GWS CLOUD Services Data Security and Privacy Policy

Choosing eASPNet Taiwan Inc. GWS CLOUD Service (hereinafter this Service) as your service provider, means you entrust us with the safe keeping of your data.eASPNet Taiwan Inc. deems the data security and privacy of our clients to be of outmost priority. eASPNet Taiwan Inc. complies with all regulations of relevant laws (for example: Personal Information Protection Act), and offer our services in strict alignment with internal procedures and data security regulations. Comprehensive protection of the security and privacy of your data is our commitment to our clients and the highest standard in which we do business.

25 November 2024 Version

Data Security Policy

This Service can provide our clients with stable and flexible GWS CLOUD Services on demand, as well as VPN connection, client-oriented Cloud Service management interface, data back-up in a different location and other back-up services that allow our clients to achieve continuity of their business operations.

To ensure security of the internet and the cloud, the cloud service center provides 24-7 monitoring services all-year-round, making full effort to minimize the impact due to abnormalities of our services. Moreover, we provide diverse cyber security value-added services, including dedicated Firewalls, IPS, DDoS protection, vulnerability scans, etc., to enhance the security of our clients' data systems. Should any data security issues occur, we can provide relevant log in accordance with operation procedures.

The Role and Responsibility of Data Security

In providing this Service, we are responsible for the infrastructure required, such as the hypervisor, host equipment needed to maintain the virtual environment, internet-related infrastructure, storage equipment, user platform and the security of the cloud data center.

You are responsible for the confirmation of data security when you rent services through the user platform, such as such as virtual hosts, firewalls, updates of operating system, vulnerability reinforcement, other software / data, or your own stored data and installed softwares etc.

Actions for Data Security

1. This Service is provided in accordance with the standards of ISO 27001, ISO 27011, ISO 27017 and ISO 27018, and periodically inspected by unbiased third party.
2. We regularly conduct security checks on the infrastructure of this Service (for example: vulnerability inspection), and continuously enhance and modify any vulnerability or security risks released by the OWASP.
3. Regular back-up and virus protection measures have been implemented for the user platform and the infrastructures of this Service. In addition, we continuously enhance and fix any vulnerabilities.
4. In terms of access management, the network for maintaining and operation is completely quarantined from internet connections and all maintenance and operations must be managed through certified hosts.

5. Our clients enjoy access to manage their own data and the we provide functions such back-up data and data restoration (for example, fast back-up and restorationof the virtual host).
6. Our clients can make inspect data operations of the last 30 days through the log function in the user interface, such as the opening, closing and copying of the virtual host. The retainment period of the log complies with the requirements under the Personal Information Protection Act. Security protection and safe keeping are implemented.
7. We have implemented strict security controls to manage and maintain the cloud data center to ensure the integrity, security and confidentiality of clients' data.
8. The NTP calibration standard for our infrastructure comes from the national standard time, but due to possible Internet transmission delays, and displayed time may differ from the national standard time.
9. When you no longer use this Services, you should notify our staff or contact the customer service center to apply for termination. We will clear all data and back-up files you have stored with us 14 days after receiving your notice to terminate this Service, we will not retain any data that belongs to you. When the system has not started the data deletion, you may apply to re-enact this Service during business hours (9:00~18:00) (relevant fees must be paid). Re-enact means to reapply for this Service and restore the rights and services you have rented.
10. If you need to retain your data, you should transfer your data through the Internet before terminating this Service, or we can assist you in exporting the data to an external storage device you provide. (Only available in VMware standard format)

Information Security Incident Report

Should you find any signs of abnormal activity during terms of this Service, please notify us in accordance with the GWS CLOUD Service Contract or through the contact information on our website. We will investigate and analyze all possible scenarios in accordance with our procedures and try our best to reduce the impact on you. We may request relevant information from you during the process and we will notify you of the results.

Should we confirm that abnormality does exist in accordance with the preceding paragraph, and that it may impact our other clients, notification will be given through announcements or email to each individual client.

In accordance with the aforementioned data security policy, we will try our best to protect your data, should we find that your data has been subject to suspicious activities (such as data loss, leak or tampering) to which we are imputed, we will notify you within 5 working days.The aforementioned notice period does not include material service abnormality or uncontrollable natural disasters.

Privacy Policy

Definition of Client Data

The term “Client Data” as used herein means the data provided and generated by clients during the use of this Service (for example: cloud host image files), not including the “account Information” required to use this Service.The term "Account Information" as used herein means the information related to the managing account which you provide to GWS CLOUD Service. For example: account name, phone number, email address, etc., "Account Information" is subject to " eASPNet Taiwan Inc. consent form for the gathering of clients’ personal information".

Storage Location of Client Data

Clients’ data to this Services will be stored within the territory of the Republic of China, we will not transfer or copy the clients’ data to a location outside of the territory of the Republic of China without acquiring consent from our clients.

Actions Taken for the Security of Client Data Security

Our management platforms are SSL encrypted to ensure the security of clients during data transfers. eASPNet Taiwan Inc. lets you decide whether your data needs to be encrypted.For relevant information on encryption, please refer to the files on operation systems and disk encryption SOP on our official website.

Data Deletion in Storage Equipment

When the storage equipment of our infrastructure malfunctions or needs updating, any data store within these equipment will be deleted and we will make sure that these data cannot be recovered in any way to ensure that our clients’ data are safe from potential data leaks.

Confidentiality of Client Data

According to the provisions of Article 7 of the GWS CLOUD Service Contract, We use the same degree of care that it uses to protect disclosure of its own confidential information of like kind (but not less than reasonable care). Not use any Confidential Information of the other Party (hereinafter referred to as the “Disclosing Party”) for any purpose outside the scope of this Contract.