G-REMOTE Security Sheet

As of：October 16th,2024

Company name: Graphtec

Service name: G-REMOTE

■Operation of Application

No.	Categories	Regulation Items	Details	Contents
1	Availability	Available Time	The time period when the service is provided. (Including a description of planned downtime for inspection/maintenance of equipment, network, etc.)	Except for maintenance period, the service is operated 365days, 24hours.
2		Notification of Planned Downtime	Prior contact to inform of downtime due to regular maintenance. (Including descriptions of timing/method of prior notice)	7 days advance notice by sending e-mail and posting on the website.
3		Advance Notice upon Termination of Service	Prior contact when the service is terminated. (Including descriptions of timing/method of prior notice)	Subject to G-REMOTE Service Terms of Service Article 24 (Discontinuation of Service). *Refer to these Terms of Service.
4		Dealing with Sudden Termination of Service	Whether the program or the configuration data of system environment can be saved or not.	Subject to the provisions of Article 24 (Discontinuation of provision).
5		Operating Ratio of Service	Availability of service (Planned available time of service) - (Downtime) ÷（Planned available time of service)	Over 99% operating ratio.
6		Disaster Recovery	Establishment of a support system / System recovery when a disaster occurs	Establish a data backup center. No regulation about recovery process. Response quickly. (Back up whole system, and check if the system is restored).
7		Alternative Measures for Serious Failure	Alternative measures when quick recovery is not possible.	Establish a data backup center. No regulation about recovery process. Response quickly. (Back up whole system, and check if the system is restored).
8		Service Offerings	Whether to publish the following information -SLA and other information on service operating ratio -Recent operating ratio -Error history (suspension period)	Only error history will be displayed in G-REMOTE notifications.
9	Reliability	Mean Time To Repair (MTTR)	Average time from failure to repair completion. (Total downtime) ÷ (Number of repairs)	Act promptly
10		Recovery Time Objective (RTO)	Target time set for resumption of service provision after a failure.	Act promptly
11		Failure Notification Process	Contact process in case of failure. (To whom, method, routes)	Notified via e-mail or website update (depending on regions).
12		Failure Notification Time	Time to notify the specified contact after detecting an abnormality.	Act promptly
13		Method of Reporting the Service Provision Status and Interval	Time interval and method for reporting service provision status.	No action will be taken if there is no problem.
14	Vulnerability Countermeasures	Implementation of version maintenance	Appropriate version maintenance of OS/middleware (including OSS) and other development components.	Implement the version maintenance.
15		Support	When to respond to detected vulnerabilities and application bugs based on severity. Operational structure for support	Deal as soon as possible A dedicated team will support.

■Support

No.	Categories	Regulation Items	Details	Contents
16	Support	Available Time of Service (Troubleshooting)	Timeframe to receive inquiries about failures.	Subject to our inquiry counter.
17		Available Time of Service (General Inquiry)	Timeframe to receive general inquiries.	Subject to our inquiry counter.

■Data Management

No.	Categories	Regulation Items	Details	Contents
18	Data Management	Backup Method	Method to handle data that belong to users, including backed up contents (counts, method of recovery, etc.), storage, format, users' access privilege, etc.	Daily back up. Data will be stored for 1 week.
19		Data Deletion Requirements	Method of deleting data that belong to users after the service is cancelled, including whether/when to delete, whether/when to dispose the storage, and data transfer.	Data will be deleted 1 year after service cancellation. The evidence of deleting data cannot be supplied.
20		Encryption Requirements for Data Protection	Whether encryption is required or not to protect data.	Not required.
21		Compensation and Insurance if Data is Leaked or Broken	Whether compensation or insurance are provided in case data is leaked or broken.	Subject to Articles 28 (Liability) and 29 (Warranty, Disclaimer).
22		Prevention of Data Leakage	Terms of use that contain provisions to prevent the unauthorized use of information and its leakage to third parties.	Subject to the provisions of Article 13 (Prohibited Matters).
23	Data Handling	Country of data center	The country in which the data center that handles the data is located (country of cloud service provider).	Japan
24		Cloud service provider	Official company name of the cloud service provider (hereinafter referred to as CSP) that actually operates the service.	SAKURA internet Inc.
25		Name of the service	The official service name and the plan edition/subservice name provided by CSP.	SAKURA's VPS

■ Security

No.	Categories	Regulation Items	Details	Contents
26	Security	Encryption Level of Communication	Encryption strength of communications exchanged with the system	HTTPS, FTP, FTPS, MQTTS (TLS1.0/1.1/1.2)
27		Restrictions on information handlers	Limit the number of users who can access the user's data. Carry out restrictions similar to the access restrictions stipulated by the user organisation.	Limitation and restriction will be enforced.
28		Security Patch	Regularly apply security patch. Prompt application of urgent security patch.	Security patch will be applied. *Adjust maintenance schedule for updates that require downtime.
29		Password Standards	Password standards for login.	Password must be: 8 characters, randomly generated from alphanumeric characters.
30		Restricted access to development/operational environment	Access to development/operational environments only from specific environments (e.g., internal or outsourced development).	Access will be restricted.
31		Notification of Security Incident	Methods for notifying users when a security incident occurs	Subject to the provisions of Article 28 (Liability) and 29 (Guarantee, Disclaimer).
32		Confidentiality	Implement physical/logical separation to prevent users from other organizations from accessing our resources.	Will be carried out.
33		Firewall	Install firewalls at the border with the Internet to appropriately close ports that are not needed for service.	Will be carried out.
34		Protocol	Port number and the protocol required to use this service	HTTPS 443 FTPS 21,990(Depends on encryption type) MQTTS 8883