Physical Security and Cybersecurity Policy and Procedures
Eagle Investors LLC

1. Introduction

Eagle Investors LLC (Eagle) prioritizes the protection of our clients' confidential information. This policy establishes comprehensive physical and cybersecurity controls to:

Maintain confidentiality: Restrict access to sensitive data and prevent unauthorized disclosure.
Preserve integrity: Ensure accuracy and completeness of information, free from alteration or manipulation.
Guarantee availability: Maintain continuous access to essential systems and data for authorized users.
All Eagle employees, contractors, and third-party vendors must comply with this policy.

A copy of this policy can always be found publicly at
https://eagle-investors.com/cybersecurity-policy/

2. Policy and Procedures

A. Risk Management

Threat Assessment: Eagle will conduct regular risk assessments to identify, analyze, and prioritize potential threats to its information security.

Vulnerability Management: Systems and applications will be routinely assessed for vulnerabilities and promptly patched to address identified weaknesses.

Business Continuity & Disaster Recovery (BCDR): A comprehensive BCDR plan will be developed and tested to ensure timely recovery from potential disruptions.

B. Critical Infrastructure Protection

System & Data Classification: Information assets will be classified based on sensitivity level to determine appropriate security controls.

Access Control: Access to critical systems and data will be granted based on the principle of least privilege and monitored for suspicious activity.

Network Security: Firewalls, intrusion detection/prevention systems (IDS/IPS), and malware protection will be employed to safeguard network resources.

C. Security Event Identification

Log Monitoring: Logs from critical systems and devices will be monitored for anomalies and suspicious activity indicative of potential security incidents.

Security Information and Event Management (SIEM): A SIEM solution will be implemented to aggregate and analyze security data from various sources for efficient incident detection.

Vulnerability Scanning: Regular vulnerability scans will be conducted to identify and address potential weaknesses before attackers exploit them.

D. Security Event Response

Incident Response Plan: A comprehensive incident response plan will outline roles, responsibilities, and procedures for handling security incidents.

Incident Reporting: All suspected security incidents must be reported promptly to the designated incident response team.

Incident Containment: Immediate action will be taken to contain identified incidents, minimize damage, and prevent further exploitation.

Investigation & Analysis: Thorough investigation will be conducted to determine the cause, scope, and impact of the incident.

Recovery & Remediation: Affected systems and data will be restored, vulnerabilities patched, and lessons learned documented for future prevention.

E. Resilience and Recovery

Backups & Data Archiving: Regular backups of critical data will be maintained and stored securely off-site for disaster recovery purposes.

System Redundancy & Failover: Critical systems will be designed with redundancy and failover capabilities to ensure continuous operation in case of disruptions.

Testing & Drills: BCDR plans and incident response procedures will be regularly tested and updated to ensure effectiveness.

3. Establishment, Implementation, Updates, and Enforcement

A. Establishment:

This policy has been reviewed and approved by Eagle's management team.
The Chief Compliance Officer is always, and only if appointed, the Chief Information Security Officer (CISO) is also responsible for the implementation and enforcement of this policy.

B. Implementation:

This policy will be communicated and documented for all employees, contractors, and third-party vendors.

Security awareness training will be provided to educate personnel on best practices and incident reporting procedures.

Necessary resources will be allocated to implement and maintain security controls.

C. Updates:

This policy will be reviewed and updated annually, or more frequently as needed, to reflect changes in technology, regulations, and threats.

Updates will be communicated to all relevant personnel.

D. Enforcement:

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contracts.
Security incidents will be investigated, and appropriate corrective action will be taken.

4. Conclusion

Eagle Investors LLC is committed to safeguarding client information through a comprehensive approach to physical and cybersecurity. This policy establishes a framework for continuous improvement and risk mitigation, ensuring the confidentiality, integrity, and availability of

sensitive data. By adhering to this policy and fostering a culture of security awareness, Eagle can build trust and maintain its leading position in the financial services industry.