แบบประเมินความสอดคล้องของระบบควบคุมการประชุมกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พ.ศ. 2563 กรณี ประเมินความสอดคล้องด้วยตนเอง

ชื่อระบบ :	**Cisco Webex**			
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท) :	**Cisco System (Thailand) LTD.**			
ช่องทางการติดต่อผู้ให้บริการ :	**02-263-7000**			
วันที่ประเมินความสอดคล้อง	**28 มกราคม 2564**			
ประเภทการประเมินความสอดคล้องด้วยตนเอง	☑ การประชุมทั่วไป	☐ การประชุมลับ	☐ การประชุมลับ (ภาครัฐ)	
ประเภทของระบบการให้บริการ	☑ On-Cloud	☐ On-Premise	☑ อื่น ๆ โปรดระบุ	
มาตรฐานที่ได้รับการรับรอง	☑ ISO/IEC 27001	☑ ISO/IEC 27701	☐ อื่น ๆ โปรดระบุ	
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง :	**ระบบ Cisco Webex ขอบเขตการประเมินสอดคล้องตามมาตรฐานความมั่นคงปลอดภัยของระบบควบคุมการประชุม พ.ศ. 2563 โดยครอบคลุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป**			

หมายเหตุ : ☒ เช่น 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	นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ระบุให้ชัดเจนว่าครอบคลุมระบบควบคุมการประชุม เป็นไปตามมาตรฐาน ISO 27001:2013 27017:2015, 27018:2019, 27701:2019. Cisco Webex ได้รับการรับรองตาม ISO ดังกล่าว โดยโครงสร้างรักษาความปลอดภัย ครอบคลุมถึง การบริหารจัดการสินทรัพย์ การควบคุมการเข้าถึง การเข้ารหัสลับข้อมูล การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ความมั่นคงปลอดภัยสำหรับการดำเนินงาน ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ และ การบริหารจัดการความเสี่ยง โดยประกาศนโยบายดังกล่าวผ่านทาง Cisco Webex Meetings Privacy Data Sheet https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html และประกาศการรับรองมาตรฐานไว้ที่ Cisco Trust Portal https://trustportal.cisco.com#/1604983821671534
1.2	ต้องทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามระยะเวลาที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีการทบทวนอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตด้านความมั่นคงปลอดภัยของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ	ISO 27001, ISO 27701	Cisco Webex ได้รับการรับรองตามมาตรฐาน ISO 27001, 27017, 27018, 27701 และมีทบทวนนโยบายการรักษาความมั่นคงสม่ำเสมอ และมีการการปรับปรุงเพื่อให้เป็นไปตามการเปลี่ยนแปลงของมาตรฐานอยู่ตลอดเวลา และได้รับรองมาตรฐานล่าสุด สามารถดูข้อมูลได้ที่ Cisco Webex Meeting Privacy Data Sheet https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf Cisco มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง โดยจะมีการประกาศวันที่และการเปลี่ยนแปลงไว้ ที่ https://www.cisco.com/c/en/us/about/legal/privacy-full.html
2 การบริหารจัดการสินทรัพย์				
2.1	ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึก หรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ทั้งนี้ หากเป็นการให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ ต้องมีบัญชีทะเบียนสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลอยู่ในราชอาณาจักรทั้งหมด และต้องมีเอกสารรับรองหรือประกาศอย่างเป็นทางการ	ทะเบียนสินทรัพย์ควรครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ผู้ให้บริการอาจระบุข้อมูลที่จำเป็นสำหรับการประเมินแนวทางการดูแลด้านความมั่นคงปลอดภัยด้านสารสนเทศ เช่น ความสำคัญของสินทรัพย์แต่ละรายการในเชิงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบของสินทรัพย์แต่ละรายการ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	Cisco Webex มีบัญชีทะเบียนสินทรัพย์ครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง เพื่อแสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึก หรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม ตามมาตรฐาน ISO27001 ISO 27017 Cisco Webex เงื่อนไขการเข้าใช้งานครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ ผ่านช่องทางที่มีความน่าเชื่อถือ ตามมาตรฐาน ISO27001 ISO 27017 , มีการแจ้งรายละเอียดเงื่อนไขผ่านทาง End User License Agreement https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf
2.2	ต้องมีเงื่อนไขการเข้าใช้งานสำหรับระบบควบคุมการประชุม ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ	เงื่อนไขการเข้าใช้งานควรครอบคลุมข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเผยแพร่ต่อผู้ร่วมประชุมและผู้เกี่ยวข้องให้สามารถนำไปปฏิบัติ ผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001, ISO 27701	
2.3	ต้องมีมาตรการแสดงให้ผู้ร่วมประชุมเห็นว่าเป็นการประชุมทั่วไป หรือการประชุมลับได้อย่างชัดเจน	ระบบควบคุมการประชุมควรมีช่องทางสำหรับการแสดงข้อมูลประเภทการประชุมว่าเป็นการประชุมทั่วไป หรือการประชุมลับ เพื่อให้ผู้ร่วมประชุมทราบ โดยอาจมีช่องทางให้ผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเอง เช่น กำหนดในหัวข้อการประชุม ฯลฯ ผู้ให้บริการควรจัดทำคู่มือการแสดงข้อมูลประเภทการประชุมให้ผู้มีหน้าที่จัดการประชุมสามารถปฏิบัติตามได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้ควบคุมการประชุมมีช่องทางสำหรับการแสดงข้อมูลประเภทการประชุมว่าเป็นการประชุมทั่วไป หรือการประชุมลับ เพื่อให้ผู้ร่วมประชุมทราบ โดยอาจมีช่องทางให้ผู้มีหน้าที่จัดการประชุมสามารถระบุได้ด้วยตนเอง เช่น กำหนดในหัวข้อการประชุม https://help.webex.com/en-us/xm3o0v/Schedule-a-Cisco-Webex-Meeting

2.4	ต้องกำหนดรายการ "ข้อมูลส่วนบุคคล" ในบัญชีทะเบียนสินทรัพย์ส่วนที่เป็นข้อมูลพร้อมทั้งกำหนดลำดับชั้นความลับ และต้องมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล	บัญชีทะเบียนสินทรัพย์ควรครอบคลุมข้อมูลประเภท "ข้อมูลส่วนบุคคล" และผู้ให้บริการควรมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล เช่น การกำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	Cisco มีบัญชีทะเบียนสินทรัพย์ควรครอบคลุมข้อมูลประเภท "ข้อมูลส่วนบุคคล" และผู้ให้บริการควรมีมาตรการในการควบคุมการจัดการข้อมูลส่วนบุคคล ตามมาตรฐาน ISO 27001 ISO 27012 และ ISO 27018, มีการกำหนดผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล วันเวลาที่อนุญาตให้เข้าถึง ช่องทางการเข้าถึง แนวทางการปฏิบัติประกาศเงื่อนไขผ่านทาง End User License Agreement https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf Data ที่ใช้เข้าถึง เหตุผลได้ถูกระบุไว้ใน https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf Cisco ได้ให้ข้อมูลของ privacy data map ไว้ใน https://trustportal.cisco.com#/1552559092865169 เพื่อแสดงถึงข้อมูลที่ Cisco Webex ได้นำไปใช้
2.5	ต้องมีขั้นตอนปฏิบัติสำหรับการลบหรือทำลายข้อมูลเกี่ยวกับการประชุม เมื่อมีเหตุให้ต้องดำเนินการ	ขั้นตอนปฏิบัติในการลบหรือทำลายข้อมูลเกี่ยวกับการประชุมควรครอบคลุมการลบหรือทำลายข้อมูลส่วนบุคคล ผู้ให้บริการควรจัดให้มีช่องทางให้ผู้มีหน้าที่จัดการประชุมดำเนินการได้เอง หรือช่องทางให้ผู้มีหน้าที่จัดการประชุมร้องขอให้ผู้ให้บริการลบหรือทำลายข้อมูลดังกล่าวได้	ISO 27001	มีมาตรการสำหรับการลบหรือทำลายข้อมูล ตามมาตรฐาน ISO 27001, ISO 27017, ISO 27018 ผู้จัดการประชุมสามารถจัดการลบหรือทำลายข้อมูลการประชุมผ่านทาง Webex Site ของผู้จัดการประชุม สามารถอ้างอิงได้จากเอกสาร เรื่อง Data Deletion & Retention https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf
3 การควบคุมการเข้าถึง				
3.1	ต้องกำหนดนโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับการประชุมอย่างมั่นคงปลอดภัย	นโยบายด้านการควบคุมการเข้าถึงสินทรัพย์ควรครอบคลุมการเข้าถึงด้านเครือข่าย และโปรแกรมประยุกต์ เป็นอย่างน้อย ผู้ให้บริการควรประกาศนโยบายให้ผู้ร่วมประชุมและผู้เกี่ยวข้องทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ	ISO 27001	Cisco มีนโยบายการควบคุมการเข้าถึงสินทรัพย์ครอบคลุมการเข้าถึงข้อมูล เครือข่าย เครื่องมือต่าง ๆ และโปรแกรมประยุกต์ ตามมาตรฐาน ISO 27001 ISO 27017 และ ISO 27018 , รายละเอียดและนโยบาย ประกาศเงื่อนไขผ่าน End User License Agreement https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf นโยบายการเข้าถึงข้อมูล ได้ถูกระบุไว้ใน https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf
3.2	ต้องกำหนดวิธีการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางการให้สิทธิ และยกเลิกสิทธิ ก่อนการเข้าร่วมประชุมของผู้ร่วมประชุม เพื่อให้ประธานในที่ประชุมหรือผู้ควบคุมระบบสามารถคัดกรองผู้ร่วมประชุมก่อนการประชุมได้ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้จัดการประชุมบน Webex สามารถ ให้สิทธิหรือยกเลิกสิทธิของผู้ที่จะเข้าร่วมประชุมได้ อ้างอิง จาก : https://help.webex.com/en-us/hol1ft/Accept-and-Reject-Registration-Requests-in-Cisco-Webex-Meetings
3.3	ต้องสามารถให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้ร่วมประชุมสามารถปฏิเสธ หรือยกเลิกสิทธิการเข้าร่วมประชุมได้ด้วยตนเอง ทั้งก่อนหรือระหว่างการประชุมได้	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้เข้าร่วมประชุม ผ่าน webex นั้น สามารถที่จะเลือก เข้าประชุมหรือไม่เข้าประชุม ได้โดยตนเอง อ้างอิง จาก : https://help.webex.com/en-us/hol1ft/Accept-and-Reject-Registration-Requests-in-Cisco-Webex-Meetings
3.4	ต้องสามารถจำกัดและควบคุมการให้สิทธิของผู้ให้บริการ	ระบบควบคุมการประชุมควรมีมาตรการรองรับการจำกัดสิทธิของผู้ให้บริการ เช่น สิทธิการเข้าถึงข้อมูลการประชุม สิทธิในการงดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	บน webex meeting สามารถ เปิดปิด ไมโครโฟน หรือกล้องได้ ตลอดระยะเวลาการประชุม และเพื่อเป็นการกำหนดสิทธิการถ่ายทอดเสียงและภาพ https://help.webex.com/en-us/n94aj5j/Mute-or-Unmute-in-Webex-Meetings-Suite#:~:text=When%20you're%20sharing%2C%20click,to%20mute%20or%20unmute%20yourself. Admin ยังสามารถตั้งค่าเพิ่มเติมเพื่อความปลอดภัยได้ https://help.webex.com/en-us/sxdj4ab/Manage-Security-for-a-Cisco-Webex-Site-in-Cisco-Webex-Control-Hub เจ้าของห้องประชุมสามารถ ล็อคห้องประชุมเลือกและจำกัดสิทธิผู้เข้าร่วมประชุม https://help.webex.com/en-us/zcvgyc/Webex-Lock-or-Unlock-Your-Meeting
3.5	ต้องสามารถแสดงสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางให้ผู้มีหน้าที่จัดประชุมหรือผู้ร่วมประชุมสามารถเรียกดูรายชื่อและจำนวนผู้ร่วมประชุม เพื่อให้สามารถพิจารณาผู้เข้าร่วมได้ตลอดระยะเวลาการประชุม	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้จัดการประชุมสามารถดูรายชื่อของผู้เข้าร่วมประชุมได้ ทั้งก่อนการประชุม จากการนัดหมายผ่านทาง calendar และระหว่างประชุม ขั้นตอนการเข้าถึงรายชื่อผู้ประชุมได้ประกาศไว้ทาง https://help.webex.com/en-us/smtewv/Meeting-Controls-in-the-Cisco-Webex-Meetings-Virtual-Desktop-App#id_104990 https://help.webex.com/en-us/ng68aeg/Search-the-Participants-List-in-a-Webex-Meeting
3.6	ต้องสามารถปรับและยกเลิกสิทธิของผู้ร่วมประชุมได้	ระบบควบคุมการประชุมควรมีช่องทางในการปรับปรุง และยกเลิกสิทธิของผู้ร่วมประชุม ในระหว่างการประชุม โดยรองรับให้ประธานหรือผู้ควบคุมการประชุม สามารถดำเนินการดังนี้เป็นอย่างน้อย (1) งดการถ่ายทอดเสียง หรือทั้งเสียงและภาพ (2) หยุดการส่งข้อมล	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	บน webex meeting สามารถ เปิดปิด ไมโครโฟน หรือกล้องได้ ตลอดระยะเวลาการประชุม https://help.webex.com/en-us/n94aj5j/Mute-or-Unmute-in-Webex-Meetings-Suite#:~:text=When%20you're%20sharing%2C%20click,to%20mute%20or%20unmute%20yourself.
3.7	ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม ทั้งนี้หากเป็นการประชุมลับต้องมีการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม	ระบบควบคุมการประชุมควรมีช่องทางในการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม โดยผู้ที่ได้รับอนุญาต และอาจกำหนดสิทธิในการเข้าถึงจากผู้มีหน้าที่จัดการประชุมได้เอง	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	โดยปกติการเข้าถึงช่องทางการควบคุมการประชุมนั้น จะระบุสิทธิ ไว้สำหรับเจ้าของ Account นั้น ๆ หรือ Admin ที่สามารถเข้าไปบริหารจัดการ Account หรือ การประชุมต่าง ๆ ที่เกิดขึ้นภายในองค์กรของตนเอง จาก Control hub อ้างอิง :https://help.webex.com/en-us/nkhozs6/Get-Started-with-Cisco-Webex-Control-Hub
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	บน webex สามารถ พิสูจน์ยืนยันตัวโดยการใช้ Password หรือทำ SSO สำหรับการ authentication ได้ อ้างอิง : https://help.webex.com/en-us/g2wy83/Configure-Single-Sign-On-SSO-Authentication-for-Attendees-for-Your-Cisco-Webex-Site. Webex สามารถ integrate กับ third-party 2FA https://www.cisco.com/c/en/us/solutions/collaboration/webex-teams/security-compliance-management/webex-teams-third-party-integrations.html ส่วนการประชุมลับนั้น สามารถใช้งาน Cisco meeting server ในการทำ multi factor authentication เพื่อ สร้างการยืนยันตัวตนที่หลากหลายมากขึ้น https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-3-1/Cisco-Meeting-Server-Release-Notes-3-1.pdf

	3.9	ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย ทั้งนี้หากเป็นการประชุมลับต้องมีการตรวจสอบรหัสผ่านที่กำหนดให้เป็นไปตามนโยบายที่กำหนดอย่างเคร่งครัด	ระบบควบคุมการประชุมควรมีการระบุถึงนโยบายการตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย เช่น รหัสผ่านที่มั่นคงปลอดภัยประกอบไปด้วยตัวอักษร ตัวเลข และอักขระพิเศษ ฯลฯ	ISO 27001	webex meeting มีการกำหนดรูปแบบในการตั้งรหัสผ่านที่มั่นคงและปลอดภัย ทั้งเรื่องของการประกอบด้วยอักขระ ตัวเลข และ อักขระพิเศษ อ้างอิง จาก : https://help.webex.com/en-us/nxsab72/Webex-Teams-Change-Your-Password#:~:text=your%20new%20password..-,If%20you%20signed%20up%20for%20a%20free%20version%20of%20Webex,1%20letter%20(a%2Dz%2CA%2DZ)
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	Cisco มีนโยบายครอบคลุมถึงการเข้ารหัสลับของข้อมูลเกี่ยวกับการประชุม และข้อมูลส่วนตัว ตามมาตรฐาน ISO 27001 ISO 27017 และ ISO 27018 , ข้อมูลถูกเข้ารหัสลับเมื่อมีการรับหรือส่งข้อมูล (data-in-transit encryption) และ ข้อมูลที่ถูกจัดเก็บ (data-at-rest encryption) นโยบายดังกล่าวได้ประกาศไว้ ใน เรื่อง Personal Data Security https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf Data in transit จะถูก encrypt โดย AES 256 for storage, Keys managed through AWS KMS ในขณะที่ data at rest, Cisco Webex Meetings เก็บ password ใช้ SHA-2 (one way hashing algorithm) File - 256-bit block AES GCM key แล้ว File key encrypted โดย primary key based บน AES HmacSHA256 https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
	4.2	ต้องบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูลอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรกำหนดวิธีการบริหารจัดการกุญแจสำหรับการเข้ารหัสลับข้อมูล เพื่อการป้องกันการเข้าถึงกุญแจสำหรับเข้ารหัสลับข้อมูลทั้งแบบระบบรหัสแบบสมมาตร (Symmetric Key Cryptography) และระบบรหัสแบบอสมมาตร (Asymmetric Key Cryptography) อย่างน้อย กุญแจที่ใช้ในการเข้ารหัสลับข้อมูลในแต่ละการประชุมควรแตกต่างกันและไม่มีการใช้ซ้ำ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	บน webex meeting ใช้รูปแบบการเข้ารหัส ในแบบ Symmetric Key ซึ่งกุญแจในการใช้สำหรับเข้ารหัสในแต่ละครั้งนั้นไม่มีการใช้ซ้ำ อ้างอิง https://help.webex.com/en-us/WBX44739/What-Does-End-to-End-Encryption-Do , https://www.cisco.com/c/en/us/products/security/encryption-explained.html ผู้จัดการประชุมจะสร้าง a random symmetric key โดยใช้ a Cryptographically Strong Secure Pseudo-Random Number Generator (CSPRNG), และสร้างรหัสลับสำหรับ key นี้ โดย 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 The traffic generated by clients is encrypted using the symmetric session key. In this model traffic cannot be deciphered by the Cisco Webex server.
5	**การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม**				
	5.1	ต้องมีขั้นตอนปฏิบัติสำหรับการเข้าถึงพื้นที่มั่นคงปลอดภัย (Secure areas)	ขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมกระบวนการที่สำคัญ เช่น การลงชื่อเข้าและออกพื้นที่ การตรวจสอบความผิดปกติของการเข้าพื้นที่ ฯลฯ	ISO 27001	บน webex มีพื้นที่ในการกรองคนก่อนเข้าใช้งาน และ อ้างอิงการกระบวน ทางด้านความปลอดภัย ในแง่การเข้าใช้งานจาก https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
6	**ความมั่นคงปลอดภัยสำหรับการดำเนินงาน**				
	6.1	ต้องมีคู่มือการใช้งานของระบบควบคุมการประชุม และเผยแพร่ให้ผู้เกี่ยวข้องสามารถนำไปปฏิบัติได้	ผู้ให้บริการควรจัดทำเอกสารของขั้นตอนปฏิบัติที่เกี่ยวข้องกับระบบควบคุมการประชุมอย่างชัดเจน รวมถึงการบริหารจัดการเอกสาร เช่น การปรับปรุงเอกสาร การจัดเก็บเอกสาร ช่องทางการเข้าถึงและสิทธิที่เกี่ยวข้อง ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	คู่มือและรายละเอียดการเข้าใช้งานในแต่ละโมดูล สามารถเข้าได้จากช่องทาง นี้ https://help.webex.com/ld-nyw95a4-CiscoWebexMeetings/Webex-Meetings#Download-and-Install
	6.2	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารการเปลี่ยนแปลงของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบควบคุมการประชุมควรครอบคลุมการประเมินผลกระทบ การมอบหมายการปรับปรุง การอนุมัติจากผู้ที่มีอำนาจ การวางแผนสำรอง และการทดสอบ เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล	ISO 27001	มีขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงและขั้นตอนตามมาตรฐาน ISO 27001 และ ISO 27017 (มีการประเมินผลกระทบ มอบหมายการปรับปรุง และอนุมัติจากผู้มีอำนาจ เพื่อวางแผนสำรอง และทดสอบ) https://trustportal.cisco.com#/1604983821671534
	6.3	ต้องมีขั้นตอนปฏิบัติเรื่องการบริหารจัดการทรัพยากรของระบบควบคุมการประชุม	ขั้นตอนปฏิบัติการบริหารขีดความสามารถของระบบควบคุมการประชุมควรครอบคลุมการติดตามปรับปรุง และคาดการณ์ความต้องการในการใช้ทรัพยากรของระบบ เพื่อให้สามารถวางแผนการใช้งานทรัพยากรให้รองรับการใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ	ISO 27001	มีขั้นตอนปฏิบัติการบริหารจัดการควบคุมการเปลี่ยนแปลงตามมาตรฐาน ISO 27001 และ ISO 27017 (มีการประเมินผลและปรับปรุง และคาดการณ์ความต้องการในการใช้ทรัพยากรอย่างต่อเนื่องและมีประสิทธิภาพตามมาตรฐาน) https://trustportal.cisco.com#/1604983821671534 และยังสามารถเข้าถึงข้อมูล ของ Memory และ CPU ได้ https://help.webex.com/en-us/nmghd9e/Check-the-Audio-and-Video-Statistics-of-Your-Cisco-Webex-Meeting
	6.4	ต้องควบคุมสภาพแวดล้อมของการพัฒนา การทดสอบ และการใช้งานจริง ซึ่งแบ่งแยกออกจากกัน	ผู้ให้บริการควรจัดให้มีการแยกสภาพแวดล้อมส่วนของการพัฒนา การทดสอบ และการทำงานจริงของระบบควบคุมการประชุม ในแต่ละส่วนออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมโดยไม่ได้รับอนุญาต และควรกำหนดสิทธิในการเข้าถึงข้อมูลของแต่ละส่วนที่แตกต่างกัน	ISO 27001	มีขั้นตอนปฏิบัติการบริหารจัดการตามมาตรฐาน ISO 27001 และ ISO 27017 และ ควบคุมสภาพแวดล้อมของการพัฒนา ทดสอบ และแยกกับระบบการใช้งานจริง และมีการตรวจสอบความมั่นคงและปลอดภัยของระบบก่อน https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
	6.5	ต้องสามารถรับมือกับภัยคุกคามประเภทมัลแวร์	ผู้ให้บริการควรจัดให้มีวิธีการตรวจจับ การป้องกัน และการกู้คืน ที่เกิดขึ้นจากภัยคุกคามโปรแกรมไม่พึงประสงค์ต่อระบบควบคุมการประชุม เช่น การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) การติดตั้งระบบตรวจจับภัยคุกคาม (Intrusion Detection System) การสำรองข้อมูล ฯลฯ	ISO 27001	มีขั้นตอนปฏิบัติการบริหารจัดการตาม มาตรฐาน ISO 27001 เพื่อตรวจจับ ป้องกัน และกู้คืน ที่เกิดจากภัยคุมคามโปรแกรมไม่พึงประสงค์ต่อระบบควบคุมการประชุม มีการวางระบบป้องกัน Intrusion Detection Systems (IDSs) และมีการ log และ monitor ตลอดเวลา https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html

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 และการกู้คืนข้อมูล ตามมาตรฐานISO 27001 ISO 27017 และ ISO 27018 ครอบคลุมรายการบัญชีทะเบียนสินทรัพย์ที่จำเป็นต้องมีการสำรองข้อมูล วิธีการสำรองข้อมูล ระบุช่วงเวลาที่ต้องจัดเก็บข้อมูลที่สำรอง มีแนวทางการทดสอบการกู้คืน มีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรม ตาม มาตรฐาน SOC 3 https://trustportal.cisco.com#/1604982898019524 Cisco Webex Global site Backup จะทำการ backup ข้อมูลทุก ๆวัน วันละหนึ่งครั้ง โดยกรณีที่การสำรองนั้นมีข้อมูลส่วนบุคคลอยู่ด้วย มีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรม เช่น ผู้ดำเนินการสำรองข้อมูล ผู้ทดสอบการกู้คืนข้อมูล ฯลฯ https://help.webex.com/en-us/31k2xo/Cisco-Webex-Global-Site-Backup หากข้อมูลถูกลบโดยผู้ใช้งาน ระบบจะมีการจัดเก็บไว้ 30 วัน
6.7	ต้องจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ และต้องมีการทบทวนอย่างเหมาะสม	ระบบควบคุมการประชุมควรถูกตั้งค่าให้จัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ร่วมประชุม โดยอย่างน้อยต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคล หรือชื่อผู้ใช้งาน (Username) วันและเวลาของการเข้าร่วมประชุม และเลิกประชุมเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากล ผู้ให้บริการควรมีการกำหนดรอบของการทบทวนข้อมูลจราจรอิเล็กทรอนิกส์อย่างน้อย 1 ครั้ง ต่อปี	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	ผู้จัดการประชุมสามารถเข้าถึงข้อมูลการประชุม ที่เกี่ยวข้างกับการใช้งานของผู้เข้าร่วมประชุม โดยสามารถเข้าได้ถึงข้อมูลที่สามารถระบุตัวบุคคล วันและเวลาของการเข้าร่วมประชุม และเลิกการประชุมโดยเทียบเวลาอ้างอิงเป็นมาตรฐานสากล สามารถ ทำ e-discovery เพื่อ ดู log ข้อมูลของผู้เข้าร่วมประชุม ซึ่งข้อมูล วัน เวลา ผู้เข้าร่วมประชุม activity, file, whiteboard count, space IDs และอื่น ๆ จะถูกจัดแสดงในรายงาน https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-control-hub/datasheet-c78-740772.html https://help.webex.com/en-us/47hkcw/View-My-Webex-Reports-on-Your-Cisco-Webex-Site และมีการทบทวนนโยบายเพื่อความมั่นคงปลอดภัยอยู่สม่ำเสมอ
6.8	ต้องมีการดูแลข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยอย่างน้อยต้องสามารถระบุผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการใช้ หรือประมวลผล	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ซึ่งมีข้อมูลส่วนบุคคลจัดเก็บอยู่ภายใน โดยครอบคลุมข้อมูล ผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการเป็นอย่างน้อย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	ผู้จัดการประชุมสามารถเข้าถึงข้อมูลการประชุม ที่เกี่ยวข้องกับการใช้งานของผู้เข้าร่วมประชุม โดยสามารถเข้าได้ถึงข้อมูลที่สามารถระบุตัวบุคคล วันและเวลา ข้อมูลของผู้เข้าร่วมประชุม ซึ่งข้อมูล วัน เวลา ผู้เข้าร่วมประชุม activity, file, whiteboard count, space IDs และอื่น ๆ จะถูกจัดแสดงในรายงาน ตามมาตรฐานสากล ISO 27018 https://help.webex.com/en-us/47hkcw/View-My-Webex-Reports-on-Your-Cisco-Webex-Site
6.9	ต้องป้องกันการเปลี่ยนแปลง และการเข้าถึงที่ไม่ได้รับอนุญาต ต่อข้อมูลจราจรอิเล็กทรอนิกส์	ผู้ให้บริการควรจัดเตรียมวิธีป้องกัน การเปลี่ยนแปลง การเข้าถึง และการลบ โดยไม่ได้รับอนุญาตต่อข้อมูลจราจรอิเล็กทรอนิกส์ เช่น การจำกัดสิทธิการดำเนินการในแต่ละฟังก์ชันการทำงาน การเฝ้าระวังและแจ้งเตือนการเข้าใช้งานที่ผิดปกติ ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีการกำหนดสิทธิของผู้ดูแลระบบ สามารถแบ่ง และ กำหนดการเข้าถึงของข้อมูลของ admin รวมถึงความสามารถในการตัดแปลงข้อมูล https://help.webex.com/en-us/nka5cbp/Assign-the-User-Management-Role-in-Webex-Site-Administration Table 1 https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-control-hub/datasheet-c78-740770.html สามารถตั้งค่าเพื่อจัดการกับการเข้าสู่ระบบที่ไม่สำเร็จ https://help.webex.com/en-us/9kb5iv/Configuring-Authentication-Authorization-and-Accounting มีการป้องกันการเปลี่ยนแปลง และการเข้าถึงที่ไม่ได้รับอนุญาต ต่อข้อมูลจราจรอิเล็กทรอนิกส์ตามมาตรฐาน ISO 27001 และ ISO 27017
6.10	ต้องจำกัดการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ รวมถึงกำหนดระยะเวลาในการลบหรือเปลี่ยนรูปข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบอย่างเหมาะสม	ผู้ให้บริการควรกำหนดวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์ โดยครอบคลุมการบันทึกกิจกรรมที่เกี่ยวข้อง เช่น การเข้าถึงข้อมูลส่วนบุคคล ฯลฯ ผู้ให้บริการควรกำหนดระยะเวลาที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระบบควบคุมการประชุม และแจ้งเงื่อนไขดังกล่าวให้ผู้มีหน้าที่จัดการประชุม หรือผู้ร่วมประชุมทราบผ่านช่องทางที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของผู้ให้บริการ ฯลฯ พร้อมกำหนดวิธีการลบ หรือการเปลี่ยนแปลงรูปแบบข้อมูลส่วนบุคคลที่จัดเก็บให้ไม่สามารถระบุตัวบุคคลได้ร่วมด้วย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27701	ข้อมูลส่วนบุคคลของผู้ใช้งาน ถูกกำหนดให้ผู้ใช้แต่ละคนเข้าถึงได้ด้วยตัวเองเพียงผู้เดียว ผู้ใช้งานสามารถเข้าถึงข้อมูลได้จาก webex site ส่วนบุคคล การเข้าถึงได้ถูกชี้แจงไว้ใน https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1552559092865169 ผู้ดูแลระบบสามารถตั้งค่า retention policy เพื่อกำหนดนโยบาย และระยะเวลาการจัดเก็บข้อมูลได้ ตั้งแต่ 30 วันเป็นต้นไป https://help.webex.com/en-us/WBX000027059/Webex-Data-Retention-FAQ มีวิธีการในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บในข้อมูลจราจรอิเล็กทรอนิกส์โดยครอบคลุมการบันทึกกิจกรรมที่เกี่ยวข้อง ตามมาตรฐาน ISO 27018
6.11	ต้องมีการจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์จากการใช้งานของผู้ควบคุมระบบและผู้ให้บริการ รวมถึงมีการทบทวนอย่างเหมาะสม โดยต้องมีการประกาศหรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบ	ผู้ให้บริการควรจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ควบคุมระบบ และควรประกาศ หรือแจ้งข้อมูลเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลให้ผู้เกี่ยวข้องทราบ ผ่านช่องทางที่มีความน่าเชื่อถือ 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	มีการจัดเก็บข้อมูล ข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูลจราจรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้งานของผู้ควบคุมระบบ ตามมาตรฐาน ISP 27001 ISO 27017 และ ISO 27018 ผู้จัดงานสามารถเข้าถึงข้อมูลการจัดเก็บของผู้เข้าร่วมประชุม และสามารถเข้าดูย้อนหลังได้ถึง 1 ปี https://help.webex.com/en-us/2tc9yx/Review-Your-Administrator-Activity-Logs-in-Cisco-Webex-Control-Hub ระบบสามารถตั้งค่าการแจ้งเตือน และจัดเก็บข้อมูลการพยายามเข้าใช้งานระบบ รวมถึงตัดสิทธิการเข้าถึงระบบหากมีการพยายามที่เกินกว่าจำนวนที่กำหนด https://help.webex.com/en-us/9kb5iv/Configuring-Authentication-Authorization-and-Accounting
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	สามารถตั้ง time zone ได้ https://help.webex.com/en-us/njfc0yg/Configure-Appearance-Options-for-Your-Webex-Site#ID-2473-0000041a

	6.13	ต้องจัดการช่องโหว่ทางเทคนิคของระบบควบคุมการประชุม โดยต้องได้รับการแก้ไขอย่างมีประสิทธิภาพ	ผู้ให้บริการควรกำหนดช่องทางในการรับแจ้งช่องโหว่ และดำเนินกิจกรรมการประเมินผลกระทบการจัดการช่องโหว่ เมื่อมีผู้แจ้งเหตุอย่างทันท่วงที พร้อมเผยแพร่รายละเอียดของช่องโหว่ให้ผู้เกี่ยวข้องทราบ ผู้ให้บริการควรมีการตรวจสอบช่องโหว่ทางเทคนิคของระบบควบคุมการประชุมอย่างน้อย 1 ครั้งต่อปี หรือเมื่อระบบควบคุมการประชุมมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้แน่ใจว่าระบบควบคุมการประชุมไม่มีความเสี่ยงรุนแรงที่อาจส่งผลต่อการให้บริการ หรือกระทบต่อข้อมูลส่วนบุคคล	ISO 27001	มีมาตรการจัดการช่องโหว่ทางเทคนิคของระบบ และมาตรการการแก้ไข รวมถึงมีการตรวจสอบช่องโหว่ทางเทคนิค(vulnerability scans) ทุกวัน ตามมาตรฐาน ISO 27001 และ ISO 27017 และมีการรายงานถึงความปลอดภัยและแก้ไขปัญหาด้านความปลอดภัยตลอด 24 ชั่วโมง โดยทีม Cisco Product Security Incident Response Team และ มีการแจ้งความน่าจะเป็นเพื่อป้องกันการเกิดเหตุด้านความปลอดภัยโดยทีม Cisco Computer Security (and Data) Incident Response Team
	6.14	ต้องทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม เช่น การตรวจประเมินภายใน (internal audit) อย่างน้อย 1 ครั้งต่อปี ฯลฯ	ISO 27001	มีการทบทวนความสอดคล้องด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม ตามมาตรฐาน 27001 และมีการตรวจประเมิน อย่างน้อยปีละครั้ง
7	**ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล**				
	7.1	ต้องบริหารจัดการเครือข่ายอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรให้มีการบริหารจัดการเครือข่าย โดยครอบคลุมมาตรการดังต่อไปนี้เป็นอย่างน้อย (1) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต (2) การป้องกันการดักรับข้อมูล (3) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย (4) การบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล (5) การป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น กำหนดให้ติดตั้งไฟร์วอลล์ และติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ ฯลฯ	ISO 27001	มีการจัดการเครือข่ายโดยครอบคลุมและปลอดภัย 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
	7.2	ต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้องต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้ ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายและขั้นตอนปฏิบัติควรครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโอนย้ายข้อความ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย ขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการเข้าถึงข้อมูลบนเครือข่ายควรกำหนดวิธีการและช่องทางการดำเนินการอย่างชัดเจน โดยอาจเชื่อมโยงแผนภาพเครือข่าย เพื่อให้แน่ใจว่าครอบคลุมการดำเนินการของระบบควบคุมการประชุม รวมถึงกรณีที่มีข้อมูลส่วนบุคคลที่รับส่งอยู่บนเครือข่ายควรมีการบันทึกกิจกรรมการดำเนินการ พร้อมผู้รับผิดชอบให้ชัดเจน	ISO 27001	มีการจัดนโยบายแล้วขั้นตอนการปฏิบัติที่ควบคลุมเรื่องการเข้าถึงรหัสลับระหว่างโอนย้ายข้อความ และข้อมูลอื่น ๆ ตามมาตรฐาน ISO 27001 และ ISO 27017 รวมไปถึงมีนโยบายการควบคุมเกี่ยวกับข้อมูลส่วนตัวตามมาตรฐาน ISO 27018 ข้อมูลส่วนบุคคลจะเป็นสิทธิของแต่ละบุคคลที่จะรับผิดชอบในการเข้าถึงหรือแบ่งปัน มีการบัญชีกข้อมูลของผู้เข้าถึงข้อมูลรวมถึงสามารถเข้าถึงข้อมูลย้อนหลังและรายงานได้ https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-control-hub/datasheet-c78-740772.html https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatamap/collaboration/webex-meetings-privacy-data-map.pdf Data in transit จะถูก encrypt โดย AES-256 for storage, Keys managed through AWS KMS ในขณะที่ data at rest, Cisco Webex Meetings เก็บ password ใช้ SHA-2 (one way hashing algorithm) File - 256-bit block AES GCM key แล้ว File key encrypted โดย primary key based บน AES HmacSHA256 https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
8	**การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย**				
	8.1	ต้องมีขั้นตอนปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม โดยหากพบว่ามีข้อมูลส่วนบุคคลรั่วไหล ต้องมีมาตรการในการจัดการอย่างมั่นคงปลอดภัย	ผู้ให้บริการควรจัดทำขั้นตอนการปฏิบัติเรื่องการรับมือเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุมที่ครอบคลุมกระบวนการดังต่อไปนี้ เป็นอย่างน้อย (1) การรับแจ้งและยืนยันเหตุฯ (2) การจำแนกเหตุฯ และประเมินผลกระทบ (3) การตอบสนองต่อเหตุฯ (4) การจัดเก็บพยานหลักฐาน ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการระบุเพิ่มเติมถึงความรับผิดชอบในแต่ละกระบวนการ ข้อมูลที่รั่วไหล การรายงานเหตุฯ ไปยังผู้เกี่ยวข้อง เป็นอย่างน้อย	ISO 27001, ISO 27701	มีกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงตาม Security Technical Implementation Guidelines (STIGs) ที่ประกาศโดย the National Institute of Standards and Technology (NIST) มีการรายงานถึงความปลอดภัยและแก้ไขปัญหาด้านความปลอดภัยตลอด 24 ชั่วโมง โดยทีม Cisco Product Security Incident Response Team และ มีการแจ้งความน่าจะเป็นเพื่อป้องกันการเกิดเหตุด้านความปลอดภัยโดยทีม Cisco Computer Security (and Data) Incident Response Team https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-room-series/white-paper-c11-743769.html Cisco มี Cisco Product Security Incident Response Team ที่บริหารจัดการในส่วนของการรับแจ้ง สืบสวน และทำรายงานเกี่ยวกับ security vulnerability information มีวิธีการ ในการรับมือ ตามขั้นตอนด้านล่าง - Awareness: PSIRT receives notification of security incident. - Active Management: PSIRT prioritizes and identifies resources. - Fix Determined: PSIRT coordinates fix and impact assessment. - Communication Plan: PSIRT sets timeframe and notification format. - Integration and Mitigation: PSIRT engages experts and executives. - Notification: PSIRT notifies all customers simultaneously. - Feedback: PSIRT incorporates feedback from customers and Cisco internal input. สามารถดูข้อมูลเพิ่มเติมได้ทาง https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-psirt-infographic.pdf และ https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html ผู้ใช้งานสามารถติดต่อได้ทาง - Cisco Security: cisco.com/security - Contact PSIRT: psirt@cisco.com - RSS feeds: http://tools.cisco.com/security/center/rss.x?i=44 - My Notifications: https://www.cisco.com/c/en/us/support/web/tools/cns/ notifications.html Cisco PSIRT openVuln API: https://developer.cisco.com/site/PSIRT/ ขั้นตอนการปฏิบัติการรับมือด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุม ตามมาตรฐาน ISO 27001 ISO 27017 และ ISO 27018

8.2	ต้องมีการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม	ผู้ให้บริการควรจัดให้มีช่องทางการรับแจ้งเหตุและรายงานด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุมการประชุม รวมถึงความขัดข้องที่ส่งผลกระทบต่อการประชุม โดยข้อมูลที่แจ้งควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) รายละเอียดผู้แจ้งเหตุฯ (2) วันเวลาที่พบเหตุฯ (3) รายละเอียดของเหตุฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีการรายงานถึงความปลอดภัยและแก้ไขปัญหาด้านความปลอดภัยตลอด 24 ชั่วโมง โดยทีม Cisco Product Security Incident Response Team และ มีการแจ้งความน่าจะเป็นเพื่อป้องกันการเกิดเหตุด้านความปลอดภัยโดยทีม Cisco Computer Security (and Data) Incident Response Team และมีการแจ้งถึงผู้ดูแลระบบทางอีเมล หากมีเหตุการณ์ทางความปลอดภัยเกิดขึ้น นอกจากนั้นผู้ใช้บริการสามารถกดรับข่าวสารแจ้งเตือนแจ้งเตือน incident ผ่าน Webex ได้เช่นกัน ผู้ใช้บริการสามารถติดต่อ รายงาน เกี่ยวกับ incident ได้ผ่านทาง เบอร์โทรศัพท์ เปิดเคสเพื่อแจ้งเหตุขัดข้อง ติดต่อเจ้าหน้าที่ผ่าน แชท และโทรศัพท์ ได้ทาง https://help.webex.com/contact การได้รับข่าวสาร ผู้ใช้บริการสามารถเปิดแจ้งเตือนเหตุผ่านทาง webex ได้เช่นกัน https://help.webex.com/en-us/WBX9000022491/Cisco-Webex-Incident-Notifications https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-room-series/white-paper-c11-743769.html
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 ผลกระทบช่วงเวลาที่เกิดผลกระทบ ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหล ผู้ให้บริการควรมีการดำเนินการเพิ่มเติมอย่างน้อยในกระบวนการการสื่อสารไปยังเจ้าของข้อมูล และผู้เกี่ยวข้อง	ISO 27001	สามารถจัดการจัดเก็บพยายานและตรวจสอบ โดยการทำ E-discovery https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-control-hub/datasheet-c78-740772.html#EdiscoverySearchandextraction มีกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงตาม Security Technical Implementation Guidelines (STIGs) ที่ประกาศโดย the National Institute of Standards and Technology (NIST) มีการรายงานถึงความปลอดภัยและแก้ไขปัญหาด้านความปลอดภัยตลอด 24 ชั่วโมง ให้กับเจ้าของข้อมูล โดยทีม Cisco Product Security Incident Response Team และ มีการแจ้งความเสี่ยงเพื่อป้องกันการเกิดเหตุด้านความปลอดภัยถึงผู้ดูแลระบบทางอีเมล โดยทีม Cisco Computer Security (and Data) Incident Response Team https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-room-series/white-paper-c11-743769.html หลังจากที่ได้รับการรายงาน cisco มีระบบที่มีการแก้ไขโดยแบ่งออกเป็นระบบความรุนแรง เพื่อจัดหาทีมที่เหมาะสมในการแก้ไข รวมไปถึงการบอกแนวทางการแก้ไข และป้องกัน ผู้ใช้บริการสามารถให้ข้อมูลเกี่ยวกับเหตุ และจะมีการติดต่อจากทีม support ไปทางอีเมลที่ผู้ให้บริการได้แจ้งไว้ หากมีเหตุเกิดขึ้น cisco จะแจ้งไปยังผู้ใช้บริการ ผ่านทาง email หรือ RSS feed สามารถดูรายละเอียดได้ทาง https://www.cisco.com/c/en/us/support/web/tac/technical-services-resource-guide.html https://help.webex.com/en-us/WBX162/How-Do-I-Contact-Webex-Customer-Services-or-Technical-Support https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf ขั้นตอนทั้งหมดนั้นเป็นไปตาม การปฏิบัติการรับมือด้านการรักษาความมั่นคงปลอดภัยของระบบควบคุม ตามมาตรฐาน ISO 27001 และ ISO 27017
8.4	ต้องมีขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างชัดเจน	ผู้ให้บริการควรจัดทำขั้นตอนปฏิบัติเรื่องการรวบรวม และจัดเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ให้บริการควรรวบรวมบันทึกกิจกรรมที่ดำเนินการ พร้อมระบุวันเวลา และวิธีการจัดเก็บอย่างชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีการรายงานถึงความปลอดภัยและแก้ไขปัญหาด้านความปลอดภัยตลอด 24 ชั่วโมง โดยทีม Cisco Product Security Incident Response Team มีการทำ threat modelling เพื่อสามารถระบุได้ถึง threat และ หลีกเลี่ยงความเสี่ยงตามที่ควร ในรายงานจะมีการระบุถึงปัญหาที่เกิดขึ้น สาเหตุ รวมถึงวันและเวลา พร้อมกับแนวทางการแก้ไขปัญหา เป็นรายงานส่งให้ผู้ดูแลระบบ https://trustportal.cisco.com#/1552559092865169 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-room-series/white-paper-c11-743769.html
9 ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ				
9.1	ต้องมีแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน	ผู้ให้บริการควรจัดทำแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน เช่น เกิดเหตุภัยพิบัติ เกิดจากโจมตีทางไซเบอร์ ฯลฯ และแผนฯ ควรครอบคลุมรายละเอียดดังต่อไปนี้เป็นอย่างน้อย (1) ผู้เกี่ยวข้อง (2) ขั้นตอนการรับมือ และกู้คืนเหตุฯ (3) กำหนดการทดสอบแผนฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีแผนการรับมือบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม ภายใต้สถานการณ์ฉุกเฉิน ตามมาตรฐาน ISO 27001:2013 27017:2015, 27018:2019, 27701:2019. Cisco Webex Global site Backup จะทำการ backup ข้อมูลทุกๆวัน วันละหนึ่งครั้ง โดยกรณีที่การสำรองนั้นมีข้อมูลส่วนบุคคลอยู่ด้วย มีการกำหนดรายละเอียดผู้เกี่ยวข้องในแต่ละกิจกรรม เช่น ผู้ดำเนินการสำรองข้อมูล ผู้ทดสอบการกู้คืนข้อมูล หากมีเหตุฉุกเฉิน ผู้ใช้บริการจะย้ายไปยัง back up site เพื่อการดำเนินงานต่อไป https://help.webex.com/en-us/31k2xo/Cisco-Webex-Global-Site-Backup
9.2	ต้องมีการซ้อมแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุมอย่างเหมาะสม	ผู้ให้บริการควรจัดให้มีการซ้อมและปรับปรุงแผนบริหารจัดการความต่อเนื่องของการให้บริการระบบควบคุมการประชุม อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจว่าแผนดังกล่าวมีความครอบคลุมการรับมือความเสี่ยงที่อาจเกิดขึ้นกับระบบควบคุมการประชุมอย่างมีประสิทธิภาพ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีการซ้อมสม่ำเสมอในระบบภายใน และผ่านตามมาตรฐานอย่างน้อยปีละ 1 ครั้ง โดยหากมีการเปลี่ยนแปลงจะมีการแจ้งให้ทราบ https://trustportal.cisco.com#/1552559092865169
9.3	ต้องมีระบบสำรองที่พร้อมให้บริการอย่างต่อเนื่องและเพียงพอต่อการให้บริการ	ระบบสำรองของระบบควบคุมการประชุมควรทำงานทดแทนระบบหลักได้อย่างปกติ และเพียงพอต่อการใช้งานตามที่มีการประเมินความพร้อมของทรัพยากรที่ใช้ ผู้ให้บริการควรจัดให้มีการทดสอบระบบสำรองเป็นประจำอย่างน้อย 1 ครั้งต่อปี ตามขั้นตอนปฏิบัติที่กำหนดขึ้น	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001	มีระบบสำรองของระบบควบคุมการประชุมที่ทำงานทดแทนระบบหลักได้อย่างปกติ และมีการเช็คความพร้อมอยู่ตามเวลา รวมถึงการ backup ข้อมูลทุก ๆ 24 ชั่วโมง และมีการทดสอบระบบอย่างต่อเนื่องอย่างน้อยปีละครั้ง มี data center ทั่วโลก เพื่อรับรอง และเพิ่มความมั่นคง เพื่อไม่ให้มีการติดขัดในการทำงานของระบบ https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html#CiscoWebexDataCenterSecurity
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	มีนโยบายการจัดการความเสี่ยงตาม ตามมาตรฐาน ISO 27001:2013 27017:2015, 27018:2019, 27701:2019. มีการแจ้งความเสี่ยงเพื่อป้องกันการเกิดเหตุด้านความปลอดภัยโดยทีม Cisco Computer Security (and Data) Incident Response Team มีการทดสอบความเสี่ยงต่างๆอยู่สม่ำเสมอ ตามมาตรฐาน SOC 3 https://trustportal.cisco.com#/1604982898019524 วิธีการลำดับการรักษาความปลอดภัยได้ชี้แจงไว้ใน https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf
	10.2	ต้องทบทวนวิธีการบริหาร จัดการความเสี่ยงอย่างสม่ำเสมอ	ผู้ให้บริการควรกำหนดระยะเวลาทบทวนวิธีการบริหารจัดการความเสี่ยง และวิธีการประเมินความเสี่ยงพร้อมดำเนินการทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การอัปเดตการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม การเปลี่ยนแปลงกฎหมายหรือมาตรฐาน ฯลฯ	ISO 27001	มีการทดสอบความเสี่ยงต่าง ๆอยู่สม่ำเสมอเพื่อทบทวนวิธีการบริหารจัดการความเสี่ยง และวิธีการประเมินความเสี่ยงพร้อมดำเนินการทบทวนตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ตามมาตรฐาน SOC 3 https://trustportal.cisco.com#/1604982898019524

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พ.ศ. 2563

แบบประเมินความสอดคล้องของระบบควบคุมการประชุมกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พ.ศ. 2563 กรณี ประเมินความสอดคล้องด้วยตนเอง

ชื่อระบบ :	**Cisco Webex**			
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท) :	**Cisco System (Thailand) LTD.**			
ช่องทางการติดต่อผู้ให้บริการ :	**02-263-7000**			
วันที่ประเมินความสอดคล้อง	**5 กุมภาพันธ์ 2564**			
ประเภทการประเมินความสอดคล้องด้วยตนเอง	☐ การประชุมทั่วไป	☑ การประชุมลับ	☐ การประชุมลับ (ภาครัฐ)	
ประเภทของระบบการให้บริการ	☑ On-Cloud	☐ On-Premise	☐ อื่น ๆ โปรดระบุ	
มาตรฐานที่ได้รับการรับรอง	☑ ISO/IEC 27001	☑ ISO/IEC 27701	☐ อื่น ๆ โปรดระบุ	
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง :	**ระบบ Cisco Webex ขอบเขตการประเมินสอดคล้องตามมาตรฐานความมั่นคงปลอดภัยของระบบควบคุมการประชุม พ.ศ. 2563 โดยครอบคลุมการประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องทั่วไป**			

หมายเหตุ : ☐ เธอ ไม่เกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อกำหนด	แนวปฏิบัติ	ความสอดคล้อง	ความสามารถของระบบควบคุมการประชุม
2 การบริหารจัดการสินทรัพย์			
2.1 ต้องมีบัญชีทะเบียนสินทรัพย์ที่แสดงให้เห็นสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุม โดยครอบคลุมทั้งสินทรัพย์ทางกายภาพ เครือข่าย โปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง ทั้งนี้ หากเป็นการให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ ต้องมีบัญชีทะเบียนสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลอยู่ในราชอาณาจักรทั้งหมด และต้องมีเอกสารรับรองหรือประกาศอย่างเป็นทางการ	ในกรณีที่ระบบควบคุมการประชุมนั้นให้บริการรองรับการประชุมเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ ผู้ให้บริการควรมีเอกสารรับรอง หรือประกาศอย่างเป็นทางการ เพื่อรับรองว่าสินทรัพย์ที่ใช้ในการบันทึกหรือประมวลผลข้อมูลทั้งหมดของระบบควบคุมการประชุมติดตั้งและให้บริการอยู่ในราชอาณาจักร และไม่จัดเก็บข้อมูลหรือหลักฐานส่วนหนึ่งส่วนใดไว้นอกราชอาณาจักร	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	Cisco มีการจัดทำทะเบียนสินทรัพย์ที่แสดงให้เห็นถึงการบันทึกและการประมวลผล ครอบคลุมทั้งกายภาพ เครือข่ายโปรแกรมประยุกต์ และข้อมูลที่เกี่ยวข้อง โดยระบบของ Cisco Webex ตั้งอยู่บน cloud ของ บริษัท ซิสโก้ ซีสเต็มส์จำกัด ตั้งอยู่ในแต่ละภูมิภาคของโลกนอกราชอาณาจักรไทย ที่มีความปลอดภัยตามมาตรฐานโลก ISO 27001, 27017 and 27018 certified, Service Organization Controls (SOC) 2 Type II audited, SOC 3 certified สามารถดูข้อมูลเพิ่มเติมได้ที่ https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html https://help.webex.com/en-us/oybc4fb/Data-Residency-in-Webex
3 การควบคุมการเข้าถึง			
3.1 ต้องสามารถจำกัดการเข้าถึงข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุม ทั้งนี้หากเป็นการประชุมลับต้องมีการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับการประชุมเพิ่มเติม	ระบบควบคุมการประชุมควรมีวิธีการเข้ารหัสลับข้อมูล หรือหลักฐานที่เกี่ยวข้องกับการประชุมเป็นอย่างน้อย	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ข้อมูลมีการเข้ารหัสลับ ทั้ง transit และ at rest ทุกการสื่อสารจะมีการเข้ารหัสลับ Cisco Webex ใช้ TLS 1.2 protocol ในการทำ signaling Media Package จะถูกทำ Advanced Encryption Standard หรือ AES ทุกข้อมูลการจัดการระบบ ต้องผ่านการ authenticate และเข้ารหัสลับ industry-standard TLS and Secure Sockets Layer [SSL] https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
3.2 ต้องสามารถพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย ทั้งนี้หากเป็นการประชุมลับต้องมีการยืนยันตัวตนแบบหลายปัจจัย	ระบบควบคุมการประชุมควรมีช่องทางพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุมอย่างมั่นคงปลอดภัย ด้วยวิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication) เป็นอย่างน้อย เช่น รหัสผ่านและ One-time Password (OTP) ในการเข้าร่วมประชุม ฯลฯ	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ผู้ใช้งานสามารถเข้าระบบโดยใช้ username และ password เฉพาะบุคคล หรือสามารถเข้าระบบด้วยการใช้ SSO เพื่อเป็นการยืนยันตัวตนกับองค์กรรวมไปถึงการใช้ SAML2 คู่กับระบบการทำ Multi-factor authenticantion ได้ สามารถ enable Multi-factor authenticantion ได้โดย ผู้ใช้งานจะต้องใส่รหัสที่ได้รับ หรือ ยืนยันตัวตนในการเข้าใช้งาน เมื่อ Multi-factor authenticantion ได้ถูกเปิดใช้งาน ผู้ใช้จะสามารถใช้ time-based, one-time password (TOTP) authenticator app เพื่อเป็นการยืนยันตัวตนได้ https://help.webex.com/en-us/52szeq/Enable-Multi-Factor-Authentication-Integration-in-Webex-Control-Hub https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html

3.3	ต้องสามารถตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย ทั้งนี้หากเป็นการประชุมลับต้องมีการตรวจสอบรหัสผ่านที่กำหนดให้เป็นไปตามนโยบายที่กำหนดอย่างเคร่งครัด	ระบบควบคุมการประชุมควรมีความสามารถในการตรวจสอบ และป้องกันการตั้งรหัสผ่านที่ไม่มั่นคงปลอดภัยของผู้ร่วมประชุมตามนโยบายการตั้งค่ารหัสผ่านที่กำหนด	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์	ระบบมีความสามารถในการตรวจสอบ และป้องกันการตั้งรหัสผ่านและมีนโยบายในการตั้งรหัสผ่าน (1) ต้องมีอย่างน้อย 8 ตัวอักษร (2) ต้องมีอักษรตัวใหญ่ (3) ต้องมีอักษรตัวเล็ก (4) ต้องมีตัวเลข (5) ต้องมีอักขระพิเศษ นอกจากนี้ผู้ดูแลระบบสามารถ ควบคุมการตั้งรหัสผ่านได้โดยกำหนด (1) ห้ามมีตัวอักษรเดียวกันเรียงกันเกิน 3 ตัว (2) ห้ามเหมือนกับ Username (3) ห้ามใช้คำว่า "password" เป็นต้น สามารถดูข้อมูลเพิ่มเติมได้ที่ https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
4 การเข้ารหัสลับข้อมูล				
4.1	ต้องกำหนดนโยบายด้านการเข้ารหัสลับข้อมูลที่ระบุถึงการเข้ารหัสลับข้อมูลที่เกี่ยวข้องกับข้อมูลบนระบบควบคุมการประชุม และข้อมูลส่วนบุคคลที่เกี่ยวข้อง ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายควรระบุให้ครอบคลุมว่าผู้ให้บริการไม่สามารถเรียกดูข้อมูลในระหว่างทางของการรับส่งข้อมูล โดยอาจเปรียบเทียบการใช้งานในลักษณะ End-to-End Encryption (E2EE) ได้ และควรระบุขอบเขต ข้อยกเว้นในความสามารถที่เกี่ยวข้องให้ชัดเจน	กระบวนการจัดการประชุมผ่านสื่ออิเล็กทรอนิกส์, ISO 27001, ISO 27701	มีนโยบายการทำ End-to-End Encryption ตามมาตรฐานสากล ISO 27001, ISO 27701 ข้อมูลที่ถูกส่งจะถูกเข้ารหัสด้วย AES 128 หรือ AES 256, สำหรับ video device ที่รับรอง media encryption กับ SRTP จะถูกเข้ารหัสด้วย AES-CM-128-HMAC-SHA1. และในส่วนของ webex app จะใช้ AES-256-GCM ในการเข้ารหัส และ key จะถูกแลกเปลี่ยนผ่าน TLS-secured signaling channels https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
7 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล				
7.1	ต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลที่เกี่ยวข้องกับระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลเกี่ยวข้อง ต้องมีมาตรการในการติดตามการปฏิบัติให้สอดคล้องกับสิ่งที่กำหนดไว้ ทั้งนี้หากเป็นการประชุมลับต้องกำหนดนโยบายที่ระบุถึงการเข้ารหัสลับข้อมูลจากต้นทางถึงปลายทาง หรือในลักษณะที่ผู้ให้บริการไม่สามารถเข้าถึงข้อมูลที่รับส่งระหว่างการประชุมได้	นโยบายและขั้นตอนปฏิบัติควรระบุให้ครอบคลุมว่าผู้ให้บริการไม่สามารถเรียกดูข้อมูลในระหว่างทางของการรับส่งข้อมูล โดยอาจเปรียบเทียบการใช้งานในลักษณะ End-to-End Encryption (E2EE) ได้ และควรระบุขอบเขต ข้อยกเว้นในความสามารถที่เกี่ยวข้องให้ชัดเจน	ISO 27001, ISO 27701	มีนโยบายการทำ End-to-End Encryption ตามมาตรฐานสากล ISO 27001, ISO 27701 สำหรับการทำ E2EE ข้อมูลที่ถูกส่งจะถูกเข้ารหัสลับและผู้ให้บริการไม่สามารถเข้าถึงข้อมูล หรือ key ในการ decrypt ข้อมูลได้ Key ในการเข้ารหัสจะถูก generate จาก meeting host และส่งไปยังผู้เข้าร่วมประชุม ผู้เข้าร่วมประชุมจะ สร้าง 2048-bit RSA public และ private key pair ข้อมูลที่ถูกส่งจะถูกเข้ารหัสด้วย AES 128 หรือ AES 256, สำหรับ video device ที่รับรอง media encryption กับ SRTP จะถูกเข้ารหัสด้วย AES-CM-128-HMAC-SHA1. และในส่วนของ webex app จะใช้ AES-256-GCM ในการเข้ารหัส สามารถดูข้อมูลเพิ่มเติมรวมถึงขอบเขตได้ทาง https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html
8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย				
8.1	ต้องมีมาตรการสำหรับการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศที่อาจส่งผลกระทบต่อระบบควบคุมการประชุม โดยกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลต้องมีการสื่อสารกับเจ้าของข้อมูลและผู้เกี่ยวข้อง ทั้งนี้ หากเป็นการประชุมลับ ต้องดำเนินการแก้ไขปัญหาช่องโหว่ทางเทคนิคในระดับรุนแรง (อ้างอิงตามข้อมูล CVSS ที่ severity ระดับ high ขึ้นไป) ให้ครบทุกรายการก่อนให้บริการ	ผู้ให้บริการควรดำเนินการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงปัญหาช่องโหว่ทางเทคนิค อย่างน้อยช่องโหว่ที่เผยแพร่ตามรายการ CVE (Common Vulnerabilities and Exposures) และช่องโหว่ที่มีการตรวจประเมินจากผู้ให้บริการ ในระดับรุนแรงอ้างอิงตามข้อมูล CVSS ที่ severity ระดับ high ขึ้นไป ให้ครบทุกรายการก่อนให้บริการ	ISO 27001, ISO 27701	Cisco มี Cisco Product Security Incident Response Team ที่บริหารจัดการในส่วนของการรับแจ้ง สืบสวน และทำรายงานเกี่ยวกับ security vulnerability information มีวิธีการ ในการรับมือ โดยจัดลำดับความรุนแรง เพื่อดำเนินการแก้ไขปัญหา และ Cisco มี Cisco Product Security Incident Response Team ที่บริหารจัดการในส่วนของการรับแจ้ง สืบสวน และทำรายงานเกี่ยวกับ security vulnerability information Cisco ใช้ CVSS Version 3.1 เป็นมาตรฐานในการจัดการและดำเนินการแก้ไขปัญหาช่องโหว่ทางเทคนิค และมีการตรวจสอบช่องโหว่ทางเทคนิคและแก้ไขตามที่เผยแพร่ จาก CVSS ในระดับ high ก่อนให้บริการ โดยใช้ตัวชี้วัด 3 ตัวในการคำนวน Base, Temporal, และ Environmental calculations นอกจากนั้น Cisco ยังใช้ Security Impact Rating (SIR) ในการแบ่งประเภทของความรุนแรง สามารถดูข้อมูลเพิ่มเติมได้ทาง https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-psirt-infographic.pdf และ https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุม พ.ศ. 2563