afinety

Checklist for Law Firms: **Essential Steps to Strengthen IT Security & Compliance**

Protecting client confidentiality while maintaining efficient workflows

Law firms handle highly sensitive client data, making them prime targets for cyber threats. A single breach can result in reputational damage, regulatory fines and loss of client trust. This checklist provides **actionable steps** to help legal practices strengthen their IT security while ensuring compliance with ABA, FTC and state regulations.

1 Establish a Security & Compliance Framework (WISP)

- ✓ **Develop a WISP** to define security policies, risk management protocols and compliance measures
- ✓ **Align WISP with laws** like ABA, FTC Safeguards Rule and state breach notification
- ✓ **Conduct an annual review and update** the WISP to adapt to evolving threats
- ✓ **Automate compliance tracking and reporting** to simplify audits and ensure ongoing adherence

2 Secure Access & Authentication

- ✓ **Implement Multi-Factor Authentication (MFA)** on all accounts, especially case management systems
- ✓ **Use strong, unique passwords** and consider **password managers** for firm-wide security
- ✓ **Enable session monitoring** to detect unauthorized logins (e.g., impossible travel detection)
- ✓ **Limit access based on user roles** to minimize exposure to sensitive information

3 Protect Privileged & Case Data

- ✓ **Encrypt sensitive files** both in transit and at rest to prevent unauthorized access
- ✓ **Use secure file-sharing solutions** for client and communications
- ✓ **Regularly audit data storage practices** to identify and eliminate shadow data vulnerabilities
- ✓ **Restrict document access** to only those who need it; avoid storing data on local devices

afinety.com
877.423.4638
linkedin.com/company/afinety

afinety

4 Defend Against Phishing & Email Threats

- **Train staff regularly** to recognize phishing attempts and social engineering tactics
- **Implement email filtering tools** to block malicious attachments and suspicious links
- **Simulate phishing attacks** internally to assess employee awareness and response
- **Establish a verification process** for email requests related to financial transactions

5 Secure Remote Work Environments

- **Use virtual desktop environments** to centralize access and secure workstations
- **Encrypt all remote connections** to prevent unauthorized interception
- **Monitor and secure Wi-Fi networks** with updated firmware and strong passwords

6 Strengthen Cloud & IT Infrastructure Security

- **Migrate IT infrastructure to secure cloud providers** like AWS to reduce on-premises vulnerabilities
- **Regularly update all software and case management tools** to patch vulnerabilities
- **Conduct annual penetration testing** to identify and address security weaknesses

7 Implement an Incident Response & Continuous Improvement Plan

- **Create a cybersecurity incident response plan** that aligns with WISP guidelines
- **Ensure firm-wide cybersecurity training** is updated frequently to include emerging threats like business email compromise (BEC)
- **Monitor security metrics** to track improvement areas and identify ongoing risks
- **Review cybersecurity policies and WISP annually** to stay ahead of evolving threats

Need help aligning your firm's IT security with compliance requirements? **Let's discuss** how to strengthen your cybersecurity strategy and ensure your policies meet ABA, FTC and state regulations.

afinety.com
877.423.4638
linkedin.com/company/afinety