Sand Beach Conservancy District Cybersecurity Policy 2025

1. Purpose

This policy establishes the cybersecurity framework for the Conservancy District's website and related online systems. Its goal is to protect District information, digital assets, and public services from unauthorized access, misuse, or disruption.

2. Scope

This policy applies to:
- All District-owned or managed websites, servers, and web applications.
- Employees, contractors, vendors, and volunteers with access to District web systems.
- All data collected, processed, or stored through the District's web platform.

3. Objectives

- Safeguard sensitive and personal data.
- Ensure the integrity and availability of public information.
- Maintain public trust through responsible management of digital assets.
- Comply with applicable federal, state, and local cybersecurity regulations.

4. Website Security Controls

4.1 Secure Design & Maintenance
- The District website shall be hosted on a secure, monitored server using current, vendor-supported operating systems.
- Regular updates and patches must be applied to web servers, CMS platforms, and plugins.
- HTTPS with valid SSL/TLS certificates is required for all web traffic.

4.2 Access Management
- User access to web administration functions must be limited to Board managers.
- Multi-Factor Authentication (MFA) must be enabled for administrative accounts.
- Role-based permissions will be implemented to restrict access according to job responsibilities.
- Access to data will be terminated immediately of exiting Board members.

4.3 Data Protection
- Personal or confidential information collected through the website must be encrypted during transmission and storage.
- Only data necessary for District operations shall be collected.
- Public records shall be handled in compliance with applicable data retention and disclosure laws.

4.4 Monitoring & Incident Response
- Website activity logs will be maintained and reviewed for signs of unauthorized access or suspicious activity.
- Any cybersecurity incidents shall be reported immediately to the IT Administrator or District Managers within 72 hours using the Cybersecurity Reporting Form pursuant to ORC

9.64 (https://ohioauditor.gov//fraud/docs/CybersecurityReportingForm.pdf) and submit to Cyber@ohioauditor.gov.

.

- The District will follow a documented Incident Response Plan, including containment, investigation, and public communication as needed.

4.5 Backups & Continuity

- Regular backups of website data and configurations must be performed and stored securely offsite.
- Backup and recovery procedures will be tested periodically to ensure rapid restoration in case of compromise.

5. Vendor & Third-Party Management

- Third-party web service providers must meet the District's cybersecurity requirements.
- Contracts with vendors shall include provisions for data security, incident reporting, and confidentiality.

6. Training & Awareness

- District staff involved in website operations shall receive online cybersecurity awareness training annually through State and Federal Agencies. https://www.cisa.gov/cybersecurity-training-exercises
- Periodic phishing simulations or tabletop exercises may be conducted to test response readiness.

7. Policy Review

This policy shall be reviewed at least annually or following any major technology change, security incident, or regulatory update.

8. Enforcement

Violations of this policy may result in disciplinary action, termination of access, or other measures as deemed appropriate by District management and applicable law.