motiva

2024 DFS Compliance Checklist

The following questions represent the core components necessary for DFS compliance. Please check off as applicable to self-evaluate your practice or organization.

☐ **Do you currently have a documented Written Cybersecurity Plan (WISP)?**
- ☐ Based on a risk assessment performed
- ☐ Able to detect cybersecurity events 24/7
- ☐ Can Identify internal and external threats
- ☐ Can fully recover from data backups

☐ **Do you have Multi-Factor Authentication (MFA) securing ALL of the following?**
- ☐ Agency Management Software
- ☐ Local PC's and Laptops
- ☐ Remote devices
- ☐ Microsoft 365
- ☐ The Cloud

☐ **Have you performed annual risk assessments and penetration testing of systems and network?**
- ☐ Have you documented all inefficiencies and written a remediation plan with timeline?
- ☐ Once you remediated the issues, did you perform another risk assessment to verify the fixes?
- ☐ Do you have documentation for annual reviews of your Policies and Procedures?

☐ **Have all staff members done annual Cybersecurity training, including social engineering?**
- ☐ Do you have documentation of their training?
- ☐ Is there a staff member designated as the DFS Compliance, Privacy, and/or Security Officer?

☐ **Do you have a complete and accurate documented asset inventory?**
- ☐ Including owner, location, sensitivity, support expiration dates, and recovery time requirements?
- ☐ Regularly maintain and update the asset inventory?
- ☐ Have a documented method for secure disposal of non-public information both digitally and physically on outdated technology such as laptops and phones?

☐ **Do you have an MDR or EDR to detect cybersecurity incidents or attempted breaches 24/ 7?**
- ☐ Are you able to provide the required reporting of minor or meaningful breaches or incidents, including those at third-party vendors or affiliates, within 72 hours to DFS?
- ☐ Do your staff members have the ability to anonymously report an incident?

AUDIT TIP: If audited, you must provide all documentation in an eligible format to auditors.

DFS Cybersecurity Compliance can be overwhelming. Work with Motiva to make sure you have everything in place. Contact us at 646-374-1820 or info@motiva.net

This checklist is composed of general questions about the measures your organization should have in place to state that you are DFS compliant, and does not qualify as legal advice. Successfully completing this checklist ***DOES NOT*** *certify that you or your organization are DFS compliant.*