# ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

# ความปลอดภัยของข้อมูลสารสนเทศกับภาคอุตสาหกรรม

**วิชญ์ศุทธ์ เมาระพงษ์**
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

สืบเนื่องจากในช่วงนี้องค์การที่ผู้เขียนปฏิบัติงานกำลังอยู่ระหว่างดำเนินการตรวจประเมินมาตรฐาน ISO จึงขอถือโอกาสนี้กล่าวถึง**มาตรฐาน** ISO (International Organization for Standardization) ซึ่งก็คือข้อกำหนด และมาตรฐานสากลที่ยอมรับกันทั่วโลก และมีบริบทในหลากหลายอุตสาหกรรม ทั้งนี้เพื่อให้การดำเนินงานขององค์การ และการให้บริการมีคุณภาพเป็นที่ยอมรับ มีความมั่นคงปลอดปลอดภัยในด้านต่าง ๆ รวมถึงสิ่งแวดล้อม และตัวของผู้บริโภคเอง สำหรับในภาคอุตสาหกรรมแล้ว มาตรฐานเหล่านี้ก็มีความสำคัญต่อการพัฒนาผลิตภัณฑ์ และบริการ เชื่อว่าในองค์การของท่านก็มีการดำเนินการเรื่องมาตรฐาน ISO ในหลาย ๆ ส่วนเช่นกัน อาทิ

- ISO 9001: ระบบบริหารคุณภาพ - เป็นมาตรฐานที่กำหนดเกณฑ์สำหรับระบบบริการลูกค้า และการจัดการคุณภาพในโรงงานอุตสาหกรรม
- ISO 14001: ระบบบริหารสิ่งแวดล้อม - เป็นมาตรฐานที่ระบุข้อกำหนดสำหรับการจัดการสิ่งแวดล้อมในโรงงานอุตสาหกรรม เพื่อลดผลกระทบต่อสิ่งแวดล้อม และป้องกันมลพิษ
- ISO 45001: ระบบบริหารสุขภาพ และความปลอดภัยทางงาน - เป็นมาตรฐานที่เน้นความปลอดภัยในโรงงาน มีเป้าหมายในการลดอุบัติเหตุ และอันตรายในการทำงาน
- ISO 50001: ระบบบริหารพลังงาน - เป็นมาตรฐานที่เน้นการจัดการพลังงานในโรงงานอุตสาหกรรม เพื่อลดค่าใช้จ่ายทางพลังงาน และลดผลกระทบต่อสิ่งแวดล้อม

โดยการปรับใช้มาตรฐาน ISO สำหรับภาคอุตสาหกรรมจะช่วยให้องค์การปรับปรุงการดำเนินงาน และสร้างความน่าเชื่อถือในตลาด นอกจากนี้ตัวมาตรฐานเองยังช่วยสร้างสภาพแวดล้อมที่ดีขึ้นในการทำงาน และประเมินประสิทธิภาพองค์การโดยการปรับปรุงการดำเนินงานนั้นเป็นเรื่องสำคัญสำหรับภาคอุตสาหกรรมเพื่อให้ดำเนินงานไปในทิศทางที่สามารถแข่งขันในตลาดโลกได้อย่างยั่งยืน

ปัจจุบัน การก้าวเข้าสู่อุตสาหกรรมยุค 4.0 ทำให้เทคโนโลยีสารสนเทศมีบทบาทสำคัญอย่างยิ่งต่อการขับเคลื่อนองค์การในเกือบทุกกระบวนการปฏิบัติงาน รวมถึงการบริหารจัดการ ปัจจัยสำคัญในการขับเคลื่อนระบบเทคโนโลยีสารสนเทศนั่นก็คือ “ข้อมูล” ทั้งที่เป็นข้อมูลขององค์การเอง ข้อมูลที่เป็นผลลัพธ์จากการดำเนินงาน การผลิต ข้อมูลข้อกำหนดการปฏิบัติงาน การจัดซื้อ ขนส่ง การติดต่อประสานงาน ข้อมูลคู่ค้า ทรัพย์สินทางปัญญา รวมไปถึงข้อมูลของลูกค้า และ

ข้อมูลที่เกี่ยวข้องกับการทำงานของภาคอุตสาหกรรมทั้งหมด ข้อมูลเหล่านี้มีความสำคัญ และส่งผลกระทบต่อการดำเนินงาน ความเชื่อมั่น ทิศทางการพัฒนาองค์การ ฯลฯ จึงมีความจำเป็นที่ต้องนำเอามาตรฐานสากลที่เกี่ยวข้องมาประยุกต์ใช้ เพื่อสร้างประสิทธิภาพในการดำเนินงาน สร้างความเชื่อมั่นในความมั่นคงปลอดภัย ความน่าเชื่อถือของข้อมูล และการยอมรับที่มีต่อองค์การในระดับสากล ซึ่งมาตรฐานสากลหนึ่งที่มีความจำเป็นนั่นคือ "มาตรฐาน ISO 27001" ซึ่งเป็นมาตรฐานหลักในกลุ่มมาตรฐาน 27000 ที่กล่าวถึงการจัดเตรียมภาพรวมของการจัดการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Management Systems: ISMS) โดยหัวข้อถัดไปจะกล่าวถึงความสำคัญ และโครงสร้างการปฏิบัติตามมาตรฐาน 27001 โดยสังเขปกัน

**มาตรฐาน ISO 27001** เป็นมาตรฐานสากลสำหรับการจัดการความปลอดภัยของข้อมูล มาตรฐานนี้เป็นเครื่องมือสำคัญสำหรับภาคอุตสาหกรรมที่ต้องปกป้องข้อมูลสำคัญขององค์การและลูกค้า มาตรฐาน ISO 27001 จะช่วยให้องค์การสามารถการจัดการความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยข้อมูล และปรับตัวให้เป็นไปตามมาตรฐานสากล

## ความสำคัญของความปลอดภัยข้อมูลในภาคอุตสาหกรรม

- **คุณภาพการให้บริการ** ความปลอดภัยข้อมูลมีผลต่อคุณภาพของการบริการที่องค์การให้แก่ลูกค้า การรั่วไหลของข้อมูลทำให้ลูกค้าสูญเสียความไว้วางใจ ส่งผลต่อภาพลักษณ์ และความน่าเชื่อถือขององค์การ
- **ความเสี่ยงทางกฎหมาย** ในหลายภาคอุตสาหกรรม องค์การจำเป็นต้องปกป้องข้อมูลลูกค้า และข้อมูลที่เกี่ยวข้องกับธุรกิจ เพื่อป้องกันความเสี่ยงทางกฎหมาย การละเมิดความปลอดภัยข้อมูลอาจทำให้องค์การต้องเผชิญกับค่าเสียหาย และการดำเนินการทางกฎหมาย
- **ความสูญเสียทางการเงิน** การรั่วไหลข้อมูลสามารถทำให้องค์การสูญเสียการลงทุน และโอกาสการขยายธุรกิจที่สำคัญ โดยเฉพาะถ้าข้อมูลลูกค้าถูกละเมิดและนำไปใช้ในทางทุจริตจนเกิดความเสียหาย อาจส่งผลให้องค์การต้องชดเชยค่าเสียหาย และสูญเสียความเชื่อมั่นที่มีต่อคู่ค้าหรือนักลงทุน
- **การสูญเสียลูกค้า** ความปลอดภัยข้อมูลเป็นปัจจัยสำคัญในการรักษาฐานลูกค้า การรั่วไหลของข้อมูลอาจทำให้ลูกค้าสูญเสียไว้เชื่อมั่นในองค์การ และหากเกิดขึ้นอย่างต่อเนื่องลูกค้าอาจเลือกย้ายไปสู่คู่แข่งอื่น ๆ ในตลาด
- **ความเสี่ยงทางธุรกิจ** การรั่วไหลข้อมูลส่งผลให้องค์การเผชิญกับความเสี่ยงทางธุรกิจ เช่น การสูญเสียข้อมูลทางธุรกิจที่มีความสำคัญ การสูญเสียโอกาสทางธุรกิจ และการสูญเสียความไว้วางใจของลูกค้า

## โครงสร้าง และหลักการทำงานของมาตรฐาน ISO 27001 และการปรับใช้

- **การกำหนดขอบเขต** ขั้นตอนแรกในการปรับใช้มาตรฐาน ISO 27001 คือการกำหนดขอบเขตของระบบความปลอดภัยข้อมูล โดยองค์การจะต้องระบุถึงข้อมูลที่จะทำการป้องกัน กำหนดระดับความสำคัญ และความลับของข้อมูลนั้น
- **การประเมินความเสี่ยง** หลังจากกำหนดขอบเขต และระบุถึงข้อมูลที่จะทำการป้องกันแล้ว องค์การต้องทำการประเมินความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยข้อมูล โดยการประเมินนี้ควรระบุความเสี่ยงที่องค์การต้องการจัดการ และความเสี่ยงที่องค์การยอมรับ
- **การกำหนดนโยบายความปลอดภัยข้อมูล** องค์การต้องกำหนดนโยบายความปลอดภัยข้อมูลที่ระบุถึงหลักการ และเป้าหมายของความปลอดภัยข้อมูล นโยบายนี้ควรรวมถึงการระบุรายละเอียดเกี่ยวกับความสำคัญของความปลอดภัยข้อมูล และระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้อง
- **การสร้างระบบบริหารความปลอดภัยข้อมูล** องค์การทำสร้างระบบบริหารความปลอดภัยข้อมูลที่เป็นระบบ


การทำงาน และกระบวนการที่เอื้อต่อการจัดการความปลอดภัยข้อมูล โดยระบบนี้ควรประกอบด้วยการวางแผนความปลอดภัย การดำเนินการความปลอดภัย การควบคุมความปลอดภัย และการประเมินความปลอดภัย ตามหลักการของวงจรบริหารงานเชิงคุณภาพ ซึ่งประกอบไปด้วย 4 ขั้นตอน Plan-Do-Check-Act หรือ PDCA

• **การดำเนินการ และตรวจสอบ** องค์การดำเนินการตามระบบความปลอดภัยข้อมูลที่สร้างขึ้น และตรวจสอบการดำเนินงานด้านการรักษาความปลอดภัยข้อมูลเพื่อดูว่าระบบทำงานได้อย่างเหมาะสมหรือไม่

• **การปรับปรุงระบบความปลอดภัยข้อมูล** องค์การควรนำข้อมูลที่ได้จากการตรวจสอบมาใช้เพื่อปรับปรุงระบบความปลอดภัยข้อมูล และกระบวนการความปลอดภัย โดยการปรับปรุงควรดำเนินการอย่างต่อเนื่องเพื่อระบบความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น

## การประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นขั้นตอนสำคัญในการจัดการความปลอดภัยข้อมูล โดยองค์การต้องสามารถระบุ และประเมินความเสี่ยงที่อาจเกิดขึ้นเกี่ยวกับความปลอดภัยข้อมูล ขั้นตอนเหล่านี้จะช่วยให้องค์การเข้าใจความเสี่ยงที่เกี่ยวข้อง และสามารถวางแผนเพื่อลดความเสี่ยงลงเท่าที่องค์การจะสามารถดำเนินการได้ โดยดำเนินการตามขั้นตอนเหล่านี้

• **การระบุความเสี่ยง** องค์การต้องระบุความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยข้อมูล โดยอาจเป็นความเสี่ยงที่เกี่ยวข้องกับการรั่วไหลข้อมูล ความเสี่ยงทางกฎหมาย หรือความเสี่ยงทางธุรกิจ

• **การประเมินความเสี่ยง** หลังจากระบุความเสี่ยง องค์การต้องประเมินความเสี่ยงเพื่อกำหนดระดับความรุนแรงของความเสี่ยง และความเสี่ยงที่เกี่ยวข้อง โดยความเสี่ยงสามารถจะถูกประเมินในระดับสูง ระดับกลาง หรือระดับต่ำ

• **การจัดการความเสี่ยง** หลังจากการประเมินความเสี่ยง องค์การต้องจัดการความเสี่ยง โดยอาจเป็นการยอมรับความเสี่ยง การลดความเสี่ยง หรือการย้ายความเสี่ยง การจัดการความเสี่ยงควรถูกเขียนเป็นแผน และได้รับการปฏิบัติตามอย่างจริงจัง

## การสร้างระบบบริหารความปลอดภัยข้อมูล

การสร้างระบบบริหารความปลอดภัยข้อมูลคือขั้นตอนสำคัญในการปรับใช้มาตรฐาน ISO 27001 โดยมีกระบวนการดังนี้ (ตามหลักการของวงจรบริหารงานเชิงคุณภาพ PDCA)

• **การวางแผนความปลอดภัย** เป็นขั้นตอนแรกในการสร้างระบบความปลอดภัยข้อมูล องค์การต้องวางแผนว่าจะทำอย่างไรเพื่อปกป้องข้อมูล และลดความเสี่ยง ซึ่งรวมถึงการกำหนดเป้าหมายของการสร้างความปลอดภัยของข้อมูล

• **การดำเนินการความปลอดภัย** หลังจากการวางแผนความปลอดภัย องค์การต้องดำเนินการความปลอดภัยตามแผนที่ได้รับการอนุมัติ รวมถึงการปรับเปลี่ยนกระบวนการ และการวางระบบความปลอดภัย

• **การควบคุมความปลอดภัย** คือการดำเนินการเพื่อตรวจสอบว่า ระบบความปลอดภัยทำงานอย่างถูกต้อง รวมถึงการตรวจสอบ และติดตามความปลอดภัยของข้อมูล และระบบที่เกี่ยวข้อง

• **การประเมินความปลอดภัย** องค์การควรทำการประเมินความปลอดภัยเพื่อสอบทานความเหมาะสม และความเป็นปกติของระบบความปลอดภัย

## การดำเนินการ และตรวจสอบ

หลังจากการสร้างระบบความปลอดภัยข้อมูล องค์การต้องดำเนินการและตรวจสอบการดำเนินการเพื่อตรวจสอบความเหมาะสม และความเป็นปกติของระบบ โดย

• **การสื่อสารสร้างความเข้าใจ** ฝึกอบรม และติดตาม องค์การต้องมีการสื่อสารเพื่อสร้างความเข้าใจ และตระหนักถึงการรักษาความปลอดภัยของข้อมูลให้กับผู้ที่เกี่ยวข้อง รวมถึงจัดฝึกอบรมถึงกระบวนการปฏิบัติที่สอดคล้องกับแผนความปลอดภัยขององค์การ และมาตรฐาน จากนั้นดำเนินการติดตามการปฏิบัติงานในส่วนต่าง ๆ เพื่อตรวจสอบว่าเป็นไปตามแผนความปลอดภัยหรือไม่

• **การดำเนินการความปลอดภัย** ควรทำอย่างต่อเนื่องเพื่อสร้างระบบความปลอดภัยข้อมูลที่มั่นคงแข็งแรง ทั้งการดำเนินการรวมถึงการปฏิบัติตามนโยบายความปลอดภัย การตรวจสอบความเสี่ยง และการปรับปรุงความปลอดภัย

• **การตรวจสอบ เป็นการดำเนินการเพื่อตรวจสอบความเหมาะสม** และความเป็นปกติของระบบความปลอดภัย และระบบอื่น ๆ ที่เกี่ยวข้อง

## การปรับปรุงระบบความปลอดภัยข้อมูล

การปรับปรุงระบบความปลอดภัยข้อมูลเป็นขั้นตอนสุดท้ายในกระบวนการจัดการความปลอดภัยข้อมูล โดย

• **การใช้ข้อมูลจากการตรวจสอบ** องค์การควรนำข้อมูลที่ได้จากการตรวจสอบมาใช้เพื่อปรับปรุงระบบความปลอดภัยข้อมูล โดยข้อมูลที่ได้จากการตรวจสอบจะสามารถช่วยให้องค์การมีความเข้าใจถึงขอบเขตการควบคุมความปลอดภัย ผลลัพธ์ และข้อบกพร่องของระบบความปลอดภัย

• **การปรับปรุง** การปรับปรุงระบบความปลอดภัยข้อมูลควรดำเนินการอย่างต่อเนื่องเพื่อทำให้ระบบมีประสิทธิภาพมากขึ้น โดยการปรับปรุงควรดำเนินการทั้งกับระบบความปลอดภัย และกระบวนการความปลอดภัยเพื่อให้ผู้ที่เกี่ยวข้องสามารถปฏิบัติตามได้อย่างเหมาะสม สอดคล้องกับการดำเนินงานขององค์การ

การปรับใช้มาตรฐาน ISO27001 ขององค์การในภาคอุตสาหกรรมยุค 4.0 กำลังกลายเป็นสิ่งที่จำเป็น ซึ่งส่งผลต่อการสร้างความน่าเชื่อถือ และการยอมรับในองค์การ ทั้งในแง่ของผลิตภัณฑ์ การบริการ รวมถึงภาพลักษณ์ เพราะข้อมูลสารสนเทศมีความสำคัญต่อการดำเนินธุรกิจในยุคปัจจุบัน และมีความสำคัญมากขึ้นอย่างต่อเนื่อง ซึ่งการปฏิบัติตามมาตรฐานส่งผลให้องค์การสามารถประเมินความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยข้อมูลได้อย่างเหมาะสม มีการวางแผนดำเนินการการปรับปรุงกระบวนการปฏิบัติงานที่สอดคล้อง จนนำไปสู่การสร้างระบบความปลอดภัยข้อมูลที่มีประสิทธิภาพ ซึ่งมีการสอบทาน การปรับปรุงอยู่อย่างต่อเนื่องเพื่อรองรับกับปัจจัย สภาพแวดล้อม และบริบทที่เปลี่ยนแปลง ส่งผลให้องค์การมีกระบวนการทำงานที่มีประสิทธิภาพมากขึ้น และมีความปลอดภัยด้านข้อมูลที่ดียิ่งขึ้น สามารถส่งต่อผลิตภัณฑ์ และบริการที่มีคุณภาพสูงขึ้นในภาคอุตสาหกรรมของตน

อนึ่ง การปรับใช้มาตรฐานควรดำเนินการร่วมกับที่ปรึกษาผู้เชี่ยวชาญด้าน ISO ที่เหมาะสมกับบริบทของอุตสาหกรรม เพื่อที่จะเป็นไปตามกรอบวิธีการที่ได้รับการยอมรับ มีความครบถ้วนในมิติที่ควรดำเนินการตามข้อกำหนดของมาตรฐาน และนำไปสู่การเข้ารับการตรวจประเมินจะองค์การที่ให้การรับรองในลำดับต่อไป

ข้อมูลอ้างอิง:
iso.org/standard/27001
bureauveritas.co.th/manage-enterprise-risk/iso-27000bsigroup.com/th-TH/ISOIEC-27001-Information-Security.th.hrnote.asia/orgdevelopment/what-is-pdca