PTIN MODULE 2

Master Study Guide

Due Diligence, Ethics & Data Security

Review these notes before taking the Module 2 quiz. Focus on due diligence, ethics, security, incident response, and quality control.

Lesson 2.1 — The Four Due-Diligence Duties

Due diligence applies to EITC, CTC/ACTC/ODC, AOTC, and Head of Household filing status.

The four duties are: complete and submit Form 8867 when required; correctly compute the credit or status; apply the knowledge requirement through reasonable follow-up questions; and keep required records for the required period.

Form 8867 is evidence of the process, not a substitute for interviewing and evaluating the taxpayer's facts.

For returns or claims filed in 2026, the lesson states a $650 penalty for each failure. Separate failures can apply to separate credits or filing status.

Lesson 2.2 — The Knowledge Requirement

A preparer may generally rely on taxpayer information in good faith unless it appears incorrect, inconsistent, or incomplete.

When something does not make sense, ask reasonable follow-up questions, document the questions and answers at the time, and retain documents relied upon.

Never create income simply to qualify a taxpayer for a credit.

Lesson 2.3 — Ethics In Daily Practice

Ethics includes accuracy, competence, confidentiality, honest communication, and independence from client pressure.

Disclose fees before preparation begins. Do not direct a taxpayer's refund to the preparer's personal account, sign blank returns, request blank authorizations, endorse refund checks, or advertise false credentials or guaranteed refunds.

Correct material errors and advise clients of consequences. Address conflicts of interest appropriately.

Circular 230 governs practice before the IRS. Preparers must also follow applicable preparer-penalty provisions, e-file rules, privacy law, and state law.

Lesson 2.4 — When To Stop A Return

Stop and escalate when facts remain unclear, documents are refused, fabricated entries are requested, identity theft is suspected, the issue exceeds the preparer's training, or the software result cannot be explained.

A professional refusal should state that an unsupported position cannot be filed and that the return can be reviewed again if missing records are obtained.

Document why the engagement was paused or ended. Do not threaten the client or disclose client information.

Lesson 2.5 — Data Security & Information Protection

Tax professionals safeguard Social Security numbers, income records, bank details, identity documents, and family information.

Firms should maintain a written information security plan (WISP) appropriate to their operations.

A WISP should identify responsible personnel, assess risks, establish safeguards, address service providers, explain incident response, and be reviewed as the business changes.

IRS Publication 5708 provides a sample framework, but each firm must adapt its plan to its own systems and risks.

Lesson 2.6 — Minimum Security Practices

Use multi-factor authentication, unique passwords in a reputable password manager, current software and firmware, full-device encryption, and automatic screen locks.

Use secure portals rather than ordinary email or text for sensitive documents.

Use role-based access, encrypted tested backups, secure disposal, and written procedures for remote work, mobile devices, contractors, and offboarding.

Do not collect Social Security cards through social-media messages, store client files in a personal photo library, or share one software login among staff.

Lesson 2.7 — Identity Theft And Incident Response

Warning signs include unexpected e-file rejects, unrequested transcripts, unfamiliar returns associated with the EFIN, unusual password resets, locked accounts, and notices for returns clients did not file.

If an incident occurs, disconnect affected systems when appropriate, preserve evidence, contact security and insurance resources, follow the WISP response plan, and make required notifications.

When taxpayer data may have been compromised, the lesson states that tax professionals should contact the local IRS Stakeholder Liaison.

Do not conceal an incident or continue using a known compromised device.

Lesson 2.8 — Recordkeeping And Quality Control

Use a written retention schedule that accounts for federal, state, e-file, due-diligence, consent, business, and insurance requirements. Different records can require different retention periods.

Quality controls can include return-review checklists, staff training, access logs, EFIN monitoring, rejected-return reports, extension reports, open-notice tracking, and post-season file audits.

The firm should know who prepared, reviewed, transmitted, and changed every return.