

**Notification of the Ministry of Information and Communication Technology**

Re: Standards for Electronic Conferencing Security

B.E. 2557<sup>1</sup>

-----

Whereas, the Announcement of the National Council for Peace and Order No. 74/2557 dated 27 June B.E. 2557 (A.D. 2014) requires that the electronic conferencing be in accordance with the standards for electronic conferencing security prescribed by the Ministry of Information and Communication Technology.

By virtue of Clause 4 of the Announcement of the National Council for Peace and Order No. 74/2557 Re: Electronic Conferencing, dated 27 June B.E. 2557 (A.D. 2014), the Minister of Information and Communication Technology has issued the Notification as follows:

**Clause 1** This Notification is called “Notification of the Ministry of Information and Communication Technology Re: Standards for Electronic Conferencing Security B.E. 2557”.

**Clause 2** This Notification shall come into force on the day following the date of its publication in the Government Gazette.

**Clause 3** In this Notification:

“**Security**” means confidentiality, integrity and availability of the conference control system, including other properties, such as authenticity, accountability, non-repudiation and reliability of electronic data relating to or arising from electronic conferencing.

“**Electronic media**” means any data or information recording media employing an electronic means by the application of an electron, electricity, electromagnetic wave or any other method in a similar manner; and shall also include the application of an optical and magnetic means, or accessories in connection with the application of any of the aforesaid means.

---

<sup>1</sup>Government Gazette, Volume 131, Special Part 246 Ngor., pages 12- 14, 4 December 2557 (A.D.2014)

**“Conference Control System”** means a computer network and/or any electronic communication device, being both hardware and software, which are interconnected as a network and communicate data by using information and communication technology, and/or telecommunications; so as to allow accessibility and usage for the conference through electronic media by the conference attendees, regardless of whether or not it is an audio conferencing or audio and video conferencing.

**“Electronic Conferencing”** means a conference required to be held by law, that is conducted through electronic media, whereby at least one third of the quorum shall physically attend the conference at the same conference venue and all of the conference attendees shall have their presence in the Kingdom of Thailand at the time the conference is held although they are not present at the same venue, but they are capable of consultation, discussion, as well as expression their opinions via electronic media.

**“Conference attendees”** include the committee members, subcommittee members, secretaries and assistant secretaries of the committee or sub-committee.

**“System controller”** means the person serving to maintain and manage a system of the Electronic Conferencing from commencement until conclusion of the conference.

**“Service provider”** means the service provider of the Conference Control System to others in the conference through electronic media under this Notification.

**Clause 4** An Electronic Conferencing shall be performed through the Conference Control System using methods of information security in accord with criteria under the Notification of the Electronic Transactions Commission, Re: Policy and Practice Guidelines on Information Security of a Government Agency B.E. 2553 or other equivalent standards; regardless of whether or not the service provider of such system is the public sector or the private sector.

There shall be audio or audio and video recordation, as the case may be, of every conference attendee throughout the conference period, including the traffic data generated by such recordation in the Conference Control System or by any other system.

Said data recordation under Paragraph 2 shall be executed in the electronic data format by storing on a secure electronic media platform and by using a reliable method pursuant to requirements attached to this Notification.

**Clause 5** The Conference Control System under Clause 4 shall at least contain the basic functional elements as follows:

(1) Enabling conference attendees to communicate with each other via audio signal or audio and visual signal through, among others, information and communication technology and/or telecommunications of wired and wireless types, such as a telephone network, computer network within an organization or Local Area Network (LAN), Integrated Services Digital Network (ISDN), Wide Area Network (WAN), internet network, microwave network, radio telecommunication network or satellites communication network;

(2) Linking two or more meeting venues together;

(3) Enabling conference attendees to communicate or interact with each other in both directions;

(4) Having a device for inputting data from one place to another through information and communication technology and/or telecommunications, such as telephone, video camera, microphone, computer, fax machine, and image scanner, etc.; and

(5) Having functional equipment to link or convert audio signal, or audio and visual signal, suitable for information and communication technology and/or telecommunication that conducive to watching and listening by conference attendees, as the case may be.

Moreover, there may be additional basic functional elements as follows:

(1) Having a device for displaying data transmitted through the information and communication technology and/or telecommunications system so that conference attendees can receive such data, such as loudspeaker, screen, video projector, document display device (hard copy), etc.;

(2) In case that the conference is held in a conference room, there shall be installation of acoustical materials suited to the condition of the conference room in order to prevent reverberation or echo.

**Clause 6** Once the person serving as the chairman at any given conference determines to organize the conference through electronic media, the person charged with arranging the conference shall implement to the application of the Conference Control System in writing before holding the conference and shall also retain the system controller competent to administer systemization for the purpose of auditing the operation and resolving problems for conference attendees by remote access. The Conference Control System shall be ready for operation before the conference is held.

**Clause 7** In the system administration under Clause 6, the chairman at the conference and/or system controller shall be able to jam the audio signal, visual signal or both; as well as be able to immediately pause data transmission to any one of conference attendees' communication machines or devices within the system upon occurrence of a necessity cause or emergency case.

**Clause 8** During the conference, all conference attendees must be able to view conference information being presented at the conference through their own communication machines or devices throughout the conference period, unless the audio signal, visual signal or both audio and visual signal is jammed or there is cessation of data transmission to any of the conference attendees' communication machines or devices upon occurrence of a necessity cause or emergency case under Clause 7.

**Clause 9** The Permanent Secretary of the Ministry of Information and Communication Technology shall have charge and control of the execution of this Notification, as well as be empowered to interpret and determine issues caused by observing this Notification.

Announced on the 24<sup>th</sup> day of November B.E. 2557 (A.D.2014)

Pornchai Rujiprapa

Minister of Information and Communication Technology

**Requirements attached to the Notification of  
the Ministry of Information and Communication Technology**  
Re: Standards for Electronic Conferencing Security B.E. 2557

-----

**Clause 1** Security measures on audio or audio and video recordation of conference attendees shall be in accordance with the following criteria:

(1) Having technology or preventive measures to preclude changes or alteration to that data, except for certifications or additional records, or any change that may ordinarily happen in the communication, storage or display which has no effect to a meaning of that data, in order for it to be confirmable that a reliable method has been applied in securing accuracy of the data since the creation thereof, and be capable of displaying that data afterwards.

(2) In the case where audio or audio and video recordation is made with the Conference Control System, there shall be the reliable procedure to identify people involved with the Conference Control System in order for it to be confirmable that only a person with a right of access has made the recorded data, which shall at least cover the following matters:

- (1) Identification;
- (2) Authentication;
- (3) Authorization; and
- (4) Accountability.

**Clause 2** In recording the traffic data created by the Conference Control System, security measures on recordation of such data shall be prescribed in order to know about the communication data the computer system, indicating the source, origin, destination, time, date, size, duration or others associated with communication of that computer system. Moreover, in storing the traffic data, the following secure and reliable methods shall be implemented:

(1) Data storage shall be kept in the media that can preserve the integrity and secure access thereto with the identification;

(2) Having a data security system to protect confidentiality of the stored data and determination of a particular degree of confidentiality which only authorized access is allowed in accessing such data in order to maintain data reliability, and to prevent both the system controller and administrator editing the stored data, for instance, storage in the Centralised Log Server or commission of the Data Archiving or Data Hashing, etc., except for individuals with relevant duties or those authorized to access such data, such as IT auditors or entrusted person.

(3) In order that the traffic data be precise and utilizable, all clock of every equipment used in service shall be set to be same with the universal time standard.