นโยบายการบริหารจัดการความมั่นคงและความปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ที่มีประสิทธิภาพที่ส่งผลต่อการทำงานงานที่มีประสิทธิผลของพนักงาน ของ บริษัท บัตรกรุงไทย จำกัด (มหาชน)

Information security and security management policy in accordance with ISO 27001 that effectively affects the effective work of employees of Krungthai Card Public Company Limited.

นางสาวทัศนีย์ คลองมีคุณ
สาขาบริหารธุรกิจ คณะบริหารธุรกิจ มหาวิทยาลัยราคำแหงประเทศไทย
คณะบริหารธุรกิจ มหาวิทยาลัยราคำแหงประเทศไทย
ผู้รับผิดชอบบทความ

Thatsanee Kongmeekun
Email: Thatsanee_ple@hotmail.com
Major: Business ,Facuty of Business Administraion
Ramkhamhaeng University, Thailand.
Corresponding author

นางสาวทัศนีย์ คลองมีคุณ

บทคัดย่อ

ในยุคที่ข้อมูลข่าวสารมีความสำคัญ ทางองค์กรจึงให้ความสำคัญในการนาเอาแนวคิดด้านการจัดการความมั่นคงปลอดภัยสารสนเทศมาประยุกต์ใช้ โดยบรรจุอยู่ในแผนแม่บทเทคโนโลยีสารสนเทศและการ ซึ่งเป็นแผนเฉพาะด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งขณะนี้อยู่ในระหว่างการดาเนินการ เพื่อให้องค์กรมีแผนในการบริหารจัดการระบบสารสนเทศขององค์กร โดยเน้นการรักษาความปลอดภัยของข้อมูลขององค์กร ซึ่งถือเป็นส่วนสำคัญส่วนหนึ่งในการบริหารหน่วยงานให้มีประสิทธิภาพ และเพื่อให้มีความมั่นคงปลอดภัยเป็นไปตามประกาศของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และพระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 โดยได้มีการนาเอามาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรฐานสากลด้าน Information Security Management System มาเป็นกรอบในการดาเนินงาน ประกอบกับ องค์กรแห่งนี้ จะต้องดาเนินการด้านสารสนเทศให้สอดคล้องกับระบบประเมินคุณภาพรัฐวิสาหกิจ จึงมีความจาเป็นในการดำเนินการด้านการจัดการความมั่นคงปลอดภัยสารสนเทศให้เป็นไปอย่างต่อเนื่องตามมาตรฐานสากล

คำสำคัญ : นโยบายการบริหาร,ความมั่นคงและปลอดภัยตามมาตราฐาน ISO 27001

ABSTRACT

In an age where information is important, the organization wishes to be important in dealing with information technology security and security. Information applied Which is included in the information technology master plan and Which is a specific plan for information technology of the organization Which is currently under the process of The organization has a plan for managing the information system of the organization. By focusing on the security of the organization's information Which is considered an important part in managing the department to be effective And in order to have Security is in accordance with the announcement of the Electronic Transactions Commission. On the policy guidelines and guidelines for securing information security of government agencies in 2010 and the Royal Decree On safe methods in electronic transactions 2010, with the introduction of n safe methods in electronic transactions 2010, with the introduction of ISO / IEC 27001, an international standard for Information Security Management System, as a framework for operating with this organization. Must carry out information technology in accordance with the state enterprise quality assessment system Therefore, it is necessary to proceed with the information security management to be in accordance with international standards.

Keywords : Management policy, Security and safety according to ISO 27001

บทนำ

ความเป็นมาและที่มาของปัญหา

บริษัท บัตรกรุงไทย จำกัด (มหาชน) เป็นบริษัทมหาชนที่ประกอบธุรกิจประเภท สินเชื่อเพื่อผู้บริโภค ประกอบธุรกิจบัตรเครดิตตลอดจนธุรกิจที่เกี่ยวเนื่องกับธุรกิจบัตรเครดิต, ธุรกิจสินเชื่อส่วนบุคคล (Personal Loan) ธุรกิจบริการรับชำระค่าสาธารณูปโภค ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ประเภทการให้บริการบัตรเครดิต การให้บริการแก่ผู้รับบัตรและให้บริการรับชำระเงินแทน ซึ่งในยุคที่ข้อมูลข่าวสารมีความสำคัญ ทางองค์กรจึงให้ความสำคัญในการนำเอาแนวคิด ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศมาประยุกต์ใช้ โดยบรรจุอยู่ในแผนแม่บทเทคโนโลยี สารสนเทศและการ ซึ่งเป็นแผนเฉพาะด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งขณะนี้อยู่ในระหว่าง การดำเนินการ เพื่อให้องค์กรมีแผนในการบริหารจัดการระบบสารสนเทศขององค์กรโดยเน้นการ รักษาความปลอดภัยของข้อมูลขององค์กร ซึ่งถือเป็นส่วน

สำคัญส่วนหนึ่งในการบริหารหน่วยงานให้มี ประสิทธิภาพ และเพื่อให้มีความมั่นคงปลอดภัยเป็นไปตามประกาศของคณะกรรมการธุรกรรม อิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยได้มีการนำเอามาตรฐาน ISO 27001 ซึ่งเป็นมาตรฐานสากล ด้าน Information Security Management System มาเป็นกรอบในการดำเนินงานประกอบกับ บริษัท บัตรกรุงไทย จำกัด (มหาชน) จะต้องดำเนินการด้านสารสนเทศให้สอดคล้องกับระบบประเมินคุณภาพ ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศให้เป็นไปอย่าง ต่อเนื่องตามมาตรฐานสากล

ดังนั้น เพื่อให้มั่นใจว่าองค์กรมีการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่เหมาะสม การตรวจสอบภายในเป็นเครื่องมือหรือผู้ช่วยที่สำคัญในการสร้างความเชื่อมั่นให้กับผู้บริหาร โดยการตรวจสอบประเมินประสิทธิภาพและประสิทธิผลการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ผู้วิจัยซึ่งปฏิบัติงานอยู่ในสายงานตรวจสอบภายในขององค์กรจึงมีแนวคิดที่จะจัดทำแนวทาง การตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยอิงตามมาตรฐาน ISO 27001 เพื่อให้ผู้ตรวจสอบภายในที่ส่วนใหญ่ไม่มีพื้นฐานทางด้านเทคโนโลยีสารสนเทศมีแนวทางการตรวจสอบ ระบบเทคโนโลยีสารสนเทศที่เป็นมาตรฐานสากลและเหมาะสมกับองค์กร รวมทั้ง การที่ ผู้ตรวจสอบภายในปฏิบัติงานตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยใช้แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศที่สอดคล้องตามมาตรฐาน ISO 27001 จะส่งผลให้ข้อมูลสารสนเทศขององค์กรมีความมั่นคงปลอดภัยยิ่งขึ้น เนื่องจากผู้บริหาร พนักงานทั่วไป และพนักงานด้านเทคโนโลยีสารสนเทศมีความตระหนักรู้ และธำรงรักษาการปฏิบัติงานให้สอดคล้องเป็นไปตามมาตรฐาน ISO 27001

วัตถุประสงค์

1.ปัจจัยส่วนบุคคลที่แตกต่างกันมีผลต่อความพอใจในการปฏิบัติงานตามนโยบายการบริหารจัดการความมั่งคงและความปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ของพนักงาน บริษัท บัตรกรุงไทย จำกัด (มหาชน)

2.เพื่อศึกษานโยบายการบริหารจัดการ มีผลต่อความพอใจในการปฏิบัติงานตามนโยบายการบริหารจัดการความมั่งคงและความปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ของพนักงาน บริษัท บัตรกรุงไทย จำกัด (มหาชน)

ขอบเขตงานวิจัย

- **ขอบเขตด้านประชากร**

ประชากรที่ทำการศึกษาในครั้งนี้เป็นพนักงานของ บริษัท บัตรกรุงไทย จำกัด (มหาชน) จำนวน 410 คน โดยเก็บข้อมูลประชากรในการตอบแบบสอบถาม

- **ขอบเขตด้านเนื้อหา**

การศึกษาครั้งนี้เป็นการศึกษานโยบายการบริหารจัดการด้านการความมั่นคงและความปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ที่มีประสิทธิภาพส่งผลให้การทำงานของพนักงาน บริษัท บัตรกรุงไทย จำกัด (มหาชน) ได้อย่างมีประสิทธิผล

1.ตัวแปรอิสระ ปัจจัยส่วนบุคคล นโยบายผู้บริหารระดับสูง บริษัท บัตรกรุงไทย จำกัด (มหาชน)

2. ตัวแปรตาม ความพอใจในการปฏิบัติงานตามนโยบายการบริหารจัดการความมั่งคงและความปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ของพนักงาน บริษัท บัตรกรุงไทย จำกัด (มหาชน)

สมมติฐานของการวิจัย

1.ปัจจัยส่วนบุคคลที่แตกต่างกันจะมีผลต่อการปฏิบัติงานตามนโยบายของผู้บริหารระดับสูงที่แตกต่างกัน

2.นโยบายการบริหารจัดการมีผลความพอใจในการปฏิบัติงานตามนโยบายการบริหารจัดการความมั่งคงและความปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ของพนักงาน บริษัท บัตรกรุงไทย จำกัด (มหาชน))

ประโยชน์ที่คาดว่าจะได้รับ

1.ทราบปัจจัยส่วนบุคคลที่แตกต่างกันจะมีผลต่อการปฏิบัติงานตามนโยบายของผู้บริหารระดับสูง

2.ทราบนโยบายการบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตราฐาน ISO 27001 ที่มีประสทธิภาพมีความสัมพันธ์กับประสิทธิผลการทำงาน ของ พนักงานบริษัท บัตรกรุงไทย จำกัด (มหาชน)

3.ทราบถึงขอกำหนดและข้อปฏิบัติให้เป็นไปตามมาตราฐานความมั่นคงปลอดภัยตามมาตราฐาน ISO 27001

การทบทวนวรรณกรรม

เมื่อกล่าวถึงคำว่า การบริหารส่วนใหญ่มักจะนึกถึงการบริหารราชการคำศัพท์ที่ใช้มี 2 คำ คือ การบริหาร (Administration) นิยมใช้กับการบริหารราชการหรือการจัดการเกี่ยวกับนโยบาย และการจัดการ (Management) นิยมใช้กับการบริหารธุรกิจเอกชนหรือการดำเนินการตามนโยบายที่กำหนดไว้ อย่างไรก็ตามคำว่า การบริหารกับคำว่า การจัดการใช้แทนกันได้ ซึ่งมีมีองค์ประกอบที่สำคัญดังต่อไปนี้

1. คนหรือบุคคล (Man) เป็นปัจจัยสำคัญของการบริหารงาน หน่วยงานหรือองค์การต่าง ๆ จำเป็นต้องมีคนที่ปฏิบัติงาน ผลงานที่ดีจะออกมาได้ต้องประกอบด้วยบุคคลที่มีคุณภาพและมีความรับผิดชอบต่อองค์การหรือหน่วยงานนั้น ๆ

2. เงิน (Money) หน่วยงานจำเป็นที่จะต้องมีงบประมาณเพื่อการบริหารงานหากขาดงบประมาณการบริหารงานของหน่วยงานก็ยากที่จะบรรลุเป้าหมาย

3. ทรัพยากรหรือวัตถุ (Material) การบริหารจำเป็นต้องมีวัสดุอุปกรณ์หรือทรัพยากรในการบริหาร หากหน่วยงานขาดวัสดุอุปกรณ์หรือทรัพยากรในการบริหารแล้วก็ย่อมจะเป็นอุปสรรคหรือก็ให้เกิดปัญหาในการบริหารงาน

4. การบริหารจัดการ (Management) เป็นภารกิจของผู้บริหารหรือผู้บังคับบัญชาโดยตรงคือเป็นกลไกและตัวประสานที่สำคัญที่สุดในการประมวลผลักดันและกำกับปัจจัยต่าง ๆ ทั้ง

สรุปว่า การบริหารเป็นการดำเนินการที่ผู้บริหารมีหน้าที่ในการสั่งการในการบริหารจัดการควบคุมและนำแผนที่กำหนดไว้ไปดำเนินการให้แล้วเสร็จ ศิริวรรณ เสรีรัตน์ และคณะ (2545, หน้า 18 -19) ได้รวบรวม ความหมายของคำว่า

การบริหาร (Administration) จะใช้ในการบริหารระดับสูงโดยเน้นที่การกำหนดนโยบายที่สำคัญและการกำหนดแผนของผู้บริหารระดับสูงเป็นค านิยมใช้ในการบริหารรัฐกิจ (Public Administration) หรือใช้ในหน่วยงานราชการและคำว่า

“ผู้บริหาร” (Administrator) จะหมายถึง ผู้บริหารที่ทำงานอยู่ในองค์กรของรัฐหรือองค์กรที่ไม่มุ่งหวังกำไร (Schermerhorn, 1999, p. G -2)

การบริหาร คือกลุ่มของกิจกรรม ประกอบด้วย การวางแผน (Planning) การจัดองค์กร (Organizing) การสั่งการ (Leading/ Directing) หรืออำนวยการ และการควบคุม (Controlling) ซึ่งจะมีความสัมพันธ์โดยตรงกับทรัพยากรขององค์กร (6M's) เพื่อนำไปใช้ให้เกิดประโยชน์และด้วยจุดมุ่งหมายสำคัญในการบรรลุความสำเร็จตามเป้าหมายขององค์กรอย่างมีประสิทธิภาพและเกิดประสิทธิผลครบถ้วน

มาตรฐาน ISO 27001 เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศที่พัฒนา โดยองค์กรสากล ISO (International Organization for Standardization) ซึ่งได้รับการยอมรับในระดับนานาชาติ เป็นมาตรฐานที่ใช้อ้างอิงกฎหมายด้านไอซีทีของประเทศ ที่มีผลบังคับใช้กับหน่วยงานต่าง ๆ อาทิ พระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 พระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 โดยเวอร์ชั่นล่าสุด คือ ISO 27001 : 2013 ประกาศใช้เมื่อวันที่ 1 ตุลาคม 2556 เป็นมาตรฐานสากลที่ได้กำหนดแนวทางดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) เพื่อสร้างความมั่นคงปลอดภัยให้กับ ระบบสารสนเทศของหน่วยงาน โดยมีกระบวนการบริหารจัดการสารสนเทศที่มีความสำคัญ ขององค์กรให้มีความมั่นคงปลอดภัยตามหลัก C I A (Confidentiality , Integrity , Availability) ซึ่งมีแนวทางการปฏิบัติตามขั้นตอนของกระบวนการดังนี้ เริ่มตั้งแต่ทำการวิเคราะห์และประเมินความเสี่ยงเพื่อทำให้ทราบว่าสารสนเทศใดที่มีความสำคัญต่อการดำเนินธุรกิจขององค์กร โอกาสที่จะเกิดความเสี่ยงและความเสียหายอันส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร จากภัยคุกคามทั้งภายในภายนอกกับสารสนเทศนั้นมากน้อยแค่ไหน มีวิธีการบริหารจัดการ ในการป้องกันความเสี่ยงดังกล่าวอย่างไร โดยจำเป็นต้องจัดลำดับความสำคัญของความเสี่ยงทั้งหมดที่พบ และพิจารณาว่าสิ่งใดจำเป็นต้องรีบบริหารจัดการก่อนและหลัง จากนั้นจึงดำเนินการตามวงจร P (Plan หรือการวางแผน) D (Do หรือการประยุกต์ใช้หรือการดำเนินการ) C (Check หรือการตรวจสอบ) A (Action หรือการบำรุงรักษาหรือการปรับปรุง) โดยเริ่มจากทำการออกแบบระบบบริหารจัดการ ซึ่งในที่นี้หมายถึงกระบวนการที่เปรียบเสมือนเป็นเครื่องมือในการรักษา ความมั่นคงปลอดภัย แต่ไม่ได้หมายรวมเพียงแค่การนำระบบเทคโนโลยีสารสนเทศมาสนับสนุน

น้าหนึ่ง กล้าหาญ (2555) ได้พัฒนาโปรแกรมประยุกต์สำหรับการประเมินความมั่นคง ปลอดภัยสารสนเทศในองค์กรปกครองส่วนท้องถิ่นในจังหวัดสุพรรณบุรี โดยอิงมาตรฐาน ISO/IEC 27001 พบว่า มีความพร้อมอยู่ในระดั บปานกลางทุกด้าน ทั้งนี้เป็นเพราะมีแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Security Policy) ที่ยังไม่ชัดเจน ซึ่งเป็นสิ่งแรกที่สำคัญและจำ เป็นสำ หรับองค์ กรที่ต้องมีเพื่อเป็นแนวทาง และสนับสนุนการรักษา ความมั่นคงปลอดภัยสารสนเทศในหน่วยงานหรือองค์กร ดังนั้นการกำหนดบทบาทขององค์กรและ บุคลากรในภาพรวมตามลำดับ คือ ผู้ นำ/ผู้บริหาร หัวหน้าหน่วยงาน และบุคลากรผู้ปฏิบัติงาน ดังนี้

1. ผู้บริหาร แสดงเจตจำนงต่อการสร้างความมั่นคงปลอดภัยสารสนเทศให้เกิดภายในองค์กร สนับสนุนการประกาศนโยบายความมั่นคงปลอดภัยสารสนเทศ เป็นต้นแบบและเสริมสร้างวัฒนธรรมแห่ง

ความมั่นคงปลอดภัยระบบสารสนเทศ การร่วมจัดทำกลยุทธ์กับบุคลากรระดับอื่นและสื่อสารชัดเจนสู่ทุกหน่วยงาน

2. หัวหน้าหน่วยงาน ช่วยสื่อสารให้ความรู้แก่ผู้ปฏิบัติ ติดตามการปฏิบัติตามนโยบาย มีการรายงานผลการดำเนินงาน สร้างบรรยากาศในการเรียนรู้

3. ผู้ปฏิบัติ ยอมรับและปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ และร่วมสร้างบรรยากาศความมั่นคงปลอดภัยให้ยั่งยืน

วิธีดำเนินการวิจัย

การวิจัยในครั้งนี้เป็นการวิจัยเชิงสำรวจ (survey research) มีวัตถุประสงค์การศึกษานโยบายการบริหารจัดการด้านการความมั่นคงและความ ปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ที่มีประสิทธิภาพส่งผลให้การทำงานของพนักงาน บริษัท บัตรกรุงไทย จำกัด (มหาชน)

ประชากรที่ใช้ในการวิจัย

ประชากรที่ใช้ในการวิจัยครั้งนี้ คือ เป็นพนักงานของ บริษัท บัตรกรุงไทย จำกัด (มหาชน) จำนวน 410 คน

กลุ่มตัวอย่างที่ใช้ในการวิจัย

กลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ ขนาดของตัวอย่างโดยจะเก็บข้อมูลใช้วิธีการคำนวณจากสูตร Taro Yamane ที่ระดับความเชื่อมั่น 95% และสัดส่วนความคลาดเคลื่อน 0.05 ได้ขนาดกลุ่มตัวอย่างจำนวน 398 คน และสำรองเผื่อความผิดพลาด 2 คน รวมกลุ่มตัวอย่างที่จะเก็บข้อมูลทั้งสิ้น 400 คน

สถิติที่ใช้วิเคราะห์ข้อมูล

สถิติที่ใช้ในการวิเคราะห์ข้อมูลสำหรับการศึกษาในครั้งนี้สามารถจำแนกออกตามแนวทางการวิเคราะห์ได้ 2 กลุ่ม ดังนี้

การวิเคราะห์เชิงพรรณนา ค่าร้อยละ (Percentage) ใช้บรรยายคุณลักษณะระชากรศาสตร์ ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

การทดสอบสมมติฐาน Independent Sample Test (t-Test) ใช้ทดสอบความแตกต่างระหว่างเพศกับการตัดสินใจเลือกซื้อสมาร์ทโฟนเป็นโทรศัพท์เครื่องที่สองของผู้บริโภคในเขตกรุงเทพมหานคร One-Way ANOVA (F-Test) และทำการเปรียบความแตกต่างแบบรายคู่ตามวิธี Scheffe สำหรับลักษณะ

ประชากรศาสตร์ที่มีความแตกต่าง และ สถิติค่าสัมประสิทธิ์ สหสัมพันธ์แบบเพียร์สัน (Pearson Correlation) เพื่อใช้วัดความสัมพันธ์ของตัวแปร

ผลการวิจัย

ผู้ตอบแบบสอบถามทั้งหมดจำนวน 400 คน ส่วนใหญ่เป็นเพศหญิง จำนวน 225 คน และเพศชาย จำนวน 175 คน คิดเป็นร้อยละ 56.3 และ 43.8 ตามลำดับ ซึ่งเป็นพนักงาน จำนวน 336 คน และผู้บริหาร จำนวน 64 คน โดยคิดเป็นร้อยละ 84.0 และ 16.0 ตามลำดับ ส่วนใหญ่มีอายุเฉลี่ยอยู่ที่ 30 – 39 ปี คิดเป็นร้อยละ 54.8 รองลงมา คือ 40 – 49 ปี, 50 – 59 ปี และ 20 – 29 ปี โดยคิดเป็นร้อยละ 22.3, 13.0 และ 10.0 ตามลำดับ โดยส่วนใหญ่มีรายได้ ประมาณ 10,001 – 20,000 บาท จำนวน 206 คน คิดเป็นร้อยละ 51.5 รองลงมาคือมีรายได้ 20,001 – 30,000 บาท, 10,000 บาทหรือน้อยกว่า, 30,001 – 40,000 บาท และ 40,001 – 50,000 บาท คิดเป็น ร้อยละ 27.3, 14.8, 3.5, 3.0 ตามลำดับ ซึ่งส่วนใหญ่จบการศึกษาระดับปริญญาตรี จำนวน 179 รองลงมาน้อยกว่าปริญญาตรี จำนวน 161 และมากกว่าปริญญาตรี จำนวน 60 คน โดยคิดเป็นร้อยละ 44.8, 40.3 และ 15.0 ตามลำดับ

ผลการศึกษาและการวิเคราะห์ตัวแปรอิสระ พบว่า ปัจจัยทางด้านนโยบายผู้บริหารระดับสูง บริษัท บัตรกรุงไทย จำกัด (มหาชน) โดยภาพรวมมีค่าเฉลี่ยอยู่ที่ 4.43 ซึ่งอยู่ในระดับมากที่สุด เมื่อพิจารณาเป็นรายข้อพบว่า ค่าเฉลี่ยสูงสุด คือ มีการควบคุมการเข้าออกห้องสารสนเทศและการสื่อสาร คิดเป็น 4.36 รองลงมา คือ มีขั้นตอนการบริหารจัดการการเปลี่ยนแปลง ซึ่งเท่ากันกับ มีขั้นตอนปฏิบัติในการเข้าถึงสารสนเทศของหน่วยงาน และมีการกำหนด แนวทางการจัดหา การพัฒนา และการบำรุงรักษาระบบ คือ 4.35, มีการควบคุมการเข้าถึงระบบสารสนเทศ และระบบเครือข่าย คิดเป็น 4.34, มีนโยบายการใช้มาตรการเข้ารหัสข้อมูล ซึ่งเท่ากันกับการสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดให้แก่พนักงาน และมีการการจัดทำบัญชีทรัพย์สิน คิดเป็นค่าเฉลี่ย 4.32, มีการเผยแพร่นโยบายความมั่นคงปลอดภัยของหน่วยงาน คิดเป็น 4.29 และมีการกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย คิดเป็นค่าเฉลี่ย 4.28 โดยนโยบายผู้บริหารระดับสูงแต่ละข้อมีการแปลผลอยู่ในระดับมากที่สุด ด้านนโยบายการบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตราฐาน ISO 27001 ที่มีประสิทธิภาพมีความสัมพันธ์กับประสิทธิผลการทำงาน ของ พนักงานบริษัท บัตรกรุงไทย จำกัด (มหาชน) (ต่อ) โดยภาพรวมมีค่าเฉลี่ยอยู่ที่ 4.45 ซึ่งอยู่ในระดับมากที่สุด เมื่อพิจารณาเป็นรายข้อพบว่า ค่าเฉลี่ยสูงสุด คือ มาตรการที่ 5 และมาตรการที่ 6 โดยคิดเป็น 4.42 รองลงมา คือ มาตรการที่ 4 ซึ่งเท่ากันกับมาตรการที่ 8 และ 10 มีค่าเฉลี่ยอยู่ที่ 4.41 ในส่วนมาตรการที่ 2,

3, 7 และ 9 มีค่าเฉลี่ยอยู่ที่ 4.38 และมาตรการที่ 1 มีค่าเฉลี่ยอยู่ที่ 4.35 โดยนโยบายผู้บริหารระดับสูงแต่ละข้อมีการแปลผลอยู่ในระดับมากที่สุด

ผลการทดสอบสมมติฐาน พบวา ปัจจัยด้านเพศ อายุ และตำแหน่งงานไม่มีความสัมพันธ์กับการปฏิบัติงานตามนโยบายผู้บริหารระดับสูง บริษัท บัตรกรุงไทย จำกัด (มหาชน) อย่างมีนัยสำคัญทางสถิติที่ 0.05 ระดับการศึกษา และรายได้เฉลี่ยครัวเรือนมีความสัมพันธ์กับการปฏิบัติงานตามนโยบายผู้บริหารระดับสูง บริษัท บัตรกรุงไทย จำกัด (มหาชน) อย่างมีนัยสำคัญทางสถิติที่ 0.05

การอภิปรายผลการวิจัย

การศึกษาวิจัยเรื่อง “นโยบายการบริหารจัดการความมั่นคงและความปลอดภัยด้านสารสนเทศตามมาตรฐาน ISO 27001 ที่มีประสิทธิภาพที่ส่งผลต่อการทำงานงานที่มีประสิทธิผลของพนักงานของบริษัท บัตรกรุงไทย จำกัด (มหาชน)” ขอสรุปการอภิปรายผลดังต่อไปนี้

ปัจจัยส่วนบุคคลที่แตกต่างกันจะมีผลต่อการปฏิบัติงานตามนโยบายของผู้บริหารระดับสูงที่แตกต่างกัน จากการศึกษาพบว่า ปัจจัยทางด้านประชากรศาสตร์ ประกอบด้วย ระดับการศึกษา และรายได้เฉลี่ยครัวเรือนมีอิทธิพลต่อการปฏิบัติงานตามนโยบายผู้บริหารระดับสูง บริษัท บัตรกรุงไทย จำกัด (มหาชน) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยพิจารณาจากค่า p – value ที่น้อยกว่า 0.05 ซึ่งขัดแย้งกับผลการศึกษาของ วรรณดี (2545) ที่ศึกษาเรื่อง ปัจจัยที่มีอิทธิพลต่อความมีประสิทธิผลในการปฏิบัติงานของเจ้าหน้าที่ตรวจสอบภายในกระทรวงศึกษาธิการ พบว่า ลักษณะส่วนบุคคลซึ่งได้แก่ เพศ อายุ ระดับการศึกษา อัตราเงินเดือน สถานภาพสมรส หน้าที่ปัจจุบัน และระยะเวลาในการทำงานในหน้าที่ปัจจุบันแตกต่างกัน ไม่มีผลต่อปัจจัยที่มีอิทธิพลพลต่อความมีประสิทธิผลในการปฏิบัติงานของเจ้าหน้าที่ตรวจสอบภายในกระทรวงศึกษาธิการ และยังขัดแย้งกับผลการศึกษาของ อารวย ดีเลิศ (2548) ที่ศึกษาประสิทธิผลในการปฏิบัติงานของพนักงานตรวจสอบภายในธนาคารเพื่อการเกษตรและสหกรณ์ พบว่า การวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยส่วนบุคคลกับประสิทธิผลในการปฏิบัติงานของพนกังานตรวจสอบภายในโดยรวมพบว่า เพศ อายุ ระดับการศึกษา วุฒิการศึกษาที่สำเร็จ และทักษะในการใช้เทคโนโลยีสารสนเทศ ไม่มีความสัมพันธ์กับประสิทธิผลในการปฏิบัติงาน ทั้งนี้เหตุที่ผลการศึกษาของผู้ศึกษาวิจัยไม่สอดคล้องกับผลการศึกษาที่ได้กล่าวมาแล้วข้างต้น อาจเนื่องมาจากบริบทภายในองค์กร รวมผลกฎระเบียนและข้อบังคับที่แตกต่างกันจึงส่งผลต่อผลการวิจัยที่แตกต่างกันดังกล่าว

นโยบายการบริหารจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 ที่มีประสิทธิภาพมีความสัมพันธ์กับประสิทธิผลการทำงานของพนักงานบริษัท บัตรกรุงไทย จำกัด (มหาชน) โดยจากการสอบถามและการวิเคราะห์พบว่า

ด้านนโยบายผู้บริหารระดับสูง ในเรื่องมีการควบคุมการเข้าออกห้องสารสนเทศและการสื่อสารได้รับมีค่าเฉลี่ยสูงสุด ซึ่งสะท้อนให้เห็นว่าผู้ปฏิบัติงานมีความตระหนักในเรื่องของบุคคลที่ควรเข้าถึงข้อมูลของบริษัท ซึ่งยังสอดคล้องไปถึงนโยบายการบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตราฐาน ISO 27001 ตามมาตรการที่ 5 การสร้างความมั่นคงปลอดภัย ทางกายภาพและสิ่งแวดล้อม ตามผลการวิเคราะห์

กล่าวโดยสรุป คือ ประสิทธิภาพการปฏิบัติงานตามนโยบายของพนักงานตามผลการศึกษาขึ้นอยู่กับระดับการศึกษา และรายได้เฉลี่ยต่อเดือน และนโยบายที่พนักงานในบริษัทตระหนักถึงที่สุด คือในด้านการจำกัดคนในการเข้าถึงข้อมูล เพื่อสร้างความมั่นคงปลอดภัย ทางกายภาพและสิ่งแวดล้อมในบริษัทของตนเอง

ข้อเสนอแนะ

หน่วยงานหรือบุคคลที่เกี่ยวข้องสามารถนำผลการวิจัยไปศึกษา ต่อยอดหรือนำไปปรับใช้ในภาคธุรกิจของตนเองได้

ข้อเสนอแนะในการทำวิจัยครั้งถัดไป

1. ควรศึกษาปัจจัยด้านอื่นๆ เพิ่มเติม นอกเหนือจากการศึกษาของผู้วิจัย เพื่อความครอบลคลุมของงานวิจัย

2. ควรมีการศึกษาพื้นที่อื่นๆ เพื่อเปรียบเทียบความเหมือนและความแตกต่างของผลการศึกษา

บรรณานุกรม

Ahmed Riad. (2015). **ISO/IEC 27001 : 2013.** 22/11/2017, website: https://www.linkedin.com/pulse/newest-integrated-model-isoiec-270012013-iso-223012012-

Best, John W. (1977). **Research in Education.** 3rd ed. Englewood Cliffs, NJ: Prentice-Hall.

Pavol Sojčí. (2012). **Tools for information security management.** website: http://is.muni.cz/

th/359439/fi_b/Sojcik_-Tools_for_information_security_management.pdf-->Sojcik_-_Tools_for_information _security_management

JOŽE ŠREKL and ANDREJKA PODBREGAR. (2014). **ENHANCING SAFETY INFORMATION SYSTEMS WITH THE USE ISO/IEC 27000.** doi: 10.7562/SE2014.4.01.03 Sarah Vonnegut. (2016). **Confidentiality Integrity Availability.** 22/11/2017, website: https://www.checkmarx.com/2016/06/24/20160624the-importance-of- database- security-and-integrity

ณัทรัฏฐ์ มณีรัสยากร. (2559). **การพัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001 ขององค์กรกรณีศึกษา บจก. เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น.** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

ธิดา ลิ่มทองวิรัตน์. (2553). **การประเมินประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO 27001 : กรณีศึกษาบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน).** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยหอการค้าไทย.

น้ำหนึ่ง กล้าหาญ. (2555). **โปรแกรมประยุกต์สำหรับการประเมินความมั่นคงปลอดภัยสารสนเทศในองค์กรปกครองส่วนท้องถิ่นในจังหวัดสุพรรณบุรี.** สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม.