



talkappi

VERY TRAVEL

Security White Paper

Version 2

ActiValues, Inc.

1 Definition of Terms

- In this Security White Paper, "Customer" refers to the contracted company (facility) that has implemented talkappi or VERY (hereinafter referred to as "the System").
- In this Security White Paper, the term "User" refers to an end user who uses the system provided by our company to the Customer.

2 Division of Responsibilities with Users

ActiValues, Inc.'s Responsibilities

ActiValues, Inc. shall implement the following security measures:

- Security measures for the system
- Protection of customer and user data stored in the system
- Security measures for middleware, operating systems, and other infrastructure used to provide the system

Customer Responsibilities

Customers must implement the following security measures:

- Appropriate management of passwords for users accessing the system admin dashboard
- Appropriate management of system admin dashboard accounts (registration, deletion, granting organization administrator privileges, etc.)

3 Data Storage Location

- Customer data is stored in the AWS Tokyo Region.
- To ensure fast and reliable access for users connecting from overseas, we use a Content Delivery Network (CDN) with servers located in North America and China.
- The disposal and reuse of devices containing data are managed in accordance with AWS policies.

4 Data Deletion

- Upon termination of the service agreement, all customer data (*1) will be completely deleted (*2).
Data to be deleted: Content including facility information, personal information related to inquiries and reservations, and admin dashboard users

***1: User activity data, such as chat history, is stored in a non-personally identifiable form and**

used to improve the service.

*2: However, we may retain logs and backups of such data to the extent necessary for system operations, such as troubleshooting or preventing unauthorized use. This applies equally even if the customer deletes the data themselves.

5 Labeling Feature

General

- Customers can add admin dashboard accounts themselves.

[Operation Guide]

- Create or delete accounts
- Configure system notification settings
- Set up various permissions for each account

*For details, please refer to the "Manual & Help" section displayed after logging into the admin dashboard.

Content Editing Feature

- Customers can edit the content data they have created through the admin dashboard.

[Operation Guide]

- Add or edit content data, change categories, modify display settings, etc.
- For details, please refer to the "Manual & Help" section displayed after logging into the admin dashboard.

Admin Dashboard > Manual & Help

6 Account Registration and Deletion

- Within the scope of the agreement, customers can freely register and delete accounts at any time by granting facility system administrator privileges.

[Operation Guide] *Only available for accounts with system administrator privileges

- Register a new account in the system
- Delete an account
- Edit account information

Settings > Account Management

7 Access Control Management

- Customers can freely change the permissions of registered accounts. By assigning system administrator privileges, customers can access the admin dashboards for various functions.

[Operation Guide] *Only available for accounts with system administrator privileges

- Add or remove facility system administrators
Settings > Account Management

8 Password Distribution Method

To send an initial password to a newly created account, check "Send account information to user" on the admin dashboard account creation screen when creating the account.

[Operation Guide]

- Register an admin dashboard account
Settings > Account Management

- Admin dashboard users can reset their own passwords if they forget them.

[Operation Guide]

- Reset the password
Admin Dashboard Top > Forgot Password? Reissue

9 Encryption Status

General

- Various customer and user information stored in the database (such as names, email addresses, and data used across various features) is stored under appropriate access controls without being encrypted. However, passwords are stored in the database in an irreversibly encrypted (hashed) state.
- Internet communications between customer devices and the system are encrypted using TLS 1.3 (SHA256withRSA-RSA 2048 bits).

10 Change Management

- Information regarding various changes, including service updates, can be viewed from "News" on the

admin dashboard.

- Additionally, in the event of service updates, we will notify you through our designated electronic methods, which include admin dashboard announcements and emails sent to the address provided to ActiValues, Inc.

11 Provision of Manuals

- The manuals available for customer use can be viewed via the link below.
 - Manual Location
Admin Dashboard > Manual & Help

12 Backup Status

General

- Various customer and user information stored in the database (such as names, email addresses, and data used across various features) is backed up on a daily basis. Backups are retained for the following periods:
Inquiry response data: During the contract period
Inquiry history data: 3 years
Reception history data: 3 years
- Please note that we do not accommodate customer requests for restoring backup data.
- Content data is distributed across international servers and stored via a CDN service.

13 Log Timestamp Information

- Logs provided within this system are displayed in the JST (UTC+9) time zone.
- Log timestamps are synchronized using AWS NTP services.

14 Vulnerability Management Information

- Our development team periodically collects vulnerability information regarding the operating systems, middleware, and other components used in the system.
- If a vulnerability patch is released for a component used in the system, it will be promptly applied after being tested in a staging environment.

15 Security Information for Development

- The system is developed primarily using PHP and Node.js (JavaScript), following the security guidelines established by IPA.

16 Incident Response

- In the event of a security incident that significantly impacts customers (such as data loss or prolonged system downtime), we aim to notify the organization administrator via email or phone, using the contact details provided at the time of contract, within 72 hours of the incident occurrence.
- For any inquiries concerning information security incidents, please contact our Customer Success team as listed at the end of this Security White Paper.

17 Customer and User Data Protection and Third-Party Disclosure

- ActiValues, Inc. is responsible for protecting the data entrusted to us by our customers. Customer and user data, including log data, is stored with restricted access permissions to prevent unauthorized access or tampering. Access is limited to authorized members of our development team only.
- However, if requested to provide customer data through legally recognized procedures, such as a court order for the production of evidence, ActiValues, Inc. may disclose the minimum necessary customer information to external parties without the customer's consent.

18 Applicable Laws and Regulations

- The agreement between the customer and ActiValues, Inc. shall be interpreted in accordance with the laws of Japan.

19 Certification

- ActiValues, Inc. has obtained ISMS certification under the ISMS Conformity Assessment Scheme

operated by the ISMS Accreditation Center (ISMS-AC).¹

20 Use of Third-Party Cloud Services

- This system uses external cloud services to operate the following functions.

Cloud Service	Function	Operating Company	Information
AWS	Infrastructure construction and operation	Amazon	Personal names, email addresses, PDF files, etc.
TEMAIRAZU	Site Controller	Temairazu, Inc.	Information related to accommodation reservations (personal names, email addresses, addresses, etc.)
TL-Lincoln	Site Controller	Seanuts Co., Ltd.	Information related to accommodation reservations (personal names, email addresses, addresses, etc.)

¹ <https://isms.jp/1st/ind/>

Revision History

Version	Revision Date	Revision Details
1.0	July 14, 2022	Initial release
1.1	October 24, 2022	1. Added definitions of terms and revised related terminology across items Minor wording adjustments
1.2	April 2, 2024	9. Specified TLS 1.3 for encrypted communication under "Encryption Status"
2.0	January 9, 2026	Revised descriptions to reflect expansion of company services, etc.

Inquiries Regarding This Document

ActiValues, Inc.
Customer Success Team
Email: info@activalues.com