แบบประเมินความสอดคล้องของระบบควบคุมการประชุมกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม เวอร์ชัน 1.1 กรณี ประเมินความสอดคล้องด้วยตนเอง

ชื่อระบบ :	**DAP e-Shareholder Meeting**
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท) :	**บริษัท ดิจิทัล แอคเซส แพลตฟอร์ม จำกัด (DAP)**
ช่องทางการติดต่อผู้ให้บริการ :	**Email: DAPOperation@set.or.th เบอร์โทรศัพท์ 02-009-9888 กด 1**
วันที่ประเมินความสอดคล้อง	**1 มกราคม 2566**
ประเภทการประเมินความสอดคล้องด้วยตนเอง	☑ การประชุมทั่วไป ☐ การประชุมลับ ☐ การประชุมลับ (ภาครัฐ)
ประเภทของระบบการให้บริการ	☑ On-Cloud ☐ On-Premise ☐ อื่น ๆ โปรดระบุ
มาตรฐานที่ได้รับการรับรอง	☐ ISO/IEC 27001 ☐ ISO/IEC 27701 ☐ อื่น ๆ โปรดระบุ
คุณลักษณะของระบบที่ประเมินความสอดคล้องด้วยตนเอง :	**ระบบ DAP e-Sharholder Meeting เป็นระบบควบคุมการประชุมสำหรับการประชุมสามัญ/วิสามัญผู้ถือหุ้นผ่านสื่ออิเล็กทรอนิกส์ โดยมีรูปแบบการให้บริการ On-Cloud** **ขอบเขตการประเมินสอดคล้องตามมาตรฐานความมั่นคงปลอดภัยของระบบควบคุมการประชุม พ.ศ. 2563 ครอบคลุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป โดยให้บริการร่วมกับการระบบประชุม Conference Microsoft 365 - Microsoft Teams ซึ่งเป็นระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ที่ได้รับการรับรอง และ Cisco Webex ซึ่งเป็นผู้ประเมินความสอดคล้องด้วยตนเอง** **หมายเหตุ: รายละเอียดสามารถดูได้ที่เว็บไซต์สำนักงานพัฒนาธุรธรรมทางอิเล็กทรอนิกส์ https://www.etda.or.th/th/Our-Service/e-meeting/announce.aspx**

หมายเหตุ : ผู้ให้บริการพิจารณาข้อกำหนดตามมาตรฐาน และทำการประเมินความสามารถของระบบด้วยตนเอง โดย สพธอ. ไม่ได้เข้าไปรับรองว่าระบบมีความสามารถสอดคล้องตามมาตรฐาน

ข้อกำหนด		แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและนโยบายการคุ้มครองข้อมูลส่วนบุคคล				
1.1	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 และผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001, ISO 27701	DAP ได้จัดทำนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล เป็นไปตามมาตรฐาน ISO โดยมีนโยบายครอบคลุมเรื่องต่าง ๆ ดังนี้ (1) การบริหารจัดการสินทรัพย์ (2) การควบคุมการเข้าถึง (3) การเข้ารหัสลับข้อมูล (4) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (5) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (6) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (7) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (8) ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (9) การบริหารจัดการความเสี่ยง โดยมีรายละเอียดนโยบายตามเอกสารอ้างอิงดังนี้ https://portal.eservice.set.or.th/documents/index.html คลิกที่นโยบายการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ และนโยบายคุ้มครองข้อมูลส่วนบุคคล
1.2	ต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีการทบทวนอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ	ISO 27001, ISO 27701	DAP มีการกำหนดแผนงานในการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล อย่างน้อย 1 ครั้งต่อปี และเมื่อมีการเปลี่ยนแปลงที่สำคัญ
2 การบริหารจัดการสินทรัพย์				
2.1	ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึก หรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ทั้งนี้ หากเป็นการให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ ต้องมีบัญชีทะเบียนสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลอยู่ในราชอาณาจักรทั้งหมด และต้องมีเอกสารรับรองหรือประกาศอย่างเป็นทางการ	ทะเบียนสินทรัพย์ควรครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ผู้ให้บริการอาจระบุข้อมูลที่จำเป็นสำหรับการประเมินแนวทางการดูแลด้านความมั่นคงปลอดภัยด้านสารสนเทศ เช่น ความสำคัญของสินทรัพย์แต่ละรายการในเชิงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบของสินทรัพย์แต่ละรายการ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP ได้จัดทำบัญชีทะเบียนสินทรัพย์ที่ครอบคลุมสินทรัพย์ทางกายภาพ เครือข่าย, ระบบปฏิบัติการ, โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง โดยจะมีการปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ
2.2	ต้องมีเงื่อนไขการเข้าใช้งานสำหรับระบบควบคุมการประชุม ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ	เงื่อนไขการเข้าใช้งานควรครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ ผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001, ISO 27701	DAP ได้จัดทำเงื่อนไขการใช้บริการระบบการควบคุมการประชุม ซึ่งครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล โดยได้มีการเผยแพร่ให้ผู้เข้าร่วมประชุมและผู้ที่เกี่ยวข้องทราบและนำไปปฏิบัติก่อนเริ่มใช้บริการ โดยมีรายละเอียดเงื่อนไขการใช้บริการตามเอกสารอ้างอิงดังนี้ https://portal.eservice.set.or.th/documents/index.html คลิกที่เงื่อนไข และข้อตกลง
2.3	ต้องมีมาตรการแสดงให้ผู้ร่วมประชุมเห็นว่าเป็นการประชุมทั่วไป หรือการประชุมลับได้อย่างชัดเจน	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงข้อมูลประเภทการประชุมว่าเป็นการประชุมทั่วไป หรือการประชุมลับ เพื่อให้ผู้ร่วมประชุมทราบ โดยอาจมีช่องทางให้ผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเอง เช่น กำหนดในหัวข้อการประชุม ฯลฯ ผู้ให้บริการควรจัดทำคู่มือการแสดงข้อมูลประเภทการประชุมให้ผู้มีหน้าที่จัดการประชุมสามารถปฏิบัติตามได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	- การประชุมสามัญผู้ถือหุ้น (AGM) / การประชุมวิสามัญผู้ถือหุ้น (EGM) ทุกวาระการประชุม เป็นการประชุมแบบทั่วไป โดยผู้จัดประชุมจะจัดทำและส่งหนังสือเชิญประชุมผู้ถือหุ้น แจ้งให้ผู้เข้าร่วมประชุมทราบว่าเป็นการประชุมทั่วไปหรือการประชุมลับอยู่แล้ว - ระบบ DAP e-Shareholder Meeting สามารถแสดงให้ผู้ร่วมประชุมทราบได้ว่าเป็นการประชุมทั่วไป หรือการ ประชุมลับ โดยผ่านช่องทางการประกาศในช่อง Chat ในห้องประชุม และผู้ที่จะเข้าร่วมการประชุมลับได้จะต้องได้อนุญาตจากผู้จัดประชุมก่อนเท่านั้น
2.4	ต้องกำหนดรายการ "ข้อมูลส่วนบุคคล" ในบัญชีทะเบียนสินทรัพย์ส่วนที่เป็นข้อมูล พร้อมทั้งกำหนดลำดับชั้นความลับ และต้องมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล	บัญชีทะเบียนสินทรัพย์ควรครอบคลุมข้อมูลประเภท "ข้อมูลส่วนบุคคล" และผู้ให้บริการควรมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล เช่น การกำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	DAP มีมาตรการในการจัดการบัญชีทะเบียนสินทรัพย์ครอบคลุมข้อมูลประเภทข้อมูลส่วนบุคคล และมีมาตรการในการจัดลำดับชั้นความลับ รวมถึงการกำหนดสิทธิในการเข้าถึงข้อมูลตามประเภทผู้ใช้งาน โดยแบ่งเป็น Admin ผู้ดูแลระบบ และผู้ใช้งานระบบ
2.5	ต้องมีขั้นตอนปฏิบัติสำหรับการลบหรือทำลายข้อมูลเกี่ยวกับการประชุม เมื่อมีเหตุให้ต้องดำเนินการ	ขั้นตอนปฏิบัติในการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมควรครอบคลุมการลบหรือทำลายข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีช่องทางให้ผู้มีหน้าที่จัดการประชุมดำเนินการได้เอง หรือช่องทางให้ผู้มีหน้าที่จัดการประชุมร้องขอให้ผู้ให้บริการลบหรือทำลายข้อมูลดังกล่าวได้	ISO 27001	- DAP ได้กำหนดเงื่อนไขการให้บริการ โดยภายหลังจากเสร็จสิ้นการประชุม DAP จะจัดส่งข้อมูลที่เกี่ยวข้องกับการประชุมให้แก่ผู้จัดประชุม และระบบควบคุมการประชุมจะเก็บข้อมูลดังกล่าวต่อไปอีก 30 วัน หลังจากนั้นจะลบหรือทำลายข้อมูลดังกล่าวออกจากระบบควบคุมการประชุม - DAP มีช่องทางให้ผู้จัดประชุมสามารถร้องขอให้ DAP ลบหรือทำลายข้อมูลดังกล่าวได้ก่อนครบกำหนดระยะเวลาข้างต้นได้ด้วย - DAP จัดให้มีช่องทางการร้องขอโดยผู้ใช้บริการสามารถแจ้งความประสงค์ได้ที่ 02-009-9888 กด 1 เพื่อดำเนินการ
3 การควบคุมการเข้าถึง				

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
3.1 ต้องกำหนดนโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุมอย่างมั่นคงปลอดภัย	นโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ควรครอบคลุมการเข้าถึงด้านเครือข่าย และโปรแกรมประยุกต์ เป็นอย่างน้อย ผู้ให้บริการควรประกาศนโยบายให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001	DAP จัดให้มีนโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุม ซึ่งครอบคลุมการเข้าถึงด้านเครือข่าย และโปรแกรมประยุกต์ ได้อย่างมั่นคงปลอดภัย ความปลอดภัย สำหรับ การสื่อสารข้อมูล (Communications security) มีการป้องกันการดำเนินการใด ๆ ที่ก่อให้เกิดความเสี่ยงต่อระบบเครือข่าย และการโอนถ่ายข้อมูล สารสนเทศทั้งภายใน และภายนอก การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance) มีการดำเนินการจัดหา การพัฒนา และการบำรุงรักษาระบบ โดยพิจารณาการกำหนดมาตรการในการรักษาความปลอดภัยให้กับระบบร่วมด้วยเสมอ โดยผู้ใช้บริการสามารถศึกษาได้จาก https://portal.eservice.set.or.th/documents/index.html คลิกที่นโยบายการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ
3.2 ต้องกำหนดวิธีการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุม เพื่อให้ประธานในที่ประชุมหรือผู้ควบคุมระบบสามารถคัดกรองผู้ร่วมประชุมก่อนการประชุมได้ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ DAP e-Shareholder Meeting มีระบบที่ให้ผู้จัดประชุมสามารถบริหารจัดการสิทธิในการเข้าร่วมประชุมของผู้เข้าร่วมประชุมได้ โดยผู้จัดประชุมจะต้องตรวจสอบสิทธิในการเข้าประชุมด้วยการให้ผู้เข้าร่วมประชุมใส่ Username และ Password ที่ได้จากผู้จัดประชุม รวมถึง OTP ที่ระบบส่งให้ผู้เข้าร่วมประชุม เพื่อแสดงการยืนยันตัวตนก่อนการเข้าประชุม
3.3 ต้องสามารถให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง ทั้งก่อนหรือระหว่างการประชุมได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ DAP e-Shareholder Meeting มีช่องทางให้ผู้ร่วมประชุมสามารถปฏิเสธหรือยกเลิกสิทธิการเข้าร่วมประชุมด้วยตนเองได้ โดยการ Log out ออกจากระบบควบคุมการประชุมได้ด้วยตนเองทั้งก่อนการประชุมหรือระหว่างการประชุม หากผู้เข้าร่วมประชุมต้องการปฏิเสธ/ยกเลิกการเข้าร่วมประชุม สามารถดำเนินการแจ้งให้ผู้ควบคุมการประชุมทราบ และดำเนินการยกเลิกได้ทันที
3.4 ต้องสามารถจำกัดและควบคุมการให้สิทธิของผู้ให้บริการ	ระบบควบคุมการประชุมควรมีมาตรการรองรับการจำกัดสิทธิของผู้ให้บริการ เช่น สิทธิการเข้าถึงข้อมูลการประชุม สิทธิในการงดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	- ระบบ DAP e-Shareholder Meeting เป็นการให้บริการบนระบบ Cloud Platform ซึ่งมีนโยบายการรักษาความลับ, ความเป็นส่วนตัวและความเป็นเจ้าของข้อมูลของผู้จัดประชุม โดย DAP จะไม่มีสิทธิใด ๆ ในข้อมูลของผู้จัดประชุมตามเงื่อนไขการให้บริการ - ระบบ DAP e-Shareholder Meeting มีระบบที่ให้ผู้จัดประชุมสามารถควบคุมระบบควบคุมการประชุมได้ เช่น การงดถ่ายทอดภาพและเสียง, การควบคุมการเปิด/ปิดไมค์หรือกล้องของผู้เข้าร่วมประชุมได้, การเชิญผู้ร่วมประชุมออกจากการประชุม เป็นต้น โดย Admin ของผู้ให้บริการจะไม่สามารถเข้าถึงการประชุมของผู้ใช้บริการได้ ยกเว้นแต่ผู้จัดประชุมมอบหมายให้ผู้ให้บริการดำเนินการแทนตามเงื่อนไขการให้บริการ
3.5 ต้องสามารถแสดงสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้มีหน้าที่จัดประชุมหรือผู้ร่วมประชุมสามารถเรียกดูรายชื่อและจำนวนผู้ร่วมประชุม เพื่อให้สามารถพิจารณาผู้เข้าร่วมได้ตลอดระยะเวลาการประชุม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ DAP e-Shareholder Meeting มีระบบให้ผู้จัดประชุมสามารถดูข้อมูลรายชื่อและจำนวนผู้ร่วมประชุมได้ตลอดระยะเวลาการประชุม และสามารถเรียกดู Report ย้อนหลังได้จากระบบด้วย โดยระบบ Cisco WebEx conference มีการแสดงข้อมูลบทบาทของผู้เข้าร่วมประชุม เช่น บทบาท Host, Co host และ Presenter เป็นต้น โดยมีขั้นตอนในการดูรายละเอียดข้อมูลดังกล่าวตามลิงก์นี้: https://help.webex.com/en-us/smtewv/Meeting-Controls-in-the-Cisco-Webex-Meetings-Virtual-Desktop-App#id_104990 นอกจากนี้เมื่อผู้เข้าร่วมประชุมต้องการใช้สิทธิในการถามคำถามสามารถแจ้งการถามคำถามได้ผ่านช่องทางของระบบ เพื่อถามคำถามต่อที่ประชุมได้ด้วยตนเอง
3.6 ต้องสามารถปรับและยกเลิกสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางในการปรับปรุง และยกเลิกสิทธิของผู้ร่วมประชุม ในระหว่างการประชุม โดยรองรับให้ประธานหรือผู้ควบคุมการประชุม สามารถดำเนินการดังนี้เป็นอย่างน้อย (1) งดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ (2) หยุดการส่งข้อมูล	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ DAP e-Shareholder Meeting ทำงานร่วมกับระบบ Conference ที่สามารถปรับเปลี่ยน และยกเลิกสิทธิของผู้เข้าร่วมประชุมในระหว่างการประชุมได้ ดังนี้ (1) งดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ (2) หยุดการส่งข้อมูล (3) ควบคุมการเปิด/ปิดไมค์หรือกล้องของผู้เข้าร่วมประชุมได้ (4) เชิญผู้ร่วมประชุมออกจากการประชุม
3.7 ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม ทั้งนี้หากเป็นการประชุมลับต้องมีการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม	ระบบควบคุมการประชุมควรมีช่องทางในการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมโดยผู้ที่ได้รับอนุญาต และอาจกำหนดสิทธิในการเข้าถึงจากผู้มีหน้าที่จัดการประชุมได้เอง	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ DAP e-Shareholder Meeting จะมีระบบการควบคุมและจัดการสิทธิในการเข้าถึงข้อมูลเฉพาะผู้ที่มีสิทธิเท่านั้น โดยมีการกำหนดให้ผู้จัดประชุมต้องแสดงตัวตนก่อนการเข้าใช้งานด้วย Username และ Password ในการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม โดยผู้ที่ไม่มีสิทธิจะไม่สามารถเข้าถึงข้อมูลดังกล่าวได้ และผู้จัดการประชุมสามารถกำหนดสิทธิได้เอง
3.8 ต้องสามารถแสดงตนด้วยวิธีการพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย ทั้งนี้หากเป็นการประชุมลับต้องมีการยืนยันตัวตนแบบหลายปัจจัย	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงตนด้วยวิธีการพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมแบบปัจจัยเดียว (Single-factor Authentication) เป็นอย่างน้อย เช่น รหัสผ่าน ฯลฯ โดยหากเป็นการจัดประชุมที่มีการใช้งานอุปกรณ์เพื่อเชื่อมต่อสถานที่มากกว่า 1 ที่ขึ้นไป เช่น Multipoint Control Unit (MCU) ฯลฯ อุปกรณ์ที่ติดตั้งควรมีการตั้งค่าเพื่อจำกัดการเข้าใช้งานเฉพาะอุปกรณ์ และเครือข่ายที่เกี่ยวข้อง เป็นอย่างน้อย ทั้งนี้ผู้ร่วมประชุมสามารถพิสูจน์ยืนยันตัวตนของผู้ร่วมประชุมด้วยการรับรองการแสดงตนของผู้ร่วมประชุมด้วยกัน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ DAP e-Shareholder Meeting กำหนดให้ผู้ร่วมประชุมต้องแสดงตัวตนของผู้เข้าร่วมประชุมแบบ Two-Factor Authentication คือการใช้ Password ร่วมกับ OTP ผ่าน sms ของมือถือที่ใช้ลงทะเบียน เพื่อยืนยันตัวตนก่อนเข้าร่วมประชุม และไม่สามารถใช้ Username เดียวกันเข้าประชุมในอุปกรณ์มากกว่า 1 ตัวได้
3.9 ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย ทั้งนี้หากเป็นการประชุมลับต้องมีการตรวจสอบรหัสผ่านที่กำหนดให้เป็นไปตามนโยบายที่กำหนดอย่างเคร่งครัด	ระบบควบคุมการประชุมควรมีการระบุถึงนโยบายการตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย เช่น รหัสผ่านที่มั่นคงปลอดภัยประกอบไปด้วยตัวอักษร ตัวเลข และอักขระพิเศษ ฯลฯ	ISO 27001	ระบบ DAP e-Shareholder Meeting มีนโยบายเกี่ยวกับตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย เช่น รหัสผ่านที่มั่นคงปลอดภัยต้องประกอบด้วยตัวอักษร ตัวเลข และอักขระพิเศษ โดยจะมีการแจ้งให้ผู้ร่วมประชุมได้รับทราบก่อนการเข้าใช้งานระบบ
4 การเข้ารหัสลับข้อมูล			

	ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
4.1	ต้องกำหนดนโยบายด้านการเข้ารหัสลับข้อมูลที่ระบุถึงการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับข้อมูลบนระบบควบคุมการประชุม และข้อมูลส่วนบุคคลที่เกี่ยวข้อง ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายควรระบุให้ครอบคลุมถึงการเข้ารหัสลับของข้อมูลที่เกี่ยวข้องกับการประชุม และข้อมูลส่วนบุคคล ด้วยวิธีการที่ได้รับการยอมรับตามมาตรฐานสากล และครอบคลุมกระบวนการเข้ารหัสลับข้อมูลในรูปแบบดังต่อไปนี้เป็นอย่างน้อย (1) การเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย (data-in-transit encryption) (2) การเข้ารหัสลับของข้อมูลที่จัดเก็บ (data-at-rest encryption)	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ DAP e-Shareholder Meeting มีการเข้ารหัสลับของข้อมูลที่เกี่ยวข้องกับการประชุมและข้อมูลส่วนบุคคล ด้วยวิธีการที่ได้รับการยอมรับตามมาตรฐานสากล และครอบคลุมกระบวนการเข้ารหัสลับข้อมูลที่ได้มาตรฐาน ISO ในรูปแบบดังต่อไปนี้ (1) เข้ารหัสลับข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย โดยการเข้ารหัสของแต่ละประชุมด้วย key ที่แตกต่างกัน ซึ่งจะทำการเข้ารหัสก่อนนำส่งข้อมูลระหว่างเครือข่าย และทำการถอดรหัสที่ปลายทาง (Data-in-transit-encryption) (2) เข้ารหัสลับของข้อมูลส่วนบุคคล อาทิ รูปถ่ายผู้เข้าประชุม และหน้าบัตรประชาชนที่จัดเก็บโดยจัดเก็บใน AZURE Blob Storage ซึ่งมีวิธีการเข้ารหัสแบบ server-side encryption (SSE) ที่สามารถเข้ารหัสข้อมูลที่เก็บบน cloud ได้อัตโนมัติ (3) การจัดเก็บวีดีโอบันทึกการประชุมผ่านระบบ conference เป็นไปตามวิธีการเข้ารหัสของ Cisco WebEx ซึ่งมีนโยบายครอบคลุมถึงการเข้ารหัสลับของข้อมูลเกี่ยวกับการประชุม และข้อมูลส่วนตัว ตามมาตรฐาน ISO 27001 ISO 27017 และ ISO 27018, ข้อมูลถูกเข้ารหัสลับเมื่อมีการรับหรือส่งข้อมูล (data-in-transit encryption) และ ข้อมูลที่ถูกจัดเก็บ (data-at-rest encryption) นโยบายดังกล่าวได้ประกาศไว้ใน เรื่อง Personal Data Security https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf
4.2	ต้องบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูล เพื่อการป้องกันการเข้าถึงกุญแจสำหรับเข้ารหัสลับข้อมูลทั้งแบบระบบรหัสแบบสมมาตร (Symmetric Key Cryptography) และระบบรหัสแบบอสมมาตร (Asymmetric Key Cryptography) อย่างน้อยกุญแจที่ใช้ในการเข้ารหัสลับข้อมูลในแต่ละการประชุมควรแตกต่างกันและไม่มีการใช้ซ้ำ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ DAP e-Shareholder Meeting เลือกใช้ Video Conference Solution Cisco WebEx ซึ่งข้อมูลที่เกี่ยวข้องกับการประชุมจะถูกจัดเก็บในฐานข้อมูลที่มีวิธีการบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลแบบสมมาตร (Symmetric Key Cryptography) นอกจากนี้ระบบจะสร้างกุญแจที่ใช้ในการเข้ารหัสลับข้อมูลในแต่ละการประชุมที่แตกต่างกันและไม่มีการใช้ซ้ำในแต่ละการประชุม ด้วยวิธีการ random symmetric key โดยใช้ Cryptographically Strong Secure Pseudo-Random Number Generator (CSPRNG), และ สร้างรหัสลับสำหรับ key นี้โดย the public key ที่ client ส่งมา, และส่ง the encrypted symmetric key กลับไปที่ client https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม				
5.1	ต้องมีขั้นตอนปฏิบัติสำหรับการเข้าถึงพื้นที่มั่นคงปลอดภัย (Secure areas)	ขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมกระบวนการที่สำคัญ เช่น การลงชื่อเข้าและออกพื้นที่ การตรวจสอบความผิดปกติของการเข้าพื้นที่ ฯลฯ	ISO 27001	ระบบ DAP e-Shareholder Meeting เลือกใช้บริการ IaaS จาก Cloud Service Provider (Azure Cloud) ที่ได้รับมาตรฐาน ISO27001 ซึ่งมีขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบควบคุมการประชุมเช่น การลงชื่อเข้าและออกพื้นที่, การควบคุมการเข้าถึงระบบ (Physical Access) โดยระบบที่ติดตั้งผ่าน Cloud มี Security Protection ดังนี้ (1) 2 Factor Authentication (2) Data Encryption (3) DDOS Protection (4) Malware Protection (5) Security Operation Center
6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน				
6.1	ต้องมีคู่มือการใช้งานของระบบควบคุมการประชุม และเผยแพร่ให้ผู้เกี่ยวข้องสามารถนำไปปฏิบัติได้	ผู้ให้บริการควรจัดทำเอกสารของขั้นตอนปฏิบัติที่เกี่ยวข้องกับระบบควบคุมการประชุมอย่างชัดเจน รวมถึงการบริหารจัดการเอกสาร เช่น การปรับปรุงเอกสาร การจัดเก็บเอกสาร ช่องทางการเข้าถึงและสิทธิที่เกี่ยวข้อง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP ได้จัดทำคู่มือปฏิบัติงานที่เกี่ยวข้องกับการเข้าใช้งานระบบ เพื่อให้ผู้จัดประชุมสามารถศึกษาและนำไปปฏิบัติงานได้ โดยมีรายละเอียดคู่มือปฏิบัติงานตามเอกสารอ้างอิงดังนี้ https://portal.eservice.set.or.th/documents/index.html คลิกที่คู่มือการใช้งาน
6.2	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารการเปลี่ยนแปลงของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมการประเมินผลกระทบ การมอบหมายการปรับปรุง การอนุมัติจากผู้ที่มีอำนาจ การวางแผนสำรอง และการทดสอบ เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล	ISO 27001	DAP ได้พัฒนาระบบ DAP e-Shareholding Meeting โดยมีการควบคุมการเปลี่ยนแปลง (Change Requrest) โดยจัดให้มีขั้นตอนกระบวนการที่จะต้องวิเคราะห์ และประเมินผลกระทบรวมถึงผู้มีอำนาจในการอนุมัติการเปลี่ยนแปลง และจัดให้มีการทดสอบเพื่อให้ทราบผลก่อนการเริ่มใช้งานจริง โดยมีแผนการทดสอบระบบงานสำรอง ตามแผน BCP ที่ได้วางไว้เป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าระบบงานที่ให้บริการสามารถทำงานต่อเนื่องได้อย่างมีประสิทธิภาพ
6.3	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารจัดการทรัพยากรของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารขีดความสามารถของระบบควบคุมการประชุมควรครอบคลุมการติดตาม ปรับปรุง และคาดการณ์ความต้องการในการใช้ทรัพยากรของระบบ เพื่อให้สามารถวางแผนการใช้งานทรัพยากรให้รองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ	ISO 27001	DAP มีระบบการ monitor ในลักษณะ real-time เพื่อตรวจสอบการใช้งานของทรัพยากรระบบเพื่อให้สามารถวางแผนการใช้งานได้อย่างต่อเนื่อง รวมถึงมีแผนการดำเนินการ หากมีการใช้ทรัพยากรระบบเกินกว่าที่กำหนดไว้ จะดำเนินการการเพิ่มขีดความสามารถของทรัพยากรทันทีเพื่อให้สามารถรองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ
6.4	ต้องควบคุมสภาพแวดล้อมของการพัฒนา การทดสอบ และการใช้งานจริงซึ่งแบ่งแยกออกจากกัน	ผู้ให้บริการควรจัดให้มีการแยกสภาพแวดล้อมส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบควบคุมการประชุม ในแต่ละส่วนออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต และควรกำหนดสิทธิในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน	ISO 27001	DAP มีการแยกสภาพแวดล้อมในส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบงานที่ให้บริการ ออกจากันอย่างชัดเจน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต โดยมีการกำหนดสิทธิการเข้าถึงในแต่ละสภาพแวดล้อมแยกออกจากกัน
6.5	ต้องสามารถรับมือกับภัยคุกคามประเภทมัลแวร์	ผู้ให้บริการควรจัดให้มีวิธีการตรวจจับ การป้องกัน และการกู้คืน ที่เกิดขึ้นจากภัยคุกคามโปรแกรมไม่พึงประสงค์ต่อระบบควบคุมการประชุม เช่น การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) การติดตั้งระบบตรวจจับภัยคุกคาม (Intrusion Detection System) การสำรองข้อมูล ฯลฯ	ISO 27001	ระบบ DAP e-Shareholder Meeting เลือกใช้บริการ IaaS จาก Cloud Service Provider (Azure Cloud) ที่ได้รับมาตรฐาน ISO27001 ซึ่งมีระบบการตรวจจับ การป้องกัน และการกู้คืนที่เกิดขึ้นจากภัยคุกคามโปรแกรมไม่พึงประสงค์
6.6	ต้องมีขั้นตอนปฏิบัติเรื่องการสำรองข้อมูลและการกู้คืนข้อมูลของระบบควบคุมการประชุม กรณีที่มีข้อมูลส่วนบุคคลต้องมีการกำหนดผู้ดำเนินการสำรองข้อมูล และกู้คืนข้อมูลส่วนบุคคลด้วย รวมถึงต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลที่สำรองให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ขั้นตอนปฏิบัติเรื่องการสำรองข้อมูล และการกู้คืนข้อมูลของระบบควบคุมการประชุมควรครอบคลุมรายการบัญชีทะเบียนสินทรัพย์ที่จำเป็นต้องมีการสำรองข้อมูล วิธีการสำรองข้อมูล พร้อมระบุช่วงเวลาที่ต้องจัดเก็บข้อมูลที่สำรอง รวมถึงแนวทางการทดสอบการกู้คืนอย่างเหมาะสม โดยกรณีที่การสำรองนั้นมีข้อมูลส่วนบุคคลอยู่ด้วย ควรมีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรม เช่น ผู้ดำเนินการสำรองข้อมูล ผู้ทดสอบการกู้คืนข้อมูล ฯลฯ ทั้งนี้ ระบบควบคุมการประชุมควรถูกกำหนดให้มีการสำรองข้อมูลบันทึกประเภทเสียงหรือทั้งเสียงและภาพ ข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงข้อมูลอื่นที่เกี่ยวข้อง เช่น ข้อมูลการแจ้งเหตุขัดข้องระหว่างการประชุม ฯลฯ อย่างน้อยเป็นระยะเวลา 7 วันนับแต่วันสิ้นสุดการประชุมในแต่ละครั้ง และควรประกาศระยะเวลาในการจัดเก็บข้อมูลที่สำรองให้ผู้เกี่ยวข้องทราบอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001, ISO 27701	- ระบบ DAP e-Shareholder Meeting เลือกใช้บริการ IaaS จาก Cloud Service Provider (Azure Cloud) ที่ได้รับมาตรฐาน ISO27001 ซึ่งมีขั้นตอนปฏิบัติเรื่องการสำรองข้อมูล และการกู้คืนข้อมูลของระบบควบคุมการประชุม โดยจะกำหนดให้มีรายการบัญชีทะเบียนสินทรัพย์ที่จำเป็นต้องมีการสำรองข้อมูล วิธีการสำรองข้อมูล พร้อมระบุช่วงเวลาที่ต้องจัดเก็บข้อมูลที่สำรอง รวมถึงแนวทางการทดสอบการกู้คืน - ระบบ DAP e-Shareholder Meeting จะมีการจัดเก็บข้อมูลที่เกี่ยวข้องกับการประชุมไว้เป็นเวลา 30 วันนับแต่วันประชุม หลังจากนั้นจะลบ/ทำลายข้อมูลออกจากระบบ โดย DAP ได้มีการแจ้งเรื่องดังกล่าวให้ผู้จัดประชุมทราบในเงื่อนไขการใช้บริการแล้ว

	ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
6.7	ต้องจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ และต้องมีการทบทวนอย่างเหมาะสม	ระบบควบคุมการประชุมควรถูกตั้งค่าให้จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยอย่างน้อยต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคล หรือชื่อผู้ใช้งาน (Username) วันและเวลาของการเข้าร่วมประชุม และเลิกประชุมเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล ผู้ให้บริการควรมีการกำหนดรอบของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างน้อย 1 ครั้ง ต่อปี	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ DAP e-Shareholder Meeting มีการจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม เช่น IP Address ที่เข้าใช้งาน, วันเวลาที่ผู้ร่วมประชุมได้เข้า-ออกจากการประชุม โดยเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล เป็นต้น
6.8	ต้องมีการดูแลข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยอย่างน้อยต้องสามารถระบุผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการใช้หรือประมวลผล	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน โดยครอบคลุมข้อมูล ผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการเป็นอย่างน้อย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	DAP มีการจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน โดยครอบคลุมข้อมูลผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการ และส่งมอบให้กับผู้จัดประชุมหลังการประชุมเสร็จสิ้น
6.9	ต้องป้องกันการเปลี่ยนแปลง และการเข้าถึงที่ไม่ได้รับอนุญาต ต่อข้อมูลจราจรอิเล็กทรอนิกส์	ผู้ให้บริการควรจัดเตรียมวิธีป้องกัน การเปลี่ยนแปลง การเข้าถึง และการลบ โดยไม่ได้รับอนุญาตต่อข้อมูลจราจรอิเล็กทรอนิกส์ เช่น การจำกัดสิทธิการดำเนินการในแต่ละฟังก์ชันการทำงาน การเฝ้าระวังและแจ้งเตือนการเข้าใช้งานที่ผิดปกติ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	1) DAP มีระบบป้องกันการเปลี่ยนแปลงและการเข้าถึงข้อมูลจราจรอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต ด้วยการกำหนดสิทธิผู้ที่จะเข้าใช้งานและจัดการข้อมูลจราจรอิเล็กทรอนิกส์ โดยควบคุมไม่ให้ผู้ไม่มีสิทธิเข้าถึงข้อมูลดังกล่าวได้ รวมถึงมีการเก็บ log ของการเข้าถึงข้อมูล log ข้อมูลการจราจรอิเล็กทรอนิกส์ไว้ทุกครั้ง 2) สำหรับส่วนของข้อมูลการจราจรอิเล็กทรอนิกส์บนระบบ conference Cisco WebEx นั้นมีการกำหนดสิทธิของผู้ดูและระบบ สามารถแบ่ง และ กำหนดการเข้าถึงของข้อมูลของ admin รวมถึงความสามารถในการตัดแปลงข้อมูล https://help.webex.com/en-us/nka5cbp/Assign-the-User-Management-Role-in-Webex-Site-Administration สามารถดูรายละเอียดการเข้าถึงข้อมูลตามสิทธิ ได้ที่ลิงก์นี้ : https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-control-hub/datasheet-c78-740770.html
6.10	ต้องจำกัดการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงกำหนดระยะเวลาในการลบหรือเปลี่ยนรูปข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยครอบคลุมการบันทึกกิจกรรมที่เกี่ยวข้อง เช่น การเข้าถึงข้อมูลส่วนบุคคล ฯลฯ ผู้ให้บริการควรกำหนดระยะเวลาที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระบบควบคุมการประชุม และแจ้งเงื่อนไขดังกล่าวให้ผู้มีหน้าที่จัดการประชุม หรือผู้ร่วมประชุมทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ พร้อมกำหนดวิธีการลบ หรือการเปลี่ยนแปลงรูปแบบข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ร่วมด้วย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	DAP มีการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ และจะจัดเก็บตามระยะเวลาที่กำหนดไว้ 30 วัน หลังส่งมอบข้อมูลให้ผู้ใช้บริการ ตามเงื่อนไขการให้บริการ โดยจะมีการแจ้งให้ผู้จัดประชุมและผู้ร่วมประชุมได้รับทราบและยอมรับเงื่อนไขดังกล่าวก่อนเริ่มใช้บริการระบบ ซึ่งระยะเวลาการจัดเก็บข้อมูลนี้สอดคล้องกับการจัดเก็บข้อมูลของระบบ conference Cisco WebEx ที่ผู้ดูแลระบบสามารถตั้งค่า retention policy เพื่อกำหนดนโยบาย ระยะเวลาการจัดเก็บข้อมูลได้ตั้งแต่ 30 วันเป็นต้นไป https://help.webex.com/en-us/WBX000027059/Webex-Data-Retention-FAQ มีวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์โดยครอบคลุมการบันทึกกิจกรรมที่เกี่ยวข้อง ตามมาตรฐาน ISO 27018
6.11	ต้องมีการจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์จากการใช้งานของผู้ควบคุมระบบ และผู้ให้บริการ รวมถึงมีการทบทวนอย่างเหมาะสม โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบ	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ควบคุมระบบ และควรประกาศ หรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบ ผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ โดยครอบคลุมกิจกรรมดังต่อไปนี้ เป็นอย่างน้อย (1) บันทึกการทำงานของระบบ (system logs) (2) บันทึกการเข้าออกระบบ (login-logout logs) (3) บันทึกการพยายามเข้าสู่ระบบ (login attempts logs) (4) บันทึกปัญหาหรือความผิดพลาดต่าง ๆ (fault logs) ผู้ให้บริการควรมีการกำหนดช่วงเวลาของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างเหมาะสม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP ได้จัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ควบคุมระบบ โดยครอบคลุมดังต่อไปนี้ (1) บันทึกการทำงานของระบบ (system logs) (2) บันทึกการเข้าออกระบบ (login-logout logs) (3) บันทึกการพยายามเข้าสู่ระบบ (login attempts logs) (4) บันทึกปัญหาหรือความผิดพลาดต่าง ๆ (fault logs) โดยจะจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง
6.12	ต้องสามารถตั้งค่า Clock synchronization ของระบบควบคุมการประชุมให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล และเป็นแหล่งเทียบเวลาในระดับ (stratum) เดียวกันทั้งระบบควบคุมการประชุม	ระบบควบคุมการประชุมควรถูกตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล เช่น สถาบันมาตรวิทยาแห่งชาติ ฯลฯ รวมถึงควรเป็นแหล่งเทียบเวลาในระดับ (stratum) เดียวกันทั้งระบบควบคุมการประชุม เช่น ตั้งค่าการใช้งานระดับ stratum-1 ให้เหมือนกันทั้งระบบควบคุมการประชุม	ISO 27001	ระบบ DAP e-Shareholder Meeting มีการควบคุมการตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล โดยเทียบเวลากับ Stratum1 ซึ่งมีการ sync เวลากับ Global Positioning System (GPS) ของ AZURE ซึ่งใช้ Microsoft-owned Stratum 1 devices
6.13	ต้องจัดการช่องโหว่ทางเทคนิคของระบบควบคุมการประชุม โดยต้องได้รับการแก้ไขอย่างมีประสิทธิภาพ	ผู้ให้บริการควรกำหนดช่องทางในการรับแจ้งช่องโหว่ และดำเนินกิจกรรมการประเมินผลกระทบ การจัดการช่องโหว่ เมื่อมีผู้แจ้งเหตุอย่างทันท่วงที พร้อมเผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ ผู้ให้บริการควรมีการตรวจสอบช่องโหว่ทางเทคนิคของระบบควบคุมการประชุมอย่างน้อย 1 ครั้งต่อปี หรือเมื่อระบบควบคุมการประชุมมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้แน่ใจว่าระบบควบคุมการประชุมไม่มีความเสี่ยงรุนแรงที่อาจส่งผลต่อการให้บริการหรือกระทบต่อข้อมูลส่วนบุคคล	ISO 27001	ระบบ DAP e-Shareholder Meeting มีระบบ Incident Management เพื่อรับแจ้งช่องโหว่ และดำเนินกิจกรรมการประเมินผลกระทบ การจัดการช่องโหว่ เมื่อมีผู้แจ้งเหตุอย่างทันท่วงที พร้อมเผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ โดยผู้ใช้บริการสามารถแจ้งช่องโหว่ได้ที่ 02-009-9888 กด 1 รวมถึงจัดให้มีการทดสอบการหาช่องโหว่อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงแก้ไขสำคัญ
6.14	ต้องทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม เช่น การตรวจประเมินภายใน (internal audit) อย่างน้อย 1 ครั้งต่อปี ฯลฯ	ISO 27001	ระบบ DAP e-Shareholder Meeting จัดให้มีการตรวจสอบโดยฝ่ายตรวจสอบภายใน และมีการตรวจสอบ Black Box Penetration Test จากผู้ตรวจสอบภายนอก อย่างน้อย 1 ครั้งต่อปี
7	**ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล**			
7.1	ต้องบริหารจัดการเครือข่ายอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดให้มีการบริหารจัดการเครือข่าย โดยครอบคลุมมาตรการดังต่อไปนี้ เป็นอย่างน้อย (1) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต (2) การป้องกันการดักรับข้อมูล (3) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย (4) การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล (5) การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ ฯลฯ	ISO 27001	ระบบ DAP e-Shareholder Meeting มีการบริหารจัดการเครือข่าย โดยครอบคลุมมาตรการ (1) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต (2) การป้องกันการดักรับข้อมูล (3) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย (4) การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล (5) การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ ฯลฯ โดยระบบที่ติดตั้งผ่าน Cloud มี Security Protection ดังนี้ (1) 2 Factor Authentication (2) Data Encryption (3) DDOS Protection (4) Malware Protection (5) Security Operation Center สำหรับในส่วนของระบบ conference cisco webEx นั้นมีการจัดการเครือข่ายโดยครอบคลุมและปลอดภัย เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต ป้องกันการดักรับข้อมูล รักษาความถูกต้องบนเครือข่าย การจัดการบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศทางไกล และป้องกันการเชื่อมต่อกับระบบภายนอก ตามมาตรฐาน ISO 27001 และ ISO 27017 https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html

	ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
7.2	ต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้องต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้ ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายและขั้นตอนปฏิบัติควรครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโอนย้ายข้อความ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย ขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการเข้าถึงข้อมูลบนเครือข่ายควรกำหนดวิธีการและช่องทางการดำเนินการอย่างชัดเจน โดยอาจเชื่อมโยงแผนภาพเครือข่าย เพื่อให้แน่ใจว่าครอบคลุมการดำเนินการของระบบควบคุมการประชุม รวมถึงกรณีที่มีข้อมูลส่วนบุคคลที่รับส่งอยู่บนเครือข่ายควรมีการบันทึกกิจกรรมการดำเนินการ พร้อมผู้รับผิดชอบให้ชัดเจน	ISO 27001	ระบบ DAP e-Shareholder Meeting มีการเชื่อมต่อข้อมูลกับผู้ร่วมประชุมผ่านช่องทางที่ปลอดภัย มีการเข้ารหัสลับข้อมูล ทั้งการใช้งานบน web-based Application และ Video Conference Solution และมีระบบมีการจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ และ Log บันทึกกิจกรรมการดำเนินการในระบบ โดยมีแนวทางการจัดการความมั่นคงปลอดภัยกับในการใช้งานระบบเครือข่ายภายในองค์กร ห้ามมิให้นำอุปกรณ์ประเภท Access Point หรืออุปกรณ์เครือข่ายอื่นใด ไปยังจุดใดจุดหนึ่งบนระบบเครือข่ายก่อนได้รับอนุญาต ห้ามมิให้ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่ายโดยไม่ได้รับอนุญาต รวมถึงการเข้าถึงระบบเครือข่ายจากระยะไกลต้องได้รับการพิสูจน์ตัวตนผู้ใช้งานอย่างเหมาะสมและต้องเป็นไปตามขั้นตอนที่กำหนด
8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย				
8.1	ต้องมีขั้นตอนปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม โดยหากพบว่ามีข้อมูลส่วนบุคคลรั่วไหล ต้องมีมาตรการในการจัดการอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดทำขั้นตอนการปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมที่ครอบคลุมกระบวนการดังต่อไปนี้เป็นอย่างน้อย (1) การรับแจ้งและยืนยันเหตุฯ (2) การจำแนกเหตุฯ และประเมินผลกระทบ (3) การตอบสนองต่อเหตุฯ (4) การจัดเก็บพยานหลักฐาน ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการระบุเพิ่มเติมถึงความรับผิดชอบในแต่ละกระบวนการ ข้อมูลที่รั่วไหล การรายงานเหตุฯ ไปยังผู้เกี่ยวข้อง เป็นอย่างน้อย	ISO 27001, ISO 27701	DAP ได้จัดให้มีขั้นตอนการปฏิบัติงานเพื่อรับมือเหตุการณ์ด้านการรักษาความปลอดภัยของระบบควบคุมการประชุมและการรั่วไหลของข้อมูลส่วนบุคคล ที่ครอบคลุมดังนี้ (1) เจ้าหน้าที่รับแจ้ง และยืนยันเหตุ (2) วิเคราะห์และจำแนกเหตุ รวมถึงการประเมินผลกระทบ (3) ประสานงานเจ้าหน้าที่เพื่อตอบสนองต่อเหตุที่เกิดขึ้น (4) เจ้าหน้าที่ที่ตอบสนองต่อเหตุ ดำเนินการจัดเก็บพยานหลักฐานที่เกี่ยวข้อง (5) รายงานเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลให้เจ้าของข้อมูลและผู้ที่เกี่ยวข้องทราบ
8.2	ต้องมีการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม	ผู้ให้บริการควรจัดให้มีช่องทางการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม โดยข้อมูลที่แจ้งควรคลอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) รายละเอียดผู้แจ้งเหตุฯ (2) วันเวลาที่พบเหตุฯ (3) รายละเอียดของเหตุฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP จัดให้มีช่องทางการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงหากพบข้อขัดข้องที่มีผลกระทบต่อการประชุม โดยสามารถแจ้งเหตุเข้ามาที่เบอร์โทรศัพท์ที่กำหนดไว้ โดยมีรายละเอียดการรับแจ้งดังนี้ (1) รายละเอียดผู้แจ้งเหตุ (2) วันเวลาที่พบเหตุ (3) รายละเอียดของเหตุ โดยผู้รับแจ้งจะดำเนินการตรวจสอบ และแก้ไขเหตุทันทีในกรณีที่กระทบต่อการประชุม หรือแจ้งวิธีการแก้ไขเหตุเบื้องต้นเพื่อให้การประชุมสามารถดำเนินการต่อไปได้
8.3	ต้องมีมาตรการสำหรับการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลต้องมีการสื่อสารกับเจ้าของข้อมูลและผู้เกี่ยวข้อง ทั้งนี้ หากเป็นการประชุมลับ ต้องดำเนินการแก้ไขปัญหาช่องโหว่ทางเทคนิคในระดับรุนแรง (อ้างอิงตามข้อมูล CVSS ที่ severity ระดับ high ขึ้นไป) ให้ครบทุกรายการก่อนให้บริการ	ผู้ให้บริการควรกำหนดวิธีการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยพิจารณาถึงองค์ประกอบดังต่อไปนี้เป็นอย่างน้อย (1) การประเมินผลกระทบของเหตุฯ (2) แนวทาง และช่องทางในการแจ้งเหตุฯ (3) การบันทึกเหตุฯ โดยให้มีการระบุรายละเอียดคำอธิบายเหตุการณ์ ช่วงเวลา ผลกระทบ ช่วงเวลาที่เกิดผลกระทบ ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการดำเนินการเพิ่มเติมอย่างน้อยในกระบวนการการสื่อสารไปยังเจ้าของข้อมูล และผู้เกี่ยวข้อง	ISO 27001	DAP ได้จัดให้มีมาตรการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม และเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล โดยเมื่อได้รับแจ้งเหตุแล้วจะดำเนินการดังนี้ (1) การประเมินผลกระทบของเหตุต่อการจัดประชุม (2) แนวทาง และช่องทางในการแจ้งเหตุ (3) การบันทึกเหตุ โดยให้มีการระบุรายละเอียดคำอธิบายเหตุการณ์ ช่วงเวลา ผลกระทบ ช่วงเวลาที่เกิดผลกระทบ (4) รายงานเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลให้เจ้าของข้อมูลและผู้ที่เกี่ยวข้องทราบ
8.4	ต้องมีขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างชัดเจน	ผู้ให้บริการควรจัดทำขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ให้บริการควรรวบรวมบันทึกกิจกรรมที่ดำเนินการ พร้อมระบุวันเวลา และวิธีการจัดเก็บอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP ได้จัดให้มีขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย โดยจะมีการบันทึกกิจกรรมที่ดำเนินการ พร้อมระบุวันเวลา และมีการรีวิว log ต่าง ๆ ครบถ้วน
9 ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ				
9.1	ต้องมีแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน	ผู้ให้บริการควรจัดทำแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน เช่น เกิดเหตุภัยพิบัติ เกิดจากโจมตีทางไซเบอร์ ฯลฯ และแผนฯ ควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) ผู้เกี่ยวข้อง (2) ขั้นตอนการรับมือ และกู้คืนเหตุฯ (3) กำหนดการทดสอบแผนฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP จัดให้มีแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน เช่น เกิดเหตุภัยพิบัติ เกิดจากโจมตีทางไซเบอร์ โดยมีรายละเอียดดังต่อไปนี้ (1) ผู้เกี่ยวข้องในการให้บริการ (2) ขั้นตอนการรับมือ และแผนการกอบกู้คืนเพื่อให้ระบบสามารถกลับมาใช้งานได้ตามปกติ (3) จัดให้มีแผนการทดสอบตามคู่มือเป็นประจำอย่างน้อยปีละ 1 ครั้ง
9.2	ต้องมีการซ้อมแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP จัดให้มีการซักซ้อมแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ และเมื่อเสร็จสิ้นการซักซ้อม จะจัดให้มีการทบทวนแผนเพื่อปรับปรุงให้เป็นปัจจุบันและมีประสิทธิภาพอยู่เสมอ
9.3	ต้องมีระบบสำรองที่พร้อมให้บริการอย่างต่อเนื่องและเพียงพอต่อการให้บริการ	ระบบสำรองของระบบควบคุมการประชุมควรทำงานทดแทนระบบหลักได้อย่างปกติและเพียงพอต่อการใช้งานตามที่มีการประเมินความพร้อมของทรัพยากรที่ใช้ ผู้ให้บริการควรจัดให้มีการทดสอบระบบสำรองเป็นประจำอย่างน้อย 1 ครั้งต่อปี ตามขั้นตอนปฏิบัติที่กำหนดขึ้น	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	DAP ได้จัดให้มีระบบสำรองของระบบควบคุมการประชุมเพื่อใช้ทำงานทดแทนระบบหลัก และจะมีการทดสอบระบบสำรองว่าสามารถทดแทนระบบหลักได้อย่างปกติและเพียงพอต่อการใช้งานเป็นประจำ อย่างน้อยปีละ 1 ครั้ง.
10 การบริการจัดการความเสี่ยงสำหรับผู้ให้บริการ				
10.1	ต้องกำหนดวิธีการบริหารจัดการความเสี่ยงตามมาตรฐานสากล หรือตามความเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการความเสี่ยง ที่ประกอบด้วย หัวข้ออย่างน้อยดังนี้ (1) วัตถุประสงค์ บทบาทและหน้าที่ (2) ขอบเขตของวิธีการบริหารจัดการความเสี่ยง (3) ขั้นตอนการประเมินความเสี่ยง (4) การประเมินผลกระทบ และโอกาสที่จะเกิดขึ้น รวมถึง ผลกระทบที่อาจส่งผลต่อการให้บริการ หมายเหตุ : ผู้ให้บริการอาจนำวิธีการบริหารจัดการ ความเสี่ยงตามมาตรฐานสากลมาประยุกต์ใช้ เช่น มาตรฐาน ISO 31000 หรือมาตรฐาน ISO/IEC 27005 ฯลฯ	ISO 27001	DAP จัดให้มีการบริหารความเสี่ยง และจัดทำแผนประเมินความเสี่ยงในการให้บริการ โดยครอบคลุม (1) วัตถุประสงค์ บทบาทและหน้าที่ (2) ขอบเขตของวิธีการบริหารจัดการความเสี่ยง (3) ขั้นตอนการประเมินความเสี่ยง (4) การประเมินผลกระทบ และโอกาสที่จะเกิดขึ้น รวมถึง ผลกระทบที่อาจส่งผลต่อการให้บริการ
10.2	ต้องทบทวนวิธีการบริหาร จัดการความเสี่ยงอย่างสม่ำเสมอ	ผู้ให้บริการควรกำหนดระยะเวลาทบทวนวิธีการบริหารจัดการความเสี่ยง และวิธีการประเมินความเสี่ยงพร้อมดำเนินการทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ	ISO 27001	DAP จัดให้มีการทบทวนการประเมินความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้ง รวมถึงกรณีมีการเปลี่ยนแปลงที่สำคัญ DAP จะดำเนินการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงดังกล่าวทันที

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม เวอร์ชัน 1.1