การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน

Compliance to IT Security Policy of Employee

อนุชิต ศรีทิพย์
สาขาการจัดการอุตสาหกรรม คณะบริหารธุรกิจ มหาวิทยาลัยรามคำแหง ประเทศไทย
ผู้รับผิดชอบบทความ

Anuchyd Srithip
Industrial Management, Faculty of Business Administration, Ramkhamhaeng University, Thailand
Corresponding author

บทคัดย่อ

การศึกษา การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน เป็นการวิจัยเชิงสำรวจ (Survey Research) โดยใช้แบบสอบถามเป็นเครื่องมือในการรวบรวมข้อมูล มีวัตถุประสงค์เพื่อศึกษาเปรียบเทียบการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานจำแนกตามปัจจัยด้านประชากรศาสตร์ และศึกษาการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานในสิ่งที่ควรปฏิบัติ และในส่วนที่ควรหลีกเลี่ยงไม่ปฏิบัติ กลุ่มตัวอย่างที่ใช้ศึกษาวิจัยครั้งนี้ ได้แก่ พนักงานของ บริษัท ดี.ที.ซี.เอ็นเตอร์ไพรส์ จำกัด จำนวน 200 คน จากนั้นนำข้อมูลที่ได้มาทำการวิเคราะห์เชิงสถิติ

ผลการศึกษาในด้านปัจจัยส่วนบุคคล โดยใช้สถิติการวิเคราะห์ข้อมูลใช้สถิติความถี่ ร้อยละ ค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐาน การทดสอบค่าที (T-Test) การทดสอบความแปรปรวนทางเดียว F-Test (One-way ANOVA) ที่ระดับนัยสำคัญทางสถิติ 0.05 พบว่าความเห็นของพนักงานที่มีปัจจัยส่วนบุคคล ได้แก่ อายุ ระดับการศึกษา ระดับตำแหน่งงาน และอายุงาน มีผลต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแตกต่างกัน การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน ระดับความเห็นด้านนโยบายในประเด็นที่ควรงดเว้นไม่ปฏิบัติ และประเด็นที่ควรปฏิบัติ โดยเฉลี่ยอยู่ใน

ระดับความเห็นมากที่สุด ยึดถือปฏิบัติอย่างเคร่งครัด ซึ่งคำถามที่ใช้ในแบบสอบถามจะเป็นคำถามที่สอบถามพฤติกรรมในการใช้ระบบคอมพิวเตอร์ในบริษัทซึ่งจะอ้างอิงข้อกำหนดในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ได้แก่ การใช้งานบัญชีผู้ใช้ Username & Password) การติดตั้งโปรแกรมคอมพิวเตอร์ การใช้งานอีเมล และการเปลี่ยนรหัสผ่านทุก 90 วัน

คำสำคัญ: นโยบายความปลอดภัยสารสนเทศ, การปฏิบัติตาม

Abstract

Compliance to IT Security Policy of Employee is survey research. We use questionnaires as a tool to collect results. We have studied for the comparison of IT security policy compliance in our business and know what we should or should not do to avoid breaking the regulations. Samples in the survey are the eomployee of D.T.C. Enterpriese Co., Ltd. For 200 people then the data were analyzed statistically.

Statistics used in ths research included both descriptive statistics as frequency, percentage, mean and the 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 emplyees with different demographic factors differed in viewpoint of IT security compliance in some respect at 0.05 level of significance.

Keywords: IT Security Policy, Compliance

บทนำ

เทคโนโลยีสารสนเทศในปัจจุบันเป็นสิ่งที่จำเป็นอย่างยิ่งในการดำเนินธุรกิจ เพราะเป็นสิ่งที่สนับสนุนความสามารถทางการแข่งขัน และเพิ่มศักยภาพในการเติบโตของธุรกิจ พิจารณาได้จากองค์กรใดที่มีการพัฒนาด้านเทคโนโลยีสารสนเทศได้อย่างต่อเนื่องและทันสมัยอยู่เสมอ องค์กรนั้นมักจะเป็นผู้นำในอุตสาหกรรมประเภทนั้นๆ จึงอาจกล่าวได้ว่าเทคโนโลยีสารสนเทศเป็นสิ่งที่จำเป็นอย่างยิ่งต่อทุกองค์กรในปัจจุบัน และเทคโนโลยีสารสนเทศยังมีอิทธิพลต่อการดำเนินธุรกิจในยุคที่เทคโนโลยีมีการเจริญก้าวหน้าอย่างก้าวกระโดด

การนำระบบเทคโนโลยีมาใช้อย่างไม่ระมัดระวัง ไม่รอบคอบ อาจก่อให้เกิดผลเสียได้เช่นกัน ปัญหาเรื่องความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นหนึ่งปัญหาที่จะทำให้เกิดความเสียหายหรือเป็นอุปสรรคในการแข่งขันขององค์กร ดังนั้นแต่ละองค์กรจึงจำเป็นต้องมีฝ่ายงานที่ดูแลรับผิดชอบเรื่องความปลอดภัยของเทคโนโลยีสารสนเทศโดยตรง มีการกำหนดนโยบาย ข้อบังคับ รวมถึงการวางระบบป้องกันที่เข้มแข็ง และประชาสัมพันธ์ให้พนักงานปฏิบัติตามเพื่อเป็นการป้องกันปัญหาที่อาจเกิดขึ้น และส่งผลกระทบต่อองค์กรตามลำดับ ทั้งนี้เมื่อมีการออกประกาศหรือกำหนดนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศแล้ว แต่พนักงานไม่รับทราบ หรือรับทราบแต่ไม่ปฏิบัติตาม หรือมีการกระทำใดๆ ที่อาจรู้เท่าไม่ถึงการณ์ และส่งผลให้ระบบสารสนเทศเกิดความเสียได้

บริษัทที่เป็นเป้าหมายของการศึกษานี้ คือ บริษัท ดี.ที.ซี.เอ็นเตอร์ไพรส์ จำกัด ซึ่งเป็นอันดับหนึ่งในการขายสินค้าและบริการด้าน GPS Tracking ในประเทศไทย ปัจจุบันบริษัทได้มีการขยายงานออกไปทั้งทางด้านการพัฒนาโปรแกรมพิเศษสำหรับบริหารจัดการงานขนส่ง การพัฒนาระบบแผนที่ Digital เพื่อมาใช้งานร่วมกับอุปกรณ์ GPS รวมถึงด้านการพัฒนาระบบการส่งข้อมูลอัจฉริยะแบบอัตโนมัติ หรือที่เรียกว่า IoT Solution ให้กับองค์กรชั้นำหรือหน่วยงานราชการต่างๆ เพื่อสร้างสินค้าและบริการรูปแบบใหม่ๆ ให้ก้าวทันนานาประเทศทั่วโลก ซึ่งบริษัทได้นำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในบริษัท เพื่อเพิ่มความสามารถในการแข่งขัน และเพิ่มประสิทธิภาพในการดำเนินงาน จากสถานการณ์ปัจจุบัน บริษัทได้ให้อิสระกับพนักงานในการใช้งานเทคโนโลยีสารสนเทศ และไม่ได้ปิดกั้นการเข้าถึงข้อมูลข่าวสารต่างๆ รวมถึงการเข้าถึงสื่อสังคมออนไลน์ ได้แก่ Facebook, Instagram, YouTube, Pantip เป็นต้น ซึ่งการให้อิสระกับพนักงานมีผลเสียตามมา คือ พนักงานมีการใช้งานเทคโนโลยีอย่างไม่เหมาะสมในเวลางาน ทำให้การทำงานของพนักงานไม่มีประสิทธิภาพเท่าที่ควร รวมถึงมีผลทำให้ระบบเครือข่ายหนาแน่นอย่างไม่จำเป็น ส่งผลกระทบกับการใช้งานระบบเครือข่ายในการทำงานของพนักงานท่านอื่นๆ

ปัญหาอีกอย่างหนึ่งที่ส่งผลเสียหายให้กับบริษัทเป็นอย่างมาก คือ ปัญหาไวรัส โดยสาเหตุอาจเกิดจากพนักงานเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ดูหนังออนไลน์ เว็บไซต์โหลดโปรแกรม Freewere เป็นต้น แม้ว่าทางบริษัทจะมีระบบป้องกันแล้ว เช่น Firewall หรือ Scan Virus แต่ในความเป็นจริง ไม่มีระบบหรือโปรแกรมใดๆ ที่สามารถป้องกันได้ 100% โดยเฉพาะเมื่อผู้ใช้งานเป็นผู้ดาวโหลดหรือเปิดช่องทางให้ไวรัสเข้ามาเอง ทั้งโดยตั้งใจหรือไม่ตั้งใจก็ตาม จากปัญหาต่างๆ บริษัทจึงได้จัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น และประกาศให้พนักงานทุกคนรับทราบ อย่างไรก็ตามปัญหาที่เกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศยังคงมีอยู่

ดังนั้นการวิจัยในครั้งนี้ ผู้วิจัยจะศึกษาถึงระดับการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จำแนกตามปัจจัยด้านประชากรศาสตร์ของพนักงาน ทั้งนี้เพื่อนำข้อมูลดังกล่าวมาเป็นแนวทางในการปรับปรุงและพัฒนาความปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม และมีประสิทธิภาพมากยิ่งขึ้น

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาเปรียบเทียบการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานจำแนกตามปัจจัยด้านประชากรศาสตร์

2. เพื่อศึกษาการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานในสิ่งที่ควรปฏิบัติ และในส่วนที่ควรหลีกเลี่ยงไม่ปฏิบัติ

ขอบเขตของการศึกษา

การศึกษาในครั้งนี้ มุ่งศึกษาระดับการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน

1. ขอบเขตด้านเนื้อหาการวิจัย การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน ตัวแปรที่ใช้ในการศึกษา มีดังต่อไปนี้

1.1 ตัวแปรอิสระ ได้แก่ ปัจจัยด้านประชากรศาสตร์ ประกอบด้วย เพศ, อายุ, ระดับการศึกษา, ตำแหน่งงาน, แผนกและฝ่าย และระยะเวลาในการทำงาน

1.2 ตัวแปรตาม การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2 ขอบเขตด้านประชากรการวิจัย ประชากรที่ใช้ในการศึกษาครั้งนี้ คือ พนักงานของบริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด จำนวนพนักงานทั้งหมด 380 คน กลุ่มตัวอย่างในการศึกษาครั้งนี้

กำหนดขนาดของตัวอย่างด้วยการใช้สูตรคำนวณขนาดตัวอย่างของ ทาโร่ ยามาเน่ (ที่มา: https://sites.google.com, สืบค้นเมื่อวันที่ 30 กรกฎาคม พ.ศ. 2563) โดยกำหนดค่าความคลาดเคลื่อนที่ 0.05 จากจำนวนประชากร 380 คน ได้กลุ่มตัวอย่างจำนวน 200 คน

3. ขอบเขตด้านพื้นที่การวิจัย พื้นที่การวิจัย คือ บริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด

4. ขอบเขตด้านระยะเวลาการวิจัย ระยะเวลาที่ใช้ในการศึกษาวิจัยครั้งนี้ ตั้งแต่วันที่ 15 กันยายน พ.ศ. 2563 ถึงวันที่ 15 ตุลาคม พ.ศ. 2563 โดยมีระยะเวลารวม 1 เดือน

สมมติฐานการวิจัย

พนักงานที่มีปัจจัยด้านประชากรศาสตร์ (เพศ, อายุ, ระดับการศึกษา, ระดับตำแหน่งงาน, ฝ่ายที่สังกัด, และระยะเวลาในการทำงาน) แตกต่างกัน มีการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแตกต่างกัน

ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. เพื่อทราบถึงปัจจัยด้านประชากรศาสตร์ที่มีผลต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานบริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด

2. เพื่อทราบถึงการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงงานบริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด

การทบทวนวรรณกรรม

ผู้วิจัยได้ทำการศึกษาค้นคว้าแนวคิด ทฤษฎี งานวิจัยที่เกี่ยวข้องและมีการทบทวนวรรณกรรมโดยใช้แนวความคิดหลายส่วนมาเป็นส่วนหนึ่งในการศึกษา ดังนี้

แนวคิดเกี่ยวกับเทคโนโลยีสารสนเทศ

1. เทคโนโลยีสารสนเทศ หมายถึง ความรู้ในผลิตภัณฑ์ หรือในกระบวนการดำเนินงานใดๆ ที่อาศัยเทคโนโลยีด้านคอมพิวเตอร์ซอฟท์แวร์ คอมพิวเตอร์ฮาร์ดวร์ การติดต่อสื่อสาร การรวบรวม และการนำข้อมูลมาใช้อย่างทันการ เพื่อก่อให้เกิดประสิทธิภาพทางด้านการผลิต การบริการ การบริหาร และการดำเนินการงาน รวมทั้งเพื่อการศึกษาและการเรียนรู้ ซึ่งจะส่งผลต่อความได้เปรียบทางด้านเศรษฐกิจ การค้า และการพัฒนาด้านคุณภาพชีวิต และคุณภาพของประชาชนในสังคม (คลังสารสนเทศของสถาบันนิติบัญญัติ, 2535)

2. เทคโนโลยีสารสนเทศ หมายถึง เทคโนโลยีสารสนเทศที่เกี่ยวกับการดำเนินงานต่างๆ เพื่อจัดทำสารสนเทศไว้ใช้งาน ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์ เทคโนโลยีโทรคมนาคม เป็นหลัก และยังรวมถึงเทคโนโลยีอื่นๆ ที่เกี่ยวข้องกับการนำข้อมูลข่าวสารมาใช้ให้เกิดประโยชน์ โดยมีคอมพิวเตอร์เป็นเครื่องมือในการจัดการ และจัดเก็บข้อมูล ส่วนการสื่อสารโทรคมนาคมใช้เป็นสื่อในการจัดส่งข้อมูล เผยแพรภาพและเยงออกเพื่อสื่อสารกัน (ศิริศักดิ์ สุขชื่น, 2540)

3. เทคโนโลยีสารสนเทศ หมายถึง เทคโนโลยีคอมพิวเตอร์และเทคโนโลยีสื่อสารที่นำมาใช้ในการจัดทำระบบสารสนเทศ และสื่อสารสนเทศ เทคโนโลยีคอมพิวเตอร์ ได้แก่ เครื่องคอมพิวเตอร์เพื่อประมวลผล จัดสร้าง และแสดงผลสารสนเทศตามที่ต้องการ เทคโนโลยีการบันทึกข้อมูล เทคโนโลยีสำหรับการแสดงผลข้อมูล เทคโนโลยีสำหรับจัดเก็บข้อมูลบนสื่อ และเทคโนโลยีสำหรับการสื่อสารส่งผ่านข้อมูล (ลัดดา โกรดิ, 2548)

4. เทคโนโลยีสารสนเทศ หมายถึง การรวมกันระหว่างเทคโนโลยีและสารสนเทศ ส่วนของเทคโนโลยีเป็นการผสมผสานระหว่างเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีอื่นๆ เช่น เทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีสื่อสารข้อมูล เทคโนโลยีคอมพิวเตอร์นั้นมีองค์ประกอบอยู่ด้วยกัน 5 องค์ประกอบ คือ ฮาร์ดแวร์ ซอฟท์แวร์ บุคลากร ข้อมูล และกระบวนการทำงาน ส่วนสารสนเทศซึ่งเป็นสิ่งที่ได้มาจากการนำข้อมูลข่าวสารมาเข้าสู่ระบบการประมวลผล เพื่อให้ได้สารสนเทศที่ใช้ในการปฏิบัติงานและตัดสินใจในเรื่องต่างๆ สถาปัตยกรรมของเทคโนโลยีสารสนเทศ เพื่อใช้งานในองค์กรนั้น มีสิ่งที่ผู้บริหารองค์กรจะต้องคำนึงถึง 2 สิ่งที่สำคัญ ได้แก่ ความต้องการของธุรกิจและโครงสร้างพื้นฐานของการใช้งานเทคโนโลยีสารสนเทศในองค์กร มีการเน้นในงานด้านการประมวลผล การใช้เทคโนโลยีสารสนเทศช่วยในการตัดสินใจ ดำเนินการควบคุม ติดตามผล และวิเคราะห์ผลงานของผู้บริหาร (วิภา เจริญกัณฑารักษ์, 2549)

แนวคิดเกี่ยวกับการรักษาความปลอดภัยของข้อมูลสารสนเทศ

1. ความปลอดภัยของข้อมูล การรักษาความปลอดภัยทางข้อมูล คือ ผลที่เกิดขึ้นจากการใช้ระบบของนโยบายและ/หรือระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุมและป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการปกป้อง) โดยไม่ได้รับอนุญาต และยังได้ให้คำจำกัดความของความปลอดภัยทางคอมพิวเตอร์ไว้ว่า “ความปลอดภัยทางคอมพิวเตอร์ คือ ระเบียบการทางเทคนิคและทางการบริหารที่นำมาใช้กับระบบคอมพิวเตอร์ เพื่อให้มั่นใจถึงความพร้อมใช้ ความถูกต้องสมบูรณ์ และความลับของข้อมูลที่ระบบคอมพิวเตอร์จัดการอยู่” (ปนิวัธน์ ทรัพย์รุ่งเรือง, 2547)

2. การรักษาความปลอดภัยของข้อมูล หมายถึง การรักษาความปลอดภัยของข้อมูล เป็นการป้องกันระบบข้อมูลข่าวสารที่เกิดจากการเข้าใช้โดยไม่ได้รับอนุญาต หรือมีการเปลี่ยนแปลงข้อมูลในการจัดเก็บ การประมวลผล หรือการสื่อสาร ซึ่งรวมถึงการวัดผลในเรื่องการตรวจตรา และการต่อต้านการคุกคาม

โดยสรุปแล้ว จัดมุ่งหมายของการรักษาความปลอดภัยของข้อมูลสารสนเทศที่จะต้องคำนึงถึงจะมีอยู่ 3 ประการ คือ

1. ความลับ (Confidentiality) คือ การที่จะต้องมั่นใจว่าข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับไม่ได้ถูกเปิดเผยและยังคงเป็นความลับอยู่

2. ความสมบูรณ์ (Integrity) คือ การที่จะต้องมั่นใจว่าข้อมูลและระบบไม่ได้ถูกแก้ไขด้วยวิธีการใดๆ ก็ตาม ที่ไม่ได้รับอนุญาต

3. ความพร้อมใช้ (Avaiability) คือ การที่จะต้องมั่นใจว่าระบบและข้อมูลที่มีอยู่สามารถใช้งานได้เมื่อต้องการ

(U.S.Government's National Information Assurance, 2549)

3. วิธีการรักษาความปลอดภัยในความลับ และด้านความพร้อมรวมถึงปัญหาที่อาจเกิดขึ้นมีดังนี้

1. การป้องกันด้านความลับ : ผู้ใช้งานจะต้องมีการระบุตัวตนเพื่อยืนยันว่ามีสิทธิ์ในการใช้งานข้อมูลสารสนเทศนั้น ถ้าผู้ใช้งานไม่มีสิทธิ์ จะไม่สามารถเข้าถึงข้อมูลนั้นๆ ได้ อย่างไรก็ตาม มีบางกรณีที่ผู้ใช้งานบางคนที่ไม่ได้ระบุตัวตน แต่สามารถเข้าใช้งานข้อมูลสารสนเทศได้ ซึ่งเกิดจากข้อมูลนั้นๆ ถูกเก็บไว้ใน External Harddisk หรือ USB Flash Drive และอุปกรณ์เหล่านี้ถูกขโมยไป

2. การป้องกันด้านความพร้อมใช้ : การป้องกันด้านความพร้อมใช้ วิธีการหลักสำหรับการป้องกันด้านความพร้อมใช้คือ การสำรองข้อมูล ซึ่งเมื่อเวลาข้อมูลต้นฉบับมีปัญหาก็จะสามารถกู้คืนกลับมาได้Mark Zimmerman จากมหาวิทยาลัย Missouri-St.Louis ได้ยกย่องว่า Malware ซึ่งเป็นคำที่ใช้เรียกกลุ่มของ Virus, Worms, Trojan Horses, Spyware, Adware เป็นต้น ซึ่งจะเป็นสิ่งที่จะกระทบต่อการรักษาความปลอดภัยของอข้มูลสารสนเทศ ทั้ง 3 ประการข้างต้นกล่าวคือ

1. ด้านความลับ – Malware เช่น Spyware อาจแอบส่งข้อมูลออกไปข้างนอกโดยผู้ใช้งานไม่รู้ตัว หรืออาจดักจับรหัสผ่านที่ผู้ใช้งานพิมพ์ลงบนคอมพิวเตอร์แล้วส่งออกไปข้าวนอก

2. ด้านความสมบูรณ์ – Malware เช่น Virus สามารถเปลี่ยนแปลงข้อมูล หรือทำลายข้อมูลสารสนเทศของพนักงาน

3. ด้านความพร้อมใช้ – Malware เช่น Trojan Horse สามารถสั่งปิด Server หรือระบบเครือข่ายทำให้ผู้ใช้งานไม่สามารถเรียกใช้งานข้อมูลได้

จากแนวคิด และตัวอย่างของความสำคัญของข้อมูลสารสนเทศ ทำให้เห็นว่าข้อมูลสารสนเทศมีความสำคัญต่อตัวบริษัทเองควรมีมาตรการเพื่อตรวจสอบว่า พนักงานมีความตระหนักเพียงพอหรือไม่ เพื่อให้แน่ใจว่าพนักงานๆ คนจะให้ความร่วมมือ และเป็นส่วนสำคัญ ที่ใช้ปกป้องรักษาความปลอดภับของข้อมูลสารสนเทศภายในบริษัท

(Gibson, 2544)

กระบวนการตัดสินใจเกี่ยวกับนวัตกรรม

กระบวนการตัดสินใจเกี่ยวกับนวัตกรรม (A Model of the Innovation Decision Process) มีอยู่หลายตัว หลายแบบด้วยกัน ในที่นี่จะเสนอตัวแบบของโรเจอร์ ที่เรียกว่า ตัวแบบกระบวนการตัดสินใจเกี่ยวกับนวัตกรรม ซึ่งเป็นตัวแบบที่ใช้กันอย่างแพร่หลาย ตัวแบบนี้แสดงกระบวนการตัดสินใจ ซึ่งแบ่งออกเป็นระยะต่างๆ ได้ 5 ระยะ ดังนี้

1. ระยะการรับรู้ (Knowledge)
2. ระยะจูงใจ (Persuasion)
3. ระยะการตัดสินใจ (Decision)
4. ระยะปฏิบัติ (Implementation)
5. ระยะขั้นการยืนยัน (Confirmation)

สรุปได้ว่าการที่บุคคลจะยอมรับและปฏิบัติตามข่าว หรือสิ่งให้นั้น ต้องผ่านการรับรู้ โดยการรับรู้ได้มากน้อยเท่านั้นขึ้นอยู่กับคุณลักษณะของบุคคลในด้านต่างๆ คือ สถานภาพทางเศรษฐกิจสังคม และการศึกษา

(Roger, 2508)

วิธีดำเนินการวิจัย

เครื่องมือที่ใช้ในการวิจัยและเก็บรวบรวมข้อมูล

1. การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้แบบสอบถามออนไลน์ (Google Form) แบ่งเป็น 3 ส่วน

2. แบบสอมถามที่ผู้วิจัยจัดสร้างขึ้นมา ได้ความอนุเคราะห์จากผู้เชียวชาญ เพื่อตรวจสอบความถูกต้อง และความน่าเชื่อถือ ของแบบสอบถาม จำนวน 3 ท่าน แล้วนำแบบสอบถามไปหาค่า

ความน่าเชื่อถือได้ (Reliability) ด้วยวิธีของ Cronbach โดยผลการวิเคราะห์ได้ค่าความน่าเชื่อถือเท่ากับ 1.00 ถือว่าอยู่ในระดับที่มีความน่าเชื่อถือ

3. ผู้วิจัยได้ดำเนินการเก็บข้อมูลในระหว่างเดือน ตุลาคม 2563

วิธีวิเคราะห์ข้อมูล

1. การวิเคร์ข้อมูลเชิงพรรณนา ใช้การแจกแจงความถี่แสดงตารางแบบร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน

2. การวิเคราะห์เพื่อทดสอบสมมติฐาน โดยใช้สถิติอ้างอิง (Inferential Statistics) ค่า T-Test ใช้การทดสอบเปรียบเทียบความแตกต่างระหว่างค่าเฉลี่ยของตัวแปรอิสระที่ระดับนัยสำคัญทางสถิติที่ 0.05

ผลการวิจัย

จากผลการวิเคราะห์ข้อมูลเกี่ยวกับการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลดภัยด้านสารสนเทศของพนักงาน ผลการวิจัยสรุปได้ดังนี้

1. ผลการวิเคราะห์ข้อมูลด้านปัจจัยส่วนบุคคลของพนักงานที่เป็นผู้ตอบแบบสอบถาม จำนวน 200 คน จำแนกตามตัวแปรได้ดังนี้

1.1 ด้านเพศ พนักงานส่วนใหญ่เป็นเพศชาย จำนวน 136 คน คิดเป็นร้อยละ 68.0 และเพศหญิง จำนวน 64 คน คิดเป็นร้อยละ 32.0

1.2 ด้านอายุ พนักงานส่วนใหญ่มีอายุน้อยกว่า 25 ปี จำนวน 83 คน คิดเป็นร้อยละ 41.5 รองลงมา อายุระหว่าง 25 - 35 ปี จำนวน 75 คน คิดเป็นร้อยละ 37.5 อายุ 36 - 45 ปี จำนวน 35 คน คิดเป็น ร้อยละ 17.5 และมากกว่า 45 ปีขึ้นไป จำนวน 7 คน คิดเป็นร้อยละ 3.5 ตามลำดับ

1.3 ด้านระดับการศึกษา พนักงานส่วนใหญ่มีระดับการศึกษาปริญญาตรี จำนวน 186 คน คิดเป็นร้อยละ 93.0 รองลงมามีระดับการศึกษาต่ำกว่าปริญญาตรี จำนวน 9 คน คิดเป็นร้อยละ 4.5 และระดับการศึกษาสูงกว่าปริญญาตรี จำนวน 5 คน คิดเป็นร้อยละ 2.5 ตามลำดับ

1.4 ด้านระดับตำแหน่งงาน พนักงานส่วนใหญ่มีระดับตำแหน่งเป็นพนักงานระดับปฏิบัติการ จำนวน 163 คน คิดเป็นร้อยละ 81.5 รองลงมาเป็นผู้จัดการและรองผู้จัดการ จำนวน 21

คน คิดเป็นร้อยละ 10.5 หัวหน้างาน จำนวน 14 คน คิดเป็นร้อยละ 7.0 และระดับผู้บริหารระดับสูง จำนวน 2 คน คิดเป็นร้อยละ 1.0 ตามลำดับ

1.5 ด้านฝ่ายที่สังกัด พนักงานส่วนใหญ่สังกัดฝ่ายบริการและปฏิบัติการ จำนวน 119 คน คิดเป็นร้อยละ 59.5 รองลงมาสังกัดฝ่ายเทคโนโลยี จำนวน 27 คน คิดเป็นร้อยละ 13.5 ฝ่ายขายและการตลาด จำนวน 20 คน คิดเป็นร้อยละ 10.0 ฝ่ายบัญชี-การเงิน จำนวน 16 คน คิดเป็นร้อยละ 8.0 ฝ่ายสินค้าและผลิตภัณฑ จำนวน 13 คน คิดเป็นร้อยละ 6.5 และฝ่ายทรัพยาบุคคล จำนวน 5 คน คดเป็นร้อยละ 2.5 ตามลำดับ

1.6 ด้านระยะเวลาในการปฏิบัติงาน พนักงานส่วนใหญ่มีระยะเวลาที่ทำงานกับบริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด ไม่เกิน 5 ปี จำนวน 119 คน คิดเป็นร้อยละ 59.5 รองลงมามีระยะเวลาที่ทำงานกับบริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด 5 – 10 ปี จำนวน 53 คน คิดเป็นร้อยละ 26.5 และมีระยะเวลาที่ทำงานกับบริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด มากกว่า 10 ปี จำนวน 28 คน คิดเป็นร้อยละ 14.0 ตามลำดับ

2. ผลการวิเคราะห์ข้อมูลการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานในส่วนที่เป็นประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ พบว่ากลุ่มผู้ตอบแบบสอบถามส่วนใหญ่มีการหลีกเลี่ยงไม่ปฏิบัติอย่างเคร่งครัด มีเพียงประเด็นการส่งอีเมลที่มีขนาดใหญ่กว่า 25 MB โดยไม่ได้แจ้งแผนกระบบเครือข่ายและบริการสารสนเทศ เพียงประเด็นเดียวที่มีการหลีกเลี่ยงไม่ปฏิบัติเป็นส่วนใหญ่ อาจเป็นด้วยกว่าการส่งอีเมลปกติในชีวิตประจำวันไม่มีการแนบไฟล์ขนาดใหญ่อยู่แล้ว จะใช้การฝากไฟล์ไว้บนระบบ FTP (File Transfer Protocol) แทน เพราะข้อจำกัดของระบบอีเมลได้ และไฟล์งานโดยปกติหากไม่ใช่ไฟล์เสียงหรือไฟล์วิดิโอ จะมีขนาดไม่ถึงอยู่แล้ว

3. ผลการวิเคราะห์ข้อมูลด้านการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน ในประเด็นที่ควรปฏิบัติ พบว่าส่วนใหญ่จะมีการยึดถือปฏิบัติโดยครบถ้วน มีเพียงประเด็นเดียวที่พนักงานอาจไม่มั่นใจในนโยบาย คือ พนักงานต้องทราบนโยบายทุกข้อ ซึ่งส่วนใหญ่ระบุว่ามีการปฏบัติปานกลาง

สรุปผลการวิเคราะห์เชิงอนุมาน

<u>สมมติฐานงานวิจัย</u> พนักงานที่มีปัจจัยด้านประชากรศาสตร์ (เพศ, อายุ, ระดับการศึกษา, ระดับตำแหน่งงาน, ฝ่ายที่สังกัด, และระยะเวลาในการทำงาน) แตกต่างกัน มีการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแตกต่างกัน

สมมติฐานข้อที่ 1.1 พนักงานเพศชายและหญิง มีความคิดเห็นต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแตกต่างกัน

ผลการทดสอบสมมติฐานพบว่า พนักงานเพศชายและหญิง มีความคิดเห็นต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยรวมไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และเมื่อพิจารณารายด้านก็ยังพบว่า ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ และประเด็นที่ควรปฏิบัติ ก็ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานข้อที่ 1.2 พนักงานที่มีอายุต่างกันมีความคิดเห็นต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแตกต่างกัน

ผลการทดสอบสมมติฐานพบว่า พนักงานกลุ่มช่วงอายุต่าง ๆ มีความคิดเห็นต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยรวมแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และเมื่อพิจารณารายด้านก็ยังพบว่า ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และประเด็นที่ควรปฏิบัติก็ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานข้อที่ 1.3 พนักงานที่มีระดับการศึกษาต่างกันมีความคิดเห็นต่อการการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแตกต่างกันโดยรวมไม่แตกต่างกัน

ผลการทดสอบสมมติฐานพบว่า พนักงานกลุ่มที่มีระดับการศึกษาต่าง ๆ มีความคิดเห็นต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยรวมแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และหากพิจารณารายด้านพบว่า ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และประเด็นที่ควรปฏิบัติก็ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานข้อที่ 1.4 พนักงานที่มีระดับตำแหน่งงานต่างกันมีความคิดเห็นต่อการการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแตกต่างกัน

ผลการทดสอบสมมติฐานพบว่า พนักงานระดับตำแหน่งงานต่าง ๆ มีความคิดเห็นต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยรวมแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และหากพิจารณารายด้านพบว่า ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และประเด็นที่ควรปฏิบัติก็ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานข้อที่ 1.5 พนักงานที่มีอายุงานต่างกันมีความคิดเห็นต่อการลดของเสียในกระบวนการผลิต และประโยชน์ที่ได้รับของบริษัทผู้ผลิตเลนส์แว่นตาแตกต่างกัน

ผลการทดสอบสมมติฐานพบว่า พนักงานกลุ่มอายุงานต่าง ๆ มีความคิดเห็นต่อการ การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยรวมแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และหากพิจารณารายด้านพบว่า ประเด็นที่ควรงดเว้นไม่ควรปฏิบัติ แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และประเด็นที่ควรปฏิบัติก็ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

จากผลการทดสอบสมมติฐานข้อที่ 1 สรุปได้ว่า ปัจจัยส่วนบุคคล ได้แก่ อายุ ระดับการศึกษา ระดับตำแหน่งงาน และอายุงาน มีผลต่อการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างมีนัยสำคัญทางสถิติที่ 0.05

อภิปรายผลการวิจัย

จากผลการศึกษาวิจัยเรื่อง การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน สามารถนำมาอภิปรายผลเพิ่มเติมได้ดังนี้

1. ผลจากการศึกษาเกี่ยวกับ การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน บริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด ระดับความคิดเห็นด้านนโยบายในประเด็นที่ควรงดเว้นไม่ควรปฏบัติ และประเด็นที่ควรปฏิบัติ โดยเฉลี่ยอยู่ในระดับเห็นด้วยมากที่สุด ยึดถือปฏิบัติอย่างเคร่งครัด ซึ่งคำถามที่ใช้ในแบบสอบถามจะเป็นคำถามที่สอบถามพฤติกรรมที่ควรปฏิบัติ ไม่ควรปฏิบัติ ในการใช้งานระบบคอมพิวเตอร์ในบริษัท ซึ่งจะอ้างอิงข้อกำหนดในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน ได้แก่ การใช้งานบัญชีผู้ใช้ (Username & Password) การติดตั้งโปรแกรมคอมพิวเตอร์ การใช้งานอีเมล การเปลี่ยนรหัสผ่านทุก 90 วัน เป็นต้น

2. ผลการวิจัยนี้สอดคล้องกับผลการศึกษาของรัชชาภรณ์ สุภาพ และศักดิ์ชาย ตั้งวรรณวิทย์ (2557) ที่ทำการศึกษาองค์กรภาครัฐ พบว่าแม้องค์กรจะมีการประกาศใช้นโยบายความ

ปลอดภัยด้านเทคโนโลยีสารสนเทศแล้ว แต่ยังมีพนักงานบางส่วนที่ยังไม่ปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตาม สัดส่วนของพนักงานที่ไม่ได้ปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ในองค์กรภาครัฐมีสัดส่วนที่สูงกว่า

3. ทั้งนี้การขับเคลื่อนนโยบายความปลดภัยด้านเทคโนโลยีสารสนเทศ หรือนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลดภัยด้านสารสนเทศ ดังกล่าวให้สัมฤทธิ์ผล อาจจำเป็นต้องมีการสร้างความตระหนัก การรับรู้ถึงภัยคุกคาม การฝึกอบรมและให้การความรู้แก่พนักงานควบคู่ไปด้วย ดังผลศึกษาของ สุพิชญา อาชวิรดา (2559) ที่รวบรวมข้อมูลจากพนักงานในองค์กรที่มีรายชื่อจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ซึ่งสรุปว่าเมื่อพนักงานเกิดความตระหนักแล้ว จะส่งผลต่อพฤติกรรมการใช้ระบบสารสนเทศในองค์กร ให้มีความมั่นคงปลอดภัยสูงขึ้น

ข้อเสนอแนะ

จากผลการศึกษาวิจัยเรื่อง เรื่อง การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน ทางบริษัทควรนำผลที่ได้จากการศึกษาวิจัยไปใช้ดังนี้

1. จากผลการศึกษาในส่วนของข้อมูลพื้นฐานของพนักงานที่ตอบแบบสอบถาม พบว่ามีพนักงานจำนวนเพียงร้อยละ 7 ที่มีการอ่านนโยบายและแนวปฏิบัตในการรักษาความมั่นคงปลดภัยด้านสารสนเทศครบถ้วน รวมถึงมีพนักงานบางส่วนที่ไม่เคยอ่านเลย ดังนั้นผู้บริหารควรมีการสนับสนุน และส่งเสริมให้พนักงานทุกท่านอ่านนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ครบถ้วน เพื่อเป็นการป้องกันไม่ให้พนักงานกรทำการที่อาจก่อให้เกิดปัญหาเรื่องความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยรู้เท่าไม่ถึงการณ์ และเพื่อไม่ให้เกิดความเสียหายกับระบบของบริษัท โดยอาจกำหนดเป็นข้อบังคับตั้งแต่พนักงานมาเริ่มงาน

2. ผลการศึกษาในส่วนของการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พบว่ามี 1 ข้อ ที่การงดเว้นควรหลีกเลี่ยงปฏิบัติอยู่ในเกณฑ์ปานกลาง และ 1 ข้อมีการยึดถือปฏิบัติตาม อยู่ในเกณฑ์ส่วนใหญ่ ทางผู้บริหารจึงควรส่งเสริม หรือหามาตรการเพื่อเน้นให้พนักงานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้เป็นไปตามนโยบายที่กำหนดไว้อย่างมีประสิทธิภาพ

3. เนื่องจากนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของบริษัท ดี.ที.ซี. เอ็นเตอร์ไพรส์ จำกัด มีการทบทวน และปรับปรุง เป็นประจำทุกปี ซึ่งในอนาคตนโยบายบางข้ออาจมีการเปลี่ยนแปลงตามสถานการณ์ของเทคโนโลยีขณะนั้น หรืออาจมีการเพิ่มเติมข้อนโยบาย เพื่อให้ครอบคลุมการใช้งานระบบเทคโนโลยีสารสนเทศให้ครอบคลุมมาก

ยิ่งขึ้น ดังนั้นจึงควรมีการทำการสำรวจควบคู่กันไป เมื่อมีการปรับปรุงนโยบายใหม่ เพื่อให้แน่ใจว่าพนักงานทุกท่านได้รับทราบนโยบายทุกข้อ

4. ผลการศึกษาพบว่า พนักงานใหญ่ส่วนปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอยู่ในระดับมากที่สุด อย่างไรก็ตามเนื่องจากคำถามในแบบสอบถามเป็นคำถามเกี่ยวกับการปฏิบัติตามกฎระเบียบของบรษัท จึงอาจทำให้ผู้ตอบแบบสอบถามตอบแบบเข้าข้างตนเอง ดังนั้นในการปฏิบัติจรงภายในบริษัท ควรใช้ระบบการตรวจสอบเพิ่มเติม เพื่อยืนยันว่าพนักงานส่วนใหญ่ปฏิบัติตามนโยบายจริงๆ เช่น ใช้ระบบคอมพิวเตอร์เพื่อตรวจสอบการใช้งาน ตรวจสอบประวัติการเข้าเว็บไซต์ หรือตรวจสอบพฤติกรรมการใช้งานระบบเทคโนโลยีสารสนเทศ ว่าพนักงานมีการใช้งานมากน้อยเพียงใด

ข้อเสนอแนะในการศึกษาครั้งต่อไป

ในการศึกษาวิจัยครั้งต่อไป ผู้วิจัยมีข้อเสนอแนะว่า ควรทำการศึกษาเพิ่มเติมในประเด็นต่อไปนี้ เพื่อให้ได้รับข้อมูลที่มีความครอบคลุมเป็นประโยชน์ต่อการวางแผนการดำเนินงาน ให้เกิดความพึงพอใจในการปฏิบัติงานสูงสูด

1. ควรศึกษาถึงการรับรู้และความตระหนักของพนักงานเกี่ยวกับประเภทและความร้ายแรงของภัยคุกคามที่มีมากับเทคโนโลยีสารสนเทศ

2. ควรศึกษาการรับรู้และความตระหนักของพนักงานเกี่ยวกับจัดเก็บข้อมูลส่วนบุคคล (PDPA)

เอกสารอ้างอิง

ถลัลย์รัฐ วรเทพพุฒิพงษ์. (2539). การนำนโยบายไปปฏิบัติ. ในเอกสารประกอบการสอนวิชา รศ.740 การนำนโยบายไปปฏิบัติ ฉบับที่ 1. สถาบันบัณฑิตพัฒนบริหารศาสตร์.

ปฐมภูมิ วิชิตโชติ. (2559). การประยุกต์การใช้เทคโนโลยีสารสนเทศ กรณีศึกษาการใช้งานโปรแกรม GLPI กรณีศึกษา: บริษัท วาลีโอ จำกัด. การค้นคว้าอิสระ บธ.ม สาขาวิชาบริหารธุรกิจ. วิทยาลัยพาณิชยศาสตร์. มหาวิทยาลัยบูรพา.

นิสัย จัทร์เกตุ. (2558). พฤติกรรมการใช้งานสารสนเทศเพื่อการศึกษาที่มีผลต่อความสำเร็จในการเรียนของนักเรียนวิทยาลัยเทคนิคชัยนาท. คณะบริหารธุรกิจ. มหาวิทยาลัเทคโนโลยีราชมงคลธัญบุรี.

สุพิกา เพชรพิทักษณ์. (2560). ปัจจัยที่ส่งผลต่อการตัดสินใจซื้อสินค้าไอทีทางออนไลน์ของผู้บริโภคในกรุงเทพมหานคร. มหาวิทยาลัยกรุงเทพ.

ฐปนพรรษ์ นุทกาญจนกุล. (2560). ผลกระทบและการเตรียมความพร้อมของนักบัญชีไทยต่อปัญญาประดิษฐ์ (AI). มหาวิทยาลัยธรรมศาสตร์.

ศศิจันทร์ ปัญจทวี. (2560). ปัจจัยที่ส่งผลต่อการยอมรับการใช้ระบบสารสนเทศ กรณีศึกษา สถาบันการพลศึกษา วิทยาเขตเชียงใหม่. มหาวิทยาลัยราชภัฏเชียงใหม่.

สิริกร สินสม. (2558). ปัจจัยที่มีผลต่อความมีวินัยในตนเองของนักเรียน ระดับมัธยมศึกษาตอนต้น โรงเรียนมัธยมศึกษา จังหวัดนนทบุรี สังกัดสำนักงานเขตพื้นที่การศึกษามัธยม เขต 3. มหาวิทยาลัยธุรกิจบัณฑิตย์.

วรรณศรี จันทโสลิด (2560). การใช้เทคโนโลยีสารสนเทศ และการสื่อสารในองค์กร กรณีศึกษา มหาวิทยาลัยมหาจุฬาลงกรราชวิทยาลัย. มหาวิทยาลัยธุรกิจบัณฑิตย์.

กัญญรัตน์ อ่อนศรี (2553). การใช้เทคโนโลยีสารสนเทศของบุคลากรโรงพยาบาลชุมชน สังกัดกระทรวงสาธารณสุข จังหวัดสระบุรี. มหาวิทยาลัยธุรกิจบัณฑิตย์.

ธนัญทร ทองจันทร์. (2558). การประยุกต์ใช้เทคโนโลยีสารสนเทศ สำหรับการพัฒนาระบบฐานข้อมูลบุคลากรในการให้บริการสารสนเทศ และการปรับขึ้นเงินเดือน โรงเรียนวรนารีเฉลิม สงขลา. มหาวิทยาลัยหาดใหญ่

สาธิมา ชลศิร. (2558). การพัฒนาการใช้เทคโนโลยีสารสนเทศ เพื่อนำไปสู่ความสำเร็จในการปฏิบัติงานของบุคลากรที่ปฏิบัติงานด้านการคลังและพัสดุในสำนักงานอธิการบดี มหาวิทยาลัย/สถาบันเทคโนโลยีพระจอมเกล้า. สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.