GUIDANCE DOCUMENT

This guidance document is advisory in nature but is binding on an agency until amended by such agency. A guidance document does not include internal procedural documents that only affect the internal operations of the agency and does not impose additional requirements or penalties on regulated parties or include confidential information or rules and regulations made in accordance with the Administrative Procedure Act. If you believe that this guidance document imposes additional requirements or penalties on regulated parties, you may request a review of the document.

NEBRASKA FINANCIAL INNOVATION ACT
STATEMENT OF POLICY #6

TECHNOLOGY PROTOCOLS, INFORMATION SECURITY, AND DISTRIBUTED LEDGER ACTIVITY

The Nebraska Department of Banking and Finance ("Department") sets forth Statement of Policy #6 regarding the considerations that a Digital Asset Depository Institution or a Digital Asset Depository Department (collectively referred to as "charters") must consider when establishing controls, policies, and procedures that address their use of technology protocols, information security, and distributed ledger activity. All statutory citations are to the Nebraska Financial Innovation Act (the "Act").

As charters under the Act utilize innovative and increasingly complex technology to carry out their business activities, charters are expected to establish controls, policies, and procedures that address their use of technology protocols, information security, and distributed ledger activity. These controls, policies, and procedures will vary depending upon the business activities of the charter and the products and services that it offers. As a part of the continuous review, monitoring, and examination of charters, the Department will review the relevant controls, policies, and procedures of the charter to ensure that they are adequate to address the uses and the risks of these sophisticated technologies upon which the charter relies.

Transaction Monitoring and Verification

Charters should establish procedures to ensure that all transactions are appropriately and reasonably monitored and subject to verification procedures, to prevent and mitigate fraud, misuse, and suspicious or illegal activity. While not an exhaustive list, the charter's controls, policies, and procedures in this area should include items such as:

- Creating protocols for monitoring and verifying transactions;
- Identifying where transactions are outside of the normal course of business, are suspicious, or are indicative of potentially fraudulent or illegal activity;
- Notifying customers and appropriate regulatory and/or law enforcement agencies, as necessary; and
- Establishing guidelines or protocols for transaction tracing, transaction pausing; claw backs, prohibitions, account suspension, and/or termination of access.

The charter should periodically simulate and test its controls, policies, and procedures to ensure that they are able to implement them practically and operationally, in an efficient and effective manner.

Business Continuity and Loss of Access

As the business activities of a charter will necessarily rely heavily on access to technology and to the Internet, charters should have plans in place to address and mitigate the impacts of a loss to this access. Such plans may be covered under an existing Business Continuity plan or Disaster Recovery Plan, but should be supplemented to cover topics such as data redundancy, technological attacks on the technological infrastructure utilized by the charter, power grid deficiencies or failures, and other relevant issues that would aid in ensuring that a charter could maintain and continue operation to the fullest extent possible, with the least disruption to the end customer, as possible.

Compliance and Reporting

The charter should be prepared to provide the Department with complete and comprehensive records regarding these controls, policies, and procedures. This includes full copies of all such documents, records, and results of internal and external testing or auditing of these controls, policies, or procedures, and documentation of changes, updates, or modifications to them.

Customer Education and Financial Literacy Efforts

Data security and fraud prevention knowledge and awareness are key parts of financial awareness and literacy. Accordingly, as a part of a charter's duties under Neb. Rev. Stat. § 8-3005(6), which requires that a charter meet the digital financial needs of the communities in which it operates and makes efforts to assist with financial literacy, a charter should develop and maintain means by which it educates its customers and the general public, which should include technology related topics such as:

- Data security tools and methods, such as encryption, multi-factor authentication, password and key management, and patch and update implementation;
- Identification of common and emerging trends in fraud and illicit activity within the digital assets space that the charter operates; and
- Relevant updates on the methods by which they may file complaints either directly with the charter or with the Department, or other regulatory agency, as may be appropriate.

Original Issue Date: August 1, 2024