Cloud Security White Paper

Version 1.3

InstaVR Inc.

1. Responsibilities of InstaVR and Cloud Service Customers

Responsibilities of InstaVR

As Cloud Service Provider, InstaVR is responsible for:

- defining and ensuring implementation of security measures for cloud services (Including security measures for middleware, OS, and other infrastructure used to provide cloud services)
- securing cloud service customer's data

InstaVR has appointed an Information Security Officer and a Systems Officer to implement the above.

Responsibilities of Cloud Service Customer

Cloud Service Customer is responsible for:

- appropriate management of passwords granted to each cloud service users
- conducting regular access reviews to maintain appropriate management of cloud service accounts (Registration, deletion, granting organization administrator privileges, etc.).

2. Data Storage

- Data received from Cloud Service Customers is stored by default in AWS Region: us-east -1 (Virginia, USA).
- Cloud service customers can submit a request to InstaVR to relocate their data to an AWS region where Amazon Simple Storage Service (Amazon S3) is available.

3. Data Deletion

- Cloud Service Customer can, at the end of a cloud service subscription, request to InstaVR to delete the data. If a Cloud Service Customer submits an application, InstaVR will logically delete all data within one months from the date of application.
- Cloud service customers cannot request InstaVR to delete their backup data. (For more information on storage period, please refer to section 11. Backup Status)
- Cloud service customers cannot request InstaVR to delete the logs. (For more information on storage period, see Section 12. Log Information)

4. Label Feature

- InstaVR provides Cloud Service Customer with the ability to segregate and label information and related assets.
- Cloud Service Customer can, from the list of information assets (User Content) on the information asset management screen of the cloud service, set an arbitrary label for each information asset.

5. Registration and Deletion of Users

- To allow Cloud Service Customers to manage Cloud Service Users access to Cloud Service, InstaVR provides Cloud Service Customer with the ability to register and delete accounts.
- Cloud Service Customers can:
  - register accounts from the “New Account Registration Screen” on the Cloud Service
  - delete accounts by ending subscriptions from the “New Account Management Screen” on the Cloud Service

6. Management of Access to Cloud Service

- InstaVR provides Cloud Service Customer a privileged (Management) account which allows Cloud Service Customers to manage accounts of Cloud Service Users.
- A privileged (Management) account has the ability to invite new cloud service users and purchase or cancel paid features for the organization. Privileged (Management) accounts are tied to email addresses.
- Cloud service Customer can use the email address change feature to grant or revoke privileges by moving a privileged (Management) account to a different email address.
- InstaVR offers two-factor authentication for Cloud Service Customers when accessing privileged (Management) accounts.

7. Password distribution

- InstaVR provides Cloud Service Customer with procedures to manage passwords and keywords (includes procedures for assigning passwords and keywords, and user authentication).
- The contents are as follows:
  - Cloud Service User sets the initial password from the web screen at the beginning.
  - Cloud Service Users can reissue password from the web screen.

8. Encryption Method

- Information on the Cloud Service is protected by Blowfish encryption method. Communication is protected by SSL/TLS encryption using HTTPS protocol.

- InstaVR will not provide another encryption method other than stated above.

9. Change Management

- InstaVR provides information to Cloud Service Customers about changes that may adversely affect Cloud Services. The following information will be provided:
  - Change type
  - Technical explanations of changes to cloud services and underlying systems.
  - Notification of commencement and completion of changes
  - Estimated date and time of change

- InstaVR strictly limits the usage of privileged utility program that bypass normal operating or security procedures. The usage authority of this program is reviewed annually.

- InstaVR provides cloud service customers with information about the latest cloud service changes and their adoption through Change Log, which is updated when changes are made to the cloud service.

10.Procedures

- InstaVR provides on web to Cloud Service Customer on instructions regarding the particularly important procedure - to cancel subscription.

11.Backups

- Data created on the cloud service are backed up daily. The backup method is a full backup. Backups are stored for seven generations, and the backup is stored in AWS US-East1 (Virginia, USA).
- InstaVR doesn't provides Cloud Service Customers with the ability to backup and restore data created on the cloud service. As a general rule, InstaVR does not access to customer data. Therefore, even if Cloud Service Customer requests such, InstaVR will not recover the User data created on the cloud service according to the Cloud Service Customer's request.
- InstaVR will do the restoration work of data created on the cloud service in case of trouble shooting. Before carrying out the restoration work, InstaVR will give notice to Cloud Service Customers of such information.
- Data received from a cloud service customer by means such as file upload is not backed up because it is certain that the original is stored by cloud service customer.

12.Logs

Capture and Protection of Event Log

- InstaVR provides Cloud Service Users with log check feature, only if they have administrator privileges. User generated logs will be stored on cloud service. The information on method of storage is provided to Cloud Service Customer.
- The content which Cloud Service User with administrator privileges can access is past one year's Cloud Service User's access log to the Cloud Service.
- Regarding privileged (Management) account, Cloud Service Customer can access to log on timestamp when used, and records from system side (e.g. CloudTrail, etc.). InstaVR provides Cloud Service Customers on all log information, and InstaVR does not capture any logs that Cloud Service Customer can not access.
- InstaVR is not obligated to respond to any request from Cloud Service Customer to provide additional log content that extends that of which normally provided.

Monitoring Cloud Services

- InstaVR provides Cloud Monitoring Capabilities to Cloud Service Customer.
- InstaVR monitors login log, storage usage and data traffics.

Clock synchronization

- Log times provided within the Cloud Service are synchronized with that of AWS.
- Cloud service customers who want to synchronize logging time with AWS should visit the Amazon Web Services blog for instructions: https://aws.amazon.com/blogs/aws/keeping-time-with-amazon-time-sync-service/

13.Vulnerability management

- The information security measures regarding vulnerability management implemented by InstaVR are as follows:

- Timing of Security Patch deployment: InstaVR regularly obtains vulnerability information from IPA and JPCERT/CC, and check if the security patch needs to be deployed to the cloud service. In case of critical vulnerabilities, InstaVR deploys security patches within 1 month (security patches for other vulnerabilities are deployed if necessary within 3 months).

- Deployment of Anti-Virus Software: InstaVR deploys anti-malware software to employees' PCs to protect from malwares. In case a malware is detected, the devices will be isolated, and anti-malware software vendor will be asked for an investigation. In the event of malware damage,

data will be restored to the state before the damage (Backup and restore procedures are in place and remains restorable).

- Vulnerability Assessment by Third Party: InstaVR conduct vulnerability assessment by a third party once a year.

- Proper separation of servers: InstaVR separate web servers, databases and batch processing systems.

- Monitor on Technical vulnerability: InstaVR regularly checks JSON feed of NATIONAL VULNERABILITY DATABASE, for the purpose to establish internal vulnerability monitoring system (resource monitoring system). Security vulnerabilities that InstaVR identified as significant, which could cause system outages that exceed its updatable SLA and unauthorized access/ information leaks, are implemented as soon as they become patchable in accordance with the monitoring status of technical vulnerabilities in external cloud services such as AWS.

- Network and Server Compliance:
  - When setting up virtual machines, InstaVR took appropriate technical measures (i.e. closed unnecessary ports and limited the protocols and services used)
  - When using virtual machines, appropriate technical means (log acquisition) were taken. LINUX is used for the OS of the virtual machine to prevent malware.
  - InstaVR has changed default values, and deleted or disabled default accounts.
  - InstaVR are implementing measures (Separate web and DB servers) that do not allow a single server to manage functions of different security levels.

- Information security education is provided to new employees when they join the company. Information security education is also provided to all company employees on a regular basis (More than once a year). We prepare test questions for each of them, and we make it a rule to take them until you pass. Internal audits are conducted by a third party with the participation of external consultants. After obtaining certification, we conduct external audits once a year.

14.Management of Information Assets

- InstaVR stores Cloud Service Customer's information assets only in the data center.

15.Security information at programming

- When programming applications, InstaVR engineers follow development standard of the used programming languages.

16.Incident Management

- In case Cloud Service Customer of Cloud Service User discovered a security incident, InstaVR provides a contact form at the corporate website to contact and notification usage.

- InstaVR has defined the scope of security incident report to a Cloud Service Customer as follows:
  - Information Security Incidents to be reported to Cloud Service Customers: 1. Outage beyond SLA, 2. Unauthorized access/information leakage, 3. Significant security vulnerabilities, identified by InstaVR, which potentially cause the above.
  - Information Security Incidents which will not be reported to Cloud Service Customers: Responses to Security Vulnerabilities in AWS, Heroku, and Other External Cloud Services Not Under InstaVR's Control.

- InstaVR sets policy on how incidents and detected and what information is disclosed, to Cloud Service Customer:
  - Outages beyond SLAs - Detected by a third-party notification system, and provide information on downtime and recovery status.
  - Unauthorized Access/Data Loss: Detected by notifications from access logs to the database and information on the affected customer and data ranges will be disclosed.
  - Significant security vulnerabilities identified by InstaVR which could cause above: Detected in on-time review and provided information on planned and response actions.

- InstaVR sets following target time for incident notification:
  - Outages beyond SLAs - Our goal is to detect outages and then notify you as they cross threshold of SLAs. Furthermore, we aim to notify as soon as it is restored.
  - Unauthorized access, information leakage, account hijacking (spoofing), and sending spam email: Once we detect an incident, we aim to notify you as soon as we know the scope of impact.
  - Significant security vulnerabilities identified by InstaVR which could cause above: Target notification within 5 business days after an incident is detected. We also aim to notify you as soon as the response is completed.

- In addition to the above, there are cases where recovery from backup is performed in non-disaster areas due to system outages caused by natural disasters.

17.Third Party Certification

- InstaVR has received ISMS certification under the ISMS Conformity Assessment Scheme, which is operated by the Information Management System Certification Center (ISMS-AC). (https://isms.jp/lst/ind/)
- InstaVR has received ISMS Cloud Security Certification (https://isms.jp/isms-cls/lst/ind/) under the ISMS Conformity Assessment Scheme, which is operated by the Information Management System Certification Center (ISMS-AC).
- InstaVR undergoes an independent audit once a year from a third party outside organization. We also undergo vulnerability diagnosis once a year. When requested by a cloud service customer (including potential cloud service customers), we provide information to the extent possible. (19. Use the form provided for service inquiries)

18.Usage of External Cloud Service

InstaVR uses AWS (Provided by Amazon Web Services), an external cloud service, and Heroku (Provided by Salesforce.com), a peer cloud service.

19.General Inquiry about the Cloud Service

- For general inquiry about the Cloud Service, contact us through the form in our corporate website. (Cloud Service Customer can contact InstaVR's Information Security Administrator and System Administrator using the same form)

20.On Revision of White Paper

- If there is a change in the content of this security white paper, InstaVR will notify the Cloud Service Customer immediately by e-mail or other means.

Revision Record

Version	Date of Rev.	Overview of the revision
1.0	2019/05/15	1st published
1.1	2019/06/13	3.Data Deletion: Added instructions on request regarding backup and log data. 8.Encryption Method: Additional information on handling other than Blowfish encryption 12.Log information: Added information on how to synchronize with AWS clock 14.Management of Information Assets: Added instructions on how to reuse SD cards in exceptional cases. 15.Security information at programming: Added description of development standards 17.Third Party Certification: Additional information on the audit conducted by a third party and the method of request 19.General Inquiry about the Cloud Service: Added instructions on how to contact InstaVR's Information Security Administrator and System Administrator.
1.2	2021/03/22	9. Change Management: Clarified on latest cloud service changes and their adoption. 13. Vulnerability Management Information: Added description on the status of technical vulnerability monitoring and implementation of external audits. 16. Incident Management: Added definition of security vulnerability. 17. Third Party Certification: Added information on the status of certification acquisition. 18. Usage of External Cloud Service: Added peer cloud service Heroku.
1.3	2022/10/07	8. Encryption status - Specified the method of protection for communications 11. Backup Status - Clarified backup status 13. Vulnerability management information - Modifications were made to the deployment of anti-virus software, as well as network and server compliance. 14. Information on the treatment of assets - adjusted according to the actual state of the business