

ISO 27001 : 2013 มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ Information Security Management Systems

ความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น ส่งผลให้ความต้องการในการดูแลความมั่นคงปลอดภัยของสารสนเทศเพิ่มสูงขึ้นด้วย องค์กรต่างๆ ทั้งภาครัฐและเอกชน ต่างก็ให้ความสำคัญอย่างมากต่อการพัฒนาระบบเพื่อการดูแลรักษาความปลอดภัยของสารสนเทศขององค์กร มีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่างๆ ที่มีต่อระบบสารสนเทศขององค์กร

มาตรฐาน ISO 27001 เป็นมาตรฐานที่พัฒนาขึ้นโดย ISO (International Organization for Standardization)

โดยเป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information security management system , ITSM) เพื่อสร้างความมั่นใจถึงประสิทธิภาพของ ความมั่นคงปลอดภัยสารสนเทศขององค์กร รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัยทั้งข้อกำหนด และระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องด้วย

แนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศ

ในการบริหารจัดการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ จะขับเคลื่อนผ่านวงจร PDCA ซึ่งประกอบด้วย การวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข (Act)

