Hancock & Associates, Inc.

Cybersecurity Policy

Introduction

Hancock & Associates, Inc., located at 7237 Oak Ridge Hwy, Knoxville, TN 37931, is committed to safeguarding the confidentiality, integrity, and availability of its information systems and data. This Cybersecurity Policy is designed to comply with the New York Department of Financial Services (NYDFS) cybersecurity requirements as outlined in 23 NYCRR Part 500.

Scope

This policy applies to all employees, contractors, vendors, and other personnel who have access to Hancock & Associates, Inc.'s information systems and data.

Policy

1. Cybersecurity Program

Hancock & Associates, Inc. shall establish and maintain a comprehensive cybersecurity program designed to protect the confidentiality, integrity, and availability of its information systems and data. The program shall be based on a risk assessment and shall be updated regularly.

2. Cybersecurity Policies and Procedures

We shall implement and maintain written policies and procedures that are approved by senior management and are designed to protect our information systems and data from unauthorized access, use, or other malicious acts.

3. Access Controls

Access to information systems and data shall be limited to authorized users. Multi-factor authentication (MFA) shall be required for access to systems containing nonpublic information.

4. Data Governance and Classification

Data shall be classified based on its sensitivity and importance. Appropriate security measures shall be implemented to protect each class of data.

5. Asset Management

An inventory of all information assets shall be maintained and reviewed regularly. Security controls appropriate to the classification of the asset shall be implemented.

6. Risk Assessment

A periodic risk assessment shall be conducted to identify and assess risks to the security of our information systems and data. The results of the risk assessment shall be used to adjust the cybersecurity program as necessary.

7. Cybersecurity Personnel

Qualified personnel shall be designated to manage and oversee the cybersecurity program. Ongoing training and education shall be provided to ensure that all personnel are aware of cybersecurity risks and best practices.

8. Third-Party Service Provider Security

Third-party service providers with access to our information systems and data shall be required to implement appropriate cybersecurity measures. Contracts with these providers shall include cybersecurity requirements.

9. Incident Response Plan

An incident response plan shall be maintained to respond to and recover from cybersecurity events. The plan shall include procedures for identifying, reporting, and responding to incidents.

10. Penetration Testing and Vulnerability Assessments

Regular penetration testing and vulnerability assessments shall be conducted to identify and address weaknesses in our information systems.

11. Audit Trail

An audit trail system shall be implemented to detect and respond to cybersecurity events. Audit logs shall be maintained and reviewed regularly.

12. Encryption

Sensitive data shall be encrypted both in transit and at rest. Strong encryption methods shall be used to protect data from unauthorized access.

13. Application Security

Security measures shall be incorporated into the development lifecycle of applications to ensure that they are secure against vulnerabilities.

14. Training and Monitoring

Regular cybersecurity training shall be provided to all personnel. Monitoring systems shall be implemented to detect unauthorized access and other malicious activities.

15. Data Retention

Data retention policies shall be implemented to ensure that data is retained only for as long as necessary for business purposes and legal compliance. Secure disposal methods shall be used for data that is no longer needed.

16. Cybersecurity Awareness

Ongoing efforts shall be made to raise cybersecurity awareness among all personnel through training, communications, and simulated phishing exercises.

Compliance and Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. Regular audits shall be conducted to ensure compliance with this policy and applicable laws and regulations.

Review and Updates

This policy shall be reviewed and updated at least annually or whenever there are significant changes to our information systems, data, or regulatory requirements.

Approval

This Cybersecurity Policy has been reviewed and approved by senior management of Hancock & Associates, Inc.

Date of Last Review: 12/01/2025

Approved by:

_____

Joshua Hancock, Program Manager

_____

Sandy, Williams, Cyber Compliance Officer

For questions or further information regarding this policy, please contact the Cybersecurity Program Manager at 865-691-6449 Ext. 108.