บทคัดย่อ

การศึกษาเรื่อง “การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษา องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย (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 มีเหตุการณ์ความเสี่ยงสูงที่เกิดขึ้นจำนวน 12 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)

Abstract

The study, " Development of Information Technology Security Policy by Applying ISO/IEC 27001 relate to Computer Crime Act 2550 Case Study of Thai Public Broadcasting Service (ThaiPBS) " is intended to reduce the risks. Occurred with the internal IT organization. Using a standard ISO/IEC2700 guidelines.

After we study from the survey while implementing by using 11 categories of standards ISO / IEC 27001 we found that the organization has been done 33.84% , in progress 10.53% and haven't start yet 55.63%

Risk events that occur within the Organization of the 25 events which are splited by risk types into 3 groups. First group: Confidentiality, access to information. Second group: Integrity, the accuracy of complete information. Third group: Availability, access to various information.

Survey results found in an organization occurred 12 high-risk events , 8 medium-risk events and 5 low-risk events. Therefore, the researcher has developed the organization standards of risk reduction based on 3 phases. First phase: to reduce high risk. Second phase: to reduce the medium risk and third phase: to reduce the low risk.

This research measures the usage of the security policy of information based on the standard ISO/IEC27001. In order to reduce risk effectively. Each policy level is separated in 2 parts. First part: the security policy for the general employees. Second part: the security policy for IT staffs.

Nevertheless, this research implement 3 phases of the organization's policies. The first part for general employees using 13 rules (First phase = 12 rules , Second phase = 0 rules and third phase = 1 rules). The second part for IT staff using 17 rules (First phase = 10 rules , Second phase = 4 rules and third phase = 3 rules).