แบบประเมินความสอดคล้องของระบบควบคุมการประชุมกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พ.ศ. 2563 กรณี ประเมินความสอดคล้องด้วยตนเอง

ชื่อระบบ :	**Quidlab FOQUS**			
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท) :	**บริษัท ควิดแลบ จำกัด**			
ช่องทางการติดต่อผู้ให้บริการ :	**Phone: +66-2-0134322 , Email: info@quidlab.com**			
วันที่ประเมินความสอดคล้อง	**21-ส.ค.-63**			
ประเภทการประเมินความสอดคล้องด้วยตนเอง	☑ การประชุมทั่วไป	☐ การประชุมลับ	☐ การประชุมลับ (ภาครัฐ)	
ประเภทของระบบการให้บริการ	☑ On-Cloud	☐ On-Premise	☐ อื่น ๆ โปรดระบุ	
มาตรฐานที่ได้รับการรับรอง	☐ ISO/IEC 27001	☐ ISO/IEC 27701	☐ อื่น ๆ โปรดระบุ	
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง :	การประเมินความสอดคล้องด้วยตนเองนี้ตรวจประเมินเพื่อการรับรอง Quidlab FOQUS, E-Meeting & Voting System ที่เกี่ยวข้องกับการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์			

หมายเหตุ : ☒ 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	Quidlab มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายการคุ้มครองข้อมูลส่วนบุคคล ครอบคลุมระบบควบคุมการประชุม มีรายละเอียดดังนี้ : (1) การบริหารจัดการสินทรัพย์ (2) การควบคุมการเข้าถึง (3) การเข้ารหัสลับข้อมูล (4) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (5) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (6) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (7) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (8) ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (9) การบริหารจัดการความเสี่ยง Quidlab มีการประกาศนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ร่วมประชุม และผู้เกี่ยวข้องทราบผ่านช่องทาง https://quidlab.com และ https://quidlab.com/img/Privacy_policy.pdf
1.2	ต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีการทบทวนอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ	ISO 27001, ISO 27701	Quidlab มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ดังนี้ : • ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายการคุ้มครองข้อมูลส่วนบุคคล มีการทบทวนอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ • ทบทวนนโยบายและการอัปเดตด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม เมื่อใดก็ตามที่มีการเปลี่ยนแปลงกฎหมายหรือมาตรฐาน
2 การบริหารจัดการสินทรัพย์				
2.1	ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึก หรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ทั้งนี้ หากเป็นการให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ ต้องมีบัญชีทะเบียนสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลอยู่ในราชอาณาจักรทั้งหมด และต้องมีเอกสารรับรองหรือประกาศอย่างเป็นทางการ	ทะเบียนสินทรัพย์ควรครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ผู้ให้บริการอาจระบุข้อมูลที่จำเป็นสำหรับการประเมินแนวทางการดูแลด้านความมั่นคงปลอดภัยด้านสารสนเทศ เช่น ความสำคัญของสินทรัพย์แต่ละรายการในเชิงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบของสินทรัพย์แต่ละรายการ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	Quidlab มีทะเบียนสินทรัพย์ที่ครอบคลุมทั้งสินทรัพย์ทางกายภาพ, แอพพลิเคชั่น, ซอฟท์แวร์, สินทรัพย์ระบบคลาวด์, การสมัครสมาชิกและสินทรัพย์อื่น ๆ แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุมเพื่อความปลอดภัยของข้อมูล ผู้รับผิดชอบของสินทรัพย์แต่ละรายการ
2.2	ต้องมีเงื่อนไขการเข้าใช้งานสำหรับระบบควบคุมการประชุม ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ	เงื่อนไขการเข้าใช้งานควรครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ ผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001, ISO 27701	Quidlab มีนโยบายการเข้าใช้งานควรครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ ผ่านช่องทาง เว็บไซต์ https://quidlab.com/e_agm.html
2.3	ต้องมีมาตรการแสดงให้ผู้ร่วมประชุมเห็นว่าเป็นการประชุมทั่วไป หรือการประชุมลับได้อย่างชัดเจน	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงข้อมูลประเภทการประชุมว่าเป็นการประชุมทั่วไป หรือการประชุมลับ เพื่อให้ผู้ร่วมประชุมทราบ โดยอาจมีช่องทางให้ผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเอง เช่น กำหนดในหัวข้อการประชุม ฯลฯ ผู้ให้บริการควรจัดทำคู่มือการแสดงข้อมูลประเภทการประชุมให้ผู้มีหน้าที่จัดการประชุมสามารถปฏิบัติตามได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	คู่มือซอฟต์แวร์การประชุมอิเล็กทรอนิกส์ของ Quidlab วางอยู่บนเว็บไซต์ ผู้ดูแลระบบและผู้จัดประชุมได้รับการฝึกอบรมเกี่ยวกับวิธีการใช้ระบบและเปลี่ยนแปลงข้อมูลที่จำเป็นตามต้องการ มีการกำหนดกำหนดในหัวข้อการประชุมของผู้จัดประชุม
2.4	ต้องกำหนดรายการ "ข้อมูลส่วนบุคคล" ในบัญชีทะเบียนสินทรัพย์ส่วนที่เป็นข้อมูลพร้อมทั้งกำหนดลำดับชั้นความลับ และต้องมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล	บัญชีทะเบียนสินทรัพย์ควรครอบคลุมข้อมูลประเภท "ข้อมูลส่วนบุคคล" และผู้ให้บริการควรมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล เช่น การกำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	Quidlab มีมาตราการควบคุมการจัดการข้อมูล กำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึงและบันทึกการเข้าถึงถูกเก็บรักษาไว้
2.5	ต้องมีขั้นตอนปฏิบัติสำหรับการลบหรือทำลายข้อมูลเกี่ยวกับการประชุม เมื่อมีเหตุให้ต้องดำเนินการ	ขั้นตอนปฏิบัติในการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมควรครอบคลุมการลบหรือทำลายข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีช่องทางให้ผู้มีหน้าที่จัดการประชุมดำเนินการได้เอง หรือช่องทางให้ผู้มีหน้าที่จัดการประชุมร้องขอให้ผู้ให้บริการลบหรือทำลายข้อมูลดังกล่าวได้	ISO 27001	นโยบายการเก็บข้อมูล นโยบายการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมของเราคือการทำลายข้อมูลการประชุมอิเล็กทรอนิกส์ทั้งหมดหลังจากการประชุมเสร็จสิ้น 15 วัน และ/หรือ เมื่อรายงานทั้งหมดถูกส่งมอบให้กับผู้จัดการประชุมผู้จัดการประชุมอาจขอให้เราเก็บข้อมูลไว้เป็นระยะเวลานานขึ้น โดยมีหลักฐานเป็นลายลักษณ์อักษร
3 การควบคุมการเข้าถึง				

ข้อกำหนด		แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
3.1	ต้องกำหนดนโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุมอย่างมั่นคงปลอดภัย	นโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ควรครอบคลุมการเข้าถึงด้านเครือข่าย และโปรแกรมประยุกต์ เป็นอย่างน้อย ผู้ให้บริการควรประกาศนโยบายให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001	Quidlab มีนโยบายในการกำหนดสิทธิ์ตามบทบาทสำหรับการเข้าถึงสินทรัพย์รวมถึงเครือข่ายและแอปพลิเคชัน ประกาศนโยบายให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางเว็บไซต์ https://quidlab.com/e_agm.html
3.2	ต้องกำหนดวิธีการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุม เพื่อให้ประธานในที่ประชุมหรือผู้ควบคุมระบบสามารถคัดกรองผู้ร่วมประชุมก่อนการประชุมได้ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ชื่อผู้ใช้และรหัสผ่านจะถูกส่งไปยังผู้ใช้ที่ได้รับอนุญาตเท่านั้น ในการเข้าถึงระบบการประชุมอิเล็กทรอนิกส์ ผู้เข้าร่วมประชุมแต่ละคนจะได้รับ Username & Password สามารถเข้าสู่ระบบได้เพียงหนึ่งคนเท่านั้น ผู้จัดการประชุม / ผู้ดูแลระบบสามารถถอนสิทธิ์การล็อกอินได้ทุกเมื่อ
3.3	ต้องสามารถให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง ทั้งก่อนหรือระหว่างการประชุมได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบการควบคุมการประชุม ผู้ร่วมประชุมสามารถสามารถปฏิเสธหรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเองได้ตลอดระหว่างการประชุม
3.4	ต้องสามารถจำกัดและควบคุมการให้สิทธิของผู้ให้บริการ	ระบบควบคุมการประชุมควรมีมาตรการรองรับการจำกัดสิทธิของผู้ให้บริการ เช่น สิทธิการเข้าถึงข้อมูลการประชุม สิทธิในการงดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้จัดการประชุม / ผู้ดูแลระบบสามารถงดการถ่ายทอดวิดีโอ / เสียงได้ตลอดเวลาในระหว่างการประชุม
3.5	ต้องสามารถแสดงสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้มีหน้าที่จัดประชุมหรือผู้ร่วมประชุมสามารถเรียกดูรายชื่อและจำนวนผู้ร่วมประชุม เพื่อให้สามารถพิจารณาผู้เข้าร่วมได้ตลอดระยะเวลาการประชุม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้จัดการประชุมสามารถดูรายการของผู้เข้าร่วมทั้งหมดที่ออนไลน์สามารถเรียกดูรายชื่อและจำนวนผู้ร่วมประชุม ได้ตลอดระยะเวลาการประชุม รวมถึงเวลาเข้าสู่ระบบ / ออกจากระบบ ที่อยู่ IP
3.6	ต้องสามารถปรับและยกเลิกสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางในการปรับปรุง และยกเลิกสิทธิของผู้ร่วมประชุม ในระหว่างการประชุม โดยรองรับให้ประธานหรือผู้ควบคุมการประชุมสามารถดำเนินการดังนี้เป็นอย่างน้อย (1) งดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ (2) หยุดการส่งข้อมูล	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้จัดการประชุม / ผู้ดูแลระบบ สามารถปรับและยกเลิกสิทธิของผู้ร่วมประชุม ในระหว่างการประชุม : (1) งดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ (2) หยุดการส่งข้อมูล"
3.7	ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม ทั้งนี้หากเป็นการประชุมลับต้องมีการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม	ระบบควบคุมการประชุมควรมีช่องทางในการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมโดยผู้ที่ได้รับอนุญาต และอาจกำหนดสิทธิในการเข้าถึงจากผู้มีหน้าที่จัดการประชุมได้เอง	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบควบคุมการประชุมสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม โดยผู้ที่ได้รับอนุญาต สามารถกำหนดสิทธิ์การเข้าถึงจากบุคคลที่รับผิดชอบการประชุม
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	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงตนด้วยวิธีการพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุม การระบุตัวตนของผู้เข้าร่วมประชุมถูกควบคุมโดยใช้ชื่อผู้ใช้และรหัสผ่าน อนุญาตให้เข้าสู่ระบบหนึ่งคนเท่านั้น ผู้จัดสามารถระบุผู้เข้าร่วมแต่ละคนได้
3.9	ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย ทั้งนี้หากเป็นการประชุมลับต้องมีการตรวจสอบรหัสผ่านที่กำหนดให้เป็นไปตามนโยบายที่กำหนดอย่างเคร่งครัด	ระบบควบคุมการประชุมควรมีการระบุถึงนโยบายการตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย เช่น รหัสผ่านที่มั่นคงปลอดภัยประกอบไปด้วยตัวอักษร ตัวเลข และอักขระพิเศษ ฯลฯ	ISO 27001	Quidlab E-meetings สนับสนุนนโยบายการตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย เพื่อสร้างรหัสผ่านที่คาดเดายาก ประกอบด้วยตัวอักษร ตัวเลขและตัวอักษรพิเศษ
4 การเข้ารหัสลับข้อมูล				
4.1	ต้องกำหนดนโยบายด้านการเข้ารหัสลับข้อมูลที่ระบุถึงการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับข้อมูลบนระบบควบคุมการประชุม และข้อมูลส่วนบุคคลที่เกี่ยวข้อง ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายควรระบุให้ครอบคลุมถึงการเข้ารหัสลับของข้อมูลที่เกี่ยวข้องกับการประชุมและข้อมูลส่วนบุคคล ด้วยวิธีการที่ได้รับการยอมรับตามมาตรฐานสากล และครอบคลุมกระบวนการเข้ารหัสลับข้อมูลในรูปแบบดังต่อไปนี้เป็นอย่างน้อย (1) การเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย (data-in-transit encryption) (2) การเข้ารหัสลับของข้อมูลที่จัดเก็บ (data-at-rest encryption)	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	Quidlab มีนโยบายที่จะรักษาความปลอดภัยในการรับส่งข้อมูล SSL เทคโนโลยีการเข้ารหัสข้อมูล เมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย และ การเข้ารหัสลับของข้อมูลที่จัดเก็บ
4.2	ต้องบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลเพื่อการป้องกันการเข้าถึงกุญแจสำหรับเข้ารหัสลับข้อมูลทั้งแบบระบบรหัสแบบสมมาตร (Symmetric Key Cryptography) และระบบรหัสแบบอสมมาตร (Asymmetric Key Cryptography) อย่างน้อยกุญแจที่ใช้ในการเข้ารหัสลับข้อมูลในแต่ละการประชุมควรแตกต่างกันและไม่มีการใช้ซ้ำ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบ E-meeting ของ Quidlab นั้นใช้เว็บเป็นพื้นฐานและจะใช้การเข้ารหัสแบบอสมมาตร (Asymmetric Key Cryptography) E2EE (การเข้ารหัสตั้งแต่ต้นทางถึงปลายทาง) การเข้ารหัสลับข้อมูลในแต่ละการประชุมแตกต่างกัน และไม่มีการใช้ซ้ำ
5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม				
5.1	ต้องมีขั้นตอนปฏิบัติสำหรับการเข้าถึงพื้นที่มั่นคงปลอดภัย (Secure areas)	ขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมกระบวนการที่สำคัญ เช่น การลงชื่อเข้าและออกพื้นที่ การตรวจสอบความผิดปกติของการเข้าพื้นที่ ฯลฯ	ISO 27001	ระบบของ Quidlab นั้นใช้ระบบคลาวด์อย่างสมบูรณ์ ซึ่งไม่ต้องการการเข้าถึงทางกายภาพใด ๆ อย่างไรก็ตามมีการกำหนดนโยบายและขั้นตอนการเข้าถึงระบบคลาวด์
6 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน				
6.1	ต้องมีคู่มือการใช้งานของระบบควบคุมการประชุม และเผยแพร่ให้ผู้เกี่ยวข้องสามารถนำไปปฏิบัติได้	ผู้ให้บริการควรจัดทำเอกสารของขั้นตอนปฏิบัติที่เกี่ยวข้องกับระบบควบคุมการประชุมอย่างชัดเจน รวมถึงการบริหารจัดการเอกสาร เช่น การปรับปรุงเอกสาร การจัดเก็บเอกสาร ช่องทางการเข้าถึงและสิทธิที่เกี่ยวข้อง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีคู่มือการใช้งานของระบบควบคุมการประชุมอย่างชัดเจน และเผยแพร่ให้ผู้เกี่ยวข้องสามารถนำไปปฏิบัติได้และมีการปรับปรุงตามนโยบายที่บังคับใช้
6.2	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารการเปลี่ยนแปลงของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมการประเมินผลกระทบ การมอบหมายการปรับปรุง การอนุมัติจากผู้ที่มีอำนาจ การวางแผนสำรอง และการทดสอบ เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล	ISO 27001	มีขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุม ซึ่งรวมถึง - ขอขั้นตอนการเปลี่ยนแปลง - ขั้นตอนการอนุมัติ - การวิเคราะห์และประเมินความเสี่ยง - การสื่อสารกับผู้มีส่วนได้เสีย - แผนการดำเนินงาน - ประกาศทบทวนการปฏิบัติงาน

ข้อกำหนด		แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
6.3	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารจัดการทรัพยากรของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารขีดความสามารถของระบบควบคุมการประชุมควรครอบคลุมการติดตาม ปรับปรุง และคาดการณ์ความต้องการในการใช้ทรัพยากรของระบบ เพื่อให้สามารถวางแผนการใช้งานทรัพยากรให้รองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ	ISO 27001	มีการดำเนินการตามขั้นตอนการจัดการโดยใช้นโยบาย scale Out & Scale Up เนื่องจากระบบ Quidlab เป็นระบบบนคลาวด์จึงสามารถกำหนดกฎอัตโนมัติเพื่อจัดการการวางแผนกำลังการใช้งานทรัพยากรให้รองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ
6.4	ต้องควบคุมสภาพแวดล้อมของการพัฒนา การทดสอบ และการใช้งานจริง ซึ่งแบ่งแยกออกจากกัน	ผู้ให้บริการควรจัดให้มีการแยกสภาพแวดล้อมส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบควบคุมการประชุม ในแต่ละส่วนออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต และควรกำหนดสิทธิในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน	ISO 27001	มีการแยกสภาพแวดล้อมส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบควบคุมการประชุม ในแต่ละส่วนออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต และมีการกำหนดสิทธิในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน
6.5	ต้องสามารถรับมือกับภัยคุกคามประเภทมัลแวร์	ผู้ให้บริการควรจัดให้มีวิธีการตรวจจับ การป้องกัน และการกู้คืน ที่เกิดขึ้นจากภัยคุกคามโปรแกรมไม่พึงประสงค์ต่อระบบควบคุมการประชุม เช่น การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) การติดตั้งระบบตรวจจับภัยคุกคาม (Intrusion Detection System) การสำรองข้อมูล ฯลฯ	ISO 27001	ระบบ E-Meeing ทั้งหมดได้รับการปกป้องโดยใช้ firewall และระบบป้องกันภัยคุกคาม มีระบบสำรองในภูมิภาคที่แตกต่างกันสำหรับ DR & BCP ในกรณีฉุกเฉินเร่งด่วนซึ่งช่วยให้สามารถกู้คืนได้อย่างรวดเร็ว
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	การสำรองข้อมูล นโยบาย Quidlab ระบุอย่างชัดเจนว่า การสำรองข้อมูลจะถูกเก็บไว้เป็นระยะเวลา 15 วันนับแต่วันสิ้นสุดการประชุมในแต่ละครั้ง ผู้จัดการประชุมสามารถร้องขอการสำรองข้อมูลเพิ่มเติมได้
6.7	ต้องจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ และต้องมีการทบทวนอย่างเหมาะสม	ระบบควบคุมการประชุมควรถูกตั้งค่าให้จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยอย่างน้อยต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคล หรือชื่อผู้ใช้งาน (Username) วันและเวลาของการเข้าร่วมประชุม และเลิกประชุมเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล ผู้ให้บริการควรมีการกำหนดรอบของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างน้อย 1 ครั้ง ต่อปี	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบควบคุมการประชุมถูกตั้งค่าให้จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยระบุตัวบุคคล ชื่อผู้ใช้งาน, วันที่และเวลา, การเข้าสู่ระบบ, ออกจากระบบ ,ที่อยู่ IP และหมายเลขพอร์ตที่ใช้จะถูกบันทึกไว้เทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล
6.8	ต้องมีการดูแลข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยอย่างน้อยต้องสามารถระบุผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการใช้ หรือประมวลผล	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน โดยครอบคลุมข้อมูล ผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการเป็นอย่างน้อย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	มีการกำหนดสิทธิ์ตามบทบาทและมีการจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน อย่างครอบคลุมข้อมูล ผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการ
6.9	ต้องป้องกันการเปลี่ยนแปลง และการเข้าถึงที่ไม่ได้รับอนุญาต ต่อข้อมูลจราจรอิเล็กทรอนิกส์	ผู้ให้บริการควรจัดเตรียมวิธีป้องกัน การเปลี่ยนแปลง การเข้าถึง และการลบ โดยไม่ได้รับอนุญาตต่อข้อมูลจราจรอิเล็กทรอนิกส์ เช่น การจำกัดสิทธิการดำเนินการในแต่ละฟังก์ชันการทำงาน การเฝ้าระวังและแจ้งเตือนการเข้าใช้งานที่ผิดปกติ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีระบบตรวจสอบ จัดเตรียมวิธีป้องกัน การเปลี่ยนแปลง การเข้าถึง และการลบ โดยไม่ได้รับอนุญาตต่อข้อมูลจราจรอิเล็กทรอนิกส์ - การอนุญาตตามบทบาท - สำรองประวัติของข้อมูล - บันทึกการดำเนินการเพื่อวัตถุประสงค์ในการตรวจสอบ
6.10	ต้องจำกัดการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงกำหนดระยะเวลาในการลบหรือเปลี่ยนรูปข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยครอบคลุมการบันทึกกิจกรรมที่เกี่ยวข้อง เช่น การเข้าถึงข้อมูลส่วนบุคคล ฯลฯ ผู้ให้บริการควรกำหนดระยะเวลาที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระบบควบคุมการประชุม และแจ้งเงื่อนไขดังกล่าวให้ผู้มีหน้าที่จัดการประชุม หรือผู้ร่วมประชุมทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ พร้อมกำหนดวิธีการลบ หรือการเปลี่ยนแปลงรูปแบบข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ร่วมด้วย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	นโยบายการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ - ลบข้อมูลข้อมูลส่วนบุคคลทั้งหมดภายใน 15 วันของการประชุม - แจ้งเงื่อนไขดังกล่าวให้ผู้มีหน้าที่จัดการประชุม หรือผู้ร่วมประชุมทราบผ่านช่องทาง เว็บไซต์ของบริษัท - มีขั้นตอนเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตตามนโยบายการประชุม & ขั้นตอนการรวบรวมข้อมูลส่วนบุคคลและนโยบายที่มีอยู่ในเว็บไซต์ของ บริษัท
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	การจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งาน ได้ประกาศผ่านช่องทางเว็บไซต์ของบริษัท https://quidlab.com/e_agm.html
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	ระบบควบคุมการประชุมควรถูกตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล NTP

ข้อกำหนด		แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
6.13	ต้องจัดการช่องโหว่ทางเทคนิคของระบบควบคุมการประชุม โดยต้องได้รับการแก้ไขอย่างมีประสิทธิภาพ	ผู้ให้บริการควรกำหนดช่องทางในการรับแจ้งช่องโหว่ และดำเนินกิจกรรมการประเมินผลกระทบ การจัดการช่องโหว่ เมื่อมีผู้แจ้งเหตุอย่างทันท่วงที พร้อมเผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ ผู้ให้บริการควรมีการตรวจสอบช่องโหว่ทางเทคนิคของระบบควบคุมการประชุมอย่างน้อย 1 ครั้งต่อปี หรือเมื่อระบบควบคุมการประชุมมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้แน่ใจว่าระบบควบคุมการประชุมไม่มีความเสี่ยงรุนแรงที่อาจส่งผลต่อการให้บริการ หรือกระทบต่อข้อมูลส่วนบุคคล	ISO 27001	บริษัท มีช่องทางในการรับแจ้งช่องโหว่ การจัดการช่องโหว่ มีการตรวจสอบช่องโหว่ทางเทคนิคของระบบควบคุมการประชุมอย่างน้อย 1 ครั้งต่อปี
6.14	ต้องทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม เช่น การตรวจประเมินภายใน (internal audit) อย่างน้อย 1 ครั้งต่อปี ฯลฯ	ISO 27001	บริษัท มีนโยบายทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมมีการตรวจสอบภายในอย่างน้อย 1 ครั้งต่อปี
7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล				
7.1	ต้องบริหารจัดการเครือข่ายอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดให้มีการบริหารจัดการเครือข่าย โดยครอบคลุมมาตรการดังต่อไปนี้เป็นอย่างน้อย (1) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต (2) การป้องกันการดักรับข้อมูล (3) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย (4) การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล (5) การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ ฯลฯ	ISO 27001	บริษัท จัดเก็บข้อมูลและซอฟต์แวร์ทั้งหมดกับผู้ให้บริการคลาวด์ที่มีชื่อเสียงซึ่งได้รับการรับรองมาตรฐาน ISO 27001 Quidlab ยังใช้มาตรการรักษาความปลอดภัยเพิ่มเติมเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตโดยใช้วิธีการรักษาความปลอดภัยต่าง ๆ เช่น Firewall, VPN, การควบคุมการเข้าถึงจากที่อยู่ IP
7.2	ต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้องต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้ ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายและขั้นตอนปฏิบัติควรครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโอนย้ายข้อความ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย ขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการเข้าถึงข้อมูลบนเครือข่ายควรกำหนดวิธีการและช่องทางการดำเนินการอย่างชัดเจน โดยอาจเชื่อมโยงแผนภาพเครือข่าย เพื่อให้แน่ใจว่าครอบคลุมการดำเนินการของระบบควบคุมการประชุม รวมถึงกรณีที่มีข้อมูลส่วนบุคคลที่รับส่งอยู่บนเครือข่ายควรมีการบันทึกกิจกรรมการดำเนินการ พร้อมผู้รับผิดชอบให้ชัดเจน	ISO 27001	นโยบายของบริษัท ครอบคลุมการเข้ารหัสข้อมูล E2EE ซึ่งรวมถึงการเข้ารหัส TLS / SSL เมื่อข้อมูลอยู่ระหว่างการจัดส่งและเก็บข้อมูลที่เข้ารหัส ขั้นตอนการปฏิบัติเพื่อควบคุมและการเข้าถึงข้อมูลบนเครือข่ายมีช่องทางการดำเนินการอย่างชัดเจนมีการเชื่อมโยงแผนภาพเครือข่ายและมีผู้ดูแลปรับปรุง
8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย				
8.1	ต้องมีขั้นตอนปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม โดยหากพบว่ามีข้อมูลส่วนบุคคลรั่วไหล ต้องมีมาตรการในการจัดการอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดทำขั้นตอนการปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมที่ครอบคลุมกระบวนการดังต่อไปนี้ เป็นอย่างน้อย (1) การรับแจ้งและยืนยันเหตุฯ (2) การจำแนกเหตุฯ และประเมินผลกระทบ (3) การตอบสนองต่อเหตุฯ (4) การจัดเก็บพยานหลักฐาน ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการระบุเพิ่มเติมถึงความรับผิดชอบในแต่ละกระบวนการ ข้อมูลที่รั่วไหล การรายงานเหตุฯ ไปยังผู้เกี่ยวข้องเป็นอย่างน้อย	ISO 27001, ISO 27701	บริษัท มีขั้นตอนในการการรับมือกับเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมและมีมาตรการในการจัดการอย่างมั่นคงปลอดภัย
8.2	ต้องมีการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม	ผู้ให้บริการควรจัดให้มีช่องทางการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม โดยข้อมูลที่แจ้งควรคลอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) รายละเอียดผู้แจ้งเหตุฯ (2) วันเวลาที่พบเหตุฯ (3) รายละเอียดของเหตุฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีช่องทางการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม โดยข้อมูลที่แจ้งควรคลอบคลุมรายละเอียดดังต่อไปนี้ (1) รายละเอียดผู้แจ้งเหตุฯ (2) วันเวลาที่พบเหตุฯ (3) รายละเอียดของเหตุฯ
8.3	ต้องมีมาตรการสำหรับการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ต้องมีการสื่อสารกับเจ้าของข้อมูลและผู้เกี่ยวข้อง ทั้งนี้ หากเป็นการประชุมลับ ต้องดำเนินการแก้ไขปัญหาช่องโหว่ทางเทคนิคในระดับรุนแรง (อ้างอิงตามข้อมูล CVSS ที่ severity ระดับ high ขึ้นไป) ให้ครบทุกรายการก่อนให้บริการ	ผู้ให้บริการควรกำหนดวิธีการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยพิจารณาถึงองค์ประกอบดังต่อไปนี้เป็นอย่างน้อย (1) การประเมินผลกระทบของเหตุฯ (2) แนวทาง และช่องทางในการแจ้งเหตุฯ (3) การบันทึกเหตุฯ โดยให้มีการระบุรายละเอียดคำอธิบายเหตุการณ์ ช่วงเวลาผลกระทบ ช่วงเวลาที่เกิดผลกระทบ ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการดำเนินการเพิ่มเติมอย่างน้อยในกระบวนการการสื่อสารไปยังเจ้าของข้อมูล และผู้เกี่ยวข้อง	ISO 27001	มีวิธีการตอบสนองต่อเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลจะแจ้งไปยังเจ้าของข้อมูลและผู้เกี่ยวข้องทันที
8.4	ต้องมีขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างชัดเจน	ผู้ให้บริการควรจัดทำขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ให้บริการควรรวบรวมบันทึกกิจกรรมที่ดำเนินการ พร้อมระบุวันเวลา และวิธีการจัดเก็บอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	บริษัท มีนโยบายในการเก็บบันทึกหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างชัดเจน
9 ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ				
9.1	ต้องมีแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมภายใต้สถานการณ์ฉุกเฉิน	ผู้ให้บริการควรจัดทำแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน เช่น เกิดเหตุภัยพิบัติ เกิดจากโจมตีทางไซเบอร์ ฯลฯ และแผนฯ ควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) ผู้เกี่ยวข้อง (2) ขั้นตอนการรับมือ และกู้คืนเหตุฯ (3) กำหนดการทดสอบแผนฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	บริษัท มีนโยบายและขั้นตอนในการจัดทำแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉินและการกู้คืนความเสียหาย

ข้อกำหนด			แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
	9.2	ต้องมีการซ้อมแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	บริษัท มีนโยบายมีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมและการกู้คืนความเสียหาย BC & DR อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ
	9.3	ต้องมีระบบสำรองที่พร้อมให้บริการอย่างต่อเนื่องและเพียงพอต่อการให้บริการ	ระบบสำรองของระบบควบคุมการประชุมควรทำงานทดแทนระบบหลักได้อย่างปกติ และเพียงพอต่อการใช้งานตามที่มีการประเมินความพร้อมของทรัพยากรที่ใช้ ผู้ให้บริการควรจัดให้มีการทดสอบระบบสำรองเป็นประจำอย่างน้อย 1 ครั้งต่อปี ตามขั้นตอนปฏิบัติที่กำหนดขึ้น	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ระบบสำรองของระบบควบคุมการประชุมจะถูกวางในพื้นที่ทางภูมิศาสตร์ที่แตกต่างกันเพื่อความต่อเนื่องทางธุรกิจ (BCP) และการกู้คืนความเสียหาย (DR) การทดสอบระบบสำรอง BC & DR จะดำเนินการอย่างน้อย 1 ครั้งต่อปี
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	มีการกำหนดนโยบายและขั้นตอนการบริหารความเสี่ยง ซึ่งครอบคลุม (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	บริษัทมีการทบทวนวิธีการบริหาร จัดการความเสี่ยงอย่างสม่ำเสมอ มีการอัปเดตการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พศ. 2563