แบบประเมินความสอดคล้องของระบบควบคุมการประชุมกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พ .ศ. 2563 กรณี ประเมินความสอดคล้องด้วยตนเอง

ชื่อระบบ :	**Community Center**		
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท) :	**บริษัท โคโนวาเซ่ จำกัด**		
ช่องทางการติดต่อผู้ให้บริการ :	**เว็บไซต์: www.conovance.com / เบอร์โทรศัพท์: 082-979-4978 / LINE: Conovance**		
วันที่ประเมินความสอดคล้อง	**23 กรกฎาคม 2563**		
ประเภทการประเมินความสอดคล้องด้วยตนเอง	☑ การประชุมสั่งไป	☐ การประชุมสั่น	☐ การประชุมสั่น (ภาครัฐ)
มาตรฐานที่ได้รับการรับรอง	☐ ISO/IEC 27001 ☐ ISO/IEC 27701	☐ อื่น ๆ โปรดระบุ	
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง :	**ระบบควบคุมการประชุม Community Center ครอบคลุม การประชุมทั้งภาพและเสียงออนไลน์, การบันองค์ประชุมออนไลน์, การลงคะแนนวาระออนไลน์, การสรุปผลองค์ประชุมและผลวาระออนไลน์ ซึ่งรายงานองค์ประชุม, รายงานวาระ และข้อมูลจารจรทางอิเล็กทรอนิกส์ซึ่งผู้มีสิทธิสามารถดูผ่านระบบได้ทันทีหลังเสร็จสิ้นการประชุม (การทำงานของระบบ: ผู้เข้าร่วมประชุมใช้แอพพลิเคชั่นและเชื่อมต่อกับระบบ Community Center ที่ให้บริการอยู่บนคลาวด์)**		

หมายเหตุ : สพธอ. ไม่เกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

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	มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ที่ครอบคลุมระบบควบคุมการประชุม ซึ่งที่มีรายละเอียดดังนี้ (1) การบริหารจัดการสินทรัพย์ (2) การควบคุมการเข้าถึง (3) การเข้ารหัสลับข้อมูล (4) การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (5) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (6) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (7) การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ (8) การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (9) การบริหารความต่อเนื่องของการดำเนินการกิจของบริษัท (10) การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (11) การกำหนดผู้รับผิดชอบ (12) การบริหารจัดการความเสี่ยงด้านความปลอดภัยไซเบอร์ มีการประกาศนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและนโยบายการคุ้มครองข้อมูลส่วนบุคคลบนเว็บไซต์บริษัท www.conovance.com
	1.2	ต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีการทบทวนอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ	ISO 27001, ISO 27701	มีการจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล 1 ครั้งต่อปีและมีการตรวจสอบและทำการอัปเดตด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุมให้เป็นไปตามการเปลี่ยนแปลงของกฎหมายหรือมาตรฐาน
2	**การบริหารจัดการสินทรัพย์**				
	2.1	ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึก หรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ทั้งนี้ หากเป็นการให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ ต้องมีบัญชีทะเบียนสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลอยู่ใน รายอาณาจักรทั้งหมด และต้องมีเอกสารรับรองหรือประกาศอย่างเป็นทางการ	ทะเบียนสินทรัพย์ควรครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ผู้ให้บริการอาจระบุข้อมูลที่จำเป็นสำหรับการประเมินแนวทางการลดแต้านความมั่นคงปลอดภัยด้านสารสนเทศ เช่น ความสำคัญของสินทรัพย์แต่ละรายการในเชิงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบของสินทรัพย์แต่ละรายการ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีการจัดทำทะเบียนสินทรัพย์และความสำคัญของสินทรัพย์ที่ครอบคลุมถึงสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ที่ใช้ในระบบ Community Center (การประชุม, การลงคะแนน, การประมวลผลข้อมูล และข้อมูลจราจรทางอิเล็กทรอนิกส์) และเงื่อนไขการเข้าใช้งานมีระบุไว้ในขั้นตอนการติดตั้งโปรแกรมให้ผู้ร่วมประชุมได้รับทราบ รวมถึงนโยบายความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลซึ่งเผยแพร่ผ่านทางเว็บไซต์บริษัท www.conovance.com
	2.2	ต้องมีเงื่อนไขการเข้าใช้งานสำหรับระบบควบคุมการประชุม ซึ่งผยแพร่ต่อผู้ร่วมประชุม และผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ	เงื่อนไขการเข้าใช้งานควรครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ ผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001, ISO 27701	
	2.3	ต้องมีมาตรการแสดงให้ผู้ร่วมประชุมเห็นว่าเป็นการประชุมทั่วไป หรือการประชุมลับได้อย่างชัดเจน	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงข้อมูลประเภทการประชุมว่าเป็นการประชุมทั่วไป หรือการประชุมลับ เพื่อให้ผู้ร่วมประชุมทราบ โดยควรมีช่องทางให้ผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเอง เช่น กำหนดในหัวข้อการประชุม ฯลฯ ผู้ให้บริการควรจัดทำคู่มือการแสดงข้อมูลประเภทการประชุมให้ผู้มีหน้าที่จัดการประชุมสามารถปฏิบัติตามได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	มีช่องทางแสดงข้อมูลประเภทของการประชุมได้ 2 ช่องทาง คือ 1.ข้อความประกาศก่อนกดเข้าห้องประชุม 2.ข้อความแสดงหัวข้อในการประชุมซึ่งผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเองและทางบริษัทมีการจัดทำคู่มือไว้บนเว็บไซต์ www.conovance.com/support.php
	2.4	ต้องกำหนดรายการ "ข้อมูลส่วนบุคคล" ในบัญชีทะเบียนสินทรัพย์ส่วนที่เป็นข้อมูลพร้อมทั้งกำหนดลำดับชั้นความลับ และต้องมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล	บัญชีทะเบียนสินทรัพย์ควรครอบคลุมข้อมูลประเภท "ข้อมูลส่วนบุคคล" และผู้ให้บริการควรมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล เช่น การกำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	บัญชีทะเบียนสินทรัพย์ครอบคลุมข้อมูลส่วนบุคคลและมีการกำหนดลำดับชั้นความลับของข้อมูล รวมถึงสิทธิการเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาต และช่องทางการเข้าถึง
	2.5	ต้องมีขั้นตอนปฏิบัติสำหรับการลบหรือทำลายข้อมูลเกี่ยวกับการประชุม เมื่อมีเหตุให้ต้องดำเนินการ	ขั้นตอนปฏิบัติในการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมควรครอบคลุมการลบหรือทำลายข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีช่องทางให้ผู้มีหน้าที่จัดการประชุมดำเนินการได้เอง หรือช่องทางให้ผู้มีหน้าที่จัดการประชุมร้องขอให้ผู้ให้บริการลบหรือทำลายข้อมูลดังกล่าวได้	ISO 27001	มีขั้นตอนในการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมและระบบ Community Center สามารถให้ผู้มีหน้าที่จัดการประชุมดำเนินการได้เองผ่านระบบ Backoffice ของระบบCommunity Center
3	**การควบคุมการเข้าถึง**				
	3.1	ต้องกำหนดนโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุมอย่างมั่นคงปลอดภัย	นโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ควรครอบคลุมการเข้าถึงด้านเครือข่าย และโปรแกรมประยุกต์ เป็นอย่างน้อย ผู้ให้บริการควรประกาศนโยบายให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001	มีการกำหนดนโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุมอย่างมั่นคงปลอดภัยให้กับเจ้าหน้าที่ที่เกี่ยวข้องสามารถเข้าถึงได้เท่านั้นตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศที่ประกาศผ่านเว็บไซต์ของทางบริษัท
	3.2	ต้องกำหนดวิธีการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุม เพื่อให้ประธานในที่ประชุมหรือผู้ควบคุมระบบสามารถคัดกรองผู้ร่วมประชุมก่อนการประชุมได้ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ Community Center สามารถให้สิทธิและยกเลิกสิทธิก่อนการเข้าร่วมการประชุมของผู้ร่วมประชุมได้ผ่านระบบ Backoffice ของระบบ Community Center
	3.3	ต้องสามารถให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้ร่วมประชุมสามารถปฏิเสธหรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง ทั้งก่อนหรือระหว่างการประชุมได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ Community Center ผู้ร่วมประชุมสามารถปฏิเสธหรือยกเลิกสิทธิการเข้าร่วมประชุมโดยการกดปุ่มไม่ยอมรับการเข้าร่วมประชุมที่หน้าประกาศก่อนเข้าห้องประชุม หรือ ระหว่างการประชุมสามารถกดปุ่มยืนยันสำหรับการออกจากห้องประชุมได้
	3.4	ต้องสามารถจำกัดและควบคุมการให้สิทธิของผู้ให้บริการ	ระบบควบคุมการประชุมควรมีมาตรการรองรับการจำกัดสิทธิของผู้ให้บริการ เช่น สิทธิการเข้าถึงข้อมูลการประชุม สิทธิในการงดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ Community Center สามารถให้ผู้จัดการประชุมเป็นคนให้สิทธิแก่ผู้ให้บริการในกรณีที่เข้าไปอยู่ในห้องประชุมของผู้จัดการประชุมได้ทำให้ผู้ให้บริการจะถูกจำกัดสิทธิการเข้าถึงข้อมูลและสิทธิการงดถ่ายทอดเสียงหรือทั้งเสียงทั้งภาพ
	3.5	ต้องสามารถแสดงสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้มีหน้าที่จัดประชุมหรือผู้ร่วมประชุม สามารถเรียกดูรายชื่อและจำนวนผู้ร่วมประชุม เพื่อให้สามารถพิจารณาผู้เข้าร่วมได้ตลอดระยะเวลาการประชุม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ Community Center สามารถให้ผู้มีหน้าที่จัดประชุมและผู้ร่วมประชุมทราบรายชื่อและจำนวนผู้ร่วมประชุมตลอดระยะเวลาการประชุมผ่านฟังก์ชัน Active User list ในห้องประชุม
	3.6	ต้องสามารถปรับและยกเลิกสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางในการปรับปรุง และยกเลิกสิทธิของผู้ร่วมประชุม ในระหว่างการประชุม โดยรองรับให้ประธานหรือผู้ควบคุมการประชุม สามารถดำเนินการดังนี้เป็นอย่างน้อย (1) งดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ (2) หยุดการส่งข้อมูล	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ Community Center สามารถปรับปรุงและยกเลิกสิทธิของผู้ร่วมประชุมในระหว่างการประชุมได้ทันทีโดยที่ประธานหรือผู้ควบคุมการประชุมทำการเลือกรายชื่อผู้เข้าร่วมประชุมจะมีเมนูที่เอาไว้ควบคุมสิทธิ์ซึ่งรวมถึง 1) งดการถ่ายทอดเสียง หรือทั้งภาพและเสียง 2) หยุดการส่งข้อมูลหน้าจอและข้อความ
	3.7	ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม ทั้งนี้หากเป็นการประชุมลับต้องมีการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม	ระบบควบคุมการประชุมควรมีช่องทางในการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมโดยผู้ที่ได้รับอนุญาต และควรกำหนดสิทธิในการเข้าถึงจากผู้มีหน้าที่จัดการประชุมได้เอง	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบ Community Center สามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมในห้องประชุมผ่านระดับสิทธิที่แตกต่างกันของผู้เข้าร่วมการประชุม ซึ่งผู้มีหน้าที่จัดการประชุมสามารถกำหนดระดับสิทธิ์นี้ให้กับผู้เข้าร่วมประชุมได้เองบนระบบ
	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 Community Center มีการแสดงตนด้วยชื่อผู้ใช้และรหัสผ่านที่มั่นคงปลอดภัย ซึ่งหากเป็นการประชุมที่ผู้จัดการประชุมต้องการยืนยันตัวตนผู้เข้าร่วมประชุมเพิ่มเติมสามารถใช้ขั้นตอนการตรวจสอบเอกสารประกอบการอนุญาตให้เข้าร่วมประชุมเพิ่มได้โดย เมื่อผู้จัดการประชุมอนุญาตให้ผู้เข้าร่วมประชุมเข้าประชุมจึงใช้ระบบ BackOffice ของระบบ Community Center ในการสร้างชื่อผู้ใช้และรหัสผ่านแบบมั่นคงปลอดภัยเพื่อให้ผู้เข้าร่วมประชุมใช้ในการยืนยันตัวตนในการเข้าร่วมประชุม โดยระบบ Community Center จะมีการควบคุมความถูกต้องของข้อประชุม โดยระบบจะไม่อนุญาตให้ผู้เข้าร่วมประชุมใช้ชื่อผู้ใช้เดียวกันเข้าประชุมในระบบพร้อมกันได้

		ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
	3.9	ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย ทั้งนี้หากเป็นการประชุมลับต้องมีการตรวจสอบรหัสผ่านที่กำหนดให้เป็นไปตามนโยบายที่กำหนดอย่างเคร่งครัด	ระบบควบคุมการประชุมควรมีการระบุถึงนโยบายการตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย เช่น รหัสผ่านที่มั่นคงปลอดภัยประกอบไปด้วยตัวอักษร ตัวเลข และอักขระพิเศษ ฯลฯ	ISO 27001	ระบบ Community Center มีการกำหนดให้การตั้งรหัสผ่านที่จะใช้งานต้องเป็นไปตามมาตรฐานรหัสผ่านที่มั่นคงปลอดภัยคือ รหัสผ่านต้องมีความยาวตั้งแต่ 6 ตัวอักษรขึ้นไป ซึ่งต้องประกอบด้วย ตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และอักขระพิเศษ
4		**การเข้ารหัสลับข้อมูล**			
	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 Community Center มีการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับการประชุม ด้วยวิธีการ ดังนี้ (1) การเข้ารหัสลับของข้อมูลการสนทนาในห้องประชุมด้วยกุญแจที่แตกต่างกันในแต่ละการประชุมโดยจะทำการเข้ารหัสก่อนทำการส่งข้อมูลระหว่างเครือข่ายและเมื่อข้อมูลไปยังปลายทางจึงทำการถอดรหัส (data-in-transit encryption) (2) การเข้ารหัสลับของข้อมูลการลงคะแนนทั้งหมดด้วยกุญแจที่แตกต่างกันในแต่ละการประชุมก่อนทำการจัดเก็บข้อมูลการลงคะแนน (data-at-rest encryption)
	4.2	ต้องบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูล เพื่อการป้องกันการเข้าถึงกุญแจสำหรับเข้ารหัสลับข้อมูลทั้งแบบระบบรหัสแบบสมมาตร (Symmetric Key Cryptography) และระบบรหัสแบบอสมมาตร (Asymmetric Key Cryptography) อย่างน้อยกุญแจที่ใช้ในการเข้ารหัสลับข้อมูลในแต่ละการประชุมควรแตกต่างกันและไม่มีการใช้ซ้ำ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	กุญแจที่ 1 เป็นกุญแจที่แตกต่างกันแต่ละการประชุมเพื่อใช้สำหรับเข้ารหัสลับข้อมูล ในการบริหารจัดการกุญแจจะมีการเข้ารหัสกุญแจที่ 1ด้วยกุญแจที่ 2ก่อนจัดเก็บกุญแจที่ 1 ลงในฐานข้อมูล โดยมีการกำหนดระดับสิทธิสำหรับผู้ที่ได้รับมอบหมายในการเข้าถึงและรักษากุญแจ
5		**การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม**			
	5.1	ต้องมีขั้นตอนปฏิบัติสำหรับการเข้าถึงพื้นที่มั่นคงปลอดภัย (Secure areas)	ขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมกระบวนการที่สำคัญ เช่น การลงชื่อเข้าและออกพื้นที่ การตรวจสอบความผิดปกติของการเข้าพื้นที่ ฯลฯ	ISO 27001	ระบบ Community Center ติดตั้งอยู่ที่Data Center ที่มีการควบคุมความปลอดภัยเรื่องการลงชื่อ เข้าออกพื้นที่และไม่อนุญาตให้ผู้ที่ไม่ได้ลงทะเบียนที่เป็นตัวแทนบริษัทที่การเข้าพื้นที่โดยเด็ดขาด
6		**ความมั่นคงปลอดภัยสำหรับการดำเนินงาน**			
	6.1	ต้องมีคู่มือการใช้งานของระบบควบคุมการประชุม และเผยแพร่ให้เกี่ยวข้องสามารถนำไปปฏิบัติได้	ผู้ให้บริการควรจัดทำเอกสารของขั้นตอนปฏิบัติที่เกี่ยวข้องกับระบบควบคุมการประชุมอย่างชัดเจน รวมถึงการบริหารจัดการเอกสาร เช่น การปรับปรุงเอกสาร การจัดเก็บเอกสาร ช่องทางการเข้าถึงและสิทธิที่เกี่ยวข้อง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ Community Center มีการจัดทำคู่มือการใช้งานของระบบควบคุมการประชุมและมีการจัดทำและปรับปรุงเอกสารขั้นตอนการทำงานของระบบควบคุมการประชุมซึ่งเผยแพร่ให้ผู้เกี่ยวข้องอยู่บนเว็บไซต์ของบริษัท www.conovance.com/support.php
	6.2	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารการเปลี่ยนแปลงของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมการประเมินผลกระทบ การมอบหมายการปรับปรุง การอนุมัติจากผู้ที่มีอำนาจ การวางแผนล่วงหน้า และการทดสอบ เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล	ISO 27001	มีขั้นตอนปฏิบัติในการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยมีการวางแผนล่วงหน้า และการแยกระบบการทดสอบกับระบบที่ใช้งานจริง รวมถึงทำการประเมินผลกระทบและอนุมัติจากผู้มีอำนาจเพื่อลดความเสียหายจากการเปลี่ยนแปลงนั้นเพื่อรักษาไว้ซึ่งความปลอดภัยของข้อมูลและความต่อเนื่องในการทำงานของระบบควบคุมการประชุม
	6.3	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารจัดการทรัพยากรของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารจัดการความสามารถของระบบควบคุมการประชุมควรครอบคลุมการติดตาม ปรับปรุง และคาดการณ์ความต้องการในการใช้ทรัพยากรของระบบ เพื่อให้สามารถวางแผนการใช้งานทรัพยากรให้รองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ	ISO 27001	มีขั้นตอน,กระบวนการและบุคคลคอยทำการตรวจสอบการบริหารจัดการทรัพยากรของระบบควบคุมการประชุมการจัดการประชุมเพื่อบริหารจัดการขีดความสามารถของระบบควบคุมการประชุมและวางแผนการใช้ทรัพยากรได้รองรับตลอดการประชุมได้อย่างต่อเนื่องและมีประสิทธิภาพ
	6.4	ต้องควบคุมสภาพแวดล้อมของการพัฒนา การทดสอบ และการใช้งานจริง ซึ่งแบ่งแยกออกจากกัน	ผู้ให้บริการควรจัดให้มีการแยกสภาพแวดล้อมส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบควบคุมการประชุม ในแต่ละส่วนออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต และควรกำหนดสิทธิ์ในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน	ISO 27001	ระบบ Community Center มีการแยกเครื่องแม่ข่ายที่ใช้ในทดสอบในกระบวนการพัฒนาและการทดสอบ แยกจากเครื่องแม่ข่ายที่ใช้ในการทำงานจริงของระบบควบคุมการประชุมเพื่อลดความเสี่ยงของการเข้าถึงหรือเปลี่ยนแปลงสภาพแวดล้อมและมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน
	6.5	ต้องสามารถรับมือกับภัยคุกคามประเภทมัลแวร์	ผู้ให้บริการควรจัดให้มีวิธีการตรวจจับ การป้องกัน และการกู้คืน ที่เกิดขึ้นจากภัยคุกคามโปรแกรมไม่พึงประสงค์ตระบบควบคุมการประชุม เช่น การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) การติดตั้งระบบตรวจจับภัยคุกคาม (Intrusion Detection System) การสร้างข้อมูล ฯลฯ	ISO 27001	ระบบ Community Center ติดตั้งอยู่บนเครื่องแม่ข่ายที่มีการติดตั้ง Firewall, โปรแกรมป้องกันไวรัสและมัลแวร์เพื่อป้องกันภัยคุกคามจากโปรแกรมไม่พึงประสงค์ และมีระบบสำรองข้อมูลการประชุมเพื่อให้ระบบควบคุมการประชุมสามารถทำงานได้อย่างต่อเนื่อง
	6.6	ต้องมีขั้นตอนปฏิบัติเรื่องการสำรองข้อมูลและการกู้คืนข้อมูลของระบบควบคุมการประชุม กรณีที่มีข้อมูลส่วนบุคคลต้องมีการกำหนดผู้ดำเนินการสำรองข้อมูล และกู้คืนข้อมูลส่วนบุคคลด้วย รวมถึงต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลที่สำรองให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ขั้นตอนปฏิบัติเรื่องการสำรองข้อมูล และการกู้คืนข้อมูลของระบบควบคุมการประชุมควรครอบคลุมรายการบัญชีทะเบียนสินทรัพย์ที่จำเป็นต้องมีการสำรองข้อมูล วิธีการสำรองข้อมูล พร้อมระบุช่วงเวลาที่ต้องจัดเก็บข้อมูลที่สำรอง รวมถึงแนวทางการทดสอบการกู้คืนอย่างเหมาะสม โดยกรณีที่การสำรองนั้นมีข้อมูลส่วนบุคคลอยู่ด้วย ควรมีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรม เช่น ผู้ดำเนินการสำรองข้อมูล ผู้ทดสอบการกู้คืนข้อมูล ฯลฯ ทั้งนี้ ระบบควบคุมการประชุมควรถูกกำหนดให้มีการสำรองข้อมูลบันทึกประเภทเสียง หรือทั้งเสียงและภาพ ข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงข้อมูลอื่นที่เกี่ยวข้อง เช่น ข้อมูลการแจ้งเหตุขัดข้องระหว่างการประชุม ฯลฯ อย่างน้อยเป็นระยะเวลา 7 วันนับแต่วันสิ้นสุดการประชุมในแต่ละครั้ง และควรประกาศระยะเวลาในการจัดเก็บข้อมูลที่สำรองให้ผู้เกี่ยวข้องทราบอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001, ISO 27701	มีขั้นตอนปฏิบัติเรื่องการสำรองข้อมูล และการกู้คืนข้อมูลของระบบ Community Center ที่ครอบคลุมรายการบัญชีทะเบียนสินทรัพย์ที่จำเป็นโดยมีรายละเอียด วิธีการสำรองข้อมูล ช่วงเวลาที่ต้องจัดเก็บข้อมูลที่สำรอง แนวทางการทดสอบการกู้คืน และมีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรมสำหรับข้อมูลส่วนบุคคล ซึ่งบริษัทมีการชี้แจ้งรายละเอียดเรื่องระยะเวลาการเก็บรักษาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการประชุมให้กับผู้ทำการจัดการประชุมทราบอย่างชัดเจนก่อนการให้บริการจัดการประชุม
	6.7	ต้องจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ และต้องมีการทบทวนอย่างเหมาะสม	ระบบควบคุมการประชุมควรถูกตั้งค่าให้จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยอย่างน้อยต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคล หรือชื่อผู้ใช้งาน (Username) วันและเวลาของการเข้าร่วมประชุม และเลิกประชุมเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล ผู้ให้บริการควรมีการกำหนดรอบของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างน้อย 1 ครั้ง ต่อปี	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ Community Center ตั้งค่าให้จัดเก็บข้อมูลจราจรทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยมีการเก็บชื่อผู้ใช้งาน (Username), ไอพีแอดเดรส (Public IP Address), วันและเวลาการเข้าร่วมและเลิกการประชุมทุกครั้งเทียบเวลาอ้างอิงเป็นมาตรฐานสากล และมีการส่งข้อมูลจราจรอิเล็กทรอนิกส์ให้กับผู้จัดการประชุมภายใน 3 วันหำการหลังจากการประชุมเสร็จสิ้น และมีการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับระบบควบคุมการประชุม 1 ครั้งต่อปี
	6.8	ต้องมีการดูแลข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยอย่างน้อยต้องสามารถระบุผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการใช้ หรือประมวลผล	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน โดยครอบคลุมข้อมูล ผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการเป็นอย่างน้อย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	มีการจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรทางอิเล็กทรอนิกส์ของระบบ Community Center ซึ่งมีข้อมูลข้อผู้ดำเนินการ วันเวลา และวัตถุประสงค์
	6.9	ต้องป้องกันการเปลี่ยนแปลง และการเข้าถึงที่ไม่ได้รับอนุญาต ต่อข้อมูลจราจรอิเล็กทรอนิกส์	ผู้ให้บริการควรจัดเตรียมวิธีป้องกัน การเปลี่ยนแปลง การเข้าถึง และการลบ โดยไม่ได้รับอนุญาตต่อข้อมูลจราจรอิเล็กทรอนิกส์ เช่น การจำกัดสิทธิการดำเนินการในแต่ละฟังก์ชันการทำงาน การฝึกระวังและแจ้งเตือนการเข้าใช้งานที่ผิดปกติ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ Community Center มีการกำหนดฟังก์ชันการทำงานเพื่อป้องกันการเปลี่ยนแปลงและการเข้าถึงที่ไม่ได้รับอนุญาตซึ่งรวมถึงข้อมูลจราจรทางอิเล็กทรอนิกส์
	6.10	ต้องจำกัดการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงกำหนดระยะเวลาในการลบหรือเปลี่ยนรูปข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยควรอนุญาตเฉพาะการบันทึกกิจกรรมที่เกี่ยวข้อง เช่น การเข้าถึงข้อมูลส่วนบุคคล ฯลฯ ผู้ให้บริการควรกำหนดระยะเวลาที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระบบควบคุมการประชุม และแจ้งเงื่อนไขดังกล่าวให้ผู้มีหน้าที่จัดการประชุม หรือผู้ร่วมประชุมทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ พร้อมกำหนดวิธีการลบ หรือการเปลี่ยนแปลงรูปแบบข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ร่วมด้วย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	ระบบ Community Center มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรทางอิเล็กทรอนิกส์และมีการแจ้งกับผู้จัดการประชุมอีกระยะเวลาในการจัดเก็บข้อมูลการประชุมรวมถึงข้อมูลจราจรทางอิเล็กทรอนิกส์ก่อนให้บริการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์
	6.11	ต้องมีการจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์จากการใช้งานของผู้ควบคุมระบบและผู้ให้บริการ รวมถึงมีการทบทวนอย่างเหมาะสม โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบ	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ควบคุมระบบ และควรประกาศ หรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ โดยครอบคลุมกิจกรรมดังต่อไปนี้เป็นอย่างน้อย (1) บันทึกการทำงานของระบบ (system logs) (2) บันทึกการเข้าออกระบบ (login-logout logs) (3) บันทึกการพยายามเข้าสู่ระบบ (login attempts logs) (4) บันทึกปัญหาหรือความผิดพลาดต่าง ๆ (fault logs) ผู้ให้บริการควรมีการกำหนดช่วงเวลาของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างเหมาะสม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ Community Center มีการจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจร คือ (1) บันทึกการทำงานของระบบ (system logs) (2) บันทึกการเข้าออกระบบ (login-logout logs) (3) บันทึกการพยายามเข้าสู่ระบบ (login attemps logs) (4) บันทึกความผิดพลาดต่าง ๆ ของระบบ (fault logs) โดยมีการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างน้อยปีละ 1 ครั้ง หรือทบทวนทันทีกรณีเหตุเร่งด่วน
	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 Community Center ใช้การตั้งค่าเวลาทั้งระบบ (ระบบจริงและระบบสำรอง) โดยเครื่องแม่ข่ายทั้งหมดที่ติดตั้งระบบควบคุมการประชุมถูกตั้งเวลาให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล

		ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
	6.13	ต้องจัดการช่องโหว่ทางเทคนิคของระบบควบคุมการประชุม โดยต้องได้รับการแก้ไขอย่างมีประสิทธิภาพ	ผู้ให้บริการควรกำหนดช่องทางในการรับแจ้งช่องโหว่ และดำเนินกิจกรรมการประเมินผลกระทบ การจัดการช่องโหว่ เมื่อมีผู้แจ้งเหตุอย่างทันท่วงที พร้อม เผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ ผู้ให้บริการควรมีการตรวจสอบช่องโหว่ทางเทคนิคของระบบควบคุมการประชุมอย่างน้อย 1 ครั้งต่อปี หรือเมื่อระบบควบคุมการประชุมมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้แน่ใจว่าระบบควบคุมการประชุมไม่มีความเสี่ยงรุนแรงที่อาจส่งผลต่อการให้บริการ หรือกระทบต่อข้อมูลส่วนบุคคล	ISO 27001	มีการตรวจสอบช่องโหว่ทางเทคนิคและการจัดการช่องโหว่ทางเทคนิคของระบบ Community Center อย่างสม่ำเสมอทุก 6 เดือนหรือเมื่อระบบมีการเปลี่ยนแปลงที่สำคัญ และมีช่องทางให้ผู้เข้าร่วมประชุมสามารถแจ้งช่องโหว่ได้ด้วยผ่านตัวโปรแกรมโดยเข้าที่เมนูช่วยเหลือจะมีฟังก์ชันให้ส่งแจ้งข้อมูลเกี่ยวกับปัญหาหรือช่องโหว่ทางเทคนิค เมื่อได้รับการแจ้งเหตุจะทำการตรวจสอบและแก้ไขพร้อมทั้งประเมินผลกระทบเพื่อเผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ
	6.14	ต้องทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม เช่น การตรวจประเมินภายใน (internal audit) อย่างน้อย 1 ครั้งต่อปี ฯลฯ	ISO 27001	มีการจัดให้มีการทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมโดยการตรวจประเมินภายใน 1 ครั้งต่อปีเป็นอย่างน้อย
7	**ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล**				
	7.1	ต้องบริหารจัดการเครือข่ายอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดให้มีการบริหารจัดการเครือข่าย โดยครอบคลุมมาตรการดังต่อไปนี้เป็นอย่างน้อย (1) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต (2) การป้องกันการดักรับข้อมูล (3) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย (4) การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล (5) การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ ฯลฯ	ISO 27001	มีการจัดการบริหารเครือข่ายโดยครอบคลุมตามหัวข้อทั้งหมดนี้ (1) มีการป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาตด้วยการติดตั้งไฟร์วอลล์และกำหนดชื่อผู้ใช้รหัสผ่านที่มั่นคงและปลอดภัย (2) มีการป้องกันการดักรับข้อมูลโดยทำการเข้ารหัสข้อมูล (3) มีการรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่ายโดยการจำกัดสิทธิการเข้าถึงและการเข้ารหัสข้อมูล (4) มีการบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกลโดยการกำหนดบุคคลและสิทธิในการเข้าถึง (5) มีการป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอกโดยการติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ป้องกันมัลแวร์
	7.2	ต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้องต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิทธิที่กำหนดไว้ ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายและขั้นตอนปฏิบัติควรครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโถบย้ายข้อความ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย ขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการเข้าถึงข้อมูลบนเครือข่ายควรกำหนดวิธีการและช่องทางการดำเนินการอย่างชัดเจน โดยอาจเชื่อมโยงแผนภาพเครือข่ายเพื่อให้แน่ใจว่าครอบคลุมการดำเนินการของระบบควบคุมการประชุม รวมถึงกรณีที่มีข้อมูลส่วนบุคคลที่รับส่งอยู่บนเครือข่ายควรมีการบันทึกกิจกรรมการดำเนินการ พร้อมผู้รับผิดชอบให้ชัดเจน	ISO 27001	มีการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่ายโดยระบบ Community Center มีการเข้ารหัสลับข้อมูลการสนทนาระหว่างโถบย้ายข้อความ ข้อมูลการลงทะเบียน และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการประชุมในห้องประชุมมีการเข้ารหัสลับในการจัดเก็บเพื่อป้องกันการเข้าถึงข้อมูลการประชุมเหล่านี้ผ่านเครือข่าย
8	**การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย**				
	8.1	ต้องมีขั้นตอนปฏิบัติเรื่องการรับเมื่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม โดยหากพบว่ามีข้อมูลส่วนบุคคลรั่วไหล ต้องมีมาตรการในการจัดการอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดทำขั้นตอนการปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมที่ครอบคลุมกระบวนการดังต่อไปนี้ เป็นอย่างน้อย (1) การรับแจ้งและยืนยันเหตุฯ (2) การจำแนกเหตุฯ และประเมินผลกระทบ (3) การตอบสนองต่อเหตุฯ (4) การจัดเก็บพยานหลักฐาน ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการระบุเพิ่มเติมถึงความรับผิดชอบในแต่ละกระบวนการ ข้อมูลที่รั่วไหล การรายงานเหตุฯ ไปยังผู้เกี่ยวข้องเป็นอย่างน้อย	ISO 27001, ISO 27701	มีขั้นตอนการปฏิบัติการรับเมื่อเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุมโดย (1) มีเจ้าหน้าที่บริษัทรับแจ้งและยืนยันเหตุเวลาทำการประชุม (2) เจ้าหน้าที่บริษัททำการจำแนกเหตุและประเมินผลกระทบ (3) มีการตอบสนองต่อเหตุโดยประสานส่วนงานผู้ที่เกี่ยวข้องเพื่อแก้ปัญหาตามแผน (4) มีการจัดเก็บพยานหลักฐานและบันทึกเหตุ ถ้าเป็นกรณีข้อมูลส่วนบุคคลรั่วไหลจะมีการดำเนินการเพิ่มเติมโดยการแจ้งไปยังผู้ที่จัดการประชุมรวมถึงสื่อสารไปยังเจ้าของข้อมูลและผู้เกี่ยวข้อง
	8.2	ต้องมีการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม	ผู้ให้บริการควรจัดให้มีช่องทางการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม โดยข้อมูลที่แจ้งควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) รายละเอียดผู้แจ้งเหตุฯ (2) วันเวลาที่พบเหตุฯ (3) รายละเอียดของเหตุฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ Community Center ที่ผู้เข้าร่วมประชุมใช้งานจะมีมนุษย์เหลือและมีหัวข้อส่งรายงานจุดบกพร่องให้ผู้ใช้งานสามารถแจ้งข้อมูลเกี่ยวกับปัญหาหรือช่องโหว่ทางเทคนิค ซึ่งจะมีรายละเอียดของผู้แจ้งเหตุ, วันเวลาที่พบเหตุ, รายละเอียดของเหตุ, และช่องทางการติดต่อกลับหาผู้แจ้งเหตุ
	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	มีมาตรการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยมี (1) การประเมินผลกระทบของเหตุ (2) มีช่องทางและวิธีการแจ้งเหตุ (3) มีบันทึกโดยระบุรายละเอียดอธิบายเหตุการณ์ ช่วงเวลา ผลกระทบ ถ้าเป็นกรณีข้อมูลส่วนบุคคลรั่วไหลจะมีการดำเนินการเพิ่มเติมโดยการแจ้งไปยังผู้ที่จัดการประชุมรวมถึงสื่อสารไปยังเจ้าของข้อมูลและผู้เกี่ยวข้อง
	8.4	ต้องมีขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างชัดเจน	ผู้ให้บริการควรจัดทำขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ให้บริการควรรวบรวมบันทึกกิจกรรมที่ดำเนินการ พร้อมระบุวันเวลา และวิธีการจัดเก็บอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	กรณีมีเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย บริษัทมีขั้นตอนปฏิบัติในการรวบรวมบันทึกกิจกรรมที่ดำเนินการพร้อมระบุเวลาของเหตุการณ์
9	**การควบคุมการเข้าถึง**				
	9.1	ต้องมีแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน	ผู้ให้บริการควรจัดทำแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน เช่น เกิดเหตุภัยพิบัติ เกิดจากโจมตีทางไซเบอร์ ฯลฯ และแผนฯ ควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) ผู้เกี่ยวข้อง (2) ขั้นตอนการรับมือ และกู้คืนเหตุฯ (3) กำหนดการทดสอบแผนฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีการจัดทำแผนบริหารจัดการความเสี่ยง และแผนบริหารความต่อเนื่องของระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉินโดยครอบคลุมรายละเอียดคือ (1) วิธีการประเมินความเสี่ยง (2) ผู้เกี่ยวข้อง (3) ขั้นตอนการรับมือและกู้คืน (4) การกำหนดและทดสอบแผน
	9.2	ต้องมีการซ้อมแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการของระบบควบคุมการประชุม Community Center 1 ครั้งต่อเป็นอย่างน้อย
	9.3	ต้องมีระบบสำรองที่พร้อมให้บริการอย่างต่อเนื่องและเพียงพอต่อการให้บริการ	ระบบสำรองของระบบควบคุมการประชุมควรทำงานทดแทนระบบหลักได้อย่างปกติ และเพียงพอต่อการใช้งานตามที่มีการประเมินความพร้อมของทรัพยากรที่ใช้ ผู้ให้บริการควรจัดให้มีการทดสอบระบบสำรองเป็นประจำอย่างน้อย 1 ครั้งต่อปี ตามขั้นตอนปฏิบัติที่กำหนดขึ้น	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบสำรองของระบบควบคุมการประชุม Community Center สามารถทำงานทดแทนระบบหลักได้อย่างปกติเนื่องจากมีทรัพยากรของเครื่องแม่ข่ายและเครือข่ายที่เพียงพอต่อการใช้งานตามที่ประเมินไว้และจัดให้มีการทดสอบระบบสำรอง 1 ครั้งต่อปี
10	**การบริการจัดการความเสี่ยงสำหรับผู้ให้บริการ**				
	10.1	ต้องกำหนดวิธีการบริหารจัดการความเสี่ยงตามมาตรฐานสากล หรือตามความเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการความเสี่ยง ที่ประกอบด้วย หัวข้ออย่างน้อยดังนี้ (1) วัตถุประสงค์ บทบาทและหน้าที่ (2) ขอบเขตของวิธีการบริหารจัดการความเสี่ยง (3) ขั้นตอนการประเมินความเสี่ยง (4) การประเมินผลกระทบ และโอกาสที่จะเกิดขึ้น รวมถึง ผลกระทบที่อาจส่งผลต่อการให้บริการ หมายเหตุ : ผู้ให้บริการควรนำวิธีการบริหารจัดการ ความเสี่ยงตามมาตรฐานสากลมาประยุกต์ใช้ เช่น มาตรฐาน ISO 31000 หรือมาตรฐาน ISO/IEC 27005 ฯลฯ	ISO 27001	มีวิธีการบริหารจัดการความเสี่ยง โดยกำหนด ผู้ที่รับผิดชอบและบทบาทหน้าที่ , หลักเกณฑ์และวิธีการประเมินความเสี่ยง, ขั้นตอนในการปฏิบัติความเสี่ยงที่ประเมิน และหาวิธีป้องกันแก้ไขหรือลดความเสี่ยงของเหตุการณ์ที่ได้เกิดขึ้น
	10.2	ต้องทบทวนวิธีการบริหาร จัดการความเสี่ยงอย่างสม่ำเสมอ	ผู้ให้บริการควรกำหนดระยะเวลาทบทวนวิธีการบริหารจัดการความเสี่ยง และวิธีการประเมินความเสี่ยงพร้อมดำเนินการทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ	ISO 27001	มีการกำหนดระยะเวลาทบทวนวิธีการบริหารจัดการความเสี่ยงปีละ 1 ครั้ง และมีการทบทวนเป็นกรณีเร่งด่วนหากเกี่ยวข้องกับด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของระบบควบคุมการประชุมรวมถึงหากเกี่ยวข้องกับการเปลี่ยนแปลงกฎหมายหรือมาตรฐาน

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พ.ศ. 2563