Cyber incident reporting rules in Thailand, Viet Nam, Indonesia and the Philippines

Read at source by RECATOOLS on 24 November 2026. English renderings of Thai, Vietnamese and Indonesian are ours and unofficial. A reading of the texts, not legal advice.

	Thailand	Viet Nam	Indonesia	Philippines
National cybersecurity statute	Cybersecurity Act B.E. 2562 (2019), in force from the day after gazettal on 27 May 2019 (s.2)	Law on Cybersecurity 116/2025/QH15, in force 1 Jul 2026 (Art. 44); ended Laws 24/2018 and 86/2015	None. RUU KKS is a bill in Commission I's working committee (session of 17 Nov 2026, reported by DPR on 18 Nov)	None. HB 9605 passed the House on 12 Aug 2026 (secondary reports); Senate status unverified
Instrument carrying the clock	Cybersecurity Regulating Committee notification B.E. 2566, clause 5 (gazetted 9 May 2023)	Decree 331/2026/NĐ-CP, Art. 31(2)(d) (in force 19 Aug 2026)	Presidential Regulation 82/2022, Art. 13(1) (24 May 2022)	No national, cross-sector cyber-incident clock found. NPC Circular 16-03, s.17(A), for notifiable personal-data breaches (s.11). Sector rule: BSP Circular 1019 (2018), 2 h for BSP-supervised institutions; status after 2024 unverified
Deadline and trigger	24 h after a significant threat is detected or occurs, to the Office of the National Cyber Security Committee; sector regulator on its own deadline	72 h from detection; 24 h initial notice for a serious incident; on detection where national security or order is involved or the system is seriously disrupted	1×24 h after the incident is found, to the sectoral team, copy to the national team	72 h from knowledge or reasonable belief of a notifiable personal-data breach (s.11), to the NPC and data subjects (s.17(A), s.18(A))
Hours in the statute itself	No: s.58 says "promptly"	No incident-reporting deadline: Art. 40(1)(c) gives none; Art. 25(2) hours answer requests	No statute	No statute; RA 10173 s.20(f) says "promptly"
Who is covered	CII organisations, state or private (s.3, s.49); state agencies with necessary changes	Law: agencies, organisations, individuals in VN (Art. 1(2)). Decree 331: systems for state IT use and online services (Art. 2)	Vital-information-infrastructure operators in 8 named sectors plus others (Art. 4(1))	RA 10175: a criminal law. EO 58 (2024): national agencies and GOCCs. Circular 16-03: personal-information controllers and processors
Regulator named	National Cyber Security Committee (s.5); Regulating Committee (s.12); the Office (s.20). Yearly threat summary filed by regulators and state agencies by 31 Jan (cl. 6)	Ministry of Public Security, focal (Art. 39(2)); Defence for its systems	BSSN coordinates	CICC (RA 10175 s.24); DICT (EO 58); NPC for personal data; BSP for supervised financial institutions
Penalty as written	Not reporting under s.57: fine up to 200,000 baht (s.73)	Not reporting a detected incident: 20–30m đồng, individual; organisations pay double (Decree 330/2026 Art. 21(2)(a), 7(1)); field cap 200m đồng for an organisation (Art. 7(3))	No sanction clause found in Regulation 82/2022	Concealing a breach of sensitive personal information: 1 yr 6 mo to 5 yrs and PhP500,000–1,000,000 (RA 10173 s.30)
ITU GCI 2024 tier	Tier 1	Tier 1	Tier 1	Tier 2

Sources: Royal Gazette (ratchakitcha.soc.go.th); Official Gazette of Viet Nam (congbao.chinhphu.vn); Presidential Regulation 82/2022, DPR e-media and BSP Circular 1019 (archived copy, Feb 2024), cited by title; Official Gazette of the Philippines and the Arellano Law Foundation's LawPhil Project reproductions; NPC Circular 16-03 (archived copy, March 2023); ITU Global Cybersecurity Index 2024. Full guide: recatools.com/guides/cyber-incident-reporting-rules-thailand-viet-nam-indonesia-philippines/