Vietnam: Legal Framework for Digital Forensics

Cybersecurity Law 2018

In Vietnam, digital forensics and incident response activities are governed by stringent national security and cybersecurity statutes. The Cybersecurity Law 2018 establishes rigorous mandates regarding data localization, critical information infrastructure protection, and the strict handling of physical and digital evidence.

1. Core Principles of the Cybersecurity Law 2018

The statute imposes comprehensive obligations on domestic and international entities operating within cyberspace in Vietnam, prioritizing national security, public order, and the integrity of digital infrastructure.

- **Protection of Critical Information Infrastructure (CII)**: Systems vital to national security, defense, and public governance are subject to heightened monitoring, mandatory security audits, and strict incident response protocols.
- **Data Localization Mandates**: Certain enterprises operating networks or providing telecommunications and digital services in Vietnam are required to store specific categories of user data locally within the territory of Vietnam.

2. Forensic Preservation Rules for IoT and Connected Devices

Handling connected hardware and Internet of Things (IoT) devices during forensic investigations demands strict adherence to isolation protocols to protect evidentiary integrity.

- **Prohibition of Internet Connection**: Connecting seized IoT devices, smart hardware, or compromised network nodes to the internet during evidence collection and triage alters original evidence, introduces remote contamination risks, and breaks the chain of custody.
- **Offline Forensics Standard**: Examiners must rely exclusively on offline forensic tools, hardware write-blockers, and specialized shielding environments (such as Faraday enclosures) to extract volatile and non-volatile telemetry.

Best Practice: Offline Isolation & Handling

Never connect seized IoT or network-attached devices to active networks during evidence acquisition. Always use hardware write-blockers and maintain strict air-gapped forensic workstations to ensure full compliance with Vietnamese evidentiary standards.

Strategic Implications for Practitioners

- **Evidentiary Integrity**: Breaching isolation protocols by permitting unauthorized network connectivity can result in the outright rejection of digital evidence in Vietnamese judicial proceedings.
- **Regulatory Alignment**: Ensure all incident response frameworks incorporate local data localization and mandatory reporting requirements when managing cross-border enterprise breaches.
- **Documentation Rigor**: Record every physical handling step, tool version, and cryptographic hash (SHA-256) in the chain of custody log to withstand rigorous legal scrutiny.
