

นโยบายและการรักษาความปลอดภัยห่วงโซ่อุปทาน (Supply Chain Security Policy)

บริษัทฯ จัดให้มีนโยบายรักษาความปลอดภัย ของห่วงโซ่อุปทาน (Supply Chain Security Policy) เพื่อนำไปปฏิบัติดูแลรักษา และปรับปรุงการจัดการเรื่องความปลอดภัย โดยมีเป้าหมายเพื่อรับประกันความปลอดภัยของ Supply Chain ป้องกันบุคลากร สินค้า โครงสร้างพื้นฐานและอุปกรณ์ รวมถึงการขนส่ง การป้องกันอุบัติเหตุ และการป้องกันผลกระทบที่มีแนวโน้มที่จะเกิดขึ้น ได้เผยแพร่ให้คู่ค้าทางธุรกิจตลอดจนพนักงานถือปฏิบัติ และมีการทบทวนมาตรการรักษาความปลอดภัย การประชุมทบทวนฯ อบรมพนักงานผู้ปฏิบัติงาน อย่างน้อยปีละ 1 ครั้ง

1. การประเมินความเสี่ยง (Risk Assessment)

บริษัทฯ ได้มีการจัดประเมินความเสี่ยงด้านความปลอดภัย และมีมาตรการป้องกัน โดยมีการทบทวนการประเมินความเสี่ยงเป็นประจำทุกปี หรือ ตามการเปลี่ยนแปลงของปัจจัยเสี่ยงที่เกิดขึ้น

2. แรงงานต้องห้าม (Prohibited Labor)

บริษัทฯ มีนโยบายไม่ให้จ้างแรงงานต้องห้ามโดยเด็ดขาด

3. คู่ค้าทางธุรกิจ (Business Partners)

บริษัทฯ มีการคัดกรองคู่ค้าทางธุรกิจ (ผู้ให้บริการ, ผู้รับเหมาช่วง, ผู้จัดการงาน, ผู้ให้บริการด้าน Logistic, บริษัทรถบรรทุก รวมไปถึงกรณีที่มีการใช้บริการคลังสินค้านอกสถานที่) เพื่อมั่นใจถึงมาตรการการรักษาความปลอดภัยที่เป็นไปตามเกณฑ์นโยบายการรักษาความปลอดภัยของห่วงโซ่อุปทาน (Supply Chain Security Policy)

☐ ในกรณีที่คู่ค้าทางธุรกิจที่เกี่ยวข้องกับสินค้าที่ส่งออกไปยังสหรัฐอเมริกา เข้าข่ายต้องปฏิบัติตามข้อกำหนดของ C-TPAT (ได้รับการรับรองให้เป็นบริษัทขนส่ง ผู้นำเข้า ทำสินค้า ด้านตรวจ นายหน้า ผู้รวบรวมสินค้าลงตู้ ฯลฯ) บริษัทฯ ต้องมีเอกสารรับรอง อาทิ ประกาศนียบัตรของ C-TPAT, หมายเลข SVI ฯลฯ ซึ่งสามารถยืนยันได้ว่าคู่ค้าทางธุรกิจเหล่านี้ผ่านการรับรองจากโครงการ C-TPAT

4. การรักษาความปลอดภัยส่วนบุคคล (Personnel Security)

บริษัทฯ จัดให้มีการตรวจสอบตัวตนของพนักงาน รวมไปถึงบุคคลภายนอกที่เข้ามาติดต่อโรงงาน และมีการตรวจสอบตำแหน่งที่มีความละเอียดอ่อน ได้แก่ พนักงานที่ทำงานโดยตรงกับสินค้า รวมไปถึงพนักงานที่เกี่ยวข้องกับการบรรจุสินค้าในตู้คอนเทนเนอร์ และ พนักงานควบคุมซีล

☐ การตรวจสอบก่อนการจ้างงาน (Pre-Employment Verification) เจ้าหน้าที่บุคคลต้องตรวจสอบข้อมูลในใบสมัครงาน อาทิ ประวัติการทำงาน และบุคคลอ้างอิงต้องได้รับการตรวจสอบยืนยันก่อนการจ้างงาน

☐ การตรวจสอบ/การสืบสวนประวัติความเป็นมา (Black ground Checks/Investigations)

☐ พนักงานใหม่ เจ้าหน้าที่แผนกบุคคลดำเนินการตรวจสอบบุคคลที่จะรับเป็นพนักงานว่ามีความสอดคล้องกับกฎข้อบังคับภายในประเทศหรือไม่ รวมทั้งตรวจสอบและสืบสวนประวัติความเป็นมา

☐ พนักงานปัจจุบัน เจ้าหน้าที่แผนกบุคคลดำเนินการตรวจสอบและสืบสวนประวัติความเป็นมาซ้ำทุก 2 ปี

MASTER

UNCONTROL

☐ ระเบียบปฏิบัติการเลิกจ้างพนักงาน (Personal Termination Procedures) กรณีที่มีการยุติการจ้างงานพนักงานแล้ว เจ้าหน้าที่แผนกบุคคลต้องขอคืนและยกเลิกบัตรประจำตัวพนักงาน และสิทธิการเข้าออกสถานประกอบการและระบบงานต่างๆ

5. การควบคุมการเข้า-ออก ทางกายภาพ (Physical Access Controls)

บริษัท มีการควบคุมสิทธิการเข้าถึง เพื่อป้องกันมิให้ผู้เข้าสู่สถานประกอบการโดยไม่ได้รับอนุญาต ซึ่งถือว่าเป็นการช่วยควบคุมดูแลพนักงานและผู้มาติดต่อ (Visitor) ตลอดจนคุ้มครองทรัพย์สินของบริษัท การควบคุมสิทธิการเข้าถึงนี้ ต้องครอบคลุมถึงการออกบัตรประจำตัวให้แก่ผู้มาติดต่อ (Visitor) และผู้จำหน่าย (Supplier) ทุกคน ณ จุดที่เป็นประตูทางเข้าด้วย

☐ พนักงาน บริษัทมีระบบการออกบัตรประจำตัวพนักงาน เพื่อการบ่งชี้ตัวตนบุคคลและควบคุมสิทธิการเข้า-ออก พนักงานต้องได้รับสิทธิการเข้า-ออก ในบริเวณที่มีการรักษาความปลอดภัย เฉพาะเมื่อพนักงานจำเป็นต้องมีการปฏิบัติหน้าที่ของตนในบริเวณดังกล่าวเท่านั้น และเจ้าหน้าที่แผนกบุคคลต้องมีระบบในการควบคุมการออกบัตรหรือยกเลิกบัตรประจำตัวพนักงาน รวมไปถึงบัตรผู้มาติดต่อ (Visitor) และผู้จำหน่าย (Supplier) ด้วย

☐ ผู้มาติดต่อ (Visitor) เมื่อผู้มาติดต่อมาถึง จะต้องแสดงบัตรประจำตัวที่มีรูปถ่าย เพื่อการเก็บบันทึกข้อมูล ผู้มาติดต่อทุกคนต้องมีเจ้าหน้าที่ของบริษัท ติดตาม และติดบัตรประจำตัวชั่วคราว (บัตร Visitor) ให้เห็นได้อย่างชัดเจนตลอดเวลา

☐ การส่งมอบ (Deliveries) รวมถึงพัสดุไปรษณีย์หรือจดหมาย เมื่อผู้ส่งมอบสินค้าหรือเจ้าหน้าที่ขนส่งพัสดุมายังด้านหน้าบริษัท ต้องแสดงบัตรประจำตัวผู้จำหน่าย และ/หรือบัตรประจำตัวที่มีรูปถ่ายตามความเหมาะสมให้กับเจ้าหน้าที่รักษาความปลอดภัยเพื่อเก็บบันทึกข้อมูล และเจ้าหน้าที่ของบริษัทต้องมีการตรวจสอบบรรจุภัณฑ์และพัสดุไปรษณีย์หรือจดหมายที่มาถึงก่อนจะมีการแจกจ่ายต่อไป

☐ กรณีที่พนักงานหรือเจ้าหน้าที่ของบริษัท ตรวจบุคคลที่ไม่ได้รับอนุญาต หรือไม่สามารถระบุตัวตนได้อย่างชัดเจน ต้องแจ้งเจ้าหน้าที่แผนกบุคคลหรือเจ้าหน้าที่รักษาความปลอดภัยเชิญตัวบุคคลดังกล่าวออกจากบริเวณ

6. การรักษาความปลอดภัยทางกายภาพ (Physical Security)

บริษัทมีระเบียบปฏิบัติและเครื่องกีดขวางหรืออุปกรณ์ป้องกันทางกายภาพที่สามารถป้องกันมิให้บุคคลอื่นสามารถเข้าถึงสถานประกอบการโดยไม่ได้รับอนุญาตโดยมีการจัดนำมาตรฐานการรักษาความปลอดภัยทางกายภาพของ C-TPAT มาประยุกต์มาใช้ในเครือข่ายห่วงโซ่อุปทานตามความเหมาะสม ดังนี้

☐ การกันรั้ว บริษัทมีการกันรั้วโดยรอบพื้นที่สถานประกอบการอย่างมิดชิด รวมถึงพื้นที่ที่มีการจัดการสินค้า เพื่อแยกการขนส่งสินค้าออกเป็นกลุ่ม

☐ ประตูทางเข้าและป้อมยาม (Gates and Gates House) ประตูทางเข้า-ออก ซึ่งมียานพาหนะและ/หรือบุคคล จะต้องเดินทางเข้า-ออก จะมีเจ้าหน้าที่รักษาความปลอดภัย และ/หรือมีระบบเฝ้าระวังอยู่ตลอดเวลา

MASTER

UNCONTROL

☐ การจอดรถ (Parking) บริษัทฯ ได้มีการจัดพื้นที่จอดรถให้บุคคลภายนอกโดยเฉพาะ เพื่อป้องกันการเข้าไปจอดในพื้นที่หรือใกล้เคียงกับบริเวณที่มีการจัดการและการจัดเก็บสินค้า

☐ โครงสร้างอาคาร (Building Structure) โครงสร้างอาคารทำมาจากวัสดุที่ทนทานต่อการจัดแ่ง เพื่อป้องกันการเข้ามาในอาคารโดยผิดกฎหมาย พร้อมกับมีการตรวจสอบและซ่อมแซมโครงสร้างอาคารสถานที่อยู่เสมอเพื่อให้มีความปลอดภัย

☐ อุปกรณ์ปิดล็อกและการควบคุมกุญแจ (Locking Devices and Key Controls) ประตูทางเข้า - ออก และรั้วมีอุปกรณ์ปิดล็อกเพื่อรักษาความปลอดภัย

แสงส่องสว่าง (Lighting) บริษัทฯ ได้จัดให้มีแสงไฟที่สามารถให้ความสว่างอย่างเพียงพอทั้งภายในและภายนอกอาคาร รวมถึงพื้นที่ทางเข้าและทางออกต่างๆ บริเวณที่มีการจัดการและการจัดเก็บสินค้า ตลอดจนแนวรั้วและลานจอดรถ

☐ กล้องโทรทัศน์วงจรปิด (Video Surveillance Camera) บริษัทฯ จัดให้มีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อตรวจตรา สอดส่องพื้นที่สถานประกอบการ และเพื่อมิให้บุคคลใดเข้าไปในบริเวณที่มีการจัดการและการจัดเก็บสินค้าโดยไม่ได้รับอนุญาต พร้อมทั้งมีระบบการสำรองข้อมูล เพื่อทวนสอบเหตุการณ์ย้อนหลังไม่น้อยกว่า 90 วัน และตั้งค่าบันทึกแบบ 24/7

7. ความปลอดภัยทางด้านไซเบอร์ (Cybersecurity)

บริษัทฯ มีการจัดทำนโยบายความปลอดภัยทางด้าน Cyber ที่ครอบคลุมเกี่ยวกับการตรวจสอบข้อมูลทางธุรกิจที่เป็นความลับ และได้รับการป้องกันการเข้าถึงข้อมูลและเอกสารขนส่ง เพื่อลดความเสี่ยงด้านความปลอดภัยทางด้าน Cyber พร้อมไปถึงการป้องกันหากพบว่ามีกระแสมัดข้อมูลที่ส่งผลให้ข้อมูลหรืออุปกรณ์สูญหาย และการกู้คืนข้อมูล

☐ บริษัทฯ มีการติดตั้ง Software ป้องกันการคุกคามทางด้าน Cyber และ Hardware จาก Malware , Viruses , Spyware , Worms , Trojans) และการบุกรุกภายใน-ภายนอก (Firewalls) ในระบบ Computer และได้รับการอัปเดตความปลอดภัยของ Cyber เป็นประจำ

☐ บริษัทฯ มีการทดสอบความปลอดภัยของโครงสร้างพื้นฐานทาง IT เป็นประจำ

☐ บริษัทฯ จัดทำระบบเพื่อระงับการเข้าถึง/ข้อมูล IT โดยที่ไม่ได้รับอนุญาต รวมไปถึงการเข้าถึงระบบภายในหรือเว็บไซต์ภายนอกที่ไม่เหมาะสม

☐ บริษัทฯ มีการทบทวนนโยบายและวิธีการรักษาความปลอดภัยทาง Cyber เป็นประจำทุกปี

☐ บริษัทฯ มีการจำกัดการเข้าถึงของผู้ใช้ตามลักษณะงานหรือหน้าที่ที่ได้รับมอบหมาย และมีการตรวจสอบการได้รับอนุญาตเข้าถึงข้อมูลเป็นประจำ และมีการยกเลิกการเข้าถึงข้อมูลเมื่อพนักงานพ้นสภาพการเป็นพนักงานของบริษัทฯ แล้วทุกกรณี

MASTER

UNCONTROL

- ☐ บริษัทฯมีการกำหนดคู่มือการเชื่อมต่อระยะไกล และมีการติดตั้งเทคโนโลยีความปลอดภัย เช่น Virtual networks (VPNs)
- ☐ บริษัทฯมีการอนุญาตให้ใช้อุปกรณ์ส่วนตัวในการทำงาน โดยจะต้องปฏิบัติตาม นโยบายและขั้นตอนการรักษาความปลอดภัยทาง Cyber ของบริษัทฯ อุปกรณ์ส่วนตัวรวมไปถึงสื่อบันทึกข้อมูล เช่น CD DVD และ USB
- ☐ บริษัทฯ มีการกำหนดการสำรองข้อมูลสัปดาห์ละ 1 ครั้ง โดยเฉพาะข้อมูลที่มีความละเอียดอ่อนและเป็นความลับจะจัดเก็บอยู่ในรูปแบบที่มีการเข้าถึงโดยรหัสผ่าน
- ☐ บริษัทฯ มีการกำหนดข้อจำกัดอุปกรณ์ด้าน IT สื่อ Hardware หรืออุปกรณ์ IT อื่นๆทั้งหมดที่มีข้อมูลที่มีความละเอียดอ่อนเกี่ยวกับการนำเข้าและส่งออก จะต้องได้รับการพิจารณาถึงปริมาณคงเหลือ เมื่อการจัดตั้งต้องได้รับการฆ่าเชื้อหรือทำลายอย่างเหมาะสม

ระเบียบลงโทษ (Accountability)

บริษัทฯได้จัดให้มีระบบการตรวจสอบการเข้าถึงการใช้งานเทคโนโลยีสารสนเทศโดยไม่ถูกต้อง เช่น การเข้าสู่ระบบโดยไม่ถูกต้อง การจัดแะ หรือดัดแปลงข้อมูลทางธุรกิจ ผู้ฝ่าฝืนหรือผิดกฎเข้าไปในระบบทั้งหมดจะต้องได้รับโทษทางวินัยที่เกี่ยวข้องตามความเหมาะสมกับการกระทำผิดนั้นๆ

8. การรักษาความปลอดภัยของการปิดผนึก (Seal Security)

บริษัทฯมีขั้นตอนการตกผนึกที่มีความปลอดภัยสูงเป็นลายลักษณ์อักษร และมาตรฐานของ Seal ต้องเป็นไปตามมาตรฐาน ISO 17712 โดย Seal ที่นำมาเก็บไว้ในสถานประกอบการ ต้องมีความปลอดภัยและมีการล็อกปิดเพื่อไม่อนุญาตผู้ที่ไม่เกี่ยวข้องเข้าถึงโดยง่าย

- ☐ บริษัทฯมีการตรวจสอบ Seal ก่อนการใช้งาน เพื่อให้แน่ใจว่า Seal มีความสมบูรณ์ และปฏิบัติตามขั้นตอนการตรวจสอบ (View / Verify / Tug / Twist (VVT)) เพื่อให้มั่นใจว่า Seal มีความปลอดภัยสูง และได้รับการปิดล็อก/ติดตั้งอย่างถูกต้องกับตู้คอนเทนเนอร์ และการทวงงานตามที่ออกแบบได้

V – ดูตราประทับและกลไกการล็อก ตรวจสอบให้แน่ใจว่าใช้งานได้

V - ตรวจสอบหมายเลข Seal number กับเอกสารจัดส่งเพื่อความถูกต้อง

T - ดึง Seal เพื่อให้แน่ใจว่า Seal ปิดล็อกอย่างถูกต้อง

T - ปิดและหมุนสลักเกลียวเพื่อให้แน่ใจว่าส่วนประกอบไม่แยกออกจากกัน หรือส่วนใดส่วนหนึ่งของ Seal หลวม

- ☐ บริษัทฯมีการบันทึกหมายเลข Seal ลงในแบบฟอร์มการตรวจสอบตู้คอนเทนเนอร์

9. การรักษาความปลอดภัยทางการเกษตร (Agricultural Security)

บริษัทฯมีขั้นตอนการป้องกันการปนเปื้อนของแมลง พืช และสัตว์ อื่นๆ ที่มองเห็นได้ในผลิตภัณฑ์,บรรจุภัณฑ์,การบรรจุ และการขนส่ง รวมถึงการปฏิบัติตามกฎข้อบังคับของ Wood Packaging Materials (WPM)

MASTER

UNCONTROL

บริษัทฯ มีการจัดเตรียมพื้นที่และตรวจสอบพื้นที่จัดเก็บสินค้าอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าไม่มีการปนเปื้อนของแมลง พืช และสัตว์อื่นๆ

10. การรักษาความปลอดภัยของตู้คอนเทนเนอร์ (Container Security)

บริษัทฯ มีขั้นตอนการตรวจสอบตู้คอนเทนเนอร์ และการ Seal ปิดตู้ เพื่อป้องกันการนำวัสดุ หรือ บุคคลที่ไม่ได้รับอนุญาตมาขนส่งสินค้าระหว่างทาง หรือ “ที่พักร” อยู่ภายใต้การควบคุม

☐ ขั้นตอนการทำงานเป็นลายลักษณ์อักษร ครอบคลุมทั้งการตรวจสอบความปลอดภัยและการตรวจสอบสินค้าทางกายภาพ จุดสำคัญสำหรับการรักษาความปลอดภัยของตู้คอนเทนเนอร์ที่มีการ modifications และการปนเปื้อนของศัตรูพืชที่มองเห็นได้ (ตามที่กำหนดไว้ในข้อ 9) และต้องไม่พบแมลงหรือพืชที่มองเห็นได้ในตู้คอนเทนเนอร์ที่ใช้บรรจุสินค้า

☐ การจัดเก็บตู้คอนเทนเนอร์ ต้องเก็บไว้ในพื้นที่ที่มีความปลอดภัย เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต

☐ การตรวจสอบตู้คอนเทนเนอร์ ก่อนทำการโหลดสินค้า บริษัทฯ มีการตรวจสอบตู้คอนเทนเนอร์ และการบันทึกการตรวจสอบตู้คอนเทนเนอร์ ลงในแบบฟอร์มและการตรวจสอบ Seal Verification (CISV) เพื่อตรวจสอบความสมบูรณ์ ลักษณะทางกายภาพของตู้คอนเทนเนอร์

☐ หากพบการปนเปื้อนของสัตว์พาหนะและพืช มองเห็นได้ระหว่างการตรวจสอบ จะต้องดำเนินการล้าง/ดูดฝุ่นเพื่อนำเอาสิ่งปนเปื้อนออก หากได้รับการประกันให้ปฏิเสธตู้คอนเทนเนอร์ และขอตู้คอนเทนเนอร์ใหม่

☐ หากมีการใช้ตู้คอนเทนเนอร์ที่ติดตั้ง Hardware อยู่ภายนอกต้องมีความแข็งแรงและทนทานในการถอดมันออก ประตู , มือจับ , แท่งกลอน , หมุดยึด , และส่วนอื่นๆ ทั้งหมดของกลไกการล็อคตู้คอนเทนเนอร์ ต้องได้รับการตรวจสอบอย่างครบถ้วน เพื่อป้องกันการจัดแะ

☐ พื้นที่ความปลอดภัย ตู้คอนเทนเนอร์ต้องมีการตรวจสอบและโหลดตู้ในพื้นที่ที่มีความปลอดภัย โดยเจ้าหน้าที่ของโรงงานที่ได้รับอนุญาตเท่านั้น เพื่อป้องกันการเข้าถึงของบุคคลที่ไม่ได้รับอนุญาต พื้นที่ควรได้รับการตรวจสอบโดยใช้เทคโนโลยีความปลอดภัย

☐ ความปลอดภัยในการขนส่ง ในระหว่างการขนส่งจากจุดที่โหลดสินค้าไปจนถึงการจัดส่งตู้คอนเทนเนอร์ไปยังท่าเรือ จะต้องได้รับการป้องกันจากการนำวัสดุที่ไม่ได้รับอนุญาต หรือวัสดุที่ไม่สามารถระบุได้ สิ่งเหล่านี้สามารถทำได้โดยใช้วิธีการดังต่อไปนี้

☐ การติดตามการเคลื่อนไหว บริษัทฯ ทำงานร่วมกับผู้ให้บริการขนส่ง เพื่อติดตามย้ายตู้คอนเทนเนอร์จากโรงงานไปยังท่าเรือ

☐ พนักงานขับรถมีการกำหนดเวลาในการ Check in ให้กับผู้จัดส่งหรือบริษัทฯ และการแจ้งให้ผู้มอบหมายงานทราบถึงการล่าช้าของเส้นทางใดๆ อันเนื่องมาจาก สภาพอากาศ , การจราจร , การหยุดพัก หรือพักรับประทานอาหาร , การเปลี่ยนแปลงเส้นทาง

MASTER

UNCONTROL

☐ การบันทึกการขนส่ง ผู้ให้บริการควรใช้บันทึกการติดตามและการตรวจสอบ หรือเทคโนโลยีที่

เทียบเท่า(Global Positioning Satellite (GPS)) เพื่อให้แน่ใจว่าตู้คอนเทนเนอร์มีความปลอดภัยในขณะที่ไป
ที่ท่าเรืออย่างน้อยที่สุด ควรมีบันทึกเวลาตู้คอนเทนเนอร์ออกจากบริษัท , การหยุดระหว่างทาง , เวลาที่มาถึง
ท่าเรือ

11. เอกสารทางการค้า (Commercial Document)

บริษัทมีขั้นตอนการตรวจสอบ เพื่อให้แน่ใจข้อมูลทั้งหมดที่ใช้ในการเคลียร์สินค้า และความชัดเจนของสินค้า
ถูกต้อง , ครบถ้วน และป้องกันการเปลี่ยน , สูญหาย หรือการแนะนำข้อมูลที่ผิดพลาด ซึ่งรวมถึงเอกสารขนส่ง เช่น
ใบกำกับสินค้า , รายการบรรจุภัณฑ์ , B/L , CISV เป็นต้น

12. การฝึกอบรม (Training, Awareness, And Reporting)

บริษัทมีการจัดอบรมสร้างความตระหนัก และการรายงานให้กับพนักงานตามหน้าที่และตำแหน่งงาน รวมไปถึง
พนักงานที่ได้รับการว่าจ้างใหม่ ด้านความปลอดภัย สำหรับพนักงานทุกคนเป็นประจำ เพื่อสร้างการรับรู้ของช่องโหว่ ด้าน
ความปลอดภัย รวมไปถึงสิ่งอำนวยความสะดวก , ยานพาหนะ และการขนส่งสินค้า รวมไปถึงกิจกรรมที่น่าสงสัยและ
เหตุการณ์ด้านความปลอดภัยกับบุคลากรที่ทำงานอยู่ในตำแหน่งที่ละเอียดอ่อน

☐ การฝึกอบรมด้านพีช บุคลากรในการตรวจอาบตู้คอนเทนเนอร์ บริษัทฯจัดให้มีการฝึกอบรมเกี่ยวกับวิธีการ
ดำเนินการตรวจสอบความปลอดภัย และการตรวจสอบทางด้านพีช ครอบคลุมถึงมาตรการป้องกันศัตรูพีช, ข้อกำหนดด้าน
กฎระเบียบที่ใช้วัสดุบรรจุภัณฑ์ที่เป็นไม้ (WPM) และสัญญาณการปนเปื้อนศัตรูพีช

☐ ความปลอดภัยในด้านเทคโนโลยีสารสนเทศ บริษัทฯจัดให้มีการอบรมนโยบายและขั้นตอนการรักษาความปลอดภัย
ทาง Cyber ของบริษัทฯ รวมถึง รหัสผ่าน/การป้องกันรหัสผ่าน และวิธีการเข้าถึง Computer โดยไม่ได้รับอนุญาต

☐ การรายงานสถานการณ์ บริษัทฯมีขั้นตอนที่เป็นลายลักษณ์อักษร สำหรับการรายงาน เหตุการณ์ด้านความ
ปลอดภัย หรือ กิจกรรมที่น่าสงสัย เกี่ยวกับวิธีการปฏิบัติงาน เช่น หลักฐานการลักลอบ , การค้นพบ , การปลอมแปลง Seal
(Seal สำหรับปิดตู้คอนเทนเนอร์) หรือการค้นพบช่องที่ซ่อนอยู่ในตู้คอนเทนเนอร์

☐ การรายงานแบบไม่เปิดเผยตัวตน บริษัทฯมีการกำหนดวิธีการรายงานปัญหาที่เกี่ยวข้องกับความปลอดภัย โดยไม่
ต้องเปิดเผยตัวตน เพื่อที่จะไม่เป็นอันตรายต่อความปลอดภัยในงานหรือการเผชิญต่อการคุกคามจากผู้อื่น

☐ การสอบสวนภายใน บริษัทฯมีการกำหนดพนักงานที่ทำหน้าที่สอบสวนภายใน สำหรับเหตุการณ์ที่เกี่ยวข้องกับ
ความปลอดภัย การสอบสวนภายในของบริษัทฯจะต้องได้รับการจัดทำเป็นเอกสาร และพร้อมให้หน่วยงานที่บังคับใช้ตาม
กฎหมายตามความเหมาะสม

นางโสพรรณ มานะธัญญา

กรรมการผู้จัดการ

บริษัท บีเอสซีเอ็ม ฟู้ดส์ จำกัด

MASTER

รับทราบนโยบายและการรักษาความปลอดภัยห่วงโซ่อุปทาน (Supply Chain Security Policy)

ข้าพเจ้า ได้รับและอ่านนโยบายและการรักษาความปลอดภัยห่วงโซ่อุปทาน (Supply Chain Security Policy) ของ บริษัท บีเอสซีเอ็ม ฟู้ดส์ จำกัด ฉบับที่ 00 โดยเข้าใจในความรับผิดชอบถึงนโยบายและแนวทางปฏิบัติโดยละเอียดแล้ว

ข้าพเจ้า ทราบดีว่าบริษัท บีเอสซีเอ็ม ฟู้ดส์ จำกัด มีนโยบายให้คู่ค้าทางธุรกิจตลอดจนพนักงานถือปฏิบัติและข้อตกลงในการปฏิบัติตามเอกสารนี้ ไม่ได้ถือว่าการทำสัญญาซื้อขาย ตลอดจนสัญญาจ้างงานแต่อย่างใด โดยหนังสือฉบับนี้ ข้าพเจ้า ขอให้ถืออย่างถาวรไว้ต่อบริษัท บีเอสซีเอ็ม ฟู้ดส์ จำกัด ณ วันที่ รับทราบเอกสารนี้

1. ข้าพเจ้า จะธำรงรักษาไว้ ซึ่งเป็นหลักการปฏิบัติงาน ให้เป็นไปตามนโยบายและการรักษาความปลอดภัยห่วงโซ่อุปทาน (Supply Chain Security Policy) จะไม่กระทำการใดๆ อันเป็นการฝ่าฝืนหรือละเมิดนโยบายและการรักษาความปลอดภัยห่วงโซ่อุปทาน (Supply Chain Security Policy) ของบริษัท บีเอสซีเอ็ม ฟู้ดส์ จำกัด ไม่ว่าส่วนใดส่วนหนึ่งหรือทั้งหมด
2. ข้าพเจ้า จะสอดส่องดูแลหากพบเห็นการกระทำใดๆ อันเป็นการฝ่าฝืนหรือละเมิดนโยบายและการรักษาความปลอดภัยห่วงโซ่อุปทาน (Supply Chain Security Policy) ของบริษัท บีเอสซีเอ็ม ฟู้ดส์ จำกัด ข้าพเจ้าจะรายงานผู้บังคับบัญชา หรือหน่วยงานที่เกี่ยวข้องรับทราบ

ลงนาม(ชื่อบริษัท)

ชื่อ-นามสกุล(ตัวบรรจง)

ตำแหน่ง.....

ลายมือชื่อ

วันที่

MASTER

UNCONTROL