



**คำแนะนำการรักษาความปลอดภัยประกอบ  
การขอเป็นผู้ประกอบการระดับมาตรฐานเออีโอ  
(Authorized Economic Operator: AEO)**

## บทนำ (Introduction)

โครงการผู้ประกอบการระดับมาตรฐานเออีโอ (Authorized Economic Operator: AEO) เริ่มมาจากเหตุการณ์การก่อการร้าย ๙๑๑ เมื่อวันที่ ๑๑ กันยายน ๒๕๔๔ เป็นต้นมา ทำให้ทั่วโลกตระหนักถึงความสำคัญของมาตรการความปลอดภัยในการขนส่งสินค้าระหว่างประเทศ จึงได้มีมาตรการเพื่อป้องกันการก่อการร้ายขึ้นหลายมาตรการ โดยนานาประเทศได้สร้างระเบียบที่เน้นหนักในเรื่องการเพิ่มความเข้มงวดด้านความปลอดภัยตั้งแต่แหล่งกำเนิดสินค้าไปตลอดห่วงโซ่อุปทานของการขนส่งสินค้า ด้วยการระบุสินค้าที่มีความเสี่ยงอันตรายสูงให้เร็วที่สุดก่อนการนำเข้า การพิจารณาผู้ประกอบการที่มีความน่าเชื่อถือสูงในด้านความปลอดภัย และกำหนดให้แจ้งข้อมูลล่วงหน้าก่อนการนำเข้า-ส่งออก โดยหน่วยงานศุลกากรของแต่ละประเทศจะต้องมีความพร้อมในการแลกเปลี่ยนข้อมูลล่วงหน้าระหว่างกันผ่านระบบอิเล็กทรอนิกส์

องค์การศุลกากรโลกหรือ WCO ได้กำหนดกรอบมาตรฐานในการรักษาความปลอดภัย และการอำนวยความสะดวกทางการค้าโลก (Framework of Standards to Secure and Facilitate Global Trade : SAFE) มีหลักการสำคัญประการหนึ่ง คือ ความร่วมมือกันระหว่างศุลกากร และผู้ประกอบการของแต่ละประเทศเพื่อสร้างความปลอดภัยตลอดห่วงโซ่อุปทานของการนำเข้าและส่งออกสินค้า โดยองค์การศุลกากรโลกได้กำหนดโครงการ Authorized Economic Operator (AEO) ขึ้นเป็นแนวทางปฏิบัติเพื่อรับรองผู้ประกอบการที่เกี่ยวข้องกับการเคลื่อนย้ายสินค้าตลอดห่วงโซ่อุปทานที่มีการดำเนินงานที่มีมาตรฐาน มีความปลอดภัยน่าเชื่อถือ ได้รับการรับรองจากศุลกากรว่าได้ปฏิบัติตามมาตรฐานขององค์การศุลกากรโลกในเรื่องการรักษาความปลอดภัยครอบคลุมตั้งแต่ผู้ผลิต ผู้นำเข้า ผู้ส่งออก ตัวแทนออกของ ผู้ขนส่ง ผู้รวบรวม คนกลาง ท่าเรือ ท่าอากาศยาน ผู้ประกอบกิจการท่ารถ คลังสินค้า ผู้จัดการหน่วย เป็นต้น ขณะนี้ได้มีหลายประเทศดำเนินโครงการ AEO แล้ว ภายใต้ชื่อเรียกที่แตกต่างกัน เช่น โครงการ Customs-Trade Partnership Against Terrorism (C-TPAT) ของประเทศสหรัฐอเมริกา โครงการ Secure Export Scheme ของประเทศนิวซีแลนด์ โครงการ Secure Trade Partnership ของประเทศสิงคโปร์ โครงการ Classified Management of Enterprises ของประเทศจีน โครงการ AEO ของประเทศเกาหลีและประเทศญี่ปุ่น เป็นต้น

ผู้ประกอบการที่สนใจเข้าร่วมโครงการ AEO จะต้อง

- (๑) จัดทำระบบการจัดการรักษาความปลอดภัย
- (๒) จัดทำการประเมินความเสี่ยงในด้านการรักษาความปลอดภัยภายในสถานประกอบการของตน โดยเปรียบเทียบกับแนวทางที่กำหนดในคำแนะนำการรักษาความปลอดภัยประกอบการขอเป็นผู้ประกอบการระดับมาตรฐานเออีโอ
- (๓) จัดทำเอกสารชี้แจงการรักษาความปลอดภัยของหน่วยงาน (Security Profile) เพื่อให้เห็นภาพรวมของบริษัทในการดำเนินมาตรการในการรักษาความปลอดภัยภายใต้คำแนะนำ นี้ไปใช้

เอกสารคำแนะนำการรักษาความปลอดภัยประกอบการขอเป็นผู้ประกอบการระดับมาตรฐานเออีโอ เป็นเอกสารที่นำเสนอเนื้อหา เพื่อใช้เป็นกรอบสำหรับกำหนดแนวทางในการพัฒนามาตรการรักษาความปลอดภัยขององค์กร รวมถึงการนำไปใช้ การติดตาม ประเมินผล และการปรับปรุงมาตรการที่มีอยู่แล้วให้มีประสิทธิภาพยิ่งขึ้น

/ ระบบการ...

## ๑. ระบบการจัดการรักษาความปลอดภัย (Security Management System)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการจะต้องสร้างระบบจัดการรักษาความปลอดภัยที่เป็นมาตรฐาน มีประสิทธิภาพ มีความต่อเนื่อง และมีการทบทวนปรับปรุงการดำเนินงานให้ทันสมัยอยู่เสมอ เพื่อลดความเสี่ยงในการดำเนินงานขององค์กร และผู้ที่เกี่ยวข้องทั้งห่วงโซ่อุปทาน โดยสาระสำคัญของระบบการจัดการความปลอดภัย มีดังนี้

- (๑) นโยบาย วัตถุประสงค์ และพันธกิจระบบการจัดการรักษาความปลอดภัยขององค์กรที่เป็นการแสดงถึงความมุ่งมั่นของผู้บริหารระดับสูงที่มีต่อการรักษาความปลอดภัย เป็นการแสดงถึงทิศทาง และหลักปฏิบัติงานสำหรับองค์กร
- (๒) การประเมินความเสี่ยงด้านการรักษาความปลอดภัย และการกำหนดมาตรการระบบการจัดการรักษาความปลอดภัย เพื่อความสำเร็จในการดำเนินงาน
- (๓) การจัดทำขั้นตอนปฏิบัติงาน การนำไปปฏิบัติ ซึ่งต้องมีการกำหนดโครงสร้างองค์กร อำนาจหน้าที่ และความรับผิดชอบอย่างชัดเจน มีการฝึกอบรมเพื่อให้เกิดการตระหนักของบุคลากรที่มีส่วนเกี่ยวข้องกับระบบการจัดการรักษาความปลอดภัย มีกระบวนการสื่อสารและควบคุมข้อมูล มีการควบคุมการปฏิบัติงานด้านการรักษาความปลอดภัย มีการเตรียมความพร้อมต่อสถานการณ์ต่างๆ การตอบสนอง และการฟื้นฟู เพื่อให้การดำเนินการมีมาตรฐาน มีประสิทธิภาพ และมีความต่อเนื่อง
- (๔) การตรวจสอบ วัดผล ประเมินผลการดำเนินงานให้เป็นไปตามมาตรฐานที่กำหนด มีการพิจารณาความผิดพลาดที่เกิดขึ้น และการแนวทางปฏิบัติต่อเหตุการณ์ที่ไม่เป็นไปตามข้อกำหนด
- (๕) การทบทวน และปรับปรุงระบบการจัดการรักษาความปลอดภัยอย่างต่อเนื่อง เพื่อให้มั่นใจว่าระบบยังมีความเหมาะสม และมีประสิทธิภาพ รวมถึงการประเมินโอกาสในการปรับปรุง และความจำเป็นที่ต้องเปลี่ยนแปลงระบบเพื่อให้ทันสมัย ต่อเนื่อง และมีประสิทธิภาพ

## ๒. การประเมินความเสี่ยง (Risk Assessment)

องค์กรที่เข้าร่วมโครงการ AEO นี้ จะต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความปลอดภัยที่อาจเกิดขึ้นในการดำเนินธุรกิจของตน รวมถึงธุรกิจที่เกี่ยวข้อง ดังนี้

### ผู้ผลิตหรือผู้จัดหาสินค้า (Manufacturers/ Suppliers)

ผู้ผลิตหรือผู้จัดหาสินค้า โดยปกติจะเป็นหน่วยงานเริ่มต้นของเครือข่ายการเคลื่อนย้ายสินค้าทั้งหมด วัตถุดิบ และสินค้าที่มาจากโรงงานเหล่านี้จะต้องมีเอกสารกำกับที่ถูกต้องตั้งแต่แรกเริ่ม เพื่อป้องกันความผิดพลาดของข้อมูล และลดขั้นตอนการตรวจสอบรายละเอียดในภายหลัง ดังนั้น การจัดทำบัญชีสินค้าที่ถูกต้อง การบรรจุหีบห่อที่มิดชิดแน่นหนา และการจัดส่งเอกสารที่ชัดเจนจะช่วยให้ผู้ผลิตหรือผู้จัดหาสินค้าสามารถจัดส่งสินค้าให้กับผู้รับสินค้าลำดับต่อไปได้อย่างปลอดภัย

### ผู้ประกอบการโรงพักสินค้า และเจ้าของโรงพักสินค้า

ผู้ประกอบการโรงพักสินค้าและเจ้าของโรงพักสินค้า จะเป็นผู้ได้รับมอบสินค้าจากผู้ผลิตหรือผู้จัดหาสินค้า เพื่อทำการเก็บรักษาและส่งต่อไปให้ผู้รับสินค้าลำดับต่อไป ดังนั้น ผู้ประกอบการโรงพักสินค้าและเจ้าของโรงพักสินค้าจะต้องมีระบบการจัดเก็บข้อมูลที่สามารถตรวจสอบสินค้าทั้งการนำเข้ามา และการจัดเก็บ ตลอดจนสามารถจัดส่งข้อมูลให้ผู้รับสินค้าลำดับต่อไปได้ทันที นอกจากนี้โรงพักสินค้าจะต้องมีระบบการรักษาความปลอดภัยที่มีประสิทธิภาพ แสดงให้เห็นว่าสินค้าที่เก็บรักษาไว้มีความปลอดภัย

### ผู้ประกอบการขนส่ง

ผู้ประกอบการขนส่งมีความรับผิดชอบหลักในการขนส่งสินค้าจากจุดหนึ่งไปยังอีกจุดหนึ่ง ดังนั้น ผู้ประกอบการขนส่งจะต้องมีมาตรการในการป้องกันมิให้ยานพาหนะที่ใช้ในการขนส่ง ถูกปล้น หรือถูกนำไปใช้ในทางที่ผิด อีกทั้งจะต้องมีระบบการจัดเก็บข้อมูลที่สามารถควบคุมและติดตามสินค้าได้อย่างมีประสิทธิภาพ สร้างความมั่นใจว่าสินค้าที่บรรทุกไปกับยานพาหนะนั้น จะไม่ถูกสับเปลี่ยนหรือทำลาย

### ผู้ประกอบการท่า/ที่

ผู้ประกอบการท่า/ที่ มีความรับผิดชอบหลักในการดูแลสินค้าและตู้คอนเทนเนอร์ ทั้งก่อนที่จะนำขึ้นเครื่องบินหรือยานพาหนะอื่น และหลังจากนำสินค้าและตู้คอนเทนเนอร์ลงจากเครื่องบินหรือยานพาหนะอื่น โดยเฉพาะอย่างยิ่ง ท่า/ที่จะเป็นจุดสุดท้ายในการส่งสินค้าออก และเป็นจุดแรกในการนำสินค้าเข้า ดังนั้น อาคารและสถานที่ที่ใช้ในการจัดเก็บสินค้าและตู้คอนเทนเนอร์ จึงควรมีระบบการรักษาความปลอดภัยที่มีประสิทธิภาพและเชื่อถือได้

### ผู้ประกอบการขนส่งทางเรือ/อากาศยาน/ทางบก

ผู้ประกอบการขนส่งทางเรือ/อากาศยาน/ทางบก มีความรับผิดชอบหลักในการขนส่งสินค้าจากจุดหนึ่งไปยังอีกจุดหนึ่ง ดังนั้น จึงควรมีมาตรการเพื่อป้องกันมิให้ยานพาหนะถูกปล้นหรือถูกสับเปลี่ยนระหว่างการเดินทาง ผู้ประกอบการควรจะมีระบบการจัดเก็บข้อมูลที่สามารถควบคุมและติดตามสินค้าที่ไปกับยานพาหนะนั้น นอกจากนี้ ผู้ประกอบการควรจะสร้างความมั่นใจว่ายานพาหนะของตน รวมทั้งสินค้าบนยานพาหนะจะไม่ถูกสับเปลี่ยนหรือทำลายได้

/ตัวแทนออก...

## ตัวแทนออกของ

ตัวแทนออกของ มีความรับผิดชอบในการดำเนินการในส่วนที่เกี่ยวข้องกับกรมศุลกากร เช่น การดำเนินพิธีศุลกากร เสียภาษีอากร และรับสินค้าที่นำเข้าหรือส่งออกไปต่างประเทศ ดังนั้น ตัวแทนออกของจะต้องมีมาตรการดำเนินการเพื่อความปลอดภัย และความถูกต้องของเอกสารและสินค้าที่รับผิดชอบอย่างชัดเจน มีมาตรฐาน เป็นที่น่าเชื่อถือ

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการจะต้องจัดทำขั้นตอนการประเมินความเสี่ยงในด้านการรักษาความปลอดภัยเกี่ยวกับห่วงโซ่อุปทาน ทั้งนี้ ควรมีรายละเอียดครอบคลุมเรื่องดังต่อไปนี้

- (๑) ขั้นตอนปฏิบัติในการประเมินความเสี่ยง โดยสามารถแสดงเป็นแผนภูมิแสดงลำดับขั้นตอน (Flow Chart) ในการประเมินความเสี่ยง
- (๒) การระบุความเสี่ยงและจุดอ่อนของระบบการจัดการรักษาความปลอดภัย
- (๓) สาเหตุที่เกิดความเสี่ยง
- (๔) ข้อกำหนด และมาตรการต่างๆ ที่นำมาใช้เพื่อลดความเสี่ยงและจุดอ่อนนั้นๆ
- (๕) บุคคลหรือหน่วยงานที่รับผิดชอบในเรื่องการประเมินความเสี่ยง
- (๖) ข้อมูลรายละเอียดอื่นๆ ที่เกี่ยวข้อง

### ๓. มาตรการรักษาความปลอดภัย (Security System)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการ จะต้องจัดทำมาตรการรักษาความปลอดภัย ซึ่งมีองค์ประกอบสำคัญ ๘ ด้าน ดังนี้

- (๑) ความปลอดภัยในการเข้า-ออกอาคารสถานที่
- (๒) ความปลอดภัยในส่วนที่เกี่ยวกับพนักงาน
- (๓) ความปลอดภัยในส่วนของพันธมิตรทางธุรกิจ
- (๔) ความปลอดภัยในส่วนที่เกี่ยวกับสินค้า
- (๕) ความปลอดภัยสำหรับยานพาหนะขนส่งสินค้า
- (๖) ความปลอดภัยทางด้านเทคโนโลยีสารสนเทศและเอกสาร
- (๗) การจัดการเหตุวิกฤตและระบบการสืบสวนเหตุการณ์
- (๘) การประเมินความเสี่ยงและการวิเคราะห์ความเสี่ยง

มาตรการรักษาความปลอดภัยที่จัดทำขึ้นจะต้องระบุรายละเอียดกิจกรรมนั้นๆ ให้มากที่สุดเท่าที่จะเป็นไปได้ รวมถึงแนบเอกสารอ้างอิง อาทิ คู่มือการปฏิบัติงานที่อธิบายถึงมาตรการรักษาความปลอดภัยต่างๆ ระบุฝ่ายรับผิดชอบ และความถี่ในการดำเนินการต่างๆ ให้ชัดเจน พร้อมเอกสารที่แสดงให้เห็นว่าได้ดำเนินการกิจกรรมนั้นๆ จริง

ในกรณีที่มีได้มีมาตรการรักษาความปลอดภัยในด้านใดด้านหนึ่ง หรือหลายด้านดังที่ได้กล่าวไว้ข้างต้น กรุณาระบุถึงสาเหตุที่มีได้กำหนดไว้ และหากองค์กรได้กำหนดมาตรการแตกต่างจากที่ระบุไว้ ขอให้จัดทำรายละเอียดมาตรการที่แตกต่างดังกล่าวไว้ในรายงานด้วย

ในกรณีมีหลายสถานที่หรือหลายสาขา และสถานที่หรือสาขานั้นมีมาตรการรักษาความปลอดภัยที่แตกต่างออกไปค่อนข้างมาก จะต้องจัดทำรายงานมาตรการรักษาความปลอดภัยแยกไว้ด้วย

สำหรับแนวทางในการจัดทำรายงานมาตรการด้านการรักษาความปลอดภัยในแต่ละด้าน สามารถดูรายละเอียดได้จากเอกสารแนบท้ายนี้

**เอกสารแนบท้าย**  
**แนวทางสำหรับจัดทำมาตรการรักษาความปลอดภัยในด้านต่างๆ**

**๑. ความปลอดภัยในการเข้า-ออกอาคารสถานที่ (Premise Security and Access Control)**

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการต้องมีระบบการป้องกันมิให้ผู้ไม่มีอำนาจ หรือผู้ไม่มีส่วนเกี่ยวข้อง เข้าไปในอาคารสถานที่ขององค์กร ไม่ว่าจะเป็นด้านในหรือด้านนอกตัวอาคารสถานที่ ระบบจะต้องสามารถตรวจสอบได้ว่า ผู้ที่เข้า-ออกในแต่ละช่องทางนั้นคือใคร มีอำนาจหน้าที่ หรือได้รับอนุญาตหรือไม่ ทั้งนี้ หน่วยงานต้องมีแผนผังแสดงทางเข้า-ออกทุกจุด และมีการควบคุมการผ่านเข้า-ออก ของจุดดังกล่าว รวมทั้งมีการวิเคราะห์หาจุดอ่อนเพื่อป้องกันการเข้าของบุคคลที่ไม่มีอำนาจหรือไม่มีส่วนเกี่ยวข้อง

การรักษาความปลอดภัยควรคำนึงถึงเรื่องดังต่อไปนี้ โดยคำนึงถึงประเภทและขนาดของธุรกิจ รวมถึงการประเมินความเสี่ยงขององค์กรและธุรกิจที่เกี่ยวข้องด้วย

	พื้นที่/บริเวณ	แนวทางการรักษาความปลอดภัย
๑.๑	อาณาเขตของรั้ว	<ul style="list-style-type: none"> <li>- ต้องมีรั้วล้อมรอบอาณาเขตทั้งหมดรวมถึงพื้นที่จัดเก็บหรือวางสินค้า ตู้คอนเทนเนอร์ หัวลากหางลากและรถบรรทุก ทั้งนี้ รั้วดังกล่าวจะต้องได้รับการดูแลอย่างสม่ำเสมอเพื่อให้อยู่ในสภาพที่ใช้งานได้ตามปกติ</li> <li>- ต้องระบุรายละเอียดของรั้วล้อมรอบ และ สิ่งกีดขวางก่อนที่จะเข้าถึงตัวสินค้าหรืออุปกรณ์ที่เกี่ยวข้อง รวมถึงรายละเอียดในการบำรุงรักษารั้วล้อมรอบ และสิ่งกีดขวางนั้น ฝ่ายรับผิดชอบและความถี่ในการตรวจสอบฯ</li> </ul>
๑.๒	ประตูรั้ว และประตูเข้า-ออก อาคารสถานที่	<ul style="list-style-type: none"> <li>- ประตูเข้า-ออก สำหรับพาหนะและ/หรือบุคคล จะต้องม้เจ้าหน้าที่ควบคุม และดูแลอยู่ตลอดเวลา</li> <li>- ต้องระบุมตรการที่ใช้ควบคุมบุคคล และยานพาหนะที่ผ่านเข้าออกประตูรั้ว และประตูเข้า-ออก อาคารสถานที่ เครื่องมือที่ใช้ควบคุมและดูแล และฝ่ายรับผิดชอบ</li> </ul>
๑.๓	บริเวณที่จอดรถ	<ul style="list-style-type: none"> <li>- ต้องมีการกำหนดพื้นที่จอดรถสำหรับพนักงาน บุคคลภายนอก รถขนส่งสินค้า และรถหัวลากอย่างชัดเจน</li> <li>- ต้องระบุพื้นที่อย่างชัดเจน มีการทำแผนผัง และมีแนวทางการประชาสัมพันธ์ให้ทราบ และปฏิบัติตามอย่างเคร่งครัด มีมาตรการในการควบคุมดูแลพื้นที่ เช่น มีเจ้าหน้าที่รักษาความปลอดภัยคอยตรวจสอบพื้นที่จอดรถโดยแยกประเภทของรถจากประเภทของสตีกเกอร์ที่ติดรถ การบันทึกการเข้าออกของรถแต่ละประเภท มีการควบคุมและกำกับพื้นที่จอดรถของบุคคลภายนอกอย่างใกล้ชิด มีการกำหนดฝ่ายรับผิดชอบ</li> <li>- การกำหนดจุดจอดรถในพื้นที่เสี่ยง เช่น จุดจอดรถที่สามารถเข้าถึงจุดขนถ่ายและเก็บสินค้า และระบุฝ่ายรับผิดชอบ</li> </ul>
๑.๔	โครงสร้างอาคารสถานที่	<ul style="list-style-type: none"> <li>- สร้างด้วยวัสดุที่ได้มาตรฐานตามที่กฎหมายกำหนด สามารถป้องกันการบุกรุก และควรได้รับการดูแลและซ่อมแซมอย่างสม่ำเสมอ เพื่อให้สามารถใช้งานได้ตามปกติ</li> <li>- ระบุรายละเอียดอาคารสถานที่ มาตรการที่ใช้ในการบำรุงรักษา และซ่อมแซมโครงสร้างอาคารสถานที่ ฝ่ายรับผิดชอบ และความถี่ในการตรวจสอบ</li> </ul>

๑.๕	อุปกรณ์ล็อก	<ul style="list-style-type: none"> <li>- หน้าต่าง ประตู และประตูรั้วทุกบานจะต้องมีอุปกรณ์ล็อก หรือเครื่องมืออื่นที่ใช้เพื่อควบคุมและป้องกันการเข้าออกพื้นที่ และมีมาตรการควบคุมดูแลและป้องกันการบุกรุก</li> <li>- ระบุรายละเอียดอุปกรณ์ปิดล็อกวิธีการควบคุมดูแล การตรวจสอบสภาพอุปกรณ์ปิดล็อกให้พร้อมใช้งาน ระบุฝ่ายรับผิดชอบ และรายละเอียดการรับผิดชอบบุญแจ รวมถึงการยืม-คืนบุญแจ</li> </ul>
๑.๖	แสงสว่าง	<ul style="list-style-type: none"> <li>- จัดให้มีแสงสว่างเพียงพอทั้งในอาคารสถานที่ และบริเวณโดยรอบทั้ง ด้านในและด้านนอก ซึ่งรวมถึงทางเข้า-ออก บริเวณรับ-ส่งสินค้า และที่เก็บสินค้า บริเวณกำแพง/รั้ว และที่จอดรถ และระบุรายละเอียดการบำรุงรักษาแสงสว่างให้อยู่ในสภาพที่สามารถใช้งานได้เหมาะสม</li> <li>- ระบุรายละเอียดของระบบแสงสว่างที่ใช้ให้เพียงพอ และเหมาะสมกับพื้นที่ (เช่น จำนวนและชนิดของหลอดไฟต่อพื้นที่วัดเป็นตารางเมตร เป็นต้น) การดูแลรักษา สภาพของอุปกรณ์ให้แสงสว่าง ระบุฝ่ายรับผิดชอบ และความถี่ในการดูแลรักษา</li> </ul>
๑.๗	ระบบแจ้งเตือนภัย และกล้องวงจรปิด	<ul style="list-style-type: none"> <li>- ติดตั้งระบบเตือนภัยและกล้องวงจรปิด เพื่อป้องกันเหตุอันตราย การบุกรุก ขยายพื้นที่ในการรักษาความปลอดภัยให้ครอบคลุม และใช้ในการสืบสวนเหตุการณ์ผิดปกติในภายหลังด้วย</li> <li>- ระบุรายละเอียดระบบเตือนภัยและกล้องวงจรปิด (จำนวนและชนิดของระบบเตือนภัยและกล้องวงจรปิด) รายละเอียดของพื้นที่ที่ระบบเตือนภัยและกล้องวงจรปิดสามารถเข้าถึงได้ รวมถึงการบำรุงรักษาและตรวจสอบระบบให้พร้อมใช้งาน ระบุฝ่ายรับผิดชอบ และความถี่ในการตรวจสอบให้ชัดเจน</li> </ul>
๑.๘	บริเวณหวงห้าม (Restricted Area)	<ul style="list-style-type: none"> <li>- กำหนดพื้นที่หวงห้ามให้ชัดเจน และประกาศให้ทราบโดยทั่วกัน</li> <li>- ในกรณีที่มีการระบุพื้นที่พิเศษ เช่น มีสินค้าอันตราย สินค้ามูลค่าสูง คลังสินค้าภัณฑ์บนให้อธิบายรายละเอียดพื้นที่ วิธีการดูแล การเข้าออกพื้นที่ และระบุฝ่ายรับผิดชอบให้ชัดเจน</li> <li>- ระบุรายละเอียดที่กำหนดพื้นที่หวงห้าม วิธีการควบคุมดูแล การเข้า-ออกพื้นที่หวงห้าม ระบุฝ่ายรับผิดชอบ</li> </ul>
๑.๙	พนักงานรักษาความปลอดภัย	<ul style="list-style-type: none"> <li>- มีมาตรการในการกำหนดตัวบุคคลหรือหน่วยงานรักษาความปลอดภัย หรืออาจใช้บริการจากบริษัทภายนอกที่รับจ้างดูแลรักษาความปลอดภัย เพื่อให้หน่วยงานมีความปลอดภัยมากยิ่งขึ้น โดยมีการกำหนดหน้าที่ความรับผิดชอบ วิธีการดำเนินการดำเนินการเพื่อรักษาความปลอดภัย และอุปกรณ์ที่ใช้ เวลาที่ปฏิบัติหน้าที่ให้เหมาะสม รวมทั้งมีวิธีการสังเกต รายงาน และการจัดการเหตุผิดปกติที่มีประสิทธิภาพ</li> </ul>
๑.๑๐	การควบคุมการเข้า-ออกของพนักงาน	<ul style="list-style-type: none"> <li>- มีการทำบัตรประจำตัวพนักงาน หรือระบบอื่นๆ ที่ใช้ระบุตัวพนักงานเพื่อควบคุมการเข้า-ออก เช่น บัตรพนักงานที่ติดรูปถ่ายสี หรือระบบพิมพ์ลายนิ้วมือ เป็นต้น</li> <li>- กำหนดให้พนักงานเข้า-ออกได้เฉพาะพื้นที่ที่ตนจำเป็นต้องเข้าไปปฏิบัติหน้าที่เท่านั้น อาจกำหนดสีของเครื่องแบบพนักงานบางตำแหน่งให้แตกต่างกัน เพื่อประโยชน์ในการระบุตำแหน่งหน้าที่ เป็นต้น และมีการกำหนดอายุบัตรประจำตัว เพื่อใช้ในการระบุตัวตนของเจ้าของบัตรที่ชัดเจน</li> </ul>



๑.๑๑	การควบคุมการ เข้า-ออกสำหรับ บุคคลภายนอก	- มีระบบควบคุมและตรวจสอบบุคคลภายนอกที่เข้ามาในองค์กร เช่น การยื่นบัตร ประจำตัว และลงทะเบียนที่จุดเข้า-ออก และต้องติดบัตรชั่วคราวในจุดที่สามารถ สังเกตได้โดยง่ายตลอดเวลาที่อยู่ในองค์กร นอกจากนี้ มีการระบุพนักงานที่ทำหน้าที่ พาบุคคลภายนอกเข้าไปในหน่วยงาน และเข้าได้เฉพาะพื้นที่ที่อนุญาตเท่านั้น
๑.๑๒	การป้องกันบุคคลที่ ไม่ได้รับอนุญาตเข้า ไปในหน่วยงาน	- ระบุรายละเอียดวิธีการสังเกต ป้องกัน และดำเนินการเมื่อพบบุคคลไม่ได้รับอนุญาต เข้าในพื้นที่ รวมถึงวิธีปฏิบัติในการรายงานเหตุการณ์เมื่อพบบุคคลไม่ได้รับอนุญาตเข้า ในพื้นที่ ระบุฝ่ายรับผิดชอบ และช่องทางการแจ้งเหตุการณ์ให้ชัดเจน และมีประสิทธิภาพ - กำหนดรูปแบบการเผยแพร่ประชาสัมพันธ์วิธีการดังกล่าวให้พนักงานทุกคนรับทราบ

## ๒. ความปลอดภัยในส่วนที่เกี่ยวข้องกับพนักงาน (Personnel Security)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการต้องมีขั้นตอนการปฏิบัติเกี่ยวกับการคัดเลือกพนักงาน และตรวจสอบพนักงานที่ทำงานอยู่อย่างสม่ำเสมอ มีการให้ความรู้ และอบรมกับพนักงานในเรื่องนโยบายการรักษาความปลอดภัยขององค์กร การปฏิบัติงานให้เกิดความปลอดภัย การตระหนักรู้ถึงผลกระทบหากไม่ปฏิบัติตาม รวมถึงความเข้าใจว่าจะดำเนินการอย่างไร หากเกิดความผิดพลาดขึ้น

### ๒.๑ การตรวจสอบข้อมูลพนักงานก่อนการจ้างงาน

มีมาตรการในการตรวจสอบข้อมูลในใบสมัครของผู้สมัครงาน อาทิ ประวัติการจ้างงานย้อนหลัง ข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุล บุคคลอ้างอิง ข้อมูลทางการศึกษา ข้อมูลทางอาชญากรรมก่อนการรับบุคคลเข้าทำงาน เพื่อให้แน่ใจว่าผู้สมัครงานมีประวัติที่ถูกต้อง ไม่เคยกระทำความผิดในส่วนที่เกี่ยวข้องกับการก่อการร้าย การกระทำความผิดทางศุลกากร หรือการกระทำความผิดทางอาญาอื่นๆ โดยเฉพาะอย่างยิ่งในตำแหน่งที่สำคัญหรือเกี่ยวข้องกับห่วงโซ่อุปทาน เช่น บัญชี จัดซื้อ คลังสินค้า พนักงานขับรถ เทคโนโลยีสารสนเทศ และอื่นๆ

การตรวจสอบและสืบสวนภูมิหลังควรจะดำเนินการตามความเหมาะสม ภายใต้กฎหมายของประเทศ ทั้งนี้ หน่วยงานอาจตรวจสอบและสืบสวนภูมิหลังของบุคคลที่จะรับเข้าทำงานโดยละเอียด หากเป็นตำแหน่งที่สำคัญหรือตำแหน่งที่มีความเสี่ยงจะเกิดความเสียหายต่อองค์กรได้สูง

### ๒.๒ การตรวจสอบภูมิหลังของพนักงานปัจจุบัน

มีขั้นตอนปฏิบัติในการดำเนินการตรวจสอบภูมิหลังของพนักงานปัจจุบัน ทั้งนี้ ขึ้นอยู่กับเหตุผลความจำเป็นตามตำแหน่งของพนักงานนั้น

องค์กรควรกำหนดให้มีการปรับปรุงข้อมูลของพนักงานแต่ละรายให้เป็นปัจจุบัน โดยเฉพาะอย่างยิ่งชื่อ-นามสกุลของพนักงาน ที่อยู่ปัจจุบัน สถานภาพ ตำแหน่งงาน โรคประจำตัว และอื่นๆ รวมถึงการเอาใจใส่ดูแลพนักงานที่มีพฤติกรรมผิดปกติ โดยคำนึงถึงสถานภาพทางสังคมหรือเศรษฐกิจที่เปลี่ยนแปลง

### ๒.๓ วิธีปฏิบัติของการสืบสภาพการเป็นพนักงาน

มีขั้นตอนปฏิบัติในการดำเนินการสำหรับพนักงานที่ลาออกจากองค์กร รวมถึงการคืนทรัพย์สินของบริษัทฯ เพื่อให้แน่ใจว่าพนักงานที่ลาออกจากองค์กรไปแล้วไม่ได้นำสินทรัพย์ใดใดขององค์กรออกไปเพื่อหาประโยชน์ส่วนตัว

มีวิธีปฏิบัติอย่างรวดเร็ว ในการยกเลิกบัตรพนักงานสำหรับการผ่านเข้า-ออก หรือการเข้าถึงระบบต่างๆ ของหน่วยงาน สำหรับพนักงานที่มีได้ทำงานกับหน่วยงานแล้ว

มีข้อกำหนดที่ชัดเจนในการระบุเงื่อนไขที่ทำให้สืบสภาพการเป็นพนักงาน และแนวทางการดำเนินการในกรณีดังกล่าว

### ๒.๔ การให้การศึกษา และการฝึกอบรม

มีการจัดให้ความรู้ และฝึกอบรมพนักงานในเรื่องการรักษาความปลอดภัย เกี่ยวกับ

(๑) นโยบายการรักษาความปลอดภัยขององค์กร

(๒) กระบวนการในส่วนที่เกี่ยวข้องกับสินค้า และเทคโนโลยีสารสนเทศ

(๓) การป้องกันมิให้ผู้ไม่ได้รับอนุญาตเข้า-ออกในหน่วยงาน และป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าพื้นที่ที่ไม่เกี่ยวข้อง และเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตได้

/(๔) การสังเกต...

- (๔) การสังเกตสิ่งผิดปกติที่จะมีผลต่อการรักษาความปลอดภัย รวมถึงวิธีการรายงาน และแจ้งเหตุผิดปกติ
- (๕) การสังเกตสินค้า บุคคล พฤติกรรมที่น่าสงสัย และการรายงานให้หน่วยงานทราบ ตามช่องทางหรือขั้นตอนปฏิบัติที่องค์กรกำหนดขึ้นและเผยแพร่ให้ทราบโดยทั่วกัน และมีการกำหนดผู้รับผิดชอบอย่างชัดเจน
- (๖) โครงการผู้ประกอบการระดับมาตรฐานเออีโอ

ความรู้ดังกล่าวควรถูกจัดอบรมให้แก่พนักงานใหม่ที่เข้าทำงาน รวมถึงการจัดอบรมให้กับพนักงานที่ได้เคยรับฟังหลักสูตรนี้มาระยะเวลาหนึ่งแล้ว (Refresher Course) เพื่อให้พนักงานเหล่านั้นได้รับทราบข่าวสาร และข้อมูลเกี่ยวกับความปลอดภัยที่เป็นปัจจุบัน

### ๓. ความปลอดภัยในส่วนของพันธมิตรทางธุรกิจ (Trading Partner Security)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการต้องประสานงานกับพันธมิตรทางธุรกิจที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เพื่อกระตุ้นให้ธุรกิจเหล่านั้นเพิ่มมาตรการรักษาความปลอดภัยโดยสมัครใจ

คำว่า “พันธมิตรทางธุรกิจ” หมายถึง ตัวบุคคล หรือองค์กรที่มีการดำเนินกิจกรรมร่วมกัน ซึ่งอาจมีกิจกรรมร่วมกันทั้งทางตรง และ/หรือทางอ้อม

#### ๓.๑ การคัดเลือกพันธมิตรทางธุรกิจ

มีการกำหนดขั้นตอนปฏิบัติ ในการคัดเลือกพันธมิตรทางธุรกิจที่เหมาะสม ระบุฝ่ายรับผิดชอบให้ชัดเจน รวมถึงการสัมภาษณ์ การตรวจสอบข้อมูลของพันธมิตร ที่ได้จากพันธมิตรเอง และจากแหล่งข้อมูลอ้างอิงภายนอก ตัวอย่างเช่น ศูนย์บริการข้อมูลทางธุรกิจ ธนาคาร และแหล่งอ้างอิงจากหน่วยงานอื่นๆ เป็นต้น

มีการกำหนดหลักเกณฑ์ในการคัดเลือกพันธมิตรทางธุรกิจที่มีความเหมาะสม ครอบคลุม ชัดเจน สำหรับพันธมิตรแต่ละประเภท หากมีการให้คะแนน ให้ระบุคำอธิบายในการให้คะแนน และแนวทางปฏิบัติสำหรับคะแนนแต่ละเกณฑ์อย่างชัดเจน

สำหรับองค์กรที่มีตัวแทนจัดซื้อในต่างประเทศ ควรมีการจัดทำคู่มือ (Vendor Compliance Manual) ให้กับตัวแทน เพื่อใช้ในการคัดเลือกพันธมิตรให้มีมาตรฐานการรักษาความปลอดภัย

#### ๓.๒ การทำสัญญา หรือการแสดงเจตนารมณ์ในการรักษาความปลอดภัย

มีข้อตกลงที่ทำกับพันธมิตรธุรกิจ หรือกำหนดให้พันธมิตรธุรกิจแสดงเจตนารมณ์ในการรักษาความปลอดภัย เป็นลายลักษณ์อักษร ซึ่งในข้อตกลงหรือเจตนารมณ์นั้น จะต้องมีคำอธิบายเกี่ยวกับสินค้า และ/หรือบริการอย่างชัดเจน แนวทางการรักษาความปลอดภัยของสินค้า และ/หรือบริการนั้น ผู้รับผิดชอบ การรักษาความลับ ขอบเขตการรับผิดชอบ หากมีการผิดข้อตกลง อายุของสัญญา และการยกเลิกสัญญา เป็นต้น

ข้อตกลงหรือเจตนารมณ์นั้น จะต้องมีบททบทวนอย่างสม่ำเสมอ หรือในกรณีมีเหตุจำเป็น เพื่อให้เหมาะสม และเป็นปัจจุบัน

#### ๓.๓ การรับรองความปลอดภัย

ในกรณีที่องค์กรหรือพันธมิตรธุรกิจได้เข้าร่วมโครงการเสริมสร้างความปลอดภัยกับองค์กรในต่างประเทศแล้ว จะต้องแสดงเอกสารหลักฐานที่ออกให้โดยศุลกากรต่างประเทศ หรือจากโครงการเสริมสร้างความปลอดภัยอื่นๆ ไว้ด้วย

#### ๓.๔ ทะเบียนพันธมิตร

มีการขึ้นทะเบียนพันธมิตรที่ผ่านกระบวนการคัดเลือก และผ่านหลักเกณฑ์การคัดเลือกตามที่กำหนด เพื่อให้มั่นใจว่าพันธมิตรที่องค์กรประสานงานด้วยมีความเหมาะสมต่อการดำเนินกิจกรรมร่วมกัน มีประสิทธิภาพ สามารถส่งมอบสินค้า และ/หรือบริการได้ตรงตามความต้องการขององค์กร

กำหนดขั้นตอนปฏิบัติการขึ้นทะเบียนพันธมิตร เงื่อนไขการขึ้นทะเบียน การตัดออกจากทะเบียนพันธมิตร ระบุฝ่ายรับผิดชอบ และรอบระยะเวลาในการแก้ไขทะเบียนพันธมิตรให้ชัดเจน

/๓.๕ การทบทวน...

## ๓.๕ การทบทวน

มีการกำหนดแนวทาง หลักเกณฑ์ รอบระยะเวลา และฝ่ายรับผิดชอบในการทบทวนมาตรฐานการปฏิบัติงาน และมาตรฐานทางด้านความปลอดภัยของพันธมิตรธุรกิจ เพื่อให้เกิดความมั่นใจว่าพันธมิตรธุรกิจได้ดำเนินการตามข้อตกลงหรือเจตนารมณ์ที่จัดทำขึ้น

มีการกำหนดแนวทางปฏิบัติเมื่อพบว่าพันธมิตรไม่ปฏิบัติตามข้อตกลง เช่น การแจ้ง การหารือ การดำเนินการแก้ไขปัญหา และการยกเลิกการดำเนินการร่วมกับพันธมิตรที่ไม่ปฏิบัติตามข้อตกลง

#### ๔. ความปลอดภัยในเรื่องสินค้า (Cargo Security)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการต้องจัดทำวิธีปฏิบัติ และกำหนดผู้รับผิดชอบแต่ละขั้นตอนเป็นลายลักษณ์อักษร ดังนี้

##### ๔.๑ การดำเนินการตรวจสอบเอกสารและสินค้า

มีการกำหนดมาตรการในการออกเอกสารที่เกี่ยวกับสินค้าหรือบริการ การรักษาความปลอดภัยของเอกสาร และการตรวจสอบความผิดปกติต่างๆ ตั้งแต่ต้นทางจนถึงปลายทาง เพื่อให้มั่นใจว่ารายละเอียดในเอกสารมีความชัดเจน สมบูรณ์ ถูกต้อง เพื่อป้องกันการสับเปลี่ยน สูญหาย หรือเปลี่ยนแปลงข้อมูล

มีมาตรการในการตรวจสอบสินค้าให้ตรงกับเอกสาร เช่น บัญชีสินค้า (Manifest) บัญชีบรรจุหีบห่อ (Packing List) ใบตราส่งสินค้า (Bill of Lading) ใบสั่งซื้อและใบจัดส่งสินค้า (Purchase/Delivery Order) ใบอนุญาต พิกัดศุลกากร และภาษี เป็นต้น รวมถึงการกำหนดรายละเอียดบุคคลที่สามที่เกี่ยวข้องในกิจกรรมนี้ เช่น ระบุผู้ดำเนินการพิธีการศุลกากร ผู้ตรวจสอบเอกสาร ผู้ขับรถและทะเบียนรถ และอื่นๆ ที่ทำหน้าที่รับหรือจัดส่งสินค้าให้ชัดเจน ก่อนสินค้าจะถูกรับมอบหรือจัดส่งไป

มีการกำหนดวิธีปฏิบัติเมื่อพบความผิดปกติเกี่ยวกับสินค้า และระบุฝ่ายรับผิดชอบ

##### ๔.๒ การติดตามและตรวจสอบสถานะสินค้า

มีการกำหนดวิธีการ และรูปแบบในการติดตามและตรวจสอบสถานะของสินค้า ตั้งแต่เป็นวัตถุดิบจนเป็นสินค้าสำเร็จรูป ระบุฝ่ายรับผิดชอบอย่างชัดเจนในแต่ละขั้นตอน เพื่อให้สามารถตรวจสอบย้อนกลับได้อย่างรวดเร็ว และถูกต้อง

หากมีการใช้โปรแกรมในการติดตามและตรวจสอบสถานะสินค้า จะต้องเป็นโปรแกรมที่มีมาตรฐาน มีความแม่นยำ มีเสถียรภาพ มีการจัดเก็บข้อมูลอย่างเป็นระเบียบ ง่ายต่อการสืบค้น

หากมีบุคคลที่สามเข้ามาเกี่ยวข้องในกระบวนการนี้ ให้ระบุผู้รับผิดชอบนั้นๆ ในขั้นตอนนั้นๆ ให้ชัดเจน

##### ๔.๓ การยืนยันความถูกต้องของข้อมูลและเอกสาร

มีการกำหนดวิธีปฏิบัติเกี่ยวกับการลงลายมือชื่อ และการประทับตราหน่วยงานสำหรับขั้นตอนที่สำคัญในการส่งมอบแต่ละจุด ตัวอย่างเช่น ขั้นตอนทางเอกสาร การจ่ายและทำลายตราผนึก การนับจำนวนสินค้าที่บรรจุทุก การตรวจสอบการบรรจุทุกสินค้า การจัดส่งสินค้า และนับจำนวนสินค้าที่ไม่ได้ขนขึ้นยานพาหนะ เอกสารต่างๆ ที่เกี่ยวข้อง กับเรื่องดังกล่าวควรมีการลงลายมือชื่อโดยบุคคลที่ทำหน้าที่รับ และจัดส่งสินค้า

ในกรณีเป็นระบบอิเล็กทรอนิกส์ ให้กำหนดวิธีปฏิบัติในการยืนยันความถูกต้องของข้อมูลในแต่ละขั้นตอนที่สำคัญ และระบุผู้รับผิดชอบแต่ละขั้นตอนให้ชัดเจน

##### ๔.๔ การตรวจสอบตู้คอนเทนเนอร์

มีมาตรการในการตรวจสอบสภาพของตู้คอนเทนเนอร์ให้สามารถใช้งานได้เหมาะสมกับประเภทสินค้า โดยอย่างน้อย ต้องมีการตรวจสอบจำนวน ๗ จุด ได้แก่

(๑) ผนังตู้ด้านหน้า

(๒) ผนังตู้ข้างซ้าย

(๓) ผนังตู้ข้างขวา

- (๔) พื้นตู้
- (๕) เพดานตู้
- (๖) ประตูตู้ทั้งด้านนอกและด้านใน
- (๗) สภาพภายนอกและด้านล่างตู้

มีการกำหนดฝ่ายรับผิดชอบ และเอกสารที่ใช้ในการตรวจสอบสภาพที่ชัดเจน

#### ๔.๕ ตราประทับและเครื่องหมาย

มาตรการควบคุมการใช้ตราประทับ และเครื่องหมายที่แนะนำให้ปฏิบัติมีดังนี้

- (๑) เป็นตราประทับและเครื่องหมายที่ออกให้โดยพนักงานที่ได้รับมอบหมายเท่านั้น
- (๒) มีเอกสารบันทึกรายละเอียดตราประทับและเครื่องหมายที่จำหน่ายออกไป โดยระบุบุคคลที่นำไปใช้ และสถานที่นำไปใช้
- (๓) ตราประทับและเครื่องหมายไม่ควรออกโดยเรียงตามลำดับหมายเลข (Strict Numbering Sequence) เพื่อป้องกันมิให้มีการคาดเดาหมายเลขได้

ตราประทับที่ติดตู้คอนเทนเนอร์ ควรใช้ตามมาตรฐาน PAS ISO ๑๗๗๑๒ หรือมาตรฐานอื่นที่สูงกว่า

#### ๔.๖ การเก็บตู้คอนเทนเนอร์และสินค้า

ตู้คอนเทนเนอร์และสินค้าจะต้องเก็บไว้ในบริเวณที่ปลอดภัย เพื่อป้องกันการบุกรุกหรือบุคคล เข้าไป โดยไม่ได้รับอนุญาต

มีการกำหนดวิธีปฏิบัติในการควบคุมพื้นที่เกี่ยวกับสินค้า และรายงานเหตุผิดปกติที่เกิดขึ้นในพื้นที่ดังกล่าว ให้หน่วยงานที่รับผิดชอบรับทราบ เพื่อป้องกันการบุกรุกพื้นที่โดยไม่ได้รับอนุญาต และไม่ให้เกิดเหตุผิดปกติในพื้นที่ดังกล่าว หรือหากเกิดเหตุผิดปกติก็สามารถควบคุมเหตุการณ์ และดำเนินการเพื่อแก้ไขปัญหาได้อย่างรวดเร็ว

มีการตรวจสอบหมายเลขทะเบียนยานพาหนะที่ทำการรับ-ส่งสินค้าให้ตรงตามที่ได้กำหนดไว้ และระบุผู้รับผิดชอบ

มีการกำหนดขั้นตอนการนำสินค้าเข้าสู่ตู้คอนเทนเนอร์ หรือรถบรรทุกสินค้าที่เหมาะสม ชัดเจน ระบุฝ่ายรับผิดชอบ และระบุพื้นที่อย่างชัดเจน

#### ๔.๗ การควบคุมสินค้าคงเหลือ

มาตรการควบคุมสินค้าคงเหลือที่แนะนำให้ปฏิบัติมีดังนี้

- (๑) การกำหนดขั้นตอนการควบคุมสินค้าคงเหลือ รอบระยะเวลา และระบุฝ่ายรับผิดชอบ
- (๒) การสำรวจสินค้าคงเหลือทั้งรับเข้าและนำออก มีพนักงานประจำคลังสินค้าที่ได้รับการฝึกฝน เพื่อการตรวจสอบสินค้าอย่างมีประสิทธิภาพ
- (๓) การให้พนักงานรายงานการตรวจสอบและการตรวจทานโดยละเอียดที่ละขั้นตอน
- (๔) การตรวจสอบสินค้าให้บ่อยขึ้นในช่วงที่มีการรับสินค้าเข้าคลังมากๆ หรือเมื่อได้รับรายงานความผิดปกติ

/๕. ความปลอดภัย...

## ๕. ความปลอดภัยสำหรับยานพาหนะขนส่งสินค้า (Conveyance Security)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการต้องมีมาตรการในการตรวจสอบยานพาหนะขนส่งสินค้าอย่างสม่ำเสมอ เพื่อให้ยานพาหนะมีสภาพที่ดี มีมาตรฐาน พร้อมใช้งาน โดยเฉพาะบริเวณที่อาจใช้เป็นพื้นที่ในการซุกซ่อนสิ่งผิดกฎหมาย เช่น บริเวณที่เก็บของและช่องว่างต่างๆ ทั้งภายในและภายนอก และจัดหาพื้นที่ปลอดภัยในการจอดยานพาหนะเพื่อป้องกันการบุกรุก/หรือเข้าไปโดยไม่ได้รับอนุญาต

ในกรณีที่ใช้บริการผู้ให้บริการขนส่ง ต้องมีข้อกำหนดด้านความปลอดภัยที่มีมาตรฐานตามโครงการผู้ประกอบการระดับมาตรฐานเออีโอในการจัดหาผู้ให้บริการ อย่างชัดเจน และเป็นลายลักษณ์อักษร

การติดตามตรวจสอบยานพาหนะ จะต้องมีมาตรการติดตามตรวจสอบยานพาหนะที่ใช้ในการเคลื่อนย้ายสินค้าทั้งภายในและภายนอกองค์กร มาตรการรักษาความปลอดภัยที่ควรนำมาใช้ มีดังนี้

(๑) ระบบอิเล็กทรอนิกส์ ตัวอย่างเช่น การใช้เครื่องรับส่งเรดาร์ (Transponders), Smart Cards, กล้องวิดีโอ กล้องถ่ายภาพดิจิทัล โทรศัพท์เคลื่อนที่ วิทยุสื่อสาร และระบบบอกพิกัดโดยใช้สัญญาณดาวเทียม GPS (Global Positioning Systems) หรือ

(๒) สมุดบันทึกรายงานการเคลื่อนย้ายสินค้า (Activity Log) หรือวิธีการอื่นๆ

- สมุดคู่มือสำหรับผู้ควบคุมยานพาหนะ

ผู้ควบคุมยานพาหนะควรได้รับการฝึกฝนทักษะในการรักษาความปลอดภัยให้กับยานพาหนะและสินค้าที่บรรทุกอย่างสม่ำเสมอ พร้อมทั้งการรายงานเหตุการณ์ที่น่าสงสัยกลับมายังองค์กร สมุดคู่มือฯ มีรายละเอียด ดังนี้

(๑) ระเบียบปฏิบัติของผู้ควบคุมยานพาหนะ

(๒) การตรวจสอบสภาพยานพาหนะก่อนการใช้งาน และการตรวจความบกพร่องของเครื่องยนต์

(๓) การใช้ความเร็วในการขับรถ การหยุดรถ การจอดรถ สัญญาณจราจร เครื่องหมายจราจร

(๔) รายละเอียดเส้นทางสำหรับรับ-ส่งสินค้า

(๕) การรักษาความลับในเรื่องข้อมูลสินค้าที่บรรทุก เส้นทาง และจุดหมายปลายทาง

(๖) ข้อกำหนดเกี่ยวกับกฎจราจร สถานที่จอดรถ สถานที่เติมเชื้อเพลิง สถานที่พักรถ และการพักรถนอกเหนือจากสถานที่กำหนด

(๗) ขั้นตอนปฏิบัติในการรายงานเหตุผิดปกติ อุบัติเหตุ เหตุสุดวิสัย เป็นลายลักษณ์อักษร

(๘) ขั้นตอนปฏิบัติในการรายงานเหตุผิดปกติกับสินค้า ตัวล็อกหรือตราประทับ เป็นลายลักษณ์อักษร

(๙) การติดตั้ง และทดสอบระบบสัญญาณเตือนภัยและอุปกรณ์ติดตาม (ถ้ามี)

- การฝึกอบรมผู้ควบคุมยานพาหนะ

ผู้ควบคุมยานพาหนะควรได้รับการอบรมในทักษะที่จำเป็น เช่น การขับขี่ปลอดภัย การตรวจสอบสภาพยานพาหนะ การรักษาความลับของสินค้า เส้นทางขนส่งสินค้า การสังเกตและรายงานเหตุผิดปกติ และทักษะอื่นๆ ที่จำเป็นสำหรับขับขี่ยานพาหนะ นอกจากนี้ ควรมีการตรวจสอบใบอนุญาตของผู้ขับรถ และมาตรฐานต่างๆ ที่เกี่ยวข้อง

/๖. ความปลอดภัย...



## ๖. ความปลอดภัยทางด้านข้อมูลเทคโนโลยีสารสนเทศและเอกสาร (Information Exchange, Access, Confidentiality and Document)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการต้องมีมาตรการรักษาความปลอดภัยของข้อมูล (ทั้งในลักษณะ ที่เป็นเอกสารและแบบอิเล็กทรอนิกส์) เพื่อป้องกันมิให้ข้อมูลถูกนำไปใช้ในทางที่ผิดหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

### - นโยบายความปลอดภัยของข้อมูล

กำหนดนโยบายที่ก่อให้เกิดความปลอดภัยของข้อมูล ซึ่งนโยบายควรประกอบไปด้วย ข้อกำหนดในการใช้งานระบบคอมพิวเตอร์ และระบบเครือข่าย สำหรับผู้ใช้งานและผู้ดูแลระบบ, ระบบสำรองข้อมูลและทดสอบการกู้ข้อมูล, ระบบการรักษาความปลอดภัย, ระบบป้องกันการเข้าถึงข้อมูล เช่น ระบบการยืนยันตัวตน อันได้แก่ เงื่อนไขในการตั้งรหัสผ่าน การเปลี่ยนรหัสผ่าน การสแกนลายนิ้วมือ ใบหน้า และ/หรือดวงตา, ระบบตรวจสอบการทำงานให้มีประสิทธิภาพ, ระบบป้องกันและแก้ไขการบุกรุก เช่น ANTI-VIRUS, FIREWALL, IDS และ IPS, การจัดทำแผนฉุกเฉินสำหรับระบบคอมพิวเตอร์และเครือข่าย, การประเมินความเสี่ยง และการกำหนดหน่วยงานรับผิดชอบอย่างชัดเจน และเป็นลายลักษณ์อักษร

มีการกำหนดแผนงานหรือแนวทางปฏิบัติในการบำรุงรักษาระบบฯ ให้พร้อมใช้งานและทันสมัย กำหนดฝ่ายรับผิดชอบ ระยะเวลา และความถี่ในการดำเนินการอย่างชัดเจน เหมาะสมกับองค์กร

มีการกำหนดแนวทางป้องกันการใช้ซอร์ฟแวร์ละเมิดลิขสิทธิ์

มีการกำหนดให้มีการทบทวนนโยบายความปลอดภัยและแนวทางปฏิบัติงานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มีความทันสมัยและมีประสิทธิภาพเหมาะสมกับองค์กร

### - การรักษาความปลอดภัย และการควบคุมการเข้าถึงข้อมูล

ใช้ระบบรักษาความปลอดภัยที่มีมาตรฐาน และมีประสิทธิภาพเหมาะสมกับองค์กร มีการกำหนดผู้มีอำนาจในการกำหนดสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน จัดทำแนวทางปฏิบัติสำหรับการขอเข้าถึงข้อมูลผู้ใช้งาน กำหนดแนวทางการปรับปรุงรายชื่อ หรือสิทธิผู้ใช้งานระบบ

มีข้อกำหนดเพื่อควบคุมการเข้าถึงข้อมูล เช่น มีการใช้ระบบการยืนยันตัวตนและพิสูจน์ตัวตนที่มีมาตรฐาน และมีประสิทธิภาพเหมาะสมกับองค์กร เช่น การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) การสแกนลายนิ้วมือ แสแกนม่านตา แสแกนใบหน้า จัดทำแนวทางปฏิบัติสำหรับการใช้ระบบยืนยันตัวตนและพิสูจน์ตัวตน เช่น การกำหนดรูปแบบของรหัสผ่าน เช่น ห้ามใช้รหัสซ้ำ และรหัสต้องมีความซับซ้อนคาดเดาได้ยาก มีการกำหนดให้มีการหมดอายุของรหัสผ่านทุกๆ ๙๐ วันเป็นอย่างน้อย การป้องกันรหัสผ่านไม่ให้บุคคลอื่นทราบ ตั้งระยะเวลาในการ log out หน้าจอ เช่น ตั้งค่าให้ log out หน้าจอทุกๆ ๑๕ นาที เมื่อไม่มีการเคลื่อนไหว เป็นต้น

มีแนวทางปฏิบัติในการกำหนดชั้นความลับของข้อมูล ตามระดับความสำคัญ เช่น ระบุผู้มีอำนาจในการกำหนดสิทธิการเข้าถึงข้อมูลต่างๆ กำหนดวิธีป้องกันข้อมูลแต่ละชนิดให้ชัดเจน และกำหนดระดับชั้นผู้มีอำนาจเข้าถึงข้อมูล และกำหนดแนวทางปฏิบัติในการเข้าถึงข้อมูล ทั้งนี้ ควรจัดทำกรทบทวนรายชื่อผู้ได้รับอนุญาตอย่างสม่ำเสมอ เพื่อให้เกิดความมั่นใจว่าบุคคลที่ได้รับอนุญาตเหล่านั้นจะไม่นำข้อมูลไปใช้ในทางที่ผิด

### - การสำรองข้อมูล (Data Backup) และการกู้ข้อมูล (Recovery Test)

กำหนดแนวทางปฏิบัติ รูปแบบ และความถี่สำหรับการสำรองข้อมูล รวมถึงสถานที่จัดเก็บต้องมีความปลอดภัย มีมาตรฐาน กำหนดแนวทางปฏิบัติสำหรับการทดสอบการกู้ข้อมูลที่ชัดเจน มีมาตรฐาน เพื่อให้สามารถดึงข้อมูลได้อย่างรวดเร็วหากเกิดเหตุผิดปกติ และมีการกำหนดเวลาสำรองข้อมูล อย่างน้อยสัปดาห์ละครั้ง

/การป้องกัน...

- การป้องกันและแก้ไขข้อมูลเมื่อมีการบุกรุก

จัดทำระบบเพื่อตรวจสอบ ป้องกัน และแก้ไขเมื่อมีการบุกรุกข้อมูลที่มีมาตรฐาน มีประสิทธิภาพ และเหมาะสมกับองค์กร กำหนดแนวทางปฏิบัติในการตรวจสอบ ป้องกันและแก้ไขเมื่อเกิดการบุกรุก กำหนดกรอบระยะเวลาในการตรวจสอบระบบให้พร้อมใช้งานได้อย่างมีประสิทธิภาพ

- การดูแลเอกสารขององค์กร

จัดทำแนวทางปฏิบัติในการดูแลเอกสารแต่ละชั้นตอนให้ชัดเจน เป็นระบบ และมีระเบียบง่ายต่อการสืบค้น ตั้งแต่การจัดทำ จัดเก็บ แก้ไขเปลี่ยนแปลง และทำลายเอกสาร ทั้งที่เป็นแบบกระดาษและอิเล็กทรอนิกส์ มีการกำหนดผู้ดูแลรับผิดชอบเอกสารอย่างชัดเจน มีการกำหนดสถานที่จัดเก็บเอกสาร และกำหนดระยะเวลาในการจัดเก็บเอกสาร แต่ละชนิดอย่างชัดเจน

- การฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

จัดฝึกอบรมให้ความรู้เกี่ยวกับนโยบายฯ และแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศ เพื่อเสริมสร้างความตระหนักรู้ และการป้องกันข้อมูล

## ๗. ข้อมูลการจัดการเหตุวิกฤต และระบบการสืบสวนเหตุการณ์ (Crisis Management and Incident Investigation)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการต้องมีมาตรการบริหารจัดการเมื่อเกิดวิกฤตการณ์ความรุนแรงหรือเหตุไม่ปลอดภัย และแนวทางดำเนินการแก้ไข ทั้งนี้ เพื่อลดผลกระทบในด้านความสูญเสีย หรือความไม่ปลอดภัยที่เกิดขึ้น วิธีปฏิบัติควรรวมถึงการวางแผนล่วงหน้า และการกำหนดขั้นตอนการปฏิบัติเมื่อมีเหตุการณ์ที่ไม่ปกติเกิดขึ้น รวมถึงมีการซ้อมแผนอย่างสม่ำเสมอ เพื่อให้แผนดังกล่าวมีความทันสมัย และเหมาะสมกับองค์กร

### - แผนฉุกเฉิน หรือแผนสำรอง

มีการจัดทำแผนฉุกเฉิน หรือแผนสำรองที่เหมาะสมกับองค์กร เป็นลายลักษณ์อักษร โดยมีการกำหนดแนวทางปฏิบัติของแผนแต่ละแผนอย่างชัดเจน ระบุผู้รับผิดชอบในแต่ละขั้นตอนให้ละเอียด จัดอบรม และซักซ้อมแผนดังกล่าวให้กับพนักงาน นอกจากนี้ ควรมีการกำหนดให้ทบทวนแผนอย่างน้อยปีละครั้ง เพื่อให้ทันสมัยสอดคล้องกับการดำเนินงานและการเปลี่ยนแปลงขององค์กร

### - แผนความต่อเนื่องทางธุรกิจ : Business Continuity Plan (BCP)

จัดทำแนวทางปฏิบัติสำหรับแผนความต่อเนื่องทางธุรกิจ เพื่อสร้างระบบการทำงานสำหรับป้องกันและฟื้นฟู ภายหลังเกิดวิกฤตการณ์ที่ส่งผลกระทบต่อธุรกิจ โดยมีการกำหนดขั้นตอนการทำแผนฯ การระงับฝ่ายรับผิดชอบ การสำรวจ และทดสอบแผน อย่างเป็นขั้นตอน ชัดเจน และเป็นลายลักษณ์อักษร

### - การจัดการเหตุการณ์ผิดปกติ

กำหนดแนวทางปฏิบัติเมื่อเกิดเหตุการณ์ผิดปกติ มีการระงับฝ่ายรับผิดชอบอย่างชัดเจน เป็นขั้นเป็นตอน และเป็นลายลักษณ์อักษร โดยเริ่มตั้งแต่การรายงานเหตุการณ์ให้ครบถ้วน การกำหนดช่องทางและรูปแบบการแจ้งเหตุฯ การตรวจสอบและวิเคราะห์สาเหตุการเกิด แนวทางการแก้ไขและป้องกันเหตุการณ์ และการเผยแพร่ประชาสัมพันธ์ และการฝึกอบรมเพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำอีก รวมไปถึงการจัดเก็บรายงานอย่างเป็นระบบ ง่ายต่อการสืบค้น และมีการจัดทำสถิติ เพื่อติดตาม และระบุแนวโน้มหรือรูปแบบของความเสี่ยงที่อาจเกิดขึ้นในอนาคต นอกจากนี้ เหตุการณ์ผิดปกติที่เกิดขึ้นต้องได้รับการแก้ไข และมีการบันทึกรายงานเป็นลายลักษณ์อักษร พร้อมแจ้งบุคคลที่เกี่ยวข้องรับทราบโดยทันที

## ๘. การประเมินความเสี่ยงและการวิเคราะห์ความเสี่ยง (Risk Assessment, Measurement, Analyses and Improvement)

ผู้ประกอบการที่ประสงค์จะเข้าร่วมโครงการควรจัดทำ การประเมินความเสี่ยงสำหรับกิจกรรมต่างๆ ที่เกิดขึ้น ในองค์กร เพื่อสังเกตและป้องกันเหตุการณ์ผิดปกติ ซึ่งทำให้องค์กรทราบถึงเหตุการณ์ที่ต้องพบเจอ การวิเคราะห์ จัดลำดับความสำคัญของเหตุการณ์ การจัดลำดับความรุนแรงของปัญหา โอกาสที่จะเกิดขึ้น ผลกระทบที่จะได้รับ จะทำให้องค์กรสามารถวางแผนหาแนวทางเพื่อรับมือกับปัญหาที่อาจจะเกิดขึ้น

### - การประเมินความเสี่ยง

ควรมีการกำหนดแนวทางปฏิบัติในการจัดการประเมินความเสี่ยงให้ชัดเจน ระบุฝ่ายรับผิดชอบ และ กำหนดความถี่ในการทบทวนความเสี่ยงใหม่ๆ ที่อาจเกิดขึ้น ให้เหมาะสมกับสภาพแวดล้อมและสภาพธุรกิจ ขั้นตอนในการจัดการประเมินความเสี่ยง เริ่มตั้งแต่การระบุเหตุการณ์ที่อาจเกิดปัญหาจากการดำเนินกิจกรรมต่างๆ ในองค์กร การกำหนดเกณฑ์มาตรฐานระดับความเสี่ยง การจัดลำดับความเสี่ยงตามระดับความรุนแรง โอกาสที่จะเกิด ระบุฝ่าย รับผิดชอบ การกำหนดแนวทางควบคุม เพื่อป้องกัน แก้ไข และลดความเสี่ยงนั้น การบันทึกและติดตามผลระดับความเสี่ยง หลังจากจัดการประเมินความเสี่ยง รวมไปถึงการตรวจสอบทบทวนประเด็นความเสี่ยงเพิ่มเติม เพื่อให้การประเมิน ความเสี่ยงมีความทันสมัย เหมาะสมกับปัจจุบัน และมีประสิทธิภาพ