NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สมาคมระบบกล้องวงจรปิดอัจฉริยะไทย
ICA
THAI INTELLIGENT CCTV ASSOCIATION

TCSG

THAILAND AI-ENABLED CCTV SECURITY GUIDELINES

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิด ที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย

Secure AI-Enabled
CCTV Systems
Safer Communities
A More Trusted Thailand

SECURE | SMART | TRUSTED | THAILAND

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	วันที่	รายละเอียดการแก้ไข	ผู้จัดทำ/แก้ไข
0.9.1	20 สิงหาคม 2569	ร่างเอกสารฉบับแรกเพื่อรับฟังความคิดเห็น	คณะทำงาน
0.9.2	11 กันยายน 2569	ปรับปรุงตามความเห็นจากการประชุมกลุ่มย่อย	คณะทำงาน
0.9.3	12 กันยายน 2569	ปรับปรุงตามความเห็นของคณะทำงาน	คณะทำงาน
0.9.4	20 กันยายน 2569	ปรับปรุงโครงสร้างและเนื้อหาเพื่อรับฟังความคิดเห็นจากประชาพิจารณ์	คณะทำงาน
0.9.5	24 กันยายน 2569	ปรับปรุงตามความเห็นจากประชาพิจารณ์	คณะทำงาน
0.9.6	27 กันยายน 2569	ปรับปรุงตามข้อสรุปจากการรับฟังความคิดเห็นสาธารณะและแก้ไขข้อผิดพลาดเชิงโครงสร้าง (รายละเอียดในภาคผนวก จ)	คณะทำงาน
1.0.0	29 กันยายน 2569	ฉบับประกาศใช้ ตรวจทานความสอดคล้องทั้งเล่มหลังการรับฟังความคิดเห็น	คณะทำงาน

คำนำ

ระบบกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV) ได้พัฒนาจากระบบบันทึกภาพแบบแยกส่วนไปสู่ระบบที่เชื่อมต่อผ่านเครือข่าย สามารถบริหารจัดการจากระยะไกล เชื่อมโยงกับระบบสารสนเทศ และใช้บริการภายนอกหรือบริการคลาวด์ เพื่อสนับสนุนการจัดเก็บ ประมวลผล และบริหารจัดการข้อมูล ระบบ CCTV จึงเป็นส่วนหนึ่งของโครงสร้างพื้นฐานดิจิทัลที่มีบทบาทต่อการรักษาความปลอดภัย การเฝ้าระวัง การตรวจสอบเหตุการณ์ และการสนับสนุนภารกิจขององค์กรทั้งภาครัฐ ภาคเอกชน และประชาชน การเชื่อมต่อและการเพิ่มความสามารถของระบบดังกล่าวทำให้ต้องพิจารณาความเสี่ยงมากกว่าความมั่นคงปลอดภัยทางกายภาพเพียงด้านเดียว โดยครอบคลุมความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล ความพร้อมใช้งานและความน่าเชื่อถือของระบบ ตลอดจนการกำกับดูแลและการดำเนินงานตลอดวงจรชีวิตของระบบ

ความเสี่ยงอาจเกิดจากหลายปัจจัย เช่น การใช้ข้อมูลยืนยันตัวตนเริ่มต้น (เช่น รหัสผ่านจากโรงงาน) การไม่ปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ การเปิดให้เข้าถึงจากระยะไกลโดยไม่มีมาตรการที่เหมาะสม การให้สิทธิในการเข้าถึงเกินความจำเป็น การจัดเก็บข้อมูลเกินระยะเวลาที่กำหนด ตลอดจนข้อจำกัดของผลิตภัณฑ์ ผู้ให้บริการ หรือส่วนประกอบในห่วงโซ่อุปทาน ความเสี่ยงเหล่านี้อาจส่งผลต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบ รวมถึงอาจส่งผลกระทบต่อสิทธิและความเป็นส่วนตัวของบุคคล

ด้วยเหตุนี้ คณะทำงานจึงได้จัดทำ **แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดสำหรับประเทศไทย (Thailand CCTV Security Guidelines)** เพื่อเป็นกรอบแนวปฏิบัติกลางสำหรับการบริหารความมั่นคงปลอดภัยของระบบ CCTV ให้เหมาะสมกับบริบทของประเทศไทย โดยอ้างอิงหลักการบริหารตามผลกระทบและความเสี่ยง มาตรฐานและแนวปฏิบัติสากล ตลอดจนกฎหมาย ประกาศและข้อกำหนดของประเทศไทยที่เกี่ยวข้อง

แนวปฏิบัตินี้ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ ตั้งแต่การกำหนดวัตถุประสงค์และความต้องการ การออกแบบ การจัดซื้อจัดจ้าง การติดตั้งและตรวจรับ การใช้งาน การบำรุงรักษาและเฝ้าระวัง การจัดการช่องโหว่ การตอบสนองต่อเหตุการณ์ การประเมินและยกระดับระบบเดิม จนถึงการเลิกใช้อุปกรณ์และการจัดการข้อมูล

แนวปฏิบัตินี้ได้รับการออกแบบให้สามารถประยุกต์ใช้กับผู้เกี่ยวข้องหลายกลุ่ม ได้แก่

- **เจ้าของระบบและองค์กรผู้ใช้งาน** เพื่อใช้กำหนดวัตถุประสงค์ ระดับความสำคัญ ความเสี่ยง ข้อกำหนด และการกำกับดูแลระบบ
- **ผู้ปฏิบัติงานและผู้ดูแลระบบ** เพื่อใช้เป็นแนวทางในการควบคุมสิทธิ การตั้งค่า การเฝ้าระวัง การบำรุงรักษา และการตอบสนองต่อเหตุการณ์
- **ผู้ติดตั้ง ผู้รวมระบบ และผู้ให้บริการ** เพื่อสนับสนุนการออกแบบ ติดตั้ง ตั้งค่า ทดสอบ ส่งมอบ และดูแลระบบอย่างมั่นคงปลอดภัย

- **ผู้ผลิตและผู้จำหน่าย** เพื่อสนับสนุนการพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย การบริหารช่องโหว่ การสนับสนุนตลอดวงจรชีวิต และการบริหารความเสี่ยงจากห่วงโซ่อุปทาน
- **ผู้จัดซื้อ ผู้กำกับดูแล และผู้ตรวจประเมิน** เพื่อใช้ประกอบการกำหนดข้อกำหนด การตรวจรับ การติดตาม และการประเมินความสอดคล้อง
- **ประชาชนและผู้ใช้งานระบบขนาดเล็ก** เพื่อใช้เป็นแนวทางพื้นฐานในการลดความเสี่ยงและคุ้มครองข้อมูลจากระบบ CCTV ที่ตนรับผิดชอบ

นอกจากนี้ คณะทำงานยังได้จัดทำ **แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย (Thailand AI-Enabled CCTV Security Guidelines)** เพื่อเป็นกรอบแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในระบบ CCTV ที่มีการใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ซึ่งมีลักษณะ ความเสี่ยง และข้อควรคำนึงเพิ่มเติมจากระบบ CCTV ทั่วไป

การนำแนวปฏิบัติไปใช้ควรดำเนินการอย่างเหมาะสมและได้สัดส่วนกับวัตถุประสงค์ บริบท ระดับความสำคัญ และความเสี่ยงของระบบ โดยไม่ผูกกับผู้ผลิต ยี่ห้อ ผลิตภัณฑ์ รูปแบบการติดตั้ง หรือเทคโนโลยีใดเป็นการเฉพาะ ทั้งนี้ แนวปฏิบัติทั้งสองฉบับนี้เป็นเพียงข้อเสนอแนะเบื้องต้นให้กับผู้ที่เกี่ยวข้อง ไม่มีสภาพบังคับใช้ ไม่สามารถใช้แทนกฎหมาย ประกาศ หลักเกณฑ์ สัญญา หรือข้อกำหนดอื่นที่มีผลใช้บังคับ

กิตติกรรมประกาศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขอขอบคุณสมาคมระบบกล้องวงจรปิดอัจฉริยะไทย (iCA) คณะทำงานและที่ปรึกษาคณะทำงานขับเคลื่อนการยกระดับความมั่นคงปลอดภัยระบบกลองวงจรปดไทย และผู้ทรงคุณวุฒิจากหลายภาคส่วน ทั้งผู้ทรงคุณวุฒิจากภาครัฐ ภาคเอกชน ภาควิชาการ ภาคประชาสังคม ทั้งที่เอ่ยนามและมิได้เอ่ยนามในที่นี้ ที่ได้สละเวลา ความรู้ และความสามารถ รวมทั้งอนุเคราะห์ข้อมูลและข้อเสนอแนะที่เป็นประโยชน์ ต่อการจัดทำ “แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดสำหรับประเทศไทย (Thailand CCTV Security Guidelines : TCSG)” ฉบับนี้จนสำเร็จ

ทุกท่านได้ใช้ความรู้ ความสามารถ และประสบการณ์ ในการให้ข้อมูลและข้อเสนอแนะอันเป็นประโยชน์ และอันทรงคุณค่า ทั้งในที่ประชุมในสถานที่และผ่านช่องทางออนไลน์ซึ่งเป็นส่วนสำคัญอย่างยิ่งในการพัฒนาแนวปฏิบัติฉบับนี้ให้สำเร็จลุล่วง

สุดท้ายนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขอขอบคุณผู้เชี่ยวชาญ หน่วยงาน และผู้ที่เกี่ยวข้องกับระบบนิเวศระบบ CCTV ที่ร่วมสนับสนุนการจัดทำแนวปฏิบัติฉบับนี้ โดยได้เสียสละทรัพยากร ให้ข้อเสนอแนะและปรับปรุงแนวปฏิบัติฉบับนี้ให้มีความครบถ้วน เป็นประโยชน์ และสามารถนำไปใช้งานได้กับองค์กรทั้งภาครัฐและเอกชน เหมาะสมกับบริบทของประเทศไทย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แนวทางการอ่านเอกสารฉบับนี้

แนวปฏิบัตินี้ควรใช้ร่วมกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดสำหรับประเทศไทย โดยมุ่งเน้นความเสี่ยงและมาตรการเพิ่มเติมที่เกิดจากการนำปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้ในการวิเคราะห์ ประมวลผล หรือสนับสนุนการตัดสินใจจากข้อมูลภาพหรือวิดีโอ

องค์กรควรเริ่มจากการกำหนดวัตถุประสงค์และกรณีใช้งาน (Use Case) ประเมินระดับผลกระทบและความเสี่ยง แล้วเลือกมาตรการที่เหมาะสมกับระดับความเสี่ยงของระบบ

แนวปฏิบัติฉบับนี้ครอบคลุมผู้เกี่ยวข้องหลายบทบาท ผู้อ่านไม่จำเป็นต้องศึกษารายละเอียดทุกส่วนในระดับเดียวกัน โดยสามารถเลือกศึกษาและประยุกต์ใช้เนื้อหาตามบทบาท หน้าที่ ลักษณะของระบบ และระดับผลกระทบและความเสี่ยงตามข้อ 3.1 ทั้งนี้ ควรศึกษาหลักการพื้นฐานและข้อกำหนดที่มีผลใช้บังคับร่วมด้วยตามความเกี่ยวข้อง

กลุ่มผู้อ่าน	ลักษณะการใช้งาน/บทบาท	ควรอ่านเป็นหลัก	ควรอ่านเพิ่มเติม
บุคคลทั่วไปที่ใช้ CCTV ที่มี AI เพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว	ใช้ความสามารถ AI เช่น การตรวจจับบุคคล วัตถุ หรือเหตุการณ์ เพื่อดูแลบ้านพักอาศัย ทรัพย์สิน หรือความปลอดภัยส่วนบุคคล โดยไม่ได้ใช้เพื่อการประกอบธุรกิจหรือการดำเนินงานขององค์กร	บทที่ 1–2, ข้อ 3.1, ข้อ 4.1	ข้อ 3.3, ข้อ 3.10–3.11 และบทที่ 6 ตามความเกี่ยวข้อง
ผู้ประกอบการรายย่อย ร้านค้า และ SME	ใช้ CCTV ที่มี AI เพื่อการประกอบธุรกิจหรือการดำเนินงานของกิจการ ไม่ว่าจะดูแลระบบเองหรือใช้บริการจากบุคคลภายนอก	บทที่ 1–3, ข้อ 4.1 และภาคผนวก ข	บทที่ 5–6 และภาคผนวก ก ตามระดับความเสี่ยง
ผู้บริหารและเจ้าของระบบ	กำหนดวัตถุประสงค์ กรณีใช้งาน ระดับผลกระทบ ความเสี่ยง การอนุมัติ และการกำกับดูแลการใช้ AI	บทที่ 1, ข้อ 3.1, บทที่ 5	บทที่ 2–4, บทที่ 6 และภาคผนวก ก–ข
ผู้ปฏิบัติงานและผู้ดูแลระบบ	ใช้งาน ดูแล ตั้งค่า เฝ้าระวัง ตรวจสอบผลลัพธ์ AI และตอบสนองเมื่อพบความผิดปกติ	ข้อ 3.4–3.6, 3.8–3.10, ข้อ 4.5 และภาคผนวก ข	ข้อ 3.1–3.3, บทที่ 5–6

กลุ่มผู้อ่าน	ลักษณะการใช้งาน/บทบาท	ควรอ่านเป็นหลัก	ควรอ่านเพิ่มเติม
ผู้ติดตั้งและผู้รวมระบบ (System Integrator: SI)	ออกแบบรายละเอียด ติดตั้ง ตั้งค่า เชื่อมต่อ ทดสอบ และส่งมอบระบบ CCTV ที่มี AI	บทที่ 4, ข้อ 5.2 และภาคผนวก ก	ข้อ 3.1, 3.7–3.8 และบทที่ 6
ผู้จัดซื้อและผู้ตรวจประเมิน	กำหนดข้อกำหนด ประเมินผลิตภัณฑ์/บริการ ตรวจสอบหลักฐาน Assurance และสนับสนุนการทดสอบและตรวจรับ	บทที่ 5 และภาคผนวก ก	ข้อ 3.1, 3.7, บทที่ 4 และบทที่ 6
ผู้ผลิต ผู้พัฒนา และผู้ให้บริการ	พัฒนา ให้บริการ ปรับปรุง บริหารช่องโหว่ การเปลี่ยนแปลงของ AI ส่วนประกอบซอฟต์แวร์ และการสนับสนุนตลอดวงจรชีวิต	บทที่ 2, ข้อ 3.4, 3.7 และบทที่ 4–5	ข้อ 3.8–3.10, บทที่ 6 และภาคผนวก ก
ผู้รับผิดชอบด้านกฎหมาย ความเป็นส่วนตัว และการกำกับดูแล	พิจารณากฎหมาย ความเป็นส่วนตัว ข้อมูลชีวมิติ การใช้ AI ความโปร่งใส และข้อกำหนดเฉพาะภาคส่วน	ข้อ 3.2–3.3 และบทที่ 6	ข้อ 3.1, 3.10–3.11 และบทที่ 5
ผู้ที่มีระบบเดิมและกำลังพิจารณาเพิ่มหรือปรับปรุงความสามารถ AI	มีระบบ CCTV ที่ใช้งานอยู่และกำลังเพิ่มเปลี่ยน หรือยกระดับ AI, Analytics, Cloud หรือการเชื่อมต่อกับระบบอื่น	ข้อ 3.1, 3.8 และบทที่ 4	บทที่ 5–6 และภาคผนวก ก–ข

สารบัญ

หน้า

บทที่ 1 บทนำ **10**
1.1 ที่มาและความจำเป็น **10**
1.2 วัตถุประสงค์ของเอกสาร **11**
1.3 ผู้ใช้เอกสารและบทบาท **11**
1.4 สถานะของเอกสาร **12**
สรุปหลักการของบทที่ 1 ..... **13**
บทที่ 2 หลักการพื้นฐาน **14**
2.1 แนวทางการจัดทำแนวปฏิบัติ **14**
2.2 ขอบเขตของคำแนะนำ **16**
2.3 หลักการพื้นฐานที่ใช้ตลอดทั้งเล่ม **16**
สรุปหลักการของบทที่ 2 ..... **18**
บทที่ 3 การกำกับดูแล ระเบียบ และกฎหมาย **19**
3.1 การจำแนกระดับความสำคัญของระบบ **19**
3.2 กรอบแนวทาง มาตรฐานอ้างอิง และกฎหมายที่เกี่ยวข้อง **26**
3.3 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล **32**
3.4 การอัปเดตเฟิร์มแวร์และการบำรุงรักษา **37**
3.5 การเฝ้าระวังและบันทึกการใช้งาน **40**
3.6 รอบการตรวจเช็คและบำรุงรักษา **43**
3.7 เฟิร์มแวร์ ช่องโหว่ และการเลือกอุปกรณ์ที่น่าเชื่อถือ **45**
3.8 การสำรองข้อมูล การกู้คืน และความต่อเนื่องทางธุรกิจ **51**
3.9 การเลิกใช้อุปกรณ์และการทำลายข้อมูล **54**
3.10 ภัยคุกคาม สัญญาณเตือน และการรับมือเหตุ **56**
3.11 การอบรมและสร้างความตระหนัก **60**
สรุปหลักการของบทที่ 3 ..... **62**
บทที่ 4 ค่าตั้งต้นด้านความมั่นคงปลอดภัย **63**
4.1 เริ่มต้นอย่างมั่นคงปลอดภัยใน 7 ข้อ **63**
4.2 การแบ่งบทบาทหน้าที่ในบทนี้ **64**
4.3 การออกแบบ **65**
4.4 การติดตั้ง **69**
4.5 การดำเนินงานในภาวะปกติและการดูแลรักษา **74**

สรุปหลักการของบทที่ 4 77
บทที่ 5 การจัดซื้อจัดจ้าง....78
5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยในการจัดซื้อ....78
5.2 การส่งมอบและการตรวจรับอย่างมั่นคงปลอดภัย 84
สรุปหลักการของบทที่ 5 87
บทที่ 6 หัวข้อที่ต้องพิจารณาเพิ่มเติม....88
6.1 การใช้บริการคลาวด์และบริการภายนอกอย่างมั่นคงปลอดภัย 88
6.2 การวิเคราะห์วิดีโออัจฉริยะและข้อมูลชีวมิติ....92
6.3 เทคโนโลยีที่เกี่ยวเนื่องและการพัฒนาในอนาคต 95
6.4 การใช้ระบบวีดีโออัจฉริยะในเพื่อควบคุมการเข้าถึงระบบที่มีความสำคัญสูง 96
สรุปหลักการของบทที่ 6 96
ภาคผนวก ก รายการตรวจสอบก่อนส่งมอบ....97
ก.1 ข้อมูลระบบ....97
ก.2 รายการตรวจสอบ 98
ก.3 ข้อกำหนดที่มีผลใช้บังคับ 100
ก.4 มาตรฐาน การรับรอง และหลักฐานการสร้างความเชื่อมั่น....101
ภาคผนวก ข รายการตรวจสอบด้วยตนเองตามรอบ.... 102
ข.1 ข้อมูลการทบทวน 102
ข.2 รายการตรวจสอบตามรอบ....102
ข.3 การทบทวนนอกเหนือจากรอบที่กำหนด....105
ภาคผนวก ค อภิธานศัพท์ 106
ภาคผนวก ง เอกสารและมาตรฐานอ้างอิง.... 108
ง.1 ระบบเฝ้าระวังด้วยวิดีโอและการวิเคราะห์วิดีโออัจฉริยะ 108
ง.2 การกำกับดูแล การบริหารความเสี่ยง และการประเมินผลกระทบของ AI....109
ง.3 ความมั่นคงปลอดภัยและความน่าเชื่อถือของ AI....109
ง.4 ความมั่นคงปลอดภัยสารสนเทศ ความเป็นส่วนตัว ห่วงโซ่อุปทาน ช่องโหว่ และบริการคลาวด์ .110
ง.5 ข้อมูลชีวมิติ....111
ง.6 กฎหมาย ประกาศ และข้อกำหนดของประเทศไทย....112
ง.7 กรอบอ้างอิงด้านกฎระเบียบต่างประเทศ....112

บทที่ 1 บทนำ

1.1 ที่มาและความจำเป็น

ระบบกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV) ได้พัฒนาจากระบบที่ใช้สำหรับบันทึกและแสดงภาพ ไปสู่ระบบที่สามารถใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพื่อช่วยตรวจจับ จำแนก ติดตาม ระบุ หรือวิเคราะห์บุคคล วัตถุ เหตุการณ์ และพฤติกรรมจากข้อมูลภาพหรือวิดีโอ รวมถึงสามารถสร้างผลลัพธ์เพื่อแจ้งเตือน สนับสนุนการตัดสินใจ หรือเชื่อมต่อกับระบบอื่นเพื่อดำเนินการต่อได้

การนำ AI มาใช้ช่วยเพิ่มประสิทธิภาพและขยายความสามารถของระบบ CCTV แต่ในขณะเดียวกันอาจก่อให้เกิดความเสี่ยงเพิ่มเติมจากระบบ CCTV ทั่วไป เช่น ความผิดพลาดของการวิเคราะห์หรือการระบุบุคคล การใช้ข้อมูลเกินกว่าวัตถุประสงค์ การติดตามหรือเชื่อมโยงข้อมูล การประมวลผลข้อมูลชีวมิติ (Biometric Data) การโจมตีหรือดัดแปลงระบบ AI ตลอดจนความเสี่ยงจากซอฟต์แวร์ แบบจำลอง AI ผู้ผลิต ผู้ให้บริการ และห่วงโซ่อุปทาน (Supply Chain)

นอกจากนี้ เมื่อผลลัพธ์จาก AI ถูกนำไปเชื่อมต่อกับส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface: API) กระบวนงานอัตโนมัติ (Workflow) ระบบควบคุมการเข้าออก หรือระบบสารสนเทศอื่น ความผิดพลาดหรือการถูกโจมตีอาจส่งผลกระทบต่อเนื่องไปยังบุคคล ทรัพย์สิน ระบบ หรือภารกิจขององค์กรได้ ความเสี่ยงจึงมิได้ขึ้นอยู่กับตัวกล้องหรือความแม่นยำของ AI เพียงอย่างเดียว แต่ขึ้นอยู่กับวัตถุประสงค์ ข้อมูล ลักษณะการใช้ผลลัพธ์ ระดับการเชื่อมต่อ และผลกระทบที่อาจเกิดขึ้นด้วย

ด้วยเหตุนี้ การรักษาความมั่นคงปลอดภัยของระบบ CCTV ที่ใช้ AI จึงควรดำเนินการโดยพิจารณาตามระดับผลกระทบและความเสี่ยง (Impact-Based and Risk-Based Approach) ตลอดวงจรชีวิต ตั้งแต่การกำหนดวัตถุประสงค์ การออกแบบ การจัดซื้อจัดจ้าง การติดตั้งและตรวจรับ การใช้งานและบำรุงรักษา การเปลี่ยนแปลงระบบ ตลอดจนการเลิกใช้งาน

แนวปฏิบัติฉบับนี้จึงจัดทำขึ้นเพื่อใช้เป็นแนวทางเพิ่มเติมจากมาตรการความมั่นคงปลอดภัยของระบบ CCTV โดยทั่วไป โดยมุ่งเน้น **ความเสี่ยงและมาตรการเพิ่มเติมที่เกิดจากการนำ AI มาใช้กับระบบ CCTV** และสามารถประยุกต์ใช้ให้เหมาะสมกับบริบท ระดับผลกระทบ และความเสี่ยงของแต่ละองค์กร

การรักษาความมั่นคงปลอดภัยของระบบ CCTV ที่ใช้ AI ควรเริ่มจากการกำหนดวัตถุประสงค์และบริบทของการใช้งาน ประเมินระดับผลกระทบและความเสี่ยง และกำหนดมาตรการที่ได้สัดส่วนกับความเสี่ยงตลอดวงจรชีวิต โดยครอบคลุมระบบ ข้อมูล AI บุคลากร ผู้ผลิต ผู้ให้บริการ และระบบที่เชื่อมต่อ ทั้งนี้ การนำ AI มาใช้ไม่ควรพิจารณาเพียงความสามารถของเทคโนโลยี แต่ควรคำนึงถึงความมั่นคงปลอดภัย ความน่าเชื่อถือ ความเป็นส่วนตัว การกำกับดูแลโดยมนุษย์ และความสามารถในการตรวจสอบและรับผิดชอบได้

1.2 วัตถุประสงค์ของเอกสาร

แนวปฏิบัติฉบับนี้มีวัตถุประสงค์เพื่อกำหนดแนวทางด้านความมั่นคงปลอดภัย การบริหารความเสี่ยง และการกำกับดูแลระบบ CCTV ที่ใช้ AI ให้สามารถนำไปประยุกต์ใช้ได้อย่างเหมาะสมและได้สัดส่วนกับระดับผลกระทบและความเสี่ยง โดยมีวัตถุประสงค์สำคัญ ดังนี้

1. เพื่อกำหนดแนวทางสำหรับการประเมินความสำคัญ ผลกระทบ และความเสี่ยงของระบบ CCTV ที่ใช้ AI และใช้ผลการประเมินดังกล่าวในการกำหนดระดับมาตรการที่เหมาะสม
2. เพื่อกำหนดมาตรการเพิ่มเติมที่เกี่ยวข้องกับความมั่นคงปลอดภัยของ AI ความเป็นส่วนตัว ข้อมูลชีวมิติ ความน่าเชื่อถือของผลลัพธ์ การกำกับดูแลโดยมนุษย์ (Human Oversight) และการเชื่อมต่อกับระบบอื่น
3. เพื่อสนับสนุนการบริหารความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ ตั้งแต่การออกแบบ การพัฒนา การจัดซื้อจัดจ้าง การติดตั้ง การตรวจรับ การใช้งาน การบำรุงรักษา การเปลี่ยนแปลง และการเลิกใช้งาน
4. เพื่อใช้เป็นแนวทางในการกำหนดข้อกำหนดในการจัดซื้อจัดจ้าง การประเมินผลิตภัณฑ์ ผู้ผลิต ผู้พัฒนา และผู้ให้บริการ ตลอดจนการกำหนดเกณฑ์การทดสอบและตรวจรับที่สามารถตรวจสอบได้
5. เพื่อสนับสนุนการพิจารณาการใช้บริการคลาวด์ (Cloud Service) บริการ AI ภายนอก สถานที่จัดเก็บและประมวลผลข้อมูล อธิปไตยข้อมูล (Data Sovereignty) และการกำหนดที่ตั้งข้อมูล (Data Localization) ตามกฎหมาย ข้อกำหนด ระดับผลกระทบ และความเสี่ยงที่เกี่ยวข้อง

สำหรับมาตรการด้านความมั่นคงปลอดภัยของระบบ CCTV โดยทั่วไปที่มิได้มีลักษณะเฉพาะจากการใช้ AI ให้พิจารณาร่วมกับ **แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดสำหรับประเทศไทย** และข้อกำหนดอื่นที่เกี่ยวข้อง

1.3 ผู้ใช้เอกสารและบทบาท

แนวปฏิบัติฉบับนี้สามารถนำไปใช้โดยหน่วยงานภาครัฐ องค์กร ผู้ประกอบการ และผู้ที่เกี่ยวข้องกับการวางแผน จัดหา พัฒนา ติดตั้ง ใช้งาน บริหาร หรือประเมินระบบ CCTV ที่ใช้ AI โดยบทบาทสำคัญอาจประกอบด้วยดังต่อไปนี้

ผู้เกี่ยวข้อง	บทบาทสำคัญ
เจ้าของระบบหรือองค์กรผู้ใช้งาน (System Owner / Deploying Organization)	กำหนดวัตถุประสงค์และกรณีใช้งาน ประเมินผลกระทบและความเสี่ยง กำหนดระดับมาตรการ อนุมัติการใช้งาน และทบทวนความเหมาะสมของระบบ
ผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการ (Manufacturer / Developer / Service Provider)	ออกแบบ พัฒนา และดูแลผลิตภัณฑ์ ซอฟต์แวร์ หรือบริการที่เกี่ยวข้องกับ AI รวมถึงการปรับปรุง การบริหารช่องโหว่ การสนับสนุน และการบริหารความมั่นคงปลอดภัยตลอดวงจรชีวิต

ผู้เกี่ยวข้อง	บทบาทสำคัญ
ผู้ติดตั้งหรือผู้บูรณาการระบบ (Installer / System Integrator)	นำข้อกำหนดด้านความมั่นคงปลอดภัยและความเสี่ยงไปใช้ในการออกแบบรายละเอียด การติดตั้ง การกำหนดค่า การเชื่อมต่อ การทดสอบ และการส่งมอบระบบ
ผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator / Operator)	ใช้งานและดูแลระบบตามสิทธิและหน้าที่ เฝ้าระวังการทำงานของระบบและ AI ตรวจสอบผลลัพธ์ และดำเนินการหรือรายงานเมื่อพบเหตุผิดปกติ
ผู้รับผิดชอบด้านการจัดซื้อจัดจ้างหรือผู้ประเมิน (Procurement / Assessor)	กำหนดหรือทบทวนข้อกำหนดในการจัดซื้อ ประเมินผลิตภัณฑ์และผู้ให้บริการ ตรวจสอบหลักฐานการสร้างความเชื่อมั่น และสนับสนุนการทดสอบและตรวจรับ

ในกรณีที่มีการใช้บริการจากผู้ให้บริการภายนอกหรือบริการคลาวด์ ควรกำหนดขอบเขตความรับผิดชอบระหว่างองค์กรผู้ใช้งานและผู้ให้บริการให้ชัดเจนตามหลักความรับผิดชอบร่วม (Shared Responsibility) โดยไม่ถือว่าการใช้บริการภายนอกเป็นการโอนความรับผิดชอบด้านความมั่นคงปลอดภัยทั้งหมดไปยังผู้ให้บริการ

1.4 สถานะของเอกสาร

แนวปฏิบัติฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบสำหรับการประยุกต์ใช้มาตรการด้านความมั่นคงปลอดภัย การบริหารความเสี่ยง และการกำกับดูแลระบบ CCTV ที่ใช้ AI มิใช่กฎหมาย กฎระเบียบ หรือมาตรฐานการรับรองผลิตภัณฑ์โดยตัวเอกสารเอง และไม่ใช้ทดแทนกฎหมาย ประกาศ ข้อกำหนดเฉพาะภาคส่วน ข้อกำหนดในการจัดซื้อจัดจ้าง สัญญา หรือข้อกำหนดอื่นที่มีผลใช้บังคับ

เพื่อให้การตีความข้อเสนอแนะในเอกสารมีความชัดเจน ให้ใช้ถ้อยคำดังต่อไปนี้

ถ้อยคำ	ความหมาย
ต้อง	ใช้เมื่อกล่าวถึงข้อกำหนดที่มีผลใช้บังคับตามกฎหมาย กฎระเบียบ ประกาศ สัญญา หรือข้อกำหนดอื่นที่เกี่ยวข้อง
ควร	ใช้สำหรับมาตรการหรือแนวทางที่แนะนำให้ดำเนินการตามมาตรฐาน แนวปฏิบัติที่ได้รับการยอมรับ หรือผลการประเมินความเสี่ยง
อาจ	ใช้สำหรับทางเลือกที่องค์กรสามารถพิจารณานำไปใช้ตามบริบท ความเหมาะสม และระดับความเสี่ยง

มาตรฐานและแนวปฏิบัติที่อ้างถึงในเอกสารนี้ใช้เป็นกรอบสนับสนุนในการกำหนดหลักการและมาตรการ มิได้หมายความว่าระบบ ผลิตภัณฑ์ ผู้ผลิต หรือผู้ให้บริการทุกกรณีต้องได้รับการรับรองตาม

มาตรฐานทั้งหมดที่อ้างถึง เว้นแต่กฎหมาย ข้อกำหนดในการจัดซื้อจัดจ้าง สัญญา หรือข้อกำหนดที่มีผลใช้บังคับกำหนดไว้เป็นอย่างอื่น

ในกรณีที่แนวปฏิบัติฉบับนี้กำหนดวิธีการประยุกต์เพิ่มเติม เช่น การแบ่งระดับมาตรการเป็น **ระดับพื้นฐาน (Baseline) ระดับเพิ่มเติม (Enhanced) และระดับความเชื่อมั่นสูง (High-Assurance)** ให้ถือเป็นวิธีการประยุกต์ใช้ของแนวปฏิบัติฉบับนี้ (Guideline-Applied Method) เพื่อช่วยให้องค์กรสามารถเชื่อมโยงผลการประเมินผลกระทบและความเสี่ยงกับระดับมาตรการที่เหมาะสม มิใช่การจัดระดับที่กำหนดโดยมาตรฐาน ISO/IEC ฉบับใดฉบับหนึ่งโดยตรง

สรุปหลักการของบทที่ 1

ระบบ CCTV ที่ใช้ AI ควรได้รับการกำกับดูแลตามวัตถุประสงค์ ระดับผลกระทบ และความเสี่ยงตลอดวงจรชีวิต โดยมาตรการที่นำมาใช้ควรได้สัดส่วนกับความเสี่ยง สามารถตรวจสอบได้ และไม่ใช้ทดแทนข้อกำหนดทางกฎหมายหรือข้อกำหนดอื่นที่มีผลใช้บังคับ

บทที่ 2 หลักการพื้นฐาน

บทนี้กำหนดหลักการและกรอบอ้างอิงสำหรับการประยุกต์ใช้แนวปฏิบัติด้านความมั่นคงปลอดภัยสำหรับระบบ CCTV ที่ใช้ AI เพื่อให้การประเมินความเสี่ยง การกำหนดมาตรการ การออกแบบ การจัดซื้อจัดจ้าง การตรวจรับ และการดำเนินงานเป็นไปในทิศทางเดียวกัน

แนวปฏิบัตินี้ใช้หลักการตามระดับผลกระทบและความเสี่ยง (Impact-Based and Risk-Based Approach) โดยมิได้กำหนดให้ระบบ CCTV ที่ใช้ AI ทุกระบบต้องใช้มาตรการในระดับเดียวกัน การกำหนดมาตรการควรพิจารณาจากวัตถุประสงค์ ลักษณะข้อมูล ความสามารถของ AI การนำผลลัพธ์ไปใช้ การเชื่อมต่อกับระบบอื่น และผลกระทบที่อาจเกิดขึ้น

2.1 แนวทางการจัดทำแนวปฏิบัติ

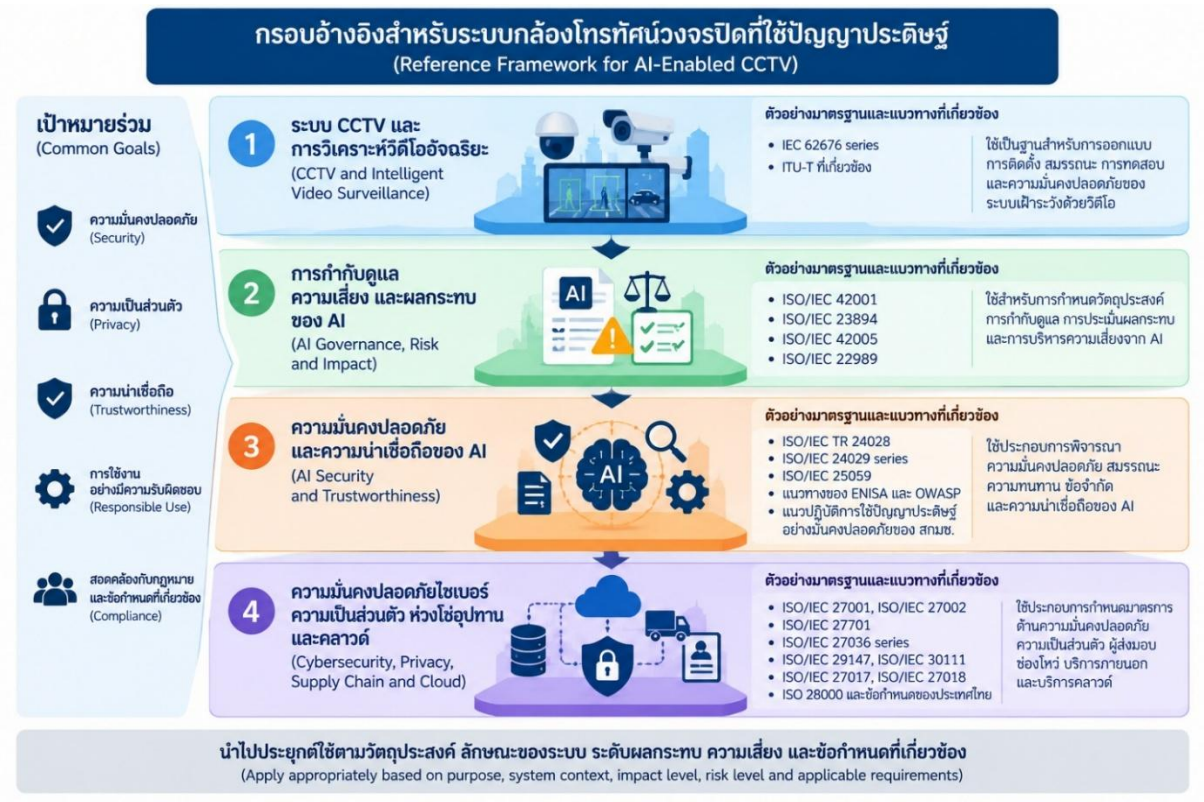
ระบบ CCTV ที่ใช้ AI มีองค์ประกอบเกี่ยวข้องกับหลายด้าน ทั้งระบบเฝ้าระวังด้วยวิดีโอ ปัญญาประดิษฐ์ ข้อมูล เครือข่าย ซอฟต์แวร์ บริการคลาวด์ และห่วงโซ่อุปทาน จึงไม่เหมาะสมที่จะใช้มาตรฐานหรือแนวปฏิบัติฉบับใดฉบับหนึ่งเป็นกรอบอ้างอิงเพียงลำพัง

แนวปฏิบัติฉบับนี้จึงรวบรวมและประยุกต์หลักการจากมาตรฐานและแนวปฏิบัติที่ได้รับการยอมรับ โดยจัดกลุ่มกรอบอ้างอิงเป็น 4 ชั้น เพื่อให้สอดคล้องกับลักษณะของระบบ CCTV ที่ใช้ AI ดังนี้

ชั้น	กรอบอ้างอิง	การนำมาใช้ในแนวปฏิบัตินี้
1. ระบบ CCTV และการวิเคราะห์วิดีโออัจฉริยะ	IEC 62676 series และข้อเสนอแนะ ITU-T ที่เกี่ยวข้อง	ใช้เป็นฐานสำหรับการออกแบบ การติดตั้ง สมรรถนะ การทดสอบ และความมั่นคงปลอดภัยของระบบเฝ้าระวังด้วยวิดีโอ
2. การกำกับดูแลความเสี่ยง และผลกระทบของ AI	ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005 และมาตรฐานที่เกี่ยวข้อง	ใช้สำหรับการกำหนดวัตถุประสงค์ การกำกับดูแล การประเมินผลกระทบ และการบริหารความเสี่ยงจาก AI
3. ความมั่นคงปลอดภัยและความน่าเชื่อถือของ AI	แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Security Guidelines) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), ISO/IEC TR 24028, ISO/IEC	ใช้ประกอบการพิจารณาความมั่นคงปลอดภัย สมรรถนะ ความทนทาน ข้อจำกัด และความน่าเชื่อถือของ AI

ชั้น	กรอบอ้างอิง	การนำมาใช้ในแนวปฏิบัตินี้
	24029 series, ISO/IEC 25059 ตลอดจนแนวทางของ ENISA และ OWASP ตามความเกี่ยวข้อง	
4. ความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัว ห่วงโซ่อุปทาน และคลาวด์	ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 27036 series, **ISO 28000**, **ISO/IEC 29147, ISO/IEC 30111, IEC 62443-4-1**, ISO/IEC 27017, ISO/IEC 27018 และข้อกำหนดของประเทศไทยที่เกี่ยวข้อง	ใช้ประกอบการกำหนดมาตรการด้านความมั่นคงปลอดภัย ความเป็นส่วนตัว ผู้ส่งมอบ ช่องโหว่ บริการภายนอก และบริการคลาวด์

การอ้างอิงมาตรฐานดังกล่าวมิได้หมายความว่าระบบ ผลิตภัณฑ์ ผู้ผลิต หรือผู้ให้บริการทุกกรณีต้องปฏิบัติตามหรือได้รับการรับรองตามมาตรฐานทั้งหมด การเลือกใช้มาตรฐานหรือหลักฐานที่เกี่ยวข้องควรพิจารณาตามวัตถุประสงค์ ลักษณะระบบ ระดับผลกระทบ ความเสี่ยง และข้อกำหนดที่มีผลใช้บังคับ



รูปที่ 1 กรอบอ้างอิงสำหรับระบบ CCTV ที่ใช้ AI

แนวปฏิบัตินี้ใช้มาตรฐานด้านระบบเฝ้าระวังด้วยวิดีโอเป็นฐาน และประยุกต์หลักการด้านการกำกับดูแล ความเสี่ยง ความมั่นคงปลอดภัย และความน่าเชื่อถือของ AI ร่วมกับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัว ห่วงโซ่อุปทาน และบริการคลาวด์ตามความเกี่ยวข้อง

2.2 ขอบเขตของคำแนะนำ

แนวปฏิบัติฉบับนี้ครอบคลุมระบบ CCTV ที่ใช้ AI หรือการวิเคราะห์วิดีโออัจฉริยะ (Intelligent Video Analytics) เพื่อช่วยตรวจจับ จำแนก วิเคราะห์ ติดตาม ระบุ หรือสร้างผลลัพธ์จากข้อมูลภาพหรือวิดีโอ โดยการประมวลผลอาจเกิดขึ้นที่ตัวกล้อง อุปกรณ์ประมวลผลส่วนขอบ (Edge Device) ระบบบริหารจัดการวิดีโอ (Video Management System: VMS) ศูนย์ข้อมูล หรือบริการคลาวด์

ตัวอย่างความสามารถที่อยู่ในขอบเขต เช่น การตรวจจับและจำแนกวัตถุ (Object Detection and Classification) การติดตามวัตถุหรือบุคคล (Tracking) การรู้จำใบหน้า (Facial Recognition) การรู้จำป้ายทะเบียน (License Plate Recognition: LPR) การวิเคราะห์พฤติกรรม (Behavioral Analytics) การวิเคราะห์ความหนาแน่นหรือการเคลื่อนที่ของบุคคล และความสามารถอื่นที่ใช้ AI วิเคราะห์ข้อมูลจากระบบ CCTV

แนวปฏิบัตินี้มุ่งเน้นความเสี่ยงและมาตรการเพิ่มเติมที่เกิดจากการใช้ AI โดยครอบคลุมประเด็นสำคัญได้แก่

1. การกำกับดูแล การประเมินผลกระทบ และการบริหารความเสี่ยงของ AI
2. ความมั่นคงปลอดภัย สมรรถนะ และความน่าเชื่อถือของ AI
3. การกำกับดูแลข้อมูล ความเป็นส่วนตัว และข้อมูลชีวมิติ
4. การกำกับดูแลโดยมนุษย์และความรับผิดชอบ
5. การเปลี่ยนแปลง AI ซอฟต์แวร์ และองค์ประกอบที่เกี่ยวข้อง
6. ความมั่นคงปลอดภัยของผู้ผลิต ผู้ให้บริการ และห่วงโซ่อุปทาน
7. การใช้บริการคลาวด์ บริการ AI ภายนอก และสถานที่จัดเก็บหรือประมวลผลข้อมูล
8. การทดสอบ การตรวจรับ การเฝ้าระวัง การทบทวน และการบริหารตลอดวงจรชีวิต

มาตรการความมั่นคงปลอดภัยทั่วไปของระบบ CCTV ซึ่งมิได้เกิดขึ้นโดยเฉพาะจากการใช้ AI ให้พิจารณาร่วมกับแนวปฏิบัติด้านความมั่นคงปลอดภัยสำหรับระบบ CCTV ของประเทศไทยและข้อกำหนดอื่นที่เกี่ยวข้อง เพื่อหลีกเลี่ยงการกำหนดมาตรการซ้ำซ้อน

2.3 หลักการพื้นฐานที่ใช้ตลอดทั้งเล่ม

การออกแบบ จัดหา ติดตั้ง ใช้งาน และบริหารระบบ CCTV ที่ใช้ AI ควรยึดหลักการพื้นฐานดังต่อไปนี้

2.3.1 วัตถุประสงค์และกรณีใช้งาน

องค์กรควรกำหนดวัตถุประสงค์และกรณีใช้งานของ AI ให้ชัดเจนก่อนการออกแบบหรือเลือกใช้เทคโนโลยี โดยระบุว่า AI ทำหน้าที่ใด ใช้ข้อมูลใด สร้างผลลัพธ์ใด และผลลัพธ์ดังกล่าวจะถูกนำไปใช้โดยบุคคลหรือระบบใด

การมีความสามารถทางเทคนิคของ AI มิได้หมายความว่าความสามารถนั้นจำเป็นหรือเหมาะสมที่จะเปิดใช้งานในทุกกรณี

2.3.2 การพิจารณาตามระดับผลกระทบและความเสี่ยง

มาตรการที่นำมาใช้ควรได้สัดส่วนกับระดับผลกระทบและความเสี่ยง โดยพิจารณาทั้งความสำคัญของระบบหรือภารกิจ (System/Mission Criticality) ผลกระทบด้านข้อมูล (Data Impact) ผลกระทบจากการใช้ AI (AI Impact) และปัจจัยที่อาจขยายผลกระทบ (Impact Amplification Factors)

ระบบที่มีความเสี่ยงแตกต่างกันจึงไม่จำเป็นต้องใช้มาตรการ การทดสอบ หรือหลักฐานการสร้างความเชื่อมั่นในระดับเดียวกัน

รายละเอียดการประเมินและกำหนดระดับมาตรการระบุไว้ในข้อ 3.1

2.3.3 ความมั่นคงปลอดภัยตั้งแต่การออกแบบและค่าตั้งต้นที่มั่นคงปลอดภัย

ความมั่นคงปลอดภัยควรถูกพิจารณาตั้งแต่การกำหนดสถาปัตยกรรม ข้อมูล ความสามารถของ AI สิทธิการเข้าถึง การเชื่อมต่อ และการนำผลลัพธ์ไปใช้ ไม่ควรรอแก้ไขภายหลังการติดตั้ง

เมื่อส่งมอบหรือเปิดใช้งาน ระบบควรเปิดเฉพาะบัญชี บริการ การเชื่อมต่อ และความสามารถของ AI ที่จำเป็นตามวัตถุประสงค์ โดยลดการเปิดใช้ความสามารถที่ไม่จำเป็น

2.3.4 การกำกับดูแลโดยมนุษย์และความรับผิดชอบ

องค์กรควรกำหนดผู้รับผิดชอบต่อการใช้ AI และจัดให้มีการกำกับดูแลโดยมนุษย์ในระดับที่เหมาะสมกับผลกระทบของระบบ ผู้เกี่ยวข้องควรสามารถเข้าใจข้อจำกัดของผลลัพธ์ ตรวจสอบหรือทวนสอบผลลัพธ์ และแทรกแซง จำกัด หรือระงับการดำเนินการเมื่อจำเป็น

การใช้ AI ไม่ควรทำให้ความรับผิดชอบต่อการตัดสินใจหรือผลกระทบที่เกิดขึ้นไม่สามารถระบุได้

2.3.5 สมรรถนะและความน่าเชื่อถือ

องค์กรควรประเมินว่า AI มีสมรรถนะและข้อจำกัดเหมาะสมกับกรณีใช้งานและสภาพแวดล้อมจริง โดยพิจารณาปัจจัยที่อาจมีผลต่อการทำงาน เช่น คุณภาพภาพ แสง มุมกล้อง ระยะทาง การบดบัง สภาพแวดล้อม และการเปลี่ยนแปลงของข้อมูลหรือบริบท

ค่าความเชื่อมั่นของ AI (Confidence Score) หรือค่าความแม่นยำโดยรวมเพียงค่าเดียวไม่ควรถูกใช้เป็นหลักฐานว่าผลลัพธ์ของ AI ถูกต้องในทุกกรณี โดยเฉพาะเมื่อผลลัพธ์ถูกนำไปใช้ในการตัดสินใจที่อาจก่อให้เกิดผลกระทบสูง

2.3.6 การป้องกันหลายชั้นและความมั่นคงปลอดภัยเฉพาะ AI

การรักษาความมั่นคงปลอดภัยควรใช้มาตรการหลายชั้น ครอบคลุมอุปกรณ์ เฟิร์มแวร์ ซอฟต์แวร์ AI ข้อมูล บัญชีและสิทธิ เครือข่าย การเชื่อมต่อ บริการภายนอก และกระบวนการบริหารจัดการ

สำหรับระบบที่ผลลัพธ์ของ AI สามารถนำไปสู่การดำเนินการต่อระบบอื่น ควรมีมาตรการจำกัดขอบเขตของผลกระทบ เพื่อไม่ให้ความผิดพลาดหรือการถูกโจมตีขององค์ประกอบหนึ่งสามารถขยายผลกระทบไปยังระบบอื่นโดยไม่มีการควบคุม

2.3.7 ความโปร่งใสและความมั่นคงปลอดภัยของห่วงโซ่อุปทาน

องค์กรควรพิจารณาความน่าเชื่อถือของผลิตภัณฑ์ ผู้ผลิต ผู้พัฒนา ผู้ติดตั้ง และผู้ให้บริการ รวมถึงความสามารถในการบริหารช่องโหว่ การปรับปรุงด้านความมั่นคงปลอดภัย การเปลี่ยนแปลงผลิตภัณฑ์ และการสนับสนุนตลอดวงจรชีวิต

ความโปร่งใสมิได้หมายถึงการเปิดเผยรายละเอียดทางเทคนิคทั้งหมด แต่ควรมีข้อมูล หลักฐาน หรือการสร้างความเชื่อมั่น (Assurance) ที่เพียงพอสำหรับการประเมินและบริหารความเสี่ยงตามความสำคัญของระบบ

2.3.8 การกำกับดูแลข้อมูลและอธิปไตยข้อมูล

องค์กรควรทราบว่าข้อมูลถูกเก็บ ประมวลผล ส่งต่อ และเข้าถึงจากที่ใด โดยใคร และอยู่ภายใต้เขตอำนาจทางกฎหมายใด โดยเฉพาะเมื่อมีการใช้บริการคลาวด์หรือบริการ AI ภายนอก

การพิจารณาอธิปไตยข้อมูล (Data Sovereignty) อาจครอบคลุมสถานที่จัดเก็บข้อมูล (Data Location) สถานที่ประมวลผล (Processing Location) เขตอำนาจทางกฎหมาย (Jurisdiction) การเข้าถึงจากต่างประเทศ ผู้ให้บริการช่วง (Subprocessor) และการควบคุมกุญแจเข้ารหัสตามความเหมาะสม

การกำหนดให้ข้อมูลจัดเก็บหรือประมวลผลภายในประเทศ (Data Localization) เป็นมาตรการหนึ่งที่อาจนำมาใช้ตามกฎหมาย ข้อกำหนด หรือผลการประเมินความเสี่ยง และไม่ควรถือว่าการจัดเก็บข้อมูลภายในประเทศเพียงอย่างเดียวทำให้ระบบมีความมั่นคงปลอดภัยครบถ้วน

สรุปหลักการของบทที่ 2

การประยุกต์ใช้แนวปฏิบัติควรเริ่มจาก **วัตถุประสงค์และบริบท ⟶ ผลกระทบและความเสี่ยง ⟶ มาตรการควบคุม ⟶ การทดสอบและสร้างความเชื่อมั่น ⟶ การติดตามและทบทวน** โดยพิจารณาร่วมกันทั้งระบบ CCTV AI ข้อมูล บุคลากร ผู้ผลิต ผู้ให้บริการ ห่วงโซ่อุปทาน และระบบที่เชื่อมต่อ

บทที่ 3 การกำกับดูแล ระเบียบ และกฎหมาย

การนำ AI มาใช้กับระบบ CCTV อาจทำให้ลักษณะและระดับความเสี่ยงแตกต่างจากระบบ CCTV ทั่วไป เนื่องจากระบบสามารถวิเคราะห์ข้อมูล สร้างผลลัพธ์ ติดตามหรือระบุบุคคล ตลอดจนส่งผลลัพธ์ไปยังระบบอื่นเพื่อสนับสนุนการตัดสินใจหรือดำเนินการต่อได้

การกำหนดมาตรการจึงควรพิจารณาจาก **วัตถุประสงค์ บริบท ระดับผลกระทบ และความเสี่ยงของระบบ** มิใช่กำหนดจากจำนวนกล้อง ประเภทอุปกรณ์ หรือการมี AI เพียงอย่างเดียว

3.1 การจำแนกระดับความสำคัญของระบบ

การจำแนกระดับความสำคัญของระบบ CCTV ที่ใช้ AI มีวัตถุประสงค์เพื่อให้สามารถกำหนดมาตรการด้านความมั่นคงปลอดภัย การทดสอบ การกำกับดูแล และระดับการสร้างความเชื่อมั่น (Assurance) ที่เหมาะสมและได้สัดส่วนกับความเสี่ยง

การประเมินควรพิจารณาอย่างน้อย 3 มิติ ได้แก่

1. **ความสำคัญของระบบหรือภารกิจ (System/Mission Criticality)**
2. **ผลกระทบด้านข้อมูล (Data Impact)**
3. **ผลกระทบจากการใช้ AI (AI Impact)**

จากนั้นพิจารณาปัจจัยที่อาจทำให้ผลกระทบขยายไปยังบุคคล ระบบ หรือภารกิจอื่น (Impact Amplification Factors) ก่อนกำหนดระดับมาตรการที่เหมาะสม

หลักสำคัญคือ **ความสำคัญของระบบ (System Criticality) ผลกระทบด้านข้อมูล (Data Impact) และผลกระทบจาก AI (AI Impact) เป็นคนละมิติและไม่ควรใช้แทนกัน**

ตัวอย่างเช่น ระบบอาจไม่ใช่ระบบภารกิจสำคัญ แต่มีการประมวลผลข้อมูลชีวมิติที่มีผลกระทบสูง หรือระบบอาจไม่มีข้อมูลชีวมิติ แต่ผลลัพธ์จาก AI ถูกใช้ควบคุมการเข้าออกพื้นที่สำคัญ จึงอาจมีผลกระทบจาก AI หรือผลกระทบต่อภารกิจในระดับสูงได้

รูปที่ 2 กรอบการประเมินผลกระทบและกำหนดระดับมาตรการสำหรับระบบ CCTV ที่ใช้ AI

3.1.1 วัตถุประสงค์ กรณีใช้งาน และบริบท

ก่อนจำแนกระดับผลกระทบ องค์กรควรกำหนดวัตถุประสงค์และกรณีใช้งาน (Use Case) ของระบบให้ชัดเจน เพื่อให้ทราบว่า AI ถูกนำมาใช้เพื่ออะไร ใช้ข้อมูลใด สร้างผลลัพธ์ใด และผลลัพธ์ถูกนำไปใช้อย่างไร ควรพิจารณาอย่างน้อยประเด็นต่อไปนี้

ประเด็น	ตัวอย่างคำถามที่ควรพิจารณา
วัตถุประสงค์	ใช้ AI เพื่ออะไร และมีความจำเป็นอย่างไร
พื้นที่และบริบท	ใช้ในพื้นที่ทั่วไป พื้นที่จำกัด พื้นที่สาธารณะ หรือพื้นที่สำคัญ
บุคคลที่เกี่ยวข้อง	บุคคลใดอาจถูกบันทึก วิเคราะห์ ติดตาม หรือได้รับผลกระทบ
ข้อมูล	มีการใช้ข้อมูลภาพ วิดีโอ ข้อมูลประกอบ (Metadata) ข้อมูลชีวมิติ หรือข้อมูลจากแหล่งอื่นหรือไม่
ความสามารถของ AI	AI ตรวจจับ จำแนก ติดตาม ระบุ หรือวิเคราะห์อะไร
การใช้ผลลัพธ์	ผลลัพธ์ใช้เพื่อแจ้งเตือน สนับสนุนการตัดสินใจ หรือดำเนินการต่อโดยอัตโนมัติ

ประเด็น	ตัวอย่างคำถามที่ควรพิจารณา
การเชื่อมต่อ	มีการส่งผลลัพธ์ไปยังระบบ บุคคล หรือบริการภายนอกใด
ผลกระทบ	หาก AI ผิดพลาด ถูกโจมตี หรือไม่พร้อมใช้งาน จะเกิดผลกระทบอย่างไร

การประเมินโดยไม่มีการกำหนดวัตถุประสงค์และกรณีใช้งานที่ชัดเจนอาจทำให้กำหนดระดับความเสี่ยงและมาตรการไม่เหมาะสมกับการใช้งานจริง

3.1.2 ความสำคัญของระบบหรือภารกิจ

องค์กรควรพิจารณาว่าระบบ CCTV ที่ใช้ AI มีความสำคัญต่อภารกิจ การรักษาความปลอดภัย หรือการดำเนินงานขององค์กรในระดับใด โดยพิจารณาผลกระทบกรณีระบบไม่สามารถให้บริการ ให้ผลลัพธ์ไม่ถูกต้อง หรือถูกควบคุมโดยไม่ได้รับอนุญาต

ตัวอย่างปัจจัยที่ควรพิจารณา ได้แก่

- ผลกระทบต่อความปลอดภัยของบุคคล
- ผลกระทบต่อทรัพย์สินหรือสถานที่สำคัญ
- ผลกระทบต่อการดำเนินงานหรือบริการสำคัญ
- ผลกระทบต่อระบบหรือโครงสร้างพื้นฐานที่เชื่อมต่อ
- ผลกระทบต่อความต่อเนื่องของภารกิจ
- ผลกระทบต่อความมั่นคงปลอดภัยขององค์กรหรือสาธารณะ

การพิจารณาความสำคัญของระบบตามแนวปฏิบัตินี้ใช้สำหรับการบริหารความเสี่ยงของ CCTV ที่มีการใช้ AI (เพื่อความกระชับ ในเอกสารนี้คำนี้จะถูกอ้างถึงว่า “CCTV-AI”) และ **ไม่ควรตีความโดยอัตโนมัติว่าเป็นการจำแนกหน่วยงานหรือระบบเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)** ตามกฎหมาย

3.1.3 ผลกระทบด้านข้อมูล

องค์กรควรประเมินผลกระทบที่อาจเกิดขึ้นจากการเก็บ ใช้ ประมวลผล เปิดเผย เปลี่ยนแปลง สูญหาย หรือไม่สามารถเข้าถึงข้อมูลที่เกี่ยวข้องกับระบบ CCTV-AI

การประเมินควรพิจารณามิติด้าน **การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability)** ร่วมกับบริบทของข้อมูล

ปัจจัยที่ควรพิจารณาอาจประกอบด้วย

1. ประเภทและความอ่อนไหวของข้อมูล
2. ความสามารถในการระบุบุคคล
3. การมีข้อมูลชีวมิติ (Biometric Data)

4. ปริมาณข้อมูลและระยะเวลาการจัดเก็บ (Data Volume and Retention)
5. การเชื่อมโยงข้อมูลจากหลายแหล่ง (Data Correlation)
6. ข้อมูลที่ AI สร้างหรืออนุมานขึ้น (Derived or Inferred Data)
7. จำนวนและลักษณะของบุคคลที่อาจได้รับผลกระทบ
8. ผลกระทบต่อภารกิจหรือบริการสำคัญหากข้อมูลถูกเปิดเผย เปลี่ยนแปลง สูญหาย หรือไม่พร้อมใช้งาน

การประเมินไม่ควรพิจารณาข้อมูลแต่ละรายการแยกจากกันเพียงอย่างเดียว เนื่องจากข้อมูลที่มีผลกระทบไม่สูงเมื่อพิจารณาแยกกัน อาจมีผลกระทบเพิ่มขึ้นเมื่อถูกสะสม เชื่อมโยง หรือวิเคราะห์ร่วมกัน

3.1.4 ผลกระทบจากการใช้ AI

ผลกระทบจาก AI ควรพิจารณาจากลักษณะของความสามารถ AI ความน่าเชื่อถือของผลลัพธ์ และผลที่อาจเกิดขึ้นเมื่อผลลัพธ์ดังกล่าวถูกนำไปใช้

ตัวอย่างประเด็นที่ควรพิจารณา ได้แก่

- AI ทำหน้าที่ตรวจจับ จำแนก ติดตาม ระบุ หรืออนุมานข้อมูลใด
- ความผิดพลาดของ AI อาจส่งผลต่อบุคคลหรือภารกิจอย่างไร
- ผลลัพธ์สามารถถูกตรวจสอบหรือแก้ไขย้อนหลังได้หรือไม่
- มีบุคคลตรวจสอบก่อนนำผลลัพธ์ไปใช้หรือไม่
- ผลลัพธ์ถูกนำไปใช้กับบุคคลจำนวนมากหรือในวงกว้างหรือไม่
- ผลกระทบที่เกิดขึ้นสามารถย้อนกลับหรือแก้ไขได้เพียงใด
- ผลลัพธ์ของ AI ถูกใช้เป็นข้อมูลประกอบ หรือเป็นตัวกระตุ้นให้เกิดการดำเนินการโดยตรง

ระดับอำนาจของผลลัพธ์ AI สามารถพิจารณาเป็นลำดับได้ เช่น

ให้ข้อมูล (Inform)

⟶ แจ้งเตือน (Alert)

⟶ เสนอแนะ (Recommend)

⟶ สนับสนุนการตัดสินใจ (Decision Support)

⟶ กระตุ้นการดำเนินการ (Trigger)

⟶ ดำเนินการโดยอัตโนมัติ (Automated Action)

โดยทั่วไป เมื่อ AI มีอำนาจต่อการดำเนินการมากขึ้น ควรพิจารณาเพิ่มระดับการทดสอบ การควบคุมสิทธิ การกำกับดูแลโดยมนุษย์ การบันทึกหลักฐาน และมาตรการจำกัดผลกระทบตามระดับความเสี่ยง

3.1.5 ปัจจัยที่อาจขยายผลกระทบ

ความเสี่ยงของระบบ CCTV ที่ใช้ AI อาจเพิ่มขึ้นอย่างมีนัยสำคัญเมื่อผลลัพธ์จาก AI ถูกนำไปใช้ในการตัดสินใจ ถูกส่งต่อไปยังระบบอื่น หรือสามารถก่อให้เกิดการดำเนินการต่อเนื่องโดยบุคคลหรือระบบอัตโนมัติ ตัวอย่างลำดับการขยายผลกระทบ เช่น **ข้อมูลหรือภาพถูกดัดแปลง ⟶ AI วิเคราะห์ผิดพลาด ⟶ ระบบเชื่อถือผลลัพธ์ ⟶ ส่งผลลัพธ์เข้าสู่กระบวนงานอัตโนมัติ (Workflow) หรือส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) ⟶ ระบบที่เชื่อมต่อดำเนินการตามผลลัพธ์ ⟶ ผลกระทบขยายออกจากระบบ CCTV**

องค์กรจึงควรพิจารณาปัจจัยที่อาจขยายผลกระทบตามความเกี่ยวข้อง เช่น

- การเชื่อมต่อผ่านส่วนเชื่อมต่อโปรแกรมประยุกต์ (API)
- กระบวนงานอัตโนมัติ (Workflow)
- ระบบควบคุมการเข้าออก (Access Control System)
- ระบบแจ้งเตือนหรือระบบสั่งการ
- ระบบบริหารอาคารหรือระบบทางกายภาพ
- ระบบหรือบริการ AI อื่น
- จำนวนบุคคล ระบบ หรือพื้นที่ที่อาจได้รับผลกระทบ
- ความเร็วที่ผลกระทบสามารถเกิดหรือแพร่กระจาย
- ความสามารถในการย้อนกลับ แก้ไข หรือระงับผลกระทบ
- ระดับการกำกับดูแลโดยมนุษย์ก่อนเกิดการดำเนินการ

ในกรณีที่มีการใช้ตัวแทน AI (AI Agent) หรือระบบที่สามารถดำเนินการหลายขั้นตอน ควรพิจารณาเพิ่มเติมถึง **สิทธิที่ได้รับ (Permission) ขอบเขตการดำเนินการ (Action Boundary) ระดับความเป็นอัตโนมัติ (Autonomy) เครื่องมือหรือระบบที่สามารถเรียกใช้ และผลกระทบที่อาจเกิดขึ้นจากการดำเนินการดังกล่าว**

หลักการนี้มิได้จำกัดเฉพาะตัวแทน AI เนื่องจาก **กลไกประมวลผลกฎ (Rule Engine) กระบวนงานอัตโนมัติ (Workflow) ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API)** หรือระบบอัตโนมัติประเภทอื่น ก็สามารถทำให้ผลกระทบจากผลลัพธ์ของ AI ขยายไปยังบุคคล ระบบ หรือภารกิจอื่นได้เช่นเดียวกัน

3.1.6 หลักการจำกัดผลกระทบ

เมื่อผลลัพธ์จาก AI สามารถก่อให้เกิดหรือขยายผลกระทบ องค์กรควรพิจารณามาตรการจำกัดผลกระทบตามความเหมาะสม เช่น

หลักการ	แนวทาง
ตรวจสอบก่อนดำเนินการ (Validate Before Action)	ตรวจสอบความน่าเชื่อถือของข้อมูลหรือผลลัพธ์ก่อนนำไปใช้ในกิจกรรมที่มีผลกระทบสูง
สิทธิเท่าที่จำเป็น (Least Privilege)	จำกัดสิทธิของบัญชี ระบบ หรือบริการ AI ให้เท่าที่จำเป็น
แยกการวิเคราะห์ออกจากการดำเนินการ	ไม่ให้ผลลัพธ์จาก AI มีอำนาจดำเนินการโดยตรงโดยไม่จำเป็น
ขอบเขตการดำเนินการ (Action Boundary)	กำหนดว่าระบบสามารถดำเนินการใดได้และไม่ได้
การกำกับดูแลโดยมนุษย์ (Human Oversight)	จัดให้บุคคลสามารถตรวจสอบ อนุมัติ แทรกแซง หรือหยุดการดำเนินการตามระดับความเสี่ยง
การจำกัดและแยกผลกระทบ (Containment)	ป้องกันไม่ให้ความผิดพลาดหรือการถูกโจมตีแพร่กระจายเกินขอบเขตที่กำหนด
การเฝ้าระวังและตรวจสอบย้อนหลัง	บันทึกเหตุการณ์ ผลลัพธ์ และการดำเนินการที่สำคัญ
สภาวะปลอดภัย (Fail-Safe)	กำหนดพฤติกรรมที่ปลอดภัยเมื่อ AI ไม่พร้อมใช้งานหรือไม่สามารถเชื่อถือผลลัพธ์ได้

มาตรการดังกล่าวควรเข้มงวดขึ้นตามระดับผลกระทบและอำนาจของ AI ต่อการดำเนินการ

3.1.7 การกำหนดระดับมาตรการ

เพื่อให้ผลการประเมินสามารถนำไปใช้ได้จริง แนวปฏิบัติฉบับนี้กำหนดระดับมาตรการและการสร้างความเชื่อมั่นเป็น 3 ระดับ ดังนี้

ระดับ	ลักษณะการนำไปใช้
B – ระดับพื้นฐาน (Baseline)	ใช้เป็นมาตรการพื้นฐานสำหรับระบบ CCTV ที่ใช้ AI โดยทั่วไป
E – ระดับเพิ่มเติม (Enhanced)	ใช้มาตรการระดับ B ร่วมกับมาตรการเพิ่มเติมเมื่อข้อมูล AI การเชื่อมต่อหรือผลกระทบของระบบทำให้ความเสี่ยงเพิ่มขึ้น
H – ระดับความเชื่อมั่นสูง (High-Assurance)	ใช้มาตรการระดับ B และ E ร่วมกับมาตรการระดับ H สำหรับระบบที่มีผลกระทบหรือความสำคัญสูง หรือกรณีที่ความผิดพลาดหรือการถูกโจมตีอาจก่อให้เกิดผลกระทบรุนแรง

ระดับดังกล่าวเป็นแบบสะสม กล่าวคือ **B ⟶ B + E ⟶ B + E + H**

การกำหนดระดับควรพิจารณาผลจาก **ความสำคัญของระบบหรือภารกิจ (System/Mission Criticality) + ผลกระทบด้านข้อมูล (Data Impact)+ ผลกระทบจาก AI (AI Impact) + ปัจจัยขยายผลกระทบ (Impact Amplification Factors)**

ไม่ควรกำหนดระดับจากปัจจัยเดียว เช่น การใช้ Facial Recognition การใช้ Cloud หรือจำนวนกล้อง โดยไม่พิจารณาบริบทและผลกระทบโดยรวม

ในกรณีที่มิติใดมิติหนึ่งมีผลกระทบสูงอย่างมีนัยสำคัญ องค์กรควรพิจารณาใช้มาตรการในระดับที่สอดคล้องกับผลกระทบดังกล่าว เว้นแต่มีเหตุผลจากการประเมินความเสี่ยงที่สามารถแสดงและตรวจสอบได้

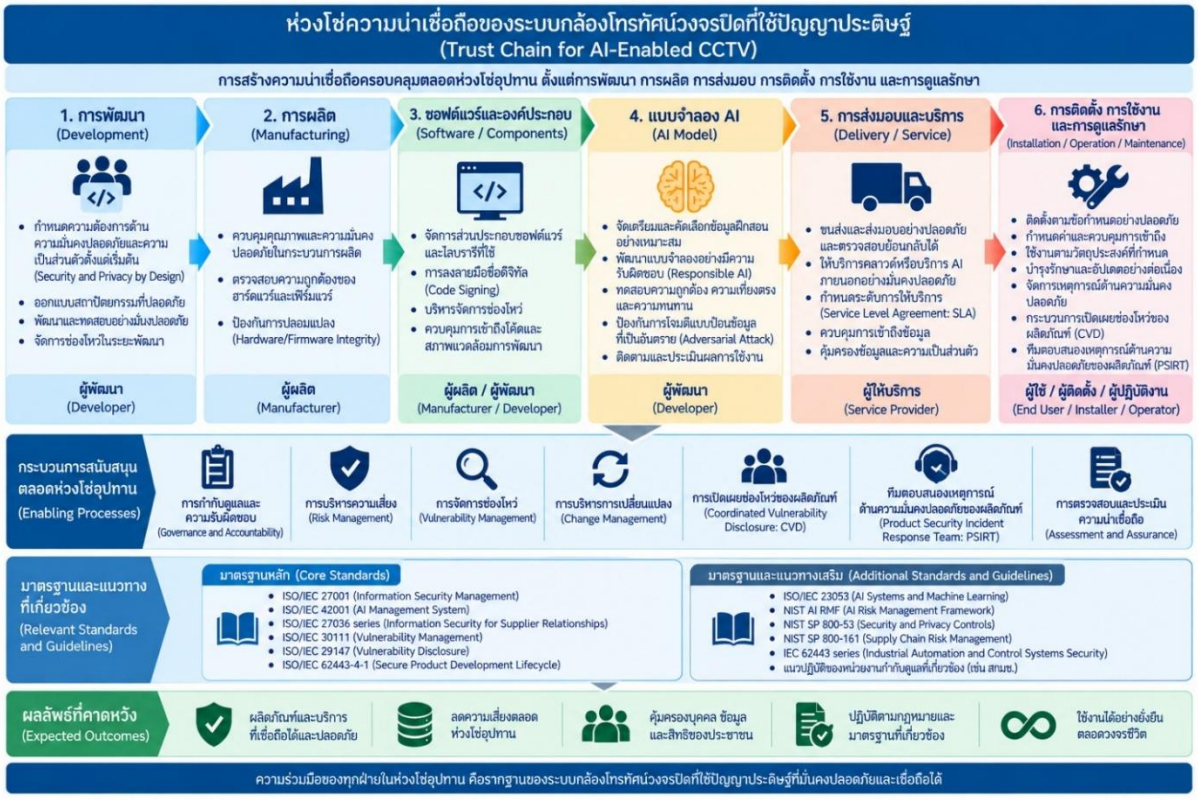
ทั้งนี้ ข้อกำหนดตามกฎหมาย กฎระเบียบ ประกาศ ข้อกำหนดเฉพาะภาคส่วน TOR หรือสัญญาที่มีผลใช้บังคับ **ไม่สามารถลดระดับหรือยกเว้นได้ด้วยการกำหนด B, E หรือ H**

3.1.8 การทบทวนและประเมินใหม่

ผลการประเมินไม่ควรถูกถือว่าใช้ได้ตลอดอายุของระบบโดยไม่มีการทบทวน องค์กรควรประเมินใหม่เมื่อมีการเปลี่ยนแปลงที่อาจมีผลต่อระดับผลกระทบหรือความเสี่ยง เช่น

- เปลี่ยนวัตถุประสงค์หรือกรณีใช้งาน
- เพิ่มหรือเปลี่ยนความสามารถของ AI
- เปลี่ยนประเภทหรือขอบเขตข้อมูล
- เพิ่มการติดตาม การระบุบุคคล หรือการเชื่อมโยงข้อมูล
- เปลี่ยนแบบจำลอง AI หรือบริการที่มีผลต่อการทำงานอย่างมีนัยสำคัญ
- เชื่อมต่อกับระบบใหม่
- เพิ่มการดำเนินการอัตโนมัติ
- เปลี่ยนผู้ให้บริการหรือสถานที่ประมวลผลข้อมูล
- พบช่องโหว่ เหตุการณ์ หรือข้อจำกัดที่มีนัยสำคัญ
- พบว่าสมรรถนะหรือความผิดพลาดของ AI เปลี่ยนไปจากที่ประเมินไว้

การเปลี่ยนแปลงทุกกรณีไม่จำเป็นต้องนำไปสู่การเพิ่มระดับมาตรการ หากองค์กรสามารถแสดงได้ว่าการเปลี่ยนแปลงดังกล่าวไม่ทำให้ระดับผลกระทบหรือความเสี่ยงเพิ่มขึ้นอย่างมีนัยสำคัญ



รูปที่ 3 ตัวอย่างการประเมินผลกระทบและกำหนดระดับมาตรการสำหรับระบบ CCTV ที่ใช้ AI

การกำหนดระดับมาตรการควรพิจารณาร่วมกันจากความสำคัญของระบบหรือภารกิจ ผลกระทบด้านข้อมูล ผลกระทบจาก AI และปัจจัยที่อาจขยายผลกระทบ เพื่อให้มาตรการที่นำมาใช้เหมาะสมและได้สัดส่วนกับความเสี่ยง

3.2 กรอบแนวทาง มาตรฐานอ้างอิง และกฎหมายที่เกี่ยวข้อง

การออกแบบ จัดหา ติดตั้ง ใช้งาน และบริหารระบบ CCTV ที่ใช้ AI อาจเกี่ยวข้องกับกฎหมาย กฎระเบียบ ประกาศ ข้อกำหนดเฉพาะภาคส่วน มาตรฐาน และแนวปฏิบัติหลายด้าน องค์กรจึงควรพิจารณาความเกี่ยวข้องและสถานะของข้อกำหนดแต่ละประเภทให้ชัดเจนก่อนนำไปประยุกต์ใช้

เพื่อป้องกันการตีความว่ามาตรฐานหรือแนวปฏิบัติทุกฉบับเป็นข้อบังคับ แนวปฏิบัตินี้แบ่งกรอบที่เกี่ยวข้องออกเป็น 3 ประเภท ดังนี้

ประเภท	สถานะ	แนวทางการใช้
ข้อกำหนดที่มีผลใช้บังคับ (Applicable Requirements)	กฎหมาย กฎระเบียบ ประกาศ ข้อกำหนดเฉพาะภาคส่วน TOR หรือสัญญาที่ใช้บังคับกับองค์กรหรือระบบนั้น	**ต้อง** ปฏิบัติตามเมื่ออยู่ในขอบเขตที่ใช้บังคับ
มาตรฐานและแนวปฏิบัติ (Standards and Good Practices)	มาตรฐานหรือแนวปฏิบัติที่ได้รับการยอมรับในระดับประเทศหรือสากล	**ควร** นำมาประยุกต์ตามวัตถุประสงค์ บริบท และความเสี่ยง
วิธีการประยุกต์ของแนวปฏิบัติฉบับนี้ (Guideline-Applied Method)	วิธีการที่แนวปฏิบัตินี้พัฒนาขึ้นเพื่อเชื่อมโยงหลักการจากแหล่งอ้างอิงต่าง ๆ กับ CCTV-AI	ใช้เพื่อสนับสนุนการนำแนวปฏิบัติไปปฏิบัติ เช่น การกำหนดระดับ B/E/H

3.2.1 กฎหมายและข้อกำหนดของประเทศไทย

องค์กรควรพิจารณากฎหมาย กฎระเบียบ ประกาศ และข้อกำหนดที่เกี่ยวข้องกับลักษณะขององค์กร ระบบ ข้อมูล และกรณีใช้งาน โดยอาจรวมถึงกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และข้อกำหนดเฉพาะภาคส่วนที่เกี่ยวข้อง

สำหรับระบบ CCTV ที่ใช้ AI การพิจารณาความเกี่ยวข้องของข้อกำหนดไม่ควรพิจารณาจากการมี AI เพียงอย่างเดียว แต่ควรพิจารณาจากกิจกรรมที่เกิดขึ้นจริง เช่น การเก็บและใช้ข้อมูลส่วนบุคคล การประมวลผลข้อมูลชีวมิติ การเชื่อมต่อกับระบบสำคัญ การใช้บริการคลาวด์ หรือการดำเนินงานในภาคส่วนที่มีกฎเกณฑ์เฉพาะ

การจำแนกความสำคัญของระบบตามข้อ 3.1 เป็นวิธีการบริหารความเสี่ยงของแนวปฏิบัติฉบับนี้ และไม่ใช้แทนหลักเกณฑ์ทางกฎหมายในการพิจารณาว่าหน่วยงานหรือระบบใดเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)

3.2.2 บริการคลาวด์และบริการ AI ภายนอก

กรณีระบบ CCTV-AI ใช้บริการคลาวด์หรือบริการ AI ภายนอก องค์กรควรพิจารณาข้อกำหนดที่ใช้บังคับกับองค์กรและบริการนั้น รวมถึงความรับผิดชอบระหว่างองค์กรผู้ใช้บริการและผู้ให้บริการ

การประเมินควรพิจารณาอย่างน้อย

สถานที่จัดเก็บข้อมูล (Data Location) ⟶ สถานที่ประมวลผล (Processing Location) ⟶ การเข้าถึงเพื่อการบริหารระบบ (Administrative Access) ⟶ ผู้ให้บริการช่วง (Subprocessor) ⟶ เขตอำนาจทางกฎหมาย (Jurisdiction) ⟶ การเข้ารหัสและการควบคุมกุญแจ (Encryption and Key Control) ⟶ การสำรองและกู้คืน ⟶ การจัดการเหตุการณ์ ⟶ การยุติหรือเปลี่ยนบริการ (Exit)

สำหรับหน่วยงาน ผู้ใช้บริการคลาวด์ และบริการที่อยู่ภายใต้ขอบเขตการใช้บังคับของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ต้องดำเนินการตามข้อกำหนดที่เกี่ยวข้องตามขอบเขตและระดับผลกระทบที่กำหนดไว้ในประกาศดังกล่าว

การกำหนดสถานที่จัดเก็บหรือประมวลผลข้อมูลภายในประเทศ (Data Localization) ควรพิจารณาตามข้อกำหนดที่มีผลใช้บังคับและผลการประเมินความเสี่ยง และไม่ควรถือเป็นมาตรการที่ทำให้ระบบมีความมั่นคงปลอดภัยครบถ้วนโดยลำพัง

รายละเอียดแนวทางสำหรับ Cloud และบริการภายนอกระบุเพิ่มเติมในข้อ 6.1

3.2.3 มาตรฐานด้านระบบเฝ้าระวังด้วยวิดีโอ

การออกแบบ การติดตั้ง การทดสอบ การตรวจรับ และการประเมินสมรรถนะของระบบ CCTV และการวิเคราะห์วิดีโออัจฉริยะ ควรพิจารณามาตรฐาน **IEC 62676 series** ตามความเกี่ยวข้องกับระบบและกรณีใช้งาน

ข้อเสนอแนะของ **ITU-T** ที่เกี่ยวข้องกับระบบเฝ้าระวังด้วยวิดีโออัจฉริยะ สถาปัตยกรรม ความมั่นคงปลอดภัย กล้องอัจฉริยะ และระบบสำหรับพัฒนาหรือใช้งานอัลกอริทึม อาจนำมาใช้เป็นกรอบอ้างอิงเพิ่มเติมตามลักษณะของระบบ

มาตรฐานเหล่านี้มีความสำคัญต่อแนวปฏิบัติฉบับนี้ เนื่องจากการประเมิน CCTV-AI ไม่ควรพิจารณาเฉพาะ AI โดยแยกออกจากคุณภาพของระบบภาพ สภาพแวดล้อม การติดตั้ง และสถาปัตยกรรมของระบบ CCTV

3.2.4 การกำกับดูแล การบริหารความเสี่ยง และการประเมินผลกระทบของ AI

แนวปฏิบัตินี้ประยุกต์หลักการจากมาตรฐานที่เกี่ยวข้อง ได้แก่

- **ISO/IEC 42001** สำหรับระบบการจัดการปัญญาประดิษฐ์ (AI Management System)
- **ISO/IEC 23894** สำหรับการบริหารความเสี่ยงของ AI (AI Risk Management)
- **ISO/IEC 42005** สำหรับการประเมินผลกระทบของระบบ AI (AI System Impact Assessment)

มาตรฐานดังกล่าวใช้สนับสนุนหลักการเรื่องการกำหนดวัตถุประสงค์ บริบท ความรับผิดชอบ การประเมินผลกระทบ การบริหารความเสี่ยง การติดตาม และการทบทวนตลอดวงจรชีวิต

อย่างไรก็ตาม การแบ่งระดับ **B – Baseline, E – Enhanced และ H – High-Assurance** ตามข้อ 3.1 เป็นวิธีการประยุกต์ของแนวปฏิบัติฉบับนี้ มิใช่ระดับที่กำหนดโดยมาตรฐานดังกล่าวโดยตรง

3.2.5 ความมั่นคงปลอดภัยและความน่าเชื่อถือของ AI

การพิจารณาความมั่นคงปลอดภัยและความน่าเชื่อถือของ AI ควรครอบคลุมทั้งการโจมตีที่มุ่งต่อ AI ความทนทานของระบบ ข้อจำกัดของแบบจำลอง คุณภาพและความเหมาะสมของผลลัพธ์ ตลอดจนผลกระทบเมื่อผลลัพธ์ถูกนำไปใช้

มาตรฐานและแนวทาง เช่น **ISO/IEC TR 24028, ISO/IEC 24029 series, ISO/IEC 25059** ตลอดจนแนวทางของ **ENISA** และ **OWASP** อาจนำมาประยุกต์ตามลักษณะและความเสี่ยงของระบบ ไม่จำเป็นต้องนำมาตรฐานทุกฉบับมาใช้กับทุกระบบ การเลือกใช้ควรสอดคล้องกับความสามารถของ AI กรณีใช้งาน และระดับผลกระทบที่ประเมินตามข้อ 3.1

สำหรับบริบทของประเทศไทย สามารถพิจารณา **แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Security Guidelines) ของ สกมช.** เป็นกรอบอ้างอิงด้านภัยคุกคาม มาตรการด้านความมั่นคงปลอดภัย และการบริหารระบบ AI ตลอดวงจรชีวิต และนำมาประยุกต์เพิ่มเติมให้เหมาะสมกับลักษณะเฉพาะของระบบ CCTV ที่ใช้ AI

3.2.6 ความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัว และห่วงโซ่อุปทาน

มาตรฐานในกลุ่ม ISO/IEC 27000 สามารถนำมาใช้สนับสนุนมาตรการพื้นฐานที่เกี่ยวข้องกับ CCTV-AI เช่น

- **ISO/IEC 27001 และ ISO/IEC 27002** สำหรับการบริหารและควบคุมความมั่นคงปลอดภัยสารสนเทศ
- **ISO/IEC 27701** สำหรับการบริหารข้อมูลส่วนบุคคลและความเป็นส่วนตัว
- **ISO/IEC 27036 series** สำหรับความสัมพันธ์กับผู้ส่งมอบและความมั่นคงปลอดภัยของห่วงโซ่อุปทาน
- **ISO/IEC 29147 และ ISO/IEC 30111** สำหรับการเปิดเผยและการจัดการช่องโหว่
- **ISO/IEC 27017 และ ISO/IEC 27018** สำหรับมาตรการด้านบริการคลาวด์ตามความเกี่ยวข้อง

แนวปฏิบัตินี้มิได้กำหนดให้องค์กรต้องได้รับรายละเอียดภายในของผลิตภัณฑ์ทั้งหมด แต่ควรมีข้อมูลหลักฐาน หรือการสร้างความเชื่อมั่น (Assurance) ที่เพียงพอสำหรับการประเมินและบริหารความเสี่ยงตามความสำคัญของระบบ

3.2.7 มาตรฐานด้านข้อมูลชีวมิติ

กรณีระบบ CCTV-AI มีการประมวลผลข้อมูลชีวมิติหรือใช้ความสามารถในการระบุหรือยืนยันบุคคล อาจพิจารณามาตรฐานที่เกี่ยวข้อง เช่น

- **ISO/IEC 24745** สำหรับการคุ้มครองข้อมูลชีวมิติ
- **ISO/IEC 19795-1** สำหรับการทดสอบและรายงานสมรรถนะของระบบชีวมิติ
- **ISO/IEC 30107 series** สำหรับการตรวจจับการโจมตีด้วยการนำเสนอลักษณะชีวมิติ (Presentation Attack Detection)

การใช้มาตรฐานทางเทคนิคดังกล่าวไม่ใช้แทนการพิจารณาความชอบด้วยกฎหมาย ความจำเป็น ความได้สัดส่วน วัตถุประสงค์ และผลกระทบต่อบุคคล

รายละเอียดเกี่ยวกับข้อมูลชีวมิติระบุเพิ่มเติมในข้อ 3.3 และ 6.2

3.2.8 ระบบที่เชื่อมต่อและการดำเนินการอัตโนมัติ

กรณีผลลัพธ์จาก CCTV-AI ถูกส่งไปยังระบบอื่น เช่น ระบบควบคุมการเข้าออก ระบบแจ้งเตือน ระบบบริหารอาคาร กระบวนงานอัตโนมัติ หรือระบบ AI อื่น การประเมินควรครอบคลุมผลกระทบที่อาจเกิดขึ้นกับระบบปลายทางด้วย

การกำหนดมาตรการไม่ควรพิจารณาเฉพาะความถูกต้องของ AI แต่ควรพิจารณา **สิทธิในการดำเนินการ ขอบเขตการดำเนินการ (Action Boundary) การกำกับดูแลโดยมนุษย์ การบันทึกเหตุการณ์ และความสามารถในการจำกัดหรือหยุดผลกระทบ**

หลักการนี้ใช้กับระบบอัตโนมัติโดยทั่วไป ไม่จำกัดเฉพาะระบบ AI Agent

3.2.9 กรอบกฎหมายและนโยบายต่างประเทศ

กฎหมายหรือกรอบกำกับดูแลของต่างประเทศอาจนำมาใช้เป็นแหล่งอ้างอิงเพื่อศึกษาหลักการและแนวโน้มในการกำกับดูแล AI โดยเฉพาะกรณีที่เกี่ยวข้องกับการระบุบุคคลจากระยะไกล ข้อมูลชีวมิติ ระบบ AI ที่มีผลกระทบสูง ความโปร่งใส และการประเมินผลกระทบต่อบุคคล

ตัวอย่างที่เกี่ยวข้อง ได้แก่ **กฎหมายปัญญาประดิษฐ์ของสหภาพยุโรป (EU Artificial Intelligence Act: EU AI Act)**

การอ้างถึง EU AI Act ในแนวปฏิบัติฉบับนี้มีวัตถุประสงค์เพื่อใช้เป็น **กรอบอ้างอิงด้านกฎระเบียบต่างประเทศ (International Regulatory Reference)** มิได้หมายความว่าข้อกำหนดดังกล่าวเป็นกฎหมายที่ใช้บังคับในประเทศไทยโดยอัตโนมัติ

กรณีองค์กรหรือกิจกรรมอยู่ภายใต้ขอบเขตการใช้บังคับของกฎหมายต่างประเทศนั้น ให้พิจารณาหน้าที่ตามกฎหมายดังกล่าวแยกต่างหาก

3.2.10 การพิจารณาความเกี่ยวข้องของข้อกำหนดและมาตรฐาน

องค์กรไม่จำเป็นต้องนำกฎหมาย มาตรฐาน หรือแนวปฏิบัติทุกฉบับที่กล่าวถึงในเอกสารนี้มาใช้กับทุกระบบ แต่ควรกำหนดความเกี่ยวข้องโดยพิจารณาจาก

องค์กรและภาคส่วน ⟶ วัตถุประสงค์ ⟶ ข้อมูล ⟶ ความสามารถของ AI ⟶ ระบบที่เชื่อมต่อ ⟶ บริการคลาวด์และบุคคลที่สาม (Cloud/Third Party) ⟶ ผลกระทบและความเสี่ยง ⟶ ข้อกำหนดที่มีผลใช้บังคับ

ผลการพิจารณาควรมีความชัดเจนเพียงพอที่จะตอบได้ว่า

ข้อกำหนดใดมีผลใช้บังคับ มาตรฐานใดนำมาใช้เป็นกรอบอ้างอิง และมาตรการใดเป็นวิธีการที่องค์กรเลือกใช้ตามผลการประเมินความเสี่ยง

ไม่จำเป็นต้องจัดทำเอกสารใหม่เฉพาะสำหรับการพิจารณาดังกล่าว หากเอกสารทะเบียนข้อกำหนด การประเมินความเสี่ยง เอกสารออกแบบ TOR สัญญา หรือหลักฐานอื่นที่องค์กรมีอยู่สามารถแสดงผลการพิจารณาและตรวจสอบย้อนหลังได้อย่างเพียงพอ

หลักการใช้อ้างอิงมาตรฐานและแนวปฏิบัติ

มาตรฐานและแนวปฏิบัติที่กล่าวถึงในเอกสารฉบับนี้มีวัตถุประสงค์เพื่อใช้เป็นกรอบอ้างอิงสำหรับการกำหนดหลักการ มาตรการ การทดสอบ และการสร้างความเชื่อมั่นตามลักษณะของระบบและระดับความเสี่ยง มิได้หมายความว่ามาตรฐานทุกฉบับมีสถานะเป็นข้อบังคับ หรือระบบ ผลิตภัณฑ์ ผู้ผลิต ผู้พัฒนา และผู้ให้บริการทุกกรณีต้องได้รับการรับรองตามมาตรฐานดังกล่าว

ในกรณีที่กฎหมาย กฎระเบียบ ประกาศ ข้อกำหนดเฉพาะภาคส่วน ข้อกำหนดในการจัดซื้อจัดจ้าง สัญญา หรือข้อกำหนดอื่นที่มีผลใช้บังคับกำหนดมาตรการหรือเงื่อนไขไว้เป็นการเฉพาะ ให้ดำเนินการตามข้อกำหนดนั้นเป็นสำคัญ ส่วนมาตรฐานและแนวปฏิบัติอื่นให้ประยุกต์ใช้ตามความเกี่ยวข้อง วัตถุประสงค์ บริบท และผลการประเมินความเสี่ยง

3.3 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

ระบบ CCTV ที่ใช้ AI สามารถสร้าง วิเคราะห์ เชื่อมโยง หรือนำข้อมูลจากภาพและวิดีโอไปใช้ในลักษณะที่แตกต่างจากระบบ CCTV ทั่วไป เช่น การติดตามบุคคล การระบุบุคคล การวิเคราะห์พฤติกรรม การสร้างข้อมูลชีวมิติ (Biometric Data) หรือการอนุมานข้อมูลเพิ่มเติมจากภาพ (Inferred Data) ซึ่งอาจทำให้ขอบเขตและผลกระทบของการประมวลผลข้อมูลส่วนบุคคลเพิ่มขึ้น

องค์กรจึงควรพิจารณาความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่การกำหนดวัตถุประสงค์ การออกแบบ การเลือกใช้ AI การจัดเก็บและเชื่อมโยงข้อมูล ตลอดจนการนำผลลัพธ์ของ AI ไปใช้ โดยปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง และใช้ผลการประเมินตามข้อ 3.1 ประกอบการกำหนดมาตรการ

3.3.1 วัตถุประสงค์และความจำเป็นของการใช้ AI

ก่อนเปิดใช้ความสามารถของ AI องค์กรควรกำหนดวัตถุประสงค์ของการประมวลผลให้ชัดเจน และพิจารณาว่าความสามารถดังกล่าวมีความจำเป็นและเหมาะสมกับวัตถุประสงค์หรือไม่

การติดตั้งกล้องเพื่อวัตถุประสงค์หนึ่งไม่ควรถูกตีความโดยอัตโนมัติว่าสามารถนำข้อมูลไปใช้กับความสามารถของ AI ทุกประเภทได้โดยไม่ต้องพิจารณาวัตถุประสงค์และข้อกำหนดที่เกี่ยวข้องเพิ่มเติม

ตัวอย่างเช่น การใช้ CCTV เพื่อรักษาความปลอดภัยของสถานที่ ไม่ได้หมายความโดยอัตโนมัติว่ามีความจำเป็นต้องเปิดใช้การรู้จำใบหน้า (Facial Recognition) การติดตามบุคคลข้ามพื้นที่ หรือการวิเคราะห์คุณลักษณะของบุคคลทุกกรณี

องค์กรควรสามารถตอบได้อย่างน้อยว่า

ใช้ AI เพื่ออะไร ⟶ จำเป็นต้องใช้ข้อมูลใด ⟶ สร้างข้อมูลหรือผลลัพธ์ใด ⟶ ใครใช้ผลลัพธ์ ⟶ ใช้เพื่อดำเนินการอะไร

3.3.2 การลดการเก็บและใช้ข้อมูลเท่าที่จำเป็น

องค์กรควรจำกัดการเก็บ ใช้ เปิดเผย และจัดเก็บข้อมูลให้เหมาะสมกับวัตถุประสงค์และความจำเป็น โดยไม่ควรเก็บข้อมูลเพิ่มเติมเพียงเพราะระบบ AI มีความสามารถทางเทคนิคในการสร้างหรือวิเคราะห์ข้อมูลดังกล่าวได้

การพิจารณาควรครอบคลุมทั้งข้อมูลต้นทางและข้อมูลที่เกิดขึ้นจาก AI เช่น

- ภาพและวิดีโอ
- ข้อมูลประกอบภาพหรือเหตุการณ์ (Metadata)
- ผลลัพธ์จากการตรวจจับหรือจำแนก
- ข้อมูลการติดตาม
- ข้อมูลชีวมิติหรือแม่แบบชีวมิติ (Biometric Template)

- ข้อมูลที่ได้จากการวิเคราะห์หรืออนุมาน (Derived or Inferred Data)
- ประวัติการแจ้งเตือนหรือผลการตัดสินใจที่เกี่ยวข้องกับ AI

การลดข้อมูลควรพิจารณาร่วมกับระยะเวลาการจัดเก็บ สิทธิการเข้าถึง การส่งต่อ และความจำเป็นในการเก็บข้อมูลแต่ละประเภท

3.3.3 ข้อมูลชีวมิติ

กรณีระบบมีการประมวลผลข้อมูลชีวมิติ เช่น การรู้จำใบหน้า องค์กรควรพิจารณาความชอบด้วยกฎหมาย วัตถุประสงค์ ความจำเป็น และมาตรการคุ้มครองข้อมูลตามข้อกำหนดที่เกี่ยวข้องก่อนนำความสามารถดังกล่าวมาใช้

มาตรการควรพิจารณาตามความเสี่ยง และอาจครอบคลุม

- การจำกัดวัตถุประสงค์และขอบเขตการใช้งาน
- การจำกัดบุคคลหรือระบบที่สามารถเข้าถึงข้อมูล
- การคุ้มครองแม่แบบหรือข้อมูลชีวมิติ
- การกำหนดระยะเวลาการเก็บรักษา
- การควบคุมการส่งต่อหรือเชื่อมโยงกับฐานข้อมูลอื่น
- การลบข้อมูลเมื่อหมดความจำเป็น
- การบันทึกและตรวจสอบการเข้าถึงหรือใช้งานที่สำคัญ

มาตรฐาน **ISO/IEC 24745** สามารถใช้เป็นกรอบอ้างอิงด้านการคุ้มครองข้อมูลชีวมิติได้ตามความเกี่ยวข้อง ส่วนการประเมินสมรรถนะและความผิดพลาดของระบบชีวมิติสามารถพิจารณามาตรฐาน **ISO/IEC 19795-1** ตามความเหมาะสม

รายละเอียดเพิ่มเติมเกี่ยวกับการวิเคราะห์ภาพอัจฉริยะและข้อมูลชีวมิติระบุในข้อ 6.2

3.3.4 การติดตาม การเชื่อมโยง และการอนุมานข้อมูล

AI สามารถทำให้ข้อมูลจาก CCTV ถูกนำไปใช้ติดตามบุคคลข้ามช่วงเวลา พื้นที่ หรือระบบ รวมถึงเชื่อมโยงกับข้อมูลจากแหล่งอื่นเพื่อสร้างข้อมูลใหม่เกี่ยวกับบุคคล

องค์กรควรพิจารณาอย่างน้อย

- พื้นที่และระยะเวลาที่สามารถติดตามบุคคลได้
- ความสามารถในการระบุตัวบุคคล
- แหล่งข้อมูลอื่นที่ถูกนำมาเชื่อมโยง
- ข้อมูลใหม่ที่เกิดจากการวิเคราะห์หรืออนุมาน
- จำนวนและลักษณะของบุคคลที่อาจได้รับผลกระทบ
- บุคคลหรือระบบที่สามารถเข้าถึงผลลัพธ์

- การนำผลลัพธ์ไปใช้ต่อ

ข้อมูลที่แต่ละส่วนอาจมีผลกระทบไม่สูงเมื่อพิจารณาแยกกัน อาจมีผลกระทบเพิ่มขึ้นอย่างมีนัยสำคัญเมื่อถูกสะสม เชื่อมโยง หรือนำมาวิเคราะห์ร่วมกัน

หากการติดตามหรือเชื่อมโยงข้อมูลทำให้ระดับผลกระทบเปลี่ยนแปลงอย่างมีนัยสำคัญ ควรนำกลับไปประเมินตามข้อ 3.1

3.3.5 ความถูกต้องของ AI และผลกระทบต่อบุคคล

ความผิดพลาดของ AI อาจทำให้บุคคลถูกตรวจจับ จำแนก ติดตาม หรือระบุอย่างไม่ถูกต้อง โดยเฉพาะเมื่อผลลัพธ์ถูกนำไปใช้ในการตัดสินใจหรือดำเนินการที่มีผลต่อบุคคล

องค์กรจึงไม่ควรประเมินเพียงค่าความแม่นยำโดยรวม แต่ควรพิจารณาประเภทและผลกระทบของความผิดพลาด เช่น

- **การแจ้งเตือนผิด (False Positive)**
- **การตรวจไม่พบเหตุที่ควรตรวจพบ (False Negative)**
- **การจำแนกผิด (Misclassification)**
- **การระบุบุคคลผิด (Misidentification)**

การประเมินควรพิจารณาร่วมกับสภาพแวดล้อมจริง คุณภาพของภาพ ลักษณะประชากรหรือบุคคลที่เกี่ยวข้อง และผลที่เกิดขึ้นเมื่อระบบผิดพลาด

สำหรับกรณีที่เกี่ยวข้องกับการระบุหรือยืนยันบุคคล อาจพิจารณาหลักการทดสอบและรายงานสมรรถนะตาม **ISO/IEC 19795-1** และมาตรฐานใน **IEC 62676 series** ที่เกี่ยวข้องกับสมรรถนะและการทดสอบระบบเฝ้าระวังด้วยวิดีโออัจฉริยะ

3.3.6 การกำกับดูแลโดยมนุษย์

กรณีที่ผลลัพธ์ของ AI อาจมีผลกระทบต่อบุคคล ควรจัดให้มีการกำกับดูแลโดยมนุษย์ในระดับที่เหมาะสมกับความเสี่ยง

ผู้ปฏิบัติงานควรสามารถ

- เข้าใจว่าผลลัพธ์ของ AI หมายถึงอะไรและมีข้อจำกัดอย่างไร
- ตรวจสอบข้อมูลหรือหลักฐานประกอบก่อนดำเนินการเมื่อจำเป็น
- หลีกเลี่ยงการเชื่อผลลัพธ์ของ AI โดยอัตโนมัติ
- แทรกแซง แก้ไข หรือระงับการใช้ผลลัพธ์เมื่อพบความผิดปกติ
- ส่งต่อหรือยกระดับการพิจารณาเมื่อผลกระทบเกินอำนาจหน้าที่

ค่าความเชื่อมั่น (Confidence Score) ไม่ควรถูกตีความว่าเป็นหลักฐานยืนยันความถูกต้องของผลลัพธ์โดยอัตโนมัติ

ระดับการกำกับดูแลควรเพิ่มขึ้นเมื่อผลลัพธ์ของ AI มีอำนาจต่อการตัดสินใจหรือการดำเนินการมากขึ้นตามหลักการในข้อ 3.1

3.3.7 การนำผลลัพธ์ของ AI ไปใช้ต่อ

องค์กรควรกำหนดขอบเขตการใช้ผลลัพธ์ของ AI ให้ชัดเจน โดยพิจารณาว่าผลลัพธ์ใดสามารถนำไปใช้โดยบุคคลหรือระบบใด และสามารถก่อให้เกิดการดำเนินการใดได้บ้าง

ควรพิจารณาอย่างน้อย

ผลลัพธ์ใด ⟶ ส่งให้ใครหรือระบบใด ⟶ ใช้เพื่ออะไร ⟶ มีการดำเนินการอัตโนมัติหรือไม่ ⟶ ใครตรวจสอบ ⟶ มีหลักฐานอะไร

ระบบที่มีผลกระทบสูงไม่ควรนำผลลัพธ์จาก AI ไปก่อให้เกิดการดำเนินการที่มีผลกระทบสูงโดยอัตโนมัติ หากไม่มีมาตรการตรวจสอบ จำกัดสิทธิ กำกับดูแล และจำกัดผลกระทบที่เหมาะสม การใช้ผลลัพธ์ในลักษณะที่แตกต่างจากวัตถุประสงค์หรือขอบเขตเดิมอย่างมีนัยสำคัญควรได้รับการประเมินผลกระทบและความเสี่ยงใหม่ตามข้อ 3.1

3.3.8 การประเมินผลกระทบด้าน AI และการคุ้มครองข้อมูล

การประเมินผลกระทบจาก AI การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล และการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยมีวัตถุประสงค์ที่เกี่ยวข้องกัน แต่ไม่ควรถูกถือว่าเป็นการประเมินประเภทเดียวกัน

การประเมิน	ประเด็นสำคัญ
การประเมินผลกระทบของระบบ AI (AI System Impact Assessment)	ผลกระทบจากวัตถุประสงค์ ความสามารถ ผลลัพธ์ และการใช้ AI ต่อบุคคล องค์กร หรือสังคม
การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)	ความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลจากการประมวลผลข้อมูลส่วนบุคคล
การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Assessment)	ภัยคุกคาม ช่องโหว่ ความเป็นไปได้ ผลกระทบ และมาตรการด้านความมั่นคงปลอดภัย
การประเมินผลกระทบต่อสิทธิขั้นพื้นฐาน (Fundamental Rights Impact Assessment: FRIA)	กรอบการประเมินผลกระทบต่อสิทธิขั้นพื้นฐานตามกฎหมายหรือกรอบกำกับดูแลที่เกี่ยวข้อง

องค์กรสามารถเชื่อมโยงการประเมินเหล่านี้เข้าด้วยกันเพื่อลดความซ้ำซ้อน หากยังสามารถแสดงวัตถุประสงค์ ขอบเขต ผลการประเมิน และมาตรการที่เกี่ยวข้องได้อย่างชัดเจน

ISO/IEC 42005 สามารถใช้เป็นกรอบสำหรับการประเมินผลกระทบของระบบ AI ส่วน FRIA ที่กล่าวถึงในแนวปฏิบัตินี้ใช้เป็นกรอบอ้างอิงด้านกฎระเบียบต่างประเทศ เช่น EU AI Act เว้นแต่องค์กรอยู่ภายใต้ข้อกำหนดที่มีผลใช้บังคับโดยตรง

3.3.9 ระยะเวลาการเก็บรักษาและการลบข้อมูล

องค์กรควรกำหนดระยะเวลาการเก็บรักษาข้อมูลตามวัตถุประสงค์ ความจำเป็น ข้อกำหนดที่เกี่ยวข้อง และระดับความเสี่ยง โดยพิจารณาข้อมูลแต่ละประเภทแยกจากกันตามความเหมาะสม

ตัวอย่างเช่น

ภาพหรือวิดีโอ ⟶ ข้อมูลประกอบ (Metadata) ⟶ ผลลัพธ์จาก AI ⟶ ข้อมูลการติดตาม ⟶ แม่แบบชีวมิติ (Biometric Template) ⟶ ข้อมูลที่ได้จากการวิเคราะห์หรืออนุมาน

การลบภาพหรือวิดีโอต้นฉบับ **ไม่ได้หมายความว่าข้อมูลที่เกิดจาก AI ถูกลบไปพร้อมกันโดยอัตโนมัติ** องค์กรจึงควรทราบว่าข้อมูลประเภทใดยังคงถูกจัดเก็บอยู่ที่ใด และกำหนดการลบหรือการคงไว้ตามวัตถุประสงค์และข้อกำหนดที่เกี่ยวข้อง

ข้อมูลที่จำเป็นต้องเก็บไว้เพื่อวัตถุประสงค์ทางกฎหมาย การตรวจสอบ หรือการสอบสวน ควรได้รับการแยกและคุ้มครองตามความเหมาะสม

3.3.10 ความโปร่งใสในการใช้ AI

องค์กรควรพิจารณาการให้ข้อมูลเกี่ยวกับการใช้ CCTV และ AI แก่บุคคลที่เกี่ยวข้องในระดับที่เหมาะสมกับลักษณะการประมวลผลและข้อกำหนดที่มีผลใช้บังคับ

ข้อมูลที่เหมาะสมอาจครอบคลุมวัตถุประสงค์ของการใช้ระบบ ประเภทของการประมวลผล AI ลักษณะข้อมูลที่เกี่ยวข้อง การนำผลลัพธ์ไปใช้ ระยะเวลาการเก็บรักษา และช่องทางที่บุคคลสามารถติดต่อหรือใช้สิทธิตามที่กฎหมายกำหนด

การมีป้ายแจ้งว่าพื้นที่มี CCTV ไม่ควรถูกตีความโดยอัตโนมัติว่าเป็นการแจ้งหรืออนุญาตให้ใช้ความสามารถ AI ทุกประเภทโดยไม่มีการพิจารณาเพิ่มเติม

3.3.11 บริการคลาวด์และผู้ให้บริการภายนอก

กรณีข้อมูลหรือผลลัพธ์จากระบบ CCTV ที่ใช้ AI ถูกส่งไปจัดเก็บ ประมวลผล หรือเข้าถึงผ่านบริการคลาวด์หรือผู้ให้บริการภายนอก องค์กรควรทราบและประเมินอย่างน้อยถึงประเภทของข้อมูลที่ถูกส่งออก สถานที่จัดเก็บข้อมูล (Data Location) สถานที่ประมวลผลข้อมูล (Processing Location) บุคคลหรือหน่วยงานที่สามารถเข้าถึงข้อมูล ผู้ให้บริการช่วง (Subprocessor) ตลอดจนเขตอำนาจทางกฎหมาย (Jurisdiction) ที่เกี่ยวข้องกับข้อมูลและบริการดังกล่าว

องค์กรควรพิจารณากฎหมาย ข้อกำหนด และเงื่อนไขที่อาจมีผลใช้บังคับต่อข้อมูลตามสถานที่จัดเก็บ สถานที่ประมวลผล ลักษณะการเข้าถึงข้อมูล และเขตอำนาจทางกฎหมายที่เกี่ยวข้อง โดยไม่ควรพิจารณาเฉพาะสถานที่ตั้งของศูนย์ข้อมูลเพียงปัจจัยเดียว

นอกจากนี้ ควรพิจารณาร่วมกับการเข้ารหัสและการควบคุมกุญแจ การบริหารเหตุการณ์ การสำรองและกู้คืน ความต่อเนื่องของบริการ ตลอดจนการคืน ลบ หรือเคลื่อนย้ายข้อมูล และการยุติหรือเปลี่ยนผู้ให้บริการ (Exit Strategy) ตามระดับผลกระทบและความเสี่ยง

สำหรับหน่วยงานหรือบริการที่อยู่ภายใต้ขอบเขตของข้อกำหนดด้านความมั่นคงปลอดภัยระบบคลาวด์ของประเทศไทย ให้ปฏิบัติตามกฎหมาย ประกาศ หรือข้อกำหนดดังกล่าวตามที่มีผลใช้บังคับ

รายละเอียดด้านบริการคลาวด์ อธิปไตยข้อมูล (Data Sovereignty) และการกำหนดที่ตั้งข้อมูล (Data Localization) ระบุเพิ่มเติมในข้อ 6.1

3.4 การอัปเดตเฟิร์มแวร์และการบำรุงรักษา

การปรับปรุงเฟิร์มแวร์ ซอฟต์แวร์ แบบจำลอง AI การตั้งค่า หรือบริการภายนอก อาจส่งผลต่อความมั่นคงปลอดภัย สมรรถนะของ AI การประมวลผลข้อมูล และการเชื่อมต่อกับระบบอื่น องค์กรจึงควรบริหารการเปลี่ยนแปลงที่มีผลต่อ CCTV-AI อย่างเป็นระบบตลอดวงจรชีวิต

การปรับปรุงระบบไม่ควรพิจารณาเฉพาะว่าการติดตั้งสำเร็จหรือระบบสามารถกลับมาให้บริการได้ แต่ควรพิจารณาด้วยว่า **ระบบยังคงทำงานตามวัตถุประสงค์ อยู่ในสถานะที่ได้รับอนุมัติ และมีระดับความเสี่ยงที่ยอมรับได้**

หลักการโดยรวมควรเป็น

ระบุการเปลี่ยนแปลง ⟶ ประเมินผลกระทบ ⟶ ทดสอบ ⟶ อนุมัติ ⟶ นำไปใช้ ⟶ ทวนสอบ ⟶ เฝ้าระวัง

3.4.1 การระบุรุ่นและองค์ประกอบที่สำคัญ

องค์กรควรสามารถระบุองค์ประกอบสำคัญของระบบที่ใช้งานอยู่ในระดับที่เพียงพอต่อการบริหารการเปลี่ยนแปลงและความเสี่ยง เช่น

- รุ่นของอุปกรณ์และเฟิร์มแวร์
- ซอฟต์แวร์หรือแพลตฟอร์มที่สำคัญ
- แบบจำลองหรือความสามารถของ AI ที่ใช้งาน
- การตั้งค่าที่มีผลต่อการทำงานของ AI
- บริการ AI หรือบริการคลาวด์ภายนอกที่สำคัญ
- การเชื่อมต่อกับระบบอื่นที่อาจได้รับผลกระทบ

ไม่จำเป็นต้องจัดทำทะเบียนใหม่แยกต่างหาก หากข้อมูลจากระบบบริหารสินทรัพย์ การบริหารการตั้งค่า เอกสารผู้ผลิต หรือหลักฐานอื่นที่องค์กรมีอยู่สามารถใช้ระบุสถานะของระบบและตรวจสอบย้อนหลังได้อย่างเพียงพอ

3.4.2 การประเมินก่อนการเปลี่ยนแปลง

ก่อนดำเนินการเปลี่ยนแปลงที่อาจมีผลต่อระบบ CCTV-AI องค์กรควรพิจารณาผลกระทบที่อาจเกิดขึ้นต่อ

ความมั่นคงปลอดภัย ⟶ ข้อมูล ⟶ สมรรถนะของ AI ⟶ สิทธิการเข้าถึง ⟶ การเชื่อมต่อ ⟶ การดำเนินการต่อของระบบอื่น ⟶ ความต่อเนื่องของบริการ

ตัวอย่างการเปลี่ยนแปลงที่ควรได้รับการพิจารณา ได้แก่ การเปลี่ยนเฟิร์มแวร์ ซอฟต์แวร์ แบบจำลอง AI ค่าการตรวจจับหรือเกณฑ์การตัดสินใจ ความสามารถของ AI วิธีประมวลผลข้อมูล ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) ระบบที่เชื่อมต่อ หรือผู้ให้บริการภายนอก

ระดับการประเมินควรได้สัดส่วนกับความสำคัญและผลกระทบของการเปลี่ยนแปลง ไม่จำเป็นต้องใช้กระบวนการประเมินในระดับเดียวกันสำหรับการเปลี่ยนแปลงทุกประเภท

3.4.3 การทดสอบและอนุมัติการเปลี่ยนแปลง

การเปลี่ยนแปลงที่มีนัยสำคัญควรได้รับการทดสอบก่อนนำไปใช้จริงตามความเหมาะสม โดยการทดสอบอาจครอบคลุม

- การทำงานของระบบหลังการเปลี่ยนแปลง
- สมรรถนะและผลลัพธ์ของ AI
- การตั้งค่าด้านความมั่นคงปลอดภัย
- บัญชีและสิทธิการเข้าถึง
- การบันทึกเหตุการณ์
- การเชื่อมต่อผ่าน API หรือระบบอื่น
- การดำเนินการอัตโนมัติที่เกี่ยวข้อง
- การทำงานในกรณีผิดปกติหรือไม่พร้อมใช้งาน

สำหรับระบบที่มีผลกระทบสูง ควรกำหนดเกณฑ์การทดสอบและผู้มีอำนาจอนุมัติให้เหมาะสมกับระดับความเสี่ยงก่อนนำการเปลี่ยนแปลงเข้าสู่ระบบใช้งานจริง

3.4.4 การทวนสอบภายหลังการเปลี่ยนแปลง

ภายหลังการเปลี่ยนแปลง องค์กรควรทวนสอบว่าระบบยังคงอยู่ในสถานะที่ได้รับอนุมัติ (Approved State) และไม่มีผลกระทบที่ไม่ได้คาดหมายต่อความมั่นคงปลอดภัยหรือการทำงานของ AI

ควรพิจารณาอย่างน้อยว่า

ระบบทำงานได้ ⟶ AI ทำงานตามที่คาดหมาย ⟶ การตั้งค่าความมั่นคงปลอดภัยยังถูกต้อง ⟶ สิทธิไม่เปลี่ยนโดยไม่ตั้งใจ ⟶ การเชื่อมต่อยังอยู่ในขอบเขต ⟶ การบันทึกเหตุการณ์และการเฝ้าระวัง (Logging and Monitoring)

หากพบความผิดปกติที่มีนัยสำคัญ ควรสามารถจำกัดผลกระทบ ย้อนกลับการเปลี่ยนแปลง หรือใช้รูปแบบการทำงานที่ปลอดภัยตามความเหมาะสม

3.4.5 การปรับปรุงด้านความมั่นคงปลอดภัยและช่องโหว่

เมื่อมีการเผยแพร่การปรับปรุงด้านความมั่นคงปลอดภัยหรือพบช่องโหว่ที่เกี่ยวข้องกับผลิตภัณฑ์หรือบริการ องค์กรควรพิจารณาว่าระบบที่ใช้งานได้รับผลกระทบหรือไม่ และกำหนดลำดับความสำคัญของการดำเนินการตามความเสี่ยง

การพิจารณาไม่ควรใช้ระดับความรุนแรงของช่องโหว่เพียงอย่างเดียว แต่ควรพิจารณาร่วมกับปัจจัย เช่น ความสามารถในการโจมตี การมีหลักฐานว่าถูกนำไปใช้โจมตีจริง ความสำคัญของระบบ ข้อมูลที่เกี่ยวข้อง และผลกระทบที่อาจเกิดขึ้น

กรณียังไม่สามารถติดตั้งการแก้ไขได้ทันที อาจใช้มาตรการลดความเสี่ยงชั่วคราว (Mitigation or Compensating Controls) ตามความเหมาะสม พร้อมติดตามจนสามารถดำเนินการแก้ไขและทวนสอบได้ รายละเอียดกระบวนการบริหารช่องโหว่ระบุในข้อ 3.7 เพื่อหลีกเลี่ยงการกำหนดกระบวนการซ้ำในส่วนนี้

3.4.6 การเปลี่ยนแปลงจากบริการภายนอก

กรณีระบบพึ่งพาบริการคลาวด์ บริการ AI หรือบริการจากผู้ให้บริการภายนอก การเปลี่ยนแปลงอาจเกิดขึ้นโดยที่องค์กรไม่ได้เป็นผู้ดำเนินการโดยตรง เช่น การเปลี่ยนแบบจำลอง AI รุ่นของบริการ API ความสามารถของระบบ เงื่อนไขการให้บริการ หรือสถานที่ประมวลผลข้อมูล

องค์กรควรกำหนดแนวทางสำหรับรับทราบและประเมินการเปลี่ยนแปลงที่มีนัยสำคัญจากผู้ให้บริการ และพิจารณาผลกระทบต่อระบบที่ใช้งานตามความเหมาะสม

สำหรับระบบที่มีผลกระทบสูง ควรพิจารณาข้อกำหนดด้านการแจ้งการเปลี่ยนแปลง การทดสอบ หรือสิทธิในการพิจารณาการเปลี่ยนแปลงที่มีนัยสำคัญไว้ตั้งแต่การจัดซื้อจัดจ้างหรือทำสัญญา

3.4.7 การสิ้นสุดการสนับสนุน

องค์กรควรติดตามระยะเวลาการสนับสนุนของอุปกรณ์ เฟิร์มแวร์ ซอฟต์แวร์ และบริการสำคัญที่เกี่ยวข้องกับระบบ CCTV-AI เพื่อป้องกันการใช้งานองค์ประกอบที่ไม่สามารถได้รับการปรับปรุงด้านความมั่นคงปลอดภัยหรือการสนับสนุนที่จำเป็น

เมื่อผลิตภัณฑ์หรือบริการใกล้สิ้นสุดการสนับสนุน (End of Support) ควรประเมินความเสี่ยงและกำหนดแนวทางที่เหมาะสม เช่น การปรับรุ่น การเปลี่ยนผลิตภัณฑ์ การจำกัดการใช้งาน หรือมาตรการลดความเสี่ยงอื่นในช่วงเปลี่ยนผ่าน

การใช้งานต่อหลังสิ้นสุดการสนับสนุนไม่ควรเกิดขึ้นโดยไม่มีการรับรู้และประเมินความเสี่ยงที่เกี่ยวข้อง

การเปลี่ยนแปลงที่มีนัยสำคัญ (Significant Change) หมายถึง การเปลี่ยนแปลงที่อาจทำให้วัตถุประสงค์ ขอบเขตการประมวลผลข้อมูล ความสามารถหรือสมรรถนะของ AI การเชื่อมต่อ การดำเนินการอัตโนมัติ หรือระดับผลกระทบและความเสี่ยงของระบบเปลี่ยนแปลงอย่างมีนัยสำคัญ

เมื่อเกิดการเปลี่ยนแปลงดังกล่าว องค์กรควรพิจารณาทบทวนหรือประเมินผลกระทบและความเสี่ยงใหม่ตามข้อ 3.1 ก่อนหรือภายหลังการเปลี่ยนแปลงตามลักษณะและความเร่งด่วนของกรณี

3.5 การเฝ้าระวังและบันทึกการใช้งาน

ระบบ CCTV ที่ใช้ AI ควรได้รับการเฝ้าระวังในระดับที่เหมาะสมกับความสำคัญ ผลกระทบ และความเสี่ยง เพื่อให้สามารถตรวจพบการเปลี่ยนแปลง ความผิดปกติ การใช้ความสามารถของ AI ที่ไม่เหมาะสม และเหตุการณ์ที่อาจส่งผลต่อความน่าเชื่อถือหรือความมั่นคงปลอดภัยของระบบ

การเฝ้าระวังไม่ควรจำกัดเฉพาะสถานะของกล้องหรือเครือข่าย แต่ควรครอบคลุมองค์ประกอบที่เกี่ยวข้องกับ AI และการนำผลลัพธ์ไปใช้ตามความเหมาะสม

3.5.1 ขอบเขตการเฝ้าระวังและการบันทึกเหตุการณ์

ขอบเขตอาจครอบคลุม

- การเข้าสู่ระบบและการเข้าถึงโดยผู้ดูแลระบบ
- การเปลี่ยนแปลงการตั้งค่าที่สำคัญ
- การเปิด ปิด หรือเปลี่ยนความสามารถของ AI
- การเปลี่ยนรุ่นของซอฟต์แวร์หรือ AI
- การเข้าถึงหรือส่งออกข้อมูลที่มีผลกระทบสูง
- ผลลัพธ์หรือเหตุการณ์จาก AI ที่มีผลต่อการดำเนินการสำคัญ
- การเชื่อมต่อผ่าน API หรือระบบอื่น
- การดำเนินการอัตโนมัติ
- เหตุการณ์ผิดปกติหรือความล้มเหลวที่สำคัญ

ไม่จำเป็นต้องบันทึกทุกกิจกรรมในรายละเอียดเท่ากัน การกำหนดการบันทึกเหตุการณ์ (Logging) ควรพิจารณาจากความจำเป็นในการตรวจสอบเหตุการณ์ การพิสูจน์ความรับผิดชอบ และระดับความเสี่ยง

3.5.2 การเฝ้าระวังการเปลี่ยนแปลงของ AI

องค์กรควรสามารถตรวจพบหรือทบทวนการเปลี่ยนแปลงที่สำคัญของ AI ในระดับที่จำเป็นต่อการบริหารความเสี่ยง เช่น แบบจำลองหรือบริการ AI รุ่น (Version) ความสามารถ (Capability) กฎ (Rule) การกำหนดค่า (Configuration) หรือค่าที่มีผลต่อผลลัพธ์ของระบบ เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือการเปลี่ยนแปลงที่ไม่ได้ผ่านกระบวนการบริหารการเปลี่ยนแปลงตามข้อ 3.4

การระบุแบบจำลองหรือรุ่นของ AI ควรดำเนินการในระดับที่ผู้ใช้งานสามารถทราบและใช้ในการประเมินผลกระทบและบริหารความเสี่ยงได้อย่างเหมาะสม โดยไม่จำเป็นต้องเปิดเผยรายละเอียดของแบบจำลอง อัลกอริทึม ไลบรารี หรือองค์ประกอบทางเทคนิคภายในทั้งหมด เว้นแต่กฎหมาย ข้อกำหนดในการจัดซื้อ สัญญา หรือผลการประเมินความเสี่ยงกำหนดให้มีการเปิดเผยเพิ่มเติม

เมื่อมีการเปลี่ยนแปลงที่อาจส่งผลอย่างมีนัยสำคัญต่อความสามารถ สมรรถนะ ความมั่นคงปลอดภัย ความเป็นส่วนตัว หรือผลลัพธ์ของ AI ผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการควรจัดให้มีข้อมูลที่เพียงพอเพื่อให้องค์กรผู้ใช้งานสามารถประเมินผลกระทบ ทดสอบ และพิจารณาความเหมาะสมก่อนหรือภายหลังการเปลี่ยนแปลงตามระดับความเสี่ยง

3.5.3 การเฝ้าระวังสมรรถนะของ AI

ควรติดตามตัวชี้วัดหรือข้อมูลที่เหมาะสมกับกรณีใช้งาน เพื่อให้สามารถตรวจพบการเปลี่ยนแปลงของสมรรถนะหรือรูปแบบความผิดพลาดที่อาจมีผลต่อความเสี่ยง

การเฝ้าระวังอาจพิจารณาการแจ้งเตือนผิด (False Positive), การตรวจไม่พบ (False Negative), การจำแนกผิด (Misclassification) และการระบุบุคคลผิด (Misidentification) หรือเหตุผิดปกติอื่นตามลักษณะของระบบ โดยไม่จำเป็นต้องใช้ตัวชี้วัดเดียวกันสำหรับ AI ทุกประเภท

เมื่อสมรรถนะเปลี่ยนแปลงอย่างมีนัยสำคัญ ควรพิจารณาสาเหตุและผลกระทบก่อนปรับค่าเกณฑ์ (Threshold) หรือการตั้งค่า (Configuration) เพื่อหลีกเลี่ยงการแก้ปัญหาที่อาจสร้างความเสี่ยงใหม่

3.5.4 การเฝ้าระวังการใช้ผลลัพธ์ของ AI

สำหรับระบบที่ผลลัพธ์ AI ถูกนำไปใช้ในการตัดสินใจหรือดำเนินการต่อ ควรสามารถตรวจสอบได้ตามความเหมาะสมว่า

AI สร้างผลลัพธ์อะไร ⟶ ผลลัพธ์ถูกส่งไปที่ใด ⟶ บุคคลหรือระบบใดนำไปใช้ ⟶ มีการดำเนินการใดเกิดขึ้น

ระดับรายละเอียดของหลักฐานควรเพิ่มขึ้นเมื่อผลลัพธ์สามารถก่อให้เกิดผลกระทบสูง

3.5.5 การเฝ้าระวังระบบที่เชื่อมต่อและการดำเนินการอัตโนมัติ

กรณีมีส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) กระบวนงานอัตโนมัติ (Workflow) หรือการดำเนินการอัตโนมัติ (Automated Action) ควรเฝ้าระวังการเรียกใช้งานที่ผิดปกติ การใช้สิทธิเกินขอบเขต การดำเนินการที่อยู่นอกขอบเขตที่ได้รับอนุมัติ (Action Boundary) และความผิดปกติของระบบปลายทางตามระดับความเสี่ยง

3.5.6 การติดตามช่องโหว่และสถานะการแก้ไข

การติดตามช่องโหว่ควรครอบคลุมทั้ง **ฝั่งผลิตภัณฑ์** และ **ฝั่งระบบที่นำผลิตภัณฑ์ไปใช้งาน**

ผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการ (Manufacturer / Developer / Service Provider) ควรสามารถตรวจสอบและประเมินช่องโหว่ที่เกี่ยวข้องกับผลิตภัณฑ์หรือบริการ ระบุรุ่นหรือองค์ประกอบที่ได้รับผลกระทบ จัดทำการแก้ไขหรือมาตรการลดความเสี่ยง สื่อสารข้อมูลที่จำเป็น และทวนสอบผลการแก้ไขตามความเหมาะสม

องค์กรผู้ใช้งานหรือเจ้าของระบบ (Deploying Organization / System Owner) ควรติดตามข้อมูลช่องโหว่ที่เกี่ยวข้อง ตรวจสอบว่าผลิตภัณฑ์หรือรุ่นดังกล่าวถูกใช้งานในระบบใด ประเมินความเสี่ยงในบริบทขององค์กร กำหนดลำดับความสำคัญ ทดสอบและนำการแก้ไขไปใช้ และติดตามสถานะจนดำเนินการแล้วเสร็จ

หลักการสำคัญคือ **ผู้ผลิตหรือผู้ให้บริการบริหารช่องโหว่ของผลิตภัณฑ์หรือบริการ ขณะที่องค์กรผู้ใช้งานบริหารความเสี่ยงที่ช่องโหว่นั้นก่อให้เกิดต่อระบบที่นำผลิตภัณฑ์หรือบริการไปใช้**

รายละเอียดกระบวนการตั้งแต่การค้นพบจนถึงการปิดประเด็นระบุในข้อ 3.7.3

3.5.7 การคุ้มครองบันทึกเหตุการณ์

บันทึกเหตุการณ์ (Logs) ที่มีความสำคัญควรได้รับการคุ้มครองจากการเข้าถึง การแก้ไข หรือลบโดยไม่ได้รับอนุญาต และมีระยะเวลาการเก็บรักษาที่เหมาะสมกับวัตถุประสงค์ ข้อกำหนด และความเสี่ยง

หาก Logs มีข้อมูลส่วนบุคคลหรือข้อมูลที่มีผลกระทบสูง ควรได้รับการคุ้มครองตามระดับของข้อมูลดังกล่าวด้วย

การเฝ้าระวัง CCTV-AI ควรทำให้สามารถตอบได้ว่า “ระบบเปลี่ยนอะไร ⟶ AI ทำงานผิดปกติหรือไม่ ⟶ ผลลัพธ์ถูกนำไปใช้ที่ใด ⟶ มีช่องโหว่หรือเหตุการณ์ใดที่ต้องดำเนินการ ⟶ และสามารถตรวจสอบย้อนหลังได้หรือไม่”

3.6 รอบการตรวจเช็คและบำรุงรักษา

ระบบ CCTV ที่ใช้ AI ควรได้รับการตรวจสอบและทบทวนตามรอบ เพื่อยืนยันว่าระบบยังคงทำงานตามวัตถุประสงค์ อยู่ในสถานะที่ได้รับอนุมัติ และมาตรการด้านความมั่นคงปลอดภัยยังเหมาะสมกับระดับผลกระทบและความเสี่ยง

รอบการตรวจสอบไม่จำเป็นต้องกำหนดเป็นระยะเวลาเดียวกันสำหรับทุกระบบ แต่ควรพิจารณาจาก **ความสำคัญของระบบหรือภารกิจ (System/Mission Criticality) ผลกระทบด้านข้อมูล (Data Impact) ผลกระทบจาก AI (AI Impact) การเปลี่ยนแปลงของระบบ และประวัติเหตุการณ์หรือความผิดปกติ** ตามความเหมาะสม

นอกจากการตรวจตามรอบแล้ว ควรมีการตรวจสอบเมื่อเกิดเหตุการณ์หรือการเปลี่ยนแปลงที่อาจทำให้ระดับผลกระทบหรือความเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ

3.6.1 ขอบเขตการตรวจสอบ

การตรวจสอบควรครอบคลุมองค์ประกอบที่มีผลต่อความมั่นคงปลอดภัยและความน่าเชื่อถือของ CCTV-AI ตามความเกี่ยวข้อง ดังนี้

ประเด็น	ตัวอย่างสิ่งที่ควรตรวจสอบ
อุปกรณ์และคุณภาพภาพ	สภาพอุปกรณ์ ตำแหน่งกล้อง มุมมอง แสง การบดบัง และคุณภาพภาพที่มีผลต่อ AI
การตั้งค่าความมั่นคงปลอดภัย	บัญชี สิทธิ การเข้าถึงจากระยะไกล (Remote Access) บริการที่เปิดใช้งาน และค่าตั้งต้นสำคัญ
AI และซอฟต์แวร์	รุ่น ความสามารถ การตั้งค่า กฎ ค่าเกณฑ์ (Threshold) และการเปลี่ยนแปลงที่สำคัญ
สมรรถนะของ AI	ความผิดพลาดหรือความเปลี่ยนแปลงของผลลัพธ์ที่มีผลต่อกรณีใช้งาน
ข้อมูล	การเก็บ ใช้ เข้าถึง ส่งต่อ เชื่อมโยง เก็บรักษา และลบข้อมูล
การเชื่อมต่อ	ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) กระบวนงานอัตโนมัติ (Workflow) บัญชีบริการ (Service Account) และระบบปลายทาง
บริการคลาวด์และบริการภายนอก (Cloud and External Services)	การเปลี่ยนแปลงบริการ ผู้ให้บริการ สิทธิ สถานที่ประมวลผล และความรับผิดชอบ

ประเด็น	ตัวอย่างสิ่งที่ควรตรวจสอบ
ช่องโหว่และการสนับสนุน	ช่องโหว่ การปรับปรุงด้านความมั่นคงปลอดภัย (Security Update) และสถานะการสนับสนุนผลิตภัณฑ์
หลักฐาน	บันทึกเหตุการณ์ (Logs) ผลการทดสอบ การอนุมัติ การเปลี่ยนแปลง และผลการแก้ไขที่จำเป็น

ไม่จำเป็นต้องตรวจสอบทุกรายการด้วยความถี่และรายละเอียดเท่ากัน โดยควรกำหนดตามระดับ B, E หรือ H และความเสี่ยงของระบบตามข้อ 3.1

3.6.2 ความถี่ตามระดับความเสี่ยง

องค์กรควรกำหนดความถี่ในการตรวจสอบให้เหมาะสมกับบริบทของระบบ โดยอาจพิจารณา **ความสำคัญของระบบ + ผลกระทบด้านข้อมูล + ผลกระทบจาก AI + สภาพแวดล้อม + ความถี่ของการเปลี่ยนแปลง + ประวัติเหตุการณ์ + ข้อกำหนดของผู้ผลิตหรือผู้ให้บริการ**

ระบบที่มีผลกระทบสูง มีการเปลี่ยนแปลงบ่อย หรือผลลัพธ์ของ AI ถูกนำไปใช้กับระบบสำคัญ อาจจำเป็นต้องได้รับการตรวจสอบบ่อยหรือมีขอบเขตการตรวจสอบมากกว่าระบบทั่วไป

แนวปฏิบัตินี้ **ไม่กำหนดระยะเวลาเดียว เช่น ทุก 3 เดือน 6 เดือน หรือ 1 ปี สำหรับทุกระบบ** เนื่องจากอาจทำให้ระดับการตรวจสอบไม่เหมาะสมกับความเสี่ยงจริง

อย่างไรก็ตาม องค์กรควรกำหนดรอบการตรวจสอบไว้ล่วงหน้าและสามารถอธิบายเหตุผลของความถี่ที่เลือกใช้ได้

3.6.3 การตรวจสอบเมื่อเกิดเหตุการณ์หรือการเปลี่ยนแปลง

นอกเหนือจากการตรวจสอบตามรอบ องค์กรควรพิจารณาตรวจสอบเพิ่มเติมเมื่อเกิดเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยหรือความน่าเชื่อถือของระบบ เช่น

- เปลี่ยนแบบจำลอง AI เฟิร์มแวร์ หรือซอฟต์แวร์ที่สำคัญ
- เปลี่ยนวัตถุประสงค์หรือเปิดใช้ความสามารถ AI เพิ่มเติม
- เปลี่ยนตำแหน่งกล้องหรือสภาพแวดล้อมที่มีผลต่อ AI
- เปลี่ยนส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) กระบวนงานอัตโนมัติ (Workflow) หรือระบบที่เชื่อมต่อ
- เพิ่มการดำเนินการอัตโนมัติ (Automated Action)
- เปลี่ยนผู้ให้บริการคลาวด์ (Cloud Service Provider) หรือผู้ให้บริการ AI ภายนอก
- พบช่องโหว่ที่มีนัยสำคัญ
- เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

- พบความเปลี่ยนแปลงของสมรรถนะหรือความผิดพลาดของ AI อย่างมีนัยสำคัญ

หากเหตุการณ์ดังกล่าวอาจทำให้ระดับผลกระทบหรือความเสี่ยงเปลี่ยนแปลง ควรพิจารณาประเมินใหม่ตามข้อ 3.1

3.6.4 การตรวจสอบระบบที่เชื่อมต่อและการดำเนินการอัตโนมัติ

กรณีระบบ CCTV ที่ใช้ AI เชื่อมต่อกับระบบอื่น องค์กรควรตรวจสอบว่าการเชื่อมต่อ ข้อมูลที่แลกเปลี่ยน สิทธิ และขอบเขตการดำเนินการยังคงเป็นไปตามที่ได้รับอนุมัติ โดยพิจารณาอย่างน้อยตามลำดับดังนี้

ระบบปลายทาง ⟶ บัญชีและสิทธิการเข้าถึง ⟶ ส่วนเชื่อมต่อระบบ (API/Interface) ⟶ ข้อมูลที่ส่งหรือรับ ⟶ เงื่อนไขกระตุ้นและกระบวนงานอัตโนมัติ (Trigger/Workflow) ⟶ การดำเนินการของระบบ ⟶ การกำกับดูแลโดยมนุษย์ (Human Oversight) ⟶ สภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe)

สำหรับระบบที่ AI สามารถเรียกใช้เครื่องมือ บริการ หรือดำเนินการต่อได้ ควรตรวจสอบสิทธิที่ได้รับ (Permission) และขอบเขตการดำเนินการ (Action Boundary) เป็นพิเศษตามระดับผลกระทบและความเสี่ยง

3.6.5 ผลการตรวจสอบและการดำเนินการแก้ไข

ผลการตรวจสอบควรมีหลักฐานเพียงพอให้สามารถติดตามได้ว่า **ตรวจอะไร ⟶ ผลเป็นอย่างไร ⟶ พบความผิดปกติหรือไม่ ⟶ ใครรับผิดชอบ ⟶ ต้องดำเนินการอะไร ⟶ สถานะเป็นอย่างไร**

องค์กรสามารถใช้ระบบหรือแบบฟอร์มที่มีอยู่ เช่น ระบบบริหารงานบำรุงรักษา ระบบ Ticket, Checklist, Risk Register หรือ Corrective Action Process โดยไม่จำเป็นต้องสร้างเอกสารใหม่ หากสามารถติดตามและตรวจสอบย้อนหลังได้อย่างเพียงพอ

สำหรับการตรวจสอบตามรอบ สามารถใช้ **ภาคผนวก ข รายการตรวจสอบด้วยตนเองตามรอบ (Periodic Self-Assessment Checklist)** เป็นแนวทางประกอบได้

หลักสำคัญ การตรวจสอบตามรอบมีวัตถุประสงค์เพื่อยืนยันว่า CCTV-AI ยังคงเหมาะสมกับวัตถุประสงค์ อยู่ในสถานะที่ได้รับอนุมัติ และมีระดับความเสี่ยงที่ยอมรับได้ มิใช่เพียงตรวจว่ากล้องหรือ AI “ยังทำงานอยู่”

3.7 เฟิร์มแวร์ ช่องโหว่ และการเลือกอุปกรณ์ที่น่าเชื่อถือ

ระบบ CCTV ที่ใช้ AI ประกอบด้วยองค์ประกอบหลายส่วน ตั้งแต่อุปกรณ์ เฟิร์มแวร์ ซอฟต์แวร์ ส่วนประกอบจากบุคคลที่สาม แบบจำลอง AI ไปจนถึงบริการคลาวด์หรือบริการ AI ภายนอก ความมั่นคง

ปลอดภัยของระบบจึงขึ้นอยู่ทั้งกับการกำหนดค่าขององค์กรและความสามารถของผู้ผลิต ผู้พัฒนา และผู้ให้บริการในการรักษาความมั่นคงปลอดภัยของผลิตภัณฑ์ตลอดวงจรชีวิต

การพิจารณาความน่าเชื่อถือจึงไม่ควรจำกัดอยู่ที่คุณสมบัติของผลิตภัณฑ์ ณ วันที่จัดซื้อ แต่ควรครอบคลุม **การพัฒนาที่มั่นคงปลอดภัย การบริหารส่วนประกอบ การปรับปรุงด้านความมั่นคงปลอดภัย การบริหารช่องโหว่ การเปลี่ยนแปลง และการสนับสนุนตลอดอายุการใช้งาน**

3.7.1 ความน่าเชื่อถือของอุปกรณ์ ผู้ผลิต และผู้ให้บริการ

องค์กรควรพิจารณาความน่าเชื่อถือของผลิตภัณฑ์และผู้เกี่ยวข้องตามระดับผลกระทบและความเสี่ยง โดยอาจพิจารณาประเด็นดังต่อไปนี้

ประเด็น	สิ่งที่ควรพิจารณา
การพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย (Secure Development)	ผู้ผลิตหรือผู้พัฒนาควรมีแนวทางด้านความมั่นคงปลอดภัยตลอดวงจรการพัฒนาผลิตภัณฑ์ ตั้งแต่การกำหนดข้อกำหนด การออกแบบ การพัฒนา การทดสอบ การบริหารช่องโหว่ การออกชุดปรับปรุง และการดูแลผลิตภัณฑ์ภายหลังการเผยแพร่ โดยระดับของกระบวนการและหลักฐานควรเหมาะสมกับลักษณะและความเสี่ยงของผลิตภัณฑ์
การปรับปรุงด้านความมั่นคงปลอดภัย	สามารถจัดทำ ทดสอบ และเผยแพร่ **ชุดปรับปรุงด้านความมั่นคงปลอดภัยสำหรับเฟิร์มแวร์หรือซอฟต์แวร์ (Firmware/Software Security Update)** พร้อมข้อมูลรุ่นที่ได้รับผลกระทบและแนวทางการนำไปใช้ได้หรือไม่
การบริหารช่องโหว่	สามารถรับทราบ ตรวจสอบ ประเมิน แก้ไข สื่อสาร และติดตามช่องโหว่ได้หรือไม่
การบริหารส่วนประกอบ	สามารถบริหารความเสี่ยงจากซอฟต์แวร์และส่วนประกอบจากบุคคลที่สามได้หรือไม่
แหล่งที่มาและความถูกต้อง (Provenance and Integrity)	สามารถตรวจสอบแหล่งที่มา รุ่น และความถูกต้องขององค์ประกอบสำคัญได้ตามความเหมาะสมหรือไม่
วงจรการสนับสนุน	มีข้อมูลระยะเวลาการสนับสนุนและการสิ้นสุดการสนับสนุน (End of Support) หรือไม่
การสนับสนุนเมื่อเกิดเหตุ	มีช่องทางและความสามารถในการสนับสนุนเมื่อพบเหตุหรือปัญหาด้านความมั่นคงปลอดภัยหรือไม่

ประเด็น	สิ่งที่ควรพิจารณา
การพึ่งพาบุคคลที่สาม	สามารถบริหารความเสี่ยงจากผู้ส่งมอบหรือบริการที่ผลิตภัณฑ์พึ่งพาได้หรือไม่
ข้อมูลหรือหลักฐานที่จำเป็น	มีข้อมูลหรือหลักฐานเพียงพอให้องค์กรประเมินและบริหารความเสี่ยงได้หรือไม่
ความถูกต้องและแหล่งที่มาของซอฟต์แวร์และชุดปรับปรุง (Software and Update Integrity)	ผลิตภัณฑ์ควรมีกลไกที่เหมาะสมสำหรับตรวจสอบความถูกต้องและแหล่งที่มาของ **เฟิร์มแวร์ ซอฟต์แวร์ หรือชุดปรับปรุง** ก่อนนำไปติดตั้ง เช่น การลงลายมือชื่อรหัสดิจิทัล (Code Signing) การตรวจสอบลายมือชื่อดิจิทัล หรือกลไกอื่นที่ให้ระดับความเชื่อมั่นเทียบเท่าตามความเหมาะสม
การตอบสนองด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ (Product Security Response)	ผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการควรมีผู้รับผิดชอบหรือกระบวนการสำหรับการตอบสนองด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ เช่น ทีมตอบสนองเหตุด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ (Product Security Incident Response Team: PSIRT) หรือกลไกที่มีหน้าที่เทียบเท่า โดยควรครอบคลุมการรับแจ้งช่องโหว่ การประสานการเปิดเผยช่องโหว่ (Coordinated Vulnerability Disclosure: CVD) การสื่อสารคำแนะนำด้านความมั่นคงปลอดภัย (Security Advisory) และการติดตามสถานะการแก้ไข

หลักฐานอาจอยู่ในรูปกระบวนการพัฒนาที่มั่นคงปลอดภัย ประวัติการปรับปรุง กระบวนการบริหารช่องโหว่ ข้อมูลวงจรชีวิตผลิตภัณฑ์ รายงานการทดสอบ การประเมินจากบุคคลที่สาม หรือการรับรองตามมาตรฐานที่เกี่ยวข้อง

การรับรอง (Certification) สามารถใช้เป็นหลักฐานการสร้างความเชื่อมั่น (Assurance Evidence) ได้ แต่ไม่ควรใช้เป็นหลักฐานเพียงอย่างเดียวในการสรุปว่าผลิตภัณฑ์เหมาะสมกับกรณีใช้งานและความเสี่ยงขององค์กร มาตรฐาน **ISO/IEC 27036 series** สามารถใช้เป็นกรอบอ้างอิงสำหรับการบริหารความสัมพันธ์กับผู้ส่งมอบและความมั่นคงปลอดภัยของห่วงโซ่อุปทานตามความเกี่ยวข้อง

3.7.2 การบริหารส่วนประกอบซอฟต์แวร์และความโปร่งใสของห่วงโซ่อุปทาน

ผลิตภัณฑ์ CCTV-AI อาจประกอบด้วยซอฟต์แวร์ ไลบรารี ส่วนประกอบโอเพนซอร์ส ส่วนประกอบจากบุคคลที่สาม และบริการภายนอกจำนวนมาก ช่องโหว่หรือการเปลี่ยนแปลงขององค์ประกอบเหล่านี้อาจส่งผลต่อความมั่นคงปลอดภัยของผลิตภัณฑ์โดยรวม

ผู้ผลิต ผู้พัฒนา และผู้ให้บริการควรมีกระบวนการที่สามารถ **ระบุส่วนประกอบที่เกี่ยวข้อง ⟶ ตรวจสอบช่องโหว่ ⟶ ประเมินผลกระทบต่อผลิตภัณฑ์ ⟶ แก้ไขหรือลดความเสี่ยง ⟶ สื่อสารข้อมูลที่จำเป็นแก่ผู้ใช้งาน**

การบริหารควรครอบคลุมตามความเหมาะสม เช่น ส่วนประกอบจากบุคคลที่สาม ส่วนประกอบโอเพนซอร์ส รุ่นและการพึ่งพา (Version and Dependency) ช่องโหว่ที่เกี่ยวข้อง แหล่งที่มาและความถูกต้อง และการเปลี่ยนแปลงองค์ประกอบสำคัญ

องค์กรผู้ใช้งาน **ไม่จำเป็นต้องได้รับรายละเอียดส่วนประกอบทั้งหมดของผลิตภัณฑ์ในทุกกรณี** แต่ควรมีข้อมูล หลักฐาน หรือการสร้างความเชื่อมั่นที่เพียงพอว่าผู้ผลิตหรือผู้ให้บริการสามารถบริหารความเสี่ยงจากส่วนประกอบและห่วงโซ่อุปทานได้อย่างเหมาะสม

ข้อมูลบางประเภทอาจได้รับผ่านข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA) การเข้าถึงแบบจำกัด การประเมิน ณ สถานที่ของผู้ผลิต หรือหลักฐานจากบุคคลที่สาม โดยระดับของข้อมูลและหลักฐานควรได้สัดส่วนกับความสำคัญและความเสี่ยงของระบบ

แนวทางดังกล่าวสามารถพิจารณาร่วมกับ **ISO/IEC 27036 series** สำหรับการบริหารความมั่นคงปลอดภัยของความสัมพันธ์กับผู้ส่งมอบและห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Supply Chain Security) และอาจพิจารณา **ISO 28000:2022** เป็นกรอบเสริมสำหรับระบบบริหารความมั่นคงปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security Management System) ตามลักษณะองค์กรและความเกี่ยวข้อง

ระดับและรายละเอียดของข้อมูลที่เปิดเผยแก่ผู้ใช้งานควรได้สัดส่วนกับระดับผลกระทบ ความเสี่ยง และความจำเป็นในการประเมินความมั่นคงปลอดภัยของระบบ โดยผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการควรจัดให้มีข้อมูลหรือหลักฐานที่เพียงพอสำหรับการประเมินและบริหารความเสี่ยงที่เกี่ยวข้องกับส่วนประกอบซอฟต์แวร์และห่วงโซ่อุปทาน

ข้อมูลดังกล่าวอาจครอบคลุมข้อมูลเกี่ยวกับส่วนประกอบซอฟต์แวร์ที่สำคัญ ส่วนประกอบจากบุคคลที่สามหรือโอเพนซอร์ส รุ่นและการพึ่งพาที่เกี่ยวข้อง ช่องโหว่ที่ทราบและมีผลกระทบต่อผลิตภัณฑ์ การปรับปรุงด้านความมั่นคงปลอดภัย และระยะเวลาการสนับสนุน ตามความเหมาะสมและระดับความเสี่ยง
ทั้งนี้ ไม่จำเป็นต้องเปิดเผยรายละเอียดทั้งหมดของผู้ส่งมอบ ส่วนประกอบซอฟต์แวร์ ซอร์สโค้ด หรือข้อมูลที่เป็นความลับทางการค้า เว้นแต่กฎหมาย ข้อกำหนดในการจัดซื้อ สัญญา หรือผลการประเมินความเสี่ยงกำหนดให้มีการเปิดเผยเพิ่มเติม โดยอาจกำหนดรูปแบบและเงื่อนไขการเปิดเผยข้อมูลให้เหมาะสมกับระดับความอ่อนไหวของข้อมูลดังกล่าว

หลักสำคัญคือ **ระดับความโปร่งใสควรเพียงพอให้ผู้ใช้งานสามารถประเมินและบริหารความเสี่ยงได้ โดยไม่จำเป็นต้องเปิดเผยรายละเอียดทางเทคนิคหรือข้อมูลห่วงโซ่อุปทานทั้งหมดโดยไม่มีความจำเป็น**

3.7.3 การจัดการและการเปิดเผยช่องโหว่

การมีช่องทางสำหรับรับแจ้งช่องโหว่เพียงอย่างเดียวไม่เพียงพอต่อการบริหารความเสี่ยง ผู้ผลิต ผู้พัฒนา และผู้ให้บริการควรมีกระบวนการที่ครอบคลุมตั้งแต่การค้นพบหรือรับทราบช่องโหว่ การตรวจสอบและประเมินผลกระทบ การจัดลำดับและแก้ไข การสื่อสาร ตลอดจนการทวนสอบและติดตามผล

กระบวนการโดยรวมอาจพิจารณาตามลำดับดังนี้ **ค้นพบหรือรับแจ้ง ⟶ ตรวจสอบ ⟶ ประเมิน ⟶ จัดลำดับ ⟶ แก้ไขหรือลดความเสี่ยง ⟶ สื่อสาร ⟶ ทวนสอบ ⟶ ปิดประเด็น**

การค้นพบและรับข้อมูลช่องโหว่

ช่องโหว่อาจถูกค้นพบจากการทดสอบภายใน นักวิจัยด้านความมั่นคงปลอดภัย ลูกค้า บุคคลที่สาม หรือแหล่งข้อมูลข่าวกรองด้านช่องโหว่ที่น่าเชื่อถือ จึงควรมีกระบวนการรับและติดตามข้อมูลจากหลายแหล่งตามความเหมาะสม

การตรวจสอบและประเมินผลกระทบ

ควรตรวจสอบว่าช่องโหว่มีอยู่จริงหรือไม่ และระบุผลิตภัณฑ์ รุ่น หรือองค์ประกอบที่ได้รับผลกระทบก่อนประเมินความรุนแรง ความสามารถในการโจมตี และผลกระทบที่อาจเกิดขึ้น

การจัดลำดับและแก้ไข

การจัดลำดับไม่ควรพิจารณาจากคะแนนความรุนแรงเพียงอย่างเดียว แต่ควรพิจารณาความสามารถในการโจมตี การมีหลักฐานการโจมตีจริง ลักษณะผลิตภัณฑ์ และผลกระทบต่อระบบที่นำผลิตภัณฑ์ไปใช้

การแก้ไขอาจเป็นชุดปรับปรุงด้านความมั่นคงปลอดภัย (Security Update) ชุดปรับปรุงเฟิร์มแวร์ (Firmware Update) คำแนะนำในการกำหนดค่า (Configuration Guidance) หรือมาตรการลดความเสี่ยงอื่น หากยังไม่สามารถแก้ไขได้ทันที ควรมีมาตรการชั่วคราวที่เหมาะสม

การสื่อสารช่องโหว่

ควรสื่อสารข้อมูลที่จำเป็นให้ผู้ใช้งานสามารถทราบได้อย่างน้อยว่า **ผลิตภัณฑ์หรือรุ่นใดได้รับผลกระทบ ผลกระทบสำคัญคืออะไร และควรดำเนินการอย่างไร** โดยคำนึงถึงความเสี่ยงจากการเปิดเผยข้อมูลทางเทคนิคที่อาจถูกนำไปใช้โจมตีด้วย

การทวนสอบและติดตามผล

ภายหลังการแก้ไข ควรทวนสอบว่ามาตรการสามารถลดหรือขจัดช่องโหว่ได้ตามที่คาดหมาย และไม่ก่อให้เกิดผลกระทบที่ไม่ยอมรับต่อการทำงานของระบบ

การดำเนินการดังกล่าวสามารถประยุกต์ใช้มาตรฐาน **ISO/IEC 29147** สำหรับกระบวนการเปิดเผยช่องโหว่ (Vulnerability Disclosure) และ **ISO/IEC 30111** สำหรับกระบวนการจัดการช่องโหว่ (Vulnerability Handling Processes) ตามความเกี่ยวข้อง โดยเฉพาะสำหรับผู้ผลิต ผู้พัฒนา และผู้ให้บริการที่ต้องรับ ตรวจสอบ วิเคราะห์ แก้ไข และสื่อสารข้อมูลช่องโหว่ของผลิตภัณฑ์หรือบริการ

หากพบว่าช่องโหว่ถูกนำไปใช้โจมตีแล้ว หรือมีเหตุอันควรสงสัยว่าระบบถูกบุกรุก ควรยกระดับจากการบริหารช่องโหว่ไปสู่กระบวนการตอบสนองเหตุการณ์ตามข้อ 3.10

3.7.4 ความน่าเชื่อถือและการควบคุมแบบจำลอง AI

แบบจำลอง AI เป็นองค์ประกอบหนึ่งที่อาจมีผลโดยตรงต่อสมรรถนะและความเสี่ยงของ CCTV-AI องค์กรจึงควรมีข้อมูลหรือหลักฐานเพียงพอที่จะทราบว่า **ระบบกำลังใช้ AI ใด มาจากแหล่งใด มีการเปลี่ยนแปลงหรือไม่ และยังเหมาะสมกับวัตถุประสงค์และความเสี่ยงที่ยอมรับไว้หรือไม่**

ควรพิจารณาตามความเหมาะสมใน 4 ด้าน ได้แก่

1. **การระบุและแหล่งที่มา (Identification and Provenance)** — สามารถระบุแบบจำลอง รุ่น หรือความสามารถสำคัญและแหล่งที่มาได้ในระดับที่จำเป็น
2. **ความถูกต้องและการควบคุมการเปลี่ยนแปลง (Integrity and Change Control)** — ป้องกันการแก้ไขหรือเปลี่ยนแบบจำลองโดยไม่ได้รับอนุญาต และนำการเปลี่ยนแปลงที่สำคัญเข้าสู่กระบวนการตามข้อ 3.4
3. **การพึ่งพา AI จากบุคคลที่สาม (Third-Party AI Dependency)** — พิจารณาความเสี่ยงจากแบบจำลองหรือบริการ AI ที่ผลิตภัณฑ์หรือระบบพึ่งพา รวมถึงการเปลี่ยนแปลงจากผู้ให้บริการ
4. **การสร้างความเชื่อมั่น (Model Assurance)** — มีผลการทดสอบ ข้อมูลสมรรถนะ ข้อจำกัด หรือหลักฐานอื่นที่เหมาะสมกับกรณีใช้งานและระดับความเสี่ยง

แนวปฏิบัตินี้มิได้กำหนดให้ผู้ผลิตต้องเปิดเผยรหัสต้นฉบับ (Source Code) น้ำหนักของแบบจำลอง (Model Weights) หรือข้อมูลฝึกสอนทั้งหมดโดยอัตโนมัติ แต่ควรมีข้อมูลหรือหลักฐานเพียงพอสำหรับการประเมินความน่าเชื่อถือและบริหารความเสี่ยงตามระดับผลกระทบ

สามารถพิจารณาหลักการจาก **ISO/IEC 42001, ISO/IEC 23894, ISO/IEC TR 24028 และ ISO/IEC 25059** รวมถึงมาตรฐานด้านระบบเฝ้าระวังด้วยวิดีโอที่เกี่ยวข้องตามกรณีใช้งาน

รูปที่ 4 ห่วงโซ่ความน่าเชื่อถือของระบบ CCTV ที่ใช้ AI

ความมั่นคงปลอดภัยของระบบขึ้นอยู่กับความน่าเชื่อถือและการบริหารความเสี่ยงขององค์ประกอบตลอดห่วงโซ่ ตั้งแต่อุปกรณ์จนถึงบริการและผู้ให้บริการที่เกี่ยวข้อง

3.8 การสำรองข้อมูล การกู้คืน และความต่อเนื่องทางธุรกิจ

การสำรองและกู้คืนระบบ CCTV ที่ใช้ AI ควรครอบคลุมองค์ประกอบที่จำเป็นต่อการทำให้ระบบกลับสู่สถานะที่ได้รับอนุมัติและเชื่อถือได้ (Approved and Trusted State) มิใช่เพียงการกู้คืนภาพ วิดีโอ หรือทำให้อุปกรณ์สามารถกลับมาเปิดใช้งานได้

องค์กรควรพิจารณาขอบเขตการสำรอง การกู้คืน และความต่อเนื่องตามความสำคัญของระบบ ผลกระทบด้านข้อมูล ผลกระทบจาก AI และการพึ่งพาระบบหรือบริการอื่นตามข้อ 3.1

3.8.1 ขอบเขตการกู้คืน

องค์ประกอบที่จำเป็นต่อการกู้คืนอาจแตกต่างกันตามสถาปัตยกรรมและกรณีใช้งาน โดยควรพิจารณาอย่างน้อยดังนี้

องค์ประกอบ	ประเด็นที่ควรพิจารณา
การตั้งค่าระบบ (Configuration)	การตั้งค่าที่จำเป็นต่อการกลับสู่สถานะที่ได้รับอนุมัติ
แบบจำลองและความสามารถของ AI (AI Model and AI Capability)	รุ่น ความสามารถ หรือองค์ประกอบ AI ที่จำเป็นต่อการให้บริการ
กฎและค่าที่สำคัญ	พื้นที่วิเคราะห์ กฎ และค่าเกณฑ์ (Analytics Zone, Rule and Threshold) หรือค่าที่มีผลต่อผลลัพธ์
การเชื่อมต่อ (Integration)	การเชื่อมต่อ API กระบวนงานอัตโนมัติ และบัญชีบริการ (API, Workflow and Service Account) และการเชื่อมต่อกับระบบอื่น
ข้อมูล (Data)	ข้อมูลที่จำเป็นต่อการดำเนินงานตามวัตถุประสงค์และข้อกำหนด
หลักฐานที่สำคัญ	Logs หรือข้อมูลที่จำเป็นต่อการตรวจสอบหรือการตอบสนองเหตุการณ์
ข้อมูลรับรองและสิทธิ	ข้อมูลรับรอง ใบรับรองดิจิทัล และกุญแจ (Credentials, Certificate and Key) ที่จำเป็น โดยต้องมีการคุ้มครองที่เหมาะสม

การสำรององค์ประกอบทุกประเภทไม่จำเป็นสำหรับทุกระบบ ขอบเขตควรกำหนดตามความจำเป็นในการกู้คืนและระดับความเสี่ยง

3.8.2 การลดข้อมูลในการสำรอง

การสำรองข้อมูลทำให้เกิดสำเนาของข้อมูลเพิ่มเติมและอาจเพิ่มพื้นที่การโจมตีหรือผลกระทบจากการเปิดเผยข้อมูล องค์กรจึงไม่ควรสำรองข้อมูลทุกประเภทโดยอัตโนมัติเพียงเพราะระบบสามารถดำเนินการได้

ควรพิจารณาความจำเป็นเป็นพิเศษสำหรับข้อมูล เช่น ข้อมูลชีวมิติ (Biometric Data) แม่แบบชีวมิติ ข้อมูลการติดตาม ข้อมูลที่ AI สร้างหรืออนุมาน และข้อมูลที่มีผลกระทบสูง

ข้อมูลสำรองควรได้รับการคุ้มครองและกำหนดระยะเวลาการเก็บรักษาตามประเภทข้อมูล วัตถุประสงค์ และข้อกำหนดที่เกี่ยวข้อง

3.8.3 การทวนสอบภายหลังการกู้คืน

การกู้คืนไม่ควรถือว่าสำเร็จเพียงเพราะระบบสามารถเปิดใช้งานได้ องค์กรควรทวนสอบองค์ประกอบที่มีผลต่อความมั่นคงปลอดภัยและความน่าเชื่อถือ เช่น **รุ่นเฟิร์มแวร์และซอฟต์แวร์ ⟶ แบบจำลอง AI ⟶ การตั้งค่าด้านความมั่นคงปลอดภัย ⟶ บัญชีและสิทธิการเข้าถึง ⟶ ความสามารถและกฎของ AI ⟶ ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) และการเชื่อมต่อ ⟶ การบันทึกเหตุการณ์และการเฝ้าระวัง ⟶ สมรรถนะของ AI**

สำหรับระบบที่มีผลกระทบสูง ควรยืนยันว่าระบบกลับสู่ **สถานะที่ได้รับอนุมัติและเชื่อถือได้ (Approved and Trusted State)** ก่อนกลับเข้าสู่การดำเนินงานตามปกติ

3.8.4 การดำเนินงานเมื่อ AI ไม่พร้อมใช้งาน

องค์กรควรกำหนดล่วงหน้าว่าระบบจะดำเนินงานอย่างไรเมื่อ AI ไม่พร้อมใช้งานหรือไม่สามารถเชื่อถือผลลัพธ์ได้ โดยระดับของมาตรการควรสัมพันธ์กับความสำคัญและผลกระทบของระบบ

แนวทางอาจประกอบด้วย **การทำงานด้วย AI ตามปกติ ⟶ การทำงานแบบจำกัด (Degraded Mode) ⟶ CCTV พื้นฐาน ⟶ การตรวจสอบโดยบุคคล ⟶ สภาวะปลอดภัย (Fail-Safe)**

ในบางกรณี การระงับความสามารถของ AI ชั่วคราวและกลับไปใช้ CCTV พื้นฐานหรือการตรวจสอบโดยบุคคล อาจมีความปลอดภัยมากกว่าการปล่อยให้ระบบใช้ผลลัพธ์ AI ที่ไม่สามารถเชื่อถือได้ต่อไป

3.8.5 ความต่อเนื่องของระบบที่เชื่อมต่อ

กรณีผลลัพธ์จาก AI ถูกส่งไปยังระบบอื่น องค์กรควรกำหนดพฤติกรรมของระบบเมื่อ AI หรือการเชื่อมต่อไม่พร้อมใช้งาน เช่น

- ระบบปลายทางจะดำเนินการอย่างไรเมื่อไม่ได้รับผลลัพธ์
- ผลลัพธ์เก่าหรือไม่สมบูรณ์สามารถนำไปใช้ต่อได้หรือไม่
- ต้องให้บุคคลอนุมัติก่อนดำเนินการหรือไม่
- กระบวนงานอัตโนมัติ (Workflow) หรือ การดำเนินการอัตโนมัติ (Automated Action) สามารถระงับได้หรือไม่
- การกลับเข้าสู่การทำงานตามปกติต้องผ่านการทวนสอบใด

ไม่ควรออกแบบให้ความล้มเหลวของ AI ทำให้ระบบที่เชื่อมต่อเข้าสู่สถานะที่ก่อให้เกิดผลกระทบสูงโดยไม่มีมาตรการควบคุม

3.8.6 การพึ่งพาบริการคลาวด์และบริการภายนอก

กรณีระบบพึ่งพาบริการคลาวด์หรือบริการ AI ภายนอก ควรพิจารณาความต่อเนื่องกรณีบริการไม่พร้อมใช้งาน เครือข่ายขัดข้อง ผู้ให้บริการเปลี่ยนแปลงหรือยุติบริการ หรือผลิตภัณฑ์สิ้นสุดการสนับสนุน

สำหรับระบบที่มีความสำคัญหรือผลกระทบสูง ควรพิจารณาความสามารถในการนำข้อมูลและการตั้งค่าที่จำเป็นออกจากบริการ ตลอดจนแนวทางเปลี่ยนหรือยุติบริการ (Exit Strategy) ตามความเหมาะสม

ในกรณีที่ระบบ CCTV ที่ใช้ AI พึ่งพาบริการคลาวด์ บริการ AI หรือบริการภายนอก องค์กรควรพิจารณาการพึ่งพาดังกล่าวร่วมกับสถานที่จัดเก็บข้อมูล (Data Location) สถานที่ประมวลผลข้อมูล (Processing Location) เขตอำนาจทางกฎหมาย (Jurisdiction) การเข้าถึงข้อมูลจากภายนอกหรือจากต่างประเทศ และการพึ่งพาผู้ให้บริการช่วง (Subprocessor) ตามความเกี่ยวข้อง

การประเมินความต่อเนื่องของบริการควรพิจารณาความเสี่ยงที่เกิดจากการเปลี่ยนแปลงหรือการหยุดให้บริการของผู้ให้บริการภายนอก รวมถึงความสามารถในการสำรองและกู้คืนข้อมูล การเคลื่อนย้ายข้อมูลหรือภาระงาน การเปลี่ยนผู้ให้บริการ และการดำเนินงานในกรณีที่บริการภายนอกไม่สามารถใช้งานได้ตามระดับความสำคัญของระบบ

3.8.7 การทดสอบการกู้คืนและความต่อเนื่อง

การสำรองข้อมูลหรือมีแผนความต่อเนื่องโดยไม่ได้ทดสอบอาจไม่เพียงพอต่อการยืนยันว่าระบบสามารถกู้คืนได้จริง องค์กรจึงควรทดสอบตามระดับความสำคัญและความเสี่ยง โดยพิจารณาอย่างน้อย **กู้คืน ⟶ ตรวจสอบการตั้งค่า ⟶ ตรวจสอบ AI ⟶ ตรวจสอบการเชื่อมต่อ ⟶ ตรวจสอบความมั่นคงปลอดภัย ⟶ กลับเข้าสู่บริการ**

สำหรับระบบที่มีผลกระทบสูง ควรทดสอบการทำงานแบบจำกัด การดำเนินงานโดยบุคคล หรือสภาวะปลอดภัยตามที่ออกแบบไว้ด้วย

หลักสำคัญ เป้าหมายของการกู้คืน CCTV ที่ใช้ AI ไม่ใช่เพียงทำให้ระบบ “กลับมาเปิดใช้งานได้” แต่ต้องสามารถกลับสู่สถานะที่ได้รับอนุมัติและเชื่อถือได้ พร้อมมีแนวทางดำเนินงานที่ปลอดภัยเมื่อ AI ไม่พร้อมใช้งาน

3.9 การเลิกใช้อุปกรณ์และการทำลายข้อมูล

การเลิกใช้ระบบ CCTV ที่ใช้ AI ควรครอบคลุมมากกว่าการถอดกล้อง ปิดระบบ หรือลบภาพและวิดีโอ เนื่องจากข้อมูลและองค์ประกอบที่เกี่ยวข้องกับ AI อาจยังคงอยู่ในอุปกรณ์ ระบบจัดเก็บข้อมูล บริการคลาวด์ ระบบที่เชื่อมต่อ หรือบัญชีของผู้ให้บริการ

องค์กรควรกำหนดขอบเขตการเลิกใช้งานให้ครอบคลุม **อุปกรณ์ ข้อมูล AI บัญชีและสิทธิ การเชื่อมต่อ และบริการภายนอก** ตามความเกี่ยวข้อง

3.9.1 ขอบเขตการเลิกใช้งาน

ก่อนเลิกใช้งาน ควรระบุองค์ประกอบที่เกี่ยวข้องตามสถาปัตยกรรมและกรณีใช้งาน อย่างน้อยตามความเหมาะสม ได้แก่

- อุปกรณ์และสื่อจัดเก็บข้อมูล
- ภาพและวิดีโอ
- ข้อมูลประกอบ (Metadata) และผลลัพธ์จาก AI
- ข้อมูลที่ AI สร้างหรืออนุมาน (Derived or Inferred Data)
- ข้อมูลชีวมิติและแม่แบบชีวมิติ (Biometric Template)
- แบบจำลองหรือองค์ประกอบของ AI

- การตั้งค่าและข้อมูลรับรอง
- บัญชีผู้ใช้และบัญชีบริการ (Service Account)
- โทเคนหรือกุญแจสำหรับ API (API Token/Key) และใบรับรองดิจิทัล (Certificate)
- ข้อมูลสำรอง
- ข้อมูลหรือสำเนาที่จัดเก็บโดยผู้ให้บริการภายนอกหรือผู้ให้บริการช่วง (Subprocessor)

ขอบเขตการเลิกใช้งานควรสอดคล้องกับการไหลของข้อมูล (Data Flow) และสถาปัตยกรรมของระบบ เพื่อป้องกันการหลงเหลือของข้อมูล บัญชี สิทธิ หรือการเชื่อมต่อที่ไม่จำเป็น

3.9.2 การลบและทำลายข้อมูล

การลบหรือทำลายข้อมูลควรพิจารณาแยกตามประเภทข้อมูล วัตถุประสงค์ ระยะเวลาการเก็บรักษา และข้อกำหนดที่มีผลใช้บังคับ

โดยเฉพาะอย่างยิ่ง การลบภาพหรือวิดีโอต้นฉบับไม่ได้หมายความว่า **ข้อมูลประกอบ (Metadata) ผลลัพธ์จาก AI (AI Output) ข้อมูลการติดตาม (Tracking Data) แม่แบบชีวมิติ (Biometric Template) หรือข้อมูลที่ได้จากการวิเคราะห์หรืออนุมาน (Derived or Inferred Data)** ถูกลบไปพร้อมกันโดยอัตโนมัติ

องค์กรควรตรวจสอบว่าข้อมูลแต่ละประเภทถูกจัดเก็บไว้ที่ใด และดำเนินการลบ ทำลาย หรือคงไว้ตามข้อกำหนดที่เกี่ยวข้อง

กรณีจำเป็นต้องเก็บข้อมูลไว้เพื่อวัตถุประสงค์ทางกฎหมาย การตรวจสอบ หรือการสอบสวน ควรแยกข้อมูลดังกล่าวและกำหนดการคุ้มครองที่เหมาะสม

3.9.3 การยกเลิกบัญชี สิทธิ และการเชื่อมต่อ

การเลิกใช้งานควรรวมถึงการยกเลิกสิทธิและการเชื่อมต่อที่เกี่ยวข้อง เช่น **บัญชีผู้ใช้ ⟶ บัญชีบริการ (Service Account) ⟶ API ⟶ โทเคนหรือกุญแจ (Token/Key) ⟶ ใบรับรองดิจิทัล (Certificate) ⟶ กระบวนงานอัตโนมัติ (Workflow) ⟶ ระบบที่เชื่อมต่อ**

ไม่ควรปล่อยให้บัญชี บริการ หรือช่องทางการเชื่อมต่อของระบบที่เลิกใช้แล้วยังคงสามารถเข้าถึงระบบอื่นได้

กรณี AI หรือระบบอัตโนมัติได้รับสิทธิในการเรียกใช้เครื่องมือหรือดำเนินการต่อ ควรยกเลิกสิทธิและขอบเขตการดำเนินการ (Action Boundary) ที่เกี่ยวข้องด้วย

3.9.4 การเลิกใช้แบบจำลอง AI และส่วนประกอบซอฟต์แวร์

เมื่อเลิกใช้หรือเปลี่ยนแบบจำลอง AI องค์กรควรป้องกันไม่ให้แบบจำลองหรือองค์ประกอบที่ถูกยกเลิกกลับมาใช้งานโดยไม่ได้รับอนุญาตหรือโดยความผิดพลาด

หากจำเป็นต้องเก็บแบบจำลอง รุ่น การตั้งค่า หรือองค์ประกอบเดิมไว้เพื่อการตรวจสอบ การสอบสวน หรือการทวนสอบย้อนหลัง ควรกำหนดสถานะให้ชัดเจนและจำกัดการเข้าถึงตามความเหมาะสม

ไม่จำเป็นต้องเก็บแบบจำลองหรือองค์ประกอบที่เลิกใช้แล้วทั้งหมดโดยอัตโนมัติ หากไม่มีความจำเป็นหรือข้อกำหนดรองรับ

3.9.5 การยุติบริการคลาวด์และบริการภายนอก

กรณีเลิกใช้บริการคลาวด์หรือบริการ AI ภายนอก ควรกำหนดกระบวนการตามความเหมาะสม เช่น **คืนข้อมูล (Data Return) ⟶ ลบข้อมูล (Data Deletion) ⟶ ยืนยันการลบตามความเหมาะสม ⟶ ยกเลิกสิทธิ ⟶ ยุติการเชื่อมต่อ**

ควรพิจารณาว่าข้อมูลอาจอยู่กับผู้ให้บริการช่วง (Subprocessor) หรือระบบสำรองของผู้ให้บริการด้วย สำหรับระบบที่มีผลกระทบสูง เงื่อนไขเกี่ยวกับการคืนและลบข้อมูล การยุติบริการ และการเปลี่ยนผู้ให้บริการควรได้รับการพิจารณาตั้งแต่ขั้นตอนการจัดซื้อจัดจ้างหรือทำสัญญา ไม่ควรรอจนถึงวันที่ต้องยุติบริการ

3.9.6 การทวนสอบการเลิกใช้งาน

ก่อนปิดกระบวนการเลิกใช้งาน ควรสามารถยืนยันได้ตามความเหมาะสมว่า **อุปกรณ์ถูกนำออกจากการใช้งาน ⟶ ข้อมูลถูกลบหรือคงไว้ตามข้อกำหนด ⟶ บัญชีและสิทธิถูกยกเลิก ⟶ ส่วนเชื่อมต่อ โทเคน กุญแจ และใบรับรองดิจิทัลที่เกี่ยวข้องถูกยกเลิก ⟶ ระบบปลายทางไม่ได้รับข้อมูลจากระบบเดิม ⟶ ผู้ให้บริการภายนอกดำเนินการตามเงื่อนไขที่กำหนด**

องค์กรสามารถใช้ Checklist หรือกระบวนการเลิกใช้งานที่มีอยู่ โดยไม่จำเป็นต้องจัดทำแบบฟอร์มเฉพาะสำหรับ CCTV-AI หากหลักฐานเดิมสามารถแสดงผลการดำเนินการและตรวจสอบย้อนหลังได้เพียงพอ

หลักสำคัญ การเลิกใช้ CCTV ที่ใช้ AI จะสมบูรณ์เมื่อ **“อุปกรณ์ ข้อมูล AI สิทธิ และการเชื่อมต่อ”** ที่ไม่จำเป็นได้รับการจัดการอย่างเหมาะสม มิใช่เพียงการปิดกล้องหรือลบวิดีโอออกจากระบบ

3.10 ภัยคุกคาม สัญญาณเตือน และการรับมือเหตุ

เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ CCTV ที่ใช้ AI อาจส่งผลมากกว่าการสูญเสียความลับ ความถูกต้อง หรือความพร้อมใช้งานของระบบ เนื่องจากการโจมตีหรือความผิดปกติอาจทำให้ AI สร้างผลลัพธ์ที่ไม่ถูกต้อง และผลลัพธ์ดังกล่าวอาจถูกนำไปใช้โดยบุคคล ระบบ หรือกระบวนการอัตโนมัติต่อไป

การตอบสนองเหตุการณ์จึงควรพิจารณาทั้ง **ระบบ ข้อมูล AI ผลลัพธ์ของ AI และระบบที่เชื่อมต่อ** โดยเฉพาะกรณีที่ผลลัพธ์สามารถนำไปสู่การตัดสินใจหรือการดำเนินการที่มีผลกระทบสูง

3.10.1 ภัยคุกคามที่เกี่ยวข้องกับ AI

องค์กรควรพิจารณาภัยคุกคามตามลักษณะและกรณีใช้งานของระบบ โดยไม่จำเป็นต้องใช้รายการภัยคุกคามเดียวกันสำหรับ CCTV-AI ทุกระบบ

ตัวอย่างภัยคุกคามที่ควรพิจารณา ได้แก่

ภัยคุกคาม	ตัวอย่างผลกระทบ
การดัดแปลงข้อมูลนำเข้า (Input Manipulation)	ทำให้ AI ตรวจไม่พบ ตรวจจับผิด หรือสร้างผลลัพธ์ที่คลาดเคลื่อน
การเปลี่ยนแปลง AI หรือการตั้งค่าโดยไม่ได้รับอนุญาต	เปลี่ยนพฤติกรรม ความสามารถ กฎ หรือผลลัพธ์ของระบบ
การโจมตีข้อมูลหรือกระบวนการเรียนรู้	ทำให้ AI เรียนรู้หรือปรับตัวจากข้อมูลที่ไม่เหมาะสม ในกรณีที่ระบบรองรับการเรียนรู้หรือปรับแบบจำลอง
ช่องโหว่ของซอฟต์แวร์หรือส่วนประกอบ	ใช้ช่องโหว่เพื่อเข้าถึง ควบคุม หรือเปลี่ยนแปลงระบบ
การโจมตีห่วงโซ่อุปทาน (Supply Chain Attack)	กระทบอุปกรณ์ เฟิร์มแวร์ ซอฟต์แวร์ AI หรือบริการที่ระบบพึ่งพา
การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	เปิดเผยหรือใช้ภาพ วิดีโอ ข้อมูลชีวมิติ หรือผลลัพธ์ AI โดยมิชอบ
การใช้ความสามารถของ AI โดยไม่ได้รับอนุญาต	เปิดใช้การติดตาม การระบุ หรือการวิเคราะห์ที่ไม่ได้รับอนุมัติ
การโจมตีบริการภายนอก	กระทบ Cloud, External AI Service หรือระบบที่เชื่อมต่อ

ความผิดพลาด เช่น การแจ้งเตือนผิด (False Positive) การตรวจไม่พบ (False Negative) หรือการระบุบุคคลผิด (Misidentification) **ไม่จำเป็นต้องเกิดจากการโจมตีเสมอไป** แต่หากมีรูปแบบผิดปกติหรือเปลี่ยนแปลงอย่างมีนัยสำคัญ ควรได้รับการตรวจสอบว่าเกิดจากข้อจำกัดของ AI การเปลี่ยนแปลงสภาพแวดล้อม ความผิดพลาดของระบบ หรือเหตุด้านความมั่นคงปลอดภัย

3.10.2 สัญญาณที่ควรได้รับการตรวจสอบ

ตัวอย่างเหตุการณ์หรือสัญญาณที่ควรได้รับการตรวจสอบตามระดับความเสี่ยง ได้แก่

- แบบจำลอง AI หรือการตั้งค่าที่สำคัญถูกเปลี่ยนโดยไม่ได้รับอนุญาต
- พบ Firmware, Software หรือองค์ประกอบที่ไม่ทราบแหล่งที่มาหรือไม่ตรงกับสถานะที่ได้รับอนุมัติ
- มีการเปิดใช้ความสามารถ AI ที่ไม่ได้รับอนุมัติ

- ผลลัพธ์หรือสมรรถนะของ AI เปลี่ยนแปลงอย่างมีนัยสำคัญโดยไม่มีเหตุผลที่ทราบ
- มีการเข้าถึง ส่งออก หรือใช้ข้อมูลชีวมิติหรือข้อมูลที่มีผลกระทบสูงอย่างผิดปกติ
- API หรือ Service Account มีรูปแบบการใช้งานผิดปกติ
- Workflow หรือ Automated Action ดำเนินการนอกขอบเขตที่ได้รับอนุมัติ
- ผู้ผลิตหรือผู้ให้บริการแจ้งเหตุการณ์ที่อาจส่งผลต่อผลิตภัณฑ์หรือบริการที่องค์กรใช้งาน
- มีเหตุอันควรสงสัยว่าช่องโหว่ที่เกี่ยวข้องกับระบบถูกนำไปใช้โจมตี

สัญญาณดังกล่าวไม่ควรถูกตีความว่าเป็นเหตุการณ์ด้านความมั่นคงปลอดภัยที่ได้รับการยืนยันแล้วทุกกรณี แต่ควรได้รับการวิเคราะห์และจัดระดับตามกระบวนการขององค์กร

3.10.3 การประเมินขอบเขตและผลกระทบของเหตุการณ์

เมื่อเกิดเหตุที่เกี่ยวข้องกับ CCTV-AI การวิเคราะห์ไม่ควรหยุดอยู่ที่คำถามว่าอุปกรณ์หรือระบบใดถูกโจมตี แต่ควรตรวจสอบผลกระทบต่อเนื่องตามความเหมาะสม **ระบบ ⟶ ข้อมูล ⟶ AI/การตั้งค่า ⟶ ผลลัพธ์ของ AI ⟶ บุคคลที่ได้รับผลกระทบ ⟶ ระบบที่เชื่อมต่อ ⟶ การดำเนินการที่เกิดขึ้น**

องค์กรควรพิจารณาว่า

- AI ถูกเปลี่ยนแปลงหรือได้รับผลกระทบหรือไม่
- ผลลัพธ์ในช่วงเวลาใดอาจไม่สามารถเชื่อถือได้
- ข้อมูลใดอาจถูกเปิดเผย เปลี่ยนแปลง หรือสูญหาย
- ผลลัพธ์ถูกส่งไปยังบุคคลหรือระบบใด
- มีการตัดสินใจหรือการดำเนินการใดเกิดขึ้นจากผลลัพธ์ดังกล่าวแล้วหรือไม่
- ผลกระทบสามารถขยายต่อไปยังระบบหรือภารกิจอื่นหรือไม่

แนวทางดังกล่าวช่วยให้องค์กรสามารถประเมิน **การขยายผลกระทบ (Impact Propagation)** ซึ่งเป็นประเด็นสำคัญของระบบ CCTV ที่ใช้ AI และเชื่อมต่อกับระบบอื่น

3.10.4 การจำกัดผลกระทบ

เมื่อมีเหตุอันควรสงสัยว่า AI หรือผลลัพธ์ไม่สามารถเชื่อถือได้ องค์กรควรสามารถจำกัดผลกระทบตามระดับความเสี่ยง

ตัวอย่างแนวทาง ได้แก่

- ระงับความสามารถของ AI ที่ได้รับผลกระทบ
- ระงับ Trigger, Workflow หรือ Automated Action
- จำกัดหรือยกเลิก API หรือ Service Account ที่เกี่ยวข้อง
- แยกระบบหรือองค์ประกอบที่ต้องสงสัย
- เปลี่ยนไปใช้การตรวจสอบโดยบุคคล

- ใช้รูปแบบการทำงานแบบจำกัด (Degraded Mode)
- เปลี่ยนเข้าสู่สภาวะปลอดภัย (Fail-Safe)

สำหรับระบบที่มีผลกระทบสูง ความสามารถในการ **หยุด จำกัด หรือแยกผลกระทบ** ควรได้รับการพิจารณาตั้งแต่ขั้นตอนการออกแบบ มิใช่รอจัดทำขึ้นภายหลังเกิดเหตุการณ์

ตัวอย่างการขยายผลกระทบที่ควรป้องกันคือ **ข้อมูลนำเข้าถูกดัดแปลง ⟶ AI วิเคราะห์ผิด ⟶ ระบบเชื่อถือผลลัพธ์ ⟶ Workflow ทำงาน ⟶ ระบบปลายทางดำเนินการผิด** หรือ **AI/Configuration ถูกเปลี่ยน ⟶ ผลลัพธ์ผิด ⟶ API ส่งต่อ ⟶ ระบบที่เชื่อมต่อดำเนินการ ⟶ ผลกระทบขยายออกจาก CCTV**

3.10.5 การตอบสนองและการกู้คืน

การตอบสนองเหตุการณ์สามารถใช้กระบวนการบริหารเหตุการณ์ด้านความมั่นคงปลอดภัยที่องค์กรมีอยู่ โดยเพิ่มประเด็นเฉพาะ CCTV-AI ตามความเกี่ยวข้อง

กระบวนการโดยรวมอาจประกอบด้วย **ตรวจพบ ⟶ วิเคราะห์ ⟶ จำกัดผลกระทบ ⟶ เก็บรักษาหลักฐาน ⟶ แก้ไข ⟶ กู้คืน ⟶ ทวนสอบ ⟶ ทบทวน** *(Detect ⟶ Analyze ⟶ Contain ⟶ Preserve Evidence ⟶ Remediate ⟶ Recover ⟶ Verify ⟶ Review)*

หลักฐานที่ควรพิจารณาเก็บรักษาตามลักษณะของเหตุอาจรวมถึง รุ่นของ AI การตั้งค่า Logs ผลลัพธ์ของ AI ข้อมูลการเชื่อมต่อ และการดำเนินการของระบบปลายทาง

ก่อนกลับเข้าสู่การดำเนินงานตามปกติ ควรทวนสอบว่าระบบกลับสู่ **สถานะที่ได้รับอนุมัติและเชื่อถือได้ (Approved and Trusted State)** ตามหลักการในข้อ 3.8

หากเหตุการณ์ทำให้วัตถุประสงค์ สมรรถนะ ความสามารถ หรือระดับความเสี่ยงของระบบเปลี่ยนแปลงอย่างมีนัยสำคัญ ควรพิจารณาประเมินใหม่ตามข้อ 3.1

3.10.6 ความสัมพันธ์ระหว่างช่องโหว่และเหตุการณ์

ควรแยกการบริหารช่องโหว่ออกจากการตอบสนองเหตุการณ์ให้ชัดเจน

พบช่องโหว่ แต่ยังไม่มีหลักฐานการโจมตี ⟶ ดำเนินการตามกระบวนการบริหารช่องโหว่ในข้อ 3.7.3

พบการใช้ประโยชน์จากช่องโหว่ หรือมีเหตุอันควรสงสัยว่าระบบถูกบุกรุก ⟶ ดำเนินการตามกระบวนการตอบสนองเหตุการณ์ในข้อ 3.10

ในกรณีหลัง องค์กรอาจต้องดำเนินการแก้ไขช่องโหว่ควบคู่กับการจำกัดผลกระทบ การเก็บรักษาหลักฐาน และการตรวจสอบขอบเขตของเหตุการณ์

หลักสำคัญ การตอบสนองเหตุการณ์ของ CCTV-AI ควรตอบได้ว่า**“ระบบใดได้รับผลกระทบ ⟶ AI ถูกกระทบหรือไม่ ⟶ ผลลัพธ์ใดอาจไม่น่าเชื่อถือ ⟶ ผลลัพธ์ถูกส่งไปที่ใด ⟶ และมีการดำเนินการใดเกิดขึ้นจากผลลัพธ์นั้นแล้วหรือไม่”**

3.11 การอบรมและสร้างความตระหนัก

บุคลากรที่เกี่ยวข้องกับระบบ CCTV ที่ใช้ AI ควรมีความรู้และความสามารถที่เหมาะสมกับบทบาท โดยไม่จำเป็นต้องเป็นผู้เชี่ยวชาญด้าน AI ทุกคน แต่ควรเข้าใจความสามารถ ข้อจำกัด ความเสี่ยง และหน้าที่ของตนในการใช้หรือบริหารระบบ

การอบรมควรพิจารณาตามบทบาท (Role-Based Training) และระดับผลกระทบของระบบ โดยใช้กระบวนการพัฒนาความรู้และความตระหนักที่องค์กรมีอยู่ได้

3.11.1 การอบรมตามบทบาท

บทบาท	ประเด็นที่ควรเข้าใจ
เจ้าของระบบ/ผู้บริหาร	วัตถุประสงค์ ผลกระทบ ความเสี่ยง การอนุมัติ และความรับผิดชอบ
ผู้ดูแลระบบ	Configuration, AI/Software Version, Access Control, Logs, Update, Backup และ Recovery
ผู้ปฏิบัติงาน	การตีความผลลัพธ์ ข้อจำกัดของ AI การทวนสอบ และการยกระดับเหตุ
ผู้ผลิต/ผู้พัฒนา/ผู้ติดตั้ง	การออกแบบ การทดสอบ การเปลี่ยนแปลง ช่องโหว่ และการส่งมอบอย่างมั่นคงปลอดภัย
ผู้จัดซื้อ/ผู้ประเมิน	ข้อกำหนด หลักฐานการสร้างความเชื่อมั่น การทดสอบ และเกณฑ์ตรวจรับ
ผู้รับผิดชอบด้าน Privacy/Compliance	วัตถุประสงค์ ข้อมูลส่วนบุคคล ข้อมูลชีวมิติ ผลกระทบ การเก็บรักษา และความโปร่งใส
ผู้รับผิดชอบเหตุการณ์	AI/Configuration/Logs ที่ต้องตรวจสอบ การจำกัดผลกระทบ และการตรวจสอบผลกระทบต่อระบบปลายทาง

3.11.2 ความเข้าใจข้อจำกัดของ AI

ผู้ที่ใช้ผลลัพธ์ของ AI ควรเข้าใจว่าประสิทธิภาพของระบบอาจได้รับผลจากปัจจัย เช่น คุณภาพของภาพ แสง มุม ระยะทาง การบดบัง สภาพแวดล้อม การเปลี่ยนแปลงของข้อมูล และข้อจำกัดของแบบจำลอง ค่าความเชื่อมั่น (Confidence Score) ไม่ควรถูกตีความว่าเป็นหลักฐานยืนยันว่าผลลัพธ์ถูกต้องโดยอัตโนมัติ

ผู้ปฏิบัติงานควรทราบว่าเมื่อใดควรตรวจสอบข้อมูลประกอบ ขอการยืนยันเพิ่มเติม หรือไม่ควรใช้ผลลัพธ์ของ AI ต่อ

3.11.3 การกำกับดูแลโดยมนุษย์ในการปฏิบัติงาน

บุคลากรที่มีหน้าที่กำกับดูแล AI ควรทราบ **เมื่อใดต้องตรวจสอบ ⟶ ต้องตรวจสอบอะไร ⟶ สามารถตัดสินใจหรือแทรกแซงได้เพียงใด ⟶ เมื่อใดต้องหยุดหรือจำกัด AI ⟶ เมื่อใดต้องยกระดับให้ผู้มีอำนาจ**

การอบรมควรช่วยลดความเสี่ยงจากการเชื่อผลลัพธ์ของระบบอัตโนมัติมากเกินไป (Automation Bias) โดยเฉพาะเมื่อ AI ถูกใช้สนับสนุนการตัดสินใจที่มีผลกระทบต่อบุคคลหรือภารกิจสำคัญ

3.11.4 ความตระหนักด้านข้อมูลและความเป็นส่วนตัว

ผู้เกี่ยวข้องควรเข้าใจว่า CCTV-AI อาจสร้างข้อมูลมากกว่าภาพและวิดีโอ เช่น Metadata, AI Output, Tracking Data, Derived/Inferred Data และ Biometric Data

การเข้าถึง ส่งออก เชื่อมโยง หรือใช้ข้อมูลเหล่านี้ควรเป็นไปตามวัตถุประสงค์ สิทธิ และข้อกำหนดที่เกี่ยวข้อง ไม่ควรถือว่าบุคคลที่สามารถดูภาพ CCTV ได้ย่อมสามารถใช้ข้อมูลหรือความสามารถ AI ทุกประเภทได้โดยอัตโนมัติ

3.11.5 ระบบที่เชื่อมต่อและการดำเนินการอัตโนมัติ

ผู้ปฏิบัติงานควรทราบว่าผลลัพธ์ของ AI ถูกส่งไปยังระบบใด และสามารถก่อให้เกิดการดำเนินการอะไรได้บ้าง โดยเฉพาะระบบที่มี Workflow, API หรือ Automated Action

บุคลากรที่เกี่ยวข้องควรทราบวิธีจำกัด ระงับ หรือเปลี่ยนเข้าสู่การดำเนินงานแบบจำกัดหรือสภาวะปลอดภัยเมื่อ AI ไม่สามารถเชื่อถือได้ ตามอำนาจหน้าที่ที่กำหนด

3.11.6 การทบทวนความรู้และการอบรม

การอบรมหรือการสื่อสารเพิ่มเติมควรได้รับการพิจารณาเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น วัตถุประสงค์ ความสามารถของ AI แบบจำลอง การเชื่อมต่อ ผู้ให้บริการ กระบวนการทำงาน หรือข้อกำหนดที่เกี่ยวข้อง รวมถึงเมื่อเกิดเหตุการณ์ที่แสดงว่าบุคลากรยังไม่เข้าใจความสามารถหรือข้อจำกัดของระบบอย่างเพียงพอ

องค์กรสามารถใช้กระบวนการอบรมและบันทึกความสามารถของบุคลากรที่มีอยู่ โดยไม่จำเป็นต้องสร้างหลักสูตรหรือแบบฟอร์มใหม่เฉพาะ CCTV-AI หากสามารถแสดงได้ว่าบุคลากรมีความรู้และความสามารถที่เหมาะสมกับหน้าที่

หลักการด้านความสามารถและความตระหนักสามารถพิจารณาร่วมกับ **ISO/IEC 42001** และหลักการบริหารความเสี่ยงตาม **ISO/IEC 23894** ตามความเกี่ยวข้อง

สรุปหลักการของบทที่ 3

การกำกับดูแลระบบ CCTV ที่ใช้ AI ควรเริ่มจากการกำหนดวัตถุประสงค์และบริบทของการใช้งาน แล้วประเมิน **ความสำคัญของระบบหรือภารกิจ (System/Mission Criticality) ผลกระทบด้านข้อมูล (Data Impact) ผลกระทบจากการใช้ AI (AI Impact)** และปัจจัยที่อาจขยายผลกระทบ เพื่อกำหนดมาตรการ การทดสอบ การกำกับดูแล และระดับการสร้างความเชื่อมั่นที่เหมาะสม

การบริหารตลอดวงจรชีวิตควรครอบคลุมความเป็นส่วนตัวและข้อมูลชีวมิติ การเปลี่ยนแปลงและการปรับปรุงระบบ การเฝ้าระวังและบันทึกเหตุการณ์ การบริหารช่องโหว่และห่วงโซ่อุปทาน การสำรองและกู้คืน การเลิกใช้งาน การตอบสนองเหตุการณ์ และความรู้ความสามารถของผู้เกี่ยวข้อง

ทั้งนี้ **ข้อกำหนดที่มีผลใช้บังคับ มาตรฐานและแนวปฏิบัติ และวิธีการประยุกต์ของแนวปฏิบัติฉบับนี้ มีสถานะแตกต่างกัน** องค์กรจึงควรพิจารณาความเกี่ยวข้องของแต่ละส่วนให้ชัดเจน และทบทวนผลการประเมินเมื่อวัตถุประสงค์ ข้อมูล ความสามารถของ AI การเชื่อมต่อ หรือระดับผลกระทบและความเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ

บทที่ 4 ค่าตั้งต้นด้านความมั่นคงปลอดภัย

บทนี้กำหนดแนวทางด้านความมั่นคงปลอดภัยสำหรับการออกแบบ ติดตั้ง ใช้งาน และบำรุงรักษาระบบ CCTV ที่ใช้ AI โดยประยุกต์หลัก **ความมั่นคงปลอดภัยตั้งแต่การออกแบบ (Security by Design)** และ **ค่าตั้งต้นที่มั่นคงปลอดภัย (Secure by Default)** ร่วมกับผลการประเมินตามข้อ 3.1

มาตรการในบทนี้ควรนำไปใช้ตามระดับ **B – Baseline, E – Enhanced และ H – High-Assurance** โดยข้อกำหนดตามกฎหมาย กฎระเบียบ TOR หรือสัญญาที่มีผลใช้บังคับยังคงต้องได้รับการปฏิบัติตามโดยไม่ขึ้นอยู่กับระดับดังกล่าว

4.1 เริ่มต้นอย่างมั่นคงปลอดภัยใน 7 ข้อ

ก่อนนำระบบ CCTV ที่ใช้ AI ไปใช้งาน องค์กรควรสามารถตอบคำถามสำคัญ 7 ข้อต่อไปนี้ได้

ข้อ	สิ่งที่ควรดำเนินการ	คำถามสำคัญ
1	**กำหนดวัตถุประสงค์ (Define Purpose)**	ใช้ AI เพื่ออะไร และจำเป็นต่อวัตถุประสงค์นั้นหรือไม่
2	**ประเมินผลกระทบและความเสี่ยง (Assess Impact and Risk)**	System Criticality, Data Impact และ AI Impact อยู่ในระดับใด
3	**กำหนดขอบเขตข้อมูล (Define Data Scope)**	เก็บ วิเคราะห์ สร้าง ส่งต่อ และเก็บรักษาข้อมูลอะไร
4	**กำหนดความสามารถและสิทธิ (Define Capability and Authority)**	AI ทำอะไรได้ ผลลัพธ์ส่งไปที่ใด และสามารถก่อให้เกิดการดำเนินการอะไร
5	**ทดสอบก่อนใช้งาน (Validate Before Operation)**	ระบบและ AI ทำงานได้ตามวัตถุประสงค์ในสภาพแวดล้อมจริงหรือไม่
6	**กำหนดการกำกับดูแลโดยมนุษย์ (Establish Human Oversight)**	ใครตรวจสอบ อนุมัติ แทรกแซง หรือหยุดการทำงานได้
7	**เฝ้าระวังและทบทวน (Monitor and Review)**	จะทราบได้อย่างไรว่าระบบเปลี่ยนแปลง ผิดปกติ หรือมีความเสี่ยงเพิ่มขึ้น

หลัก 7 ข้อนี้สามารถใช้เป็น **Quick-Start Checklist** สำหรับผู้บริหาร เจ้าของระบบ ผู้จัดซื้อ ผู้ติดตั้ง และผู้ตรวจประเมิน ก่อนเข้าสู่รายละเอียดในข้อ 4.3–4.5

หลักสำคัญ การเริ่มต้นอย่างมั่นคงปลอดภัยไม่ควรเริ่มจากคำถามว่า “จะซื้อกล้องหรือ AI รุ่นใด” แต่ควรเริ่มจาก **“ใช้เพื่ออะไร ⟶ มีผลกระทบอะไร ⟶ ต้องควบคุมอะไร ⟶ และจะยืนยันได้อย่างไรว่าระบบทำงานตามที่ต้องการ”**

4.2 การแบ่งบทบาทหน้าที่ในบทนี้

การรักษาความมั่นคงปลอดภัยของ CCTV-AI เป็นความรับผิดชอบร่วมของหลายฝ่าย โดยเฉพาะเมื่อระบบประกอบด้วยผลิตภัณฑ์ บริการ AI คลาวด์ และการติดตั้งจากผู้ให้บริการหลายราย

องค์กรควรกำหนดบทบาทและความรับผิดชอบให้ชัดเจนเพียงพอที่จะทราบว่า **ใครกำหนดความต้องการ ใครออกแบบ ใครตั้งค่า ใครอนุมัติ ใครใช้งาน ใครติดตาม และใครรับผิดชอบเมื่อเกิดปัญหา**

บทบาท	ความรับผิดชอบหลัก
เจ้าของระบบ (System Owner)	กำหนดวัตถุประสงค์ ยอมรับความเสี่ยง อนุมัติความสามารถสำคัญ และกำกับการใช้งาน
ผู้ผลิต/ผู้พัฒนา (Manufacturer/Developer)	ความมั่นคงปลอดภัยของผลิตภัณฑ์ AI/Software การปรับปรุงช่องโหว่ และการสนับสนุนตลอดวงจรชีวิต
ผู้ติดตั้ง/ผู้บูรณาการระบบ (Installer/System Integrator)	ออกแบบและติดตั้งตามข้อกำหนด ตั้งค่าอย่างมั่นคงปลอดภัย ทดสอบ และส่งมอบระบบ
ผู้ให้บริการภายนอก (External Service Provider)	ให้บริการตามขอบเขตและมาตรการที่ตกลง รวมถึง Cloud/AI Service ตามความเกี่ยวข้อง
ผู้ดูแลระบบ (Administrator)	Configuration, Accounts, Access, Updates, Logs, Backup และการบำรุงรักษา
ผู้ปฏิบัติงาน (Operator)	ใช้ระบบและผลลัพธ์ AI ตามวัตถุประสงค์ ทวนสอบ และยกระดับเหตุเมื่อจำเป็น
ผู้จัดซื้อ/ผู้ประเมิน (Procurement/Assessor)	กำหนดและตรวจสอบข้อกำหนด หลักฐาน การทดสอบ และเกณฑ์ตรวจรับ

กรณีมีบริการคลาวด์หรือบริการภายนอก ควรกำหนด **ความรับผิดชอบร่วม (Shared Responsibility)** ให้ชัดเจน โดยไม่ควรถือว่าการใช้บริการภายนอกเป็นการโอนความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยหรือการคุ้มครองข้อมูลไปยังผู้ให้บริการ

ไม่จำเป็นต้องสร้างตำแหน่งใหม่สำหรับทุกบทบาท หากองค์กรสามารถมอบหมายความรับผิดชอบดังกล่าวให้กับหน่วยงานหรือบุคลากรที่มีอยู่ได้อย่างชัดเจน

4.3 การออกแบบ

การออกแบบ CCTV ที่ใช้ AI ควรพิจารณาความมั่นคงปลอดภัย ความเป็นส่วนตัว ความน่าเชื่อถือของ AI และการจำกัดผลกระทบตั้งแต่เริ่มต้น มิใช่เพิ่มมาตรการภายหลังจากกำหนดสถาปัตยกรรมและเลือกผลิตภัณฑ์แล้ว

ผลการประเมินตามข้อ 3.1 ควรถูกนำมาใช้เป็นข้อมูลนำเข้าสำหรับการออกแบบ เพื่อให้มาตรการทางเทคนิคและการบริหารสอดคล้องกับระดับ B, E หรือ H ของระบบ

4.3.1 การออกแบบตามวัตถุประสงค์และความสามารถของ AI

องค์กรควรกำหนดความสามารถของ AI ที่จำเป็นต่อกรณีใช้งาน และไม่ควรเปิดใช้ความสามารถเพิ่มเติมเพียงเพราะผลิตภัณฑ์รองรับ

ควรกำหนดให้ชัดเจนว่า **กล้องตรวจจับอะไร ⟶ AI วิเคราะห์อะไร ⟶ สร้างผลลัพธ์อะไร ⟶ ใครหรือระบบใดได้รับผลลัพธ์ ⟶ ผลลัพธ์นำไปทำอะไร**

ตัวอย่างเช่น ระบบที่ต้องการเพียงตรวจจับบุคคลเข้าสู่พื้นที่ ไม่จำเป็นต้องเปิดใช้การรู้จำใบหน้า การติดตามบุคคลข้ามพื้นที่ หรือความสามารถในการวิเคราะห์อื่น หากไม่มีวัตถุประสงค์และความจำเป็นรองรับ

หลักการนี้สนับสนุนทั้งการลดพื้นที่การโจมตี (Attack Surface) การลดการประมวลผลข้อมูลที่ไม่จำเป็น และการจำกัดผลกระทบจาก AI

4.3.2 สถาปัตยกรรมและตำแหน่งการประมวลผล

การออกแบบควรระบุว่าองค์ประกอบสำคัญของ CCTV-AI อยู่และทำงานที่ใด เช่น **Camera/Edge ⟶ Network ⟶ AI Processing ⟶ VMS/Platform ⟶ Storage ⟶ Cloud/External Service ⟶ Connected System**

องค์กรควรทราบอย่างน้อยว่า

- AI ประมวลผลที่กล้อง Edge, Data Center หรือ Cloud
- ข้อมูลใดออกจากกล้องหรือสถานที่ขององค์กร
- ข้อมูลใดถูกส่งไปยังบริการภายนอก
- ระบบใดเก็บภาพ วิดีโอ Metadata และ AI Output
- บุคคลหรือระบบใดสามารถเข้าถึงองค์ประกอบแต่ละส่วน
- การเชื่อมต่อใดมีความสำคัญต่อการทำงานของระบบ
- ระบบสามารถทำงานอย่างไรเมื่อการเชื่อมต่อหรือบริการภายนอกไม่พร้อมใช้งาน

การเลือก Edge, On-Premises หรือ Cloud ไม่ควรถูกตัดสินว่าปลอดภัยหรือไม่ปลอดภัยจากรูปแบบการติดตั้งเพียงอย่างเดียว แต่ควรพิจารณาร่วมกับผลกระทบ ความเสี่ยง ความสามารถในการควบคุม และข้อกำหนดที่มีผลใช้บังคับ

4.3.3 การออกแบบการไหลของข้อมูล

ควรสามารถระบุการไหลของข้อมูลสำคัญตั้งแต่การเก็บข้อมูลจนถึงการลบหรือยุติการใช้งาน อย่างน้อยควรทราบว่า **ข้อมูลอะไร ⟶ มาจากไหน ⟶ ประมวลผลที่ใด ⟶ ถูกส่งไปที่ใด ⟶ ใครเข้าถึง ⟶ เก็บไว้นานเท่าใด ⟶ ลบอย่างไร**

การออกแบบควรครอบคลุมไม่เฉพาะภาพและวิดีโอ แต่รวมถึง Metadata, AI Output, Tracking Data, Biometric Data และ Derived/Inferred Data ตามความเกี่ยวข้อง

สำหรับระบบที่มีผลกระทบสูง ควรสามารถตรวจสอบ Data Flow ได้เพียงพอที่จะประเมินผลกระทบจากการเชื่อมต่อ การส่งข้อมูลออก และการใช้บริการภายนอก

4.3.4 การออกแบบการควบคุมการเข้าถึงและการเชื่อมต่อ

การเข้าถึงระบบและการเชื่อมต่อระหว่างองค์ประกอบควรใช้หลัก **สิทธิเท่าที่จำเป็น (Least Privilege)** และจำกัดเฉพาะสิ่งที่จำเป็นต่อการดำเนินงาน

ควรพิจารณาอย่างน้อย

- บัญชีผู้ดูแลและผู้ใช้งาน
- Service Account
- Remote Access
- API และ Interface
- Token, Key และ Certificate
- การเชื่อมต่อจากผู้ผลิตหรือผู้ให้บริการ
- สิทธิในการดู ส่งออก เปลี่ยนแปลง หรือลบข้อมูล
- สิทธิในการเปิด ปิด หรือเปลี่ยนความสามารถของ AI

ระบบที่มีผลกระทบสูงควรลดการใช้บัญชีหรือข้อมูลรับรองร่วมกัน และควรสามารถระบุการดำเนินการสำคัญกลับไปยังบุคคลหรือระบบที่เกี่ยวข้องได้ตามความเหมาะสม

4.3.5 การออกแบบการใช้ผลลัพธ์และอำนาจของ AI

การออกแบบควรกำหนดอย่างชัดเจนว่าผลลัพธ์ของ AI มีอำนาจต่อการดำเนินการเพียงใด ตามลำดับที่กำหนดไว้ในข้อ 3.1 เช่น **Inform ⟶ Alert ⟶ Recommend ⟶ Decision Support ⟶ Trigger ⟶ Automated Action**

เมื่อผลลัพธ์ของ AI มีอำนาจเพิ่มขึ้น มาตรการควบคุมควรเพิ่มขึ้นตามความเสี่ยง โดยเฉพาะกรณี **Trigger หรือ Automated Action** ควรกำหนด

- ระบบหรือการดำเนินการที่ AI สามารถกระตุ้นได้
- เงื่อนไขก่อนดำเนินการ

- สิทธิที่ใช้
- ขอบเขตการดำเนินการ (Action Boundary)
- การตรวจสอบหรืออนุมัติโดยบุคคล
- วิธีระงับหรือหยุดการดำเนินการ
- หลักฐานที่ต้องบันทึก

ไม่ควรให้ AI มีสิทธิหรืออำนาจมากกว่าที่จำเป็นต่อกรณีใช้งาน

4.3.6 การออกแบบการกำกับดูแลโดยมนุษย์

การกำกับดูแลโดยมนุษย์ไม่ควรถูกกำหนดเพียงว่า “มีคนตรวจสอบ” แต่ควรออกแบบให้บุคคลสามารถดำเนินการได้จริง

ควรกำหนดตามความเสี่ยงว่า **ใครตรวจสอบ ⟶ ตรวจสอบเมื่อใด ⟶ เห็นข้อมูลอะไร ⟶ สามารถอนุมัติหรือปฏิเสธได้หรือไม่ ⟶ สามารถหยุดหรือจำกัด AI ได้หรือไม่ ⟶ ต้องยกระดับให้ใคร**

สำหรับผลลัพธ์ที่มีผลกระทบสูง ผู้ตรวจสอบควรได้รับข้อมูลที่เพียงพอต่อการตัดสินใจ และไม่ควรถูกบังคับโดยการออกแบบระบบให้ทำได้เพียงยืนยันผลลัพธ์ของ AI โดยไม่มีทางเลือกที่เหมาะสม

4.3.7 การออกแบบเพื่อจำกัดผลกระทบ

ระบบควรได้รับการออกแบบเพื่อป้องกันไม่ให้ความผิดพลาดหรือการถูกโจมตีในองค์ประกอบหนึ่งขยายผลกระทบโดยไม่จำเป็นไปยังองค์ประกอบอื่น

ควรพิจารณาหลักการ เช่น

- **การแยกส่วน (Segmentation)**
- **สิทธิเท่าที่จำเป็น (Least Privilege)**
- **การแยกการวิเคราะห์ออกจากการดำเนินการ**
- **ขอบเขตการดำเนินการ (Action Boundary)**
- **การทวนสอบก่อนดำเนินการ (Validate Before Action)**
- **การจำกัดผลกระทบ (Containment)**

ตัวอย่างเช่น การที่ AI ตรวจพบบุคคลไม่ควรหมายความโดยอัตโนมัติว่า AI ต้องได้รับสิทธิโดยตรงในการควบคุมระบบ Access Control หากวัตถุประสงค์สามารถบรรลุได้ด้วยการส่ง Alert ให้บุคคลตรวจสอบก่อน

หลักสำคัญคือ **ยิ่งผลลัพธ์ของ AI สามารถก่อให้เกิดผลกระทบต่อระบบอื่นได้มากเท่าใด การออกแบบยิ่งควรลดอำนาจ จำกัดขอบเขต และเพิ่มการทวนสอบก่อนดำเนินการมากขึ้นตามระดับความเสี่ยง**

4.3.8 การออกแบบสำหรับความล้มเหลวและการทำงานแบบจำกัด

องค์กรควรกำหนดพฤติกรรมของระบบเมื่อ AI ไม่พร้อมใช้งาน ให้ผลลัพธ์ผิดปกติ หรือบริการที่ระบบพึ่งพาไม่สามารถใช้งานได้

แนวทางอาจประกอบด้วย **AI Operation ⟶ Degraded Mode ⟶ Basic CCTV ⟶ Human Review ⟶ Fail-Safe**

การเลือกสถานะที่เหมาะสมควรพิจารณาผลกระทบของแต่ละกรณี ไม่ควรถือว่าการ “เปิดระบบต่อไป” หรือ “ปิดระบบทั้งหมด” เป็นทางเลือกที่ปลอดภัยที่สุดเสมอ

สำหรับระบบที่เชื่อมต่อกับการดำเนินการทางกายภาพหรือภารกิจสำคัญ ควรกำหนดพฤติกรรมเมื่อเกิดความล้มเหลวไว้อย่างชัดเจนและทดสอบได้

4.3.9 การออกแบบเพื่อการทดสอบและตรวจสอบย้อนหลัง

ระบบควรได้รับการออกแบบให้สามารถทดสอบและสร้างหลักฐานได้เพียงพอต่อระดับความเสี่ยง เช่น

- ระบุรุ่นและสถานะขององค์ประกอบสำคัญได้
- ทดสอบ AI ในสภาพแวดล้อมที่เหมาะสมได้
- ตรวจสอบ Configuration ที่สำคัญได้
- ตรวจสอบการเปลี่ยนแปลงได้
- บันทึกเหตุการณ์สำคัญได้
- เชื่อมโยง AI Output กับการดำเนินการที่เกี่ยวข้องได้
- ทดสอบ Degraded Mode หรือ Fail-Safe ได้
- ตรวจสอบการเชื่อมต่อและ Action Boundary ได้

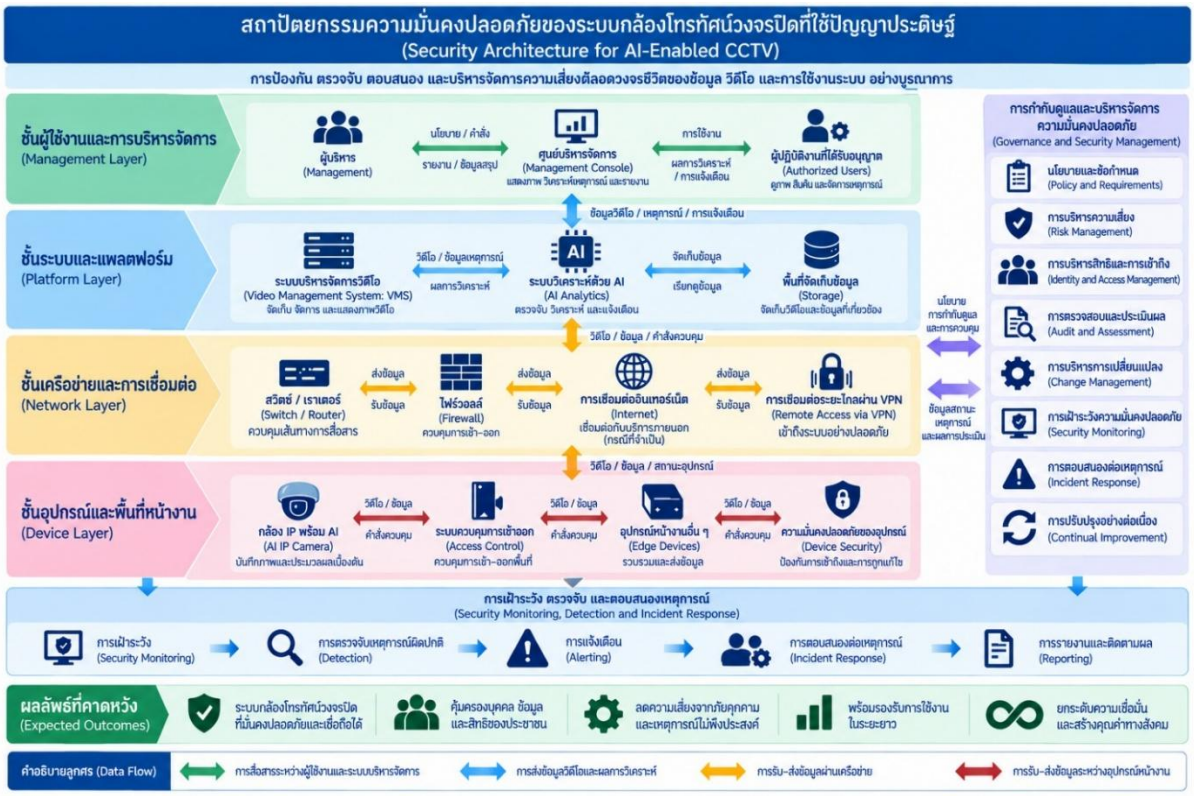
สำหรับระดับ H ควรให้ความสำคัญกับหลักฐานที่สามารถแสดงได้ว่า **ระบบไม่ได้เพียงทำงาน แต่ทำงานภายใต้ขอบเขตและมาตรการที่ได้รับอนุมัติ**

4.3.10 การทบทวนและยอมรับการออกแบบ

ก่อนเข้าสู่ขั้นตอนติดตั้ง องค์กรควรทบทวนว่าการออกแบบสอดคล้องกับ **Purpose ⟶ Impact/Risk ⟶ B/E/H ⟶ Data ⟶ AI Capability ⟶ Architecture ⟶ Security Controls ⟶ Human Oversight ⟶ Testing Requirements**

ข้อจำกัดหรือความเสี่ยงที่ยังคงเหลือ (Residual Risk) และมีนัยสำคัญควรได้รับการระบุและพิจารณาโดยผู้มีอำนาจที่เหมาะสม

ไม่จำเป็นต้องจัดทำ Design Review Form ใหม่เฉพาะ CCTV-AI หากเอกสารออกแบบ TOR, Architecture, Risk Assessment หรือหลักฐานอื่นสามารถแสดงการพิจารณาดังกล่าวได้อย่างเพียงพอ



รูปที่ 5 สถาปัตยกรรมด้านความมั่นคงปลอดภัยสำหรับระบบ CCTV ที่ใช้ AI

สถาปัตยกรรมด้านความมั่นคงปลอดภัยของ CCTV ที่ใช้ AI ควรครอบคลุมตั้งแต่แหล่งข้อมูล การประมวลผล AI แพลตฟอร์ม การใช้ผลลัพธ์ ไปจนถึงระบบที่เชื่อมต่อ โดยมีมาตรการควบคุมที่สามารถป้องกัน ตรวจพบ จำกัด และตรวจสอบผลกระทบได้ตลอดเส้นทาง

4.4 การติดตั้ง

การติดตั้งระบบ CCTV ที่ใช้ AI ควรดำเนินการให้สอดคล้องกับการออกแบบ ข้อกำหนดด้านความมั่นคงปลอดภัย และระดับมาตรการที่กำหนดตามข้อ 3.1 โดยให้ความสำคัญกับ **ค่าตั้งต้นที่มั่นคงปลอดภัย (Secure by Default)** และการทดสอบก่อนเปิดใช้งานจริง

การติดตั้งไม่ควรถือว่าสมบูรณ์เพียงเมื่อกล้องสามารถแสดงภาพหรือ AI สามารถสร้างผลลัพธ์ได้ แต่ควรยืนยันว่า **อุปกรณ์ การตั้งค่า AI บัญชีและสิทธิ การเชื่อมต่อ การบันทึกเหตุการณ์ และมาตรการจำกัดผลกระทบ** เป็นไปตามที่ได้รับอนุมัติ

แนวทางการติดตั้งและทดสอบระบบเฝ้าระวังด้วยวิดีโอสามารถพิจารณา **IEC 62676 series** ตามความเกี่ยวข้อง โดยเฉพาะหลักการที่เกี่ยวข้องกับการออกแบบ การติดตั้ง การทดสอบ การตรวจรับ และสมรรถนะของระบบ

4.4.1 การตรวจสอบก่อนติดตั้ง

ก่อนติดตั้งหรือเชื่อมต่ออุปกรณ์เข้าสู่ระบบใช้งานจริง ควรตรวจสอบตามความเหมาะสมว่า

- อุปกรณ์และรุ่นตรงตามที่ได้รับอนุมัติ
- Firmware และ Software มาจากแหล่งที่เชื่อถือได้
- ความสามารถ AI ตรงตามวัตถุประสงค์และขอบเขตที่กำหนด
- ผลิตภัณฑ์ยังอยู่ในระยะการสนับสนุน
- ทราบช่องโหว่หรือข้อจำกัดสำคัญที่เกี่ยวข้อง
- มีข้อมูลที่จำเป็นสำหรับการตั้งค่า การปรับปรุง และการดูแลรักษา
- องค์ประกอบหรือบริการภายนอกที่สำคัญเป็นไปตามการออกแบบ

หากมีความแตกต่างจากรายการที่ได้รับอนุมัติ ควรประเมินผลกระทบก่อนนำไปใช้งาน ไม่ควรเปลี่ยนอุปกรณ์ รุ่น หรือบริการที่มีผลต่อความเสี่ยงโดยไม่มีการพิจารณาที่เหมาะสม

4.4.2 การตั้งค่าที่มั่นคงปลอดภัย

ระบบควรได้รับการตั้งค่าให้เปิดใช้งานเฉพาะบัญชี บริการ Protocol การเชื่อมต่อ และความสามารถที่จำเป็นต่อการใช้งาน

ควรพิจารณาอย่างน้อย **บัญชีและข้อมูลรับรอง ⟶ สิทธิ ⟶ Network Service ⟶ Remote Access ⟶ Interface/API ⟶ Logging ⟶ Time Synchronization ⟶ Security Update**

บัญชีหรือรหัสผ่านค่าตั้งต้นที่ไม่เหมาะสมควรได้รับการเปลี่ยน ปิด หรือจัดการก่อนเปิดใช้งานจริงตามความสามารถของผลิตภัณฑ์

บริการหรือความสามารถที่ไม่จำเป็นควรถูกปิดหรือจำกัดตามความเหมาะสม โดยเฉพาะ Remote Administration, External Connectivity และบริการที่สามารถเปลี่ยนการตั้งค่าหรือความสามารถของ AI

4.4.3 การตั้งค่าความสามารถของ AI

การตั้งค่า AI ควรสอดคล้องกับวัตถุประสงค์และกรณีใช้งานที่ได้รับอนุมัติ เช่น

- ประเภท Analytics ที่เปิดใช้งาน
- พื้นที่หรือขอบเขตการวิเคราะห์
- Rule และเงื่อนไขการตรวจจับ
- Threshold หรือค่าที่มีผลต่อผลลัพธ์
- ข้อมูลหรือฐานข้อมูลที่ AI สามารถใช้
- การสร้างและจัดเก็บ AI Output
- การส่ง Alert หรือผลลัพธ์ไปยังระบบอื่น
- การดำเนินการอัตโนมัติที่ได้รับอนุญาต

ไม่ควรเปิดใช้ความสามารถเพิ่มเติมเพียงเพื่อทดลองหรือเพราะผลิตภัณฑ์รองรับ หากความสามารถดังกล่าวเพิ่มการประมวลผลข้อมูลหรือความเสี่ยงโดยไม่มีวัตถุประสงค์รองรับ

ค่าที่มีผลสำคัญต่อพฤติกรรมของ AI ควรสามารถระบุและตรวจสอบย้อนหลังได้ตามระดับความเสี่ยง

4.4.4 การติดตั้งกล้องให้เหมาะสมกับการทำงานของ AI

สมรรถนะของ AI ขึ้นอยู่กับคุณภาพของข้อมูลภาพที่ระบบได้รับ การติดตั้งจึงควรพิจารณาสภาพแวดล้อมจริงและวัตถุประสงค์ของการวิเคราะห์ ไม่ใช่พิจารณาเพียงว่ากล้องสามารถมองเห็นพื้นที่ได้

ควรพิจารณาปัจจัย เช่น

- ตำแหน่งและมุมกล้อง
- ระยะห่างจากวัตถุหรือพื้นที่เป้าหมาย
- แสงและการเปลี่ยนแปลงของแสง
- การบดบัง
- การเคลื่อนไหว
- ความละเอียดและคุณภาพของภาพ
- สภาพแวดล้อมที่อาจเปลี่ยนแปลง
- ความเหมาะสมของภาพกับ AI Use Case ที่กำหนด

การทดสอบควรดำเนินการในสภาพที่เป็นตัวแทนของการใช้งานจริงตามความเหมาะสม ไม่ควรสรุปว่าสมรรถนะของ AI เพียงพอจากข้อมูลจำเพาะของผลิตภัณฑ์หรือผลการทดสอบในสภาพแวดล้อมอื่นเพียงอย่างเดียว หลักการด้านการออกแบบ การติดตั้ง และการทดสอบระบบเฝ้าระวังด้วยวิดีโอสามารถพิจารณา **IEC 62676-4** และมาตรฐานใน IEC 62676 series ที่เกี่ยวข้อง

4.4.5 การติดตั้งและทดสอบการเชื่อมต่อ

การเชื่อมต่อระบบ CCTV ที่ใช้ AI กับระบบบริหารจัดการวิดีโอ (Video Management System: VMS) บริการคลาวด์ (Cloud Service) ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) กระบวนงานอัตโนมัติ (Workflow) ระบบควบคุมการเข้าออก (Access Control System) หรือระบบอื่น ควรได้รับการตรวจสอบว่าเป็นไปตามสถาปัตยกรรมและขอบเขตที่ได้รับอนุมัติ

ควรตรวจสอบอย่างน้อยตามลำดับดังนี้ **ระบบต้นทาง ⟶ ระบบปลายทาง ⟶ ข้อมูลที่แลกเปลี่ยน ⟶ วิธีการหรือส่วนเชื่อมต่อระบบ (Protocol/API) ⟶ บัญชีและสิทธิ (Account/Permission) ⟶ เงื่อนไขกระตุ้นการทำงาน (Trigger) ⟶ การดำเนินการของระบบ (Action)**

สำหรับการเชื่อมต่อที่สามารถก่อให้เกิดการดำเนินการต่อระบบอื่น ควรทดสอบทั้งกรณีปกติและกรณีที่ AI ให้ผลลัพธ์ผิด ไม่พร้อมใช้งาน หรือการเชื่อมต่อขัดข้องตามระดับความเสี่ยง

การทดสอบควรยืนยันว่า **ขอบเขตการดำเนินการ (Action Boundary)** และ **การกำกับดูแลโดยมนุษย์ (Human Oversight)** สามารถทำงานได้ตามที่ออกแบบและได้รับอนุมัติไว้

4.4.6 การเข้าถึงจากระยะไกลและการเข้าถึงของผู้ให้บริการ

การเข้าถึงระบบจากระยะไกลของผู้ดูแล ผู้ติดตั้ง ผู้ผลิต หรือผู้ให้บริการควรถูกจำกัดตามความจำเป็นและระดับความเสี่ยง

ควรพิจารณา

- ผู้ใดได้รับอนุญาต
- เข้าถึงระบบใด
- มีสิทธิระดับใด
- ใช้ช่องทางใด
- ต้องได้รับการอนุมัติหรือไม่
- มีการบันทึกกิจกรรมหรือไม่
- สิทธิเป็นแบบถาวรหรือชั่วคราว
- เมื่อสิ้นสุดงานจะยกเลิกสิทธิอย่างไร

บัญชีชั่วคราวหรือสิทธิที่ใช้ระหว่างการติดตั้งไม่ควรหลงเหลืออยู่หลังการส่งมอบโดยไม่มีความจำเป็นและการอนุมัติที่ชัดเจน

4.4.7 การทดสอบก่อนเปิดใช้งาน

ก่อนเปิดใช้งานจริง ควรทดสอบให้ครอบคลุมทั้งการทำงานของระบบ สมรรถนะของ AI ความมั่นคงปลอดภัย และการเชื่อมต่อกับระบบอื่น ตามระดับผลกระทบและความเสี่ยง

การทดสอบควรสามารถตอบได้อย่างน้อยว่า **ระบบทำงานตามที่ออกแบบหรือไม่ ⟶ AI ทำงานตามกรณีใช้งาน (Use Case) หรือไม่ ⟶ ผลลัพธ์อยู่ในระดับที่ยอมรับได้หรือไม่ ⟶ การตั้งค่าด้านความมั่นคงปลอดภัย (Security Configuration) ถูกต้องหรือไม่ ⟶ บัญชีและสิทธิถูกต้องหรือไม่ ⟶ การบันทึกเหตุการณ์ (Logging) ทำงานหรือไม่ ⟶ ระบบปลายทางตอบสนองตามที่ออกแบบหรือไม่**

สำหรับระบบที่มีผลกระทบสูง ควรทดสอบเพิ่มเติมในสถานการณ์ที่เกี่ยวข้อง เช่น

- AI ให้ผลลัพธ์ผิดหรือไม่แน่นอน
- AI หรือบริการภายนอกไม่พร้อมใช้งาน
- ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) หรือระบบปลายทางไม่ตอบสนอง
- การดำเนินการอัตโนมัติ (Automated Action) ถูกจำกัดให้อยู่ภายในขอบเขตการดำเนินการ (Action Boundary)
- บุคลากรที่ได้รับมอบหมายสามารถแทรกแซง ระงับ หรือหยุดการดำเนินการได้

- การทำงานแบบจำกัด (Degraded Mode) สามารถทำงานได้ตามที่กำหนด
- ระบบสามารถเข้าสู่สภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe) ตามที่ออกแบบไว้

กรณีใช้การวิเคราะห์วิดีโออัจฉริยะ ควรพิจารณาหลักการด้านการทดสอบสมรรถนะตามมาตรฐานใน IEC 62676 series ที่เกี่ยวข้องกับประเภทของระบบและกรณีใช้งาน

4.4.8 การจัดการความแตกต่างจากแบบหรือข้อกำหนด

หากการติดตั้งจริงแตกต่างจากแบบ ข้อกำหนด หรือผลิตภัณฑ์ที่ได้รับอนุมัติ ควรบันทึกและพิจารณาผลกระทบตามความสำคัญของความแตกต่าง

ความแตกต่างที่มีผลต่อข้อมูล ความสามารถ AI การเชื่อมต่อ ความมั่นคงปลอดภัย หรือระดับความเสี่ยง ไม่ควรถูกยอมรับเพียงเพราะระบบสามารถทำงานได้

หากเป็นการเปลี่ยนแปลงที่มีนัยสำคัญ (Significant Change) ควรประเมินใหม่ตามข้อ 3.1

4.4.9 การกำหนดสถานะก่อนส่งมอบ

เมื่อการติดตั้งและทดสอบแล้วเสร็จ ควรกำหนดสถานะของระบบที่ได้รับอนุมัติเป็นข้อมูลอ้างอิงสำหรับการใช้งาน การบำรุงรักษา และการบริหารการเปลี่ยนแปลงต่อไป

ข้อมูลอาจประกอบด้วยตามความเหมาะสม เช่น **อุปกรณ์และรุ่น ⟶ เฟิร์มแวร์และซอฟต์แวร์ (Firmware/Software) ⟶ ความสามารถและแบบจำลอง AI (AI Capability/Model) ⟶ การตั้งค่า (Configuration) ⟶ บัญชีและบทบาท (Accounts/Roles) ⟶ การเชื่อมต่อกับระบบอื่น (Integration) ⟶ การเข้าถึงจากระยะไกล (Remote Access) ⟶ การบันทึกเหตุการณ์ (Logging) ⟶ ผลการทดสอบ (Test Result)**

ไม่จำเป็นต้องจัดทำเอกสารค่าฐาน (Baseline) ใหม่ทั้งหมด หากข้อมูลจาก **ระบบบริหารการตั้งค่า (Configuration Management) ทะเบียนสินทรัพย์ (Asset Inventory) ระบบบริหารจัดการวิดีโอ (VMS) เอกสารส่งมอบ** หรือระบบอื่นที่องค์กรมีอยู่ สามารถแสดงสถานะที่ได้รับอนุมัติและตรวจสอบย้อนหลังได้อย่างเพียงพอ

สถานะดังกล่าวควรใช้เป็นฐานสำหรับการพิจารณาระหว่างการใช้งานว่า ระบบยังคงอยู่ใน **สถานะที่ได้รับอนุมัติและเชื่อถือได้ (Approved and Trusted State)** หรือไม่

รายละเอียดการตรวจรับและส่งมอบระบุเพิ่มเติมในข้อ 5.2 และภาคผนวก ก

หลักสำคัญ การติดตั้งระบบ CCTV ที่ใช้ AI อย่างมั่นคงปลอดภัยควรยืนยันว่า ติดตั้งถูกต้อง ⟶ ตั้งค่าถูกต้อง ⟶ AI ทำงานเหมาะสม ⟶ การเชื่อมต่ออยู่ในขอบเขตที่ได้รับอนุมัติ ⟶ ระบบพร้อมสำหรับการใช้งานจริง

4.5 การดำเนินงานในภาวะปกติและการดูแลรักษา

ภายหลังการเปิดใช้งาน เป้าหมายของการดำเนินงานและบำรุงรักษา CCTV-AI คือการรักษาให้ระบบยังคงทำงานตามวัตถุประสงค์ อยู่ภายใต้ขอบเขตที่ได้รับอนุมัติ และมีระดับความเสี่ยงที่ยอมรับได้ตลอดวงจรชีวิต แนวปฏิบัตินี้เรียกสภาวะดังกล่าวว่า **สถานะที่ได้รับอนุมัติและเชื่อถือได้ (Approved and Trusted State)**

การดำเนินงานจึงไม่ควรตรวจสอบเพียงว่าอุปกรณ์ Online หรือ AI ยังสามารถสร้างผลลัพธ์ได้ แต่ควรพิจารณาว่า **ระบบยังเป็นระบบเดียวกับที่ได้รับการประเมิน ทดสอบ และอนุมัติไว้หรือไม่**

4.5.1 การรักษาสถานะที่ได้รับอนุมัติ

องค์กรควรสามารถตรวจพบหรือทบทวนการเปลี่ยนแปลงที่สำคัญจากสถานะที่ได้รับอนุมัติ เช่น

- เฟิร์มแวร์หรือซอฟต์แวร์ (Firmware/Software) เปลี่ยนแปลง
- แบบจำลองหรือความสามารถของ AI (AI Model/AI Capability) เปลี่ยนแปลง
- กฎหรือค่าเกณฑ์ที่สำคัญ (Rule/Threshold) เปลี่ยนแปลง
- บัญชีหรือสิทธิการเข้าถึงเปลี่ยนแปลง
- การเข้าถึงจากระยะไกล (Remote Access) เปลี่ยนแปลง
- ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) หรือระบบที่เชื่อมต่อเปลี่ยนแปลง
- บริการคลาวด์หรือบริการภายนอก (Cloud/External Service) เปลี่ยนแปลง
- ความสามารถในการบันทึกเหตุการณ์และการเฝ้าระวัง (Logging and Monitoring) เปลี่ยนแปลง

การเปลี่ยนแปลงที่ได้รับอนุมัติควรดำเนินการตามข้อ 3.4 ส่วนการเปลี่ยนแปลงที่ไม่ทราบสาเหตุหรือไม่ได้รับอนุญาตควรได้รับการตรวจสอบตามระดับความเสี่ยง

4.5.2 การรักษาสมรรถนะและความน่าเชื่อถือของ AI

สมรรถนะของ AI อาจเปลี่ยนแปลงแม้ไม่มีการเปลี่ยนแบบจำลอง เนื่องจากสภาพแวดล้อม กล้อง แสง พื้นที่ การใช้งาน หรือข้อมูลที่ระบบได้รับเปลี่ยนไป

องค์กรควรติดตามสมรรถนะในระดับที่เหมาะสมกับกรณีใช้งาน โดยเฉพาะความผิดพลาดที่มีผลต่อบุคคล ความปลอดภัย หรือภารกิจสำคัญ

เมื่อพบว่าสมรรถนะเปลี่ยนแปลงอย่างมีนัยสำคัญ ไม่ควรแก้ไขด้วยการปรับ Threshold หรือ Configuration โดยอัตโนมัติ แต่ควรพิจารณาสาเหตุ ผลกระทบ และความจำเป็นในการทดสอบใหม่ หลักการด้านการติดตามสมรรถนะระบุเพิ่มเติมในข้อ 3.5

4.5.3 การบริหารการเปลี่ยนแปลงระหว่างการใช้งาน

การเปลี่ยน Firmware, Software, AI Model, Configuration, Integration หรือบริการภายนอก ควรผ่านกระบวนการตามข้อ 3.4

หลักการสำคัญคือ **เปลี่ยน ⟶ ประเมิน ⟶ ทดสอบ ⟶ อนุมัติ ⟶ ใช้งาน ⟶ ทวนสอบ**

หากเป็น **การเปลี่ยนแปลงที่มีนัยสำคัญ (Significant Change)** ซึ่งอาจทำให้วัตถุประสงค์ ข้อมูล ความสามารถ AI การเชื่อมต่อ หรือผลกระทบเปลี่ยนแปลง ควรกลับไปประเมินข้อ 3.1

4.5.4 การบริหารช่องโหว่และการปรับปรุง

องค์กรควรติดตามช่องโหว่และ Security Update ที่เกี่ยวข้องกับผลิตภัณฑ์และบริการที่ใช้งาน และเชื่อมโยงข้อมูลดังกล่าวกับระบบที่ได้รับผลกระทบ

การดำเนินการควรเป็นแบบอิงความเสี่ยง (Risk-Based) โดยพิจารณาทั้งความรุนแรง ความสามารถในการโจมตี ความสำคัญของระบบ และผลกระทบต่อการใช้งานจริง

รายละเอียดกระบวนการบริหารช่องโหว่ไม่จำเป็นต้องกำหนดซ้ำในบทนี้ โดยให้ใช้ข้อ 3.7.3 เป็นหลัก

4.5.5 การทบทวนบัญชี สิทธิ และการเชื่อมต่อ

ควรทบทวนบัญชี สิทธิ การเข้าถึงจากระยะไกล (Remote Access) บัญชีบริการ (Service Account) ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) และการเชื่อมต่อกับระบบอื่น ตามระดับความเสี่ยงและการเปลี่ยนแปลงที่เกิดขึ้น

ควรให้ความสำคัญเป็นพิเศษตามลำดับ เช่น สิทธิระดับสูง (Privileged Access) ⟶ การเข้าถึงของผู้ผลิตหรือผู้ให้บริการ (Vendor Access) ⟶ บัญชีบริการ (Service Account) ⟶ สิทธิในการเรียกใช้ API (API Permission) ⟶ การดำเนินการอัตโนมัติ (Automated Action)

สิทธิที่ไม่มีความจำเป็นหรือไม่สอดคล้องกับบทบาทควรถูกลดหรือยกเลิก

การทบทวนควรครอบคลุมทั้ง **“บุคคลใดสามารถเข้าถึงระบบได้”** และ **“ระบบหนึ่งสามารถดำเนินการต่ออีกระบบหนึ่งได้เพียงใด”**

4.5.6 การทบทวนความเหมาะสมของการใช้งานอย่างต่อเนื่อง

แม้ระบบจะยังทำงานตามข้อกำหนดทางเทคนิค องค์กรควรทบทวนเป็นระยะว่าการใช้ AI ยังคงเหมาะสมกับวัตถุประสงค์เดิมหรือไม่

ควรพิจารณาเมื่อมีการเปลี่ยนแปลง เช่น **Purpose ⟶ Environment ⟶ Data ⟶ AI Capability ⟶ Users ⟶ Connected Systems ⟶ Legal/Contractual Requirements**

หากความสามารถบางอย่างไม่มีความจำเป็นอีกต่อไป ควรพิจารณาปิดหรือลดขอบเขตแทนการเปิดใช้งานต่อเพียงเพราะระบบรองรับ

หลักการนี้ช่วยป้องกัน **การขยายขอบเขตการใช้งานโดยไม่ได้ตั้งใจ (Function or Purpose Creep)**

4.5.7 การดำเนินงานเมื่อ AI ไม่สามารถเชื่อถือได้

องค์กรควรมีแนวทางที่ผู้ปฏิบัติงานสามารถนำไปใช้ได้เมื่อ AI ไม่พร้อมใช้งาน มีความผิดปกติ หรือมีเหตุอันควรสงสัยว่าผลลัพธ์ไม่น่าเชื่อถือ

แนวทางอาจพิจารณาตามลำดับ เช่น **จำกัดความสามารถของ AI ⟶ ระงับการดำเนินการอัตโนมัติ (Automated Action) ⟶ กลับไปใช้ CCTV พื้นฐาน ⟶ ตรวจสอบโดยบุคลากร (Human Review) ⟶ เข้าสู่สภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe)**

ผู้ปฏิบัติงานควรทราบว่าใครมีอำนาจดำเนินการดังกล่าว และเงื่อนไขใดที่ต้องยกระดับไปยังเจ้าของระบบหรือผู้รับผิดชอบเหตุการณ์

ไม่ควรปล่อยให้ระบบดำเนินการอัตโนมัติต่อไปเพียงเพราะยังไม่มีการยืนยันว่าเกิดเหตุโจมตี หากมีหลักฐานเพียงพอว่าผลลัพธ์อาจก่อให้เกิดผลกระทบที่ไม่ยอมรับ

4.5.8 การเก็บรักษาหลักฐานและการทบทวน

องค์กรควรมีหลักฐานเพียงพอสำหรับแสดงว่าระบบได้รับการดูแลตามระดับความเสี่ยง เช่น

- ผลการตรวจสอบตามรอบ
- ประวัติการเปลี่ยนแปลง
- ผลการทดสอบที่สำคัญ
- การทบทวนสิทธิ
- สถานะช่องโหว่และการแก้ไข
- เหตุการณ์และการดำเนินการ
- ผลการติดตามสมรรถนะ AI
- การประเมินใหม่เมื่อเกิด Significant Change

ไม่จำเป็นต้องสร้างหลักฐานหรือแบบฟอร์มซ้ำ หากข้อมูลจาก **ระบบบริหารจัดการวิดีโอ (VMS) ระบบติดตามงานหรือปัญหา (Ticketing System) บันทึกการเปลี่ยนแปลง (Change Record) หลักฐานการทบทวนสิทธิ (Access Review) บันทึกการบำรุงรักษา (Maintenance Record) บันทึกเหตุการณ์ (Incident Record)** หรือระบบอื่นที่องค์กรใช้อยู่ สามารถแสดงการดำเนินงานและตรวจสอบย้อนหลังได้อย่างเพียงพอ

สำหรับการทบทวนตามรอบ สามารถใช้ **ภาคผนวก ข รายการตรวจสอบด้วยตนเองตามรอบ (Periodic Self-Assessment Checklist)** ประกอบการตรวจสอบได้

สรุปหลักการของบทที่ 4

การรักษาความมั่นคงปลอดภัยของระบบ CCTV ที่ใช้ AI ไม่สิ้นสุดเมื่อระบบผ่านการติดตั้งและตรวจรับ แต่ควรรักษาให้ระบบอยู่ใน **สถานะที่ได้รับอนุมัติและเชื่อถือได้ (Approved and Trusted State)** ตลอดวงจรชีวิต

การออกแบบ ติดตั้ง ใช้งาน และบำรุงรักษาควรควบคุมความสามารถของ AI ข้อมูล บัญชีและสิทธิการเชื่อมต่อ และการนำผลลัพธ์ไปใช้ พร้อมจัดให้มีการทดสอบ การกำกับดูแลโดยมนุษย์ การเฝ้าระวัง การจัดการการเปลี่ยนแปลง และมาตรการจำกัดผลกระทบตามระดับความเสี่ยง โดยเฉพาะเมื่อผลลัพธ์จาก AI สามารถก่อให้เกิดการดำเนินการต่อระบบอื่นได้

บทที่ 5 การจัดซื้อจัดจ้าง

การจัดซื้อระบบ CCTV ที่ใช้ AI ควรนำผลการประเมินตามข้อ 3.1 และข้อกำหนดด้านการออกแบบตามบทที่ 4 มาใช้กำหนดคุณลักษณะ ข้อกำหนดด้านความมั่นคงปลอดภัย และเกณฑ์การตรวจรับให้เหมาะสมกับระดับผลกระทบและความเสี่ยง

ข้อกำหนดควรมีลักษณะ **เป็นกลางต่อผู้ผลิตและเทคโนโลยี (Vendor-Neutral and Technology-Neutral) สามารถตรวจสอบได้ และได้สัดส่วนกับความเสี่ยง** โดยไม่กำหนดรายละเอียดที่เกินความจำเป็นต่อวัตถุประสงค์ของระบบ

5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยในการจัดซื้อ

ก่อนจัดทำข้อกำหนดในการจัดซื้อ องค์กรควรกำหนดให้ชัดเจนว่า **ต้องการให้ AI ทำอะไร ใช้ข้อมูลใด ผลลัพธ์ถูกนำไปใช้อย่างไร และระบบมีระดับ B, E หรือ H ตามข้อ 3.1**

ข้อกำหนดควรเชื่อมโยงได้อย่างน้อยกับ **วัตถุประสงค์ ⟶ ความเสี่ยง ⟶ ข้อกำหนด ⟶ หลักฐาน ⟶ เกณฑ์ตรวจรับ**

5.1.1 วัตถุประสงค์และความสามารถของ AI

ข้อกำหนดควรระบุกรณีใช้งาน (Use Case) และความสามารถของ AI ที่จำเป็นต่อวัตถุประสงค์ เช่น การตรวจจับ การจำแนก การติดตาม การรู้จำ หรือการวิเคราะห์เหตุการณ์

ควรกำหนดด้วยว่าผลลัพธ์ของ AI จะถูกนำไปใช้อย่างไร โดยอาจพิจารณาตามลำดับดังนี้ **ให้ข้อมูล ⟶ แจ้งเตือน ⟶ สนับสนุนการตัดสินใจ ⟶ กระตุ้นการดำเนินการ ⟶ ดำเนินการโดยอัตโนมัติ**

หากผลลัพธ์จาก AI (AI Output) สามารถก่อให้เกิดผลกระทบต่อบุคคล ระบบ หรือภารกิจอื่น ควรกำหนดมาตรการเพิ่มเติมให้เหมาะสมกับระดับผลกระทบและความเสี่ยงตามข้อ 3.1

ไม่ควรกำหนดหรือเปิดใช้ความสามารถของ AI ที่ไม่มีความจำเป็นต่อวัตถุประสงค์เพียงเพราะผลิตภัณฑ์สามารถรองรับได้

5.1.2 สมรรถนะและเงื่อนไขการใช้งาน

ข้อกำหนดด้านสมรรถนะของ AI ควรสัมพันธ์กับกรณีใช้งานและสภาพแวดล้อมจริง และสามารถนำไปใช้เป็นเกณฑ์ตรวจรับได้

ควรพิจารณาตามความเหมาะสม เช่น

- สิ่ง บุคคล หรือเหตุการณ์ที่ต้องตรวจจับ จำแนก ติดตาม หรือระบุ
- สภาพแสง มุมกล้อง ระยะทาง การบดบัง และสภาพแวดล้อมที่มีผลต่อการทำงาน
- ประเภทของความผิดพลาดที่ต้องพิจารณา

- ระดับสมรรถนะที่ยอมรับได้
- วิธีการและเงื่อนไขการทดสอบ
- ข้อจำกัดของระบบที่ผู้ใช้งานควรทราบ

ไม่ควรกำหนดเพียงว่า “AI ต้องมีความแม่นยำสูง” โดยไม่มีเกณฑ์ วิธีการ หรือเงื่อนไขการทดสอบที่สามารถตรวจสอบได้

มาตรฐาน IEC 62676 series สามารถนำมาใช้ประกอบการกำหนดข้อกำหนดและการทดสอบระบบเฝ้าระวังด้วยวิดีโอและการวิเคราะห์วิดีโออัจฉริยะตามความเกี่ยวข้อง

5.1.3 ข้อกำหนดด้านความมั่นคงปลอดภัยของผลิตภัณฑ์

องค์กรควรกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยที่จำเป็นตามระดับผลกระทบและความเสี่ยง โดยอาจครอบคลุม

- การยืนยันตัวตนและการควบคุมสิทธิ
- การบริหารบัญชีผู้ดูแลและบัญชีบริการ (Service Account)
- การควบคุมการเข้าถึงจากระยะไกล (Remote Access)
- การเข้ารหัสข้อมูลตามความเหมาะสม
- การบันทึกเหตุการณ์ (Logging)
- การตั้งค่าที่มั่นคงปลอดภัย
- การปิดบริการหรือส่วนเชื่อมต่อระบบ (Interface) ที่ไม่จำเป็น
- การปรับปรุงเฟิร์มแวร์และซอฟต์แวร์ (Firmware and Software Update) อย่างมั่นคงปลอดภัย
- การตรวจสอบความถูกต้องและแหล่งที่มาของชุดปรับปรุง
- การสำรองและกู้คืนการตั้งค่าที่สำคัญ

ข้อกำหนดควรเน้น **ผลลัพธ์ด้านความมั่นคงปลอดภัย (Security Outcome)** มากกว่าการกำหนดวิธีการทางเทคนิคเพียงรูปแบบเดียว เว้นแต่มีข้อกำหนดที่มีผลใช้บังคับหรือมีเหตุผลด้านความเสี่ยงรองรับ

5.1.4 ความน่าเชื่อถือของ AI และผู้ผลิต

องค์กรควรพิจารณาความน่าเชื่อถือของระบบ AI รวมถึงความสามารถของผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการในการดูแลสมรรถนะ ความมั่นคงปลอดภัย และความเสี่ยงของผลิตภัณฑ์ตลอดระยะเวลาการใช้งาน ควรพิจารณาอย่างน้อยในเรื่อง

- มาตรฐานหรือแนวปฏิบัติที่เกี่ยวข้องกับผลิตภัณฑ์และองค์กร
- ผลการทดสอบหรือหลักฐานด้านสมรรถนะของ AI
- ข้อจำกัดและเงื่อนไขการใช้งานที่สำคัญ
- กระบวนการพัฒนาและควบคุมการเปลี่ยนแปลง

- กระบวนการบริหารช่องโหว่และการปรับปรุงด้านความมั่นคงปลอดภัย
- ระยะเวลาการสนับสนุนและการสิ้นสุดการสนับสนุน
- ความสามารถในการสนับสนุนเมื่อเกิดเหตุ

องค์กรอาจใช้ใบรับรองมาตรฐาน (Certification) รายงานผลการทดสอบ ผลการประเมินจากบุคคลที่สาม เอกสารทางเทคนิค หรือหลักฐานอื่นที่น่าเชื่อถือประกอบการพิจารณา

มาตรฐานที่อาจเกี่ยวข้อง เช่น IEC 62676 series, ISO/IEC 42001, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27036 series, ISO/IEC 29147 และ ISO/IEC 30111 ตามลักษณะของผลิตภัณฑ์ ผู้ผลิต และระดับความเสี่ยง

การมีใบรับรองมาตรฐานเพียงอย่างเดียวไม่ควรใช้เป็นหลักฐานว่าผลิตภัณฑ์เหมาะสมกับกรณีใช้งานขององค์กรโดยอัตโนมัติ

หลักสำคัญ องค์กรไม่จำเป็นต้องได้รับรายละเอียดภายในของ AI ทั้งหมด แต่ควรมีข้อมูลหรือหลักฐานที่เพียงพอเพื่อสร้างความเชื่อมั่นว่า ผลิตภัณฑ์มีสมรรถนะและความมั่นคงปลอดภัยที่เหมาะสม และผู้ผลิตสามารถดูแลผลิตภัณฑ์ตลอดวงจรชีวิต

5.1.5 ข้อกำหนดด้านข้อมูลและความเป็นส่วนตัว

ข้อกำหนดในการจัดซื้อควรทำให้องค์กรสามารถทราบและควบคุมวงจรการใช้ข้อมูลได้ตามความเหมาะสม โดยพิจารณาอย่างน้อยตามลำดับดังนี้ **ข้อมูลใดถูกเก็บ ⟶ ประมวลผลที่ใด ⟶ จัดเก็บที่ใด ⟶ ใครสามารถเข้าถึง ⟶ ส่งต่อให้ใคร ⟶ เก็บไว้นานเพียงใด ⟶ ลบหรือคืนข้อมูลอย่างไร**

ควรให้ความสำคัญเป็นพิเศษเมื่อมีข้อมูลชีวมิติ ข้อมูลการติดตาม หรือข้อมูลที่ AI สร้างหรืออนุมานขึ้น ข้อกำหนดควรสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและข้อกำหนดอื่นที่เกี่ยวข้อง รวมถึงอาจพิจารณาหลักการด้านการบริหารความเป็นส่วนตัวตาม ISO/IEC 27701 ตามความเหมาะสม

5.1.6 ข้อกำหนดสำหรับบริการคลาวด์และบริการภายนอก

กรณีใช้บริการคลาวด์หรือบริการ AI ภายนอก ควรกำหนดข้อพิจารณาที่จำเป็นตามระดับผลกระทบและความเสี่ยง เช่น

- สถานที่จัดเก็บข้อมูล (Data Location)
- สถานที่ประมวลผล (Processing Location)
- เขตอำนาจทางกฎหมาย (Jurisdiction)
- การเข้าถึงข้อมูลโดยผู้ให้บริการ
- ผู้ให้บริการช่วง (Subprocessor)
- การเข้ารหัสและการควบคุมกุญแจ
- การแจ้งเหตุด้านความมั่นคงปลอดภัย
- การสำรองและกู้คืน
- การเปลี่ยนแปลงบริการที่มีนัยสำคัญ
- การคืนและลบข้อมูล
- การยุติหรือเปลี่ยนผู้ให้บริการ (Exit Strategy)

การกำหนดให้ข้อมูลจัดเก็บหรือประมวลผลภายในประเทศ (Data Localization) ให้พิจารณาตามกฎหมาย ข้อกำหนดที่มีผลใช้บังคับ และผลการประเมินความเสี่ยง โดยควรพิจารณาร่วมกับอธิปไตยข้อมูล (Data Sovereignty) และไม่ควรใช้สถานที่จัดเก็บข้อมูล (Data Location) เพียงปัจจัยเดียวในการสรุปว่าบริการมีความมั่นคงปลอดภัยเพียงพอ

5.1.7 ความมั่นคงปลอดภัยของห่วงโซ่อุปทาน

องค์กรควรพิจารณาความเสี่ยงจากผู้ผลิต ผู้พัฒนา ผู้ติดตั้ง ผู้ให้บริการ และองค์ประกอบจากบุคคลที่สามที่เกี่ยวข้องกับระบบ CCTV ที่ใช้ AI ตลอดวงจรชีวิต

ควรพิจารณาตามความเสี่ยง เช่น

- การพัฒนาและดูแลผลิตภัณฑ์อย่างมั่นคงปลอดภัย
- การบริหารส่วนประกอบซอฟต์แวร์และองค์ประกอบจากบุคคลที่สาม
- การติดตามช่องโหว่ที่เกี่ยวข้อง
- การควบคุมแหล่งที่มาและความถูกต้องของชุดปรับปรุง
- การแจ้งข้อมูลด้านความมั่นคงปลอดภัย
- ระยะเวลาการสนับสนุนผลิตภัณฑ์
- ความสามารถในการจัดการความเสี่ยงจากผู้ส่งมอบช่วง

องค์กรไม่จำเป็นต้องได้รับรายละเอียดส่วนประกอบทั้งหมดของผลิตภัณฑ์ แต่ควรได้รับข้อมูลหลักฐาน หรือการสร้างความเชื่อมั่น (Assurance) ที่เพียงพอต่อการบริหารความเสี่ยง

สามารถพิจารณา ISO/IEC 27036 series เป็นกรอบอ้างอิงตามความเกี่ยวข้อง

5.1.8 การบริหารช่องโหว่และการปรับปรุงด้านความมั่นคงปลอดภัย

ผลิตภัณฑ์ ผู้ผลิต ผู้พัฒนา และผู้ให้บริการควรมีกระบวนการบริหารช่องโหว่และการปรับปรุงด้านความมั่นคงปลอดภัยตลอดระยะเวลาการสนับสนุน

องค์กรควรสามารถได้รับข้อมูลที่จำเป็นเมื่อพบช่องโหว่ที่มีผลต่อผลิตภัณฑ์หรือบริการ โดยอย่างน้อยควรทราบว่า **ผลิตภัณฑ์หรือรุ่นใดได้รับผลกระทบ ⟶ ลักษณะและผลกระทบของช่องโหว่ ⟶ การแก้ไขหรือชุดปรับปรุง (Update) ⟶ มาตรการลดความเสี่ยงระหว่างรอการแก้ไข ⟶ การทวนสอบผลการแก้ไข**

การมีช่องทางรับแจ้งช่องโหว่เพียงอย่างเดียวไม่ควรถือว่าเพียงพอ ควรมีกระบวนการที่ครอบคลุม **ค้นพบหรือรับแจ้ง ⟶ ตรวจสอบ ⟶ ประเมิน ⟶ จัดลำดับ ⟶ แก้ไขหรือลดความเสี่ยง ⟶ สื่อสาร ⟶ ทวนสอบ ⟶ ปิดประเด็น**

สามารถพิจารณา ISO/IEC 29147 และ ISO/IEC 30111 เป็นกรอบอ้างอิงตามความเกี่ยวข้อง

5.1.9 การเชื่อมต่อและการดำเนินการอัตโนมัติ

หากระบบ CCTV ที่ใช้ AI เชื่อมต่อกับระบบอื่น ควรกำหนดขอบเขตของข้อมูล สิทธิ และการดำเนินการให้ชัดเจน โดยอย่างน้อยควรทราบว่า **AI ส่งผลลัพธ์อะไร ⟶ ส่งไปยังระบบใด ⟶ ใช้สิทธิใด ⟶ ระบบปลายทางสามารถดำเนินการอะไร ⟶ ใครตรวจสอบ อนุมัติ หรือหยุดการดำเนินการได้**

ควรใช้หลักสิทธิเท่าที่จำเป็น (Least Privilege) และกำหนดขอบเขตการดำเนินการ (Action Boundary) ให้เหมาะสมกับความเสี่ยง

สำหรับระบบที่มีผลกระทบสูง ควรพิจารณาการกำกับดูแลโดยมนุษย์ (Human Oversight) การบันทึกหลักฐาน ความสามารถในการจำกัดหรือระงับการทำงาน และสภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe) ตามความเหมาะสม

5.1.10 หลักฐานประกอบการประเมิน

องค์กรควรกำหนดหลักฐานที่ใช้ยืนยันข้อกำหนดสำคัญให้เหมาะสมกับระดับผลกระทบและความเสี่ยง โดยหลักฐานอาจอยู่ในรูป

- เอกสารทางเทคนิค
- รายงานผลการทดสอบ
- การสาธิต
- การรับรองมาตรฐาน
- ผลการประเมินจากบุคคลที่สาม
- ผลการทดสอบด้านความมั่นคงปลอดภัย

- หลักฐานกระบวนการของผู้ผลิต
- การตรวจสอบภายใต้ข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA)
- หลักฐานอื่นที่สามารถสร้างความเชื่อมั่นได้

สำหรับระบบระดับ H อาจกำหนดหลักฐานที่มีระดับความเป็นอิสระหรือความน่าเชื่อถือสูงขึ้นตามระดับความเสี่ยง

ไม่ควรกำหนดให้ผู้ผลิตต้องเปิดเผยข้อมูลที่เป็นความลับทั้งหมด หากสามารถใช้หลักฐานอื่นเพื่อสร้างความเชื่อมั่นได้อย่างเพียงพอ

5.1.11 เกณฑ์การตรวจรับ

ข้อกำหนดที่สำคัญควรถูกกำหนดให้สามารถตรวจสอบหรือทดสอบได้ตั้งแต่ขั้นตอนการจัดซื้อ โดยควรเชื่อมโยงได้ตามหลักดังนี้ **ข้อกำหนด (Requirement) ⟶ วิธีตรวจสอบหรือหลักฐาน (Evidence/Test) ⟶ เกณฑ์ยอมรับ (Acceptance Criteria)**

ตัวอย่างเช่น

ข้อกำหนด	วิธีตรวจสอบ
AI ทำงานตามกรณีใช้งาน (Use Case)	ทดสอบกับสถานการณ์และสภาพแวดล้อมที่กำหนด
การควบคุมการเข้าถึงจากระยะไกล (Remote Access)	ตรวจสอบการตั้งค่า (Configuration) และทดสอบการเข้าถึง
การบันทึกเหตุการณ์ (Logging)	สร้างเหตุการณ์ทดสอบและตรวจสอบบันทึก
ส่วนเชื่อมต่อโปรแกรมประยุกต์และการเชื่อมต่อระบบ (API/Integration)	ทดสอบข้อมูล สิทธิ และขอบเขตการดำเนินการ
สมรรถนะของ AI (AI Performance)	ทดสอบตามเกณฑ์และเงื่อนไขที่กำหนด
สภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe)	จำลองกรณี AI หรือบริการสำคัญไม่พร้อมใช้งาน
วงจรการสนับสนุนผลิตภัณฑ์ (Support Lifecycle)	ตรวจสอบข้อมูลการสนับสนุนจากผู้ผลิต

ไม่ควรกำหนดข้อกำหนดที่ไม่สามารถตรวจสอบได้ เช่น “ระบบต้องมีความมั่นคงปลอดภัยสูง” หรือ “AI ต้องมีความแม่นยำสูง” โดยไม่มีเกณฑ์ วิธีการทดสอบ หรือหลักฐานประกอบ

หลักสำคัญของข้อ 5.1: การจัดซื้อระบบ CCTV ที่ใช้ AI ควรกำหนดให้ชัดเจนว่า **ต้องการผลลัพธ์อะไร ⟶ ความเสี่ยงใดต้องได้รับการควบคุม ⟶ ต้องการหลักฐานอะไร ⟶ และจะตรวจรับอย่างไร**

5.2 การส่งมอบและการตรวจรับอย่างมั่นคงปลอดภัย

การตรวจรับระบบ CCTV ที่ใช้ AI ควรยืนยันว่าระบบที่ติดตั้งจริงตรงตามขอบเขตและข้อกำหนดที่ได้รับอนุมัติ ทำงานตามกรณีใช้งาน มีมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม และสามารถบริหารดูแลต่อได้

การตรวจรับไม่ควรจำกัดอยู่เพียงการตรวจว่ากล้องสามารถแสดงภาพ บันทึกข้อมูล หรือ AI สามารถสร้างผลลัพธ์ได้

5.2.1 การตรวจสอบระบบที่ส่งมอบ

ควรตรวจสอบองค์ประกอบสำคัญตามความเหมาะสม เช่น **อุปกรณ์ ⟶ เฟิร์มแวร์และซอฟต์แวร์ (Firmware/Software) ⟶ ความสามารถของ AI (AI Capability) ⟶ การตั้งค่า (Configuration) ⟶ ข้อมูล (Data) ⟶ การเข้าถึงและสิทธิ (Access) ⟶ การเชื่อมต่อระบบ (Integration) ⟶ บริการภายนอก (External Service)**

ระบบที่ส่งมอบควรตรงตามสิ่งที่ได้รับอนุมัติและข้อกำหนดในการจัดซื้อ

หากพบความแตกต่างที่มีนัยสำคัญ ควรประเมินผลกระทบและความเสี่ยงก่อนการยอมรับระบบ

5.2.2 การทดสอบสมรรถนะและการทำงานของ AI

AI ควรได้รับการทดสอบตามกรณีใช้งานและเกณฑ์ตรวจรับที่กำหนดไว้

การทดสอบควรพิจารณาอย่างน้อยว่า **AI ทำงานตามวัตถุประสงค์หรือไม่ ⟶ ผลลัพธ์อยู่ในระดับที่ยอมรับได้หรือไม่ ⟶ รูปแบบความผิดพลาดอยู่ในระดับที่ยอมรับได้หรือไม่ ⟶ ข้อจำกัดสำคัญได้รับการรับทราบหรือไม่**

สำหรับระบบระดับ E หรือ H ควรเพิ่มความเข้มของการทดสอบตามระดับผลกระทบและความเสี่ยง เช่น การทดสอบในสภาพแวดล้อมจริง หรือสถานการณ์ที่ความผิดพลาดอาจก่อให้เกิดผลกระทบสูง

5.2.3 การตรวจสอบความมั่นคงปลอดภัยก่อนเปิดใช้งาน

ควรตรวจสอบตามความเหมาะสมว่า

- บัญชีและสิทธิถูกกำหนดอย่างเหมาะสม
- ไม่มีข้อมูลรับรองเริ่มต้น (Default Credential) ที่ไม่เหมาะสม
- บริการที่ไม่จำเป็นถูกปิด
- การเข้าถึงจากระยะไกล (Remote Access) ได้รับการควบคุม
- การบันทึกเหตุการณ์ (Logging) สามารถใช้งานได้
- เฟิร์มแวร์และซอฟต์แวร์ (Firmware and Software) อยู่ในสถานะที่ได้รับอนุมัติ
- ความสามารถของ AI (AI Capability) ตรงตามขอบเขตที่กำหนด

- ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) และการเชื่อมต่อระบบเป็นไปตามการออกแบบ

ผลการตรวจสอบควรถูกใช้เป็นข้อมูลสำหรับกำหนดค่าฐานที่ได้รับอนุมัติ (Approved Baseline) ตามข้อ 4.4

5.2.4 การตรวจสอบการเชื่อมต่อและการดำเนินการต่อ

หากผลลัพธ์จาก AI (AI Output) ถูกส่งต่อไปยังระบบอื่น ควรทดสอบเส้นทางสำคัญตามลำดับ เช่น **ผลลัพธ์จาก AI ⟶ ส่วนเชื่อมต่อระบบ (API/Interface) ⟶ กระบวนงานอัตโนมัติ (Workflow) ⟶ การตัดสินใจหรือการอนุมัติ (Decision/Approval) ⟶ การดำเนินการของระบบ (Action)**

สำหรับระบบที่มีการดำเนินการอัตโนมัติ (Automated Action) ควรทดสอบว่าการดำเนินการอยู่ภายในขอบเขตการดำเนินการ (Action Boundary) ที่ได้รับอนุญาต และสามารถจำกัด ระงับ หรือเข้าสู่สภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe) ได้เมื่อจำเป็น

5.2.5 การส่งมอบข้อมูลและเอกสาร

ผู้ส่งมอบควรจัดให้มีข้อมูลที่จำเป็นต่อการบริหารและดูแลระบบอย่างต่อเนื่องตามความเหมาะสม เช่น

- ข้อมูลอุปกรณ์และรุ่น
- เฟิร์มแวร์และซอฟต์แวร์ (Firmware and Software) ที่สำคัญ
- ความสามารถของ AI (AI Capability) หรือข้อมูลเกี่ยวกับ AI ที่จำเป็นต่อการบริหารระบบ
- การตั้งค่า (Configuration) ที่สำคัญ
- ข้อมูลการเชื่อมต่อกับระบบอื่น
- คู่มือการใช้งานและบำรุงรักษา
- วิธีการปรับปรุงระบบ การสำรอง และการกู้คืน (Update, Backup and Recovery)
- ช่องทางสนับสนุนและการบริหารช่องโหว่
- ข้อมูลวงจรการสนับสนุน
- รายงานผลการทดสอบและตรวจรับ

ไม่จำเป็นต้องกำหนดรูปแบบเอกสารเพียงรูปแบบเดียว หากข้อมูลและหลักฐานที่ได้รับเพียงพอต่อการใช้งาน การบริหารความเสี่ยง และการตรวจสอบย้อนหลัง

5.2.6 การยกเลิกสิทธิของผู้ติดตั้งและบัญชีชั่วคราว

ก่อนเปิดใช้งานจริง ควรตรวจสอบบัญชี สิทธิ และช่องทางการเข้าถึงที่ถูกสร้างขึ้นระหว่างการติดตั้ง เช่น **บัญชีชั่วคราว (Temporary Account) ⟶ บัญชีผู้ติดตั้ง (Installer Account) ⟶ การเข้าถึงจากระยะไกล (Remote Access) ⟶ โทเคนหรือกุญแจ (Token/Key) ⟶ การเชื่อมต่อเพื่อการทดสอบ (Test Connection)**

รายการที่ไม่มีความจำเป็นควรถูกยกเลิก หรือลดสิทธิให้เหลือเท่าที่จำเป็นก่อนเปิดใช้งานจริง

หากจำเป็นต้องคงการเข้าถึงของผู้ผลิตหรือผู้ให้บริการเพื่อสนับสนุนระบบ ควรกำหนดขอบเขตสิทธิ วิธีการอนุญาต การบันทึกเหตุการณ์ และการทบทวนสิทธิให้เหมาะสมกับระดับความเสี่ยง

5.2.7 การตรวจสอบมาตรฐาน การรับรอง และหลักฐาน

หากข้อกำหนดในการจัดซื้อ (TOR) หรือสัญญากำหนดมาตรฐาน การรับรอง ผลการทดสอบ หรือหลักฐานการสร้างความเชื่อมั่น องค์กรควรตรวจสอบอย่างน้อยว่า **หลักฐานมีอยู่จริง ⟶ ยังมีผลหรืออยู่ในสถานะที่เหมาะสม ⟶ ขอบข่ายครอบคลุมผลิตภัณฑ์ องค์กร หรือบริการที่จัดหา ⟶ ผู้ออกหรือผู้ประเมินเป็นไปตามข้อกำหนด ⟶ หลักฐานตรงกับสิ่งที่ส่งมอบ**

ตัวอย่างมาตรฐานที่อาจเกี่ยวข้อง ได้แก่

- IEC 62676 series
- ISO/IEC 42001
- ISO/IEC 27001
- ISO/IEC 27701
- ISO/IEC 27036 series
- ISO/IEC 29147
- ISO/IEC 30111

รายการดังกล่าวเป็นเพียงตัวอย่าง และไม่ควรตีความว่าผู้ผลิต ผลิตภัณฑ์ หรือผู้ให้บริการทุกกรณีต้องได้รับการรับรองตามมาตรฐานทั้งหมด

5.2.8 การตรวจสอบบริการคลาวด์ สถานที่จัดเก็บข้อมูล และอธิปไตยข้อมูล

กรณีใช้บริการคลาวด์หรือบริการภายนอก ควรตรวจสอบว่าสภาพแวดล้อมที่ใช้งานจริงตรงตามข้อกำหนดที่ได้รับอนุมัติ โดยเฉพาะ

- สถานที่จัดเก็บข้อมูล (Data Location)
- สถานที่ประมวลผล (Processing Location)
- เขตอำนาจทางกฎหมาย (Jurisdiction)
- ผู้ให้บริการช่วง (Subprocessor)
- การเข้าถึงจากภายนอกหรือจากต่างประเทศ
- การควบคุมกุญแจเข้ารหัสตามความเกี่ยวข้อง
- เงื่อนไขการคืนและลบข้อมูล

หากกฎหมาย ประกาศ ข้อกำหนดในการจัดซื้อ (TOR) สัญญา หรือผลการประเมินความเสี่ยงกำหนดเงื่อนไขด้านการกำหนดที่ตั้งข้อมูล (Data Localization) หรืออธิปไตยข้อมูล (Data Sovereignty) ควรตรวจสอบหลักฐานว่าระบบที่ส่งมอบเป็นไปตามเงื่อนไขดังกล่าว

5.2.9 การจัดการข้อบกพร่องและความเสี่ยงคงเหลือ

ข้อบกพร่องหรือประเด็นที่ยังไม่แล้วเสร็จควรได้รับการบันทึกและกำหนดแนวทางดำเนินการอย่างน้อยตามลำดับดังนี้ **ประเด็น ⟶ ผลกระทบ ⟶ มาตรการชั่วคราวหรือการแก้ไข ⟶ ผู้รับผิดชอบ ⟶ กำหนดเวลา ⟶ การติดตามผล**

กรณีมีความเสี่ยงคงเหลือ (Residual Risk) ที่มีนัยสำคัญ ควรได้รับการพิจารณาและยอมรับโดยผู้มีอำนาจตามกระบวนการบริหารความเสี่ยงขององค์กร

การลงนามตรวจรับทางเทคนิคไม่ควรถูกตีความโดยอัตโนมัติว่าเป็นการยอมรับความเสี่ยงทั้งหมดของระบบ

5.2.10 ผลการตรวจรับ

ผลการตรวจรับควรสรุปได้อย่างน้อยเป็น

☐ **ผ่านและพร้อมเปิดใช้งาน**

☐ **ผ่านโดยมีเงื่อนไข**

☐ **ต้องดำเนินการแก้ไขก่อนเปิดใช้งาน**

สำหรับกรณีผ่านโดยมีเงื่อนไข ควรกำหนดผู้รับผิดชอบ กำหนดเวลา มาตรการที่จำเป็น และการติดตามจนประเด็นได้รับการดำเนินการในระดับที่ยอมรับได้

สามารถใช้ **ภาคผนวก ก รายการตรวจสอบก่อนส่งมอบ (Pre-Handover Checklist)** เป็นเครื่องมือประกอบการตรวจรับได้

สรุปหลักการของบทที่ 5

การจัดซื้อจัดจ้างระบบ CCTV ที่ใช้ AI ควรเชื่อมโยงอย่างตรวจสอบย้อนหลังได้ตั้งแต่ **วัตถุประสงค์และกรณีใช้งาน ⟶ ผลกระทบและความเสี่ยง ⟶ ข้อกำหนดในการจัดซื้อจัดจ้าง ⟶ หลักฐานความสอดคล้อง ⟶ การทดสอบและตรวจรับ ⟶ การสนับสนุนตลอดวงจรชีวิต**

การประเมินไม่ควรพิจารณาเฉพาะคุณสมบัติทางเทคนิค ราคา หรือใบรับรองมาตรฐาน แต่ควรครอบคลุมสมรรถนะและข้อจำกัดของ AI ความมั่นคงปลอดภัยของผลิตภัณฑ์ การบริหารช่องโหว่ ความน่าเชื่อถือของผู้ผลิตและผู้ให้บริการ ห่วงโซ่อุปทาน การเปลี่ยนแปลงและการสนับสนุนผลิตภัณฑ์ ตลอดจนความสามารถในการแสดงหลักฐานและตรวจสอบได้ตามระดับผลกระทบและความเสี่ยง

บทที่ 6 หัวข้อที่ต้องพิจารณาเพิ่มเติม

ระบบ CCTV ที่ใช้ AI อาจมีรูปแบบการประมวลผลและการเชื่อมต่อที่หลากหลาย เช่น การประมวลผลภายในกล้อง การประมวลผลที่ Edge หรือศูนย์ข้อมูล การใช้บริการคลาวด์ หรือการใช้บริการ AI จากภายนอก รวมถึงอาจมีการประมวลผลข้อมูลชีวมิติหรือการติดตามบุคคล

กรณีดังกล่าวอาจทำให้ระดับผลกระทบและความเสี่ยงเพิ่มขึ้น องค์กรจึงควรพิจารณามาตรการเพิ่มเติมตามลักษณะของระบบและผลการประเมินตามข้อ 3.1

6.1 การใช้บริการคลาวด์และบริการภายนอกอย่างมั่นคงปลอดภัย

การใช้บริการคลาวด์หรือบริการ AI ภายนอกร่วมกับ CCTV-AI ควรพิจารณาทั้งด้านความมั่นคงปลอดภัย ความเป็นส่วนตัว ความต่อเนื่องของบริการ และอธิปไตยข้อมูล โดยไม่ควรพิจารณาเฉพาะความสะดวกในการใช้งานหรือสถานที่จัดเก็บข้อมูลเพียงอย่างเดียว

6.1.1 สถานที่จัดเก็บและประมวลผลข้อมูล

องค์กรควรทราบในระดับที่เหมาะสมว่า **ข้อมูลใดถูกส่งออก ⟶ จัดเก็บที่ใด ⟶ ประมวลผลที่ใด ⟶ ใครสามารถเข้าถึง ⟶ อยู่ภายใต้เขตอำนาจทางกฎหมายใด**

ควรพิจารณาอย่างน้อย

- สถานที่จัดเก็บข้อมูล (Data Location)
- สถานที่ประมวลผล (Processing Location)
- เขตอำนาจทางกฎหมาย (Jurisdiction)
- การเข้าถึงเพื่อการบริหารระบบจากภายนอกหรือจากต่างประเทศ
- ผู้ให้บริการช่วง (Subprocessor)
- การสำรองและสำเนาข้อมูลที่อาจอยู่ในพื้นที่อื่น

การกำหนดให้ข้อมูลอยู่ภายในประเทศ (Data Localization) ควรพิจารณาตามกฎหมาย ข้อกำหนดที่มีผลใช้บังคับ และผลการประเมินความเสี่ยง โดยไม่ควรตีความว่าการจัดเก็บข้อมูลภายในประเทศเพียงอย่างเดียวทำให้ระบบมีความมั่นคงปลอดภัยครบถ้วน

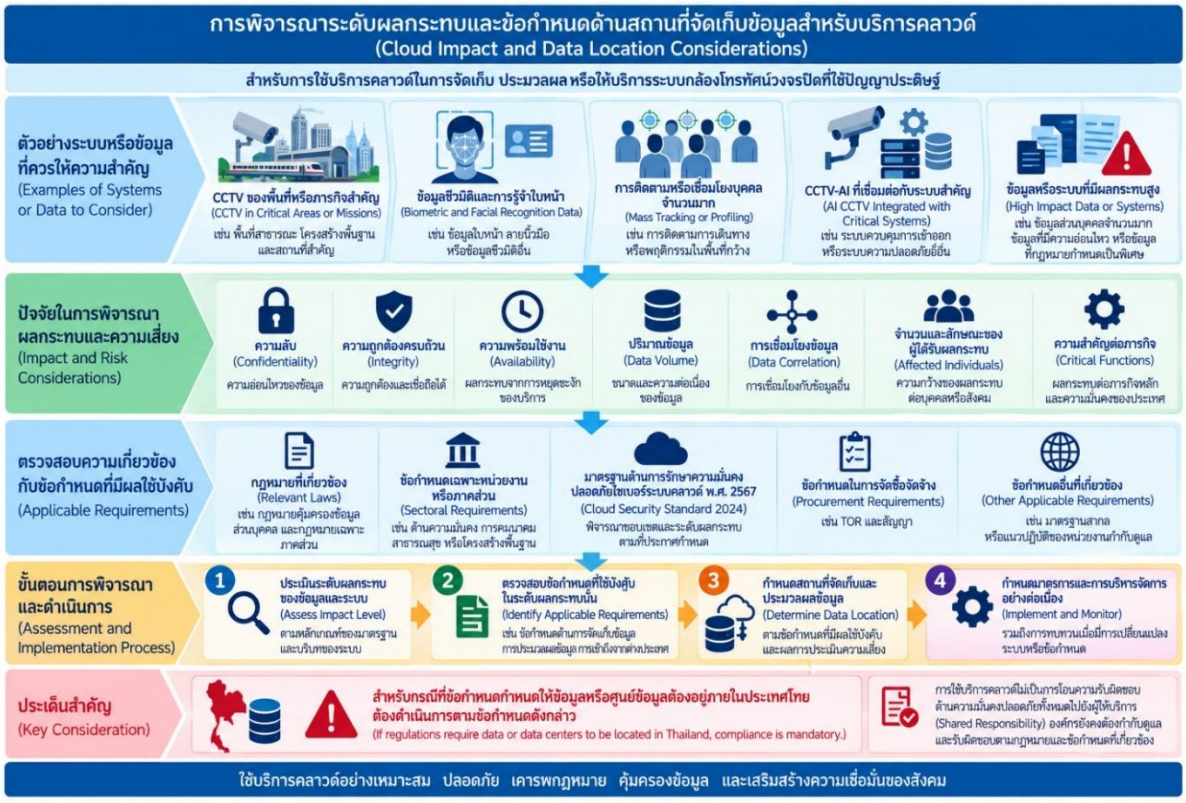
6.1.2 อธิปไตยข้อมูล

การพิจารณาอธิปไตยข้อมูลควรครอบคลุมมากกว่าสถานที่ตั้งของศูนย์ข้อมูล โดยพิจารณาว่าองค์กรยังสามารถกำกับ ควบคุม และบังคับใช้ข้อกำหนดที่เกี่ยวข้องกับข้อมูลได้เพียงใด

ปัจจัยที่ควรพิจารณา เช่น

- กฎหมายหรือเขตอำนาจที่มีผลต่อผู้ให้บริการและข้อมูล
- การเข้าถึงข้อมูลโดยบุคลากรหรือผู้ให้บริการจากต่างประเทศ
- ผู้ให้บริการช่วงและห่วงโซ่การให้บริการ
- การเข้ารหัสและการควบคุมกุญแจ (Encryption Key Control)
- ความสามารถในการตรวจสอบหรือได้รับหลักฐานจากผู้ให้บริการ
- การคืน ลบ หรือเคลื่อนย้ายข้อมูลเมื่อยุติบริการ
- ความสามารถในการเปลี่ยนผู้ให้บริการโดยไม่สูญเสียการควบคุมข้อมูล

สำหรับระบบหรือข้อมูลที่มีผลกระทบสูง ควรเพิ่มระดับการพิจารณาและหลักฐานที่เกี่ยวข้องตามความเหมาะสม



รูปที่ 6 การพิจารณาระดับผลกระทบและข้อกำหนดด้านสถานที่จัดเก็บข้อมูลสำหรับบริการคลาวด์

หลักสำคัญ การกำหนดที่ตั้งข้อมูล (Data Localization) เป็นมาตรการหนึ่งที่อาจนำมาใช้เพื่อสนับสนุนการบริหารอธิปไตยข้อมูล (Data Sovereignty) แต่ไม่ใช่มาตรการทั้งหมดที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยและการควบคุมข้อมูล

การพิจารณาอธิปไตยข้อมูลไม่ควรพิจารณาจากสถานที่จัดเก็บข้อมูลเพียงปัจจัยเดียว แต่ควรพิจารณามาตรการที่เกี่ยวข้องร่วมกันตามระดับผลกระทบและความเสี่ยง ได้แก่ สถานที่จัดเก็บข้อมูล (Data Location) สถานที่ประมวลผลข้อมูล (Processing Location) เขตอำนาจทางกฎหมาย (Jurisdiction) การเข้าถึงข้อมูลจากภายนอกหรือจากต่างประเทศ ผู้ให้บริการช่วง (Subprocessor) การเข้ารหัสและการควบคุมกุญแจ การสำรองและกู้คืนข้อมูล ความสามารถในการเคลื่อนย้ายข้อมูลหรือภาระงาน ตลอดจนการยุติหรือเปลี่ยนผู้ให้บริการ (Exit Strategy)

การกำหนดให้ข้อมูลจัดเก็บหรือประมวลผลภายในประเทศ (Data Localization) เป็นมาตรการหนึ่งที่สามารถนำมาใช้เพื่อสนับสนุนอธิปไตยข้อมูล โดยควรพิจารณาตามกฎหมาย ข้อกำหนดที่มีผลใช้บังคับ ลักษณะและความสำคัญของข้อมูล ระดับผลกระทบ และผลการประเมินความเสี่ยง ทั้งนี้ การจัดเก็บข้อมูลภายในประเทศเพียงอย่างเดียวไม่ควรถูกใช้เป็นหลักฐานว่าระบบมีอธิปไตยข้อมูลหรือมีความมั่นคงปลอดภัยอย่างเพียงพอ

สำหรับระบบที่มีระดับผลกระทบหรือความสำคัญสูง องค์กรควรพิจารณาความสามารถในการควบคุมข้อมูลและกุญแจเข้ารหัส การเข้าถึงข้อมูลโดยผู้ให้บริการหรือบุคคลจากภายนอกประเทศ ความสามารถในการตรวจสอบผู้ให้บริการช่วง ตลอดจนความสามารถในการเคลื่อนย้ายข้อมูลและเปลี่ยนผู้ให้บริการ เพื่อลดการพึ่งพาผู้ให้บริการรายเดียวและสนับสนุนความต่อเนื่องของบริการตามความเหมาะสม

6.1.3 การแบ่งความรับผิดชอบกับผู้ให้บริการ

องค์กรควรกำหนดให้ชัดเจนว่าองค์กรและผู้ให้บริการรับผิดชอบมาตรการใด โดยอาจพิจารณาตามลำดับ เช่น **บัญชีและสิทธิ ⟶ การตั้งค่า ⟶ การเข้ารหัส ⟶ การสำรองและกู้คืน ⟶ การบันทึกเหตุการณ์ (Logging) ⟶ การบริหารช่องโหว่ (Vulnerability Management) ⟶ การจัดการเหตุการณ์ (Incident Management) ⟶ การคืนหรือลบข้อมูล (Data Return/Deletion)**

การใช้บริการคลาวด์หรือบริการ AI ภายนอกไม่ควรถูกตีความว่าเป็นการโอนความรับผิดชอบด้านความมั่นคงปลอดภัยทั้งหมดไปยังผู้ให้บริการ

ในทางกลับกัน องค์กรไม่จำเป็นต้องควบคุมองค์ประกอบที่ผู้ให้บริการเป็นผู้รับผิดชอบโดยตรง หากมีการกำหนดหน้าที่และหลักฐานการสร้างความเชื่อมั่นที่เหมาะสม

6.1.4 การคุ้มครองการเข้าถึงและข้อมูล

การเข้าถึงระบบผ่าน Web Application, Mobile Application, Remote Management หรือบริการภายนอกควรถูกจำกัดให้เฉพาะผู้ที่ได้รับอนุญาตและเท่าที่จำเป็น

ควรพิจารณาตามความเสี่ยง เช่น

- การยืนยันตัวตน
- การกำหนดสิทธิตามบทบาท

- การควบคุมบัญชีผู้ดูแล
- การบันทึกการเข้าถึงที่สำคัญ
- การควบคุมการดาวน์โหลดหรือส่งออกข้อมูล
- การเข้ารหัสข้อมูลขณะส่งและขณะจัดเก็บตามความเหมาะสม
- การยกเลิกสิทธิเมื่อหมดความจำเป็น

สำหรับระบบที่มีผลกระทบสูง ควรเพิ่มความเข้มของมาตรการตามผลการประเมินความเสี่ยง

6.1.5 ความต่อเนื่องและการออกจากบริการ

องค์กรควรพิจารณาว่าหาก **บริการคลาวด์ (Cloud Service) บริการ AI ภายนอก (External AI Service)** หรือการเชื่อมต่อเครือข่ายไม่พร้อมใช้งาน ระบบ CCTV ที่ใช้ AI จะยังสามารถสนับสนุนภารกิจที่จำเป็นได้หรือไม่

แนวทางอาจพิจารณาตามลำดับ เช่น **บริการตามปกติ ⟶ การทำงานแบบจำกัด (Degraded Mode) ⟶ CCTV พื้นฐาน ⟶ การตรวจสอบโดยบุคลากร ⟶ สภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe)**

สำหรับระบบที่มีความสำคัญสูง ควรกำหนดความสามารถในการนำข้อมูล การตั้งค่า และหลักฐานที่จำเป็นกลับคืน รวมถึง **แนวทางการเปลี่ยนหรือยุติบริการ (Exit Strategy)** ตั้งแต่ก่อนเริ่มใช้บริการ

6.1.6 มาตรฐานและข้อกำหนดที่เกี่ยวข้อง

กรณีองค์กรหรือบริการอยู่ในขอบเขตของข้อกำหนดด้านความมั่นคงปลอดภัยระบบคลาวด์ของประเทศไทย ให้ดำเนินการตามข้อกำหนดที่มีผลใช้บังคับ

มาตรฐานสากล เช่น **ISO/IEC 27017** สำหรับมาตรการความมั่นคงปลอดภัยของบริการคลาวด์ และ **ISO/IEC 27018** สำหรับการคุ้มครองข้อมูลส่วนบุคคลใน Public Cloud อาจใช้เป็นกรอบอ้างอิงเพิ่มเติมตามความเหมาะสม

หลักสำคัญของข้อ 6.1: การใช้ Cloud สำหรับ CCTV-AI ควรพิจารณา **“ข้อมูลอะไร ⟶ อยู่และประมวลผลที่ใด ⟶ ใครควบคุมอะไร ⟶ อยู่ภายใต้กฎหมายใด ⟶ หากบริการเปลี่ยนหรือหยุด จะดำเนินการอย่างไร”**

6.2 การวิเคราะห์วิดีโออัจฉริยะและข้อมูลชีวมิติ

การใช้ AI กับ CCTV สามารถเพิ่มความสามารถจากการบันทึกภาพไปสู่การตรวจจับ จำแนก ติดตาม ระบุ และสร้างข้อสรุปเกี่ยวกับบุคคลหรือเหตุการณ์ ซึ่งอาจเพิ่มผลกระทบด้านความเป็นส่วนตัว ความถูกต้องของผลลัพธ์ และสิทธิของบุคคล

การเพิ่มความสามารถ AI จึงควรพิจารณาว่า **ความสามารถใหม่ทำให้วัตถุประสงค์ ลักษณะข้อมูล หรือระดับผลกระทบของระบบเปลี่ยนไปหรือไม่**

6.2.1 การวิเคราะห์วิดีโออัจฉริยะ

ความสามารถ เช่น Object Detection, Classification, Tracking, License Plate Recognition หรือ Behavioral Analytics ควรมีวัตถุประสงค์ที่ชัดเจนและสัมพันธ์กับความจำเป็นขององค์กร

ควรพิจารณา **วัตถุประสงค์ ⟶ ข้อมูลที่ใช้ ⟶ สิ่งที่ AI วิเคราะห์ ⟶ ผลลัพธ์ที่สร้าง ⟶ ผู้ที่ใช้ผลลัพธ์ ⟶ การดำเนินการที่ตามมา**

ยิ่งผลลัพธ์ถูกนำไปใช้กับการตัดสินใจหรือการดำเนินการที่มีผลกระทบสูง ยิ่งควรเพิ่มระดับการทดสอบ การกำกับดูแล และการตรวจสอบย้อนหลัง

6.2.2 การระบุและติดตามบุคคล

ระบบที่สามารถระบุ ติดตาม หรือเชื่อมโยงกิจกรรมของบุคคลข้ามเวลา พื้นที่ หรือแหล่งข้อมูล ควรได้รับการประเมินความเสี่ยงเพิ่มเติม

ควรพิจารณาอย่างน้อย

- ความจำเป็นและวัตถุประสงค์
- ขอบเขตพื้นที่และระยะเวลาการติดตาม
- จำนวนและลักษณะของบุคคลที่อาจได้รับผลกระทบ
- ความสามารถในการระบุตัวบุคคล
- การเชื่อมโยงกับฐานข้อมูลหรือระบบอื่น
- การนำผลลัพธ์ไปใช้
- ผลกระทบหาก AI ให้ผลลัพธ์ผิด

การมีความสามารถทางเทคนิคในการติดตามบุคคล ไม่ควรถือเป็นเหตุผลเพียงพอในการเปิดใช้ความสามารถดังกล่าว

6.2.3 ข้อมูลชีวมิติ

กรณี CCTV-AI ประมวลผลข้อมูลชีวมิติ เช่น ใบหน้า หรือลักษณะเฉพาะของบุคคลเพื่อการระบุหรือยืนยันตัวบุคคล ควรเพิ่มระดับการควบคุมให้เหมาะสมกับผลกระทบและข้อกำหนดที่เกี่ยวข้อง

ควรพิจารณาเป็นพิเศษในเรื่อง

- ความชอบด้วยกฎหมายและความจำเป็น
- การจำกัดวัตถุประสงค์
- การควบคุมสิทธิการเข้าถึง
- การคุ้มครองข้อมูลและแม่แบบชีวมิติ
- ระยะเวลาการเก็บรักษา
- การส่งต่อหรือเชื่อมโยงข้อมูล
- การลบข้อมูลเมื่อหมดความจำเป็น
- ผลกระทบจากการระบุบุคคลผิด

มาตรฐาน **ISO/IEC 24745** สามารถใช้เป็นกรอบอ้างอิงด้านการคุ้มครองข้อมูลชีวมิติได้ตามความเกี่ยวข้อง

6.2.4 สมรรถนะและความผิดพลาดของระบบชีวมิติ

การประเมินระบบชีวมิติไม่ควรพิจารณาเฉพาะค่าความแม่นยำโดยรวม แต่ควรพิจารณาประเภทและผลกระทบของความผิดพลาด เช่น

- การยอมรับบุคคลผิด
- การปฏิเสธบุคคลที่ถูกต้อง
- การระบุบุคคลผิด
- การไม่สามารถตรวจจับหรือจับคู่ได้ในบางสภาพแวดล้อม

การทดสอบควรสัมพันธ์กับกรณีใช้งาน สภาพแวดล้อม คุณภาพข้อมูล และลักษณะของกลุ่มบุคคลที่เกี่ยวข้อง

มาตรฐาน **ISO/IEC 19795-1** สามารถใช้ประกอบการทดสอบและรายงานสมรรถนะของระบบชีวมิติได้ตามความเหมาะสม

ค่าความเชื่อมั่น (Confidence Score) หรือผลการจับคู่ (Match) ไม่ควรถูกตีความว่าเป็นการยืนยันตัวบุคคลที่ถูกต้องโดยอัตโนมัติ

6.2.5 การป้องกันการหลอกระบบชีวมิติ

สำหรับระบบที่ใช้ข้อมูลชีวมิติเพื่อการระบุหรือยืนยันบุคคลในบริบทที่มีความเสี่ยง ควรพิจารณาความเสี่ยงจากการใช้ภาพ วัตถุ หรือวิธีการอื่นเพื่อหลอกระบบ

ระดับของมาตรการควรสัมพันธ์กับวัตถุประสงค์และผลกระทบของระบบ โดยอาจพิจารณา **ISO/IEC 30107 series** ด้านการตรวจจับการโจมตีด้วยการนำเสนอลักษณะชีวมิติ (Presentation Attack Detection) ตามความเหมาะสม

6.2.6 การกำกับดูแลผลลัพธ์ที่มีผลกระทบสูง

เมื่อ AI Output ถูกนำไปใช้กับการตัดสินใจหรือการดำเนินการที่อาจส่งผลกระทบสูงต่อบุคคล ควรมีมาตรการกำกับดูแลที่เพิ่มขึ้น เช่น

- การตรวจสอบข้อมูลหรือหลักฐานประกอบ
- การทวนสอบโดยบุคลากร (Human Review)
- การกำหนดผู้มีอำนาจตัดสินใจ
- การบันทึกเหตุการณ์หรือเหตุผลที่สำคัญ
- การแก้ไขเมื่อพบผลลัพธ์ผิด
- การหยุดหรือระงับการใช้ AI Output

ระดับการกำกับดูแลควรสัมพันธ์กับความรุนแรงและความสามารถในการย้อนกลับของผลกระทบ

6.2.7 การประเมินก่อนเพิ่มความสามารถ AI ใหม่

การเพิ่มความสามารถ AI ให้กับระบบเดิมควรได้รับการพิจารณาก่อนเปิดใช้งาน โดยเฉพาะเมื่อทำให้เกิด **ข้อมูลใหม่ ⟶ การวิเคราะห์ใหม่ ⟶ การติดตามหรือระบุบุคคลเพิ่มขึ้น ⟶ การเชื่อมต่อใหม่ ⟶ การตัดสินใจหรือการดำเนินการใหม่**

หากการเปลี่ยนแปลงดังกล่าวอาจมีผลต่อวัตถุประสงค์ ข้อมูล บุคคลที่ได้รับผลกระทบ หรือระดับอำนาจของ AI ควรพิจารณาเป็นการเปลี่ยนแปลงที่มีนัยสำคัญ และประเมินใหม่ตามข้อ 3.1

หลักสำคัญของข้อ 6.2: การนำ AI มาเพิ่มความสามารถให้ CCTV ไม่ควรพิจารณาเพียงว่า “ระบบสามารถทำได้หรือไม่” แต่ควรพิจารณาว่า **“จำเป็นหรือไม่ ⟶ มีผลกระทบต่อใคร ⟶ ผลลัพธ์เชื่อถือได้เพียงใด ⟶ ใครเป็นผู้ใช้หรือตัดสินใจ ⟶ และมีมาตรการควบคุมเพียงพอหรือไม่”**

6.3 เทคโนโลยีที่เกี่ยวเนื่องและการพัฒนาในอนาคต

แนวปฏิบัติฉบับนี้มุ่งเน้นระบบกล้องโทรทัศน์วงจรปิดที่ใช้ AI อย่างไรก็ตาม เทคโนโลยีการบันทึกและวิเคราะห์ภาพกำลังถูกนำไปใช้กับอุปกรณ์และระบบประเภทอื่นมากขึ้น เช่น กล้องบันทึกภาพในยานพาหนะ (Vehicle-Mounted Camera/Dashcam) กล้องภายในห้องโดยสาร ระบบตรวจสอบผู้ขับขี่ (Driver Monitoring System: DMS) กล้องบนอากาศยานไร้คนขับ (Drone/UAS) อุปกรณ์สวมใส่ที่มีกล้อง (Body-Worn Camera) และระบบกล้องเคลื่อนที่อื่น ซึ่งอาจมีความสามารถในการตรวจจับ จำแนก ติดตาม ระบุตัวบุคคล หรือวิเคราะห์ข้อมูลด้วย AI ในลักษณะใกล้เคียงกับระบบ CCTV ที่ใช้ AI

แม้ระบบดังกล่าวอาจไม่อยู่ภายใต้ความหมายของ CCTV ในทุกกรณี แต่หลักการด้านการกำหนดวัตถุประสงค์ (Purpose) การประเมินผลกระทบและความเสี่ยง (Impact and Risk Assessment) การคุ้มครองข้อมูล (Data Protection) การกำกับดูแลโดยมนุษย์ (Human Oversight) ความมั่นคงปลอดภัยของ AI (AI Security) การควบคุมการเชื่อมต่อกับระบบอื่น และการบริหารความเสี่ยงตลอดวงจรชีวิตที่กำหนดไว้ในแนวปฏิบัติฉบับนี้ อาจนำมาประยุกต์ใช้ได้ตามความเหมาะสม

โดยเฉพาะกรณีที่ผลการวิเคราะห์จาก AI ถูกนำไปเชื่อมโยงกับการควบคุมยานพาหนะ การแจ้งเตือนการบังคับใช้กฎหมาย การพิสูจน์ตัวบุคคล หรือการตัดสินใจที่อาจส่งผลต่อบุคคล ความปลอดภัย หรือภารกิจสำคัญ ควรพิจารณาผลกระทบจากระบบที่เชื่อมต่อและการดำเนินการต่อเนื่องจากผลลัพธ์ของ AI (Downstream Impact) เพิ่มเติมตามระดับความเสี่ยง

การพัฒนาแนวทางหรือข้อกำหนดสำหรับเทคโนโลยีดังกล่าวในอนาคตควรพิจารณาร่วมกับหน่วยงานกำกับดูแล หน่วยงานเจ้าของภารกิจ และหน่วยงานที่มีอำนาจตามกฎหมายที่เกี่ยวข้อง เพื่อให้การกำกับดูแลสอดคล้องกับลักษณะการใช้งาน ความเสี่ยง และข้อกำหนดเฉพาะของแต่ละภาคส่วน

การกล่าวถึงเทคโนโลยีที่เกี่ยวเนื่องในข้อนี้มีวัตถุประสงค์เพื่อแสดงแนวทางการประยุกต์หลักการด้านความมั่นคงปลอดภัยและการบริหารความเสี่ยง มิได้มีผลเป็นการกำหนดให้เทคโนโลยีดังกล่าวมีสถานะเป็นระบบ CCTV ตามกฎหมาย มาตรฐาน หรือข้อกำหนดเฉพาะภาคส่วนโดยอัตโนมัติ

6.4 การใช้ระบบวีดีโออัจฉริยะในเพื่อควบคุมการเข้าถึงระบบที่มีความสำคัญสูง

ในกรณีที่องค์กรมีการใช้ระบบวีดีโออัจฉริยะเพื่อควบคุมการเข้าถึงระบบที่มีความสำคัญสูง เช่น การใช้กล้อง License Plate Recognition (LPR) ในการอ่านป้ายทะเบียนรถยนต์เข้าออกสถานที่ หรือการใช้กล้องในการตรวจจับใบหน้า ระบุและตรวจสอบตัวตนด้วยใบหน้าของผู้ที่เข้าออกอาคารที่ต้องการการควบคุมที่เข้มงวด ระบบวีดีโออัจฉริยะเหล่านี้อาจให้ผลลัพธ์ที่ผิดพลาด เช่น อ่านป้ายทะเบียนผิดพลาดหรือยืนยันตัวตนผิดพลาด ทำให้ผู้ที่ไม่มีสิทธิเข้าถึงสถานที่สามารถเข้าไปยังสถานที่ดังกล่าวได้ หรือระบบเกิดความบกพร่องไม่พร้อมใช้งานทำให้เกิดปัญหาในการควบคุมการเข้าถึงสถานที่ ซึ่งความผิดพลาดนี้อาจเกิดได้จากหลายปัจจัย เช่น ผู้ถูกตรวจสอบมีการปลอมแปลงป้ายทะเบียนรถยนต์ มีการใช้รูปภาพถ่ายหรือ Deepfake เพื่อหลอกกล้อง หรือเกิดจากความผิดพลาดจากการทำงานของระบบวีดีโออัจฉริยะเอง

หน่วยงานควรพิจารณามีการประเมินและตรวจสอบความถูกต้องแม่นยำของการทำงานของระบบวีดีโออัจฉริยะเป็นประจำ มีระบบสำรองหรือมีมาตรการควบคุมทางเลือกอื่นเผื่อในกรณีที่ระบบหลักขัดข้อง และควรพิจารณาการควบคุมการเข้าถึงแบบหลายปัจจัยกับระบบที่มีความสำคัญสูง เช่น การใช้ LPR ร่วมกับการแสดงบัตรประจำตัวของผู้ที่เข้าสถานที่ การใช้กล้องระบุและตรวจสอบตัวตนด้วยใบหน้าร่วมกับรหัสผ่าน

สรุปหลักการของบทที่ 6

การใช้บริการคลาวด์ บริการ AI ภายนอก การวิเคราะห์วิดีโออัจฉริยะ ข้อมูลชีวมิติ และเทคโนโลยีที่เกี่ยวเนื่อง ควรได้รับการพิจารณาตาม **วัตถุประสงค์ ลักษณะข้อมูล สถานที่จัดเก็บและประมวลผล เขตอำนาจทางกฎหมาย สมรรถนะและข้อจำกัดของ AI การนำผลลัพธ์ไปใช้ และผลกระทบที่อาจเกิดขึ้น**

มาตรการที่นำมาใช้ควรได้สัดส่วนกับระดับผลกระทบและความเสี่ยง และต้องไม่ลดทอนหน้าที่ตามกฎหมาย ประกาศ ข้อกำหนดเฉพาะภาคส่วน ข้อกำหนดของหน่วยงานกำกับดูแล หรือสัญญาที่มีผลใช้บังคับ สำหรับเทคโนโลยีที่มิได้มีสถานะเป็น CCTV โดยตรง หลักการในแนวปฏิบัติฉบับนี้อาจนำไปประยุกต์ใช้ตามความเหมาะสม โดยไม่ถือว่าเป็นการกำหนดสถานะทางกฎหมายของเทคโนโลยีนั้นโดยอัตโนมัติ

ภาคผนวก ก รายการตรวจสอบก่อนส่งมอบ

รายการตรวจสอบนี้ใช้สำหรับตรวจสอบระบบ CCTV ที่ใช้ AI ก่อนการส่งมอบหรือเปิดใช้งาน เพื่อยืนยันว่าระบบได้รับการติดตั้ง กำหนดค่า ทดสอบ และจัดเตรียมข้อมูลหรือหลักฐานที่จำเป็นตามข้อกำหนดที่ได้รับอนุมัติ

การเลือกระดับการตรวจสอบให้พิจารณาจากผลการประเมินตามข้อ 3.1 ดังนี้

- **B – ระดับพื้นฐาน (Baseline)** สำหรับระบบ CCTV-AI โดยทั่วไป
- **E – ระดับเพิ่มเติม (Enhanced)** ใช้ร่วมกับ B เมื่อผลกระทบหรือความเสี่ยงเพิ่มขึ้น
- **H – ระดับความเชื่อมั่นสูง (High-Assurance)** ใช้ร่วมกับ B และ E สำหรับระบบที่มีผลกระทบหรือความสำคัญสูง

กรณีระบุว่า **ไม่เกี่ยวข้อง (N/A)** ควรระบุเหตุผลประกอบ

ก.1 ข้อมูลระบบ

รายการ	รายละเอียด
ชื่อระบบ/โครงการ	
หน่วยงาน/พื้นที่ใช้งาน	
เจ้าของระบบ (System Owner)	
กรณีใช้งานหลัก (Use Case)	
ระดับมาตรการ	☐ B ☐ E ☐ H
TOR/สัญญา/เอกสารอ้างอิง	
วันที่ตรวจสอบ	
ผู้ตรวจสอบ	

ก.2 รายการตรวจสอบ

ลำดับ	รายการตรวจสอบ	ระดับ	ผ่าน	ไม่ผ่าน	N/A	หลักฐาน/หมายเหตุ
1	ระบบ อุปกรณ์ ซอฟต์แวร์ และความสามารถของ AI ตรงตามขอบเขตที่ได้รับอนุมัติ	B	☐	☐	☐	
2	เปิดใช้งานเฉพาะความสามารถของ AI และบริการที่จำเป็นตามกรณีใช้งาน	B	☐	☐	☐	
3	ตำแหน่งกล้อง มุมมอง สภาพแสง และคุณภาพภาพเหมาะสมกับการทำงานของ AI	B	☐	☐	☐	
4	AI ได้รับการทดสอบตามกรณีใช้งานและเกณฑ์ตรวจรับที่กำหนด	B	☐	☐	☐	
5	บัญชี รหัสผ่าน ค่าตั้งต้น และสิทธิการเข้าถึงได้รับการควบคุมอย่างเหมาะสม	B	☐	☐	☐	
6	การเข้าถึงจากระยะไกล (Remote Access) ถูกปิดเมื่อไม่จำเป็น หรือได้รับการควบคุมเมื่อจำเป็น	B	☐	☐	☐	
7	การบันทึกเหตุการณ์ (Logging) ที่จำเป็นได้รับการเปิดใช้งานและสามารถตรวจสอบย้อนหลังได้	B	☐	☐	☐	
8	วิธีการปรับปรุงระบบ สำรองข้อมูล และกู้คืนได้รับการกำหนดหรือส่งมอบ	B	☐	☐	☐	
9	บัญชีหรือสิทธิชั่วคราวของผู้ติดตั้งได้รับการยกเลิกหรือได้รับอนุมัติให้คงไว้	B	☐	☐	☐	
10	เอกสารและข้อมูลที่จำเป็นต่อการใช้งานและบำรุงรักษาได้รับการส่งมอบ	B	☐	☐	☐	
11	สมรรถนะของ AI ได้รับการทดสอบในสภาพแวดล้อมที่สอดคล้องกับการใช้งานจริง	E	☐	☐	☐	
12	ข้อจำกัด เงื่อนไขการใช้งาน และปัจจัยที่อาจกระทบสมรรถนะของ AI ได้รับการชี้แจง	E	☐	☐	☐	

ลำดับ	รายการตรวจสอบ	ระดับ	ผ่าน	ไม่ผ่าน	N/A	หลักฐาน/หมายเหตุ
13	การเก็บ ใช้ ประมวลผล เข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล ข้อมูลชีวมิติ หรือข้อมูลที่ AI สร้างขึ้นได้รับการควบคุมตามข้อกำหนดที่เกี่ยวข้อง	E	☐	☐	☐	
14	ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) กระบวนงานอัตโนมัติ (Workflow) และการเชื่อมต่อกับระบบอื่นเป็นไปตามขอบเขตที่ได้รับอนุมัติ	E	☐	☐	☐	
15	มีการกำกับดูแลโดยมนุษย์ (Human Oversight) ที่เหมาะสมกับระดับผลกระทบ	E	☐	☐	☐	
16	กรณีใช้บริการคลาวด์ (Cloud Service) หรือบริการภายนอก (External Service) มีข้อมูลเกี่ยวกับสถานที่จัดเก็บและประมวลผลข้อมูล ผู้ให้บริการที่เกี่ยวข้อง และการแบ่งความรับผิดชอบอย่างเพียงพอ	E	☐	☐	☐	
17	มีมาตรฐาน การรับรอง ผลการทดสอบ หรือหลักฐานการสร้างความเชื่อมั่นตามที่ TOR หรือสัญญากำหนด	E	☐	☐	☐	
18	มีข้อมูลเกี่ยวกับการสนับสนุน การปรับปรุงด้านความมั่นคงปลอดภัย และการบริหารช่องโหว่ของผู้ผลิตหรือผู้ให้บริการ	E	☐	☐	☐	
19	มีข้อมูลหรือหลักฐานด้านการบริหารผู้ส่งมอบและความมั่นคงปลอดภัยของห่วงโซ่อุปทาน	E	☐	☐	☐	
20	การดำเนินการอัตโนมัติ (Automated Action) ได้รับการทดสอบและจำกัดให้อยู่ภายในขอบเขตการดำเนินการ (Action Boundary) ที่ได้รับอนุมัติ	H	☐	☐	☐	
21	ระบบสามารถจำกัด ระงับ หรือเข้าสู่การทำงานแบบจำกัด (Degraded Mode) หรือสภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe) เมื่อ AI ไม่พร้อมใช้งานหรือไม่สามารถเชื่อถือผลลัพธ์ได้	H	☐	☐	☐	

ลำดับ	รายการตรวจสอบ	ระดับ	ผ่าน	ไม่ผ่าน	N/A	หลักฐาน/หมายเหตุ
22	การเชื่อมต่อกับระบบหรือภารกิจสำคัญได้รับการทดสอบเพื่อจำกัดการขยายผลกระทบ	H	☐	☐	☐	
23	สถานที่จัดเก็บข้อมูล (Data Location) สถานที่ประมวลผล (Processing Location) เขตอำนาจทางกฎหมาย (Jurisdiction) และการเข้าถึงจากภายนอกได้รับการประเมินตามระดับผลกระทบ ความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง	H	☐	☐	☐	
24	มีผลการทดสอบหรือหลักฐานการสร้างความเชื่อมั่นเพิ่มเติมสำหรับระบบที่มีผลกระทบหรือความสำคัญสูง ตามที่กำหนด	H	☐	☐	☐	

หมายเหตุ การตรวจสอบรุ่น แบบจำลอง หรือความสามารถของ AI ให้ดำเนินการในระดับที่เพียงพอต่อการยืนยันระบบที่ส่งมอบ การบริหารการเปลี่ยนแปลง และการประเมินความเสี่ยง โดยไม่จำเป็นต้องเปิดเผยรายละเอียดของแบบจำลอง อัลกอริทึม ไลบรารี หรือองค์ประกอบทางเทคนิคภายในทั้งหมด เว้นแต่กฎหมาย ข้อกำหนดในการจัดซื้อ (TOR) สัญญา หรือผลการประเมินความเสี่ยงกำหนดไว้เป็นอย่างอื่น

ก.3 ข้อกำหนดที่มีผลใช้บังคับ

ประเด็น	ใช้บังคับ	ไม่ใช้บังคับ	หลักฐาน/หมายเหตุ
กฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล	☐	☐	
ข้อกำหนดที่เกี่ยวข้องกับข้อมูลชีวมิติหรือข้อมูลที่มีความอ่อนไหว	☐	☐	
ข้อกำหนดด้านความมั่นคงปลอดภัยของบริการคลาวด์	☐	☐	
ข้อกำหนดเกี่ยวกับสถานที่จัดเก็บหรือประมวลผลข้อมูล (Data Localization)	☐	☐	
ข้อกำหนดเฉพาะภาคส่วน ระบบ หรือภารกิจสำคัญ	☐	☐	
มาตรฐาน การรับรอง หรือหลักฐานที่กำหนดใน TOR หรือสัญญา	☐	☐	

หมายเหตุ การกำหนดให้ข้อมูลจัดเก็บหรือประมวลผลภายในประเทศ (Data Localization) ให้พิจารณาตามกฎหมาย ข้อกำหนดที่มีผลใช้บังคับ และผลการประเมินความเสี่ยง โดยควรพิจารณาร่วมกับอธิปไตยข้อมูล (Data Sovereignty) ซึ่งครอบคลุมสถานที่จัดเก็บและประมวลผล เขตอำนาจทางกฎหมาย การเข้าถึงจากต่างประเทศ ผู้ให้บริการช่วง และการควบคุมกุญแจเข้ารหัสตามความเหมาะสม

ก.4 มาตรฐาน การรับรอง และหลักฐานการสร้างความเชื่อมั่น

กรณี TOR สัญญา หรือผลการประเมินความเสี่ยงกำหนดให้มีมาตรฐาน การรับรอง หรือผลการทดสอบ ควรตรวจสอบว่า **หลักฐานมีอยู่จริง ยังมีผล ขอบข่ายเกี่ยวข้องกับสิ่งที่จัดหา และออกหรือประเมินโดยหน่วยงานที่เหมาะสม**

ด้าน	ตัวอย่างมาตรฐานหรือหลักฐาน
ระบบ CCTV และการวิเคราะห์วิดีโออัจฉริยะ (Intelligent Video Analytics)	IEC 62676 series ตามความเกี่ยวข้อง
การกำกับดูแล AI	ISO/IEC 42001 หรือหลักฐานระบบการบริหารที่เกี่ยวข้อง
ความมั่นคงปลอดภัยสารสนเทศ	ISO/IEC 27001 หรือหลักฐานที่เกี่ยวข้อง
ความเป็นส่วนตัว	ISO/IEC 27701 หรือหลักฐานที่เกี่ยวข้อง
ความมั่นคงปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security)	ISO/IEC 27036 series หรือหลักฐานกระบวนการที่เกี่ยวข้อง
การจัดการและการเปิดเผยช่องโหว่ (Vulnerability Handling and Disclosure)	ISO/IEC 29147, ISO/IEC 30111 หรือหลักฐานกระบวนการที่เกี่ยวข้อง
สมรรถนะหรือความน่าเชื่อถือ	รายงานผลการทดสอบ (Test Report) การประเมินจากบุคคลที่สาม (Third-Party Assessment) หรือหลักฐานตามมาตรฐานที่เกี่ยวข้อง

การมีใบรับรองมาตรฐานเพียงอย่างเดียวไม่ควรใช้ทดแทนการประเมินความเหมาะสมของระบบต่อกรณีใช้งานจริง

ภาคผนวก ข รายการตรวจสอบด้วยตนเองตามรอบ

รายการตรวจสอบนี้ใช้สำหรับทบทวนระบบ CCTV ที่ใช้ AI ภายหลังเปิดใช้งาน เพื่อประเมินว่าระบบยังคงอยู่ในสถานะที่ได้รับอนุมัติและเชื่อถือได้ และมาตรการควบคุมยังเหมาะสมกับระดับผลกระทบและความเสี่ยง

ข.1 ข้อมูลการทบทวน

รายการ	รายละเอียด
ชื่อระบบ/พื้นที่	
เจ้าของระบบ (System Owner)	
กรณีใช้งานหลัก (Use Case)	
ระดับมาตรการ	☐ B ☐ E ☐ H
วันที่ทบทวน	
ผู้ทบทวน	
วันที่ทบทวนครั้งก่อน	
วันที่กำหนดทบทวนครั้งถัดไป	

ข.2 รายการตรวจสอบตามรอบ

ลำดับ	รายการตรวจสอบ	ระดับ	ปกติ	ต้องดำเนินการ	N/A	หลักฐาน/หมายเหตุ
1	วัตถุประสงค์และกรณีใช้งานของ AI ยังเป็นไปตามที่ได้รับอนุมัติ	B	☐	☐	☐	
2	ไม่มีการเปิดใช้หรือเปลี่ยนความสามารถ AI ที่มีนัยสำคัญโดยไม่ได้รับอนุมัติ	B	☐	☐	☐	
3	ตำแหน่งกล้อง มุมมอง สภาพแสง และคุณภาพภาพยังเหมาะสมกับ AI	B	☐	☐	☐	
4	การตั้งค่าที่สำคัญยังสอดคล้องกับค่าฐานที่ได้รับอนุมัติ (Approved Baseline)	B	☐	☐	☐	

ลำดับ	รายการตรวจสอบ	ระดับ	ปกติ	ต้องดำเนินการ	N/A	หลักฐาน/หมายเหตุ
5	บัญชีและสิทธิการเข้าถึงยังเหมาะสมกับหน้าที่และความจำเป็น	B	☐	☐	☐	
6	การเข้าถึงจากระยะไกล (Remote Access) และสิทธิของผู้ผลิตหรือผู้ให้บริการยังมีความจำเป็นและได้รับการควบคุม	B	☐	☐	☐	
7	การบันทึกเหตุการณ์ (Logging) และการเฝ้าระวังยังทำงานได้ และสามารถตรวจสอบย้อนหลังได้	B	☐	☐	☐	
8	ช่องโหว่และชุดปรับปรุงด้านความมั่นคงปลอดภัย (Security Update) ที่เกี่ยวข้องได้รับการติดตาม ประเมิน และดำเนินการตามความเหมาะสม	B	☐	☐	☐	
9	ผลิตภัณฑ์ ซอฟต์แวร์ และบริการสำคัญยังอยู่ในระยะการสนับสนุน หรือมีแผนรองรับกรณีสิ้นสุดการสนับสนุน (End of Support)	B	☐	☐	☐	
10	การสำรองและกู้คืนข้อมูล การตั้งค่า และองค์ประกอบที่จำเป็นยังสามารถดำเนินการได้ตามที่กำหนด	B	☐	☐	☐	
11	สมรรถนะและความผิดพลาดของ AI ยังอยู่ในระดับที่ยอมรับได้สำหรับกรณีใช้งาน	E	☐	☐	☐	
12	การเก็บ ใช้ เข้าถึง เชื่อมโยง เก็บรักษา และลบข้อมูล รวมถึงข้อมูลที่ AI สร้างหรืออนุมานขึ้น ยังคงสอดคล้องกับวัตถุประสงค์และข้อกำหนดที่เกี่ยวข้อง	E	☐	☐	☐	
13	ส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) กระบวนงานอัตโนมัติ (Workflow) และการ	E	☐	☐	☐	

ลำดับ	รายการตรวจสอบ	ระดับ	ปกติ	ต้องดำเนินการ	N/A	หลักฐาน/หมายเหตุ
	เชื่อมต่อกับระบบอื่นยังอยู่ในขอบเขตที่ได้รับอนุมัติ					
14	การกำกับดูแลโดยมนุษย์ (Human Oversight) ยังสามารถดำเนินการได้ตามที่กำหนด	E	☐	☐	☐	
15	บริการคลาวด์ (Cloud Service) หรือบริการภายนอก (External Service) ไม่มีการเปลี่ยนแปลงที่มีนัยสำคัญโดยไม่ได้รับการประเมินและอนุมัติตามกระบวนการที่กำหนด	E	☐	☐	☐	
16	เหตุการณ์ ความผิดพลาด ข้อร้องเรียน หรือผลกระทบที่เกี่ยวข้องกับ AI ได้รับการทบทวนและนำไปใช้ปรับปรุงตามความเหมาะสม	E	☐	☐	☐	
17	การดำเนินการอัตโนมัติ (Automated Action) และขอบเขตการดำเนินการ (Action Boundary) ยังคงเป็นไปตามที่ได้รับอนุมัติ	H	☐	☐	☐	
18	การทำงานแบบจำกัด (Degraded Mode) หรือสภาวะปลอดภัยเมื่อเกิดความล้มเหลว (Fail-Safe) ยังคงสามารถใช้งานได้ตามที่กำหนด	H	☐	☐	☐	
19	กรณีมีข้อกำหนดเกี่ยวกับสถานที่จัดเก็บข้อมูล (Data Location) เขตอำนาจทางกฎหมาย (Jurisdiction) หรืออธิปไตยข้อมูล (Data Sovereignty) ได้มีการทบทวนว่ายังคงเป็นไปตามเงื่อนไขและข้อกำหนดที่เกี่ยวข้อง	E/H	☐	☐	☐	
20	การเปลี่ยนแปลงที่มีนัยสำคัญต่อวัตถุประสงค์ ข้อมูล ความสามารถของ AI การเชื่อมต่อ หรือระดับผลกระทบและความเสี่ยง ได้รับการประเมินใหม่ตามความเหมาะสม	E/H	☐	☐	☐	

ข.3 การทบทวนนอกเหนือจากรอบที่กำหนด

ควรพิจารณาทบทวนหรือประเมินใหม่เมื่อเกิดการเปลี่ยนแปลงหรือเหตุการณ์ที่มีนัยสำคัญ เช่น

- เปลี่ยนวัตถุประสงค์หรือกรณีใช้งาน
- เพิ่มหรือเปลี่ยนความสามารถของ AI
- เปลี่ยนแบบจำลอง ซอฟต์แวร์ หรือบริการ AI ที่สำคัญ
- เพิ่มการติดตามหรือระบุบุคคล
- เชื่อมต่อกับระบบใหม่
- เพิ่มการดำเนินการอัตโนมัติ (Automated Action)
- เปลี่ยนผู้ให้บริการคลาวด์ (Cloud Service Provider) หรือผู้ให้บริการ AI ภายนอก
- เปลี่ยนสถานที่จัดเก็บข้อมูล (Data Location) หรือสถานที่ประมวลผล (Processing Location)
- พบช่องโหว่หรือเหตุด้านความมั่นคงปลอดภัยที่มีนัยสำคัญ
- พบการเปลี่ยนแปลงของสมรรถนะหรือรูปแบบความผิดพลาดของ AI อย่างมีนัยสำคัญ
- เกิดผลกระทบต่อบุคคล ระบบ หรือภารกิจที่มีนัยสำคัญ

ไม่จำเป็นต้องประเมินใหม่ทั้งหมด หากองค์กรสามารถแสดงได้ว่าการเปลี่ยนแปลงดังกล่าวไม่มีผลต่อระดับผลกระทบหรือความเสี่ยงอย่างมีนัยสำคัญ

ภาคผนวก ค อภิธานศัพท์

คำศัพท์	ความหมาย
ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	ระบบที่สามารถประมวลผลข้อมูลเพื่อสร้างผลลัพธ์ เช่น การตรวจจับ จำแนก วิเคราะห์ หรือสนับสนุนการตัดสินใจ
ระบบ CCTV ที่ใช้ AI (AI-Enabled CCTV)	ระบบ CCTV ที่ใช้ AI หรือการวิเคราะห์วิดีโออัจฉริยะเพื่อประมวลผลภาพ วิดีโอ หรือข้อมูลที่เกี่ยวข้อง
การวิเคราะห์วิดีโออัจฉริยะ (Intelligent Video Analytics)	การใช้ AI หรือระบบอัตโนมัติเพื่อวิเคราะห์วัตถุ บุคคล เหตุการณ์ หรือพฤติกรรมจากภาพหรือวิดีโอ
กรณีใช้งาน (Use Case)	วัตถุประสงค์และลักษณะการนำความสามารถของระบบไปใช้ในบริบทที่กำหนด
ผลลัพธ์จาก AI (AI Output)	ผลลัพธ์ที่ AI สร้างจากการประมวลผล เช่น การตรวจจับ การจำแนก คะแนน หรือการแจ้งเตือน
แบบจำลอง AI (AI Model)	องค์ประกอบของระบบ AI ที่ใช้ประมวลผลข้อมูลเพื่อสร้างผลลัพธ์
ค่าความเชื่อมั่น (Confidence Score)	ค่าที่ระบบใช้แสดงระดับความเชื่อมั่นต่อผลลัพธ์ตามกลไกของระบบ ซึ่งไม่ควรตีความว่าเป็นการยืนยันความถูกต้องโดยอัตโนมัติ
ข้อมูลชีวมิติ (Biometric Data)	ข้อมูลที่เกี่ยวข้องกับลักษณะทางกายภาพ สรีรวิทยา หรือพฤติกรรมของบุคคล ซึ่งอาจใช้เพื่อระบุหรือยืนยันบุคคล
ข้อมูลที่ได้จากการอนุมาน (Inferred Data)	ข้อมูลหรือข้อสรุปที่เกิดจากการวิเคราะห์ข้อมูลต้นทาง
การกำกับดูแลโดยมนุษย์ (Human Oversight)	การที่บุคลากรสามารถตรวจสอบ พิจารณา แทรกแซง หรือหยุดการใช้ผลลัพธ์หรือการดำเนินการของ AI
ขอบเขตการดำเนินการ (Action Boundary)	ขอบเขตที่กำหนดว่าระบบ AI หรือระบบอัตโนมัติได้รับอนุญาตให้ดำเนินการใดได้
การทำงานแบบจำกัด (Degraded Mode)	รูปแบบการทำงานที่ยังคงให้บริการบางส่วนเมื่อ AI หรือองค์ประกอบสำคัญไม่พร้อมใช้งาน
สภาวะปลอดภัย (Fail-Safe)	สภาวะที่ระบบเปลี่ยนไปสู่รูปแบบที่ช่วยลดผลกระทบเมื่อเกิดความผิดพลาด

คำศัพท์	ความหมาย
ค่าฐานที่ได้รับอนุมัติ (Approved Baseline)	สถานะหรือค่าตั้งต้นสำคัญของระบบที่ได้รับการตรวจสอบและอนุมัติให้ใช้เป็นข้อมูลอ้างอิง
สถานะที่ได้รับอนุมัติและเชื่อถือได้ (Approved and Trusted State)	สถานะที่ระบบยังคงสอดคล้องกับค่าฐานที่ได้รับอนุมัติ มีสมรรถนะและมาตรการควบคุมที่เหมาะสม และไม่มีการเปลี่ยนแปลงที่ทำให้ความเสี่ยงเกินระดับที่ยอมรับ
การสร้างความเชื่อมั่น (Assurance)	ข้อมูล หลักฐาน การทดสอบ การประเมิน หรือวิธีการอื่นที่ใช้สนับสนุนความมั่นใจว่าข้อกำหนดหรือมาตรการได้รับการดำเนินการอย่างเหมาะสม
การเปลี่ยนแปลงที่มีนัยสำคัญ (Significant Change)	การเปลี่ยนแปลงที่อาจทำให้วัตถุประสงค์ ข้อมูล ความสามารถ AI การเชื่อมต่อ หรือระดับผลกระทบและความเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ
อธิปไตยข้อมูล (Data Sovereignty)	ความสามารถและข้อจำกัดในการกำกับ ควบคุม และใช้ข้อมูลภายใต้กฎหมาย เขตอำนาจ และเงื่อนไขของสถานที่หรือผู้ให้บริการที่เกี่ยวข้อง
การกำหนดที่ตั้งข้อมูล (Data Localization)	ข้อกำหนดหรือมาตรการที่กำหนดให้ข้อมูลบางประเภทจัดเก็บหรือประมวลผลภายในพื้นที่หรือประเทศที่กำหนด
ผู้ให้บริการช่วง (Subprocessor)	ผู้ให้บริการที่ผู้ให้บริการหลักใช้เพื่อดำเนินการประมวลผลข้อมูลหรือให้บริการบางส่วน

ภาคผนวก ง เอกสารและมาตรฐานอ้างอิง

มาตรฐาน แนวปฏิบัติ กฎหมาย และกรอบอ้างอิงที่ระบุในภาคผนวกนี้ใช้เพื่อสนับสนุนการจัดทำและการประยุกต์ใช้แนวปฏิบัติฉบับนี้ตามความเกี่ยวข้องกับลักษณะของระบบ วัตถุประสงค์ ระดับผลกระทบ และความเสี่ยง มิได้หมายความว่าระบบ ผลิตภัณฑ์ ผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการทุกกรณีต้องปฏิบัติตามหรือได้รับการรับรองตามมาตรฐานทุกฉบับที่กล่าวถึง

ในการนำไปใช้งาน ควรพิจารณาฉบับของมาตรฐานที่มีผลใช้งานและเหมาะสมกับบริบท ณ เวลาที่นำไปประยุกต์ใช้ เว้นแต่กฎหมาย ประกาศ ข้อกำหนดเฉพาะภาคส่วน ข้อกำหนดในการจัดซื้อจัดจ้าง สัญญา หรือข้อกำหนดอื่นที่มีผลใช้บังคับกำหนดไว้เป็นการเฉพาะ

ง.1 ระบบเฝ้าระวังด้วยวิดีโอและการวิเคราะห์วิดีโออัจฉริยะ

IEC 62676 series — Video surveillance systems for use in security applications

ใช้เป็นกรอบสำหรับการออกแบบ การติดตั้ง การใช้งาน สมรรถนะ และการทดสอบระบบเฝ้าระวังด้วยวิดีโอตามส่วนที่เกี่ยวข้อง

IEC 62676-4 — Video surveillance systems for use in security applications — Part 4: Application guidelines

ใช้ประกอบการออกแบบและประยุกต์ใช้ระบบเฝ้าระวังด้วยวิดีโอให้เหมาะสมกับวัตถุประสงค์และสภาพแวดล้อมการใช้งาน

ข้อเสนอแนะ ITU-T ในกลุ่ม F.743 ที่เกี่ยวข้องกับระบบเฝ้าระวังด้วยวิดีโออัจฉริยะ (Intelligent Video Surveillance)

ใช้เป็นกรอบประกอบการพิจารณาข้อกำหนด สถาปัตยกรรม กล้องอัจฉริยะ และความมั่นคงปลอดภัยของระบบเฝ้าระวังด้วยวิดีโออัจฉริยะตามกรณีใช้งาน

ข้อเสนอแนะ ITU-T ในกลุ่ม H.626 ที่เกี่ยวข้องกับระบบเฝ้าระวังด้วยวิดีโออัจฉริยะ

ใช้เป็นกรอบประกอบการพิจารณาสถาปัตยกรรมและองค์ประกอบของระบบเฝ้าระวังด้วยวิดีโออัจฉริยะตามความเกี่ยวข้อง

ง.2 การกำกับดูแล การบริหารความเสี่ยง และการประเมินผลกระทบของ AI

ISO/IEC 42001:2023 — Information technology — Artificial intelligence — Management system

ใช้เป็นกรอบสำหรับระบบการจัดการปัญญาประดิษฐ์ (AI Management System) และการกำกับดูแล AI อย่างเป็นระบบตลอดวงจรชีวิต

ISO/IEC 23894:2023 — Information technology — Artificial intelligence — Guidance on risk management

ใช้เป็นกรอบสำหรับการระบุ ประเมิน และบริหารความเสี่ยงที่เกี่ยวข้องกับ AI

ISO/IEC 42005 — Artificial intelligence — AI system impact assessment

ใช้เป็นกรอบสำหรับการประเมินผลกระทบของระบบ AI (AI System Impact Assessment) ตามวัตถุประสงค์ บริบท และผู้ที่อาจได้รับผลกระทบ

ISO/IEC 22989 — Information technology — Artificial intelligence — Artificial intelligence concepts and terminology

ใช้เป็นกรอบอ้างอิงสำหรับแนวคิดและคำศัพท์พื้นฐานด้านปัญญาประดิษฐ์

ง.3 ความมั่นคงปลอดภัยและความน่าเชื่อถือของ AI

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) — แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Security Guidelines)

ใช้เป็นกรอบอ้างอิงของประเทศไทยสำหรับภัยคุกคาม มาตรการด้านความมั่นคงปลอดภัย และการบริหารระบบ AI ตลอดวงจรชีวิต

ISO/IEC TR 24028 — Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence

ใช้เป็นกรอบประกอบการพิจารณาคุณลักษณะและประเด็นด้านความน่าเชื่อถือของ AI

ISO/IEC 24029 series — Artificial intelligence — Assessment of the robustness of neural networks

ใช้เป็นกรอบประกอบการประเมินความทนทาน (Robustness) ของระบบ AI ที่ใช้โครงข่ายประสาทเทียมตามความเกี่ยวข้อง

ISO/IEC 25059 — Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems

ใช้เป็นกรอบประกอบการพิจารณาคุณภาพและคุณลักษณะที่เกี่ยวข้องกับระบบ AI

แนวทางด้านความมั่นคงปลอดภัยของ AI ของ European Union Agency for Cybersecurity (ENISA) ที่เกี่ยวข้อง

ใช้เป็นแหล่งอ้างอิงประกอบด้านภัยคุกคาม ความเสี่ยง และมาตรการด้านความมั่นคงปลอดภัยของ AI ตามความเหมาะสม

แนวทางด้านความมั่นคงปลอดภัย AI/ML ของ Open Worldwide Application Security Project (OWASP) ที่เกี่ยวข้อง

ใช้เป็นแหล่งอ้างอิงประกอบด้านรูปแบบการโจมตี ช่องโหว่ และแนวทางลดความเสี่ยงของระบบ AI/ML ตามความเหมาะสม

ง.4 ความมั่นคงปลอดภัยสารสนเทศ ความเป็นส่วนตัว ห่วงโซ่อุปทาน ช่องโหว่ และบริการคลาวด์

ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ใช้เป็นกรอบสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls

ใช้เป็นกรอบอ้างอิงสำหรับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

ISO/IEC 27701:2025 — Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

ใช้เป็นกรอบสำหรับระบบบริหารจัดการข้อมูลส่วนบุคคลและความเป็นส่วนตัว (Privacy Information Management System: PIMS)

ISO/IEC 27036 series — Cybersecurity — Supplier relationships

ใช้เป็นกรอบสำหรับการบริหารความสัมพันธ์กับผู้ส่งมอบและความมั่นคงปลอดภัยของห่วงโซ่อุปทาน โดยพิจารณาส่วนที่เกี่ยวข้องกับผลิตภัณฑ์ บริการ และห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสารตามกรณีใช้งาน

ISO/IEC 29147:2018 — Information technology — Security techniques — Vulnerability disclosure

ใช้เป็นกรอบสำหรับกระบวนการรับแจ้งและการเปิดเผยข้อมูลช่องโหว่ (Vulnerability Disclosure)

ISO/IEC 30111:2019 — Information technology — Security techniques — Vulnerability handling processes

ใช้เป็นกรอบสำหรับกระบวนการตรวจสอบ วิเคราะห์ จัดการ แก้ไข และติดตามช่องโหว่ (Vulnerability Handling)

ISO/IEC 27017 — Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

ใช้เป็นกรอบสำหรับมาตรการด้านความมั่นคงปลอดภัยของบริการคลาวด์ และการกำหนดความรับผิดชอบที่เกี่ยวข้องระหว่างผู้ใช้บริการและผู้ให้บริการคลาวด์

ISO/IEC 27018 — Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

ใช้เป็นกรอบสำหรับการคุ้มครองข้อมูลส่วนบุคคลในบริการคลาวด์สาธารณะเมื่อผู้ให้บริการคลาวด์ทำหน้าที่เป็นผู้ประมวลผลข้อมูล

มาตรฐานประกอบที่อาจพิจารณาตามบริบท

ISO 28000:2022 — Security and resilience — Security management systems — Requirements

อาจใช้เป็นกรอบประกอบสำหรับระบบบริหารจัดการด้านความมั่นคงปลอดภัยและความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่อุปทานตามลักษณะขององค์กร

IEC 62443-4-1 — Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements

อาจใช้เป็นกรอบประกอบสำหรับกระบวนการพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย (Secure Product Development Lifecycle) ตามความเหมาะสมกับลักษณะผลิตภัณฑ์และขอบเขตของมาตรฐาน

ง.5 ข้อมูลชีวมิติ

ISO/IEC 24745 — Information security, cybersecurity and privacy protection — Biometric information protection

ใช้เป็นกรอบสำหรับการคุ้มครองข้อมูลและแม่แบบชีวมิติ (Biometric Information Protection)

ISO/IEC 19795-1 — Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

ใช้เป็นกรอบสำหรับหลักการทดสอบ การวัด และการรายงานสมรรถนะของระบบชีวมิติ

ISO/IEC 30107 series — Information technology — Biometric presentation attack detection

ใช้เป็นกรอบสำหรับการป้องกันและตรวจจับการโจมตีด้วยการนำเสนอลักษณะชีวมิติ (Presentation Attack Detection: PAD) ตามส่วนที่เกี่ยวข้อง

ง.6 กฎหมาย ประกาศ และข้อกำหนดของประเทศไทย

กฎหมาย ประกาศ มาตรฐาน และข้อกำหนดของประเทศไทยที่เกี่ยวข้องกับระบบ CCTV ที่ใช้ AI ให้พิจารณาตามลักษณะขององค์กร ระบบ ข้อมูล กรณีใช้งาน และขอบเขตที่มีผลใช้บังคับ โดยอาจรวมถึงรายการต่อไปนี้

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง ใช้เป็นกรอบสำหรับหน้าที่และการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามขอบเขตที่กฎหมายกำหนด

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง ใช้เป็นกรอบสำหรับการเก็บ ใช้ เปิดเผย และคุ้มครองข้อมูลส่วนบุคคล รวมถึงการประมวลผลข้อมูลที่อาจมีความอ่อนไหวตามกรณีที่เกี่ยวข้อง

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายลำดับรองที่เกี่ยวข้อง ใช้ประกอบการพิจารณาหน้าที่และข้อกำหนดที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามขอบเขตที่กฎหมายกำหนด

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ใช้สำหรับหน่วยงาน ผู้ใช้บริการคลาวด์ และผู้ให้บริการที่อยู่ภายใต้ขอบเขตการใช้บังคับของประกาศ โดยให้พิจารณาข้อกำหนดตามระดับผลกระทบและขอบเขตที่กำหนดไว้ในประกาศ

กฎหมาย กฎ ระเบียบ ประกาศ หรือข้อกำหนดเฉพาะภาคส่วนที่เกี่ยวข้อง ให้พิจารณาเพิ่มเติมตามประเภทหน่วยงาน ภารกิจ ระบบ ข้อมูล และวัตถุประสงค์ของการใช้ CCTV ที่ใช้ AI

ง.7 กรอบอ้างอิงด้านกฎระเบียบต่างประเทศ

Regulation (EU) 2024/1689 — Artificial Intelligence Act (EU AI Act) ใช้เป็นกรอบอ้างอิงด้านกฎระเบียบต่างประเทศสำหรับศึกษาหลักการและแนวโน้มด้านการกำกับดูแล AI เช่น ระบบ AI ที่มีผลกระทบสูง การใช้ข้อมูลชีวมิติ ความโปร่งใส การกำกับดูแลโดยมนุษย์ และการประเมินผลกระทบ ทั้งนี้ มิได้มีผลใช้บังคับในประเทศไทยโดยอัตโนมัติ เว้นแต่องค์กรหรือกิจกรรมอยู่ภายใต้ขอบเขตของกฎหมายดังกล่าว

หมายเหตุการใช้เอกสารอ้างอิง

รายการมาตรฐานและกรอบอ้างอิงข้างต้นมิได้มีวัตถุประสงค์ให้ทุกองค์กรนำมาตรฐานทุกฉบับมาใช้กับทุกระบบ การเลือกใช้ควรพิจารณาจากวัตถุประสงค์ ลักษณะของระบบ ความสามารถของ AI ประเภทและความสำคัญของข้อมูล ระบบที่เชื่อมต่อ ระดับผลกระทบและความเสี่ยง ตลอดจนกฎหมายและข้อกำหนดที่มีผลใช้บังคับ

ก่อนนำไปใช้ในการจัดซื้อจัดจ้าง การกำหนดข้อกำหนดทางเทคนิค การตรวจรับ หรือการอ้างอิงในเอกสารทางการ ควรตรวจสอบเลขฉบับ ปี และสถานะปัจจุบันของมาตรฐานจากหน่วยงานเจ้าของมาตรฐานอีกครั้ง