NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สมาคมระบบกล้องวงจรปิดอัจฉริยะไทย
ICA
THAI INTELLIGENT CCTV ASSOCIATION

TCSG

THAILAND CCTV SECURITY GUIDELINES

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดสำหรับประเทศไทย

Secure 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 ให้ข้อเสนอแนะและปรับปรุงแนวปฏิบัติฉบับนี้ให้มีความครบถ้วนเป็นประโยชน์ และสามารถนำไปใช้งานได้กับองค์กรทั้งภาครัฐและเอกชน เหมาะสมกับบริบทของประเทศไทย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แนวทางการอ่านเอกสารฉบับนี้

แนวปฏิบัติฉบับนี้ครอบคลุมการกำกับดูแลและข้อกำหนดที่เกี่ยวข้อง การกำหนดระดับความสำคัญและความเสี่ยง มาตรการด้านความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ การจัดซื้อจัดจ้างและการตรวจรับ ตลอดจนข้อพิจารณาสำหรับบริการคลาวด์ บริการภายนอก แอปพลิเคชันและการเข้าถึงจากระยะไกล และระบบที่มีการใช้งานร่วมกับปัญญาประดิษฐ์

ผู้อ่านสามารถเลือกศึกษาเนื้อหาตามบทบาท หน้าที่ ลักษณะ และระดับความสำคัญและความเสี่ยงของระบบที่ใช้งาน โดยเอกสารฉบับนี้มีโครงสร้างเนื้อหาดังต่อไปนี้

โครงสร้างของแนวปฏิบัติ

บทที่ 1 บทนำ

กำหนดที่มา วัตถุประสงค์ ผู้ใช้เอกสาร สถานะและหลักการพื้นฐานของแนวปฏิบัติ

บทที่ 2 การกำกับดูแล ข้อกำหนด และกฎหมาย

ครอบคลุมการกำหนดระดับการประยุกต์ใช้มาตรการ กรอบมาตรฐานและข้อกำหนดที่เกี่ยวข้อง ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนการอบรมและสร้างความตระหนัก

บทที่ 3 ค่าตั้งต้นด้านความมั่นคงปลอดภัยตลอดวงจรชีวิตระบบ

ครอบคลุมมาตรการตั้งแต่การออกแบบและเลือกอุปกรณ์ การติดตั้ง การใช้งาน การบำรุงรักษาและเฝ้าระวัง การจัดการช่องโหว่และเหตุการณ์ การประเมินระบบเดิม และการเลิกใช้งาน

บทที่ 4 การจัดซื้อจัดจ้าง

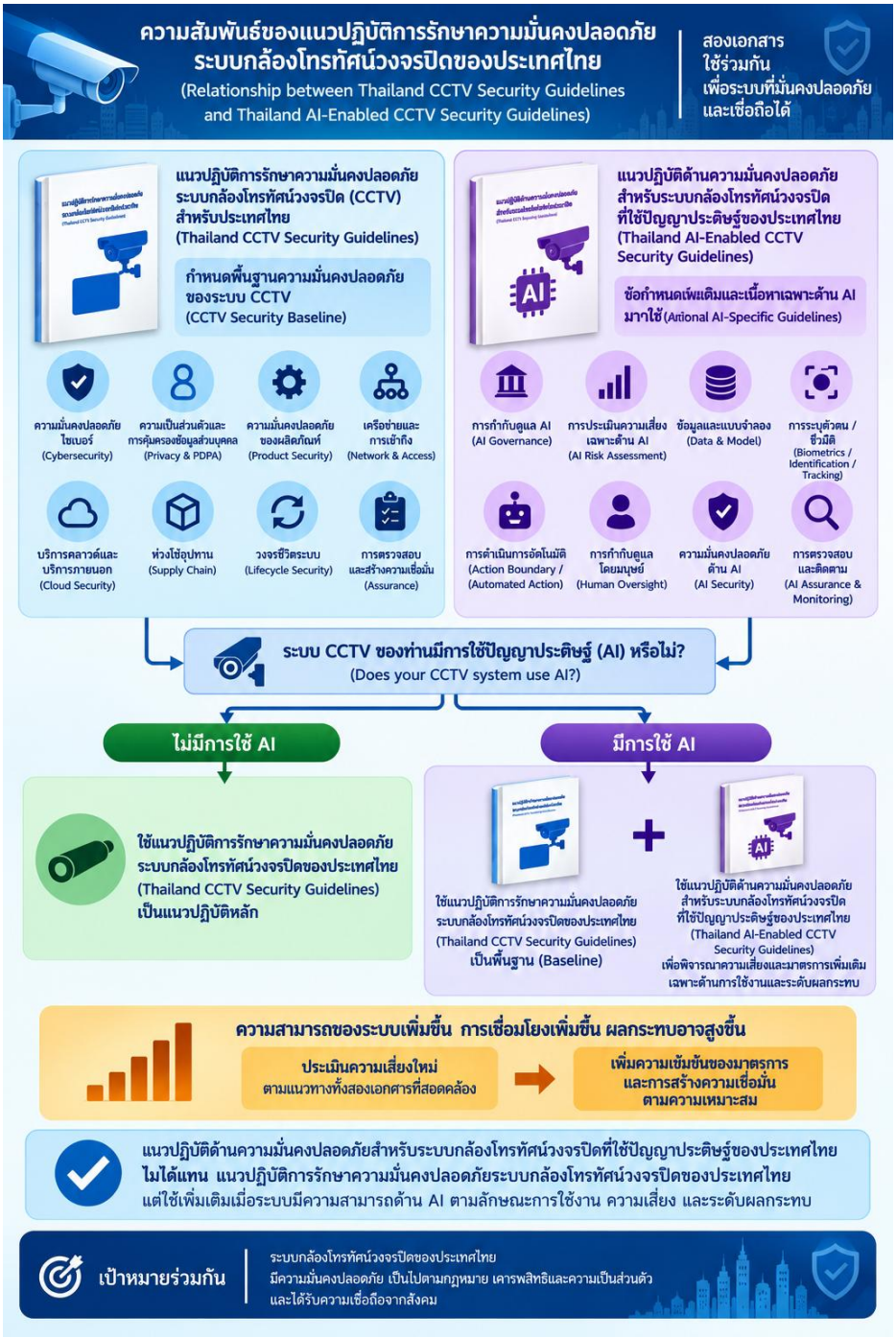
กำหนดแนวทางสำหรับการจัดทำข้อกำหนด การประเมินผลิตภัณฑ์และผู้ให้บริการ การตรวจรับ และหลักฐานประกอบการสร้างความเชื่อมั่น

บทที่ 5 หัวข้อที่ต้องพิจารณาเพิ่มเติม

ครอบคลุมบริการคลาวด์ บริการภายนอก แอปพลิเคชันและการเข้าถึงจากระยะไกล แนวทางการในการใช้แนวปฏิบัติทั้งสองฉบับในการรักษาความมั่นคงปลอดภัยระบบ CCTV ที่มีการใช้งานร่วมกับ AI และการทำงานร่วมกันระหว่างหน่วยงานในภาวะฉุกเฉิน

ภาคผนวก ก–ง

ประกอบด้วยรายการตรวจสอบก่อนส่งมอบ รายการประเมินตนเองตามรอบ อภิธานศัพท์ และเอกสาร กฎหมาย และมาตรฐานอ้างอิง



รูปที่ 1 ความสัมพันธ์ระหว่างแนวปฏิบัติทั้งสองฉบับเพื่อการรักษาความมั่นคงปลอดภัย CCTV ที่ครอบคลุม

ระบบ CCTV ทั่วไปให้ใช้แนวปฏิบัติฉบับนี้เป็นหลัก สำหรับระบบที่มีความสามารถด้าน AI ให้ใช้มาตรการของแนวปฏิบัติฉบับนี้เป็นค่าตั้งต้นด้านความมั่นคงปลอดภัย และพิจารณาความเสี่ยงและมาตรการเพิ่มเติมตามลักษณะการใช้งานและระดับผลกระทบดังอธิบายในแนวปฏิบัติฉบับที่สอง

ตารางแนวทางการอ่านตามกลุ่มผู้ใช้งาน

กลุ่มผู้อ่าน	ลักษณะการใช้งาน/บทบาท	ควรอ่านเป็นหลัก	ควรอ่านเพิ่มเติม
บุคคลทั่วไปที่ใช้ CCTV เพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว	ใช้ CCTV เพื่อดูแลบ้านพักอาศัย ทรัพย์สิน หรือความปลอดภัยส่วนบุคคล โดยไม่ได้ใช้เพื่อการประกอบธุรกิจหรือการดำเนินงานขององค์กร	ข้อ 3.1 และข้อ 5.1	ข้อ 2.3 เฉพาะเมื่อเกี่ยวข้อง และข้อ 3.2.1.7
ผู้ประกอบการรายย่อย ร้านค้า และ SME	ใช้ CCTV เพื่อการประกอบธุรกิจหรือการดำเนินงานของกิจการ ไม่ว่าจะดูแลระบบเองหรือใช้บริการจากบุคคลภายนอก	บทที่ 1, ข้อ 2.1, ข้อ 2.3, ข้อ 3.1 และภาคผนวก ข	ข้อ 3.2.1, ข้อ 3.4 และข้อ 5.1
ผู้บริหารและผู้กำกับดูแลขององค์กร	กำหนดทิศทาง อนุมัติ กำกับดูแลความเสี่ยง และติดตามการบริหารจัดการระบบ CCTV ขององค์กร	บทที่ 1–2, ข้อ 3.1 และบทที่ 4	ข้อ 3.5–3.8, บทที่ 5 และภาคผนวก ข
ผู้ปฏิบัติงานและผู้ดูแลระบบ	ปฏิบัติงาน บริหารบัญชีและสิทธิ ตั้งค่า เฝ้าระวัง บำรุงรักษา ปรับปรุง และตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับระบบ	ข้อ 3.3–3.8 และภาคผนวก ข	ข้อ 2.3, ข้อ 2.4 และบทที่ 5
ผู้ติดตั้งและผู้รวมระบบ (System Integrator: SI)	ออกแบบ ติดตั้ง ตั้งค่า ทดสอบ ส่งมอบ เชื่อมต่อ หรือบำรุงรักษาระบบตามขอบเขตที่ได้รับมอบหมาย	บทที่ 3, ข้อ 4.2 และภาคผนวก ก	ข้อ 2.1–2.3 และข้อ 4.1
ผู้จัดซื้อและผู้ตรวจประเมิน	กำหนดข้อกำหนด คัดเลือก จัดหา ตรวจรับ หรือประเมินความสอดคล้องและหลักฐานด้านความมั่นคงปลอดภัย	บทที่ 4, ภาคผนวก ก และภาคผนวก ง	ข้อ 2.1–2.3, ข้อ 3.2.5 และภาคผนวก ข

กลุ่มผู้อ่าน	ลักษณะการใช้งาน/บทบาท	ควรอ่านเป็นหลัก	ควรอ่านเพิ่มเติม
ผู้ผลิตและผู้จำหน่าย	ผลิต พัฒนา จัดหา จำหน่าย สนับสนุน หรือให้ข้อมูลด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ตลอดวงจรชีวิต	ข้อ 3.2.5 และข้อ 4.1	ข้อ 3.3–3.5 และข้อ 3.7
ผู้ที่มีระบบเดิมและกำลังพิจารณาปรับปรุง	มีระบบ CCTV ที่ใช้งานอยู่และต้องการประเมิน ปรับปรุง ทดแทน หรือยกระดับมาตรการด้านความมั่นคงปลอดภัย	ข้อ 3.7, ข้อ 3.1 และข้อ 2.1	ข้อ 3.2.2–3.2.5 และข้อ 3.5
ผู้เกี่ยวข้องกับระบบ CCTV ที่มี AI	ใช้ พัฒนา จัดหา ติดตั้ง หรือกำกับดูแล CCTV ที่มีการใช้ AI หรือความสามารถที่อาศัย AI	แนวปฏิบัติฉบับนี้เป็นค่าตั้งต้น โดยเฉพาะบทที่ 2–5	แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย สำหรับความเสี่ยงและมาตรการเฉพาะด้าน AI

หมายเหตุ: การจัดกลุ่มข้างต้นมีวัตถุประสงค์เพื่อช่วยให้ผู้อ่านเลือกศึกษาเนื้อหาที่เกี่ยวข้องกับลักษณะการใช้งานและบทบาทของตน บุคคลหรือองค์กรหนึ่งอาจมีมากกว่าหนึ่งบทบาท และควรพิจารณาเนื้อหาที่เกี่ยวข้องกับทุกบทบาทของตน รวมถึงกฎหมาย ข้อกำหนดตามสัญญา และข้อกำหนดเฉพาะภาคส่วนที่เกี่ยวข้อง

วิธีอ่านระดับมาตรการในตาราง

แนวปฏิบัติฉบับนี้แบ่งระดับมาตรการเป็น 3 ระดับ ได้แก่

- **ระดับพื้นฐาน (Baseline: B)**
- **ระดับเพิ่มเติม (Enhanced: E)**
- **ระดับความเชื่อมั่นสูง (High-Assurance: H)**

ผู้อ่านควรเริ่มจากการประเมินระดับความสำคัญและความเสี่ยงตามหัวข้อ 2.1 แล้วพิจารณามาตรการในระดับที่เหมาะสม ทั้งนี้ ระบบที่อยู่ในระดับสูงขึ้นควรครอบคลุมหลักการสำคัญของระดับก่อนหน้า และเพิ่มความเข้มงวดของมาตรการ การตรวจสอบ หรือหลักฐานตามความเสี่ยง ทั้งนี้ การจัดระดับ B/E/H เป็นวิธีการสำหรับกำหนดความเข้มข้นของมาตรการตามแนวปฏิบัติฉบับนี้ มิใช่การจำแนกสถานะทางกฎหมายขององค์กร และไม่สามารถใช้แทนข้อกำหนดตามกฎหมาย ประกาศ สัญญา หรือข้อกำหนดเฉพาะที่มีผลใช้บังคับ

ในตารางในส่วนที่เหลือของเอกสาร มีคำแนะนำความเข้มงวดในการใช้มาตรการ ให้ตีความดังนี้

สถานะ	ความหมาย
พึงปฏิบัติ	มาตรการหลักที่แนะนำสำหรับระดับนั้น หากเลือกวิธีอื่นควรสามารถอธิบายเหตุผลและแสดงได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสม
ควรพิจารณา	มาตรการเพิ่มเติมที่สามารถนำมาใช้ตามบริบท ระดับความเสี่ยง และความพร้อมขององค์กร
—	มิได้กำหนดเป็นการเฉพาะสำหรับระดับนั้น แต่อาจนำมาใช้ได้เมื่อเหมาะสม

สารบัญ

หน้า

บทที่ 1 บทนำ **16**
1.1 ที่มาของปัญหา **16**
1.2 วัตถุประสงค์ของเอกสาร **17**
1.3 ผู้ใช้เอกสารและบทบาท **18**
1.4 วิธีการยกร่างเอกสารนี้ **20**
1.5 ขอบเขตของคำแนะนำและวิธีอ่านตาราง **20**
1.6 หลักการพื้นฐานที่ใช้ตลอดทั้งเล่ม **21**
สรุปหลักการของบทที่ 1 ..... **23**
บทที่ 2 การกำกับดูแล ข้อกำหนด และกฎหมาย **24**
2.1 การกำหนดระดับการประยุกต์ใช้มาตรการตามความสำคัญและความเสี่ยง **24**
2.1.1 เหตุผลในการจำแนกระดับความสำคัญของระบบ **24**
2.1.2 ระดับความสำคัญของระบบ **24**
2.1.3 ปัจจัยที่ใช้พิจารณาระดับความสำคัญของระบบ **25**
2.1.4 แบบประเมินตนเองเพื่อจัดระดับความสำคัญของระบบ **26**
2.1.5 การแบ่งบทบาทหน้าที่ **28**
2.2 กรอบแนวทาง มาตรฐานอ้างอิง และกฎหมายที่เกี่ยวข้อง **30**
2.2.1 มาตรฐานและกรอบอ้างอิงหลัก **30**
2.2.2 กฎหมายและข้อกำหนดของประเทศไทยที่เกี่ยวข้อง **31**
2.3 การปกป้องคุ้มครองข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล **32**
2.3.1 การกำหนดวัตถุประสงค์ ความจำเป็น และฐานทางกฎหมาย **32**
2.3.2 ป้ายแจ้งและประกาศความเป็นส่วนตัว **33**
2.3.3 การใช้สิทธิของเจ้าของข้อมูลและการเปิดเผยข้อมูลแก่บุคคลภายนอก **33**
2.3.4 การจัดการเหตุละเมิดข้อมูลส่วนบุคคล **34**
2.3.5 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล **35**
2.3.6 การแบ่งบทบาทหน้าที่ **35**
2.4 การอบรมและสร้างความตระหนัก **36**
สรุปหลักการของบทที่ 2 ..... **37**
บทที่ 3 ค่าตั้งต้นด้านความมั่นคงปลอดภัยตลอดวงจรชีวิตระบบ **38**
3.1 เริ่มต้นอย่างมั่นคงปลอดภัยใน 7 ข้อ **39**
3.2 การออกแบบและการเลือกอุปกรณ์ **40**

3.2.1 การออกแบบ ตำแหน่ง และการวางกล้อง 40
3.2.2 ความละเอียดและคุณภาพของภาพ 47
3.2.3 ระยะเวลาการเก็บรักษาและการลบข้อมูล 49
3.2.4 การคำนวณขนาดพื้นที่จัดเก็บ 50
3.2.5 การเลือกอุปกรณ์ที่น่าเชื่อถือและความมั่นคงปลอดภัยของห่วงโซ่อุปทาน 52
3.3 การติดตั้ง 57
3.3.1 ความมั่นคงปลอดภัยทางกายภาพ 57
3.3.2 ระบบสายสัญญาณและโครงสร้างพื้นฐานการเชื่อมต่อ 58
3.3.3 สถาปัตยกรรมเครือข่าย การแบ่งโซน และหลักการไม่ให้ความเชื่อถือโดยปริยาย 59
3.3.4 การควบคุมพอร์ตและบริการเครือข่าย 63
3.3.5 การทดสอบและตรวจรับด้านเทคนิคหลังการติดตั้ง 65
3.4 การดำเนินงานอย่างมั่นคงปลอดภัย 66
3.4.1 ช่องทางบริหารจัดการที่มั่นคงปลอดภัย 66
3.4.2 การเข้ารหัสและการจัดการใบรับรอง 67
3.4.3 บัญชีผู้ใช้และการกำหนดสิทธิ 68
3.4.4 รหัสผ่าน ข้อมูลยืนยันตัวตน และการพิสูจน์ตัวตน 68
3.4.5 การดู การค้นหา และการส่งออกภาพ 69
3.5 การบำรุงรักษาและการเฝ้าระวัง 70
3.5.1 การปรับปรุงเฟิร์มแวร์ ซอฟต์แวร์ และการบำรุงรักษาระบบ 70
3.5.2 การเฝ้าระวังและการบันทึกเหตุการณ์ 72
3.5.3 รอบการตรวจสอบและการบำรุงรักษา 74
3.5.4 การสำรองข้อมูล การกู้คืน และความต่อเนื่อง 75
3.5.5 การบริหารงานบำรุงรักษาและสัญญาบริการ 76
3.5.6 การส่งซ่อมหรือส่งอุปกรณ์ออกนอกสถานที่ 78
3.6 ภัยคุกคาม สัญญาณผิดปกติ และการตอบสนองต่อเหตุการณ์ 79
3.6.1 ตัวอย่างภัยคุกคาม 79
3.6.2 ตัวอย่างสัญญาณผิดปกติ 80
3.6.3 กระบวนการตอบสนองต่อเหตุการณ์ 80
3.7 การประเมินและยกระดับระบบเดิมที่ติดตั้งใช้งานแล้ว 81
3.7.1 การสำรวจสภาพระบบเดิม 81
3.7.2 การจำแนกสภาพระบบเดิม 83
3.7.3 เกณฑ์การตัดสินใจในการปรับปรุงระบบเดิม 83

3.7.4 อายุการใช้งานและการวางแผนทดแทน 84
3.7.5 มาตรการชดเชย 84
3.7.6 แผนการเปลี่ยนผ่าน 85
3.7.7 ข้อควรพิจารณาด้านข้อมูลส่วนบุคคลเมื่อปรับปรุงหรือเปลี่ยนระบบ 86
3.8 การเลิกใช้อุปกรณ์และการจัดการข้อมูล 86
3.8.1 หลักการจัดการข้อมูลก่อนเลิกใช้งาน 87
3.8.2 หลักฐานการเลิกใช้งาน 87
สรุปหลักการของบทที่ 3 87
บทที่ 4 การจัดซื้อจัดจ้าง 88
4.1 ข้อกำหนดด้านความมั่นคงปลอดภัยในการจัดซื้อ 88
4.1.1 ข้อกำหนดทั่วไปด้านความมั่นคงปลอดภัย 88
4.1.2 การรับรอง ผลการทดสอบ และฉลากด้านความมั่นคงปลอดภัย 103
4.2 การส่งมอบและการตรวจรับอย่างมั่นคงปลอดภัย 103
4.2.1 การตรวจสอบระบบที่ส่งมอบ 104
4.2.2 การตรวจรับคุณภาพของภาพและสมรรถนะ 104
4.2.3 การตรวจสอบด้านความมั่นคงปลอดภัยก่อนเปิดใช้งาน 105
4.2.4 การส่งมอบข้อมูลและเอกสาร 106
4.2.5 การยกเลิกสิทธิและช่องทางชั่วคราว 107
4.2.6 การตรวจสอบหลักฐานการรับรองและผลการทดสอบ 107
4.2.7 การตรวจสอบบริการคลาวด์และบริการภายนอก 108
4.2.8 การจัดการข้อบกพร่องและความเสี่ยงคงเหลือ 108
4.2.9 ผลการตรวจรับ 109
สรุปหลักการของบทที่ 4 109
บทที่ 5 หัวข้อที่ต้องพิจารณาเพิ่มเติม 110
5.1 การใช้แอปพลิเคชัน อุปกรณ์เคลื่อนที่ คลาวด์ และบริการภายนอกอย่างมั่นคงปลอดภัย 110
5.1.1 การใช้แอปพลิเคชันและการเข้าถึงจากอุปกรณ์เคลื่อนที่ 112
5.1.2 ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย 113
5.1.3 สถานที่จัดเก็บ การประมวลผล และอธิปไตยข้อมูล 114
5.1.4 การเลือกผู้ให้บริการและความรับผิดชอบร่วม 115
5.1.5 การคุ้มครองข้อมูลส่วนบุคคลและการใช้ผู้ให้บริการภายนอก 115
5.1.6 การจัดการระยะเวลาเก็บรักษา การคืน และการลบข้อมูล 116
5.1.7 การแจ้งเหตุและการเปลี่ยนแปลงบริการ 117

5.1.8 การยุติหรือเปลี่ยนบริการ 118
5.2 ระบบ CCTV ที่ใช้การวิเคราะห์วิดีโอ ปัญญาประดิษฐ์ หรือข้อมูลชีวมิติ 118
5.2.1 เมื่อใดควรใช้แนวปฏิบัติ CCTV-AI เพิ่มเติม 119
5.2.2 การพิจารณาเพิ่มเติมสำหรับระบบที่มีความสามารถด้านปัญญาประดิษฐ์ 119
5.2.3 ความสัมพันธ์ระหว่างแนวปฏิบัติ CCTV ทั้งสองฉบับ 120
5.3 การทำงานร่วมกันระหว่างหน่วยงานและการแบ่งปันข้อมูลในภาวะฉุกเฉิน 123
สรุปหลักการของบทที่ 5 124
ภาคผนวก ก รายการตรวจสอบก่อนส่งมอบ 126
ก.1 ข้อมูลทั่วไปของระบบ 126
ก.2 การตรวจสอบการออกแบบ ตำแหน่งติดตั้ง และคุณภาพของภาพ 127
ก.3 อุปกรณ์ การติดตั้ง และสภาพแวดล้อม 128
ก.4 เครือข่ายและการเชื่อมต่อ 129
ก.5 บัญชีผู้ใช้งาน การพิสูจน์ตัวตน และสิทธิการเข้าถึง 130
ก.6 การเข้ารหัส ใบรับรอง และกุญแจ 131
ก.7 บันทึกเหตุการณ์ การเฝ้าระวัง และเวลา 132
ก.8 การจัดเก็บข้อมูล การสำรอง และการกู้คืน 132
ก.9 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล 133
ก.10 บริการคลาวด์และบริการภายนอก 134
ก.11 เอกสารและข้อมูลที่ต้องส่งมอบ 135
ก.12 สรุปผลการตรวจรับก่อนเปิดใช้งาน 136
ภาคผนวก ข รายการประเมินตนเองตามรอบ 137
ข.1 ข้อมูลการทบทวน 137
ข.2 การประเมินตามรอบ 138
ข.2.1 วัตถุประสงค์ พื้นที่ และความเหมาะสมของการใช้งาน 138
ข.2.2 สถานะอุปกรณ์ ซอฟต์แวร์ และการสนับสนุน 139
ข.2.3 บัญชีผู้ใช้งานและสิทธิการเข้าถึง 140
ข.2.4 เครือข่ายและค่าตั้งด้านความมั่นคงปลอดภัย 141
ข.2.5 บันทึกเหตุการณ์และการเฝ้าระวัง 141
ข.2.6 การจัดเก็บข้อมูล การสำรอง และการกู้คืน 142
ข.2.7 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล 143
ข.2.8 บริการคลาวด์และบริการภายนอก 143
ข.3 การทบทวนเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ 144

ข.4 สรุปผลการทบทวน 145
หลักการใช้ภาคผนวก ข 146
ภาคผนวก ค อภิธานศัพท์ (Glossary) 147
ค.1 ระบบ CCTV และคุณภาพของภาพ 147
ค.2 องค์ประกอบและการทำงานของระบบ 148
ค.3 เครือข่ายและการควบคุมการเข้าถึง 149
ค.4 การตั้งค่า การเฝ้าระวัง และการตรวจสอบ 150
ค.5 ช่องโหว่ ความมั่นคงปลอดภัยของผลิตภัณฑ์ และวงจรชีวิต 151
ค.6 ส่วนประกอบซอฟต์แวร์และห่วงโซ่อุปทาน 153
ค.7 การบริหารความเสี่ยงและการสร้างความเชื่อมั่น 154
ค.8 การจัดการข้อมูลและหลักฐาน 155
ค.9 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล 156
ค.10 คลาวด์ สถานที่จัดเก็บข้อมูล และเขตอำนาจทางกฎหมาย 157
ค.11 ปัญญาประดิษฐ์และข้อมูลชีวมิติ 158
ภาคผนวก ง เอกสาร กฎหมาย และมาตรฐานอ้างอิง 160
ง.1 กฎหมายและข้อกำหนดของประเทศไทย 160
ง.2 ระบบเฝ้าระวังด้วยวิดีโอ 160
ง.3 ความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัว 161
ง.4 ความมั่นคงปลอดภัยของผลิตภัณฑ์และระบบที่เชื่อมต่อ 161
ง.5 การเปิดเผยและการจัดการช่องโหว่ 161
ง.6 บริการคลาวด์ 162
ง.7 ข้อมูลชีวมิติและระบบ CCTV ที่ใช้ AI 162
ง.8 หลักการใช้เอกสารอ้างอิง 162

บทที่ 1 บทนำ

1.1 ที่มาของปัญหา

ระบบกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV) มีบทบาทสำคัญต่อการรักษาความปลอดภัย การเฝ้าระวัง การตรวจสอบเหตุการณ์ และการสนับสนุนภารกิจของหน่วยงานทั้งภาครัฐ ภาคเอกชน และประชาชน ระบบ CCTV ในปัจจุบันได้พัฒนาจากระบบบันทึกภาพแบบแยกส่วนไปสู่ระบบที่เชื่อมต่อผ่านเครือข่าย สามารถบริหารจัดการจากระยะไกล เชื่อมโยงกับระบบสารสนเทศอื่น และอาจใช้บริการคลาวด์สำหรับการจัดเก็บ ประมวลผล หรือบริหารจัดการข้อมูล

การเปลี่ยนแปลงดังกล่าวทำให้ระบบ CCTV มิได้เป็นเพียงระบบทางกายภาพสำหรับบันทึกภาพ แต่เป็นส่วนหนึ่งของระบบสารสนเทศและโครงสร้างพื้นฐานดิจิทัลขององค์กร ซึ่งอาจเผชิญความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัว ความพร้อมใช้งาน และความน่าเชื่อถือของข้อมูล

ความเสี่ยงที่สำคัญสามารถพิจารณาได้อย่างน้อย 4 ด้าน ดังนี้

1) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

กล้อง เครื่องบันทึก ระบบบริหารจัดการวิดีโอ (Video Management System: VMS) อุปกรณ์เครือข่าย ระบบจัดเก็บข้อมูล และส่วนประกอบอื่นของระบบ CCTV อาจมีช่องโหว่หรือการตั้งค่าที่ไม่เหมาะสม เช่น การใช้ข้อมูลยืนยันตัวตนเริ่มต้น (เช่นรหัสผ่านจากโรงงาน) การไม่ปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ การเปิดบริการเครือข่ายที่ไม่จำเป็น การกำหนดสิทธิไม่เหมาะสม หรือการเปิดให้เข้าถึงระบบจากภายนอกโดยไม่มีมาตรการควบคุมที่เพียงพอ ช่องโหว่หรือการตั้งค่าดังกล่าวอาจทำให้ผู้ไม่ได้รับอนุญาตเข้าถึงภาพหรือข้อมูล ควบคุมอุปกรณ์ เปลี่ยนแปลงการตั้งค่า ทำให้ระบบไม่สามารถให้บริการ หรือใช้ระบบ CCTV เป็นช่องทางในการเข้าถึงระบบอื่นขององค์กร

2) ความเสี่ยงด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

ภาพ วิดีโอ เสียง หรือข้อมูลอื่นที่ระบบ CCTV เก็บรวบรวมอาจสามารถใช้ระบุตัวบุคคลได้ ซึ่งจะกลายเป็นข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การกำหนดตำแหน่งและมุมมองของกล้อง ระยะเวลาเก็บรักษา การเข้าถึง การใช้ การเปิดเผย การส่งออก และการทำลายข้อมูล จึงต้องพิจารณาความจำเป็น ความได้สัดส่วน และข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

3) ความเสี่ยงด้านความพร้อมใช้งานและความน่าเชื่อถือของระบบ

ระบบ CCTV ควรสามารถเก็บบันทึกข้อมูลได้อย่างเหมาะสม เพื่อที่เมื่อเกิดเหตุการณ์ที่จำเป็นต้องตรวจสอบ ผู้ใช้งานสามารถเข้าถึงและใช้งานข้อมูลที่เก็บบันทึกไว้ได้ ระบบที่ออกแบบ ติดตั้ง หรือบำรุงรักษาไม่เหมาะสมอาจทำให้ข้อมูลไม่สามารถนำมาใช้ตามวัตถุประสงค์ เช่น กล้องไม่สามารถใช้งานได้ คุณภาพของภาพไม่เพียงพอ พื้นที่จัดเก็บไม่เพียงพอ เวลาในระบบไม่ถูกต้อง ข้อมูลสูญหาย หรือไม่สามารถตรวจพบความผิดปกติของระบบได้อย่างทันท่วงที ดังนั้น ความมั่นคงปลอดภัยของระบบ CCTV จึงควร

ครอบคลุมทั้งการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) รวมถึงความสามารถในการตรวจสอบย้อนหลังตามวัตถุประสงค์ของระบบ

4) ความเสี่ยงด้านการกำกับดูแลและการดำเนินงาน

แม้อุปกรณ์จะมีคุณสมบัติด้านความมั่นคงปลอดภัยที่เหมาะสม ความเสี่ยงยังอาจเกิดจากการดำเนินงานและการใช้งานที่ไม่เหมาะสม เช่น การใช้บัญชีร่วมกัน การกำหนดสิทธิเกินความจำเป็น การส่งต่อภาพผ่านช่องทางที่ไม่ได้รับอนุญาต การไม่เพิกถอนสิทธิเมื่อบุคลากรหรือผู้รับจ้างสิ้นสุดหน้าที่ การไม่มีผู้รับผิดชอบในการปรับปรุงระบบ หรือการไม่มีการตรวจสอบและบำรุงรักษาตามรอบ

การรักษาความมั่นคงปลอดภัยของระบบ CCTV จึงไม่สามารถดำเนินการได้ด้วยการเลือกผลิตภัณฑ์หรือเทคโนโลยีเพียงอย่างเดียว แต่ต้องอาศัยการกำกับดูแล การบริหารความเสี่ยง การออกแบบ การจัดซื้อจัดจ้าง การติดตั้งและตั้งค่า การดำเนินงาน การบำรุงรักษา การเฝ้าระวัง การตอบสนองต่อเหตุการณ์ และการเลิกใช้งานอย่างเหมาะสมตลอดวงจรชีวิตของระบบ

นอกจากนี้ ระบบ CCTV ที่ใช้งานอยู่เดิมอาจมีข้อจำกัดด้านเทคโนโลยี อายุการใช้งาน ความสามารถในการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ ความสามารถในการบันทึกเหตุการณ์ หรือการรองรับมาตรการด้านความมั่นคงปลอดภัยในปัจจุบัน

สำหรับการประยุกต์ใช้แนวปฏิบัตินี้กับระบบ CCTV ที่มีอยู่เดิม ผู้ใช้งานหรือองค์กรควรประเมินความเสี่ยง กำหนดมาตรการชดเชย และวางแผนปรับปรุงหรือทดแทนระบบอย่างเหมาะสม

1.2 วัตถุประสงค์ของเอกสาร

แนวปฏิบัติฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบสำหรับการรักษาความมั่นคงปลอดภัยของระบบ CCTV ในประเทศไทย โดยมีวัตถุประสงค์ดังต่อไปนี้

1. กำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัยที่สามารถประยุกต์ใช้กับระบบ CCTV ที่มีขนาด ลักษณะการใช้งาน และระดับความสำคัญแตกต่างกัน
2. สนับสนุนการบริหารตามระดับผลกระทบและความเสี่ยง เพื่อให้องค์กรสามารถเลือกมาตรการที่เหมาะสมและได้สัดส่วนกับบริบทของระบบ
3. สนับสนุนการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ ตั้งแต่การวางแผนและออกแบบ การจัดซื้อจัดจ้าง การติดตั้งและตรวจรับ การดำเนินงาน การบำรุงรักษาและเฝ้าระวัง การตอบสนองต่อเหตุการณ์ ตลอดจนการเลิกใช้งานและการจัดการข้อมูล
4. สนับสนุนการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว โดยคำนึงถึงวัตถุประสงค์ความจำเป็น ความได้สัดส่วน การจำกัดการเก็บรวบรวมและใช้ข้อมูล ระยะเวลาเก็บรักษา และการควบคุมการเข้าถึงและเปิดเผยข้อมูล
5. สนับสนุนการกำกับดูแลการใช้บริการคลาวด์และบริการภายนอกที่เกี่ยวข้องกับระบบ CCTV โดยพิจารณาความมั่นคงปลอดภัย ความเป็นส่วนตัว สถานที่จัดเก็บและประมวลผลข้อมูล เขตอำนาจ

ทางกฎหมาย การเข้าถึงข้อมูล การเข้ารหัสและการควบคุมกุญแจ ความพร้อมใช้งาน และความสามารถในการยุติหรือเปลี่ยนบริการ ตามระดับความสำคัญและผลการประเมินความเสี่ยงของระบบ

6. สนับสนุนการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการจัดซื้อจัดจ้าง การตรวจรับ การบริหารผู้ให้บริการ และการบริหารห่วงโซ่อุปทาน โดยไม่ผูกกับผู้ผลิต ยี่ห้อ ผลิตภัณฑ์ หรือรูปแบบเทคโนโลยีใดเป็นการเฉพาะ

7. กำหนดกรอบความรับผิดชอบระหว่างเจ้าของระบบ ผู้ใช้งาน ผู้ดูแลระบบ ผู้ติดตั้ง ผู้รวมระบบ ผู้ให้บริการ และผู้เกี่ยวข้อง เพื่อให้สามารถกำกับดูแลและตรวจสอบได้ตลอดวงจรชีวิตของระบบ

ขอบเขตของระบบที่ครอบคลุม

แนวปฏิบัติฉบับนี้ครอบคลุมองค์ประกอบทั้งหมดที่ประกอบกันเป็นระบบ CCTV เช่น กล้องและอุปกรณ์รับภาพ เครื่องบันทึก (NVR/DVR) ระบบบริหารวิดีโอ (VMS) ระบบจัดเก็บข้อมูลและการสำรองข้อมูล อุปกรณ์เครือข่ายและอุปกรณ์ป้องกันเครือข่ายที่ให้บริการแก่ระบบ CCTV เครื่องลูกข่ายและแอปพลิเคชันสำหรับดูภาพ อุปกรณ์เคลื่อนที่ บริการคลาวด์และบริการภายนอก ตลอดจนระบบด้านความมั่นคงปลอดภัยโดยรอบที่เชื่อมต่อหรือรับข้อมูลจากระบบ CCTV เช่น ระบบควบคุมการเข้าออก ระบบแจ้งเตือน และระบบเฝ้าระวังกลาง (SIEM/SOC) ทั้งนี้ มาตรการสำหรับองค์ประกอบใดให้พิจารณาตามบทบาทขององค์ประกอบนั้นในระบบและระดับความสำคัญของระบบโดยรวม

สถานะของเอกสาร

แนวปฏิบัติฉบับนี้เป็นแนวทางด้านความมั่นคงปลอดภัยที่พัฒนาขึ้นโดยอ้างอิงหลักการบริหารความเสี่ยง มาตรฐานและแนวปฏิบัติสากล ตลอดจนกฎหมายและข้อกำหนดที่เกี่ยวข้องของประเทศไทย มิได้มีสถานะเป็นกฎหมายหรือข้อบังคับโดยตัวเอกสารเอง

องค์กรควรนำแนวปฏิบัตินี้ไปประยุกต์ใช้ให้เหมาะสมกับวัตถุประสงค์ บริบท ระดับความสำคัญ และความเสี่ยงของระบบ ทั้งนี้ หากองค์กรอยู่ภายใต้กฎหมาย ประกาศ หลักเกณฑ์ สัญญา หรือข้อกำหนดเฉพาะให้ถือปฏิบัติตามข้อกำหนดดังกล่าวเป็นลำดับแรก

ระดับความสำคัญของระบบที่กำหนดในแนวปฏิบัตินี้เป็นเครื่องมือสำหรับเลือกมาตรการด้านความมั่นคงปลอดภัยให้เหมาะสมกับความเสี่ยง มิใช่การจำแนกระดับการปฏิบัติตามกฎหมาย และมิได้ลดทอนหน้าที่ตามกฎหมายหรือข้อกำหนดที่มีผลใช้บังคับกับองค์กร

1.3 ผู้ใช้เอกสารและบทบาท

แนวปฏิบัติฉบับนี้จัดทำขึ้นสำหรับผู้เกี่ยวข้องกับระบบ CCTV ตลอดวงจรชีวิตของระบบ โดยบุคคลหรือหน่วยงานหนึ่งอาจมีมากกว่าหนึ่งบทบาทตามโครงสร้าง ขนาด และบริบทขององค์กร

บทบาท	ตัวอย่างผู้เกี่ยวข้อง	ความรับผิดชอบหลัก
เจ้าของระบบ/ผู้ใช้งาน	เจ้าของสถานที่ หน่วยงานเจ้าของระบบ ผู้บริหาร ฝ่ายรักษาความปลอดภัย ฝ่ายเทคโนโลยีสารสนเทศ	กำหนดวัตถุประสงค์ ระดับความสำคัญ ข้อกำหนด ความเสี่ยง และกำกับดูแลการใช้งาน
ผู้ปฏิบัติงาน/ผู้ดูแลระบบ	เจ้าหน้าที่ศูนย์ควบคุม ผู้ดูแล VMS/NVR ผู้ดูแลเครือข่าย ผู้ได้รับสิทธิเข้าถึงข้อมูล	ดำเนินงาน บริหารสิทธิ เฝ้าระวัง ตรวจสอบ บันทึก และรายงานเหตุการณ์
ผู้ติดตั้ง/ผู้รวมระบบ/ผู้ให้บริการ	ผู้ออกแบบ ผู้ติดตั้ง ผู้รวมระบบ ผู้ให้บริการบำรุงรักษา	ออกแบบ เลือกอุปกรณ์ ติดตั้ง ตั้งค่า ทดสอบ ส่งมอบ และสนับสนุนระบบตามขอบเขตที่กำหนด
ผู้ผลิต/ผู้จำหน่าย	ผู้ผลิตอุปกรณ์ ผู้พัฒนาซอฟต์แวร์ ผู้แทนจำหน่าย	พัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย บริหารและเปิดเผยช่องโหว่ ออกการปรับปรุงด้านความมั่นคงปลอดภัย และแจ้งสถานะ EoL/EoS
ผู้จัดซื้อ/ผู้กำกับดูแล/ผู้ตรวจประเมิน	ฝ่ายจัดซื้อ ผู้บริหารความเสี่ยง ผู้ตรวจสอบภายใน ผู้ตรวจประเมิน	กำหนดข้อกำหนดในการจัดซื้อ ตรวจรับ ติดตาม และประเมินความสอดคล้อง

การแบ่งบทบาทดังกล่าวมีวัตถุประสงค์เพื่อให้สามารถระบุความรับผิดชอบได้อย่างชัดเจน และเป็นข้อมูลอ้างอิงเท่านั้น มิได้กำหนดให้องค์กรต้องจัดโครงสร้างบุคลากรตามรูปแบบดังกล่าว

องค์กรขนาดเล็กอาจมีบุคคลหนึ่งรับผิดชอบหลายบทบาทได้ แต่สำหรับกิจกรรมที่มีความสำคัญ ควรกำหนดให้สามารถระบุได้ว่า

1. ใครกำหนด
2. ใครอนุมัติ
3. ใครดำเนินการ
4. ใครตรวจสอบ
5. ใครรับผิดชอบเมื่อเกิดเหตุ

1.4 วิธีการยกร่างเอกสารนี้

แนวปฏิบัติฉบับนี้จัดทำขึ้นโดยสังเคราะห์หลักการจากมาตรฐานและแนวปฏิบัติสากลที่เกี่ยวข้องกับระบบ CCTV ความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัว บริการคลาวด์ ความมั่นคงปลอดภัยของผลิตภัณฑ์และห่วงโซ่อุปทาน จากนั้นได้ประยุกต์ให้เหมาะสมกับบริบทการใช้งานและกฎหมายของประเทศไทย โดยยึดหลักสำคัญดังต่อไปนี้

1) ความเป็นกลางด้านผู้ผลิตและเทคโนโลยี

กำหนดมาตรการจากผลลัพธ์ด้านความมั่นคงปลอดภัยที่ต้องการ โดยไม่ผูกกับผู้ผลิต ยี่ห้อ รุ่นผลิตภัณฑ์ หรือรูปแบบการติดตั้งใดเป็นการเฉพาะ เว้นแต่มีข้อกำหนดที่มีผลใช้บังคับหรือเหตุผลด้านความเสี่ยงรองรับ

2) การพิจารณาตามผลกระทบและความเสี่ยง

ระดับของมาตรการควรสัมพันธ์กับวัตถุประสงค์ ลักษณะข้อมูล การเชื่อมต่อ ความสำคัญของระบบ ภัยคุกคาม และผลกระทบที่อาจเกิดขึ้น ระบบ CCTV แต่ละระบบอาจพิจารณาใช้มาตรการในระดับที่แตกต่างกันตามความเหมาะสมและความจำเป็น

3) การแยกข้อกำหนดตามกฎหมายออกจากข้อเสนอแนะทางเทคนิค

ข้อกำหนดตามกฎหมายของประเทศไทย กฎระเบียบ หรือมาตรฐานที่เกี่ยวข้องที่มีผลใช้บังคับกับองค์กรยังคงต้องปฏิบัติตามโดยไม่ขึ้นอยู่กับระดับความสำคัญของระบบตามที่แนะนำในแนวปฏิบัตินี้ ส่วนมาตรการทางเทคนิคและการบริหารอื่นควรเลือกใช้ตามความเสี่ยงและบริบท

4) การรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิต

พิจารณาความเสี่ยงตั้งแต่การกำหนดวัตถุประสงค์ การออกแบบ การจัดซื้อ การติดตั้ง การตรวจรับ การใช้งาน การบำรุงรักษา การเฝ้าระวัง การตอบสนองต่อเหตุการณ์ การปรับปรุงระบบ จนถึงการเลิกใช้งานและการจัดการข้อมูล

5) การป้องกันเชิงลึก

ไม่พึ่งพามาตรการด้านความมั่นคงปลอดภัยเพียงมาตรการเดียว แต่ใช้มาตรการด้านบุคลากร กระบวนการ เทคโนโลยี และกายภาพร่วมกันตามความเหมาะสม

6) การตรวจสอบและสร้างความเชื่อมั่น

มาตรการที่กำหนดควรสามารถตรวจสอบได้ว่ามีการดำเนินการจริงและให้ผลตามวัตถุประสงค์ โดยระดับและรูปแบบของหลักฐานควรสัมพันธ์กับระดับความสำคัญและความเสี่ยงของระบบ

1.5 ขอบเขตของคำแนะนำและวิธีอ่านตาราง

แนวปฏิบัติฉบับนี้ใช้หลัก **ความได้สัดส่วนของมาตรการ** โดยกำหนดระดับการประยุกต์ใช้มาตรการด้านความมั่นคงปลอดภัยตามระดับความสำคัญและความเสี่ยงของระบบ

ระดับที่ใช้ในเอกสารประกอบด้วย

- **ระดับพื้นฐาน (Baseline: B)** สำหรับมาตรการพื้นฐานที่ระบบ CCTV ควรมี
- **ระดับเพิ่มเติม (Enhanced: E)** สำหรับระบบที่มีความสำคัญหรือมีความเสี่ยงเพิ่มขึ้น
- **ระดับความเชื่อมั่นสูง (High-Assurance: H)** สำหรับระบบที่อาจก่อให้เกิดผลกระทบสูง และต้องการมาตรการ การตรวจสอบ หรือหลักฐานที่เข้มงวดมากขึ้น

ระดับดังกล่าวควรพิจารณาจากบริบทและผลการประเมินความเสี่ยงโดยรวม ไม่ควรกำหนดจากปัจจัยใดปัจจัยหนึ่งเพียงอย่างเดียว เช่น ประเภทองค์กร เทคโนโลยี รูปแบบการติดตั้ง หรือรูปแบบบริการ ดังนั้น การเป็นระบบภายในองค์กร คลาวด์ส่วนตัว คลาวด์สาธารณะ หรือคลาวด์แบบผสม ตลอดจนการเป็นองค์กรขนาดใหญ่หรือขนาดเล็ก มิได้ทำให้ระบบอยู่ในระดับใดโดยอัตโนมัติ

สำหรับตารางมาตรการในเอกสาร ให้ใช้ความหมายดังต่อไปนี้

สถานะ	ความหมาย
พึงปฏิบัติ	มาตรการหลักที่แนะนำสำหรับระดับนั้น หากเลือกวิธีอื่นควรสามารถอธิบายเหตุผลและแสดงได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสม
ควรพิจารณา	มาตรการเพิ่มเติมที่สามารถนำมาใช้ตามบริบท ระดับความเสี่ยง และความพร้อมขององค์กร
—	มิได้กำหนดเป็นการเฉพาะสำหรับระดับนั้น แต่อาจนำมาใช้ได้เมื่อเหมาะสม

1.6 หลักการพื้นฐานที่ใช้ตลอดทั้งเล่ม

การประยุกต์ใช้แนวปฏิบัติฉบับนี้ควรยึดหลักการต่อไปนี้ตลอดวงจรชีวิตของระบบ

หลักการ	สาระสำคัญ	ตัวอย่างการประยุกต์ใช้กับ CCTV
การบริหารตามความเสี่ยง (Risk-Based Approach)	เลือกมาตรการตามระดับความเสี่ยงและผลกระทบ	เพิ่มความเข้มงวดของการควบคุมสำหรับระบบที่มีผลกระทบสูง
ความมั่นคงปลอดภัยตั้งแต่การออกแบบและโดยค่าเริ่มต้น (Secure by Design and by Default)	ออกแบบและกำหนดค่าตั้งต้นให้มีความมั่นคงปลอดภัย	ไม่ใช้ข้อมูลยืนยันตัวตนเริ่มต้นร่วม ปิดบริการที่ไม่จำเป็น และจำกัดการเชื่อมต่อตั้งแต่เริ่มต้น
ความเป็นส่วนตัวตั้งแต่การออกแบบ (Privacy by Design)	คำนึงถึงความเป็นส่วนตัวตั้งแต่กำหนดวัตถุประสงค์และออกแบบระบบ	จำกัดมุมกล้องเท่าที่จำเป็น ใช้การปิดบังพื้นที่ในภาพ เมื่อเหมาะสม

หลักการ	สาระสำคัญ	ตัวอย่างการประยุกต์ใช้กับ CCTV
การป้องกันเชิงลึก (Defense in Depth)	ใช้มาตรการหลายชั้นร่วมกัน	การแบ่งเครือข่าย การควบคุมการเข้าถึง การเข้ารหัส การบันทึกเหตุการณ์ และการเฝ้าระวัง
การให้สิทธิเท่าที่จำเป็น (Least Privilege)	ให้สิทธิเฉพาะเท่าที่จำเป็นต่อหน้าที่	แยกสิทธิผู้ดูภาพ ผู้ส่งออกข้อมูล และผู้ดูแลระบบ
หลักการไม่ให้ความเชื่อถือโดยปริยาย (Zero Trust Principles)	ไม่ถือว่าผู้ใช้ อุปกรณ์ หรือการเชื่อมต่อมีความน่าเชื่อถือเพียงเพราะอยู่ภายในเครือข่าย	พิสูจน์ตัวตน จำกัดการเชื่อมต่อ และตรวจสอบการเข้าถึงตามความเสี่ยง
การจำกัดตามวัตถุประสงค์และการใช้ข้อมูลเท่าที่จำเป็น (Purpose Limitation and Data Minimization)	เก็บ ใช้ และเปิดเผยข้อมูลเท่าที่จำเป็นต่อวัตถุประสงค์	จำกัดมุมกล้อง ระยะเวลาเก็บรักษา การบันทึกเสียง และการส่งออกข้อมูล
ความรับผิดชอบและการตรวจสอบได้ (Accountability)	สามารถแสดงเหตุผล การตัดสินใจ การดำเนินการ และหลักฐานที่เกี่ยวข้องได้	บันทึกการกำหนดสิทธิ การส่งออกข้อมูล การเปลี่ยนแปลงระบบ และผลการตรวจสอบ
การกำกับดูแลข้อมูล (Data Governance)	ทราบว่าข้อมูลถูกเก็บ ใช้ ประมวลผล ส่งต่อ เข้าถึง และทำลายอย่างไร	กำหนดเจ้าของข้อมูล ระยะเวลาเก็บรักษา สิทธิ และการจัดการตลอดวงจรชีวิต
การกำกับดูแลผู้ให้บริการและห่วงโซ่อุปทาน (Third-Party and Supply Chain Governance)	ความมั่นคงปลอดภัยต้องครอบคลุมผู้ให้บริการและส่วนประกอบภายนอก	กำหนดข้อกำหนดใน TOR/สัญญา การจัดการช่องโหว่ การสนับสนุน และการสิ้นสุดบริการ
การเฝ้าระวังและปรับปรุงอย่างต่อเนื่อง (Continuous Monitoring and Improvement)	ความมั่นคงปลอดภัยไม่สิ้นสุดเมื่อส่งมอบระบบ	ตรวจสอบสถานะระบบ ช่องโหว่ การอัปเดต บันทึกเหตุการณ์ และทบทวนความเสี่ยงตามรอบ

หลักสำคัญของแนวปฏิบัติฉบับนี้จึงไม่ควรเริ่มจากคำถามว่า **“ควรเลือกกล้อง ยี่ห้อ หรือเทคโนโลยีใด”** แต่ควรเริ่มจาก **ระบบถูกใช้เพื่อวัตถุประสงค์ใด ⟶ หากเกิดเหตุจะมีผลกระทบอย่างไร ⟶ มีความเสี่ยงใด ⟶ ต้องมีมาตรการใด ⟶ และจะยืนยันได้อย่างไรว่ามาตรการและระบบทำงานตามที่กำหนด**

สรุปหลักการของบทที่ 1

แนวปฏิบัติฉบับนี้กำหนดกรอบการรักษาความมั่นคงปลอดภัยของระบบ CCTV โดยพิจารณาร่วมกันทั้งความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล ความพร้อมใช้งานและความน่าเชื่อถือของระบบ ตลอดจนการกำกับดูแลและการดำเนินงาน เพื่อให้การรักษาความมั่นคงปลอดภัยครอบคลุมตลอดวงจรชีวิตของระบบ

การประยุกต์ใช้แนวปฏิบัติควรยึดหลักการบริหารตามผลกระทบและความเสี่ยง ความได้สัดส่วนของมาตรการ ความเป็นกลางด้านผู้ผลิตและเทคโนโลยี การรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัวตั้งแต่การออกแบบ การป้องกันเชิงลึก การให้สิทธิเท่าที่จำเป็น และความสามารถในการตรวจสอบและสร้างความเชื่อมั่น

การแบ่งระดับความเข้มข้นของมาตรการเป็นระดับ พื้นฐาน (Baseline: B) ระดับเพิ่มเติม (Enhanced: E) และระดับความเชื่อมั่นสูง (High-Assurance: H) ใช้เพื่อช่วยกำหนดความเข้มข้นของมาตรการให้เหมาะสมกับบริบทและความเสี่ยง มิใช่การจัดประเภทองค์กรตามกฎหมาย และไม่ใช้ทดแทนหน้าที่ตามกฎหมาย ประกาศ หลักเกณฑ์ สัญญา หรือข้อกำหนดเฉพาะที่มีผลใช้บังคับ

การดำเนินการรักษาความมั่นคงปลอดภัยของระบบ CCTV จะต้องดำเนินการตลอดวงจรชีวิตครอบคลุมตั้งแต่การระบุวัตถุประสงค์ไปจนถึงการตรวจสอบมาตรการและระบบสามารถดำเนินงานได้ตามที่กำหนดหรือไม่

บทที่ 2 การกำกับดูแล ข้อกำหนด และกฎหมาย

การรักษาความมั่นคงปลอดภัยของระบบกล้องโทรทัศน์วงจรปิดไม่ควรพิจารณาเฉพาะคุณสมบัติทางเทคนิคของกล้องหรืออุปกรณ์ แต่ควรครอบคลุมการกำกับดูแล ความรับผิดชอบ การบริหารความเสี่ยง ข้อกำหนดที่มีผลใช้บังคับ การคุ้มครองข้อมูลส่วนบุคคล และการสร้างความตระหนักแก่ผู้เกี่ยวข้อง มาตรการที่นำมาใช้ควรเหมาะสมและได้สัดส่วนกับวัตถุประสงค์ บริบท ระดับความสำคัญ ผลกระทบ และความเสี่ยงของระบบ โดยกำหนดให้ระบบ CCTV แต่ละระบบใช้มาตรการในระดับที่เหมาะสมกับระบบนั้น ๆ

บทนี้ครอบคลุมการจำแนกระดับความสำคัญของระบบ กรอบมาตรฐานและข้อกำหนดที่เกี่ยวข้อง การคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว ตลอดจนการอบรมและสร้างความตระหนักแก่ผู้เกี่ยวข้อง

2.1 การกำหนดระดับการประยุกต์ใช้มาตรการตามความสำคัญและความเสี่ยง

2.1.1 เหตุผลในการจำแนกระดับความสำคัญของระบบ

ระบบ CCTV มีวัตถุประสงค์ ลักษณะข้อมูล สภาพแวดล้อม การเชื่อมต่อ และผลกระทบที่อาจเกิดขึ้นแตกต่างกัน การกำหนดให้ทุกระบบใช้มาตรการด้านความมั่นคงปลอดภัยในระดับเดียวกันจึงอาจไม่เหมาะสม ทั้งในกรณีที่มาตรการเข้มงวดเกินความจำเป็นซึ่งจะเป็นการเพิ่มต้นทุนในการบริหารจัดการและอาจจะกระทบต่อการใช้งาน และกรณีที่มาตรการไม่เพียงพอต่อความเสี่ยงซึ่งจะทำให้ระบบไม่สามารถป้องกันและรับมือจากภัยคุกคามได้และอาจได้รับผลกระทบมากกว่าที่องค์กรหรือผู้ใช้งานยอมรับได้

2.1.2 ระดับความสำคัญของระบบ

แนวปฏิบัติฉบับนี้จึงกำหนดระดับการประยุกต์ใช้มาตรการ 3 ระดับ ได้แก่ **ระดับพื้นฐาน (Baseline: B) ระดับเพิ่มเติม (Enhanced: E) และระดับความเชื่อมั่นสูง (High-Assurance: H)** เพื่อให้องค์กรสามารถกำหนดมาตรการ การตรวจสอบ และระดับการสร้างความเชื่อมั่นให้เหมาะสมกับผลกระทบและความเสี่ยง การจำแนกดังกล่าวเป็นวิธีการประยุกต์ใช้แนวปฏิบัติฉบับนี้ มิใช่การจัดประเภทองค์กรตามกฎหมาย และมิใช่การจำแนกโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หากองค์กรหรือระบบอยู่ภายใต้กฎหมาย ประกาศ หลักเกณฑ์ สัญญา หรือข้อกำหนดเฉพาะ ให้ถือปฏิบัติตามข้อกำหนดดังกล่าว

ระดับ	ลักษณะของระบบและผลกระทบ
ระดับพื้นฐาน (Baseline: B)	ผลกระทบโดยรวมอยู่ในวงจำกัด ระบบไม่มีบทบาทสำคัญต่อภารกิจหรือความปลอดภัยในระดับสูง และการหยุดชะงักสามารถจัดการได้โดยไม่ก่อให้เกิดผลกระทบอย่างมีนัยสำคัญ

ระดับ	ลักษณะของระบบและผลกระทบ
ระดับเพิ่มเติม (Enhanced: E)	การรั่วไหล การเปลี่ยนแปลง หรือการหยุดชะงักอาจส่งผลกระทบอย่างมีนัยสำคัญต่อบุคคล การดำเนินงาน ทรัพย์สิน ชื่อเสียง หรือภารกิจขององค์กร
ระดับความเชื่อมั่นสูง (High-Assurance: H)	ความผิดพลาด การถูกโจมตี การรั่วไหล หรือการหยุดชะงักอาจก่อให้เกิดผลกระทบสูงต่อความปลอดภัยของบุคคล ภารกิจสำคัญ บริการสำคัญ หรือระบบอื่นที่เชื่อมต่อ

ระดับที่สูงขึ้นควรครอบคลุมหลักการของระดับก่อนหน้าและเพิ่มความเข้มงวดตามความเสี่ยง โดยไม่จำเป็นต้องหมายถึงการใช้เทคโนโลยีที่ซับซ้อนหรือมีต้นทุนสูงกว่าเสมอไป

2.1.3 ปัจจัยที่ใช้พิจารณาระดับความสำคัญของระบบ

การกำหนดระดับความสำคัญไม่ควรพิจารณาจากปัจจัยเดียว เช่น ประเภทสถานที่ จำนวนกล้อง ขนาดองค์กร หรือเทคโนโลยี แต่ควรพิจารณาจากผลกระทบและบริบทของระบบโดยรวม อย่างน้อย 4 มิติ ดังนี้

ปัจจัยที่พิจารณา	ประเด็นที่ควรพิจารณา
1. ความสำคัญของระบบหรือภารกิจ (System/Mission Criticality)	บทบาทของ CCTV ต่อความปลอดภัยของบุคคล ทรัพย์สิน สถานที่สำคัญ การดำเนินงาน บริการหรือภารกิจสำคัญ รวมถึงความสามารถในการดำเนินงานเมื่อระบบไม่พร้อมใช้งาน
2. ผลกระทบด้านข้อมูล (Data Impact)	ความสามารถในการระบุตัวบุคคล ลักษณะและปริมาณข้อมูล จำนวนบุคคลที่ได้รับผลกระทบ พื้นที่ที่มีความคาดหวังด้านความเป็นส่วนตัว การบันทึกเสียง การเชื่อมโยงหรือเปิดเผยข้อมูล และผลกระทบหากข้อมูลรั่วไหลหรือถูกใช้โดยไม่ได้รับอนุญาต
3. การเชื่อมต่อและการเปิดรับความเสี่ยง (Connectivity and Exposure)	การเชื่อมต่ออินเทอร์เน็ต การเข้าถึงจากระยะไกล การเชื่อมต่อกับระบบสารสนเทศหรือระบบเทคโนโลยีปฏิบัติการ (Operational Technology: OT) การใช้บริการคลาวด์หรือบริการภายนอก และการเข้าถึงโดยผู้รับจ้างหรือบุคคลภายนอก
4. ผลกระทบจากความล้มเหลวหรือการถูกโจมตี (Operational and Security Impact)	ผลกระทบจากการหยุดให้บริการ การสูญหายหรือเปลี่ยนแปลงข้อมูล การสูญเสียความสามารถในการตรวจสอบเหตุการณ์ การละเมิดข้อมูลส่วนบุคคล การขยายผลไปยังระบบอื่น รวมถึงผลกระทบด้านกฎหมาย สัญญา การเงิน หรือชื่อเสียง

ประเภทของสถานที่สามารถใช้เป็นข้อมูลประกอบการประเมินได้ แต่ไม่ควรใช้เป็นเกณฑ์ตัดสินระดับโดยอัตโนมัติ ระบบ CCTV ขนาดเล็กที่สนับสนุนภารกิจสำคัญอาจต้องใช้มาตรการเข้มงวดกว่าระบบขนาดใหญ่ที่มีผลกระทบโดยรวมจำกัด

นอกจากปัจจัยและแนวทางในการประเมินระดับความสำคัญและความเข้มข้นของมาตรการที่ได้นำเสนอก่อนหน้าแล้ว หากมีปัจจัยเพิ่มเติมดังต่อไปนี้ องค์กรและผู้ใช้งานอาจพิจารณายกระดับมาตรการได้ตามความเหมาะสม

ปัจจัยเพิ่มเติมที่ควรพิจารณา	ตัวอย่าง
ความสำคัญต่อระบบหรือภารกิจอื่น	CCTV เชื่อมต่อหรือสนับสนุนระบบหรือภารกิจสำคัญ
การเปิดรับจากภายนอก	Internet-facing, Remote Access หรือการเชื่อมต่อจากเครือข่ายภายนอก
บุคคลภายนอก	ผู้ให้บริการ ผู้รับจ้าง หรือผู้ผลิตสามารถเข้าถึงระบบ
ผลกระทบด้านข้อมูล	มีข้อมูลจำนวนมาก ข้อมูลที่อาจก่อให้เกิดผลกระทบสูง หรือการเชื่อมโยงข้อมูลจากหลายระบบ
ประวัติและภัยคุกคาม	เคยเกิดเหตุ หรือมีภัยคุกคาม/ช่องโหว่ที่เกี่ยวข้องอย่างมีนัยสำคัญ
ข้อกำหนดเฉพาะ	กฎหมาย ประกาศ ข้อกำหนดของหน่วยงานกำกับ สัญญา หรือข้อกำหนดขององค์กร

หลักสำคัญคือการประเมินผลกระทบของระบบ มิใช่การจัดระดับจากชื่อ ประเภท หรือขนาดของสถานที่

2.1.4 แบบประเมินตนเองเพื่อจัดระดับความสำคัญของระบบ

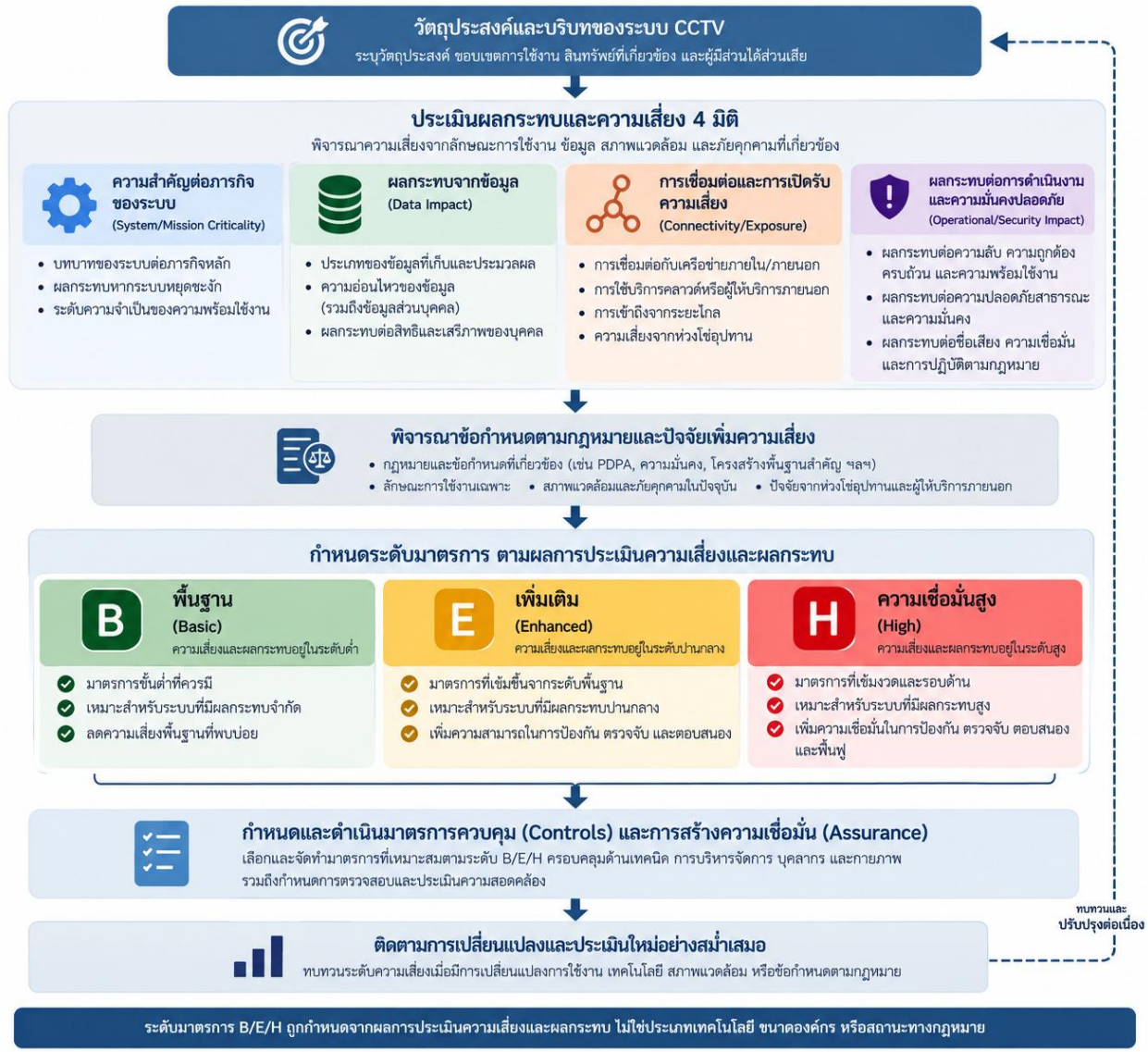
มิติที่ประเมิน	ต่ำ	ปานกลาง	สูง
ความสำคัญต่อภารกิจ	ผลกระทบจำกัดและยังสามารถดำเนินงานต่อได้	กระทบการดำเนินงานอย่างมีนัยสำคัญ	กระทบความปลอดภัย ภารกิจ หรือบริการสำคัญ
ผลกระทบด้านข้อมูล	ข้อมูลและจำนวนผู้ได้รับผลกระทบจำกัด	มีข้อมูลส่วนบุคคลหรือผู้ได้รับผลกระทบจำนวนมาก	การเปิดเผยหรือใช้ข้อมูลโดยไม่ได้รับอนุญาตอาจก่อให้เกิดผลกระทบสูง

มิติที่ประเมิน	ต่ำ	ปานกลาง	สูง
การเชื่อมต่อและการเปิดรับความเสี่ยง	ระบบแยกส่วนและมีช่องทางเข้าถึงจำกัด	มีการเข้าถึงจากระยะไกลหรือเชื่อมต่อกับระบบอื่นบางส่วน	เชื่อมต่อหลายระบบ ใช้บริการภายนอก หรือมีช่องทางเข้าถึงที่มีผลกระทบสูง
ผลกระทบเมื่อระบบถูกโจมตีหรือหยุดทำงาน	ผลกระทบจำกัดและสามารถแก้ไขได้โดยง่าย	กระทบการรักษาความปลอดภัยหรือการดำเนินงาน	อาจก่อให้เกิดผลกระทบรุนแรงหรือขยายไปยังระบบหรือภารกิจอื่น

แนวทางการแปลผล

- หากทุกมิติอยู่ในระดับต่ำเป็นหลัก สามารถเริ่มพิจารณาจาก **ระดับพื้นฐาน (B)**
- หากมีมิติหนึ่งหรือหลายมิติอยู่ในระดับปานกลาง ควรพิจารณา **ระดับเพิ่มเติม (E)**
- หากมีมิติสำคัญอยู่ในระดับสูง โดยเฉพาะด้านความปลอดภัยของบุคคล ภารกิจสำคัญ หรือผลกระทบด้านข้อมูล ควรพิจารณา **ระดับความเชื่อมั่นสูง (H)**

ไม่ควรใช้การเฉลี่ยเพื่อลดทอนผลกระทบระดับสูง หากผลกระทบในมิติสำคัญอยู่ในระดับสูง ควรพิจารณามาตรการที่สอดคล้องกับผลกระทบนั้น หรือดำเนินการประเมินความเสี่ยงเพิ่มเติมและบันทึกเหตุผลของระดับที่เลือก



รูปที่ 2 กรอบการประเมินผลกระทบและความเสี่ยงเพื่อกำหนดระดับมาตรการรักษาความมั่นคงปลอดภัยของระบบ CCTV

2.1.5 การแบ่งบทบาทหน้าที่

การรักษาความมั่นคงปลอดภัยสำหรับระบบ CCTV ไม่ใช่หน้าที่ของผู้ติดตั้ง/ผู้รวมระบบหรือเจ้าของระบบ/องค์กรผู้ใช้งานฝ่ายใดฝ่ายหนึ่ง แต่เป็นความรับผิดชอบร่วมกัน แต่ละฝ่ายควรทำความเข้าใจและแบ่งขอบเขตหน้าที่ความรับผิดชอบอย่างชัดเจนเพื่อให้ครอบคลุมการรักษาความมั่นคงปลอดภัยอย่างรอบด้าน

การกำหนดระดับความสำคัญเป็นความรับผิดชอบของเจ้าของระบบหรือองค์กรผู้ใช้งาน เนื่องจากเป็นผู้ทราบวัตถุประสงค์ ผลกระทบ และข้อกำหนดที่เกี่ยวข้อง ส่วนผู้ติดตั้งหรือผู้รวมระบบมีหน้าที่สนับสนุนข้อมูลทางเทคนิคและนำผลการประเมินไปใช้ในการออกแบบและกำหนดมาตรการ

แนวทางการแบ่งหน้าที่และความรับผิดชอบ ดังนี้

ผู้ติดตั้ง/ผู้รวมระบบ

1. ขอข้อมูลวัตถุประสงค์ ระดับความสำคัญ และข้อกำหนดก่อนออกแบบ
2. แปลงผลการประเมินเป็นข้อกำหนดทางเทคนิค
3. สำรวจพื้นที่ ออกแบบ ติดตั้ง และตั้งค่าให้สอดคล้องกับระดับที่กำหนด
4. แจ้งข้อจำกัดทางเทคนิคและความเสี่ยงที่พบ
5. เสนอแนวทางทางเทคนิคที่ช่วยเพิ่มความมั่นคงปลอดภัย
6. ทดสอบและประเมินผลว่าระบบที่ติดตั้งเป็นไปตามข้อกำหนดหรือไม่
7. ส่งมอบข้อมูลและหลักฐานที่จำเป็นต่อการบริหารระบบ
8. ดำเนินการเปลี่ยนแปลง ลบ คืน หรือทำลายข้อมูลตามที่ได้รับอนุมัติ
9. แจ้งสถานะ EoL/EoS และข้อจำกัดของระบบ

เจ้าของระบบ/องค์กรผู้ใช้งาน

1. กำหนดวัตถุประสงค์และบริบทของระบบ
2. ประเมินผลกระทบและกำหนดระดับ B/E/H
3. ระบุข้อกำหนดทางกฎหมาย สัญญา และข้อกำหนดเฉพาะ
4. ระบุพื้นที่ที่ต้องเฝ้าระวัง พื้นที่อ่อนไหว และพื้นที่ที่ไม่ควรบันทึก
5. กำหนดและอนุมัติระยะเวลาการเก็บรักษาข้อมูล
6. พิจารณาและอนุมัติความเสี่ยงที่ยอมรับได้
7. ร่วมทดสอบและประเมินระบบที่ติดตั้งว่าเป็นไปตามข้อกำหนดหรือไม่
8. กำหนดผู้รับผิดชอบการอัปเดต การทบทวนสิทธิ การตรวจสอบ Log และการเฝ้าระวัง
9. กำหนดแนวทางสำรอง กู้คืน และรับมือเหตุ
10. ทบทวนระดับเมื่อระบบหรือบริบทเปลี่ยนแปลง
11. อนุมัติการเปลี่ยนแปลงและการเลิกใช้งาน
12. วางแผนงบประมาณบำรุงรักษาและทดแทน

องค์กรขนาดเล็กอาจให้บุคคลหนึ่งปฏิบัติหลายบทบาทได้ แต่ควรสามารถระบุได้ว่า ใครกำหนด ใครอนุมัติ ใครดำเนินการ ใครตรวจสอบ และใครรับผิดชอบเมื่อเกิดเหตุ

ในแต่ละกิจกรรมที่ต้องมีการดำเนินการร่วมกันทั้งฝั่งผู้ติดตั้ง/ผู้รวมระบบและฝั่งเจ้าของระบบ/องค์กรผู้ใช้งาน ควรมีการตกลงแบ่งหน้าที่และความรับผิดชอบให้ชัดเจน เพื่อให้แต่ละฝ่ายดำเนินการตามขอบเขตหน้าที่ความรับผิดชอบได้ครบถ้วนตามข้อกำหนดและไม่ดำเนินการทับซ้อนกัน

2.2 กรอบแนวทาง มาตรฐานอ้างอิง และกฎหมายที่เกี่ยวข้อง

2.2.1 มาตรฐานและกรอบอ้างอิงหลัก

เอกสารฉบับนี้ได้ศึกษาและสังเคราะห์ข้อมูลจากมาตรฐานและกรอบอ้างอิงหลักดังต่อไปนี้

กลุ่มมาตรฐาน	มาตรฐาน/กรอบอ้างอิง	การประยุกต์ใช้กับระบบ CCTV
ระบบเฝ้าระวังด้วยวิดีโอ	IEC 62676 series และข้อเสนอแนะ ITU-T ที่เกี่ยวข้อง	สถาปัตยกรรม การออกแบบ สมรรถนะ คุณภาพของภาพ การติดตั้ง และการทดสอบตรวจรับ
ความมั่นคงปลอดภัยสารสนเทศ	ISO/IEC 27001, ISO/IEC 27002	การบริหารสินทรัพย์ การควบคุมการเข้าถึง การตั้งค่าเครือข่าย บันทึกเหตุการณ์ เหตุการณ์ ผู้ให้บริการ และความต่อเนื่อง
OT/ICS และ Product Security	IEC 62443 series รวมถึง IEC 62443-4-1 ตามความเกี่ยวข้อง	การแบ่งโซนและการสื่อสารระหว่างโซน การจำกัดการเชื่อมต่อ การป้องกันเชิงลึก และกระบวนการพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย
ความเป็นส่วนตัว	ISO/IEC 27701	กรอบสนับสนุนการบริหารข้อมูลส่วนบุคคลและความเป็นส่วนตัวร่วมกับกฎหมายของประเทศไทย
ผู้ให้บริการและห่วงโซ่อุปทาน	ISO/IEC 27036 series	การบริหารผู้ส่งมอบ ผู้รับจ้าง และความเสี่ยงจากห่วงโซ่อุปทาน
การบริหารช่องโหว่	ISO/IEC 29147, ISO/IEC 30111	การเปิดเผยช่องโหว่ การรับและวิเคราะห์ช่องโหว่ การประสานงานแก้ไข และการสื่อสาร
บริการคลาวด์	ISO/IEC 27017, ISO/IEC 27018	มาตรการและความรับผิดชอบด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลสำหรับบริการคลาวด์

มาตรฐานดังกล่าวใช้เป็นกรอบสนับสนุนการกำหนดหลักการ มาตรการ การทดสอบ และการสร้างความเชื่อมั่น มิได้หมายความว่าทุกระบบต้องใช้ทุกมาตรฐาน หรือทุกผลิตภัณฑ์และผู้ให้บริการต้องได้รับการรับรองตามมาตรฐานทั้งหมด

การได้รับใบรับรองหรือผ่านการประเมินตามมาตรฐานใดมาตรฐานหนึ่งควรถือเป็น หลักฐานประกอบการสร้างความเชื่อมั่น มิใช่หลักฐานเพียงอย่างเดียวในการสรุปว่าระบบมีความมั่นคงปลอดภัยเพียงพอสำหรับทุกบริบท

2.2.2 กฎหมายและข้อกำหนดของประเทศไทยที่เกี่ยวข้อง

กฎหมายและข้อกำหนดหลักของประเทศไทยที่เกี่ยวข้องที่ผู้อ่านควรพิจารณา มีดังต่อไปนี้

กฎหมายหรือข้อกำหนด	ประเด็นที่ควรพิจารณา
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และข้อกำหนดที่เกี่ยวข้อง	หน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรหรือระบบที่อยู่ภายใต้ขอบเขตของกฎหมาย ทั้งนี้ ระดับ B/E/H ในแนวปฏิบัตินี้ไม่ใช่การจำแนก CII
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง	วัตถุประสงค์และฐานในการประมวลผล การแจ้งรายละเอียด การใช้และเปิดเผย ระยะเวลาเก็บรักษา ความมั่นคงปลอดภัย สิทธิของเจ้าของข้อมูล เหตุละเมิด ผู้ประมวลผลข้อมูล และการส่งหรือโอนข้อมูลตามความเกี่ยวข้อง
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติมและข้อกำหนดที่เกี่ยวข้อง	หน้าที่เกี่ยวกับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ตามบทบาทและลักษณะของระบบ โดยไม่ควรสรุปว่าระบบ CCTV ทุกระบบมีหน้าที่เก็บ Log ในรูปแบบหรือระยะเวลาเดียวกัน
กฎหมายหรือข้อกำหนดสำหรับหน่วยงานของรัฐ	ข้อกำหนดด้านข้อมูล ระบบดิจิทัล คลาวด์ การจัดซื้อจัดจ้าง หรือข้อกำหนดเฉพาะของหน่วยงานตามความเกี่ยวข้อง
ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567	ใช้พิจารณาเมื่อองค์กรหรือระบบอยู่ในขอบเขตการใช้บังคับของประกาศ โดยครอบคลุมการกำกับดูแล การบริหารความเสี่ยง บทบาทและความรับผิดชอบของผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ มาตรการด้านความมั่นคงปลอดภัย การประเมินผู้ให้บริการ และข้อกำหนดอื่นที่เกี่ยวข้องกับการใช้บริการคลาวด์ ทั้งนี้ ประกาศมีผลบังคับใช้ตั้งแต่วันที่ 10 กันยายน 2569
ข้อกำหนดเฉพาะภาคส่วน	ข้อกำหนดของหน่วยงานกำกับดูแลสำหรับภาคการเงิน พลังงาน โทรคมนาคม สาธารณสุข การขนส่ง หรือภาคส่วนอื่น
สัญญาและข้อกำหนดการจัดซื้อจัดจ้าง	SLA ความพร้อมใช้งาน การสำรองและกู้คืน การเก็บบันทึก การเข้ารหัส การบริหารช่องโหว่ การแจ้งเหตุ การคืนหรือลบข้อมูล และการสิ้นสุดบริการ

รายการกฎหมายและข้อกำหนดที่นำเสนอข้างต้นเป็นเพียงส่วนหนึ่งของรายการกฎหมายและข้อกำหนดที่เกี่ยวข้อง อาจไม่ครอบคลุมข้อกำหนดที่เกี่ยวข้องทั้งหมดสำหรับทุกองค์กร แต่ละองค์กรควรระบุและทบทวนข้อกำหนดที่เกี่ยวข้องกับบริบทของตนอย่างเป็นระบบ

การนำแนวทางในหัวข้อนี้ไปประยุกต์ใช้ควรพิจารณาลักษณะและวัตถุประสงค์ของการใช้งาน CCTV รวมถึงกฎหมายและข้อกำหนดที่เกี่ยวข้อง ในกรณีที่บุคคลใช้ CCTV เพื่อประโยชน์ส่วนตนหรือกิจกรรมในครอบครัวเท่านั้น ให้พิจารณาขอบเขตและข้อยกเว้นตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม หากลักษณะหรือวัตถุประสงค์ของการใช้งานอยู่นอกขอบเขตดังกล่าว หรือเป็นการใช้งานเพื่อการประกอบธุรกิจ การดำเนินงานขององค์กร หรือวัตถุประสงค์อื่น ผู้ใช้งานควรพิจารณาหน้าที่ตามกฎหมายและข้อกำหนดที่เกี่ยวข้องเพิ่มเติม

2.3 การปกป้องคุ้มครองข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

การนำแนวทางในหัวข้อนี้ไปใช้ควรเริ่มจากการพิจารณาลักษณะและวัตถุประสงค์ของการใช้งาน CCTV ในกรณีที่บุคคลติดตั้งและใช้ CCTV เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น เช่น การดูแลความปลอดภัยในชีวิตและทรัพย์สินภายในบ้านพักอาศัย การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลดังกล่าวอยู่ในข้อยกเว้นตามมาตรา 4 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อย่างไรก็ดี ข้อยกเว้นดังกล่าวมิได้หมายความว่าผู้ใช้งานสามารถนำภาพไปใช้หรือเผยแพร่ได้โดยไม่มีข้อจำกัด การเผยแพร่ภาพที่กระทบสิทธิ ความเป็นส่วนตัว หรือชื่อเสียงของบุคคลอื่นอาจขัดต่อกฎหมายอื่นที่เกี่ยวข้อง ผู้ใช้งานจึงควรกำหนดมุมกล้องเท่าที่จำเป็น หลีกเลี่ยงการบันทึกพื้นที่ส่วนตัวของบุคคลอื่น

หากเป็นการใช้งานเพื่อการประกอบธุรกิจ การดำเนินงานขององค์กร หรือวัตถุประสงค์อื่นที่อยู่นอกขอบเขตข้างต้น ผู้ใช้งานควรพิจารณาหน้าที่ตามกฎหมายและแนวทางตามที่แสดงในหัวข้อนี้

สำหรับองค์กรในหลายกรณีการใช้งาน ระบบ CCTV อาจมีการเก็บรวบรวมและประมวลผลข้อมูลเกี่ยวกับบุคคลจำนวนมาก องค์กรจึงควรพิจารณาการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่การกำหนดวัตถุประสงค์ การวางตำแหน่งกล้อง ระยะเวลาเก็บรักษา การควบคุมการเข้าถึง การเปิดเผย การส่งออก จนถึงการลบหรือทำลายข้อมูล ซึ่งการคุ้มครองข้อมูลส่วนบุคคลไม่ได้มีเฉพาะในด้านการรักษาความลับหรือการปกป้องคุ้มครองข้อมูลส่วนบุคคลเท่านั้น ยังต้องคำนึงถึงความถูกต้องครบถ้วนสมบูรณ์ และความพร้อมใช้งานด้วย

มาตรการด้านการปกป้องคุ้มครองข้อมูลส่วนบุคคลควรใช้หลักความเป็นส่วนตัวตั้งแต่การออกแบบ (Privacy by Design) และการใช้ข้อมูลเท่าที่จำเป็น (Data Minimization) ร่วมกับข้อกำหนดตามกฎหมายที่เกี่ยวข้อง เนื้อหาในหัวข้อนี้สำหรับระบบ CCTV ที่มีการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง **แนวทางและคำแนะนำในหัวข้อนี้นำเสนอเพื่อเป็นแนวทางให้กับผู้อ่านเบื้องต้นเท่านั้น อาจไม่ครอบคลุมทุกข้อกำหนดตามที่ระบุในกฎหมาย ผู้อ่านควรศึกษารายละเอียดเพิ่มเติมจากกฎหมายที่เกี่ยวข้อง**

2.3.1 การกำหนดวัตถุประสงค์ ความจำเป็น และฐานทางกฎหมาย

ก่อนติดตั้งระบบ CCTV หรือเปลี่ยนแปลงลักษณะการใช้งาน องค์กรควรกำหนดวัตถุประสงค์ของการประมวลผลให้ชัดเจน และพิจารณาว่าการใช้ CCTV มีความจำเป็นและได้สัดส่วนกับวัตถุประสงค์ดังกล่าว

หรือไม่ วัตถุประสงค์อาจรวมถึง การรักษาความปลอดภัยของบุคคลและทรัพย์สิน การควบคุมการเข้าออก การตรวจสอบเหตุการณ์ การสนับสนุนการสอบสวน หรือการรักษาความปลอดภัยในการปฏิบัติงาน ทั้งนี้ องค์กรควรพิจารณาฐานทางกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบทบาทและลักษณะการประมวลผลของตน การพิจารณาควรดำเนินตามลำดับ ดังนี้

วัตถุประสงค์ ⟶ ความจำเป็นในการใช้ CCTV ⟶ พื้นที่ที่จำเป็นต้องบันทึก ⟶ ข้อมูลที่จำเป็น ⟶ ระยะเวลาที่จำเป็นต้องเก็บรักษา ⟶ ผู้ที่จำเป็นต้องเข้าถึง

ไม่ควรติดตั้งกล้องหรือเก็บรวบรวมข้อมูลเพียงเพราะเทคโนโลยีสามารถดำเนินการได้ และไม่ควรขยายขอบเขตการใช้งานเกินกว่าวัตถุประสงค์โดยไม่มีเหตุผลที่เหมาะสม

หากมีการเปลี่ยนแปลงวัตถุประสงค์อย่างมีนัยสำคัญ ควรทบทวนความชอบด้วยกฎหมาย ความจำเป็น ความได้สัดส่วน ผลกระทบต่อความเป็นส่วนตัว และความเสี่ยงก่อนนำการใช้งานใหม่ไปปฏิบัติ

2.3.2 ป้ายแจ้งและประกาศความเป็นส่วนตัว

องค์กรควรจัดให้มีการแจ้งข้อมูลเกี่ยวกับการใช้ CCTV ตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง โดยอาจใช้การแจ้งข้อมูลเป็นลำดับชั้น (Layered Notice) เพื่อให้บุคคลสามารถรับทราบข้อมูลสำคัญได้โดยง่าย และมีช่องทางสำหรับศึกษารายละเอียดเพิ่มเติม

ตัวอย่างการแจ้งข้อมูล สามารถแจ้งข้อมูลผ่านป้ายแจ้ง (CCTV Notice) โดยข้อมูลในป้ายแจ้งเบื้องต้นอาจประกอบด้วย

- การแจ้งว่าพื้นที่มีการใช้ CCTV
- วัตถุประสงค์หลักของการใช้ CCTV
- ชื่อหรือข้อมูลระบุตัวผู้รับผิดชอบหรือองค์กร
- ช่องทางสำหรับศึกษารายละเอียดเพิ่มเติม

ประกาศความเป็นส่วนตัวฉบับรายละเอียดอาจครอบคลุมวัตถุประสงค์ ฐานในการประมวลผล ประเภทข้อมูล ระยะเวลาการเก็บรักษา การเปิดเผยหรือผู้รับข้อมูล ผู้ให้บริการที่เกี่ยวข้อง สิทธิของเจ้าของข้อมูล และช่องทางติดต่อ ตามที่กฎหมายและบริบทกำหนด

การมีป้ายแจ้ง **ไม่ควรถูกตีความว่าเป็นขอและได้รับความยินยอมโดยอัตโนมัติ** และไม่ได้ทำให้องค์กรสามารถนำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นได้โดยไม่ต้องพิจารณาความชอบด้วยกฎหมายและข้อกำหนดที่เกี่ยวข้องเพิ่มเติม

2.3.3 การใช้สิทธิของเจ้าของข้อมูลและการเปิดเผยข้อมูลแก่บุคคลภายนอก

องค์กรควรกำหนดกระบวนการรับ พิจารณา และดำเนินการเกี่ยวกับคำขอของเจ้าของข้อมูลที่เกี่ยวข้องกับข้อมูลจากระบบ CCTV ให้สอดคล้องกับกฎหมายและบทบาทขององค์กร

กระบวนการควรพิจารณาอย่างน้อยถึง

- ผู้มีอำนาจรับเรื่อง พิจารณา และอนุมัติ
- วิธีการยืนยันตัวบุคคลของผู้ยื่นคำขอ
- วิธีการค้นหาและระบุข้อมูลที่เกี่ยวข้อง
- สิทธิและข้อมูลของบุคคลอื่นที่ปรากฏในภาพ
- การปิดบังหรือจำกัดการเปิดเผยข้อมูลของบุคคลอื่นเมื่อจำเป็น
- วิธีการส่งมอบข้อมูลอย่างมั่นคงปลอดภัย
- การบันทึกหลักฐานการพิจารณาและดำเนินการ

การเปิดเผยข้อมูลแก่ตำรวจ หน่วยงานของรัฐ คู่สัญญา บริษัทประกัน หรือบุคคลภายนอกอื่น ควรได้รับการพิจารณาตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง และควรมีหลักฐานที่สามารถตรวจสอบได้ถึงเหตุผลผู้อนุมัติ ขอบเขตข้อมูล และวิธีการเปิดเผยตามความเหมาะสม

2.3.4 การจัดการเหตุละเมิดข้อมูลส่วนบุคคล

องค์กรควรเชื่อมโยงกระบวนการจัดการเหตุละเมิดข้อมูลส่วนบุคคลเข้ากับกระบวนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ CCTV

เหตุการณ์ที่ควรได้รับการประเมิน เช่น

- บุคคลที่ไม่ได้รับอนุญาตสามารถดูหรือเข้าถึงข้อมูลได้
- ภาพหรือวิดีโอถูกส่งออก เปิดเผย หรือเผยแพร่โดยไม่ได้รับอนุญาต
- บัญชีผู้ใช้งานหรือบัญชีผู้ดูแลระบบถูกบุกรุก
- อุปกรณ์หรือสื่อบันทึกข้อมูลสูญหาย
- ข้อมูลถูกลบ เปลี่ยนแปลง หรือไม่สามารถเข้าถึงได้โดยไม่ได้รับอนุญาต
- ผู้ให้บริการภายนอกเกิดเหตุที่เกี่ยวข้องกับข้อมูล CCTV ขององค์กร

กระบวนการควรครอบคลุมขั้นตอนดังนี้

ตรวจพบ ⟶ จำกัดขอบเขตของเหตุ ⟶ ประเมินข้อมูลและผลกระทบ ⟶ เก็บรักษาหลักฐาน ⟶ แจ้งผู้รับผิดชอบ ⟶ ดำเนินการตามข้อกำหนดที่มีผลใช้บังคับ ⟶ แก้ไขและป้องกันการเกิดซ้ำ

องค์กรควรกำหนดบทบาท ช่องทางการรายงาน การยกระดับเหตุ การประเมินผลกระทบ และผู้มีอำนาจตัดสินใจให้ชัดเจน เพื่อให้สามารถดำเนินการภายในระยะเวลาที่กฎหมายหรือข้อกำหนดที่เกี่ยวข้องกำหนด

2.3.5 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

องค์กรควรพิจารณาความจำเป็นในการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) ตามหลักเกณฑ์และข้อกำหนดที่มีผลใช้บังคับที่เกี่ยวข้อง โดยเฉพาะกรณีที่ลักษณะการประมวลผลอาจมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล

การประเมินควรพิจารณาอย่างน้อยดังนี้

- วัตถุประสงค์และความจำเป็นของการใช้ CCTV
- ขอบเขตและพื้นที่การเฝ้าระวัง
- ประเภท ปริมาณ และความละเอียดอ่อนของข้อมูล
- จำนวนและลักษณะของบุคคลที่อาจได้รับผลกระทบ
- ระยะเวลาการเก็บรักษา
- การเชื่อมโยง เปิดเผย หรือส่งต่อข้อมูล
- ผู้ให้บริการหรือบุคคลภายนอกที่เกี่ยวข้อง
- ผลกระทบที่อาจเกิดขึ้นต่อบุคคล
- มาตรการป้องกันและลดความเสี่ยง

สำหรับระบบ CCTV ที่มีการใช้ AI การวิเคราะห์ขั้นสูง การระบุหรือยืนยันบุคคล หรือการประมวลผลข้อมูลชีวมิติ ควรพิจารณาความเสี่ยงและมาตรการเพิ่มเติมตาม แนวปฏิบัติด้านความมั่นคงปลอดภัยสำหรับระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์ของประเทศไทย (Thailand AI-Enabled CCTV Security Guidelines)

2.3.6 การแบ่งบทบาทหน้าที่

การกำหนดบทบาทด้านการคุ้มครองข้อมูลส่วนบุคคลควรสอดคล้องกับบทบาทตามกฎหมายและการดำเนินงานจริงขององค์กร โดยไม่ควรสรุปจากชื่อตำแหน่งหรือคู่สัญญาเพียงอย่างเดียว ตัวอย่างบทบาทและความรับผิดชอบหลักดังแสดงในตาราง

บทบาท	ความรับผิดชอบหลัก
เจ้าของระบบ/ผู้ควบคุมข้อมูลส่วนบุคคล	กำหนดวัตถุประสงค์ พิจารณาฐานทางกฎหมาย กำหนดระยะเวลาเก็บรักษา การเปิดเผย การดำเนินการเกี่ยวกับสิทธิ และการบริหารผู้ให้บริการ
ผู้ดูแลระบบ	ดำเนินการด้านบัญชีและสิทธิ บันทึกเหตุการณ์ การสำรอง การลบ และการดูแลระบบตามนโยบายและข้อกำหนดที่ได้รับอนุมัติ
ผู้ปฏิบัติงาน	ดู ใช้ ค้นหา หรือส่งออกข้อมูลเฉพาะตามสิทธิและวัตถุประสงค์ที่กำหนด
ผู้ติดตั้ง/ผู้รวมระบบ	ออกแบบและตั้งค่าระบบให้รองรับข้อกำหนดด้านความมั่นคงปลอดภัยและความเป็นส่วนตัว โดยไม่คงสิทธิหรือข้อมูลเกินความจำเป็นหลังส่งมอบ

บทบาท	ความรับผิดชอบหลัก
ผู้ประมวลผลข้อมูลส่วนบุคคล/ผู้ให้บริการภายนอก	ดำเนินการตามบทบาท คำสั่ง สัญญา และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)	ให้คำแนะนำและตรวจสอบการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบ CCTV ในกรณีที่องค์กรมีหน้าที่ต้องจัดให้มีตามมาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

2.4 การอบรมและสร้างความตระหนัก

การอบรมและสร้างความตระหนักควรสัมพันธ์กับบทบาท หน้าที่ และความเสี่ยงของผู้เกี่ยวข้อง โดยการอบรมควรจัดเนื้อหาให้เหมาะสมกับแต่ละกลุ่มผู้เรียน ตัวอย่างความรู้และความตระหนักที่แต่ละกลุ่มควรมีดังแสดงในตาราง

กลุ่มผู้เกี่ยวข้อง	ความรู้และความตระหนักที่ควรมี
เจ้าของระบบและผู้บริหาร	วัตถุประสงค์และความเสี่ยงของระบบ ข้อกำหนดที่เกี่ยวข้อง การกำหนดระดับความสำคัญ ความรับผิดชอบขององค์กร ความเสี่ยงจากผู้ให้บริการและบริการคลาวด์ และการยอมรับความเสี่ยง
ผู้ดูแลระบบ	การตั้งค่าอย่างมั่นคงปลอดภัย บัญชีและสิทธิ การพิสูจน์ตัวตน การเข้าถึงจากระยะไกล การแบ่งเครือข่าย การอัปเดตและบริหารช่องโหว่ บันทึกเหตุการณ์ การสำรองและกู้คืน และการตอบสนองต่อเหตุ
ผู้ปฏิบัติงาน	วัตถุประสงค์การใช้ CCTV ขอบเขตสิทธิ การดู ค้นหา และส่งออกข้อมูล การไม่ใช้บัญชีร่วมกัน การคุ้มครองข้อมูลส่วนบุคคล และการรายงานเหตุผิดปกติ
ผู้ติดตั้ง ผู้รับจ้างและผู้ให้บริการ	ข้อกำหนดด้านความมั่นคงปลอดภัย ค่าตั้งที่ได้รับอนุมัติ การควบคุมบัญชีชั่วคราวและการเข้าถึงจากระยะไกล การรักษาความลับ การจัดการข้อมูลระหว่างบำรุงรักษาและการคืนหรือเพิกถอนสิทธิเมื่อสิ้นสุดงาน

การอบรมหรือการสร้างความตระหนักควรดำเนินการเมื่อเริ่มปฏิบัติหน้าที่ เมื่อบทบาทหรือระบบมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เมื่อเกิดเหตุการณ์ที่มีบทเรียนสำคัญ และตามรอบที่องค์กรกำหนดโดยพิจารณาจากความเสี่ยง องค์กรสามารถใช้รูปแบบการอบรม การประชุม การสื่อสารภายใน คู่มือ หรือวิธีการอื่นที่เหมาะสม โดยควรสามารถแสดงได้ว่าบุคลากรที่เกี่ยวข้องได้รับข้อมูลและมีความรู้ที่จำเป็นต่อหน้าที่ของตน

สรุปหลักการของบทที่ 2

การกำกับดูแลระบบ CCTV ควรดำเนินการโดยอาศัยหลักการบริหารตามผลกระทบและความเสี่ยงร่วมกับการพิจารณากฎหมาย ข้อกำหนด และบริบทขององค์กร เพื่อให้สามารถกำหนดระดับความสำคัญและเลือกมาตรการด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวได้อย่างเหมาะสมและได้สัดส่วน

การกำหนดระดับความสำคัญของระบบและมาตรการที่ใช้ควรพิจารณาจากวัตถุประสงค์ของระบบ ความสำคัญต่อภารกิจ ลักษณะและผลกระทบของข้อมูล การเชื่อมต่อ และผลกระทบหากระบบถูกโจมตีหรือไม่สามารถให้บริการได้ โดยไม่ควรใช้ประเภทองค์กร จำนวนกล้อง รูปแบบบริการคลาวด์ หรือเทคโนโลยีใดเป็นปัจจัยเดียวในการกำหนดระดับ ทั้งนี้ องค์กรยังจำเป็นต้องปฏิบัติตามกฎหมายหรือข้อกำหนดเฉพาะที่เกี่ยวข้องกับองค์กร ข้อมูลในเอกสารฉบับนี้เป็นเพียงข้อเสนอแนะเท่านั้น

บทที่ 3 ค่าตั้งต้นด้านความมั่นคงปลอดภัยตลอดวงจรชีวิตระบบ

บทนี้นำเสนอค่าตั้งต้นและแนวปฏิบัติด้านความมั่นคงปลอดภัยสำหรับระบบ CCTV ตลอดวงจรชีวิตของระบบ ตั้งแต่การกำหนดความต้องการ การออกแบบและเลือกอุปกรณ์ การติดตั้งและตั้งค่าระบบ การทดสอบและตรวจรับ การใช้งานและควบคุมการเข้าถึง การบำรุงรักษาและเฝ้าระวัง การจัดการช่องโหว่และเหตุการณ์ด้านความมั่นคงปลอดภัย การประเมินและยกระดับระบบเดิม ตลอดจนการเลิกใช้อุปกรณ์และการจัดการข้อมูลอย่างเหมาะสม

สำหรับระบบที่ติดตั้งใช้งานอยู่แล้ว องค์กรไม่จำเป็นต้องเปลี่ยนระบบทั้งหมดในคราวเดียว แต่ควรประเมินสภาพและความเสี่ยงของระบบเดิม ระบุช่องว่าง จัดลำดับความสำคัญ และพิจารณาการปรับตั้งค่า การเพิ่มมาตรการชดเชย การปรับปรุงองค์ประกอบบางส่วน หรือการวางแผนทดแทนระบบตามระดับความเสี่ยงและความเหมาะสม

รูปที่ 3 วงจรชีวิตความมั่นคงปลอดภัยของระบบ CCTV (CCTV Security Lifecycle)

3.1 เริ่มต้นอย่างมั่นคงปลอดภัยใน 7 ข้อ

มาตรการในหัวข้อนี้เป็นแนวทางเริ่มต้น (Quick Start) สำหรับองค์กรที่ต้องการลดความเสี่ยงสำคัญของระบบ CCTV หรือยังไม่สามารถดำเนินมาตรการทั้งหมดในบทนี้ได้ในคราวเดียว ทั้งนี้ การดำเนินการตาม Quick Start มิได้ใช้ทดแทนการประเมินความเสี่ยงหรือมาตรการอื่นที่เกี่ยวข้อง โดยเฉพาะสำหรับระบบที่มีความสำคัญระดับ E และ H

สิ่งที่ต้องดำเนินการ	ผู้รับผิดชอบหลัก	B	E	H
1. จัดการข้อมูลยืนยันตัวตนเริ่มต้น (Default Credentials) ของกล้อง เครื่องบันทึก ระบบบริหารจัดการ แอปพลิเคชัน และองค์ประกอบอื่นก่อนเปิดใช้งาน	ทั้งสองฝ่าย	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
2. ไม่เปิดกล้อง เครื่องบันทึก หรือส่วนบริหารจัดการให้เข้าถึงจากอินเทอร์เน็ตโดยตรงโดยไม่จำเป็น และใช้ช่องทางการเข้าถึงที่ได้รับอนุมัติ	ผู้ติดตั้ง/ผู้ดูแลระบบ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
3. ใช้การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับบัญชีสิทธิสูงและการเข้าถึงจากระยะไกล เมื่อระบบรองรับ	ผู้ใช้งาน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
4. มีกระบวนการติดตาม ประเมิน และติดตั้งการปรับปรุงด้านความมั่นคงปลอดภัย (Security Update) และเฟิร์มแวร์อย่างเหมาะสม	ทั้งสองฝ่าย	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
5. กำหนดวัตถุประสงค์การใช้ CCTV และดำเนินมาตรการด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล	ผู้ใช้งาน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
6. กำหนดระยะเวลาเก็บรักษาข้อมูล และจัดให้มีการลบ ทำลาย หรือเขียนทับเมื่อครบกำหนด เว้นแต่มีเหตุอันชอบธรรมให้เก็บรักษาต่อ	ผู้ใช้งาน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
7. กำหนดผู้รับผิดชอบระบบ ช่องทางรายงานเหตุ และผู้มีอำนาจตัดสินใจเมื่อเกิดเหตุการณ์ผิดปกติ	ผู้ใช้งาน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

หมายเหตุ สำหรับระบบภายในบ้านและกิจการขนาดเล็กและระบบที่ผู้ใช้งานไม่มีบุคลากรด้านเทคนิค ผู้ติดตั้งหรือผู้ให้บริการควรดำเนินการตั้งค่าด้านความมั่นคงปลอดภัยที่จำเป็นก่อนส่งมอบ เช่น การเปลี่ยน

ข้อมูลยืนยันตัวตนเริ่มต้น การจำกัดการเข้าถึงจากอินเทอร์เน็ต การเปิดใช้การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เมื่อระบบรองรับ และการตั้งค่าการปรับปรุงด้านความมั่นคงปลอดภัย โดยควรส่งมอบสิทธิ บัญชี และข้อมูลที่จำเป็นต่อการบริหารจัดการระบบให้แก่เจ้าของระบบอย่างเหมาะสม

สิ่งที่ต้องเน้นย้ำ ผลิตภัณฑ์ไม่ควรใช้ข้อมูลยืนยันตัวตนเริ่มต้นแบบเดียวกันกับอุปกรณ์จำนวนมากซึ่งเป็นการเพิ่มความเสี่ยงและผลกระทบในกรณีที่ข้อมูลยืนยันตัวตนเริ่มต้นรั่วไหลหรือถูกละเมิด โดยอาจใช้ข้อมูลยืนยันตัวตนเฉพาะอุปกรณ์ การกำหนดให้ผู้ใช้งานตั้งข้อมูลยืนยันตัวตนเมื่อเริ่มใช้งาน หรือกลไกอื่นที่ให้ผลด้านความมั่นคงปลอดภัยเทียบเท่า

3.2 การออกแบบและการเลือกอุปกรณ์

การออกแบบระบบ CCTV ควรเริ่มจากวัตถุประสงค์ ผลลัพธ์ที่ต้องการ และบริบทของพื้นที่ ก่อนพิจารณาจำนวนกล้อง ความละเอียด รุ่น หรือเทคโนโลยีของอุปกรณ์

การเลือกอุปกรณ์ที่มีคุณสมบัติสูงไม่สามารถชดเชยการกำหนดวัตถุประสงค์หรือตำแหน่งติดตั้งที่ไม่เหมาะสมได้ การออกแบบจึงควรพิจารณาร่วมกันทั้งความต้องการเชิงปฏิบัติการ คุณภาพของภาพ การปกป้องคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยไซเบอร์ ความมั่นคงปลอดภัยทางกายภาพ ความพร้อมใช้งาน ความสามารถในการบำรุงรักษา และความสามารถในการสนับสนุนระบบตลอดอายุการใช้งาน

3.2.1 การออกแบบ ตำแหน่ง และการวางกล้อง

ผู้ใช้งานควรกำหนดว่า ต้องการเห็นอะไร ที่ใด และเพื่อวัตถุประสงค์ใด ส่วนผู้ติดตั้งหรือผู้รวมระบบมีหน้าที่แปลงความต้องการดังกล่าวเป็นตำแหน่ง ความสูง มุมมอง เลนส์ สภาพแสง สถาปัตยกรรม และอุปกรณ์ที่เหมาะสม

ข้อบกพร่องของระบบ CCTV จำนวนหนึ่งเกิดจากการออกแบบหรือการวางตำแหน่งที่ไม่เหมาะสม เช่น ติดตั้งกล้องสูงเกินไปจนไม่สามารถเห็นรายละเอียดที่ต้องการ ติดตั้งย้อนแสง หรือครอบคลุมพื้นที่เกินความจำเป็น การกำหนด Point Operational Requirements (POR) และการสำรวจพื้นที่อย่างเหมาะสมจึงช่วยลดความเสี่ยงและต้นทุนในการแก้ไขภายหลัง

3.2.1.1 ลำดับขั้นการออกแบบที่แนะนำ

ขั้น	กิจกรรม	ผลลัพธ์ที่ต้องได้	ผู้รับผิดชอบหลัก
1	กำหนด POR	วัตถุประสงค์และระดับรายละเอียดของภาพที่ต้องการในแต่ละจุด	ผู้ใช้งาน โดยผู้ติดตั้งสนับสนุน
2	สำรวจพื้นที่จริง	ผังพื้นที่ ระยะ สภาพแสง สิ่งกีดขวาง พลังงาน และเส้นทางสื่อสาร	ผู้ติดตั้ง

ขั้น	กิจกรรม	ผลลัพธ์ที่ต้องได้	ผู้รับผิดชอบหลัก
3	ออกแบบตำแหน่ง มุมมอง และเลนส์	ผังตำแหน่งกล้องและพื้นที่ครอบคลุม (Field of View)	ผู้ติดตั้ง
4	ออกแบบเครือข่าย พื้นที่จัดเก็บ และมาตรการด้านความมั่นคงปลอดภัย	สถาปัตยกรรมระบบ เครือข่าย พื้นที่จัดเก็บ และข้อกำหนดด้านความมั่นคงปลอดภัย	ผู้ติดตั้ง
5	ทบทวนด้านการปกป้องและคุ้มครองข้อมูลส่วนบุคคลและข้อกำหนดที่เกี่ยวข้อง	จุดที่ต้องปรับมุม ปิดบัง จำกัด หรือใช้มาตรการเพิ่มเติม	ทั้งสองฝ่าย
6	ติดตั้ง ปรับตั้ง และทดสอบในสภาพแวดล้อมจริง	ผลทดสอบภาพและการทำงาน	ผู้ติดตั้ง
7	ตรวจรับและส่งมอบ	ผลการตรวจรับ เอกสาร As-built ค่าตั้ง และคู่มือที่จำเป็น	ทั้งสองฝ่าย

3.2.1.2 การกำหนดความต้องการเชิงปฏิบัติการรายจุด (Point Operational Requirements: POR)

ก่อนกำหนดประเภทหรือคุณสมบัติของกล้อง ควรกำหนด POR สำหรับแต่ละจุดติดตั้งอย่างน้อยในประเด็นดังต่อไปนี้

ประเด็น	คำถามที่ควรตอบ
วัตถุประสงค์	ต้องการใช้ภาพเพื่ออะไร เช่น ตรวจพบเหตุ สังเกต จดจำ หรือระบุตัวบุคคล
ระดับรายละเอียดของภาพ	ต้องการระดับ Detection, Observation, Recognition หรือ Identification หรือไม่
พื้นที่และระยะ	ต้องครอบคลุมพื้นที่กว้างเพียงใด และเป้าหมายอยู่ห่างจากกล้องประมาณเท่าใด
ช่วงเวลาการใช้งาน	ใช้ในเวลากลางวัน กลางคืน หรือทั้งสองช่วง
สภาพแสง	มีแสงย้อน แสงน้อย แสงจากยานพาหนะ หรือความแตกต่างของแสงสูงหรือไม่
รูปแบบการใช้งาน	ต้องใช้ภาพแบบเวลาจริง ภาพย้อนหลัง หรือทั้งสองแบบ

ประเด็น	คำถามที่ควรตอบ
ระยะเวลาเก็บรักษา	ต้องเก็บข้อมูลนานเท่าใดและมีเหตุผลใดรองรับ
ความเป็นส่วนตัว	มีพื้นที่ของบุคคลอื่นหรือพื้นที่ที่ไม่จำเป็นต้องบันทึกอยู่ในมุมกล้องหรือไม่
ความมั่นคงปลอดภัยทางกายภาพ	กล้องมีความเสี่ยงต่อการบดบัง หมุน ถอด ทำลาย หรือเข้าถึงปุ่ม Reset หรือไม่
ความพร้อมใช้งาน	หากกล้องจุดนี้ไม่ทำงานจะมีผลกระทบอย่างไร และต้องมีมาตรการสำรองหรือไม่

3.2.1.3 สิ่งที่ต้องคำนึงถึงก่อนกำหนดตำแหน่งกล้อง

สิ่งที่ต้องคำนึงก่อนกำหนดตำแหน่งกล้องมีดังต่อไปนี้

ประเด็น	สิ่งที่ต้องพิจารณา	ข้อผิดพลาดที่พบบ่อย
วัตถุประสงค์	POR และระดับ DORI	ใช้กล้องตัวเดียวให้ทั้งภาพรวมและรายละเอียดระดับ Identification
ความสูงและมุมก้ม	พื้นที่ครอบคลุม รายละเอียด ความเสี่ยงต่อการถูกทำลาย และการบำรุงรักษา	ติดตั้งสูงเกินไปจนไม่เห็นรายละเอียดที่ต้องการ
ระยะและเลนส์	Field of View และทางยาวโฟกัส	ใช้เลนส์มุมกว้างกับเป้าหมายที่อยู่ไกล
ทิศทางแสง	แสงย้อน ประตู กระจก หน้าต่าง	บุคคลหรือวัตถุกลายเป็นเงามืด
กลางคืน/IR	ระยะ IR และการสะท้อน	IR สะท้อนกลับจากผนังหรือกระจก
สิ่งกีดขวาง	ต้นไม้ ป้าย ประตู โครงสร้าง	ไม่พิจารณาการเปลี่ยนแปลงของพื้นที่
ความเป็นส่วนตัว	จำกัดมุมมองและใช้ Privacy Mask เมื่อเหมาะสม	บันทึกพื้นที่เกินความจำเป็น
ความมั่นคงปลอดภัยทางกายภาพ	การถอด หมุน Reset หรือทำลาย	ติดตั้งในจุดที่เข้าถึงได้ง่าย
พลังงานและสายสัญญาณ	PoE กำลังไฟ ระยะสาย และความต่อเนื่อง	กำลังไฟไม่เพียงพอในสภาพใช้งานจริง
สภาพแวดล้อม	IP/IK อุณหภูมิ ความชื้น ฝุ่น ไอเค็ม	ใช้อุปกรณ์ไม่เหมาะกับพื้นที่

ประเด็น	สิ่งที่ต้องพิจารณา	ข้อผิดพลาดที่พบบ่อย
การบำรุงรักษา	ความสามารถในการเข้าถึงอย่างปลอดภัย	ติดตั้งในตำแหน่งที่บำรุงรักษายาก
ความซ้ำซ้อน	จุดสำคัญอาจต้องมีมุมมองซ้อนทับหรือวิธีสำรอง	พึ่งพากล้องตัวเดียวในจุดวิกฤต

3.2.1.4 ความสูงติดตั้งและมุมก้ม

ความสูงในการติดตั้งและมุมก้มของกล้องควรกำหนดโดยพิจารณาจากผลลัพธ์ของภาพที่ต้องการและข้อจำกัดของพื้นที่ มากกว่ากำหนดจากค่าความสูงมาตรฐานเพียงค่าเดียว โดยควรพิจารณาร่วมกับข้อกำหนดเชิงปฏิบัติการของจุดติดตั้ง (Point Operational Requirements: POR) ระดับรายละเอียดของภาพตาม DORI ความหนาแน่นของพิกเซลบนเป้าหมาย (Pixel Density) ระยะห่าง พื้นที่ครอบคลุม สภาพแสง ความเสี่ยงจากการถูกทำลาย และความสามารถในการเข้าถึงเพื่อบำรุงรักษา

การติดตั้งกล้องในตำแหน่งที่สูงขึ้นอาจช่วยลดความเสี่ยงจากการถูกแตะต้องหรือทำลาย แต่หากสูงหรือมีมุมก้มมากเกินไป อาจทำให้ได้ภาพส่วนบนของศีรษะมากกว่ารายละเอียดของใบหน้าหรือวัตถุที่ต้องการในทางกลับกัน การติดตั้งในระดับต่ำอาจให้รายละเอียดของภาพดีขึ้น แต่เพิ่มความเสี่ยงจากการถูกบดบัง เคลื่อนย้าย หรือทำลาย

ดังนั้น ค่าความสูงและมุมในตารางต่อไปนี้ควรใช้เป็น แนวทางอ้างอิงเชิงปฏิบัติ มิใช่ข้อกำหนดตายตัว และควรยืนยันผลจากภาพจริง ณ ตำแหน่งติดตั้ง

ตำแหน่งหรือภารกิจ	แนวทางด้านความสูงและมุมมอง	ข้อพิจารณา
ทางเข้า–ออกบุคคล	ให้มุมกล้องสามารถเห็นใบหน้าหรือรายละเอียดที่จำเป็นตาม POR	หลีกเลี่ยงมุมก้มมากเกินไปและแสงย้อนจากประตูหรือกระจก
ทางเข้า–ออกยานพาหนะ	กำหนดระดับและมุมให้เหมาะกับวัตถุประสงค์ เช่น เห็นยานพาหนะ ลักษณะรถ หรือป้ายทะเบียน	พิจารณาความเร็วของรถ แสงจากไฟหน้า และสภาพกลางวัน/กลางคืน
ทางเดิน	ให้แนวภาพสัมพันธ์กับทิศทางการเคลื่อนที่ของบุคคล	หากมีการเข้าออกหลายทิศทาง อาจต้องใช้หลายมุม
ห้องหรือพื้นที่ทั่วไป	กำหนดมุมให้เห็นพื้นที่ตามวัตถุประสงค์โดยไม่เก็บภาพเกินความจำเป็น	ระวังจุดอับ สิ่งกีดขวาง และพื้นที่ที่มีความคาดหวังด้านความเป็นส่วนตัว

ตำแหน่งหรือภารกิจ	แนวทางด้านความสูงและมุมมอง	ข้อพิจารณา
พื้นที่เปิดหรือโถงสูง	อาจใช้กล้องภาพรวมร่วมกับกล้องเฉพาะจุด	ไม่ควรคาดหวังให้กล้องภาพรวมทำหน้าที่ระบุตัว หากความหนาแน่นของพิกเซลไม่เพียงพอ
จุดสำคัญหรือพื้นที่ความเสี่ยงสูง	กำหนดตำแหน่งและมุมจากระดับรายละเอียดของภาพที่ต้องการ และอาจพิจารณามุมมองซ้อนทับ	ควรลดการพึ่งพากล้องเพียงตัวเดียวเมื่อความล้มเหลวอาจมีผลกระทบสูง
พื้นที่เสี่ยงต่อการทำลายกล้อง	อาจติดตั้งในตำแหน่งที่เข้าถึงได้ยากขึ้นหรือใช้มาตรการป้องกันทางกายภาพเพิ่มเติม	ต้องไม่ทำให้คุณภาพของภาพลดลงจนไม่ตอบวัตถุประสงค์

ในการตรวจรับควรตรวจสอบ ภาพจริงในสภาพใช้งานจริง ทั้งกลางวัน กลางคืน หรือสภาวะสำคัญตาม POR แทนการยืนยันจากความสูงหรือมุมที่ระบุในแบบติดตั้งเพียงอย่างเดียว

3.2.1.5 การวางกล้องตามลักษณะห้องและพื้นที่

ตำแหน่งการวางกล้องในแต่ละพื้นที่มีความแตกต่างกัน ผู้อ่านสามารถใช้ข้อมูลในตารางด้านล่างเป็นแนวทางอ้างอิงในการวางกล้อง

ลักษณะพื้นที่	แนวทางการวางกล้อง	สิ่งที่ควรระวัง
ห้องขนาดเล็ก	พิจารณามุมที่ครอบคลุมทางเข้าและพื้นที่สำคัญ	การติดเหนือประตูอาจไม่เห็นใบหน้าผู้เข้าพื้นที่อย่างเหมาะสม
ห้องขนาดกลางหรือใหญ่	ใช้หลายมุมมองตามความจำเป็น	จุดอับจากเสา ผนัง หรือสิ่งติดตั้ง
ห้องโถงสูงหรือพื้นที่เปิด	ใช้กล้องภาพรวมร่วมกับกล้องเฉพาะจุด	ไม่ควรใช้ภาพรวมเพื่อ Identification หากรายละเอียดไม่เพียงพอ
ทางเดิน	วางตามแนวการเคลื่อนที่	หากเข้าออกหลายทิศทางอาจต้องใช้หลายมุม
บันได/ชานพัก	ให้เห็นแนวการเคลื่อนที่และทางเข้าออก	ต้องไม่กระทบความปลอดภัยของอาคาร

ลักษณะพื้นที่	แนวทางการวางกล้อง	สิ่งที่ควรระวัง
ห้องระบบ	ครอบคลุมทางเข้าออกและพื้นที่สำคัญ	ควรเชื่อมโยงกับการควบคุมการเข้าถึงทางกายภาพ
จุดรับชำระเงิน	เห็นบุคคลและบริบทที่จำเป็น	หลีกเลี่ยงการบันทึกข้อมูลลับเกินวัตถุประสงค์
ลานจอดรถ	ใช้ภาพรวมร่วมกับจุดเข้าออก	แสงไฟรถและสภาพกลางคืน
ทางเข้าอาคารที่มีกระจก	พิจารณา WDR และมุมกล้อง	แสงย้อนอาจทำให้รายละเอียดสูญหาย

3.2.1.6 การพิจารณาจุดติดตั้งตามลักษณะการใช้งาน

ลักษณะของสถานที่สามารถใช้เป็นข้อมูลเริ่มต้นในการสำรวจจุดที่อาจมีความสำคัญต่อการรักษาความปลอดภัย แต่ไม่ควรใช้ประเภทสถานที่เป็นเกณฑ์กำหนดตำแหน่ง จำนวน หรือระดับมาตรการของกล้องโดยอัตโนมัติ องค์กรควรกำหนดจุดติดตั้งจากวัตถุประสงค์ ความเสี่ยง ลักษณะการเคลื่อนที่ของบุคคลหรือทรัพย์สิน ผลกระทบหากไม่มีภาพ และความเป็นส่วนตัวของบุคคลในพื้นที่

ลักษณะการใช้งาน	จุดที่มักมีความสำคัญต่อการรักษาความปลอดภัย	จุดเพิ่มเติมที่อาจพิจารณาตามความเสี่ยง
อาคารสำนักงาน	ทางเข้า–ออกหลัก จุดติดต่อหรือพื้นที่สำคัญ	ทางเดิน ลิฟต์ พื้นที่จัดเก็บทรัพย์สิน ห้องระบบหรือพื้นที่จำกัดสิทธิ
ร้านค้า/พื้นที่ให้บริการ	ทางเข้า–ออก จุดชำระเงิน พื้นที่ทรัพย์สินสำคัญ	พื้นที่จัดเก็บสินค้า จุดรับ–ส่งสินค้า หรือพื้นที่เสี่ยงต่อเหตุการณ์
คลังสินค้า/โรงงาน	ทางเข้า–ออกบุคคลและยานพาหนะ จุดรับ–ส่งสินค้า พื้นที่ทรัพย์สินสำคัญ	แนวรั้ว จุดอับ พื้นที่กระบวนการสำคัญ หรือพื้นที่จำกัดสิทธิ
สถานศึกษา	ทางเข้า–ออก พื้นที่สาธารณะหรือพื้นที่ที่มีเหตุผลด้านความปลอดภัย	พื้นที่กิจกรรม ทางเดิน หรือจุดเสี่ยงตามผลการประเมิน โดยต้องให้ความสำคัญกับความเป็นส่วนตัวของเด็กและบุคลากร
สถานพยาบาล	ทางเข้า–ออก พื้นที่สาธารณะ จุดรักษาความปลอดภัย และพื้นที่ทรัพย์สินสำคัญ	ห้องระบบ พื้นที่จำกัดสิทธิ หรือจุดที่มีความเสี่ยง โดยต้องระมัดระวังพื้นที่รักษาและข้อมูลของผู้ป่วยเป็นพิเศษ

ลักษณะการใช้งาน	จุดที่มักมีความสำคัญต่อการรักษาความปลอดภัย	จุดเพิ่มเติมที่อาจพิจารณาตามความเสี่ยง
ศูนย์ข้อมูล/ห้องระบบ	ทางเข้า–ออก พื้นที่ควบคุมการเข้าถึง และทางเข้าอุปกรณ์สำคัญ	แนวทางเข้าถึง พื้นที่สนับสนุน หรือจุดที่ต้องใช้ตรวจสอบเหตุการณ์
ลานจอดรถ	ทางเข้า–ออก พื้นที่จอด และเส้นทางสัญจรหลัก	จุดอับ ทางเชื่อมอาคาร จุดชำระค่าบริการ หรือพื้นที่เสี่ยง
พื้นที่สาธารณะ	ทางเข้า–ออก เส้นทางสัญจร หรือจุดที่มีเหตุผลด้านความปลอดภัย	พื้นที่รวมกลุ่ม จุดอับ หรือพื้นที่ที่มีประวัติเหตุการณ์

ตารางดังกล่าวเป็นเพียง แนวทางเริ่มต้นในการสำรวจ มิใช่รายการบังคับว่าต้องติดตั้งกล้องทุกตำแหน่ง องค์กรควรหลีกเลี่ยงการติดตั้งที่เก็บภาพเกินวัตถุประสงค์หรือกระทบความเป็นส่วนตัวโดยไม่จำเป็น

3.2.1.7 พื้นที่ที่ไม่ควรติดตั้งหรือควรระมัดระวังเป็นพิเศษ

การใช้ CCTV ในพื้นที่ที่บุคคลมีความคาดหวังด้านความเป็นส่วนตัวสูงควรได้รับการพิจารณาอย่างรอบคอบ และควรหลีกเลี่ยงหากไม่มีความจำเป็นและเหตุผลที่เหมาะสม ควรพิจารณาอย่างน้อยถึงความจำเป็น วัตถุประสงค์ ความได้สัดส่วน ทางเลือกที่มีผลกระทบน้อยกว่า ฐานหรือข้อกำหนดทางกฎหมาย ขอบเขตของภาพ ระยะเวลาเก็บรักษา ผู้ที่สามารถเข้าถึง และมาตรการลดผลกระทบ

พื้นที่ที่ควรระมัดระวังเป็นพิเศษ เช่น ห้องน้ำ ห้องอาบน้ำ ห้องเปลี่ยนเสื้อผ้า พื้นที่รักษาหรือพักผู้ป่วย พื้นที่พักส่วนบุคคล พื้นที่ทำงานหรือพักผ่อนที่บุคลากรอยู่เป็นเวลานาน และพื้นที่ของบุคคลอื่นที่อยู่นอกขอบเขตความรับผิดชอบขององค์กร

การบันทึกเสียงเป็นการจัดเก็บและประมวลผลข้อมูลเพิ่มเติมจากการบันทึกภาพ จึงไม่ควรเปิดเป็นค่าตั้งต้นโดยไม่มีวัตถุประสงค์และการประเมินที่ชัดเจน หากมีความจำเป็นควรพิจารณาความชอบด้วยกฎหมาย ความจำเป็น ความได้สัดส่วน การแจ้งข้อมูล และมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติม

3.2.1.8 แสงสว่างและสภาพแวดล้อม

แสงสว่างและสภาพแวดล้อมส่งผลกระทบโดยตรงต่อการทำงานและข้อมูลที่เก็บบันทึกโดยกล้อง ควรมีการคำนึงถึงประเด็นดังต่อไปนี้

ประเด็น	แนวทางพิจารณา
ระดับแสง	มีแสงเพียงพอและสม่ำเสมอในพื้นที่เป้าหมาย
แสงย้อน	พิจารณา WDR หรือมาตรการทางแสงอื่นที่เหมาะสม

ประเด็น	แนวทางพิจารณา
การใช้งานกลางคืน	พิจารณา IR หรือไฟส่องสว่างเสริมตามระยะ
การสะท้อน IR	หลีกเลี่ยงการสะท้อนจากกระจก ผนัง หรือวัตถุใกล้กล้อง
ฝุ่นและน้ำ	เลือกระดับการป้องกัน IP ให้เหมาะกับพื้นที่
แรงกระแทก	พิจารณาระดับ IK ตามความเสี่ยง
อุณหภูมิและความชื้น	ตรวจสอบช่วงการทำงานของอุปกรณ์
การกัดกร่อน	พิจารณาวัสดุและตัวเรือนตามสภาพแวดล้อม
ไฟกระชาก/ฟ้าผ่า	พิจารณาการป้องกันไฟกระชากและการต่อลงดิน
การสั่นสะเทือน	หลีกเลี่ยงจุดติดตั้งที่ไม่มั่นคงหรือใช้มาตรการรองรับ

3.2.2 ความละเอียดและคุณภาพของภาพ

การเลือกกล้องไม่ควรพิจารณาจากจำนวนเมกะพิกเซล (Megapixel) เพียงอย่างเดียว เนื่องจากคุณภาพของภาพที่สามารถนำไปใช้ตามวัตถุประสงค์ขึ้นอยู่กับความหนาแน่นของพิกเซลบนเป้าหมาย ระยะ มุมมอง เลนส์ สภาพแสง การเคลื่อนไหว อัตราเฟรม การบีบอัด และการตั้งค่าของระบบ

แนวคิด DORI สามารถใช้เป็นกรอบอ้างอิงในการเชื่อมโยงวัตถุประสงค์กับระดับรายละเอียดของภาพตาม IEC 62676 series ที่เกี่ยวข้อง โดยมีคำอธิบายโดยย่อและตัวอย่างดังต่อไปนี้

ระดับ	ความหมายโดยสรุป	ตัวอย่างการใช้
Detection	ตรวจพบว่ามีบุคคลหรือวัตถุอยู่ในพื้นที่	ตรวจพบการปรากฏตัวหรือการเคลื่อนไหว
Observation	สังเกตรายละเอียดทั่วไปหรือกิจกรรม	ดูลักษณะ การแต่งกาย หรือพฤติกรรมโดยรวม
Recognition	มีรายละเอียดเพียงพอสำหรับจดจำบุคคลหรือวัตถุที่รู้จัก	จดจำบุคคลที่เคยพบ
Identification	มีรายละเอียดเหมาะสมกับการระบุตัวตามวัตถุประสงค์	จุดเข้าออกที่ต้องการรายละเอียดสูง

ความหนาแน่นของพิกเซล (Pixel Density) เป็นจำนวนพิกเซลที่ครอบคลุมเป้าหมายต่อหน่วยระยะในพื้นที่จริง ซึ่งมักแสดงเป็น พิกเซลต่อเมตร (Pixels per Meter: PPM) และสามารถใช้ประกอบการประเมินว่าภาพมีรายละเอียดเพียงพอต่อวัตถุประสงค์ตามระดับ DORI หรือไม่

ระดับ DORI	วัตถุประสงค์โดยสรุป	ค่าความหนาแน่นของพิกเซลอ้างอิง
Detection	ตรวจพบว่ามีบุคคลหรือวัตถุอยู่ในพื้นที่	ประมาณ ≥ 25 PPM
Observation	สังเกตลักษณะหรือกิจกรรมโดยรวม	ประมาณ ≥ 62 PPM
Recognition	มีรายละเอียดเพียงพอสำหรับจดจำบุคคลหรือวัตถุที่รู้จัก	ประมาณ ≥ 125 PPM
Identification	มีรายละเอียดในระดับที่เหมาะสมต่อการระบุตัวตามวัตถุประสงค์	ประมาณ ≥ 250 PPM

หมายเหตุ: แนวคิด DORI และค่าความหนาแน่นของพิกเซลในตารางข้างต้นเป็นกรอบอ้างอิงที่ใช้กันอย่างแพร่หลายสำหรับการสื่อสารความต้องการด้านรายละเอียดของภาพ และมีที่มาจากแนวทางใน IEC 62676-4 ฉบับก่อนหน้า ทั้งนี้ IEC 62676-4:2025 ได้ปรับปรุงแนวทางเกี่ยวกับขนาดวัตถุและความหนาแน่นของพิกเซลสำหรับระบบเฝ้าระวังด้วยวิดีโอ ดังนั้น หากโครงการกำหนดให้อ้างอิง IEC 62676-4:2025 ควรใช้เกณฑ์และวิธีการประเมินตามฉบับดังกล่าวเป็นหลัก

ไม่ว่าจะแสดงความต้องการด้วย DORI หรือเกณฑ์ตาม IEC 62676-4:2025 ควรมีการตรวจสอบผลลัพธ์ของภาพในสภาพใช้งานจริง โดยพิจารณาร่วมกับสภาพแสง มุมมอง เลนส์ การเคลื่อนไหว การบีบอัด อัตราเฟรม และวัตถุประสงค์ของแต่ละจุดติดตั้ง ตัวอย่างเช่น กล้องที่มีจำนวนพิกเซลสูงอาจยังไม่สามารถให้ภาพระดับ Identification ได้ หากพื้นที่ครอบคลุมกว้างเกินไป บุคคลอยู่ไกลจากกล้อง มีแสงย้อนรุนแรง หรือภาพเกิดการเบลอจากการเคลื่อนไหว ตัวอย่างปัจจัยและผลกระทบที่มีต่อภาพดังแสดงในตารางต่อไปนี้

ปัจจัย	ผลกระทบที่ควรพิจารณา
แสง	แสงไม่เพียงพอหรือแสงย้อนทำให้รายละเอียดสูญหาย
การเคลื่อนไหว	Shutter ไม่เหมาะสมทำให้เกิด Motion Blur
Focus	จำนวนพิกเซลเพียงพอแต่ Focus ไม่ถูกต้องยังไม่ตอบวัตถุประสงค์
Compression	การบีบอัดสูงอาจทำให้รายละเอียดสำคัญสูญหาย
Frame Rate	ต้องสัมพันธ์กับลักษณะการเคลื่อนที่ของเป้าหมาย
Dynamic Range	มีผลต่อฉากที่มีความต่างของแสงสูง

ปัจจัย	ผลกระทบที่ควรพิจารณา
Noise	สภาพแสงต่ำอาจทำให้รายละเอียดลดลง
Viewing Angle	มุมไม่เหมาะสมอาจไม่เห็นลักษณะที่ต้องการ
สภาพแวดล้อม	ฝน หมอก ฝุ่น หรือความชื้นอาจลดคุณภาพของภาพ

การทดสอบและตรวจรับระบบ CCTV ควรพิสูจน์ว่า **ภาพตอบ POR ในสภาพใช้งานจริง** ไม่ควรยืนยันเพียงว่ากล้องมี Resolution ตามข้อกำหนดของผลิตภัณฑ์

3.2.3 ระยะเวลาการเก็บรักษาและการลบข้อมูล

การกำหนดระยะเวลาเก็บรักษาควรพิจารณาจากวัตถุประสงค์ ความจำเป็น ความเสี่ยง ระยะเวลาที่องค์กรต้องใช้ในการตรวจพบและตรวจสอบเหตุ ตลอดจนกฎหมาย ข้อกำหนดเฉพาะภาคส่วน และสัญญาที่เกี่ยวข้อง ไม่ควรกำหนด Retention จากขนาดพื้นที่จัดเก็บที่มีอยู่ หรือเก็บข้อมูลให้นานที่สุดเพียงเพราะเทคโนโลยีสามารถรองรับได้

มาตรการ	B	E	H
กำหนด Retention Period และเหตุผลรองรับ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ตั้งค่าการลบ เขียนทับ หรือทำลายเมื่อครบกำหนด	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ตรวจสอบค่าที่ตั้งจริงกับนโยบาย	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
กำหนดระยะเวลาเก็บรักษาให้ครอบคลุมข้อมูลใน NVR/VMS อุปกรณ์ปลายทาง คลาวด์ ข้อมูลสำรอง และข้อมูลที่ส่งออก ตามความเกี่ยวข้อง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
แยกและป้องกันข้อมูลเหตุการณ์ที่ต้องเก็บเกินรอบปกติ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
มีกระบวนการระงับการลบชั่วคราว (Hold) พร้อมเหตุผลและผู้อนุมัติ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ทบทวน Retention เมื่อวัตถุประสงค์หรือข้อกำหนดเปลี่ยน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

3.2.4 การคำนวณขนาดพื้นที่จัดเก็บ

การคำนวณพื้นที่จัดเก็บควรดำเนินการก่อนจัดซื้อและตรวจสอบอีกครั้งหลังเปิดใช้งาน โดยปริมาณข้อมูลจริงขึ้นอยู่กับหลายปัจจัย เช่น Bitrate, Codec, Frame Rate, Scene Complexity, รูปแบบการบันทึก และ Metadata

3.2.4.1 สูตรประมาณการพื้นฐาน

พื้นที่ต่อกล้องต่อวัน (GB) ≈ Bitrate (Mbps) × 10.8

ดังนั้น

พื้นที่รวม (GB) ≈ Bitrate × 10.8 × จำนวนกล้อง × จำนวนวันที่เก็บ

ตัวอย่าง กล้อง 16 ตัว Bitrate เฉลี่ย 6 Mbps และ Retention 30 วัน

6 × 10.8 × 16 × 30 ≈ 31,104 GB หรือประมาณ 31 TB

ค่าดังกล่าวเป็นความจุข้อมูลโดยประมาณ ยังไม่รวม RAID, Hot Spare, File System Overhead, Reserved Capacity และพื้นที่สำรองอื่น

การกำหนดพื้นที่จัดเก็บจริงควรใช้ค่าจากการออกแบบและทดสอบระบบจริง และควรตรวจสอบหลังเปิดใช้งานว่า **ระยะเวลาที่สามารถเรียกดูภาพย้อนหลังได้จริงสอดคล้องกับระยะเวลาการเก็บรักษาที่องค์กรกำหนด**

3.2.4.2 ปัจจัยที่ต้องพิจารณาเพิ่มเติม

ตัวอย่างปัจจัยอื่น ๆ ที่มีผลต่อขนาดพื้นที่ในการเก็บข้อมูลดังแสดงในตารางต่อไปนี้

ปัจจัย	ผลต่อการคำนวณ
Resolution	ความละเอียดสูงขึ้นโดยทั่วไปเพิ่ม Bitrate
Frame Rate	อัตราเฟรมสูงขึ้นอาจเพิ่มข้อมูล
Codec	ประสิทธิภาพการบีบอัดแตกต่างกัน
CBR/VBR	ปริมาณข้อมูลจริงอาจต่างจากค่าประมาณ
Scene Complexity	ภาพที่มีการเคลื่อนไหวหรือรายละเอียดมากใช้ Bitrate สูงขึ้น
Recording Mode	Continuous และ Event Recording ให้ปริมาณข้อมูลต่างกัน
Audio/Metadata	เพิ่มพื้นที่จัดเก็บ
RAID/Redundancy	ทำให้ความจุใช้งานจริงต่ำกว่าความจุดิบ

ปัจจัย	ผลต่อการคำนวณ
Growth Margin	ควรเผื่อการขยายตามความเหมาะสม

3.2.4.3 ความพร้อมใช้งานและการบริหารพื้นที่จัดเก็บ

พื้นที่จัดเก็บของระบบ CCTV ต้องได้รับการบริหารให้สามารถเก็บและเรียกใช้ข้อมูลได้ตามวัตถุประสงค์ มิใช่พิจารณาเฉพาะความจุของดิสก์ในวันที่ติดตั้ง

องค์กรควรตรวจสอบทั้งความจุที่ใช้งานได้จริง สถานะอุปกรณ์จัดเก็บ การแจ้งเตือนเมื่อพื้นที่ใกล้เต็ม ความสามารถในการรองรับความเสียหายของอุปกรณ์ และระยะเวลาการเก็บภาพที่เกิดขึ้นจริง

มาตรการ	B	E	H
ใช้อุปกรณ์จัดเก็บที่เหมาะกับลักษณะการบันทึกต่อเนื่อง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ตรวจสอบพื้นที่ว่างและระยะเวลาการเก็บภาพจริง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
แจ้งเตือนเมื่อพื้นที่ใกล้เต็มหรืออุปกรณ์จัดเก็บมีความผิดปกติ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้กลไกเพิ่มความทนทานต่อความเสียหายของดิสก์ เช่น RAID ตามความเหมาะสม	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
รองรับการบันทึกที่อุปกรณ์ปลายทางเมื่อการเชื่อมต่อขัดข้อง (Edge Recording) หรือการเติมข้อมูลกลับอัตโนมัติเมื่อเครือข่ายกลับมา เช่น Automatic Network Replenishment (ANR) หรือกลไกเทียบเท่า	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
คำนวณแบนด์วิดท์เครือข่ายร่วมกับพื้นที่จัดเก็บ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
มีการสำรองข้อมูลหรือกลไกกู้คืนสำหรับข้อมูลหรือการตั้งค่าที่สำคัญตามผลการประเมินความเสี่ยง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
จัดทำและเก็บหลักฐานการคำนวณและการตรวจสอบระยะเวลาจัดเก็บจริง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

ข้อควรทราบ: การทำ RAID ช่วยเพิ่มความทนทานต่อความเสียหายของดิสก์บางกรณี แต่ **ไม่ถือเป็นการสำรองข้อมูล (Backup)** เนื่องจากไม่สามารถป้องกันความเสียหายทุกประเภท เช่น การลบข้อมูลโดยไม่ตั้งใจ การโจมตี การตั้งค่าผิดพลาด หรือความเสียหายที่เกิดกับระบบจัดเก็บทั้งชุด

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณาความต่อเนื่องของการบันทึก การกู้คืนข้อมูลและการตั้งค่า ตลอดจนความสามารถในการตรวจพบความผิดปกติของระบบจัดเก็บอย่างทันท่วงที

ข้อควรทราบ: พื้นที่จัดเก็บ “ภาพ” กับ “Log” เป็นคนละส่วนกัน ภาพวิดีโอโดยทั่วไปอาจใช้พื้นที่ระดับกิกะไบต์ต่อกล้องต่อวันและเก็บตามระยะเวลา ส่วน Log การใช้งาน (เช่น การเข้าสู่ระบบ การเปลี่ยนค่า การส่งออกภาพ) มีขนาดเล็กมาก โดยทั่วไปไม่กี่เมกะไบต์ต่ออุปกรณ์ต่อเดือน แต่ต้องเก็บนานกว่าภาพ และควรเก็บแยกจากดิสก์ภาพเพื่อไม่ให้ถูกเขียนทับ

3.2.5 การเลือกอุปกรณ์ที่น่าเชื่อถือและความมั่นคงปลอดภัยของห่วงโซ่อุปทาน

การเลือกอุปกรณ์สำหรับระบบ CCTV ไม่ควรพิจารณาเฉพาะคุณสมบัติด้านสมรรถนะหรือราคาเป็นปัจจัยหลักเพียงอย่างเดียว แต่ควรพิจารณาความมั่นคงปลอดภัยของผลิตภัณฑ์และความสามารถในการสนับสนุนตลอดวงจรชีวิตร่วมด้วย เนื่องจากความเสี่ยงอาจเกิดจากตัวผลิตภัณฑ์ ซอฟต์แวร์หรือเฟิร์มแวร์ ส่วนประกอบจากบุคคลที่สาม ผู้ผลิต ผู้ส่งมอบ ผู้ให้บริการ ตลอดจนกระบวนการสนับสนุนและบำรุงรักษาหลังการส่งมอบ

ประเด็นที่ควรพิจารณาจึงครอบคลุมการพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัยและผู้ผลิตที่เชื่อถือได้ การจัดการและการเปิดเผยช่องโหว่ การบริหารส่วนประกอบซอฟต์แวร์และความโปร่งใสของห่วงโซ่อุปทาน ความสามารถในการทำงานร่วมกัน การสนับสนุนตลอดอายุผลิตภัณฑ์ ตลอดจนหลักฐานที่ใช้สร้างความเชื่อมั่นว่าผลิตภัณฑ์หรือระบบสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยที่องค์กรกำหนด

ระดับความเข้มงวดของมาตรการ ข้อกำหนด และหลักฐานที่ใช้ประกอบการพิจารณาควรสัมพันธ์กับระดับความสำคัญและความเสี่ยงของระบบ

3.2.5.1 การพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัยและผู้ผลิตที่เชื่อถือได้

ผลิตภัณฑ์ที่นำมาใช้ควรมาจากผู้ผลิตที่นำหลักความมั่นคงปลอดภัยตั้งแต่การออกแบบและโดยค่าเริ่มต้น (Secure by Design and by Default) มาใช้ในกระบวนการพัฒนาผลิตภัณฑ์ (Secure Development Lifecycle: SDL) ครอบคลุมการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัย การออกแบบ การพัฒนา การทดสอบ การส่งมอบ และการดูแลผลิตภัณฑ์หลังจำหน่าย กรอบอ้างอิงที่ใช้แสดงหลักฐานได้ เช่น IEC 62443-4-1 สำหรับกระบวนการพัฒนาผลิตภัณฑ์ IEC 62443-4-2 สำหรับข้อกำหนดทางเทคนิคของส่วนประกอบ และ ETSI EN 303 645 สำหรับอุปกรณ์ IoT สำหรับผู้บริโภค

ผู้ผลิตที่เชื่อถือได้ (Trusted Manufacturer) ในความหมายของแนวปฏิบัตินี้ มิได้พิจารณาจากขนาดหรือสัญชาติของผู้ผลิต แต่พิจารณาจากความสามารถที่แสดงหลักฐานได้ ได้แก่ กระบวนการพัฒนาอย่างมั่นคงปลอดภัย การบริหารและเปิดเผยช่องโหว่ ความโปร่งใสของส่วนประกอบซอฟต์แวร์ การสนับสนุนตลอดวงจรชีวิตผลิตภัณฑ์ และหลักฐานการสร้างความเชื่อมั่น โดยระดับหลักฐานที่ต้องการให้เป็นไปตามระดับ B/E/H ของระบบ

3.2.5.2 การบริหารจัดการและการเปิดเผยช่องโหว่

ผู้ผลิตควรมีช่องทางรับแจ้งช่องโหว่และผู้รับผิดชอบในการวิเคราะห์ ประสานงาน และสื่อสาร โดยอาจมีทีมตอบสนองเหตุด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ (Product Security Incident Response Team: PSIRT) หรือหน่วยงาน/กระบวนการอื่นที่ทำหน้าที่เทียบเท่า สามารถใช้ ISO/IEC 29147 และ ISO/IEC 30111 เป็นกรอบอ้างอิงตามความเหมาะสม

หากยังไม่มี Patch หรือ Security Update ควรพิจารณามาตรการบรรเทาความเสี่ยง เช่น การปิดบริการที่ได้รับผลกระทบ การจำกัด Network Access การเพิ่ม Network Segmentation การจำกัด Remote Access การเพิ่ม Monitoring หรือการใช้มาตรการชดเชยอื่น

3.2.5.3 การบริหารส่วนประกอบซอฟต์แวร์และความโปร่งใสของห่วงโซ่อุปทาน

ผู้ผลิตหรือผู้ให้บริการควรสามารถทราบ บริหาร และติดตามส่วนประกอบซอฟต์แวร์ที่มีความสำคัญ รวมถึงส่วนประกอบจากบุคคลที่สาม เพื่อสนับสนุนการติดตามช่องโหว่ การประเมินผลกระทบ การอัปเดต และการตอบสนองเมื่อพบความเสี่ยง

แนวปฏิบัตินี้ไม่กำหนดรูปแบบเอกสารหรือเครื่องมือเฉพาะ และไม่กำหนดให้ต้องเปิดเผยรายการส่วนประกอบทั้งหมดต่อสาธารณะ หากสามารถแสดงหลักฐานที่เพียงพอต่อการบริหารความเสี่ยงได้

3.2.5.4 การทำงานร่วมกันและการลดการผูกติดผู้ให้บริการ

ระบบ CCTV มักประกอบด้วยผลิตภัณฑ์และบริการหลายส่วน เช่น กล้อง ระบบบริหารจัดการวิดีโอ เครื่องบันทึก ระบบจัดเก็บข้อมูล อุปกรณ์เครือข่าย โปรแกรมประยุกต์ และบริการภายนอก การออกแบบจึงควรพิจารณาความสามารถในการทำงานร่วมกันและความสามารถในการเปลี่ยน ทดแทน หรือย้ายส่วนประกอบของระบบโดยไม่เกิดผลกระทบที่ไม่เหมาะสม

ประเด็นที่ควรพิจารณา ได้แก่

ประเด็น	สิ่งที่ควรพิจารณา
มาตรฐานการทำงานร่วมกัน	รองรับมาตรฐานหรือโปรไฟล์ที่เกี่ยวข้อง เช่น ONVIF ตามฟังก์ชันที่ต้องใช้งานจริง
ส่วนเชื่อมต่อระบบ (API/Interface)	มีเอกสารและสามารถควบคุมการเข้าถึงส่วนเชื่อมต่อได้อย่างเหมาะสม
การส่งออกข้อมูล	สามารถส่งออกภาพ วิดีโอ บันทึกเหตุการณ์ หรือข้อมูลที่จำเป็นในรูปแบบที่สามารถนำไปใช้ต่อได้

ประเด็น	สิ่งที่ควรพิจารณา
การย้ายข้อมูล	สามารถนำข้อมูลที่จำเป็นออกจากระบบเมื่อเปลี่ยนผลิตภัณฑ์หรือผู้ให้บริการ
การย้ายค่าตั้งระบบ	ควรสามารถสำรอง ส่งออก หรือจัดทำเอกสารค่าตั้งสำคัญเพื่อสนับสนุนการกู้คืนหรือการเปลี่ยนระบบ
การเปลี่ยนส่วนประกอบ	สามารถเปลี่ยนกล้อง เครื่องบันทึก ระบบจัดเก็บ หรือส่วนประกอบอื่นได้ตามความเหมาะสม โดยไม่จำเป็นต้องเปลี่ยนระบบทั้งหมด
การทดสอบการทำงานร่วมกัน	ทดสอบตามกรณีใช้งานจริงที่องค์กรต้องการก่อนการตรวจรับ

การระบุว่าผลิตภัณฑ์ **“รองรับ ONVIF”** เพียงอย่างเดียวไม่เพียงพอ เนื่องจากผลิตภัณฑ์อาจรองรับโปรไฟล์หรือความสามารถแตกต่างกัน องค์กรจึงควรกำหนดฟังก์ชันที่ต้องการ เช่น การรับส่งภาพ การค้นหาอุปกรณ์ การควบคุมกล้อง การจัดการเหตุการณ์ หรือการบันทึก และทดสอบการทำงานร่วมกันตามกรณีใช้งานจริง

การลดการผูกติดผู้ให้บริการ (Vendor Lock-in) มิได้หมายความว่าต้องหลีกเลี่ยงระบบจากผู้ผลิตรายเดียวเสมอไป แต่หมายถึงองค์กรควรทราบข้อจำกัดและมีความสามารถที่เหมาะสมในการ **เข้าถึงข้อมูล ส่งออกข้อมูล สำรองค่าตั้ง เปลี่ยนส่วนประกอบ เปลี่ยนผู้ให้บริการ หรือยุติบริการ** โดยไม่ทำให้เกิดความเสี่ยงหรือค่าใช้จ่ายที่ไม่สมเหตุผล

3.2.5.5 การรับรอง ผลการทดสอบ และหลักฐานการสร้างความเชื่อมั่น

การรับรองมาตรฐาน รายงานผลการทดสอบ หรือหลักฐานจากผู้ผลิตและหน่วยงานอิสระสามารถใช้สนับสนุนการประเมินความมั่นคงปลอดภัยของผลิตภัณฑ์หรือระบบได้ แต่ไม่ควรใช้ใบรับรองหรือผลการทดสอบเพียงรายการเดียวเป็นข้อสรุปว่าระบบมีความมั่นคงปลอดภัยเพียงพอสำหรับทุกบริบท

ก่อนใช้หลักฐานดังกล่าว องค์กรควรพิจารณาอย่างน้อยดังนี้

ประเด็น	สิ่งที่ควรตรวจสอบ
ขอบเขต (Scope)	หลักฐานครอบคลุมผลิตภัณฑ์ ระบบ กระบวนการ หรือบริการส่วนใด
รุ่นและเวอร์ชัน	รุ่นฮาร์ดแวร์ ซอฟต์แวร์ หรือเฟิร์มแวร์ตรงกับสิ่งที่นำมาใช้งานจริงหรือไม่
เกณฑ์ที่ใช้ทดสอบ	การทดสอบหรือการรับรองประเมินคุณสมบัติด้านใด และสอดคล้องกับความเสี่ยงที่ต้องการควบคุมหรือไม่
ระยะเวลาที่มีผล	หลักฐานยังมีผลและมีความเป็นปัจจุบันหรือไม่

ประเด็น	สิ่งที่ควรตรวจสอบ
ผู้ออกหลักฐาน	เป็นผู้ผลิต ห้องปฏิบัติการ หน่วยรับรอง หรือหน่วยงานอิสระ และมีบทบาทอย่างไร
ความเป็นอิสระ	ระดับความเป็นอิสระของผู้ประเมินเหมาะสมกับระดับความเชื่อมั่นที่ต้องการหรือไม่
ข้อจำกัด	มีข้อยกเว้น สมมติฐาน หรือเงื่อนไขที่ทำให้ผลไม่ครอบคลุมระบบจริงหรือไม่
ความสามารถในการสอบกลับ	สามารถเชื่อมโยงหลักฐานกับผลิตภัณฑ์ รุ่น เวอร์ชัน หรือระบบที่ส่งมอบจริงได้หรือไม่

สำหรับระบบระดับความเชื่อมั่นสูง (High-Assurance: H) อาจพิจารณาหลักฐานจากการทดสอบหรือการประเมินที่มีความเป็นอิสระและมีขอบเขตชัดเจนมากขึ้นตามระดับความเสี่ยง เช่น รายงานการทดสอบเจาะระบบ (Penetration Test) หรือการประเมินช่องโหว่ (Vulnerability Assessment) โดยผู้ประเมินที่เป็นอิสระ

หลักฐานการสร้างความเชื่อมั่นอาจประกอบด้วยเอกสารทางเทคนิค รายงานผลการทดสอบ ผลการประเมินด้านความมั่นคงปลอดภัย หลักฐานกระบวนการพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย หลักฐานการจัดการช่องโหว่ หรือการรับรองตามมาตรฐานที่เกี่ยวข้อง โดยควรเลือกใช้ให้เหมาะสมกับข้อกำหนดและความเสี่ยงของระบบ

3.2.5.6 รากฐานความเชื่อถือในฮาร์ดแวร์และการบันทึกเหตุการณ์ระดับอุปกรณ์

อุปกรณ์ที่ไม่สามารถยืนยันได้ว่าเฟิร์มแวร์ที่ทำงานอยู่เป็นของแท้และไม่ถูกดัดแปลง หรือไม่สามารถเก็บกุญแจและใบรับรองอย่างปลอดภัย ย่อมทำให้มาตรการเข้ารหัส การพิสูจน์ตัวตนอุปกรณ์ และการตรวจสอบย้อนหลังอ่อนแอลง สำหรับระบบระดับเพิ่มเติม (E) และระดับความเชื่อมั่นสูง (H) จึงควรพิจารณาคุณสมบัติต่อไปนี้เป็นเกณฑ์ในการเลือกอุปกรณ์

มาตรการ	B	E	H
อุปกรณ์รองรับการเริ่มต้นระบบอย่างมั่นคงปลอดภัย (Secure Boot) และเฟิร์มแวร์ที่ลงนามดิจิทัล (Signed Firmware) โดยปฏิเสธเฟิร์มแวร์ที่ไม่ผ่านการตรวจสอบ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
มีรากฐานความเชื่อถือในฮาร์ดแวร์ (Hardware Root of Trust) เช่น Trusted Platform Module (TPM), Secure Element หรือเทคโนโลยีที่ให้ระดับความเชื่อมั่นเทียบเท่า	—	ควรพิจารณา	พึงปฏิบัติ

มาตรการ	B	E	H
เพื่อสนับสนุนการจัดเก็บและปกป้องกุญแจเข้ารหัส การตรวจสอบความถูกต้องของกระบวนการเริ่มต้นระบบหรือเฟิร์มแวร์ และการยืนยันความน่าเชื่อถือของอุปกรณ์			
รองรับการตรวจสอบความถูกต้องของเฟิร์มแวร์และการยืนยันตัวตนหรือความน่าเชื่อถือของอุปกรณ์ (Firmware Integrity Verification / Device Attestation) โดยอาจใช้ข้อมูลประจำตัวอุปกรณ์ตามมาตรฐานที่เกี่ยวข้อง เช่น IEEE 802.1AR หรือกลไกที่ให้ระดับความเชื่อมั่นเทียบเท่า	—	ควรพิจารณา	พึงปฏิบัติ
กลไกป้องกันและตรวจจับการดัดแปลงทางกายภาพ (Anti-Tamper) เช่น แจ้งเตือนเมื่อฝาครอบถูกเปิด ถูกถอด หรือถูกกดปุ่มรีเซ็ต	—	ควรพิจารณา	พึงปฏิบัติ
เข้ารหัสข้อมูลสำคัญที่จัดเก็บบนอุปกรณ์ (เช่น SD Card หรือ Edge Storage) และมีมาตรการปกป้องกุญแจเข้ารหัสอย่างเหมาะสม เช่น การใช้ Hardware Root of Trust หรือกลไกที่ให้ระดับความเชื่อมั่นเทียบเท่า	—	ควรพิจารณา	พึงปฏิบัติ
บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยที่ระดับอุปกรณ์ (Device-Level Logging) เช่น การเข้าสู่ระบบ การเปลี่ยนค่าตั้ง การอัปเดตเฟิร์มแวร์ การรีเซ็ต และการเข้าถึงที่ล้มเหลว โดยสามารถส่งออกไปยัง Syslog/SIEM แบบเข้ารหัสได้	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ปิดหรือปกป้องส่วนเชื่อมต่อสำหรับแก้ไขข้อบกพร่องทางฮาร์ดแวร์ (เช่น UART/JTAG) ในผลิตภัณฑ์ที่จำหน่าย	—	ควรพิจารณา	พึงปฏิบัติ

แนวปฏิบัตินี้ไม่กำหนดให้ต้องใช้เทคโนโลยีหรือชิปเฉพาะรุ่นใด หากผู้ผลิตสามารถแสดงได้ว่ากลไกที่ใช้ให้ระดับความเชื่อมั่นเทียบเท่า สำหรับระบบที่มีการประมวลผลที่อุปกรณ์ปลายทาง (Edge Processing) เช่น การวิเคราะห์ภาพบนกล้อง การคุ้มครองข้อมูลและโมเดลบนอุปกรณ์ด้วยกลไกข้างต้น รวมถึงการเข้ารหัสข้อมูลตั้งแต่อุปกรณ์ปลายทางจนถึงระบบบันทึกหรือคลาวด์ (Edge-to-Cloud) ยิ่งมีความสำคัญ เนื่องจากอุปกรณ์ปลายทางมักติดตั้งในพื้นที่ที่บุคคลภายนอกเข้าถึงได้

3.3 การติดตั้ง

การติดตั้งระบบ CCTV ควรดำเนินการตามแบบ สถาปัตยกรรม ข้อกำหนดด้านความมั่นคงปลอดภัย และเงื่อนไขที่ได้รับอนุมัติจากเจ้าของระบบ โดยไม่ควรเพิ่มบัญชี บริการ ช่องทางการเชื่อมต่อ หรือค่าตั้งชั่วคราวที่ไม่ได้รับอนุมัติ เพียงเพื่ออำนวยความสะดวกในการติดตั้งหรือบำรุงรักษา

การติดตั้งควรพิจารณาร่วมกันทั้งความมั่นคงปลอดภัยทางกายภาพ การแบ่งเครือข่าย การจำกัดพอร์ตและบริการ การตั้งค่าระบบ ตลอดจนการทดสอบและตรวจรับในสภาพแวดล้อมจริงก่อนเปิดใช้งาน

3.3.1 ความมั่นคงปลอดภัยทางกายภาพ

ผู้ที่ต้องพิจารณา: ผู้ติดตั้งหรือผู้รวมระบบเป็นหลัก โดยเจ้าของระบบควรกำหนดข้อกำหนดและตรวจรับมาตรการที่เกี่ยวข้อง

การใช้มาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์เพียงอย่างเดียวอาจไม่เพียงพอ หากบุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงตัวอุปกรณ์ สื่อบันทึก สายสัญญาณ พอร์ตเครือข่าย ปุ่ม Reset หรือส่วนบริหารจัดการของระบบได้โดยง่าย การรักษาความมั่นคงปลอดภัยทางกายภาพควรคำนึงถึงมาตรการอย่างน้อยดังต่อไปนี้

มาตรการ	B	E	H
ติดตั้งกล้องและอุปกรณ์ในตำแหน่งที่ลดความเสี่ยงจากการถอด บดบัง หมุน หรือดัดแปลง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
จัดเก็บ NVR/DVR/VMS Server, Storage และอุปกรณ์เครือข่ายในพื้นที่ที่ควบคุมการเข้าถึง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
เก็บหลักฐานการเข้าถึงพื้นที่จัดเก็บอุปกรณ์สำคัญตามความเสี่ยง	—	ควรพิจารณา	พึงปฏิบัติ
ป้องกันสายสัญญาณและสายไฟจากการตัดต่อหรือเข้าถึงโดยไม่ได้รับอนุญาต	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ป้องกันหรือปิดพอร์ตทางกายภาพที่ไม่จำเป็น	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
จำกัดการเข้าถึงปุ่ม Reset หรือกลไกคืนค่าโรงงาน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
จำกัดหรือปิดการใช้สื่อบันทึกที่ตัวอุปกรณ์เมื่อไม่จำเป็น	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ

มาตรการ	B	E	H
จัดให้มีไฟฟ้าสำรองสำหรับองค์ประกอบที่มีความสำคัญ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ตรวจจับการบดบัง การเปลี่ยนมุม หรือการงัดแงะเมื่อระบบรองรับ	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ
ใช้มาตรการป้องกันไฟกระชากหรือฟ้าผ่าตามสภาพแวดล้อม	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ติดรหัสอุปกรณ์และเชื่อมโยงกับทะเบียนทรัพย์สิน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

การควบคุมสภาพแวดล้อม

สำหรับอุปกรณ์ที่มีความสำคัญ ควรพิจารณาปัจจัยด้านสภาพแวดล้อมที่อาจกระทบต่อความพร้อมใช้งานและอายุการใช้งานของอุปกรณ์

ปัจจัย	แนวทางพิจารณา
อุณหภูมิ	อยู่ในช่วงการทำงานที่ผู้ผลิตกำหนด
ความชื้น	ไม่เกินระดับที่อาจกระทบต่ออุปกรณ์
ฝุ่นและน้ำ	เลือกการป้องกันตามสภาพแวดล้อม
การสั่นสะเทือน	ใช้จุดติดตั้งและอุปกรณ์ยึดที่เหมาะสม
ไฟฟ้าขัดข้อง	พิจารณา UPS หรือแหล่งจ่ายไฟสำรอง
ไฟกระชาก	ใช้อุปกรณ์ป้องกันตามความเหมาะสม
การระบายอากาศ	รองรับภาระความร้อนของอุปกรณ์
การเข้าถึงพื้นที่	จำกัดเฉพาะผู้ได้รับอนุญาต

3.3.2 ระบบสายสัญญาณและโครงสร้างพื้นฐานการเชื่อมต่อ

ระบบสายสัญญาณและการเชื่อมต่อที่ใช้กับระบบ CCTV ควรได้รับการออกแบบ ติดตั้ง ป้องกัน และทดสอบให้เหมาะสมกับประเภทของระบบ สภาพแวดล้อม ลักษณะการใช้งาน และระดับความสำคัญของระบบ โดยพิจารณาความมั่นคงปลอดภัยทางกายภาพ ความพร้อมใช้งาน คุณภาพการส่งสัญญาณ การจ่ายไฟผ่าน

เครือข่าย (Power over Ethernet: PoE) และความเสี่ยงจากการเข้าถึง การรบกวน หรือความเสียหายต่อสายสัญญาณ

การออกแบบ ติดตั้ง และทดสอบควรพิจารณามาตรฐานสากลที่เกี่ยวข้องตามประเภทของระบบและเทคโนโลยี เช่น IEC 62676-4, ISO/IEC 11801 series, ANSI/TIA-568 series และ EN 50173 series รวมถึง IEEE 802.3 สำหรับระบบเครือข่าย Ethernet และการจ่ายไฟผ่านเครือข่าย (Power over Ethernet: PoE) ตามความเกี่ยวข้อง หรือมาตรฐานอื่นที่ให้ระดับสมรรถนะและความเชื่อมั่นเทียบเท่า

ระดับความเข้มงวดของมาตรการด้านระบบสายสัญญาณและโครงสร้างพื้นฐานการเชื่อมต่อควรสัมพันธ์กับระดับความสำคัญ สภาพแวดล้อม และความเสี่ยงของระบบ โดยสามารถพิจารณาแนวทางตามระดับ B/E/H ดังต่อไปนี้

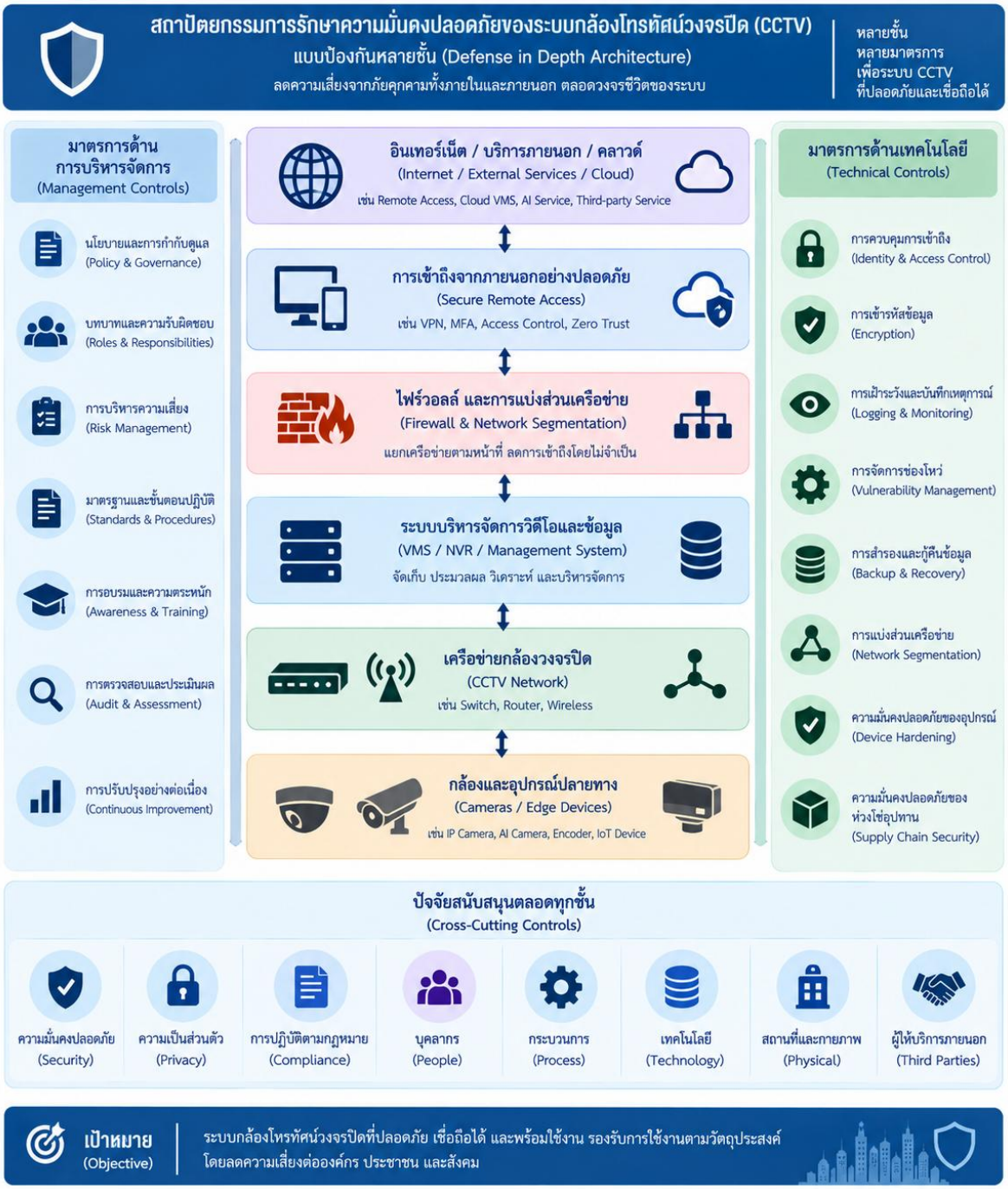
มาตรการ	B	E	H
ระบบสายสัญญาณและการเชื่อมต่อได้รับการติดตั้งและป้องกันให้เหมาะสมกับสภาพแวดล้อมและการใช้งาน	**พึงปฏิบัติ**	**พึงปฏิบัติ**	**พึงปฏิบัติ**
ทดสอบระบบสายสัญญาณและการเชื่อมต่อตามมาตรฐานหรือวิธีการที่เกี่ยวข้อง และเก็บผลการทดสอบไว้เป็นหลักฐาน	**ควรพิจารณา**	**พึงปฏิบัติ**	**พึงปฏิบัติ พร้อมหลักฐานผลการทดสอบ**
เพิ่มมาตรการป้องกันสาย จุดเชื่อมต่อ และเส้นทางสายจากการเข้าถึงโดยไม่ได้รับอนุญาต การตัดต่อ การรบกวน หรือความเสียหาย ตามระดับความเสี่ยง	**ควรพิจารณา**	**พึงปฏิบัติ**	**พึงปฏิบัติ พร้อมมาตรการป้องกันตามความเสี่ยง**

3.3.3 สถาปัตยกรรมเครือข่าย การแบ่งโซน และหลักการไม่ให้ความเชื่อถือโดยปริยาย

ผู้ที่ต้องพิจารณา: ผู้ติดตั้งหรือผู้รวมระบบเป็นหลัก โดยเจ้าของระบบและผู้รับผิดชอบด้านเครือข่ายควรเห็นชอบและสามารถบริหารจัดการต่อได้หลังการส่งมอบ

ระบบ CCTV ที่เชื่อมต่อเครือข่ายควรได้รับการออกแบบตามหลักการป้องกันเชิงลึก จำกัดการสื่อสารที่จำเป็น จำกัดเส้นทางการสื่อสารเท่าที่จำเป็น จำกัดบริการ ไม่ถือว่าผู้ใช้หรืออุปกรณ์มีความน่าเชื่อถือเพียงเพราะอยู่ภายในเครือข่ายขององค์กร ตรวจสอบและบันทึกตามความเสี่ยง

การแบ่งเครือข่ายช่วยลดผลกระทบเมื่ออุปกรณ์หนึ่งถูกโจมตี และช่วยจำกัดการเคลื่อนย้ายของภัยคุกคามไปยังระบบอื่น



รูปที่ 4 สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยระบบ CCTV โดยใช้มาตรการป้องกันเชิงลึก

ระบบ CCTV ควรใช้มาตรการป้องกันเชิงลึก ครอบคลุมอุปกรณ์ เครือข่าย ระบบบริหารจัดการ การเข้าถึงจากระยะไกล และบริการภายนอก โดยสนับสนุนด้วยการควบคุมสิทธิ การเข้ารหัส การบันทึกและเฝ้าระวัง การจัดการช่องโหว่ การสำรองและกู้คืน และการบริหารห่วงโซ่อุปทาน

3.3.3.1 ตัวอย่างการแบ่งโซนเครือข่าย

ตารางต่อไปนี้เป็นสถาปัตยกรรมอ้างอิง องค์กรสามารถปรับจำนวนและลักษณะของโซนให้เหมาะสมกับระบบจริง

โซนตัวอย่าง	องค์ประกอบ	แนวทางควบคุม
โซนกล้อง/อุปกรณ์ปลายทาง (Camera/Edge Zone)	กล้อง ตัวเข้ารหัส และ Edge Device	จำกัดการส่งสารไปยัง NVR/VMS หรือระบบที่จำเป็น และจำกัดการเชื่อมต่อออกภายนอก
โซนบันทึกและบริหารจัดการ (Recording/Management Zone)	NVR/DVR/VMS, Storage, Management Server	จำกัดการเข้าถึงจากผู้ใช้และระบบอื่นด้วยมาตรการควบคุมเครือข่าย
โซนผู้ใช้งาน/ศูนย์ควบคุม (User/Control Zone)	Workstation, Operator Console	ใช้การพิสูจน์ตัวตนและกำหนดสิทธิตามบทบาท
โซนการเข้าถึงจากภายนอก (Remote Access Zone)	Remote Support, External Administrator	อนุญาตเฉพาะช่องทางที่ได้รับอนุมัติ จำกัดสิทธิ ระยะเวลา และบันทึกการเข้าถึง

3.3.3.2 การประยุกต์หลักการไม่ให้ความเชื่อถือโดยปริยาย

การประยุกต์หลัก Zero Trust ไม่ได้หมายความว่าองค์กรต้องใช้ผลิตภัณฑ์หรือเทคโนโลยีประเภทใดเป็นการเฉพาะ แต่หมายถึงการตรวจสอบตัวตน สิทธิ บริบท และความจำเป็นก่อนอนุญาตการเข้าถึง

หลักการสำคัญ ได้แก่

- ตรวจสอบตัวตนของผู้ใช้และอุปกรณ์ก่อนอนุญาต
- ไม่ให้ความเชื่อถือโดยอัตโนมัติเพียงเพราะอยู่ในเครือข่ายภายใน
- ให้สิทธิเท่าที่จำเป็น (Least Privilege)
- จำกัดสิทธิของผู้ให้บริการภายนอกตามวัตถุประสงค์และระยะเวลา
- จำกัดการเคลื่อนที่ระหว่างส่วนต่าง ๆ ของเครือข่าย (Lateral Movement)
- เฝ้าระวังการเชื่อมต่อที่ผิดปกติ
- ทบทวนสิทธิและช่องทางการเชื่อมต่อเมื่อบริบทเปลี่ยนแปลง

มาตรการ	B	E	H
แยกเครือข่าย CCTV ออกจากเครือข่ายผู้ใช้งานทั่วไปตามความเหมาะสม	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ไม่เปิดกล้องหรือส่วนบริหารจัดการสู่อินเทอร์เน็ตโดยตรงโดยไม่จำเป็น	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
การเข้าถึงจากระยะไกลผ่านช่องทางที่ได้รับอนุมัติ	พึงปฏิบัติ	พึงปฏิบัติ พร้อม MFA ตามความเสี่ยง	พึงปฏิบัติ พร้อม MFA ตามความเสี่ยง
ใช้ Firewall หรือมาตรการเทียบเท่าควบคุมการสื่อสารระหว่างโซน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้หลัก Default Deny สำหรับเส้นทางหรือบริการที่ต้องควบคุม	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
แยก Management Plane, Video/Recording และ User Access ตามความเสี่ยง	—	ควรพิจารณา	พึงปฏิบัติ
จำกัด Lateral Movement หรือใช้ Micro-segmentation	—	ควรพิจารณา	พึงปฏิบัติ
ใช้ Network Access Control (NAC) หรือกลไกเทียบเท่าตามความเหมาะสม	—	ควรพิจารณา	พึงปฏิบัติตามความเสี่ยง
ใช้ IDS/IPS หรือกลไกตรวจจับความผิดปกติ	—	ควรพิจารณา	พึงปฏิบัติตามความเสี่ยง
จัดทำทะเบียน IP และแผนผังเครือข่าย	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ปรับปรุง Network Diagram เมื่อมีการเปลี่ยนแปลงสำคัญ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

3.3.3.3 การเชื่อมต่อกับระบบ OT หรือระบบควบคุมอาคาร

หากระบบ CCTV เชื่อมต่อหรือใช้โครงสร้างพื้นฐานร่วมกับระบบเทคโนโลยีปฏิบัติการ (Operational Technology: OT) ระบบบริหารอาคาร หรือระบบควบคุมอื่น ควรพิจารณาผลกระทบระหว่างระบบทั้งสองด้าน ควรหลีกเลี่ยงการเชื่อมต่อโดยตรงโดยไม่มีการกำหนดขอบเขตและการควบคุมที่ชัดเจน และสามารถประยุกต์แนวคิดการแบ่งโซนและช่องทางการสื่อสาร (Zones and Conduits) ตาม IEC 62443 series ตามความเหมาะสม

3.3.3.4 การเชื่อมต่อผ่านบริการ P2P หรือบริการภายนอก

บริการเชื่อมต่อแบบ P2P หรือบริการคลาวด์ของผู้ผลิตอาจช่วยให้ผู้ใช้งานเข้าถึงระบบจากภายนอกได้สะดวก แต่ควรได้รับการกำกับในลักษณะเดียวกับช่องทางการเข้าถึงจากระยะไกลอื่น

ก่อนเปิดใช้งานควรพิจารณาประเด็นดังต่อไปนี้

ประเด็น	คำถามที่ควรตอบ
ช่องทางการเชื่อมต่อ	เชื่อมต่อผ่านระบบหรือบริการใด
ข้อมูลที่ส่งออก	มีข้อมูลหรือ Metadata ใดถูกส่งออกจากองค์กร
สถานที่ให้บริการ	เซิร์ฟเวอร์หรือบริการอยู่ที่ใดตามข้อมูลที่ผู้ให้บริการเปิดเผย
ผู้ที่เข้าถึงได้	ใครสามารถสนับสนุนหรือบริหารระบบได้
การพิสูจน์ตัวตน	รองรับ MFA หรือไม่
การควบคุมบริการ	สามารถปิดหรือจำกัดบริการได้หรือไม่
การบันทึกเหตุการณ์	มี Log ที่เพียงพอหรือไม่
การยุติบริการ	สามารถย้ายหรือยุติบริการอย่างไร

การใช้ P2P หรือ Cloud ไม่ควรถูกสรุปว่าปลอดภัยหรือไม่ปลอดภัยจากชื่อของเทคโนโลยีเพียงอย่างเดียว แต่ควรประเมินจากสถาปัตยกรรม การควบคุม และความเสี่ยงจริง

3.3.4 การควบคุมพอร์ตและบริการเครือข่าย

ผู้ที่ต้องพิจารณา: ผู้ติดตั้งหรือผู้รวมระบบเป็นหลัก และเจ้าของระบบควรควบคุมไม่ให้มีการเปิดบริการภายหลังโดยไม่มีการอนุมัติ

อุปกรณ์ควรเปิดใช้งานเฉพาะบริการ โพรโทคอล และส่วนเชื่อมต่อที่จำเป็น ตามหลักการเปิดใช้เฉพาะฟังก์ชันที่จำเป็น (Least Functionality)

3.3.4.1 ตัวอย่างบริการและโพรโทคอลพร้อมทั้งแนวทางการพิจารณา

บริการ/โพรโทคอล	แนวทางพิจารณา	ข้อควรระวัง
HTTPS/TLS	ใช้สำหรับส่วนบริหารจัดการเมื่อรองรับ	ต้องบริหาร Certificate และ Trust อย่างเหมาะสม
HTTP แบบไม่เข้ารหัส	ปิดหรือจำกัดเมื่อมีช่องทางที่เข้ารหัสทดแทน	ข้อมูลยืนยันตัวตนและข้อมูลบริหารอาจถูกดักรับ
RTSP/Video Streaming	เปิดเฉพาะเมื่อจำเป็นและจำกัดต้นทาง/ปลายทาง	ควรพิจารณาการพิสูจน์ตัวตนและการป้องกันข้อมูล
ONVIF	เปิดเฉพาะ Feature/Profile ที่จำเป็น	ควรกำหนดบัญชีและสิทธิให้เหมาะสม
SSH	เปิดเฉพาะเมื่อจำเป็น	จำกัดต้นทาง บัญชี และบันทึกเหตุการณ์การเข้าถึง
Telnet	หลีกเลี่ยงเมื่อมีทางเลือกที่มั่นคงปลอดภัยกว่า	ไม่มีการป้องกันข้อมูลที่เหมาะสม
SNMP	เปิดเมื่อจำเป็นสำหรับ Monitoring	หากรองรับควรพิจารณา SNMPv3
UPnP	ปิดเมื่อไม่มีความจำเป็น	อาจเปิดการเชื่อมต่อโดยอัตโนมัติ
FTP	หลีกเลี่ยงสำหรับข้อมูลสำคัญเมื่อมีทางเลือกที่เหมาะสมกว่า	ไม่มีการเข้ารหัสโดยค่าเริ่มต้น
P2P/Cloud Connectivity	เปิดเฉพาะเมื่อได้รับอนุมัติ	เป็นช่องทางออกภายนอกที่ต้องกำกับ
Discovery Services	จำกัดหรือปิดเมื่อไม่จำเป็น	ลดการเปิดเผยรายละเอียดของระบบ

หมายเลข Port ที่ใช้จริงอาจแตกต่างตามผู้ผลิต รุ่น และค่าตั้ง จึงควรจัดทำรายการ Port/Protocol/Service ของระบบจริง พร้อมเหตุผลในการใช้งาน

3.3.4.2 มาตรการควบคุม

ตัวอย่างมาตรการการควบคุมพอร์ตและบริการเครือข่ายดังแสดงในตารางต่อไปนี้

มาตรการ	B	E	H
เปิดเฉพาะบริการที่จำเป็น	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ปิดบริการหรือโพรโทคอลที่ไม่จำเป็นหรือมีความเสี่ยงสูงเมื่อมีทางเลือกที่เหมาะสมกว่า	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
จำกัดแหล่งที่สามารถเข้าถึงบริการบริหารจัดการ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้ Allow-list หรือกลไกเทียบเท่า	—	ควรพิจารณา	พึงปฏิบัติ
ทบทวน Port/Service ตามรอบและเมื่อมีการเปลี่ยนแปลง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
จัดทำรายการ Port/Protocol/Service และเหตุผล	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ปิดบริการชั่วคราวที่ใช้ระหว่างติดตั้งหรือบำรุงรักษาเมื่อสิ้นสุดงาน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

3.3.5 การทดสอบและตรวจรับด้านเทคนิคหลังการติดตั้ง

ก่อนเปิดใช้งานระบบ ควรตรวจสอบว่าระบบที่ติดตั้งจริงตรงตามวัตถุประสงค์ แบบ และข้อกำหนดทางเทคนิคที่ได้รับอนุมัติ ไม่ควรตรวจสอบเพียงว่ากล้องสามารถแสดงและบันทึกภาพได้หรือไม่โดยไม่ตรวจสอบข้อกำหนดที่ได้ระบุไว้

ประเด็นตรวจรับ	สิ่งที่ควรยืนยัน
ตำแหน่งและมุมกล้อง	ตรงตามแบบและตอบ POR
คุณภาพของภาพ	ตอบ DORI และภารกิจในระยะจริง
กลางวัน/กลางคืน	คุณภาพเหมาะสมในช่วงเวลาที่ต้องให้บริการ
สิ่งกีดขวาง	ไม่มีสิ่งกีดขวางที่ทำให้วัตถุประสงค์ไม่บรรลุ
ความเป็นส่วนตัว	ไม่มีมุมมองเกินขอบเขต และ Privacy Mask ทำงานตามที่กำหนด
การบันทึกเสียง	สถานะตรงตามที่ได้รับอนุมัติ
เวลา	กล้อง NVR/VMS และองค์ประกอบสำคัญมีเวลาสอดคล้องกัน
Retention	สามารถเก็บข้อมูลได้ตามระยะเวลาที่กำหนด

ประเด็นตรวจรับ	สิ่งที่ควรยืนยัน
Network/Segmentation	ตรงตามสถาปัตยกรรมที่ได้รับอนุมัติ
Port/Service	เปิดเฉพาะรายการที่จำเป็น
Firmware/Software	Version ได้รับการตรวจสอบและบันทึก
Log/Alert	ทำงานตามข้อกำหนด
Backup/Recovery	ผ่านการทดสอบในขอบเขตที่เกี่ยวข้อง
As-built	เอกสารตรงกับระบบจริง

3.4 การดำเนินงานอย่างมั่นคงปลอดภัย

เมื่อระบบผ่านการตรวจรับและเปิดใช้งานแล้ว องค์กรควรรักษาระบบให้อยู่ในสถานะให้เป็นไปตามที่ได้รับอนุมัติ และควบคุมการเข้าถึง การเปลี่ยนแปลง การใช้ข้อมูล และการบริหารระบบบอย่างเหมาะสม

องค์กรควรคำนึงถึงและตอบประเด็นเหล่านี้ได้

ใครเข้าถึงอะไร ⟶ ผ่านช่องทางใด ⟶ ทำอะไรได้ ⟶ มีหลักฐานอะไร ⟶ และสิทธินั้นยังจำเป็นหรือไม่

3.4.1 ช่องทางบริหารจัดการที่มั่นคงปลอดภัย

องค์กรควรมีมาตรการในการบริหารจัดการที่มั่นคงปลอดภัย โดยมีตัวอย่างมาตรการดังนี้

มาตรการ	B	E	H
จำกัดส่วนบริหารจัดการให้เข้าถึงเฉพาะเครือข่ายหรือผู้ใช้ที่ได้รับอนุญาต	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ใช้ช่องทางที่มีการป้องกันข้อมูลระหว่างส่งเมื่อระบบรองรับ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ไม่เปิดส่วนบริหารจัดการสู่อินเทอร์เน็ตโดยตรงโดยไม่จำเป็น	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
การบริหารจากระยะไกลผ่านช่องทางที่ได้รับอนุมัติ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ พร้อม MFA ตามความเสี่ยง
จำกัด Vendor/Third-Party Access ตามเวลาและวัตถุประสงค์	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

มาตรการ	B	E	H
บันทึกการเข้าถึงและกิจกรรมสำคัญของผู้ดูแลระบบ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
แยกเครือข่ายหรือส่วนบริหารจัดการตามความเสี่ยง	—	ควรพิจารณา	พึงปฏิบัติ

3.4.2 การเข้ารหัสและการจัดการใบรับรอง

ควรใช้การเข้ารหัสในจุดที่เหมาะสมกับความเสี่ยง โดยเฉพาะช่องทางบริหาร การเข้าถึงจากระยะไกล การเชื่อมต่อผ่านเครือข่ายที่ไม่เชื่อถือ และข้อมูลที่มีความสำคัญ

องค์กรควรสามารถระบุได้ว่า

ข้อมูลใดได้รับการเข้ารหัส ⟶ อยู่ระหว่างส่งหรือขณะจัดเก็บ ⟶ ใช้กุญแจใด ⟶ ใครควบคุม ⟶ ต่ออายุหรือเพิกถอนอย่างไร

มาตรการ	B	E	H
ใช้ TLS หรือกลไกที่เหมาะสมสำหรับ Management Interface/API	พึงปฏิบัติเมื่อรองรับ	พึงปฏิบัติ	พึงปฏิบัติ
หลีกเลี่ยง Protocol หรือ Cryptographic Configuration ที่ล้าสมัย	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
บริหาร Certificate และ Trust อย่างเหมาะสม	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
เข้ารหัส Video Stream ตามความเสี่ยง	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ
เข้ารหัสข้อมูลขณะจัดเก็บตามความเสี่ยง	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ
เข้ารหัสไฟล์หรือสื่อส่งออกเมื่อจำเป็น	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ติดตามอายุ Certificate/Key และต่ออายุหรือเพิกถอนตามความจำเป็น	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

ไม่ควรกำหนด Private CA หรือเทคโนโลยีเฉพาะเป็นข้อบังคับหากมีกลไกอื่นที่ให้ผลด้านความมั่นคงปลอดภัยเหมาะสมกับความเสี่ยง

3.4.3 บัญชีผู้ใช้และการกำหนดสิทธิ

ควรใช้หลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) และแยกสิทธิตามหน้าที่จริง

มาตรการ	B	E	H
แยกบทบาทผู้ดูภาพและผู้ดูแลระบบ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
แยกสิทธิ ดู/ค้นหา/ส่งออก/ตั้งค่า	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้บัญชีที่สามารถระบุตัวผู้ใช้งานได้	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
หลีกเลี่ยงบัญชีผู้ดูแลระบบที่ใช้ร่วมกัน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ปิด Guest/Anonymous/Unused Account	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ใช้ RBAC เมื่อระบบรองรับ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
เชื่อมกับระบบบริหารตัวตนของผู้ใช้งานในองค์กรตามความเหมาะสม	—	ควรพิจารณา	พึงปฏิบัติตามสถาปัตยกรรม
ทบทวนสิทธิตามความเสี่ยงและการเปลี่ยนแปลง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
เพิกถอนสิทธิเมื่อพ้นหน้าที่หรือสิ้นสุดสัญญา	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ควบคุมสิทธิ Vendor/Third Party เป็นการเฉพาะ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

ความถี่ในการทบทวนสิทธิควรสัมพันธ์กับระดับความเสี่ยง จำนวนผู้ใช้งาน อัตราการเปลี่ยนแปลงบุคลากร ลักษณะของสิทธิ และข้อกำหนดที่เกี่ยวข้อง ไม่จำเป็นต้องกำหนดรอบเวลาเดียวกันสำหรับทุกระบบ

3.4.4 รหัสผ่าน ข้อมูลยืนยันตัวตน และการพิสูจน์ตัวตน

มาตรการควรมุ่งลดความเสี่ยงจากข้อมูลยืนยันตัวตนเริ่มต้น รหัสผ่านอ่อนแอ การใช้ข้อมูลยืนยันตัวตนซ้ำ การเก็บข้อมูลยืนยันตัวตนอย่างไม่เหมาะสม และการใช้ Session หรือ Token โดยไม่ได้รับอนุญาต

มาตรการ	B	E	H
เปลี่ยนหรือจัดการข้อมูลยืนยันตัวตนเริ่มต้นก่อนใช้งาน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ใช้รหัสผ่านหรือ Passphrase ที่เหมาะสมกับความเสี่ยง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ไม่ใช้รหัสผ่านเดียวกันกับหลายอุปกรณ์โดยไม่มีเหตุผล	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

มาตรการ	B	E	H
ตรวจสอบรหัสผ่านที่อ่อนแอหรือรั่วไหลเมื่อกระบวนการรองรับ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้ MFA สำหรับบัญชีสิทธิสูงและการเข้าถึงจากระยะไกล ตามความเสี่ยง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
เปลี่ยน Credential เมื่อสงสัยหรือมีหลักฐานว่ารั่วไหล	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ป้องกันการเดารหัสผ่าน (Brute Force) ด้วยการจำกัดอัตราการพยายาม (Rate Limiting) หรือการล็อกบัญชีชั่วคราว (Temporary Lockout) เมื่อระบบรองรับ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
กำหนด Session Timeout ตามความเสี่ยง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
เก็บ Credential ด้วยวิธีที่ได้รับการป้องกัน	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

ไม่ควรกำหนดจำนวนอักขระหรือขนาดของข้อมูลยืนยันตัวตนเดียวสำหรับระบบทุกประเภท แต่ควรกำหนดคุณภาพของข้อมูลยืนยันตัวตนให้เหมาะสมกับความเสี่ยง และลดการพึ่งพารหัสผ่านเพียงปัจจัยเดียวสำหรับการเข้าถึงระบบและข้อมูลที่มีความสำคัญ

3.4.5 การดู การค้นหา และการส่งออกภาพ

การดูภาพย้อนหลัง การค้นหา การส่งออก และการเปิดเผยข้อมูลเป็นกิจกรรมที่อาจกระทบทั้งความมั่นคงปลอดภัย ความเป็นส่วนตัว และความสามารถในการใช้ข้อมูลเป็นหลักฐาน

มาตรการ	B	E	H
จำกัดสิทธิการดูภาพย้อนหลังตามบทบาท	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
จำกัดสิทธิในการค้นหาและส่งออกข้อมูล	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
การส่งออกมีเหตุผลและผู้อนุมัติตามความเสี่ยง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
บันทึกผู้ส่งออก เวลา ช่วงข้อมูล วัตถุประสงค์ และผู้รับ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ป้องกันไฟล์หรือสื่อที่ส่งออก	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้ Digital Signature หรือกลไกตรวจสอบ Integrity เมื่อจำเป็น	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ

มาตรการ	B	E	H
รักษาลำดับการครอบครองหลักฐาน (Chain of Custody) เมื่อข้อมูลใช้เป็นหลักฐาน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
มีขั้นตอนการเปิดเผยข้อมูลแก่บุคคลภายนอก (ควรพิจารณาความเหมาะสมในการเปิดเผยตามบริบท มีเหตุผลที่เพียงพอหรือฐานกฎหมายในการเปิดเผยหรือไม่)	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

กรณีข้อมูลมีแนวโน้มถูกใช้เป็นหลักฐาน ควรสามารถยืนยันได้ว่า ข้อมูลมาจากระบบใด ช่วงเวลาใด ใครส่งออก เมื่อใด มีการเปลี่ยนแปลงหรือไม่ และส่งมอบให้ใคร

3.5 การบำรุงรักษาและการเฝ้าระวัง

ระบบ CCTV ควรได้รับการบำรุงรักษาและเฝ้าระวังอย่างต่อเนื่องภายหลังการติดตั้งและเปิดใช้งาน เพื่อให้ระบบยังคงมีความพร้อมใช้งาน คุณภาพของภาพ ระดับความมั่นคงปลอดภัย และความสามารถในการตรวจสอบย้อนหลังตามวัตถุประสงค์ที่กำหนด

การบำรุงรักษาไม่ควรจำกัดเฉพาะการซ่อมแซมเมื่ออุปกรณ์ชำรุด แต่ควรครอบคลุมการบำรุงรักษาเชิงป้องกัน การจัดการช่องโหว่ การปรับปรุงซอฟต์แวร์และเฟิร์มแวร์ การเฝ้าระวังสถานะระบบ การตรวจสอบบันทึกเหตุการณ์ การสำรองและกู้คืน ตลอดจนการติดตามสถานะการสนับสนุนของผลิตภัณฑ์

องค์กรควรกำหนดให้ชัดเจนว่า

ใครเป็นผู้ตรวจสอบ ⟶ ตรวจสอบเรื่องใด ⟶ ตรวจสอบเมื่อใด ⟶ เมื่อพบความผิดปกติใครเป็นผู้ดำเนินการ ⟶ และต้องมีหลักฐานใด

3.5.1 การปรับปรุงเฟิร์มแวร์ ซอฟต์แวร์ และการบำรุงรักษาระบบ

ผู้ที่ต้องพิจารณา: เจ้าของระบบ ผู้ดูแลระบบ ผู้ติดตั้ง และผู้ให้บริการตามบทบาทและขอบเขตความรับผิดชอบที่กำหนด

โดยทั่วไประบบ CCTV มีอายุการใช้งานหลายปี ขณะที่ช่องโหว่และภัยคุกคามมีการเปลี่ยนแปลงอย่างต่อเนื่อง อุปกรณ์ที่ยังสามารถทำงานได้ตามปกติอาจมีความเสี่ยงเพิ่มขึ้นหากไม่ได้รับการปรับปรุงด้านความมั่นคงปลอดภัย หรือผู้ผลิตยุติการสนับสนุนแล้ว มาตรการในการลดความเสี่ยงที่เกี่ยวข้องมีดังต่อไปนี้

มาตรการ	B	E	H
กำหนดผู้รับผิดชอบในการติดตามและปรับปรุงเฟิร์มแวร์หรือซอฟต์แวร์	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

มาตรการ	B	E	H
ติดตามประกาศแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Advisory) และข้อมูลช่องโหว่ของผลิตภัณฑ์ที่ใช้งาน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
จัดทำทะเบียนรุ่นและเวอร์ชันขององค์ประกอบสำคัญ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ประเมินความเร่งด่วนในการแก้ไขจากความรุนแรง การเปิดรับความเสี่ยง และผลกระทบของระบบ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ทดสอบการปรับปรุงก่อนนำไปใช้กับระบบจริง เมื่อการปรับปรุงอาจกระทบความต่อเนื่องของบริการ	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ
มีแผนย้อนกลับหรือกู้คืนกรณีการปรับปรุงไม่สำเร็จ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ตรวจสอบแหล่งที่มาและความถูกต้องของเฟิร์มแวร์หรือซอฟต์แวร์ก่อนติดตั้ง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
กำหนดมาตรการลดความเสี่ยงชั่วคราวกรณียังไม่สามารถติดตั้ง Patch หรือ Security Update ได้	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ทบทวนสถานะสิ้นสุดอายุผลิตภัณฑ์และการสนับสนุน (EoL/EoS)	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

การกำหนดความเร่งด่วนในการแก้ไขช่องโหว่

ไม่ควรพิจารณาความเร่งด่วนจากคะแนนความรุนแรงของช่องโหว่เพียงปัจจัยเดียว แต่ควรพิจารณาร่วมกับปัจจัยอื่น ๆ อย่างน้อยดังนี้

ปัจจัย	ประเด็นที่ควรพิจารณา
ความรุนแรงของช่องโหว่	ผลกระทบต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน
การโจมตีที่เกิดขึ้นจริง	มีหลักฐานการโจมตีหรือมีเครื่องมือโจมตีเผยแพร่แล้วหรือไม่
การเปิดรับความเสี่ยง	อุปกรณ์สามารถเข้าถึงจากภายนอก หรือเชื่อมต่อกับระบบอื่นในระดับใด
สิทธิที่ผู้โจมตีอาจได้รับ	สามารถดูภาพ เปลี่ยนค่าตั้ง ควบคุมระบบ หรือเข้าถึงระบบอื่นได้หรือไม่
ความสำคัญของระบบ	ระบบมีผลต่อภารกิจ ความปลอดภัย หรือบริการสำคัญเพียงใด
ความพร้อมของการแก้ไข	มี Patch, Update หรือมาตรการบรรเทาความเสี่ยงแล้วหรือไม่

ปัจจัย	ประเด็นที่ควรพิจารณา
ผลกระทบจากการปรับปรุง	การหยุดหรือปรับปรุงระบบจะกระทบต่อภารกิจหรือไม่

องค์กรสามารถกำหนดกรอบเวลาในการดำเนินการตามระดับความเสี่ยงและข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ของตนเอง

3.5.2 การเฝ้าระวังและการบันทึกเหตุการณ์

ผู้ที่ต้องพิจารณา: ผู้ติดตั้งหรือผู้รวมระบบควรตั้งค่าให้ระบบสามารถสร้างบันทึกเหตุการณ์ที่จำเป็นส่วนเจ้าของระบบหรือผู้ดูแลระบบควรกำหนดผู้รับผิดชอบในการตรวจสอบและตอบสนอง

การบันทึกเหตุการณ์ควรมีวัตถุประสงค์เพื่อสนับสนุนการตรวจจับความผิดปกติ การตรวจสอบย้อนหลัง และการสืบค้นเหตุการณ์ ไม่ควรเปิดการบันทึกข้อมูลจำนวนมากโดยไม่มีวัตถุประสงค์หรือไม่มีผู้รับผิดชอบในการนำข้อมูลไปใช้ เนื่องจากอาจเป็นการเพิ่มภาระ (เช่น พื้นที่การจัดเก็บข้อมูล) และเพิ่มความเสี่ยง (เช่น มีข้อมูลละเอียดอ่อนที่ผู้ไม่ประสงค์ดีอาจนำไปใช้ในทางที่ไม่เหมาะสมได้) โดยที่ไม่สมดุลกับประโยชน์ที่จะได้รับ

เหตุการณ์ที่ควรพิจารณาบันทึกตามความสามารถของระบบ ได้แก่

- การเข้าสู่ระบบและออกจากระบบ
- การเข้าสู่ระบบไม่สำเร็จ
- การเพิ่ม ลบ หรือเปลี่ยนแปลงบัญชีและสิทธิ
- การเปลี่ยนแปลงค่าตั้งระบบ
- การเปิดหรือใช้งานช่องทางการเข้าถึงจากระยะไกล
- การปรับปรุงเฟิร์มแวร์หรือซอฟต์แวร์
- การส่งออกข้อมูล
- การเปลี่ยนแปลงระยะเวลาเก็บรักษา
- กล้องหรืออุปกรณ์ไม่สามารถให้บริการ
- พื้นที่จัดเก็บหรือดิสก์เกิดความผิดปกติ
- การเปลี่ยนแปลงเวลาในระบบ
- การงัดแงะ การบดบัง หรือการเปลี่ยนมุมกล้อง
- การเชื่อมต่อกับปลายทางที่ผิดปกติ

มาตรการที่เกี่ยวข้องมีดังต่อไปนี้

มาตรการ	B	E	H
เปิดการบันทึกเหตุการณ์สำคัญที่ระบบรองรับ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ตั้งเวลาอุปกรณ์และระบบที่เกี่ยวข้องให้สอดคล้องกัน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

มาตรการ	B	E	H
ส่งบันทึกเหตุการณ์ไปยังระบบส่วนกลางตามความเหมาะสม	—	ควรพิจารณา	พึงปฏิบัติ
กำหนดการแจ้งเตือนสำหรับเหตุการณ์ที่มีความสำคัญ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
เฝ้าระวังการเชื่อมต่อออกไปยังปลายทางที่ผิดปกติ	—	ควรพิจารณา	พึงปฏิบัติ
กำหนดรอบการทบทวนบันทึกเหตุการณ์ตามความเสี่ยง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ป้องกันบันทึกเหตุการณ์จากการแก้ไขหรือลบโดยไม่ได้รับอนุญาต	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
กำหนดระยะเวลาเก็บรักษาบันทึกเหตุการณ์ตามกฎหมาย ข้อกำหนด และวัตถุประสงค์	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

ตัวอย่างเหตุการณ์ที่ควรพิจารณาแจ้งเตือน

เหตุการณ์	เหตุผลที่ควรพิจารณา
การเข้าสู่ระบบไม่สำเร็จจำนวนมาก	อาจเป็นการพยายามเดารหัสผ่านหรือโจมตีบัญชี
การเข้าสู่ระบบจากแหล่งที่มาหรือช่วงเวลาผิดปกติ	อาจเป็นการใช้ข้อมูลยืนยันตัวตนโดยไม่ได้รับอนุญาต
การเพิ่มบัญชีหรือสิทธิระดับสูง	อาจก่อให้เกิดสิทธิเกินความจำเป็น
การเปิดช่องทางการเข้าถึงจากระยะไกล	เพิ่มพื้นที่การโจมตีจากภายนอก
การเปลี่ยนค่าตั้งสำคัญ	อาจกระทบความมั่นคงปลอดภัยหรือการทำงานของระบบ
การส่งออกข้อมูลจำนวนมาก	อาจเป็นการใช้หรือเปิดเผยข้อมูลผิดวัตถุประสงค์
กล้องหลายตัวไม่สามารถให้บริการพร้อมกัน	อาจเกิดจากปัญหาเครือข่าย ไฟฟ้า หรือการโจมตี
พื้นที่จัดเก็บใกล้เต็มหรือดิสก์ผิดปกติ	อาจทำให้ข้อมูลไม่ถูกบันทึกตาม Retention
การเชื่อมต่อไปยังปลายทางที่ไม่ทราบที่มา	อาจเป็นพฤติกรรมผิดปกติหรือการเชื่อมต่อที่ไม่ได้รับอนุมัติ
การเปลี่ยนเวลาในระบบ	อาจกระทบความถูกต้องของหลักฐานและการตรวจสอบย้อนหลัง

ระยะเวลาการเก็บรักษาบันทึกเหตุการณ์

ระยะเวลาเก็บรักษาควรกำหนดจาก

ข้อกำหนดที่มีผลใช้บังคับ + วัตถุประสงค์ในการตรวจสอบ + ความเสี่ยง + ความสามารถในการจัดเก็บ

ไม่ควรกำหนดระยะเวลาเดียวสำหรับระบบ CCTV ทุกประเภทโดยอัตโนมัติ หากกฎหมายหรือข้อกำหนดที่เกี่ยวข้องมิได้กำหนดเช่นนั้น ไม่ควรเก็บรักษาบันทึกเหตุการณ์ไว้นานเกินจำเป็น หรือสั้นเกินไปควรเก็บตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้องกำหนด หรือตามความจำเป็น

3.5.3 รอบการตรวจสอบและการบำรุงรักษา

องค์กรควรกำหนดรอบการตรวจสอบโดยพิจารณาจากระดับความสำคัญของระบบ สภาพแวดล้อม อัตราการเปลี่ยนแปลง ประวัติความขัดข้อง และผลกระทบหากระบบไม่สามารถให้บริการได้ โดยมีรายการตรวจสอบเบื้องต้นดังนี้

รายการตรวจสอบ	ประเด็นที่ควรยืนยัน
สถานะของกล้อง	ออนไลน์ สามารถบันทึกภาพ และไม่มีช่วงข้อมูลขาดหายผิดปกติ
คุณภาพของภาพ	จุดโฟกัส มุมกล้อง แสง อินฟราเรด WDR และสิ่งบดบัง
ระยะเวลาเก็บรักษา	สามารถเรียกดูข้อมูลย้อนหลังได้ครบตามระยะเวลาที่กำหนด
พื้นที่จัดเก็บ	มีพื้นที่เพียงพอ ดิสก์ไม่มีความผิดปกติ และระบบแจ้งเตือนทำงาน
เฟิร์มแวร์และซอฟต์แวร์	เวอร์ชันยังได้รับการสนับสนุนและประเด็นช่องโหว่ได้รับการพิจารณา
บัญชีและสิทธิ	ผู้มีสิทธิยังมีความจำเป็น และไม่มีบัญชีที่ไม่ควรคงอยู่
บันทึกเหตุการณ์	มีการบันทึกและสามารถเรียกใช้ได้
การเข้าถึงจากระยะไกล	ช่องทางและบัญชียังคงเป็นไปตามที่ได้รับอนุมัติ
การสำรองและกู้คืน	การสำรองยังทำงานและสามารถกู้คืนได้ตามที่กำหนด
สภาพทางกายภาพ	ตู้ สาย กล้อง จุดยึด ระบบไฟสำรอง และสภาพแวดล้อมอยู่ในสภาพเหมาะสม
การตั้งค่าระบบ	ไม่มีการเปลี่ยนแปลงจากค่าฐานที่ได้รับอนุมัติโดยไม่มีการอนุมัติ
สถานะ EoL/EoS	มีการติดตามสถานะการสนับสนุนและแผนทดแทน

การกำหนดความถี่

ควรพิจารณาเพิ่มความถี่ในการตรวจสอบเมื่อ

- ระบบมีผลกระทบสูง
- มีประวัติขัดข้องหรือเหตุด้านความมั่นคงปลอดภัย
- อยู่ในสภาพแวดล้อมที่รุนแรง
- มีการเปลี่ยนแปลงค่าตั้งหรืออุปกรณ์บ่อย
- มีผู้ให้บริการหลายรายสามารถเข้าถึงระบบ
- มีกฎหมาย ข้อกำหนด หรือสัญญากำหนดรอบการตรวจสอบเฉพาะ

การเฝ้าระวังอัตโนมัติและการแจ้งเตือนสามารถช่วยลดภาระการตรวจสอบด้วยมือ แต่ไม่ควรใช้แทนการทบทวนโดยผู้รับผิดชอบทั้งหมด

3.5.4 การสำรองข้อมูล การกู้คืน และความต่อเนื่อง

ผู้ที่ต้องพิจารณา: เจ้าของระบบ ผู้ติดตั้ง และผู้ให้บริการตามขอบเขตความรับผิดชอบ

การสำรองข้อมูลของระบบ CCTV ไม่จำเป็นต้องหมายถึงการสำรองวิดีโอทั้งหมดในทุกกรณี แต่ควรเริ่มจากการระบุว่าองค์ประกอบใดมีความจำเป็นต่อการกู้คืนระบบและภารกิจ ข้อมูลหรือองค์ประกอบที่ควรพิจารณา ได้แก่

- ค่าตั้งระบบ
- รายการอุปกรณ์
- ค่าตั้งเครือข่าย
- ค่าตั้ง NVR/VMS
- ใบอนุญาตใช้งาน
- ใบรับรองและกุญแจเข้ารหัสที่จำเป็น
- โครงสร้างบัญชีและสิทธิในระดับที่เหมาะสม
- เอกสารแบบที่ติดตั้งจริง (As-built)
- ข้อมูลเหตุการณ์สำคัญ
- บันทึกเหตุการณ์ที่จำเป็นต่อการตรวจสอบ

มาตรการพื้นฐานที่เกี่ยวข้องมีดังต่อไปนี้

มาตรการ	B	E	H
สำรองค่าตั้งและข้อมูลที่จำเป็นต่อการกู้คืน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
แยกเก็บข้อมูลเหตุการณ์สำคัญจากระบบหลักเมื่อจำเป็น	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

มาตรการ	B	E	H
ทดสอบการกู้คืนตามระดับความเสี่ยง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ป้องกันข้อมูลสำรองจากการถูกลบหรือเข้ารหัสพร้อมกับระบบหลัก	—	ควรพิจารณา	พึงปฏิบัติ
พิจารณาการสำรองแบบออฟไลน์หรือแบบแก้ไขไม่ได้ (Immutable Backup) ตามความสำคัญ	—	ควรพิจารณา	พึงปฏิบัติ
กำหนดเป้าหมายการกู้คืน เช่น RTO/RPO เมื่อระบบมีความสำคัญต่อภารกิจ	—	ควรพิจารณา	พึงปฏิบัติ
จัดให้มีระบบไฟสำรองสำหรับองค์ประกอบที่จำเป็น	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้การบันทึกที่อุปกรณ์ปลายทางหรือกลไกเทียบเท่าเมื่อการขาดเครือข่ายมีผลกระทบสูง	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ

ข้อควรทราบ: การทำ RAID มีวัตถุประสงค์หลักเพื่อเพิ่มความทนทานของพื้นที่จัดเก็บต่อความเสียหายของดิสก์ มิใช่เพื่อการสำรองข้อมูล

3.5.5 การบริหารงานบำรุงรักษาและสัญญาบริการ

ผู้ที่ต้องพิจารณา: เจ้าของระบบเป็นผู้กำหนดขอบเขต ระดับบริการ และข้อกำหนดด้านความมั่นคงปลอดภัย ส่วนผู้ให้บริการหรือผู้รับจ้างดำเนินการและรายงานผลตามข้อตกลง

การบำรุงรักษาควรพิจารณาทั้งด้านความพร้อมใช้งานและความมั่นคงปลอดภัย ไม่ควรจำกัดเฉพาะการซ่อมแซมอุปกรณ์เมื่อเกิดความขัดข้อง ประเภทหลักของการบำรุงรักษามีดังต่อไปนี้

ประเภทการบำรุงรักษา	วัตถุประสงค์	ตัวอย่าง
การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance)	ลดโอกาสเกิดความขัดข้อง	ทำความสะอาด ตรวจจุมุม ตรวจสาย ทดสอบ UPS และตรวจสุขภาพพื้นที่จัดเก็บ
การบำรุงรักษาเชิงแก้ไข (Corrective Maintenance)	แก้ไขเมื่อเกิดปัญหา	เปลี่ยนอุปกรณ์ ซ่อมสาย หรือกู้คืนระบบหลังขัดข้อง
การบำรุงรักษาเชิงคาดการณ์ (Predictive Maintenance)	ใช้ข้อมูลเพื่อคาดการณ์ความเสียหาย	ตรวจ S.M.A.R.T. อุณหภูมิ แนวโน้มข้อผิดพลาด หรือความถี่ของการขาดการเชื่อมต่อ

ประเภทการบำรุงรักษา	วัตถุประสงค์	ตัวอย่าง
การบำรุงรักษาด้านความมั่นคงปลอดภัย (Security Maintenance)	ลดความเสี่ยงจากช่องโหว่และภัยคุกคาม	Patch, Firmware Update, Certificate Renewal, Account Review และ Hardening

3.5.5.1 องค์ประกอบของข้อตกลงบำรุงรักษา

ข้อตกลงบำรุงรักษาควรครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้

หัวข้อ	สิ่งที่ควรกำหนด
ขอบเขตอุปกรณ์	รุ่น จำนวน ตำแหน่ง และรายการที่อยู่ในความรับผิดชอบ
งานบำรุงรักษาเชิงป้องกันและเชิงแก้ไข	รายการงานและรอบการดำเนินการ
ระดับการให้บริการ (SLA)	เวลาตอบสนอง เวลากู้คืน และเวลาการแก้ไขตามระดับผลกระทบ
อะไหล่และอุปกรณ์ทดแทน	เงื่อนไขการสำรองและเปลี่ยนอุปกรณ์
เฟิร์มแวร์และช่องโหว่	ผู้รับผิดชอบในการติดตาม แจ้ง และดำเนินการ
การเข้าถึงจากระยะไกล	วิธีอนุมัติ ช่องทาง ระยะเวลา และการบันทึก
บัญชีของผู้ให้บริการ	บัญชีรายบุคคล สิทธิ ระยะเวลา และการเพิกถอน
การนำอุปกรณ์ออกนอกสถานที่	การจัดการข้อมูลและสื่อบันทึกก่อนส่งซ่อม
การรักษาความลับและการคุ้มครองข้อมูล	ขอบเขตการเข้าถึงและข้อกำหนดที่เกี่ยวข้อง
การสนับสนุนกรณีเกิดเหตุ	ผู้ประสานงาน วิธีติดต่อ และเวลาตอบสนอง
การรายงานผล	ใบงาน ผลการตรวจ ประเด็นความเสี่ยง และข้อเสนอแนะ
สถานะ EoL/EoS	การแจ้งล่วงหน้าและแผนทดแทน
การสิ้นสุดสัญญา	การคืนหรือเพิกถอนสิทธิ บัญชี เอกสาร ข้อมูล และสำเนาที่ผู้รับจ้างถือครอง

3.5.5.2 ตัวชี้วัดด้านการบำรุงรักษา

องค์กรควรมีการตั้งตัวชี้วัดด้านการบำรุงรักษาเพื่อให้ทราบว่าการบำรุงรักษามีประสิทธิภาพและเป็นไปตามข้อกำหนดที่เกี่ยวข้องหรือไม่ ค่าเป้าหมายควรกำหนดจากความสำคัญของระบบ ข้อตกลงระดับการ

ให้บริการ ความเสี่ยงที่องค์กรยอมรับได้ และข้อกำหนดที่เกี่ยวข้อง โดยมีแนวทางในการตั้งตัวชี้วัดด้านการบำรุงรักษาดังต่อไปนี้

ตัวชี้วัด	วิธีการวัด
ความพร้อมใช้งานของกล้อง (Camera Availability)	ร้อยละของเวลาที่กล้องสามารถให้บริการและบันทึกข้อมูลได้
ความครบถ้วนของข้อมูลย้อนหลัง	ตรวจว่าข้อมูลย้อนหลังครบตามระยะเวลาการเก็บรักษาที่กำหนด
เวลาเฉลี่ยในการกู้คืนหรือแก้ไข (Mean Time to Repair/Restore: MTTR)	ระยะเวลาตั้งแต่ตรวจพบหรือรับแจ้งจนระบบกลับมาให้บริการ
สัดส่วนอุปกรณ์ที่ยังได้รับการสนับสนุน	เปรียบเทียบทะเบียนทรัพย์สินกับสถานะ EoL/EoS
จำนวนอุปกรณ์ที่สิ้นสุดการสนับสนุนแต่ยังใช้งาน	ตรวจว่ามีการประเมินความเสี่ยงและแผนทดแทนหรือไม่
ความครบถ้วนของแผนบำรุงรักษาเชิงป้องกัน	งานที่ดำเนินการจริงเทียบกับแผน
ความครบถ้วนของการปรับปรุงด้านความมั่นคงปลอดภัย	รายการที่ได้รับการประเมินและดำเนินการตามระดับความเสี่ยง

3.5.6 การส่งซ่อมหรือส่งอุปกรณ์ออกนอกสถานที่

ก่อนส่งอุปกรณ์ที่มีสื่อจัดเก็บข้อมูลออกนอกการควบคุมขององค์กร ควรพิจารณา

- ถอดสื่อจัดเก็บออก หากสามารถดำเนินการได้
- ลบข้อมูลก่อนส่งตามความเหมาะสม
- เข้ารหัสสื่อจัดเก็บ หากยังจำเป็นต้องคงข้อมูลไว้
- กำหนดลำดับการครอบครองอุปกรณ์หรือหลักฐาน (Chain of Custody)
- ระบุผู้ส่งและผู้รับ
- กำหนดเงื่อนไขการรักษาความลับ
- ห้ามทำสำเนาข้อมูลโดยไม่ได้รับอนุญาต
- ตรวจสอบอุปกรณ์และค่าตั้งเมื่อได้รับคืน

3.6 ภัยคุกคาม สัญญาณผิดปกติ และการตอบสนองต่อเหตุการณ์

ผู้ที่ต้องพิจารณา: เจ้าของระบบเป็นผู้รับผิดชอบหลักในการกำกับดูแลและตัดสินใจ ส่วนผู้ติดตั้งหรือผู้ให้บริการควรสนับสนุนด้านเทคนิคตามขอบเขตสัญญา

ระบบ CCTV อาจเป็นทั้งเป้าหมายของการโจมตีและช่องทางในการเข้าถึงระบบอื่น ความเสี่ยงจึงไม่ได้จำกัดเพียงการสูญเสียภาพ แต่รวมถึงการเข้าควบคุมอุปกรณ์ การเปิดเผยหรือเปลี่ยนแปลงข้อมูล การหยุดชะงักของบริการ และการใช้ระบบ CCTV เป็นจุดเริ่มต้นในการโจมตีระบบอื่น

3.6.1 ตัวอย่างภัยคุกคาม

กลุ่มภัยคุกคาม	ตัวอย่าง
ข้อมูลยืนยันตัวตนและการพิสูจน์ตัวตน	ข้อมูลยืนยันตัวตนเริ่มต้นหรือรหัสผ่านอ่อนแอ การเดารหัสผ่าน การนำข้อมูลยืนยันตัวตนที่รั่วไหลมาใช้
ช่องโหว่ของผลิตภัณฑ์	ช่องโหว่ของเฟิร์มแวร์ ซอฟต์แวร์ หรือส่วนประกอบ
การเชื่อมต่อกับเครือข่ายภายนอกโดยไม่มีมาตรการควบคุมที่เหมาะสม	การเปิดระบบสู่อินเทอร์เน็ตหรือการเข้าถึงจากระยะไกลที่ไม่มีการควบคุมเพียงพอ
มัลแวร์	Malware, Botnet หรือ Ransomware
การใช้สิทธิในทางที่ไม่เหมาะสม	การใช้บัญชีสิทธิสูงผิดวัตถุประสงค์ หรือบัญชีผู้ให้บริการที่ไม่ได้เพิกถอน
การดัดแปลงทางกายภาพ	การถอด หมุน บดบัง หรือแก้ไขอุปกรณ์โดยไม่ได้รับอนุญาต
การเปลี่ยนค่าตั้งโดยไม่ได้รับอนุญาต	การเปลี่ยน Configuration ที่ส่งผลต่อความมั่นคงปลอดภัยหรือการบันทึก
การรั่วไหลของข้อมูล	การส่งออกหรือถ่ายโอนข้อมูลออกจากระบบโดยไม่ได้รับอนุญาต
ความเสี่ยงจากห่วงโซ่อุปทาน	การถูกโจมตีผ่านซอฟต์แวร์ ส่วนประกอบ ผู้ผลิต หรือผู้ให้บริการ

3.6.2 ตัวอย่างสัญญาณผิดปกติ

เหตุการณ์เหล่านี้อาจเป็นสัญญาณแสดงถึงความผิดปกติที่เกิดขึ้นและควรตรวจสอบและดำเนินการในส่วนที่เกี่ยวข้อง เช่น

- กล้องหรืออุปกรณ์เริ่มต้นใหม่โดยไม่มีเหตุผล
- ค่าตั้งระบบถูกเปลี่ยนโดยไม่ได้รับอนุญาต
- มีบัญชีใหม่หรือมีการเปลี่ยนสิทธิที่ไม่สามารถอธิบายได้
- มีการเข้าสู่ระบบไม่สำเร็จจำนวนมาก
- กล้องส่งข้อมูลไปยังปลายทางที่ไม่รู้จัก
- กล้องหลายตัวไม่สามารถให้บริการพร้อมกัน
- ข้อมูลย้อนหลังหายหรือถูกลบผิดปกติ
- พื้นที่จัดเก็บถูกเข้ารหัสหรือไม่สามารถเข้าถึงได้
- เฟิร์มแวร์หรือซอฟต์แวร์ถูกเปลี่ยนโดยไม่ทราบที่มา
- ผู้ดูแลระบบไม่สามารถเข้าใช้บัญชีได้
- ปริมาณการสื่อสารในเครือข่ายเพิ่มขึ้นผิดปกติ

3.6.3 กระบวนการตอบสนองต่อเหตุการณ์

เมื่อมีการตรวจพบและยืนยันเหตุการณ์ ควรมีการบันทึกแหล่งที่มาของการแจ้งเหตุและบันทึกเวลาที่ทราบเหตุ จากนั้นเริ่มกระบวนการตอบสนอง โดยควรสอดคล้องกับกระบวนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยขององค์กร และครอบคลุมอย่างน้อย 6 ขั้นตอนดังต่อไปนี้

ขั้นตอน	แนวทางดำเนินการ
1. จำกัดและควบคุมเหตุ (Contain)	จำกัดหรือปิดการเชื่อมต่อ แยกอุปกรณ์ ระงับบัญชีหรือช่องทางการเข้าถึงที่สงสัย และป้องกันไม่ให้เหตุขยายไปยังระบบอื่น
2. ประเมินเหตุ (Assess)	ระบุระบบ อุปกรณ์ บัญชี ข้อมูล ช่วงเวลา และขอบเขตผลกระทบ รวมถึงประเมินว่ามีข้อมูลส่วนบุคคลเกี่ยวข้องหรือไม่ พร้อมเก็บรักษาบันทึกเหตุการณ์และหลักฐานก่อนรีเซ็ตหรือแก้ไขอุปกรณ์
3. แก้ไขสาเหตุและช่องโหว่ (Remediate)	ติดตั้ง Patch เปลี่ยน Credential เพิกถอน Token/Certificate ลบ Malware ปิดช่องทางที่ไม่จำเป็น หรือคืนค่าตั้งที่มั่นคงปลอดภัย
4. กู้คืนระบบ (Recover)	กู้คืนจากแหล่งที่เชื่อถือได้ ตรวจสอบค่าตั้งและการทำงาน และเฝ้าระวังเป็นพิเศษภายหลังการกู้คืน

ขั้นตอน	แนวทางดำเนินการ
5. รายงานและสื่อสาร (Report)	รายงานต่อผู้รับผิดชอบ หน่วยงานภายใน หรือหน่วยงานภายนอกตามกฎหมาย ข้อกำหนด และสัญญาที่เกี่ยวข้อง
6. ทบทวนและปรับปรุง (Improve)	วิเคราะห์สาเหตุ ระบุช่องว่าง ปรับปรุงมาตรการ ความเสี่ยง ขั้นตอน และการอบรม

องค์กรควรพิจารณามาตรการอย่างน้อยดังต่อไปนี้

มาตรการ	B	E	H
กำหนดผู้รับผิดชอบและช่องทางแจ้งเหตุ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
สามารถแยกหรือจำกัดอุปกรณ์ที่สงสัยว่าถูกโจมตี	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
เก็บรักษาบันทึกเหตุการณ์และหลักฐานก่อน Reset เมื่อสามารถทำได้	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
มีขั้นตอนตอบสนองต่อเหตุการณ์	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ทดสอบหรือซ้อมกระบวนการตามระดับความเสี่ยง	—	ควรพิจารณา	พึงปฏิบัติ
เพิกถอน Credential, Session หรือสิทธิที่เกี่ยวข้องเมื่อจำเป็น	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ดำเนินการรายงานตามกฎหมายหรือข้อกำหนดที่ใช้บังคับ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ทบทวนเหตุการณ์ภายหลังการแก้ไข	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

3.7 การประเมินและยกระดับระบบเดิมที่ติดตั้งใช้งานแล้ว

ระบบ CCTV ที่ติดตั้งใช้งานมาเป็นระยะเวลานานอาจยังสามารถให้บริการได้ แต่ไม่รองรับมาตรการบางประการที่เหมาะสมกับความเสี่ยงในปัจจุบัน เช่น ไม่สามารถปรับปรุงเฟิร์มแวร์ ไม่มีบันทึกเหตุการณ์ ใช้บัญชีร่วมกัน ไม่รองรับการเข้ารหัส หรือผู้ผลิตยุติการสนับสนุนแล้ว

การตัดสินใจปรับปรุงหรือทดแทนระบบไม่ควรพิจารณาจากอายุของอุปกรณ์เพียงอย่างเดียว แต่ควรพิจารณาจากผลกระทบ ช่องว่าง ความเสี่ยง ความสามารถในการใช้มาตรการชดเชย และความเหมาะสมของต้นทุน

3.7.1 การสำรวจสภาพระบบเดิม

การสำรวจสภาพระบบเดิมควรครอบคลุมหัวข้ออย่างน้อยดังนี้

สิ่งที่ต้องสำรวจ	วิธีตรวจสอบ	ประเด็นที่เกี่ยวข้อง
ชนิดและสถาปัตยกรรมระบบ	ตรวจอุปกรณ์ สาย และการเชื่อมต่อ	สถาปัตยกรรมและเครือข่าย
จำนวนกล้อง รุ่น เวอร์ชัน และตำแหน่ง	สำรวจหน้างานและทะเบียนทรัพย์สิน	สินทรัพย์และการออกแบบ
คุณภาพของภาพจริง	ทดสอบตาม POR/DORI	คุณภาพของภาพ
ระยะเวลาเก็บรักษาจริง	ตรวจวันที่เก่าสุดที่ยังเรียกดูได้	การเก็บรักษาและพื้นที่จัดเก็บ
เฟิร์มแวร์และซอฟต์แวร์	ตรวจเวอร์ชันและสถานะการสนับสนุน	ช่องโหว่และ EoS
บัญชีและสิทธิ	ตรวจบัญชีและบทบาท	การควบคุมการเข้าถึง
การเปิดรับจากอินเทอร์เน็ตหรือระยะไกล	ตรวจ Port, NAT, P2P และ Remote Service	ความมั่นคงปลอดภัยเครือข่าย
การเข้ารหัส	ตรวจช่องทางบริหารและการรับส่งข้อมูล	การคุ้มครองข้อมูล
บันทึกเหตุการณ์	ตรวจประเภทเหตุการณ์ที่สามารถบันทึกได้	การเฝ้าระวัง
การสำรองและกู้คืน	ตรวจข้อมูลสำรองและผลการทดสอบกู้คืน	ความต่อเนื่อง
สภาพทางกายภาพ	ตรวจสภาพอุปกรณ์และการติดตั้ง	การบำรุงรักษา
สถานะ EoL/EoS	ตรวจข้อมูลจากผู้ผลิต	วงจรชีวิตผลิตภัณฑ์

3.7.2 การจำแนกสภาพระบบเดิม

องค์กรควรมีการกำหนดและจำแนกสภาพของระบบเดิมที่สอดคล้องกับบริบทขององค์กร ตัวอย่างแนวทางการจำแนกสภาพระบบเดิมดังแสดงต่อไปนี้

สถานะ	ลักษณะ	แนวทางหลัก
ก. ใช้งานต่อได้โดยปรับตั้งค่า	อุปกรณ์ยังได้รับการสนับสนุน และช่องว่างส่วนใหญ่เกิดจากค่าตั้งหรือกระบวนการ	ปรับความมั่นคงปลอดภัยและกระบวนการ
ข. ต้องปรับปรุงบางส่วน	มีบางองค์ประกอบไม่ตอบวัตถุประสงค์หรือมีความเสี่ยงสูง	ปรับปรุงหรือเปลี่ยนเฉพาะองค์ประกอบที่จำเป็น
ค. ต้องเปลี่ยนองค์ประกอบแกนกลาง	NVR/VMS/Network หรือส่วนสำคัญไม่รองรับมาตรการที่จำเป็น	เปลี่ยนองค์ประกอบหลัก โดยอาจคงอุปกรณ์บางส่วนไว้
ง. ต้องดำเนินการเร่งด่วน	พบช่องโหว่รุนแรง การเปิดรับอินเทอร์เน็ตหรือหลักฐานการถูกโจมตี	จำกัดความเสี่ยงก่อน แล้วดำเนินการปรับปรุงหรือเปลี่ยนผ่าน

3.7.3 เกณฑ์การตัดสินใจในการปรับปรุงระบบเดิม

เมื่อมีการประเมินสภาพระบบเดิมแล้ว องค์กรควรมีการดำเนินการปรับปรุงแก้ไขที่เหมาะสม โดยตัวอย่างสภาพที่พบและแนวทางที่ควรพิจารณาดำเนินการมีดังต่อไปนี้

สภาพที่พบ	แนวทางที่ควรพิจารณา
ยังใช้ข้อมูลยืนยันตัวตนเริ่มต้นหรือบัญชีร่วมกัน	แก้ไขค่าตั้งและข้อมูลยืนยันตัวตนโดยเร่งด่วน
เปิดระบบสู่อินเทอร์เน็ตโดยไม่มีการควบคุมเพียงพอ	จำกัดหรือปิดการเชื่อมต่อ และออกแบบการเข้าถึงจากระยะไกลใหม่
ระยะเวลาเก็บรักษาไม่ครบ	เพิ่มพื้นที่จัดเก็บหรือปรับค่าตั้ง
คุณภาพของภาพไม่ตอบ POR/DORI	ปรับมุม เลนส์ แสง หรือเปลี่ยนเฉพาะจุด
สมรรถนะกลางคืนหรือ WDR ไม่เพียงพอ	ปรับแสง ตำแหน่ง หรือค่าตั้งก่อนพิจารณาเปลี่ยนอุปกรณ์
NVR/VMS ไม่รองรับการแบ่งสิทธิ บันทึกเหตุการณ์หรือการเข้ารหัสที่จำเป็น	เปลี่ยนระบบแกนกลางหรือเพิ่มชั้นควบคุม

สภาพที่พบ	แนวทางที่ควรพิจารณา
ผลิตภัณฑ์สิ้นสุดการสนับสนุนและมีช่องโหว่ที่ไม่สามารถแก้ไข	ใช้มาตรการชดเชยและจัดทำแผนทดแทน
บริการ P2P หรือ Cloud ไม่สามารถประเมินการควบคุมได้เพียงพอ	ทบทวนบริการ สถาปัตยกรรม หรือผู้ให้บริการ
หลายองค์ประกอบไม่ตอบค่าตั้งต้นด้านความมั่นคงปลอดภัยและต้นทุนแก้ไขสูง	พิจารณาการทดแทนหรือย้ายระบบ

3.7.4 อายุการใช้งานและการวางแผนทดแทน

อายุการใช้งานสามารถใช้เป็นข้อมูลประกอบการวางแผนงบประมาณ แต่ไม่ควรใช้เป็นเกณฑ์ให้เปลี่ยนอุปกรณ์โดยอัตโนมัติ

เกณฑ์ที่ควรพิจารณาร่วมกัน ได้แก่

- สถานะสิ้นสุดการสนับสนุน
- ความสามารถในการรับการปรับปรุงด้านความมั่นคงปลอดภัย
- การเสื่อมสภาพของฮาร์ดแวร์
- สมรรถนะไม่ตอบวัตถุประสงค์
- ความพร้อมของอะไหล่
- อัตราการขัดข้อง
- ความสามารถในการทำงานร่วมกับระบบอื่น
- ต้นทุนการบำรุงรักษา
- ความเสี่ยงคงเหลือ

3.7.5 มาตรการชดเชย

ในกรณีที่พบความเสี่ยงที่จำเป็นต้องได้รับการแก้ไขยังไม่สามารถแก้ไขหรือทดแทนระบบได้ มาตรการชดเชยสามารถนำมาใช้เพื่อลดความเสี่ยงในช่วงเวลาหนึ่งชั่วคราวได้ แต่ควรมีผู้รับผิดชอบ กำหนดระยะเวลา และทบทวนความเพียงพออย่างต่อเนื่อง

มาตรการ	B	E	H
แยกระบบเดิมออกจากเครือข่ายอื่น	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
จำกัดหรือปิดการเปิดรับอินเทอร์เน็ตและการเข้าถึงจากระยะไกลที่ไม่จำเป็น	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

มาตรการ	B	E	H
จำกัดแหล่งที่สามารถเข้าถึงส่วนบริหารจัดการ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ใช้ Gateway, VMS หรือ Firewall เป็นชั้นควบคุมเพิ่มเติม	—	ควรพิจารณา	พึงปฏิบัติ
ใช้บันทึกเหตุการณ์จากระบบอื่นเพื่อชดเชยข้อจำกัดของอุปกรณ์	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
เพิ่มมาตรการควบคุมทางกายภาพ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
เพิ่มความถี่ในการตรวจสอบ	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
จำกัดจำนวนผู้มีสิทธิและระยะเวลาในการเข้าถึง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
บันทึกการยอมรับความเสี่ยง พร้อมผู้อนุมัติและวันที่ทบทวน	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

ทั้งนี้มาตรการชดเชยควรถือเป็นกลไกบริหารความเสี่ยง ไม่ควรถูกใช้เพื่อเลื่อนการแก้ไขข้อบกพร่องที่ทราบอยู่แล้วออกไปโดยไม่มีกำหนด

3.7.6 แผนการเปลี่ยนผ่าน

ในกรณีที่เห็นควรปรับปรุงระบบเดิม ควรจัดลำดับจากระดับความเสี่ยงและผลกระทบ มากกว่าความสะดวกในการดำเนินงาน โดยมีแนวทางการแบ่งระยะการดำเนินการดังต่อไปนี้

ระยะ	วัตถุประสงค์	ตัวอย่างการดำเนินการ
ระยะที่ 1 ลดความเสี่ยงเร่งด่วน	ลดช่องโหว่หรือการเปิดรับที่มีความเสี่ยงสูง	เปลี่ยน Credential ปิด Internet Exposure ยกเลิกบัญชีที่ไม่จำเป็น
ระยะที่ 2 ปรับค่าตั้งต้นด้านความมั่นคงปลอดภัย	ให้ระบบมีมาตรการพื้นฐานที่เหมาะสม	Segmentation, Logging, Time Synchronization, RBAC
ระยะที่ 3 ปรับปรุงองค์ประกอบสำคัญ	เปลี่ยนองค์ประกอบที่ไม่ตอบภารกิจหรือสิ้นสุดการสนับสนุน	กล้อง พื้นที่จัดเก็บ NVR/VMS หรืออุปกรณ์เครือข่าย
ระยะที่ 4 ปรับสถาปัตยกรรมระยะยาว	รองรับความต้องการด้านความมั่นคงปลอดภัยและการบริหารในอนาคต	สถาปัตยกรรม VMS การเฝ้าระวัง การสำรองและกู้คืน และการเชื่อมต่อ

3.7.7 ข้อควรพิจารณาด้านข้อมูลส่วนบุคคลเมื่อปรับปรุงหรือเปลี่ยนระบบ

เมื่อปรับปรุงหรือเปลี่ยนระบบ ควรพิจารณาอย่างน้อยว่า

- ข้อมูลในระบบเดิมยังต้องได้รับการคุ้มครองจนกว่าจะลบหรือทำลายอย่างเหมาะสม
- ไม่ควรย้ายข้อมูลเก่าทั้งหมดเข้าสู่ระบบใหม่โดยอัตโนมัติ หากข้อมูลเกินระยะเวลาเก็บรักษาที่กำหนด
- การเปลี่ยนผู้ให้บริการอาจทำให้บทบาทด้านการประมวลผลข้อมูลเปลี่ยนแปลง
- ควรทบทวนสัญญา ข้อตกลงประมวลผลข้อมูล และเอกสารที่เกี่ยวข้องตามความจำเป็น
- การเพิ่มจำนวนกล้องหรือเปลี่ยนมุมควรทบทวนวัตถุประสงค์ ความจำเป็น และความได้สัดส่วน
- หากระบบใหม่เพิ่มความสามารถด้าน AI หรือข้อมูลชีวมิติ ควรพิจารณาประเด็นที่เกี่ยวข้องดังแนะนำใน แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย เพิ่มเติม

3.8 การเลิกใช้อุปกรณ์และการจัดการข้อมูล

การเลิกใช้อุปกรณ์ไม่ควรถือว่าสิ้นสุดเพียงเมื่อถอดกล้อง เครื่องบันทึก หรืออุปกรณ์ออกจากระบบ เนื่องจากอุปกรณ์อาจยังคงมีข้อมูลภาพ บันทึกเหตุการณ์ ค่าตั้ง ข้อมูลยืนยันตัวตน ใบรับรอง กุญแจเข้ารหัส Token หรือข้อมูลการเชื่อมต่อกับบริการภายนอก การเลิกใช้งานควรครอบคลุมทั้งการจัดการข้อมูล การเพิกถอนสิทธิ การยกเลิกการเชื่อมต่อ การปรับปรุงทะเบียนทรัพย์สิน และการจัดทำหลักฐานตามระดับความเสี่ยง

มาตรการที่ควรพิจารณาดำเนินการควรมีอย่างน้อยดังต่อไปนี้

มาตรการ	B	E	H
ระบุข้อมูลและข้อมูลยืนยันตัวตนที่ยังอยู่ในอุปกรณ์	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ย้ายหรือเก็บรักษาเฉพาะข้อมูลที่ยังมีความจำเป็น	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ลบหรือทำลายข้อมูลตามความเสี่ยงและประเภทสื่อ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
คืนค่าโรงงานภายหลังจัดการข้อมูลที่จำเป็นแล้ว เมื่อเหมาะสม	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
ถอนอุปกรณ์ออกจาก Cloud, VMS หรือระบบบริหารจัดการ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
เพิกถอนบัญชี ใบรับรอง กุญแจ และ Token ที่เกี่ยวข้อง	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
ปรับปรุงทะเบียนทรัพย์สินและแผนผังเครือข่าย	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
จัดทำหลักฐานการลบหรือทำลายตามระดับความเสี่ยง	ควรพิจารณา	ควรพิจารณา	พึงปฏิบัติ
ควบคุมการส่งอุปกรณ์ออกซ่อมหรือออกนอกสถานที่	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ

3.8.1 หลักการจัดการข้อมูลก่อนเลิกใช้งาน

ก่อนลบหรือทำลายข้อมูล ควรพิจารณาอย่างน้อย

1. มีข้อมูลใดที่ยังอยู่ภายใต้ระยะเวลาเก็บรักษาหรือการระงับการลบชั่วคราวหรือไม่
2. มีข้อมูลใดที่ต้องย้ายไปยังระบบใหม่หรือไม่
3. มีข้อมูลที่ต้องเก็บรักษาเพื่อการสอบสวน ข้อพิพาท หรือข้อกำหนดอื่นหรือไม่
4. อุปกรณ์จะถูกนำกลับมาใช้ ขาย คืนผู้ให้บริการ ส่งซ่อม หรือทำลาย
5. วิธีการลบหรือทำลายเหมาะสมกับประเภทของสื่อจัดเก็บหรือไม่

3.8.2 หลักฐานการเลิกใช้งาน

สำหรับระบบที่มีความสำคัญ ควรพิจารณาจัดเก็บหลักฐานอย่างเหมาะสม เช่น

รายการ	ตัวอย่างข้อมูล
การระบุอุปกรณ์	รหัสทรัพย์สิน หมายเลขประจำเครื่อง รุ่น
วันที่	วันที่เลิกใช้ ลบ หรือทำลาย
การอนุมัติ	ผู้อนุมัติการเลิกใช้งาน
วิธีดำเนินการ	การลบ การทำลาย การคืนผู้ให้บริการ หรือการนำกลับมาใช้
ผู้ดำเนินการ	ผู้ดำเนินการและผู้รับรอง
การเพิกถอนสิทธิ	บัญชี Certificate, Key, Token หรือ Cloud Registration
หลักฐานประกอบ	ใบรับรองการทำลายหรือหลักฐานอื่นตามความเหมาะสม

สรุปหลักการของบทที่ 3

การรักษาความมั่นคงปลอดภัยของระบบ CCTV ควรดำเนินการอย่างต่อเนื่องตลอดวงจรชีวิต ตั้งแต่การออกแบบและเลือกอุปกรณ์ การติดตั้ง การใช้งาน การบำรุงรักษาและเฝ้าระวัง การจัดการช่องโหว่และเหตุการณ์ ตลอดจนการปรับปรุงระบบเดิมและการเลิกใช้งาน โดยมาตรการที่เลือกใช้ควรสัมพันธ์กับวัตถุประสงค์ ผลกระทบ และระดับความเสี่ยงของระบบ

มาตรการทางเทคนิคควรถูกนำมาใช้ร่วมกับมาตรการด้านบุคลากร กระบวนการ และการกำกับดูแล โดยไม่ควรพึ่งพาเทคโนโลยีหรือมาตรการใดเพียงอย่างเดียว และควรมีหลักฐานเพียงพอเพื่อยืนยันว่าระบบยังคงทำงานและได้รับการควบคุมตามที่กำหนด

บทที่ 4 การจัดซื้อจัดจ้าง

การรักษาความมั่นคงปลอดภัยของระบบ CCTV ควรเริ่มตั้งแต่การกำหนดความต้องการและข้อกำหนดในการจัดซื้อจัดจ้าง ไม่ควรรอให้ระบบติดตั้งเสร็จแล้วจึงเพิ่มมาตรการด้านความมั่นคงปลอดภัยภายหลัง เนื่องจากความสามารถบางประการ เช่น การควบคุมบัญชีและสิทธิ การบันทึกเหตุการณ์ การปรับปรุงเฟิร์มแวร์ การจัดการช่องโหว่ การเข้ารหัส หรือการสนับสนุนตลอดวงจรชีวิต ขึ้นอยู่กับความสามารถของผลิตภัณฑ์และผู้ให้บริการตั้งแต่ต้น

การจัดซื้อจัดจ้างจึงควรพิจารณาร่วมกันทั้งด้านความเหมาะสมกับวัตถุประสงค์ สมรรถนะ ความมั่นคงปลอดภัย ความเป็นส่วนตัว ความสามารถในการบำรุงรักษา ความน่าเชื่อถือของผู้ผลิตและผู้ให้บริการ ความมั่นคงปลอดภัยของห่วงโซ่อุปทาน ความสามารถในการทำงานร่วมกับระบบอื่น และความสามารถในการย้าย เปลี่ยน หรือยุติบริการในอนาคต

ข้อกำหนดควรเขียนในลักษณะเป็นกลางด้านผู้ผลิตและเทคโนโลยี และสามารถตรวจสอบได้ โดยมุ่งกำหนด ผลลัพธ์ด้านความมั่นคงปลอดภัยที่ต้องการ มากกว่าการกำหนดยี่ห้อ ผลิตภัณฑ์ หรือเทคโนโลยีเฉพาะโดยไม่มีเหตุผลรองรับ

4.1 ข้อกำหนดด้านความมั่นคงปลอดภัยในการจัดซื้อ

ผู้ที่ต้องพิจารณา: เจ้าของระบบหรือผู้จัดซื้อเป็นผู้กำหนดความต้องการและเกณฑ์ในข้อกำหนดการจัดซื้อหรือ TOR ส่วนผู้เสนอราคา ผู้ติดตั้ง หรือผู้รวมระบบมีหน้าที่แสดงความสามารถและหลักฐานให้สอดคล้องกับข้อกำหนด

ข้อกำหนดในการจัดซื้อควรสัมพันธ์กับระดับความสำคัญ B/E/H ตามบทที่ 2 และผลการประเมินความเสี่ยง ข้อกำหนดที่กำหนดไว้ควรสามารถตรวจสอบได้ในขั้นตอนพิจารณาข้อเสนอ การทดสอบ หรือการตรวจรับ ไม่ควรใช้ถ้อยคำกว้าง เช่น “ระบบต้องมีความมั่นคงปลอดภัยสูง” โดยไม่มีเกณฑ์หรือหลักฐานที่สามารถตรวจสอบได้ ควรกำหนดข้อกำหนดที่ต้องการให้ชัดเจน เช่น “ระบบต้องสามารถกำหนดสิทธิผู้ใช้งานตามบทบาท และแยกสิทธิการดูภาพ การค้นหา การส่งออกข้อมูล และการบริหารระบบได้ โดยผู้เสนอราคาต้องแสดงเอกสารทางเทคนิคหรือสาธิตการทำงาน และต้องสามารถทดสอบได้ก่อนตรวจรับ”

4.1.1 ข้อกำหนดทั่วไปด้านความมั่นคงปลอดภัย

ข้อกำหนดควรครอบคลุมตามความเกี่ยวข้องทั้ง ผลิตภัณฑ์ ระบบ ผู้ผลิต ผู้ให้บริการ และบริการภายนอก โดยระดับของข้อกำหนดและหลักฐานควรสัมพันธ์กับผลกระทบและความเสี่ยง

4.1.1.1. บัญชี การพิสูจน์ตัวตน และการควบคุมสิทธิ

ประเด็น	ข้อกำหนดที่ควรพิจารณา
ข้อมูลยืนยันตัวตนเริ่มต้น	ไม่ใช้ข้อมูลยืนยันตัวตนเริ่มต้นแบบเดียวกันในอุปกรณ์จำนวนมากจนก่อให้เกิดความเสี่ยง และสามารถกำหนดข้อมูลยืนยันตัวตนใหม่ก่อนใช้งาน
บัญชีผู้ใช้งาน	สามารถสร้างบัญชีที่ระบุตัวผู้ใช้งานได้
การแบ่งสิทธิ	สามารถแยกสิทธิตามบทบาท เช่น ดูภาพ ค้นหา ส่งออก และบริหารระบบ
บัญชีที่ไม่ใช้งาน	สามารถปิดหรือลบบัญชีที่ไม่จำเป็น
บัญชีสิทธิสูง	สามารถจำกัดและตรวจสอบการใช้บัญชีผู้ดูแลระบบ
MFA	รองรับการพิสูจน์ตัวตนหลายปัจจัยสำหรับบัญชีหรือช่องทางที่มีความสำคัญตามความเสี่ยง
บัญชีผู้ให้บริการ	สามารถกำหนดสิทธิ ระยะเวลา และเพิกถอนบัญชีของผู้ให้บริการภายนอก
Credential/Session	สามารถเปลี่ยนหรือเพิกถอนข้อมูลยืนยันตัวตน Session หรือ Token เมื่อจำเป็น

สำหรับระบบระดับ E หรือ H ควรพิจารณาความสามารถในการกำหนดสิทธิแบบอิงบทบาท (Role-Based Access Control: RBAC) และการเชื่อมต่อกับระบบบริหารตัวตนของผู้ใช้งานในองค์กรตามความเหมาะสม

4.1.1.2. การตั้งค่าที่มั่นคงปลอดภัย

ผลิตภัณฑ์และระบบควรสามารถตั้งค่าให้ลดฟังก์ชันและบริการที่ไม่จำเป็น และควบคุมการเปลี่ยนแปลงค่าตั้งได้อย่างเหมาะสม

ประเด็น	ข้อกำหนดที่ควรพิจารณา
พอร์ตและบริการ	สามารถปิดพอร์ต บริการ หรือฟังก์ชันที่ไม่จำเป็น
ส่วนบริหารจัดการ	รองรับช่องทางบริหารจัดการที่มีการป้องกันข้อมูลอย่างเหมาะสม
การเข้าถึงจากภายนอก	ไม่จำเป็นต้องเปิดกล้องหรือส่วนบริหารจัดการสู่อินเทอร์เน็ตโดยตรง
การเข้าถึงจากระยะไกล	สามารถจำกัดหรือปิด Remote Access ได้
แหล่งที่มาของการบริหาร	สามารถจำกัดเครือข่ายหรือแหล่งที่สามารถเข้าถึงส่วนบริหาร
การสำรองค่าตั้ง	สามารถสำรองและกู้คืนค่าตั้งสำคัญ

ประเด็น	ข้อกำหนดที่ควรพิจารณา
เวลา	รองรับการตั้งเวลาให้สอดคล้องกับแหล่งเวลาที่เชื่อถือได้
ค่าฐาน	สามารถจัดทำหรือบันทึกค่าตั้งฐานเพื่อใช้ตรวจสอบการเปลี่ยนแปลงภายหลัง

หากระบบใช้บริการ P2P บริการคลาวด์ หรือบริการเชื่อมต่อของผู้ผลิต ควรสามารถระบุ ปิด หรือควบคุมการใช้งานดังกล่าวได้อย่างชัดเจน

4.1.1.3. การบันทึกเหตุการณ์และการเฝ้าระวัง

ระบบควรสามารถบันทึกเหตุการณ์ที่จำเป็นต่อการตรวจสอบตามระดับความเสี่ยง เช่น

- การเข้าสู่ระบบและการเข้าสู่ระบบไม่สำเร็จ
- การเพิ่ม ลบ หรือเปลี่ยนบัญชีและสิทธิ
- การเปลี่ยนค่าตั้งระบบ
- การเปิดหรือใช้การเข้าถึงจากระยะไกล
- การส่งออกข้อมูล
- การปรับปรุงระบบ
- การทำงานผิดปกติของกล้องหรือพื้นที่จัดเก็บ

สำหรับระบบระดับ E หรือ H ควรพิจารณาความสามารถในการส่งบันทึกเหตุการณ์ไปยังระบบส่วนกลาง รวมถึงความสามารถในการป้องกันบันทึกเหตุการณ์จากการแก้ไขหรือลบโดยไม่ได้รับอนุญาต

4.1.1.4. การปรับปรุงด้านความมั่นคงปลอดภัยและการบริหารช่องโหว่

ผู้ผลิตหรือผู้ให้บริการควรสามารถแสดงให้เห็นว่ามีกระบวนการติดตาม รับแจ้ง ประเมิน แก้ไข และสื่อสารเกี่ยวกับช่องโหว่ของผลิตภัณฑ์ตลอดระยะเวลาที่ผลิตภัณฑ์ยังได้รับการสนับสนุน

การบริหารช่องโหว่ไม่ควรหมายถึงเพียงการจัดให้มีไฟล์ปรับปรุงหรือแพตช์ (Patch) เมื่อเกิดปัญหา แต่ควรครอบคลุมตั้งแต่การรับทราบช่องโหว่ การประเมินว่าผลิตภัณฑ์หรือรุ่นใดได้รับผลกระทบ การพัฒนาและทดสอบวิธีแก้ไข ตลอดจนการแจ้งผู้ใช้งานเกี่ยวกับผลกระทบและแนวทางดำเนินการ

องค์กรควรพิจารณากำหนดข้อกำหนดในการจัดซื้ออย่างน้อยดังนี้

ประเด็น	ข้อกำหนดที่ควรพิจารณา
ช่องทางรับแจ้งช่องโหว่	ผู้ผลิตควรมีช่องทางที่ชัดเจนสำหรับรับแจ้งช่องโหว่จากผู้ใช้งาน ผู้ให้บริการ นักวิจัย หรือบุคคลภายนอก
การประเมินผลกระทบ	สามารถระบุได้ว่าช่องโหว่ส่งผลต่อผลิตภัณฑ์ รุ่น หรือเวอร์ชันใด และมีผลกระทบด้านใด

ประเด็น	ข้อกำหนดที่ควรพิจารณา
การแก้ไขหรือบรรเทาความเสี่ยง	มีการจัดทำแพตช์ การปรับปรุงเฟิร์มแวร์ มาตรการตั้งค่าชั่วคราว หรือมาตรการลดความเสี่ยงอื่นตามความเหมาะสม
การแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Advisory)	มีช่องทางเผยแพร่ข้อมูลเกี่ยวกับช่องโหว่ ผลิตภัณฑ์ที่ได้รับผลกระทบ วิธีแก้ไข และข้อควรดำเนินการ
การปรับปรุงด้านความมั่นคงปลอดภัย (Security Update)	สามารถเผยแพร่ ติดตั้ง และตรวจสอบการปรับปรุงได้อย่างเหมาะสม
กรณียังไม่มีแพตช์	มีคำแนะนำเกี่ยวกับมาตรการบรรเทาความเสี่ยง เช่น การปิดฟังก์ชัน การจำกัดการเชื่อมต่อ หรือการเพิ่มมาตรการเฝ้าระวัง
การสนับสนุนตลอดวงจรชีวิต	มีข้อมูลเกี่ยวกับระยะเวลาที่ผลิตภัณฑ์จะได้รับการแก้ไขช่องโหว่และการปรับปรุงด้านความมั่นคงปลอดภัย
สถานะ EoL/EoS	แจ้งสถานะสิ้นสุดอายุผลิตภัณฑ์ (End of Life: EoL) และสิ้นสุดการสนับสนุน (End of Support: EoS) พร้อมวันที่และผลกระทบที่เกี่ยวข้อง

ผู้ผลิตอาจมี ทีมตอบสนองเหตุด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ (Product Security Incident Response Team: PSIRT) หรือใช้ทีม หน่วยงาน หรือกระบวนการอื่นที่สามารถทำหน้าที่ในการรับแจ้ง วิเคราะห์ ประสานงาน แก้ไข และสื่อสารช่องโหว่ได้อย่างเหมาะสม

มาตรฐาน **ISO/IEC 29147** สามารถใช้เป็นกรอบอ้างอิงด้านการเปิดเผยช่องโหว่อย่างประสานงาน (Coordinated Vulnerability Disclosure: CVD) และ **ISO/IEC 30111** สามารถใช้เป็นกรอบอ้างอิงด้านกระบวนการจัดการช่องโหว่ของผลิตภัณฑ์ตามความเหมาะสม

4.1.1.5. ความถูกต้องและความน่าเชื่อถือของซอฟต์แวร์และเฟิร์มแวร์

ผลิตภัณฑ์ควรมีกลไกที่ช่วยให้องค์กรสามารถตรวจสอบได้ว่า ซอฟต์แวร์หรือเฟิร์มแวร์ที่นำมาติดตั้งหรือปรับปรุงมาจากแหล่งที่เชื่อถือได้ และไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาตระหว่างกระบวนการแจกจ่ายหรือติดตั้ง

ประเด็นที่ควรพิจารณา ได้แก่

- สามารถตรวจสอบแหล่งที่มาของไฟล์ปรับปรุงได้
- สามารถตรวจสอบความถูกต้องครบถ้วนของไฟล์ก่อนการติดตั้ง
- ระบบไม่ยอมรับเฟิร์มแวร์หรือซอฟต์แวร์ที่ไม่ผ่านการตรวจสอบตามกลไกที่กำหนด
- มีกระบวนการป้องกันหรือตรวจจับการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต

- มีวิธีกู้คืนหรือย้อนกลับเมื่อการปรับปรุงไม่สำเร็จตามความเหมาะสม

กลไกที่ใช้สามารถแตกต่างกันตามสถาปัตยกรรม เช่น ลายมือชื่อดิจิทัล (Digital Signature) การตรวจสอบด้วยวิธีการเข้ารหัส (Cryptographic Verification) หรือ การเริ่มต้นระบบอย่างมั่นคงปลอดภัย (Secure Boot)

สำหรับระบบที่มีความสำคัญหรือความเสี่ยงสูง อาจพิจารณาใช้กลไกรากฐานความเชื่อมั่นจากฮาร์ดแวร์ (Hardware-based Root of Trust) หรือกลไกที่ให้ระดับความเชื่อมั่นเทียบเท่า เพื่อสนับสนุนการตรวจสอบความถูกต้องของกระบวนการเริ่มต้นระบบ การปกป้องกุญแจเข้ารหัส หรือการยืนยันความน่าเชื่อถือของซอฟต์แวร์และเฟิร์มแวร์ ทั้งนี้ แนวปฏิบัตินี้มิได้กำหนดให้ต้องใช้เทคโนโลยีใดเทคโนโลยีหนึ่งโดยเฉพาะ เช่น Trusted Platform Module (TPM) หรือ Secure Element

การเลือกใช้กลไกดังกล่าวควรพิจารณาตามระดับความสำคัญของระบบ ผลกระทบที่อาจเกิดขึ้น ความเสี่ยง สถาปัตยกรรม และความสามารถของอุปกรณ์ โดยแนวปฏิบัตินี้ไม่กำหนดให้ต้องใช้เทคโนโลยีใดเพียงรูปแบบเดียว หากผู้ผลิตสามารถแสดงได้ว่ากลไกที่นำมาใช้ให้ระดับความเชื่อมั่นที่เหมาะสมต่อแหล่งที่มา ความถูกต้องครบถ้วน และความน่าเชื่อถือของซอฟต์แวร์หรือเฟิร์มแวร์

4.1.1.6. การเข้ารหัสและการคุ้มครองข้อมูล

ระบบ CCTV มีข้อมูลหลายประเภทที่อาจต้องได้รับการคุ้มครอง เช่น ภาพและวิดีโอ ข้อมูลยืนยันตัวตน บันทึกเหตุการณ์ ค่าตั้งระบบ และข้อมูลที่ถูกส่งออกจากระบบ ดังนั้น การกำหนดข้อกำหนดด้านการเข้ารหัสควรพิจารณาจากลักษณะข้อมูล ช่องทางการรับส่ง และระดับความเสี่ยง

องค์กรควรพิจารณาอย่างน้อยดังนี้

ประเด็น	สิ่งที่ควรพิจารณา
การบริหารระบบ	ช่องทางเข้าสู่ส่วนบริหารจัดการควรได้รับการป้องกันข้อมูลระหว่างส่ง เช่น การใช้ TLS หรือกลไกที่ให้ผลเทียบเท่า
การรับส่งวิดีโอ	ควรประเมินว่าช่องทางใดมีความเสี่ยงและจำเป็นต้องป้องกันการดักรับหรือแก้ไขข้อมูล
ข้อมูลที่จัดเก็บ	สำหรับระบบหรือข้อมูลที่มีผลกระทบสูง ควรพิจารณาการเข้ารหัสข้อมูลขณะจัดเก็บตามความเหมาะสม
ข้อมูลที่ส่งออก	ไฟล์หรือสื่อที่นำออกจากระบบควรได้รับการป้องกันตามความเสี่ยง โดยเฉพาะเมื่อส่งผ่านบุคคลหรือช่องทางภายนอก
ใบรับรองดิจิทัล (Digital Certificate)	ควรกำหนดผู้รับผิดชอบ การออก การต่ออายุ การเปลี่ยน และการเพิกถอน

ประเด็น	สิ่งที่ควรพิจารณา
กุญแจเข้ารหัส (Cryptographic Key)	ควรกำหนดว่าใครเป็นผู้ควบคุมกุญแจและสามารถเข้าถึงได้ภายใต้เงื่อนไขใด

4.1.1.7. คุณภาพของภาพและสมรรถนะของระบบ

คุณภาพของระบบ CCTV ไม่ควรประเมินจากจำนวนพิกเซลหรือความละเอียดของกล้องเพียงอย่างเดียว เนื่องจากกล้องที่มีความละเอียดสูงอาจยังไม่สามารถให้ภาพที่เหมาะสมกับวัตถุประสงค์ได้ หากตำแหน่งติดตั้ง ระยะ มุมมอง เลนส์ สภาพแสง การเคลื่อนไหว หรือการบีบอัดข้อมูลไม่เหมาะสม

ดังนั้น ข้อกำหนดในการจัดซื้อควรเริ่มจาก ความต้องการเชิงปฏิบัติการรายจุด (Point Operational Requirements: POR) ซึ่งระบุว่าภาพจากแต่ละจุดต้องสามารถใช้ทำอะไรได้ แล้วจึงกำหนดคุณลักษณะและเกณฑ์ตรวจรับที่สามารถพิสูจน์ได้

ตัวอย่างประเด็นที่ควรพิจารณา ได้แก่

ประเด็น	ความหมายและสิ่งที่ควรกำหนด
ระดับ DORI	กำหนดว่าภาพในแต่ละจุดต้องใช้เพื่อการตรวจพบ (Detection) การสังเกต (Observation) การจดจำ (Recognition) หรือการระบุตัว (Identification) ตามวัตถุประสงค์
ความหนาแน่นของพิกเซล (Pixel Density)	จำนวนพิกเซลที่ครอบคลุมเป้าหมายในพื้นที่จริง เพื่อช่วยประเมินว่าภาพมีรายละเอียดเพียงพอต่อระดับ DORI ที่ต้องการหรือไม่
พื้นที่ครอบคลุมของภาพ (Field of View)	ขอบเขตพื้นที่ที่กล้องต้องครอบคลุม โดยไม่กว้างหรือแคบจนไม่ตอบวัตถุประสงค์
ระยะและเลนส์	เลนส์และระยะติดตั้งควรทำให้เป้าหมายมีขนาดและรายละเอียดเหมาะสมกับ POR
การใช้งานกลางวันและกลางคืน	ควรทดสอบคุณภาพของภาพในช่วงเวลาที่ระบบต้องใช้งานจริง ไม่ใช่เฉพาะสภาพแสงที่เหมาะสม
ช่วงไดนามิกกว้าง (Wide Dynamic Range: WDR)	พิจารณาในบริเวณที่มีทั้งส่วนสว่างและมืดมาก เช่น ทางเข้าอาคารที่มีแสงจากภายนอก
สมรรถนะในสภาพแสงต่ำ (Low-Light Performance)	พิจารณาเมื่อระบบต้องใช้งานในพื้นที่ที่มีแสงจำกัด

ประเด็น	ความหมายและสิ่งที่ควรกำหนด
แสงอินฟราเรด (Infrared: IR)	พิจารณาระยะใช้งานและการสะท้อนกลับจากกระจก ผนัง หรือวัตถุใกล้กล้อง
อัตราเฟรม (Frame Rate)	กำหนดให้เหมาะกับความเร็วและลักษณะการเคลื่อนไหวของเป้าหมาย
การบีบอัดข้อมูล (Compression)	ต้องไม่ลดคุณภาพของภาพจนไม่สามารถใช้ตามวัตถุประสงค์
ระยะเวลาเก็บรักษา (Retention Period)	ระบบต้องสามารถจัดเก็บข้อมูลได้ครบตามระยะเวลาที่องค์กรกำหนด
ความจุพื้นที่จัดเก็บ	ต้องคำนวณจากจำนวนกล้อง อัตราข้อมูล รูปแบบการบันทึก และระยะเวลาเก็บรักษา
ความพร้อมใช้งานของระบบ (Availability)	ระบบควรมีระดับความพร้อมใช้งานเหมาะสมกับความสำคัญของภารกิจ และสามารถตรวจพบความผิดปกติได้

ตัวอย่างการกำหนด TOR ที่ไม่เหมาะสม คือ “กล้องต้องมีความละเอียดไม่น้อยกว่า 8 Megapixel” เพียงอย่างเดียว เนื่องจากไม่สามารถยืนยันได้ว่าภาพจะตอบวัตถุประสงค์ของแต่ละจุดหรือไม่ ตัวอย่างที่เหมาะสมกว่า คือ “จุดติดตั้งบริเวณทางเข้าหลักต้องสามารถให้ภาพในระดับที่ตอบความต้องการเชิงปฏิบัติการสำหรับการจดจำหรือระบุตัวตามที่กำหนดใน POR โดยผู้เสนอราคาต้องแสดงการคำนวณหรือการออกแบบที่เกี่ยวข้อง และต้องทดสอบในสภาพใช้งานจริงก่อนตรวจรับ”

4.1.1.8. การทำงานร่วมกันและความสามารถในการเปลี่ยนหรือย้ายระบบ

องค์กรควรพิจารณาความสามารถของระบบในการทำงานร่วมกับอุปกรณ์หรือระบบอื่น เพื่อช่วยลดความเสี่ยงจากการผูกติดกับผู้ผลิตหรือผู้ให้บริการรายเดียว และช่วยให้องค์กรสามารถปรับปรุงหรือเปลี่ยนบางองค์ประกอบของระบบได้ในอนาคตโดยไม่จำเป็นต้องเปลี่ยนระบบทั้งหมด

ประเด็นที่ควรพิจารณา ได้แก่

ประเด็น	สิ่งที่ควรพิจารณา
มาตรฐานการทำงานร่วมกัน	รองรับมาตรฐานหรือ Profile ที่เกี่ยวข้อง เช่น ONVIF ตามฟังก์ชันที่ต้องใช้งานจริง
ส่วนเชื่อมต่อระบบ (API/Interface)	มีเอกสารและสามารถเชื่อมต่อกับระบบอื่นตามที่กำหนด

ประเด็น	สิ่งที่ควรพิจารณา
การส่งออกข้อมูล	สามารถส่งออกวิดีโอ ภาพ หรือข้อมูลที่จำเป็นในรูปแบบที่สามารถนำไปใช้งานต่อได้
การย้ายข้อมูลและค่าตั้ง	สามารถนำข้อมูลหรือค่าตั้งที่จำเป็นออกจากระบบเมื่อเปลี่ยนผลิตภัณฑ์หรือผู้ให้บริการ
การเปลี่ยนองค์ประกอบบางส่วน	สามารถเปลี่ยนกล้อง พื้นที่จัดเก็บ หรือองค์ประกอบอื่นโดยไม่ต้องเปลี่ยนระบบทั้งหมดโดยไม่มีเหตุผล
การทดสอบการทำงานร่วมกัน	ต้องสามารถทดสอบตามกรณีใช้งานที่องค์กรต้องการจริง

การระบุว่าอุปกรณ์ “รองรับ ONVIF” เพียงอย่างเดียวไม่เพียงพอ เพราะผลิตภัณฑ์อาจรองรับคนละ Profile หรือรองรับฟังก์ชันไม่เท่ากัน จึงควรกำหนด กรณีใช้งาน (Use Case) ที่ต้องการและทดสอบการทำงานจริง

4.1.1.9. ความมั่นคงปลอดภัยของห่วงโซ่อุปทาน

ความมั่นคงปลอดภัยของระบบ CCTV ไม่ได้ขึ้นอยู่กับกล้องหรือผู้ผลิตอุปกรณ์หลักเพียงรายเดียว แต่เกี่ยวข้องกับซอฟต์แวร์ เฟิร์มแวร์ ส่วนประกอบจากบุคคลที่สาม ระบบบริหารวิดีโอ ผู้ให้บริการคลาวด์ ผู้ติดตั้ง ผู้รวมระบบ และผู้ให้บริการบำรุงรักษา

องค์กรจึงควรประเมินว่าผู้ผลิตหรือผู้ให้บริการสามารถบริหารความเสี่ยงของผลิตภัณฑ์และส่วนประกอบตลอดวงจรชีวิตได้หรือไม่

การบริหารส่วนประกอบซอฟต์แวร์และความโปร่งใสของห่วงโซ่อุปทาน

ผู้ผลิตหรือผู้ให้บริการควรมีกระบวนการที่ช่วยให้สามารถทราบ บริหาร และติดตามส่วนประกอบซอฟต์แวร์ที่สำคัญ รวมถึงซอฟต์แวร์จากบุคคลที่สาม เพื่อให้สามารถตอบคำถามสำคัญได้ เช่น

- เมื่อมีการประกาศช่องโหว่ของส่วนประกอบหนึ่ง สามารถระบุได้หรือไม่ว่าผลิตภัณฑ์รุ่นใดได้รับผลกระทบ
- สามารถประเมินผลกระทบและความรุนแรงได้หรือไม่
- สามารถกำหนดการแก้ไขหรือมาตรการบรรเทาได้หรือไม่
- สามารถแจ้งผู้ใช้งานที่ได้รับผลกระทบได้หรือไม่
- สามารถติดตามส่วนประกอบดังกล่าวตลอดระยะเวลาการสนับสนุนผลิตภัณฑ์ได้หรือไม่

องค์กรสามารถกำหนดให้ผู้ผลิตแสดงหลักฐานเกี่ยวกับความสามารถดังกล่าวตามระดับความเสี่ยง โดยไม่จำเป็นต้องกำหนดให้เปิดเผยรายการส่วนประกอบซอฟต์แวร์ทั้งหมดต่อสาธารณะ หรือกำหนดให้ใช้รูปแบบเอกสารเฉพาะเพียงรูปแบบเดียว

4.1.1.10. การสนับสนุนตลอดวงจรชีวิตผลิตภัณฑ์และบริการ

TOR หรือสัญญาควรกำหนดว่า ผู้ผลิตหรือผู้ให้บริการจะสนับสนุนผลิตภัณฑ์ในด้านใดและนานเพียงใด เพื่อให้องค์กรสามารถประเมินต้นทุนและความเสี่ยงตลอดอายุการใช้งาน ไม่ใช่พิจารณาเฉพาะระยะรับประกันอุปกรณ์ ควรครอบคลุมประเด็นดังต่อไปนี้

ประเด็น	สิ่งที่ควรกำหนด
ระยะรับประกัน	ระยะเวลาและขอบเขตการรับประกันฮาร์ดแวร์และซอฟต์แวร์
การสนับสนุนทางเทคนิค	ช่องทางและระยะเวลาที่สามารถขอรับการสนับสนุน
การปรับปรุงเฟิร์มแวร์และซอฟต์แวร์	ระยะเวลาที่จะได้รับการแก้ไขข้อผิดพลาดและการปรับปรุง
การปรับปรุงด้านความมั่นคงปลอดภัย	ระยะเวลาที่ผู้ผลิตจะออกการแก้ไขช่องโหว่ที่เกี่ยวข้อง
อะไหล่และอุปกรณ์ทดแทน	ความพร้อมของอะไหล่และเงื่อนไขในการเปลี่ยนอุปกรณ์
การแจ้งเตือนช่องโหว่	ช่องทางที่องค์กรจะได้รับ Security Advisory หรือข้อมูลที่จำเป็น
สถานะสิ้นสุดอายุผลิตภัณฑ์ (EoL)	วันที่หรือช่วงเวลาที่ผู้ผลิตยุติการจำหน่ายหรือเข้าสู่ช่วงสิ้นสุดวงจรชีวิตของผลิตภัณฑ์
สถานะสิ้นสุดการสนับสนุน (EoS)	วันที่ที่ผู้ผลิตจะยุติการสนับสนุนบางส่วนหรือทั้งหมด เช่น Security Update, Firmware, อะไหล่ หรือ Technical Support
การแจ้งล่วงหน้า	ผู้ผลิตควรแจ้งสถานะ EoL/EoS ล่วงหน้าในระยะเวลาที่เหมาะสม เพื่อให้องค์กรสามารถวางแผนงบประมาณและการทดแทน
การยุติหรือเปลี่ยนบริการ	กำหนดการคืนข้อมูล ลบข้อมูล เพิกถอนสิทธิ และสนับสนุนการเปลี่ยนผ่านเมื่อสิ้นสุดบริการ

ดังนั้น ไม่ควรใช้ข้อความสั้น ๆ ว่า “ผู้ขายต้องแจ้ง EoL/EoS” เพียงอย่างเดียว แต่ควรกำหนดว่า “ผู้ผลิตหรือผู้ให้บริการต้องแจ้งสถานะสิ้นสุดอายุผลิตภัณฑ์ (End of Life: EoL) และสถานะสิ้นสุดการสนับสนุน (End of Support: EoS) รวมถึงวันที่มีผล ขอบเขตการสนับสนุนที่ยุติลง และแนวทางการปรับปรุงหรือทดแทน เพื่อให้องค์กรสามารถบริหารความเสี่ยงและวางแผนวงจรชีวิตของระบบได้อย่างเหมาะสม”

4.1.1.11. ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

ระบบ CCTV อาจเก็บรวบรวมภาพ วิดีโอ เสียง หรือข้อมูลอื่นที่สามารถเชื่อมโยงกับบุคคลได้ ดังนั้น ข้อกำหนดในการจัดซื้อควรช่วยให้องค์กรสามารถปฏิบัติตามนโยบายด้านความเป็นส่วนตัวและข้อกำหนดทางกฎหมายที่เกี่ยวข้องได้ตลอดวงจรชีวิตของข้อมูล

ข้อกำหนดไม่ควรพิจารณาเฉพาะว่าระบบ “สามารถบันทึกภาพได้” แต่ควรพิจารณาด้วยว่าองค์กรสามารถ จำกัดการเก็บ ใช้ เข้าถึง เปิดเผย เก็บรักษา และลบข้อมูล ได้ตามวัตถุประสงค์และระดับความเสี่ยงหรือไม่ โดยมีประเด็นที่ควรพิจารณาอย่างน้อยดังนี้

ประเด็น	สิ่งที่ควรกำหนดหรือพิจารณา
การจำกัดมุมมองของกล้อง	สามารถกำหนดมุมมองให้ครอบคลุมเฉพาะพื้นที่ที่จำเป็นต่อวัตถุประสงค์
การปิดบังพื้นที่ในภาพ (Privacy Mask)	สามารถปิดบังพื้นที่ที่ไม่จำเป็นต้องบันทึกหรือแสดงผลตามความเหมาะสม
การกำหนดระยะเวลาเก็บรักษาข้อมูล (Retention Period)	สามารถกำหนดและบังคับใช้ระยะเวลาเก็บรักษาตามนโยบายขององค์กร
การลบหรือเขียนทับข้อมูล	สามารถลบ เขียนทับ หรือจัดการข้อมูลเมื่อครบกำหนดได้อย่างเหมาะสม
การควบคุมการเข้าถึง	สามารถจำกัดสิทธิในการดู ค้นหา ส่งออก หรือบริหารข้อมูลตามหน้าที่
การบันทึกกิจกรรม	สามารถตรวจสอบได้ว่าใครเข้าถึงหรือส่งออกข้อมูลเมื่อใด ตามระดับความเสี่ยง
การส่งออกข้อมูล	สามารถควบคุมผู้มีสิทธิ รูปแบบ และวิธีการส่งออกข้อมูลได้
การคุ้มครองข้อมูลที่ส่งออก	สามารถใช้การเข้ารหัส รหัสผ่าน หรือมาตรการอื่นตามความเหมาะสม
การจัดการข้อมูลเมื่อสิ้นสุดบริการ	สามารถคืน ย้าย หรือลบข้อมูลจากระบบและบริการภายนอกได้
การใช้ผู้ให้บริการภายนอก	สามารถกำหนดและควบคุมขอบเขตที่ผู้ให้บริการสามารถเข้าถึงหรือประมวลผลข้อมูลได้

หากผู้ให้บริการภายนอกสามารถเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลแทนองค์กร ควรกำหนดบทบาท หน้าที่ มาตรการรักษาความมั่นคงปลอดภัย การจัดการเหตุ การคืนหรือลบข้อมูล และการใช้ผู้ให้บริการช่วงให้ชัดเจนในสัญญาหรือข้อตกลงที่เกี่ยวข้อง

การมีคุณสมบัติด้านความเป็นส่วนตัวในผลิตภัณฑ์เป็นเพียงเครื่องมือสนับสนุนการปฏิบัติตามข้อกำหนด มิได้ทำให้การใช้ระบบมีความชอบด้วยกฎหมายโดยอัตโนมัติ

4.1.1.12. บริการคลาวด์และบริการภายนอก

หากระบบ CCTV ใช้บริการคลาวด์หรือบริการจากภายนอกสำหรับการจัดเก็บข้อมูล การดูภาพจากระยะไกล การแจ้งเตือน การบริหารอุปกรณ์ การสำรองข้อมูล หรือการสนับสนุนทางเทคนิค องค์กรควรกำหนดข้อกำหนดที่ทำให้สามารถประเมินได้ว่า ข้อมูลอยู่ที่ใด ใครเข้าถึงได้ ใครรับผิดชอบส่วนใด และเมื่อยุติบริการจะจัดการข้อมูลอย่างไร

การเลือกใช้บริการคลาวด์ไม่ควรพิจารณาจากรูปแบบบริการเพียงอย่างเดียว เช่น Public Cloud, Private Cloud หรือ Hybrid Cloud แต่ควรพิจารณาจากมาตรการควบคุม ความรับผิดชอบ สถานที่จัดเก็บและประมวลผลข้อมูล เขตอำนาจทางกฎหมาย การเข้าถึงข้อมูล การเข้ารหัส ความพร้อมใช้งาน และความสามารถในการเปลี่ยนหรือยุติบริการ

ประเด็นที่ควรกำหนดในการจัดซื้อหรือสัญญาควรพิจารณาดังนี้

ประเด็น	สิ่งที่ควรกำหนดหรือขอหลักฐาน
สถานที่จัดเก็บข้อมูล (Data Location)	ข้อมูลหลัก ข้อมูลสำรอง และข้อมูลที่เกี่ยวข้องถูกจัดเก็บในประเทศหรือภูมิภาคใด
สถานที่ประมวลผลข้อมูล (Processing Location)	มีการประมวลผลข้อมูลจากพื้นที่หรือประเทศใด
เขตอำนาจทางกฎหมาย (Jurisdiction)	กฎหมายหรือเขตอำนาจใดอาจมีผลต่อข้อมูลหรือผู้ให้บริการ
การเข้าถึงเพื่อบริหารระบบ (Administrative Access)	บุคลากรหรือผู้ให้บริการใดสามารถเข้าถึงระบบหรือข้อมูล และเข้าถึงจากพื้นที่ใด
ผู้ให้บริการช่วง (Subprocessor)	มีผู้ให้บริการรายอื่นเข้ามาเกี่ยวข้องหรือไม่ และมีวิธีแจ้งการเปลี่ยนแปลงอย่างไร
การเข้ารหัสและการควบคุมกุญแจ	ข้อมูลได้รับการเข้ารหัสอย่างไร และใครเป็นผู้ควบคุมกุญแจเข้ารหัส
การสำรองและกู้คืนข้อมูล	มีการสำรองข้อมูลไว้ที่ใด และสามารถกู้คืนภายใต้เงื่อนไขใด
การแจ้งเหตุด้านความมั่นคงปลอดภัย	ผู้ให้บริการต้องแจ้งเหตุประเภทใด ผ่านช่องทางใด และภายในระยะเวลาที่เหมาะสมกับข้อกำหนด

ประเด็น	สิ่งที่ควรกำหนดหรือขอหลักฐาน
การเปลี่ยนแปลงบริการที่มีนัยสำคัญ	มีการแจ้งเมื่อเปลี่ยนสถานที่จัดเก็บ ผู้ให้บริการช่วง หรือมาตรการสำคัญหรือไม่
การคืนหรือส่งออกข้อมูล	สามารถนำข้อมูลกลับออกจากบริการในรูปแบบที่ใช้งานต่อได้หรือไม่
การลบข้อมูลอย่างมั่นคงปลอดภัย	ครอบคลุมข้อมูลหลัก ข้อมูลสำรอง สำเนา และข้อมูลที่เกี่ยวข้องตามความเหมาะสม
การยุติหรือเปลี่ยนบริการ (Exit Strategy)	มีแนวทางย้ายข้อมูล เพิกถอนสิทธิ ลบข้อมูล และเปลี่ยนไปใช้บริการอื่นอย่างไร

หากมีกฎหมาย ประกาศ นโยบายองค์กร หรือข้อกำหนดเฉพาะที่กำหนดให้ข้อมูลบางประเภทต้องจัดเก็บหรือประมวลผลภายในประเทศไทย เงื่อนไขดังกล่าวควรถูกกำหนดอย่างชัดเจนในข้อกำหนดการจัดซื้อและสามารถตรวจสอบได้

อย่างไรก็ตาม การจัดเก็บข้อมูลภายในประเทศไทยเพียงอย่างเดียว ไม่ควรถูกตีความว่าทำให้ระบบมีความมั่นคงปลอดภัยโดยอัตโนมัติ หากยังมีการเข้าถึงเพื่อบริหารจากภายนอก การควบคุมกุญแจโดยบุคคลอื่นหรือการใช้ผู้ให้บริการช่วงที่องค์กรไม่สามารถกำกับดูแลได้อย่างเหมาะสม

4.1.1.13. การสนับสนุนตลอดวงจรชีวิตของผลิตภัณฑ์และบริการ

ระบบ CCTV มักมีอายุการใช้งานหลายปี ขณะที่ผลิตภัณฑ์ ซอฟต์แวร์ เฟิร์มแวร์ และบริการที่เกี่ยวข้องอาจมีระยะเวลาการสนับสนุนสั้นกว่านั้น การจัดซื้อจึงควรพิจารณาความสามารถในการดูแลระบบตลอดวงจรชีวิต ไม่ใช่พิจารณาเฉพาะระยะเวลารับประกันฮาร์ดแวร์

องค์กรควรกำหนดให้ผู้ผลิตหรือผู้ให้บริการเปิดเผยข้อมูลที่เพียงพอสำหรับการวางแผนบำรุงรักษา การปรับปรุงด้านความมั่นคงปลอดภัย และการทดแทนผลิตภัณฑ์ ประเด็นที่ควรพิจารณามีดังต่อไปนี้

ประเด็น	สิ่งที่ควรกำหนด
ระยะเวลารับประกัน (Warranty)	ระยะเวลาและขอบเขตการรับประกันอุปกรณ์ ซอฟต์แวร์ และบริการ
การสนับสนุนทางเทคนิค (Technical Support)	ช่องทางให้บริการ ช่วงเวลาที่ให้บริการ และระดับการสนับสนุน
การปรับปรุงซอฟต์แวร์และเฟิร์มแวร์	ระยะเวลาที่ผลิตภัณฑ์จะได้รับการแก้ไขข้อผิดพลาดและปรับปรุงระบบ

ประเด็น	สิ่งที่ควรกำหนด
การปรับปรุงด้านความมั่นคงปลอดภัย (Security Update)	ระยะเวลาที่ผู้ผลิตจะสนับสนุนการแก้ไขช่องโหว่ที่มีผลต่อผลิตภัณฑ์
การแจ้งเตือนช่องโหว่	ช่องทางที่ผู้ใช้งานจะได้รับประกาศแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Advisory)
อะไหล่และอุปกรณ์ทดแทน	ระยะเวลาที่มีอะไหล่หรืออุปกรณ์ทดแทนพร้อมใช้งาน
สถานะสิ้นสุดอายุผลิตภัณฑ์ (End of Life: EoL)	วันที่หรือช่วงที่ผลิตภัณฑ์เข้าสู่ระยะสิ้นสุดวงจรชีวิต เช่น ยุติการจำหน่ายหรือเริ่มลดระดับการสนับสนุน
สถานะสิ้นสุดการสนับสนุน (End of Support: EoS)	วันที่ผู้ผลิตยุติการสนับสนุนบางส่วนหรือทั้งหมด เช่น การแก้ไขช่องโหว่ การปรับปรุงเฟิร์มแวร์ อะไหล่ หรือการสนับสนุนทางเทคนิค
การแจ้งล่วงหน้า	ระยะเวลาที่ผู้ผลิตต้องแจ้งก่อน EoL/EoS เพื่อให้องค์กรสามารถวางแผนได้
การเปลี่ยนผ่าน	แนวทางในการย้ายข้อมูล ค่าตั้ง หรือบริการไปยังผลิตภัณฑ์หรือระบบใหม่

4.1.1.14. หลักฐานประกอบการประเมินและการสร้างความเชื่อมั่น

ข้อกำหนดด้านความมั่นคงปลอดภัยที่ไม่สามารถตรวจสอบได้จะทำให้การจัดซื้อและการตรวจรับมีความคลุมเครือ ดังนั้น สำหรับข้อกำหนดที่มีความสำคัญควรกำหนดไว้ตั้งแต่ต้นว่า ผู้เสนอราคาต้องแสดงหลักฐานประเภทใด หรือองค์กรจะตรวจสอบอย่างไร

หลักฐานสามารถมีได้หลายระดับ ไม่จำเป็นต้องเป็นใบรับรองจากบุคคลที่สามทุกกรณี ระดับของหลักฐานควรสัมพันธ์กับระดับความเสี่ยงและผลกระทบของระบบ แนวทางการแบ่งประเภทหลักฐานมีดังต่อไปนี้

ประเภทหลักฐาน	ตัวอย่าง	สิ่งที่ใช้ยืนยัน
เอกสารคุณลักษณะทางเทคนิค	Product Specification, Datasheet	ความสามารถพื้นฐานของผลิตภัณฑ์
คู่มือการตั้งค่าและความมั่นคงปลอดภัย	Security Guide, Hardening Guide	ความสามารถในการตั้งค่าและควบคุมระบบ
นโยบายของผู้ผลิต	Product Lifecycle Policy, Vulnerability Disclosure Policy	กระบวนการดูแลผลิตภัณฑ์และช่องโหว่

ประเภทหลักฐาน	ตัวอย่าง	สิ่งที่ใช้ยืนยัน
ประกาศแจ้งเตือนด้านความมั่นคงปลอดภัย	Security Advisory	ความสามารถในการสื่อสารและจัดการช่องโหว่
การสาธิตการทำงาน	Demonstration	ความสามารถที่สามารถตรวจสอบได้ในทางปฏิบัติ
ผลการทดสอบ	Test Report	ผลการทดสอบตามเกณฑ์ที่กำหนด
หลักฐานจากบุคคลที่สาม	Independent Assessment	การประเมินโดยหน่วยงานที่เป็นอิสระจากผู้ผลิต
ใบรับรองมาตรฐาน	Certification	การประเมินตามขอบเขตและมาตรฐานที่กำหนด
หลักฐานกระบวนการ	Secure Development หรือ Vulnerability Handling Evidence	ความสามารถของกระบวนการผู้ผลิต
หลักฐานภายใต้ข้อตกลงรักษาความลับ	เอกสารที่เปิดเผยเฉพาะผู้ประเมิน	ข้อมูลที่มีความอ่อนไหวหรือเป็นทรัพย์สินทางปัญญา

สำหรับระบบระดับความเชื่อมั่นสูง (High-Assurance: H) อาจกำหนดให้ใช้หลักฐานที่มีระดับความเป็นอิสระ ความละเอียด หรือความสามารถในการตรวจสอบย้อนกลับสูงขึ้นตามความเสี่ยง

อย่างไรก็ตาม ไม่ควรกำหนดว่าใบรับรองเพียงฉบับเดียวใช้แทนหลักฐานทั้งหมด เนื่องจากใบรับรองแต่ละประเภทมีขอบเขตและข้อจำกัดแตกต่างกัน

4.1.1.15. เกณฑ์การตรวจรับ

ข้อกำหนดในการจัดซื้อที่สำคัญควรเชื่อมโยงกับ วิธีการตรวจสอบและเกณฑ์การยอมรับ ตั้งแต่ก่อนประกาศ TOR หรือก่อนลงนามสัญญา เพื่อป้องกันปัญหาเมื่อถึงขั้นตรวจรับ เช่น ผู้จัดซื้อไม่สามารถระบุได้ว่าคุณสมบัติที่เสนอ “ผ่าน” หรือ “ไม่ผ่าน” จากหลักฐานใด ตัวอย่างเช่น

ข้อกำหนด	วิธีตรวจสอบ	เกณฑ์การยอมรับ
คุณภาพของภาพตาม POR/DORI	ทดสอบภาพในระยะและสภาพจริง	ภาพให้รายละเอียดตามระดับที่กำหนด
การกำหนดสิทธิผู้ใช้งาน	สร้างบัญชีทดสอบหลายบทบาท	แต่ละบทบาททำได้เฉพาะสิทธิที่ได้รับ

ข้อกำหนด	วิธีตรวจสอบ	เกณฑ์การยอมรับ
การพิสูจน์ตัวตนหลายปัจจัย (MFA)	ทดลองเข้าสู่ระบบด้วยบัญชีที่กำหนด	ระบบต้องใช้ปัจจัยเพิ่มเติมตามข้อกำหนด
การเข้าถึงจากระยะไกล	ตรวจค่าตั้งและทดลองเชื่อมต่อ	ไม่มีช่องทางที่ไม่ได้รับอนุมัติ
การบันทึกเหตุการณ์	สร้างเหตุการณ์ทดสอบ เช่น Login Failure หรือ Configuration Change	ระบบสร้างบันทึกและสามารถเรียกตรวจสอบได้
การปรับปรุงเฟิร์มแวร์	ตรวจเอกสารและสาธิตกระบวนการ	สามารถปรับปรุงจากแหล่งที่เชื่อถือได้และตรวจสอบความถูกต้องได้
ระยะเวลาเก็บรักษาข้อมูล	ตรวจค่าตั้งและข้อมูลย้อนหลัง	รองรับระยะเวลาที่องค์กรกำหนด
การควบคุมพอร์ตและบริการ	ตรวจค่าตั้งหรือการสื่อสารเครือข่าย	เปิดเฉพาะรายการที่ได้รับอนุมัติ
การสำรองและกู้คืน	ทดสอบการกู้คืน	สามารถกู้คืนองค์ประกอบที่กำหนดได้
การทำงานร่วมกัน	เชื่อมต่อกับอุปกรณ์หรือระบบที่กำหนด	สามารถทำงานตามกรณีใช้งานที่กำหนด
การสนับสนุนผลิตภัณฑ์	ตรวจเอกสารจากผู้ผลิต	มีข้อมูลเกี่ยวกับช่วงการสนับสนุน EoL/EoS และช่องทาง Security Advisory

การเขียนเกณฑ์ตรวจรับให้ชัดเจนตั้งแต่ต้นช่วยลดการตีความที่แตกต่างกันระหว่างเจ้าของระบบ ผู้จัดซื้อ ผู้เสนอราคา ผู้ติดตั้ง และคณะกรรมการตรวจรับ

4.1.2 การรับรอง ผลการทดสอบ และฉลากด้านความมั่นคงปลอดภัย

ใบรับรอง ผลการทดสอบ หรือฉลากด้านความมั่นคงปลอดภัยสามารถใช้เป็นหลักฐานประกอบการประเมินความน่าเชื่อถือของผลิตภัณฑ์หรือผู้ให้บริการได้ โดยเฉพาะในกรณีที่องค์กรไม่สามารถทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยทุกประการได้ด้วยตนเอง

อย่างไรก็ตาม การได้รับใบรับรองหรือฉลากไม่ควรถูกตีความว่าผลิตภัณฑ์มีความมั่นคงปลอดภัยเพียงพอสำหรับทุกบริบท และการไม่มีใบรับรองก็ไม่ควรถูกใช้เป็นเหตุผลเพียงอย่างเดียวในการสรุปว่าผลิตภัณฑ์ไม่เหมาะสม

องค์กรควรพิจารณาอย่างน้อย

ประเด็น	สิ่งที่ควรตรวจสอบ
ขอบเขตการรับรอง (Scope)	ครอบคลุมผลิตภัณฑ์ ระบบ หรือกระบวนการใด
รุ่นและเวอร์ชัน	ตรงกับฮาร์ดแวร์ เฟิร์มแวร์ และซอฟต์แวร์ที่จัดซื้อจริงหรือไม่
มาตรฐานหรือเกณฑ์ที่ใช้	เกี่ยวข้องกับความเสี่ยงและคุณสมบัติที่ต้องการประเมินหรือไม่
สถานะของใบรับรอง	ยังมีผลอยู่หรือหมดอายุแล้ว
หน่วยงานที่ออกหลักฐาน	มีความน่าเชื่อถือและเหมาะสมกับประเภทการประเมินหรือไม่
ความเป็นอิสระ	เป็นการประเมินตนเอง การประเมินโดยบุคคลที่สอง หรือการประเมินโดยบุคคลที่สาม
ข้อจำกัด	มีส่วนใดที่ไม่อยู่ในขอบเขตหรือมีเงื่อนไขพิเศษหรือไม่
การตรวจสอบย้อนกลับ	สามารถเชื่อมโยงหลักฐานกับผลิตภัณฑ์ที่ส่งมอบจริงได้หรือไม่

ฉลากหรือระบบรับรองของต่างประเทศสามารถใช้เป็น หลักฐานประกอบ ได้ตามความเกี่ยวข้อง แต่ไม่ควรนำข้อกำหนดทางกฎหมายหรือเกณฑ์บังคับของประเทศอื่นมาใช้เป็นข้อบังคับสำหรับระบบ CCTV ในประเทศไทยโดยอัตโนมัติ เนื่องจากฉลากหรือระบบรับรองของต่างประเทศอาจไม่ครอบคลุมหรือเหมาะสมกับบริบทในประเทศไทย เช่น การรองรับและความทนทานในการทำงานในสภาวะแวดล้อมที่แตกต่างกัน หรือกฎหมายหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

4.2 การส่งมอบและการตรวจรับอย่างมั่นคงปลอดภัย

การส่งมอบระบบ CCTV ไม่ควรถือว่าเสร็จสมบูรณ์เพียงเมื่อกล้องสามารถแสดงและบันทึกภาพได้ แต่ควรยืนยันว่า ระบบที่ติดตั้งจริงตรงตามแบบและข้อกำหนดที่ได้รับอนุมัติ สามารถทำงานตามวัตถุประสงค์ มีมาตรการด้านความมั่นคงปลอดภัยตามที่กำหนด และไม่มีบัญชี ช่องทาง หรือค่าตั้งชั่วคราวที่ไม่จำเป็น

หลงเหลืออยู่ การส่งมอบที่สมบูรณ์ควรทำให้เจ้าของระบบสามารถ บริหาร ใช้งาน บำรุงรักษา ตรวจสอบ กู้คืน และปรับปรุงระบบต่อได้โดยไม่จำเป็นต้องพึ่งพาผู้ติดตั้งเกินความจำเป็น

4.2.1 การตรวจสอบระบบที่ส่งมอบ

ควรตรวจสอบว่าองค์ประกอบที่ติดตั้งจริงตรงกับรายการ แบบ และข้อกำหนดที่ได้รับอนุมัติ

รายการ	สิ่งที่ควรตรวจสอบ
กล้อง	จำนวน รุ่น หมายเลขประจำเครื่อง และตำแหน่ง
เครื่องบันทึกและระบบบริหารวิดีโอ	รุ่น เวอร์ชัน และใบอนุญาตใช้งาน
พื้นที่จัดเก็บ	ประเภท ความจุ และการตั้งค่าที่เกี่ยวข้อง
อุปกรณ์เครือข่าย	รุ่น การเชื่อมต่อ และการแบ่งเครือข่าย
เฟิร์มแวร์และซอฟต์แวร์	เวอร์ชันที่ติดตั้งจริง
ค่าตั้งระบบ	ตรงกับค่าที่ได้รับอนุมัติ
บริการคลาวด์หรือบริการภายนอก	ตรงกับขอบเขตที่ได้รับอนุมัติ
การเข้าถึงจากระยะไกล	ช่องทาง บัญชี และผู้ที่สามารถเข้าถึง
การเชื่อมต่อกับระบบอื่น	ตรงกับสถาปัตยกรรมและขอบเขตที่กำหนด

หากสิ่งที่ติดตั้งจริงแตกต่างจาก TOR แบบ หรือข้อเสนออย่างมีนัยสำคัญ ควรประเมินผลกระทบและได้รับการอนุมัติก่อนการตรวจรับ

4.2.2 การตรวจรับคุณภาพของภาพและสมรรถนะ

การตรวจรับควรดำเนินการในสภาพใช้งานจริงหรือสภาพที่ใกล้เคียงกับการใช้งานจริง และใช้ความต้องการเชิงปฏิบัติการรายจุด (POR) เป็นฐานในการพิจารณา

ประเด็น	สิ่งที่ควรตรวจสอบ
พื้นที่ครอบคลุมของภาพ	ภาพครอบคลุมพื้นที่ตามที่กำหนด
ระดับ DORI	รายละเอียดของภาพตอบวัตถุประสงค์ของแต่ละจุด
การใช้งานกลางวันและกลางคืน	ภาพสามารถใช้งานได้ในช่วงเวลาที่ต้องให้บริการ
การจัดการแสง	WDR, Low-Light หรือ IR ทำงานเหมาะสมกับพื้นที่
การเคลื่อนไหว	ไม่มีภาพเบลอจากการเคลื่อนไหวจนไม่สามารถใช้ตามวัตถุประสงค์

ประเด็น	สิ่งที่ควรตรวจสอบ
การบันทึก	สามารถบันทึกข้อมูลได้อย่างต่อเนื่องตามที่กำหนด
การเรียกดูย้อนหลัง	สามารถค้นหาและเล่นข้อมูลได้ถูกต้อง
การส่งออก	สามารถส่งออกข้อมูลตามสิทธิและรูปแบบที่กำหนด
ระยะเวลาเก็บรักษา	สามารถเก็บข้อมูลย้อนหลังได้ตามระยะเวลาที่กำหนด
ความจุพื้นที่จัดเก็บ	มีความจุเพียงพอและระบบแจ้งเตือนทำงาน
ความต่อเนื่องและการกู้คืน	ทดสอบตามข้อกำหนดสำหรับระบบที่มีความสำคัญ

ไม่ควรตรวจรับคุณภาพของภาพจากความละเอียดหรือเอกสารคุณลักษณะของกล้องเพียงอย่างเดียว

4.2.3 การตรวจสอบด้านความมั่นคงปลอดภัยก่อนเปิดใช้งาน

ก่อนเปิดใช้งานจริง ควรยืนยันว่าองค์ประกอบสำคัญได้รับการตั้งค่าในสถานะที่ได้รับอนุมัติ

ประเด็น	สิ่งที่ควรยืนยัน
ข้อมูลยืนยันตัวตนเริ่มต้น	ถูกเปลี่ยน ยกเลิก หรือจัดการแล้ว
บัญชีผู้ใช้งาน	สร้างตามผู้ใช้งานจริงและบทบาท
บัญชีติดตั้งหรือทดสอบ	ถูกลบ ปิด หรือควบคุมตามความจำเป็น
บัญชี Guest/Anonymous	ถูกปิดหรือจำกัดตามข้อกำหนด
พอร์ตและบริการ	เปิดเฉพาะรายการที่ได้รับอนุมัติ
ส่วนบริหารจัดการ	จำกัดการเข้าถึงตามเครือข่ายและสิทธิที่กำหนด
การเข้าถึงจากระยะไกล	ใช้เฉพาะช่องทางที่ได้รับอนุมัติ
การพิสูจน์ตัวตนหลายปัจจัย	ทำงานตามข้อกำหนดสำหรับบัญชีหรือช่องทางที่เกี่ยวข้อง
เฟิร์มแวร์และซอฟต์แวร์	อยู่ในเวอร์ชันที่ได้รับอนุมัติและยังได้รับการสนับสนุน
บันทึกเหตุการณ์	สามารถสร้างและเรียกตรวจสอบได้
เวลา	อุปกรณ์และระบบสำคัญมีเวลาสอดคล้องกัน
Retention	ตรงกับนโยบายหรือข้อกำหนด
การสำรองและกู้คืน	ผ่านการทดสอบตามขอบเขต
การเข้ารหัสและใบรับรอง	ตั้งค่าและบริหารตามข้อกำหนด

ประเด็น	สิ่งที่ควรยืนยัน
การแบ่งเครือข่าย	ตรงกับสถาปัตยกรรมที่ได้รับอนุมัติ
บริการ P2P/Cloud	ตรงกับขอบเขตที่ได้รับอนุมัติ

ผลการตรวจสอบนี้ควรใช้เป็น ค่าฐานที่ได้รับอนุมัติ (Approved Configuration Baseline) สำหรับการควบคุมและตรวจสอบการเปลี่ยนแปลงในระยะต่อไป

4.2.4 การส่งมอบข้อมูลและเอกสาร

เอกสารที่ส่งมอบควรเพียงพอให้เจ้าของระบบสามารถบริหาร บำรุงรักษา ตรวจสอบ และกู้คืนระบบได้โดยไม่ต้องพึ่งพาความรู้ของผู้ติดตั้งเพียงบุคคลเดียว เอกสารควรครอบคลุมกลุ่มข้อมูลดังต่อไปนี้

กลุ่มข้อมูล	ตัวอย่าง
ทะเบียนอุปกรณ์	รหัสทรัพย์สิน รุ่น หมายเลขประจำเครื่อง และตำแหน่ง
รุ่นซอฟต์แวร์และเฟิร์มแวร์	เวอร์ชันที่ติดตั้งจริง
ผังและสถาปัตยกรรม	Camera Layout, Network Diagram และแบบที่ติดตั้งจริง (As-built)
ข้อมูลเครือข่าย	IP Address, VLAN, Port/Protocol/Service
บัญชีและสิทธิ	โครงสร้างบทบาทและสิทธิที่กำหนด
ระยะเวลาเก็บรักษาและพื้นที่จัดเก็บ	ค่าตั้งและผลการคำนวณความจุ
การสำรองและกู้คืน	ขั้นตอน ค่าตั้ง และผลการทดสอบ
การบำรุงรักษา	แผนและขั้นตอนการบำรุงรักษา
การปรับปรุงระบบ	ขั้นตอนการปรับปรุงเฟิร์มแวร์และซอฟต์แวร์
ความมั่นคงปลอดภัย	คู่มือการตั้งค่าหรือการเสริมความมั่นคงปลอดภัย
การจัดการช่องโหว่	ช่องทาง Security Advisory และ Vulnerability Reporting
วงจรชีวิตผลิตภัณฑ์	ระยะสนับสนุนและข้อมูล EoL/EoS
ผลการทดสอบและตรวจรับ	Test Result และ Acceptance Result
ประเด็นคงค้าง	ข้อยกเว้น ข้อบกพร่อง และความเสี่ยงคงเหลือ

ไม่จำเป็นต้องสร้างเอกสารใหม่แยกสำหรับทุกรายการ หากข้อมูลดังกล่าวมีอยู่ในระบบ คู่มือ แบบ หรือหลักฐานอื่นที่เจ้าของระบบสามารถเข้าถึงและตรวจสอบได้

4.2.5 การยกเลิกสิทธิและช่องทางชั่วคราว

ภายหลังการตรวจรับและก่อนเปิดใช้งานจริง ควรยกเลิกบัญชี สิทธิ ช่องทางการเข้าถึงจากระยะไกล และค่าตั้งที่ใช้เฉพาะระหว่างการติดตั้ง ทดสอบ หรือส่งมอบ ซึ่งไม่มีความจำเป็นต่อการดำเนินงานปกติ เช่น

1) บัญชีสำหรับการติดตั้งระบบ (Installation Account)
2) บัญชีสำหรับการทดสอบระบบ (Test Account)
3) บัญชีผู้ใช้งานชั่วคราว (Temporary Account)
4) รหัสผ่านชั่วคราว (Temporary Password)
5) ช่องทางการสนับสนุนจากระยะไกล (Remote Support)
6) โทเคนหรือกุญแจสำหรับการพิสูจน์ตัวตนชั่วคราว (Temporary Authentication Token or Key)
7) กฎของไฟร์วอลล์ที่กำหนดไว้ชั่วคราว (Temporary Firewall Rule)
8) พอร์ตหรือบริการเครือข่ายที่เปิดใช้งานเพื่อการติดตั้งหรือทดสอบ (Port or Network Service)

ผู้ติดตั้งหรือผู้ให้บริการไม่ควรคงสิทธิการเข้าถึงระบบของลูกค้าไว้โดยไม่จำเป็น หากจำเป็นต้องคงสิทธิเพื่อการบำรุงรักษาหรือการให้บริการ ควรกำหนดให้ใช้บัญชีที่สามารถระบุตัวบุคคลได้ พร้อมกำหนดวัตถุประสงค์ ขอบเขตสิทธิ วิธีการอนุมัติ ระยะเวลา การพิสูจน์ตัวตน การบันทึกกิจกรรม การเพิกถอนสิทธิ และการตรวจสอบการใช้งานตามความเหมาะสมกับระดับความเสี่ยง

4.2.6 การตรวจสอบหลักฐานการรับรองและผลการทดสอบ

หากข้อกำหนดการจัดซื้อหรือสัญญากำหนดให้มีใบรับรอง รายงานผลการทดสอบ หรือหลักฐานจากบุคคลที่สาม ควรตรวจสอบมากกว่าการยืนยันว่า “มีเอกสาร” ควรยืนยันว่า หลักฐานมีอยู่จริง ยังมีผลขอบเขตตรงกับสิ่งที่จัดซื้อ รุ่นและเวอร์ชันตรง หน่วยงานที่ออกหลักฐานตรงตามข้อกำหนด และสามารถเชื่อมโยงกับผลิตภัณฑ์ที่ส่งมอบจริง

หากหลักฐานใช้กับคนละรุ่น คนละเวอร์ชัน หรือครอบคลุมเฉพาะบางองค์ประกอบ ไม่ควรถือว่าครอบคลุมระบบที่จัดซื้อทั้งหมดโดยอัตโนมัติ

4.2.7 การตรวจสอบบริการคลาวด์และบริการภายนอก

กรณีระบบใช้บริการคลาวด์หรือบริการภายนอก ควรตรวจสอบว่าสภาพแวดล้อมที่ใช้งานจริงตรงกับสิ่งที่กำหนดใน TOR และสัญญา ประเด็นที่ควรพิจารณาและสิ่งที่ควรตรวจสอบมีดังต่อไปนี้

ประเด็น	สิ่งที่ควรตรวจสอบ
สถานที่จัดเก็บข้อมูล	ตรงกับที่ได้รับอนุมัติหรือไม่
สถานที่ประมวลผล	ตรงกับที่แจ้งไว้หรือไม่
เขตอำนาจทางกฎหมาย	มีการเปลี่ยนแปลงหรือไม่
ผู้ให้บริการช่วง	มีรายใหม่ที่ต้องประเมินหรือไม่
การเข้าถึงเพื่อบริหาร	ใครสามารถเข้าถึงและจากพื้นที่ใด
การเข้ารหัสและกุญแจ	การควบคุมเป็นไปตามข้อกำหนดหรือไม่
การสำรองและกู้คืน	สถานที่และวิธีการตรงกับสัญญาหรือไม่
การแจ้งเหตุ	มีช่องทางและเงื่อนไขตามข้อตกลงหรือไม่
การคืนข้อมูล	สามารถส่งออกข้อมูลได้ตามที่กำหนด
การลบข้อมูล	ครอบคลุมข้อมูลหลัก ข้อมูลสำรอง และสำเนาที่เกี่ยวข้อง
การยุติบริการ	มีแผนและสามารถดำเนินการได้

4.2.8 การจัดการข้อบกพร่องและความเสี่ยงคงเหลือ

หากยังมีข้อบกพร่องหรือข้อกำหนดบางรายการที่ยังไม่แล้วเสร็จ ไม่ควรบันทึกเพียงว่า “แก้ไขภายหลัง” แต่ควรกำหนดให้สามารถติดตามและตัดสินใจด้านความเสี่ยงได้อย่างชัดเจน

รายการ	สิ่งที่ควรบันทึก
ประเด็น	ข้อบกพร่องหรือช่องว่างที่พบ
ผลกระทบ	ผลกระทบต่อข้อมูล ระบบ หรือภารกิจ
ระดับความเสี่ยง	ระดับหรือเหตุผลในการประเมิน
มาตรการชั่วคราว	วิธีลดความเสี่ยงระหว่างรอแก้ไข
การดำเนินการ	สิ่งที่ต้องแก้ไข
ผู้รับผิดชอบ	บุคคลหรือหน่วยงานที่รับผิดชอบ

รายการ	สิ่งที่ควรบันทึก
กำหนดเวลา	วันที่ต้องดำเนินการแล้วเสร็จ
สถานะ	เปิด อยู่ระหว่างดำเนินการ หรือปิดแล้ว

ความเสี่ยงคงเหลือ (Residual Risk) หมายถึงความเสี่ยงที่ยังเหลืออยู่หลังจากใช้มาตรการควบคุมแล้ว หากมีนัยสำคัญ ควรได้รับการพิจารณาและยอมรับโดยผู้มีอำนาจตามกระบวนการบริหารความเสี่ยงขององค์กร

การลงนามตรวจรับทางเทคนิคไม่ควรถูกตีความโดยอัตโนมัติว่าเป็นการยอมรับความเสี่ยงทั้งหมดของระบบ

4.2.9 ผลการตรวจรับ

ผู้ตรวจรับควรมีการระบุผลการตรวจรับที่ชัดเจนพร้อมระบุเหตุผลในการให้ผลการตรวจรับนั้น ซึ่งต้องมีการประเมินตามเกณฑ์ที่ได้กำหนดไว้ ตัวอย่างแนวทางผลการตรวจรับดังแสดงต่อไปนี้

ผลการตรวจรับ	ความหมาย
ผ่านและพร้อมเปิดใช้งาน	ข้อกำหนดสำคัญได้รับการตรวจสอบแล้ว และไม่มีประเด็นที่ทำให้ไม่ควรเปิดใช้งาน
ผ่านโดยมีเงื่อนไข	ยังมีประเด็นต้องดำเนินการ แต่มีมาตรการลดความเสี่ยง ผู้รับผิดชอบ และกำหนดเวลาแล้ว
ต้องแก้ไขก่อนเปิดใช้งาน	มีข้อบกพร่องหรือความเสี่ยงที่ยังไม่อยู่ในระดับที่องค์กรยอมรับได้

กรณีผ่านโดยมีเงื่อนไข ควรติดตามจนประเด็นได้รับการแก้ไขหรือได้รับการพิจารณาความเสี่ยงอย่างเป็นทางการ ไม่ควรปล่อยให้ประเด็นคงค้างโดยไม่มีกำหนด

สรุปหลักการของบทที่ 4

การจัดซื้อจัดจ้างระบบ CCTV ควรกำหนดข้อกำหนดให้ครอบคลุมทั้งสมรรถนะ ความมั่นคงปลอดภัย ความเป็นส่วนตัว การบำรุงรักษา การจัดการช่องโหว่ การสนับสนุนตลอดวงจรชีวิต และการบริหารผู้ให้บริการ โดยระดับของข้อกำหนดควรสัมพันธ์กับระดับความสำคัญและความเสี่ยงของระบบ

ข้อกำหนดที่สำคัญควรสามารถเชื่อมโยงกับหลักฐาน วิธีการตรวจสอบ และเกณฑ์การยอมรับอย่างชัดเจน เพื่อให้การพิจารณาข้อเสนอและการตรวจรับสามารถดำเนินการได้อย่างเป็นระบบและลดการพึ่งพาคำกล่าวอ้างของผู้ผลิตเพียงอย่างเดียว

บทที่ 5 หัวข้อที่ต้องพิจารณาเพิ่มเติม

นอกเหนือจากมาตรการพื้นฐานตามวงจรชีวิตของระบบที่กำหนดไว้ในบทที่ 3 และข้อกำหนดด้านการจัดซื้อจัดจ้างในบทที่ 4 ระบบ CCTV บางรูปแบบอาจมีองค์ประกอบหรือบริการเพิ่มเติมที่ทำให้ลักษณะความเสี่ยงเปลี่ยนแปลงไป เช่น การใช้แอปพลิเคชันบนอุปกรณ์เคลื่อนที่ การเข้าถึงจากระยะไกล การใช้บริการคลาวด์ การพึ่งพาผู้ให้บริการภายนอก หรือการเพิ่มความสามารถด้านการวิเคราะห์วิดีโอและปัญญาประดิษฐ์

การใช้เทคโนโลยีหรือรูปแบบบริการดังกล่าวไม่ควรถูกสรุปว่า “ปลอดภัยกว่า” หรือ “มีความเสี่ยงกว่า” จากชื่อหรือประเภทของเทคโนโลยีเพียงอย่างเดียว แต่ควรพิจารณาจากวัตถุประสงค์ ลักษณะข้อมูล สถาปัตยกรรม การเชื่อมต่อ ผู้ที่สามารถเข้าถึง สถานที่จัดเก็บและประมวลผล เขตอำนาจทางกฎหมาย มาตรการควบคุม ตลอดจนความสามารถในการเปลี่ยนหรือยุติบริการ ระบบภายในองค์กรที่ไม่ได้รับการปรับปรุง มีบัญชีร่วม ไม่มีการบันทึกเหตุการณ์ และเปิดช่องทางการเข้าถึงจากระยะไกลโดยไม่มีการควบคุม อาจมีความเสี่ยงสูงกว่าบริการคลาวด์ที่ได้รับการบริหารและตรวจสอบอย่างเป็นระบบในทางกลับกัน บริการคลาวด์ที่องค์กรไม่สามารถทราบได้ว่าข้อมูลจัดเก็บที่ใด ใครสามารถเข้าถึง กุญแจเข้ารหัสอยู่ภายใต้การควบคุมของใคร หรือจะลบข้อมูลอย่างไรเมื่อยุติบริการ ก็อาจไม่เหมาะสมกับระบบที่มีผลกระทบสูง

ดังนั้น การพิจารณาความมั่นคงปลอดภัยควรประเมินจาก ความเสี่ยงและมาตรการควบคุมที่เกิดขึ้นจริง มากกว่าชื่อของรูปแบบบริการ

แนวทางในบทนี้จึงมีวัตถุประสงค์เพื่อช่วยให้องค์กรพิจารณาความเสี่ยงเพิ่มเติมจากบริการหรือความสามารถที่อยู่นอกเหนือจากระบบ CCTV พื้นฐาน โดยยังคงใช้หลักการบริหารตามผลกระทบและความเสี่ยง รวมถึงระดับ B/E/H ตามบทที่ 2

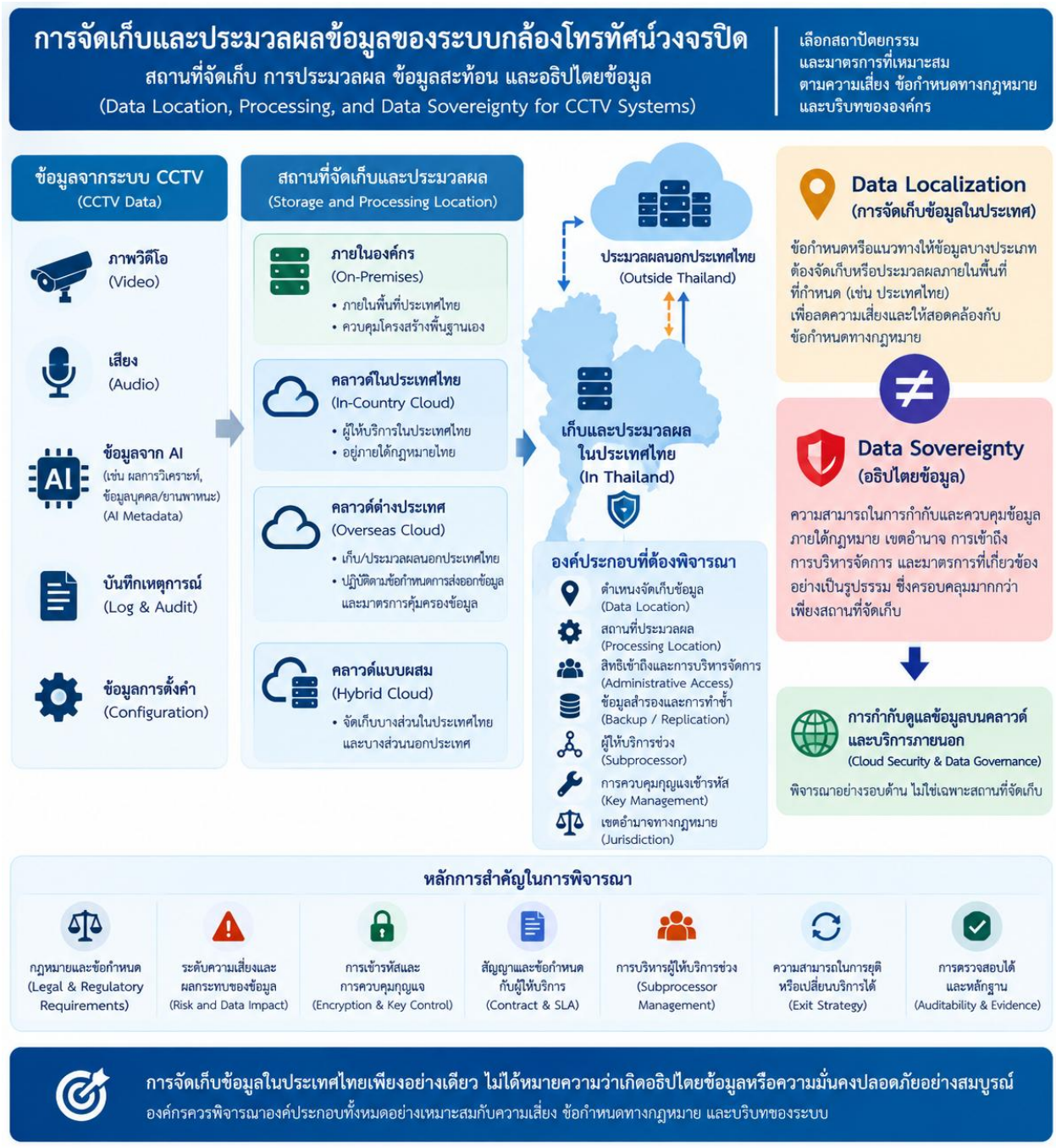
5.1 การใช้แอปพลิเคชัน อุปกรณ์เคลื่อนที่ คลาวด์ และบริการภายนอกอย่างมั่นคงปลอดภัย

ระบบ CCTV ในปัจจุบันอาจใช้บริการภายนอกเพื่อสนับสนุนการดูภาพจากระยะไกล การจัดเก็บข้อมูล การสำรองข้อมูล การแจ้งเตือน การบริหารอุปกรณ์ การปรับปรุงเฟิร์มแวร์ การจัดการบัญชี หรือการสนับสนุนทางเทคนิค

การใช้บริการดังกล่าวสามารถเพิ่มความสะดวก ความยืดหยุ่น และความสามารถในการบริหารจัดการระบบได้ แต่ในขณะเดียวกันอาจทำให้ข้อมูล การเข้าถึง หรือความสามารถในการควบคุมบางส่วนอยู่นอกโครงสร้างพื้นฐานที่องค์กรบริหารโดยตรง

องค์กรจึงควรพิจารณาอย่างน้อยว่า

ข้อมูลใดถูกส่งออกจากองค์กร ⟶ จัดเก็บที่ใด ⟶ ประมวลผลที่ใด ⟶ ใครสามารถเข้าถึง ⟶ ใครรับผิดชอบส่วนใด ⟶ หากเกิดเหตุจะดำเนินการอย่างไร ⟶ และหากต้องยุติบริการจะนำข้อมูลและระบบกลับมาอย่างไร



รูปที่ 5 การกำกับดูแลสถานที่จัดเก็บ การประมวลผล และอธิปไตยข้อมูลของระบบ CCTV

การกำหนดสถานที่จัดเก็บข้อมูล (Data Location) หรือการกำหนดให้ข้อมูลอยู่ภายในประเทศ (Data Localization) เป็นเพียงส่วนหนึ่งของการกำกับดูแลข้อมูล องค์กรควรพิจารณาร่วมกับสถานที่ประมวลผล การเข้าถึงเพื่อบริหารจัดการ การสำรองและทำซ้ำข้อมูล ผู้ให้บริการช่วง การควบคุมกุญแจเข้ารหัส และเขตอำนาจทางกฎหมาย เพื่อให้สามารถกำกับดูแลข้อมูลและความเสี่ยงได้อย่างเหมาะสม

5.1.1 การใช้แอปพลิเคชันและการเข้าถึงจากอุปกรณ์เคลื่อนที่

การเข้าถึงระบบ CCTV ผ่านโทรศัพท์เคลื่อนที่ แท็บเล็ต หรือแอปพลิเคชันสามารถเพิ่มความสะดวกในการเฝ้าระวังและการตอบสนองต่อเหตุ แต่ควรได้รับการควบคุมในลักษณะเดียวกับช่องทางการเข้าถึงระบบจากระยะไกลอื่น องค์กรควรพิจารณาทั้งความมั่นคงปลอดภัยของบัญชี แอปพลิเคชัน อุปกรณ์เคลื่อนที่ และข้อมูลที่อาจถูกบันทึกไว้ภายในอุปกรณ์ ประเด็นที่ควรพิจารณาเบื้องต้นมีดังต่อไปนี้

ประเด็น	แนวทางที่ควรพิจารณา
บัญชีผู้ใช้งาน	ควรใช้บัญชีที่สามารถระบุตัวผู้ใช้งานได้ และหลีกเลี่ยงการใช้บัญชีร่วมกัน
การพิสูจน์ตัวตนหลายปัจจัย (MFA)	ควรใช้สำหรับบัญชีสิทธิสูงหรือการเข้าถึงจากภายนอกเมื่อบริการรองรับ
สิทธิของผู้ใช้งาน	จำกัดสิทธิในการดูภาพย้อนหลัง ส่งออกข้อมูล หรือบริหารระบบตามหน้าที่
การแชร์ภาพหรือ Link	ไม่ควรเปิดการแชร์แบบสาธารณะหรือแบบไม่ต้องพิสูจน์ตัวตนโดยไม่มีเหตุผลและการควบคุมที่เหมาะสม
อุปกรณ์เคลื่อนที่	ควรมี Screen Lock ใช้ระบบปฏิบัติการที่ยังได้รับการสนับสนุน และไม่ควรถูกดัดแปลงจนลดกลไกด้านความมั่นคงปลอดภัย
การสูญหายของอุปกรณ์	ควรสามารถยกเลิก Session, Token หรือบัญชีที่เกี่ยวข้องได้
การบันทึกข้อมูลลงอุปกรณ์	ไม่ควรบันทึกภาพหรือข้อมูล CCTV ลงในพื้นที่ส่วนบุคคลโดยไม่จำเป็น
การปรับปรุงแอปพลิเคชัน	ควรติดตามและติดตั้งเวอร์ชันที่ยังได้รับการสนับสนุน
การแจ้งเตือนการเข้าสู่ระบบ	ควรเปิดใช้งานเมื่อระบบรองรับและเหมาะสมกับความเสี่ยง

สำหรับระบบที่มีความเสี่ยงสูง องค์กรอาจพิจารณาใช้ระบบบริหารอุปกรณ์เคลื่อนที่ (Mobile Device Management: MDM) หรือมาตรการอื่นที่ให้ผลด้านความมั่นคงปลอดภัยเทียบเท่า

5.1.2 ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของประเทศไทย

สำหรับองค์กรที่อยู่ภายใต้ขอบเขตของ **ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567** การใช้บริการคลาวด์สำหรับระบบ CCTV ควรพิจารณาข้อกำหนดตามประกาศดังกล่าวเพิ่มเติมจากแนวปฏิบัติฉบับนี้

ประกาศดังกล่าวมีผลบังคับใช้ตั้งแต่วันที่ **10 กันยายน 2569** และกำหนดกรอบการกำกับดูแลและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการใช้บริการคลาวด์ รวมถึงบทบาทและความรับผิดชอบของผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) และผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) ตามขอบเขตที่ประกาศกำหนด

องค์กรที่อยู่ภายใต้ขอบเขตควรพิจารณาอย่างน้อย

ประเด็น	แนวทางการพิจารณา
บทบาทขององค์กร	ระบุว่าองค์กรอยู่ในฐานะผู้ใช้บริการคลาวด์ (CSC) หรือมีบทบาทอื่นตามประกาศ
การประเมินผลกระทบ	พิจารณาระดับผลกระทบของข้อมูลหรือระบบที่นำขึ้นใช้บริการคลาวด์ตามข้อกำหนดที่เกี่ยวข้อง
การประเมินผู้ให้บริการ	ตรวจสอบว่าผู้ให้บริการมีคุณสมบัติและมาตรการควบคุมตามระดับที่เกี่ยวข้อง
การแบ่งความรับผิดชอบ	กำหนดความรับผิดชอบระหว่าง CSC และ CSP ให้ชัดเจน รวมถึงส่วนที่ต้องดำเนินการร่วมกัน
ข้อกำหนดในสัญญา	กำหนดมาตรการ บทบาท การแจ้งเหตุ การจัดการข้อมูล และการยุติบริการให้สอดคล้องกับข้อกำหนดที่เกี่ยวข้อง
การติดตามและทบทวน	ทบทวนผู้ให้บริการและการใช้บริการเมื่อบริบท ความเสี่ยง หรือข้อกำหนดเปลี่ยนแปลง
การรับรองหรือหลักฐาน	พิจารณาหลักฐานหรือการรับรองของผู้ให้บริการตามระดับผลกระทบและข้อกำหนดที่เกี่ยวข้อง

สำหรับบางกรณี โดยเฉพาะการให้บริการคลาวด์แก่ระบบที่มีผลกระทบระดับสูง ประกาศกำหนดข้อกำหนดเพิ่มเติมเกี่ยวกับคุณสมบัติของผู้ให้บริการและการรับรอง เช่น ISO/IEC 27017 หรือ CSA STAR Level 2 ตามเงื่อนไขที่กำหนด จึงควรตรวจสอบข้อกำหนดที่ใช้กับระบบจริง ไม่ควรนำเงื่อนไขดังกล่าวไปใช้เหมารวมกับระบบ CCTV ทุกประเภท

แนวปฏิบัติฉบับนี้มิได้ใช้แทนมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 หากองค์กรอยู่ภายใต้ขอบเขตของประกาศดังกล่าว ให้ถือปฏิบัติตามข้อกำหนดของประกาศควบคู่กัน

5.1.3 สถานที่จัดเก็บ การประมวลผล และอธิปไตยข้อมูล

การประเมินบริการคลาวด์ไม่ควรพิจารณาเพียงว่า “ศูนย์ข้อมูลอยู่ที่ประเทศใด” แต่ควรพิจารณาวงจรชีวิตและการควบคุมข้อมูลโดยรวม เพราะข้อมูลอาจถูกจัดเก็บ ประมวลผล สำรอง บริหาร หรือเข้าถึงจากหลายสถานที่ องค์กรควรสามารถตอบคำถามอย่างน้อยดังต่อไปนี้

ประเด็น	คำถามที่ควรตอบ
สถานที่จัดเก็บข้อมูล (Data Location)	ข้อมูลหลักและข้อมูลสำรองถูกจัดเก็บที่ใด
สถานที่ประมวลผล (Processing Location)	การประมวลผลข้อมูลเกิดขึ้นในประเทศหรือภูมิภาคใด
เขตอำนาจทางกฎหมาย (Jurisdiction)	กฎหมายหรือเขตอำนาจใดอาจมีผลต่อข้อมูลหรือผู้ให้บริการ
การเข้าถึงเพื่อบริหาร (Administrative Access)	บุคลากรหรือผู้ให้บริการจากพื้นที่ใดสามารถเข้าถึงระบบหรือข้อมูลได้
ผู้ให้บริการช่วง (Subprocessor)	มีผู้ให้บริการรายอื่นเกี่ยวข้องกับการจัดเก็บ ประมวลผล หรือสนับสนุนหรือไม่
การควบคุมกุญแจเข้ารหัส	ใครเป็นผู้ควบคุมหรือสามารถเข้าถึงกุญแจเข้ารหัส
ข้อมูลสำรองและสำเนา	Backup, Replica, Cache หรือสำเนาอื่นอยู่ที่ใด
การสนับสนุนทางเทคนิค	การเข้าถึงเพื่อแก้ไขปัญหาหรือบำรุงรักษาดำเนินการจากที่ใด

การกำหนดสถานที่จัดเก็บหรือประมวลผลข้อมูล

องค์กรอาจกำหนดให้ข้อมูลบางประเภทจัดเก็บหรือประมวลผลภายในประเทศไทย เมื่อมีเหตุผลจาก

- กฎหมายหรือประกาศที่มีผลใช้บังคับ
- ข้อกำหนดเฉพาะภาคส่วน
- นโยบายขององค์กร
- ข้อกำหนดในการจัดซื้อจัดจ้าง
- สัญญา
- ผลการประเมินความเสี่ยง

อย่างไรก็ตาม การจัดเก็บข้อมูลภายในประเทศไทยเพียงอย่างเดียวไม่ควรถูกตีความว่าทำให้ข้อมูลมีความมั่นคงปลอดภัยหรือมีอธิปไตยข้อมูลอย่างสมบูรณ์โดยอัตโนมัติ หากการบริหารระบบ การควบคุมกุญแจ การเข้าถึงข้อมูล หรือการสนับสนุนยังสามารถดำเนินการจากเขตอำนาจอื่นโดยไม่มีมาตรการควบคุมที่เหมาะสม

5.1.4 การเลือกผู้ให้บริการและความรับผิดชอบร่วม

การใช้บริการภายนอกทำให้ความรับผิดชอบบางส่วนถูกแบ่งระหว่างองค์กรและผู้ให้บริการ องค์กรจึงควรกำหนดให้ชัดเจนว่า ใครรับผิดชอบการควบคุมใด และเมื่อเกิดเหตุใครเป็นผู้ดำเนินการ ตัวอย่างประเด็นในการพิจารณาและตกลงการแบ่งความรับผิดชอบดังแสดงในต่อไปนี้

ประเด็น	คำถามที่ควรตอบ
ผู้ให้บริการหลักและผู้ให้บริการช่วง	ใครเป็นผู้ให้บริการหลัก และมีผู้ให้บริการช่วงรายใดเกี่ยวข้อง
ความรับผิดชอบด้านความมั่นคงปลอดภัย	ส่วนใดผู้ให้บริการรับผิดชอบ และส่วนใดองค์กรต้องกำหนดหรือดำเนินการเอง
บัญชีและสิทธิ	ใครบริหารบัญชี MFA สิทธิผู้ดูแลระบบ และสิทธิพิเศษ
การเข้ารหัสและกุญแจ	ใครเป็นผู้จัดการการเข้ารหัสและกุญแจ
บันทึกเหตุการณ์	ใครเก็บ Log และองค์กรสามารถเข้าถึงหรือขอข้อมูลได้หรือไม่
ช่องโหว่และการปรับปรุง	ใครรับผิดชอบ Patch, Security Update และ Security Advisory
การสำรองและกู้คืน	ใครเป็นผู้สำรองข้อมูล และสามารถกู้คืนได้ภายใต้เงื่อนไขใด
การจัดการเหตุการณ์	ผู้ให้บริการต้องแจ้งเหตุอย่างไร ใครเป็นผู้ประสานงาน และใครรับผิดชอบแต่ละขั้นตอน
วงจรชีวิตข้อมูล	ใครรับผิดชอบการเก็บรักษา คืน และลบข้อมูล
การยุติบริการ	ใครรับผิดชอบการนำข้อมูล ค่าตั้ง บัญชี และสิทธิออกจากบริการ

การแบ่งความรับผิดชอบควรได้รับการบันทึกในสัญญา เอกสารบริการ เมทริกซ์ความรับผิดชอบ (Responsibility Matrix) หรือหลักฐานอื่นตามความเหมาะสม โดยแต่ละองค์กรสามารถตกลงการแบ่งบทบาทความรับผิดชอบให้เหมาะสมในแต่ละกรณีการใช้งานได้

5.1.5 การคุ้มครองข้อมูลส่วนบุคคลและการใช้ผู้ให้บริการภายนอก

หากผู้ให้บริการสามารถเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลแทนองค์กร ควรกำหนดบทบาทหน้าที่ และมาตรการที่เกี่ยวข้องให้ชัดเจนและสอดคล้องกับกฎหมายที่มีผลใช้บังคับ ควรพิจารณาอย่างน้อย

ประเด็น	สิ่งที่ควรกำหนด
ขอบเขตข้อมูล	ผู้ให้บริการสามารถเข้าถึงข้อมูลประเภทใด
วัตถุประสงค์	การประมวลผลดำเนินการเพื่อวัตถุประสงค์ใด
คำสั่งของผู้ควบคุมข้อมูล	ผู้ให้บริการดำเนินการตามคำสั่งหรือเงื่อนไขใด

ประเด็น	สิ่งที่ควรกำหนด
การรักษาความลับ	บุคลากรของผู้ให้บริการมีหน้าที่รักษาความลับอย่างไร
มาตรการด้านความมั่นคงปลอดภัย	ใช้มาตรการใดเพื่อป้องกันข้อมูล
ผู้ให้บริการช่วง	มีเงื่อนไขในการแต่งตั้งหรือเปลี่ยนผู้ให้บริการช่วงอย่างไร
การแจ้งเหตุละเมิดข้อมูล	ต้องแจ้งเหตุประเภทใด ผ่านช่องทางใด และภายในระยะเวลาที่เหมาะสม
การสนับสนุนสิทธิของเจ้าของข้อมูล	ผู้ให้บริการต้องช่วยดำเนินการอย่างไรเมื่อมีคำขอ
การคืนข้อมูล	เมื่อสิ้นสุดบริการ จะคืนข้อมูลในรูปแบบใด
การลบข้อมูลอย่างมั่นคงปลอดภัย	ลบข้อมูลหลัก ข้อมูลสำรอง และสำเนาที่เกี่ยวข้องอย่างไร
สิทธิในการตรวจสอบ	องค์กรสามารถขอหลักฐานหรือประเมินการควบคุมได้ในระดับใด

การมีใบรับรองมาตรฐานของผู้ให้บริการสามารถใช้เป็นหลักฐานประกอบได้ แต่ไม่ควรใช้แทนการพิจารณาบทบาท สัญญา ขอบเขตบริการ และมาตรการควบคุมที่เกี่ยวข้อง มาตรฐาน เช่น **ISO/IEC 27017** และ **ISO/IEC 27018** สามารถใช้เป็นกรอบอ้างอิงเพิ่มเติมสำหรับบริการคลาวด์ตามความเหมาะสม

5.1.6 การจัดการระยะเวลาเก็บรักษา การคืน และการลบข้อมูล

บริการคลาวด์หรือบริการภายนอกควรสามารถรองรับนโยบายการเก็บรักษาข้อมูลขององค์กร และควรมีความชัดเจนว่าข้อมูลถูกเก็บอยู่ในองค์ประกอบใดบ้าง ควรพิจารณาครอบคลุมตามความเกี่ยวข้องถึง

- พื้นที่จัดเก็บหลัก (Primary Storage)
- ข้อมูลสำรอง (Backup)
- สำเนาหรือข้อมูลที่ทำซ้ำ (Replica)
- ข้อมูลชั่วคราว (Cache)
- ข้อมูลที่ส่งออก
- บันทึกเหตุการณ์และข้อมูลกำกับ (Log/Metadata)

ตัวอย่างมาตรการที่ควรพิจารณามีดังนี้

มาตรการ	B	E	H
สามารถกำหนดระยะเวลาเก็บรักษาให้สอดคล้องกับนโยบายองค์กร	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ

มาตรการ	B	E	H
มีวิธีคืนหรือส่งออกข้อมูลเมื่อจำเป็น	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
กำหนดวิธีและระยะเวลาการลบเมื่อสิ้นสุดบริการ	พึงปฏิบัติ	พึงปฏิบัติ	พึงปฏิบัติ
การลบครอบคลุมข้อมูลสำรองหรือสำเนาตามความเกี่ยวข้อง	ควรพิจารณา	พึงปฏิบัติ	พึงปฏิบัติ
สามารถให้หลักฐานการลบตามระดับความเสี่ยง	—	ควรพิจารณา	พึงปฏิบัติ

ไม่ควรกำหนดระยะเวลาลบข้อมูล เช่น “ภายใน 30 วัน” เป็นค่าเดียวสำหรับทุกบริการโดยไม่มีเหตุผลรองรับ หากไม่มีกฎหมายหรือข้อกำหนดกำหนดไว้ ควรกำหนดระยะเวลาที่เหมาะสมในสัญญาหรือเงื่อนไขบริการตามความเสี่ยงและความสามารถทางเทคนิค

5.1.7 การแจ้งเหตุและการเปลี่ยนแปลงบริการ

ผู้ให้บริการควรมีช่องทางและกระบวนการแจ้งเหตุหรือการเปลี่ยนแปลงที่อาจมีผลต่อความมั่นคงปลอดภัย ความเป็นส่วนตัว หรือความต่อเนื่องของระบบ เหตุการณ์หรือการเปลี่ยนแปลงที่ควรพิจารณากำหนดให้แจ้ง ได้แก่

ประเภท	ตัวอย่าง
เหตุด้านความมั่นคงปลอดภัย	การเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล หรือการโจมตีบริการ
เหตุละเมิดข้อมูลส่วนบุคคล	เหตุที่เกี่ยวข้องกับข้อมูล CCTV ขององค์กร
การหยุดชะงักของบริการ	บริการไม่สามารถให้บริการได้ในระดับที่มีนัยสำคัญ
เหตุเกี่ยวกับกุญแจหรือการเข้ารหัส	กุญแจรั่วไหล สูญหาย หรือถูกเปลี่ยนโดยไม่ได้รับอนุญาต
การเปลี่ยนสถานที่จัดเก็บหรือประมวลผล	ย้ายข้อมูลไปยังประเทศ ภูมิภาค หรือศูนย์ข้อมูลใหม่
การเปลี่ยนผู้ให้บริการช่วง	เพิ่มหรือเปลี่ยนผู้ให้บริการที่เกี่ยวข้องกับข้อมูล
การเปลี่ยนมาตรการสำคัญ	เปลี่ยนวิธีพิสูจน์ตัวตน การเข้ารหัส หรือมาตรการที่มีผลต่อความเสี่ยง
การยุติฟังก์ชันหรือการสนับสนุน	ยุติ Feature, API หรือบริการที่องค์กรพึ่งพา

ระยะเวลาการแจ้งควรกำหนดจากกฎหมาย ความรุนแรงของเหตุ ความต้องการในการตอบสนอง และความเสี่ยงขององค์กร ไม่จำเป็นต้องใช้กรอบเวลา 24 48 หรือ 72 ชั่วโมงเดียวกันสำหรับเหตุทุกประเภท

5.1.8 การยุติหรือเปลี่ยนบริการ

องค์กรควรพิจารณาแนวทางและแผนการยุติหรือเปลี่ยนบริการตั้งแต่ก่อนเริ่มใช้งาน เพื่อป้องกันการพึ่งพาผู้ให้บริการจนไม่สามารถย้ายข้อมูลหรือระบบได้เมื่อมีความจำเป็น แผนการยุติหรือเปลี่ยนบริการควรตอบคำถามอย่างน้อยดังต่อไปนี้

ประเด็น	คำถามที่ควรตอบ
ข้อมูล	จะนำข้อมูลกลับออกมาอย่างไรและในรูปแบบใด
ค่าตั้งระบบ	สามารถส่งออกค่าตั้งหรือข้อมูลการกำหนดระบบได้หรือไม่
บัญชีและสิทธิ	ต้องเพิกถอนบัญชี สิทธิ Session หรือ Token ใด
กุญแจและใบรับรอง	ต้องยกเลิกหรือเปลี่ยนกุญแจหรือใบรับรองใด
ข้อมูลสำรอง	ข้อมูลสำรองจะถูกเก็บไว้นานเท่าใดและลบเมื่อใด
การลบข้อมูล	ผู้ให้บริการจะลบข้อมูลจากระบบหลักและสำเนาที่เกี่ยวข้องอย่างไร
หลักฐาน	สามารถขอหลักฐานการลบหรือปิดบริการได้หรือไม่
ความต่อเนื่อง	หากบริการหยุดให้บริการก่อนการย้ายเสร็จ จะดำเนินงานต่ออย่างไร

5.2 ระบบ CCTV ที่ใช้การวิเคราะห์วิดีโอ ปัญญาประดิษฐ์ หรือข้อมูลชีวมิติ

ระบบ CCTV ที่มีการใช้ปัญญาประดิษฐ์ การวิเคราะห์วิดีโอขั้นสูง การระบุหรือติดตามบุคคล หรือการประมวลผลข้อมูลชีวมิติ อาจทำให้ลักษณะของข้อมูล วัตถุประสงค์การใช้งาน ความสามารถในการตัดสินใจ และผลกระทบต่อบุคคลแตกต่างจากระบบ CCTV ทั่วไป

แนวปฏิบัติฉบับนี้แนะนำมาตรการพื้นฐานด้านความมั่นคงปลอดภัยของระบบ CCTV ส่วนการประเมินและมาตรการเฉพาะด้าน AI ควรศึกษาเพิ่มเติมจาก แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย (เพื่อความกระชับ ในหัวข้อนี้แนวปฏิบัตินี้จะถูกอ้างถึงว่า “แนวปฏิบัติ CCTV-AI”) ตามลักษณะการใช้งานและระดับผลกระทบ

แนวทางดังกล่าวช่วยหลีกเลี่ยงความซ้ำซ้อนของเนื้อหาระหว่างสองเอกสาร และทำให้ระบบที่มี AI ยังคงใช้มาตรการพื้นฐานของ CCTV เช่น Network Security, Access Control, Product Security, Logging, Retention, Incident Response และ Lifecycle Management ร่วมกับมาตรการเฉพาะด้าน AI

5.2.1 เมื่อใดควรใช้แนวปฏิบัติ CCTV-AI เพิ่มเติม

องค์กรควรพิจารณาใช้ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย เพิ่มเติม เมื่อระบบมีความสามารถ เช่น

ความสามารถ	ตัวอย่าง
การตรวจจับด้วย AI	ตรวจจับบุคคล ยานพาหนะ วัตถุ หรือเหตุการณ์ด้วยแบบจำลอง AI
การจำแนกประเภท	จำแนกบุคคล วัตถุ หรือพฤติกรรมตามคุณลักษณะที่กำหนด
การติดตาม	ติดตามบุคคลหรือวัตถุข้ามเวลา พื้นที่ หรือกล้องหลายตัว
การวิเคราะห์พฤติกรรม	ประเมินรูปแบบการเคลื่อนไหวหรือพฤติกรรมจากข้อมูลวิดีโอ
การอ่านป้ายทะเบียนด้วย AI	วิเคราะห์หรืออ่านข้อความจากป้ายทะเบียน
การระบุหรือยืนยันบุคคล	เปรียบเทียบข้อมูลเพื่อระบุหรือยืนยันตัวบุคคล
การรู้จำใบหน้า	ใช้ลักษณะใบหน้าเพื่อค้นหา ระบุ หรือยืนยันบุคคล
การประมวลผลข้อมูลชีวมิติ	ใช้ลักษณะทางกายภาพหรือชีวลักษณะเพื่อวัตถุประสงค์เกี่ยวกับตัวบุคคล
การสร้างคะแนนหรือข้อสรุปเกี่ยวกับบุคคล	สร้างคะแนน ประเภท หรือข้อสรุปจากข้อมูลวิดีโอ
การเชื่อมโยงกับฐานข้อมูลอื่น	นำผล AI ไปเชื่อมกับข้อมูลบุคคลหรือระบบอื่น
การดำเนินการต่อโดยอัตโนมัติ	ใช้ผล AI เพื่อแจ้งเตือน ปลดล็อก ปิดกั้น หรือสั่งการระบบอื่น

หลักการสำคัญ คือ การรักษาความมั่นคงปลอดภัยของระบบ CCTV ที่มีการใช้ปัญญาประดิษฐ์ (AI-Enabled CCTV) ควรประกอบด้วยมาตรการพื้นฐานด้านความมั่นคงปลอดภัยของระบบ CCTV ตามแนวปฏิบัติฉบับนี้ ร่วมกับการประเมินความเสี่ยงและการกำหนดมาตรการเพิ่มเติมที่เกี่ยวข้องกับการใช้ปัญญาประดิษฐ์ตาม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย

5.2.2 การพิจารณาเพิ่มเติมสำหรับระบบที่มีความสามารถด้านปัญญาประดิษฐ์

เมื่อมีการเพิ่มความสามารถด้าน AI ให้แก่ระบบ CCTV องค์กรควรใช้มาตรการด้านความมั่นคงปลอดภัยตามแนวปฏิบัติฉบับนี้เป็น ค่าตั้งต้นด้านความมั่นคงปลอดภัย (Security Baseline) และประเมินความเสี่ยงเพิ่มเติมที่เกิดจากการใช้ AI ตามลักษณะการใช้งานและระดับผลกระทบ

การมีฟังก์ชัน AI อยู่ในกล้อง ระบบบริหารจัดการวิดีโอ บริการคลาวด์ หรือผลิตภัณฑ์ที่จัดซื้อมา มิได้หมายความว่าองค์กรควรเปิดใช้งานฟังก์ชันดังกล่าวโดยอัตโนมัติ ก่อนนำมาใช้งานควรพิจารณาวัตถุประสงค์ความจำเป็น ลักษณะข้อมูล ผลกระทบต่อบุคคล การเชื่อมโยงกับระบบอื่น และผลกระทบหากผลลัพธ์ของ AI ไม่ถูกต้อง ประเด็นที่ควรพิจารณาเบื้องต้น ได้แก่

ประเด็น	แนวทางพิจารณา
วัตถุประสงค์และความจำเป็น	ระบุว่าต้องการใช้ AI เพื่อวัตถุประสงค์ใด และการใช้ AI มีความจำเป็นและได้สัดส่วนหรือไม่
ข้อมูลที่ใช้และข้อมูลที่สร้างขึ้น	พิจารณาว่าระบบใช้ภาพ วิดีโอ ข้อมูลชีวมิติ ข้อมูลจากระบบอื่น หรือสร้างข้อมูลจากการวิเคราะห์หรืออนุมานเพิ่มเติมหรือไม่
ผลกระทบต่อบุคคล	พิจารณาผลกระทบหากระบบตรวจจับ จำแนก ระบุ หรือติดตามบุคคลผิดพลาด
การเชื่อมโยงกับระบบอื่น	พิจารณาว่าผลลัพธ์จาก AI ถูกนำไปใช้กับฐานข้อมูล ระบบควบคุมการเข้าออก ระบบแจ้งเตือน หรือระบบอื่นหรือไม่
การดำเนินการอัตโนมัติ	หากผลลัพธ์จาก AI สามารถทำให้เกิดการดำเนินการโดยอัตโนมัติ ควรพิจารณาขอบเขตอำนาจ การอนุมัติ การตรวจสอบ และความสามารถในการหยุดหรือแทรกแซงตามระดับผลกระทบ
ข้อมูลชีวมิติ	หากมีการระบุหรือยืนยันตัวบุคคลด้วยข้อมูลชีวมิติ ควรพิจารณาข้อกำหนดด้านกฎหมาย ความเป็นส่วนตัว ความมั่นคงปลอดภัย และความถูกต้องของระบบเพิ่มเติม
การกำกับดูแลและความรับผิดชอบ	กำหนดผู้รับผิดชอบ ผู้อนุมัติ ผู้ตรวจสอบ และกลไกติดตามผลการใช้งาน AI ให้ชัดเจน

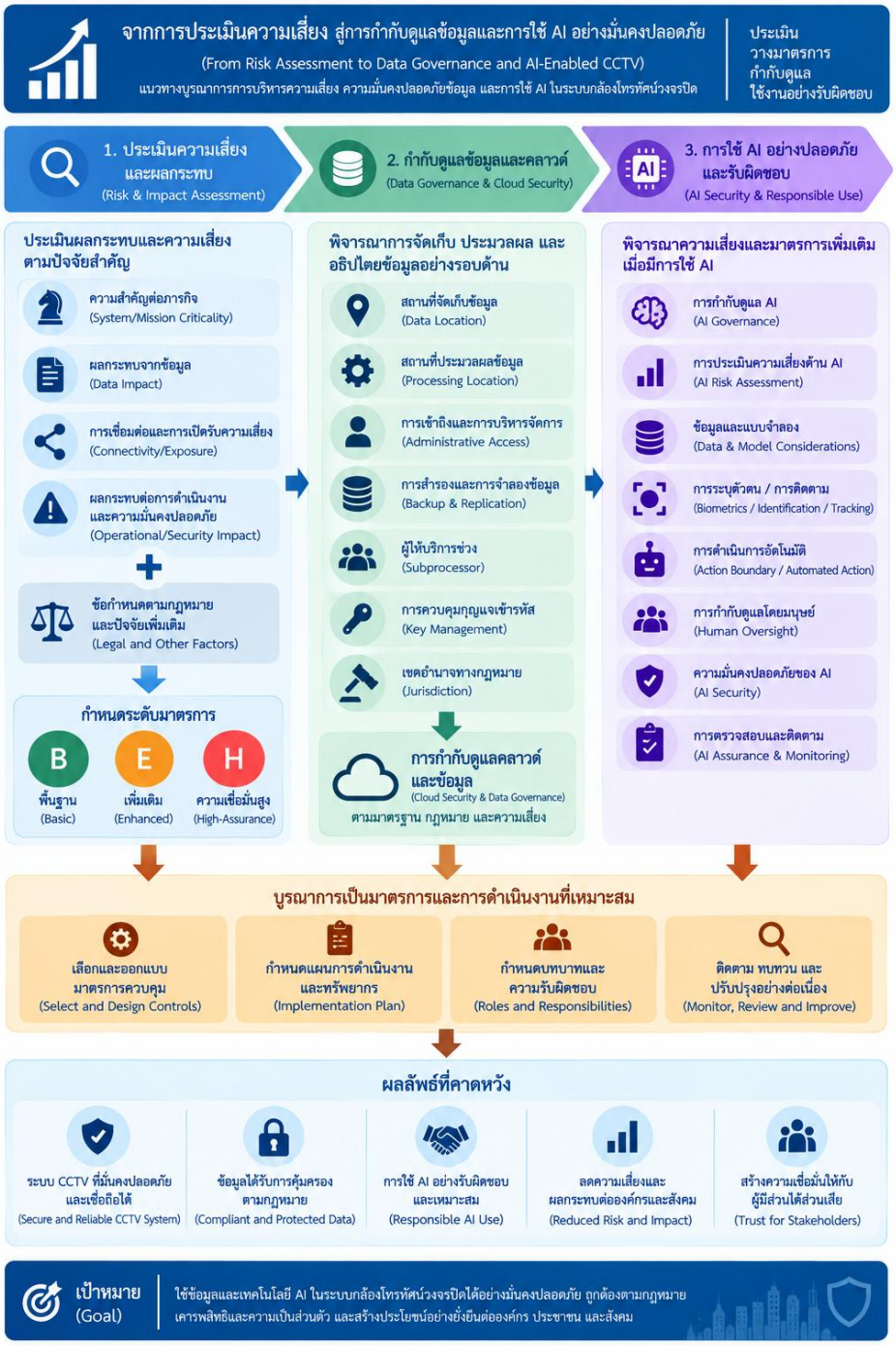
องค์กรสามารถศึกษารายละเอียดเกี่ยวกับการบริหารความเสี่ยงด้าน AI (AI Risk Management) การประเมินผลกระทบของ AI (AI Impact Assessment) ความมั่นคงปลอดภัยของ AI (AI Security) การกำกับดูแลโดยมนุษย์ (Human Oversight) ความถูกต้องและความทนทานของระบบ ตลอดจนมาตรการสำหรับข้อมูลชีวมิติและการดำเนินการอัตโนมัติ จากแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย

5.2.3 ความสัมพันธ์ระหว่างแนวปฏิบัติ CCTV ทั้งสองฉบับ

แนวปฏิบัติฉบับนี้กำหนดมาตรการพื้นฐานด้านความมั่นคงปลอดภัยสำหรับระบบ CCTV โดยไม่ขึ้นอยู่กับว่าระบบมีการใช้ AI หรือไม่ ส่วน แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย กำหนดแนวทางเพิ่มเติมสำหรับความเสี่ยงที่เกิดจากการใช้ AI การ

วิเคราะห์ข้อมูลขั้นสูง การประมวลผลข้อมูลชีวมิติ และการนำผลลัพธ์จาก AI ไปใช้ในการตัดสินใจหรือดำเนินการ ดังนั้น ระบบ CCTV ที่มี AI ควรใช้แนวปฏิบัติทั้งสองฉบับร่วมกันตามลักษณะของระบบ ดังนี้

ลักษณะของระบบ	แนวปฏิบัติ CCTV ฉบับนี้	แนวปฏิบัติ CCTV-AI
CCTV สำหรับดูและบันทึกภาพทั่วไป	ใช้เป็นหลัก	ไม่จำเป็น
CCTV เชื่อมต่อเครือข่ายหรือบริการคลาวด์ แต่ไม่มี AI	ใช้เป็นหลัก	ไม่จำเป็น
การตรวจจับการเคลื่อนไหวพื้นฐานที่ไม่ได้ใช้ AI	ใช้เป็นหลัก	พิจารณาตามลักษณะการทำงานจริง
การตรวจจับหรือจำแนกบุคคล ยานพาหนะ หรือวัตถุด้วย AI	ใช้เป็นพื้นฐาน	ใช้เพิ่มเติม
การติดตามบุคคลหรือวัตถุด้วย AI	ใช้เป็นพื้นฐาน	ใช้เพิ่มเติม
การอ่านป้ายทะเบียนโดยใช้ AI	ใช้เป็นพื้นฐาน	ใช้เพิ่มเติม
การรู้จำใบหน้าหรือการประมวลผลข้อมูลชีวมิติ	ใช้เป็นพื้นฐาน	ใช้เพิ่มเติม
AI เชื่อมโยงผลลัพธ์กับฐานข้อมูลหรือระบบอื่น	ใช้เป็นพื้นฐาน	ใช้เพิ่มเติม
AI ใช้ผลลัพธ์เพื่อสั่งการหรือดำเนินการโดยอัตโนมัติ	ใช้เป็นพื้นฐาน	ใช้เพิ่มเติม โดยพิจารณามาตรการกำกับดูแลตามระดับผลกระทบ



รูปที่ 6 กรอบบูรณาการจากการประเมินความเสี่ยงสู่การกำกับดูแลข้อมูล คลาวด์ และระบบ CCTV ที่ใช้ AI

การบริหารระบบ CCTV ควรเชื่อมโยงการประเมินความเสี่ยงกับการกำหนดระดับมาตรการ การกำกับดูแลข้อมูลและบริการคลาวด์ และมาตรการเพิ่มเติมเมื่อมีการใช้ AI เพื่อให้ระดับการควบคุม การกำกับดูแล และการสร้างความเชื่อมั่นสอดคล้องกับความเสี่ยงและผลกระทบของระบบ

5.3 การทำงานร่วมกันระหว่างหน่วยงานและการแบ่งปันข้อมูลในภาวะฉุกเฉิน

สำหรับหน่วยงานของรัฐ องค์กรปกครองส่วนท้องถิ่น ผู้ดูแลโครงสร้างพื้นฐาน และโครงการเมืองอัจฉริยะ ที่อาจต้องเชื่อมต่อหรือแบ่งปันทรัพยากรกล้องระหว่างหน่วยงานแบบเรียลไทม์ในภาวะฉุกเฉินหรือสาธารณภัย เช่น ภัยธรรมชาติ อาคารถล่ม อัคคีภัย แก๊สระเบิด การค้นหาบุคคลสูญหาย การติดตามผู้ก่อเหตุ หรือการวิเคราะห์เพื่อป้องกันการก่อการร้าย ซึ่งในทางปฏิบัติมักติดข้อจำกัดด้านกฎหมาย ระเบียบ และเทคนิคจนไม่สามารถทำงานร่วมกันได้ทันเวลา

แนวปฏิบัตินี้ไม่สร้างอำนาจหรือหน้าที่ใหม่ในการเปิดเผยข้อมูล การแบ่งปันข้อมูลระหว่างหน่วยงานยังคงต้องเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการป้องกันและบรรเทาสาธารณภัย และอำนาจหน้าที่ของแต่ละหน่วยงาน ประเด็นต่อไปนี้มีวัตถุประสงค์เพื่อให้หน่วยงานเตรียมความพร้อมไว้ล่วงหน้า เพื่อให้เมื่อเกิดเหตุสามารถดำเนินการได้อย่างถูกต้อง รวดเร็ว และตรวจสอบได้

ประเด็น	ข้อควรพิจารณา
ข้อตกลงล่วงหน้า	จัดทำบันทึกข้อตกลงหรือข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement) ระหว่างหน่วยงานไว้ก่อนเกิดเหตุ ระบุวัตถุประสงค์ เงื่อนไขการเปิดใช้ ผู้มีอำนาจอนุมัติ ขอบเขตกล้อง/พื้นที่ ระยะเวลา และการยุติการแบ่งปัน
ฐานทางกฎหมายและอำนาจหน้าที่	ระบุฐานทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ใช้สำหรับแต่ละกรณี เช่น การป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล หรือการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ รวมถึงอำนาจหน้าที่ตามกฎหมายว่าด้วยการป้องกันและบรรเทาสาธารณภัยและกฎหมายเฉพาะที่เกี่ยวข้อง โดยปรึกษาฝ่ายกฎหมายและตรวจสอบประกาศฉบับปัจจุบัน
ลำดับความสำคัญของกรณี	จัดกลุ่มกรณีตามลำดับ เช่น (1) ภัยต่อชีวิตและสาธารณภัย เช่น อัคคีภัย อาคารถล่ม แก๊สระเบิด อุทกภัย (2) การค้นหาบุคคลสูญหายและผู้ประสบภัย (3) การติดตามผู้ก่อเหตุและการวิเคราะห์ภัยคุกคาม (4) การบริหารจัดการเมืองอัจฉริยะ (Smart City) และการประมวลผลจากกลุ่มกล้อง/เซนเซอร์ โดยกรณีที่มีลำดับต่ำกว่าควรมีเงื่อนไขและการอนุมัติที่เข้มงวดกว่า
กลไกทางเทคนิคในการเชื่อมต่อ	ใช้ช่องทางที่เข้ารหัสและเป็นมาตรฐาน เช่น การส่งต่อภาพผ่าน ONVIF/RTSP over TLS การเชื่อม VMS ระหว่างหน่วยงาน (Federation) หรือ API ที่มีการพิสูจน์ตัวตน ผ่านโซนกันชน (DMZ) ที่แยกจากเครือข่ายภายใน ไม่เปิดกล้องหรือเครื่องบันทึกสู่อินเทอร์เน็ตโดยตรง

ประเด็น	ข้อควรพิจารณา
สิทธิชั่วคราวและการควบคุม	ให้สิทธิเฉพาะกล้อง พื้นที่ และช่วงเวลาที่จำเป็น มีวันหมดอายุอัตโนมัติ ต้องได้รับอนุมัติจากผู้มีอำนาจของหน่วยงานเจ้าของกล้อง และบันทึกทุกการเข้าถึงและการส่งออกไว้เป็นหลักฐาน (Audit Log และ Chain of Custody)
คุณภาพและความพร้อมใช้งาน	ทดสอบการเชื่อมต่อและซ้อมแผนร่วมกันตามรอบ กำหนดการทำงานเมื่อเครือข่ายหลักล้มเหลว (เช่น ช่องทางสำรอง การบันทึกที่อุปกรณ์ปลายทาง) และตรวจสอบเวลา (NTP) ให้ตรงกันทุกหน่วยงาน
เมืองอัจฉริยะ แฝดดิจิทัล และการประมวลผลแบบกลุ่ม	หากเชื่อมข้อมูลกล้องเข้ากับแพลตฟอร์ม Smart City, Digital Twin หรือการวิเคราะห์จากกล้องและสมาร์ทเซนเซอร์แบบกลุ่ม ควรใช้ข้อมูลที่ลดทอนการระบุตัวบุคคล (เช่น สถิติ เหตุการณ์ ตำแหน่ง) เป็นค่าเริ่มต้น และเปิดการเข้าถึงภาพจริงเฉพาะเมื่อมีเหตุและได้รับอนุมัติ พร้อมประเมินความเสี่ยงเพิ่มเติมตามแนวปฏิบัติ CCTV-AI
การยุติและการทำลายข้อมูล	เมื่อสิ้นสุดเหตุการณ์ ให้เพิกถอนสิทธิ ยุติการส่งต่อภาพ ตกลงว่าหน่วยงานผู้รับจะเก็บหรือทำลายข้อมูลอย่างไร และบันทึกสรุปการแบ่งปันข้อมูลไว้เป็นหลักฐาน

หน่วยงานที่คาดว่าจะต้องแบ่งปันข้อมูลบ่อยครั้งควรออกแบบระบบให้รองรับตั้งแต่ต้น โดยจัดให้มีจุดเชื่อมต่อที่ควบคุมได้ แทนการเปิดสิทธิเฉพาะกิจในภาวะเร่งด่วน และควรทบทวนข้อตกลงและซ้อมแผนร่วมกับหน่วยงานที่เกี่ยวข้องอย่างน้อยปีละครั้ง

สรุปหลักการของบทที่ 5

การใช้แอปพลิเคชัน อุปกรณ์เคลื่อนที่ บริการคลาวด์ ผู้ให้บริการภายนอก หรือความสามารถด้าน AI อาจทำให้ขอบเขตการเชื่อมต่อ การประมวลผลข้อมูล ผู้ที่สามารถเข้าถึงระบบ และผลกระทบจากการใช้งานแตกต่างจากระบบ CCTV พื้นฐาน องค์กรจึงควรประเมินความเสี่ยงเพิ่มเติมตามลักษณะของบริการและเทคโนโลยีที่นำมาใช้

สำหรับบริการคลาวด์และบริการภายนอก ควรพิจารณาร่วมกันทั้งสถานที่จัดเก็บและประมวลผลข้อมูล เขตอำนาจทางกฎหมาย การเข้าถึงเพื่อบริหาร การควบคุมกุญแจ ผู้ให้บริการช่วง ความรับผิดชอบร่วม และความสามารถในการคืน ลบ หรือย้ายข้อมูลเมื่อสิ้นสุดบริการ โดยไม่ควรใช้รูปแบบการติดตั้งหรือสถานที่จัดเก็บข้อมูลเพียงปัจจัยเดียวในการสรุประดับความมั่นคงปลอดภัย

สำหรับระบบ CCTV ที่มีการใช้ AI ควรใช้มาตรการด้านความมั่นคงปลอดภัยของระบบ CCTV ทั่วไปเป็นพื้นฐานตามที่ได้แนะนำในเอกสารฉบับนี้ และประเมินความเสี่ยงเพิ่มเติมจากวัตถุประสงค์ ข้อมูล การวิเคราะห์หรืออนุมาน การเชื่อมโยงกับระบบอื่น การใช้ข้อมูลชีวมิติ และผลกระทบจากการนำผลลัพธ์ของ AI ไปใช้ โดยรายละเอียดของมาตรการเฉพาะด้าน AI ให้พิจารณาตาม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย

การพิจารณามาตรการเพิ่มเติมควรเริ่มจากวัตถุประสงค์และบริบทของการใช้งาน ประเมินข้อมูลและการเชื่อมต่อ ระบุผู้รับผิดชอบและข้อกำหนดที่เกี่ยวข้อง ประเมินผลกระทบและความเสี่ยง กำหนดมาตรการควบคุม และติดตามทบทวนตลอดวงจรชีวิตของระบบ

สำหรับการแบ่งปันข้อมูลระหว่างหน่วยงานในภาวะฉุกเฉิน ให้ใช้หลักฐานและกรอบความรับผิดชอบที่มีอยู่แล้วตามแนวปฏิบัตินี้เป็นฐาน จัดทำข้อตกลงและกลไกไว้ล่วงหน้า และคงหลักความจำเป็น ความได้สัดส่วน และการตรวจสอบได้ตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ภาคผนวก ก รายการตรวจสอบก่อนส่งมอบ

ภาคผนวกนี้ใช้เป็นรายการตรวจสอบสำหรับเจ้าของระบบ ผู้ติดตั้ง ผู้รวมระบบ และผู้ตรวจรับ ก่อนเปิดใช้งานระบบ CCTV เพื่อยืนยันว่าระบบที่ติดตั้งและส่งมอบสอดคล้องกับขอบเขต แบบ และข้อกำหนดที่ได้รับอนุมัติ มีมาตรการด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลที่เหมาะสม และมีข้อมูลหรือเอกสารเพียงพอสำหรับการบริหาร บำรุงรักษา และตรวจสอบระบบในระยะต่อไป

รายการตรวจสอบนี้เป็นแนวทางพื้นฐาน องค์กรสามารถเพิ่มเติม ปรับลด หรือกำหนดระดับรายละเอียดตามระดับความสำคัญ B/E/H ลักษณะการใช้งาน สถาปัตยกรรมของระบบ และผลการประเมินความเสี่ยง โดยไม่จำเป็นต้องใช้ทุกรายการกับทุกระบบ

ผลการตรวจสอบแนะนำให้ใช้สถานะดังต่อไปนี้

สถานะ	ความหมาย
ผ่าน	ตรวจสอบแล้วและเป็นไปตามข้อกำหนด
ต้องแก้ไข	ยังไม่เป็นไปตามข้อกำหนดและต้องดำเนินการแก้ไข
ผ่านโดยมีเงื่อนไข	สามารถรับมอบได้โดยมีมาตรการชั่วคราว ผู้รับผิดชอบ และกำหนดเวลาแก้ไข
ไม่เกี่ยวข้อง	ไม่ใช้กับระบบหรือขอบเขตที่ตรวจสอบ โดยควรระบุเหตุผลเมื่อจำเป็น

ก.1 ข้อมูลทั่วไปของระบบ

รายการ	ข้อมูล
ชื่อโครงการ/ระบบ	
หน่วยงานเจ้าของระบบ	
พื้นที่ติดตั้ง	
ผู้ผลิต/ผู้จำหน่าย	
ผู้ติดตั้งหรือผู้รวมระบบ	
ผู้ให้บริการบำรุงรักษา	
วันที่ตรวจรับ	
ผู้ตรวจรับ	
ระดับความสำคัญของระบบ	☐ B ☐ E ☐ H
จำนวนกล้อง	

รายการ	ข้อมูล
ระบบบริหารวิดีโอ/เครื่องบันทึก	
ระบบจัดเก็บข้อมูล	
ใช้บริการคลาวด์หรือบริการภายนอก	☐ ใช่ ☐ ไม่ใช่
มีการเข้าถึงจากระยะไกล	☐ ใช่ ☐ ไม่ใช่
มีการใช้ AI หรือข้อมูลชีวมิติ	☐ ใช่ ☐ ไม่ใช่

กรณีมีการใช้ AI หรือข้อมูลชีวมิติ ควรพิจารณา แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย เพิ่มเติมตามลักษณะและระดับผลกระทบของระบบ

ก.2 การตรวจสอบการออกแบบ ตำแหน่งติดตั้ง และคุณภาพของภาพ

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
วัตถุประสงค์ของกล้องแต่ละจุดได้รับการกำหนดไว้อย่างชัดเจน		
ตำแหน่งและมุมมองของกล้องตรงกับแบบที่ได้รับอนุมัติ		
พื้นที่ครอบคลุมของภาพเหมาะสมกับวัตถุประสงค์		
ระดับรายละเอียดของภาพสอดคล้องกับความต้องการเชิงปฏิบัติการรายจุด (Point Operational Requirements: POR)		
กรณีมีการกำหนดระดับ DORI ได้ตรวจสอบระดับการตรวจพบ การสังเกต การจดจำ หรือการระบุตัวตามวัตถุประสงค์แล้ว		
ความหนาแน่นของพิกเซล (Pixel Density) เพียงพอต่อวัตถุประสงค์ของจุดติดตั้ง		
ได้ทดสอบคุณภาพของภาพในสภาพกลางวันและกลางคืนตามช่วงเวลาการใช้งานจริง		
พื้นที่ที่มีความแตกต่างของแสงสูงได้รับการทดสอบการทำงานของช่วงไดนามิกกว้าง (Wide Dynamic Range: WDR) หรือมาตรการที่เกี่ยวข้อง		

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
กรณีใช้แสงอินฟราเรด (Infrared: IR) ได้ตรวจสอบระยะและปัญหาการสะท้อนกลับแล้ว		
ไม่มีวัตถุหรือสภาพแวดล้อมที่ทำให้เกิดจุดอับโดยไม่เหมาะสม		
กล้องไม่ครอบคลุมพื้นที่ที่ไม่จำเป็นหรือพื้นที่ต้องห้ามเกินกว่าวัตถุประสงค์		
มีการกำหนดพื้นที่ปิดบังภาพ (Privacy Mask) ตามที่ได้รับอนุมัติ		
การบันทึกเสียงถูกปิด เว้นแต่มีวัตถุประสงค์และการอนุมัติที่เหมาะสม		

ข้อสังเกต: ไม่ควรตรวจรับจากจำนวนพิกเซลหรือความละเอียดของกล้องเพียงอย่างเดียว แต่ควรพิจารณาว่าภาพที่ได้จากการติดตั้งจริงสามารถตอบวัตถุประสงค์ที่กำหนดไว้หรือไม่

ก.3 อุปกรณ์ การติดตั้ง และสภาพแวดล้อม

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
รุ่นและจำนวนอุปกรณ์ตรงกับรายการที่ได้รับอนุมัติ		
หมายเลขประจำเครื่อง (Serial Number) ได้รับการบันทึกในทะเบียนอุปกรณ์		
รุ่นเฟิร์มแวร์และซอฟต์แวร์ได้รับการตรวจสอบและบันทึก		
ซอฟต์แวร์และเฟิร์มแวร์ที่ติดตั้งหรือปรับปรุงสามารถตรวจสอบแหล่งที่มาและความถูกต้องครบถ้วนได้ตามกลไกที่ผลิตภัณฑ์หรือระบบรองรับ		
สำหรับระบบที่มีความสำคัญหรือความเสี่ยงสูง ได้พิจารณากลไกรากฐานความเชื่อมั่นจากฮาร์ดแวร์ (Hardware-based Root of Trust) หรือกลไกที่ให้ระดับความเชื่อมั่นเทียบเท่า ตามความเหมาะสม		
อุปกรณ์อยู่ในสถานะที่ผู้ผลิตยังให้การสนับสนุน		
กล้องและอุปกรณ์สำคัญได้รับการติดตั้งอย่างมั่นคงและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตตามความเหมาะสม		

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
เครื่องบันทึก ระบบบริหารวิดีโอ และระบบจัดเก็บข้อมูลอยู่ในพื้นที่ที่มีการควบคุมทางกายภาพ		
อุปกรณ์เครือข่ายและจุดเชื่อมต่อได้รับการป้องกันตามความเหมาะสม		
ระบบไฟฟ้าและเครื่องสำรองไฟ (Uninterruptible Power Supply: UPS) เป็นไปตามข้อกำหนด		
สภาพแวดล้อม เช่น อุณหภูมิ ความชื้น ฝุ่น น้ำ หรือการสั่นสะเทือน เหมาะสมกับอุปกรณ์		
สายสัญญาณและสายไฟได้รับการติดตั้งและระบุอย่างเหมาะสม		
ระบบสายสัญญาณและการเชื่อมต่อได้รับการตรวจสอบและทดสอบตามมาตรฐานสากลที่เกี่ยวข้อง หรือมาตรฐานที่ให้ระดับสมรรถนะเทียบเท่า และมีความเหมาะสมกับสภาพแวดล้อมและระดับความสำคัญของระบบ		ผลการตรวจรับ/ผลการทดสอบ/เอกสารที่เกี่ยวข้อง

ก.4 เครือข่ายและการเชื่อมต่อ

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
ผังเครือข่ายตรงกับระบบที่ติดตั้งจริง		
กล้องและองค์ประกอบ CCTV ถูกแบ่งเครือข่ายตามสถาปัตยกรรมที่ได้รับอนุมัติ		
กฎ Firewall หรือรายการควบคุมการเข้าถึงเครือข่าย (Access Control List: ACL) เปิดเฉพาะการสื่อสารที่จำเป็น		
พอร์ต โพรโทคอล และบริการที่ไม่จำเป็นถูกปิดหรือจำกัด		
ไม่มีการเปิดระบบสู่ Internet โดยตรงโดยไม่ได้รับอนุมัติ		
บริการ Universal Plug and Play (UPnP), Peer-to-Peer (P2P), Dynamic DNS หรือ Port Forwarding ถูกปิดหรือควบคุมตามความจำเป็น		

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
ช่องทางการเข้าถึงจากระยะไกล (Remote Access) ตรงกับช่องทางที่ได้รับอนุมัติ		
การเชื่อมต่อกับระบบอื่นตรงกับขอบเขตและสถาปัตยกรรมที่ได้รับอนุมัติ		
หมายเลข IP และข้อมูลเครือข่ายสำคัญได้รับการบันทึกในเอกสารส่งมอบ		

ประเด็นสำคัญคือ ไม่ควรพิจารณาเพียงว่าระบบ “เชื่อมต่อได้” เพียงอย่างเดียวแต่ต้องยืนยันด้วยว่ามีเฉพาะการเชื่อมต่อที่จำเป็นและได้รับอนุมัติ

ก.5 บัญชีผู้ใช้งาน การพิสูจน์ตัวตน และสิทธิการเข้าถึง

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
ไม่มีข้อมูลยืนยันตัวตนเริ่มต้น (Default Credentials) ที่ยังคงใช้งานโดยไม่ได้รับการจัดการ		
บัญชีผู้ใช้งานสามารถระบุตัวผู้ใช้งานได้ตามความเหมาะสม		
บัญชีติดตั้ง บัญชีทดสอบ และบัญชีชั่วคราวถูกลบ ปิด หรือควบคุมแล้ว		
บัญชี Guest หรือ Anonymous ถูกปิด เว้นแต่มีเหตุผลและได้รับอนุมัติ		
สิทธิถูกกำหนดตามบทบาทและหน้าที่		
สิทธิผู้ดูแลระบบ (Administrator Privilege) ถูกจำกัดเฉพาะผู้ที่จำเป็น		
การดูภาพสด การดูย้อนหลัง การส่งออก และการบริหารระบบสามารถแยกสิทธิได้ตามความเหมาะสม		
การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) ถูกเปิดใช้กับบัญชีหรือช่องทางที่กำหนด		

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
บัญชีสำหรับการติดตั้งระบบ บัญชีสำหรับการทดสอบระบบ และบัญชีผู้ใช้งานชั่วคราว ถูกลบ ปิด หรือควบคุมแล้วตามความเหมาะสม		
สิทธิหรือช่องทางการเข้าถึงของผู้ติดตั้ง ผู้รวมระบบ หรือผู้ให้บริการที่ไม่มีความจำเป็นภายหลังการส่งมอบ ถูกเพิกถอนหรือปิดใช้งานแล้ว		
กรณีมีความจำเป็นต้องคงสิทธิของผู้ติดตั้ง ผู้รวมระบบ หรือผู้ให้บริการเพื่อการบำรุงรักษาหรือการให้บริการ ได้กำหนดวัตถุประสงค์ ขอบเขตสิทธิ ระยะเวลา วิธีการอนุมัติ การพิสูจน์ตัวตน การบันทึกกิจกรรม และการเพิกถอนสิทธิไว้อย่างเหมาะสม		
มีรายการบัญชี บทบาท และสิทธิที่ใช้งานจริงสำหรับส่งมอบให้เจ้าของระบบ		

ก.6 การเข้ารหัส ใบรับรอง และกุญแจ

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
ช่องทางบริหารระบบใช้การสื่อสารที่ได้รับการป้องกันตามข้อกำหนด		
มีการตรวจสอบใบรับรองดิจิทัล (Digital Certificate) ที่ใช้กับระบบ		
ไม่มีใบรับรองหรือกุญแจสำหรับการติดตั้งหรือทดสอบหลงเหลือโดยไม่จำเป็น		
กุญแจเข้ารหัส (Cryptographic Key) ถูกควบคุมโดยผู้รับผิดชอบที่กำหนด		
การส่งออกข้อมูลได้รับการป้องกันตามระดับความเสี่ยง		
กรณีมีการเข้ารหัสข้อมูลที่จัดเก็บ ได้ตรวจสอบว่าการตั้งค่าทำงานตามข้อกำหนด		

ไม่ควรตรวจสอบเพียงว่า “ระบบรองรับ Encryption” แต่ควรยืนยันว่า ฟังก์ชันที่กำหนดถูกเปิดใช้จริง และการควบคุมกุญแจหรือใบรับรองมีผู้รับผิดชอบชัดเจน

ก.7 บันทึกเหตุการณ์ การเฝ้าระวัง และเวลา

รายการตรวจสอบ	ผล	หมายเหตุ/ หลักฐาน
ระบบสามารถบันทึกการเข้าสู่ระบบและความพยายามเข้าสู่ระบบที่ไม่สำเร็จ		
การเปลี่ยนบัญชี สิทธิ หรือค่าตั้งสำคัญสามารถตรวจสอบย้อนหลังได้		
การเข้าถึงจากระยะไกลได้รับการบันทึกตามความเหมาะสม		
การส่งออก ลบ หรือดำเนินการสำคัญกับข้อมูลได้รับการบันทึกตามระดับความเสี่ยง		
ระบบสามารถตรวจพบหรือแจ้งเตือนเหตุสำคัญ เช่น กล้อง Offline หรือพื้นที่จัดเก็บผิดปกติ		
ระยะเวลาเก็บรักษาบันทึกเหตุการณ์เป็นไปตามข้อกำหนดขององค์กร		
บันทึกเหตุการณ์ได้รับการป้องกันจากการแก้ไขหรือลบโดยไม่ได้รับอนุญาตตามระดับความเสี่ยง		
กล้อง เครื่องบันทึก ระบบบริหารวิดีโอ และระบบที่เกี่ยวข้องมีเวลาสอดคล้องกัน		
แหล่งอ้างอิงเวลาหรือกลไกการปรับเทียบเวลาได้รับการกำหนดอย่างเหมาะสม		

ก.8 การจัดเก็บข้อมูล การสำรอง และการกู้คืน

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
ระยะเวลาเก็บรักษาภาพและวิดีโอตรงกับข้อกำหนด		
ความจุพื้นที่จัดเก็บเพียงพอกับจำนวนกล้อง อัตราข้อมูล และระยะเวลาเก็บรักษา		
การเขียนทับหรือลบข้อมูลเมื่อครบกำหนดทำงานตามที่กำหนด		
ระบบมีการแจ้งเตือนเมื่อพื้นที่จัดเก็บผิดปกติหรือใกล้เต็มตามความเหมาะสม		

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
ค่าตั้งระบบที่สำคัญได้รับการสำรอง		
เอกสารและข้อมูลที่จำเป็นต่อการกู้คืนได้รับการสำรองตามความเหมาะสม		
มีการทดสอบการกู้คืน (Restore Test) ในขอบเขตที่กำหนด		
สำหรับระบบที่มีความสำคัญ มีการกำหนดความต้องการด้านระยะเวลาการกู้คืนและการสูญเสียข้อมูลที่ยอมรับได้ตามความเหมาะสม		
กลไกสำรองข้อมูลได้รับการป้องกันจากการเข้าถึงหรือการทำลายโดยไม่ได้รับอนุญาตตามระดับความเสี่ยง		

ควรเข้าใจว่า การใช้ RAID หรือการทำสำเนาข้อมูลภายในระบบเดียวกันไม่ควรถูกถือว่าเป็นการสำรองข้อมูลที่เพียงพอโดยอัตโนมัติ เพราะอาจได้รับผลกระทบจากเหตุเดียวกันกับระบบหลัก

ก.9 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
มีการกำหนดวัตถุประสงค์ของการใช้ CCTV		
พื้นที่และมุมมองของกล้องสอดคล้องกับวัตถุประสงค์		
มีป้ายหรือการแจ้งรายละเอียดเกี่ยวกับการใช้ CCTV ตามที่เกี่ยวข้อง		
การบันทึกเสียงถูกปิด เว้นแต่มีวัตถุประสงค์ ฐานทางกฎหมาย และการอนุมัติที่เหมาะสม		
มีการกำหนดระยะเวลาเก็บรักษาข้อมูล		
สิทธิในการดู ค้นหา ส่งออก และเปิดเผยข้อมูลได้รับการควบคุม		
มีช่องทางหรือกระบวนการรองรับคำขอใช้สิทธิของเจ้าของข้อมูลตามที่เกี่ยวข้อง		
มีขั้นตอนจัดการเหตุละเมิดข้อมูลส่วนบุคคล		
กรณีใช้ผู้ประมวลผลข้อมูลส่วนบุคคล มีการกำหนดหน้าที่และข้อตกลงที่เกี่ยวข้อง		

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
กรณีมีความเสี่ยงสูง ได้พิจารณาความจำเป็นในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)		
กรณีมีการส่งหรือโอนข้อมูลออกนอกประเทศไทย ได้พิจารณาข้อกำหนดที่เกี่ยวข้อง		

ก.10 บริการคลาวด์และบริการภายนอก

รายการตรวจสอบในหัวข้อนี้ให้ใช้เฉพาะกรณีที่ระบบ CCTV มีการใช้บริการคลาวด์หรือบริการภายนอกที่เกี่ยวข้อง

รายการตรวจสอบ	ผล	หมายเหตุ/หลักฐาน
ระบุสถานที่จัดเก็บข้อมูล (Data Location) ได้		
ระบุสถานที่ประมวลผลข้อมูล (Processing Location) ได้		
ทราบเขตอำนาจทางกฎหมายที่เกี่ยวข้อง		
ทราบผู้ให้บริการหลักและผู้ให้บริการช่วงที่เกี่ยวข้อง		
ระบุผู้ที่สามารถเข้าถึงระบบหรือข้อมูลเพื่อบริหารและสนับสนุนได้		
ความรับผิดชอบระหว่างองค์กรกับผู้ให้บริการได้รับการกำหนด		
การเข้ารหัสและการควบคุมกุญแจตรงกับข้อกำหนด		
สถานที่และวิธีสำรองข้อมูลตรงกับข้อกำหนด		
มีช่องทางและเงื่อนไขในการแจ้งเหตุ		
สามารถคืนหรือส่งออกข้อมูลเมื่อสิ้นสุดบริการ		
มีข้อกำหนดเกี่ยวกับการลบข้อมูลหลัก ข้อมูลสำรอง และสำเนาที่เกี่ยวข้อง		
มีแนวทางการยุติหรือเปลี่ยนบริการ (Exit Strategy)		

ก.11 เอกสารและข้อมูลที่ต้องส่งมอบ

เอกสาร/ข้อมูล	ส่งมอบ	หมายเหตุ
ผังตำแหน่งกล้อง (Camera Layout)		
ความต้องการเชิงปฏิบัติการรายจุด (POR)		
แบบที่ติดตั้งจริง (As-built Diagram)		
ทะเบียนอุปกรณ์ (Asset List)		
รุ่นเฟิร์มแวร์และซอฟต์แวร์		
ผังเครือข่าย (Network Diagram)		
หมายเลข IP และข้อมูลเครือข่ายที่จำเป็น		
รายการพอร์ต โพรโทคอล และบริการ		
รายการบัญชี บทบาท และสิทธิ		
ผลทดสอบคุณภาพของภาพและ POR/DORI		
ผลทดสอบกลางวันและกลางคืน		
ค่าระยะเวลาเก็บรักษาข้อมูล		
ผลการคำนวณพื้นที่จัดเก็บ		
ขั้นตอนและผลการทดสอบสำรอง/กู้คืน		
ค่าฐานการตั้งค่าที่ได้รับอนุมัติ (Approved Configuration Baseline)		
คู่มือการเสริมความมั่นคงปลอดภัย (Security Hardening Guide) ตามที่เกี่ยวข้อง		
กระบวนการปรับปรุงซอฟต์แวร์และเฟิร์มแวร์		
ข้อมูลหรือหลักฐานเกี่ยวกับกลไกการตรวจสอบความถูกต้องของซอฟต์แวร์และเฟิร์มแวร์ตามที่เกี่ยวข้อง		
ช่องทางรับประกาศแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Advisory)		
ช่องทางแจ้งช่องโหว่		
ข้อมูลระยะเวลาการสนับสนุนและ EoL/EoS		

เอกสาร/ข้อมูล	ส่งมอบ	หมายเหตุ
คู่มือการใช้งานและบำรุงรักษา		
รายชื่อและช่องทางติดต่อเมื่อเกิดเหตุ		
ผลการทดสอบและเอกสารตรวจรับ		
รายการข้อยกเว้น ประเด็นคงค้าง และความเสี่ยงคงเหลือ		

ไม่จำเป็นต้องจัดทำเอกสารแยกใหม่สำหรับทุกรายการ หากข้อมูลดังกล่าวมีอยู่ในเอกสารหรือระบบอื่นและสามารถเข้าถึง ตรวจสอบ และส่งมอบให้เจ้าของระบบได้อย่างเหมาะสม

ก.12 สรุปผลการตรวจรับก่อนเปิดใช้งาน

ผล	ความหมาย
☐ **ผ่านและพร้อมเปิดใช้งาน**	ข้อกำหนดสำคัญได้รับการตรวจสอบและไม่มีประเด็นที่ทำให้ไม่ควรเปิดใช้งาน
☐ **ผ่านโดยมีเงื่อนไข**	มีประเด็นคงค้าง แต่มีมาตรการชั่วคราว ผู้รับผิดชอบ และกำหนดเวลาแก้ไขแล้ว
☐ **ต้องแก้ไขก่อนเปิดใช้งาน**	มีข้อบกพร่องหรือความเสี่ยงที่ยังไม่ควรยอมรับก่อนเปิดใช้งาน

รายการประเด็นคงค้าง

ประเด็น	ความเสี่ยง/ผลกระทบ	มาตรการชั่วคราว	การดำเนินการ	ผู้รับผิดชอบ	กำหนดเวลา	สถานะ

ผู้แทนเจ้าของระบบ: _____ วันที่ _____
ผู้ติดตั้ง/ผู้รวมระบบ: _____ วันที่ _____
ผู้ตรวจรับ: _____ วันที่ _____

ภาคผนวก ข รายการประเมินตนเองตามรอบ

ภาคผนวกนี้ใช้เป็นแนวทางสำหรับเจ้าของระบบ ผู้ดูแลระบบ ผู้รับผิดชอบด้านความมั่นคงปลอดภัย และผู้ที่เกี่ยวข้อง ในการทบทวนระบบ CCTV ที่เปิดใช้งานแล้ว เพื่อประเมินว่าระบบยังคงทำงานตามวัตถุประสงค์ มีมาตรการควบคุมที่เหมาะสม และไม่มีการเปลี่ยนแปลงที่ทำให้ระดับความเสี่ยงเพิ่มขึ้นโดยไม่ได้รับการประเมินหรือจัดการ

การประเมินตามรอบ ไม่ใช่การตรวจรับระบบใหม่ซ้ำอีกครั้ง แต่เน้นการตอบคำถามสำคัญว่า **ระบบยังคงตอบวัตถุประสงค์หรือไม่ ⟶ มีอะไรเปลี่ยนแปลงไปหรือไม่ ⟶ มาตรการควบคุมยังทำงานหรือไม่ ⟶ มีความเสี่ยงใหม่หรือไม่ ⟶ และต้องดำเนินการเพิ่มเติมอย่างไร**

องค์กรควรกำหนดรอบการประเมินให้เหมาะสมกับระดับความสำคัญของระบบ ผลกระทบ ความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง และควรประเมินเพิ่มเติมเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ แต่ละระบบอาจมีรอบการประเมินที่แตกต่างกัน

ผลการประเมินแต่ละรายการอาจใช้สถานะดังต่อไปนี้

สถานะ	ความหมาย
สอดคล้อง/เหมาะสม	ตรวจสอบแล้วและยังคงเป็นไปตามข้อกำหนด
ต้องปรับปรุง	พบประเด็นที่ควรแก้ไข แต่ยังสามารถดำเนินงานต่อได้ภายใต้มาตรการที่เหมาะสม
ต้องประเมินเพิ่มเติม	มีการเปลี่ยนแปลงหรือข้อมูลไม่เพียงพอที่จะสรุปได้
ไม่สอดคล้อง/ต้องดำเนินการ	พบข้อบกพร่องหรือความเสี่ยงที่ต้องได้รับการแก้ไข
ไม่เกี่ยวข้อง	รายการดังกล่าวไม่ใช้กับระบบที่ประเมิน

ข.1 ข้อมูลการทบทวน

รายการ	ข้อมูล
ชื่อระบบ/โครงการ	
หน่วยงานเจ้าของระบบ	
พื้นที่หรือสถานที่	
ผู้รับผิดชอบระบบ	
วันที่ประเมิน	

รายการ	ข้อมูล
ผู้ประเมิน	
วันที่ประเมินครั้งก่อน	
ระดับความสำคัญของระบบ	☐ B ☐ E ☐ H
จำนวนกล้องปัจจุบัน	
มีบริการคลาวด์/บริการภายนอก	☐ ใช่ ☐ ไม่ใช่
มีการเข้าถึงจากระยะไกล	☐ ใช่ ☐ ไม่ใช่
มี AI/ข้อมูลชีวมิติ	☐ ใช่ ☐ ไม่ใช่
มีการเปลี่ยนแปลงสำคัญจากครั้งก่อน	☐ มี ☐ ไม่มี

หากมีการเปลี่ยนแปลงสำคัญ ควรระบุโดยสรุป:

.....

ข.2 การประเมินตามรอบ

ข.2.1 วัตถุประสงค์ พื้นที่ และความเหมาะสมของการใช้งาน

ระบบ CCTV อาจมีการใช้งานต่อเนื่องเป็นเวลาหลายปี ขณะที่วัตถุประสงค์ พื้นที่ สภาพแวดล้อม หรือกระบวนการขององค์กรอาจเปลี่ยนแปลง การทบทวนจึงควรพิจารณาว่าเหตุผลและรูปแบบการใช้ CCTV ยังคงเหมาะสมกับสภาพปัจจุบันหรือไม่

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
วัตถุประสงค์ของการใช้ CCTV ยังคงชัดเจนและเหมาะสม		
ตำแหน่งและมุมมองของกล้องยังสอดคล้องกับวัตถุประสงค์		
ไม่มีการเปลี่ยนแปลงพื้นที่ที่ทำให้เกิดจุดอับหรือพื้นที่ที่ไม่จำเป็นถูกบันทึกเพิ่มขึ้น		
คุณภาพของภาพยังเพียงพอต่อความต้องการเชิงปฏิบัติการรายจุด (POR)		
คุณภาพของภาพกลางวันและกลางคืนยังเหมาะสม		
พื้นที่ปิดบังภาพ (Privacy Mask) ยังคงถูกต้อง		

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
การบันทึกเสียงยังเป็นไปตามวัตถุประสงค์และข้อกำหนดที่ได้รับอนุมัติ		
ป้ายหรือการแจ้งเกี่ยวกับ CCTV ยังอยู่ในตำแหน่งที่เหมาะสมและมีข้อมูลที่เกี่ยวข้องครบถ้วน		

ไม่จำเป็นต้องทดสอบ POR/DORI ใหม่ทั้งหมดในทุกครั้ง หากไม่มีการเปลี่ยนแปลงที่เกี่ยวข้อง แต่ควรทดสอบใหม่เมื่อมีการย้ายกล้อง เปลี่ยนเลนส์ เปลี่ยนความละเอียด เปลี่ยนสภาพแสง หรือเปลี่ยนวัตถุประสงค์ของจุดติดตั้ง

ข.2.2 สถานะอุปกรณ์ ซอฟต์แวร์ และการสนับสนุน

การทบทวนไม่ควรพิจารณาเพียงว่าอุปกรณ์ “ยังใช้งานได้” แต่ควรพิจารณาด้วยว่าอุปกรณ์ยังได้รับการสนับสนุน สามารถแก้ไขช่องโหว่ และยังเหมาะสมกับระดับความเสี่ยงของระบบหรือไม่

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
กล้อง เครื่องบันทึก และอุปกรณ์สำคัญยังทำงานตามปกติ		
รุ่นเฟิร์มแวร์และซอฟต์แวร์ได้รับการบันทึกและสามารถตรวจสอบได้		
มีการติดตามประกาศแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Advisory) ที่เกี่ยวข้อง		
ช่องโหว่ที่เกี่ยวข้องได้รับการประเมินและดำเนินการตามระดับความเสี่ยง		
การปรับปรุงด้านความมั่นคงปลอดภัยที่จำเป็นได้รับการดำเนินการ		
ไม่มีการเปลี่ยนแปลงซอฟต์แวร์หรือเฟิร์มแวร์ที่ทำให้กลไกด้านความถูกต้อง ความน่าเชื่อถือ หรือการสนับสนุนด้านความมั่นคงปลอดภัยลดลงโดยไม่ได้รับการประเมิน		
อุปกรณ์และซอฟต์แวร์ยังอยู่ในช่วงที่ผู้ผลิตให้การสนับสนุน		
มีการติดตามสถานะสิ้นสุดอายุผลิตภัณฑ์ (EoL) และสิ้นสุดการสนับสนุน (EoS)		

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
อุปกรณ์ที่ใกล้ EoL/EoS มีแผนปรับปรุง ทดแทน หรือมาตรการชดเชยตามความเหมาะสม		
อุปกรณ์ที่ชำรุดหรือเสื่อมสภาพได้รับการซ่อมแซมหรือเปลี่ยนตามความเหมาะสม		

การพบว่าอุปกรณ์เข้าสู่ EoL/EoS ไม่จำเป็นต้องหมายความว่าต้องหยุดใช้งานทันทีในทุกกรณี แต่ควรประเมินความเสี่ยง ความสามารถในการแก้ไขช่องโหว่ มาตรการชดเชย และแผนการทดแทนตามบทที่ 3

ข.2.3 บัญชีผู้ใช้งานและสิทธิการเข้าถึง

การทบทวนสิทธิควรยืนยันว่า **ผู้**ที่ยังมีสิทธิเป็นผู้ที่ยังจำเป็นต้องใช้สิทธินั้นจริง และระดับสิทธิยังสอดคล้องกับหน้าที่ปัจจุบัน

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
รายการบัญชีผู้ใช้งานปัจจุบันสามารถตรวจสอบได้		
บัญชีของผู้ที่พ้นหน้าที่ ลาออก หรือไม่จำเป็นถูกปิดหรือเพิกถอนแล้ว		
สิทธิของผู้ใช้งานยังสอดคล้องกับบทบาทและหน้าที่		
สิทธิผู้ดูแลระบบถูกจำกัดเฉพาะผู้ที่จำเป็น		
ไม่มีบัญชีร่วมโดยไม่มีเหตุผลหรือมาตรการควบคุมที่เหมาะสม		
ไม่มีบัญชีทดสอบหรือบัญชีชั่วคราวที่หลงเหลือโดยไม่จำเป็น		
การพิสูจน์ตัวตนหลายปัจจัย (MFA) ยังทำงานตามข้อกำหนด		
สิทธิของผู้ให้บริการหรือผู้บำรุงรักษายังคงมีความจำเป็น		
การเข้าถึงจากระยะไกลได้รับการอนุมัติและสามารถตรวจสอบย้อนหลังได้		
มีหลักฐานการทบทวนสิทธิตามรอบที่องค์กรกำหนด		

สำหรับระบบสำคัญ การทบทวนไม่ควรตรวจเพียงรายชื่อผู้ใช้งาน แต่ควรตรวจสิทธิจริงในระบบเพื่อยืนยันว่าไม่มีการสะสมสิทธิหรือสิทธิพิเศษที่ไม่จำเป็น

ข.2.4 เครือข่ายและค่าตั้งด้านความมั่นคงปลอดภัย

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
สถาปัตยกรรมเครือข่ายยังตรงกับแบบที่ได้รับอนุมัติ		
การแบ่งเครือข่ายยังคงทำงานตามที่กำหนด		
Firewall/ACL เปิดเฉพาะการสื่อสารที่จำเป็น		
ไม่มี Port หรือ Service ใหม่ที่ไม่ได้รับอนุมัติ		
ไม่มีการเปิดระบบสู่ Internet โดยตรงโดยไม่ได้รับอนุมัติ		
P2P, UPnP, Port Forwarding หรือบริการที่มีความเสี่ยงถูกปิดหรือควบคุมตามข้อกำหนด		
ช่องทาง Remote Access ยังคงเป็นไปตามที่ได้รับอนุมัติ		
ไม่มีการเปลี่ยนค่าตั้งสำคัญโดยไม่ผ่านกระบวนการที่กำหนด		
ค่าฐานการตั้งค่าที่ได้รับอนุมัติ (Approved Configuration Baseline) ยังคงสามารถใช้เปรียบเทียบกับระบบจริงได้		

หากพบความแตกต่างจากค่าฐาน ไม่ควรสรุปว่าเป็นความผิดปกติโดยอัตโนมัติ แต่ควรตรวจสอบว่าเป็น การเปลี่ยนแปลงที่ได้รับอนุมัติ หรือเป็นการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต

ข.2.5 บันทึกเหตุการณ์และการเฝ้าระวัง

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
ระบบยังสร้างบันทึกเหตุการณ์ที่สำคัญได้ตามข้อกำหนด		
สามารถตรวจสอบการเข้าสู่ระบบและความพยายามเข้าสู่ระบบที่ไม่สำเร็จ		
การเปลี่ยนสิทธิหรือค่าตั้งสำคัญสามารถตรวจสอบย้อนหลังได้		
การเข้าถึงจากระยะไกลสามารถตรวจสอบย้อนหลังได้		
เหตุการณ์สำคัญ เช่น กล้อง Offline หรือพื้นที่จัดเก็บผิดปกติ สามารถตรวจพบได้		

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
เวลาในระบบและอุปกรณ์สำคัญยังสอดคล้องกัน		
ระยะเวลาเก็บรักษาบันทึกเหตุการณ์ยังเป็นไปตามข้อกำหนด		
มีการทบทวนเหตุการณ์หรือการแจ้งเตือนตามรอบที่กำหนด		
ไม่มีหลักฐานว่าบันทึกเหตุการณ์ถูกลบหรือแก้ไขโดยไม่ได้รับอนุญาต		

ข.2.6 การจัดเก็บข้อมูล การสำรอง และการกู้คืน

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
ระบบยังเก็บข้อมูลย้อนหลังได้ตามระยะเวลาที่กำหนด		
ความจุพื้นที่จัดเก็บยังเพียงพอเมื่อเทียบกับจำนวนกล้องและค่าตั้งปัจจุบัน		
การลบหรือเขียนทับข้อมูลเมื่อครบกำหนดยังทำงานตามที่กำหนด		
ไม่มีความผิดปกติของพื้นที่จัดเก็บที่ไม่ได้รับการแก้ไข		
ข้อมูลหรือค่าตั้งที่กำหนดให้สำรองยังได้รับการสำรอง		
ข้อมูลสำรองยังสามารถเข้าถึงได้เมื่อจำเป็น		
มีการทดสอบการกู้คืนตามรอบและขอบเขตที่องค์กรกำหนด		
สำหรับระบบสำคัญ ผลการทดสอบยังสอดคล้องกับความต้องการด้านการกู้คืน		

จุดสำคัญคือ **การมี Backup ไม่เพียงพอหากไม่สามารถยืนยันได้ว่าสามารถกู้คืนได้จริง** ดังนั้นระบบที่มีความสำคัญควรมีหลักฐานการทดสอบการกู้คืนตามรอบที่เหมาะสม

ข.2.7 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
วัตถุประสงค์ในการใช้ CCTV ยังไม่เปลี่ยนแปลงอย่างมีนัยสำคัญ		
การเก็บข้อมูลยังจำกัดเท่าที่จำเป็นต่อวัตถุประสงค์		
ป้ายหรือการแจ้งรายละเอียดเกี่ยวกับ CCTV ยังเหมาะสม		
ระยะเวลาเก็บรักษาข้อมูลยังเหมาะสมและถูกนำไปใช้จริง		
สิทธิในการดู ค้นหา ส่งออก และเปิดเผยข้อมูลยังถูกควบคุม		
กระบวนการรองรับคำขอใช้สิทธิยังสามารถดำเนินการได้		
กระบวนการจัดการเหตุละเมิดข้อมูลส่วนบุคคลยังเป็นปัจจุบัน		
ผู้ให้บริการที่เกี่ยวข้องยังมีบทบาทและข้อตกลงที่เหมาะสม		
การเปลี่ยนแปลงที่มีผลต่อความเป็นส่วนตัวได้รับการประเมิน		
หากระดับความเสี่ยงเปลี่ยนแปลง ได้พิจารณาความจำเป็นในการทบทวน DPIA		

ข.2.8 บริการคลาวด์และบริการภายนอก

สำหรับระบบที่ใช้บริการคลาวด์หรือบริการภายนอก ไม่ควรทบทวนเพียงว่า “บริการยังใช้งานได้” แต่ควรตรวจว่าข้อเท็จจริงสำคัญเกี่ยวกับบริการยังตรงกับสิ่งที่องค์กรเคยประเมินและอนุมัติหรือไม่

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
สถานที่จัดเก็บข้อมูลยังเป็นไปตามที่ได้รับอนุมัติ		
สถานที่ประมวลผลข้อมูลไม่มีการเปลี่ยนแปลงที่ยังไม่ได้ประเมิน		
ผู้ให้บริการช่วงไม่มีการเปลี่ยนแปลงที่มีนัยสำคัญโดยไม่ได้รับการประเมิน		
การเข้าถึงเพื่อบริหารระบบยังเป็นไปตามเงื่อนไขที่กำหนด		
การควบคุมกุญแจเข้ารหัสยังเป็นไปตามข้อตกลง		
การสำรองและกู้คืนข้อมูลยังเป็นไปตามข้อกำหนด		

รายการประเมิน	ผล	หมายเหตุ/การดำเนินการ
ช่องทางแจ้งเหตุของผู้ให้บริการยังสามารถใช้งานได้		
ข้อตกลงหรือสัญญาที่เกี่ยวข้องยังมีผลและเหมาะสม		
ผู้ให้บริการยังสามารถคืน ส่งออก และลบข้อมูลตามเงื่อนไขที่กำหนด		
แผนการยุติหรือเปลี่ยนบริการ (Exit Strategy) ยังสามารถดำเนินการได้		

ข.3 การทบทวนเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ

นอกเหนือจากการประเมินตามรอบ องค์กรควรพิจารณาประเมินระบบเพิ่มเติมเมื่อเกิดการเปลี่ยนแปลงที่อาจทำให้ลักษณะความเสี่ยงแตกต่างจากที่เคยประเมินไว้

การเปลี่ยนแปลงที่ควรกระตุ้นให้มีการทบทวน ได้แก่

การเปลี่ยนแปลง	สิ่งที่ควรพิจารณา
เปลี่ยนวัตถุประสงค์การใช้ CCTV	ประเมินความจำเป็น ขอบเขตข้อมูล และข้อกำหนดที่เกี่ยวข้องใหม่
เพิ่มหรือย้ายกล้อง	ทบทวน POR พื้นที่ครอบคลุม ความเป็นส่วนตัว และสถาปัตยกรรม
เพิ่มพื้นที่หรือจำนวนผู้ใช้งานอย่างมีนัยสำคัญ	ทบทวนสมรรถนะ สิทธิ และความสามารถในการบริหาร
เชื่อมต่อ Internet หรือ Cloud เพิ่มเติม	ทบทวน Exposure, Remote Access, Data Location และผู้ให้บริการ
เปลี่ยนผู้ให้บริการ	ทบทวนความรับผิดชอบ สัญญา ข้อมูล และ Exit Strategy
เปลี่ยนสถานที่จัดเก็บหรือประมวลผลข้อมูล	ทบทวนข้อกำหนดด้านข้อมูล เขตอำนาจทางกฎหมาย และความเสี่ยง
เพิ่มการเข้าถึงจากระยะไกล	ทบทวนการพิสูจน์ตัวตน สิทธิ ช่องทาง และ Logging
เชื่อมต่อกับระบบหรือฐานข้อมูลใหม่	ทบทวนขอบเขตข้อมูล สิทธิ การไหลของข้อมูล และผลกระทบ
พบช่องโหว่ร้ายแรง	ประเมินผลกระทบ มาตรการแก้ไขหรือมาตรการชดเชย
ผลิตภัณฑ์เข้าสู่ EoL/EoS	ประเมินความเสี่ยงและจัดทำแผนปรับปรุงหรือทดแทน

การเปลี่ยนแปลง	สิ่งที่ควรพิจารณา
เกิดเหตุด้านความมั่นคงปลอดภัย	ทบทวนสาเหตุ มาตรการควบคุม และความเสี่ยง
เกิดเหตุละเมิดข้อมูลส่วนบุคคล	ทบทวนมาตรการด้านข้อมูล การเข้าถึง และกระบวนการตอบสนอง
ข้อกำหนดทางกฎหมายหรือสัญญาเปลี่ยนแปลง	ประเมินผลกระทบต่อระบบและมาตรการที่ใช้อยู่
เปิดใช้การบันทึกเสียง	ประเมินวัตถุประสงค์ ความจำเป็น กฎหมาย และมาตรการเพิ่มเติม
เพิ่ม AI, Facial Recognition หรือ Biometrics	ประเมินผลกระทบและใช้ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย เพิ่มเติม

กรณีเพิ่มความสามารถด้าน AI

ไม่ควรถือว่าการเพิ่ม AI เป็นเพียงการเพิ่มฟังก์ชันของซอฟต์แวร์ หากความสามารถใหม่ทำให้ระบบสามารถวิเคราะห์ จำแนก ระบุ ติดตาม สร้างข้อสรุปเกี่ยวกับบุคคล หรือสั่งการระบบอื่นได้

ควรพิจารณาอย่างน้อยว่า

AI ทำหน้าที่อะไร ⟶ ใช้หรือสร้างข้อมูลอะไร ⟶ เชื่อมโยงกับระบบใด ⟶ สร้างผลลัพธ์อะไร ⟶ ผลลัพธ์ถูกนำไปใช้อย่างไร ⟶ หากผลลัพธ์ผิดพลาดจะเกิดผลกระทบใด ⟶ และมีผู้ใดสามารถตรวจสอบ แทรกแซง หรือระงับการดำเนินการได้

หากการเปลี่ยนแปลงทำให้ลักษณะการใช้ AI หรือระดับผลกระทบเปลี่ยนไป ควรทบทวนตาม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย เพิ่มเติม

ข.4 สรุปผลการทบทวน

ผลการทบทวน	ความหมาย
☐ **ยังคงเหมาะสม**	ระบบและมาตรการควบคุมยังเหมาะสมกับวัตถุประสงค์และระดับความเสี่ยง ไม่พบช่องว่างที่มีนัยสำคัญ
☐ **ต้องปรับปรุง**	พบประเด็นที่ต้องแก้ไขหรือปรับปรุง แต่ยังสามารถดำเนินงานต่อได้ภายใต้มาตรการที่เหมาะสม

ผลการทบทวน	ความหมาย
☐ **ต้องประเมินความเสี่ยงใหม่**	บริบท วัตถุประสงค์ สถาปัตยกรรม ข้อมูล เทคโนโลยี หรือระดับผลกระทบเปลี่ยนแปลงอย่างมีนัยสำคัญ
☐ **ต้องจำกัดหรือระงับการใช้งานบางส่วน**	พบความเสี่ยงหรือข้อบกพร่องที่ไม่ควรปล่อยให้ดำเนินงานต่อโดยไม่มีมาตรการเพิ่มเติม

แผนการดำเนินการ

ประเด็น	ความเสี่ยง/ผลกระทบ	การดำเนินการ	ผู้รับผิดชอบ	กำหนดเวลา	สถานะ

ผู้ประเมิน: _____ วันที่ _____
ผู้รับผิดชอบระบบ: _____ วันที่ _____
ผู้อนุมัติ/รับทราบ: _____ วันที่ _____

หลักการใช้ภาคผนวก ข

รายการประเมินตนเองตามรอบเป็นเครื่องมือสนับสนุนการทบทวน มิได้ใช้แทนการประเมินความเสี่ยง การตรวจสอบเชิงเทคนิค หรือการตรวจประเมินตามข้อกำหนดอื่นที่เกี่ยวข้อง หากพบการเปลี่ยนแปลง เหตุการณ์ หรือช่องว่างที่มีนัยสำคัญ องค์กรควรประเมินความเสี่ยงและกำหนดมาตรการเพิ่มเติมตามความเหมาะสม

ภาคผนวก ค อภิธานศัพท์ (Glossary)

อภิธานศัพท์นี้รวบรวมคำศัพท์สำคัญที่ใช้ในแนวปฏิบัติฉบับนี้ เพื่อสนับสนุนให้ผู้อ่าน ผู้ใช้งาน ผู้ติดตั้ง ผู้จัดซื้อ ผู้ให้บริการ และผู้ตรวจประเมินสามารถตีความคำศัพท์ทางเทคนิคและคำศัพท์ด้านการกำกับดูแลได้อย่างสอดคล้องกัน

คำอธิบายต่อไปนี้เป็นคำอธิบายโดยสรุปสำหรับบริบทของแนวปฏิบัติฉบับนี้ มิได้มีวัตถุประสงค์เพื่อแทนนิยามอย่างเป็นทางการตามกฎหมาย มาตรฐาน หรือข้อกำหนดที่เกี่ยวข้อง หากมีนิยามเฉพาะในกฎหมายหรือข้อกำหนดที่มีผลใช้บังคับ ให้ใช้นิยามดังกล่าวเป็นหลัก

ค.1 ระบบ CCTV และคุณภาพของภาพ

คำศัพท์	ความหมายโดยย่อ
ระบบกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV)	ระบบสำหรับเฝ้าระวัง บันทึก แสดงผล ค้นหา หรือบริหารจัดการข้อมูลภาพและวิดีโอ โดยอาจประกอบด้วยกล้อง เครื่องบันทึก ระบบบริหารวิดีโอ ระบบจัดเก็บข้อมูล เครือข่าย และบริการอื่นที่เกี่ยวข้อง
ความต้องการเชิงปฏิบัติการรายจุด (Point Operational Requirements: POR)	ความต้องการของแต่ละจุดติดตั้งกล้อง โดยระบุว่าต้องการเห็นอะไรที่ใด เพื่อวัตถุประสงค์ใด และต้องการรายละเอียดของภาพในระดับใด เพื่อนำไปใช้ในการออกแบบ เลือกอุปกรณ์ และกำหนดเกณฑ์ตรวจรับ
DORI	กรอบสำหรับพิจารณาระดับรายละเอียดของภาพ ประกอบด้วย การตรวจพบ (Detection) การสังเกต (Observation) การจดจำ (Recognition) และการระบุตัว (Identification) ตาม IEC 62676 series ที่เกี่ยวข้อง
การตรวจพบ (Detection)	ระดับรายละเอียดของภาพที่เพียงพอสำหรับตรวจพบว่ามีบุคคลหรือวัตถุอยู่ในพื้นที่ โดยยังไม่จำเป็นต้องทราบรายละเอียดของบุคคลหรือวัตถุนั้น
การสังเกต (Observation)	ระดับรายละเอียดที่ช่วยให้สามารถสังเกตลักษณะทั่วไป การแต่งกาย การเคลื่อนไหว หรือกิจกรรมของบุคคลหรือวัตถุได้
การจดจำ (Recognition)	ระดับรายละเอียดที่ช่วยให้สามารถจดจำบุคคลหรือวัตถุที่เคยรู้จักหรือพบมาก่อนได้
การระบุตัว (Identification)	ระดับรายละเอียดที่เหมาะสมกับวัตถุประสงค์ในการระบุตัวบุคคลหรือวัตถุ โดยต้องพิจารณาร่วมกับบริบทและคุณภาพของภาพ

คำศัพท์	ความหมายโดยย่อ
ความหนาแน่นของพิกเซล (Pixel Density / Pixels per Meter PPM)	จำนวนพิกเซลที่ครอบคลุมเป้าหมายในพื้นที่จริง โดยมักแสดงเป็นพิกเซลต่อเมตร และใช้ประกอบการออกแบบหรือประเมินระดับ DORI
พื้นที่ครอบคลุมของภาพ (Field of View: FOV)	ขอบเขตพื้นที่ที่กล้องสามารถมองเห็นได้จากตำแหน่งติดตั้ง เลนส์ และค่าตั้งที่กำหนด
ช่วงไดนามิกกว้าง (Wide Dynamic Range: WDR)	ความสามารถของกล้องในการรักษารายละเอียดของภาพในฉากที่มีส่วนสว่างและมืดแตกต่างกันมาก เช่น ทางเข้าอาคารที่มีแสงจากภายนอก
แสงอินฟราเรด (Infrared: IR)	แสงในช่วงอินฟราเรดที่ใช้สนับสนุนการบันทึกภาพในสภาพแสงต่ำหรือเวลากลางคืน โดยอาจต้องพิจารณาระยะใช้งานและการสะท้อนกลับ
อัตราเฟรม (Frame Rate)	จำนวนภาพที่ระบบบันทึกหรือแสดงต่อหนึ่งวินาที ซึ่งมีผลต่อความต่อเนื่องของภาพและความสามารถในการมองเห็นวัตถุที่เคลื่อนที่
อัตราข้อมูล (Bitrate)	ปริมาณข้อมูลที่ใช้ในการส่งหรือบันทึกวิดีโอต่อหน่วยเวลา ซึ่งมีผลต่อแบนด์วิดท์และพื้นที่จัดเก็บ
การบีบอัดข้อมูล (Compression)	กระบวนการลดขนาดข้อมูลวิดีโอเพื่อประหยัดแบนด์วิดท์หรือพื้นที่จัดเก็บ โดยการบีบอัดที่สูงเกินไปอาจทำให้รายละเอียดของภาพลดลง

ค.2 องค์ประกอบและการทำงานของระบบ

คำศัพท์	ความหมายโดยย่อ
ระบบบริหารวิดีโอ (Video Management System: VMS)	ระบบหรือซอฟต์แวร์สำหรับบริหารกล้อง วิดีโอ ผู้ใช้งาน สิทธิ การบันทึก การค้นหา การส่งออก และฟังก์ชันอื่นที่เกี่ยวข้อง
เครื่องบันทึกวิดีโอผ่านเครือข่าย (Network Video Recorder: NVR)	เครื่องหรือระบบสำหรับรับและบันทึกวิดีโอจากกล้องผ่านเครือข่าย
เครื่องบันทึกวิดีโอดิจิทัล (Digital Video Recorder: DVR)	เครื่องบันทึกวิดีโอดิจิทัล โดยทั่วไปใช้กับกล้องหรือสัญญาณวิดีโอที่ DVR รองรับโดยตรง

คำศัพท์	ความหมายโดยย่อ
การบันทึกที่อุปกรณ์ปลายทาง (Edge Recording)	การบันทึกวิดีโอหรือข้อมูลที่กล้องหรืออุปกรณ์ปลายทาง เช่น การบันทึกลง SD Card เพื่อให้ยังสามารถบันทึกได้เมื่อระบบส่วนกลางหรือเครือข่ายไม่พร้อมใช้งาน
การนำข้อมูลกลับเข้าสู่ระบบโดยอัตโนมัติ (Automatic Network Replenishment: ANR)	กลไกที่นำข้อมูลที่บันทึกไว้ในกล้องหรืออุปกรณ์ปลายทางระหว่างที่เครือข่ายขัดข้องกลับเข้าสู่ระบบบันทึกหลักเมื่อการเชื่อมต่อกลับคืน
มาตรฐานความร่วมมือเพื่อมาตรฐานส่วนต่อประสานวิดีโอเครือข่ายแบบเปิด (Open Network Video Interface Forum : ONVIF)	ข้อกำหนดและโปรไฟล์แบบเปิดที่ใช้สนับสนุนการทำงานร่วมกันระหว่างผลิตภัณฑ์ด้านระบบรักษาความปลอดภัยทางกายภาพและระบบเฝ้าระวังด้วยวิดีโอ
ความสามารถในการทำงานร่วมกัน (Interoperability)	ความสามารถของอุปกรณ์ ระบบ หรือบริการจากองค์ประกอบหรือผู้ผลิตต่างกันในการทำงานร่วมกันตามฟังก์ชันที่กำหนด
การผูกติดกับผู้ผลิตหรือผู้ให้บริการรายเดียว (Vendor Lock-in)	สภาวะที่องค์กรพึ่งพาผู้ผลิตหรือผู้ให้บริการรายหนึ่งมากจนการเปลี่ยน ย้าย เชื่อมต่อ หรือทดแทนระบบทำได้ยาก ใช้เวลานาน หรือมีต้นทุนสูง

ค.3 เครือข่ายและการควบคุมการเข้าถึง

คำศัพท์	ความหมายโดยย่อ
เครือข่ายท้องถิ่นเสมือน (Virtual Local Area Network: VLAN)	การแบ่งเครือข่ายเชิงตรรกะเพื่อช่วยแยกการสื่อสารระหว่างอุปกรณ์หรือกลุ่มระบบ
การแบ่งเครือข่าย (Network Segmentation)	การแบ่งระบบเครือข่ายออกเป็นส่วนหรือโซน และกำหนดการสื่อสารระหว่างส่วนตามความจำเป็นและระดับความเสี่ยง
หลักการไม่ให้ความเชื่อถือโดยปริยาย (Zero Trust Principles)	หลักการที่ไม่ให้ความเชื่อถือผู้ใช้ อุปกรณ์ หรือการเชื่อมต่อโดยอัตโนมัติจากตำแหน่งในเครือข่าย แต่พิจารณาตัวตน สิทธิ บริบท และความจำเป็นก่อนอนุญาต

คำศัพท์	ความหมายโดยย่อ
เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)	กลไกสำหรับสร้างช่องทางการสื่อสารที่ได้รับการป้องกันผ่านเครือข่ายอื่น เช่น อินเทอร์เน็ต เพื่อสนับสนุนการเข้าถึงจากระยะไกล
การเข้าถึงเครือข่ายตามหลัก Zero Trust (Zero Trust Network Access: ZTNA)	แนวทางควบคุมการเข้าถึงทรัพยากรโดยพิจารณาตัวตน สิทธิ บริบท และนโยบายก่อนอนุญาตการเชื่อมต่อ
การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA)	การพิสูจน์ตัวตนโดยใช้ปัจจัยอย่างน้อยสองประเภทที่แตกต่างกัน เช่น สิ่งที่ผู้ใช้รู้ สิ่งที่ผู้ใช้มี หรือคุณลักษณะเฉพาะของผู้ใช้
การควบคุมสิทธิตามบทบาท (Role-Based Access Control: RBAC)	การกำหนดสิทธิให้กับผู้ใช้งานตามบทบาทและหน้าที่ แทนการกำหนดสิทธิแบบอิสระเป็นรายบุคคลทุกกรณี
การให้สิทธิเท่าที่จำเป็น (Least Privilege)	หลักการให้สิทธิเฉพาะเท่าที่จำเป็นต่อการปฏิบัติหน้าที่ และไม่ให้สิทธิเกินความจำเป็น
การปฏิเสธโดยค่าเริ่มต้น (Default Deny)	หลักการปฏิเสธการเข้าถึงหรือการสื่อสารโดยค่าเริ่มต้น และอนุญาตเฉพาะรายการที่ได้รับการกำหนดไว้อย่างชัดเจน
การเปิดใช้เฉพาะฟังก์ชันที่จำเป็น (Least Functionality)	หลักการเปิดใช้งานเฉพาะฟังก์ชัน บริการ พอร์ต หรือโพรโทคอลที่จำเป็นต่อการปฏิบัติงาน เพื่อลดพื้นที่การโจมตี
การเข้าถึงจากระยะไกล (Remote Access)	การเข้าถึงระบบหรืออุปกรณ์จากภายนอกเครือข่ายหรือสถานที่ที่ระบบติดตั้ง เช่น ผ่าน VPN, ZTNA หรือบริการภายนอก

ค.4 การตั้งค่า การเฝ้าระวัง และการตรวจสอบ

คำศัพท์	ความหมายโดยย่อ
การตั้งค่าอย่างมั่นคงปลอดภัย (Secure Configuration)	การกำหนดค่าระบบเพื่อลดความเสี่ยง เช่น ปิดบริการที่ไม่จำเป็น จำกัดสิทธิ และใช้ช่องทางบริหารที่ได้รับการป้องกัน
ค่าฐานการตั้งค่าที่ได้รับอนุมัติ (Configuration Baseline)	ชุดค่าตั้งของระบบที่ได้รับการกำหนด ทบทวน และอนุมัติให้ใช้เป็นค่าฐานสำหรับการดำเนินงานและตรวจสอบการเปลี่ยนแปลง

คำศัพท์	ความหมายโดยย่อ
บันทึกเหตุการณ์เพื่อการตรวจสอบ (Audit Log)	บันทึกกิจกรรมหรือเหตุการณ์สำคัญที่ใช้สนับสนุนการตรวจสอบย้อนหลัง เช่น การเข้าสู่ระบบ การเปลี่ยนสิทธิ หรือการเปลี่ยนค่าตั้ง
ระบบบริหารข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM)	ระบบที่รวบรวม เชื่อมโยง วิเคราะห์ และช่วยแจ้งเตือนจากบันทึกเหตุการณ์หรือข้อมูลด้านความมั่นคงปลอดภัยจากหลายแหล่ง
การเฝ้าระวัง (Monitoring)	กระบวนการติดตามสถานะ เหตุการณ์ ประสิทธิภาพ หรือพฤติกรรมของระบบ เพื่อให้สามารถตรวจพบความผิดปกติได้อย่างเหมาะสม
การประสานเวลา (Time Synchronization)	การทำให้นาฬิกาของกล้อง เครื่องบันทึก ระบบบริหาร และระบบที่เกี่ยวข้องมีเวลาอ้างอิงสอดคล้องกัน เพื่อสนับสนุนการตรวจสอบเหตุการณ์

ค.5 ช่องโหว่ ความมั่นคงปลอดภัยของผลิตภัณฑ์ และวงจรชีวิต

คำศัพท์	ความหมายโดยย่อ
ช่องโหว่ (Vulnerability)	จุดอ่อนของผลิตภัณฑ์ ระบบ ซอฟต์แวร์ ค่าตั้ง หรือกระบวนการที่อาจถูกใช้เพื่อก่อให้เกิดผลกระทบด้านความมั่นคงปลอดภัย
CVE (Common Vulnerabilities and Exposures)	ระบบหมายเลขอ้างอิงสำหรับช่องโหว่ที่เปิดเผยต่อสาธารณะ เพื่อช่วยให้หน่วยงานและผู้ผลิตสามารถอ้างถึงช่องโหว่เดียวกันได้อย่างสอดคล้อง
การเปิดเผยข้อมูลช่องโหว่ (Vulnerability Disclosure)	กระบวนการรับแจ้ง ประสานงาน และสื่อสารข้อมูลเกี่ยวกับช่องโหว่ระหว่างผู้ค้นพบ ผู้ผลิต ผู้ให้บริการ และผู้เกี่ยวข้อง
การเปิดเผยช่องโหว่อย่างประสานงาน (Coordinated Vulnerability Disclosure: CVD)	กระบวนการที่ผู้ค้นพบช่องโหว่ ผู้ผลิต ผู้ให้บริการ และผู้เกี่ยวข้องร่วมกันรับแจ้ง วิเคราะห์ ยืนยัน แก้ไขหรือบรรเทา และสื่อสารข้อมูลอย่างเหมาะสม โดยคำนึงถึงการลดความเสี่ยงต่อผู้ใช้งานก่อนหรือร่วมกับการเปิดเผยข้อมูล

คำศัพท์	ความหมายโดยย่อ
การจัดการช่องโหว่ของผลิตภัณฑ์ (Vulnerability Handling)	กระบวนการตั้งแต่การรับหรือค้นพบช่องโหว่ การตรวจสอบและยืนยัน การประเมินผลกระทบ การจัดลำดับความสำคัญ การพัฒนาและทดสอบการแก้ไขหรือมาตรการบรรเทา การสื่อสาร ตลอดจนการติดตามผลหลังการแก้ไข
ประกาศแจ้งเตือนด้านความมั่นคงปลอดภัย (Security Advisory)	ข้อมูลที่ผู้ผลิตหรือผู้ให้บริการเผยแพร่เกี่ยวกับช่องโหว่ผลิตภัณฑ์หรือเวอร์ชันที่ได้รับผลกระทบ ผลกระทบ การแก้ไข และมาตรการลดความเสี่ยง
แพตช์หรือการแก้ไข (Patch)	การปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์เพื่อแก้ไขข้อผิดพลาดหรือช่องโหว่เฉพาะรายการ
การปรับปรุงด้านความมั่นคงปลอดภัย (Security Update)	การปรับปรุงซอฟต์แวร์ เฟิร์มแวร์ หรือองค์ประกอบที่มีวัตถุประสงค์เพื่อแก้ไขหรือลดความเสี่ยงด้านความมั่นคงปลอดภัย
เฟิร์มแวร์ที่ตรวจสอบแหล่งที่มาและความถูกต้องได้ (Signed Firmware)	เฟิร์มแวร์ที่ใช้ลายมือชื่อดิจิทัลหรือกลไกเทียบเท่าเพื่อช่วยยืนยันแหล่งที่มาและตรวจสอบว่าข้อมูลไม่ได้ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
การเริ่มต้นระบบอย่างมั่นคงปลอดภัย (Secure Boot)	กลไกที่ช่วยตรวจสอบความน่าเชื่อถือของซอฟต์แวร์หรือองค์ประกอบที่ถูกโหลดระหว่างการเริ่มต้นระบบ และป้องกันการโหลดองค์ประกอบที่ไม่ได้รับอนุญาตตามกลไกที่กำหนด
ความมั่นคงปลอดภัยของผลิตภัณฑ์ (Product Security)	การบริหารความมั่นคงปลอดภัยของผลิตภัณฑ์ตลอดวงจรชีวิต ตั้งแต่การกำหนดข้อกำหนด การออกแบบและพัฒนา การทดสอบ การส่งมอบ การอัปเดต การจัดการช่องโหว่ การตอบสนองต่อเหตุ และการยุติการสนับสนุน
ทีมตอบสนองเหตุด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ (Product Security Incident Response Team: PSIRT)	ทีม หน่วยงาน หรือกลไกที่รับผิดชอบการรับแจ้ง วิเคราะห์ ประสานงาน แก้ไข และสื่อสารประเด็นด้านช่องโหว่หรือความมั่นคงปลอดภัยของผลิตภัณฑ์ ทั้งนี้ องค์กรอาจใช้ชื่อหรือรูปแบบอื่นได้หากทำหน้าที่เทียบเท่า

คำศัพท์	ความหมายโดยย่อ
สถานะสิ้นสุดอายุผลิตภัณฑ์ (End of Life: EoL)	ช่วงหรือสถานะที่ผลิตภัณฑ์เข้าสู่ระยะสิ้นสุดวงจรชีวิตตามนโยบายของผู้ผลิต เช่น ยุติการจำหน่ายหรือเริ่มลดระดับการสนับสนุน ทั้งนี้ รายละเอียดอาจแตกต่างกันตามผู้ผลิต
สถานะสิ้นสุดการสนับสนุน (End of Support: EoS)	วันที่หรือสถานะที่ผู้ผลิตยุติการสนับสนุนบางส่วนหรือทั้งหมด เช่น การแก้ไขช่องโหว่ การปรับปรุงเฟิร์มแวร์ อะไหล่ หรือการสนับสนุนทางเทคนิค
การแจ้ง EoL/EoS	การแจ้งให้ผู้ใช้งานทราบล่วงหน้าเกี่ยวกับวันที่ ขอบเขตการสนับสนุนที่จะสิ้นสุด และแนวทางปรับปรุงหรือทดแทนเพื่อให้องค์กรสามารถวางแผนและบริหารความเสี่ยงได้
กระบวนการพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย (Secure Development Lifecycle: SDL)	กระบวนการของผู้ผลิตที่นำข้อกำหนดด้านความมั่นคงปลอดภัยเข้าไปในทุกขั้นตอนของการพัฒนาผลิตภัณฑ์ ตั้งแต่การออกแบบ การพัฒนา การทดสอบ จนถึงการดูแลหลังจำหน่าย เช่น ตาม IEC 62443-4-1
รากฐานความเชื่อถือในฮาร์ดแวร์ (Hardware Root of Trust)	องค์ประกอบฮาร์ดแวร์ที่เชื่อถือได้โดยการออกแบบ เช่น TPM หรือ Secure Element ใช้เป็นจุดเริ่มต้นในการตรวจสอบเฟิร์มแวร์ จัดเก็บกุญแจ และยืนยันตัวตนของอุปกรณ์
การยืนยันความน่าเชื่อถือของอุปกรณ์ (Device Attestation)	กลไกที่อุปกรณ์แสดงหลักฐานทางการเข้ารหัสต่อระบบอื่นว่าเป็นอุปกรณ์ของแท้และทำงานด้วยเฟิร์มแวร์ที่ไม่ถูกดัดแปลง
การป้องกันการดัดแปลง (Anti-Tamper)	กลไกทางกายภาพหรือทางตรรกะที่ป้องกันหรือตรวจจับการเปิด ถอด หรือแก้ไขอุปกรณ์โดยไม่ได้รับอนุญาต

ค.6 ส่วนประกอบซอฟต์แวร์และห่วงโซ่อุปทาน

คำศัพท์	ความหมายโดยย่อ
ส่วนประกอบซอฟต์แวร์ (Software Component)	ซอฟต์แวร์ ไลบรารี โมดูล กรอบการพัฒนา (Framework) หรือองค์ประกอบซอฟต์แวร์อื่นที่เป็นส่วนหนึ่งของผลิตภัณฑ์หรือระบบ รวมถึงส่วนประกอบจากบุคคลที่สามตามความเกี่ยวข้อง

คำศัพท์	ความหมายโดยย่อ
การบริหารส่วนประกอบซอฟต์แวร์ (Software Component Management)	กระบวนการในการระบุ ติดตาม ประเมิน และบริหารส่วนประกอบซอฟต์แวร์ที่มีความสำคัญ เพื่อสนับสนุนการติดตามช่องโหว่ การอัปเดต และการตอบสนองต่อเหตุ
ความโปร่งใสของห่วงโซ่อุปทาน (Supply Chain Transparency)	ความสามารถในการมีข้อมูลและหลักฐานเพียงพอเพื่อทำความเข้าใจและบริหารความเสี่ยงที่เกี่ยวข้องกับส่วนประกอบ ผู้ส่งมอบ หรือบริการที่เป็นส่วนหนึ่งของผลิตภัณฑ์หรือระบบ โดยไม่จำเป็นต้องเปิดเผยข้อมูลลับทางการค้าต่อสาธารณะทั้งหมด
การบริหารส่วนประกอบซอฟต์แวร์และความโปร่งใสของห่วงโซ่อุปทาน (Software Component Management and Supply Chain Transparency)	กระบวนการที่ช่วยให้องค์กรหรือผู้ผลิตสามารถทราบ บริหาร และติดตามส่วนประกอบซอฟต์แวร์และผู้เกี่ยวข้องในห่วงโซ่อุปทาน เพื่อสนับสนุนการติดตามช่องโหว่ การประเมินผลกระทบ การปรับปรุง การตอบสนองต่อเหตุ และการบริหารความเสี่ยง โดยไม่กำหนดว่าต้องใช้รูปแบบเอกสารหรือเครื่องมือเพียงรูปแบบเดียว
ความมั่นคงปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security)	การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยที่เกิดจากผู้ผลิต ผู้ส่งมอบ ผู้ให้บริการ ซอฟต์แวร์ ส่วนประกอบ และบริการที่เกี่ยวข้องกับผลิตภัณฑ์หรือระบบตลอดวงจรชีวิต
ผู้ให้บริการช่วง (Subprocessor)	ผู้ประมวลผลข้อมูลหรือผู้ให้บริการรายอื่นที่ผู้ให้บริการหลักนำมาใช้เพื่อสนับสนุนการประมวลผลหรือการให้บริการ

ค.7 การบริหารความเสี่ยงและการสร้างความเชื่อมั่น

คำศัพท์	ความหมายโดยย่อ
มาตรการชดเชย (Compensating Control)	มาตรการอื่นที่นำมาใช้เพื่อลดความเสี่ยง เมื่อยังไม่สามารถใช้มาตรการหลักหรือแก้ไขข้อจำกัดของระบบได้ โดยควรมีการประเมินความเพียงพอและทบทวนตามความเหมาะสม
ความเสี่ยงคงเหลือ (Residual Risk)	ความเสี่ยงที่ยังเหลืออยู่หลังจากดำเนินมาตรการควบคุมหรือมาตรการลดความเสี่ยงแล้ว

คำศัพท์	ความหมายโดยย่อ
การสร้างความเชื่อมั่น (Assurance)	ระดับความเชื่อมั่นที่เกิดจากหลักฐาน การทดสอบ การตรวจสอบ การประเมิน หรือการรับรอง ว่าระบบหรือมาตรการทำงานตามข้อกำหนดที่กำหนดไว้
หลักฐานประกอบการสร้างความเชื่อมั่น (Assurance Evidence)	เอกสาร ผลทดสอบ ใบรับรอง การสาธิต หรือหลักฐานอื่นที่ใช้สนับสนุนการประเมินว่าผลิตภัณฑ์ ระบบ หรือมาตรการมีความสามารถตามที่กำหนด
การยอมรับความเสี่ยง (Risk Acceptance)	การตัดสินใจของผู้มีอำนาจว่าความเสี่ยงคงเหลืออยู่ในระดับที่องค์กรยอมรับได้ภายใต้เงื่อนไขที่กำหนด
ค่าตั้งต้นด้านความมั่นคงปลอดภัย (Security Baseline)	ชุดมาตรการหรือข้อกำหนดพื้นฐานที่องค์กรกำหนดให้ใช้เป็นจุดเริ่มต้นสำหรับระบบตามระดับความสำคัญและความเสี่ยง
ระดับพื้นฐาน (Baseline: B)	ระดับมาตรการพื้นฐานสำหรับระบบที่มีผลกระทบและความเสี่ยงโดยรวมในระดับที่สามารถบริหารได้ด้วยมาตรการพื้นฐานที่กำหนด
ระดับเพิ่มเติม (Enhanced: E)	ระดับที่ต้องเพิ่มความเข้มงวดของมาตรการ การตรวจสอบ หรือหลักฐาน เนื่องจากมีผลกระทบหรือความเสี่ยงสูงกว่าระดับพื้นฐาน
ระดับความเชื่อมั่นสูง (High-Assurance: H)	ระดับสำหรับระบบที่อาจมีผลกระทบสูงและต้องการมาตรการ การทดสอบ การเฝ้าระวัง หรือหลักฐานที่เข้มงวดมากขึ้น

ค.8 การจัดการข้อมูลและหลักฐาน

คำศัพท์	ความหมายโดยย่อ
ระยะเวลาการเก็บรักษาข้อมูล (Retention Period)	ระยะเวลาที่องค์กรกำหนดให้เก็บรักษาข้อมูลก่อนลบ ทำลาย หรือเขียนทับ ตามวัตถุประสงค์ ความจำเป็น ความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง
การระงับการลบข้อมูลชั่วคราว (Hold)	การหยุดกระบวนการลบหรือเขียนทับข้อมูลตามรอบปกติชั่วคราว เนื่องจากมีเหตุผล เช่น การสอบสวน ข้อพิพาท หรือข้อกำหนดทางกฎหมาย
พื้นที่จัดเก็บที่แก้ไขไม่ได้ตามเงื่อนไขที่กำหนด (Immutable Storage)	พื้นที่จัดเก็บที่ออกแบบให้ข้อมูลไม่สามารถถูกแก้ไขหรือลบได้ในช่วงเวลาหรือภายใต้เงื่อนไขที่กำหนด

คำศัพท์	ความหมายโดยย่อ
การปิดบังพื้นที่ในภาพ (Privacy Mask)	การกำหนดพื้นที่บางส่วนของภาพไม่ให้แสดงหรือบันทึก เพื่อจำกัดข้อมูลที่ไม่จำเป็นต่อวัตถุประสงค์
การใช้ข้อมูลเท่าที่จำเป็น (Data Minimization)	หลักการเก็บ ใช้ เปิดเผย หรือประมวลผลข้อมูลเฉพาะเท่าที่จำเป็นต่อวัตถุประสงค์
ค่าแฮชเชิงเข้ารหัส (Cryptographic Hash)	ค่าที่คำนวณจากข้อมูลด้วยวิธีทางการเข้ารหัส เพื่อใช้สนับสนุนการตรวจสอบว่าข้อมูลมีการเปลี่ยนแปลงหรือไม่
ลำดับการครอบครองหลักฐาน (Chain of Custody)	การบันทึกและรักษาความต่อเนื่องของการครอบครอง การเข้าถึง การส่งมอบ และการจัดการหลักฐาน เพื่อสนับสนุนความน่าเชื่อถือและการตรวจสอบย้อนหลัง
ข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement)	ข้อตกลงระหว่างหน่วยงานที่กำหนดวัตถุประสงค์ ฐานทางกฎหมาย ขอบเขต เงื่อนไข ระยะเวลา และความรับผิดชอบในการแบ่งปันข้อมูลจากระบบ CCTV

ค.9 ความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

คำศัพท์	ความหมายโดยย่อ
บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA)	บันทึกเกี่ยวกับกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามบทบาทและข้อกำหนดที่เกี่ยวข้อง
ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)	ข้อตกลงที่กำหนดบทบาท หน้าที่ และเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคลระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลตามความเกี่ยวข้อง
การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)	การประเมินการประมวลผลที่อาจมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล เพื่อระบุความเสี่ยงและมาตรการลดผลกระทบตามหลักเกณฑ์ที่เกี่ยวข้อง
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)	บุคคลหรือหน่วยงานที่ปฏิบัติหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลตามเงื่อนไขที่กฎหมายกำหนด

คำศัพท์	ความหมายโดยย่อ
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลที่มีอำนาจตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมาย
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ตามกฎหมายที่เกี่ยวข้อง
เหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)	เหตุการณ์ที่ทำให้ข้อมูลส่วนบุคคลถูกทำลาย สูญหาย เปลี่ยนแปลง เปิดเผย หรือเข้าถึงโดยไม่ได้รับอนุญาตหรือโดยไม่ชอบ

ค.10 คลาวด์ สถานที่จัดเก็บข้อมูล และเขตอำนาจทางกฎหมาย

คำศัพท์	ความหมายโดยย่อ
ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC)	บุคคลหรือองค์กรที่ใช้บริการคลาวด์จากผู้ให้บริการ และมีหน้าที่กำหนดหรือดำเนินมาตรการในส่วนที่อยู่ภายใต้ความรับผิดชอบของตนตามรูปแบบบริการ สัญญา และข้อกำหนดที่เกี่ยวข้อง
ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP)	บุคคลหรือองค์กรที่ให้บริการคลาวด์แก่ผู้ใช้บริการ และรับผิดชอบการให้บริการและมาตรการด้านความมั่นคงปลอดภัยตามขอบเขตบริการ สัญญา และข้อกำหนดที่เกี่ยวข้อง
สถานที่จัดเก็บข้อมูล (Data Location)	สถานที่ทางกายภาพ ประเทศ หรือภูมิภาคที่ข้อมูลถูกจัดเก็บอยู่จริงในช่วงเวลาหนึ่ง
สถานที่ประมวลผลข้อมูล (Processing Location)	สถานที่หรือพื้นที่ที่มีการประมวลผล วิเคราะห์ จัดการ หรือดำเนินการอื่นกับข้อมูล
ถิ่นที่อยู่ของข้อมูล (Data Residency)	ประเทศหรือภูมิภาคที่กำหนดหรือคาดหมายให้ข้อมูลถูกจัดเก็บหรือประมวลผลตามรูปแบบบริการ นโยบาย หรือข้อตกลง
การกำหนดให้ข้อมูลอยู่ในพื้นที่หรือประเทศที่กำหนด (Data Localization)	ข้อกำหนดให้ข้อมูลบางประเภทต้องจัดเก็บ ประมวลผล หรือดำเนินการบางประการภายในพื้นที่หรือประเทศที่กำหนด

คำศัพท์	ความหมายโดยย่อ
อธิปไตยข้อมูล (Data Sovereignty)	การกำกับและควบคุมข้อมูลภายใต้กฎหมาย เขตอำนาจ และเงื่อนไขที่เกี่ยวข้องกับสถานที่จัดเก็บ การประมวลผล การบริหาร และการเข้าถึงข้อมูล
เขตอำนาจทางกฎหมาย (Jurisdiction)	เขตอำนาจหรือระบบกฎหมายที่อาจมีผลต่อข้อมูล ระบบ ผู้ให้บริการ บุคลากร หรือการดำเนินการที่เกี่ยวข้อง
ความรับผิดชอบร่วม (Shared Responsibility)	หลักการแบ่งความรับผิดชอบด้านความมั่นคงปลอดภัย การบริหารระบบ และข้อมูลระหว่างองค์กรกับผู้ให้บริการ โดยต้องระบุให้ชัดว่าแต่ละฝ่ายรับผิดชอบส่วนใด
แผนการยุติหรือเปลี่ยนบริการ (Exit Strategy)	แผนสำหรับการยุติ เปลี่ยน หรือย้ายบริการ ซึ่งครอบคลุมการนำข้อมูลกลับ การย้ายระบบ การเพิกถอนสิทธิ การลบข้อมูล และการรักษาความต่อเนื่องของบริการ

ความแตกต่างโดยสรุป

Data Location = ข้อมูลอยู่ที่ไหน

Processing Location = ข้อมูลถูกประมวลผลที่ไหน

Data Localization = มีข้อกำหนดให้ข้อมูลต้องอยู่หรือประมวลผลที่ไหน

Data Sovereignty = ข้อมูลอยู่ภายใต้กฎหมายหรือเขตอำนาจใดบ้าง

ค.11 ปัญญาประดิษฐ์และข้อมูลชีวมิติ

คำศัพท์	ความหมายโดยย่อ
ระบบ CCTV ที่มีการใช้ปัญญาประดิษฐ์ (AI-Enabled CCTV)	ระบบ CCTV ที่ใช้ AI เพื่อสนับสนุนการตรวจจับ จำแนก ติดตาม ระบุ วิเคราะห์ หรือสร้างผลลัพธ์จากข้อมูลภาพ วิดีโอ หรือข้อมูลที่เกี่ยวข้อง
ข้อมูลชีวมิติ (Biometric Data)	ข้อมูลที่เกิดจากการใช้เทคนิคเฉพาะในการประมวลผลลักษณะทางกายภาพ ทางสรีรวิทยา พฤติกรรม หรือชีวลักษณะ เพื่อวัตถุประสงค์เกี่ยวกับการระบุหรือยืนยันตัวบุคคลตามบริบทและกฎหมายที่เกี่ยวข้อง

คำศัพท์	ความหมายโดยย่อ
การรู้จำใบหน้า (Facial Recognition)	การประมวลผลลักษณะใบหน้าเพื่อเปรียบเทียบ ค้นหา ระบุ หรือยืนยันบุคคล โดยอาจเกี่ยวข้องกับข้อมูลชีวมิติตามลักษณะการใช้งานและกฎหมายที่เกี่ยวข้อง
ผลบวกเท็จ (False Positive)	กรณีที่ระบบระบุว่าพบเหตุ บุคคล หรือเงื่อนไขที่กำหนด ทั้งที่ข้อเท็จจริงไม่ได้เกิดขึ้น
ผลลบเท็จ (False Negative)	กรณีที่ระบบไม่ตรวจพบเหตุ บุคคล หรือเงื่อนไขที่เกิดขึ้นจริง
การกำกับดูแลโดยมนุษย์ (Human Oversight)	การกำหนดบทบาทและกลไกให้มนุษย์สามารถติดตาม ตรวจสอบ ทวนสอบ แทรกแซง หรือหยุดการทำงานของระบบ AI ได้ตามความเหมาะสม
การหยุดหรือแทรกแซงโดยมนุษย์ (Human Override)	ความสามารถของผู้มีอำนาจในการหยุด ระงับ เปลี่ยน หรือแทนที่การดำเนินการของระบบอัตโนมัติเมื่อจำเป็น
ขอบเขตการดำเนินการ (Action Boundary)	ขอบเขตที่กำหนดว่าระบบ AI สามารถดำเนินการหรือสั่งการเรื่องใดได้และไม่ได้ เพื่อลดผลกระทบจากการทำงานเกินวัตถุประสงค์หรือสิทธิที่กำหนด

ภาคผนวก ง เอกสาร กฎหมาย และมาตรฐานอ้างอิง

เอกสารอ้างอิงในภาคผนวกนี้ใช้เป็นกรอบสนับสนุนการจัดทำและประยุกต์ใช้แนวปฏิบัติฉบับนี้ โดยการอ้างอิงมาตรฐานมิได้หมายความว่าระบบ CCTV ทุกระบบต้องปฏิบัติตามหรือได้รับการรับรองตามมาตรฐานทุกฉบับ

สำหรับกฎหมาย ประกาศ หลักเกณฑ์ หรือข้อกำหนดของประเทศไทย องค์กรควรตรวจสอบฉบับที่มีผลใช้บังคับกับตน ณ เวลาที่นำแนวปฏิบัติไปใช้ รวมถึงข้อกำหนดเฉพาะของหน่วยงานกำกับดูแล สัญญา และข้อกำหนดเฉพาะภาคส่วนที่เกี่ยวข้อง

ง.1 กฎหมายและข้อกำหนดของประเทศไทย

1. **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** และกฎหมายลำดับรอง ประกาศ หลักเกณฑ์ หรือข้อกำหนดที่เกี่ยวข้อง
2. **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562** และกฎหมายลำดับรอง ประกาศ และแนวปฏิบัติที่เกี่ยวข้อง
3. **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม** และกฎหมายลำดับรองที่เกี่ยวข้อง ตามบทบาทและลักษณะของระบบ
4. **ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567** สำหรับองค์กร ระบบ หรือบริการที่อยู่ภายใต้ขอบเขตการใช้บังคับของประกาศ โดยประกาศมีผลบังคับใช้ตั้งแต่วันที่ 10 กันยายน 2569
5. กฎหมาย ประกาศ หลักเกณฑ์ หรือข้อกำหนดเฉพาะภาคส่วนที่เกี่ยวข้องกับลักษณะขององค์กร ระบบ ข้อมูล หรือบริการ
6. สัญญา ข้อกำหนดการจัดซื้อจัดจ้าง ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และนโยบายขององค์กรที่เกี่ยวข้อง

หมายเหตุ: การจัดระดับ B/E/H ตามแนวปฏิบัติฉบับนี้มิได้ใช้แทนการจำแนก การประเมินผลกระทบ หรือข้อกำหนดตามกฎหมายและประกาศของประเทศไทย

ง.2 ระบบเฝ้าระวังด้วยวิดีโอ

- IEC 62676-4:2025 — Video surveillance systems for use in security applications — Part 4: Application guidelines ใช้เป็นกรอบอ้างอิงหลักสำหรับการวางแผน การกำหนดความต้องการเชิงปฏิบัติการ การสำรวจพื้นที่ การออกแบบ การเลือกอุปกรณ์และเลนส์ คุณภาพของภาพ ความหนาแน่นของพิกเซล การติดตั้ง การทดสอบ การตรวจรับ การดำเนินงาน และการบำรุงรักษาระบบเฝ้าระวังด้วยวิดีโอ
- IEC 62676 series ส่วนอื่น สามารถนำมาใช้ตามลักษณะของระบบและความเกี่ยวข้อง

- ข้อเสนอแนะของ สหภาพโทรคมนาคมระหว่างประเทศ ภาคการมาตรฐานโทรคมนาคม (International Telecommunication Union – Telecommunication Standardization Sector: ITU-T) ที่เกี่ยวข้องกับระบบเฝ้าระวังด้วยวิดีโอ สามารถใช้เป็นข้อมูลอ้างอิงเพิ่มเติมตามความเหมาะสม

องค์กรควรตรวจสอบฉบับและส่วนของมาตรฐานที่ใช้จริง เนื่องจากมาตรฐานในชุดเดียวกันอาจครอบคลุมวัตถุประสงค์ ขอบเขต และวิธีการประเมินแตกต่างกัน

ง.3 ความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัว

- **ISO/IEC 27001 — Information security management systems**
- **ISO/IEC 27002 — Information security controls**
- **ISO/IEC 27701 — Privacy information management systems**
- **ISO/IEC 27036 series — Information security for supplier relationships**

มาตรฐานกลุ่มนี้ใช้เป็นกรอบสนับสนุนด้านการกำกับดูแล การบริหารความเสี่ยง การควบคุมการเข้าถึง การจัดการทรัพย์สิน การบันทึกเหตุการณ์ การบริหารผู้ให้บริการ ความต่อเนื่อง และการบริหารข้อมูลส่วนบุคคลตามความเกี่ยวข้อง

ง.4 ความมั่นคงปลอดภัยของผลิตภัณฑ์และระบบที่เชื่อมต่อ

- **IEC 62443 series — Security for industrial automation and control systems**
- **IEC 62443-4-1 — Secure product development lifecycle requirements** ตามความเกี่ยวข้อง
- **IEC 62443-4-2 — Technical security requirements for IACS components** ตามความเกี่ยวข้อง
- **ETSI EN 303 645 — Cyber Security for Consumer Internet of Things: Baseline Requirements**
- **IEEE 802.1AR — Secure Device Identity**

มาตรฐานกลุ่มนี้สามารถใช้สนับสนุนแนวคิดการป้องกันเชิงลึก การแบ่งโซนและช่องทางการสื่อสาร ตลอดจนกระบวนการพัฒนาผลิตภัณฑ์อย่างมั่นคงปลอดภัย โดยไม่ควรตีความว่าระบบ CCTV ทุกระบบเป็นระบบ OT หรือ ICS

ง.5 การเปิดเผยและการจัดการช่องโหว่

- **ISO/IEC 29147 — Vulnerability disclosure**
- **ISO/IEC 30111 — Vulnerability handling processes**

มาตรฐานดังกล่าวใช้เป็นกรอบสนับสนุนการรับแจ้ง วิเคราะห์ ประเมิน ประสานงาน แก้ไขหรือบรรเทา และสื่อสารเกี่ยวกับช่องโหว่ รวมถึงการเปิดเผยช่องโหว่อย่างประสานงาน (Coordinated Vulnerability Disclosure: CVD)

องค์กรควรตรวจสอบฉบับที่เป็นปัจจุบันของมาตรฐานดังกล่าว ณ เวลาที่นำไปใช้อ้างอิง

ง.6 บริการคลาวด์

- **ISO/IEC 27017 — Information security controls for cloud services**
- **ISO/IEC 27018 — Protection of personally identifiable information in public clouds acting as PII processors**
- **ISO/IEC 27701 — Privacy information management systems** ตามความเกี่ยวข้อง
- **ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567** สำหรับกรณีที่อยู่ภายใต้ขอบเขตการใช้บังคับ

การอ้างอิงมาตรฐานสากลด้านคลาวด์ไม่ใช้แทนหน้าที่ตามประกาศของประเทศไทยที่มีผลใช้บังคับ

ง.7 ข้อมูลชีวมิติและระบบ CCTV ที่ใช้ AI

สำหรับระบบ CCTV ที่มีการใช้ AI หรือข้อมูลชีวมิติ สามารถพิจารณามาตรฐานที่เกี่ยวข้องตามลักษณะการใช้งาน เช่น

- **ISO/IEC 24745 — Biometric information protection**
- **ISO/IEC 19795 series — Biometric performance testing and reporting**
- **ISO/IEC 30107 series — Biometric presentation attack detection**
- มาตรฐานและแนวทางด้านการบริหารความเสี่ยงและความมั่นคงปลอดภัยของ AI ที่ระบุใน แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบกล้องโทรทัศน์วงจรปิดที่ใช้ปัญญาประดิษฐ์สำหรับประเทศไทย

ง.8 หลักการใช้เอกสารอ้างอิง

การนำมาตรฐาน เอกสารรับรอง รายงานผลการทดสอบ หรือแนวทางจากหน่วยงานอื่นมาใช้ ควรพิจารณาอย่างน้อยถึง

- ความเกี่ยวข้องกับระบบและความเสี่ยงที่ต้องการควบคุม
- ขอบเขตของมาตรฐานหรือหลักฐาน
- รุ่นและเวอร์ชันของผลิตภัณฑ์หรือระบบ
- สถานะและความเป็นปัจจุบันของเอกสาร

- ข้อจำกัดหรือข้อยกเว้น
- ระดับความเป็นอิสระของการประเมิน

การอ้างอิงมาตรฐานหรือการมีใบรับรองไม่ควรถูกใช้เป็นปัจจัยเพียงอย่างเดียวในการสรุปว่าระบบมีความมั่นคงปลอดภัยเพียงพอสำหรับบริบทใดบริบทหนึ่ง