CLS and FTC Compliance

Part I - FTC Start with Security Guidelines

	Implemented in CLS	User’s responsibility
Section 1: Start with security		
Don’t collect personal information you don’t need.	✓ All personal data is required for reporting.	
Hold onto information only as long as you have a legitimate business need.	✓ EP allows deletion of old data at user’s request.	
Don’t use personal information when it’s not necessary.	✓ Personal data is only used when required for reporting.	
Section 2: Control access to data sensibly		
Restrict access to sensitive data.		✓
Limit administrative access.		✓
Section 3: Require secure passwords and authentication		
Insist on complex and unique passwords.	✓ CLS provides multiple methods of password protection. Users determine whether to implement and the level of password complexity.	
Store passwords securely.		✓
Guard against brute force attacks.		✓
Protect against authentication bypass.	✓ CLS provides multiple methods of password protection. Users determine whether to implement.	
Section 4: Store sensitive personal information securely and protect it during transmission		
Keep sensitive information secure throughout its lifecycle.	✓ EINs, SSNs, TINs and banking information have been protected using proprietary encryption routines for many years. *CLS is being updated so that the employee’s Date of Birth will also be encrypted.* Backup files sent to FMSI are protected by a password unique for each FMSI customer.	
Use industry-tested and accepted methods.	*While we are confident in the proprietary encryption routines used in CLS, we are researching accepted industry standards to determine whether they may provide increased security.*	

	Implemented in CLS	User’s responsibility
Ensure proper configuration.	✓ The encryption methods used and the password required to access ledger files isn’t documented anywhere outside CLS programs.	
Section 5: Segment your network and monitor who’s trying to get in and out		
Segment your network.		✓
Monitor activity on your network.		✓
Section 6: Secure remote access to your network		
Ensure endpoint security.		✓
Put sensible access limits in place.		✓
Section 7: Apply sound security practices when developing new products		
Train your engineers in secure coding.	✓ Any newly required sensitive data elements will be encrypted.	
Follow platform guidelines for security.	✓ All data is stored locally on the customer’s computers. There is no vulnerability of files being stored across cloud-based networks.	
Verify that privacy and security features work.	✓ Storing and retrieving any newly required sensitive data will be thoroughly tested.	
Test for common vulnerabilities.	✓ Storing and retrieving any newly required sensitive data will be thoroughly tested.	
Section 8: Make sure service providers implement reasonable security measures		
Put it in writing.	✓ *CLS documentation is being updated to list all data that is encrypted or password protected*.	
Verify compliance.	✓ Sensitive data is encrypted and ledger backup files are password protected.	
Section 9: Put procedures in place to keep your security current and address vulnerabilities that may arise		
Update and patch software as needed.	✓ CLS updates are posted as known bugs are corrected and customers are notified via email of their availability.	
Heed credible security warnings and move quickly to fix them.		✓ It is the customer’s responsibility to install updates in a timely manner.
Section 10: Secure paper, physical media and devices		
Securely store sensitive files.		✓
Protect devices that process personal information.		✓

	Implemented in CLS	User’s responsibility
Keep safety standards in place when data is en route.	✓ Sensitive data is encrypted and ledger backup files are password protected.	
Dispose of sensitive data securely.	✓ EP allows deletion of old data at user’s request.	

Part II – FTC Safeguards Rule Requirements

	Applies to all tax/payroll preparers	Exemption for tax/payroll preparers with less than 5000 clients
1. Designate a qualified individual to implement and supervise your company's information security program.	✓	
2. Develop a written risk assessment based on the *Start with Security Guidelines*.		✓
3. Design and implement safeguards to control the risks identified through risk assessment.	✓	
4. Scheduled testing and or continuous monitoring of effectiveness of your safeguards.		✓
5. Ensure personnel is trained and enacting your security program.	✓	
6. Monitor service providers with access to client data.	✓	
7. Evaluate and adjust your security program current.	✓	
8. Create a written incident response plan.		✓
9. Require your qualified individual to report annually to your board of directors (or senior officer responsible for changes in information security).		✓