State-Regulated RIA Cybersecurity Compliance Checklist

As a state-regulated Registered Investment Adviser (RIA), you are expected to protect sensitive client information and demonstrate that you have reasonable cybersecurity safeguards in place.

At **Palisade Cybersecurity**, we help Registered Investment Advisors stay secure, compliant, and audit-ready, without adding complexity.

Below is a breakdown of what state regulators typically require:

Governance & Documentation

1. ☐ Written Information Security Program (WISP)
2. ☐ Cybersecurity policies & procedures
3. ☐ Defined security roles and responsibilities
4. ☐ Annual policy review documentation

Risk Management

1. ☐ Annual cybersecurity risk assessment
2. ☐ Risk register with remediation tracking
3. ☐ Documented risk treatment decisions

Client Data Protection

1. ☐ Protection of Non-Public Personal Information
2. ☐ Encryption of data in transit and at rest
3. ☐ Secure storage of client records

Access Controls

1. ☐ Multi-Factor Authentication enabled
2. ☐ Unique user accounts
3. ☐ Strong password policy
4. ☐ Least privilege access

Vendor Risk Management

1. ☐ Vendor inventory list
2. ☐ Risk classification of vendors
3. ☐ Security questionnaires
4. ☐ Contract security clauses

Security Awareness Training

1. ☐ Annual employee training
2. ☐ Phishing simulations
3. ☐ Training completion records

Incident Response

1. ☐ Written Incident Response Plan
2. ☐ Defined escalation procedures
3. ☐ Breach notification process

Business Continuity

1. ☐ Data backup procedures
2. ☐ Recovery testing
3. ☐ Ransomware response strategy

Ready to strengthen your cybersecurity and compliance posture? Contact Palisade Cybersecurity today to schedule a consultation.