ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

เพื่อปรับปรุงมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม ให้สอดคล้องตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๗ ที่แก้ไขเพิ่มเติมมาตรฐานการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ เพื่อลดข้อจำกัด และเพิ่มทางเลือกในการใช้บริการระบบควบคุมการประชุมสำหรับการประชุมลับของหน่วยงานของรัฐให้เหมาะสมและมีประสิทธิภาพยิ่งขึ้น

อาศัยอำนาจตามความในข้อ ๒๔ ของประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ ซึ่งแก้ไขเพิ่มเติมโดยประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัย ของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๔ จึงให้ยกเลิกประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม ฉบับลงวันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๓ และประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๗

(นายชัยชนะ มิตรพันธ์)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

มาตรฐานการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของระบบควบคุมการประชุม

เวอร์ชัน 2.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สิงหาคม 2567

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ซึ่งมีขอบเขตครอบคลุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป และเรื่องลับ สำหรับให้ผู้ให้บริการระบบควบคุมการประชุมมีแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมที่เป็นมาตรฐานเดียวกัน และเพื่อสร้างความน่าเชื่อถือให้กับระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ ซึ่งมีความสอดคล้องตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 และที่แก้ไขเพิ่มเติม โดยมาตรฐานฯ ฉบับนี้ ได้พัฒนาอ้างอิงตามแนวมาตรฐานของ

1) ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems - Requirements, 2013.
2) ISO/IEC 27001:2022, Information Technology - Security Techniques – Information Security Management Systems - Requirements, 2022.
3) ISO/IEC 27002:2013, Information technology - Security techniques – Code of practice for information security controls, 2013.
4) ISO/IEC 27002:2022, Information Technology - Security Techniques – Code of Practice for Information Security Controls, 2022.
5) ISO/IEC 27701:2019, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines, 2019.
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) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เลขที่ มธอ.11 เล่ม 2-2566 : ข้อกำหนดของการพิสูจน์ตัวตน.
8) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เลขที่ มธอ.11 เล่ม 3-2566 : ข้อกำหนดของการยืนยันตัวตน.

นอกจากนี้ ผู้เกี่ยวข้องอาจพิจารณามาตรฐานอื่นเพิ่มเติมตามความเหมาะสมของการให้บริการ เช่น ISO/IEC 27017:2015, Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services ISO/IEC 27018:2019 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors ฯลฯ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา (อาคารบี) ชั้นที่ 6 เลขที่ 120 หมู่ที่ 3 ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
อีเมล: estandard.center@etda.or.th
เว็บไซต์: www.etda.or.th

คำนำ

เนื่องด้วยสถานการณ์การระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 ซึ่งเกิดขึ้นในหลายประเทศทั่วโลกรวมถึงประเทศไทย องค์การอนามัยโลกจึงได้ประกาศให้เป็นภาวการณ์แพร่ระบาดใหญ่ทั่วโลกในปี พ.ศ. 2562 ทำให้รัฐบาลต้องใช้มาตรการที่เข้มข้นในการควบคุมการระบาดของโรคตามคำแนะนำขององค์การอนามัยโลก โดยเฉพาะการเว้นระยะห่างทางสังคม (social distancing) ส่งผลให้การปฏิบัติงานของภาครัฐและการดำเนินกิจกรรมทางเศรษฐกิจของภาคเอกชนเกือบทุกภาคส่วนที่เกี่ยวข้องกับการประชุมเพื่อปรึกษาหารือกันตามปกติ ต้องดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ทั้งนี้ การปรับเปลี่ยนพฤติกรรมหลังการระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 ทำให้การประชุมผ่านสื่ออิเล็กทรอนิกส์กลายมาเป็นแนวทางหลักในการประชุมในยุคปัจจุบันและเป็นที่นิยมใช้มากขึ้น

หน่วยงานของรัฐและเอกชนต่างเผชิญกับความท้าทายในการเลือกระบบควบคุมการประชุมที่เหมาะสมกับองค์กรของตน ไม่ว่าจะเป็นเรื่องความสามารถของระบบ ฟังก์ชันการทำงาน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การรักษาความลับ การคุ้มครองข้อมูลส่วนบุคคล ตลอดจนการปฏิบัติตามระเบียบและกฎหมายที่เกี่ยวข้อง ทั้งนี้เพื่อตอบโจทย์ความต้องการทางธุรกิจ และลดความเสี่ยงในเรื่องต่าง ๆ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ดำเนินการจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมตามความในข้อ 24 ของประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 ซึ่งแก้ไขเพิ่มเติมโดยประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2567 เพื่อสร้างความมั่นใจให้กับหน่วยงานของรัฐและเอกชนในการใช้บริการระบบควบคุมการประชุม ทั้งนี้ มาตรฐานฯ ฉบับนี้ ได้ผ่านการพัฒนาและปรับให้เข้ากับการให้บริการของระบบควบคุมการประชุม โดยยึดหลักจากแนวมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นที่ยอมรับในระดับประเทศ และระดับสากล รวมถึงสอดคล้องกับประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 และที่แก้ไขเพิ่มเติม ด้วย

สารบัญ

สารบัญรูปภาพ

สารบัญตาราง

1. ขอบข่าย

มาตรฐานฯ ฉบับนี้ เป็นข้อกำหนดและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับระบบควบคุมการประชุม โดยครอบคลุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป และเรื่องลับ เพื่อให้ผู้ให้บริการมีแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมที่เป็นมาตรฐานเดียวกัน

มาตรฐานฯ ฉบับนี้ อ้างอิงข้อกำหนดและแนวปฏิบัติฯ จากมาตรฐานสากลและมาตรฐานอื่นที่เกี่ยวข้อง โดยมีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

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

2. บทนิยาม

2.1 การประชุมผ่านสื่ออิเล็กทรอนิกส์ หมายถึง การประชุมที่กฎหมายบัญญัติให้ต้องมีการประชุมที่ได้กระทำผ่านสื่ออิเล็กทรอนิกส์ โดยให้ผู้ร่วมประชุมที่มิได้อยู่ในสถานที่เดียวกันและสามารถประชุมปรึกษาหารือและแสดงความคิดเห็นระหว่างกันได้ผ่านสื่ออิเล็กทรอนิกส์

2.2 ผู้ร่วมประชุม หมายถึง ประธานกรรมการ รองประธานกรรมการ กรรมการ อนุกรรมการ เลขานุการและผู้ช่วยเลขานุการของคณะกรรมการ คณะอนุกรรมการ หรือคณะบุคคลอื่นตามที่กฎหมายกำหนด และให้หมายความรวมถึงผู้ซึ่งต้องชี้แจง แสดงความคิดเห็นต่อคณะกรรมการ คณะอนุกรรมการ หรือคณะบุคคลนั้นด้วย

2.3 อิเล็กทรอนิกส์ หมายถึง การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็กหรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น

2.4 ระบบควบคุมการประชุม หมายถึง ระบบเครือข่ายคอมพิวเตอร์ และ/หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เชื่อมโยงกันเป็นเครือข่าย และมีการสื่อสารข้อมูลกันโดยใช้เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือการโทรคมนาคม เพื่อให้ผู้ร่วมประชุมสามารถเข้าถึงและใช้งานสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ไม่ว่าจะเป็นการประชุมด้วยเสียงหรือทั้งเสียงและภาพ

2.5 ผู้ให้บริการ หมายถึง ผู้ให้บริการระบบควบคุมการประชุม

2.6 ผู้ควบคุมระบบ หมายถึง ผู้ทำหน้าที่ดูแลและบริหารจัดการระบบควบคุมการประชุม

3. โครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

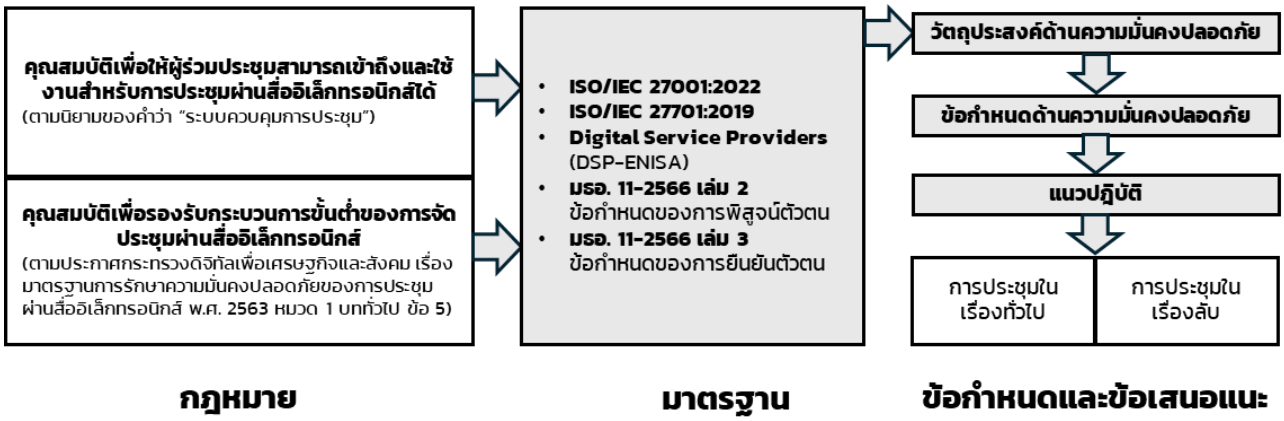
3.1 แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 ได้กำหนดนิยามของระบบควบคุมการประชุมเอาไว้เป็น “ระบบเครือข่ายคอมพิวเตอร์ และ/หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เชื่อมโยงกันเป็นเครือข่าย และมีการสื่อสารข้อมูลกันโดยใช้เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือการโทรคมนาคม เพื่อให้ผู้ร่วมประชุมสามารถเข้าถึงและใช้งานสำหรับการประชุมผ่านสื่ออิเล็กทรอนิกส์ได้ไม่ว่าจะเป็นการประชุมด้วยเสียงหรือทั้งเสียงและภาพ” ซึ่งประกาศเดียวกัน ในหมวด 1 บททั่วไป ข้อ 5 การจัดประชุมผ่านสื่ออิเล็กทรอนิกส์อย่างน้อยต้องมีกระบวนการ ดังต่อไปนี้

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

ทั้งนี้ ระบบควบคุมการประชุมจึงต้องมีคุณสมบัติต่าง ๆ เพื่อรองรับกระบวนการดังกล่าวของการจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ในส่วนที่เกี่ยวข้องด้วย

ดังนั้น มาตรฐานฯ ฉบับนี้ จึงมีเนื้อหาครอบคลุมทั้งในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม และตามกระบวนการการจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ โดยอ้างอิงจากมาตรฐานสากลและมาตรฐานอื่นที่เกี่ยวข้อง ทั้งนี้ได้จัดทำเป็นข้อกำหนดและแนวปฏิบัติโดยแยกตามการประชุมในเรื่องทั่วไป และการประชุมในเรื่องลับ รายละเอียดตามรูปที่ 1 แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม



รูปที่ 1 แนวคิดของโครงสร้างมาตรฐานการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของระบบควบคุมการประชุม

3.2 วัตถุประสงค์ของมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมเป็นข้อกำหนดและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับระบบควบคุมการประชุมของผู้ให้บริการ ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) การรักษาสภาพพร้อมใช้งาน (Availability) ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) ความน่าเชื่อถือ (Reliability) รวมถึงการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลของข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้อง หรือเกิดจากการประชุม โดยผู้ให้บริการต้องดำเนินการตามข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ แบ่งออกเป็น 10 วัตถุประสงค์ ได้แก่

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

ซึ่งวัตถุประสงค์แต่ละข้อจะประกอบด้วยข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ข้อกำหนด) แนวปฏิบัติ และความสอดคล้องของข้อกำหนดต่อมาตรฐาน หรือกระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์ที่เทียบเคียง ตามระบุในข้อ 4 "มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม"

4. มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

4.1 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป

4.1.1 วัตถุประสงค์ที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมให้สอดคล้องกับวัตถุประสงค์ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

ตารางที่ 1 วัตถุประสงค์ที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมระบบควบคุมการประชุม รวมถึงประกาศให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบ	นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ควรมีการระบุให้ชัดเจนว่าครอบคลุมระบบควบคุมการประชุม ทั้งนี้ควรมีรายละเอียดที่กำหนดตามหัวข้อดังนี้ 1) การบริหารจัดการสินทรัพย์ 2) การควบคุมการเข้าถึง 3) การเข้ารหัสลับข้อมูล 4) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม 5) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน 6) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล 7) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย 8) ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ 9) การบริหารจัดการความเสี่ยง ผู้ให้บริการควรมีการประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ร่วมประชุม และผู้เกี่ยวข้องทราบผ่านช่องทางที่มี	ISO 27001, ISO 27701

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
	ความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ	
2. ต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีการทบทวนอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน	ISO 27001, ISO 27701

4.1.2 วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

เพื่อระบุสินทรัพย์ที่เกี่ยวข้องกับระบบควบคุมการประชุมและกำหนดความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

ตารางที่ 2 วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึก หรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม	ทะเบียนสินทรัพย์ควรครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ผู้ให้บริการอาจระบุข้อมูลที่จำเป็นสำหรับการประเมินแนวทางการดูแลด้านความมั่นคงปลอดภัยด้านสารสนเทศ เช่น ความสำคัญของสินทรัพย์แต่ละรายการในเชิงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบของสินทรัพย์แต่ละรายการ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001
2. ต้องมีเงื่อนไขการเข้าใช้งานสำหรับระบบควบคุมการประชุม ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ	เงื่อนไขการเข้าใช้งานควรครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้	ISO 27001, ISO 27701

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
	สามารถนำไปปฏิบัติ ผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ	
3. ต้องมีมาตรการแสดงให้ผู้ร่วมประชุมเห็นว่าเป็นการประชุมในเรื่องทั่วไป หรือการประชุมในเรื่องลับได้อย่างชัดเจน	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงข้อมูลประเภทการประชุมว่าเป็นการประชุมในเรื่องทั่วไป หรือการประชุมในเรื่องลับ เพื่อให้ผู้ร่วมประชุมทราบ โดยอาจมีช่องทางให้ผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเอง เช่น กำหนดในหัวข้อการประชุม ผู้ให้บริการควรจัดทำคู่มือการแสดงข้อมูลประเภทการประชุมให้ผู้มีหน้าที่จัดการประชุมสามารถปฏิบัติตามได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
4. ต้องกำหนดรายการ "ข้อมูลส่วนบุคคล" ในบัญชีทะเบียนสินทรัพย์ส่วนที่เป็นข้อมูล พร้อมทั้งกำหนดลำดับชั้นความลับ และต้องมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล	บัญชีทะเบียนสินทรัพย์ควรครอบคลุมข้อมูลประเภท "ข้อมูลส่วนบุคคล" และผู้ให้บริการควรมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล เช่น การกำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึง	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701
5. ต้องมีขั้นตอนปฏิบัติสำหรับการลบหรือทำลายข้อมูลเกี่ยวกับการประชุม เมื่อมีเหตุให้ต้องดำเนินการ	ขั้นตอนปฏิบัติในการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมควรครอบคลุมการลบหรือทำลายข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีช่องทางให้ผู้มีหน้าที่จัดการประชุมดำเนินการได้เอง หรือช่องทางให้ผู้มีหน้าที่จัดการประชุมร้องขอให้ผู้ให้บริการลบหรือทำลายข้อมูลดังกล่าวได้	ISO 27001

4.1.3 วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

เพื่อจำกัดการเข้าถึงระบบควบคุมการประชุมและอุปกรณ์ประมวลผลข้อมูล

ตารางที่ 3 วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องกำหนดนโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุมอย่างมั่นคงปลอดภัย	นโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ควรครอบคลุมการเข้าถึงด้านเครือข่าย และโปรแกรมประยุกต์ เป็นอย่างน้อย ผู้ให้บริการควรประกาศนโยบายให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ	ISO 27001
2. ต้องกำหนดวิธีการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุม เพื่อให้ประธานในที่ประชุมหรือผู้ควบคุมระบบสามารถคัดกรองผู้ร่วมประชุมก่อนการประชุมได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
3. ต้องสามารถให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง ทั้งก่อนหรือระหว่างการประชุมได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
4. ต้องสามารถจำกัดและควบคุมการให้สิทธิของผู้ให้บริการ	ระบบควบคุมการประชุมควรมีมาตรการรองรับการจำกัดสิทธิของผู้ให้บริการ เช่น สิทธิการเข้าถึงข้อมูลการประชุม สิทธิในการงดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
5. ต้องสามารถแสดงสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้มีหน้าที่จัดประชุมหรือผู้ร่วมประชุมสามารถเรียกดูรายชื่อ และจำนวนผู้ร่วมประชุม เพื่อให้สามารถพิจารณาผู้เข้าร่วมได้ตลอดระยะเวลาการประชุม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
6. ต้องสามารถปรับและยกเลิกสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางในการปรับปรุง และยกเลิกสิทธิของผู้ร่วมประชุม ในระหว่างการประชุม โดยรองรับให้ประธานหรือผู้ควบคุมการประชุม สามารถดำเนินการดังนี้เป็นอย่างน้อย 1) งดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
	2) หยุดการส่งข้อมูล	
7. ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม	ระบบควบคุมการประชุมควรมีช่องทางในการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมโดยผู้ที่ได้รับอนุญาต และอาจกำหนดสิทธิในการเข้าถึงจากผู้มีหน้าที่จัดการประชุมได้เอง	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
8. ต้องสามารถแสดงตนด้วยวิธีการพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงตนด้วยวิธีการพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมแบบปัจจัยเดียว (Single-factor Authentication) เป็นอย่างน้อย เช่น รหัสผ่าน โดยหากเป็นการจัดประชุมที่มีการใช้งานอุปกรณ์เพื่อเชื่อมต่อสถานที่มากกว่า 1 ที่ขึ้นไป เช่น Multipoint Control Unit (MCU) อุปกรณ์ที่ติดตั้งควรมีการตั้งค่าเพื่อจำกัดการเข้าใช้งานเฉพาะอุปกรณ์ และเครือข่ายที่เกี่ยวข้อง เป็นอย่างน้อย ทั้งนี้ผู้ร่วมประชุมสามารถพิสูจน์ยืนยันและตัวตนของผู้ร่วมประชุมด้วยการรับรองการแสดงตนของผู้ร่วมประชุมด้วยกัน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
9. ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย	ระบบควบคุมการประชุมควรมีการระบุถึงนโยบายการตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย เช่น รหัสผ่านที่มั่นคงปลอดภัยประกอบไปด้วยตัวอักษร ตัวเลข และอักขระพิเศษ	ISO 27001

4.1.4 วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

เพื่อให้มั่นใจได้ว่าการใช้งานการเข้ารหัสลับข้อมูลเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันไม่ให้ความลับหรือข้อมูลส่วนบุคคลรั่วไหล และรักษาความถูกต้องครบถ้วนของข้อมูล

ตารางที่ 4 วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องกำหนดนโยบายด้านการเข้ารหัสลับข้อมูลที่ระบุถึงการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับข้อมูลบนระบบควบคุมการประชุม และข้อมูลส่วนบุคคลที่เกี่ยวข้อง	นโยบายควรระบุให้ครอบคลุมถึงการเข้ารหัสลับของข้อมูลที่เกี่ยวข้องกับการประชุม และข้อมูลส่วนบุคคล ด้วยวิธีการที่ได้รับการยอมรับตามมาตรฐานสากล และครอบคลุมกระบวนการเข้ารหัสลับข้อมูลในรูปแบบดังต่อไปนี้เป็นอย่างน้อย 1) การเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย (data-in-transit encryption) 2) การเข้ารหัสลับของข้อมูลที่จัดเก็บ (data-at-rest encryption)	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001
2. ต้องบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูล เพื่อการป้องกันการเข้าถึงกุญแจสำหรับเข้ารหัสลับข้อมูล ทั้งแบบระบบรหัสแบบสมมาตร (Symmetric Key Cryptography) และ ระบบรหัสแบบอสมมาตร (Asymmetric Key Cryptography) อย่างน้อย กุญแจที่ใช้ในการเข้ารหัสลับข้อมูลในแต่ละการประชุมควรแตกต่างกัน และไม่มีการใช้ซ้ำ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001

4.1.5 วัตถุประสงค์ที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

เพื่อป้องกันความเสียหาย การเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การแทรกแซงระบบและอุปกรณ์ประมวลผลข้อมูลของระบบควบคุมการประชุม

ตารางที่ 5 วัตถุประสงค์ที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องมีขั้นตอนปฏิบัติสำหรับการเข้าถึงพื้นที่มั่นคงปลอดภัย (Secure areas)	ขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมกระบวนการที่สำคัญ เช่น การลงชื่อเข้าและออกพื้นที่ การตรวจสอบความผิดปกติของการเข้าพื้นที่	ISO 27001

4.1.6 วัตถุประสงค์ที่ 6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

เพื่อให้มั่นใจว่าการดำเนินงานของระบบควบคุมการประชุมมีความถูกต้องและมั่นคงปลอดภัย

ตารางที่ 6 วัตถุประสงค์ที่ 6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องมีคู่มือการใช้งานของระบบควบคุมการประชุม และเผยแพร่ให้ผู้เกี่ยวข้องสามารถนำไปปฏิบัติได้	ผู้ให้บริการควรจัดทำเอกสารของขั้นตอนปฏิบัติที่เกี่ยวข้องกับระบบควบคุมการประชุมอย่างชัดเจน รวมถึงการบริหารจัดการเอกสาร เช่น การปรับปรุงเอกสาร การจัดเก็บเอกสาร ช่องทางการเข้าถึงและสิทธิที่เกี่ยวข้อง	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001
2. ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารการเปลี่ยนแปลงของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมการประเมินผลกระทบ การมอบหมายการปรับปรุง การอนุมัติจากผู้ที่มีอำนาจ การวางแผนสำรอง และการทดสอบ เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล	ISO 27001
3. ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารจัดการทรัพยากรของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารขีดความสามารถของระบบควบคุมการประชุมควรครอบคลุมการติดตาม ปรับปรุง และคาดการณ์ความต้องการในการใช้ทรัพยากรของระบบ เพื่อให้สามารถวางแผนการใช้	ISO 27001

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
	งานทรัพยากรให้รองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ	
4. ต้องควบคุมสภาพแวดล้อมของการพัฒนา การทดสอบ และการใช้งานจริง ซึ่งแบ่งแยกออกจากกัน	ผู้ให้บริการควรจัดให้มีการแยกสภาพแวดล้อมส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบควบคุมการประชุม ในแต่ละส่วนออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต และควรกำหนดสิทธิในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน	ISO 27001
5. ต้องสามารถรับมือกับภัยคุกคามประเภทมัลแวร์	ผู้ให้บริการควรจัดให้มีวิธีการตรวจจับ การป้องกัน และการกู้คืน ที่เกิดขึ้นจากภัยคุกคามจากโปรแกรมไม่พึงประสงค์ต่อระบบควบคุมการประชุม เช่น การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) การติดตั้งระบบตรวจจับภัยคุกคาม (Intrusion Detection System) การสำรองข้อมูล	ISO 27001
6. ต้องมีขั้นตอนปฏิบัติเรื่องการสำรองข้อมูลและการกู้คืนข้อมูลของระบบควบคุมการประชุม กรณีที่มีข้อมูลส่วนบุคคลต้องมีการกำหนดผู้ดำเนินการสำรองข้อมูล และกู้คืนข้อมูลส่วนบุคคลด้วย รวมถึงต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลที่สำรองให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ขั้นตอนปฏิบัติเรื่องการสำรองข้อมูล และการกู้คืนข้อมูลของระบบควบคุมการประชุมควรครอบคลุมรายการบัญชีทะเบียนสินทรัพย์ที่จำเป็นต้องมีการสำรองข้อมูล วิธีการสำรองข้อมูล พร้อมระบุช่วงเวลาที่ต้องจัดเก็บข้อมูลที่สำรอง รวมถึงแนวทางการทดสอบการกู้คืนอย่างเหมาะสม โดยกรณีที่การสำรองนั้นมีข้อมูลส่วนบุคคลอยู่ด้วย ควรมีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรม เช่น ผู้ดำเนินการสำรองข้อมูล ผู้ทดสอบการกู้คืนข้อมูล ทั้งนี้ ระบบควบคุมการประชุมควรถูกกำหนดให้มีการสำรองข้อมูลบันทึกประเภทเสียงหรือทั้งเสียงและภาพ ข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงข้อมูลอื่นที่เกี่ยวข้อง เช่น ข้อมูลการแจ้งเหตุขัดข้องระหว่างการประชุม ฯลฯ อย่างน้อยเป็นระยะเวลา 7 วันนับแต่วันสิ้นสุดการประชุมในแต่ละครั้ง และควรประกาศระยะเวลาในการจัดเก็บข้อมูลที่สำรองให้ผู้เกี่ยวข้องทราบอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001, ISO 27701

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
7. ต้องจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ และต้องมีการทบทวนอย่างเหมาะสม	ระบบควบคุมการประชุมควรถูกตั้งค่าให้จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยอย่างน้อยต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคล หรือชื่อผู้ใช้งาน (Username) วันและเวลาของการเข้าร่วมประชุม และเลิกประชุมเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล ผู้ให้บริการควรมีการกำหนดรอบของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างน้อย 1 ครั้ง ต่อปี	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001
8. ต้องมีการดูแลข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยอย่างน้อยต้องสามารถระบุผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการใช้หรือประมวลผล	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน โดยครอบคลุมข้อมูลผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการ เป็นอย่างน้อย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701
9. ต้องป้องกันการเปลี่ยนแปลง และการเข้าถึงที่ไม่ได้รับอนุญาต ต่อข้อมูลจราจรอิเล็กทรอนิกส์	ผู้ให้บริการควรจัดเตรียมวิธีป้องกัน การเปลี่ยนแปลง การเข้าถึง การลบ โดยไม่ได้รับอนุญาตต่อข้อมูลจราจรอิเล็กทรอนิกส์ เช่น การจำกัดสิทธิการดำเนินการในแต่ละฟังก์ชันการทำงาน การเฝ้าระวังและแจ้งเตือนการเข้าใช้งานที่ผิดปกติ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001
10. ต้องจำกัดการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงกำหนดระยะเวลาในการลบหรือเปลี่ยนรูปข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยครอบคลุมการบันทึกกิจกรรมที่เกี่ยวข้อง เช่น การเข้าถึงข้อมูลส่วนบุคคล ผู้ให้บริการควรกำหนดระยะเวลาที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระบบควบคุมการประชุม และแจ้งเงื่อนไขดังกล่าวให้ผู้มีหน้าที่จัดการประชุม หรือผู้ร่วมประชุมทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ พร้อมกำหนดวิธีการลบ หรือการเปลี่ยนแปลงรูปแบบข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ร่วมด้วย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
11. ต้องมีการจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์จากการใช้งานของผู้ควบคุมระบบและผู้ให้บริการ รวมถึงมีการทบทวนอย่างเหมาะสม โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบ	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ควบคุมระบบ และควรประกาศ หรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ โดยครอบคลุมกิจกรรมดังต่อไปนี้เป็นอย่างน้อย 1) บันทึกการทำงานของระบบ (system logs) 2) บันทึกการเข้าออกระบบ (login-logout logs) 3) บันทึกการพยายามเข้าสู่ระบบ (login attempts logs) 4) บันทึกปัญหาหรือความผิดพลาดต่าง ๆ (fault logs) ผู้ให้บริการควรมีการกำหนดช่วงเวลาของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างเหมาะสม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001
12. ต้องสามารถตั้งค่า Clock synchronization ของระบบควบคุมการประชุมให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล และเป็นแหล่งเทียบเวลาในระดับ (stratum) เดียวกันทั้งระบบควบคุมการประชุม	ระบบควบคุมการประชุมควรถูกตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล เช่น สถาบันมาตรวิทยาแห่งชาติ รวมถึงควรเป็นแหล่งเทียบเวลาในระดับ (stratum) เดียวกันทั้งระบบควบคุมการประชุม เช่น ตั้งค่าการใช้งานระดับ stratum-1 ให้เหมือนกันทั้งระบบควบคุมการประชุม	ISO 27001
13. ต้องจัดการช่องโหว่ทางเทคนิคของระบบควบคุมการประชุม โดยต้องได้รับการแก้ไขอย่างมีประสิทธิภาพ	ผู้ให้บริการควรกำหนดช่องทางในการรับแจ้งช่องโหว่ และดำเนินกิจกรรมการประเมินผลกระทบ การจัดการช่องโหว่ เมื่อมีผู้แจ้งเหตุอย่างทันท่วงที พร้อมเผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ ผู้ให้บริการควรมีการตรวจสอบช่องโหว่ทางเทคนิคของระบบควบคุมการประชุมอย่างน้อย 1 ครั้งต่อปี หรือเมื่อระบบควบคุมการประชุมมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้แน่ใจว่าระบบควบคุม	ISO 27001

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
	การประชุมไม่มีความเสี่ยงรุนแรงที่อาจส่งผลต่อการให้บริการ หรือกระทบต่อข้อมูลส่วนบุคคล	
14. ต้องทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม เช่น การตรวจประเมินภายใน (internal audit) อย่างน้อย 1 ครั้งต่อปี	ISO 27001

4.1.7 วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

เพื่อให้มั่นใจว่าการสื่อสารข้อมูลในระบบเครือข่ายและอุปกรณ์ประมวลผลของระบบควบคุมการประชุมมีความมั่นคงปลอดภัย

ตารางที่ 7 วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องบริหารจัดการเครือข่ายอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดให้มีการบริหารจัดการเครือข่าย โดยครอบคลุมมาตรการดังต่อไปนี้เป็นอย่างน้อย 1) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต 2) การป้องกันการดักรับข้อมูล 3) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย 4) การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล 5) การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ป้องกันมัลแวร์	ISO 27001
2. ต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่ายและขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วน	นโยบายและขั้นตอนปฏิบัติควรครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโอนย้ายข้อความ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย ขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการเข้าถึงข้อมูลบนเครือข่ายควรกำหนดวิธีการ และช่องทางการดำเนินการอย่างชัดเจน โดยอาจกับการเชื่อมโยง	ISO 27001

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
บุคคลเกี่ยวข้อง ต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้	แผนภาพเครือข่าย เพื่อให้แน่ใจว่าครอบคลุมการดำเนินการของระบบควบคุมการประชุม รวมถึงกรณีที่มีข้อมูลส่วนบุคคลที่รับส่งอยู่บนเครือข่ายควรมีการบันทึกกิจกรรมการดำเนินการ พร้อมผู้รับผิดชอบให้ชัดเจน	

4.1.8 วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

เพื่อให้มั่นใจว่าการบริหารจัดการเหตุขัดข้องของระบบควบคุมการประชุมและการสื่อสารเกี่ยวกับข้อบกพร่องและสถานการณ์ด้านความมั่นคงปลอดภัย มีการควบคุมดูแลเป็นขั้นตอนและมีประสิทธิภาพ

ตารางที่ 8 วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องมีขั้นตอนปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม โดยหากพบว่ามีข้อมูลส่วนบุคคลรั่วไหล ต้องมีมาตรการในการจัดการอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดทำขั้นตอนการปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมที่ครอบคลุมกระบวนการดังต่อไปนี้เป็นอย่างน้อย 1) การรับแจ้งและยืนยันเหตุฯ 2) การจำแนกเหตุฯ และประเมินผลกระทบ 3) การตอบสนองต่อเหตุฯ 4) การจัดเก็บพยานหลักฐาน ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการระบุเพิ่มเติมถึงความรับผิดชอบในแต่ละกระบวนการ ข้อมูลที่รั่วไหล การรายงานเหตุฯ ไปยังผู้เกี่ยวข้อง เป็นอย่างน้อย	ISO 27001, ISO 27701
2. ต้องมีการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม	ผู้ให้บริการควรจัดให้มีช่องทางการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม โดยข้อมูลที่แจ้งควรคลอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย 1) รายละเอียดผู้แจ้งเหตุฯ 2) วันเวลาที่พบเหตุฯ 3) รายละเอียดของเหตุฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
3. ต้องมีมาตรการสำหรับการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลต้องมีการสื่อสารกับเจ้าของข้อมูลและผู้เกี่ยวข้อง	ผู้ให้บริการควรกำหนดวิธีการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยพิจารณาถึงองค์ประกอบดังต่อไปนี้เป็นอย่างน้อย 1) การประเมินผลกระทบของเหตุฯ 2) แนวทาง และช่องทางในการแจ้งเหตุฯ 3) การบันทึกเหตุฯ โดยให้มีการระบุรายละเอียด คำอธิบายเหตุการณ์ ช่วงเวลา ผลกระทบ ช่วงเวลาที่เกิดผลกระทบ ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการดำเนินการเพิ่มเติมอย่างน้อยในกระบวนการการสื่อสารไปยังเจ้าของข้อมูล และผู้เกี่ยวข้อง	ISO 27001
4. ต้องมีขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างชัดเจน	ผู้ให้บริการควรจัดทำขั้นตอนปฏิบัติเรื่องการรวบรวมและจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ให้บริการควรรวบรวมบันทึกกิจกรรมที่ดำเนินการพร้อมระบุวันเวลา และวิธีการจัดเก็บอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001

4.1.9 วัตถุประสงค์ที่ 9 ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ

เพื่อความต่อเนื่องในการให้บริการระบบควบคุมการประชุม

ตารางที่ 9 วัตถุประสงค์ที่ 9 ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องมีแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน	ผู้ให้บริการควรจัดทำแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมภายใต้สถานการณ์ฉุกเฉิน เช่น เกิดเหตุภัยพิบัติ เกิดจากโจมตีทางไซเบอร์ และแผนฯ ควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย 1) ผู้เกี่ยวข้อง 2) ขั้นตอนการรับมือ และกู้คืนเหตุฯ 3) กำหนดการทดสอบแผนฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
2. ต้องมีการซ้อมแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001
3. ต้องมีระบบสำรองที่พร้อมให้บริการอย่างต่อเนื่องและเพียงพอต่อการให้บริการ	ระบบสำรองของระบบควบคุมการประชุมควรทำงานทดแทนระบบหลักได้อย่างปกติ และเพียงพอต่อการใช้งานตามที่มีการประเมินความพร้อมของทรัพยากรที่ใช้ ผู้ให้บริการควรจัดให้มีการทดสอบระบบสำรองเป็นประจำอย่างน้อย 1 ครั้งต่อปี ตามขั้นตอนปฏิบัติที่กำหนดขึ้น	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001

4.1.10 วัตถุประสงค์ที่ 10 การบริการจัดการความเสี่ยงสำหรับผู้ให้บริการ

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม ให้สอดคล้องกับวัตถุประสงค์ของมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม

ตารางที่ 10 วัตถุประสงค์ที่ 10 การบริการจัดการความเสี่ยงสำหรับผู้ให้บริการ

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องกำหนดวิธีการบริหารจัดการความเสี่ยงตามมาตรฐานสากล หรือตามความเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการความเสี่ยง ที่ประกอบด้วย หัวข้ออย่างน้อยดังนี้ 1) วัตถุประสงค์ บทบาทและหน้าที่ 2) ขอบเขตของวิธีการบริหารจัดการความเสี่ยง 3) ขั้นตอนการประเมินความเสี่ยง 4) การประเมินผลกระทบ และโอกาสที่จะเกิดขึ้น รวมถึง ผลกระทบที่อาจส่งผลต่อการให้บริการ หมายเหตุ : ผู้ให้บริการอาจนำวิธีการบริหารจัดการความเสี่ยงตามมาตรฐานสากลมาประยุกต์ใช้ เช่น มาตรฐาน ISO 31000 หรือมาตรฐาน ISO/IEC 27005	ISO 27001

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
2. ต้องทบทวนวิธีการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ	ผู้ให้บริการควรกำหนดระยะเวลาทบทวนวิธีการบริหารจัดการความเสี่ยง และวิธีการประเมินความเสี่ยง พร้อมดำเนินการทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน	ISO 27001

4.2 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ

การจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ นอกจากต้องปฏิบัติตามหัวข้อ 4.1 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไปแล้ว ยังต้องดำเนินการตามข้อกำหนดเพิ่มเติมที่ระบุในวัตถุประสงค์ดังต่อไปนี้

(1) วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

(2) วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

(3) วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

(4) วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

(5) วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

4.2.1 วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

เพื่อระบุสินทรัพย์ที่เกี่ยวข้องกับระบบควบคุมการประชุมและกำหนดความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

ตารางที่ 11 วัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม โดยครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง	ทะเบียนสินทรัพย์ควรครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์

4.2.2 วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

เพื่อจำกัดการเข้าถึงระบบควบคุมการประชุมและอุปกรณ์ประมวลผลข้อมูล

ตารางที่ 11 วัตถุประสงค์ที่ 3 การควบคุมการเข้าถึง

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
2. ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม และต้องมีการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม	ระบบควบคุมการประชุมควรมีวิธีการเข้ารหัสลับข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
3. ต้องสามารถพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย และต้องมีการยืนยันตัวตนแบบหลายปัจจัย	ระบบควบคุมการประชุมควรมีช่องทางพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย ด้วยวิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication) เป็นอย่างน้อย เช่น รหัสผ่านและ One-time Password (OTP) ในการเข้าร่วมประชุม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
4. ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย และต้องมีการตรวจสอบรหัสผ่านที่กำหนดให้เป็นไปตามนโยบายที่กำหนดอย่างเคร่งครัด	ระบบควบคุมการประชุมควรมีความสามารถในการตรวจสอบ และป้องกันการตั้งรหัสผ่านที่ไม่มั่นคงปลอดภัยของผู้ร่วมประชุมตามนโยบายการตั้งค่ารหัสผ่านที่กำหนด	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์

4.2.3 วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

เพื่อให้มั่นใจได้ว่าการใช้งานการเข้ารหัสลับข้อมูลเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันไม่ให้ความลับหรือข้อมูลส่วนบุคคลรั่วไหล และรักษาความถูกต้องครบถ้วนของข้อมูล

ตารางที่ 12 วัตถุประสงค์ที่ 4 การเข้ารหัสลับข้อมูล

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องกำหนดนโยบายด้านการเข้ารหัสลับข้อมูลซึ่งระบุถึง (1) การเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับข้อมูลบนระบบควบคุมการประชุม	นโยบายควรระบุให้ครอบคลุมว่าผู้ให้บริการไม่สามารถเรียกดูข้อมูลในระหว่างทางของการรับส่งข้อมูล โดยอาจเปรียบเทียบการใช้งานในลักษณะ End-to-End Encryption (E2EE) ได้ และควรระบุขอบเขต ข้อยกเว้นในความสามารถที่เกี่ยวข้องให้ชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001, ISO 27701

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
และข้อมูลส่วนบุคคลที่เกี่ยวข้อง (2) การเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้		

4.2.4 วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

เพื่อให้มั่นใจว่าข้อมูลในระบบเครือข่ายและอุปกรณ์ประมวลผลของระบบควบคุมการประชุมมีความมั่นคงปลอดภัย

ตารางที่ 13 วัตถุประสงค์ที่ 7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้อง ต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้ และต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายและขั้นตอนปฏิบัติควรระบุให้ครอบคลุมว่าผู้ให้บริการไม่สามารถเรียกดูข้อมูลในระหว่างทางของการรับส่งข้อมูล โดยอาจเปรียบเทียบการใช้งานในลักษณะ End-to-End Encryption (E2EE) ได้ และควรระบุขอบเขต ข้อยกเว้นในความสามารถที่เกี่ยวข้องให้ชัดเจน	ISO 27001, ISO 27701

4.2.5 วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

เพื่อมั่นใจว่าการบริหารจัดการเหตุขัดข้องของระบบควบคุมการประชุมและการสื่อสารเกี่ยวกับข้อบกพร่องและสถานการณ์ด้านความมั่นคงปลอดภัย มีการควบคุมดูแลเป็นขั้นตอนและมีประสิทธิภาพ

ตารางที่ 14 วัตถุประสงค์ที่ 8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง
1. ต้องมีมาตรการสำหรับการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลต้องมีการสื่อสารกับเจ้าของข้อมูลและผู้เกี่ยวข้อง และต้องดำเนินการแก้ไขปัญหาช่องโหว่ทางเทคนิคในระดับรุนแรง (อ้างอิงตามข้อมูล CVSS ที่ severity ระดับ high ขึ้นไป) ให้ครบทุกรายการก่อนให้บริการ	ผู้ให้บริการควรดำเนินการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงปัญหาช่องโหว่ทางเทคนิค อย่างน้อยช่องโหว่ที่เผยแพร่ตามรายการ CVE (Common Vulnerabilities and Exposures) และช่องโหว่ที่มีการตรวจประเมินจากผู้ให้บริการ ในระดับรุนแรงอ้างอิงตามข้อมูล CVSS ที่ severity ระดับ high ขึ้นไป ให้ครบทุกรายการก่อนให้บริการ	ISO 27001, ISO 27701

5. บรรณานุกรม

1. พระราชกำหนดว่าด้วยเรื่องการประชุมผ่านสื่ออิเล็กทรอนิกส์ 2563.
2. ประกาศคณะรักษาความสงบแห่งชาติ ฉบับที่ 74/2557 เรื่อง การประชุมผ่านสื่ออิเล็กทรอนิกส์.
3. ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544 แก้ไขเพิ่มเติม ฉบับที่ 2 พ.ศ. 2561.
4. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563.
5. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2564.
6. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2567.
7. คู่มือมาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (มีนาคม 2563) กลุ่มงานกฎหมายและระเบียบ กองกฎหมาย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.
8. European Union Agency for Network and Information Security (ENISA), Technical guidelines for the implementation of minimum security measures for Digital Service Providers, December, 2016.
9. ISO/IEC 27001:2022, Information Technology - Security Techniques – Information Security Management Systems - Requirements, 2022.
10. ISO/IEC 27002:2022, Information Technology - Security Techniques – Code of Practice for Information Security Controls, 2022.
11. ISO/IEC 27005:2018, Information technology - Security techniques - Information security risk management, 2018.
12. ISO/IEC 27701:2019, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines, 2019.
13. ISO 31000:2018, Risk management – Guidelines, 2018.
14. มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เลขที่ มธอ.11 เล่ม 2-2566 : ข้อกำหนดของการพิสูจน์ตัวตน.
15. มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เลขที่ มธอ.11 เล่ม 3-2566 : ข้อกำหนดของการยืนยันตัวตน.
16. Tom E., Mike F., Adam P. (2019). Magic Quadrant for Meeting Solutions. GARTNER Research. ID G00350493.

6. ภาคผนวก

ตารางที่ 15 เปรียบเทียบวัตถุประสงค์การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กับมาตรฐานต่าง ๆ

วัตถุประสงค์การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	ISO 27001	ENISA	ISO 27701	มธอ. 11-2566 เล่ม 2	มธอ. 11-2566 เล่ม 3
1. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล	●	●	●		
2. การบริหารจัดการสินทรัพย์	●	●	●		
3. การควบคุมการเข้าถึง	●	●	●	●	●
4. การเข้ารหัสลับข้อมูล	●	●	●		
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	●	●			
6. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน	●	●			
7. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล	●	●	●		
8. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย	●	●	●		
9. ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ	●	●			
10. การบริหารจัดการความเสี่ยงสำหรับผู้ให้บริการ	●	●	●		

ประวัติการแก้ไข

เวอร์ชัน	วันที่แก้ไข	รายละเอียด
1.1	-	– เวอร์ชันที่เผยแพร่ครั้งแรก
2.0	สิงหาคม 2567	– ปรับแก้เอกสารอ้างอิง โดย 1) เพิ่มเติมการอ้างอิงประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2567 2) เพิ่มเติมการอ้างอิงมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27002:2022 3) ปรับปรุงการอ้างอิงเอกสาร ขมธอ. 19-2561 เป็น มธอ. 11-2566 เล่ม 2 และ ขมธอ. 20-2561 เป็น มธอ. 11-2566 เล่ม 3 – ปรับปรุงโครงสร้างเอกสาร โดยตัดรายละเอียดเกี่ยวกับการประชุมในเรื่องลับที่ปรากฏอยู่ในข้อกำหนดสำหรับการประชุมในเรื่องทั่วไปออก – ปรับแก้ข้อ 4.2 การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับในวัตถุประสงค์ที่ 2 การบริหารจัดการสินทรัพย์ โดยตัดข้อกำหนดที่เกี่ยวกับการประชุมเรื่องที่มีชั้นความลับหน่วยงานของรัฐ