ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์: กรณีศึกษา บริษัท ไทยรัฐ กรุ๊ป

THE RELATIONSHIP BETWEEN THE PERCEPTION AND THE USE OF COMPUTER INFORMATION SECURITY SYSTEMS: A CASE STUDY OF THAIRATH GROUP

ปริญทรรศน์ นิลมณี

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาบริหารธุรกิจมหาบัณฑิต วิชาเอกระบบสารสนเทศ
คณะบริหารธุรกิจ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ปีการศึกษา 2561

ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษา: บริษัท ไทยรัฐ กรุ๊ป

ปริญทรรศน์ นิลมณี

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาบริหารธุรกิจมหาบัณฑิต วิชาเอกระบบสารสนเทศ
คณะบริหารธุรกิจ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ปีการศึกษา 2561

หัวข้อการค้นคว้าอิสระ	ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์: กรณีศึกษา บริษัท ไทยรัฐ กรุ๊ป The Relationship between the Perception and the use of Computer Information Security Systems: A Case Study of Thairath group
ชื่อ - นามสกุล	นายปริญทรรศน์ นิลมณี
วิชาเอก	ระบบสารสนเทศ
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์สุรีรัตน์ อินทร์หม้อ, D.Tech.Sc.
ปีการศึกษา	2561

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ
(รองศาสตราจารย์วีระ บุญจริง, Ph.D.)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์สุภาพร คูพิมาย, ปร.ด.)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์สุรีรัตน์ อินทร์หม้อ, D.Tech.Sc.)

คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี อนุมัติการค้นคว้าอิสระฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะบริหารธุรกิจ
(ผู้ช่วยศาสตราจารย์นาถรพี ชัยมงคล, ปร.ด.)
วันที่ 5 เดือน มิถุนายน พ.ศ. 2562

หัวข้อการค้นคว้าอิสระ	ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษา: บริษัท ไทยรัฐ กรุ๊ป
ชื่อ - นามสกุล	นายปริญทรรศน์ นิลมณี
วิชาเอก	ระบบสารสนเทศ
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์สุรีรัตน์ อินทร์หม้อ, D.Tech.Sc.
ปีการศึกษา	2561

บทคัดย่อ

การค้นคว้าอิสระนี้มีวัตถุประสงค์เพื่อ 1) เพื่อศึกษาปัจจัยที่มีผลต่อการรับรู้และการใช้งานระบบรักษาความปลอดภัยทางคอมพิวเตอร์ของพนักงานในองค์กร 2) เพื่อนำผลการค้นคว้าวิจัยที่ได้ไปเป็นข้อมูลในการให้ความรู้กับพนักงานในการใช้งานระบบคอมพิวเตอร์ที่ปลอดภัยและกำหนดมาตรการในการป้องกันภัยคุกคาม

กลุ่มตัวอย่างที่ใช้ในการศึกษา คือ กลุ่มพนักงานระบบปฏิบัติการที่ใช้งานเครื่องคอมพิวเตอร์ในบริษัทไทยรัฐ กรุ๊ป จำนวน 327 คน ใช้วิธีการสุ่มตัวอย่างแบบแบ่งชั้นภูมิและสถิติที่ใช้ในการวิเคราะห์ข้อมูล คือ สถิติเชิงพรรณนา ประกอบด้วย ความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน สถิติเชิงอนุมาน ประกอบด้วย Independent Samples t-test, One-way ANOVA, LSD และ Pearson's Correlation ที่ระดับนัยสำคัญทางสถิติ 0.05

ผลการศึกษาพบว่าผู้ตอบแบบสอบถามส่วนใหญ่เป็นพนักงานที่มีอายุ 26-30 ปี ระดับการศึกษาปริญญาตรี ส่วนมากจะอยู่แผนกบรรณาธิการข่าว และมีอายุการทำงานที่ 1-2 ปี จากการศึกษาจะพบว่าพนักงานส่วนใหญ่จะทราบถึงนโยบายในการเข้าถึงข้อมูลของบริษัท เพื่อใช้ในการทำงาน แต่พนักงานส่วนใหญ่ยังขาดความรู้ในเรื่องของการรักษาความปลอดภัยระบบคอมพิวเตอร์ เช่น โปรแกรมประสงค์ร้าย ซึ่งจะต้องให้ความสำคัญกับพนักงานในเรื่องของความรู้ความเข้าใจ และการปฏิบัติงานที่เหมาะสมในการทำงาน และจากการศึกษาจะเห็นได้ว่าความรู้เรื่องการรักษาความปลอดภัยระบบมีความสัมพันธ์กับพฤติกรรมการใช้งานความปลอดภัยระบบคอมพิวเตอร์

คำสำคัญ : ความปลอดภัยระบบคอมพิวเตอร์ ภัยคุกคาม มาตรการในการป้องกันภัยคุกคาม

Independent Study Title	The Relationship Between The Perception and The Use of Computer Information Security Systems: A Case Study of Thairath Group
Name - Surname	Mr. Parintas Nilmanee
Major Subject	Information System
Independent Study Advisor	Assistance Professor Sureerut Inmor, D.Tech.Sc.
Academic Year	2018

ABSTRACT

This independent study aimed to : 1) to study the factors affecting the perception and the use of the computer security system of staff in the organization, and 2) to apply the results of the research to instruction for the staff in the computer security system and to set of threat prevention.

The sample of the study was the group of three hundred twenty-seven operating system staffs who worked with computers at Thairath Group. The stratified random sampling method was employed. The statistics used for analysis in this study were descriptive statistics including frequency, percentage, mean, and standard deviation, and statistics including independent samples t-test, one-way ANOVA, LSD, and MLR at a statistical significance level of 0.05.

The results showed that the respondents were mostly staff, aged 26-30 years, with undergraduate degrees. Most of them were in the editorial department and had worked between 1-2 years. From the study, it was found that most staff were aware of policies for access to the company's information used for work. However, most staff lacked knowledge of computer system security, like malicious programs. The staff must be provided instruction, which will ensure they understand the optimum operation of the programs. The study showed that knowledge of the computer system security was correlated with the use behavior of computer system security.

Keywords: computer security system, threat, measure of threat prevention

กิตติกรรมประกาศ

การศึกษาเรื่อง “ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษาบริษัท ไทยรัฐ กรุ๊ป”

ขอกราบขอบพระคุณคุณพ่อ คุณแม่ ที่คอยดูแล ให้กำลังใจ และเอาใจใส่ลูกเป็น อย่างดีตลอดเวลา รวมทั้งเป็นแรงใจให้อดทนเพื่อฝ่าฟันกับปัญหาและอุปสรรคต่าง ๆ และ ขอขอบคุณเพื่อน ๆ ทุกท่านที่ได้ช่วยเหลือซึ่งกัน และกันไม่ว่าจะยามทุกข์ ยามสุข ทุกคน ต่างก็ช่วยเหลือซึ่งกันและกัน เพราะ ทุกคนรวมใจเป็นหนึ่งเดียว

ขอกราบขอบพระคุณท่าน ผู้ช่วยศาสตราจารย์ ดร.สุรีรัตน์ อินทร์หม้อ อาจารย์ที่ปรึกษา ที่ท่านได้ เสียสละเวลาอันมีค่ายิ่ง ในการให้คำปรึกษา คำแนะนำ ข้อมูลที่สำคัญ ตลอดจนแนวคิดต่าง ๆ ที่เป็นประโยชน์ต่องานวิจัย เพื่อให้งานวิจัยเป็นงานชิ้นที่สมบูรณ์และ ขอขอบคุณ รองศาสตราจารย์ ดร.วีระ บุญจริง และผู้ช่วยศาสตราจารย์ ดร.สุภาพร คูพิมาย ที่ให้ความกรุณาเป็นประธานกรรมการและคณะกรรมการสอบวิจัยในครั้งนี้

และขอขอบพระคุณองค์กรกรณีตัวอย่างที่เอื้อเฟื้อข้อมูลต่าง ๆ รวมทั้งพนักงานทุก ท่านในองค์การฯ ที่กรุณาสละเวลาในการตอบแบบสอบถาม เพื่อนำมาจัดทำงานวิจัยชิ้นนี้ และ ขอขอบคุณพี่ ๆ เพื่อน ๆ ทุกคน ที่ให้การช่วยเหลือ ให้กำลังใจและให้ความคิดเห็นดี ๆ รวมถึง ขอขอบคุณเจ้าหน้าที่ของมหาวิทยาลัย มหาวิทยาลัยธรรมศาสตร์ที่ให้ข้อมูล เกี่ยวกับระเบียบ ขั้นตอนและช่วยประสานงานในการทำงานวิจัย

สุดท้ายนี้ผู้วิจัยขอยกความดีที่เกิดขึ้นจากงานวิจัยฉบับนี้ มอบแด่ผู้มีพระคุณทุกท่าน ที่กล่าวมา หากมีข้อบกพร่องประการใดผู้วิจัยขอน้อมรับไว้และขออภัยมา ณ ที่นี้ด้วย

ปริญทรรศน์ นิลมณี

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

สารบัญตาราง (ต่อ)

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

ค้นคว้าอิสระเรื่อง ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษาบริษัท ไทยรัฐ กรุ๊ป โดยมีความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ สมมติฐาน ขอบเขตของการวิจัย คำจำกัดความในการวิจัย กรอบแนวคิดในการวิจัย และประโยชน์ที่คาดว่าจะได้รับ ดังนี้

1.1 ที่มาและความสำคัญ

เมื่อกล่าวถึงการรักษาความปลอดภัย สิ่งที่ผู้คนคำนึงถึงเป็นสิ่งแรกคือ การค้นหาการบุกรุกของผู้ไม่ประสงค์ดีกับระบบคอมพิวเตอร์ซึ่งนิยมเรียกว่า “แฮกเกอร์” รวมถึงการกำจัดโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อทำลายความมั่นคงปลอดภัยของคอมพิวเตอร์ หรือมัลแวร์ประเภทต่าง ๆ โดยไม่ตระหนักรู้ถึงความหมายที่แท้จริงของ “ความมั่นคงปลอดภัย” ของระบบคอมพิวเตอร์ ซึ่งแท้จริงแล้วมีความหมายครอบคลุมถึง การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้งานของทรัพยากรในระบบคอมพิวเตอร์ในทุก ๆ ระดับ เริ่มต้นตั้งแต่อุปกรณ์ฮาร์ดแวร์ ระบบปฏิบัติการต่าง ๆ ซอฟต์แวร์ต่าง ๆ ที่ถูกติดตั้ง และการเชื่อมต่อกันเป็นเครือข่าย และรวมถึงข้อมูลหรือสารสนเทศที่ถูกจัดเก็บและประมาลผลโดยอุปกรณ์และซอฟต์แวร์ที่เชื่อมต่อกันเป็นระบบ ความหมายของการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์จึงมีขอบเขตมากกว่าการรักษาความปลอดภัยให้กับคอมพิวเตอร์หรืออุปกรณ์เพียงอย่างเดียว (กรกช วิไลลักษณ์ , 2012)

ในระบบเครือข่ายนั้นมีผู้ร่วมใช้เป็นจำนวนมาก ดังนั้นจึงมีทั้งผู้ประสงค์ดีและประสงค์ร้ายควบคู่กันไป สิ่งที่พบเห็นบ่อย ๆ ในระบบเครือข่ายก็คืออาชญากรรมทางด้านเครือข่ายคอมพิวเตอร์หลายประเภทด้วยกัน เช่น พวกที่คอยดักจับสัญญาณผู้อื่นโดยการใช้เครื่องมือพิเศษจั้มสายเคเบิ้ลแล้วแอบบันทึกสัญญาณ พวกแฮกเกอร์ (Hackers) ซึ่งได้แก่ ผู้ที่มีความเชี่ยวชาญด้านคอมพิวเตอร์เข้าไปเจาะระบบคอมพิวเตอร์ผ่านเครือข่าย หรือไวรัสคอมพิวเตอร์ (Virus Computer) ซึ่งเป็นโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นมาโดยมุ่งหวังในการก่อกวนหรือทำลายข้อมูลในระบบในการรักษาความ

ปลอดภัยในระบบเครือข่าย องค์กรจำนวนมากได้สร้างเครือข่ายคอมพิวเตอร์เพื่อใช้งานในองค์กร มีการใช้มาตรฐานเดียวกับเครือข่ายอินเทอร์เน็ต โดยเรียกเครือข่ายเฉพาะองค์กรนี้ว่า อินทราเน็ต อินทราเน็ตเชื่อมโยงผู้ใช้ทุกคนในองค์กรให้ทำงานร่วมกัน มีการกำหนดการทำงานเป็นทีมเรียกว่า Workgroup แต่ละทีมมีระบบข้อมูลข่าวสารเป็นของตนเอง มีสถานีบริการข้อมูลเรียกว่า เซิร์ฟเวอร์ การทำงานในระดับ Workgroup จึงเน้นเป้าหมายเฉพาะกลุ่ม เช่น ทีมงานทางด้านการขาย ทีมงานทางด้านบัญชี การเงิน การผลิต ฯลฯ

ถึงแม้ว่าทางองค์กรจะมีวิธีการในการรับมือด้านความปลอดภัยของระบบคอมพิวเตอร์ได้ดีเพียงใด แต่ปัจจัยสำคัญที่จะสามารถช่วยให้รับมือกับความเสี่ยงด้านความปลอดภัยของระบบคอมพิวเตอร์คือ การบริหารความสี่ยง กฎระเบียบ ข้อบังคับ ทัศนคติ และความรู้ความเข้าใจในการรับรู้ความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานของพนักงานในองค์กร เช่น การดาวน์โหลดบนเว็บไซต์ที่ไม่มีความน่าเชื่อถือ การใช้งานแฟรชไดร์ที่อาจติดไวรัส เนื่องจากปัจจุบันภัยคุกคามต่าง ๆ อาจส่งผลทำให้เกิดความเสียหายกับความมั่นคงระบบคอมพิวเตอร์และธุรกิจในองค์กรเป็นอย่างมาก

บริษัท ไทยรัฐ กรุ๊ป เป็นองค์กรที่ทำธุรกิจที่เกี่ยวข้องกับข่าวและสื่อต่าง ๆ ที่ต้องให้ความสำคัญอย่างมากกับข้อมูลในฐานข้อมูล ซึ่งจะเป็นหน้าที่ของเจ้าหน้าที่ดูแลรักษาความปลอดภัยจากการดำเนินงานของฝ่ายเทคโนโลยีสารสนเทศที่ผ่านมาพบว่าเกิดปัญหาที่สร้างความเสียหายให้กับข้อมูลทางคอมพิวเตอร์บ่อยครั้ง อันนำไปสู่ความผิดพลาดในการดำเนินงาน อีกทั้งในการทำงานพนักงานสามารถเข้าถึงข้อมูลที่ไม่จำเป็นต่อการใช้งาน จึงเป็นปัจจัยสำคัญที่พนักงานจะเป็นผู้ก่อให้เกิดความเสียหายได้ จึงต้องให้ความสำคัญอย่างมากในการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ เพื่อไม่ให้เกิดความเสียหาย และสามารถใช้งานได้อย่างต่อเนื่อง ซึ่งจำเป็นที่จะต้องส่งเสริมให้พนักงานเกิดความรู้และสามารถใช้งานระบบคอมพิวเตอร์ได้อย่างเหมาะสม

ดังนั้นผู้ทำการวิจัยจึงคิดทำการศึกษาเรื่องความสัมพันธ์ระหว่างการรับรู้ และการใช้งานของระบบรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ เพื่อเป็นแนวทางในการเสริมสร้างความตระหนัก และเสริมสร้างความรู้ให้กับพนักงานในองค์กรถึงเรื่องของความเสี่ยงในการใช้งานของพนักงาน และเป็นข้อมูลในการกำหนดนโยบายด้านความปลอดภัยเพื่อป้องกันไม่ให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ในองค์กร

1.2 จุดประสงค์ของงานวิจัย

เพื่อศึกษาปัจจัยที่มีผลต่อการรับรู้และการใช้งานระบบรักษาความปลอดภัยทางคอมพิวเตอร์ของพนักงานในองค์กร

1.3 สมมติฐานการวิจัย

1.3.1 ปัจจัยส่วนบุคคลที่แตกต่างกัน ส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

1.3.2 ระดับความรู้เรื่องความปลอดภัยมีความสัมพันธ์กับพฤติกรรมการใช้งานระบบรักษาความปลอดภัย

1.4 ขอบเขตของการวิจัย

1.4.1 ขอบเขตด้านเนื้อหา

ศึกษาด้านลักษณะทางประชากรศาสตร์ ระดับความรู้ด้านความปลอดภัยและพฤติกรรมการใช้งานระบบความปลอดภัย เพื่อให้เข้าใจถึงความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร อันนำไปสู่การอบรมและสร้างความตระหนักในเรื่องความปลอดภัย

1.4.2 ขอบเขตด้านประชากร

ประชากร ได้แก่ กลุ่มพนักงานระบบปฏิบัติการที่ใช้งานเครื่องคอมพิวเตอร์ในบริษัทไทยรัฐ กรุ๊ป จะประกอบไปด้วย 4 บริษัทย่อย จำนวนรวมทั้งหมด 2,167 คน คือ

ตารางที่ 1.1 แสดงจำนวนพนักงานในบริษัท ไทยรัฐ กรุ๊ป

บริษัท	จำนวน (คน)
1. บริษัท วัชรพล จำกัด	1,493
2. บริษัท ที.เอส.อี แอดเวอร์ไทซิ่ง จำกัด	23
3. บริษัท ทริปเปิล วี บรอดคาสท์ จำกัด	496
4. บริษัท เทรนด วีจี 3 จำกัด	155
รวม	**2,167**

1.4.3 ขอบเขตด้านกลุ่มตัวอย่าง

กลุ่มตัวอย่าง ได่แก่ พนักงานที่ใช้ระบบคอมพิวเตอร์ในการปฏิบัติงานของบริษัท ไทยรัฐ กรุ๊ป อ้างจากตารางของเครซี่และมอร์แกนจำนวน 327 คน

1.4.4 ขอบเขตด้านระยะเวลา

ระยะเวลาที่ศึกษาในการศึกษาครั้งนี้ ตั้งแต่เดือนมกราคมถึงเดือนกุมภาพันธ์ 2562

1.5 คำจำกัดความในการวิจัย

1.5.1 ความรู้ หมายถึง สิ่งที่สั่งสมมาจากการศึกษาเล่าเรียน การค้นคว้าหรือประสบการณ์ รวมทั้งความสามารถเชิงปฏิบัติและทักษะความเข้าใจ หรือสารสนเทศที่ได้รับมาจากประสบการณ์ สิ่งที่ได้รับมาจากการได้ยิน ได้ฟัง การคิดหรือการปฏิบัติในแต่ละสาขา

1.5.2 ความเข้าใจ หมายถึง ความสามารถที่บุคคลนำความรู้ ความจดจำ มาปรับปรุงเพื่อใช้งานได้

1.5.3 ความเสี่ยง หมายถึง จุดอ่อนของระบบรักษาความมั่นคง ซึ่งอาจเกิดขึ้นได้ในขั้นตอนของการปฏิบัติงาน การออกแบบ การนำระบบไปใช้ เช่น ระบบอาจไม่มีการตรวจสอบสิทธิ์ในการเข้าใช้งานของผู้ใช้ ทำให้บุคคลอื่น เข้ามาแก้ไขข้อมูล หรือทำลายระบบได้

1.5.4 ภัยคุกคาม หมายถึง เป็นลักษณะของเหตุการณ์ต่าง ๆ ซึ่งถ้าหากเกิดขึ้นแล้วอาจส่งผลถึง ความสูญเสียและความเสียหายของระบบได้

1.5.5 ความมั่นคง (Security) หมายถึง การดูแลจัดการให้ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล พ้นจากภัยคุกคามต่าง ๆ รวมทั้งการถูกโขมย และการถูกใช้งานเพื่อประโยชน์ส่วนตน

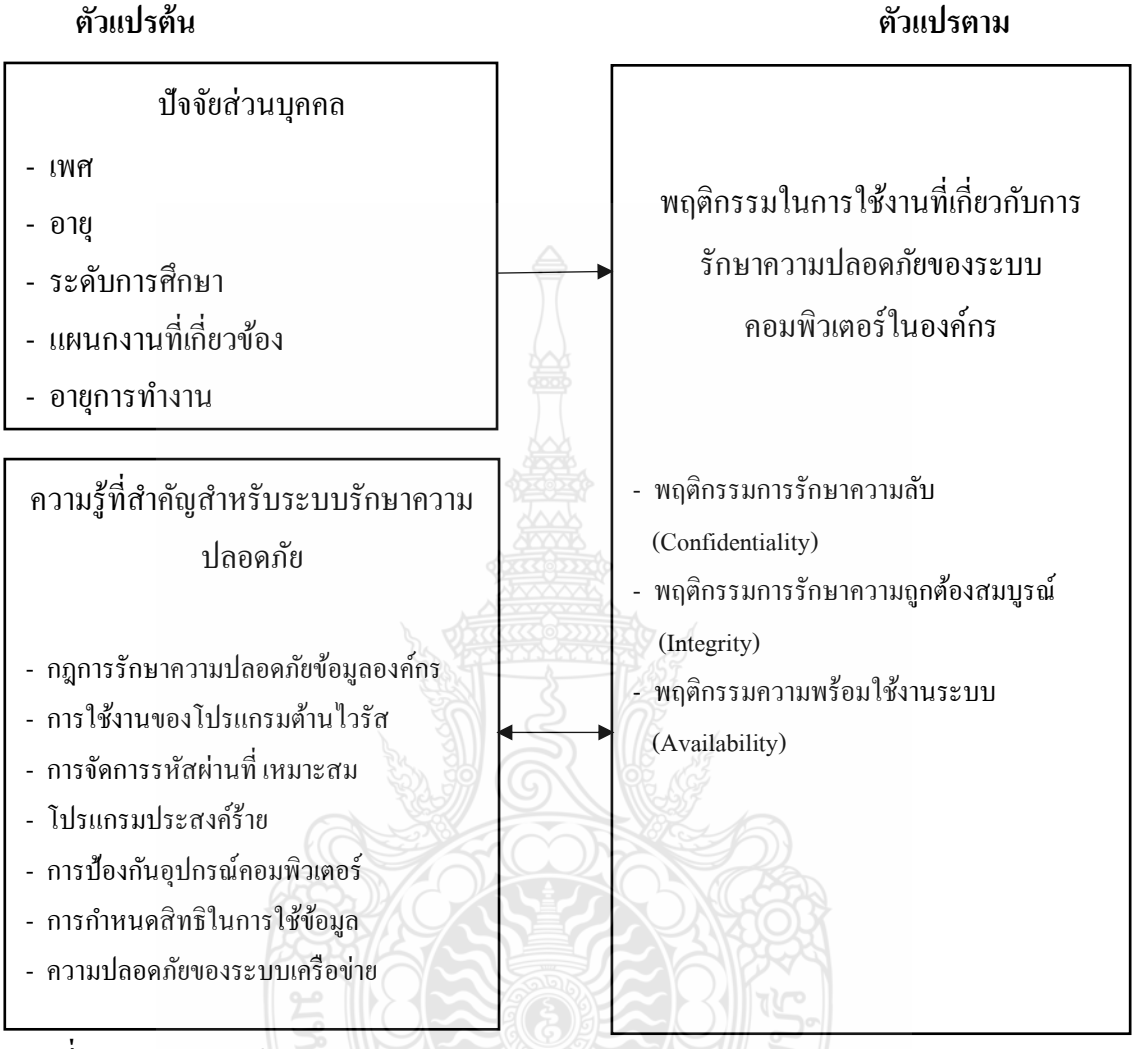
1.5.6 ความมั่นคงของระบบสารสนเทศ (Information System Security) หมายถึง การทำให้ข้อมูลที่ผ่านการประมวลผลแล้ว รอดพ้นจากอันตราย และความเสียหายจากภัยคุกคาม

1.5.7 พฤติกรรม หมายถึง กริยาอาการหรือปฏิกิริยาที่แสดงออกหรือเกิดขึ้น เมื่อเผชิญกับสิ่งเร้า ซึ่งจะมาจากภายในร่างกายหรือภายนอกร่างกายก็ได้ และปฏิกิริยาที่แสดงออกนี้มิได้เป็นพฤติกรรมทางกายเท่านั้น แต่รวมถึงพฤติกรรมที่เกี่ยวกับจิตใจด้วย

1.5.8 ระบบรักษาความปลอดภัย หมายถึง ระบบที่มีหน้าที่ช่วยสอดส่องดูแลความเรียบร้อยและป้องกันอันตรายที่จะเกิดขึ้นได้อย่างดีเยี่ยมด้วยเทคโนโลยีและระบบตรวจจับที่ทันสมัย สามารถทำงานได้ตลอด 24 ชั่วโมงต้องตอบสนองความต้องการของผู้ใช้งานได้เป็นอย่างดี โดยมีการออกแบบให้ครอบคลุมพื้นที่ใช้งาน เลือกใช้อุปกรณ์ที่ได้มาตรฐาน เหมาะสมกันสภาวะของการใช้งานและพื้นที่ที่ใช้งาน โดยต้องมีระบบการจัดการและบริหารข้อมูลที่มีประสิทธิภาพ สะดวกในการใช้งานและสะดวกในการบำรุงรักษาระบบ

1.5.9 ความรู้ทางด้านความมั่นคง หมายถึง ความรู้ที่เข้าใจถึงการป้องกันสารสนเทศและองค์ประกอบอื่นที่เกี่ยวกับการรักษาความปลอดภัยทางข้อมูล Information Security หรือผลที่เกิดขึ้นจากการใช้ระบบหรือนโยบายและระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต

1.6 กรอบแนวคิดในงานวิจัย



ภาพที่ 1 กรอบแนวคิดในงานวิจัย

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1.7.1 ทำให้ทราบถึงพฤติกรรมการใช้งานรักษาความปลอดภัยของผู้ใช้งานเครื่องคอมพิวเตอร์ ที่ส่งผลต่อความปลอดภัยระบบคอมพิวเตอร์ในองค์กร

1.7.2 ทำให้ทราบถึงความรู้ ความเข้าใจของพนักงานที่มีต่อการป้องกันภัยคุกคาม และความปลอดภัยของระบบคอมพิวเตอร์

1.7.3 สามารถนำผลการศึกษาไปใช้เป็นแนวทางให้ผู้ที่มีความสนใจในเรื่องของความปลอดภัยของระบบคอมพิวเตอร์ในองค์กรต่อไป

บทที่ 2
ทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง

การศึกษาเรื่อง ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษาบริษัท ไทยรัฐ กรุ๊ป ผู้ศึกษาได้ศึกษาแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ดังนี้

2.1 ข้อมูลเกี่ยวกับไทยรัฐกรุ๊ป

2.2 แนวคิดเกี่ยวกับความรู้

2.3 แนวคิดเกี่ยวกับความปลอดภัยของสารสนเทศ

2.4 งานวิจัยที่เกี่ยวข้อง

2.1 ข้อมูเกี่ยวกับไทยรัฐกรุ๊ป

บริษัทไทยรัฐ กรุ๊ป ประกอบไปด้วย 4 บริษัทย่อย มีจำนวนพนักงานรวมทั้งหมด 2,167 คน มี ดังนี้

ตารางที่ 2.1 แสดงจำนวนพนักงานในบริษัท ไทยรัฐ กรุ๊ป

บริษัท	จำนวน (คน)
1. บริษัท วัชรพล จำกัด	1,493
2. บริษัท ที.เอส.อี แอดเวอร์ไทซิ่ง จำกัด	23
3. บริษัท ทริปเปิล วี บรอดคาสท์ จำกัด	496
4. บริษัท เทรนด วีจี 3 จำกัด	155
รวม	**2,167**

ภาพที่ 2.1 ตราสัญลักษณ์ของหนังสือพิมพ์ไทยรัฐ

ที่มา : https://www.thairath.co.th

โดยประวัติความเป็นมาเริ่มต้นจากเมื่อวันศุกร์ที่ 18 เมษายน พ.ศ. 2518 กำพลจดทะเบียนก่อตั้งนิติบุคคลประเภทบริษัทจำกัดขึ้น ในชื่อบริษัท วัชรพล จำกัด เพื่อเป็นเจ้าของกิจการหนังสือพิมพ์ไทยรัฐ และเป็นผู้บริจาคทุนทรัพย์ในการก่อสร้างโรงเรียนไทยรัฐวิทยาทั้ง 101 แห่ง โดยตั้งแต่ พ.ศ. 2539 จนถึงปัจจุบัน คุณหญิงประณีตศิลป์ วัชรพล ภริยาของกำพล ดำรงตำแหน่งประธานกรรมการบริษัท เฉพาะกองบรรณาธิการ 262 คน อาคารทั้งหมด 13 หลัง บนพื้นที่ 39 ไร่ 9 ตารางวา และศูนย์ข่าวในส่วนภูมิภาค 35 แห่ง ทั้งนี้ บจก.วัชรพล มีทุนจดทะเบียนเริ่มต้นที่ 1 ล้านบาท จากนั้น มีการเพิ่มทุนจดทะเบียนอีกหลายครั้งต่อมาในวันจันทร์ที่ 29 กันยายน พ.ศ. 2551 บจก.วัชรพล ก่อตั้งบริษัท เทรนด์ วีจี 3 จำกัด ขึ้นเป็นกิจการในเครือ สำหรับดำเนินธุรกิจสื่อประสม ที่เกี่ยวข้องกับหนังสือพิมพ์ไทยรัฐ คือเว็บไซต์ ไทยรัฐออนไลน์ (www.thairath.co.th), บริการข้อความสั้นผ่านโทรศัพท์เคลื่อนที่, สื่อดิจิตอลหลายรูปแบบ รวมถึงให้บริการรับส่งข้อมูลภาพและเสียง, บริการข้อมูลข่าวสารต่าง ๆ ในเชิงพาณิชย์ ผ่านเครือข่ายอินเทอร์เน็ตและโทรศัพท์เคลื่อนที่ ทั้งในและต่างประเทศ โดยมีหนังสือพิมพ์ไทยรัฐเป็นแหล่งข้อมูลข่าวสารหลัก และมีการจัดทำแอปพลิเคชันสำหรับระบบปฏิบัติการบนอุปกรณ์พกพา ได้แก่ ไอโอเอส แอนดรอยด์ แบล็คเบอร์รี่ โอเอส วินโดวส์ โฟน รวมถึงวินโดวส์ 8 และวินโดวส์ อาร์ทีอีกด้วย โดยแอปพลิเคชันไทยรัฐในอุปกรณ์ไอแพด ได้รับรางวัลเหรียญทองแดง จากการประกาศผลรางวัลสื่อดิจิตอลยอดเยี่ยมแห่งเอเชีย ครั้งที่ 3 ในการสัมมนาสื่อดิจิตอลแห่งเอเชีย ซึ่งจัดโดยสมาคมหนังสือพิมพ์และผู้ผลิตสื่อสิ่งพิมพ์โลก

ในปัจจุบันไทยรัฐมีแผนการทำธุรกิจในสื่อโทรทัศน์ และวิทยุอินเทอร์เน็ต โดยการเปิดเผยของนายวัชร วัชรพล ผู้ช่วยประธานกรรมการบริหาร บริษัท วัชรพล จำกัด เพื่อลงทุนทำธุรกิจโทรทัศน์อย่างเต็มรูปแบบ ทั้งการสร้างสตูดิโอ การสั่งซื้ออุปกรณ์ การเตรียมบุคลากร สถานที่ และการรองรับการออกอากาศผ่านวิทยุอินเทอร์เน็ตอีกด้วย

2.2 แนวความคิดเกี่ยวกับความรู้

2.2.1 ความหมายเกี่ยวกับความรู้

ประภาเพ็ญ สุวรรณ (2526, น. 16) ได้ให้ความหมายเกี่ยวกับความรู้ว่า เป็นพฤติกรรมขั้นต้นซึ่งผู้ศึกษาจำได้ อาจจะมาจากการนึกได้ การมองเห็น หรือการได้ยิน คำจำกัดความหมายเกี่ยวกับความรู้ ความหมาย ข้อเท็จจริง ทฤษฎี โครงสร้าง กฎวิธีการแก้ปัญหา มาตราฐาน เป็นต้น

ราชบัณฑิตยสถาน พ.ศ. 2542 (ราชบัณฑิตยสถาน, 2546) ได้ให้ความหมายของคำว่า “ความรู้” ว่า เป็นสิ่งที่สะสมจากการค้นคว้าศึกษาเล่าเรียนหรือประสบการณ์ และความสามารถเชิงปฏิบัติ ความเข้าใจหรือการได้รับสารสนเทศจากประสบการณ์ที่ได้ฟัง ได้คิด การคิดหรือการปฏิบัติองค์วิชาในแต่ละสาขา

ความรู้ (Knowledge) เป็นขั้นแรกของพฤติกรรมที่เกี่ยวข้องกับความสามารถในการจดจำหรืออาจจะโดยการมองเห็น การได้ยิน หรือได้ฟัง ความรู้เป็นหนึ่งในขั้นตอนการเรียนรู้ ซึ่งประกอบไปด้วยคำจำกัดความ ความหมาย ทฤษฎี โครงสร้าง ข้อเท็จจริง มาตรฐาน และวิธีการแก้ปัญหาเป็นต้น ซึ่งกล่าวได้ว่าความรู้เป็นเรื่องของการจำได้ ระลึกได้ โดยไม่ต้องใช้ความคิดที่ซับซ้อน ด้วยเหตุนี้การจำ จึงเป็นกระบวนการที่สำคัญที่สุดในทางจิตวิทยา และเป็นขั้นตอนที่นำไปสู่พฤติกรรมที่ก่อให้เกิดความความเข้าใจ การนำความรู้ไปใช้ในด้านต่าง ๆ เช่น การวิเคราะห์ การสังเคราะห์ การประเมินผล ซึ่งเป็นขั้นตอนที่ต้องใช้ความคิดและความสามารถทางสมองมากขึ้นตามลำดับ ส่วนความเข้าใจ (Comprehension) จะเห็นว่าเป็นขั้นตอนต่อมาจากความรู้ โดยจะต้องใช้ทักษะและความสามารถของสมองในชั้นที่สูงขึ้นจนถึงระดับของการสื่อความหมาย อาจจะเป็นไปได้โดยการใช้ปากเปล่า ภาษา ข้อเขียน หรือการใช้สัญลักษณ์ โดยจะเกิดขึ้นหลังจากที่ได้รับข่าวสารมาแล้ว โดยจากการฟัง การมองเห้น หรือการได้ยิน แล้วแสดงออกมาในรูปของทักษะหรือการแปลความหมายต่าง ๆ เช่น การบรรยายข่าวสารต่าง ๆ ที่ได้ยินมาเป็นรูปแบบคำพูดของตนเอง การแปลความหมาย

จากภาษาหนึ่งไปอีกภาษาหนึ่ง โดยที่คงความหมายเดิมไว้ หรืออาจเป็นการแสดงความคิดเห็น หรือการให้ข้อสรุปก็ได้

บุญธรรม กิจปรีดาบริสุทธิ์ (2549 , น. 55) ได้ให้ความหมายเกี่ยวกับความรู้ว่า ความรู้เป็นข้อเท็จจริง ที่มีทั้งถูกและผิดเป็นไปตามหลักวิชา และหลักเหตุผลของวิทยาศาสตร์ที่สามารถพิสูจน์หรือตรวจสอบได้ ความรู้เป็นภูมิปัญญา (Intellectual) เป็นผลการเรียนรู้ (Learning) และการแก้ปัญหา (Problem-Solving) สามารถวัดได้ด้วยการทดสอบหรือแบบวัด ดังนั้นคำว่า "ความรู้" เป็นเพียงแนวคิดของพฤติกรรม เป็นสิ่งที่ได้มาการศึกษาค้นคว้าหรือมาจากประสบการณ์ซึ่งสอดคล้องกับหลักของวิทยาศาสตร์คือ การที่สามารถพิสูจน์หรือตรวจสอบได้

เสรี พงศ์พิศ (2549 , น. 9) ได้ให้ความหมายถึงการเรียนรู้ว่าในที่นี้ว่า การเรียนรู้สามารถจัดการกับทรัพยากร และทุนที่มีอยู่อย่างมีประสิทธิภาพจำเป็นที่จะต้องมีการเรียนรู้ที่เป็นความรู้ใหม่และมีเหมาะสมกับชาวบ้านที่ไม่ใช่การเข้าโรงเรียนเพื่อศึกษาเล่าเรียน แต่เป็นกระบวนการที่ได้เห็น ได้ยิน ได้สัมผัส ได้ปฏิบัติทำด้วนมือของตนเอง การเรียนรู้ใหม่เป็นความรู้ที่ผสมผสานและบูรณาการอย่างเป็นองค์รวม ซึ่งแนวคิดนั้นสอดคล้องกับ ประเวศ วะสี (2535 , น. 6-11) กล่าวถึงองค์ประกอบที่เป็นการพัฒนาชนบทอย่างยั่งยืน มี 3 องค์ประกอบ คือ 1) องค์กรชุมชน 2) ความรู้ 3) กระบวนการเรียนรู้

เบนจามิน บลูม (Benjamin S. Bloom อ้างถึงใน อักษร สวัสดี 2542, น. 26-28) ได้บอกถึงความหมายของความรู้ว่า เรื่องที่เกี่ยวกับสิ่งที่ละลึกถึงสิ่งเฉพาะ รวมถึงโครงการวัตถุประสงค์ด้านความรู้ โดยเน้นเรื่องของกระบวนการทางจิตวิทยาของความจำ อันเป็นกระบวนการที่เชื่อมโยงเกี่ยวกับการจัดระเบียบ โดยในปี ค.ศ. 1965 บลูมและคณะ ได้ทำการเสนอเกี่ยวกับการรับรู้หรือสุทธิพิสัย (Cognitive Domain) ว่าประกอบไปด้วยความรู้ประกอบไปด้วย 6 ระดับ ซึ่งจะพิจารณาจากความรู้ในขั้นต่ำ ไปยังความรู้ในระดับขั้นสูงขึ้น โดยบลูมและคณะได้แจกแจงรายละเอียด ดังนี้

1) ความรู้ (Knowledge) หมายถึง การเรียนรู้ที่เน้นถึงการจำแนกการละลึกได้ถึงความคิด วัตถุ และปรากฏการณ์ต่าง ๆ ซึ่งจะเป็นความทรงจำที่เริ่มจากสิ่งง่าย ๆ เป็รอิสระแก่กัน ไปจนถึงความจำที่เริ่มยุ่งยากซับซ้อน และมีความสัมพันธ์ต่อกัน

2) ความเข้าใจหรือความคิดรวบยอด (Comprehension) หมายถึง เป็นความสามารถทางสติปัญญาในการขยายความรู้ ความทรงจำ ให้กว้างออกไปจากเดิมอย่างมีความสมเหตุสมผล การแสดงพฤติกรรม ความสามารถในการแปลความหมาย และการสรุปหรือการขยายในสิ่งใดสิ่งหนึ่ง

3) การนำไปปรับใช้ (Application) หมายถึง การนำความสามารถในการนำความรู้ความเข้าใจ โดยเฉพาะความคิดรวบยอดมาผสมผสานกับความสามารถในการแปลความหมาย การสรุปหรือการขยายความโดยการใช้ความคิดรวบยอดไปแก้ปัญหาในเรื่องนั้น ๆ

4) การวิเคราะห์ (Analysis) หมายถึง เป็นทักษะความสามารถที่สูงกว่าความเข้าใจ และการนำไปใช้โดยมีลักษณะของการแยกแยะในสิ่งที่จะพิจารณาเป็นส่วนย่อยที่มีความสัมพันธ์กัน รวมถึงการสืบค้นความสัมพันธ์ต่าง ๆ เพื่อดูว่าส่วนประกอบย่อยนั้นสามารถเข้ากันได้หรือไม่ทีจะทำให้เกิดความเข้าใจในเรื่องของสิ่งหนึ่งสิ่งใดอย่างแท้จริง

5) การสังเคราะห์ (Synthesis) เป็นความสามารถในการรวบรวมส่วนย่อย ๆ หรือส่วนที่ใหญ่ๆ เข้าด้วยกันเพื่อที่จะให้เป็นเรื่องรวมเป็นหนึ่งเดียวกัน การสังเคราะห์จะมีลักษณะของกระบวนรวบรวมเนื้อหาสาระต่างๆ เข้าด้วยกัน เพื่อทำการสร้างรูปแบบหรือโครงสร้างที่ยังไม่ชัดเจนซึ่งจะต้องอาศัยความคิดสร้างสรรค์ภายใต้ขอบเขตของสิ่งที่กำหนด

6) การประเมิน (Evaluation) หมายถึง ความสามารถในการตัดสินในเรื่องของความคิดค่านิยม ผลงาน วิธีการและเนื้อหาสาระเพื่อวัตถุประสงค์บางอย่างโดยมีการกำหนดกฎเกณฑ์เป็นพื้นฐานในการพิจารณาตัดสินการประเมินผล ซึ่งถือได้ว่าเป็นขั้นตอนสูงสุดของพุทธิลักษณะที่จะต้องใช้ความรู้ความเข้าใจมาปรับใช้ในการวิเคราะห์และการสังเคราะห์เข้ามาพิจารณาประกอบกันเพื่อทำการประเมินในเรื่องใดเรื่องหนึ่ง

2.2.2 ประเภทของความรู้

ประเภทของความรู้มีด้วยกัน 2 ประเภท ดังนี้

1) ความรู้ฝังลึก (Tacit Knowledge) เป็นความรู้ที่เกิดขึ้นในตัวของแต่ละบุคคลนั้นเกิดจากการเรียนรู้ ประสบการณ์ ทักษะ ความคิดสร้างสรรค์ หรือสิ่งที่เกิดจากพรสวรรค์ต่าง ๆ เป็นสิ่งที่สื่อสารออกาในรูปของลายลัดษณ์อักษรได้ยาก สามารถพัฒนาและแบ่งกันกันได้ และเป็นสิ่งที่เป็นข้อได้เปรียบในการแข่งขัน

2) ความรู้ชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่เป้นเหตุเป็นผล สามารถรวบรวมและถ่ายทอดออกมาในรูปแบบต่าง ๆ ได้ เช่น รูปแบบของหนังสือ คู่มือ เอกสารหรืองานวิจัยต่าง ๆ เป็นความรู้ที่ทำให้ผู้อื่นสามารถเข้าใจได้เองและเข้าถึงได้ง่าย

2.2.3 ระดับของความรู้

ความรู้สามารถแบ่งได้เป็น 4 ระดับ

1) ความรู้เชิงทฤษฎี (Know-What) เป็นความรู้เชิงทฤษฎีล้วน ๆ เปรียบเสมือนความรู้ของผู้จบปริญญาตรีมาหมาดๆ เมื่อนำความรู้เหล่านี้ไปใช้งาน ก็จะได้ผลบ้าง ไม่ได้ผลบ้าง

2) ความรู้เชิงทฤษฎีและเชิงบริบท (Know-How) เป็นความรู้เกี่ยวกับลำดับขั้นตอนในการทำงานของงานหนึ่งๆ ความรู้เชิงทฤษฎีแตกต่างจากความรู้ทั่วไป ที่ความรู้ของโนว์ฮาวสามารถนำมาใช้ในการทำงานได้โดยตรง ลักษณะของความรู้ชนิดนี้จะใช้ในการแก้ปัญหาในการทำงานเป็นส่วนใหญ่

3) ความรู้ในระดับที่อธิบายเหตุผล (Know-Why) เป็นความรู้ในระดับที่อธิบายเหตุผลได้ ว่าทำไมความรู้นั้น ๆ จึงใช้ได้ผลในบริบทหนึ่ง แต่ใช้ไม่ได้ผลในอีกบริบทหนึ่ง ซึ่งผลของประสบการณ์แก้ปัญหาที่ซับซ้อนและนำมาแลกเปลี่ยนความรู้กับผู้อื่น และเอาความรู้จากผู้อื่นไปใช้ในบริบทของตนเองได้

4) ความรู้ในระดับคุณค่าความเชื่อ (Care-Why) เป็นความรู้ในระดับคุณค่า ความเชื่อ ซึ่งจะเป็นแรงขับดันมาจากภายในจิตใจ ให้ต้องกระทำสิ่งนั้น ๆ เมื่อเผชิญสถานการณ์ จะเป็นการประมวลวิเคราะห์ความรู้ที่ตนเองมีอยู่และความรู้ที่ตนเองได้รับมาสร้างเป็นองค์ความรู้ใหม่ เช่น การสร้างต้นแบบ ทฤษฎีใหม่มาใช้ในการทำงานได้

2.3 แนวคิดเกี่ยวกับความปลอดภัยของสารสนเทศ

ความมั่นคงปลอดภัยของสารสนเทศ เริ่มต้นจากความต้องการความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ในยุคแรก ๆ เพราะว่ามีภัยคุกคามต่อความปลอดภัยของระบบคอมพิวเตอร์เป็นภัยคุกคามทางกายภาพ เช่น เกิดการลักขโมยอุปกรณ์ และการโจรกรรมผลผลิตต่าง ๆ ที่ได้จากระบบหรืออาจเกิดการก่อวินาศกรรม เป็นต้น ในต่อมาเมื่อเทคโนโลยีมีความพัฒนาและก้าวหน้าเพิ่มมากขึ้นก็เกิดภัยคุกคามในหลายรูปแบบ เช่น การลักลอบที่จะเข้าระบบโดยไม่ได้รับอนุญาต เกิดการโจรกรรมข้อมูลที่เป็นความลับ ตลอดจนเกิดการทำลายระบบด้วยวิธีการต่าง ๆ เป็นผลทำให้เกิดความเสียหายทั้งบุคคลและทรัพย์สินเป็นอย่างมาก ดังนั้นต้องมีการกำหนดขอบเขตของความปลอดภัยของสารสนเทศ

2.3.1 ความรู้ด้านการรักษาความปลอดภัยของข้อมูล

E. Whitman and J. Mattord ได้นิยามความหมายของ ความปลอดภัย (Security) ไว้ว่า หมายถึงคุณภาพหรือสถานะที่มีความปลอดภัย กล่าวคือ อยู่ในสถานะที่ไม่มีอันตรายและสามารถวางใจได้ว่าได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือเหตุบังเอิญต่าง ๆ

นอกจากนี้ Institute for Security and Open Methodologies ยังกล่าวเพิ่มเติมอีกว่าความปลอดภัย คือ รูปแบบของการป้องกัน โดยทำการแบ่งแยกกันอย่างชัดเจนระหว่างทรัพย์สินกับภัยคุกคาม ซึ่งอาจเรียกการแบ่งแยกนี้ได้อย่างง่าย ๆ ว่า การควบคุม ทั้งนี้อาจรวมไปถึงการแปรสภาพทรัพย์สิน หรือการเปลี่ยนแปลงรูปแบบของภัยคุกคาม

จากนิยามดังกล่าวข้างต้นนั้น สามารถสรุปความหมายของ ความมั่นคงปลอดภัยได้ว่าเป็นรูปแบบของการป้องกันให้ทรัพย์สินอยู่ในสถานะที่ปราศจากอันตรายหรือภัยคุกคามที่เกิดขึ้นโดยตั้งใจและโดยบังเอิญ

1) การเข้ารหัส (Cryptography) คือ การทำให้ข้อมูลที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ ด้วยการเข้ารหัส (Encryption) ทำให้ข้อมูลนั้นเป็นความลับ ซึ่งผู้ที่มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ด้วยการถอดรหัส (Decryption)

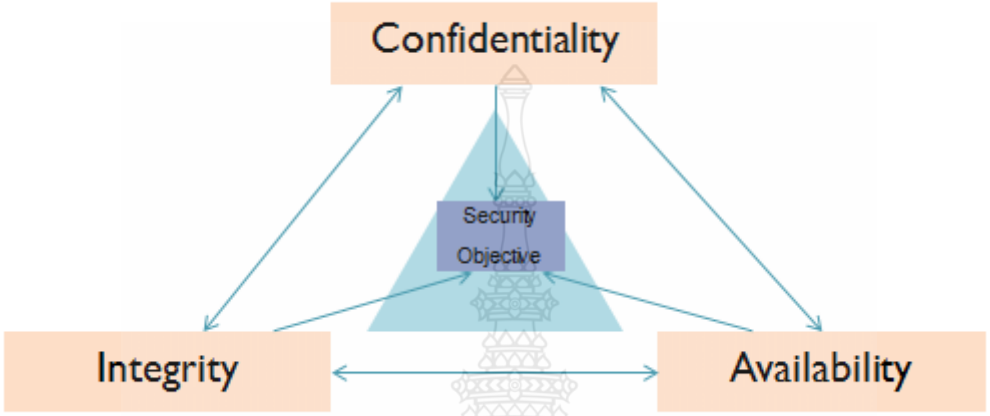
2) ลายมือชื่อดิจิทัล (Digital Signature) ลายมือชื่อดิจิตอล (Digital Signature) หรือเรียกอีกอย่างว่า ลายเซ็นดิจิตอล ใช้ในการระบุตัวบุคคลเพื่อแสดงถึงเจตนาในการยอมรับเนื้อหาในสัญญานั้น ๆ และป้องกันการปฏิเสธความรับผิดชอบ เพิ่มความน่าเชื่อถือในการทำธุรกรรมร่วมกัน

การรักษาความปลอดภัยบนระบบเครือข่าย SSL (Secure Sockets Layer)

SSL ใช้ในการรักษาความปลอดภัยสำหรับการทำธุรกรรมต่าง ๆ ผ่านอินเทอร์เน็ตซึ่ง SSL นั้นจะใช้ในการเข้ารหัส (Encrypt) ข้อมูล ใช้ในการตรวจสอบและยืนยันฝ่ายผู้ขายว่ามีตัวตนอยู่จริง (บุรินทร์ รุจจนพันธุ์ , 2559)

2.3.2 แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

องค์ประกอบที่ได้รับการยอมรับอย่างกว้างขวางของความปลอดภัยของข้อมูลโดยทั่วไป มักจะพูดถึง C.I.A. Triangle ดังนี้



ภาพที่ 2.2 องค์ประกอบของความมั่นคงปลอดภัยของสารสนเทศ

ที่มา : Oranuch Kongsri , 2558

Confidentiality (ความลับ)

เป็นการรับประกันว่า บุคคลมีสิทธิ์และได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึงข้อมูลได้ สารสนเทศที่ถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต จะถือเป็นสารสนเทศที่เป็นความลับถูกเปิดเผย ซึ่งองค์กรจะต้องมีมาตรการป้องกัน เช่น

- การจัดรูปแบบประเภทของสารสนเทศ
- การรักษาความปลอดภัยให้กับแหล่งข้อมูล
- การกำหนดนโยบายความมั่นคงปลอดภัยและการนำไปใช้งาน
- การให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยเพื่อให้เกิดความรู้และการนำไปใช้

Integrity (ความถูกต้อง ความสมบูรณ์)

ความถูกต้องครบถ้วน และไม่มีสิ่งปลอมปน ทำให้สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน เช่น ถูกทำให้เสียหาย ไฟล์หาย

เนื่องจาก Virus , Worm หรือ Hacker ทำการปลอมปน เพื่อสร้างความเสียหายให้กับข้อมูลองค์กร เพื่อให้ได้ยอดเงินในบัญชีธนาคารหรือทำการแก้ไขราคาในการสั่งซื้อ

Availability (ความพร้อมใช้งานของระบบ)

สารสนเทศจะต้องถูกเข้าใช้หรือสามารถเรียกใช้งานได้อย่างราบรื่น โดยบุคคลใช้ระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นบุคคลใช้ระบบที่ไม่ได้รับอนุญาต การจะเข้าถึงก็จะล้มเหลวถูกขัดขวาง เช่น การป้องกันด้านเนื้อหางานวิจัยห้องสมุด เนื้อหางานวิจัยพร้อมที่ใช้ต่อบุคคลใช้ที่ได้รับอนุญาต คือสมาชิกของห้องสมุดนั่นเอง จึงต้องมีการระบุตัวตน (Identification) ว่าเป็นสมาชิกห้องสมุดและพิสูจน์ได้ว่าได้รับอนุญาตจริง (Authorization)

2.3.3 องค์ประกอบของระบบสารสนเทศ กับความมั่นคงปลอดภัยสารสนเทศ

1. Software จะต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ ภายใต้เวลาต้นทุน และกำลังคนที่จำกัดซึ่งจะทำภายหลังการพัฒนาซอฟต์แวร์เสร็จแล้ว

2. Hardware จะใช้นโยบายเดียวกับสินทรัพยที่จับต้องได้ขององค์กร คือการป้องกันจากการถูกลักขโมยหรือภัยอันตรายต่าง ๆ รวมถึงการจัดสถานที่จะต้องมีความปลอดภัยให้กับอุปกรณ์หรือฮาร์ดแวร์

3. Data ข้อมูลหรือสารสนเทศเป็นทรัพยากรที่มีค่าขององค์กร การที่จะป้องกันที่แน่นหนาก็จะมีความจำเป็นสำหรับข้อมูลที่เป็นความลับซึ่งจะต้องอาศัยเรื่องนโยบายความปลอดภัย และกลไกป้องกันที่ดีควบคู่กัน

4. People บุคลากร คือภัยคุกคามที่มีผลต่อสารสนเทศที่ถูกมองข้ามมากที่สุดโดยเฉพาะบุคลากรที่ไม่มีจรรยาบรรณในอาชีพ ทำให้เป็นจุดอ่อนต่อการโจมตีจึงได้มีการศึกษาอย่างจริงจังเรียกว่า Social Engineering ซึ่งเป็นการป้องกันการหลอกลวงบุคลากร เพื่อที่จะเปิดเผยข้อมูลบางอย่างเพื่อที่จะทำการเข้าสู่ระบบได้

5. Procedure ขั้นตอนการทำงานเป็นอีกองค์ประกอบที่ถูกมองข้าม หากมิจฉาชีพทราบขั้นตอนการทำงานก็จะสามารถพบจุดอ่อนเพื่อก่อให้เกิดความเสียหายต่อองค์กรและลูกค้าขององค์กร

6. Network เครือข่ายคอมพิวเตอร์ การเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ อาจทำให้เกิดอาชญากรรมและเกิดภัยคุกคามระบบคอมพิวเตอร์โดยเฉพาะการเชื่อมต่อระบบสารสนเทศเข้ากับเครือข่ายอินเทอร์เน็ต

2.3.4 อุปสรรคของงานความมั่นคงปลอดภัยของสารสนเทศ

- ความปลอดภัย คือ การเพิ่มขั้นตอนต่าง ๆ ทำให้เกิดความไม่สะดวก เนื่องจากต้องเสียเวลาในการใส่ password และกระบวนการอื่น ๆ ในการพิสูจน์ตัวตนผู้ใช้งาน
- มีความซับซ้อนบางอย่างในคอมพิวเตอร์ ที่ผู้ใช้ทั่วไปไม่ทราบ เช่น Registry , Port , Service ที่เหล่านี้จะทราบในแวดวงของ Programmer หรือผู้ดูแลระบบ
- ผู้ใช้คอมพิวเตอร์ขาดความระมัดระวัง
- การพัฒนาซอฟต์แวร์ที่ไม่คำนึงถึงความปลอดภัย
- แนวโน้มเทคโนโลยีสารสนเทศคือการแบ่งปัน ไม่ใช่การป้องกัน
- มีการเข้าถึงข้อมูลได้จากทุกสถานที่
- ความปลอดภัยอาจจะไม่ได้เกิดขึ้นที่ซอฟแวร์และฮาร์ดแวร์เพียง อย่างเดียว
- มิจฉาชีพมีความเชี่ยวชาญ (ในการเจาะข้อมูลของผู้อื่น)
- ฝ่ายบริหารมีความละเลย ไม่ให้ความสำคัญแก่ความปลอดภัย

2.3.5 มาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799

ปัจจุบันพัฒนาการของการนำมาตรฐานการรักษาความมั่นคงปลอดภัยมาประยุกต์ใช้กับระบบสารสนเทศในองค์กรเริ่มเป็นที่แพร่หลายมากขึ้น ได้มีการรวบรวมมาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 และ ISO/IEC 17799 ซึ่งจัดเป็นมาตรฐานที่ได้รับการยอมรับจากหลายประเทศในการนำไปใช้บริหารจัดการระบบสารสนเทศขององค์กร หากจะกล่าวถึงเกี่ยวกับความเป็นมา และพัฒนาการของมาตรฐานที่ผ่านมาในภูมิภาคเอเชียแปซิฟิกและประเทศไทย ตลอดจนความแตกต่างระหว่างมาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799 และบทสรุปสาระสำคัญของมาตรฐานใน ปี 2550 ฉบับปรับปรุงล่าสุดเพื่อเป็นแนวทางสำหรับการบริหารจัดการด้านความมั่นคงปลอดภัยให้เกิดประสิทธิภาพมากยิ่งขึ้น

การพัฒนาการมาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799 ของประเทศไทย หลังจากที่ประเทศไทยได้มีการประกาศใช้พระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์เมื่อ

ปี พ.ศ. 2544 และมีการแต่งตั้งคณะกรรรมการทางอิเล็กทรอนิกส์ขึ้นเพื่อทำหน้าที่หลัก 5 ประการด้วยกัน และหนึ่งในหน้าที่นั้น ได้แก่ การเสนอแนะนโยบายและมาตรการด้านความมั่นคงให้เกิดความเชื่อมั่นและปลอดภัยในระบบคอมพิวเตอร์หรือเครือข่ายของประเทศไทยในการประกอบธุรกรรมอิเล็กทรอนิกส์ โดยมีการมอบหมายให้ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) ในฐานะที่เป็นหน่วยงานวิจัยและพัฒนาด้านความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายข้อมูลสารสนเทศ อีกทั้งยังได้ศึกษาวิจัยและพัฒนาทางด้านมาตรฐานความมั่นคงปลอดภัยด้วย

นอกจากนี้ ในเวทีความร่วมมือ RAISS ประเทศไทยในฐานะหนึ่งในประเทศสมาชิก ได้มอบหมายให้ตัวแทนจาก ThaiCERT ได้เข้าร่วมการประชุมและผลจากการร่วมงานกันทำให้คณะทำงานได้นำเสนอ Paper เพื่อเป็นแนวทางใช้งานของเจ้าหน้าที่ที่มีหน้าที่ดูแลระบบและเครือข่ายให้เป็นแนวทางที่ปฏิบัติงานประจำวันได้อย่างมั่นคงปลอดภัย โดยได้นำมาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799 มาผนวกเป็นแนวทางหรือคู่มือปฏิบัติงานประจำวันของผู้ดูแลระบบและเครือข่าย ซึ่งหลังจากได้มีการนำเสนอให้กับเวทีดังกล่าว กลุ่มผู้เข้าร่วมประชุมต่างให้ความเห็นกับการนำเสนอนี้ว่าเป็นพัฒนาการที่สามารถนำไปใช้งานได้จริงและมีประเด็นที่ครอบคลุมมาตรฐานความปลอดภัยที่ค่อนข้างครบถ้วน

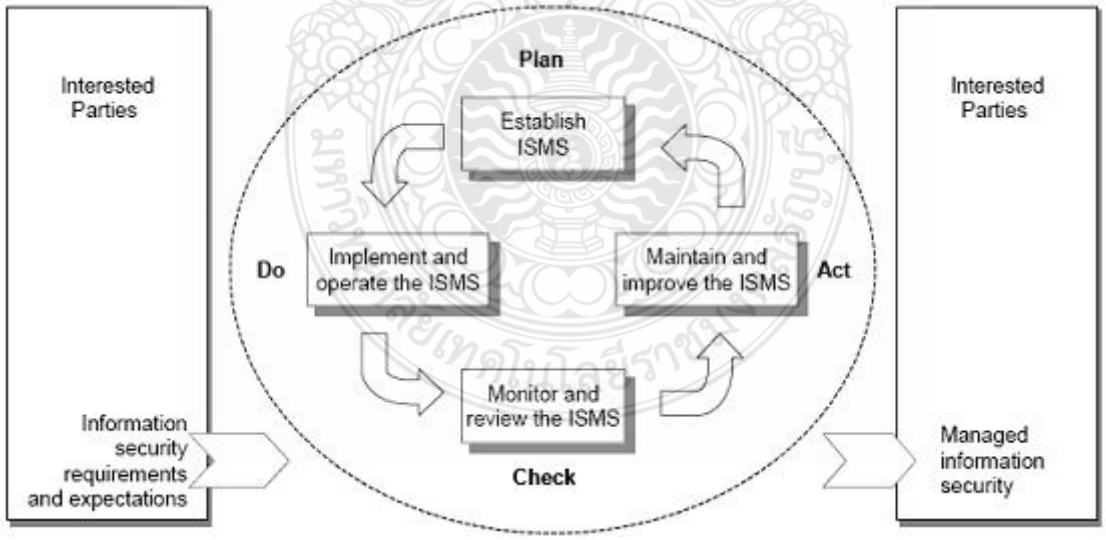
ซึ่งภายหลังได้มีการพัฒนาและแปลร่างมาตรฐานฉบับภาษาไทยขึ้น และส่งมอบให้คณะอนุกรรมการด้านความมั่นคง ภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์นำไปประกอบการพิจารณาเป็นแนวทางศึกษา ก่อนที่จะจัดทำร่างมาตรฐานรักษาความปลอดภัยที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์ออกมาเผยแพร่ โดยได้มีการดำเนินการปรับปรุงแก้ไขร่างมาตรฐานที่จัดทำขึ้นและได้นำร่างมาตรฐานดังกล่าวประชาสัมพันธ์และรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้องและประชาชนอีกจำนวนหลายครั้ง รวมถึงได้มีการปรับปรุงร่างมาตรฐานดังกล่าวจนมีความสมบูรณ์และทันสมัย สำหรับมาตรฐานฉบับปรับปรุงล่าสุดภายใต้ชื่อ มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550

2.3.6 ความแตกต่างระหว่างมาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799

สำหรับมาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799 นี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และใช้เป็นมาตรฐานอ้างอิงเพื่อ

เป็นแนวทางในการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลายซึ่งในด้านความแตกต่างระหว่างมาตรฐานทั้งสองสามารถอธิบายได้ ดังนี้

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานเป็นที่ได้รับความนิยมอย่างมาก และมีการเผยแพร่ในปัจจุบัน และกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS (Information Security Management) ให้กับองค์กร ซึ่งวัตถุประสงค์ของมาตรฐานนี้เพื่อให้องค์กรสามารถทำการบริหารจัดการในด้านความปลอดภัยได้อย่างมีระบบ และมีความเหมาะสมต่อการดำเนินธุรกิจขององค์กร มาตรฐานดังกล่าวมีหัวข้อที่เกี่ยวข้อง ได้แก่ 1) ขอบเขต (Scope) 2) ศัพท์เทคนิคและนิยาม (Terms and Definitions) 3) โครงสร้างของมาตรฐาน (Structure of this Standard) 4) การประเมินความเสี่ยงและการจัดการกับความเสี่ยง ลด/ โอนย้าย/ ยอมรับความเสี่ยง (Risk Assessment and Treatment) นอกจากนี้ มาตรฐาน ISO/IEC 27001 ยังประกอบด้วยไปด้วยวงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (P-C-D-A) ดังแสดงในภาพที่ 2.3 และมีการใช้แนวทางการประเมินความเสี่ยงเพื่อมาประกอบการพิจารณาในการหาวิธีการหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม



ภาพที่ 2.3 วงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (P-C-D-A)
ที่มา : ระบบสารสนเทศเพื่อการจัดการม , 2559

มาตรฐาน ISO/IEC 17799 เป็นมาตรฐานที่มีการกล่าวถึงเรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001 รายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบโดยแบ่งหัวข้อหลักที่เกี่ยวข้องกับระบบ และให้แนวทางว่าผู้จัดทำควรปฏิบัติอย่างไร ซึ่งผู้ใช้สามารถเพิ่มเติมมาตรการหรือใช้วิธีการที่มีความปลอดภัยเพียงพอ หรือเหมาะสมตามที่องค์กรได้ประเมินไว้ ซึ่งหัวข้อสำคัญหรือ 11 โดเมนหลักในมาตรฐานดังกล่าว มีดังนี้

1) นโยบายความปลอดภัยขององค์กร (Security Policy)

2) โครงสร้างด้านความปลอดภัยสำหรับองค์กร (Organization of Information Security)

3) การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

4) ความปลอดภัยที่เกี่ยวข้องกับด้านบุคลากร (Human Resources Security)

5) การสร้างความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communication and Operations Management)

7) การควบคุมการเข้าถึง (Access Control)

8) การจัดหา การพัฒนาและบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)

9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับเรื่องของความปลอดภัยขององค์กร (Information Security Incident Management)

10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

11) การปฏิบัติตามข้อกำหนด (Compliance)

ดังนั้นจึงสรุปได้ว่า ความแตกต่างของมาตรฐาน ISO/IEC 27001 และมาตรฐาน ISO/IEC 17799 คือ มาตรฐาน ISO/IEC 27001 จะเน้นเรื่องข้อกำหนดในการจัดทำระบบ ISMS ให้กับองค์กรตามขั้นตอน Plan-Do-Check-Act และจะใช้แนวทางในการประเมินความเสี่ยงเพื่อมาประกอบการพิจารณาเพื่อหาวิธีการหรือมาตรการที่เหมาะสม ส่วนมาตรฐาน ISO/IEC 17799 จะเน้นในเรื่องวิธีปฏิบัติที่จะนำไปสู่ระบบ ISMS ที่องค์กรได้จัดทำขึ้น ที่จะต้องเป็นไปตามมาตรฐาน ISO/IEC 27001 ที่กำหนดไว้ด้วย

2.4 งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องกับการรับรู้ การใช้งานความมั่นคงทางคอมพิวเตอร์ ที่มีความใกล้เคียงกันและใช้อ้างอิงในงานวิจัยนี้ มีดังนี้

ทรงชล มหารมณ์ (2548) ได้ทำการศึกษาเรื่อง “การวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูล สำหรับองค์กรขนาดกลางและขนาดใหญ่ในเขตกรุงเทพมหานคร” ข้อมูลที่ใช้ในการศึกษาเป็นกลุ่มตัวอย่าง 400 ชุด ทำการวิเคราะห์ข้อมูลสถิติเชิงพรรณนาในการหาค่าสถิติพื้นฐานของผู้ตอบแบบสอบถามโดยการคำนวณหาค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และ ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) และใช้สถิติเชิงอนุมานในรูปแบบมีพารามิเตอร์เพื่อทดสอบความแตกต่างระหว่างค่าเฉลี่ยของประชากรตั้งแต่ 2 กลุ่มขึ้นไปที่เป็นอิสระกัน (Independent Samples Test) สรุปผลการวิจัยสำหรับการเปรียบเทียบความแตกต่างของตัวแปรมากกว่า 2 ตัว การรักษาความปลอดภัยของข้อมูลสารสนเทศภายในองค์กร ทั้งในส่วนองค์กรขนาดเล็ก กลางหรือใหญ่ก็ตามเป็นสิ่งที่ควรตระหนักเป็นอย่างยิ่งในปัจจุบันเพราะโลกในยุคปัจจุบันเป็นโลกแห่งข้อมูล ข่าวสาร การเก็บรักษาข้อมูล ให้ปลอดภัยจึงเป็นสิ่งสำคัญกับตัวบุคคลและตัวองค์กร สำหรับการวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูลสารสนเทศขององค์กรขนาดกลางและขนาดใหญ่ในกรุงเทพมหานครนี้ ได้จัดกลุ่มประเภทความเสี่ยงตามความปลอดภัยของข้อมูล 3 ประการ ได้แก่ ความถูกต้องและสมบูรณ์ของข้อมูล (Integrity) ความลับและความน่าเชื่อถือของข้อมูล (Confidentiality) และความพร้อมใช้งานของระบบ (Availability)

จากงานวิจัยพบว่าภัยคุกคามที่ก่อให้เกิดความเสี่ยงต่อการรักษาความปลอดภัยข้อมูลที่มีความเสี่ยงในระดับสูง ซึ่งองค์กรขนาดกลาง และใหญ่ควรให้ความสนใจ และหาแนวทางการแก้ไข ซึ่งในที่นี่จะยกแนวทาง 8 ภัยคุกคาม เรียงลำดับตามความเสี่ยงจากสูงไปต่ำ ดังนี้

1. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล
2. การรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด
3. การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้
4. การปกป้องรหัสผ่าน (Password) อย่างไม่เหมาะสม
5. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม
6. พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม
7. ระบบรักษาความปลอดภัยข้อมูล ไม่มีการเปลี่ยนแปลงให้ทันสมัย
8. การออกแบบระบบซับซ้อนเกินไป

ซึ่งภัยคุกคามดังกล่าวส่วนหนึ่งจะมาจากการที่ภายในองค์กรมีการเชื่อมต่ออินเตอร์เน็ต ทำให้อาจเกิดผู้บุกรุกที่จะเข้ามาสร้างปัญหาให้กับองค์กร สามารถเข้ามาผ่านทางเครือข่ายอินเทอร์เน็ต หากระบบการรักษาความปลอดภัยขององค์กรไม่มีประสิทธิภาพที่มากเพียงพอ ดังนั้นความเสี่ยงสามารถเกิดขึ้นได้จากภายในองค์กรเองเช่นกัน เมื่อผู้บุกรุกเป็นพนักงานในองค์กร

แนวทางการป้องกันและแก้ปัญหาจากภัยคุกคามที่เกิดขึ้นควรจะสอดคล้องกับการจัดการบริหารระบบความปลอดภัยที่มีประสิทธิภาพ ซึ่งโดยสรุปแล้วสามารถแบ่งได้ การควบคุมความเสี่ยงในการรักษาความปลอดภัยข้อมูลขององค์กรเป็น 3 ส่วนหลัก ได้แก่

1. การควบคุมที่เกี่ยวข้องกับบุคลากรในองค์กร เช่นการจัดฝึกอบรมพนักงาน

2. การควบคุมที่เกี่ยวข้องกับกระบวนการทางานและนโยบายองค์กร เช่น การควบคุมการเข้าใช้ข้อมูล (Access Control), การสำรองและกู้ข้อมูล (Backup and Recovery) เพื่อเป็นการป้องกันการสูญหายของข้อมูลที่ยังใช้งานอยู่

3. การควบคุมที่เกี่ยวข้องกับการใช้เทคโนโลยีภายในองค์กร เช่น การจัดทำกระบวนการและนโยบายที่เหมาะสมในการควบคุมใช้งานเทคโนโลยีต่าง ๆ

สามารถ เจตนเสน (2553) ได้ทำการศึกษาเรื่อง “แนวทางการสร้างนโยบายการรักษาความปลอดภัยของข้อมูลสารสนเทศสำหรับองค์กร : กรณีศึกษา บริษัท ไทยออโต้เซลส์ จำกัด” ได้มีการศึกษาและวิเคราะห์ถึงแนวทางการสร้างนโยบายการรักษาความปลอดภัยของข้อมูลสารสนเทศขององค์กรที่มีประสิทธิภาพในการนำมาใช้กับองค์กรได้อย่างเหมาะสม และได้มีโครงการที่จะทำการปรับปรุง แก้ไข นโยบายการรักษาความปลอดภัยของข้อมูลสารสนเทศที่มีอยู่เดิมให้มีความครอบคลุมกับพฤติกรรมของผู้ใช้งานในองค์กร และเทคโนโลยีที่เปลี่ยนไปจากการวางนโยบายเดิม โดยมีการเก็บข้อมูลจากกลุ่มตัวอย่างจำนวน 300 ชุด จากพนักงานบริษัท ไทยออโต้เซลส์ จำกัด ซึ่งสรุปผลการศึกษาความปลอดภัยข้อมูลสารสนเทศที่สำคัญขององค์กรพบว่า ขั้นตอนกระบวนการที่มีการแสดงขั้นตอนที่ชัดเจน ใครทำอะไร ติดต่อกับใคร แต่ขาดในส่วนของการระบุชี้ชัดถึงข้อมูลที่สูญหายว่ามีข้อมูลอะไรที่สูญหายไป เป็นข้อมูลที่สำคัญหรือไม่ เนื่องจากจะสร้างความเสียหายหากข้อมูลไปตกอยู่ในมือของคู่แข่งทางธุรกิจ รวมถึงวิธีการป้องกันหากเกิดเหตุการณ์ลักษณะนี้

ภูมินทร์ ภูดวงสี (2550) ได้ทำการศึกษาเรื่อง “การศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยสารสนเทศภายในองค์กร กรณีศึกษา บริษัท NEC Corporation (Thailand) Ltd. เพื่อศึกษาการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร เป็นการศึกษาถึงแนวทางการ

วิเคราะห์ความสี่ยงของระบบข้อมูล การนำแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศมาใช้และการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยเริ่มจากการเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับองค์กร ศึกษาขั้นตอนการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ ศึกษาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ศึกษาวิเคราะห์ปัจจัยที่มีผลต่อการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ ความเสี่ยงของระบบข้อมูลต่าง ๆ จากการศึกษาพบว่าปัจจัยด้านระบบเทคโนโลยีสารสนเทศขององค์กรถูกคุกคามโดยไวรัสหรือแฮกเกอร์ มีผลต่อการพัฒนาด้านความมั่นคงปลอดภัยสารสนเทศมากที่สุด รองลงมาเป็นด้านความต้องการของลูกค้าที่มีความต้องการความมั่นคงปลอดภัยสารสนเทศ จึงมีการฝึกอบรมพนักงานให้ตระหนักถึงความมั่นคงปลอดภัยสารสนเทศเป็นประเด็นที่ควรได้รับการพัฒนา ปรับปรุง แก้ไขมากที่สุด และควบคุมการเข้าถึงของระบบสารสนเทศ เช่น การบริหารงานรหัสผ่านสำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ

วศิน รำพึงกิจ (2552) ได้ทำการศึกษาเรื่อง “การสำรวจภัยคุกคามทางคอมพิวเตอร์และการรักษาความปลอดภัยข้อมูลสารสนเทศ ของธนาคารพาณิชย์ในประเทศไทย” จากการศึกษาพบว่าภัยคุกคามด้านสารสนเทศส่งผลให้เกิดความเสียหายต่อธนาคารพาณิชย์ในประเทศไทยอยู่ในเกณฑ์ต่ำเนื่องจากมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยด้านสารสนเทศของธนาคารพาณิชย์ในประเทศไทยอยู่ในระดับสูง มีการใช้เทคโนโลยีด้านการรักษาความปลอดภัยด้านสารสนเทศที่เหมาะสม มีการตรวจสอบตามลำดับ คือตรวจสอบความปลอดภัยโดยบุคลากรภายในองค์กร ทดสอบหาความบกพร่องด้านความปลอดภัยสารสนเทศ และตรวจสอบความปลอดภัยสารสนเทศโดยองค์กรภายนอก แต่การใช้เครื่องมืออัตโนมัติ (Automated Tools) และโปรแกรมเฝ้าติดตามผ่านเว็บไซต์ (Web Activity Monitoring Software) ยังไม่เป็นที่นิยมทั้งที่เครื่องมือและโปรแกรมดังกล่าวมีความสำคัญเพื่อให้ผู้ดูแลระบบพบความผิดปกติจากภัยด้านสารสนเทศอย่างทันท่วงทีซึ่งสอดคล้องกับความสนใจด้านการฝึกอบรมด้านการรักษาความปลอดภัยสารสนเทศ ที่พบว่าผู้มีส่วนเกี่ยวข้องให้ความสนใจกับการควบคุมและรักษาความปลอดภัยมากด้านเทคโนโลยีรักษาความปลอดภัย แสดงให้เห็นความใส่ใจเพื่อให้เกิดความปลอดภัยสูงสุดของธนาคาร ซึ่งถือเป็นเรื่องที่บุคลากรของธนาคารทุกธนาคารต้องปฏิบัติโดยเคร่งครัด เพื่อสร้างความน่าเชื่อถือให้กับผู้ใช้บริการและความน่าเชื่อถือต่อธนาคารที่มีการทำธุรกรรมร่วมกัน

อัครา วัฒนโยธิน (2553) ได้ทำการศึกษาเรื่อง “ความตระหนักของพนักงานต่อการป้องกันรักษาทรัพย์สินทางด้านสารสนเทศ กรณีศึกษา การไฟฟ้าส่วนภูมิภาค สำนักงานกลาง”

เพื่อทำการศึกษาความตระหนักต่อการป้องกันรักษาทรัพย์สินทางด้านสารสนเทศของพนักงานการไฟฟ้าส่วนภูมิภาค ภายในสำนักกลาง โดยได้ทำการศึกษาจากประชากรจำนวน 346 คน จากระดับความรู้ความเข้าใจเกี่ยวกับนโยบายรักษาความปลอดภัยทางด้านทรัพย์สินสารสนเทศของการไฟฟ้าส่วนภูมิภาคของกลุ่มตัวอย่างนั้นพบว่า ระดับความรู้ความเข้าใจเกี่ยวกับนโยบายรักษาความปลอดภัยทางด้านทรัพย์สินสารสนเทศของการไฟฟ้าส่วนภูมิภาคของกลุ่มตัวอย่างในแต่ละข้อนั้น กลุ่มตัวอย่างตอบถูกต้องมากกว่า 80% จากระดับทัศนคติเกี่ยวกับนโยบายรักษาความปลอดภัยทางด้านทรัพย์สินสารสนเทศของการไฟฟ้าส่วนภูมิภาคของกลุ่มตัวอย่างเมื่อพิจารณาภาพรวมพบว่ากลุ่มตัวอย่างมีค่าเฉลี่ยของทัศนคติที่เห็นด้วยเกี่ยวกับการรักษาความปลอดภัยทางสารสนเทศ จากระดับการรับรู้ข้อมูลข่าวสารเกี่ยวกับการรักษาความปลอดภัยทางด้านทรัพย์สินสารสนเทศของการไฟฟ้าส่วนภูมิภาคของกลุ่มตัวอย่างเมื่อพิจารณาภาพรวมพบว่ากลุ่มตัวอย่างมีค่าเฉลี่ยการรับรู้ข้อมูลข่าวสารค่อนข้างน้อยเกี่ยวกับการรักษาความปลอดภัยทางด้านทรัพย์สินสารสนเทศ และระดับความตระหนักต่อการรักษาความปลอดภัยทางด้านทรัพย์สินสารสนเทศของการไฟฟ้าส่วนภูมิภาคของกลุ่มตัวอย่างเมื่อพิจารณาภาพรวมพบว่ากลุ่มตัวอย่างมีค่าเฉลี่ยของความตระหนักค่อนข้างมากเกี่ยวกับการรักษาความปลอดภัยทางด้านทรัพย์สินสารสนเทศ

วราภรณ์ ธวิทย์ชัยพร (2549) ได้ทำการศึกษาเรื่อง “แนวทางการนำ Information Security Managament มาใช้ในการจัดระเบียบการบริหารจัดการด้านความปลอดภัยสารสนเทศ กรณีศึกษาบริษัทให้คำปรึกษาด้านสารสนเทศแห่งหนึ่ง ได้ทำการศึกษาพบว่าการรักษาความปลอดภัยสารสนเทศในบริษัทกรณีศึกษามีการให้ความสำคัญด้านเทคโนโลยีเป็นอย่างสูง และไม่ได้ให้ความสำคัญกับด้านกระบวนการและด้านบุคลากร รวมถึงการตรวจสอบกระบวนการต่าง ๆ ที่ต้องปฏิบัติตามนโยบายที่กำหนดไว้และมักพบความผิดพลาดจากการปฏิบัติงานในด้านการรักษาความปลอดภัยสารสนเทศอยู่อย่างเสมอ ซึ่งนำความเสียหายให้แก่บริษัท ทั้งความเสียหายในด้านความไว้วางใจของลูกค้าซึ่งไม่สามารถประมาณค่าเป็นตัวเงินได้ และความเสียหายด้านตัวเงินอีกหลายประการ จึงมีแนวทางในการรักษาความปลอดภัยสารสนเทศโดยคำนึงถึงเป้าหมายทางธุรกิจของบริษัทเป็นหลัก หลังจากนั้นจึงได้นำข้อมูลทั้งในส่วนที่ได้จากความต้องการด้านความปลอดภัยสารสนเทศและจากมาตรฐานสากลที่เกี่ยวข้อง และนำไปให้ผู้ที่รับผิดชอบโดยตรงพิจารณาความเหมาะสม รวมถึงการประสานงานกันระหว่างผู้ปฏิบัติงานและผู้ควบคุมดูแล

รังสิต งามพรประเสริฐ (2547) ได้ทำการศึกษาเรื่อง “นโยบายการรักษาความปลอดภัยสารสนเทศ กรณีศึกษาบริษัท XYZ จำกัด” เพื่อศึกษาแนวทางการสร้างนโยบายการรักษาความปลอดภัยของข้อมูลที่มีการนาเทคโนโลยีสารสนเทศต่าง ๆ มาใช้ และศึกษาวิธีการวิเคราะห์ความเสี่ยงของสารสนเทศของบริษัท XYZ โดยใช้มาตรฐาน ISO17799 เป็นเครื่องมือในการสร้างนโยบายดังกล่าว ผลที่ได้จากงานวิจัยทำให้สามารถสรุปความเสี่ยงหลักขององค์กรได้จากการประเมินความเสี่ยง ได้แก่ การโจมตีจากไวรัสผ่านทางอินเทอร์เน็ต , การให้ข้อมูลแก่ลูกค้าและคู่ค้า และมีการจัดเก็บข้อมูลสำคัญและอีเมล์ไว้ที่เครื่องลูกข่าย เป็นต้น ซึ่งได้มีการนำประเด็นที่มีความเสี่ยงสูงมาพิจารณาแก้ไขและปรับปรุง เพื่อลดหรือป้องกันความเสี่ยงนั้น ๆ และจากการเก็บรวบรวมข้อมูลและศึกษาพบว่าแนวทางการจัดการความปลอดภัยสารสนเทศควรครอบคลุมทั้งประเด็นด้านเทคนิคและการบริหารจัดการ ซึ่งแนวทางที่ได้รับความนิยมและได้รับการพิสูจน์แล้วคือ มาตรฐาน ISO 17799 จึงสามารถสรุปการจัดทำนโยบายด้านความปลอดภัยข้อมูลออกเป็น 2 ส่วนคือ แนวทางการบริหารจัดการและแนวทางการจัดการทางเทคนิค

จากการศึกษางานวิจัยนี้มีการศึกษาแนวคิดและทฤษฎีต่าง ๆ เพื่อที่จะใช้ในการสร้างนโยบายการรักษาความความมั่นคงปลอดภัยของข้อมูล ได้แก่ Information Security , ISMF , BS ISO/IEC 17799:2000 , กระบวนการพัฒนาความปลอดภัยอย่างต่อเนื่อง (Model PDCA) และการวิเคราะห์ความเสี่ยง ซึ่งในการทำงานวิจัยเรื่อง “การศึกษาและจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ .ศ. 2544” ได้นำในส่วนของการประเมินความเสี่ยงเป็นอีกส่วนหนึ่งในทฤษฎีการวิเคราะห์ความเสี่ยง โดยมีการใช้แบบจำลองที่มีการกำหนดระดับความรุนแรงและโอกาสในการเกิดความเสี่ยงเพื่อนำมากำหนดระดับความเสี่ยงมาใช้เพื่อเป็นแนวทางในการทำวิจัย และในส่วนของโอกาสในการเกิดความเสี่ยงที่ใช้ข้อมูลจากแหล่งข้อมูลจากการสำรวจหรือมาจากความเห็นของผู้ดูแลระบบและระดับความรุนแรงที่เกิดขึ้นซึ่งมีการเก็บรวบรวมจากผู้ดูแลระบบนั้นไม่มีสถิติหรือมาตรฐานใด ๆ มารองรับ ซึ่งอาจจะทำให้ขาดความน่าเชื่อถือและอาจเกิดความผิดพลาดในการประเมินความเสี่ยงขึ้นได้

บทที่ 3
วิธีดำเนินการวิจัย

สำหรับการศึกษาเรื่อง ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษาบริษัท ไทยรัฐ กรุ๊ป เป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยการใช้วิจัยเชิงสำรวจ (Survey Research Method) และมีวิธีการเก็บข้อมูลด้วยแบบสอบถาม (Questionnaire) ซึ่งผู้ทำการศึกษาได้กำหนดแนวทางในการศึกษา โดยมีลำดับขั้นตอนทางการศึกษาโดยมีลำดับขั้นตอนในการศึกษาและมี ระเบียบวิธีการศึกษาในด้าน การกำหนดประชากร การสุ่มกลุ่ม ตัวอย่าง การเก็บรวบรวมข้อมูล การจัดทำและการวิเคราะห์ข้อมูล รวมถึง สถิติที่ใช้ในการศึกษา ดังนี้

3.1 ประชากรและกลุ่มตัวอย่าง
3.2 เครื่องมือที่ใช้ในการวิจัย
3.3 การเก็บรวบรวมข้อมูล
3.4 วิธีการวิเคราะห์ข้อมูล

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัยคือผู้ที่ใช้งานทั้งเพศชายและเพศหญิงแต่ละฝ่าย แต่ละแผนกที่เป็นพนักงานในบริษัท ไทยรัฐ กรุ๊ป ที่มีส่วนในการใช้งานเครื่องคอมพิวเตอร์ จำนวนทั้งหมด 2,167 คน

ตารางที่ 3.1 แสดงจำนวนพนักงานในบริษัท ไทยรัฐ กรุ๊ป

บริษัท	จำนวน (คน)
1. บริษัท วัชรพล จำกัด	1,493
2. บริษัท ที.เอส.อี แอดเวอร์ไทซิ่ง จำกัด	23
3. บริษัท ทริปเปิล วี บรอดคาสท์ จำกัด	496
4. บริษัท เทรนด วีจี 3 จำกัด	155
รวม	**2,167**

ขนาดประชากร	ขนาดตัวอย่าง	ขนาดประชากร	ขนาดตัวอย่าง	ขนาดประชากร	ขนาดตัวอย่าง	ขนาดประชากร	ขนาดตัวอย่าง	ขนาดประชากร	ขนาดตัวอย่าง
10	10	100	80	280	162	800	260	2,800	338
15	14	110	86	290	165	850	265	3,000	341
20	19	120	92	300	169	900	269	3,500	346
25	24	130	97	320	175	950	274	4,000	351
30	28	140	103	340	181	1,000	278	4,500	354
35	32	150	108	360	186	1,100	285	5,000	357
40	36	160	113	380	191	1,200	291	6,000	361
45	40	170	118	400	196	1,300	297	7,000	364
50	44	180	123	420	201	1,400	302	8,000	367
55	48	190	127	440	205	1,500	306	9,000	368
60	52	200	132	460	210	1,600	310	10,000	370
65	56	210	136	480	214	1,700	313	15,000	375
70	59	220	140	500	217	1,800	317	20,000	377
75	63	230	144	550	226	1,900	320	30,000	379
80	66	240	148	600	234	2,000	322	40,000	380
85	70	250	152	650	242	2,200	327	50,000	381
90	73	260	155	700	248	2,400	331	75,000	382
95	76	270	159	750	254	2,600	335	100,000	384

ภาพที่ 3.1 ขนาดของกลุ่มตัวอย่างของเครซี่และมอร์แกน

ที่มา : Robert V. Krejcie and Earyle W. Morgan. Educational and Psychological Measurement

จำนวนกลุ่มตัวอย่าง

สำหรับการวิจัยในครั้งนี้ผู้วิจัยได้กำหนดกลุ่มตัวอย่างในการวิจัยคือพนักงานในบริษัทไทยรัฐ กรุ๊ป โดยทำการเก็บข้อมูลจากพนักงาน เพศชาย เพศหญิงในแต่ละฝ่าย แต่ละแผนก ที่มีการใช้งานเครื่องคอมพิวเตอร์ในบริษัท เพื่อศึกษาถึงความรู้ ทัศนคติ และการใช้งานของพนักงาน โดยจัดเก็บข้อมูลทั้งหมดจำนวน 327 คน โดยใช้สูตรคำนวณหาขนาดของกลุ่มตัวอย่างในการศึกษานี้ได้โดยใช้สูตรการหาขนาดของกลุ่มตัวอย่างแบบทราบจำนวนประชากร ดังนั้นผู้วิจัยจึงทำการกำหนดขนาดกลุ่มตัวอย่างโดยตารางสำเร็จรูปของเครซี่และมอร์แกนที่ระดับความเชื่อมั่นร้อยละ 95 และมีความคลาดเคลื่อนร้อยละ 5

ตารางที่ 3.2 นำมาแบ่งตามอัตราส่วนของประชากร ดังนี้

บริษัท	จำนวน (คน)	อัตราส่วนประชากร
1. บริษัท วัชรพล จำกัด	1,493	225
2. บริษัท ที.เอส.อี แอดเวอร์ไทซิ่ง จำกัด	23	4
3. บริษัท ทริปเปิล วี บรอดคาสท์ จำกัด	496	75
4. บริษัท เทรนด วีจี 3 จำกัด	155	23
รวม	**2,167**	**327**

วิธีการสุ่มตัวอย่าง

ข้อมูลที่ใช้ในกระบวนการศึกษา ได้แก่ การจัดทำข้อมูล การรวบรวมข้อมูล การวิเคราะห์ข้อมูล การแปลความหมายและการสรุปผล ประกอบด้วย

1) แหล่งข้อมูลปฐมภูมิ เป็นข้อมูลที่ผู้วิจัยได้เก็บรวบรวมเอง โดยใช้แบบสอบถามเก็บข้อมูลจากกลุ่มตัวอย่างจำนวน 327 ชุด เป็นผู้ที่ถูกคัดเลือกให้เป็นตัวแทนของประชากรทั้งหมดและเป็นผู้ที่มีความสามารถในการตอบแบบสอบถาม

2) แหล่งข้อมูลทุติยภูมิ เน้นข้อมูลที่ผู้วิจัยเก็บรวบรวมมาจากแหล่งที่สามารถอ้างอิงได้และมีความน่าเชื่อถือ ได้แก่ หนังสือ เอกสารเกี่ยวกับงานวิจัยที่ผ่านมาแต่มีความเกี่ยวข้องกับงานวิจัยในครั้งนี้และวารสาร สิ่งพิมพ์ทางวิชาการทั้งที่ใช้ระบบเอกสารและระบบออนไลน์

กลุ่มตัวอย่างสำหรับงานวิจัยนี้ ผู้วิจัยได้เลือกกลุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็น (Non Probability Sampling) คือไม่ได้กำหนดโอกาสหรือความน่าจะเป็นที่กลุ่มตัวอย่างจะได้รับเลือกมาจากประชากรทั้งหมด โดยใช้วิธีการแบบเฉพาะเจาะจง (Purposive Sampling) เพื่อให้ได้ให้กับกลุ่มตัวอย่างพนักงานที่ใช้งานเครื่องคอมพิวเตอร์ ในแผนกต่าง ๆ ในบริษัท ไทยรัฐ กรุ๊ป โดยวิธีการแจกแบบสอบถามจำนวน 327 ชุด

3.2 เครื่องมือที่ใช้ในการวิจัย

แบบสอบถาม (Questionnaires) คือ เครื่องมือหลักที่ใช้ในการวิจัย ที่ใช้ในการสำรวจเป็นการรวบรวมข้อมูลโดยผู้วิจัยได้มีการทบทวนแนวคิดและทฤษฎีต่าง ๆ ที่เกี่ยวข้องเพื่อสร้างกรอบแนวความคิดเพื่อเป็นแนวทางในการค้นคว้าและพัฒนาไปสู่แบบสอบถามเพื่อเก็บข้อมูลประชากรกลุ่มตัวอย่างด้วยวิธีวิจัยเชิงสำรวจแบบปลายเปิด (Closed Ended Question) ผู้วิจัยมีคำตอบให้ผู้ตอบแบบสอบถามได้เลือกตอบโดยแบ่งแบบสอบถามออกเป็น 3 ส่วน

ส่วนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลด้านประชากรศาสตร์โดยคำถามข้อมูลทั่วไปของผู้ใช้งานคอมพิวเตอร์มีจำนวน 5 ข้อ ได้แก่ เพศ อายุ ระดับการศึกษา แผนกงานที่เกี่ยวข้อง อายุการทำงาน โดยเป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว (Close Ended Question)

ส่วนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลเกี่ยวกับความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กร โดยจะถามพนักงานที่ใช้งานเครื่องคอมพิวเตอร์ในองค์กรในเรื่องของความรู้ดังนี้

- กฎการรักษาความปลอดภัยข้อมูลองค์กร
- การใช้งานของโปรแกรมต้านไวรัส
- การจัดการรหัสผ่านที่เหมาะสม
- ความหมายของโปรแกรมประสงค์ร้ายต่อระบบ
- การป้องกันอุปกรณ์คอมพิวเตอร์จากความเสียหาย
- การกำหนดสิทธิในการใช้ข้อมูล

- การรักษาความปลอดภัยของระบบเครือข่าย

จะเป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว (Close Ended Question) โดยแบ่งเกณฑ์การวัดและเกณฑ์การให้คะแนนแบ่งเป็น 5 ระดับ ดังนี้

เกณฑ์การวัดและเกณฑ์การให้คะแนนแบ่งเป็น 5 ระดับ ดังนี้

5	หมายถึง	มีความรู้มากที่สุด
4	หมายถึง	มีความรู้มาก
3	หมายถึง	มีความรู้ปานกลาง
2	หมายถึง	มีความรู้น้อย
1	หมายถึง	มีความรู้น้อยที่สุด

แบบมาตราส่วนค่า 5 ระดับ

$$\frac{\textbf{คะแนนสูงสุด - คะแนนต่ำสุด}}{\textbf{จำนวนระดับ}} = \frac{\textbf{5 - 1}}{\textbf{5}}$$

ระดับ 1	ค่าเฉลี่ย	1.00 - 1.80	แปลความว่า	มีความรู้น้อยที่สุด
ระดับ 2	ค่าเฉลี่ย	1.81 - 2.60	แปลความว่า	มีความรู้น้อย
ระดับ 3	ค่าเฉลี่ย	2.61 - 3.40	แปลความว่า	มีความรู้ปานกลาง
ระดับ 4	ค่าเฉลี่ย	3.41 - 4.20	แปลความว่า	มีความรู้มาก
ระดับ 5	ค่าเฉลี่ย	4.21 - 5.00	แปลความว่า	มีความรู้มากที่สุด

ส่วนที่ 3 แบบสอบถามเกี่ยวกับข้อมูลเกี่ยวกับพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร โดยจะถามพนักงานที่ใช้งานเครื่องคอมพิวเตอร์ในองค์กรในเรื่องของพฤติกรรมการใช้งาน โดยจะแบ่งเป็นพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) มีดังนี้

- การรักษาความลับของ Username และ Password
- การอนุญาตให้ผู้อื่นใช้ข้อมูลที่ตนเองรับผิดชอบ

- การนำเข้าข้อมูลจากเว็บไซต์ที่ไม่มั่นใจในความปลอดภัย
- ออกจากระบบ (Logoff) ทุกครั้งเมื่อไม่ได้อยู่ที่เครื่อง
- การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) มีดังนี้

- การปรับปรุงข้อมูลที่ทันสมัย
- ปฏิบัติตามนโยบายด้านสิทธิ์การใช้ข้อมูล
- ปฏิบัติตามนโยบายด้านความปลอดภัย
- การอบรมเรื่องความปลอดภัย
- ปฏิบัติงานด้วยความเข้าใจระบบ

พฤติกรรมในการใช้งานที่เกี่ยวกับการเข้าถึงข้อมูลต่างๆ ได้เมื่อต้องการ (Availability) มีดังนี้

- การใช้งานโปรแกรมตรวจสอบไวรัส
- ระบบสามารถใช้งานได้ตลอดเวลา
- อุปกรณ์และโปรแกรมมีความพร้อมในการใช้งาน
- อุปกรณ์เครือข่ายมีความพร้อมในการใช้งาน
- มีการทำสำรองข้อมูล

โดยแบ่งเกณฑ์การวัดและเกณฑ์การให้คะแนนแบ่งเป็น 5 ระดับ ดังนี้

เกณฑ์การวัดและเกณฑ์การให้คะแนนแบ่งเป็น 5 ระดับ ดังนี้

5	หมายถึง	ปฏิบัติเป็นประจำ (มากที่สุด)
4	หมายถึง	ปฏิบัติบ่อยครั้ง (มาก)
3	หมายถึง	ปฏิบัติปานกลาง
2	หมายถึง	ปฏิบัติน้อยครั้ง (น้อย)
1	หมายถึง	ปฏิบัติน้อยที่สุด (ไม่มีเลย)

การวิเคราะห์คำถามแบบมาตรส่วนประมาณค่า (Rating Scale) 5 ระดับ โดยใช้ค่าทางสถิติคะแนนเฉลี่ยเลขาคณิต (Arithmetic Mean) กำหนดช่วงวัด ดังนี้

แบบมาตราส่วนค่า 5 ระดับ

$$\frac{\text{คะแนนสูงสุด - คะแนนต่ำสุด}}{\text{จำนวนระดับ}} = \frac{5 - 1}{5}$$

ระดับ 1 ค่าเฉลี่ย 1.00 - 1.80 แปลความว่า ปฏิบัติน้อยที่สุด
ระดับ 2 ค่าเฉลี่ย 1.81 - 2.60 แปลความว่า ปฏิบัติน้อยครั้ง
ระดับ 3 ค่าเฉลี่ย 2.61 - 3.40 แปลความว่า ปฏิบัติปานกลาง
ระดับ 4 ค่าเฉลี่ย 3.41 - 4.20 แปลความว่า ปฏิบัติมาก
ระดับ 5 ค่าเฉลี่ย 4.21 - 5.00 แปลความว่า ปฏิบัติมากที่สุด

การทดสอบเครื่องมือ

ผู้ศึกษาได้เสนอแบบสอบถามที่สร้างขึ้นไปทดสอบหาความเที่ยงตรงและความเชื่อมั่น ดังนี้

1. การหาความเที่ยงตรง (Validity) โดยการนำแบบสอบถามที่ผู้จัดทำได้ทำขึ้นไปเสนอต่อผู้เชี่ยวชาญ เพื่อพิจารณาความถูกต้องของเนื้อหา (Content Validity) นำมาแก้ไขข้อบกพร่อง

2. การทดสอบความเชื่อมั่น (Reliability) แบบสอบถามที่ทำการแก้ไขแล้ว ผู้ศึกษาจะทำการทดสอบ Pre-Test กับกลุ่มตัวอย่างที่คล้ายกับกลุ่มตัวอย่างจริง เพื่อทดสอบความเชื่อมั่นของแบบสอบถาม จำนวน 30 ชุด โดยสิ่งที่จะพิจารณาว่าผู้ตอบแบบสอบถามเข้าใจหรือไม่ หรือมีปัญหากับการตอบแบบสอบถามหรือไม่และหลังจาก Pre-Test แล้วนำมาทดสอบความเชื่อมั่น เมื่อพบว่าแบบสอบถามมีความเชื่อมั่น (Reliability) จึงนำไปใช้เป็นเครื่องมือในการเก็บข้อมูล

3.3 การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูล ในการศึกษา เรื่องความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษาบริษัท ไทยรัฐ กรุ๊ป ในครั้งนี้ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลตามขั้นตอน ดังนี้

1. ข้อมูลทุติยภูมิ (Secondary Data) ได้จากการศึกษาค้นคว้าจากข้อมูลที่มีผู้รวบรวมไว้ดังนี้

1.1 หนังสือพิมพ์ วารสาร สิ่งพิมพ์ต่าง ๆ

1.2 ข้อมูลทางอินเทอร์เน็ต

1.3 หนังสือทางวิชาการ บทความ สารนิพนธ์ วิทยานิพนธ์ และรายงานวิจัยที่เกี่ยวข้อง

2. แหล่งข้อมูลปฐมภูมิ (Primary Data) ซึ่งได้จากการใช้แบบสอบถาม เป็นเครื่องมือในการเก็บข้อมูลจากกลุ่มตัวอย่างเป้าหมายจำนวน 327 คน ที่เป็นพนักงานที่ใช้งานเครื่องคอมพิวเตอร์ดังนี้

2.1 ผู้วิจัยนำแบบสอบถามไปดำเนินการสอบถามกับ กลุ่มเป้าหมายที่เป็นพนักงานที่ใช้งานเครื่องคอมพิวเตอร์ โดยเก็บตัวอย่างตามจำนวนกลุ่มตัวอย่าง

2.2 นำแบบสอบถามที่ได้มาทาการลงรหัสเพื่อนำไปวิเคราะห์ข้อมูลทางสถิติต่อไป

3.4 การวิเคราะห์ข้อมูล

เมื่อได้รวบรวมข้อมูลเรียบร้อยแล้ว ผู้ศึกษาได้ทำการลงรหัส และนำมาประมวลผลข้อมูลทางคอมพิวเตอร์ โดยการใช้โปรแกรมสำเร็จรูป SPSS เพื่อการวิเคราะห์ข้อมูลนำเสนอและสรุปผลในการศึกษาครั้งนี้ได้ทำการคำนวณค่าสถิติต่าง ๆ

1. สถิติเชิงพรรณนา (Descriptive Statistic) เพื่ออธิบายลักษณะทั่วไปของกลุ่มตัวอย่าง ได้แก่ ร้อยละ (Percentage) ค่าเฉลี่ย (Arithmetic Mean) และค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อใช้ในการพรรณนาข้อมูลตัวแปรด้านต่าง ๆ ดังนี้

1.1 ตัวแปรที่เป็นข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ได้แก่ เพศ อายุ ระดับการศึกษา แผนกงานที่เกี่ยวข้องและอายุการทำงาน เพื่ออธิบายข้อมูลที่ได้ของกลุ่มตัวอย่างในเรื่องของความรู้ ความเข้าใจ ในการใช้งานระบบคอมพิวเตอร์อย่างปลอดภัยในส่วนของข้อมูลและระบบคอมพิวเตอร์ผ่านทางค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) เป็นข้อมูลประกอบการแปลความหมายเชิงบรรยาย

2. สถิติเชิงอนุมาน (Inferential Statistics) เพื่อทดสอบสมมติฐานเพื่อหาค่าความสัมพันธ์และความแตกต่างของตัวแปรมากกว่า 1 กลุ่ม โดยการใช้ค่าสถิติ ดังนี้

2.1 ใช้สถิติ F-test หรือ One way ANOVA ใช้วิเคราะห์เปรียบเทียบ 2 กลุ่มขึ้นไป และจะทำการทดสอบต่อไปว่าคู่ใดบ้างที่แตกต่างกัน หรือคู่ใดบ้างที่ไม่แตกต่างกัน โดยวิธีนี้มีการ

ทดสอบชื่อว่า วิธีการเปรียบเทียบเชิงซ้อน ตาม Least-Significant Different เช่น อายุ ระดับการศึกษา แผนกงานที่เกี่ยวข้องของพนักงานในองค์กร เป็นต้น

2.2 ใช้สถิติ T-test ใช้วิเคราะห์เปรียบเทียบค่าเฉลี่ยระหว่างกลุ่มตัวอย่าง 2 กลุ่ม เป็นอิสระจากกันข้อมูลที่รวบรวมได้อยู่ในระดับ อันตรภาคหรืออัตราส่วน เช่น เพศของพนักงานในองค์กร เป็นต้น

2.3 ใช้ Pearson Correlation ในการหาค่าความสัมพันธ์เป็นวิธีที่ใช้วัดความสัมพันธ์ระหว่างตัวแปร หรือข้อมูล 2 ชุด โดยที่ตัวแปร เพื่อหาค่าความสัมพันธ์ระหว่างความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กรและพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร โดยใช้เกณฑ์การแปลความหมายค่าสัมประสิทธิ์สหสัมพันธ์ (กัลยา วานิชย์บัญชา , 2545)

ค่าสัมประสิทธิ์สหสัมพันธ์	ระดับความสัมพันธ์
ตั้งแต่ 0.8 - 1.00	มีความสัมพันธ์ในระดับสูงมาก
ตั้งแต่ 0.61 - 0.80	มีความสัมพันธ์ในระดับสูง
ตั้งแต่ 0.40 - 0.60	มีความสัมพันธ์ในระดับปานกลาง
ตั้งแต่ 0.21 - 0.40	มีความสัมพันธ์ในระดับน้อย
ตั้งแต่ 0.10 - 0.20	มีความสัมพันธ์ในระดับน้อยมาก

บทที่ 4
ผลการวิเคราะห์

การศึกษา ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษา บริษัท ไทยรัฐ กรุ๊ป ในครั้งนี้ได้รวบรวมข้อมูลโดยการตอบแบบสอบถามจากพนักงานที่ใช้งานเครื่องคอมพิวเตอร์ จำนวน 327 ชุด และได้รับการตอบกลับทั้งสิ้น 327 ชุด การตอบแบบสอบถามในครั้งนี้จึงมีความสมบูรณ์ทั้งสิ้น 327 ชุด และได้ใช้โปรแกรมสำเร็จรูปทางสถิติเข้ามาช่วยในการวิเคราะห์ข้อมูลและการประมวลผลข้อมูลโดยกำหนดสัญลักษณ์และตัวแปรที่ใช้ในการวิเคราะห์ข้อมูล ดังนี้

สัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูล

n	แทน	จำนวนประชากรกลุ่มตัวอย่าง
$\overline{X}$	แทน	ค่าเฉลี่ยเลขคณิต
SD	แทน	ค่าส่วนเบี่ยงเบนมาตรฐาน
t	แทน	ค่าสถิติที่ใช้ในการแจกแจงความถี่แบบ (t-Distribution)
F	แทน	ค่าสถิติที่ใช้ในการแจกแจงความถี่แบบ (F-Distribution)
SS	แทน	ผลบวกกำลังสองของคะแนน
MS	แทน	ค่าคะแนนเฉลี่ยกำลังสองของคะแนน
LSD	แทน	ค่าผลต่อนัยสำคัญที่คำนวณได้สำหรับประชากรกลุ่ม I และ J
Sig.	แทน	ระดับนัยสำคัญทางสถิติใช้ในการทดสอบสมมติฐาน
*	แทน	ความมีนัยสำคัญทางสถิติที่ระดับ 0.05
R	แทน	ค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณ
R Square	แทน	ค่าสัมประสิทธิ์การพยากรณ์

4.1 การนำเสนอผลการวิเคราะห์ข้อมูล

การนำเสนอการวิเคราะห์ข้อมูลที่ได้จากการเก็บแบบสอบถามเชิงปริมาณตามจำนวนกลุ่มตัวอย่างที่กำหนดไว้ของการค้นคว้าอิสระ เรื่องความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษา บริษัท ไทยรัฐ กรุ๊ป โดยทำการนำเสนอผลการวิเคราะห์ข้อมูลแบ่งออกเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 การวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ส่วนที่ 2 การวิเคราะห์ข้อมูลความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ส่วนที่ 3 การวิเคราะห์ข้อมูลพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ส่วนที่ 4 การวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐาน

4.2 ผลการวิเคราะห์ข้อมูล

ส่วนที่ 1 การวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ตารางที่ 4.1 แสดงจำนวน (ความถี่) และค่าร้อยละ ลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม จำแนกเพศ

เพศ	จำนวน (คน)	ร้อยละ
1. เพศชาย	190	58.1
2. เพศหญิง	137	41.9
รวม	**327**	**100.00**

จากตารางที่ 4.1 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคล จำนวน 327 คน จำแนกเพศ พบว่าผู้ตอบแบบสอบถามส่วนใหญ่เพศชายมีจำนวน 190 คน คิดเป็นร้อยละ 58.1 และเพศหญิง จำนวน 137 คน คิดเป็นร้อยละ 41.9 โดยกลุ่มผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศชายมากกว่าเพศหญิง

ตารางที่ 4.2 แสดงจำนวนค่าร้อยละ ลักษณะส่วนบุคคลของผู้ตอบแบบสอบถามจำแนกตามอายุ

อายุ	จำนวน (คน)	ร้อยละ
1. 21 - 25 ปี	43	13.1
2. 26 - 30 ปี	115	35.2
3. 31 - 35 ปี	65	19.9
4. 36 - 40 ปี	68	20.8
5. 41 - 45 ปี	26	8.0
6. 46 ปีขึ้นไป	10	3.1
รวม	**327**	**100.00**

จากตารางที่ 4.2 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวน 327 คน จำแนกตามอายุ พบว่า กลุ่มผู้ตอบแบบสอบถามส่วนใหญ่อายุ 26 - 30 ปี ร้อยละ 35.2 และส่วนน้อยมีอายุ 46 ปีขึ้นไป ร้อยละ 8.0 เนื่องจากประชากรในเครือไทยรัฐกรุ๊ป ส่วนใหญ่เป็นกลุ่มคนรุ่นใหม่ทั้งคนที่เพิ่งจบการศึกษาและคนที่มีประสบการณ์ในการทำงานมาก่อน ทำให้กลุ่มอายุของพนักงานที่ตอบแบบสอบถามจะอยู่ในช่วงอายุ 26-30 ปี

ตารางที่ 4.3 แสดงจำนวน (ความถี่) และค่าร้อยละ ลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม จำแนกตามระดับการศึกษา

ระดับการศึกษา	จำนวน (คน)	ร้อยละ
1. ปริญญาตรี	310	94.8
2. สูงกว่าปริญญาตรี	17	5.2
รวม	**327**	**100.00**

จากตารางที่ 4.3 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวน 327 คน ส่วนใหญ่เป็นผู้ที่มีวุฒิการศึกษาในระดับปริญญาตรี ร้อยละ 94.8 และวุฒิการศึกษาสูงกว่าปริญญาตรี ร้อยละ 5.2 เพราะว่าเป็นการแจกแบบสอบถามจากกลุ่มตัวอย่างในสำนักงาน ซึ่งต้องมีวุฒิการศึกษาในการรับสมัครที่ระดับปริญญาตรี ดังนั้นกลุ่มระดับการศึกษาปริญาตรีจึงมีจำนวนผู้ตอบแบบสอบถามมากที่สุด

ตารางที่ 4.4 แสดงจำนวน (ความถี่) และค่าร้อยละ ลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม จำแนกตามแผนกงานที่เกี่ยวข้อง

อาชีพ	จำนวน (คน)	ร้อยละ
1. บรรณาธิการข่าว	104	31.8
2. การขาย / การตลาด	48	14.7
3. เลขานุการ / แอดมินฝ่าย	10	3.1
4. เทคโนโลยีสารสนเทศ	22	6.7
5. กฎหมาย	31	9.5
6. โปรแกรมเมอร์	6	1.8
7. ทรัพยากรมนุษย์	25	7.6
8. กราฟฟิก / ตัดต่อ	46	14.1
9. พัสดุ / กองซ่อมบำรุง	35	10.7
รวม	**327**	**100.00**

จากตารางที่ 4.4 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวน 327 คน จำแนกตามแผนกงานที่เกี่ยวข้อง พบว่าแผนกงานที่มีผู้ตอบแบบสอบถามมากที่สุดคือแผนกบรรณาธิการข่าว ร้อยละ 31.8 ซึ่งบริษัท ไทยรัฐ กรุ๊ป เป็นองค์กรที่เกี่ยวกับทางด้านของสื่อต่าง ๆ จึงจำเป็นที่จะต้องมีพนักงานบรรณาธิการข่าวในส่วนต่าง ๆ และแผนกงานที่เกี่ยวข้องที่มีผู้ตอบแบบสอบถามน้อยที่สุดคือ แผนกโปรแกรมเมอร์ ร้อยละ 1.8 เนื่องจากบริษัทมีการจ้างทำโปรแกรมจากหน่วยงานภายนอก จึงทำให้กลุ่มคนในแผนกโปรแกรมเมอร์มีจำนวนน้อยและมีหน้าที่ในดูแลเว็บไซต์และแอพพลิเคชันของบริษัท

ตารางที่ 4.5 แสดงจำนวน (ความถี่) และค่าร้อยละ ลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม จำแนกตามอายุการทำงาน

อายุการทำงาน	จำนวน (คน)	ร้อยละ
1. น้อยกว่า 1 ปี	16	4.9
2. 1 - 2 ปี	114	34.9
3. 3 - 4 ปี	93	28.4
4. 5 - 10 ปี	82	25.1
5. มากกว่า 10 ปี	22	6.7
รวม	**327**	**100.00**

จากตารางที่ 4.5 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวน 327 คน จำแนกตามอายุการทำงาน พบว่าส่วนใหญ่อายุการทำงานของพนักงานอยู่ที่ 1-2 ปี ร้อยละ 34.9 และกลุ่มอายุการทำงานน้อยที่สุดอยู่ที่ 1 ปี เนื่องจากพนักงานไทยรัฐ กรุ๊ป เป็นองค์กรเกี่ยวกับสื่อ จึงจะเห็นได้ว่าส่วนใหญ่เป็นกลุ่มคนรุ่นใหม่ที่เพิ่งจบการศึกษา และมาจากผู้ที่มีประสบการณ์การทำงานในองค์กรอื่น และมาสมัครงานในบริษัทไทยรัฐ กรุ๊ป ทำให้มีกลุ่มคนที่มีอายุการทำงานระหว่าง 1-2 ปี เป็นจำนวนมากกว่ากลุ่มอื่น ๆ

ส่วนที่ 2 การวิเคราะห์ข้อมูลความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ตารางที่ 4.6 แสดงจำนวนร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐานของความรู้ในความปลอดภัย

ความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กร	ระดับความสำคัญ					$\overline{X}$	SD	แปลผล	อันดับ
	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด				
1. กฎการรักษาความปลอดภัยข้อมูลองค์กร	104 (31.8)	177 (54.1)	41 (12.5)	5 (1.5)	-	4.16	0.693	มาก	1
2. การใช้งานของโปรแกรมต้านไวรัส	93 (28.4)	162 (49.5)	55 (16.8)	14 (4.3)	3 (0.9)	4.00	0.842	มาก	2
3. การจัดการรหัสผ่านที่เหมาะสม	70 (21.4)	154 (47.1)	78 (23.9)	21 (6.4)	4 (1.2)	3.81	0.887	มาก	3
4. ความหมายของโปรแกรมประสงค์ร้ายต่อระบบ	54 (16.5)	126 (32.5)	87 (26.6)	57 (17.4)	3 (0.9)	3.52	0.993	มาก	7
5. การป้องกันอุปกรณ์คอมพิวเตอร์จากความเสียหาย	77 (23.5)	133 (40.7)	85 (26.0)	31 (9.5)	1 (0.3)	3.78	0.925	มาก	4
6. การกำหนดสิทธิในการใช้ข้อมูล	63 (19.3)	124 (37.9)	90 (27.5)	45 (13.8)	5 (1.5)	3.60	0.998	มาก	5
7. การรักษาความปลอดภัยของระบบเครือข่าย	64 (19.6)	118 (36.1)	95 (29.1)	47 (14.4)	3 (0.9)	3.59	0.989	มาก	6
ภาพรวม	**62 (19.0)**	**139 (42.5)**	**110 (33.6)**	**14 (4.3)**	**2 (0.6)**	**3.75**	**0.832**	**มาก**	

จากตารางที่ 4.6 ผลการวิเคราะห์ข้อมูลจำนวนร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐานของความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กรในภาพรวม พบว่าความรู้ในเรื่องของกฎการรักษาความปลอดภัยข้อมูลองค์กร หมายความว่าพนักงานในบริษัท ไทยรัฐ กรุ๊ป มีความรู้เกี่ยวกับการรักษความปลอดภัยของข้อมูลองค์กร ที่จะต้องใช้ในการทำงาน และจะพบว่าความรู้ในเรื่องของความหมายของโปรแกรมประสงค์ร้ายมีค่าเฉลี่ยน้อยที่สุด หมายความว่าพนักงานในบริษัท ไทยรัฐ กรุ๊ป ยังขาดความรู้ในเรื่องของโปรแกรมประสงค์ร้ายที่อาจส่งผลต่อระบบคอมพิวเตอร์ และจะเห็นพนักงานยังขาดความรู้ในเรื่องของการรักษาความปลอดภัยของระบบเครือข่าย การกำหนดสิทธิ์ในการใช้ข้อมูล และการจัดการรหัสผ่านที่เหมาะสม ดังนั้นฝ่ายเทคโนโลยีสารสนเทศควรที่จะมีการอบรมในเรื่องของความรู้ที่เกี่ยวกับโปรแกรมสงค์ร้าย และความรู้เกี่ยวกับการรักษาความ

ปลอดภัยของระบบเครือข่ายในเบื้องต้น เช่น เรื่องของการดาวน์โหลดและติดตั้งซอฟต์แวร์ที่ไม่ปลอดภัยเพื่อให้พนักงานได้ตระหนักถึงภัยของโปรแกรมประสงค์ร้ายที่อาจส่งผลต่อระบบคอมพิวเตอร์ในบริษัท รวมถึงการให้ความรู้เกี่ยวกับการตั้งรหัสผ่านที่เหมาะสมเพื่อให้เกิดความปลอดภัยในการเข้าถึงข้อมูล

ส่วนที่ 3 การวิเคราะห์ข้อมูลพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ตารางที่ 4.7 แสดงจำนวนร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐานของพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)

พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ	ระดับความสำคัญ					$\overline{X}$	SD	แปลผล	อันดับ
	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด				
1. การรักษาความลับของ Username และ Password	165 (50.5)	135 (41.3)	27 (8.3)	-	-	4.42	0.641	มากที่สุด	1
2. การไม่อนุญาตให้ผู้อื่นใช้ข้อมูลที่ตนเองรับผิดชอบ	134 (41.0)	156 (47.7)	36 (11.0)	1 (0.3)	-	4.29	0.669	มากที่สุด	2
3.การนำเข้าข้อมูลจากเว็บไซต์ที่ไม่มั่นใจในความปลอดภัย	21 (21.7)	125 (38.2)	120 (36.7)	11 (3.4)	-	3.78	0.821	มาก	3
4. หากท่านไม่อยู่ที่เครื่องคอมพิวเตอร์ของท่าน ท่านทำการ logoff ออกจากระบบทุกครั้ง	57 (17.4)	117 (35.8)	123 (37.6)	22 (6.7)	8 (2.4)	3.59	0.935	มาก	4
5. การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ	42 (12.8)	107 (32.7)	133 (40.7)	24 (7.3)	21 (6.4)	3.38	0.014	ปานกลาง	5
ภาพรวม	**48 (14.7)**	**187 (57.2)**	**87 (26.6)**	**5 (1.5)**	**-**	**3.85**	**0.673**	**มาก**	

จากตารางที่ 4.7 ผลการวิเคราะห์ข้อมูลจำนวนร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนของพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) ในภาพรวม พบว่า พฤติกรรมการรักษาความลับของ Username และ Password มีค่าเฉลี่ยมากที่สุด หมายความว่า พนักงานมีพฤติกรรมการรักษาความลับของ Username และ Password และพนักงานมีพฤติกรรมที่ไม่อนุญาตให้ผู้อื่นใช้ข้อมูลที่ตนเองรับผิดชอบในการเข้าข้อมูลต่าง ๆ แต่จะเห็นได้ว่า พฤติกรรมการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอมีค่าเฉลี่ยที่น้อยที่สุด หมายความว่าพนักงานไม่ได้ทำการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ และพฤติกรรมการ Logoff ออกจากระบบทุกครั้งเมื่อไม่ได้อยู่ที่เครื่องคอมพิวเตอร์ รวมถึงเรื่องของการนำเข้าข้อมูลจากเว็บไซต์ที่ไม่มั่นใจในความปลอดภัย เพราะฉะนั้นจึงควรให้ความรู้ความเข้าใจกับพนักงานในเรื่องของการปลี่ยนเปลี่ยนรหัสอย่างสม่ำเสมอและให้ความรู้ความเข้าใจในเรื่องของการออกจากระบบทุกครั้งที่ไม่ใช้งานแล้ว หรือเมื่อไม่อยู่กับเครื่องคอมพิวเตอร์เพื่อความปลอดภัยของข้อมูล และให้ความรู้กับพนักงานเกี่ยวกับการไม่นำเข้าข้อมูลจากเว็บไซต์ที่ไม่ปลอดภัย เพื่อเป็นการป้องกันไม่ให้เกิดความเสี่ยงที่จะเกิดขึ้นกับข้อมูลได้

ตารางที่ 4.8 แสดงจำนวนร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐานของพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)

พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล	ระดับความสำคัญ					$\overline{X}$	SD	แปลผล	อันดับ
	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด				
1. การปรับปรุงข้อมูลที่ทันสมัย	71 (21.7)	180 (55.0)	70 (21.4)	5 (1.5)	1 (0.3)	3.96	0.721	มาก	3
2. ปฏิบัติตามนโยบายด้านสิทธิ์การใช้ข้อมูล	80 (24.5)	188 (57.5)	57 (17.4)	2 (0.6)	-	4.06	0.664	มาก	1
3. ปฏิบัติตามนโยบายด้านความปลอดภัย	76 (23.2)	182 (55.7)	64 (19.6)	5 (1.5)	-	4.01	0.701	มาก	2
4. การอบรมเรื่องความปลอดภัย	45 (13.8)	122 (37.3)	118 (36.1)	37 (11.3)	5 (1.5)	3.50	0.920	มาก	5
5. ปฏิบัติงานด้วยความเข้าใจระบบ	63 (19.3)	178 (54.4)	70 (21.4)	15 (4.6)	1 (0.3)	3.88	0.778	มาก	4
ภาพรวม	**51 (15.6)**	**202 (61.8)**	**70 (21.4)**	**4 (1.2)**	**-**	**3.92**	**0.643**	**มาก**	

จากตารางที่ 4.8 ผลการวิเคราะห์ข้อมูลจำนวนร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐานของพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) ในภาพรวม พบว่าพฤติกรรมการปฏิบัติตามนโยบายด้านสิทธิ์การใช้ข้อมูลมีค่าเฉลี่ยมากที่สุด หมายความว่าพนักงานปฏิบัติตามนโยบายด้านสิทธิ์การใช้ข้อมูลและปฏิบัติตามนโยบายด้านความปลอดภัย เนื่องจากบริษัทได้มีการอบรมให้กับพนักงานที่มาทำงานในวันแรกของการทำงาน และได้บอกถึงนโยบายด้านสิทธิ์การใช้ข้อมูลและด้านความปลอดภัย เพื่อให้พนักงานทราบถึงวิธีการและขั้นตอนการปฏิบัติ แต่จะเห็นได้ว่าการอบรมเรื่องความปลอดภัยมีค่าเฉลี่ยน้อยที่สุด หมายความว่าบริษัทยังให้ความสำคัญกับเรื่องของความปลอดภัยทางด้านสารสนเทศในระดับน้อย ดังนั้นจึงควรให้ความรู้กับพนักงานในเรื่องของความปลอดภัยของระบบ เพื่อให้พนักงานเกิดความเข้าระบบในการทำงาน และมีการให้ความรู้กับพนักงานในเรื่องของการปรับปรุงข้อมูล เพื่อให้ข้อมูลมีความทันสมัยและมีความเป็นปัจจุบันมากขึ้น

ตารางที่ 4.9 แสดงจำนวนร้อยละ ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานของพฤติกรรมในการใช้งานที่เกี่ยวกับการเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ (Availability)

พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่างๆ ได้เมื่อต้องการ	**ระดับความสำคัญ**					$\overline{X}$	**SD**	**แปลผล**	**อันดับ**
	มากที่สุด	**มาก**	**ปานกลาง**	**น้อย**	**น้อยที่สุด**				
1.การใช้งานโปรแกรมตรวจสอบไวรัส	50 (15.3)	127 (38.8)	116 (35.5)	26 (8.0)	8 (2.4)	3.57	0.927	มาก	4
2.ระบบสามารถใช้งานได้ตลอดเวลา	54 (16.5)	159 (48.6)	105 (32.1)	7 (2.1)	2 (0.6)	3.78	0.763	มาก	3
3.อุปกรณ์และโปรแกรมมีความพร้อมในการใช้งาน	65 (19.9)	164 (50.2)	92 (28.1)	6 (1.8)	-	3.88	0.735	มาก	1
4. อุปกรณ์เครือข่ายมีความพร้อมในการใช้งาน	65 (19.9)	153 (46.8)	103 (31.5)	6 (1.8)	-	3.85	0.752	มาก	2
5. มีการทำสำรองข้อมูล	39 (11.9)	118 (36.1)	111 (33.9)	44 (13.5)	15 (4.6)	3.37	0.010	มาก	5
ภาพรวม	**44 (13.5)**	**153 (16.8)**	**121 (37.0)**	**8 (2.4)**	**1 (0.3)**	**3.71**	**0.739**	**มาก**	

จากตารางที่ 4.9 ผลการวิเคราะห์ข้อมูลจำนวนร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐานของพฤติกรรมในการใช้งานที่เกี่ยวกับการพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) ในภาพรวมพบว่าอุปกรณ์และโปรแกรมมีความพร้อมในการใช้งานมีค่าเฉลี่ยมากที่สุด หมายความว่าฮาร์ดแวร์และซอฟต์มีความพร้อมเพื่อให้กับพนักงานในการทำงาน และอุปกรณ์เครือข่ายของบริษัทก็มีความพร้อมในการใช้งาน เนื่องจากมีการตรวจเช็คและดูแลรักษาฮาร์แวร์ ซอฟต์แวร์ และอุปกรณ์เครือข่ายเพื่อให้มีความพร้อมในการใช้งาน รองรับการทำงานของพนักงานได้ แต่จะพบว่าพฤติกรรมการทำสำรองข้อมูลมีค่าเฉลี่ยในระดับน้อยที่สุดหมายความว่าพนักงานส่วนใหญ่ไม่ได้ให้ความสนใจกับการสำรองข้อมูล ซึ่งอาจส่งผลเสียกับข้อมูลได้ เช่น เครื่องคอมพิวเตอร์เกิดการขัดข้องกับฮาร์ดดิสก์จะส่งผลให้ข้อมูลไม่สามารถกู้กลับมาได้ เป็นต้น ดังนั้นทางบริษัทจึงควรให้คำแนะนำกับพนักงานในการทำสำรองข้อมูล รวมถึงเรื่องของการใช้งานโปรแกรมตรวจสอบไวรัส ทางแผนกที่เกี่ยวข้องกับระบบคอมพิวเตอร์ควรให้ความสำคัญในการตรวจสอบไวรัส และให้ความรู้กับพนักงานเพื่อไม่ให้เกิดผลเสียกับทั้งฮาร์ดแวร์และซอฟต์แวร์ของบริษัท

ส่วนที่ 4 การวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐาน

สมมติฐานที่ 1 ปัจจัยส่วนบุคคลที่แตกต่างกัน ส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

สมมติฐานที่ 1.1 เพศที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

H_0 : เพศที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่ไม่แตกต่างกัน

H_1 : เพศที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

สำหรับสถิติที่ใช้ในการวิเคราะห์จะใช้สถิติ Independent Samples t-test เพื่อทดสอบความแตกต่างค่าเฉลี่ยของค่าประชากร 2 กลุ่ม โดยปฏิเสธสมมติฐานหลัก (H_0) เมื่อพบว่าค่า Sig น้อยกว่า 0.05

ตารางที่ 4.10 การทดสอบความแตกต่างระหว่างลักษณะส่วนบุคคลด้านเพศส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์

พฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร	เพศ	$\overline{X}$	SD	t	df	Sig.
1. พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)	ชาย	3.94	0.684	2.944	325	**0.003***
	หญิง	3.72	0.639			
2. พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)	ชาย	3.99	0.638	2.583	325	**0.010***
	หญิง	3.81	0.636			
3. พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)	ชาย	3.74	0.699	1.029	325	0.304
	หญิง	3.66	0.790			
ภาพรวม	**ชาย**	**3.91**	**0.627**	**2.400**	**325**	**0.017**
	หญิง	**3.74**	**0.622**			

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.10 ผลการทดสอบความแตกต่างระหว่างเพศที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ ทำการทดสอบโดยการใช้สถิติ Independent Samples t-test เพื่อทดสอบความแตกต่างของค่าเฉลี่ยของประชากร 2 กลุ่ม ผลการวิเคราะห์พบว่าเพศชายมีพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) มากกว่าพนักงานหญิง อย่างมีนัยสำคัญทางสถิติ อาจเป็นไปได้ว่าพนักงานชายมีการใช้งานระบบและเจอปัญหาความปลอดภัยมากกว่าพนักงานหญิงจึงทำให้มีความตระหนักรู้สูงกว่าพนักงานหญิง ดังนั้นในการฝึกอบรมจึงควรให้ความสนใจกับพนักงานหญิงเพิ่มขึ้น เพื่อเพิ่มความสนใจและสร้างความเข้าใจในการใช้งานมากขึ้น

สมมติฐานที่ 1.2 อายุแตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

H_0 : อายุที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่ไม่แตกต่างกัน

H_1 : อายุที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

สำหรับสถิติที่ใช้ในการวิเคราะห์จะใช้สถิติ F-test หรือ One-way ANOVA เพื่อทดสอบความแตกต่างค่าเฉลี่ยของค่าประชากรมากกว่า 2 กลุ่ม โดยระดับความเชื่อมั่นที่ 95% ซึ่งปฏิเสธสมมติฐานหลัก (H_0) เมื่อพบว่าค่า Sig น้อยกว่า 0.05

ตารางที่ 4.11 การทดสอบความแตกต่างกันระหว่างลักษณะส่วนบุคคลด้านอายุส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์

พฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร	ความแปรปรวน	SS	df	MS	F	Sig.
1. พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)	ระหว่างกลุ่ม	4.501	5	0.900	2.018	0.076
	ภายในกลุ่ม	143.157	321	0.446		
	รวม	147.657	326			
2. พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)	ระหว่างกลุ่ม	1.297	5	0.259	0.624	0.682
	ภายในกลุ่ม	133.473	321	0.416		
	รวม	134.771	326			
3. พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)	ระหว่างกลุ่ม	2.092	5	0.418	0.764	0.576
	ภายในกลุ่ม	175.725	321	0.547		
	รวม	177.817	326			
ภาพรวม	**ระหว่างกลุ่ม**	**1.838**	**5**	**0.368**	**0.928**	**0.463**
	ภายในกลุ่ม	**127.244**	**321**	**0.396**		
	รวม	**129.083**	**326**			

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.11 ผลการทดสอบความแตกต่างระหว่างอายุที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ ทำการทดสอบโดยการใช้สถิติ One-way ANOVA เพื่อทดสอบความแตกต่างของค่าเฉลี่ยของประชากรมากกว่า 2 กลุ่ม ผลการวิเคราะห์พบว่าอายุที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ในภาพรวมที่ไม่แตกต่างกันอย่างมีนัยสำคัญ หมายความว่า อายุส่งผลกับพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) เนื่องจากพนักงานที่อายุมาก มีประสบการณ์มากกว่าพนักงานที่อายุน้อย ดังนั้นพนักงานที่มีอายุมากจึงมีสิทธิ์ในการเข้าถึงข้อมูลที่มากกว่า สรุปได้ว่า อายุที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่ไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

สมมติฐานที่ 1.3 ระดับการศึกษาที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

H_0 *:* ระดับการศึกษาที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่ไม่แตกต่างกัน

H_1 *:* ระดับการศึกษาที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

สำหรับสถิติที่ใช้ในการวิเคราะห์จะใช้สถิติ Independent Samples t-test เพื่อทดสอบความแตกต่างค่าเฉลี่ยของค่าประชากร 2 กลุ่ม โดยปฏิเสธสมมติฐานหลัก (H_0) เมื่อพบว่าค่า Sig น้อยกว่า 0.05

ตารางที่ 4.12 การทดสอบความแตกต่างระหว่างลักษณะส่วนบุคคลด้านระดับการศึกษาส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์

พฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร	ระดับการศึกษา	$\overline{X}$	SD	t	df	Sig.
1. พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)	ปริญญาตรี สูงกว่าปริญญาตรี	3.83 4.29	0.670 0.588	-2.823	325	**0.005***
2. พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)	ปริญญาตรี สูงกว่าปริญญาตรี	3.90 4.29	0.640 0.588	-2.501	325	0.013
3. พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)	ปริญญาตรี สูงกว่าปริญญาตรี	3.67 4.35	0.725 0.702	0.918	325	**0.000***
ภาพรวม	**ปริญญาตรี สูงกว่าปริญญาตรี**	**3.80 4.47**	**0.617 0.514**	**-4.397**	**325**	**0.000***

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.12 ผลการทดสอบความแตกต่างระหว่างระดับการศึกษาที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ ทำการทดสอบโดยการใช้สถิติ Independent Samples t-test เพื่อทดสอบความแตกต่างของค่าเฉลี่ยของประชากร 2 กลุ่ม ผลการวิเคราะห์พบว่าระดับการศึกษาสูงกว่าปริญญาตรีมีพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) และพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) ที่สูงกว่าระดับปริญญาตรีอย่างมีนัยสำคัญทางสถิติ หมายความว่าพนักงานที่มีระดับการศึกษาที่สูงกว่าปริญญาตรี ส่วนใหญ่แล้วจะเป็นผู้ที่มีตำแหน่งทางการทำงาน ทำให้การทำงานส่วนใหญ่แล้วจะดูภาพรวมของการทำงาน ทำให้มีพฤติกรรมการใช้งานระบบมากกว่าเมื่อเทียบกับพนักงานที่มีการศึกษาระดับปริญญาตรี จะเป็นพนักงานที่อยู่ระดับปฏิบัติการจึงมีการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่น้อยกว่า

สมมติฐานที่ 1.4 แผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

H_0 *:* แผนกงานที่เกี่ยวข้องที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่ไม่แตกต่างกัน

H_1 *:* แผนกงานที่เกี่ยวข้องที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

สำหรับสถิติที่ใช้ในการวิเคราะห์จะใช้สถิติ F-test หรือ One-way ANOVA เพื่อทดสอบความแตกต่างค่าเฉลี่ยของค่าประชากรมากกว่า 2 กลุ่ม โดยระดับความเชื่อมั่นที่ 95% ซึ่งปฏิเสธสมมติฐานหลัก (H_0) เมื่อพบว่าค่า Sig น้อยกว่า 0.05

ตารางที่ 4.13 การทดสอบความแตกต่างระหว่างลักษณะส่วนบุคคลด้านแผนกงานที่เกี่ยวข้องส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์

พฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร	ความแปรปรวน	SS	df	MS	F	Sig.
1. พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)	ระหว่างกลุ่ม	19.036	8	2.379	5.883	**0.000***
	ภายในกลุ่ม	128.622	318	0.404		
	รวม	147.657	326			
2. พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)	ระหว่างกลุ่ม	23.835	8	2.979	8.541	**0.000***
	ภายในกลุ่ม	110.935	318	0.349		
	รวม	134.771	326			
3. พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)	ระหว่างกลุ่ม	21.706	8	2.713	5.527	**0.000***
	ภายในกลุ่ม	156.111	318	0.491		
	รวม	177.817	326			
ภาพรวม	**ระหว่างกลุ่ม**	**20.990**	**8**	**2.624**	**7.719**	**0.000***
	ภายในกลุ่ม	**108.092**	**318**	**0.340**		
	รวม	**129.083**	**326**			

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.13 ผลการทดสอบความแตกต่างระหว่างแผนกงานที่เกี่ยวข้องที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ทำการทดสอบโดยการใช้สถิติ One-way ANOVA เพื่อทดสอบความแตกต่างของค่าเฉลี่ยของประชากรมากกว่า 2 กลุ่ม ผลการวิเคราะห์พบว่าแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ในภาพรวมที่แตกต่างกัน โดยมีค่า Sig. เท่ากับ 0.000 ซึ่งน้อยกว่าระดับนัยสำคัญ 0.05 สรุปได้ว่า แผนกงานที่เกี่ยวข้องที่แตกต่างกันส่งผลต่อส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

เมื่อพิจารณาเป็นรายด้าน พบว่า ด้านพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) และด้านพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) ผลการทดสอบ มีค่า Sig. เท่ากับ 0.000 ทั้งสามด้านซึ่งน้อยกว่าระดับนัยสำคัญ 0.05 จึงสรุปได้ว่า แผนกงานที่เกี่ยวข้องที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน จึงทำการทดสอบความแตกต่างรายคู่โดยวิธี LSD ดังแสดงในตารางที่ 4.14

ตารางที่ 4.14 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)

แผนกงานที่เกี่ยวข้อง	**กลุ่ม J**	**บรรณาธิการข่าว**	**การขาย การตลาด**	**เลขานุการ / แอดมินฝ่าย**	**เทคโนโลยีสารสนเทศ**	**กฎหมาย**	**โปรแกรมเมอร์**	**ทรัพยากรมนุษย์**	**กราฟฟิก / ตัดต่อ**	**พัสดุ / ก่อสร้าง ซ่อมบำรุง**
กลุ่ม I	**Mean**	**3.86**	**3.90**	**3.90**	**4.41**	**4.06**	**3.83**	**3.44**	**3.91**	**3.43**
บรรณาธิการข่าว	3.86	-	-0.040 (0.718)	-0.044 (0.834)	-0.553 **(0.000)***	-0.209 (0.110)	0.022 (0.933)	0.416 **(0.004)***	-0.057 (0.611)	0.427 **(0.001)***
การขาย / การตลาด	3.90		-	-0.004 (0.985)	-0.513 (0.002)	-0.169 (0.251)	0.063 (0.821)	0.456 **(0.004)***	-0.017 (0.896)	0.467 **(0.001)***
เลขานุการ / แอดมินฝ่าย	3.90			-	-0.509 **(0.037)***	-0.165 (0.477)	0.067 (0.839)	0.460 (0.054)	-0.013 (0.953)	0.471 **(0.040)***

ตารางที่ 4.14 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) (ต่อ)

แผนกงานที่เกี่ยวข้อง	กลุ่ม J	บรรณาธิการข่าว	การขาย การตลาด	เลขานุการ/แอดมินฝ่าย	เทคโนโลยีสารสนเทศ	กฎหมาย	โปรแกรมเมอร์	ทรัพยากรมนุษย์	กราฟฟิก / ตัดต่อ	พัสดุ / กองซ่อมบำรุง
เทคโนโลยีสารสนเทศ	4.41				-	0.345 (0.053)	0.576 (0.050)	0.969 **(0.000)***	0.496 **(0.003)***	0.981 **(0.000)***
กฎหมาย	4.06					-	0.231 (0.416)	0.625 **(0.000)***	0.151 (0.306)	0.636 **(0.000)***
โปรแกรมเมอร์	3.83						-	0.393 (0.175)	-0.080 (0.773)	0.405 (0.151)
ทรัพยากรมนุษย์	3.44							-	-0.473 **(0.003)***	0.011 (0.945)
กราฟฟิก / ตัดต่อ	3.91								-	0.484 **(0.001)***
พัสดุ / กองซ่อมบำรุง	3.43									-

* มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.14 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) ที่แตกต่างกัน พบว่า กลุ่มแผนกงานเทคโนโลยีสารสนเทศ มีการใช้งานด้านสิทธิ์ในการเข้าถึงข้อมูลสูงกว่าเกือบทุกกลุ่ม อันได้แก่ แผนกบรรณาธิการ เลขานุการ/แอดมินฝ่าย ทรัพยากรมนุษย์ กราฟฟิก/ตัดต่อ และพัสดุ/กองซ่อมบำรุงอย่างมีนัยสำคัญทางสถิติ อันเนื่องมาจากแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ในการดูแลสิทธิ์ในการเข้าถึงข้อมูลของฝ่ายต่าง ๆ จึงทำให้ฝ่ายเทคโนโลยีสารสนเทศจำเป็นที่จะต้องสามารถเข้าถึงสิทธิ์ในการเข้าข้อมูลของแผนกต่าง ๆ เพื่อในการจัดการ และป้องกันปัญหาการใช้งานของพนักงานในแผนกต่าง ๆ ในส่วนของแผนกทรัพยากรมนุษย์มีการใช้งานด้านสิทธิ์ในการเข้าถึงข้อมูล ได้แก่ แผนกบรรณาธิการข่าว แผนกการขาย/การตลาด เทคโนโลยีสารสนเทศ กราฟฟิก/ตัดต่อและกฎหมาย อันเนื่องมาจาก แผนกทรัพยากรมนุษย์

มีความจำเป็นที่จะต้องดูแลในเรื่องของบุคลากรในแต่ละแผนก และการจัดการเวลาเข้าออกงานของพนักงานในแต่ละแผนก รวมถึงการจัดกิจกรรมให้กับพนักงาน และแผนกพัสดุ/กองซ่อมบำรุง มีการใช้งานด้านสิทธิ์ในการเข้าถึงข้อมูลน้อยที่สุดเกือบทุกกลุ่มอันเนื่องมาจากแผนกพัสดุ/กองซ่อมบำรุง มีลักษณะของงานที่ไม่เกี่ยวข้องกับแผนกอื่น เช่น แผนกพัสดุ จะมะหน้าที่ในการดูแล จัดการจัดเก็บวัสดุ อุปกรณ์ต่าง ๆ ที่ใช้ในบริษัท และแผนกกองซ่อมบำรุง จะมีหน้าที่ในการดูแลเกี่ยวกับอะไหล่และยานยนต์ จึงไม่มีความจำเป็นที่จะต้องมีสิทธิ์ที่จะเข้าถึงข้อมูลของแผนกอื่น ๆ

ตารางที่ 4.15 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)

แผนกงานที่เกี่ยวข้อง	**กลุ่ม J**	**บรรณาธิการข่าว**	**การขาย การตลาด**	**เลขานุการ / แอดมินฝ่าย**	**เทคโนโลยีสารสนเทศ**	**กฎหมาย**	**โปรแกรมเมอร์**	**ทรัพยากรมนุษย์**	**กราฟฟิก / ตัดต่อ**	**พัสดุ / กองซ่อมบำรุง**
กลุ่ม I	**Mean**	**3.87**	**3.98**	**3.90**	**4.64**	**4.00**	**4.83**	**3.56**	**3.89**	**3.60**
บรรณาธิการข่าว	3.87	-	-0.114 (0.270)	-0.035 (0.860)	-0.771 **(0.000)***	-0.135 (0.266)	-0.968 **(0.000)***	0.305 (0.021)	-0.026 (0.804)	0.265 **(0.022)***
การขาย / การตลาด	3.98		-	0.079 (0.700)	-0.657 **(0.000)***	-0.021 (0.878)	-0.854 (0.001)	0.419 (0.004)	0.088 (0.471)	0.379 **(0.004)***
เลขานุการ / แอดมินฝ่าย	3.90			-	-0.736 **(0.001)***	-0.100 (0.642)	-0.933 **(0.002)***	0.340 (0.125)	0.009 (0.966)	0.300 (0.158)
เทคโนโลยีสารสนเทศ	4.64				-	0.636 **(0.000)***	-0.197 0.470	1.076 **(0.000)***	0.745 **(0.000)***	1.036 **(0.000)***
กฎหมาย	4.00					-	0.833 **(0.002)***	0.440 **(0.006)***	0.109 (0.429)	4.000 **(0.006)***
โปรแกรมเมอร์	4.83						-	1.273 **(0.000)***	0.942 **(0.000)***	1.233 **(0.000)***
ทรัพยากรมนุษย์	3.56							-	-0.331 (0.025)	-0.040 (0.796)

ตารางที่ 4.15 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) (ต่อ)

แผนกงานที่เกี่ยวข้อง	กลุ่ม J	บรรณาธิการข่าว	การขายการตลาด	เลขานุการ / แอดมินฝ่าย	เทคโนโลยีสารสนเทศ	กฎหมาย	โปรแกรมเมอร์	ทรัพยากรมนุษย์	กราฟฟิก / ตัดต่อ	พัสดุ / กองซ่อมบำรุง
กราฟฟิก / ตัดต่อ	3.89								-	-0.040 (0.796)
พัสดุ / กองซ่อมบำรุง	3.60									-

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.14 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) ที่แตกต่างกัน พบว่า กลุ่มแผนกงานโปรแกรมเมอร์ มีค่าเฉลี่ยมากกว่า กลุ่มแผนกเทคโนโลยีสารสนเทศ กฎหมาย ทรัพยากรณ์มนุษย์ กราฟฟิค/ตัดต่อ กองซ่อมบำรุงตามลำดับอย่างมีนัยสำคัญทางสถิติ หมายความว่าแผนกโปรแกรมเมอร์เป็นแผนกที่ดูแลเกี่ยวกับเว็บไซต์และแอพพลิเคชันของบริษัท จึงต้องมีความจำเป็นจะต้องดูแลจัดการเว็บไซต์และแอพพลิเคชันให้มีความพร้อมสำหรับการใช้งานต่าง ๆ มากกว่าส่วนของแผนกเลขานุการ /แอดมินฝ่าย กฎหมาย และบรรณาธิการข่าว จะเห็นได้ว่าแผนกบรรณาธิการข่าวเป็นฝ่ายที่มีการเขียนข่าวและค้นหาข่าวจึงเป็นฝ่ายที่มีความสำคัญที่จะสร้างความถูกต้องของเนื้อหาต่าง ๆ จะเห็นได้ว่าแผนกทรัพยากรมนุษย์ กราฟฟิก/ตัดต่อ พัสดุ/กองซ่อมบำรุง มีค่าเฉลี่ยน้อยหมายความว่าแผนกเหล่านี้ไม่มีส่วนร่วมโดยตรงกับการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูลในการทำงาน

ตารางที่ 4.16 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับการเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ (Availability)

แผนกงานที่เกี่ยวข้อง	กลุ่ม J	บรรณาธิการข่าว	การขาย การตลาด	เลขานุการ / แอดมินฝ่าย	เทคโนโลยีสารสนเทศ	กฎหมาย	โปรแกรมเมอร์	ทรัพยากรมนุษย์	กราฟฟิก / ตัดต่อ	พัสดุ / กองซ่อมบำรุง
กลุ่ม I	**Mean**	**3.62**	**3.63**	**4.10**	**4.41**	**3.97**	**3.83**	**3.40**	**3.78**	**3.40**
บรรณาธิการข่าว	3.62	-	-0.010 (0.937)	-0.485 **(0.037)***	-0.794 **(0.000)***	-0.352 **(0.015)***	-0.218 (0.459)	0.215 (0.169)	-0.167 (0.179)	0.215 (0.117)
การขาย / การตลาด	3.63		-	-0.475 (0.052)	-0.784 **(0.000)***	-0.343 **(0.035)***	-0.208 (0.493)	0.225 0.194	-0.158 (0.276)	0.225 (0.150)
เลขานุการ / แอดมินฝ่าย	4.10			-	-0.309 (0.248)	0.132 (0.604)	0.267 (0.462)	0.700 **(0.008)***	0.317 (0.195)	0.700 **(0.006)***
เทคโนโลยีสารสนเทศ	4.41				-	0.441 **(0.025)***	0.576 (0.075)	1.009 **(0.000)***	0.626 (0.001)	1.009 **(0.000)***
กฎหมาย	3.97					-	0.134 (0.667)	0.568 **(0.003)***	0.185 (0.256)	0.568 **(0.001)***
โปรแกรมเมอร์	3.83						-	0.433 (0.175)	0.051 (0.868)	0.433 (0.163)
ทรัพยากรมนุษย์	3.40							-	-0.383 (0.029)	0.000 (1.000)
กราฟฟิก / ตัดต่อ	3.78								-	0.383 (0.029)
พัสดุ / กองซ่อมบำรุง	3.40									-

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.16 การเปรียบเทียบค่าเฉลี่ยรายคู่ของแผนกงานที่เกี่ยวข้องแตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) ที่แตกต่างกัน พบว่า กลุ่มแผนกงานเทคโนโลยีสารสนเทศ มีค่าเฉลี่ยมากกว่าแผนกเลขานุการ/แอดมิน แผนกกฎหมาย แผนกโปแกรมเมอร์ ทรัพยากรมนุษย์อย่างมีนัยสำคัญทางสถิติ หมายความว่าแผนกเทคโนโลยีสารสนเทศ สามารถเข้าถึงข้อมูลได้ตามต้องการมากกว่าแผนกอื่น ๆ เนื่องจากแผนกเทคโนโลยีสารสนเทศ

จะต้องทำการดูแลระบบและดูแลข้อมูลของแผนกต่าง ๆ ไม่ว่าจะเป็นแผนกบรรณาธิการข่าว แผนกการขาย /การตลาด และสามารถแก้ไขปัญหาได้ เมื่อเกิดความขัดข้องของระบบ จึงจำเป็นที่จะต้องเข้าถึงข้อมูลได้ตามต้องการ ในส่วนของแผนกเลขานุการ/แอดมินฝ่าย จะสามารถเข้าถึงข้อมูลได้ตามต้องการ เนื่องจากฝ่ายเลขานุการและแอดมินฝ่าย จะต้องดูแลเกี่ยวกับงานและเอกสารในแผนก เช่น การเบิกโอทีของพนักงาน การแจ้งซ่อมอุปกรณ์ในแผนก เป็นต้น ในส่วนของแผนกกฎหมายจะมีลักษณะของงานที่ดูแลในเรื่องของการตรวจสอบ คดีความและป้องกันไม่ให้เกิดความผิดต่าง ๆ ตามกฎหมายจึงมีการเข้าถึงข้อมูลที่น้อยกว่าฝ่ายเทคโนโลยีสารสนเทศและในส่วนแผนกทรัพยากรณ์มนุษย์และแผนกพัสดุ/กองซ่อมบำรุง เป็นแผนกที่มีการใช้งานที่เกี่ยวข้องกับการเข้าถึงข้อมูลได้ตามต้องการน้อยกว่าแผนกเลขานุการ/แอดมินฝ่าย เทคโนโลยีสารสนเทศ และกฎหมาย เนื่องจากเป็นแผนกที่ลักษณะของงานส่วนมากไม่มีการเข้าระบบคอมพิวเตอร์ จึงมีการเข้าระบบคอมพิวเตอร์เป็นส่วนน้อย

สมมติฐานที่ 1.5 อายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

H_0 : อายุการทำงานที่แตกต่างกันส่งผลต่อส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่ไม่แตกต่างกัน

H_1 : อายุการทำงานที่แตกต่างกันส่งผลต่อส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

สำหรับสถิติที่ใช้ในการวิเคราะห์จะใช้สถิติ F-test หรือ One-way ANOVA เพื่อทดสอบความแตกต่างค่าเฉลี่ยของค่าประชากรมากกว่า 2 กลุ่ม โดยระดับความเชื่อมั่นที่ 95% ซึ่งปฏิเสธสมมติฐานหลัก (H_0) เมื่อพบว่าค่า Sig น้อยกว่า 0.05

ตารางที่ 4.17 การทดสอบความแตกต่างระหว่างลักษณะส่วนบุคคลที่มีอายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์

พฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร		ความแปรปรวน	SS	df	MS	F	Sig.
1.	พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)	ระหว่างกลุ่ม	4.861	4	1.215	2.740	**0.029***
		ภายในกลุ่ม	142.797	322	0.443		
		รวม	147.657	326			
2.	พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)	ระหว่างกลุ่ม	3.797	4	0.949	2.334	0.056
		ภายในกลุ่ม	130.974	322	0.407		
		รวม	134.771	326			
3.	พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)	ระหว่างกลุ่ม	6.102	4	1.526	2.861	**0.024***
		ภายในกลุ่ม	171.714	322	0.533		
		รวม	177.817	326			
ภาพรวม		**ระหว่างกลุ่ม**	**4.388**	**4**	**1.097**	**2.833**	**0.025**
		ภายในกลุ่ม	**124.695**	**322**	**0.387**		
		รวม	**129.083**	**326**			

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.17 ผลการทดสอบความแตกต่างระหว่างอายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ ทำการทดสอบโดยการใช้สถิติ One-way ANOVA เพื่อทดสอบความแตกต่างของค่าเฉลี่ยของประชากรมากกว่า 2 กลุ่ม ผลการวิเคราะห์พบว่าอายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ในภาพรวมแตกต่างกัน โดยมีค่า Sig. เท่ากับ 0.025 ซึ่งน้อยกว่าระดับนัยสำคัญ 0.05 สรุปได้ว่า อายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

เมื่อพิจารณาเป็นรายด้าน พบว่า ด้านพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) และด้านพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) ผลการทดสอบ มีค่า Sig. เท่ากับ 0.029 และ 0.024 ซึ่งน้อยกว่าระดับนัยสำคัญ 0.05 จึงสรุปได้ว่า อายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์แตกต่างกัน ส่วนด้านพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้อง

สมบูรณ์ของข้อมูล (Integrity) ผลการทดสอบ มีค่า Sig. เท่ากับ 0.056 ซึ่งมากกว่าระดับนัยสำคัญ 0.05 จึงสรุปได้ว่า รายได้อายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์แตกต่างกัน จึงทำการทดสอบความแตกต่างรายคู่โดยวิธี LSD ดังแสดงในตารางที่ 4.18

ตารางที่ 4.18 แสดงการเปรียบเทียบค่าเฉลี่ยรายคู่ของอายุการทำงานที่แตกต่างกันส่งผลต่อการส่งผลส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่างๆ (Confidentiality)

อายุการทำงาน	**กลุ่ม J**	น้อยกว่า 1 ปี	1 - 2 ปี	3 - 4 ปี	5 - 10 ปี	มากกว่า 10 ปี
กลุ่ม I	**Mean**	3.44	3.78	3.87	3.96	4.00
น้อยกว่า 1 ปี	3.44	-	-0.343 (0.054)	-0.433 **(0.017)***	-0.526 **(0.004)***	-0.563 **(0.011)***
1 - 2 ปี	3.78		-	-0.090 (0.333)	-0.183 (0.059)	-0.219 0.158
3 - 4 ปี	3.87			-	-0.092 (0.360)	-0.129 0.414
5 - 10 ปี	3.96				-	-0.037 (-0.819)
มากกว่า 10 ปี	4.00					

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.18 ผลจากการเปรียบเทียบค่าเฉลี่ยรายคู่ของอายุการทำงานที่แตกต่างกันส่งผลต่อการส่งผลส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่างๆ (Confidentiality) แตกต่างกัน พบว่า กลุ่มที่มีอายุการทำงานมากกว่า 10 ปี มีค่าเฉลี่ยมากกว่า กลุ่มที่มีอายุการทำงาน 5 - 10 ปี และ อายุการทำงาน 3 - 4 ปี อย่างมีนัยสำคัญทางสถิติ หมายความว่าพนักงานที่มีอายุการทำงานมากกว่า 10 ปี ส่งผลต่อการส่งผลส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ เนื่องจากมีความรู้มีความสามารถและมีตำแหน่งงานที่มากกว่ากลุ่มพนักงานที่มีอายุการทำงานน้อยกว่า 1 ปี ในส่วนของอายุการทำงาน 5 - 10 ปี และ 3 - 4 ปี เป็นกลุ่มพนักงานที่มีประสบการณ์ในการทำงานที่มากกว่ากลุ่มพนักงานที่มีอายุการทำงานน้อยกว่า 1 ปี ซึ่งพนักงานที่มีอายุการทำงานน้อยกว่า 1 ปี อาจเป็นพนักงานที่อยู่ในช่วง

ทดลองงานหรือมีประสบการณ์การทำงานน้อย ดังนั้นทางแผนกเทคโนโลยีสารสนเทศจะมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ โดยจะมีการแบ่งสิทธิ์ตามแผนก ฝ่าย และตำแหน่งงานในการเข้าถึงข้อมูลต่าง ๆ

ตารางที่ 4.19 แสดงการเปรียบเทียบค่าเฉลี่ยรายคู่ของอายุการทำงานที่แตกต่างกันส่งผลต่อการส่งผลส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)

อายุการทำงาน	**กลุ่ม J**	น้อยกว่า 1 ปี	1 - 2 ปี	3 - 4 ปี	5 - 10 ปี	มากกว่า 10 ปี
กลุ่ม I	**Mean**	3.38	3.59	3.73	3.85	3.91
น้อยกว่า 1 ปี	3.38	-	-0.213 (0.276)	-0.356 (0.072)	-0.479 **(0.017)***	-0.534 **(0.027)***
1 - 2 ปี	3.59		-	-0.143 (0.161)	-0.266 **(0.012)***	-0.321 (0.060)
3 - 4 ปี	3.73			-	-0.122 (0.269)	-0.178 (0.305)
5 - 10 ปี	3.85				-	-0.055 (0.752)
มากกว่า 10 ปี	3.91					

* มีนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4.19 ผลจากการเปรียบเทียบค่าเฉลี่ยรายคู่ของอายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กรที่แตกต่างกันด้านพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) เป็นแบบรายคู่ พบว่ากลุ่มที่มีอายุการทำงานมากกว่า 10 ปี มีค่าเฉลี่ยมากกว่ากลุ่มที่มีอายุการทำงาน 5 - 10 ปี ตามลำดับอย่างมีนัยสำคัญทางสถิติ หมายความว่ากลุ่มอายุการทำงานมากกว่า 10 ปี สามารถที่จะเข้าดูข้อมูลต่าง ๆ ได้ตามต้องการ เนื่องจากอายุการทำงานมากกว่า 10 ปี จะเป็นพนักงานที่มีตำแหน่งทางการทำงาน ในส่วนของอายุการทำงาน 5 - 10 ปี จะเป็นผู้ที่มีประสบการณ์การทำงานมากกว่ากลุ่มอายุการทำงาน 1 - 2 ปี ดังนั้นบริษัทจะมีการดูแลระบบเพื่อให้พนักงานสามารถเข้าถึงข้อมูลได้ และมีการเข้าถึงข้อมูลโดยแบ่งตามแผนก และสิทธิ์ในการเข้าถึงของแต่ละพนักงาน

สมมติฐานที่ 2 ระดับความรู้เรื่องความปลอดภัยมีความสัมพันธ์กับพฤติกรรมการใช้งานระบบรักษาความปลอดภัย

สำหรับสถิติที่ใช้ในการวิเคราะห์จะใช้การทดสอบด้วยการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์ของเพียรสัน (Pearson's Product Moment Correlation Coefficient) โดยระดับความเชื่อมั่นที่ 95% ซึ่งปฏิเสธสมมติฐานหลัก (H_0) เมื่อพบว่าค่า Sig น้อยกว่า 0.05

ตารางที่ 4.20 ผลการวิเคราะห์การหาค่าความสัมพันธ์ของระดับความรู้เรื่องความปลอดภัยและพฤติกรรมการใช้งานระบบรักษาความปลอดภัย

พฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร	**ระดับความรู้เรื่องความปลอดภัย**			
	r (Pearson Correlation)	**Sig. (2-tailed)**	**ระดับความสัมพันธ์**	**ทิศทาง**
พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality)	0.536	**0.000***	ปานกลาง	เดียวกัน
พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)	0.489	**0.000***	ปานกลาง	เดียวกัน
พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)	0.629	**0.000***	สูง	เดียวกัน

* มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.20 ผลการวิเคราะห์ความสัมพันธ์เรื่องระดับความรู้เรื่องความปลอดภัยมีความสัมพันธ์กับพฤติกรรมการใช้งานระบบรักษาความปลอดภัย ประกอบด้วย พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) มีความสัมพันธ์ต่อพฤติกรรมการใช้งานระบบรักษาความปลอดภัย พบว่า ความรู้มีความสัมพันธ์กับพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) สูงกว่าพฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)

และพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) อย่างมีนักสำคัญ หมายความว่าพนักงานมีความรู้ในเรื่องของการใช้งานที่เข้าถึงข้อมูลต่าง ๆ ได้และสามารถเข้าถึงข้อมูลต่าง ๆ ได้ แต่ในส่วนของความรู้การใช้งานสิทธิ์ในการเข้าถึงข้อมูล และการใช้งานเกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูลอยู่ในระดับปานกลาง ดังนั้นบริษัทจะต้องมีการให้ความสำคัญที่จะสร้างความรู้และความเข้าใจในพฤติกรรมทั้งสามด้าน คือพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และพฤติกรรมในการใช้งานที่เกี่ยวกับความร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) เพราะหากพนักงานขาดความรู้จะส่งผลต่อพฤติกรรมในการใช้งานที่จะส่งผลต่อระบบความปลอดภัยคอมพิวเตอร์ ดังนั้นบริษัทจะต้องมีการอบรมความรู้ในเรื่องของการใช้งาน และในเรื่องของความปลอดภัยระบบคอมพิวเตอร์ให้กับพนักงาน

บทที่ 5
สรุปผลการวิจัย การอภิปรายผล และข้อเสนอแนะ

การศึกษาเรื่อง ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษา บริษัท ไทยรัฐ กรุ๊ป ในครั้งนี้ได้รวบรวมข้อมูลโดยการตอบแบบสอบถามจากพนักงานที่ใช้งานเครื่องคอมพิวเตอร์ จำนวน 327 ชุด สามารถสรุปผลการวิจัยได้ดังนี้

5.1 สรุปผลการวิจัย

5.2 การอภิปรายผลการวิจัย

5.3 ข้อเสนอแนะที่ได้จากการวิจัย

5.4 ข้อเสนอแนะสำหรับองค์กร

5.5 งานวิจัยที่เกี่ยวเนื่องในอนาคต

5.1 สรุปผลการวิจัย

ส่วนที่ 1 การวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม ผลการศึกษาพบว่าผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศชาย อยู่ในช่วงอายุ 26 - 30 ปี ซึ่งมีระดับการศึกษาอยู่ที่ระดับปริญญาตรี โดยส่วนผู้ที่ตอบแบบสอบถามส่วนใหญ่อยู่แผนกบรรณาธิการข่าว และมีอายุการทำงานระหว่าง 1-2 ปี จากผลการสำรวจจะเห็นว่าพนักงานของบริษัท ไทยรัฐ กรุ๊ป จะเป็นกลุ่มคนรุ่นใหม่ ที่เพิ่งจบการศึกษาหรือมีประสบการณ์ทำงานมาก่อน

ส่วนที่ 2 การวิเคราะห์ข้อมูลความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ผลการศึกษาพบว่า ความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กรอยู่ในระดับมาก เมื่อพิจารณารายละเอียดพบว่า กฎการรักษาความปลอดภัยข้อมูลองค์กร มีความสำคัญอยู่ในระดับมากที่สุด จะเห็นได้ว่าพนักงานมีความรู้ในเรื่องของความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กรที่ใช้ในการทำงาน แต่จะเห็นได้ว่าความรู้เกี่ยวกับความหมายของโปรแกรมประสงค์ร้ายต่อระบบอยู่ในระดับน้อยที่สุด หมายความว่าพนักงานยังขาดความรู้ในเรื่องของโปรแกรมประสงค์ร้าย ที่อาจส่งผลต่อความปลอดภัย ระบบคอมพิวเตอร์ของบริษัท ส่งผลให้เกิดพฤติกรรมที่อาจส่งผลเสียตามมา ดังนั้นทางบริษัทจะต้องมีการให้ความรู้กับพนักงานในเรื่องของ

ความปลอดภัยของระบบคอมพิวเตอร์ รวมถึงความรู้ในทุกด้าน เช่น การจัดการรหัสผ่านที่เหมาะสม การป้องกันอุปกรณ์คอมพิวเตอร์จากความเสียหาย การกำหนดสิทธิในการใช้ข้อมูล การรักษาความปลอดภัยของระบบเครือข่าย เป็นต้น เพื่อให้พนักงานมีความรู้และความเข้าใจซึ่งนำไปสู่พฤติกรรมการใช้งานที่ปลอดภัยกับระบบคอมพิวเตอร์มากขึ้น

ส่วนที่ 3 การวิเคราะห์ข้อมูลพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม

ผลการศึกษาพบว่า พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) ในเรื่องของการรักษาความลับของ Username และ Password มีความสำคัญอยู่ในระดับที่มากที่สุด หมายความว่าพนักงานมีพฤติกรรมที่จะเก็บรักษาความลับของ Username และ Password และพนักงานมีพฤติกรรมที่ไม่ให้ผู้อื่นมาใช้งาน Username และ Password ของตนเอง แต่จะเห็นได้ว่า พฤติกรรมการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอมีค่าเฉลี่ยที่น้อยที่สุด หมายความว่าพนักงานไม่ได้ทำการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ ในส่วนของพฤติกรรมการ Logoff ออกจากระบบทุกครั้งเมื่อไม่ได้อยู่ที่เครื่องคอมพิวเตอร์ รวมถึงเรื่องของการนำเข้าข้อมูลจากเว็บไซต์ที่ไม่มั่นใจในความปลอดภัย เพราะฉะนั้นจึงควรให้ความรู้ความเข้าใจกับพนักงานในเรื่องของการปลี่ยนเปลี่ยนรหัสอย่างสม่ำเสมอและให้ความรู้ความเข้าใจในเรื่องของการออกจากระบบทุกครั้งที่ไม่ใช้งานแล้วหรือเมื่อไม่อยู่กับเครื่องคอมพิวเตอร์เพื่อความปลอดภัยของข้อมูล และให้ความรู้กับพนักงานเกี่ยวกับการไม่นำเข้าข้อมูลจากเว็บไซต์ที่ไม่ปลอดภัย เพื่อเป็นการป้องกันไม่ให้เกิดความเสี่ยงที่จะเกิดขึ้นกับข้อมูลได้

ผลการศึกษาพบว่า พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) จะพบว่าพนักงานปฏิบัติตามนโยบายด้านสิทธิ์การใช้ข้อมูล มีความสำคัญอยู่ในระดับที่มากกว่าอันดับอื่น ๆ หมายความว่าพนักงานมีความรู้ที่ส่งผลต่อพฤติกรรมในการปฏิบัติตามนโยบายด้านสิทธิ์ในการใช้ข้อมูล ซึ่งเกิดจากบริษัทได้มีการอบรมพนักงาน ในวันแรกของการทำงานส่งผลให้พนักงานส่วนใหญ่จะมีความรู้ในเรื่องของนโยบายด้านสิทธิ์การใช้ข้อมูล แต่จะเห็นได้ว่าพนักงานยังขาดในเรื่องของพฤติกรรมการอบรมเรื่องความปลอดภัย ดังนั้นทางบริษัท จึงควรที่จะมีการจัดอบรมและให้ความรู้กับพนักงาน เพื่อให้เกิดความรู้ความเข้าใจ และการปฏิบัติที่ถูกต้องในเรื่องความปลอดภัยระบบคอมพิวเตอร์ และควรมีการให้ความสำคัญกับในเรื่องอื่น ๆ ด้วย เช่น การสร้างความเข้าใจพนักงานในการปฏิบัติงานด้วยความเข้าใจระบบ และการปรับปรุงข้อมูลที่ทันสมัย เพื่อให้สามารถนำข้อมูลมาใช้งานได้ถูกต้องและเป็นปัจจุบัน เป็นต้น

ผลการศึกษาพบว่า พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) จะเห็นได้ว่าอุปกรณ์ โปรแกรมและอุปกรณ์เครือข่ายมีความพร้อมในการใช้งาน เนื่องจากทางบริษัท มีการดูแลอุปกรณ์และโปรแกรม เพื่อให้เพียงพอต่อการใช้งานของพนักงานในบริษัทและเพื่อให้การทำงานของพนักงานสามารถดำเนินการต่อ แต่จะเห็นได้ว่าพฤติกรรมของพนักงานในเรื่องของการทำสำรองข้อมูล ยังอยู่ในระดับที่น้อย หมายความว่าพนักงานยังขาดความรู้ที่จะทำการสำรองข้อมูล จึงควรที่จะมีการอบรมเพื่อให้ความรู้ความเข้าใจกับพนักงานเพื่อบอกถึงความสำคัญของการทำสำรองข้อมูล เพื่อให้เกิดการปฏิบัติของพนักงานในเรื่องของการทำสำรองข้อมูล รวมถึงในเรื่องของการให้ความสำคัญกับเรื่องของการใช้งานโปรแกรมตรวจสอบไวรัสทางแผนกที่เกี่ยวข้องกับระบบคอมพิวเตอร์ควรให้ความสำคัญในการตรวจสอบไวรัส และให้ความรู้กับพนักงานเพื่อไม่ให้เกิดผลเสียกับทั้งฮาร์ดแวร์และซอฟต์แวร์ของบริษัท

ส่วนที่ 4 การวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐาน

สมมติฐานที่ 1 ปัจจัยส่วนบุคคลที่แตกต่างกัน ส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน จะเห็นได้ว่าเพศที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์แตกต่างกัน ในส่วนของอายุแตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน ส่วนของระดับการศึกษาที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน ส่วนของแผนกงานที่เกี่ยวข้องที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน และอายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน

สมมติฐานที่ 2 ระดับความรู้เรื่องความปลอดภัยมีความสัมพันธ์กับพฤติกรรมการใช้งานระบบรักษาความปลอดภัย จะเห็นได้ว่าความรู้ของพนักงานมีความสัมพันธ์กับพฤติกรรมการใช้งานระบบรักษาความปลอดภัย อย่างมีนัยสำคัญทางสถิติ หมายความว่าพนักงานมีความรู้ในเรื่องของการใช้งานที่เข้าถึงข้อมูลต่าง ๆ ได้ตามต้องการมากที่สุด แต่ความรู้ในเรื่องการใช้งานสิทธิ์ในการเข้าถึงข้อมูล และการใช้งานเกี่ยวกับคงามถูกต้องสมบูรณ์ของข้อมูลยังอยู่ในรระดับที่น้อยกว่า ดังนั้นบริษัทจึงควรมีการอบรมเพื่อให้ความรู้ ความเข้าใจกับพนักงานในบริษัท เพื่อให้เกิดเป็นพฤติกรรมที่ถูกต้องและสามารถสร้างความปลอดภัยให้กับระบบคอมพิวเตอร์ได้

5.2 การอภิปรายผลการวิจัย

จากการศึกษาเรื่อง ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษา บริษัท ไทยรัฐ กรุ๊ป สามารถนำผลการวิจัยมาอภิปรายผลได้ ดังนี้

ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม พบว่า อายุการทำงานที่แตกต่างกันส่งผลต่อพฤติกรรมการใช้งานระบบความปลอดภัยทางคอมพิวเตอร์ที่แตกต่างกัน หมายความว่า พนักงานที่มีอายุการทำงานมากกว่า 10 ปี ส่งผลต่อการส่งผลส่งผลต่อพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ เนื่องจากมีความรู้มีความสามารถและมีตำแหน่งงานที่มากกว่ากลุ่มพนักงานที่มีอายุการทำงานน้อยกว่า 1 ปี พนักงานที่มีอายุการทำงานน้อยกว่า 1 ปี อาจเป็นพนักงานที่อยู่ในช่วงทดลองงานหรือมีประสบการณ์การทำงานน้อย สอดคล้องกับงานวิจัยของ อัครา วัฒนโยธิน (2553) ได้ทำการศึกษาเรื่อง ความตระหนักของพนักงานต่อการป้องกันรักษาทรัพย์สินทางด้านสารสนเทศ กรณีศึกษา: การไฟฟ้าส่วนภูมิภาค สำนักงานกลางผลการศึกษาพบว่ากลุ่มของพนักงานที่มีระดับความตระหนักและพฤติกรรมในการป้องกันรักษาทรัพย์สินสารสนเทศคือพนักงานที่มีอายุการทำงานมาก่อนมีการศึกษาระดับปริญญาตรี มีระดับตำแหน่ง 4 - 5 และมีระยะเวลาในการทำงาน 3 - 4 ปี ซึ่งเป็นกลุ่มของพนักงานที่เข้ามาทำงานได้ระยะหนึ่งแล้วที่จะมีความตระหนักรู้ในการป้องกันรักษาทรัพย์สินทางด้านสารสนเทศได้

ผลการวิเคราะห์ในเรื่องของความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ พนักงานมีความรู้เกี่ยวกับการรักษความปลอดภัยของข้อมูลองค์กร ที่จะต้องใช้ในการทำงาน และจะพบว่าความรู้ในเรื่องของความหมายของโปรแกรมประสงค์ร้ายมีค่าเฉลี่ยน้อยที่สุด หมายความว่าพนักงานยังขาดความรู้ในเรื่องของโปรแกรมประสงค์ร้ายที่อาจส่งผลต่อระบบคอมพิวเตอร์ และจะเห็นว่าพนักงานยังขาดความรู้ในเรื่องของการรักษาความปลอดภัยของระบบเครือข่าย ดังนั้นจึงควรมีการอบรมเพื่อให้ความรู้ในเรื่องของความปลอดภัยระบบคอมพิวเตอร์ และมีการจัดทำนโยบายในการรักษาความปลอดภัยระบบคอมพิวเตอร์ สอดคล้องกับงานวิจัยของ วิภาวรรณ คุ้มศิริ (2552) ได้ทำการการศึกษาเรื่อง การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : กรณีศึกษาองค์การกระจายเสียง และแพร่ภาพสาธารณะแห่งประเทศไทย ผลการศึกษาพบว่าบริษัทพบความเสี่ยงที่จะเกิดขึ้น จึงได้ทำการสร้างมาตรการและนโยบายในการป้องกันความเสี่ยงที่อาจจะเกิดขึ้นโดยแบ่งตามประเภทของ CIA

คือสิทธิในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) ความถูกต้องสมบูรณ์ของข้อมูล (Integrity) ความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)

5.3 ข้อเสนอแนะที่ได้จากการวิจัย

จากการศึกษาเรื่อง ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษาบริษัท ไทยรัฐ กรุ๊ป

5.3.1 จากจุดประสงค์ของงานวิจัยเพื่อศึกษาปัจจัยที่มีผลต่อการรับรู้และการใช้งานระบบรักษาความปลอดภัยทางคอมพิวเตอร์ของพนักงานในองค์กร วัดระดับความรู้ด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ของพนักงานบริษัท ไทยรัฐ กรุ๊ป และนำผลการค้นคว้าวิจัยที่ได้ไปเป็นข้อมูลในการให้ความรู้กับพนักงาน ในการใช้งานระบบคอมพิวเตอร์ที่ปลอดภัยและกำหนดมาตรการในการป้องกันภัยคุกคาม ซึ่งจากผลการศึกษาพบว่าพนักงานมีความรู้ในเรื่องของนโยบายการทำงานในบริษัท แต่ยังขาดความรู้ในเรื่องความปลอดภัย เช่น ความรู้เรื่องของประแกรมประสงค์ร้าย การตั้งรหัสผ่านที่ปลอดภัย การทำสำรองข้อมูล การอบรมเรื่องของความปลอดภัยของระบบคอมพิวเตอร์ เป็นต้น ดังนั้นทางบริษัทควรมีการจัดอบรมเพื่อสร้างความรู้ให้กับพนักงานในเรื่องของวิธีการปฏิบัติการใช้งานที่ปลอดภัยให้กับพนักงานในบริษัท เพื่อให้เกิดเป็นพฤติกรรมที่ถูกต้องและเหมาะสม และที่สำคัญบริษัทควรให้ความสำคัญในเรื่องของความปลอดภัยระบบคอมพิวเตอร์โดยให้แผนกงานที่เกี่ยวข้องกับระบบคอมพิวเตอร์มีการตรวจสอบดูแลและป้องกันความเสี่ยงที่อาจเกิดกับระบบความปลอดภัยคอมพิวเตอร์ได้

5.3.2 จากการศึกษาจะพบว่าประโยชน์ของการศึกษานี้ทำให้ทราบถึงพฤติกรรมการใช้งานรักษาความปลอดภัยของผู้ใช้งานเครื่องคอมพิวเตอร์ ที่ส่งผลต่อความปลอดภัยระบบคอมพิวเตอร์ในองค์กร เพื่อให้ทราบถึงความรู้และความเข้าใจของพนักงานที่มีต่อการป้องกันภัยคุกคาม และความปลอดภัยของระบบคอมพิวเตอร์ และสามารถนำผลการศึกษาไปใช้เป็นแนวทางให้ผู้ที่มีความสนใจในเรื่องของความปลอดภัยของระบบคอมพิวเตอร์ในองค์กรต่อไป ดังนั้นบริษัทควรมีการจัดทำนโยบายการรักษาความปลอดภัยในบริษัท และมีการจัดอบรมเพื่อเป็นการสร้างความรู้ให้กับพนักงานในบริษัท เพื่อให้มีพฤติกรรมการใช้งานที่ปลอดภัยต่อระบบคอมพิวเตอร์ และบริษัทควรมีการประยุกต์นำความรู้ในเรื่องของการรักษาความปลอดภัย เพื่อให้เกิดประสิทธิภาพมากยิ่งขึ้น

5.3.3 จากผลการศึกษานั้นจะพบว่าความรู้มีความสัมพันธ์กันกับพฤติกรรมการใช้งานระบบรักษาความปลอดภัย ประกอบด้วยพฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)

และพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) ซึ่งจะเห็นได้ว่าพนักงานจะมีความรู้เรื่องของพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบ ต่าง ๆ ได้เมื่อต้องการ (Availability) หมายความว่าพนักงานสามารถเข้าใช้งานข้อมูลในการทำงานได้อย่างดี ทั้งนี้บริษัทควรให้ความสำคัญกับความรู้ในด้านอื่น ๆ ด้วยเช่นกัน เพราะจะทำให้พนักงานเกิดความเข้าใจและมีพฤติกรรมการทำงานที่เหมาะสม เช่น ความรู้ด้านพฤติกรรมการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล และการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล เป็นต้น

5.4 ข้อเสนอแนะสำหรับองค์กร

5.4.1 บริษัทควรที่จะมีมาตรการรักษาความปลอดภัยภายในที่เกี่ยวของกับ 3 มาตรการความปลอดภัยระบบ คือ พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ (Confidentiality) พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และพฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability) ประกาศเป็นนโยบายทางด้านความมั่นคงทางสารสนเทศ และเมื่อได้นำมาใช้แล้วสามารถลดความเสี่ยงให้ได้ผลดียิ่งขึ้นจึงจำเป็นอย่างมากที่ควรได้รับการผลักดันและการสนับสนุนจากทุกส่วนงานที่เกี่ยวข้อง

5.4.2 บริษัทควรให้ความสำคัญกับเรื่องของความปลอดภัยของระบบคอมพิวเตอร์ภายในบริษัท ดังนั้นจึงควรที่จะมีการจัดอบรมพนักงานและให้ความรู้กับพนักงานในเรื่องของความปลอดภัยระบบคอมพิวเตอร์ เป็นผลให้พนักงานมีความรู้และความเข้าใจที่จะปฏิบัติอย่างเหมาะสมและถูกวิธีเพื่อให้เกิดการประยุกต์ใช้อย่างมีประสิทธิภาพมากยิ่งขึ้น รวมถึงหน่วยงานที่เกี่ยวข้องควรให้ความสำคัญในการการป้องกันและรับมือที่จะเกิดความเสี่ยงกับระบบคอมพิวเตอร์ในอนาคตได้

5.4.3 มีการสร้างนโยบายความมั่นคงของระบบคอมพิวเตอร์และนำไปใช้ ซึ่งบริษัทควรมีการทบทวนและการประเมินความเสี่ยง และตรวจสอบนโยบายอยู่อย่างสม่ำเสมอ เพราะในอนาคตเทคโนโลยีมีการเปลี่ยนแปลงอยู่เสมอ

5.5 งานวิจัยที่เกี่ยวเนื่องในอนาคต

ควรทำงานวิจัยด้านปัญหาภัยคุกคามทางระบบคอมพิวเตอร์ที่เกิดขึ้นในการปฏิบัติงาน เนื่องจากธุรกิจของบริษัท ไทยรัฐ กรุ๊ป เป็นธุรกิจเฉพาะทางด้านงานสื่อสารมวลชน อาจมีภัยคุกตามเฉพาะที่ต้องเฝ้าระวัง จึงควรที่จะมีการศึกษาและทำการดูแลระบบคอมพิวเตอร์ หากสามารถทราบถึงภัยคุกคามได้จะทำให้มีการเตรียมรับมือ และแก้ไขได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

บรรณานุกรม

กัลยา วานิชย์บัญชา. (2545). **การใช้ SPSS for Windows ในการวิเคราะห์ข้อมูล** (พิมพ์ครั้งที่ 6). ภาควิชาสถิติ คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย.

กรกช วิไลลักษณ์. (2012). **ความมั่นคงปลอดภัยระบบคอมพิวเตอร์**. นนทบุรี : มหาวิทยาลัยสุโขทัยธรรมาธิราช

ชัยญามล เลิศสงคราม. (2552). **การศึกษาและจัดทำแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร ด้วยมาตรการ มาตรฐาน ISO/IEC 27001 การณีศึกษามหาวิทยาลัยราชภัฏสวนดุสิต**. (การค้นคว้าอิสระปริญญามหาบัณฑิต, มหวิทยาลัยธรรมศาสตร์).

ภูมินทร์ ภูดวงสี. (2550). **การศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยของสารสนเทศภายในองค์กร กรณีศึกษา บริษัท NEC Corporation (Thailand) Ltd**. (การค้นคว้าอิสระปริญญามหาบัณฑิต, มหวิทยาลัยธรรมศาสตร์).

วราภรณ์ ธวิทย์ชัยพร. (2549). **แนวทางการนำ Information Security Management มาใช้ในการจัดระเบียบการบริหารจัดการด้านความปลอดภัยสารสนเทศ กรณีศึกษา: บริษัทให้คำปรึกษาด้านสารสนเทศแห่งหนึ่ง**. (การค้นคว้าอิสระปริญญามหาบัณฑิต, มหวิทยาลัย ธรรมศาสตร์)

วศิน รำพึงกิจ. (2552). **การสำรวจภัยคุกคามทางคอมพิวเตอร์และการรักษาความปลอดภัยข้อมูลสารสนเทศ ของธนาคารพาณิชย์ในประเทศไทย**. (การค้นคว้าอิสระปริญญามหาบัณฑิต, มหวิทยาลัยธรรมศาสตร์)

วิภาวรรณ คุ้มศิริ. (2552). **การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษาองค์การกระจายเสียง และแพร่ภาพสาธารณะแห่งประเทศไทย**. (การค้นคว้าอิสระปริญญามหาบัณฑิต, มหวิทยาลัยธรรมศาสตร์).

บรรณานุกรม (ต่อ)

สามารถ เจตนเสน. (2553). **แนวทางการสร้างนโยบายการรักษาความปลอดภัยของข้อมูลสารสนเทศสำหรับองค์กร กรณีศึกษา บริษัท ไทยออโต้เซลส์ จำกัด**. (การค้นคว้าอิสระปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์).

สิริยากร กิติศรีวรพันธุ์. (ม.ป.ป.). **ระบบความปลอดภัยของระบบสารสนเทศ แนวคิดการรักษาความปลอดภัย**. สืบค้นจาก http://naowarat57.blogspot.com/2013/08/computer-security.html.

ใจชนก ภาคอัต. (2557). **การจัดการความรู้ด้านการประกันคุณภาพการศึกษาของสถาบันบัณฑิตพัฒนบริหารศาสตร์**. (การค้นคว้าอิสระปริญญามหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์).

บุญธรรม กิจปรีดาบริสุทธิ์. (2549). **เทคนิคการสร้างเครื่องมือรวมรวบข้อมูลสำหรับการวิจัย**. (พิมพ์ครั้งที่ 6). กรุงเทพฯ: จามจุรี.

พรสุดา อสิพงษ์. (ม.ป.ป.). **ประวัติความเป็นมายุค 1-6.** สืบค้นจาก https://www.thairath.co.th/corporate/generation1.

ประภา เพ็ญสุวรรณ. (2526). **ทัศนะคติการวัดการเปรียบเทียบพฤติกรรมอนามัย**. กรุงเทพฯ : โอเดียนสโตร์.

ประเวศ วะสี. (2539). **ปฏิรูปการศึกษาไทยการยกเครื่องทางปัญญา**. กรุงเทพมหานคร : บริษัทสร้างสื่อจำกัด.

พรทิพย์ กาญจนนิยต และคณะ. (2546). **การจัดการความรู้ : สู่วงจรคุณภาพที่เพิ่มพูน**. กรุงเทพมหานคร : สำนักมาตรฐานอุดมศึกษา สำนักงานปลัดทบวงมหาวิทยาลัย.

ชุมพล ศฤงคารศิริ. (2537). **ระบบสารสนเทศเพื่อการจัดการ. เรื่องที่ 2 มาตราฐานการความปลอดภัย**. สืบค้นจาก http://pop-mis.blogspot.com/2016/01/12-2.html.

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย. (2558). **พื้นฐานของความปลอดภัยระบบคอมพิวเตอร์ที่ผู้ดูและระบบควรทราบ**. สืบค้นจาก http://thaicert.nectec.or.th/paper/basic.php.

บรรณานุกรม (ต่อ)

เสรี พงศ์พิศ. (2549).**แผนชีวิตเศรษฐกิจชุมชน**.กรุงเทพฯ: โรงพิมพ์เจริญวิทย์การพิมพ์.

เศรษฐพงศ์ มะลิสุวรรณ. (2552). **มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 และ ISO/IEC 17799 ฉบับประเทศไทย**. ปทุมธานี : มหาวิทยาลัยรังสิต

ThaiCERT. (2550). **มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5)**. สืบค้นจาก http://oknation.nationtv.tv/blog/weblog/2009/02/27/entry-4.

Whitman, Michae. (2008). **Principles of Information Security Third** (3rd ed). Boston, MA : Information Security and Assurance.

Oranuch Kongsri (2558). **ความมั่นคงปลอดภัยของสารสนเทศ.** สืบค้นจาก http://jjsao.blogspot.com/2015/05/blog-post.html.

ภาคผนวก

ภาคผนวก ก
แบบสอบถาม

แบบสอบถามเพื่อการวิจัย

เรื่อง “ความสัมพันธ์ระหว่างการรับรู้และการใช้งานระบบการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ กรณีศึกษา บริษัท ไทยรัฐ กรุ๊ป”

คำชี้แจง

แบบสอบถามเพื่อการวิจัยฉบับนี้ มีวัตถุประสงค์เพื่อการศึกษาระดับความรู้ ทัศนคติ การใช้งานระบบคอมพิวเตอร์ในองค์กรและศึกษาแนวทางในการป้องกันภัยคุกคามต่อระบบคอมพิวเตอร์ในองค์กร เพื่อเป็นข้อมูลในการให้ความรู้กับพนักงาน ในการใช้งานระบบคอมพิวเตอร์ที่มั่นคงปลอดภัยในองค์กร

กรุณาตอบแบบสอบถามตามความเป็นจริง หรือตามความคิดเห็นของท่านมากที่สุด ข้อมูลที่ได้รับ จะแปลผลการวิจัยในภาพรวม เพื่อใช้ประกอบการศึกษาของปริญญาธุรกิจมหาบัณฑิต คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ผู้วิจัยจะเก็บข้อมูลของท่านไว้เป็นความลับ และใช้ประโยชน์เฉพาะงานวิจัยนี้เท่านั้น ไม่มีผลกระทบต่อท่านและหน่วยงานของท่านแต่อย่างใด

แบบสอบถามบ่งออกเป็น 3 ตอน ได้แก่

ตอนที่ 1 ข้อมูลเกี่ยวกับข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 ข้อมูลเกี่ยวกับความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กร

ตอนที่ 3 ข้อมูลเกี่ยวกับพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร

ขอบพระคุณทุกท่านที่ได้สละเวลาอันมีค่าของท่านตอบแบบสอบถามนี้

นายปริญทรรศน์ นิลมณี
นิสิตปริญญาโท คณะบริหารธุรกิจ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ตอนที่ 1 ข้อมูลเกี่ยวกับข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

คำชี้แจง : กรุณาใส่เครื่องหมาย ✓ ลงใน ☐ หน้าตำตอบที่ตรงกับข้อมูลทั่วไปของท่านมากที่สุดเพียงช่องเดียวเท่านั้น

1. เพศ

☐ 1. ชาย ☐ 2. หญิง

2. อายุ

☐ 1. 21 - 25 ปี ☐ 2. 26 - 30 ปี

☐ 3. 31 - 35 ปี ☐ 4. 36 - 40 ปี

☐ 5. 41 - 45 ปี ☐ 5. 46 ปีขึ้นไป

3. ระดับการศึกษา

☐ 1. ปริญญาตรี ☐ 2. สูงกว่าปริญญาตรี

4. แผนกงานที่เกี่ยวข้อง

☐ 1. บรรณาธิการข่าว ☐ 2. การขาย / การตลาด

☐ 3. เลขานุการ / แอดมินฝ่าย ☐ 4. เทคโนโลยีสารสนเทศ

☐ 5. กฎหมาย ☐ 6. โปรแกรมเมอร์

☐ 7. ทรัพยากรมนุษย์ ☐ 8. กราฟฟิก / ตัดต่อ

☐ 9. พัสดุ / กองซ่อมบำรุง

5. อายุการทำงาน

☐ 1. น้อยกว่า 1 ปี ☐ 2. 1 - 2 ปี

☐ 3. 3 - 4 ปี ☐ 4. 5 - 10 ปี

☐ 5. มากกว่า 10 ปี

ส่วนที่ 2 ข้อมูลเกี่ยวกับความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กร

คำชี้แจง:กรุณาตอบคำถามและใส่เครื่องหมาย □ ลงใน □ ในช่องที่ตรงกับความคิดเห็นของท่านมากที่สุด

ความรู้ในความปลอดภัยของการใช้งานระบบคอมพิวเตอร์ในองค์กร	ระดับความรู้				
	5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
1. กฎการรักษาความปลอดภัยข้อมูลองค์กร					
2. การใช้งานของโปรแกรมต้านไวรัส					
3. การจัดการรหัสผ่านที่เหมาะสม					
4. ความหมายของโปรแกรมประสงค์ร้ายต่อระบบ (Virus , Trojan , Worm)					
5. การป้องกันอุปกรณ์คอมพิวเตอร์จากความเสียหาย เช่น - การดึงปลั๊กโดยไม่ได้ shut down เครื่อง - การไม่รับประทานอาหารและน้ำ บริเวณเครื่องคอมพิวเตอร์ - การติดตั้งเครื่อง UPS					
6. การกำหนดสิทธิในการใช้ข้อมูล (การ login เข้าใช้งาน ไฟล์แชร์ และขอบเขตการใช้งานข้อมูล)					
7. การรักษาความปลอดภัยของระบบเครือข่าย					

ส่วนที่ 3 ข้อมูลเกี่ยวกับพฤติกรรมในการใช้งานที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กร เช่น สิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ ความถูกต้องสมบูรณ์ของข้อมูล และการเข้าถึงข้อมูลต่างๆ ได้เมื่อต้องการ เป็นต้น

คำชี้แจง : กรุณาตอบคำถามและใส่เครื่องหมาย □ ลงใน □ ในช่องที่ตรงกับความคิดเห็นของท่านมากที่สุด

พฤติกรรมในการใช้งานที่เกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลต่างๆ (Confidentiality)	**ระดับการปฏิบัติ**				
	5 ปฏิบัติเป็นประจำ	**4 ปฏิบัติบ่อยครั้ง**	**3 ปฏิบัติปานกลาง**	**2 ปฏิบัติน้อยครั้ง**	**1 ปฏิบัติน้อยที่สุด**
1. การรักษาความลับของ Username และ Password					
2. การไม่อนุญาตให้ผู้อื่นใช้ข้อมูลที่ตนเองรับผิดชอบ					
3. การนำเข้าข้อมูลจากเว็บไซต์ที่ไม่มั่นใจในความปลอดภัย					
4. หากท่านไม่อยู่ที่เครื่องคอมพิวเตอร์ของท่าน ท่านทำการ logoff ออกจากระบบทุกครั้ง					
5. การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ					

พฤติกรรมในการใช้งานที่เกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูล (Integrity)	ระดับการปฏิบัติ				
	5 ปฏิบัติเป็นประจำ	4 ปฏิบัติบ่อยครั้ง	3 ปฏิบัติปานกลาง	2 ปฏิบัติน้อยครั้ง	1 ปฏิบัติน้อยที่สุด
1. การปรับปรุงข้อมูลที่ทันสมัย					
2. ปฏิบัติตามนโยบายด้านสิทธิ์การใช้ข้อมูล					
3. ปฏิบัติตามนโยบายด้านความปลอดภัย					
4. การอบรมเรื่องความปลอดภัย					
5. ปฏิบัติงานด้วยความเข้าใจระบบ					
พฤติกรรมในการใช้งานที่เกี่ยวกับความพร้อมใช้งานระบบต่าง ๆ ได้เมื่อต้องการ (Availability)	ระดับการปฏิบัติ				
	5 ปฏิบัติเป็นประจำ	4 ปฏิบัติบ่อยครั้ง	3 ปฏิบัติปานกลาง	2 ปฏิบัติน้อยครั้ง	1 ปฏิบัติน้อยที่สุด
1. การใช้งานโปรแกรมตรวจสอบไวรัส					
2. ระบบสามารถใช้งานได้ตลอดเวลา					
3. อุปกรณ์และโปรแกรมมีความพร้อมในการใช้งาน					
4. อุปกรณ์เครือข่ายมีความพร้อมในการใช้งาน					
5. มีการทำสำรองข้อมูล					

ขอขอบพระคุณผู้ตอบแบบสอบถามทุกท่านที่สละเวลาอันมีค่าของท่านมาร่วมตอบแบบสอบถามในครั้งนี้

ประวัติผู้เขียน

ชื่อ - สกุล	นายปริญทรรศน์ นิลมณี
วัน เดือน ปีเกิด	20 กันยายน 2537
ที่อยู่	บ้านเลขที่ 200/377 หมู่ที่ 1 ซอยเปรมประชา ตำบลหลักหก อำเภอเมือง จังหวัดปทุมธานี 12000
การศึกษา	ปริญญาตรี คณะบริหารธุรกิจและเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคล ตะวันออก วิทยาเขตจักรพงษภูวนารถ
เบอร์โทรศัพท์	087-517-7216
อีเมล์	parintas_n@rmutt.ac.th