Introduction

Purpose:

The mission of the Information Security Program is to ensure that DataBank Holdings, Ltd. (and subsidiaries or DBA's) information systems, and customer information systems (to the extent services are contracted) are reasonably protected from threats. This is accomplished by implementing a standardized control framework that balances business and customer needs.

The Information Security Program will balance the cost of information security controls and compliance standards with the risks to our business, thus protecting the confidentiality, integrity, and availability of DataBank and customer information systems.

Philosophy of Information Security:

Information security is the combination of processes and controls implemented to protect information or an information asset from various threats identified or unknown. Ensuring that DataBank is able to continue to function in a manner that can maintain customer trust and financial stability is a vital component of this baseline policy and a secure environment.

Information can be defined as data endowed with meaning, purpose, and value. Information and information assets exist in many forms, such as printed or handwritten documentation, verbal communications, and electronically generated documentation, ideas, and words. At DataBank, the value of information or an information asset, or the risk of loss of control of the information or information asset, either perceived or real, drives the security mechanisms that are put in place to protect it. DataBank has defined a Risk Management Framework (RMF) to determine the baseline, minimum set of controls necessary to protect information assets, and function as a business. This minimum set of controls is NIST SP800-53R4.

Information security is characterized as the preservation of confidentiality, integrity, and availability (CIA) of information and information assets.

Confidentiality – Prevents unauthorized disclosure of information or compromise of information assets.

Integrity – Prevents unauthorized modification of information and information assets.

Availability – Prevents disruption of service and productivity of information and information systems assets.

Information security is achieved by implementing a set of controls consisting of policies, standards, and procedures. Once established, the objectives of these controls are to minimize or mitigate risks to an acceptable level and provide protection of information systems that are required by DataBank and customers to meet the operational, financial, and regulatory requirements of the business. Elimination of risk is not practical in today's high risk, high threat environment.

This information security policy manual is designed as the minimum set of security controls necessary to protect the information and information assets held or processed by DataBank. This document defines specific policies within eighteen (18) broader security domains based on the NIST SP800-53 standards. Application and system owners, department managers, decision makers, and customers should consider additional controls for information and information assets that the RMF defines with higher risk.

Scope:

The information security policies and standards outlined in this manual apply to all employees, contractors, consultants, and temporary/contingent workers and other end users, including end-users affiliated with third parties with access to DataBank information systems. The policies and standards apply to all information systems owned by DataBank and all components of the information systems under the accountability and responsibility of DataBank. This includes but is not limited to servers, desktops, laptops, mobile devices, telephone systems, network and network communication systems, storage devices, backup devices and affiliated systems, DataBank administered and developed applications, physical protection assets, and other scenarios applicable. These policies and standards may apply to customer systems as directed by each individual statement.

Out of scope of this policy and standard's manual are customer applications, customer databases, customer administered operating systems, customer-owned and administered hardware and devices, mobile devices, customer-defined and administered policies, standards, and procedures, etc.

All in-scope end users are responsible for complying with the information security policies and are required to acknowledge they have read and understood these policies (see Personnel Security and Awareness and Training policies for specific acknowledgment requirements).

Roles and Responsibilities:

This section provides roles and responsibilities for personnel who have security or related governance responsibility for protecting the information and information systems they operate, manage, and support. The National Institute of Standards and Technology (NIST) information security-related publications will be a primary reference used to develop procedures, standards, guidance, and other directives in support of DataBank policy. DataBank directives will supplement, clarify, and implement NIST and other compliance standards for DataBank systems, operations, and environments.

All roles and responsibilities are assigned and maintained in accordance with Personnel Security policies (13.01).

Accountability and Ownership: The Chief Information Security Officer (CISO) is the accountable owner of this policy and standards document. The CISO is the official responsible for directing the implementation of the enterprise information security program. The Chief Information Security Officer will:

- Make risk determinations and/or provide guidance to business unit heads regarding risk.
- Develop, document, maintain and implement the information security program, which includes in part the policies and standards within this document.
- Ensure enforcement and compliance of information security programs.
- Assist members of the management team and other key officials with the strategic development of the organization securely.
- Establish minimum, mandatory risk-based technical, operational, and management information security control requirements.
- Report compliance failures and policy violations.
- Report security and compliance performance metrics to the leadership team.
- Develop and manage a security awareness and training program.
- Investigate security incidents and coordinate their resolution or mitigation as defined in the Incident Response Policy and Plan.

- Assist business owners in assessing their data for classification and advise them of available policies, standards, controls, procedures, and best practices.
- Implement an information security awareness program.
- Serve as security liaison from DataBank to entities such as law enforcement, auditors, legal services, facility owners, etc.
- Provide consulting services for information security throughout the enterprise, based on the policies and standards established by this document.

Senior Leadership (L1) (includes specific roles of CEO, COO, Sr VP of Managed Services, CTO, and CFO) is responsible for ensuring that the CISO carries out the assigned roles and responsibilities. Additional roles and responsibilities are:

- Ensuring that information security management processes are integrated with the organization's strategic and operational planning.
- Ensuring the Senior Leadership and other key officials provide information security for the information and information systems that support the operations, functions, and assets under their control.
- Delegate to the Chief Information Security Officer the authority, budget, and operational capacity to ensure compliance with this program.
- Assisting the Chief Information Security Officer in ensuring that subordinate Management Staff understands and implements the information security responsibilities within their assigned staff/teams.
- Report any violations of policy, compliance policies or otherwise discrepancies to the Chief Information Security Officer.
- Ensure Human Resources enforcement of information security policies, standards, and procedures.
- Provide resolution regarding risk and policy decisions that the Management Staff, CISO, and others may disagree on.

Management Staff (includes specific roles of Sr. Director of Data Center Operations, VP of Customer Operations, VP of Technical Operations, Sr. VP of Sales, Sr. VP of Marketing, Sr. Director of Development, Director of Support, Sr. Director of Hosting Solutions, VP of Finance and any similar or subsequent role) are responsible for implementing the directed policies, standards, procedures and control objectives as defined by this document and other supplemental knowledgebase articles and similar resources. Additional roles and responsibilities are:

- Implementing and executing the appropriate security procedures and control techniques for systems and operations under assigned control.
- Issue supplemental, department, or system-level guidance for compliance with established policies, standards, and procedures.
- Coordinating and consulting with the CISO when established guidance is unclear, in need of revising or additional guidance is necessary.
- Ensuring all employees, assigned contractors, and other-directed users complete annual security awareness and any assigned role-specific training.
- Ensure that all employees, assigned contractors, and other-directed users take immediate action to comply with risk determinations, incident response, and similar directives from the CISO in order to a) mitigate the impact of a potential security risk or compromise and/or b) respond to a real or perceived threat, security event, or security incident.
- Respond to information security requests for data, audit responses and test cases, and other reporting requirements.

- Complying with all posted Rules of Behavior for sensitive systems (e.g., FedRAMP) and ensuring complete adherence to such by subordinates.
- Ensuring Human Resources enforcement of information security policies, standards, and procedures.
- Reporting any violations of policy, compliance failures, or other discrepancies to the Chief Information Security Officer.

Information Security, Physical Security, and Compliance Staff (includes specific roles of Director of Security or Compliance, Director of Physical Security, Physical Security Architect/Engineer, Security Architect/Engineer, and Compliance Engineer – all levels). Information Security and Compliance staff are responsible for helping the CISO complete security and compliance duties (as described above). Additional roles and responsibilities are:

- Implementing policies, standards, procedures, and control techniques identified within this policy document.
- Coordinating risk assessments for specific enterprise systems.
- Conducting audits and control reviews as directed by the CISO.
- Maintaining the defensive and reporting information security systems such as (but not limited to) the DDoS Protection, IPS, Log Collector, Anti-Virus, WAF and other devices and systems.
- Reporting any violations of policy, compliance failures, or otherwise discrepancies to the Chief Information Security Officer and making recommendations for remediation or corrective actions.
- Coordinating with the information owners, system owners, other Management Staff, and service providers, e.g., cloud services, regarding the Information Security Program requirements for assigned services during their entire lifecycles.
- Coordinating with information owners to decide who has access to the service (and with what types of privileges or access rights) in accordance with the policies of this document and other directives.
- Coordinating with information owners for determining if additional or modified guidance, policies, standards, and procedures are needed beyond those provided in this policy. If additional rules are needed, or modifications required, Security and Compliance staff will coordinate with the CISO and information owners to establish and publish necessary statements.
- Following the Federal Risk and Authorization Management Program (FedRAMP), Health Information Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI-DSS), International Organization for Standardization (ISO), and Sarbanes-Oxley (SOX)requirements where applicable.
- Following other compliance standards as directed by the CISO.
- Coordinating with information owners to ensure systems are properly categorized according to information categorizations for enterprise services.
- Conduct Continuous Monitoring efforts. Ensuring all controls are assessed prior to systems becoming operational, and minimally a subset of controls are assessed annually thereafter for enterprise services.
- Coordinating with information owners to identify controls required to adequately protect information stored, processed, or transmitted by systems for enterprise services.
- Ensuring customers deploy and operate systems according to the security requirements documented in security plans and are clear on their responsibilities for the security of the systems.

- Maintain and continually improve a personal security and compliance skillset.
- Complete annual security awareness and any assigned role specific training.

Employees Designated As Risk Designation High and Medium Responsibilities (Database Administrator, Developer, Technical Account Manager, Support Engineer, Support Supervisor, Accounting Specialist, Windows Engineer (all levels), Linux Systems Engineer (all levels), Backup Administrator, Network Engineer (all levels), Cloud Services Engineer (all levels), Storage Engineer (all levels), Implementations Engineer (all levels), Project Manager, Marketing Manager, Marketing Specialist, Account Manager (all levels), Enterprise Account Executive, Solutions Architect, data center operations technicians (all levels) are responsible for:

- Implementing policies, procedures, and control techniques identified in the information security program.
- Completing role-based information security training and credentialing as defined under the Information Security Program.

Management Commitment:

The DataBank management team is committed to Information Security being a top priority of the organization. Commitment to this function is demonstrated through the assignment of the Chief Information Security Officer (CISO) as an executive, maintaining professionally trained information security staffing, adequate budget allotment, auditing and committed to ensuring a compliant environment not only for DataBank but also its customers.

Coordination among Organizational Entities:

The DataBank CISO is responsible for fostering and maintaining good relationships not only with peers on the management team but also personnel within the organization. The CISO demonstrates coordination with organization entities through various means, including security awareness training, product-specific training, peer-to-peer/1x1 management meetings, and other methods. If your team or function desires the input of the CISO or another security team member, please let us know at Security@DataBank.com

Compliance:

To be effective, information security is a collaborative team effort involving the participation and support from every end-user. All end-users of DataBank information systems are responsible for properly using security controls that DataBank makes available, including technical, administrative, or other appropriate measures for protecting information systems.

All end-users of DataBank information systems must comply with this policy. End-users who are found in violation of policies and standards are subject to disciplinary action up to and including immediate termination of employment, contracts, or other agreements.

Policy Governance Model:

A policy governance model (known as the Carver model) is designed to convey the needs and desires of the governing body, in this case the CISO, and permit the end-user to operate effectively within a secure and compliant environment. Policy governance is designed to define and guide the relationships between the CISO, stakeholders, and end-users. Its purpose is to consistently and accurately communicate to stakeholders and end-users what the CISO needs to accurately and effectively complete his/her task of ensuring security and compliance for the organization while at the same time providing maneuverability for the stakeholders to complete their tasks. It is then expected that the stakeholders will implement the policies on behalf of the CISO. The CISO and his/her team will then work with third-party auditors to trust and verify that the policies have been implemented effectively.

Policy vs. Standards:

Policies are defined as statements, rules, or assertions that specify the correct or expected behavior, setting, or configuration of an entity (person or corporation) or system. The policies in this manual have been approved by management. Policies must be followed to ensure a secure environment and audit compliance.

Standards are defined as guidelines established as a model or example of expected behavior, setting, or configurations of an entity (person or corporation) or system. Standards in this manual have been approved by management. Standards should be followed and adhered to, although small deviations may exist for performance or operational function.

When a deviation from policy or significant deviation from standard exists, these should be reported immediately to the security team for evaluation as a possible exception, alteration of the policy or standard statement, or corrective actions (POA&M). Reporting of policy or standards violation is encouraged.

Monitoring:

All activities pertaining to DataBank information systems are subject to monitoring, logging, and review. In addition to regular internal audits, information systems are subject to monitoring for security policy compliance.

Enforcement:

The CISO is responsible for enforcing compliance with the DataBank information security program, policies, and standards. The CISO works in conjunction with the Dir of HR/Personnel Security Officer in enforcing program aspects that involve personnel security and sanctions.

Exceptions:

DataBank allows for exceptions to the Information Security policies and standards in specific circumstances where mitigating controls are implemented to reduce the associated risk or conditions dictate.

An exception is defined as a deviation from the identified security policy or standard although the policy is not intended to be changed for the organization. Exceptions are granted with the expectation that the requesting party will expeditiously devise and implement a solution that allows for a return to normal security operations.

Exception requests are presented by the manager of the department (System Owner) responsible for the product requesting an exception. Exceptions are granted by the CISO either solely or in conjunction with the Information Security and Privacy Review Board. Open exceptions must be reviewed on an annual basis by the CISO and the requesting entity. Review of Update and Maintenance (Change Control):

Any change to this document must be approved by the Chief Information Security Officer.

Questions:

Questions can be submitted via email to compliance@DataBank.com