

# Thailand Sets New Security Standards for Electronic Meetings

On May 26, 2020, Thailand's Ministry of Digital Economy and Society issued a new Notification Re: Security Standards of Meetings via Electronic Means, which came into effect the following day. The notification details the mandatory security standards and procedures that meeting organizers must comply with when convening electronic meetings under the [recent Royal Decree on Teleconferences through Electronic Means B.E. 2563 \(2020\)](#) (which has been in effect since April 19, 2020). The key elements of the notification are explained in further detail below.

## General Security Standard for Electronic Meetings

The meeting organizer must inform all attendees that the meeting is an electronic meeting held under the royal decree. They must be able to carry out the following processes:

No.	Process	Conditions
1	Verify identity of the attendees before the meeting starts	The organizer may adopt a traditional approach, such as asking one attendee to verify another, or use identity verification technology such as usernames and passwords or SMS one time passwords (which are common in Thailand, and known as OTPs).
2	Facilitate communication by audio or both audio and video	The organizer must provide attendees with sufficient bandwidth and sufficiently clear and continuous audio, or audio and video, to allow them to interact and exchange ideas in the meeting.  The chairman of the meeting must be able to control and restrict participation of the attendees, e.g. by using a function to temporarily and immediately suspend any attendee's audio and video feed or stop interaction between them in case of emergency.
3	Provide attendees access to meeting documents	Attendees must be able to access documents and data presented during the meeting.
4	Facilitate voting	Attendees must be able to vote at the electronic meeting whether the meeting selects general vote or secret vote. The organizer shall accommodate the following mechanism of each voting manner: <ol style="list-style-type: none"> <li><b>General vote.</b> Open voting conducted in any manner that permits the attendees to vote and express opinions openly (e.g. verbally).</li> <li><b>Secret vote.</b> Closed voting where only the number of votes is collected and counted without disclosing the identity of the voter (e.g. by online questionnaire).</li> </ol>

No.	Process	Conditions
5	Store meeting data and evidence	The organizer must store all data, including: <ul style="list-style-type: none"> <li>a. The method used to verify identity of attendees, including the total number and names of attendees recorded in the minutes;</li> <li>b. The method and results of voting, recorded in the minutes;</li> <li>c. Recording of audio or both audio and video of meeting, (except confidential meetings—see below);</li> <li>d. Any disruptions during the meeting; and,</li> <li>e. Attendees’ electronic traffic data, e.g. usernames, date and time of login and logout.</li> </ul>
6	Report disruptions and errors	The attendees must be able to report disruptions and errors during the meeting, and the organizer must arrange for proper solutions and preventive measures.

### Special Security Standards for Confidential Electronic Meetings

If an electronic meeting is held for confidential matters, the following additional requirements apply:

- ▶ The meeting organizer must set up security measures to prevent unauthorized access to the meeting, data, and documents;
- ▶ Each individual attendee must affirm to the meeting that no unauthorized person has access to meeting and the attendee is attending the meeting from an access-controlled place; and,
- ▶ Recording audio or video during the confidential electronic meeting is prohibited.

### IT Security Standards

The notification sets five principles of IT security standards for electronic meetings:

1. Confidentiality—IT mechanisms to prevent unauthorized access.
2. Integrity—IT mechanisms to prevent modifications, loss, and damage.
3. Availability—IT mechanisms to ensure functionality and access.
4. Privacy and protection of personal data.
5. Other IT measures, such as authenticity, accountability, non-repudiation, and reliability.

The Electronic Transactions Development Agency (ETDA) is empowered to set forth additional IT security standards for meeting control systems. In addition, the ETDA, or another agency designated by the ETDA, may provide services for verification and certification of qualifying meeting control systems, which should be announced soon.

Any electronic meetings which were already arranged prior to the notification coming into effect (on May 27, 2020), but which have not yet been held, can be held in accordance with the previous security standards for electronic meetings issued in 2014, provided they are held within 60 days of May 27.

For more information on this development, or on any aspect of doing business in Thailand, please contact Supasit Saypan at [supasit.s@tilleke.com](mailto:supasit.s@tilleke.com) or +66 2056 5994.

bangkok | hanoi | ho chi minh city | jakarta | phnom penh | vientiane | yangon  
[www.tilleke.com](http://www.tilleke.com)

### **Our Commitment to Continuous Client Service**

During the COVID-19 outbreak, we are focused on maintaining high-quality client services while ensuring the safety and wellbeing of our team. Over the past several weeks, Tilleke & Gibbins has implemented our Business Continuity Plan across our offices in Cambodia, Indonesia, Laos, Myanmar, Thailand, and Vietnam. The vast majority of our team members are now working remotely, and based on our robust technology infrastructure, we are providing our full range of services as usual. We are now carrying out all client meetings through the use of technology, and, as many of you will have already experienced, this is proving to be a highly effective solution. By implementing a range of technology and agile working measures, we will ensure that you continue to receive the highest quality services with the fastest possible response times from our team. We know that you are facing complex business challenges during this crisis, and we have put together a bank of practical resources tracking the legal developments in the region as they happen—you can access them all at [this link](#). In addition, we want to assure you that our team will be continuously available to help you navigate these issues across Southeast Asia. If you have any queries about these measures, please contact your usual client service partner, or email [communications@tilleke.com](mailto:communications@tilleke.com).

Stay well, safe, and healthy.