Thailand: Legal Framework for Digital Forensics

Computer Crime Act B.E. 2550 (2007)

In Thailand, cyber investigations and electronic evidence processing are governed primarily by the Computer Crime Act B.E. 2550 (2007) and its subsequent amendments. The statute establishes severe legal penalties for unauthorized computer access, data interception, and tampering with digital records.

1. Core Statutory Provisions & Investigator Obligations

The Computer Crime Act outlines clear boundaries for handling computer data, system integrity, and service provider responsibilities during criminal and corporate inquiries.

- **Prohibition of Data Alteration**: Altering, falsifying, or compromising forensic findings or electronic evidence is treated as a severe criminal offense under Thai law. Examiners and investigators are held to rigorous standards of objective integrity.
- **Service Provider Duties**: Designated service providers must retain traffic data for a minimum statutory period (typically 90 days or longer upon official request) to support law enforcement tracing and attribution.

2. Investigative Integrity and Ethical Compliance

Forensic practitioners operating within Thailand must maintain absolute impartiality and transparency throughout the digital evidence lifecycle.

- **Refusal of Unethical Directives**: Examiners must categorically refuse any employer, client, or external pressure to manipulate, suppress, or alter forensic analysis results or report conclusions.
- **Enforcement Reporting**: Unethical or illegal requests to tamper with evidence must be formally documented and, where appropriate, reported to specialized authorities such as the Royal Thai Police Cyber Crime Suppression Division (CCSD).

Best Practice: Immutable Record Keeping

Document all communications, tool outputs, and chain-of-custody ledgers immutably. Given the criminal liability associated with evidence tampering under Thai law, maintaining cryptographically verified hash logs (SHA-256) is vital to prove that analytical findings remain unaltered from acquisition to presentation.

Strategic Implications for Practitioners

- **Absolute Accountability**: Personal criminal liability for altering forensic data demands uncompromising adherence to standardized, validated forensic workflows.
- **Standardized Tooling**: Utilize NIST-validated software and hardware write-blockers to ensure original data remains completely untouched during acquisition.
- **Transparent Reporting**: Clearly state methodology, limitations, and tool parameters in all expert reports to withstand judicial examination in Thai courts.
