CYBERSECURITY POLICY MANUAL

Mikel Wealth Management, LLC
Effective Date: January 26, 2026
Last Revised: January 26, 2026
Next Review Date: January 24, 2027
Chief Compliance Officer: Cindy A. Mikel
Contact: 210-569-2805 | cindy@mikelwealthmanagement.com

1. PURPOSE AND SCOPE

This Cybersecurity Policy establishes procedures to protect Mikel Wealth Management, LLC's client data, confidential information, and business operations from cyber threats and unauthorized access.
Regulatory Requirements: This policy implements TSSB Item 17 (Privacy Policy) and addresses SEC Regulation S-P (Safeguards Rule) requirements for investment advisers handling nonpublic personal information.

Covered Information:

- Client personal and financial information (names, SSN, addresses, account data)
- Investment recommendations and strategies
- Firm confidential information (proprietary processes, financial records)
- Employee information (payroll, personnel files)

Applies To:

- Cindy A. Mikel (Owner, President, CCO, IAR)
- Sonja R. Miller (Secretary, Administrative Support)
- All contractors, consultants, and third-party service providers
- All devices and systems accessing firm information

2. INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Chief Compliance Officer (Cindy A. Mikel)

Responsibilities:

- Establish and maintain cybersecurity policies and procedures
- Conduct annual risk assessments
- Approve security tools and implementations
- Review and respond to security incidents
- Ensure regulatory compliance
- Coordinate with third-party security vendors
- Report cybersecurity status quarterly
- Maintain documentation of security activities and incidents

Administrative Support (Sonja R. Miller)

Responsibilities:

- Follow all access control and security policies
- Report suspected security incidents immediately to CCO
- Complete annual security awareness training
- Protect client and firm confidential information
- Use secure methods for handling and transmitting data
- Maintain physical security of office and documents

3. DATA PROTECTION AND ACCESS CONTROL

Data Classification

Level 1 - Confidential (Highest):

- Client personal financial information (SSN, account numbers, holdings)
- Client investment strategies and recommendations
- Fee schedules and pricing information
- Security credentials and passwords

Handling Requirements:

- Encryption required for storage and transmission
- Access restricted to authorized personnel only
- Printed documents locked in secured cabinet
- Secure shredding when destroyed
- No external sharing without written client authorization

Level 2 - Internal Confidential:

- Internal policies and procedures
- Employee records and payroll information
- Vendor contracts and pricing

Handling Requirements:

- Password protection or encryption recommended
- Access limited to relevant personnel
- Secure storage and standard destruction procedures

Multi-Factor Authentication (MFA)

MFA is required for all critical accounts:

- Email (Microsoft Outlook 365)
- Cloud storage (ShareFile)
- Banking and custodial account access
- Any remote access or VPN connections

Implementation:

- MFA enabled using Microsoft Authenticator, SMS, or hardware token
- MFA recovery codes printed and stored securely
- Alternative authentication method maintained if primary fails
- MFA credentials never shared between users

Password Policy

Password Requirements for All Users:

- Minimum 14 characters
- Include uppercase letters, lowercase letters, numbers, and special characters
- No dictionary words or common phrases
- Changed every 90 days
- Changed immediately if suspected compromise
- Automatic account lockout after 10 failed login attempts

Password Management:

- Passwords stored in password manager or encrypted file
- Master password stored in secure location accessible only to authorized personnel
- Never share passwords via email, phone, or chat
- Never write passwords on post-it notes or unsecured documents

Session Management

Timeout and Security:

- Automatic logout after 15 minutes of inactivity for devices with client data access
- Manual logout required before leaving workstation
- All files closed and saved before logout
- VPN connections terminated when session ends

4. SECURE DATA HANDLING AND STORAGE

ShareFile for Document and File Management

All documents, files, and encrypted messages containing sensitive information are managed through ShareFile:

ShareFile Security Requirements:

- All client files and confidential documents stored in ShareFile
- End-to-end encryption for sensitive file sharing
- Encrypted messages for transmitting personal or financial information
- Access permissions set to minimum necessary level
- File access logs maintained
- Shared files have expiration dates when possible
- External sharing disabled except when necessary with password protection

File Handling Procedures:

- Never email Level 1 Confidential information (client SSN, account numbers, strategies)
- Use ShareFile encrypted messages for sensitive client communications
- Confirm recipient before sharing sensitive files
- Include security disclaimer for ShareFile links containing confidential information
- Re-verify recipients before sending sensitive information

Email Security (Microsoft Outlook 365)

Email Access Security:

- Multi-factor authentication required for all email login
- Session timeout after 30 minutes of inactivity
- Suspicious login alerts enabled
- Email forwarding restricted to known addresses only
- External email warnings applied to messages from outside firm

Email Best Practices:

- Never send Level 1 Confidential information via standard email
- Use ShareFile encrypted messages instead of email for sensitive data
- Digital signatures enabled for client communications
- Do not click links in unsolicited emails
- Do not open attachments from unknown senders
- Report suspicious emails to CCO immediately

Cloud Storage and Backup

ShareFile Cloud Storage:

- Used for all client files, firm documents, and collaborative work
- Encryption enabled by default
- Access permissions restricted
- File access tracking enabled
- Automatic versioning and recovery capabilities

Backblaze Backup Storage:

- Used for automated backup of critical files and systems
- Encryption in transit and at rest
- Automated daily backup schedule
- Tested restoration procedures quarterly
- Backup integrity verified monthly
- Off-site storage for disaster recovery

Physical Document Security

Office Document Storage:

- Client files stored in locked metal filing cabinets
- Filing cabinet keys held only by CCO
- Sensitive documents stored in locked drawer
- No client files left on desks overnight
- Confidential documents printed only when necessary
- Visitors not allowed in file areas unescorted

Document Destruction:

- Commercial shredding service for confidential documents (cross-cut shredding)
- Certificate of destruction obtained from shredding service
- Destruction log maintained with dates and quantities
- Destruction authorized by CCO
- Hard drives: Certified destruction service
- Destruction frequency: Monthly or as retention limits reached

---

5. INCIDENT RESPONSE AND BREACH NOTIFICATION

Cyber Incident Definition

Reportable Incidents Include:

- Unauthorized access to systems or data
- Suspected or confirmed data breach
- Malware infection or ransomware attack
- Loss or theft of devices containing client data
- Accidental disclosure of confidential information
- Phishing attack resulting in credential compromise
- System failure affecting client data availability

Incident Response Procedure

Step 1: Detection and Reporting (Immediate)

- Any employee discovering incident reports to CCO immediately
- Emergency contact: Cindy Mikel at 210-569-2805
- Verbal report followed by email documentation within 1 hour
- Do NOT investigate or attempt to fix on own initiative

Step 2: Containment (Within 1-2 Hours)

- CCO isolates affected systems from network if necessary
- Affected user accounts disabled or password reset
- Charles Schwab custodian contacted if custodial systems affected
- Preserve evidence: Maintain system logs and screenshots
- Continue operations on unaffected systems

Step 3: Investigation (Within 24 Hours)

- Determine scope: What systems and data affected?
- Determine cause: How did incident occur?
- Determine timeline: When did it start and duration?
- Identify affected individuals: Which clients impacted?
- Document findings in Incident Report

Step 4: Client Notification (Within 24-72 Hours)

- If client personal information potentially affected, notify clients
- Notification includes: description of incident, information affected, mitigating steps, client protective actions, CCO contact information

Step 5: Regulatory Notification (As Required)

- SEC notification if required (substantial damage to client interests)
- Texas Board notification if required by state regulations
- Charles Schwab notification if custodial systems affected
- Law enforcement notification if criminal activity suspected

Step 6: Recovery and Remediation (Days/Weeks)

- Restore systems from clean backups (Backblaze verified backups)
- Patch vulnerabilities that allowed incident
- Update security controls to prevent recurrence
- Provide client credit monitoring if identity theft risk
- Document all remediation actions taken

Step 7: Post-Incident Review (Within 30 Days)

- Conduct incident post-mortem with CCO
- Identify root causes and contributing factors
- Evaluate effectiveness of response procedures
- Update incident response procedures if needed
- Communicate lessons learned to staff
- Update annual risk assessment based on incident

Incident Documentation

Incident Report Contents:

- Date and time of detection
- Description of incident
- Systems and data affected
- Number of clients potentially impacted
- Root cause analysis
- Containment and remediation actions taken
- Client notification timeline
- Regulatory notifications made
- Lessons learned and preventive measures

Records Retention:

- Incident reports maintained for minimum 5 years
- Reports stored in secure, encrypted ShareFile folder
- Access limited to CCO and authorized personnel

---

6. THIRD-PARTY SERVICE PROVIDER SECURITY

Critical Service Providers

Primary Service Providers:

Service	Provider	Security Standard
Custodian	Charles Schwab & Co.	SSAE 16 SOC 2 Type II, MFA, Encryption
Email/Cloud	Microsoft Office 365	SOC 2 Type II, ISO 27001, MFA, Encryption
Document Sharing	Citrix ShareFile	Encryption at rest/transit, Access controls
File Backup	Backblaze	AES-256 encryption, Automated daily backup
Email Hosting	Go Daddy	Standard security controls

Table 1: Primary Service Providers and Security Standards

Vendor Risk Assessment

Assessment Process:

- Evaluate vendor security practices and certifications
- Request security questionnaire or audit report
- Review vendor's privacy and security policies
- Verify professional liability and cyber insurance
- Check regulatory compliance and audit results
- Review data protection and encryption practices

Vendor Security Requirements

Contractual Obligations:

- Data security and confidentiality requirements
- Encryption in transit and at rest
- Access control and authentication requirements
- Audit rights and security audit access
- Incident notification and response requirements
- Compliance with applicable regulations (SEC Regulation S-P)

- Data retention and secure destruction procedures
- Prohibition on unauthorized data sharing or sale
- Business continuity and disaster recovery capabilities

Ongoing Vendor Monitoring

Annual Review:

- Assess vendor security changes or incidents
- Review vendor audit reports (SOC 2, ISO 27001)
- Verify compliance with contractual security obligations
- Evaluate vendor performance and responsiveness
- Determine if vendor relationship should continue

Incident Response:

- If vendor experiences security incident, request detailed incident information
- Request impact assessment on firm's data and remediation actions taken
- Evaluate need for incident notification to clients
- Consider terminating relationship if incident serious

---

7. EMPLOYEE TRAINING AND COMPLIANCE

Mandatory Security Training

Initial Training (Upon Hire):

- All employees complete cybersecurity training before accessing systems
- Topics covered: Cybersecurity Policy, passwords/MFA, phishing/social engineering, confidential information handling, incident reporting, email security, physical security, mobile device security
- Training completion documented with employee signature
- Q&A session with CCO

Annual Refresher Training:

- Mandatory for all employees (January)
- Updated training covering policy changes, emerging threats, lessons learned from incidents, updated procedures, new tools/systems

Security Awareness Program

Monthly Awareness Communications:

- Monthly emails addressing security topics
- Topics rotated throughout year (passwords, phishing, physical security, data classification, incident reporting, social engineering, remote work, mobile security, data protection, vendor security, business continuity, policy updates)

Phishing Simulation Program:

- Quarterly simulated phishing emails sent to employees
- Educational purpose - no disciplinary action
- Results tracked to identify employees needing additional training

Employee Security Responsibilities

All Employees:

- Maintain password and MFA credential security
- Complete all mandatory training
- Comply with all security policies
- Report security incidents immediately to CCO
- Protect client and firm confidential information
- Use secure methods for handling data
- Lock workstation when away
- Participate in phishing simulations
- Escort and monitor office visitors

---

8. COMPLIANCE MONITORING AND AUDIT

Quarterly Compliance Review

Validation Checklist (Quarterly):

- All systems have current security patches
- Antivirus signatures are current
- Backups occurring and restorable (Backblaze verified)
- MFA enabled on critical accounts
- Encryption active on devices
- Physical security controls in place
- Staff have completed training
- Incident log maintained
- ShareFile access logs reviewed

Audit Documentation:

- Document checklist results
- Address any non-compliance items immediately
- Document remediation and timeline

Annual Security Audit

Timing: December 31 (concurrent with annual risk assessment)

Scope:

- Review of all cybersecurity controls
- Validation of policy compliance
- Vulnerability assessment results (if conducted)
- Incident history and trends
- Employee training completion
- Third-party vendor security status
- Business continuity plan effectiveness
- Data retention and destruction procedures

Audit Procedures:

1. Conduct comprehensive security assessment
2. Document findings in formal audit report
3. Identify gaps or non-compliance areas
4. Prioritize corrective actions
5. Develop remediation plan with target dates
6. Assign responsibility for corrections
7. Schedule follow-up to verify completion

Audit Documentation:

- Audit report maintained in secure ShareFile folder
- Report includes executive summary and detailed findings
- Remediation tracking with target completion dates
- Management sign-off on findings and action plans

Security Metrics and Reporting

Key Performance Indicators (KPIs):

- Number of security incidents by month/quarter/year
- Incident response time (detection to containment)
- Employee training completion rate (target: 100%)
- Phishing simulation click rate (target: <5% click, >95% report)
- System uptime and availability
- Backup restoration success rate (target: 100%)
- Third-party vendor security compliance rate

Quarterly Reporting:

- CCO prepares quarterly security status report
- Report includes KPIs, incidents, trends, and issues
- Report covers: incidents and status, compliance status, training/awareness activities, vendor status, action items

---

CONTACT INFORMATION AND ESCALATION

Security Concerns or Incidents:
Chief Compliance Officer: Cindy A. Mikel

- Office: 210-569-2805
- Email: cindy@mikelwealthmanagement.com

Reporting Channels:

- Employees report suspected security incidents immediately to CCO
- Anonymous reporting: Contact CCO verbally and request anonymity
- External reports: Clients can report security concerns to CCO

Escalation Procedures:

- Critical incidents (ongoing breach, ransomware): Contact CCO immediately by phone
- Significant incidents: Email within 1 hour with follow-up phone call
- Non-urgent concerns: Email within 24 hours

APPENDIX A: GLOSSARY OF CYBERSECURITY TERMS

Access Control: Restriction of user access to systems and data based on role and need-to-know principle
Authentication: Verification of user identity through passwords, MFA, or biometric methods
Backup: Copy of data and systems maintained for disaster recovery purposes
Breach: Unauthorized access to or theft of confidential or personal information
Encryption: Conversion of readable information into unreadable code to prevent unauthorized access
Firewall: Hardware or software device that controls network traffic between internal network and internet
Incident: Security event such as unauthorized access, data theft, malware infection, or system failure
Malware: Malicious software including viruses, worms, trojans, ransomware, and spyware
Multi-Factor Authentication (MFA): Requirement for multiple forms of verification (password + biometric + hardware token)
Phishing: Fraudulent emails or messages attempting to trick user into revealing sensitive information
Ransomware: Malware that encrypts files and demands payment for decryption
Vulnerability: Weakness in systems or applications that can be exploited by attackers
VPN (Virtual Private Network): Encrypted connection allowing secure remote access to firm networks

APPENDIX B: INCIDENT RESPONSE CONTACT LIST

Role	Name	Phone	Email
Chief Compliance Officer	Cindy A. Mikel	210-569-2805	cindy@mikelwealthmanagement.com
Administrative Support	Sonja R. Miller	972-XXX-XXXX	sonja@mikelwealthmanagement.com

Table 2: Internal Contacts

Service	Provider	Contact Phone
Custodian	Charles Schwab	1-866-855-7520
Email/Cloud	Microsoft	1-800-642-7676
Document Sharing	Citrix ShareFile	[Provider Support]
File Backup	Backblaze	[Provider Support]
Email Hosting	Go Daddy	[Provider Support]

Table 3: External Service Provider Contacts

DOCUMENT INFORMATION
Document Prepared By: Cindy A. Mikel, Chief Compliance Officer
Date Prepared: January 26, 2026
Effective Date: January 26, 2026
Next Review Date: January 24, 2027

ACKNOWLEDGMENT OF RECEIPT
I acknowledge that I have received and reviewed the Cybersecurity Policy Manual for Mikel Wealth Management, LLC, effective January 26, 2026. I understand and agree to comply with all policies and procedures outlined in this manual.
Employee Name: ____________________________

Employee Signature: __________________________

Date: __________________________

Witness/CCO Signature: __________________________