# HOW TO START COMPLIANT & STAY COMPLIANT

GRYPHIN ADVANTAGE

## SETTING UP YOUR PRACTICE

All documents below are non-client facing and are required in order to maintain a compliant practice.

- ✓ Privacy Breach Policy & Procedures
- ✓ AML/ATF Policy & Procedure
- ✓ Complaint File
- ✓ CE Credits
- ✓ E&O
- ✓ FTC (Fair Treatment of Consumers)
- ✓ Gryphin Advantage Code of Conduct

*CONSIDERATIONS*

*Business Continuity Agreement*

## NEW ACCOUNT OPENING REQUIREMENTS

### LIFE/CI/DI INSURANCE SALE

All documents below are client facing and need to be completed and placed into the client file, every time a NEW Account is set up.

- ✓ Advisor Disclosure Document
- ✓ Needs Analysis
- ✓ Illustration
- ✓ Reason Why Letter

*CONSIDERATIONS*

*Fact Finder*

*Types Of Insurance*

*LIRD (if applicable)*

### SEGREGATED FUND/GIC/ANNUITY SALE

- ✓ Advisor Disclosure Document
- ✓ Seg Fund Fee Disclosure
- ✓ Information Folder
- ✓ Fund Facts
- ✓ Copy of Investment Application
- ✓ Reason Why Letter

*CONSIDERATIONS*

*Fact Finder*

*Questionnaire*

*Leverage Loan Documents*

## SUPPLEMENTARY CLIENT FILE DOCUMENTS

All documents below are client facing and only need to be completed once per client file.

- ✓ Privacy Consent
- ✓ Antispam C.A.S.L
- ✓ Letter of Engagement
- ✓ Trusted Contact Person (TCP)

## CYBERSECURITY REQUIREMENTS

All cybersecurity measures below are mandatory to protect client data and maintain regulatory compliance. These requirements must be implemented, documented, and regularly reviewed.

*MULTI-FACTOR AUTHENTICATION (MFA)*

- *Enable MFA on all business email accounts*
- *Require MFA for all client management systems*
- *Implement MFA for remote access tools*
- *Document MFA enrolment for all staff*
- *Regular verification of MFA status*

*POLICIES & PROCEDURES*

- *Information Security Policy*
- *Incident Response Plan*
- *Data Breach Notification Procedure*
- *Remote Work Security Guidelines*
- *Password Management Policy*
- *Annual policy review and updates*

*CYBERSECURITY TRAINING*

- *Annual security awareness training for all staff*
- *Phishing simulation exercises (quarterly)*
- *Data handling best practices*
- *Social engineering awareness*
- *Training completion documentation*
- *New employee onboarding security module*

# CYBERSECURITY REQUIREMENTS

*DATA ENCRYPTION*

- *Encrypt all devices containing client data*
- *Email encryption for sensitive communications*
- *Encrypted backup solutions*
- *Secure file transfer protocols*
- *Encryption key management procedures*
- *Regular encryption audit and verification*

*AI USE & POLICY*

- *Acceptable Use Policy for AI tools*
- *Client data protection in AI systems*
- *AI tool approval and vetting process*
- *Disclosure requirements for AI use*
- *Regular review of AI outputs for accuracy*
- *Staff training on responsible AI use*