2026

Written Information Security Plan

IRS Publication 4557 Compliant

Riverside Accounting

CA

WISP Version: 2026 | Effective: January 1, 2026

Generated by WISP-Creator | 2026 Annual Security Plan

This document must be reviewed and updated annually per IRS requirements

About This Document

Purpose

This Written Information Security Plan (WISP) is a federally mandated document required by the FTC Safeguards Rule (16 CFR 314) for all professional tax preparers. It establishes your firm's policies and procedures for protecting client personally identifiable information (PII), including Social Security numbers, financial records, and tax return data.

This document serves three critical functions:

1. **Compliance** - Demonstrates your firm meets IRS and FTC data security requirements
2. **Protection** - Provides a framework for safeguarding client information
3. **Response** - Guides your team through security incidents when they occur

How to Use This Document

Policy Sections

Each section contains specific policies tailored to your firm. Review these with all employees and ensure everyone understands their responsibilities.

Checklists [ ]

Throughout this document, you'll find checkbox items. These are actionable checklists for specific procedures. When performing tasks like incident response, data destruction, or employee offboarding, use these as step-by-step guides to ensure nothing is missed.

Document Control

Your WISP is a living document. The IRS requires annual review and updates. Update your WISP when:

- Your firm's size or operations change
- You adopt new technology or systems
- A security incident reveals gaps
- Regulations change

Required Actions

1. READ - All employees must read and understand this document
2. SIGN - Employees should acknowledge receipt and understanding
3. STORE - Keep copies both on-site and in secure cloud/offsite storage
4. REVIEW - Conduct annual reviews (suggested: each May after tax season)
5. UPDATE - Revise as your firm and technology evolve

Questions? Contact your Data Security Coordinator listed on the cover page.

Incident Response Plan

INCIDENT RESPONSE PLAN

COMPLIANCE STATUS SUMMARY

1. SECURITY INCIDENT DEFINITION

For purposes of this plan, a security incident is defined as any event that:
- Compromises the confidentiality, integrity, or availability of Federal Tax Information (FTI)
- Results in unauthorized access to taxpayer data including SSNs, bank accounts, tax returns, or business financials
- Involves suspected or confirmed data breach, malware infection, or system compromise
- Constitutes a violation of IRS Publication 4557 safeguarding requirements
- Creates potential identity theft risk for clients or the firm

2. IMMEDIATE RESPONSE PROCEDURES (0-24 HOURS)

2.1 Initial Detection and Response Team Activation
1. Incident Discovery: Any employee discovering a potential security incident must immediately notify the firm owner/designated security officer
2. Initial Assessment: Within 1 hour, determine incident severity level:
   - Critical: Confirmed breach of taxpayer data
   - High: Suspected breach or system compromise
   - Medium: Security control failure without confirmed data access
   - Low: Attempted but unsuccessful attack

2.2 IT Support Engagement
The firm maintains access to qualified IT support personnel who will be contacted within 2 hours of incident detection to assist with technical assessment and response activities.

2.3 Documentation Requirements
1. Incident Log: Create written record including:
   - Date and time of discovery
   - Nature of incident
   - Systems/data potentially affected
   - Initial response actions taken
   - Personnel involved

3. CONTAINMENT PROCEDURES

3.1 Immediate Containment (Hours 1-4)
1. Isolate Affected Systems: Disconnect compromised systems from network while preserving evidence
2. Secure Physical Access: Restrict access to affected workstations and server areas

3. Change Passwords: Reset credentials for potentially compromised accounts
4. Network Monitoring: Monitor network traffic for signs of continued unauthorized activity

3.2 Evidence Preservation
1. Preserve system logs and audit trails
2. Document all containment actions taken
3. Maintain chain of custody for digital evidence

4. ASSESSMENT AND DOCUMENTATION

4.1 Damage Assessment
Within 24-48 hours, complete comprehensive assessment including:
1. Data Inventory: Identify specific taxpayer records potentially compromised
2. System Impact: Document affected hardware, software, and network components
3. Timeline Analysis: Establish incident timeline and duration of potential exposure
4. Root Cause Analysis: Determine how the incident occurred

4.2 Documentation Package
Maintain complete incident file containing:
- Initial incident report
- Assessment findings
- Response actions taken
- Evidence collected
- Communication records

5. NOTIFICATION REQUIREMENTS

5.1 IRS Notification
Timeline: Within 24 hours of confirming FTI compromise
Method: Contact IRS at 866-562-5422 or email FFTIP@IRS.gov
Information Required:
- Firm name, address, and EIN
- Nature and scope of incident
- Number of taxpayers potentially affected
- Remediation steps taken

5.2 Client Notification
Timeline: Within 72 hours of incident confirmation
Method: Written notice via certified mail and telephone contact
Content: Description of incident, data potentially affected, steps taken, and protective measures clients should consider

5.3 State Authority Notification
California Requirements: Notify California Attorney General within specified timeframes per CA Civil

Code Section 1798.29 if personal information compromised

5.4 Insurance Notification
CURRENT STATE: Riverside Accounting does not currently maintain cyber liability insurance coverage.

REGULATORY REQUIREMENT: While not mandated by IRS regulations, cyber liability insurance provides critical financial protection and incident response resources for tax practices handling sensitive taxpayer data.

GAP REMEDIATION PLAN:
- Obtain quotes from qualified cyber liability insurers by March 31, 2026
- Secure appropriate coverage limits (minimum $1M recommended) by June 30, 2026
- Ensure policy includes first-party coverage for notification costs, credit monitoring, and business interruption
- Verify coverage includes regulatory fines and penalties

COMPENSATING CONTROLS:
- Maintain incident response fund of $10,000 for immediate response costs
- Pre-identify breach notification vendors and legal counsel
- Document all incident response costs for potential future insurance claims

6. RECOVERY PROCEDURES

6.1 System Restoration
1. Malware Removal: Ensure complete elimination of malicious software
2. System Hardening: Apply security patches and configuration changes
3. Data Integrity Verification: Confirm data has not been altered or corrupted
4. Backup Restoration: Restore systems from clean backups if necessary

6.2 Operational Recovery
1. Service Restoration: Gradually restore normal business operations
2. Additional Monitoring: Implement enhanced monitoring for 90 days post-incident
3. Staff Training: Provide additional security awareness training based on incident lessons

7. POST-INCIDENT REVIEW PROCESS

7.1 Incident Review Meeting
Timeline: Within 30 days of incident resolution
Participants: Firm owner, affected staff, IT support personnel
Agenda:
- Incident timeline review
- Response effectiveness assessment
- Control failure analysis
- Improvement recommendations

7.2 WISP Updates
Based on incident findings, update this Written Information Security Plan within 60 days to address identified vulnerabilities and improve response procedures.

7.3 Regulatory Compliance Review
Ensure all IRS Publication 4557 requirements were met during incident response and document any compliance gaps for immediate remediation.

7.4 Annual Testing
Conduct tabletop exercises annually to test incident response procedures and maintain staff readiness.

Document Version: 1.0
Effective Date: January 1, 2026
Review Date: January 1, 2027
Owner: Riverside Accounting Management

This Incident Response Plan is designed to ensure compliance with IRS Publication 4557 and California state data protection requirements.

Password & Authentication Policy

PASSWORD & AUTHENTICATION POLICY

COMPLIANCE STATUS SUMMARY

[x] COMPLIANT AREAS
- Multi-Factor Authentication implementation (Authenticator App)
- Password manager deployment across organization
- Minimum password length requirements (12-15 characters)
- Prohibition of shared credentials

IN-PROGRESS REMEDIATION
- None

GAPS REQUIRING REMEDIATION
- None

1. PASSWORD REQUIREMENTS

1.1 Password Complexity Standards
Riverside Accounting enforces the following password requirements for all systems containing customer information:

- Minimum Length: 12 characters minimum for all accounts
- Complexity Requirements: Passwords must contain at least three of the following four character types:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Special characters (!@#$%^&*)
- Password History: Systems prevent reuse of the last 12 passwords
- Dictionary Protection: Passwords cannot contain common dictionary words or personal information

1.2 Password Rotation Policy
- Standard Accounts: Passwords expire every 90 days
- Administrative Accounts: Passwords expire every 60 days
- Service Accounts: Passwords are changed annually or upon personnel changes
- Emergency Override: Immediate password changes required upon suspected compromise

2. MULTI-FACTOR AUTHENTICATION (MFA)

2.1 FTC Safeguards Rule Compliance
In accordance with FTC Safeguards Rule 16 CFR 314.4(c)(5), Riverside Accounting has implemented multi-factor authentication for all personnel accessing customer information systems.

2.2 MFA Implementation
- Primary Method: Microsoft Authenticator app for time-based one-time passwords (TOTP)
- Coverage: MFA is required for:
  - Tax preparation software access
  - Cloud storage platforms containing customer data
  - Email systems
  - Remote desktop connections
  - Administrative system access
- Backup Authentication: SMS-based codes available as secondary option
- Enrollment: All employees complete MFA enrollment within first day of employment

2.3 MFA Exception Handling
- Emergency Access: Designated Information Security Officer maintains emergency bypass codes
- Device Loss: Employees report lost MFA devices immediately for account security reset
- Temporary Exemptions: Not permitted under any circumstances

3. ACCOUNT LOCKOUT PROCEDURES

3.1 Automated Lockout Parameters
- Failed Attempts: Accounts lock after 5 consecutive failed authentication attempts
- Lockout Duration: 30-minute automatic lockout period
- Progressive Delays: Implement increasing delay between failed attempts (1 second, 5 seconds, 15 seconds, etc.)

3.2 Account Unlock Procedures
- Self-Service: Employees may unlock accounts using MFA verification after lockout period
- Administrative Override: Information Security Officer can perform immediate unlock with business justification
- Documentation: All manual unlocks are logged and reviewed monthly

4. PASSWORD STORAGE AND MANAGER REQUIREMENTS

4.1 Password Manager Implementation
Riverside Accounting utilizes enterprise-grade password management solutions for all business credentials:

- Approved Solution: Bitwarden Business deployed across all workstations
- Mandatory Usage: All business passwords must be stored in the password manager
- Unique Passwords: Password manager generates unique passwords for each system
- Encrypted Storage: All passwords encrypted using AES-256 encryption
- Regular Audits: Monthly reviews of password manager usage and security

4.2 Master Password Requirements

- Length: Minimum 16 characters
- Complexity: Must include uppercase, lowercase, numbers, and special characters
- Uniqueness: Master passwords cannot be used for any other purpose
- Rotation: Changed every 180 days or upon personnel changes

5. SHARED CREDENTIAL PROHIBITION

5.1 Individual Account Policy
Riverside Accounting strictly prohibits shared login credentials:

- Individual Accounts: Each employee maintains unique login credentials for all systems
- Accountability: Individual accounts ensure proper audit trails and access control
- Exception Policy: No exceptions permitted for shared credentials
- Generic Accounts: Generic or shared accounts are not permitted for any business systems

5.2 Violation Consequences
- First Violation: Written warning and mandatory security training
- Repeat Violations: Progressive disciplinary action up to termination
- Security Impact: Immediate credential reset and security assessment

6. SERVICE ACCOUNT MANAGEMENT

6.1 Service Account Standards
- Naming Convention: Service accounts follow standardized naming (SVC[Application][Function])
- Documentation: Complete inventory maintained with purpose, owner, and access rights
- Rotation Schedule: Credentials changed annually and upon personnel changes
- Monitoring: Service account activity monitored for anomalous behavior

6.2 Access Control
- Principle of Least Privilege: Service accounts granted minimum necessary permissions
- Regular Review: Quarterly access reviews to validate continued need
- Approval Process: New service accounts require Information Security Officer approval

7. AUTHENTICATION LOGGING REQUIREMENTS

7.1 Logging Standards
Riverside Accounting maintains comprehensive authentication logs:

- Events Logged:
  - Successful and failed login attempts
  - Password changes and resets
  - Account lockouts and unlocks
  - MFA enrollment and authentication events
  - Administrative access to authentication systems

7.2 Log Management
- Retention Period: Authentication logs retained for minimum 3 years
- Real-Time Monitoring: Failed authentication attempts trigger immediate alerts
- Regular Review: Weekly review of authentication anomalies
- Secure Storage: Logs stored in tamper-evident, encrypted format

7.3 Incident Response Integration
- Automated Alerts: Multiple failed attempts trigger incident response procedures
- Analysis Requirements: All authentication anomalies investigated within 24 hours
- Documentation: Results of investigations documented and retained

8. POLICY ENFORCEMENT AND COMPLIANCE

8.1 Training Requirements
- Initial Training: All new employees complete password security training within first week
- Annual Refresher: Mandatory annual security awareness training
- Incident-Based Training: Additional training required following security incidents

8.2 Compliance Monitoring
- Regular Audits: Quarterly compliance assessments of password and authentication controls
- Metrics Tracking: Monthly reporting on password policy compliance metrics
- Continuous Improvement: Annual policy review and updates based on threat landscape

Policy Effective Date: January 1, 2026
Next Review Date: January 1, 2027
Policy Owner: Information Security Officer
Approved By: Riverside Accounting Management

Data Protection & Encryption

DATA PROTECTION & ENCRYPTION POLICY

Riverside Accounting
California Tax Practice
Policy Effective Date: January 2026

COMPLIANCE STATUS SUMMARY

1. DATA CLASSIFICATION FRAMEWORK

1.1 Data Categories
Riverside Accounting handles the following classifications of sensitive information:

Level 1 - Tax Records & Returns
- Federal and state tax returns
- IRS Forms (W-2, 1099, K-1, etc.)
- Tax workpapers and calculations
- Prior year returns and amendments

Level 2 - Personally Identifiable Information (PII)
- Social Security Numbers
- Employer Identification Numbers
- Driver's license numbers
- Date of birth information

Level 3 - Financial Data
- Bank account information
- Investment statements
- Business financial records
- Credit card information (if processed)

1.2 Data Handling Requirements
All Level 1-3 data requires encryption protection per IRS Publication 4557 and FTC Safeguards Rule 16 CFR Part 314.

2. STORAGE ENCRYPTION REQUIREMENTS

2.1 Local Storage Encryption

CURRENT STATE: Client data is currently stored on local computers and external drives without encryption protection.

REGULATORY REQUIREMENT: FTC Safeguards Rule 16 CFR Section 314.4(b) mandates encryption of customer information stored electronically. IRS Publication 4557 requires tax preparers to encrypt sensitive taxpayer data.

GAP REMEDIATION PLAN:
- Phase 1 (by February 15, 2026): Install BitLocker encryption on all Windows workstations storing client data
- Phase 2 (by February 28, 2026): Implement hardware-encrypted external drives (minimum AES-256 encryption)
- Phase 3 (by February 28, 2026): Complete data migration to encrypted storage with verification testing

COMPENSATING CONTROLS: Until full encryption implementation, client data access is restricted to authorized personnel only, workstations are physically secured after hours, and external drives are stored in locked cabinets.

2.2 Encryption Standards
Upon implementation, all storage encryption will meet:
- Algorithm: AES-256 bit encryption minimum
- Key Management: Unique encryption keys per device
- Authentication: Multi-factor authentication for key access

3. DATA TRANSMISSION SECURITY

3.1 Email Communication Encryption

CURRENT STATE: Client communications currently use standard email without encryption protection.

REGULATORY REQUIREMENT: IRS Publication 4557 Section 3.2 requires encrypted transmission of taxpayer information. FTC Safeguards Rule mandates secure transmission of customer data.

GAP REMEDIATION PLAN:
- Phase 1 (by March 1, 2026): Implement encrypted email solution (ProtonMail Business or Microsoft 365 with encryption)
- Phase 2 (by March 15, 2026): Train all staff on encrypted email protocols
- Phase 3 (by March 15, 2026): Establish client communication procedures requiring encryption for all tax-related correspondence

COMPENSATING CONTROLS: Until encrypted email implementation, sensitive client information is not transmitted via email, and phone communication is used for urgent matters requiring data exchange.

3.2 File Transfer Security
When implemented, all electronic file transfers will use:
- Protocol: TLS 1.3 encryption minimum
- Authentication: Password protection and user verification

- Logging: All transfers recorded with timestamps

4. BACKUP SYSTEM SECURITY

4.1 Current Backup Enhancement

CURRENT STATE: Data backups currently utilize external drive storage only, creating single point of failure risk.

REGULATORY REQUIREMENT: FTC Safeguards Rule requires comprehensive data protection including secure backup procedures to prevent data loss.

PARTIAL COMPLIANCE - UPGRADE COMMITMENT:
By March 30, 2026, Riverside Accounting will implement a dual backup system combining local encrypted external drives with secure cloud backup service, ensuring redundant protection and meeting FTC requirements for data availability and protection.

4.2 Enhanced Backup Requirements (Effective March 30, 2026)
- Frequency: Daily automated backups during non-business hours
- Encryption: AES-256 encryption for all backup data
- Storage: Combination of encrypted local drives and SOC 2 Type II certified cloud service
- Testing: Monthly backup restoration testing
- Retention: 7-year retention per IRS requirements

5. ACCESS CONTROLS & KEY MANAGEMENT

5.1 User Authentication
All encrypted systems require:
- Primary Authentication: Unique username and complex password
- Secondary Authentication: Multi-factor authentication via mobile app or hardware token
- Session Management: Automatic timeout after 30 minutes of inactivity

5.2 Encryption Key Management
- Key Storage: Hardware security modules or certified key management systems
- Key Rotation: Annual key rotation for all systems
- Key Recovery: Secure key escrow procedures for business continuity
- Access Logging: All key access events logged and monitored

6. INCIDENT RESPONSE PROCEDURES

6.1 Data Breach Response
In case of suspected encryption failure or data exposure:
1. Immediate Action: Isolate affected systems within 1 hour
2. Assessment: Determine scope of potential data exposure within 24 hours

3. Notification: Report to IRS and affected clients per regulatory requirements
4. Remediation: Implement corrective measures and strengthen controls

6.2 Monitoring and Auditing
- Daily: Automated encryption status monitoring
- Weekly: Access log review and analysis
- Quarterly: Comprehensive security assessment
- Annually: Full encryption policy review and update

7. COMPLIANCE MONITORING

7.1 Regular Assessments
- Monthly: Encryption system functionality verification
- Quarterly: Staff compliance training and testing
- Annually: Third-party security assessment
- As Needed: Policy updates based on regulatory changes

7.2 Documentation Requirements
All encryption-related activities will be documented including:
- Implementation timelines and milestones
- Staff training completion records
- System testing and validation results
- Incident response actions and outcomes

Policy Review Date: January 2027
Next Update: As required by regulatory changes or security incidents

Authorized by:
[Signature Block for Riverside Accounting Principal]
Date: _

This policy is designed for compliance with IRS Publication 4557, FTC Safeguards Rule 16 CFR Part 314, and California state data protection requirements. Regular updates ensure continued regulatory alignment.

Employee Security & Training

EMPLOYEE SECURITY & TRAINING POLICY

Riverside Accounting - California
Effective Date: January 1, 2026
Document Classification: WISP Section 4

COMPLIANCE STATUS SUMMARY

1. SCOPE AND APPLICABILITY

This Employee Security & Training Policy applies to all personnel at Riverside Accounting who have access to Federal Tax Information (FTI) and client data systems. Given our firm size of 2-5 employees with 2-3 employees having client data access, this policy establishes mandatory security requirements for all staff members.

2. BACKGROUND CHECK REQUIREMENTS

CURRENT STATE: Riverside Accounting does not currently conduct background checks on new hires who will handle taxpayer data.

REGULATORY REQUIREMENT: IRS Publication 4557 Section 4.3.2 recommends background investigations for employees with access to FTI, stating "Consider conducting background investigations on employees who will have access to FTI."

GAP REMEDIATION PLAN:
- By February 15, 2026: Establish partnership with approved background check provider
- By March 1, 2026: Implement background check requirement for all new hires
- By March 31, 2026: Complete background checks for current employees handling client data
- Background checks must include criminal history, employment verification, and reference checks

COMPENSATING CONTROLS: Until background check program is implemented:
- All new hires undergo 30-day probationary period with enhanced supervision
- Client data access limited to essential functions only during probationary period
- Daily review of system access logs for new employees

3. SECURITY AWARENESS TRAINING REQUIREMENTS

Initial Training Requirements

CURRENT STATE: Employees do not receive formal security training upon hire or at any point during employment.

REGULATORY REQUIREMENT: FTC Safeguards Rule 16 CFR 314.4(c) requires "regular training of employees regarding the security measures" and IRS Publication 4557 mandates security awareness training for all personnel with FTI access.

GAP REMEDIATION PLAN:
- By January 31, 2026: Develop comprehensive security training curriculum
- By February 28, 2026: Conduct initial security training for all current employees
- Effective March 1, 2026: All new hires must complete security training within first week of employment

COMPENSATING CONTROLS: Until formal training program is established:
- Employees receive verbal security briefing covering password requirements and data handling
- Written security guidelines provided to all staff
- Weekly security reminders via email

Ongoing Training Requirements

CURRENT STATE: No ongoing security training program exists.

REGULATORY REQUIREMENT: Annual security training is required under FTC Safeguards Rule and IRS Publication 4557 guidelines.

GAP REMEDIATION PLAN:
- Annual security training mandatory for all employees beginning April 2026
- Training must cover: phishing awareness, password security, physical security, incident reporting
- Training completion tracking and documentation required

COMPENSATING CONTROLS: Until annual training program is operational:
- Monthly security tips distributed to all staff
- Quarterly security discussions during team meetings

4. ACCEPTABLE USE POLICY

All employees with system access must comply with the following acceptable use requirements:

- System Access: Limited to authorized business purposes only
- Password Requirements: Minimum 12 characters, unique passwords, changed every 90 days
- Data Handling: Client data may only be accessed, processed, and stored according to firm procedures
- Personal Use: Minimal personal use permitted during breaks, subject to all security controls
- Software Installation: Prohibited without IT approval
- Email Security: All attachments and links must be verified before opening
- Physical Security: Workstations must be locked when unattended, documents secured

5. WISP ACKNOWLEDGMENT REQUIREMENTS

All employees must:
- Read and acknowledge receipt of complete WISP within first week of employment
- Sign annual WISP acknowledgment confirming understanding of security obligations
- Report suspected security incidents immediately to firm management
- Acknowledge understanding that security violations may result in disciplinary action up to and including termination

Acknowledgment Documentation Required:
- Initial WISP receipt acknowledgment (within 5 days of hire)
- Annual policy review acknowledgment (due each January)
- Training completion certificates
- Incident reporting acknowledgments

6. CONTRACTOR AND SEASONAL STAFF SECURITY

Status: Not applicable - Riverside Accounting confirmed no use of contractors or seasonal staff.

Should the firm engage contractors or seasonal workers in the future, they will be subject to the same security requirements as permanent employees, including background checks, training, and WISP acknowledgment.

7. TERMINATION AND OFFBOARDING PROCEDURES

CURRENT STATE: Riverside Accounting does not have a formal termination and offboarding process for departing employees.

REGULATORY REQUIREMENT: IRS Publication 4557 Section 4.5 requires "procedures for terminating employee access to FTI and related systems" and FTC Safeguards Rule requires prompt revocation of access rights upon termination.

GAP REMEDIATION PLAN:
- By February 15, 2026: Develop and implement formal offboarding checklist
- Effective immediately: All employee terminations require same-day access revocation
- By March 1, 2026: Create system for tracking and documenting all offboarding activities

COMPENSATING CONTROLS: Until formal offboarding process is implemented:
- IT passwords changed immediately upon employee departure notification
- Physical office keys and equipment retrieved same day
- Manual review of all system access within 24 hours of termination

Required Offboarding Steps:
- Immediate revocation of all system access and passwords
- Collection of all firm property including keys, devices, and documents
- Review and secure any pending client files or projects

- Documentation of offboarding completion with signatures and dates
- Exit interview addressing confidentiality obligations

8. DISCIPLINARY ACTIONS FOR SECURITY VIOLATIONS

Security violations will result in progressive disciplinary action:

Minor Violations (password policy, workstation security):
- First offense: Verbal warning and retraining
- Second offense: Written warning
- Third offense: Performance improvement plan

Major Violations (unauthorized data access, policy violations compromising client data):
- First offense: Written warning and mandatory retraining
- Second offense: Suspension without pay
- Third offense: Termination

Severe Violations (data theft, intentional security breaches):
- Immediate termination and potential legal action

All disciplinary actions will be documented and maintained in employee files.

9. POLICY REVIEW AND UPDATES

This policy will be reviewed annually and updated as needed to maintain compliance with evolving regulations. Next scheduled review: January 2027.

Document Control:
Version: 1.0
Approved By: [Firm Owner/Managing Partner]
Date: January 1, 2026
Next Review: January 1, 2027

Physical Security

PHYSICAL SECURITY POLICY

COMPLIANCE STATUS SUMMARY

1. OFFICE ACCESS CONTROLS

1.1 Physical Access Management
Riverside Accounting maintains secure access controls for our private office suite through a multi-layered approach:

- Primary Access: Office suite is secured with commercial-grade locks and protected by our monitored security alarm system
- Key Management: Physical keys are issued only to authorized personnel with documented key holder registry maintained
- Access Monitoring: Security alarm system provides 24/7 monitoring and immediate alert capabilities for unauthorized access attempts

1.2 After-Hours Security
- Security alarm system is activated during all non-business hours
- Last employee leaving must verify alarm activation and secure all entry points
- Emergency contact procedures are established with security monitoring service

2. VISITOR MANAGEMENT

2.1 Client Visit Procedures
Given that clients regularly visit our office, Riverside Accounting implements the following visitor management protocols:

- Reception Protocol: All visitors must check in at reception and state purpose of visit
- Escort Requirements: Clients are escorted to designated meeting areas and not permitted unaccompanied access to work areas containing confidential information
- Visitor Log: Maintain written record of all visitors including name, company, purpose, time in/out, and employee contact
- Confidential Area Restrictions: Work areas containing FTI and client files are off-limits to all visitors

2.2 Non-Client Visitors
- Service providers and vendors must be scheduled in advance and escorted at all times
- Delivery personnel are restricted to reception area only
- Visitor badges or identification must be worn when provided

3. WORKSTATION SECURITY

3.1 Physical Workstation Protection
- Screen Positioning: Computer monitors are positioned to prevent unauthorized viewing from public areas, doorways, or windows
- Automatic Screen Locks: All workstations are configured with automatic screen locks activating after 15 minutes of inactivity
- Manual Locking: Employees must manually lock screens when leaving workstation unattended
- Privacy Screens: Privacy filters are utilized on monitors in areas where shoulder surfing risks exist

3.2 Workstation Environment
- Workstations are positioned away from high-traffic areas and visitor sight lines
- Cable management ensures no tripping hazards or equipment damage risks
- Adequate lighting is maintained to prevent eye strain and security monitoring

4. DOCUMENT STORAGE AND HANDLING

4.1 Physical Document Security
Riverside Accounting maintains robust document security through our established locked filing cabinet system:

- Secure Storage: All client documents, FTI, and confidential materials are stored in locked filing cabinets when not in active use
- Access Control: Filing cabinet keys are restricted to authorized personnel only
- Document Classification: Files are organized by sensitivity level with appropriate storage locations assigned
- Retention Management: Document retention schedule is maintained with secure disposal procedures for expired materials

4.2 Document Handling Procedures
- Documents containing FTI are never left unattended on desks or work surfaces
- Confidential materials are transported in sealed envelopes or locked containers
- Copy/print operations involving sensitive data require immediate retrieval and verification

5. CLEAN DESK POLICY

5.1 Daily Workspace Requirements
Riverside Accounting enforces a comprehensive clean desk policy to protect confidential information:

- End-of-Day Protocol: All documents, files, and materials must be secured in locked storage before leaving the office
- Active Work Management: Only documents currently being worked on may remain on desk surfaces during business hours
- Electronic Media: USB drives, CDs, and portable storage devices must be secured in locked storage when not in use
- Client Information: No client names, SSNs, or FTI may be visible on desk surfaces, whiteboards, or

computer screens when workstation is unattended

5.2 Compliance Monitoring
- Daily compliance checks are performed by designated security officer
- Monthly clean desk audits document adherence and identify improvement areas
- Employee training on clean desk procedures is conducted annually

6. DEVICE SECURITY

6.1 Laptop and Mobile Device Controls
- Physical Security: Laptops are secured with cable locks when used in office environment
- Transport Security: Mobile devices and laptops are kept in locked vehicles or carried personally when transported
- Storage Requirements: After-hours device storage in locked, secure locations within the office
- Access Controls: All devices require password/PIN authentication with automatic lock features enabled

6.2 Personal Device Management
- Personal devices are prohibited from accessing firm networks or client data
- Bring-Your-Own-Device (BYOD) policies restrict personal device use for business purposes
- Client information may not be stored on or accessed through personal devices

7. HOME OFFICE SECURITY (WHEN APPLICABLE)

7.1 Remote Work Environment
When employees work from home offices, the following security requirements apply:

- Physical Security: Home office space must be in a private area not accessible to family members or visitors
- Document Handling: Physical documents may not be taken to home offices without specific authorization
- Equipment Security: Firm-issued equipment must be stored securely when not in use
- Network Security: Home internet connections must meet firm security standards with VPN requirements for all business access

7.2 Home Office Compliance
- Home office security assessments are conducted before remote work approval
- Regular compliance verification through virtual security reviews
- Incident reporting procedures for any home office security breaches

8. INCIDENT RESPONSE AND REPORTING

8.1 Physical Security Incidents
- All physical security breaches must be reported immediately to the designated security officer
- Incident documentation includes time, location, nature of incident, and potential data exposure
- Client notification procedures are followed when FTI may have been compromised

8.2 Emergency Procedures
- Emergency contact information is maintained for all security systems
- Business continuity plan addresses physical security during emergencies
- Backup procedures ensure continued protection of confidential information during disruptions

Document Control
- Version: 2026.1
- Effective Date: January 1, 2026
- Review Cycle: Annual
- Next Review: January 1, 2027
- Approved By: [Principal Name]
- Date Approved: [Date]

This policy meets IRS Publication 4557 requirements for physical security safeguards.

Third-Party Vendor Management

THIRD-PARTY VENDOR MANAGEMENT POLICY

COMPLIANCE STATUS SUMMARY
Riverside Accounting - Third-Party Vendor Management
Assessment Date: January 2026

Status Legend
- [x] Compliant: Policy implemented and operational
- In Progress: Implementation underway with target completion date
- Gap: Requires immediate attention with remediation deadline

Current Compliance Status
- [x] Vendor Security Review Process: Active security practice assessments implemented
- [x] Written Vendor Agreements: Contractual data protection requirements in place

1. VENDOR SECURITY ASSESSMENT REQUIREMENTS

Riverside Accounting maintains comprehensive security assessment protocols for all third-party vendors handling client tax information and financial data. The firm conducts thorough security evaluations before engaging new vendors and performs ongoing assessments of existing vendor relationships.

Initial Security Assessment Process
All prospective vendors undergo mandatory security assessments that evaluate:
- Data encryption capabilities (both in transit and at rest)
- Access control mechanisms and user authentication protocols
- Physical security measures for data centers and facilities
- Incident response procedures and breach notification protocols
- Compliance with relevant regulatory standards (SOC 2, ISO 27001, etc.)
- Data backup and disaster recovery capabilities
- Employee background check requirements and security training programs

Risk Classification Framework
Vendors are classified into risk categories based on their access to client data:
- High Risk: Direct access to client tax returns, financial records, or personally identifiable information
- Medium Risk: Limited access to client data or systems that could impact data security
- Low Risk: No direct access to client data but providing services that could affect overall security posture

2. DUE DILIGENCE CHECKLIST FOR NEW VENDORS

Prior to engaging any new vendor, Riverside Accounting completes a comprehensive due diligence process that includes:

Documentation Requirements
- Current cybersecurity certifications and compliance attestations
- Detailed security policies and procedures documentation
- Insurance coverage verification (cyber liability and errors & omissions)
- Financial stability assessment and business continuity planning
- References from other accounting firms or similar professional services clients

Technical Evaluation
- Penetration testing results and vulnerability assessments
- Data encryption standards and key management procedures
- Multi-factor authentication implementation
- Network security architecture documentation
- Software development lifecycle security controls (for software vendors)

Legal and Regulatory Compliance
- Evidence of compliance with applicable state and federal regulations
- Data processing agreements and privacy policy review
- Subcontractor and fourth-party vendor disclosure
- Jurisdiction and data residency confirmations

3. REQUIRED CONTRACTUAL SECURITY PROVISIONS

All vendor agreements include mandatory security provisions that protect client information and ensure regulatory compliance. These contractual requirements address data protection, incident response, and vendor accountability.

Data Protection Clauses
Vendor contracts specify:
- Permitted uses and limitations on client data processing
- Data encryption requirements meeting current industry standards
- Prohibition on unauthorized data sharing or disclosure
- Employee access restrictions and need-to-know principles
- Secure data transmission protocols for all client information exchanges

Security Standards and Compliance
Contracts require vendors to:
- Maintain appropriate cybersecurity frameworks and controls
- Provide annual security assessment reports or certifications
- Comply with all applicable privacy and data protection laws
- Submit to periodic security audits as requested by the firm
- Maintain cyber liability insurance coverage with specified minimum limits

Incident Response and Notification
Vendor agreements mandate:

- Immediate notification of security incidents involving client data (within 24 hours)
- Detailed incident reporting including scope, cause, and remediation actions
- Cooperation with firm's incident response procedures
- Forensic investigation support when required
- Documentation preservation for regulatory reporting purposes

4. ONGOING VENDOR MONITORING PROCEDURES

Riverside Accounting implements continuous monitoring of vendor security posture and performance through regular assessments and communication protocols.

Regular Security Reviews
The firm conducts:
- Annual security questionnaires for all vendors handling client data
- Quarterly check-ins with high-risk vendors regarding security updates
- Review of vendor security certifications and compliance attestations
- Assessment of any material changes to vendor security practices or infrastructure

Performance Monitoring
Ongoing vendor oversight includes:
- Service level agreement compliance tracking
- Data breach and incident history monitoring
- Financial stability and business continuity assessment
- Client satisfaction and service quality evaluation

Documentation and Record Keeping
All vendor monitoring activities are documented through:
- Vendor risk assessment databases with current security status
- Communication logs for security-related discussions
- Compliance certificate and attestation filing systems
- Incident tracking and resolution documentation

5. DATA SHARING LIMITATIONS WITH VENDORS

Strict data sharing protocols govern all vendor relationships to ensure client information protection and regulatory compliance.

Data Minimization Principles
Vendors receive only the minimum data necessary to perform contracted services:
- Client information sharing limited to specific business purposes
- Temporary data access provisions with automatic expiration dates
- Segregation of client data by engagement or service type
- Regular review and purging of unnecessary data holdings

Access Control Requirements
Data sharing arrangements include:
- Role-based access controls limiting vendor employee access
- Multi-factor authentication for all vendor system access
- Session monitoring and logging for data access activities
- Geographic and IP-based access restrictions where appropriate

Data Processing Limitations
Contracts specify strict limitations on vendor data processing:
- Prohibition on data mining or analysis beyond contracted services
- Restrictions on combining client data with other datasets
- Limitations on data retention periods and deletion requirements
- Prohibition on using client data for vendor's own business purposes

6. VENDOR INCIDENT NOTIFICATION REQUIREMENTS

Comprehensive incident notification protocols ensure rapid response to security events and maintain regulatory compliance obligations.

Immediate Notification Procedures
Vendors must provide immediate notification (within 24 hours) for:
- Suspected or confirmed data breaches involving client information
- Unauthorized access attempts to systems containing client data
- Malware infections or security compromises affecting client data
- Physical security incidents at vendor facilities storing client information
- System outages or disruptions affecting data availability or integrity

Incident Reporting Requirements
Detailed incident reports must include:
- Timeline of the security incident from detection to containment
- Scope and nature of compromised client information
- Root cause analysis and contributing factors
- Immediate containment and remediation actions taken
- Long-term corrective measures to prevent recurrence

Communication Protocols
Incident notification procedures specify:
- Primary and secondary contact methods for emergency communications
- Escalation procedures for senior management notification
- Client notification timelines and communication responsibilities
- Regulatory reporting coordination and documentation requirements
- Media response and public communication protocols

7. VENDOR TERMINATION AND DATA RETURN PROCEDURES

Secure vendor termination procedures ensure complete data recovery and destruction while maintaining client confidentiality throughout the process.

Data Return Requirements
Upon contract termination or expiration:
- Complete return of all client data in agreed-upon formats within 30 days
- Secure deletion of client data from all vendor systems and backups
- Certificate of data destruction from vendor's senior management
- Return or secure destruction of physical documents and storage media
- Removal of client data from vendor disaster recovery and archive systems

System Access Termination
Vendor termination procedures include:
- Immediate revocation of all system access credentials and permissions
- Deactivation of vendor-specific user accounts and authentication tokens
- Removal of vendor personnel from facility access control systems
- Recovery of any firm-owned equipment, software licenses, or access devices
- Documentation of all access termination activities and confirmations

Transition Planning
Orderly vendor transitions require:
- Detailed handover documentation for replacement vendors
- Client data transfer protocols maintaining confidentiality and integrity
- Service continuity planning to minimize client disruption
- Final security assessment and compliance verification
- Legal review of termination compliance and outstanding obligations

Post-Termination Monitoring
Following vendor termination:
- Verification of complete data return and destruction within 60 days
- Monitoring for any unauthorized use or disclosure of former client data
- Final invoicing and contract closure documentation
- Lessons learned analysis for future vendor selection and management
- Client notification of vendor changes affecting their services

Policy Effective Date: January 1, 2026
Next Review Date: January 1, 2027
Policy Owner: [Designated Security Officer]
Approved By: [Managing Partner]

This policy is reviewed annually and updated as necessary to maintain compliance with evolving regulatory requirements and industry best practices.

Data Retention & Disposal

DATA RETENTION & DISPOSAL POLICY

COMPLIANCE STATUS SUMMARY

1. RECORD RETENTION REQUIREMENTS

1.1 Retention Periods by Document Type

Riverside Accounting maintains comprehensive records in accordance with IRS requirements and professional standards:

Tax Returns and Supporting Documentation: 7 Years
- Original and amended tax returns (Forms 1040, 1120, 1065, 1041, etc.)
- Supporting schedules and attachments
- Electronic filing acknowledgments and confirmations
- Client-provided source documents and substantiation

Workpapers and Client Files: 7 Years
- Tax preparation worksheets and calculations
- Research memoranda and tax position documentation
- Client correspondence and communication records
- Engagement letters and fee agreements

Business Records: 7 Years
- Accounts receivable and billing records
- Professional liability insurance documentation
- Continuing education certificates and compliance records

1.2 Legal and Regulatory Framework

Our retention schedule complies with:
- IRC Section 6001 requiring taxpayer record retention
- California Business and Professions Code Section 5096
- IRS Circular 230 requirements for tax practitioners
- AICPA Code of Professional Conduct standards

2. SECURE DOCUMENT DESTRUCTION PROCEDURES

2.1 Paper Document Destruction

Riverside Accounting employs cross-cut shredding for all confidential paper documents containing client information. Our procedures ensure:

- Cross-Cut Shredding Standard: All documents are destroyed using cross-cut shredders that produce particles no larger than 1/32" x 1/2" (Level P-4 security)
- Immediate Destruction: Documents are shredded immediately upon reaching retention expiration
- Supervised Process: Document destruction is conducted under direct supervision of authorized personnel
- Witness Requirements: Two authorized employees must witness destruction of highly sensitive documents

2.2 Certificate of Destruction

For each destruction event, we maintain certificates documenting:
- Date of destruction
- Types and volume of documents destroyed
- Method of destruction employed
- Names of witnessing personnel
- Signature of responsible party

3. ELECTRONIC DATA DESTRUCTION

3.1 Professional Hardware Disposal

Riverside Accounting utilizes professional data destruction services for all computer hardware and storage devices. Our process ensures:

NIST 800-88 Compliance: All electronic media sanitization follows NIST Special Publication 800-88 Rev. 1 guidelines for secure data destruction.

Professional Service Requirements:
- Certified data destruction vendor selection
- On-site or secure facility destruction options
- NIST-compliant sanitization methods (purging/destroying)
- Certificate of destruction for each device
- Chain of custody documentation

3.2 Data Sanitization Standards

Hard Disk Drives: Physical destruction or cryptographic erasure meeting NIST standards
Solid State Drives: Cryptographic erasure or physical destruction due to wear-leveling concerns
Mobile Devices: Factory reset followed by cryptographic wiping
Backup Media: Physical destruction or cryptographic overwriting

4. CLIENT DATA DELETION PROCEDURES

4.1 Client Request Process

Riverside Accounting maintains established procedures for handling client data deletion requests:

Request Documentation: All deletion requests are documented in writing with client signature and date
Verification Process: Client identity verification before processing any deletion request
Retention Override: Legal and regulatory retention requirements supersede client deletion requests
Scope Definition: Clear documentation of which data will be deleted vs. retained for compliance

4.2 Deletion Implementation

Electronic Records: Secure deletion using NIST-approved sanitization methods
Paper Records: Cross-cut shredding following standard destruction procedures
Backup Systems: Verification that deleted data is removed from all backup systems
Completion Certificate: Written confirmation provided to client upon deletion completion

5. RETENTION SCHEDULE MANAGEMENT

5.1 Documentation and Tracking

Annual Review Process: Retention schedules are reviewed annually in January for accuracy and compliance
Client File Indexing: Each client file includes creation date, retention period, and scheduled destruction date
Destruction Calendar: Monthly calendar maintained identifying files eligible for destruction
Compliance Monitoring: Regular audits ensure adherence to established retention periods

5.2 Storage and Access Controls

Physical Security: Paper records stored in locked filing cabinets with restricted access
Environmental Protection: Climate-controlled storage areas protecting document integrity
Electronic Security: Digital records protected with encryption and access controls
Inventory Management: Regular inventory of retained records ensuring complete accountability

6. POLICY COMPLIANCE AND MONITORING

6.1 Training and Awareness

All Riverside Accounting personnel receive annual training on:
- Record retention requirements and schedules
- Proper document destruction procedures
- Client confidentiality obligations
- Data security best practices

6.2 Policy Updates and Review

This policy is reviewed annually and updated as necessary to reflect:
- Changes in federal and state regulations
- Updates to professional standards
- Technological advancement in data destruction
- Client service requirements and industry best practices

Policy Effective Date: January 1, 2026
Next Review Date: January 1, 2027
Responsible Party: [Managing Partner/Office Manager]
Approved By: [Firm Principal Signature]

2026 WISP Acknowledgment & Approval

This 2026 Written Information Security Plan has been reviewed and approved for implementation at Riverside Accounting.

WISP Version: 2026

This document covers the 2026 compliance year. Per IRS guidelines, annual review is required.

Designated Security Coordinator:

_____ _____

Signature Date

Firm Principal / Owner:

_____ _____

Signature Date

Annual Review Schedule

Per IRS Publication 4557, this WISP must be reviewed and updated at least annually, or whenever there is a material change to business operations or security practices.

Next Review Due: January 1, 2027

To update your WISP for 2027, visit wisp-creator.com