การปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของพนักงาน ในระบบของบริษัทพัฒนาอสังหาริมทรัพย์ขนาดใหญ่รายหนึ่ง

Employees' Compliance to IT Security Policy in the System of a Large Real Estate Development Company

ภัคพล จันทนวรานนท์ และเอกรินทร์ วิบูลย์ตั้งมั่น

Pakkaphol Chantanawaranont and Akarin Vibultangman

หลักสูตรบริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยเนชั่น

Master of of Business Administration Program, Nation University

บทคัดย่อ

การวิจัยเชิงสำรวจนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของพนักงานในระบบของบริษัทพัฒนาอสังหาริมทรัพย์ขนาดใหญ่รายหนึ่ง (2) เปรียบเทียบการปฏิบัติตามนโยบายฯ ของพนักงานจำแนกตามปัจจัยด้านประชากรศาสตร์ (เพศ อายุ ระดับการศึกษา ตำแหน่งงาน ประสบการณ์การทำงาน) รวบรวมข้อมูลโดยใช้แบบสอบถามกับกลุ่มตัวอย่างพนักงานจำนวน 120 คน วิเคราะห์ข้อมูลโดยใช้โปรแกรมสำเร็จรูปทางสถิติ สถิติที่ใช้ประกอบด้วยสถิติเชิงพรรณนา (ความถี่ ร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน) และสถิติเชิงอนุมาน (การทดสอบ t-test และ F-test) ผลการวิจัยพบว่า โดยรวมทุกข้อ พนักงานประพฤติตนตามหลักการปฏิบัติตามนโยบายฯ ในระดับมากที่สุด ในส่วนของการศึกษาเปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ พบว่าผู้ตอบแบบสอบถามที่มีปัจจัยด้านประชากรศาสตร์แตกต่างกัน มีความคิดเห็นเกี่ยวกับประเด็นที่ควรงดเว้นไม่ควรปฏิบัติแตกต่างกันในบางประเด็น ในทำนองเดียวกันในการศึกษาเปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรยึดถือปฏิบัติ พบว่า ผู้ตอบแบบสอบถามที่มีปัจจัยด้านประชากรศาสตร์แตกต่างกัน มีความคิดเห็นเกี่ยวกับประเด็นที่ควรยึดถือปฏิบัติแตกต่างกันในบางประเด็น ที่ระดับนัยสำคัญทางสถิติ 0.05

คำสำคัญ: นโยบายความปลอดภัยสารสนเทศ, การปฏิบัติตาม

Abstract

The objectives of this survey research were to (1) study employees' compliance to IT security policy in the system of a large real estate company and (2) compare IT security policy compliance based upon employees' demographic factors (sex, age, education, rank, and working experience). Data were collected using questionnaires. Samples included 120 employees. Data were analyzed using statistical software. Statistics used in this study included both descriptive statistics (frequency, percentage, mean and standard deviation) and inferential statistics (t-test and F-test). The outcome of the study revealed that, overall, the scores denoting compliance to IT security policy were highest on a given rating scale. The study also showed that employees with different demographic factors differed

in their viewpoints on “Don’ts list” of IT security policy compliance in some respects. On the other hand, employees with different demographic factors differed in their viewpoints on “Do’s list” of IT security policy compliance in some respects at 0.05 level of significance.

Keywords: IT security policy, compliance

บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศเป็นสิ่งจำเป็นสำหรับการดำเนินงานธุรกิจทุกประเภท เพราะจะเป็นสิ่งที่ช่วยสร้างความสามารถในการแข่งขัน และเพิ่มศักยภาพในการเติบโตของธุรกิจ โดยจะเห็นได้ว่า ถ้าองค์กรใดมีการพัฒนาด้านเทคโนโลยีสารสนเทศได้อย่างรวดเร็วและทันสมัยอยู่ตลอดเวลา องค์กรนั้นมักจะเป็นผู้นำในอุตสาหกรรมนั้น ๆ ตามไปด้วย จึงอาจกล่าวได้ว่าเทคโนโลยีสารสนเทศเป็นสิ่งจำเป็นต่อทุกองค์กร และมีอิทธิพลต่อการดำเนินธุรกิจในยุคที่เทคโนโลยีมีความเจริญก้าวหน้าอย่างรวดเร็ว

อย่างไรก็ตามการนำระบบเทคโนโลยีสารสนเทศมาใช้อย่างไม่รอบคอบนั้น อาจก่อให้เกิดผลเสียได้เช่นกัน ปัญหาเรื่องความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นปัญหาหนึ่งที่จะทำให้เกิดความเสียหายต่อความสามารถในการแข่งขันขององค์กร ดังนั้นในแต่ละองค์กรจึงจำเป็นต้องมีหน่วยงานที่ดูแลรับผิดชอบในเรื่องความปลอดภัยของเทคโนโลยีสารสนเทศ มีการวางระบบป้องกันรวมถึงการกำหนดนโยบาย ข้อบังคับ และประกาศต่าง ๆ ให้พนักงานปฏิบัติตามเพื่อเป็นการป้องกันปัญหาที่อาจเกิดขึ้น และส่งผลกระทบต่อองค์กร ทั้งนี้ แม้ว่าจะมีการออกนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศแล้ว แต่ถ้าพนักงานไม่รับทราบ หรือรับทราบแต่ไม่ปฏิบัติตามและกระทำการใด ๆ ที่อาจรู้เท่าไม่ถึงการณ์ และส่งผลให้ระบบสารเทศเกิดความเสียหายได้

บริษัทที่เป็นเป้าหมายของการศึกษานี้ เป็นบริษัทมหาชนชั้นนำของประเทศไทย ที่ดำเนินธุรกิจด้านการลงทุนและพัฒนาอสังหาริมทรัพย์ ได้นำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในบริษัท เพื่อเพิ่มความสามารถในการแข่งขัน และเพิ่มประสิทธิภาพในการดำเนินงาน ซึ่งสถานการณ์ปัจจุบัน บริษัทได้ให้อิสระกับพนักงานในการใช้งานเทคโนโลยีสารสนเทศ และไม่ได้ปิดกั้นการเข้าถึงข้อมูลข่าวสารต่าง ๆ รวมถึงสื่อสังคมออนไลน์ต่าง ๆ เช่น Facebook, Youtube และอื่น ๆ ซึ่งการให้อิสระกับพนักงานดังนี้ มีผลเสียตามมาคือ พนักงานมีการใช้งานเทคโนโลยีอย่างไม่เหมาะสมในเวลางาน ทำให้การทำงานของพนักงานเองไม่มีประสิทธิภาพเท่าที่ควร รวมถึงมีผลทำให้ระบบเครือข่ายหนาแน่นอย่างไม่จำเป็น ส่งผลกระทบกับการใช้งานระบบเครือข่ายของพนักงานคนอื่น ๆ

ปัญหาอีกอย่างหนึ่งที่ส่งผลเสียหายกับบริษัทเป็นอย่างมากคือ ปัญหาไวรัสคอมพิวเตอร์ โดยสาเหตุอาจเกิดจากพนักงานเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ดูหนังฟรี เว็บไซต์โหลดโปรแกรมฟรี เป็นต้น แม้ว่าทางบริษัทจะมีการป้องกันผ่านระบบของบริษัทแล้ว เช่น ไฟร์วอล หรือ โปรแกรมตรวจจับไวรัส แต่ในความเป็นจริง ไม่มีระบบใดที่ป้องกันได้อย่างสมบูรณ์ โดยเฉพาะถ้าผู้ใช้งานเป็นผู้เปิดช่องทางให้ไวรัสเข้ามาเอง ทั้งตั้งใจและโดยไม่ตั้งใจ จากปัญหาต่าง ๆ ดังกล่าว บริษัทจึงได้จัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น และประกาศให้พนักงานทุกคนรับทราบ อย่างไรก็ตามปัญหาที่เกิดจาการใช้งานเทคโนโลยีสารสนเทศอย่างไม่เหมาะสมยังคงมีอยู่

ดังนั้น ในการวิจัยครั้งนี้ ผู้วิจัยจะศึกษาถึงระดับการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของพนักงาน และ ศึกษาเปรียบเทียบการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศในระบบของบริษัทฯ จำแนกตามปัจจัยด้านประชากรศาสตร์ของพนักงาน ทั้งนี้เพื่อนำข้อมูลดังกล่าวมาเป็นแนวทางในการปรับปรุงและพัฒนาความปลอดภัยด้านเทคโนโลยีสารสนเทศในระบบของบริษัทได้อย่างเหมาะสม และมีประสิทธิภาพยิ่งขึ้น

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของประชากรในส่วนที่เป็นสิ่งที่ควรปฏิบัติ และในส่วนที่ควรหลีกเลี่ยงไม่ปฏิบัติ

2. เพื่อศึกษาเปรียบเทียบการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของประชากรจำแนกตามปัจจัยด้านประชากรศาสตร์

แนวคิดทฤษฎีที่เกี่ยวข้อง

ผู้วิจัยจึงได้ศึกษาแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องเพื่อนำมาเป็นแนวทางในการศึกษาวิจัยดังต่อไปนี้

แนวคิดเกี่ยวกับเทคโนโลยีสารสนเทศ

คลังสารสนเทศของสถาบันนิติบัญญัติ (1992) ให้ความหมายของเทคโนโลยีสารสนเทศว่า ความรู้ในผลิตภัณฑ์ หรือใน กระบวนการดำเนินงานใด ๆ ที่อาศัยเทคโนโลยีทางด้านคอมพิวเตอร์ซอฟต์แวร์ คอมพิวเตอร์ฮาร์ดแวร์ การติดต่อสื่อสาร การรวบรวม และการนำข้อมูลมาใช้อย่างทันการ เพื่อก่อให้เกิดประสิทธิภาพทางทางด้านการผลิต การบริการ การบริหาร และ การดำเนินงาน รวมทั้งเพื่อการศึกษาและการเรียนรู้ซึ่งจะส่งผลต่อความได้เปรียบ ทางด้านเศรษฐกิจ การค้า และการพัฒนาด้านคุณภาพชีวิตและคุณภาพของประชาชนในสังคม

ศิริศักดิ์ สุขชื่น (1997) กล่าวว่า “เทคโนโลยีสารสนเทศ” หมายถึง เทคโนโลยีสารสนเทศ ที่เกี่ยวกับการดำเนินงานต่าง ๆ เพื่อจัดทำสารสนเทศไว้ใช้งาน ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์ เทคโนโลยีโทรคมนาคมเป็นหลัก และยังรวมถึงเทคโนโลยีอื่น ๆ ที่เกี่ยวข้องกับการนำข้อมูลข่าวสารมาใช้ให้เกิดประโยชน์ โดยมีคอมพิวเตอร์เป็นเครื่องมือในการ จัดการและจัดเก็บข้อมูล ส่วนการสื่อสารโทรคมนาคมใช้เป็นสื่อในการจัดส่งข้อมูล เผยแพร่ภาพ และเสียงออกไปเพื่อสื่อสารกัน

ลัดดา โกรดิ (2005) ให้ความหมายเทคโนโลยีสารสนเทศ หมายถึง เทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารที่นำมาใช้ในการจัดทำระบบสารสนเทศ และสื่อสารสนเทศ เทคโนโลยีคอมพิวเตอร์ได้แก่ เครื่องคอมพิวเตอร์เพื่อการประมวลผล จัดสร้าง และแสดงผลสารสนเทศตามที่ต้องการ เทคโนโลยีการบันทึกข้อมูล เทคโนโลยี สำหรับการแสดงผลข้อมูล เทคโนโลยีสำหรับจัดเก็บข้อมูลบนสื่อ และเทคโนโลยีสำหรับการสื่อสารส่งผ่านข้อมูล

วิภา เจริญกัณฑารักษ์ (2006) ให้ความ หมายเทคโนโลยีสารสนเทศ หมายถึงการรวมกันระหว่างเทคโนโลยีและสารสนเทศ ส่วนของเทคโนโลยีเป็นการผสมผสานระหว่างเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีอื่น ๆ เช่น เทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีสื่อสาร ข้อมูล เทคโนโลยีคอมพิวเตอร์นั้นมีองค์ประกอบอยู่ด้วยกัน 5 องค์ประกอบ คือ ฮาร์ดแวร์ซอฟต์แวร์บุคลากร ข้อมูล และกระบวนการทำงาน ส่วนสารสนเทศซึ่งเป็นสิ่งที่ได้มาจากการนำข้อมูลข่าวสารมาเข้าสู่ระบบการประมวลผล เพื่อให้ได้สารสนเทศที่ใช้ในการปฏิบัติงานและติดสินใจในเรื่องต่าง ๆ สถาปัตยกรรมของเทคโนโลยีสารสนเทศเพื่อใช้งานในองค์การนั้น มีสิ่งที่ผู้บริหารองค์การจะต้องคำนึงถึง 2 สิ่งที่สำคัญได้แก่ความต้องการของธุรกิจและโครงสร้างพื้นฐานของการใช้เทคโนโลยี สารสนเทศในองค์การ มีการเน้นในงานด้านการประมวลผล การใช้เทคโนโลยีสารสนเทศ ช่วยในการตัดสินใจ ดำเนินการ ควบคุม ติดตามผล และวิเคราะห์ผลงานของผู้บริหาร

แนวคิดเกี่ยวกับการยอมรับและการปฏิบัติ

Foster (1973) ให้ความหมายการยอมรับไว้ว่า การยอมรับจะเกิดขึ้นได้หากมีการเรียนรู้ด้วยตนเอง และการเรียนรู้จะได้ผลดีก็ต่อเมื่อ บุคคลนั้นได้ทดลองปฏิบัติ

Rogers and Shoemaker (1971) ให้ความหมายการยอมรับไว้ว่าเป็นกระบวนการทางจิตใจของบุคคลแต่ละคนที่เริ่มต้นตั้งแต่การรับรู้ข่าวเกี่ยวกับสิ่งนั้น ๆ ไปจนถึงการยอมรับสิ่งนั้น ๆ ไปใช้อย่างเปิดเผย

พรรณทิพา แอดำ (2006) กล่าวถึงการยอมรับสิ่งใหม่ว่าเป็นกระบวนการอย่างหนึ่งที่ช่วยพัฒนาคุณสมบัติของบุคคล เช่น ความรู้ ค่านิยม ทัศนคติ ทำให้สมาชิกของสังคมได้รับรู้การเปลี่ยนแปลง มีความรู้ความเข้าใจในสิ่งใหม่ ๆ ได้ง่าย นอกจากนี้การติดต่อสัมพันธ์ กับบุคคลต่าง ๆ อยู่เสมอ ความสนใจรับรู้ข่าวสารใหม่ ๆ มีส่วนสำคัญยิ่ง ต่อการก่อให้เกิดการรับรู้ ความสนใจ และพยายามนำไปปฏิบัติในที่สุด

จากแนวคิดต่าง ๆ สรุปได้ว่า การยอมรับคือ กระบวนการทางความคิดของผู้บริโภค ในการแสดงพฤติกรรม นับตั้งแต่จากการรับรู้นวัตกรรมใหม่ครั้งแรก ไปจนถึงการยอมรับนวัตกรรมใหม่ โดยที่กระบวนการตัดสินใจนั้นมีการเปลี่ยนแปลงอย่างเป็นระบบและต้องอาศัยเวลา

กระบวนการตัดสินใจเกี่ยวกับนวัตกรรม

กระบวนการตัดสินใจเกี่ยวกับนวัตกรรม (a model of the innovation decision process) มีอยู่หลายตัวแบบด้วยกัน ในที่นี่จะเสนอตัวแบบของโรเจอร์ ที่เรียกว่า ตัวแบบกระบวนการตัดสินใจเกี่ยวกับนวัตกรรม (Rogers, 1968) ซึ่งเป็นตัวแบบที่ใช้กันอย่างแพร่หลายตัวแบบนี้แสดงกระบวนการตัดสินใจซึ่งแบ่งเป็นระยะต่าง ๆ ได้ 5 ระยะ คือ ระยะการรับรู้ (knowledge) ระยะจูงใจ (persuasion) ระยะการตัดสินใจ (decision) ระยะปฏิบัติ (implementation) และ ระยะขั้นการยืนยัน (confirmation)

สรุปได้ว่าการที่บุคคลจะยอมรับและปฏิบัติตามข่าว หรือ สิ่งใหม่ ๆ นั้น ต้องผ่านการรับรู้ โดยการรับรู้ได้มากน้อยนั้น ขึ้นอยู่กับคุณลักษณะของบุคคลในด้านต่าง ๆ คือ สถานภาพทางเศรษฐกิจ สังคม และการศึกษา

แนวคิดเกี่ยวกับการรักษาความปลอดภัยของข้อมูลสารสนเทศ

ปนิวัธน์ ทรัพย์รุ่งเรือง (2004) ได้ให้คำจำกัดความของความปลอดภัยของข้อมูลไว้ว่า “การรักษาความปลอดภัยทางข้อมูล คือ ผลที่เกิดขึ้นจากการใช้ระบบของนโยบายและ/หรือระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการปกป้อง) โดยไม่ได้รับอนุญาต” และยังได้ให้คำจำกัดความของความปลอดภัยทางคอมพิวเตอร์ ไว้ว่า “ความปลอดภัยทางคอมพิวเตอร์ คือ ระเบียบการทางเทคนิคและทางการบริหารที่นำมาใช้กับระบบคอมพิวเตอร์เพื่อให้มั่นใจถึงความพร้อมใช้ ความถูกต้องสมบูรณ์ และความลับของข้อมูลที่ระบบคอมพิวเตอร์จัดการอยู่”

U.S. Government’s National Information Assurance (2006) ของสหรัฐอเมริกาได้ให้นิยามของการรักษาความปลอดภัยของข้อมูลไว้ว่า “การรักษาความปลอดภัยของข้อมูลเป็นการป้องกันระบบข้อมูลข่าวสารที่เกิดจากการเข้าใช้โดยไม่ได้รับอนุญาต หรือมีการเปลี่ยนแปลงข้อมูล ในการจัดเก็บ การประมวลผล หรือ การสื่อสาร ซึ่งรวมถึงการวัดผลในเรื่องการตรวจตรา และการต่อต้านการคุกคาม”

โดยสรุปแล้ว จุดมุ่งหมายของการรักษาความปลอดภัยของข้อมูลสารสนเทศที่จะต้องคำนึงถึงจะมีอยู่ 3 ประการ คือ

1. ความลับ (confidentiality) คือ การที่จะต้องมั่นใจว่าข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับไม่ได้ถูกเปิดเผยและยังคงเป็นความลับอยู่

2. ความสมบูรณ์ (integrity) คือ การที่จะต้องมั่นใจว่าข้อมูลและระบบไม่ได้ถูกแก้ไขด้วยวิธีการใด ๆ ก็ตาม ที่ไม่ได้รับอนุญาต

3. ความพร้อมใช้ (availability) คือ การที่จะต้องมั่นใจว่าระบบและข้อมูลที่มีอยู่สามารถใช้ได้เมื่อต้องการ

Gibson (2011) ได้ ยกตัวอย่างถึงวิธีการรักษาความปลอดภัยในด้านความลับ และด้านความพร้อมใช้ รวมถึงปัญหาที่อาจเกิดขึ้น ดังนี้

การป้องกันด้านความลับ: ผู้ใช้งานต้องมีการระบุตัวตนเพื่อยืนยันว่ามีสิทธิ์ในการใช้งานข้อมูลสารสนเทศนั้น ถ้าผู้ใช้งานไม่มีสิทธิ์ จะไม่สามารถเข้าถึงข้อมูลนั้น ๆ ได้ อย่างไรก็ตาม มีบางกรณีที่ผู้ใช้งานบางคนที่ไม่ได้ระบุตัวตนแต่สามารถเข้าใช้งานข้อมูลสารสนเทศได้ ซึ่งเกิดจากข้อมูลนั้น ๆ ถูกเก็บไว้ใน External Harddisk หรือ USB flash drive และอุปกรณ์เหล่านี้ถูกขโมยไป

การป้องกันด้านความพร้อมใช้: วิธีการหลักสำหรับการป้องกันด้านความพร้อมใช้คือ การสำรองข้อมูล ซึ่งเมื่อเวลาข้อมูลต้นฉบับมีปัญหาก็จะสามารถกู้คืนกลับมาได้ Mark Zimmerman จากมหาวิทยาลัย Missouri–St. Louis ได้ยกตัวอย่างว่า Malware ซึ่ง เป็นคำที่ใช้เรียก กลุ่มของ Virus, Worms, Trojan horses, Spyware, Adware, etc. จะเป็นสิ่งที่จะกระทบต่อการรักษาความปลอดภัยของข้อมูลสารสนเทศ ทั้ง 3 ประการข้างต้น กล่าวคือ

1. ด้านความลับ – Malware เช่น spyware อาจแอบส่งข้อมูลออกไปข้างนอกโดยผู้ใช้งานไม่รู้ตัว หรืออาจดักจับรหัสผ่านที่ผู้ใช้งานพิมพ์ลงบนคอมพิวเตอร์แล้วส่งออกไปข้างนอก

2. ด้านความสมบูรณ์ – Malware เช่น Virus สามารถเปลี่ยนแปลงข้อมูล หรือทำลายข้อมูลสารสนเทศของผู้ใช้งาน

3. ด้านความพร้อมใช้ – Malware เช่น Trojan horse สามารถสั่งปิด server หรือ ระบบเครือข่ายทำให้ผู้ใช้งานไม่สามารถเรียกใช้งานข้อมูลได้

จากแนวคิด และตัวอย่างของความสำคัญของข้อมูลสารสนเทศ ทำให้เห็นว่าข้อมูลสารสนเทศมีความสำคัญต่อบริษัทในหลาย ๆ ประเด็น ดังนั้นพนักงานจึงต้องมีความตระหนักในเรื่องของการรักษาความปลอดภัยของข้อมูล และตัวบริษัทเองควรมีมาตรการเพื่อตรวจสอบว่าพนักงานมีความตระหนักเพียงพอหรือไม่ เพื่อให้แน่ใจว่าพนักงานทุก ๆ คนจะให้ความร่วมมือ และเป็นส่วนสำคัญที่ช่วยปกป้องรักษาความปลอดภัยของข้อมูลสารสนเทศภายในบริษัท

งานวิจัยที่เกี่ยวข้อง

รัชชาภรณ์ สุภาพ และศักดิ์ชาย ตั้งวรรณวิทย์ (2014) ทำการศึกษาเรื่อง การจัดทำแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 กรณีศึกษา: สำนักงานรัฐบาลอิเล็กทรอนิกส์ (มหาชน) กลุ่มตัวอย่างได้แก่ ผู้ใช้งานเทคโนโลยีสารสนเทศในองค์กรภาครัฐผลการวิจัยพบว่า เจ้าหน้าที่ภายในองค์กรส่วนมากยังไม่ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ISO/ICE 27001

สุพิชญา อาชวิรดา (2016) ทำการศึกษาเรื่อง ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร โดยกลุ่มตัวอย่างได้จากพนักงานในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยจำนวน 240 คน ผลการวิจัยพบว่า การรับรู้ถึงภัยคุกคาม การฝึกอบรมและให้ความรู้ความเข้าใจในระบบสารสนเทศ ล้วนส่งผลต่อการตระหนักถึงความปลอดภัย

ผู้วิจัยอาศัยแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องดังกล่าวเป็นแนวทางในการศึกษาการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของพนักงานในระบบของ บริษัทพัฒนาอสังหาริมทรัพย์รายหนึ่ง และศึกษาปัจจัยที่มีความสัมพันธ์ต่อการปฏิบัติตามนโยบายเพื่อหาแนวทางในการแก้ไขหรือสนับสนุนให้พนักงานทำตามนโยบายได้มากขึ้น และเพื่อนำข้อมูลที่ได้ไปเป็นแนวทางในการแก้ไขปรับปรุงการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศในระบบของบริษัทฯ ต่อไป ปัจจุบัน บริษัทฯ จัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วยคำแนะนำเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบโครงข่าย จำนวน 22 ข้อ คำแนะนำในการใช้รหัสลับส่วนบุคคล 5 ข้อ คำแนะนำในการใช้อีเมล์ 15 ข้อ และคำแนะนำอื่น 3 ข้อ

ตัวแปรต้น	ตัวแปรตาม
ปัจจัยด้านประชากรศาสตร์ - เพศ - อายุ - ระดับการศึกษา - ระดับตำแหน่งงาน - ระยะเวลาในการทำงาน	**การปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ**

ภาพ 1 กรอบแนวคิดการวิจัย

สมมติฐานการวิจัย

พนักงานที่มีปัจจัยด้านประชากรศาสตร์ (เพศ อายุ ระดับการศึกษา ตำแหน่งงาน ระยะเวลาในการทำงาน) แตกต่างกัน มีการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศแตกต่างกัน

วิธีดำเนินการวิจัย

ขอบเขตด้านเนื้อหา: มุ่งศึกษาการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ขอบเขตด้านประชากร: ครอบคลุมพนักงานที่ทำหน้าที่ในหน่วยงานต่าง ๆ ที่ทำงานโดยใช้เครื่องคอมพิวเตอร์ ระบบโครงข่าย และอุปกรณ์ที่เกี่ยวข้องกับข้อมูลสารสนเทศ

ขอบเขตด้านสถานที่: มุ่งศึกษาพนักงานที่ทำงาน ณ สำนักงานของบริษัทพัฒนาอสังหาริมทรัพย์รายหนึ่ง และสำนักงานของบริษัทในเครือ

ขอบเขตด้านเวลา: งานวิจัยนี้จะดำเนินการตั้งแต่วันที่ 1 พฤศจิกายน พ.ศ. 2558 ถึง วันที่ 30 พฤศจิกายน พ.ศ. 2558 เป็นระยะเวลา 1 เดือน

ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัยครั้งนี้เป็นพนักงานในหน่วยงานต่าง ๆ ซึ่งประกอบด้วยพนักงานจำนวน 172 คน ที่ทำงานโดยใช้เครื่องคอมพิวเตอร์ ระบบโครงข่าย และอุปกรณ์ที่เกี่ยวข้องกับข้อมูลสารสนเทศ ในระบบของบริษัทพัฒนาอสังหาริมทรัพย์รายหนึ่ง

การกำหนดขนาดของกลุ่มตัวอย่างใช้สูตรการคำนวณของ Taro Yamane (1973) โดยใช้จำนวนประชากร 172 คน และกำหนดค่าความผิดพลาดที่ยอมให้เกิดได้เท่ากับ 0.05 พบว่าได้ขนาดของกลุ่มตัวอย่าง 120 ราย

วิธีการเก็บตัวอย่างใช้วิธีการสุ่มตัวอย่างแบบง่าย (simple random sampling) คัดเลือกพนักงานจำนวน 120 คน จากทั้งหมด 172 คน

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยครั้งนี้คือ แบบสอบถาม (questionnaires) จำนวน 31 ข้อ ซึ่งผู้วิจัยได้สร้างขึ้นจาก คำแนะนำเกี่ยวกับการใช้งานคอมพิวเตอร์และระบบโครงข่าย คำแนะนำในการใช้รหัสลับส่วนบุคคล คำแนะนำในการใช้อีเมล์ และคำแนะนำอื่น ๆ ที่อยู่ในนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศรวมถึงทฤษฎี แนวคิดต่าง ๆ และผลงานที่เกี่ยวข้องอื่น ๆ โดยตั้งคำถามครอบคลุมวัตถุประสงค์ที่ต้องการศึกษา ซึ่งแบ่งออกเป็น 2 ส่วนคือ

ส่วนที่ 1 เป็นคำถามเกี่ยวกับปัจจัยด้านประชากรศาสตร์ของกลุ่มตัวอย่าง โดยให้ทำเครื่องหมายถูกในช่องที่กำหนด ซึ่งประกอบด้วยคำถามเรื่อง เพศ อายุ ระดับการศึกษา ระดับตำแหน่งงาน ระยะเวลาในการทำงาน และข้อมูลเบ็ดเตล็ดของกลุ่มตัวอย่าง ได้แก่ การฝึกอบรมด้านคอมพิวเตอร์ การฝึกอบรมด้านคอมพิวเตอร์และฝึกปฏิบัติกับเครื่องคอมพิวเตอร์ การนำความรู้มาใช้งานหลังการฝึกอบรม และความครบถ้วนในการอ่านนโยบายความปลอดภัย

ส่วนที่ 2 เป็นคำถามเกี่ยวกับการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศในระบบของ บริษัท พัฒนาอสังหาริมทรัพย์รายหนึ่ง

ในการทดสอบคุณภาพของแบบสอบถามซึ่งเป็นเครื่องมือที่ใช้ในการวิจัย ผู้วิจัยได้ดำเนินการดังนี้

ขั้นตอนที่ 1 ผู้วิจัยได้ขอให้ผู้ทรงคุณวุฒิ 3 ท่าน ทำการตรวจสอบความเที่ยงตรงของเนื้อหา (content validity) ที่มีในแบบสอบถามโดยการคำนวณหา Index of Item Objective Congruence (IOC) โดยคำถามข้อที่มี IOC เกิน 0.67 จะคงอยู่ในแบบสอบถาม

ขั้นตอนที่ 2 นำแบบสอบถามที่ปรับปรุงแก้ไขแล้วตามขั้นตอนที่ 1 ไปทำการทดสอบ (pre-test) กับกลุ่มตัวอย่างจำนวน 30 คน จากนั้นนำมาวิเคราะห์หาค่าความเชื่อมั่น (reliability) โดยใช้สูตรการคำนวณหาค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's alpha coefficient) พบว่าในส่วนของคำถามที่ควรงดเว้นไม่พึงปฏิบัติมีค่า Cronbach's alpha เท่ากับ 0.711 ในส่วนของคำถามที่ควรปฏิบัติมีค่า Cronbach's alpha เท่ากับ 0.490

สถิติที่ใช้ในการวิเคราะห์ข้อมูล

สถิติที่ใช้ในการวิจัย ประกอบด้วยสถิติเชิงพรรณนา ได้แก่ การแจกแจงความถี่ (frequency) ค่าร้อยละ (percentage) ค่าเฉลี่ย (means) ส่วนเบี่ยงเบนมาตรฐาน (SD) และสถิติเชิงอนุมานได้แก่ การทดสอบด้วยค่าสถิติ t และการทดสอบด้วยค่าสถิติ F

ตาราง 1

แสดงความถี่และร้อยละของผู้ตอบแบบสอบถาม ในข้อมูลด้านประชากรศาสตร์

ข้อมูลด้านประชากรศาสตร์		จำนวน	ร้อยละ
1. เพศ	ชาย	36	30
	หญิง	84	70
	รวมทั้งหมด	120	100
2. อายุ	21-30 ปี	29	24.2
	31-40 ปี	63	52.5
	41-50 ปี	16	13.3
	มากกว่า 50 ปี	12	10.0
	รวมทั้งหมด	120	100.0
3. ระดับการศึกษา	ต่ำกว่า ป.ตรี	2	1.7
	ป.ตรี หรือเทียบเท่า	66	55.0
	สูงกว่า ป.ตรี	52	43.3
	รวมทั้งหมด	120	100.0
4. ระดับตำแหน่งงาน	1-3	40	33.3
	4-6	67	55.8
	7 ขึ้นไป	13	10.8
	รวมทั้งหมด	120	100.0
5. ประสบการณ์การทำงานในระบบของบริษัทอมตะ	น้อยกว่า 3 ปี	49	40.8
	3-9 ปี	33	27.5
	มากกว่า 9 ปีขึ้นไป	38	31.7
	รวมทั้งหมด	120	100.0
6. การฝึกอบรมด้านคอมพิวเตอร์	เคย	108	90.0
	ไม่เคย	12	10.0
	รวมทั้งหมด	120	100.0
7. การฝึกอบรมด้านคอมพิวเตอร์ และฝึกปฏิบัติกับเครื่องคอมพิวเตอร์	เคย	96	80.0
	ไม่เคย	24	20.0
	รวมทั้งหมด	120	100.0

ตาราง 1

แสดงความถี่และร้อยละของผู้ตอบแบบสอบถาม ในข้อมูลด้านประชากรศาสตร์ (ต่อ)

ข้อมูลด้านประชากรศาสตร์		จำนวน	ร้อยละ
8. ได้นำความรู้มาใช้งานภายหลังจากการเข้ารับการฝึกอบรมด้านคอมพิวเตอร์	เคย	105	87.5
	ไม่เคย	15	12.5
	รวมทั้งหมด	120	100.0
9. การอ่านนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่บริษัทประกาศ	ไม่เคยอ่าน	6	5.0
	อ่านผ่าน ๆ	84	70.0
	อ่านครบถ้วน	30	25.0
	รวมทั้งหมด	120	100.0

ผลการวิจัย

กลุ่มตัวอย่างในการศึกษาส่วนใหญ่เป็นเพศหญิง (ร้อยละ 70) มีอายุระหว่าง 31-40 ปี (ร้อยละ 52.5) มีการศึกษาในระดับปริญญาตรีหรือเทียบเท่า (ร้อยละ 55.0) มีตำแหน่งงานในระดับ 4-6 (ร้อยละ 55.8) มีประสบการณ์การทำงานในระบบของบริษัทฯ น้อยกว่า 3 ปี (ร้อยละ 40.8) มีการฝึกอบรมด้านคอมพิวเตอร์ (ร้อยละ 90.0) มีการฝึกอบรมด้านคอมพิวเตอร์และฝึกปฏิบัติกับเครื่องคอมพิวเตอร์ (ร้อยละ 80.0) เคยนำความรู้มาใช้งานภายหลังจากการเข้ารับการฝึกอบรม (ร้อยละ 87.5) มีการอ่านนโยบายความปลอดภัยแบบผ่าน ๆ (ร้อยละ 70.0) (ตารางที่ 1)

ตารางที่ 2 แสดงให้เห็นว่าในเรื่องการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศในส่วนที่เป็นประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ กลุ่มผู้ตอบแบบสอบถามส่วนใหญ่มีการหลีกเลี่ยงไม่ปฏิบัติอย่างเคร่งครัด มีเพียงประเด็นการส่งอีเมล์ที่มีขนาดใหญ่กว่า 15 MB โดยไม่ได้แจ้ง ฝ่าย IT เพียงประเด็นเดียวที่มีการหลีกเลี่ยงไม่ปฏิบัติเป็นส่วนใหญ่ อาจเป็นด้วยว่า การส่งอีเมล์ธรรมดาในชีวิตประจำวันไม่มีการแนบไฟล์ขนาดใหญ่อยู่แล้ว เพราะข้อจำกัดของเว็บที่ใช้ส่งอีเมล์ได้ และไฟล์ที่ใช้งานโดยปกติหากไม่ใช่ไฟล์เสียงหรือไฟล์วิดิโอจะมีขนาดไม่ถึงอยู่แล้ว

ตาราง 2

แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และการแปลผลเรื่องการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศในส่วนที่เป็นประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ

ข้อ	ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ	$\bar{X}$	SD	แปลผล
1	ท่านให้ผู้อื่นใช้งานคอมพิวเตอร์ของบริษัทได้โดยไม่ได้รับอนุญาตจากหัวหน้างาน	1.70	.460	หลีกเลี่ยงอย่างเคร่งครัด
2	ท่านให้ผู้อื่นใช้ชื่อบัญชี (username & password) ของท่านในการทำงาน	1.32	.594	หลีกเลี่ยงอย่างเคร่งครัด
3	ท่านมีโปรแกรมคอมพิวเตอร์อื่นนอกเหนือจากที่บริษัทกำหนดในเครื่องที่ท่านรับผิดชอบ	1.42	.657	หลีกเลี่ยงอย่างเคร่งครัด
4	ท่านเปลี่ยนแปลงอุปกรณ์คอมพิวเตอร์ที่ท่านรับผิดชอบด้วยตนเอง	1.12	.453	หลีกเลี่ยงอย่างเคร่งครัด

ตาราง 2

แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และการแปลผลเรื่องการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศในส่วนที่เป็นประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ (ต่อ)

ข้อ	ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ	$\overline{X}$	SD	แปลผล
5	ท่านติดตั้งหรือให้ผู้อื่นติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์บนเครื่องที่ท่านรับผิดชอบ	1.36	.577	หลีกเลี่ยงอย่างเคร่งครัด
6	ท่านนำอุปกรณ์ส่วนตัวอื่น ๆ มาใช้กับระบบของบริษัทโดยไม่ได้รับการอนุมัติจากหัวหน้างาน	1.20	.544	หลีกเลี่ยงอย่างเคร่งครัด
7	ท่านใช้คอมพิวเตอร์และระบบโครงข่ายเพื่อวัตถุประสงค์ทางการค้าส่วนตัว	1.02	.129	หลีกเลี่ยงอย่างเคร่งครัด
8	ท่านอ่านข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต	1.01	.091	หลีกเลี่ยงอย่างเคร่งครัด
9	ท่านแก้ไขข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต	1.02	.129	หลีกเลี่ยงอย่างเคร่งครัด
10	ท่านโหลดไฟล์ที่ไม่เกี่ยวกับงานในเวลางาน	1.23	.463	หลีกเลี่ยงอย่างเคร่งครัด
11	ท่านใช้งานเว็บไซต์สังคมออนไลน์ เช่น Facebook Youtube หรืออื่น ๆ โดยไม่เกี่ยวกับการทำงานในระหว่างเวลางาน	1.57	.657	หลีกเลี่ยงอย่างเคร่งครัด
12	ท่านเล่นเกมผ่านทางอินเทอร์เน็ตของบริษัท	1.04	.239	หลีกเลี่ยงอย่างเคร่งครัด
13	ท่านดูหนังผ่านทางอินเทอร์เน็ตของบริษัท	1.33	.637	หลีกเลี่ยงอย่างเคร่งครัด
14	ท่านฟังเพลงผ่านทางอินเทอร์เน็ตของบริษัท	1.31	.619	หลีกเลี่ยงอย่างเคร่งครัด
15	ท่านเปิดเผยข้อมูลที่มีความสำคัญต่อบริษัทให้แก่บุคคลอื่นโดยไม่ได้รับอนุญาต	1.01	.091	หลีกเลี่ยงอย่างเคร่งครัด
16	ท่านแสดงความคิดเห็นเกี่ยวกับการทำงานของบริษัทในเว็บไซต์หรือสื่อสังคมออนไลน์ต่าง ๆ ในลักษณะที่ก่อให้เกิดความเสียหาย	1.02	.129	หลีกเลี่ยงอย่างเคร่งครัด
17	ท่านเขียนหรือบันทึกรหัสลับ(password)ไว้ในสถานที่ที่ผู้อื่นสามารถพบเห็นได้ง่าย	1.23	.510	หลีกเลี่ยงอย่างเคร่งครัด
18	ท่านส่งอีเมล์ให้บุคคลที่สามโดยไม่เกี่ยวข้องกับงาน	1.34	.855	หลีกเลี่ยงอย่างเคร่งครัด
19	ท่านนำข้อมูลในอีเมล์ของบุคคลอื่นไปใช้โดยไม่ได้รับอนุญาต	1.00	.000	หลีกเลี่ยงอย่างเคร่งครัด
20	ท่านใช้ชื่ออีเมล์ของบริษัทเพื่อลงทะเบียนในเว็บไซต์ต่าง ๆ	1.37	.699	หลีกเลี่ยงอย่างเคร่งครัด
21	ท่านส่งอีเมล์ที่มีขนาดใหญ่กว่า 15 MB โดยไม่ได้แจ้งฝ่าย IT	1.98	1.155	หลีกเลี่ยงอย่างเคร่งครัด
22	ท่านเปิดไฟล์แนบในอีเมล์ที่ได้รับจากบุคคลที่ไม่รู้จัก	1.53	.661	หลีกเลี่ยงอย่างเคร่งครัด
23	ท่านทำสำเนาโปรแกรมที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต	1.05	.286	หลีกเลี่ยงอย่างเคร่งครัด
24	ท่านเล่นเกมคอมพิวเตอร์ในระหว่างเวลาทำงาน	1.04	.201	หลีกเลี่ยงอย่างเคร่งครัด

ตาราง 3

แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และการแปลผลเรื่องการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศในส่วนที่เป็นประเด็นที่ควรปฏิบัติ

ข้อ	ประเด็นที่ควรปฏิบัติตาม	$\bar{X}$	SD	แปลผล
1	ท่านยอมรับข้อกำหนดเกี่ยวกับนโยบายรักษาความปลอดภัยของฝ่าย IT อย่างไม่มีเงื่อนไข	4.39	.813	ยึดถือปฏิบัติครบถ้วน
2	ท่านทราบนโยบายครบทุกข้อ	3.39	.998	ยึดถือปฏิบัติครบถ้วน
3	ท่านแจ้งฝ่าย IT เมื่อพบว่ามีโปรแกรมที่ไม่มีลิขสิทธิ์บนเครื่องของท่าน	4.43	.775	ยึดถือปฏิบัติครบถ้วน
4	ท่านเปลี่ยนรหัสลับทุก ๆ 60 วัน	4.51	.686	ยึดถือปฏิบัติครบถ้วน
5	ท่านตรวจสอบชื่ออีเมล์ผู้รับอย่างระมัดระวังเสมอ เพื่อป้องกันการส่งผิดพลาด	4.35	.657	ยึดถือปฏิบัติครบถ้วน

ในเรื่องการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศในส่วนที่เป็นประเด็นที่ควรปฏิบัติตาม ส่วนใหญ่จะมีการยึดถือปฏิบัติโดยครบถ้วน มีเพียงประเด็นเดียวที่ผู้ปฏิบัติอาจไม่มั่นใจในนโยบาย คือ ผู้ปฏิบัติต้องทราบนโยบายทุกข้อ ซึ่งส่วนใหญ่ระบุว่ามีการปฏิบัติปานกลาง (ตารางที่ 3)

ในส่วนของการศึกษาเปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ พบว่าผู้ตอบแบบสอบถามที่มีปัจจัยด้านประชากรศาสตร์ (เพศ อายุ ระดับการศึกษา ตำแหน่งงาน ระยะเวลาในการทำงาน) แตกต่างกัน มีความคิดเห็นเกี่ยวกับประเด็นที่ควรงดเว้นไม่ควรปฏิบัติแตกต่างกันในบางประเด็น (ตารางที่ 4)

ตาราง 4

เปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรงดเว้นไม่ควรปฏิบัติจำแนกตามเพศ อายุ ระดับการศึกษา ตำแหน่งงาน ระยะเวลาในการทำงานของผู้ตอบแบบสอบถาม

ข้อ	ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ	เพศ	อายุ	ระดับการศึกษา	ตำแหน่งงาน	ระยะเวลาในการทำงาน
		t	F	F	F	F
1	ท่านให้ผู้อื่นใช้งานคอมพิวเตอร์ของบริษัทได้โดยไม่ได้รับอนุญาตจากหัวหน้างาน	.105	1.513	7.728*	4.794*	3.974*
2	ท่านให้ผู้อื่นใช้ชื่อบัญชี (username & password) ของท่านในการทำงาน	-.804	1.307	.653	.356	.516
3	ท่านมีโปรแกรมคอมพิวเตอร์อื่นนอกเหนือจากที่บริษัทกำหนดในเครื่องที่ท่านรับผิดชอบ	.818	3.882*	.920	4.420*	6.180*
4	ท่านเปลี่ยนแปลงอุปกรณ์คอมพิวเตอร์ที่ท่านรับผิดชอบด้วยตนเอง	1.686	2.496	.345	3.276*	1.893

ตาราง 4
เปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรงดเว้นไม่ควรปฏิบัติจำแนกตามเพศ อายุ ระดับการศึกษา ตำแหน่งงาน ระยะเวลาในการทำงานของผู้ตอบแบบสอบถาม (ต่อ)

ข้อ	ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ	เพศ	อายุ	ระดับการศึกษา	ตำแหน่งงาน	ระยะเวลาในการทำงาน
		t	F	F	F	F
5	ท่านติดตั้งหรือให้ผู้อื่นติดตั้งโปรแกรมที่ไม่มีลิขสิทธิ์บนเครื่องที่ท่านรับผิดชอบ	.034	2.722*	9.627*	7.263*	1.374
6	ท่านนำอุปกรณ์ส่วนตัวอื่น ๆ มาใช้กับระบบของบริษัท โดยไม่ได้รับการอนุมัติจากหัวหน้างาน	-1.290	.709	.398	1.201	5.911*
7	ท่านใช้คอมพิวเตอร์และระบบโครงข่ายเพื่อวัตถุประสงค์ทางการค้าส่วนตัว	2.204	.602	.031	.197	2.736
8	ท่านอ่านข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต	-.653	3.164*	.650	4.347*	1.325
9	ท่านแก้ไขข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต	2.204*	.602	1.326	.795	2.736
10	ท่านโหลดไฟล์ที่ไม่เกี่ยวกับงานในเวลางาน	-1.916	2.929*	.825	9.946*	1.546
11	ท่านใช้งานเว็บไซต์สังคมออนไลน์ เช่น Facebook Youtube หรืออื่น ๆ โดยไม่เกี่ยวกับการทำงานในระหว่างเวลางาน	.091	3.839*	6.011*	2.794	1.022
12	ท่านเล่นเกมผ่านทางอินเทอร์เน็ตของบริษัท	3.016*	1.104	5.662*	.482	.844
13	ท่านดูหนังผ่านทางอินเทอร์เน็ตของบริษัท	1.032	1.666	.289	2.535	.582
14	ท่านฟังเพลงผ่านทางอินเทอร์เน็ตของบริษัท	-.674	2.708*	.574	546	1.438
15	ท่านเปิดเผยข้อมูลที่มีความสำคัญต่อบริษัทให้แก่บุคคลอื่นโดยไม่ได้รับอนุญาต	1.536	.296	.650	.391	1.325
16	ท่านแสดงความคิดเห็นเกี่ยวกับการทำงานของบริษัทในเว็บไซต์หรือสื่อสังคมออนไลน์ต่าง ๆ ในลักษณะที่ก่อให้เกิดความเสียหาย	2.204*	.602	1.326	.795	2.736
17	ท่านเขียนหรือบันทึกรหัสลับ (password) ไว้ในสถานที่ที่ผู้อื่นสามารถพบเห็นได้ง่าย	-.428	1.420	.248	1.700	.417
18	ท่านส่งอีเมล์ให้บุคคลที่สามโดยไม่เกี่ยวข้องกับงาน	.162	.731	1.345	.227	.999
19	ท่านนำข้อมูลในอีเมล์ของบุคคลอื่นไปใช้โดยไม่ได้รับอนุญาต	0		n/a	n/a	n/a
20	ท่านใช้ชื่ออีเมล์ของบริษัทเพื่อลงทะเบียนในเว็บไซต์ต่าง ๆ	.142	1.332	5.992*	2.770	2.24
21	ท่านส่งอีเมล์ที่มีขนาดใหญ่กว่า 15 MB โดยไม่ได้แจ้งฝ่าย IT	-.964	3.482*	.84	.363	.239

ตาราง 4

เปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรงดเว้นไม่ควรปฏิบัติจำแนกตามเพศ อายุ ระดับการศึกษา ตำแหน่งงาน ระยะเวลาในการทำงานของผู้ตอบแบบสอบถาม (ต่อ)

ข้อ	ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ	เพศ	อายุ	ระดับการศึกษา	ตำแหน่งงาน	ระยะเวลาในการทำงาน
		t	F	F	F	F
22	ท่านเปิดไฟล์แนบในอีเมล์ที่ได้รับจากบุคคลที่ไม่รู้จัก	-1.178	.989	3.240*	.786	5.676*
23	ท่านทำสำเนาโปรแกรมที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต	3.029*	1.113	2.466	1.467	.905
24	ท่านเล่นเกมคอมพิวเตอร์ในระหว่างเวลาทำงาน	.495	1.383	.061	.947	7.574*

*การทดสอบด้วยสถิติ t และ F มีนัยสำคัญที่ $\alpha = 0.05$

ตาราง 5

เปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรยึดถือปฏิบัติจำแนกตามเพศ อายุ ระดับการศึกษา ตำแหน่งงาน ระยะเวลาในการทำงานของผู้ตอบแบบสอบถาม

ข้อ	ประเด็นที่ควรปฏิบัติตาม	เพศ	อายุ	ระดับการศึกษา	ตำแหน่งงาน	ระยะเวลาในการทำงาน
1	ท่านยอมรับข้อกำหนดเกี่ยวกับนโยบายรักษาความปลอดภัยของฝ่าย IT อย่างไม่มีเงื่อนไข	2.744*	2.562	5.255*	5.332*	.271
2	ท่านทราบนโยบายครบทุกข้อ	3.764*	5.218*	.635	5.580*	5.836*
3	ท่านแจ้งฝ่าย IT เมื่อพบว่ามีโปรแกรมที่ไม่มีลิขสิทธิ์บนเครื่องของท่าน	1.657	3.526*	.805	1.334	3.563*
4	ท่านเปลี่ยนรหัสลับทุก ๆ 60 วัน	-.376	1.583	.665	.214	3.140*
5	ท่านตรวจสอบชื่ออีเมล์ผู้รับอย่างระมัดระวังเสมอเพื่อป้องกันการส่งผิดพลาด	-.181	.352	4.675*	12.113*	7.255*

*การทดสอบด้วยสถิติ t และ F มีนัยสำคัญที่ $\alpha = 0.05$

ในทำนองเดียวกันในการศึกษาเปรียบเทียบความคิดเห็นเกี่ยวกับประเด็นที่ควรยึดถือปฏิบัติ พบว่า ผู้ตอบแบบสอบถามที่มีปัจจัยด้านประชากรศาสตร์ (เพศ อายุ ระดับการศึกษา ตำแหน่งงาน ระยะเวลาในการทำงาน) แตกต่างกัน มีความคิดเห็นเกี่ยวกับประเด็นที่ควรยึดถือปฏิบัติแตกต่างกันในบางประเด็น ทั้งนี้ที่ระดับนัยสำคัญทางสถิติ 0.05 (ตารางที่ 5)

การอภิปรายผล

ผลการวิจัยนี้สอดคล้องกับผลการศึกษาของ รัชชาภรณ์ สุภาพ และศักดิ์ชาย ตั้งวรรณวิทย์ (2014) ที่ทำการศึกษาองค์กรภาครัฐ พบว่าแม้องค์กรมีการประกาศใช้นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศแล้ว แต่ยังมีพนักงานบางส่วนที่ยังไม่ปฏิบัติตามนโยบายฯ

อย่างไรก็ตาม สัดส่วนของพนักงานที่ไม่ได้ปฏิบัติตามนโยบายฯ ในองค์กรภาครัฐมีสัดส่วนที่สูงกว่า

ทั้งนี้ การขับเคลื่อนนโยบายฯ ดังกล่าวให้สัมฤทธิ์ผล อาจจำเป็นต้องมีการสร้างความตระหนัก การรับรู้ถึงภัยคุมคาม การฝึกอบรมและให้ความรู้แก่พนักงานควบคู่ไปด้วย ดังผลการศึกษาของ สุพิชญา อาชวิรดา (2016) ที่รวบรวมข้อมูลจากพนักงานในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ซึ่งสรุปว่าเมื่อพนักงานเกิดความตระหนักแล้ว จะส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร ให้มีความมั่นคงปลอดภัยสูงขึ้น

ข้อเสนอแนะการวิจัยครั้งนี้

จากการศึกษา “การปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของพนักงานในระบบของบริษัทพัฒนาอสังหาริมทรัพย์รายหนึ่งนี้ ผู้ศึกษามีข้อเสนอแนะดังนี้

1. จากผลการศึกษาในส่วนของข้อมูลพื้นฐานของผู้ตอบแบบสอบถาม พบว่ามีพนักงานจำนวนเพียงร้อยละ 25 ที่มีการอ่านนโยบายความปลอดภัยอย่างครบถ้วน รวมถึงมีพนักงานบางส่วนที่ไม่เคยอ่านเลย ดังนั้น ผู้บริหารควรมีการสนับสนุน และส่งเสริมให้พนักงานทุกคนอ่านนโยบายให้ครบถ้วน เพื่อเป็นการป้องกันไม่ให้พนักงานกระทำการที่อาจก่อให้เกิดปัญหาเรื่องความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยรู้เท่าไม่ถึงการณ์ และเพื่อไม่ให้เกิดความเสียหายกับระบบของบริษัท โดยอาจเพิ่มเติมช่องทางการสื่อสาร เช่น ประกาศนโยบายผ่านทางเสียงตามสาย หรือ ประกาศในที่ประชุมพนักงาน และเนื่องจากนโยบายมีหลายข้อ พนักงานอาจรับรู้ได้ไม่หมดในคราวเดียว จึงอาจใช้วิธีการทยอยประกาศตามความเหมาะสม เป็นต้น

2. ผลการศึกษาในส่วนของการปฏิบัติตามนโยบายความปลอดภัย พบว่ามี 1 ข้อ ที่การงดเว้นควรหลีกเลี่ยงไม่ปฏิบัติ อยู่ในเกณฑ์ปานกลาง และ 1 ข้อมีการยึดถือปฏิบัติตาม อยู่ในเกณฑ์ เป็นส่วนใหญ่ ทางผู้บริหารจึงควรส่งเสริม หรือ หามาตรการ เพื่อเน้นให้พนักงานปฏิบัติตามนโยบายใน 2 ข้อดังกล่าว เพื่อให้เป็นไปตามนโยบายที่ได้กำหนดไว้อย่างมีประสิทธิภาพ

3. เนื่องจากนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ในระบบของบริษัทพัฒนาอสังหาริมทรัพย์รายหนึ่งนี้ มีการทบทวน และปรับปรุง เป็นประจำทุกปี ซึ่งในอนาคต นโยบายบางข้ออาจมีการเปลี่ยนแปลงตามสถานการณ์ของเทคโนโลยีขณะนั้น หรือ อาจมีการเพิ่มเติมข้อนโยบาย เพื่อให้ครอบคลุม การใช้งานระบบเทคโนโลยีให้ครอบคลุมมากยิ่งขึ้น ดังนั้น จึงควรมีการทำการสำรวจควบคู่กันไป เมื่อมีการปรับปรุงนโยบายใหม่ เพื่อให้แน่ใจว่า พนักงานทุกคนได้รับทราบนโยบายทุกข้อ

4. ผลการศึกษาพบว่า พนักงานส่วนใหญ่ปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศอยู่ในระดับมากที่สุด อย่างไรก็ตามเนื่องจากคำถามในแบบสอบถามเป็นคำถามเกี่ยวกับการปฏิบัติตามกฎระเบียบของบริษัท จึงอาจทำให้ผู้ตอบแบบสอบถามตอบแบบเข้าข้างตนเองได้ ดังนั้น ในการปฏิบัติงานจริงภายในบริษัท ควรใช้ระบบตรวจสอบเพิ่มเติม เพื่อยืนยันว่าพนักงานส่วนใหญ่ปฏิบัติตามนโยบายจริง ๆ เช่น ใช้ระบบคอมพิวเตอร์เพื่อตรวจสอบการ ใช้งานของผู้ตอบแบบสอบถาม ประวัติการเข้าใช้งานเว็บไซต์ หรือ ตรวจสอบว่ามีพนักงานที่ส่งอีเมล์ขนาดใหญ่กว่า 15 MB มากน้อยเพียงใด

ข้อเสนอแนะการวิจัยครั้งต่อไป

ควรทำการศึกษาถึงการรับรู้และความตระหนักของพนักงานเกี่ยวกับประเภทและความร้ายแรงของภัยคุกคามที่มีมากับเทคโนโลยีสารสนเทศ

References

Airdum, P. (2006). *Adoption of information technology of civil servants of office of the permanent secretary, ministry of energy. special problem*. Master of Public Administration (General Management) Thesis, Burapha University. (in Thai)

Archavajirada, S. (2016). Factors affecting the security level of information systems in organization. *Journal of information systems in Business*, *2*(2), 67-79. (in Thai)

Foster, G. (1973). *Traditional societies and technological change*. New York: Harper & Row.

Gibson, D. (2011). *Understanding the security triad (confidentiality, integrity, and availability)*. Retrieved from www.pearsonitcertification.com/articles/article.aspx?p=1708668

Groti, L. (2005). *Use of internet to access information sources by faculties and students of Suranaree university of technology*, *Nakhon Ratchasima.* Nakhon Ratchasima: Suranaree University of Technology Intellectual Repository. (in Thai)

Jaroenpuntaruk, V. (2006). *The development of the e-learning lesson for distant learning*. Nonthaburi: Sukhothai Thammathirat Open University. (in Thai)

Legislative Institutional Repository of Thailand. (1992). *Regulations of the office of the prime minister on information technology promotion and development B.E. 2535*. Retrieved from http://dl.parliament.go.th/handle/lirt/86309 (in Thai)

Rogers, E. (1968). *Diffusion of innovation.* New York: The Free.

Rogers, E., & Shoemaker, F. (1971). *Communication of innovation*. New York: The Free.

Subrungruang, P. (2004). *Security of your computer.* Bangkok: Provision. (in Thai)

Sukchuen, S. (1997). *Implementation of the national information technology policy: A case study of the office of the civil service commission*. Master of Political Science Thesis, Ramkhamhaeng University. (in Thai)

Suphap, R., & Tangwannawit, S. (2014). The guidance for security operation of information technology using ISO/IEC 27001 standard: A case study of electronic government agency (Public Organization). *The 10th National Conference on Computing and Information Technology*, Bangkok. (in Thai)

Yamane, T. (1973). *Statistics: An introductory analysis*. New York: Harper and Row.

U.S. Government's National Information Assurance. (2006). *CNSS instruction 4009, Revised June 2006*. Retrieved from http://www.cnss.gov/asset/pdf/cnssi_4009.pdf