Cyber Incident and CERT-In Reporting - One-page Control Sheet

Professional technology-law control master for cyber incident and cert-in reporting

Five-step rule

1. Identify the legal trigger, responsible actor and evidence relevant to cyber incident and cert-in reporting.
2. Read the Act with all effective Rules, regulations, notifications, directions, guidelines and forum procedure as at the event date.
3. Separate substantive obligation, operational workflow, filing or reporting, enforcement consequence, remedy, appeal and limitation.
4. Maintain a reproducible source pack, decision memo, approval trail and transaction-level evidence.
5. Apply connected company, contract, tax, accounting, data, competition, consumer, insolvency and sector-law overlays independently.

Evidence pack

Official source; classification memo; authority; operative document; notices/consents; calculations; logs; filing/payment/delivery proof; remediation and appeal chronology.

Red flags

Wrong actor or jurisdiction; outdated rule; missing exception analysis; bundled consent; undocumented approval; threshold calculation without source data; delayed filing; incomplete logs; assuming contract overrides mandatory law.

Decision

Proceed only when the legal trigger, current source, owner, control, evidence, exposure, remedy and forum have been documented.