CLOUD CUSTOMER PROCESS MANUAL

Classification	CONFIDENTIAL
Document Version	1.1
ISO 27001:2022 Reference	As Applicable
ISO 27017:2015 Reference	As Applicable
Approved Date	1/11/2024

DOCUMENT PROPERTIES	
Distribution	DataBank Customers
Classification	CONFIDENTIAL
Document Owner	ISMS Manager
Next Scheduled Review	January, 2025
Printed documents are uncontrolled. Refer to secure network location for controlled versions.	

REVISION HISTORY			
Date	**Revision #**	**Description of Changes**	**Revised by**
7/13/2022	0.1	Initial Version	Brian Schlegel
4/6/2023	0.2	Converted to ISMS Standard	Derek Price
4/10/2023	0.3	Formatting changes & content throughout	Derek Price
4/18/2023	1.0	Release Version	Sam Scavera
12/14/2023	1.1	Updated to 27001:2022, Updated Purpose, Updated Section 3	Derek Price
1/11/2024	1.1	Reviewed and Approved by the ISMS Steering Committee	Derek Price

Table of Contents

1 Purpose, Scope, and Users

This DataBank Cloud Customer Process Manual ("Process Manual") provides Customers a description of the Hosting Services provided by DataBank IMX ("DataBank"). Capitalized terms not defined in this Process Manual have the meanings set forth in DataBank's Hosting Agreement.

An electronic copy of the latest Process Manual is available to customers through the DataBank website at https://www.databankimx.com/legal. This Process Manual is reviewed by DataBank as required and any revisions would be posted at the above listed web location.

Users of this document are DataBank cloud customers and other interested parties.

2 System Description

The DataBank Cloud Platform provided by Amazon Web Services (AWS) is a multi-instance hosting platform for products and services offered by DataBank. DataBank employees consult with the Customer in order to deploy, manage, and maintain their software while hosted on the DataBank Cloud Platform.

2.1 Infrastructure

The hardware components associated with the DataBank Cloud Platform are run by AWS data centers. These data centers deploy and manage ongoing security controls such as: Business Continuity & Disaster Recovery, Governance, & Risk, and Monitoring & Logging. More information is provided via this link: https://aws.amazon.com/compliance/data-center/controls/ DataBank does not own, manage, or operate the hosted infrastructure that comprises the DataBank Cloud Platform.

2.2 Software

The DataBank Cloud Platform offers hosting services for products and services owned, resold, or migrated by DataBank.

2.3 System Boundaries

The systems that compose the DataBank Cloud Platform are limited to shared components such as network devices, servers, and software that are physically installed and operating within the Hosting network infrastructure. This system boundary also includes the network connectivity, power, physical security, and environmental services provided by AWS at the data centers in which this network infrastructure is collocated.

DataBank is not responsible for any system components that are not within this system boundary, including network devices, network connectivity, workstations, servers, and software owned and operated by the Customer or other third parties. DataBank may provide support for these components at its reasonable discretion.

3 DataBank Responsibilities

DataBank will:

1. Provide access to the Hosted Solution for use by the Customer by installing and managing system components within the DataBank Cloud Platform system boundaries, as defined within this document. This hosting service will be delivered in a manner that is consistent with *DataBank's Cloud Hosting Agreement*.
2. Manage Hosted Infrastructure configuration changes performed on behalf of Customer based on written requests from authorized Customer employees or authorized third parties.
3. Report and respond to qualified security incidents. If DataBank has determined the Customer's Hosted Solution has been negatively impacted by a security incident, DataBank will deliver a root-cause analysis summary to the Customer's designated point-of-contact. Such notice will not be unreasonably delayed but will only occur after initial corrective actions have been taken to contain the threat and stabilization of the DataBank Cloud Platform has been completed. Assistance from the Customer may be required. DataBank's *Incident Response Plan* will be executed as required.
4. Respond to reported availability incidents. This may include, but is not limited to, activities required to restore access to the Customer's Hosted Solution by conducting a data center failover. If Customer has reported an availability incident to DataBank Technical Support, DataBank will deliver a root-cause analysis summary to the Customer's designated point-of-contact. Such notice will not be unreasonably delayed but will only occur after initial corrective actions have been taken to contain the threat and stabilization of the DataBank Cloud Platform has been completed. Assistance from Customer may be required. DataBank's *Incident Response Plan* will be executed as required.
5. Maintain disaster recovery preparations, including scheduled data and periodic reviews.
6. Use commercially reasonable efforts to test and validate work performed by DataBank employees and vendors within the Customer's Hosted Solution.
7. Use commercially reasonable efforts to monitor the overall security and availability of the DataBank Cloud Platform.

8. Upon request of Customer, provide information on available features and functionality of the DataBank Cloud Platform that could assist Customer in storing confidential or personal identifying information.
9. Store Customer data in the Continental US, at approved AWS data centers, typically US-East-1/2 & US-West-1/2. Applicable jurisdictions have authority.
10. Maintain the following operational policies and procedures:
    a. *Cloud Customer Account Provisioning Procedure*.
    b. *Password Policy* applicable to the Hosted Solution.
    c. *Cloud Encryption Policy*.
    d. *Cloud Backup Policy*.
    e. *Cloud Software Team Technology Charter*
    f. *Cloud Customer Process Manual*
11. Upon request of Customer, provide a logging report with approval from DataBank's Information Security Team
12. Synchronize systems clocks to the AWS time service.
13. Deploy, manage, and maintain Anti-Malware, encryption, and SEIM tools.
14. Subscribe to the AWS Shared Responsibility Model; more information can be found at the following link: https://aws.amazon.com/compliance/shared-responsibility-model/

* All Italicized documents above have been attested to by a 3rd party as part of DataBank's ISO 27001/27017 certification process, available upon request with executed Mutual Non-Disclosure Agreement

3.1 Policies & Procedures

3.1.1 Change Management Procedure

DataBank follows internal change management procedures when changes are initiated by DataBank, when Customer requests DataBank to make a change on their behalf to existing systems, or when new systems are deployed to the DataBank Cloud Platform. Generally, change requests are submitted via a change management system and are then evaluated by subject matter experts. Upon approval by such subject matter experts, changes are implemented, documented, and tested. In the event an issue occurs with the approved change, rollback procedures, documented as part of the change request, are performed in order to return the system to its original state.

Customer is responsible for testing all configuration changes, authentication changes, and upgrades to their Hosted Solution. In cases where the Customer relies upon DataBank to implement changes on its behalf, a written request describing the change must be submitted.

3.1.2 Cloud Encryption Policy

Customer Data may be uploaded via SFTP, TLS/SSL, or through an OnBase services API over a TLS/SSL connection to the DataBank Cloud Platform. DataBank requires all customers to have their data encrypted at rest and by default using an AES 256-bit encryption cipher. Strict access control is in place for Customer Data within the DataBank Cloud Platform. Customer administrators control user access, user permissions, and data retention with respect to the Hosted Solution. In the event Customer elects to modify the use of or turn off the encryption, Customer does so at its own risk. Customer maintains ownership of all Customer Data uploaded to their Hosted Solution through the full lifecycle period.

3.1.3 Customer Account Provisioning Procedure.

As a multi-instance hosting platform, the DataBank Cloud Platform provides logically dedicated storage for each customer, which prevents the documents and metadata belonging to multiple tenants from being comingled. Access to documents, meta-data, output command, configuration commands, and processing commands are controlled via permissions that are assigned to user groups within the Hosted Solution by the Customer. Customers manage the user group membership and authentication records for their users via configuration screens within the applicable web server software or the Hosted Solution configuration application. Multi-factor authentication is required before any DataBank employee is permitted administrative access to the DataBank Cloud Platform. DataBank employee access is provisioned using the least-privilege methodology.

- Employees of Customer are not permitted to share their Hosted Solution login credentials (e.g., passwords, tokens, personal certificates, etc.) with other users.
- Customer must remove all inactive Hosted Solution accounts in a timely manner (e.g., when an employee is terminated).

3.1.4 Incident Response

If Customer administrators believe they have experienced a security incident, they should contact their appropriate Technical Support contact as soon as possible after discovering the incident. The DataBank Technical Support representative will serve as the primary point of contact for the duration of the support issue unless Customer is otherwise advised by DataBank.

DataBank maintains and utilizes a standardized security *Incident Response Plan*. This Plan includes the following high-level event sequence:

a. Incident Trigger Phase
b. Evaluation & Categorization Phase
c. Escalation Phase

d. Response Phase
e. Recovery Phase
f. De-Escalation Phase
g. Post-Incident Review Phase

4 Customer Responsibilities

Customer will:

1. Access the Hosted Solution remotely.
2. Provide web browser software, other compatible client software, and necessary communications equipment to access the Hosted Solution.
3. Provide workstations that meet or exceed DataBank's minimum requirements for each software module installed.
4. Install and manage system components outside of the DataBank Cloud Platform system boundaries, as described in this document.
5. Be responsible for user authorization of access to the environment to Hosted Solution.
6. Control user group membership and the related permissions within the Hosted Solution.
7. Be responsible for user revocation of access to the environment immediately for unauthorized users, and reporting changes to DataBank as soon as possible to prevent inappropriate access and privileges.
8. Designate to DataBank the appropriate point-of-contact who is authorized to communicate Customer's policies, submit Hosted Solution configuration requests to DataBank, or speak authoritatively on behalf of the Customer.
9. Be responsible for all distribution of output under their control within the Hosted Solution or performed by DataBank based on a written request from an authorized employee of Customer. An example would be documents that Customer sends to third parties via e-mail.
10. Identify and make use of Hosted Solution features to properly store confidential information and personal identifying information.
11. Be responsible for ensuring the Hosted Solution meets Customer's legal and/or compliance obligations.
12. Be responsible for all testing of the Hosted Solution upon installation prior to any production use, except as otherwise set forth in a DataBank Statement of Work.
13. Be responsible for all testing of any configuration changes to the Hosted Solution software, except as otherwise set forth in a DataBank Statement of Work.
14. Transfer files to the DataBank Cloud Platform using supported protocols and standards.
15. Use commercially reasonable efforts to monitor business processes and quality controls that are unique to the Customer's Hosted Solution. This

includes batch processing of documents uploaded to the DataBank Cloud Platform.

16. Report and respond to security and availability incidents of which Customer becomes aware. Customer should report all such incidents to DataBank's Technical Support Department. The DataBank Technical Support representative will serve as the primary point of contact for the duration of the support issue unless Customer is advised differently by DataBank.
17. Work collaboratively with DataBank to respond to incidents, including security and availability incidents.