CHECKLIST

Cybersecurity essentials for investment funds

Cybersecurity is a critical concern for pooled investment vehicles such as hedge funds and private equity funds, as these entities handle sensitive financial data while operating within an increasingly complex regulatory landscape. This checklist is designed to help you assess and strengthen your cybersecurity posture by addressing key areas. By proactively implementing these best practices, you can help mitigate potential threats, safeguard your investors' trust, and maintain compliance with industry standards.

1. Access Controls and Authentication:

- ☐ **Strong passwords:** Enforce complex passwords with a mix of characters and regular password resets.
- ☐ **Multi-factor authentication (MFA):** Require users to provide multiple forms of identification to access sensitive systems.
- ☐ **Least privilege principle:** Grant only the minimum necessary access levels to users based on their role.
- ☐ **Regular access reviews:** Periodically audit user access to identify and revoke unnecessary permissions.

2. Data Encryption:

- ☐ **Encryption at rest:** Encrypt all sensitive data stored on servers and devices.
- ☐ **Encryption in transit:** Securely encrypt data transmitted across networks.
- ☐ **Key management:** Implement robust key management practices to control access to encryption keys.

3. Network Security:

- ☐ **Firewalls:** Utilize robust firewalls to filter incoming and outgoing network traffic.
- ☐ **Intrusion detection/prevention systems (IDS/IPS):** Monitor network activity for potential threats and take preventative actions.
- ☐ **Network segmentation:** Separate critical systems from less sensitive networks to limit the spread of attacks.

4. Data Backup and Recovery:

- [ ] **Regular backups:** Regularly back up critical data to offsite locations.
- [ ] **Disaster recovery and business continuity plan:** Develop a plan to restore data and operations in case of a major incident.

5. Security Monitoring and Incident Response:

- [ ] **Log management:** Centralize system logs to identify potential security issues.
- [ ] **Security information and event management (SIEM):** Monitor logs for anomalies and potential threats.
- [ ] **Incident response plan:** Define procedures for detecting, containing, reporting, and mitigating security incidents.

6. Employee Training and Awareness:

- [ ] **Regular cybersecurity training:** Educate employees on phishing scams, password hygiene, and other security best practices.
- [ ] **Phishing simulations:** Conduct periodic phishing simulations to test employee awareness.

7. Third-Party Risk Management:

- [ ] **Vendor due diligence:** Assess the cybersecurity posture of all third-party vendors with access to sensitive data.
- [ ] **Contractual agreements:** Include security provisions and incident reporting in contracts with vendors.

8. Compliance and Regulatory Adherence:

- [ ] **Industry standards:** Adhere to relevant data privacy laws, such as GDPR and CCPA, and comply with cybersecurity and regulatory guidelines, including those issued by the SEC and various States.
- [ ] **Regular assessments:** Conduct periodic security risk assessments and audits to identify vulnerabilities and ensure compliance.