CYBERSECURITY OPERATIONS GUIDE

GRYPHIN ADVANTAGE

IMPLEMENTATION

PURPOSE

This guide moves beyond regulatory theory to provide a direct operational playbook. It is designed for immediate implementation, focusing exclusively on the practical procedures, tools, and policies required to secure your practice.

TIER 1: THE NON-NEGOTIABLE BASELINE (THE "BIG 3")

For the greatest and most immediate impact on your security posture, prioritize these three core actions. They are proven to mitigate over 90% of common attack vectors.

1. **Mandate Multi-Factor Authentication (MFA)**
   - **What it is:** A password + a second code (usually from a phone app).
   - **The Action:** Enable MFA on every single account that offers it. **No exceptions.**
   - **Priority List:**
     - Email
     - CRM
     - Custodial Platforms
     - Password Manager
   - **Policy:** Use an authenticator app over SMS (text messages). SMS is vulnerable to "SIM-swapping" attacks.

2. **Deploy a Business-Grade Password Manager**
   - **What it is:** A secure, shared vault for all practice passwords
   - **The Action:** Purchase a team plan. This is not the same as a free personal manager.
   - **Policy:**
     - Mandate Use: All passwords related to the practice must be stored in the manager.
     - Enforce Strength: Set the policy to require 16+ character, complex, unique passwords for all logins.
     - No Sharing: Credentials are never shared via email, text, or sticky note. Use the manager's secure "share" function.
     - Master Password: The one password to the manager must be incredibly strong and never written down.

3. **Implement a Secure File & Email Portal**
    - **What it is:** A secure, encrypted way to send and receive sensitive client documents (tax returns, account forms, statements).
    - **The Action:** Stop using email attachments for sensitive data. Subscribe to a dedicated portal (e.g., ShareFile, Encyro, or your CRM's built-in portal)
    - **Policy:**
        - "All transfer of PII (Personally Identifiable Information) or financial documents to or from a client must be conducted through the firm's approved secure portal."

TIER 2: HARDENING YOUR TECHNOLOGY (THE "TECH STACK")

This is how you lock down your actual hardware and network.

Workstation Security Policy (Laptops & Desktops)
This is a policy you create and have every employee (and yourself) sign.

- **Full-Disk Encryption: This is mandatory.**
    - Windows: Enable BitLocker (comes with Pro versions).
    - Mac: Enable FileVault.
    - This makes a lost or stolen laptop's data unreadable.
- **Use Standard User Accounts:**
    - No one, including the advisor, should use an "Administrator" account for daily work.
    - Action: Have your IT provider (or do it yourself) create a "Standard User" account for daily use. You only use the "Admin" account to install new software. This single step prevents most malware from installing itself.
- **Move Beyond Antivirus to EDR:**
    - Think of basic antivirus as a security guard with a list of known criminals. It only stops threats it already knows.
    - EDR (Endpoint Detection & Response) is smarter. It's like a detective that watches for suspicious behavior. Instead of just looking for known criminals, it stops anyone—even someone who looks innocent—if they suddenly try to pick a lock or break a window.
    - This is how EDR catches modern threats like ransomware, which often look like normal programs at first.
- **Aggressive Patch Management:**
    - Action: Enable automatic updates for your Operating System (Windows/macOS) and all third-party applications (Adobe, Zoom, web browsers). Out-of-date software is the main way hackers get in.
- **Enforce Screen Locks:**
    - Action: Set all workstations to automatically lock after 5-10 minutes of inactivity. This is a non-negotiable physical security control.

Network & Wi-Fi Security

- **Segment Your Network:**
  - Action: Your Wi-Fi router should have at least two networks:
    - [PracticeName]-Corporate: For employee laptops and practice devices ONLY.
    - [PracticeName]-Guest: For clients, employee personal phones, and all other "untrusted" devices.
- This prevents a compromised personal phone or client laptop from being on the same network as your sensitive data.

- **Mandate a VPN for All Remote Work:**
  - Action: All staff, including you, must use a Virtual Private Network (VPN) to connect to office resources when working remotely (e.g., from home, a hotel, or a coffee shop). This encrypts your entire connection.

TIER 3: BULLETPROOFING YOUR WORKFLOWS (THE "HUMAN FIREWALL")

Once technology controls are in place, you must secure your internal processes and workflows.

The "Do Not Pay" Wire & EFT Fraud Prevention Policy

This is your single most important financial process.

Subject: MANDATORY Procedure for All Fund Movement Requests

Treat all digital requests for client fund movements (via email, text, or social media) as fraudulent until positively verified.

- **ISOLATE:** Do not reply, click links, or forward the suspicious message.
- **CALL:** Initiate an outbound phone call to the client.
- **USE A KNOWN NUMBER:** You must use a verified phone number from your CRM or an original client file. DO NOT use any phone number provided in the new request's signature or body.
- **VERBALLY CONFIRM:** Speak live with the client and confirm these details:
  - "Did you send a request to move $[Amount]?"
  - "Please verbally confirm the full destination account number and institution name."
  - (Optional: Use a pre-arranged challenge question or passcode).
- **DOCUMENT:** After confirmation, log the call, date, time, and details in the CRM as an audit record.
- **FINAL RULE:** If you cannot speak live with the client, the transfer does not happen.
- **RED FLAGS:** A sense of urgency, an emotional appeal, or a last-minute change to instructions are classic indicators of fraud. There are no exceptions to this policy.

The Data Lifecycle Checklist

You are responsible for data from its creation to its destruction.

Step 1: Data Mapping (Know Where It Lives)
Create a simple spreadsheet. Where is your client PII?
Examples: CRM, custodian platform, email server (M365/Google), your laptop's "Downloads" folder, shared cloud drive, financial planning software, paper files.

Step 2: Data Minimization (Stop Collecting What You Don't Need)
Review your onboarding forms. Are you collecting information you don't actually need? Stop saving client tax returns to your local drive. Keep them in the secure portal or encrypted cloud.

Step 3: Set Retention & Destruction Timelines
Policy: "All client financial records will be retained for [X] years (e.g., 7 or 10) as required by regulators. After this period, the data will be securely destroyed."

Step 4: Secure Disposal (This is Critical)
Paper: All client documents are cross-cut shredded, not just thrown in the recycling.
Digital: Deleting a file is not enough.
When retiring an old computer, the hard drive must be physically destroyed or "securely wiped" using a data-erasure utility.
For cloud data, understand your vendor's "delete" function (e.g., "Empty the Trash").

TIER 4: THE NEXT LEVEL (HOW TO TEST YOUR DEFENSES)

Vendor Due Diligence: You inherit the risk of your vendors (CRM, cloud storage, etc.).

- Action: Before signing with a new tech vendor, ask for their SOC 2 Type II report. This is a standard third-party audit of their security controls. If they don't have one, or won't provide it, that is a major red flag.

Phishing Simulations:

- Action: Don't just tell your team about phishing; test them. Use a service to send safe, simulated phishing emails to your own team. This is the single best way to train them to spot a real attack.

Vulnerability Scanning:

- Action: Once a year, consider hiring an external IT security firm to run a vulnerability scan or penetration test against your practice. This is a "friendly hacker" who will find the holes in your security before a real attacker does.

This material is intended solely for licensed advisors affiliated with The Gryphin Advantage. It outlines general cybersecurity practices aligned with current industry and regulatory expectations. It is not a substitute for independent legal or IT guidance. Advisors remain individually responsible for ensuring that their technology, storage, and communication methods meet regulatory and carrier requirements.

GRYPHIN
ADVANTAGE

PROTECTING
CLIENT DATA
EVERY MESSAGE

GRYPHIN
ADVANTAGE

IMPLEMENTATION

PURPOSE

Email remains the #1 source of data breaches in financial services. This guide helps advisors ensure that all client communications meet privacy, carrier, and FSRA expectations.

CORE PRINCIPLES

Core Principle	What It Means	Examples
Encrypt when sending sensitive data	Use Microsoft 365 "Encrypt" or your secure email portal when sharing sensitive information, policy numbers, or banking info.	*"Send with Encryption" in Outlook before clicking Send.*
Never send unprotected attachments	Password-protect all PDFs containing personal or financial information.	*Use Adobe's "Encrypt with Password" feature or Windows' built-in "Compress + Encrypt."*
Verify before you send	Double-check recipient names and addresses. Autocomplete errors are the most common cause of privacy incidents.	*Type the first few letters manually; confirm before attaching files.*
Use secure file transfer for large documents	Prefer secure client portals, or carrier upload portals instead of email attachments.	*Upload the document, then share a time-limited link with "View only" permission.*

Core Principle	What It Means	Examples
Limit client data in subject lines	Never include names, policy numbers, or SINs in the subject line.	*Use neutral phrasing like "Policy Update" instead of "Jane Smith Policy #123456."*
Retain emails in compliance folders	File key client communications in your compliance approved storage (OneDrive, SharePoint, or CRM).	*Avoid storing messages locally on personal devices.*

SAMPLE EMAIL LANGAUGE

When sending a password-protected document:

"For your privacy, I've encrypted the attached document. The password will be sent to you in a separate email/text."

When using a secure link:

"To ensure your information remains protected, I've shared your file through a secure client portal. The link will expire in 7 days."

QUICK DO & DON'T VISUAL

Encrypt or password-protect attachments

Use secure links

Send passwords separately

Delete client data from sent folder

Use company devices only

Send client info unencrypted

Use Dropbox or personal Gmail

Include passwords in same email

Keep sensitive info in inbox long-term

Send from personal or shared computers