หัวข้อการค้นคว้าอิสระ	การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษา องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย Development of Information Technology Security policy by Applying ISO/IEC 27001 relate to Computer Crime Act 2551 A case study of Thai Public Broadcasting Service (ThaiPBS)
ชื่อผู้เขียน	นางสาววิภาวรรณ คุ้มศิริ Miss Wipawan Kumsiri
แผนกวิชา/คณะ	สาขาวิชาการบริหารเทคโนโลยี วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ดร. กมล เกียรติเรืองกมลา
ปีการศึกษา	2551

บทคัดย่อ

การศึกษาเรื่อง “การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษาองค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย (ThaiPBS)” มีวัตถุประสงค์เพื่อต้องการ ลดความเสี่ยงต่างๆ ที่เกิดขึ้นกับระบบสารสนเทศภายในองค์การฯ โดยการใช้มาตรฐาน ISO/IEC27001 เป็นแนวทางปฏิบัติ

ผลการศึกษาพบว่าจากการสำรวจการดำเนินงาน ตามมาตรฐาน ISO/IEC 27001 ทั้ง 11 หมวด พบว่า องค์การฯ ได้ดำเนินการตามมาตรฐาน ISO/IEC27001 แล้วเสร็จ คิดเป็นร้อยละ 33.84 และกำลังดำเนินการคิดเป็นร้อยละ 10.53 และอีกร้อยละ 55.63 ที่องค์การฯ ยังไม่เริ่มดำเนินการ

และจากผลการสำรวจเหตุการณ์ความเสี่ยงที่เกิดขึ้นภายในองค์การฯ ทั้ง 25 เหตุการณ์ โดยทั้ง 25 เหตุการณ์จะถูกจัดแบ่งตามประเภทของความเสี่ยงทั้ง 3 ด้าน คือ ด้านที่ 1 Confidentiality - สิทธิในการเข้าถึงข้อมูลต่างๆ , ด้านที่ 2 Integrity - ความถูกต้องสมบูรณ์ของข้อมูล ด้านที่ 3 Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ

จะพบว่าในปัจจุบันองค์การฯ มีเหตุการณ์ความเสี่ยงสูงที่เกิดขึ้นจำนวน12 เหตุการณ์ ความเสี่ยงปานกลางจำนวน 8 เหตุการณ์ ความเสี่ยงต่ำจำนวน 5 เหตุการณ์ ดังนั้น ทางผู้วิจัย จึงได้ทำการวางมาตรการเพื่อลดความเสี่ยงที่เกิดขึ้น ไว้เป็น 3 ระยะ คือ ระยะที่ 1 มาตรการในการลดความเสี่ยงสูง , ระยะที่ 2 มาตรการในการลดความเสี่ยงปานกลาง และระยะที่ 3 มาตรการในการลดความเสี่ยงต่ำ

อย่างไรก็ตามผู้วิจัยได้ออกแบบมาตรการ เพื่อใช้เป็นนโยบายด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ตามแนวทางมาตรฐาน ISO/IEC27001 เพื่อเป็นกรอบในการลดความเสี่ยงให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งนโยบายในแต่ละระยะจะถูกแบ่งออกเป็น 2 ส่วนคือ ส่วนที่ 1 สำหรับพนักงานทั่วไป ส่วนที่ 2 สำหรับเจ้าหน้าที่สารสนเทศ โดยการลดความเสี่ยงทั้ง 3 ระยะ องค์การฯ จะมีนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ แบ่งเป็น ส่วนที่ 1 สำหรับพนักงานทั่วไป จำนวน 13 ข้อ (ระยะที่ 1 = 12 ข้อ , ระยะที่ 2 = 0 ข้อ , ระยะที่ 3 = 1 ข้อ) ส่วนที่ 2 สำหรับเจ้าหน้าที่สารสนเทศจำนวน 17 ข้อ (ระยะที่ 1 = 10 ข้อ , ระยะที่ 2 = 4 ข้อ , ระยะที่ 3 = 3 ข้อ)