Ark Advisors LLC
wealth management

Cybersecurity and Data Protection

Ark and its investment advisors have adopted policies and procedures reasonably designed to safeguard your personal and financial information. Ensuring the confidentiality, integrity, and security of your data is of utmost importance to us.

This disclosure is not, and is not intended to be, a complete explanation of Ark policies and procedures related to cybersecurity and data protection. Should you have questions about our policy, please contact our office at 309-661-2000.

Our Commitment to Data Security:

At Ark Advisors, LLC, we employ advanced cybersecurity technologies and best practices to protect your sensitive information from unauthorized access, disclosure, alteration, and destruction. These measures include but are not limited to:

1. Data Encryption: Your data is encrypted both in transit and at rest, ensuring that it remains secure during transmission and storage.
2. Firewalls and Intrusion Detection Systems: We utilize firewalls and intrusion detection systems to monitor and block unauthorized access attempts, protecting our network from external threats.
3. Regular Security Audits: We conduct regular security audits and assessments to identify and address potential vulnerabilities in our systems and processes.
4. Employee Training: Our staff is trained on cybersecurity awareness and best practices to recognize and mitigate potential security risks effectively.
5. Secure Data Centers: Your data is stores in secure, state-of-the-art data centers with robust physical and environmental controls to prevent unauthorized access.

Overview of Ark Information Security Policy:

Ark's information security policy aligns with the latest NIST Cybersecurity Framework (NIST CSF). The following categories are included in this framework with adaptations aligned to NIST Small Business best practices:

- Identify (ID) – Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect (PR) – Develop and implement the appropriate safeguards to ensure delivery of critical business services.
- Detect (DE) – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond (RS) – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover (RC) – Develop and implement the appropriate activities to maintain plans for diligence

and to restore any capabilities or services that were impaired due to a cybersecurity event.

Compliance

Ark and its investment advisors will regularly review our policies and procedures related to cybersecurity and data protection in alignment with updates to the NIST framework, new regulations, updates to best practices, and ongoing learnings with cyber incidents. Ark security policies may change at any time under the discretion and approval of the CISO.

Cybersecurity Insurance

Ark Advisors, LLC will maintain Cybersecurity insurance in alignment with our standards and guidelines presented in our Information Security Policy.

Your Role in Cybersecurity

While Ark takes significant steps to protect your data, it is essential for Clients to remain vigilant and follow these best practices:

1. Use Strong Passwords: Create strong, unique passwords for your online accounts and change them regularly.
2. Beware of Phishing Attempts: Be cautious about emails or messages asking for sensitive information. Always verify the sender's authenticity before responding.
3. Update Software: Keep your operating system, antivirus software, and applications up-to-date to protect against known vulnerabilities.
4. Secure Your Devices: Enable security features such as passcodes or biometric authentication on your devices to prevent unauthorized access.

Incident Response

In the event of a cybersecurity incident, Ark has a comprehensive incident response plan in place. This plan includes notifying affected clients promptly and taking necessary actions to mitigate the impact of the incident.

If you suspect any authorized activity related to your account or have concerns about cybersecurity, please contact our office at 309-661-2000.