Financial Firms Cybersecurity Compliance Checklist

D1 DEFEND
CYBER THREAT DEFENSE

- [ ] **Designate a Cybersecurity Governance Team**
  - Ensure dedicated oversight of cybersecurity initiatives.
- [ ] **Regular Risk Assessment of Financial Data and Systems**
  - Focus on threats specific to financial services and customer data.
- [ ] **Implement Advanced Data Security Measures**
  - Use encryption, intrusion detection systems, and secure transaction processes.
- [ ] **Adhere to Regulatory Compliance Standards**
  - Comply with regulations like GLBA, SEC, FINRA, and others relevant to financial services.
- [ ] **Conduct Ongoing Employee Training**
  - **Regular training on evolving cyber threats and security protocols.**
- [ ] **Develop a Comprehensive Incident Response Plan**
  - **Include procedures for quick detection, response, and recovery from cybersecurity incidents.**
- [ ] **Manage Third-Party Vendor Risks**
  - Assess and monitor the cybersecurity practices of all associated vendors.
- [ ] **Regularly Update and Test Security Systems**
  - Conduct regular training sessions on cyber threats and safe practices.
- [ ] **Document and Report Cybersecurity Efforts**
  - Keep detailed records for regulatory compliance and auditing purposes.
- [ ] **Ensure Physical Security of Data Centers Policies Regularly**
  - Protect physical locations where sensitive data is stored or processed.

Ever Wonder What Your Business Cybersecurity Compliance Score is?

Contact us today to know your Cybersecurity Compliance Score for free!
+1 (714) 988 3493 or cs@d1defend.com
www.d1defend.com

Schedule your D1 Diagnosis