldn’t be able to use hicloud CaaS after 17 recovery, the system automatically terminates your hicloud CaaS on the 17th day, and we will not retain any data. You must apply to recovery within above period, but value-added services (such as

本文件未經中華電信許可禁止引用或翻印。

firewall services, load balancing, monitoring, etc.) still need to rebuild.

4.11 If you need to retain your data, you should transfer it to a template file and return it using the S3 service before you terminate the service.

4.12 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.

5 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.

5.1 Collect, process and your rights

We will collect the following information:

5.1.1 Personal information: name, English name, certificate number (identity certificate 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, 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.

5.2 The above customer information will be used for the following purposes:

5.2.1 Customer service, such as service exception handling, paper application process, user experience, etc.

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

5.2.3 Network address registration, if you have used the Internet address (IP), according to the regulations, you need to log in user information.

5.2.4 Other legal regulations (such as the Personal Information Protection Act, etc.), and partnership.

5.3 According to the relevant regulation of law, you may request the inquiry, read, copy, correction and stop collecting, processing, utilizing and deleting the above-mentioned customer information. When enforcing rights mentioned above, you need to dial the customer service phone number 0800-080-365.

5.4 All mentioned in 5.3 comply with the relevant law and service contract. We will

本文件未經中華電信許可禁止引用或翻印。

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.

6 Data self-protection measures:

6.1 Data: According to Article 46 of Chunghwa Telecom's hicloud service lease contract, we have the obligation to keep your data confidential. We will publish statistical information on the website regularly. The number of times of information we published are stated in the above-mentioned Article 46.

6.2 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. 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 to prevent others from reading your information.

7 Storage location

All customer data and customer information of the Service are stored in the territory of the Republic of China. We will not remove or copy your data outside the country without your consent.

8 Data encryption

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

9 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.

10 Information security incident handling

10.1 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.).

本文件未經中華電信許可禁止引用或翻印。

10.2 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.

10.3 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.

10.4 Recommended measures: When an information security incident occurs, it is recommended that you use the backup or restore function provided by us to recover data, and at the same time contact your information security personnel or manufacturer. If you do not have security personnel, you can contact the company's business for You suggest and plan security services.

11 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.

If any discrepancy between the foregoing articles or the service contract in the Chinese and English versions, the Chinese version should be main priority.

本文件未經中華電信許可禁止引用或翻印。