CONTACT

+662 679 6005
+662 679 6041
www.ilct.co.th
law@ilct.co.th

New Regulations Aim to Improve Cybersecurity Training and Set Minimum Standards for Cloud Security

This article aims to provide an overview of the recent National Cyber Security Committee (NCSC) announcements published in the Royal Gazette, covering cybersecurity training and cloud security.

Entities covered by the Cybersecurity Act B.E. 2562 (2019)
Before diving into the announcements, it is important that we outline which entities are covered by the Cybersecurity Act.

Under the act, the following entities are covered:

- Governmental agencies
- Organization of critical information infrastructure
  - Section 3 defines this as a governmental agency or a private organization that has a mission of or provides critical information infrastructure service.
- Supervising or regulating organization
  - Section 3 defines this as a governmental agency or private organization, or a person appointed by law to have regulatory powers over governmental agencies or organization of critical infrastructure.

The first announcement by the NCSC provides guidelines for training personnel of governmental agencies and organizations with critical information infrastructure covered under the Cybersecurity Act. This announcement is due to come into force one year after the date of publication in the Royal Gazette.

Section 8 of the announcement requires entities covered by the Cybersecurity Act to implement training programs to improve cybersecurity skills of their personnel. These training programs can be centralized or decentralized.

Section 9 of the announcement sets out the minimum frequency of training program evaluation of one year, in response to the evolving threat landscape. The evaluation needs to cover training materials such as instructional documents, and the delivery of training.

In addition, the annex to the announcement lays out more detail on training programs with some key components briefly outlined below:

The training covers two broad areas:

- 1. Personnel skillsets: aims to develop the necessary skills for personnel to effectively carry out the duty of maintaining cybersecurity within their organizations.

CONTACT

+662 679 6005
+662 679 6041
www.ilct.co.th
law@ilct.co.th

New Regulations Aim to Improve Cybersecurity Training and Set Minimum Standards for Cloud Security

- 2. Work ecosystem: aims to promote a work environment that is conducive to continuous learning and skill development by personnel responsible for maintaining cybersecurity.

There are three primary areas covered in the announcements:

1. Awareness
2. Training
3. Education

In the annex, the following organizational roles are identified for training:

1. Agency Head
2. Chief Information Officer (CIO)
3. Cybersecurity Program Manager
4. Manager
5. Users

This announcement from the NCSC, mainly aimed at cloud service providers, aims to set standards to enhance cybersecurity of cloud-based systems. This announcement is due to come into force two years after the date of publication in the Royal Gazette.

In the annex to the announcement, the standards cover governmental agencies, organizations with critical information infrastructure, and providers of cloud services to such organizations under the Cybersecurity Act.

In the annex, the NCSC divided cloud security standards into two broad categories:

- Cloud Security Governance: Includes standards relating to information security policies, compliance, and organizational security.
- Cloud Infrastructure Security and Operation: Includes standards relating to matters such as physical and environmental security, technical safeguards, human resource management and cryptography.

The frequency of assessment depends on whether the entity is a user of a cloud service, or is a provider of cloud services, and the level of impact.

- For low-impact cloud users, the minimum frequency of assessment is self-assessment at least once per year.

CONTACT

+662 679 6005
+662 679 6041
www.ilct.co.th
law@ilct.co.th

New Regulations Aim to Improve Cybersecurity Training and Set Minimum Standards for Cloud Security

- For medium and high-impact cloud users, and cloud providers of all impact levels, assessment must be carried out by external bodies in a three-year cycle consisting of:
  - Certification in year one, and
  - Survey in years two and three.
- In addition, for providers of cloud services of all impact levels, at least an ISO/IEC 27001 Certification and CSA STAR Level 1/CCM Lite are required.

Under Section 6, entities covered by the Cybersecurity Act must report to the NCSC within 30 days once implementation of the required standards has been completed.

Both NCSC's announcements do not appear to contain any penalties in an event that an entity covered by the Cybersecurity Act fails to follow the prescribed guidelines, however:

- Section 53 Paragraph 2 gives the Cybersecurity Regulating Committee (CRC) the power to compel organization of critical information infrastructure and governmental agencies to comply with applicable standards.
  - Failure to comply could amount to disobeying official order, the punishment for which is provided in the Penal Code.
- Section 73 penalizes the failure of the organization of critical information infrastructure to report a cyber threat incident without reasonable justification under Section 57.
  - Punishment is a fine of not exceeding 200,000 baht.
- In case of a juristic person, Section 77 places criminal liability with the director, manager or any person responsible for the operation of the juristic person.

This article briefly lays out the requirements for cloud security and cybersecurity training that entities covered by the Cybersecurity Act are expected to follow. Since both NCSC announcements contain lots of details in their annexes, complying with the cybersecurity training and cloud security requirements can be a complex issue. As always, we strongly recommend seeking professional legal assistance. Feel free to contact us at law@ilct.co.th for further guidance.