

(ร่าง) มาตรฐานการรักษาความมั่นคงปลอดภัยด้าน  
สารสนเทศของระบบควบคุมการประชุม

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์  
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม จัดทำขึ้นสำหรับผู้ให้บริการระบบควบคุมการประชุมใช้เป็นแนวปฏิบัติ เพื่อสร้างความน่าเชื่อถือให้กับระบบควบคุมการประชุม และสอดคล้องตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 โดยมาตรฐานฯ ฉบับนี้ ได้พัฒนาตามแนวมาตรฐานของ

- 1) ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems - Requirements, 2013.
- 2) ISO/IEC 27002:2013, Information technology - Security techniques – Code of practice for information security controls, 2013.
- 3) ISO/IEC 27701:2019, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines, 2019.
- 4) European Union Agency for Network and Information Security (ENISA), Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, December, 2016.
- 5) ประกาศมาตรฐานฯ เกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย เรื่อง แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน เลขที่ ขมธอ. 19-2561, 2561.
- 6) ประกาศมาตรฐานฯ เกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย เรื่อง แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน เลขที่ ขมธอ. 20-2561, 2561.

นอกจากนี้ยังได้มีการเปิดรับฟังความคิดเห็นกับหน่วยงานที่เกี่ยวข้อง เพื่อให้มาตรฐานฯ ฉบับนี้ มีความสมบูรณ์ครบถ้วนและสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ โนน ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9

แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200

Website: [www.etcha.or.th](http://www.etcha.or.th)

# คำนำ

เนื่องด้วยปัจจุบันได้เกิดสถานการณ์การระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 ในหลายประเทศทั่วโลก รวมทั้งประเทศไทย องค์การอนามัยโลกจึงได้ประกาศให้เป็นภาวะการแพร่ระบาดใหญ่ทั่วโลก และขณะนี้ยังไม่มีแนวทางการรักษาที่ชัดเจน ทำให้รัฐบาลต้องใช้มาตรการที่เข้มข้นเพื่อควบคุมการระบาดของโรคตามคำแนะนำขององค์การอนามัยโลก โดยเฉพาะอย่างยิ่ง การเว้นระยะห่างทางสังคม (social distancing) ทำให้การปฏิบัติงานของภาครัฐและการประกอบกิจกรรมในทางเศรษฐกิจของเอกชนเกือบทุกภาคส่วน อันเกี่ยวข้องกับการประชุมเพื่อปรึกษาหารือกันตามปกติ ต้องดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ จึงทำให้การประชุมผ่านสื่ออิเล็กทรอนิกส์ได้กลายมาเป็นหนึ่งในแนวทางการประชุมในยุคปัจจุบัน

ในการนี้หน่วยงานของรัฐและเอกชนต่างเผชิญกับความท้าทายในการเลือกระบบควบคุมการประชุมที่เหมาะสมกับองค์กรของตน ไม่ว่าจะเป็นเรื่องความสามารถของระบบ ฟังก์ชันการทำงาน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การรักษาความลับ การคุ้มครองข้อมูลส่วนบุคคล ตลอดจนการปฏิบัติตามระเบียบและกฎหมายที่เกี่ยวข้อง ทั้งนี้เพื่อตอบสนองต่อความต้องการทางธุรกิจ และลดความเสี่ยงในเรื่องต่าง ๆ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ดำเนินการจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมตามความในข้อ 24 ของประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 เพื่อสร้างความมั่นใจให้กับหน่วยงานของรัฐและเอกชนในการใช้บริการระบบควบคุมการประชุมของผู้ให้บริการ ทั้งนี้มาตรฐานฯ ฉบับนี้ ได้ผ่านการพัฒนาและปรับให้เข้ากับการให้บริการของระบบควบคุมการประชุม โดยยึดหลักจากแนวมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นที่ยอมรับในระดับประเทศ และระดับสากล

# สารบัญ

1.	ขอบข่าย .....	1
2.	บทนิยาม .....	2
3.	โครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯ .....	3
3.1	แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯ .....	3
3.2	วัตถุประสงค์ของมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯ .....	4
4.	มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯ .....	5
4.1	การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป.....	5
4.1.1.	วัตถุประสงค์ที่ 1 นโยบายความมั่นคงปลอดภัยระบบสารสนเทศฯ .....	5
4.1.2.	วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์.....	7
4.1.3.	วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง .....	9
4.1.4.	วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล.....	12
4.1.5.	วัตถุประสงค์ที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม .....	13
4.1.6.	วัตถุประสงค์ที่ 6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน .....	14
4.1.7.	วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล .....	18
4.1.8.	วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย.....	20
4.1.9.	วัตถุประสงค์ที่ 9 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ .....	22
4.1.10.	วัตถุประสงค์ที่ 10 การบริการจัดการความเสี่ยงสำหรับผู้ให้บริการ .....	23
4.2	การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ .....	24
4.2.1.	วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์.....	24
4.2.2.	วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง .....	25
4.2.3.	วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล.....	27
4.2.4.	วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล .....	28
4.2.5.	วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย.....	29
5.	เอกสารอ้างอิง.....	30
6.	ภาคผนวก .....	31

## สารบัญรูปภาพ

รูปที่ 1 แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมของผู้ให้บริการ.....4

## สารบัญตาราง

### การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป

ตารางที่ 1	วัตถุประสงค์ที่ 1	นโยบายความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล .....	5
ตารางที่ 2	วัตถุประสงค์ที่ 2	การบริหารจัดการสินทรัพย์ .....	7
ตารางที่ 3	วัตถุประสงค์ที่ 3	การควบคุมการเข้าถึง .....	9
ตารางที่ 4	วัตถุประสงค์ที่ 4	การเข้ารหัสลับข้อมูล .....	12
ตารางที่ 5	วัตถุประสงค์ที่ 5	การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม .....	13
ตารางที่ 6	วัตถุประสงค์ที่ 6	ความมั่นคงปลอดภัยสำหรับการดำเนินงาน .....	14
ตารางที่ 7	วัตถุประสงค์ที่ 7	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล .....	18
ตารางที่ 8	วัตถุประสงค์ที่ 8	การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย .....	20
ตารางที่ 9	วัตถุประสงค์ที่ 9	ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ ..	22
ตารางที่ 10	วัตถุประสงค์ที่ 10	การบริหารจัดการความเสี่ยงสำหรับผู้ให้บริการ .....	23

### การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ

ตารางที่ 11	วัตถุประสงค์ที่ 2	การบริหารจัดการสินทรัพย์ .....	24
ตารางที่ 12	วัตถุประสงค์ที่ 3	การควบคุมการเข้าถึง .....	25
ตารางที่ 13	วัตถุประสงค์ที่ 4	การเข้ารหัสลับข้อมูล .....	27
ตารางที่ 14	วัตถุประสงค์ที่ 7	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล .....	28
ตารางที่ 15	วัตถุประสงค์ที่ 8	การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย .....	29

### ภาคผนวก

ตารางที่ 16	เปรียบเทียบวัตถุประสงค์ด้านความมั่นคงปลอดภัยกับมาตรฐานสากล และมาตรฐานอื่น ๆ .....	31
-------------	---	----

## 1. ขอบข่าย

มาตรฐานฯ ฉบับนี้ เป็นข้อกำหนดและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ สำหรับระบบควบคุมการประชุม โดยครอบคลุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป และการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ เพื่อให้ผู้ให้บริการมีแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานเดียวกัน

มาตรฐานฯ ฉบับนี้ อ้างอิงข้อกำหนดจากมาตรฐานสากลและมาตรฐานอื่นที่เกี่ยวข้อง โดยมีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

- “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ซึ่งต้องปฏิบัติตาม
- “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อเสนอแนะ (recommendation)
- “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

## 2. บทนิยาม

- 1) “การประชุมผ่านสื่ออิเล็กทรอนิกส์” หมายความว่า การประชุมที่กฎหมายบัญญัติให้ต้องมีการประชุมที่ได้กระทำผ่านสื่ออิเล็กทรอนิกส์ โดยให้ผู้ร่วมประชุมที่มีได้อยู่ในสถานที่เดียวกันและสามารถประชุมปรึกษาหารือและแสดงความคิดเห็นระหว่างกันได้ผ่านสื่ออิเล็กทรอนิกส์
- 2) “ผู้ร่วมประชุม” หมายความว่า ประธานกรรมการ รองประธานกรรมการ กรรมการอนุกรรมการ เลขานุการ และผู้ช่วยเลขานุการของคณะกรรมการ คณะอนุกรรมการ หรือคณะบุคคลอื่นตามที่กฎหมายกำหนด และให้หมายความรวมถึงผู้ซึ่งต้องชี้แจง แสดงความคิดเห็นต่อคณะกรรมการ คณะอนุกรรมการ หรือคณะบุคคลนั้นด้วย
- 3) “อิเล็กทรอนิกส์” หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น
- 4) “ระบบควบคุมการประชุม” หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ และ/หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เชื่อมโยงกันเป็นเครือข่าย และมีการสื่อสารข้อมูลกันโดยใช้เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือการโทรคมนาคม เพื่อให้ผู้ร่วมประชุมสามารถเข้าถึงและใช้งานสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ไม่ว่าจะเป็นการประชุมด้วยเสียงหรือทั้งเสียงและภาพ
- 5) “ผู้ให้บริการ” หมายความว่า ผู้ให้บริการระบบควบคุมการประชุม
- 6) “ผู้ควบคุมระบบ” หมายความว่า ผู้ทำหน้าที่ดูแลและบริหารจัดการระบบควบคุมการประชุม



### 3. โครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

#### 3.1 แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

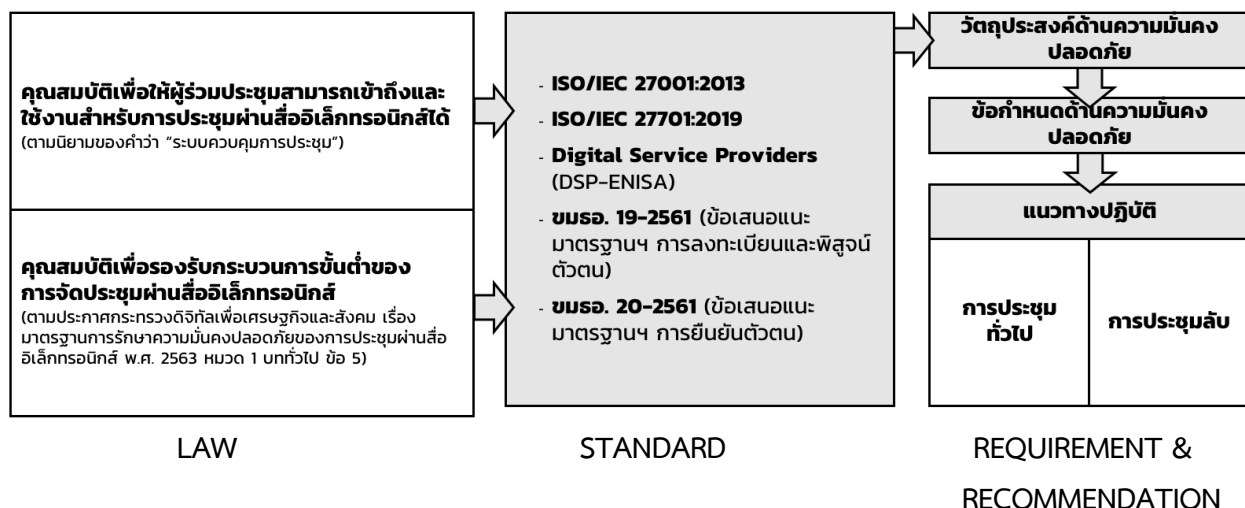
ตามเนื้อหาของประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 ซึ่งได้กำหนดนิยามของระบบควบคุมการประชุมเอาไว้เป็น “ระบบเครือข่ายคอมพิวเตอร์ และ/หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เชื่อมโยงกันเป็นเครือข่าย และมีการสื่อสารข้อมูลกันโดยใช้เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือการโทรคมนาคม เพื่อให้ผู้ร่วมประชุมสามารถเข้าถึงและใช้งานสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ไม่ว่าจะเป็นการประชุมด้วยเสียงหรือทั้งเสียงและภาพ” ซึ่งประกาศเดียวกัน ในหมวด 1 บททั่วไป ข้อ 5 การจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ อย่างน้อยต้องมีกระบวนการ ดังต่อไปนี้

- (1) การแสดงตนของผู้ร่วมประชุมผ่านสื่ออิเล็กทรอนิกส์ก่อนการประชุม
- (2) การสื่อสารหรือมีปฏิสัมพันธ์กันได้ด้วยเสียง หรือทั้งเสียงและภาพ
- (3) การเข้าถึงเอกสารประกอบการประชุมของผู้ร่วมประชุม
- (4) การลงคะแนนของผู้ร่วมประชุม ทั้งการลงคะแนนโดยเปิดเผยและการลงคะแนนลับ (หากมี)
- (5) การจัดเก็บข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ ซึ่งรวมถึงการบันทึกเสียง หรือทั้งเสียงและภาพ แล้วแต่กรณี ของผู้ร่วมประชุมทุกคนตลอดระยะเวลาที่มีการประชุม เว้นแต่เป็นการประชุมลับ
- (6) การจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ของผู้ร่วมประชุมทุกคนไว้เป็นหลักฐาน
- (7) การแจ้งเหตุขัดข้องในระหว่างการประชุม

ทั้งนี้ ระบบควบคุมการประชุมจึงต้องมีคุณสมบัติต่าง ๆ เพื่อรองรับกระบวนการดังกล่าวของการจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ในส่วนที่เกี่ยวข้องด้วย

ดังนั้น มาตรฐานฯ ฉบับนี้ จึงมีเนื้อหาครอบคลุมทั้งในเรื่องความมั่นคงปลอดภัยด้านสารสนเทศตามกระบวนการของระบบควบคุมการประชุม เช่น การจัดเก็บข้อมูลจราจรทางอิเล็กทรอนิกส์ ฯลฯ โดยอ้างอิงจากมาตรฐานสากลและมาตรฐานอื่นที่เกี่ยวข้อง ทั้งนี้ได้จัดทำเป็นข้อกำหนดและแนวปฏิบัติโดยแยกตามการประชุมทั่วไป และการประชุมลับ รายละเอียดตามรูปที่ 1 *แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัย*

*ด้านสารสนเทศของระบบควบคุมการประชุมของผู้ให้บริการ*



รูปที่ 1 แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัย  
ด้านสารสนเทศของระบบควบคุมการประชุมของผู้ให้บริการ

### 3.2 วัตถุประสงค์ของมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมเป็นข้อกำหนดและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับระบบควบคุมการประชุมของผู้ให้บริการ ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) การรักษาสภาพพร้อมใช้งาน (Availability) ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) ความน่าเชื่อถือ (Reliability) รวมถึงการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลของข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องหรือเกิดจากการประชุม โดยผู้ให้บริการต้องดำเนินการตามข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ แบ่งออกเป็น 10 วัตถุประสงค์ ได้แก่

1. นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล
2. การบริหารจัดการสินทรัพย์
3. การควบคุมการเข้าถึง
4. การเข้ารหัสลับข้อมูล
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
6. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน
7. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล
8. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
9. ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ
10. การบริหารจัดการความเสี่ยง

ซึ่งวัตถุประสงค์จะประกอบด้วยข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศและแนวปฏิบัติสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ ตามหัวข้อ 4

#### 4. มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

##### 4.1 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป

##### 4.1.1. วัตถุประสงค์ที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศของระบบควบคุมการประชุมให้สอดคล้องกับวัตถุประสงค์ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

##### ตารางที่ 1 วัตถุประสงค์ที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องกำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ที่ครอบคลุมระบบควบคุมการประชุม รวมถึงประกาศให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบ</p>	<p>นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ควรมีการระบุให้ชัดเจนว่าครอบคลุมระบบควบคุมการประชุม ทั้งนี้ควรมีรายละเอียดที่กำหนดตามหัวข้อดังนี้</p> <ol style="list-style-type: none"> <li>(1) การบริหารจัดการสินทรัพย์</li> <li>(2) การควบคุมการเข้าถึง</li> <li>(3) การเข้ารหัสลับข้อมูล</li> <li>(4) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม</li> <li>(5) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน</li> <li>(6) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล</li> <li>(7) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย</li> <li>(8) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ</li> <li>(9) การบริหารจัดการความเสี่ยง</li> </ol> <p>ผู้ให้บริการควรมีการประกาศนโยบายฯ ให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ</p>
<p>2. ต้องทบทวนนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายการคุ้มครองข้อมูลส่วนบุคคลตาม</p>	<p>ผู้ให้บริการควรจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตด้านความมั่นคงปลอดภัย</p>

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
ระยะเวลาที่เหมาะสม หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ	ระบบสารสนเทศของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือ มาตรฐาน ฯลฯ

#### 4.1.2. วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

เพื่อระบุสินทรัพย์ที่เกี่ยวข้องกับระบบควบคุมการประชุมและกำหนดความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

ตารางที่ 2 วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึก หรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม</p> <p>ทั้งนี้ หากเป็นการให้บริการรองรับการประชุมเรื่องที่มีขึ้นความลับของหน่วยงานของรัฐต้องมีบัญชีทะเบียนสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลอยู่ในราชอาณาจักรทั้งหมด และต้องมีเอกสารรับรองหรือประกาศอย่างเป็นทางการ</p>	<p>ทะเบียนสินทรัพย์ควรครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูล ที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม</p> <p>ผู้ให้บริการอาจระบุข้อมูลที่จำเป็นสำหรับการประเมินแนวทางการดูแลด้านความมั่นคงปลอดภัย เช่น ความสำคัญของสินทรัพย์แต่ละรายการในเชิงการรักษาความมั่นคงปลอดภัย ผู้รับผิดชอบของสินทรัพย์แต่ละรายการ ฯลฯ</p>
<p>2. ต้องมีเงื่อนไขการใช้งานสำหรับระบบควบคุมการประชุม ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ</p>	<p>เงื่อนไขการใช้งานควรครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ ผ่านช่องทางมีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ</p>

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>3. ต้องมีมาตรการแสดงให้ผู้ร่วมประชุมเห็นว่าเป็นการประชุมทั่วไป หรือการประชุมลับได้อย่างชัดเจน</p>	<p>ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงข้อมูลประเภทการประชุมว่าเป็นการประชุมทั่วไป หรือการประชุมลับ เพื่อให้ผู้ร่วมประชุมทราบ โดยอาจให้ผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเอง เช่น กำหนดในหัวข้อการประชุม ฯลฯ</p> <p>ผู้ให้บริการควรจัดทำคู่มือการแสดงข้อมูลประเภทการประชุมให้ผู้มีหน้าที่จัดการประชุมสามารถปฏิบัติตามได้</p>
<p>4. ต้องกำหนดรายการ "ข้อมูลส่วนบุคคล" ในบัญชีทะเบียนสิทธิส่วนบุคคลที่เป็นข้อมูล พร้อมทั้งกำหนดลำดับชั้นความลับ และต้องมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล</p>	<p>บัญชีทะเบียนสิทธิควรรวมข้อมูลประเภท "ข้อมูลส่วนบุคคล" และผู้ให้บริการควรมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล เช่น การกำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึง ฯลฯ</p>
<p>5. ต้องมีขั้นตอนปฏิบัติสำหรับการลบหรือทำลายข้อมูลเกี่ยวกับการประชุม เมื่อมีเหตุให้ต้องดำเนินการ</p>	<p>ขั้นตอนปฏิบัติในการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมควรรวมข้อมูลส่วนบุคคล</p> <p>ผู้ให้บริการควรจัดให้มีช่องทางให้ผู้มีหน้าที่จัดการประชุมดำเนินการได้เอง หรือช่องทางให้ผู้มีหน้าที่จัดการประชุมร้องขอให้ผู้ให้บริการลบหรือทำลายข้อมูลดังกล่าวได้</p>

#### 4.1.3. วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

เพื่อจำกัดการเข้าถึงระบบควบคุมการประชุมและอุปกรณ์ประมวลผลข้อมูล

##### ตารางที่ 3 วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
1. ต้องกำหนดนโยบายการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุม อย่างมั่นคงปลอดภัย	นโยบายการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องของ <u>ควร</u> ครอบคลุมการเข้าถึงด้านเครือข่าย และโปรแกรมประยุกต์ เป็นอย่างน้อย  ผู้ให้บริการ <u>ควร</u> ประกาศนโยบายฯ ให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางมีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ
2. ต้องกำหนดวิธีการให้สิทธิและยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุมได้	ระบบควบคุมการประชุม <u>ควรมี</u> ช่องทางการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุม เพื่อให้ประธานในที่ประชุมหรือผู้ควบคุมระบบสามารถคัดกรองผู้ร่วมประชุมก่อนการประชุมได้ ฯลฯ
3. ต้องสามารถให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง	ระบบควบคุมการประชุม <u>ควรมี</u> ช่องทางให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง ทั้งก่อนหรือระหว่างการประชุมได้
4. ต้องสามารถจำกัดและควบคุมการให้สิทธิของผู้ให้บริการ	ระบบควบคุมการประชุม <u>ควรมี</u> มาตรการรองรับการจำกัดสิทธิของผู้ให้บริการ เช่น สิทธิการเข้าถึงข้อมูลการประชุม สิทธิในการงดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ ฯลฯ
5. ต้องสามารถแสดงสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุม <u>ควรมี</u> ช่องทางให้ผู้มีหน้าที่จัดประชุมหรือผู้ร่วมประชุมสามารถเรียกดูรายชื่อ และจำนวนผู้ร่วมประชุม เพื่อให้สามารถพิจารณาผู้เข้าร่วมได้ตลอดระยะเวลาการประชุม

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>6. ต้องสามารถปรับและยกเลิกสิทธิของผู้ร่วมประชุมได้</p>	<p>ระบบควบคุมการประชุมควรมีช่องทางในการปรับและยกเลิกสิทธิของผู้ร่วมประชุม ในระหว่างการประชุม โดยรองรับให้ประธานหรือผู้ควบคุมการประชุมสามารถดำเนินการดังนี้เป็นอย่างน้อย</p> <p>(1) งดการถ่ายทอดเสียงหรือทั้งภาพและเสียง</p> <p>(2) หยุดการส่งข้อมูล</p> <p>(3) ยกเลิกการเข้าประชุมของผู้ร่วมประชุม</p>
<p>7. ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม</p> <p>ทั้งนี้หากเป็นการประชุมลับ ต้องมีการรหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม</p>	<p>ระบบควบคุมการประชุมควรมีช่องทางในการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมโดยผู้ที่ได้รับอนุญาต และอาจกำหนดสิทธิในการเข้าถึงจากผู้มีหน้าที่จัดการประชุมได้เอง</p>
<p>8. ต้องสามารถพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย</p> <p>ทั้งนี้หากเป็นการประชุมลับ ต้องมีการยืนยันตัวตนแบบหลายปัจจัย</p>	<p>ระบบควบคุมการประชุมควรมีช่องทางพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย ด้วยวิธีการยืนยันตัวตนแบบปัจจัยเดียว (Single-factor Authentication) เป็นอย่างน้อย เช่น รหัสผ่าน ฯลฯ</p>
<p>9. ต้องสามารถตั้งค่านโยบายที่มั่นคงปลอดภัย</p>	<p>ระบบควบคุมการประชุมควรมีการกำหนดนโยบายการตั้งค่านโยบายที่มั่นคงปลอดภัย เช่น รหัสผ่านที่มั่นคงปลอดภัยประกอบไปด้วยตัวอักษร ตัวเลข และอักขระพิเศษ ฯลฯ</p>



ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>ทั้งนี้หากเป็นการประชุมลับ          ต้องมีการตรวจสอบรหัสผ่าน          ที่กำหนดให้เป็นไปตาม          นโยบายที่กำหนดอย่าง          เคร่งครัด</p>	

#### 4.1.4. วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

เพื่อให้มั่นใจได้ว่าการใช้งานการเข้ารหัสลับข้อมูลเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันไม่ให้ความลับหรือข้อมูลส่วนบุคคลรั่วไหล และรักษาความถูกต้องครบถ้วนของข้อมูล

ตารางที่ 4 วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับข้อมูลบนระบบควบคุมการประชุม และข้อมูลส่วนบุคคลที่เกี่ยวข้อง</p> <p>ทั้งนี้หากเป็นการประชุมลับ ต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง (End-to-End Encryption (E2EE))</p>	<p>นโยบายควรระบุให้ครอบคลุมถึงการเข้ารหัสลับของข้อมูลที่เกี่ยวข้องกับการประชุม และข้อมูลส่วนบุคคล ด้วยวิธีการที่ได้รับการยอมรับตามมาตรฐานสากล และครอบคลุมกระบวนการเข้ารหัสลับข้อมูลในรูปแบบดังต่อไปนี้เป็นอย่างน้อย</p> <p>(1) การเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย (data-in-transit encryption)</p> <p>(2) การเข้ารหัสลับของที่จัดเก็บ (data-at-rest encryption)</p>
<p>2. ต้องบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลอย่างมั่นคงปลอดภัย</p>	<p>ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูล โดยครอบคลุมแนวทางดังต่อไปนี้เป็นอย่างน้อย</p> <p>(1) การป้องกันการเข้าถึงกุญแจสำหรับเข้ารหัสลับข้อมูลทั้งแบบระบบรหัสแบบสมมาตร (Symmetric Key Cryptography) และ ระบบรหัสแบบอสมมาตร (Asymmetric Key Cryptography)</p> <p>(2) การกำหนดอายุการใช้งานของกุญแจที่เข้ารหัสลับ</p>

#### 4.1.5. วัตถุประสงค์ที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

เพื่อป้องกันความเสียหาย การเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การแทรกแซงระบบและอุปกรณ์ ประมวลผลข้อมูลของระบบควบคุมการประชุม

#### ตารางที่ 5 วัตถุประสงค์ที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
1. ต้องมีขั้นตอนปฏิบัติสำหรับการเข้าถึงพื้นที่มั่นคงปลอดภัย (Secure areas)	ขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมกระบวนการที่สำคัญ เช่น การลงชื่อเข้าและออกพื้นที่ การตรวจสอบความผิดปกติของการเข้าพื้นที่ ฯลฯ

#### 4.1.6. วัตถุประสงค์ที่ 6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

เพื่อให้มั่นใจว่าการดำเนินงานของระบบควบคุมการประชุมมีความถูกต้องและมั่นคงปลอดภัย

##### ตารางที่ 6 วัตถุประสงค์ที่ 6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
1. <u>ต้องมีคู่มือการใช้งานของระบบควบคุมการประชุม และเผยแพร่ให้ผู้เกี่ยวข้องสามารถนำไปปฏิบัติได้</u>	ผู้ให้บริการ <u>ควร</u> จัดทำเอกสารของขั้นตอนปฏิบัติที่เกี่ยวข้องกับระบบควบคุมการประชุมอย่างชัดเจน รวมถึงการบริหารจัดการเอกสาร เช่น การปรับปรุงเอกสาร การจัดเก็บเอกสาร ช่องทางการเข้าถึงและสิทธิ์ที่เกี่ยวข้อง ฯลฯ
2. <u>ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารการเปลี่ยนแปลงของระบบควบคุมการประชุม</u>	ขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุม <u>ควร</u> ครอบคลุมการประเมินผลกระทบ การมอบหมายการปรับปรุง การอนุมัติจากผู้ที่มีอำนาจ การวางแผนสำรอง และการทดสอบ เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล
3. <u>ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารจัดการทรัพยากรของระบบควบคุมการประชุม</u>	ขั้นตอนปฏิบัติการบริหารขีดความสามารถของระบบควบคุมการประชุม <u>ควร</u> ครอบคลุมการติดตาม ปรับปรุง และคาดการณ์ความต้องการในการใช้ทรัพยากรของระบบ เพื่อให้สามารถวางแผนการใช้งานทรัพยากรให้รองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ
4. <u>ต้องควบคุมสภาพแวดล้อมของการพัฒนา การทดสอบ และการใช้งานจริง ซึ่งแบ่งแยกออกจากกัน</u>	ผู้ให้บริการ <u>ควร</u> จัดให้มีการแยกสภาพแวดล้อมส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบควบคุมการประชุม ในแต่ละส่วนออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต และ <u>ควร</u> กำหนดสิทธิ์ในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน
5. <u>ต้องสามารถรับมือกับภัยคุกคามประเภทมัลแวร์</u>	ผู้ให้บริการ <u>ควร</u> จัดให้มีวิธีการตรวจจับ การป้องกัน และการกู้คืน ที่เกิดขึ้นจากภัยคุกคามจากโปรแกรมไม่พึงประสงค์ต่อระบบควบคุมการประชุม เช่น การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) การติดตั้งระบบตรวจจับภัยคุกคาม (Intrusion Detection System) การสำรองข้อมูล ฯลฯ

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>6. ต้องมีขั้นตอนปฏิบัติเรื่องการสำรองข้อมูลและการกู้คืนอย่างเหมาะสม กรณีที่มีข้อมูลส่วนบุคคลต้องมีการกำหนดผู้ดำเนินการสำรองข้อมูลและกู้คืนข้อมูลส่วนบุคคลด้วย</p>	<p>ขั้นตอนปฏิบัติเรื่องการสำรองข้อมูล และการกู้คืนข้อมูลของระบบควบคุมการประชุมควรครอบคลุมรายการบัญชีทะเบียนสินทรัพย์ที่จำเป็นต้องมีการสำรองข้อมูล วิธีการสำรองข้อมูล พร้อมระบุช่วงเวลาที่ต้องจัดเก็บข้อมูลที่สำรองรวมถึงแนวทางการทดสอบการกู้คืนอย่างเหมาะสม โดยกรณีที่มีการสำรองนั้นมีข้อมูลส่วนบุคคลอยู่ด้วย ควรมีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรม เช่น ผู้ดำเนินการสำรองข้อมูล ผู้ทดสอบการกู้คืนข้อมูล ฯลฯ</p> <p>ทั้งนี้ ระบบควบคุมการประชุมควรถูกตั้งค่าให้สำรองข้อมูลบันทึกประเภทเสียงหรือทั้งเสียงและภาพ ข้อมูลจราจรทางอิเล็กทรอนิกส์ รวมถึงข้อมูลอื่นที่เกี่ยวข้อง เช่น ข้อมูลการแจ้งเตือนขัดข้องระหว่างการประชุม ฯลฯ อย่างน้อยเป็นระยะเวลา 7 วันนับแต่วันสิ้นสุดการประชุมในแต่ละครั้ง</p>
<p>7. ต้องจัดเก็บข้อมูลจราจรทางอิเล็กทรอนิกส์ และต้องมีการทบทวนอย่างเหมาะสม</p>	<p>ระบบควบคุมการประชุมควรถูกตั้งค่าให้จัดเก็บข้อมูลจราจรทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยอย่างน้อยต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคลหรือชื่อผู้ใช้งาน (Username) วันและเวลาของการเข้าร่วมประชุม และเลิกประชุมเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล</p> <p>ผู้ให้บริการควรมีการกำหนดรอบของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างน้อย 1 ครั้งต่อปี</p>
<p>8. ต้องมีการดูแลข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรทางอิเล็กทรอนิกส์ โดยอย่างน้อยต้องสามารถระบุผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการใช้ หรือประมวลผล</p>	<p>ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรทางอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน โดยครอบคลุมข้อมูลผู้ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการ เป็นอย่างน้อย</p>
<p>9. ต้องป้องกันการเปลี่ยนแปลงและการเข้าถึงที่ไม่ได้รับ</p>	<p>ผู้ให้บริการควรจัดเตรียมวิธีป้องกัน การเปลี่ยนแปลง การเข้าถึง การลบ โดยไม่ได้รับอนุญาตต่อข้อมูลจราจรทางอิเล็กทรอนิกส์ เช่น การจำกัดสิทธิการ</p>

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
อนุญาต ต่อข้อมูลจราจรทางอิเล็กทรอนิกส์	ดำเนินการในแต่ละฟังก์ชันการทำงาน การเฝ้าระวังและแจ้งเตือนการเข้าใช้งานที่ผิดปกติ ฯลฯ
10. ต้องจำกัดการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรทางอิเล็กทรอนิกส์ รวมถึงกำหนดระยะเวลาในการลบหรือเปลี่ยนรูปข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้	<p>ผู้ให้บริการควรกำหนดวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรทางอิเล็กทรอนิกส์ โดยครอบคลุมการบันทึกกิจกรรมที่เกี่ยวข้อง เช่น การเข้าถึงข้อมูลส่วนบุคคล ฯลฯ</p> <p>ผู้ให้บริการควรกำหนดระยะเวลาที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระบบควบคุมการประชุม พร้อมกำหนดวิธีการลบ หรือการเปลี่ยนแปลงรูปแบบข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้</p>
11. ต้องมีจัดเก็บข้อมูลจราจรทางอิเล็กทรอนิกส์จากการใช้งานของผู้ควบคุมระบบและผู้ให้บริการ และมีการทบทวนอย่างเหมาะสม	<p>ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรทางที่เกี่ยวข้องกับการใช้งานของผู้ควบคุมระบบ โดยครอบคลุมกิจกรรมดังต่อไปนี้เป็นอย่างน้อย</p> <ul style="list-style-type: none"> <li>(1) บันทึกการทำงานของระบบ (system logs)</li> <li>(2) บันทึกการเข้าออกระบบ (login-logout logs)</li> <li>(3) บันทึกการพยายามเข้าสู่ระบบ (login attempts logs)</li> <li>(4) บันทึกปัญหาหรือความผิดพลาดต่าง ๆ (fault logs)</li> </ul> <p>ผู้ให้บริการควรมีการกำหนดช่วงเวลาของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างเหมาะสม</p>
12. ต้องสามารถตั้งค่า Clock synchronisation ของระบบควบคุมการประชุมให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล และเป็นแหล่งเทียบเวลาในระดับ (Stratum) เดียวกันทั้งระบบควบคุมการประชุม	ระบบควบคุมการประชุมควรถูกตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล เช่น สถาบันมาตรวิทยาแห่งชาติ ฯลฯ รวมถึงควรเป็นแหล่งเทียบเวลาในระดับ (Stratum) เดียวกันทั้งระบบควบคุมการประชุม เช่น ตั้งค่าการใช้งานระดับ Stratum-1 ให้เหมือนกันทั้งระบบควบคุมการประชุม

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>13. <u>ต้อง</u>จัดการช่องโหว่ทางเทคนิคของระบบควบคุมการประชุม โดยต้องได้รับการแก้ไขอย่างมีประสิทธิภาพ</p>	<p>ผู้ให้บริการ<u>ควร</u>กำหนดช่องทางในการรับแจ้งช่องโหว่ และดำเนินกิจกรรมการประเมินผลกระทบ การจัดการช่องโหว่ เมื่อมีผู้แจ้งเหตุอย่างทันท่วงที พร้อมเผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ</p> <p>ผู้ให้บริการ<u>ควรมี</u>การตรวจสอบช่องโหว่ทางเทคนิคของระบบควบคุมการประชุมอย่างน้อย 1 ครั้งต่อปี หรือเมื่อระบบควบคุมการประชุมมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้แน่ใจว่าระบบควบคุมการประชุมไม่มีความเสี่ยงรุนแรงที่อาจส่งผลกระทบต่อการใช้บริการ</p>
<p>14. <u>ต้อง</u>ทบทวนความสอดคล้องด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุมอย่างเหมาะสม</p>	<p>ผู้ให้บริการ<u>ควร</u>จัดให้มีการทบทวนความสอดคล้องด้านมาตรการความมั่นคงปลอดภัยของระบบควบคุมการประชุม เช่น การตรวจประเมินภายใน (internal audit) อย่างน้อย 1 ครั้งต่อปี ฯลฯ</p>

#### 4.1.7. วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

เพื่อให้มั่นใจว่าการสื่อสารข้อมูลในระบบเครือข่ายและอุปกรณ์ประมวลผลของระบบควบคุมการประชุม มีความมั่นคงปลอดภัย

ตารางที่ 7 วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องบริหารจัดการเครือข่ายอย่างมั่นคงปลอดภัย</p>	<p>ผู้ให้บริการควรจัดให้มีการบริหารจัดการเครือข่าย โดยครอบคลุมมาตรการดังต่อไปนี้เป็นอย่างน้อย</p> <ul style="list-style-type: none"> <li>(1) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต</li> <li>(2) การป้องกันการดักจับข้อมูล</li> <li>(3) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย</li> <li>(4) การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล</li> <li>(5) การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ดักจับมัลแวร์บนเครือข่าย ฯลฯ</li> </ul>
<p>2. ต้องกำหนดนโยบายความมั่นคงปลอดภัยของเครือข่ายและขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้องต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้</p> <p>ทั้งนี้หากเป็นการประชุมลับ ต้องกำหนดนโยบายที่ระบุถึง</p>	<p>นโยบายความมั่นคงปลอดภัยของเครือข่ายควรครอบคลุมเรื่องการเข้ารหัสลับ ข้อมูลระหว่างโอนย้ายข้อความ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย</p> <p>ขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการเข้าถึงข้อมูลบนเครือข่ายควรกำหนดวิธีการ และช่องทางการดำเนินการอย่างชัดเจน โดยอาจกับการเชื่อมโยงแผนภาพเครือข่าย เพื่อให้แน่ใจว่าครอบคลุมการดำเนินการของระบบควบคุมการประชุม รวมถึงกรณีที่มีข้อมูลส่วนบุคคลที่รับส่งอยู่บนเครือข่ายควรมีการบันทึกกิจกรรมการดำเนินการ พร้อมผู้รับผิดชอบให้ชัดเจน</p>



ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
การเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง (End-to-End Encryption (E2EE))	

#### 4.1.8. วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

เพื่อมั่นใจว่าการบริหารจัดการเหตุขัดข้องของระบบควบคุมการประชุมและการสื่อสารเกี่ยวกับข้อบกพร่องและสถานการณ์ด้านความมั่นคงปลอดภัย มีการควบคุมดูแลเป็นขั้นตอนและมีประสิทธิภาพ

#### ตารางที่ 8 วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. <u>ต้องมีขั้นตอนปฏิบัติ</u>เรื่องการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม โดยหากพบว่าข้อมูลส่วนบุคคลรั่วไหล ต้องมีมาตรการในการจัดการอย่างมั่นคงปลอดภัย</p>	<p>ผู้ให้บริการ<u>ควร</u>จัดทำขั้นตอนการปฏิบัติเรื่องการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุมที่ครอบคลุมกระบวนการดังต่อไปนี้เป็นอย่างน้อย</p> <ol style="list-style-type: none"> <li>(1) การรับแจ้งและยืนยันเหตุฯ</li> <li>(2) การจำแนกเหตุฯ และประเมินผลกระทบ</li> <li>(3) การตอบสนองต่อเหตุฯ</li> <li>(4) การจัดเก็บพยานหลักฐาน</li> </ol> <p>ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการ<u>ควรมี</u>การระบุเพิ่มเติมถึงความรับผิดชอบในแต่ละกระบวนการ ข้อมูลที่รั่วไหล การรายงานเหตุฯ ไปยังผู้เกี่ยวข้อง เป็นอย่างน้อย</p>
<p>2. <u>ต้องมีการรับแจ้งเหตุ</u>และรายงานด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม</p>	<p>ผู้ให้บริการ<u>ควร</u>จัดให้มีช่องทางการรับแจ้งเหตุและรายงานด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม โดยข้อมูลที่แจ้งควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย</p> <ol style="list-style-type: none"> <li>(1) รายละเอียดผู้แจ้งเหตุฯ</li> <li>(2) วันเวลาที่พบเหตุฯ</li> <li>(3) รายละเอียดของเหตุฯ</li> </ol>
<p>3. <u>ต้องมีมาตรการ</u>สำหรับการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุม</p>	<p>ผู้ให้บริการ<u>ควร</u>กำหนดวิธีการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยพิจารณาถึงองค์ประกอบดังต่อไปนี้เป็นอย่างน้อย</p> <ol style="list-style-type: none"> <li>(1) การประเมินผลกระทบของเหตุฯ</li> </ol>

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>การประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลต้องมี การสื่อสารกับเจ้าของข้อมูล และผู้เกี่ยวข้อง</p> <p>ทั้งนี้ หากเป็นการประชุมลับ ต้องดำเนินการแก้ไขปัญหา ช่องโหว่ทางเทคนิคในระดับ รุนแรงที่ (อ้างอิงตาม CVSS ที่ severity ระดับ high ขึ้นไป) พบบนระบบควบคุมการ ประชุมครบทุกรายการก่อน ให้บริการ</p>	<p>(2) แนวทางและช่องทางในการแจ้งเหตุฯ</p> <p>(3) การบันทึกเหตุฯ โดยให้มีการระบุรายละเอียดคำอธิบายเหตุการณ์ ช่วงเวลา ผลกระทบ ช่วงเวลาที่เกิดผลกระทบ</p> <p>ในกรณีที่มิข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการระบุงค์ประกอบ เพิ่มเติมถึงการสื่อสารไปยังเจ้าของข้อมูลและผู้เกี่ยวข้อง</p>
<p>4. ต้องมีขั้นตอนปฏิบัติเรื่องการ รวบรวม และจัดเก็บหลักฐาน ที่เกี่ยวข้องับเหตุการณ์ด้าน ความมั่นคงปลอดภัยอย่าง ชัดเจน</p>	<p>ผู้ให้บริการควรจัดทำขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่ เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย</p> <p>ผู้ให้บริการควรรวบรวมบันทึกกิจกรรมที่ดำเนินการ พร้อมระบุวันเวลา และ วิธีการจัดเก็บอย่างเป็นระบบ</p>

4.1.9. วัตถุประสงค์ที่ 9 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ

เพื่อความต่อเนื่องในการบริหารจัดการความมั่นคงปลอดภัยสำหรับระบบควบคุมการประชุม

ตารางที่ 9 วัตถุประสงค์ที่ 9 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องมีแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมภายใต้สถานการณ์ฉุกเฉิน</p>	<p>ผู้ให้บริการ<u>ควร</u>จัดทำแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน เช่น เกิดเหตุภัยพิบัติ เกิดจากโจมตีทางไซเบอร์ ฯลฯ และแผนฯ <u>ควร</u>ครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย</p> <ol style="list-style-type: none"> <li>(1) ผู้เกี่ยวข้อง</li> <li>(2) ขั้นตอนการรับมือ และกู้คืนสถานการณ์</li> <li>(3) กำหนดการทดสอบแผน</li> </ol>
<p>2. ต้องมีการซ้อมแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมอย่างเหมาะสม</p>	<p>ผู้ให้บริการ<u>ควร</u>จัดให้มีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ</p>
<p>3. ต้องมีระบบสำรองที่พร้อมให้บริการอย่างต่อเนื่องและเพียงพอต่อการให้บริการ</p>	<p>ระบบสำรองของระบบควบคุมการประชุม<u>ควร</u>ทำงานทดแทนระบบหลักได้อย่างปกติ และเพียงพอต่อการใช้งานตามที่มีการประเมินความพร้อมของทรัพยากรที่ใช้</p> <p>ผู้ให้บริการ<u>ควร</u>จัดให้มีการทดสอบระบบสำรองเป็นประจำอย่างน้อย 1 ครั้งต่อปีตามขั้นตอนปฏิบัติที่กำหนดขึ้น</p>

#### 4.1.10. วัตถุประสงค์ที่ 10 การบริการจัดการความเสี่ยงสำหรับผู้ให้บริการ

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม ให้สอดคล้องกับวัตถุประสงค์ของมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

#### ตารางที่ 10 วัตถุประสงค์ที่ 10 การบริการจัดการความเสี่ยงสำหรับผู้ให้บริการ

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องกำหนดวิธีการบริหารจัดการความเสี่ยงตามมาตรฐานสากล หรือตามความเหมาะสม</p>	<p>ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการความเสี่ยง ที่ประกอบด้วย หัวข้ออย่างน้อยดังนี้</p> <ol style="list-style-type: none"> <li>(1) วัตถุประสงค์ บทบาทและหน้าที่</li> <li>(2) ขอบเขตของวิธีการบริหารจัดการความเสี่ยง</li> <li>(3) ขั้นตอนการประเมินความเสี่ยง</li> <li>(4) การประเมินผลกระทบ และโอกาสที่จะเกิดขึ้น รวมถึง ผลกระทบที่อาจส่งผลต่อการให้บริการ</li> </ol> <p>หมายเหตุ : ผู้ให้บริการอาจนำวิธีการบริหารจัดการ ความเสี่ยงตามมาตรฐานสากลมาประยุกต์ใช้ เช่น มาตรฐาน ISO 31000 หรือมาตรฐาน ISO/IEC 27005 ฯลฯ</p>
<p>2. ต้องทบทวนวิธีการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ</p>	<p>ผู้ให้บริการควรกำหนดระยะเวลาทบทวนวิธีการบริหารจัดการความเสี่ยง และวิธีการประเมินความเสี่ยงพร้อมดำเนินการ ทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตด้านความมั่นคงปลอดภัย ระบบสารสนเทศของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ</p>

## 4.2 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ

การจัดประชุมผ่านสื่อในเรื่องลับ นอกจากต้องปฏิบัติตามหัวข้อ 4.1 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไปแล้ว ให้ดำเนินการตามข้อ 4.2 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ เป็นการเพิ่มเติมด้วย

### 4.2.1. วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

เพื่อระบุสินทรัพย์ที่เกี่ยวข้องกับระบบควบคุมการประชุมและกำหนดความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

#### ตารางที่ 11 วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. <u>ต้องมีบัญชีทะเบียนสินทรัพย์</u> ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม โดยครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง</p> <p>ทั้งนี้ หากเป็นการให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ <u>ต้องมีบัญชีทะเบียนสินทรัพย์</u> ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลอยู่ในราชอาณาจักรทั้งหมด และ</p>	<p><u>ควรมีเอกสารรับรอง</u> หรือประกาศอย่างเป็นทางการ เพื่อรับรองว่าสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุมอยู่ในราชอาณาจักร ในกรณีที่ระบบควบคุมการประชุมนั้นให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ</p>

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
ต้องมีเอกสารรับรองหรือประกาศอย่างเป็นทางการ	

#### 4.2.2. วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

เพื่อจำกัดการเข้าถึงระบบควบคุมการประชุมและอุปกรณ์ประมวลผลข้อมูล

##### ตารางที่ 12 วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. <u>ต้อง</u>สามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม</p> <p>ทั้งนี้หากเป็นการประชุมลับ <u>ต้องมี</u>การรหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม</p>	<p><u>ควรมี</u>วิธีการเข้ารหัสลับข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย</p>
<p>2. <u>ต้อง</u>สามารถพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย</p> <p>ทั้งนี้หากเป็นการประชุมลับ <u>ต้องมี</u>การยืนยันตัวตนแบบหลายปัจจัย</p>	<p><u>ควร</u>จัดให้มีช่องทางพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย ด้วยวิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication) เป็นอย่างน้อย เช่น รหัสผ่านและ One-time Password (OTP) ในการเข้าร่วมประชุม ฯลฯ</p>

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>3. ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย</p> <p>ทั้งนี้หากเป็นการประชุมลับ ต้องมีการตรวจสอบรหัสผ่านที่กำหนดให้เป็นไปตามนโยบายที่กำหนดอย่างเคร่งครัด</p>	<p>ควรจัดให้มีการตรวจสอบและป้องกันการตั้งรหัสผ่านที่ไม่มั่นคงปลอดภัยของผู้ร่วมประชุม</p>



#### 4.2.3. วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

เพื่อให้มั่นใจได้ว่าการใช้งานการเข้ารหัสลับข้อมูลเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันไม่ให้ความลับหรือข้อมูลส่วนบุคคลรั่วไหล และรักษาความถูกต้องครบถ้วนของข้อมูล

##### ตารางที่ 13 วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องกำหนดนโยบายที่ระบุถึง การเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับข้อมูลบนระบบ ควบคุมการประชุม และข้อมูลส่วนบุคคลที่เกี่ยวข้อง</p> <p>ทั้งนี้หากเป็นการประชุมลับ ต้องกำหนดนโยบายที่ระบุถึง การเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง (End-to-End Encryption (E2EE))</p>	<p>ควรจัดทำนโยบายของการเข้ารหัสลับที่แสดงให้เห็นว่าผู้ให้บริการไม่สามารถเรียกดูข้อมูลในระหว่างทางของการรับส่งข้อมูล โดยอาจเปรียบเทียบการใช้งานในลักษณะ End-to-End Encryption (E2EE) ได้</p>

#### 4.2.4. วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

เพื่อให้มั่นใจว่าข้อมูลในระบบเครือข่ายและอุปกรณ์ประมวลผลของระบบควบคุมการประชุมมีความมั่นคงปลอดภัย

##### ตารางที่ 14 วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้องต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้</p> <p>ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุดังกล่าวถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง (End-to-End Encryption (E2EE))</p>	<p>ควรจัดทำนโยบายและขั้นตอนการปฏิบัติการในการควบคุมการถ่ายโอนข้อมูลการประชุมและข้อมูลส่วนบุคคลของระบบควบคุมการประชุม ควรแสดงให้เห็นว่าผู้ให้บริการไม่สามารถเรียกดูข้อมูลในระหว่างทางของการรับส่งข้อมูล โดยอาจเปรียบเทียบการใช้งานในลักษณะ End-to-End Encryption (E2EE) ได้</p>

#### 4.2.5. วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

เพื่อมั่นใจว่าการบริหารจัดการเหตุขัดข้องของระบบควบคุมการประชุมและการสื่อสารเกี่ยวกับข้อบกพร่องและสถานการณ์ด้านความมั่นคงปลอดภัย มีการควบคุมดูแลเป็นขั้นตอนและมีประสิทธิภาพ

#### ตารางที่ 15 วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

ข้อกำหนดด้านความมั่นคงปลอดภัย	แนวปฏิบัติ
<p>1. ต้องมีการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุมโดยกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลต้องมีมาตรการในการสื่อสารกับเจ้าของข้อมูลและผู้เกี่ยวข้อง</p> <p>ทั้งนี้ หากเป็นการประชุมลับต้องมีการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย รวมถึงปัญหาช่องโหว่ทางเทคนิคในระดับรุนแรงที่พบบนระบบควบคุมการประชุมครบทุกรายการก่อนให้บริการ</p>	<p><u>ควรมีการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย รวมถึงปัญหาช่องโหว่ทางเทคนิคในระดับรุนแรงที่พบบนระบบควบคุมการประชุมทุกรายการก่อนให้บริการ</u></p>

## 5. เอกสารอ้างอิง

1. “พระราชกำหนดว่าด้วยเรื่องการประชุมผ่านสื่ออิเล็กทรอนิกส์ 2563” (19 เมษายน 2563) ราชกิจจานุเบกษา เล่ม 137 ตอนที่ 30 ก หน้า 20 - 23
2. “ประกาศคณะรักษาความสงบแห่งชาติ ฉบับที่ 74/2557 เรื่อง การประชุมผ่านสื่ออิเล็กทรอนิกส์” (4 กรกฎาคม 2557) ราชกิจจานุเบกษา เล่ม 131 ตอนพิเศษ 142 ง หน้า 11 - 12
3. “ระเบียบว่าด้วยการรักษาความลับทางราชการ (ฉบับที่ 2) พ.ศ. 2561 (26 มิถุนายน 2561) ราชกิจจานุเบกษา เล่ม 135 ตอนพิเศษ 148 ง หน้า 1 - 3
4. “ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563” (... 2563) ราชกิจจานุเบกษา เล่ม ... ตอนที่ ... หน้า ...
5. คู่มือมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (มีนาคม 2563) กลุ่มงานกฎหมายและระเบียบ กองกฎหมาย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
6. European Union Agency for Network and Information Security (ENISA), Technical guidelines for the implementation of minimum security measures for Digital Service Providers, December, 2016.
7. ISO/IEC 27001:2013, Information Technology - Security Techniques – Information Security Management Systems - Requirements, 2013.
8. ISO/IEC 27002:2013, Information Technology - Security Techniques – Code of Practice for Information Security Controls, 2013.
9. ISO/IEC 27005:2018, Information technology - Security techniques - Information security risk management, 2018
10. ISO/IEC 27701:2019, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines, 2019.
11. ISO 31000:2018, Risk management – Guidelines, 2018
12. ประกาศมาตรฐานฯ เกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย เรื่อง แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน เลขที่ ชมธอ. 19-2561, 2561
13. ประกาศมาตรฐานฯ เกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย เรื่อง แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน เลขที่ ชมธอ. 20-2561, 2561
14. Tom E., Mike F., Adam P. (2019). Magic Quadrant for Meeting Solutions. *GARTNER Research*. ID G00350493.

## 6. ภาคผนวก

ตารางที่ 16 เปรียบเทียบวัตถุประสงค์ด้านความมั่นคงปลอดภัยกับมาตรฐานสากล และมาตรฐานอื่น ๆ

วัตถุประสงค์ด้านความมั่นคงปลอดภัย	ISO 27001	ENISA	ISO 27701	ชมธอ. 19	ชมธอ. 20
1. นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล	●	●	●		
2. การบริหารจัดการสินทรัพย์	●	●	●		
3. การควบคุมการเข้าถึง	●	●	●	●	●
4. การเข้ารหัสลับข้อมูล	●	●	●		
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	●	●			
6. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน	●	●			
7. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล	●	●	●		
8. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย	●	●	●		
9. ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ	●	●			
10. การบริหารจัดการความเสี่ยงสำหรับผู้ให้บริการ	●	●	●		