Access Control Policy v1.0

Harbor Wealth Management
Shivpuri, Bilasi Town, B. Deoghar, Jharkhand

16/04/24

Table of Content

1. Introduction

Harbor Wealth Management, a premier boutique investment firm, prioritizes client confidentiality and regulatory compliance. Our comprehensive security policies ensure robust protection of sensitive financial data, reflecting our unwavering commitment to excellence in wealth management services.

2. History

Version	Description	From	To	Author
1.0	Initial Version	**16/04/2024**	Current	Abhinav Deep

3. Access Control Policy

a. Introduction/ Policy Statement

At Harbor Wealth Management, we are dedicated to safeguarding the confidentiality, integrity, and availability of our clients' financial information. This Access Control Policy outlines our commitment to controlling access to digital and physical assets, ensuring compliance with regulatory requirements, and mitigating the risk of unauthorized access and data breaches. Through the implementation of rigorous access control measures, we strive to maintain the trust and confidence of our clients, stakeholders, and regulatory authorities, while upholding the highest standards of security and integrity in wealth management services.

b. Definition and Terms

c. Purpose

The purpose of the Access Control Policy for Harbor Wealth Management is to establish clear guidelines and procedures for controlling access to digital and physical assets, ensuring the confidentiality, integrity, and availability of sensitive information. By formalizing access control mechanisms, the policy shall mitigate the risk of unauthorized access, data breaches, and regulatory non-compliance. The policy shall protect client confidentiality, maintain the trust and confidence of stakeholders, and safeguard the company's reputation and financial interests. Through the implementation of access controls aligned with industry best practices and regulatory requirements, the policy shall enhance cybersecurity resilience, minimize security risks, and support the company's commitment to excellence in wealth management services.

d. Scope

- Covered Assets:
  The policy applies to all digital assets, including but not limited to client financial records, investment portfolios, transaction data, personally identifiable information (PII) of clients and employees, physical assets such as servers, computers, and storage devices etc...
- Applicability:
  The policy applies to all employees, contractors, vendors, and any other individuals who have access to Harbor Wealth Management's assets, systems, or facilities. It encompasses all locations where company assets are stored or accessed, including office premises, data centers, and remote work environments.

e. Policy

1. Access Control Mechanisms:

- Define authentication methods (e.g., passwords, biometrics) and authorization controls (e.g., role-based access control) for accessing digital assets.
- Specify procedures for granting, modifying, and revoking access privileges based on employees' roles and responsibilities.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Safeguards Rule (§ 314.4), which requires financial institutions to implement access controls to protect customer information.

- **NIST CSF Guideline:** Protect Function, Access Control category (PR.AC), which emphasizes the implementation of controls to ensure that only authorized users have access to systems and data.

2. User Authentication:

- Establish requirements for strong and secure user authentication, including the use of complex passwords, multi-factor authentication (MFA), and periodic password changes.
- Outline procedures for managing user accounts, including account creation, deactivation, and password reset processes.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Financial Privacy Rule (§ 313.3), which mandates the protection of customer information through secure authentication methods.
- **NIST CSF Guideline:** Protect Function, Identity Management and Access Control category (PR.AC), which includes guidelines for establishing user authentication mechanisms.

3. Access Review and Monitoring:

- Detailed procedures for regularly reviewing access privileges to ensure alignment with employees' roles and responsibilities.
- Specify mechanisms for monitoring user activity, logging access events, and detecting unauthorized access attempts.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Safeguards Rule (§ 314.4), which requires financial institutions to regularly monitor access to customer information.
- **NIST CSF Guideline:** Detect Function, Anomalies and Events category (DE.AE), which emphasizes the importance of monitoring user activity and access events for detecting unauthorized access attempts.

4. Remote Access Control:

Define policies and controls for securely accessing company resources from remote locations, including the use of virtual private networks (VPNs) and secure remote desktop protocols.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Safeguards Rule (§ 314.4), which requires financial institutions to implement controls for remote access to customer information.
- **NIST CSF Guideline:** Protect Function, Remote Access Management category (PR.AC), which provides guidance on securely managing remote access to organizational systems and data.

5. Physical Access Control:

- Establish measures for controlling physical access to office premises, data centers, and other facilities, including the use of access cards, biometric authentication, and surveillance systems.
- Specify procedures for granting temporary access to visitors and contractors.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Safeguards Rule (§ 314.4), which requires financial institutions to control physical access to customer information.
- **NIST CSF Guideline:** Protect Function, Physical Access Controls category (PR.PT), which outlines controls for controlling physical access to facilities and assets.

6. Data Access Controls:

- Define procedures for classifying data based on sensitivity and implementing access controls accordingly.
- Specify encryption requirements for protecting sensitive data both at rest and in transit.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Safeguards Rule (§ 314.4), which requires financial institutions to implement controls for access to customer information.
- **NIST CSF Guideline:** Protect Function, Data Security category (PR.DS), which provides guidance on implementing access controls to protect sensitive data.

7. Privileged Access Management (PAM):

- Outline policies and controls for managing privileged accounts and access to critical systems and data.
- Define procedures for monitoring and auditing privileged access to mitigate the risk of insider threats and unauthorized access.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Safeguards Rule (§ 314.4), which requires financial institutions to manage privileged access to customer information.
- **NIST CSF Guideline:** Protect Function, Identity Management and Access Control category (PR.AC), which includes guidelines for managing privileged access to organizational systems.

8. Third-Party Access Control:

- Specify requirements and controls for managing access by third-party vendors, contractors, and service providers.
- Establish contractual agreements and oversight mechanisms to ensure compliance with security policies and standards.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Financial Privacy Rule (§ 313.6), which requires financial institutions to implement controls for sharing customer information with third parties.

- **NIST CSF Guideline:** Protect Function, External Parties category (PR.IP), which provides guidance on managing access by external parties to organizational systems and data.

9. Training and Awareness:

- Emphasize the importance of employee training and awareness programs to ensure understanding and compliance with access control policies and procedures.
- Provide guidance on recognizing and reporting suspicious activities and security incidents.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Safeguards Rule (§ 314.4), which requires financial institutions to provide training to employees on safeguarding customer information.
- **NIST CSF Guideline:** Identify Function, Awareness and Training category (ID.AT), which emphasizes the importance of providing cybersecurity awareness and training to employees.

10. Compliance and Enforcement:

- Ensure alignment with relevant regulatory requirements, such as the Gramm-Leach-Bliley Act (GLBA), SEC regulations, and industry standards.
- Specify consequences for non-compliance with access control policies, including disciplinary actions and legal measures.

Supporting standard's clauses and guidelines:

- **GLBA Clause:** Financial Privacy Rule (§ 313.5), which requires financial institutions to establish procedures for ensuring compliance with privacy policies.
- **NIST CSF Guideline:** Respond Function, Recovery Planning category (RS.RP), which includes guidelines for establishing procedures for compliance with cybersecurity policies and standards.

f. Exception

- In few instances, company's systems may require to be exempted from the Access Management Processes due to possible technical difficulties or third-party contractual obligations.
- Any such exceptions to the current policy must be documented and approved via the Harbor Wealth Management's Exceptions Management Process.

g. Roles and Responsibilities

Roles	Responsibilities
Access Control Administrator	Responsible for managing user accounts and access privileges in accordance with the Access Control Policy.

Security Analyst	Conducts regular risk assessments and vulnerability scans to identify potential security risks and gaps in access controls.
Compliance Officer	Ensures that access control practices and procedures adhere to regulatory requirements, including the Gramm-Leach-Bliley Act (GLBA) and other relevant standards.
Training and Awareness Coordinator	Develops and delivers training programs to educate employees on access control policies, procedures, and best practices.
Incident Response Team Member	Participates in incident response activities related to access control incidents, such as unauthorized access attempts or data breaches.
Physical Security Officer	Oversees physical access control measures, such as access cards, biometric authentication, and surveillance systems.

Sponsor Acceptance

Approved by the Sponsor Date ----------

_____