Steuben Area Economic Development Corporation

Cybersecurity and Information Technology Policy

The Steuben Area Economic Development Corporation (Corporation) has developed a comprehensive Cybersecurity and Information Technology Policy to ensure the security, privacy, and effective management of its IT resources. This policy covers various aspects including data protection, incident response, acceptable use, network security, backup and disaster recovery, end-user security awareness training, and governance and compliance. It outlines the Corporation's commitment to safeguarding sensitive information, maintaining operational continuity, and complying with relevant federal and state regulations while emphasizing the importance of proactive measures, regular audits, and employee training to mitigate risks and ensure the integrity and availability of the Corporation's information systems.

Data Protection and Privacy

1. Purpose

To outline how we collect, use, disclose, and safeguard information in compliance with applicable federal and New York State laws. The Corporation is committed to protecting the privacy and security of personal and sensitive information provided by individuals, businesses, and other stakeholders.

2. Information Collected

- **Personal Identification Information:** Name, address, phone number, email address, date of birth, Social Security Number, tax identification number, etc.
- **Business Information:** Business name, industry, financial information, business address, contact information, etc.
- **Financial Information:** Income, business tax filings, and other financial data required for financing or grant applications.
- **Project Information:** Details related to business development projects, development plans, and environmental assessments.
- **Other Sensitive Data:** Any other personal or business data voluntarily provided to us.

3. How Information is Used

To provide services and programs, including financing, grants, tax incentives, and other economic development support, including the assessment of eligibility for various programs and services. In addition, to assess and improve operations and services, communication with clients and other stakeholders, compliance with legal and regulatory requirements and fraud prevention and security.

4. Data Sharing and Disclosure

- **Service Providers:** Third-party vendors assisting with our programs and services, required to protect your information in accordance with applicable laws.
- **Government Agencies:** Federal, state, or local government agencies as part of program requirements, audits, or investigations.
- **Legal Compliance:** Information disclosed if required by law, regulation, or legal process.
- **Business Transfers:** Data may be transferred in the event of a merger, acquisition, or sale of assets.

5. Data Security

The Corporation takes the protection of information seriously and uses reasonable physical, technical, and administrative security measures to safeguard your data from unauthorized access, use, or disclosure. These measures include encryption, secure servers, and access control protocols.

6. Data Retention

Data Retention will follow the established Corporation Record Retention Policy.

7. Client Rights and Choices

- **Access:** Request access to the personal information we hold about you.
- **Correction:** Request corrections to any inaccuracies in your personal information.
- **Deletion:** Request the deletion of your personal information, subject to legal or contractual restrictions.
- **Opt-Out:** Opt-out of receiving promotional or marketing communications.
- **Complaints:** File a complaint with the New York State Department of Financial Services or the appropriate federal Agency.

8. Cookies and Tracking Technologies

The Corporation website may use cookies, web beacons, and other tracking technologies to enhance user experience and analyze site traffic. The use of cookies can be controlled through browser settings.

Acceptable Use

1. Purpose

To establish guidelines for the appropriate use of technological resources, systems, and services provided by the IDA.

2. Scope

Applies to all employees, contractors, vendors, consultants, and any other individuals granted access to the IDA's technological resources including computers, networks, email, internet access, and any other equipment or systems owned, operated, or maintained by the IDA.

3. Prohibited Activities

- **Illegal Activities**: Engaging in any activity that violates federal, state, or local laws.
- **Unlawful Content**: Accessing, distributing, or storing illegal, offensive, defamatory, or sexually explicit materials.
- **Unauthorized Access**: Attempting to gain unauthorized access to systems, accounts, or data.
- **Malicious Activities**: Deliberate creation, introduction, or dissemination of viruses, malware, or other harmful software.
- **Infringement of Intellectual Property**: Using or distributing software, music, videos, or other content in violation of copyright laws.
- **Disruption of Service**: Using systems or networks in a way that causes or may cause disruption to services or resources for others.

5. Confidentiality

All users are expected to respect the confidentiality and privacy of data and information. Sharing or disclosing sensitive information to unauthorized individuals or entities is strictly prohibited.

6. Internet Access, Email, and Communication Systems

Internet access is provided to employees for business-related purposes. Personal internet usage should be kept to a minimum and must not interfere with work responsibilities. Users are prohibited from accessing websites or using Corporation communication systems for the promotion of illegal activities, hate speech, gambling, harassment, solicitation, or any form of abusive communication.

Network Security and Monitoring

1. Purpose

To outline security measures and monitoring practices to safeguard the Corporation's network infrastructure. The policy aims to protect critical data, including personally identifiable information (PII), financial records, and intellectual property, from unauthorized access, cyber threats, and data breaches.

2. Network Access Control

Network access will be granted only to authorized personnel. The following guidelines apply:

- **Authentication**: Multi-factor authentication (MFA) must be enabled for accessing sensitive systems or data.
- **Authorization**: Access permissions will be granted based on the principle of least privilege.
- **Role-Based Access Control**: Employees and contractors will have access only to the resources necessary for their roles.
- **Users** must take all reasonable precautions to secure devices and accounts, including using strong passwords and updating them regularly.
- **Sharing** login credentials, leaving devices unattended while logged in, or allowing others to use a personal account is prohibited.

3. Security Monitoring

The corporation will deploy and maintain security monitoring tools to detect and respond to threats.

4. Data Protection and Encryption

Sensitive data must be encrypted both at rest and in transit using industry-standard protocols. Regular encrypted backups of critical data are also required.

Incident Response, Backup, and Disaster Recovery

1. Purpose

To establish guidelines and procedures for identifying, responding to, and managing security incidents and to ensure that the Corporation can recover its critical business functions and sensitive data in the event of an unexpected incident, disaster, or failure.

2. Incident Detection and Reporting

Employees and contractors report suspected incidents immediately; reports include description, date/time, affected systems, and actions taken. Reports should include a description of the incident, the date and time of occurrence, any affected systems, and any actions taken to mitigate the incident.

3. Backup Procedures

- **Backup Storage and Frequency:** Per Microsoft 365 protocols**.**
- **Backup Security:** All backup data will be encrypted using industry-standard encryption protocols. Access to backup data will be restricted to authorized personnel only.

4. Disaster Recovery Procedures

- **Incident Response and Recovery Activation**. In the event of a disaster, an Incident Response Team (IRT) will be formed and assigned roles, including recovery of systems, communication, and coordination with external stakeholders.
- **Data Restoration Process**. The disaster recovery team will restore data from backups starting with the most critical systems, ensuring the restoration of key services first. Restoration of full systems will be carried out from cloud-based backups if on-site infrastructure is unavailable.
- **Alternate Site/Failover Solutions**. A secondary disaster recovery site will be maintained (either in the cloud or at a physical location) to support business continuity operations in case the primary site is unavailable. Cloud-based systems should have failover mechanisms to ensure minimal downtime.

End User Security Awareness Training

1. Purpose

To ensure that all employees, contractors, and relevant stakeholders within the Corporation understand their roles and responsibilities in protecting the organization's information systems and data.

2. Training Objectives and Content. Overview of Cybersecurity, Social Engineering and Phishing Awareness, Strong Password Practices, Safe Use of Devices and Networks, Data Protection and Incident

Response and/or other information technology related information that is in compliance with the NYS SHIELD Act (Stop Hacks and Improve Electronic Data Security Act) of 2019.

Governance and Compliance

1. Purpose

To ensure confidentiality, integrity, and availability of the Corporation's information systems and data. This policy sets forth the standards for compliance with applicable cybersecurity and IT regulations and mandates the regular audit of IT systems to identify and address risks. The policy aligns with federal and state laws, including New York State's cybersecurity requirements (23 NYCRR 500), as well as industry standards and best practices.

2. Scope

This policy applies to all employees, contractors, vendors, systems, networks, applications, and data owned or operated by the IDA, including but not limited to financial systems and records, project data, employee records, contractor and vendor data, any other data critical to the daily operations of the IDA. The policy covers incidents involving cyber threats, physical security breaches, data breaches, system outages, and other security-related events.

3. Regulatory and Cybersecurity Compliance Requirements

The Corporation will adopt an IT security governance framework that includes policies, procedures, standards, and risk management practices based on NIST, ISO, or other industry standards.

- **New York State Cybersecurity Regulations (23 NYCRR 500):** Compliance with the NYDFS regulations for financial institutions and related entities in New York, ensuring the protection of nonpublic information.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework:** Adopting best practices from NIST to protect the confidentiality, integrity, and availability of critical infrastructure.
- **Federal Information Security Modernization Act (FISMA):** If applicable, adherence to FISMA and related Federal Information Processing Standards (FIPS).
- **General Data Protection Regulation (GDPR):** For handling any personal data from EU residents, ensuring compliance with data protection requirements.

4. Policy Review and Update

This policy will be reviewed at least annually, or more frequently if necessary due to changes in laws, regulations, or the organization's IT infrastructure. Updates will be made to address evolving cybersecurity threats, compliance requirements, or operational changes.

5. Security Audits and Assessments

The Corporation will perform regular internal and external security audits to evaluate the effectiveness of the network, cybersecurity, and information technology infrastructure.

6. Enforcement and Monitoring

The Corporation reserves the right to monitor the use of its technological resources to ensure compliance with this policy. Any violation of this policy may result in disciplinary action, up to and including termination of employment or contractual relationships, as well as legal action if warranted. The Corporation also reserves the right to temporarily suspend access to its systems or services during investigations of potential violations.

5. Exceptions

Approved by the Executive Director and documented with justification.