Information Security Program

AssetMark is dedicated to the security and integrity of the data we manage in order to provide services to our financial advisors, clients and vendors. Vulnerable or compromised technology assets could result in business disruption, financial loss, reputational loss and regulatory or legal penalties. This document describes the security controls in place, including physical, application, system, and operational security. The key features of the Information Security Program are:

- Governance and risk
- Training and awareness
- Vendor management
- Security architecture
- Security operations
- Testing
- Incident response

GOVERNANCE AND RISK

AssetMark has multiple committees working to provide oversight and executive support for security related risks, including fraud. Committees meet regularly and provide support for a companywide security risk management program. High-level decisions regarding data privacy, governance, and compliance are made by the committees.

Information Security Policy

The Information Security Policy is reviewed and updated at least annually. The key features of the policy are:

- System access
- Configuration management
- Personal user identification and accountability
- IT governance
- Physical security
- Remote access
- Wireless connections
- Exchanges of information
- Intranet and internet
- Information security awareness
- Email
- Mobile
- Operations security
- Policy exceptions
- Enforcement

IT Governance

The IT Governance Program monitors policy compliance.

Information Security Incident Response

AssetMark maintains an incident response plan for responding to a security incident. The plan is updated annually, or as needed throughout the year. All security incidents and threats are reported to IT and documented and tracked in AssetMark's internal tracking system. All security and fraud incidents are reported to Compliance.

Business Continuity Planning

To ensure the continuity of critical services to our clients and plan for the protection of our employees, company assets and information, AssetMark's Business Continuity Management Plan utilizes a holistic approach, integrating traditional IT system recovery processes (Disaster Recovery Plan) and employee safety and disaster preparedness, crisis management planning and business continuity planning. The key features of the Business Continuity Plans are:

- Crisis management escalation and communication processes utilizing mass notification tools
- Identification and prioritization of mission critical business processes constructed from a business impact analysis that includes:
  - Owners for each process
  - Recovery time objectives of critical technology associated with these processes
  - Resources required to perform mission critical functions during an event
- Annual testing and ongoing updates to plans to ensure an accurate representation of business recoverability needs
- Continuity planning for critical business functions in short-term (less than one week) and long-term (greater than one week) scenarios:
  - Short-term continuity plans call for remote office functionality for mission critical groups, including the call center, trading team and account operations.
  - Long-term incident scenarios call for mission critical groups to relocate to alternate work locations, which are geographically dispersed AssetMark locations.
  - Many of our mission-critical groups have implemented cross training for critical processes among similar departments in alternate AssetMark locations to assist in the continuity of those business functions when one location is impacted. Additionally, our call center has team members located in multiple locations.
- Recovery strategies for mission critical processes consider loss of technology, loss of facility and loss of workforce.
- Employee Safety Program covering all AssetMark locations with certain employees designated as Safety Leaders and Safety Captains at each location.
  - Safety Leaders and Floor Wardens are responsible for assisting in emergency evacuations and play a critical role in the communication structure during a crisis event
  - Testing conducted under the Safety Program includes an annual fire drill, annual earthquake drill for California locations and tests of the mass notification tool
  - Safety Leaders and Floor Wardens attend periodic training on the Safety Program and can attend CPR and AED training every two years

Disaster Recovery Planning

AssetMark has instituted disaster prevention measures to limit the likelihood of a computing outage.

Production systems reside in a Tier 3 data center with physical and infrastructural measures in place. Network computer hardware and software is safeguarded to prevent unauthorized physical access, use or theft, as well as to minimize potential damage from disasters. Various security measures are in place to limit physical access to valuable computer equipment, software and information located on computer systems.

Security systems are designed and implemented to prevent unauthorized access to information stored on the company's computer network. Restrictions imposed by security measures minimize the risk of accidental or malicious deleting of data or access to sensitive, confidential information.

Production server data is backed up in real-time through data mirroring technologies to disaster recovery servers located at an alternate disaster recovery location. That same alternate location contains stand-by applications and database servers ready to take the production load should the Disaster Recovery Plan be invoked. These servers are kept up to date with current application software as a standard course of business.

Quarterly Risk Assessment

A quarterly security risk assessment is conducted to ensure we are actively reviewing our security posture and constantly making improvements.

TRAINING AND AWARENESS

Annual Employee Training

AssetMark employees are required to complete information and data security training annually to ensure they are aware of the most common security threats and how to detect them. This includes tips such as social engineering tactics, and how to identify email phishing attacks and safely handle sensitive data. Additionally, certain employees, based upon their job functions or roles within the firm, are required to take client Security and Fraud Awareness Training.

The training covers:

- Employee responsibility to report security incidents
- Definition of a security incident
- Security "incident" vs. "breach"
- Definition of a fraud incident
- Security and Fraud Incident Report; first response and how to report an incident

VENDOR MANAGEMENT

Vendor Risk Assessments

Vendor risk assessments are conducted in coordination with Legal, Risk, and IT. Vendors who will have access to, or will process AssetMark proprietary data or PII are further vetted by the Information Security Committee. Additionally, risk assessments are completed on an annual basis for all significant vendors.

Network Access Rights & Controls

Vendors may require network access to provide services to AssetMark. The identified individuals are only granted access rights to the necessary systems/programs using the least privileged model. Access rights are discontinued immediately upon termination and are audited quarterly.

SECURITY ARCHITECTURE

Physical Security

AssetMark has implemented badge access and security cameras for all offices and data centers. AssetMark systems reside in Tier 3 cloud computing platforms and third party-managed data centers outside of California. Background checks are completed on all employees and contractors and non-disclosure agreements are in place with certain vendors. Physical security controls include:

- Access that is limited to data center technicians and periodically granted to AssetMark employees and vendors on an as-needed basis
- Security camera monitoring
- Fire suppression system

Software Architecture

AssetMark's eWealthManager platform is hosted in Microsoft Azure that complies with the SOC 1 and SOC 2 Type 2 standards. They are audited annually to ensure they remain in compliance with pre-defined control criteria relating to security, availability, processing integrity, confidentiality, and privacy of a system and its information. A 3-tier architecture is used for eWealthManager for added security by separating the presentation layer, functional process logic and back-end databases using next-generation firewalls. Security controls are in place to limit access to production systems to authorized users only.

Firewalls

AssetMark employs next-generation firewalls to protect data and assets utilizing a combination of access control lists and intrusion prevention systems on the network perimeter to inspect all inbound traffic to our datacenter and block malicious traffic. All traffic is logged and sent to a third party-managed security services provider for analysis. The firewalls are configured for high availability and pass traffic to redundant load balancers for maximum uptime.

Secure Data Transfers

Third-party partner integrations utilize secure protocols and mechanisms such as SSL, SFTP, and PGP encryption to ensure data is secured in transport and at rest.

Web Filtering

AssetMark employs web filtering via next-generation firewalls to block access to malicious websites. The filter also examines web-based traffic for potential spyware, Trojans and viruses that may be trying to connect to the Internet.

Mobile Device Management

Mobile Device Management (MDM) is installed for all mobile access to AssetMark email. Policy requires a corporate device to access AssetMark data. If an exception is approved, the personal device is not granted access to email unless MDM is maintained on the device. Mobile device authentication is enforced, and data will be automatically wiped after a fixed number of invalid attempts.

Shared Password Management

In some instances, shared passwords for administrative accounts are necessary. Only those authorized by their role have access to shared passwords. Shared passwords are changed upon an administrator's termination. Quarterly checks are performed to ensure proper password management. All shared passwords are stored in an encrypted password management system with auditing capabilities.

Email Protection

AssetMark supports TLS for all email transmissions and emails are protected against SPAM, viruses and malware. An Advanced Threat Protection service (ATP) is also deployed to safeguard against phishing attempts and malicious URLs and attachments. Any URLs or attachments that are categorized as unsafe are blocked from being delivered to the recipient.

All inbound/outbound emails are archived by a third party and stored in a read-only state. Emails that contain sensitive PII information are flagged by the system and forwarded to the Compliance department for review.

Anti-Virus and Anti-Malware

Enterprise class antivirus and anti-malware software has been implemented across all client and server computing systems which are monitored by a third-party security provider. The end users are prohibited from disabling or uninstalling these products. Additional safeguards have been implemented to ensure the security products cannot be uninstalled even if the user has gained elevated administrative access to the machine.

Geo IP Blocking (Offices and Data Center Inbound) and International GEO IP Reporting

AssetMark blocks international network traffic from accessing our office networks. Additionally, VPN access is restricted to only US states as well as authorized international vendors. Reports are generated on international IPs connecting to eWealthManager and reviewed for suspicious activity.

Multi-Factor Authentication (MFA)

AssetMark has implemented multi-factor authentication for all remote network access, email, and website access to eWealthManager.

SECURITY OPERATIONS

Employee Security

AssetMark utilizes a third party to conduct background checks, SSN verifications, I-9 documentation and E-verify, and credit checks for all new employees or current employees transitioning to roles which require additional clearance or licensing checks. The process is all automated through the third party's online system and sends out any required legal notices or candidate signoffs.

Physical Media Data Security & Disposal

Locked shred bins are placed throughout the AssetMark offices for disposal of confidential documents.

AssetMark maintains a clean desk policy, which requires all employees to secure confidential information from visibility when not being used. When workstations, servers and storage devices are removed from active inventory, the hard drives are removed and destroyed according to DOD standards.

Removable media such as CDs, DVDs and USB storage devices are prohibited except for authorized individuals. DLP (data loss prevention) software has been installed on end user machines to prevent the use of removable media. Authorized users that require the ability to use USB storage devices will automatically have their drives encrypted and password protected once connected to the user machine. Users do not have the ability to disable or tamper with these features.

Access Privileges

Employee access to network resources and data is role-based. AssetMark employs the "principle of least privilege," giving users access to the necessary data and systems that are essential to perform their job.

Human Resources immediately notifies IT when an employee is terminated or leaves the company and system and network access is removed upon termination through Active Directory. System access is reviewed regularly by management and tracked through the IT Governance process.

Password Policy

All users are assigned unique user IDs and are required to comply with the AssetMark password policy:

- Password complexity enforced
- Account lockout enabled after a certain amount of invalid attempts

Workstation & Back-Office Network Security

Workstations are a standard build of Windows and include virus protection. Microsoft Office is the standard productivity suite. Additional software is installed based on role. Security hardening is enforced on all workstations and servers according to industry best practices. Workstations are set to a locking screensaver through Group Policy settings that cannot be disabled by the user. Standard users do not have administrative access to their local workstations as an added security measure. All laptops are encrypted to protect against data theft. Additionally, data loss protection software removes the ability to remove data via portable media.

Security & Event Monitoring

AssetMark has contracted with a leading third-party- managed security services provider with a security operation center available 24/7 and industry-leading SIEM platform (Security Information Event Management).

Security Vulnerability Scanning

External and internal vulnerability scans are conducted on a regular basis using third-party software to ensure our systems are protected from the latest internet threats.

Patch Management

AssetMark has implemented a patch management schedule to ensure that all critical OS patches are applied monthly. Third-party software patching occurs monthly or as needed.

Penetration Testing

A third-party is used to conduct internal and external Penetration Testing as well as Security Controls Testing on an annual basis. They provide results to the Information Security Team for analysis, prioritization, and remediation where required.

DDoS Protection

A cloud-based service is utilized to provide a multi-faced approach to DDoS (Distributed Denial of Service) defense, providing blanketed protection from all DDoS attacks. A 24/7 security team is constantly monitoring our traffic patterns to ensure only legitimate traffic can access our eWealthManager platform.

Change Control Management

AssetMark has a change control management process that is required for all changes impacting production. Changes must be approved and scheduled by the Change Advisory Board (CAB). Changes are tracked through AssetMark's internal ticketing system. Industry best practices are employed throughout our Software Development Life Cycle. All system changes have the code peer reviewed and are approved by Quality Assurance (QA) prior to being approved for release. All changes and releases are tracked and documented in our ticketing system.

Certificate Management

An inventory of all security certificates is maintained in a centralized repository. The certificates and passphrase information are stored in an encrypted repository that is restricted to authorized users.

File Server and Active Directory (AD) Auditing

Auditing software monitors all changes made to AD and access operations to sensitive folders on the network. Reports are generated automatically and sent to the compliance team for review. Email alerts are configured to notify the security team when specific events occur, such as elevating an account to be a domain administrator.

TESTING

All tests are documented in AssetMark's internal ticketing system. Action items from tests are documented and tracked to completion. Plan updates are made based on results from the test.

Business Continuity

Scenario-based Business Continuity Plan (BCP) Testing is completed on an annual basis. Action items are documented, assigned owners, and tracked through completion.

Disaster Recovery

Periodic Disaster Recovery testing is completed throughout the year to ensure AssetMark's ability to recover critical systems and data in the event of an outage.

Crisis

An annual scenario-based crisis management test is completed with the Crisis Team. Action items are documented, assigned owners, and tracked through completion. The scenario changes from year to year and considers current industry concerns.

Security Incident Response

An annual cyber security tabletop exercise is completed to assess AssetMark's response to a potential cyber security incident. The plan is updated based on the results of the test.

Phishing

AssetMark-crafted phishing emails are sent to groups of employees and contractors. Results of tests are logged, and escalation procedures are in place for those who fail the test. The testing results are reviewed on a regular basis by the Information Security Committee.

AssetMark, Inc.

1655 Grant Street
10th Floor
Concord, CA 94520-2445
800-664-5345

M24-102329 | 02/2024