CTI TECHNOLOGY
we make IT happen

MacHero™

Incident Response Workflow for Illinois Law Firms

1 Incident Detected

Security alert, suspicious login, ransomware trigger, vendor notification, etc.

↓

2 Activate Incident Response Team

IT lead · managing partner · legal counsel · cyber insurer contact

↓

3 Contain the Threat

Isolate affected systems · disable compromised accounts · prevent lateral movement

↓

4 Preserve Evidence & Investigate

Secure logs · engage forensic support if needed · determine scope of exposure

↓

Reportable Breach Under IL Law?

↓ **IF YES**

5 Notification & Legal Obligations

- Notify affected clients (RPC 1.6 considerations)
- Comply with Illinois Personal Information Protection Act (PIPA)
- Notify Illinois Attorney General if threshold met
- Coordinate with malpractice carrier

↓

6 Restore & Validate Systems

Restore from validated backups · confirm document management & email integrity · monitor for reinfection

↓

7 Resume Operations

Document actions taken · track operational impact · stabilize environment

↓

8 Post-Incident Review

Update IR plan · assess control gaps · conduct internal debrief

Designed in alignment with the Illinois Personal Information Protection Act (815 ILCS 530), Illinois Rules of Professional Conduct 1.6, and ISBA cybersecurity guidance.