Cybersecurity Implementation Timeline for Small Businesses

This timeline includes key dates for DFS-licensed individual producers, mortgage loan originators, and other businesses that qualify for exemptions under Sections 500.19 (a), (c), and (d) of the amended Cybersecurity Regulation.

**Indicates actions that are not required for Covered Entities that qualify for 500.19(c) and (d) exemptions. 500.19(c) exemptions apply to entities that do not maintain nonpublic information and 500.19(d) exemptions apply to captive insurers.*

This guide is provided for general planning purposes. Please consult the text of the Cybersecurity Regulation for specific requirements.

December 1, 2023
Section 500.17
Notifying DFS of cybersecurity events continues to be required. What's new: Ransomware deployment and any ransom payments made must be reported.

April 29, 2024
Section 500.9
- Risk assessments continue to be required. What's new: Risk assessments must be reviewed and updated at least annually, and whenever a change in the business or technology causes a material change to the business' cyber risk.

Section 500.3*
- After assessing your risks, update your policies to address these issues if needed:
  - Data retention
  - End of life management (phasing out unsupported technical products with vulnerabilities)
  - Remote access controls
  - Systems and network monitoring
  - Security awareness and training
  - Systems and application security
  - Incident notification
  - Vulnerability management

November 1, 2025
Section 500.12*
Comply with enhanced MFA requirements.

Section 500.13(a)
Implement new asset inventory requirements.

November 1, 2023
Section 500.19
More businesses qualify for exemptions (limited and full). Check to confirm eligibility for an exemption.

April 15, 2024
Section 500.17(b)
Annual compliance submissions continue to be due. What's new: Determine whether to file one of two new forms: Certification of Material Compliance or Acknowledgment of Noncompliance.

November 1, 2024
Section 500.12(a)*
Implement multifactor authentication (MFA) requirements outlined in Section 500.12(a) if you have not already done so.

Section 500.14(a)(3)*
Provide all personnel at your business at least annual cybersecurity awareness training.

May 1, 2025
Section 500.7*
- Implement enhanced requirements regarding limiting user access privileges, including privileged account access.
- Review access privileges and remove or disable accounts and access that are no longer necessary.
- Disable or securely configure all protocols that permit remote control of devices.
- Promptly terminate access following personnel departures.
- Implement a reasonable written password policy to the extent you use passwords.