วารสาร Mahidol R2R e-Journal ปีที่ 11 ฉบับที่ 2 ประจำเดือนพฤษภาคม-สิงหาคม 2567
Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

การศึกษาเปรียบเทียบวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ ระหว่างบุคลากรในขอบเขตและบุคลากรที่อยู่นอกขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก คณะแพทยศาสตร์ศิริราชพยาบาล

A Comparison Study of Organizational Information Security Culture between Personnel within and outside the Scope of Information Security Management System, Golden Jubilee Medical Center, Faculty of Medicine Siriraj Hospital

อนุกูล คำโมนะ[1*] และ ทศพล ปึงธนานุกิจ[2]
Anukool Khammona[1*] and Tossapon Puengtananukij[2]

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) เพื่อศึกษาการรับรู้วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรศูนย์การแพทย์กาญจนาภิเษก 2) เพื่อศึกษาเปรียบเทียบวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศจำแนกตามปัจจัยส่วนบุคคล และตามหน่วยงานที่อยู่ในขอบเขตและที่อยู่นอกขอบเขต การบริหารความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก กลุ่มตัวอย่างเป็นบุคลากรที่ทำงานในศูนย์การแพทย์กาญจนาภิเษก คณะแพทยศาสตร์ศิริราชพยาบาล จำนวน 308 คน ใช้การสุ่มตัวอย่างแบบชั้นภูมิ และจัดกลุ่มบุคลากรโดยใช้เกณฑ์กลุ่มบุคลากรหน่วยงานในขอบเขตและบุคลากรที่อยู่นอกขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูล วิเคราะห์ข้อมูลด้วยสถิติร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และวิเคราะห์เปรียบเทียบโดยใช้โปรแกรม spss

ผลการวิจัยพบว่าภาพรวมบุคลากรศูนย์การแพทย์กาญจนาภิเษกมีวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศอยู่ในระดับที่ผ่านเกณฑ์ ทั้งนี้เมื่อพิจารณาเปรียบเทียบระหว่างบุคลากรในขอบเขตและบุคลากรที่อยู่นอกขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ พบว่าไม่มีความแตกต่างกันอย่างมีนัยสำคัญที่ระดับ .05

คำสำคัญ วัฒนธรรมองค์กร; ความมั่นคงปลอดภัยสารสนเทศ

---

[1] กลุ่มงานพัฒนาคุณภาพ ศูนย์การแพทย์กาญจนาภิเษก คณะแพทยศาสตร์ศิริราชพยาบาล

[2] งานเวชสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก คณะแพทยศาสตร์ศิริราชพยาบาล

[1] Quality Improvement Division, Golden Jubilee Medical Center, Faculty of Medicine Siriraj Hospital

[2] Information Technology Division, Golden Jubilee Medical Center, Faculty of Medicine Siriraj Hospital

* Corresponding author: e-mail: anukool.kh@gmail.com

วารสาร Mahidol R2R e-Journal ปีที่ 11 ฉบับที่ 2 ประจำเดือนพฤษภาคม-สิงหาคม 2567
Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

Abstract

The objectives of this research were: 1) to study the information security culture of Golden Jubilee Medical Center, 2) to examine the information security culture as it relates to personal factors and departments within and outside the scope of the information security management system at Golden Jubilee Medical Center. The sample was randomly selected using stratified random sampling, and it was grouped by departments within and outside the scope of the information security management system. The study instrument used was a questionnaire. Data were collected and analyzed using percentages, means, standard deviations, and statistical tests performed using SPSS.

The results showed that the personnel of Golden Jubilee Medical Center have an information security culture that meets the criteria. However, when comparing personnel within the scope of the information security management system with those outside the scope, the statistics showed no significant difference ($p > .05$)

Keywords: Organizational culture; Information Security

บทนำ

ข้อมูลเป็นหนึ่งในทรัพย์สินที่มีค่าที่สุดในองค์กร ความมั่นคงปลอดภัยสารสนเทศ คือ การปกป้องข้อมูลที่มีความสำคัญ เพื่อการรักษาความลับ (confidentiality), ความถูกต้อง ครบถ้วน สมบูรณ์ (integrity), และความพร้อมใช้ของข้อมูล (availability), (AlHogail & Mirza, 2014) ตามรูปที่ 1

รูปที่ 1 สามเหลี่ยมความมั่นคงปลอดภัยสารสนเทศ

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

กลยุทธ์ ข้อควรระวัง และมาตรการรับมือหลายอย่างได้รับการพัฒนา ฝึกฝน และเรียนรู้ ตลอดช่วงครึ่งศตวรรษที่ผ่านมา ทั้งทางด้านเทคนิคในการรักษาความมั่นคงปลอดภัยที่มักจะเน้นที่ความปลอดภัยของระบบคอมพิวเตอร์ และการมีส่วนร่วมของฝ่ายบริหาร เช่น การกำกับดูแลและสนับสนุนกิจกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการใช้มาตรฐานการตรวจสอบการปฏิบัติตามข้อกำหนด การขอรับการรับรอง และการวัดผล นอกจากนี้ยังมีความพยายามในการบริหารจัดการทรัพยากรมนุษย์เพื่อปกป้องและรักษาความปลอดภัยของข้อมูล อย่างไรก็ตามปัจจุบันจุดสนใจอยู่ที่การพัฒนาวัฒนธรรมการรักษาความมั่นคงปลอดภัยของข้อมูล (Ngo, et al. 2005) เพื่อเพิ่มประสิทธิภาพของในการรักษาความมั่นคงปลอดภัยสารสนเทศ และลดอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่มีสาเหตุจากบุคคล

สมมติฐานที่หลากหลายได้ถูกนำเสนอขึ้นมาเพื่ออธิบายเกี่ยวกับวัฒนธรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ทั้งความรู้ ความเชื่อ การรับรู้ ทัศนคติ ระเบียบแบบแผน และค่านิยมของบุคคลที่เกี่ยวข้องกับความปลอดภัยของข้อมูลต่างถูกเรียกโดยรวมว่า "วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ"

วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Culture: ISC) เป็นวัฒนธรรมย่อยภายในองค์กรที่สนับสนุนการดำเนินงานเกี่ยวกับข้อมูลภายในองค์กรให้เกิดความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยสารสนเทศเป็นส่วนสำคัญในการทำงานของบุคลากรทุกคนอย่างแยกไม่ออก (Schlienger & Teufel, 2003). องค์กรต้องมั่นใจว่าวัฒนธรรมของตนเอื้ออำนวยต่อการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อที่จะดำเนินการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม วัฒนธรรมการรักษาความมั่นคงปลอดภัยสารสนเทศที่ดีจะส่งเสริมให้พนักงานปฏิบัติงานในลักษณะที่ปลอดภัยยิ่งขึ้น โดยลดจำนวนอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศลง (Da Veiga & Martins, 2015)

ศูนย์การแพทย์กาญจนาภิเษกได้นำระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC27001 มาใช้ตั้งแต่ปี 2555 โดยเริ่มจาก 3 หน่วยงาน ได้แก่ งานเวชสารสนเทศ งานเวชระเบียน และศูนย์เทคนิคการแพทย์และรังสีเทคนิคนานาชาติ ต่อมามีการขยายขอบเขตการดำเนินการให้ครอบคลุมงานทรัพยากรบุคคล งานการคลัง งานเภสัชกรรม งานพัฒนาคุณภาพ ศูนย์ตรวจสุขภาพ งานวิศวกรรมบริการ และงานอาคารสถานที่และยานพาหนะ รวมเป็น 10 หน่วยงาน ในปี 2563 เมื่อศูนย์การแพทย์กาญจนาภิเษกอยู่ภายใต้นโยบายความมั่นคงปลอดภัยสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลตามโครงสร้างใหม่ จำเป็นต้องดำเนินการมาตรฐานนี้กับทุกหน่วยงาน จึงเป็นที่น่าศึกษาว่าวัฒนธรรมความมั่นคงปลอดภัยสารสนเทศของบุคลากรในหน่วยงานภายในขอบเขตกับนอกขอบเขตจะมีความแตกต่างกันอย่างไร โดยทั้งบุคลากรภายในและภายนอกขอบเขตจะได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศเหมือนกัน แต่บุคลากรภายในขอบเขตจะได้รับการอบรมเกี่ยวกับมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนนโยบาย ระเบียบปฏิบัติที่เกี่ยวข้อง นอกจากนี้หน่วยงานภายในขอบเขตจะถูกตรวจสอบโดยผู้ตรวจสอบภายใน และผู้ตรวจสอบภายนอกอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าหน่วยงานดังกล่าวมีการดำเนินการสอดคล้องกับข้อกำหนดของมาตรฐาน เป้าหมายของการศึกษานี้คือการการศึกษาวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ เปรียบเทียบระหว่างบุคลากรในขอบเขตและบุคลากรที่อยู่นอกขอบเขต การบริหารความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก คณะแพทยศาสตร์ศิริราชพยาบาล เพื่อพัฒนา

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

แนวทางส่งเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก ต่อไป

มาตรฐาน ISO/IEC 27001 ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ISO/IEC 27001 เป็นมาตรฐานสากล ด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ ขององค์กรระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization - ISO) ประกาศใช้อย่างเป็นทางการครั้งแรกเมื่อปี ค.ศ.2005 ปัจจุบันเป็นฉบับที่ 3 ปี ค.ศ.2022 มีข้อกำหนดเพื่อให้องค์กรนำไปประยุกต์ใช้ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ข้อกำหนดในมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO27001:2022 มีทั้งหมด 10 ข้อ แบ่งออกเป็น 2 ส่วน คือ 1. บทนำ (Clause 1-3) และ 2. ข้อกำหนด (Clause 4-10) นอกจากนี้ในมาตรฐาน ISO/IEC27001:2022 ยังมีการกำหนดมาตรการควบคุมไว้ใน Annex A ของมาตรฐาน จำนวนทั้งสิ้น 4 หมวด 93 ข้อ เพื่อให้องค์กรเลือกนำไปใช้ในการควบคุมความเสี่ยงที่เกี่ยวข้อง

วัตถุประสงค์ของการวิจัย (Objective)

1. เพื่อศึกษาการรับรู้วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรศูนย์การแพทย์กาญจนาภิเษก

2. เพื่อวิเคราะห์เปรียบเทียบวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศจำแนกตามปัจจัยส่วนบุคคล และบุคลากรตามหน่วยงานที่อยู่ในขอบเขตและบุคลากรที่อยู่นอกขอบเขต การบริหารความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก

วิธีการศึกษา

1. ประชากรและกลุ่มตัวอย่าง

การศึกษาวิจัยนี้เป็นการศึกษากับบุคลากรศูนย์การแพทย์กาญจนาภิเษก คณะแพทยศาสตร์ศิริราชพยาบาล ที่ปฏิบัติงานเต็มเวลาเกิน 6 เดือน จำนวนบุคลากรทั้งหมด 935 คน นำมาคำนวณกลุ่มตัวอย่างที่ระดับความเชื่อมั่นร้อยละ 95 ค่าความผิดพลาดร้อยละ 5 และค่า drop out 10% โดยวิเคราะห์ตามกลุ่มเป้าหมายที่ต้องการศึกษาโดยใช้สูตรของ ทาโร ยามาเน่ ผลการคำนวนจำนวนประชากรกลุ่มตัวอย่าง แบ่งตามกลุ่มเป้าหมาย ดังตารางที่ 1

ตารางที่ 1 ผลการคำนวนจำนวนประชากรกลุ่มตัวอย่าง แบ่งตามกลุ่มเป้าหมาย

กลุ่มบุคลากร	จำนวนบุคลากร	Calculate +10% drop out
บุคลากรในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ	133	110
บุคลากรนอกขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ	758	284
รวม	**935**	**394**

2. การสร้างเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลและตรวจสอบคุณภาพเครื่องมือ

ผู้วิจัยได้ใช้แบบสอบถามในการเก็บรวบรวมข้อมูล โดยมีขั้นตอนในการสร้าง และตรวจสอบคุณภาพ ดังนี้

1.1. สร้างเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเพื่อวิเคราะห์วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ ตามโครงสร้างของ ISCA dimensions (Da Veiga & Martins, 2015) โดยปรับปรุงจาก Information Security Culture Assessment (ISCA) questionnaire instrument ซึ่งเป็นแบบประเมินวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศของ Professor Adéle Da Veiga ที่ได้รับการยอมรับอย่างแพร่หลายในการ

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

ประเมินวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้สอดคล้องกับบริบทขององค์กร โดยผู้วิจัยได้ติดต่อเพื่อขออนุญาติใช้แบบสอบถามดังกล่าวกับผู้จัดทำและได้รับอนุญาติให้ใช้แบบสอบถามดังกล่าวแล้ว ในการแปลแบบสอบถามใช้หลักการ Forward and back translation โดยผู้แปลจำนวน 2 คน มีคุณสมบัติคือ (1) เป็นผู้ที่มีความรู้ทั้งสองภาษา (ภาษาอังกฤษและภาษาไทย) ในระดับดี และมีคะแนนภาษาอังกฤษเทียบเคียงมาตรฐานสากล (CEFR) ระดับสูง C1 ขึ้นไป และ (2) ไม่เคยเห็นต้นฉบับแบบสอบถามมาก่อน

1.2. ตรวจสอบเครื่องมือ ด้วยการส่งแบบสอบถามให้ผู้เชี่ยวชาญประเมินความเหมาะสมของตรวจสอบให้แบบสอบถามมีความถูกต้องเที่ยงตรงเชิงเนื้อหาของข้อคำถามแต่ละข้อตามวัตถุประสงค์งานวิจัย โดยผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ/ความมั่นคงปลอดภัยไซเบอร์, ด้านการประเมินวัฒนธรรมองค์กร, ด้านการพัฒนาคุณภาพ/บริหารจัดการความเสี่ยง และด้านการคุ้มครองข้อมูลส่วนบุคคล ที่มีประสบการณ์ในการทำงานในด้านดังกล่าวทั้งในระดับองค์กรหรือในระดับประเทศ หรือมีผลงานวิจัยที่เกี่ยวข้องในด้านนั้น ๆ จำนวนผู้เชี่ยวชาญจำนวน 3 ท่าน จากนั้นนำผลการประเมินจากผู้เชี่ยวชาญมาวิเคราะห์ค่า IOC (Index of item objective congruence) โดยใช้ข้อคำถามที่มีค่า IOC ตั้งแต่ 0.5 ขึ้นไป ในส่วนข้อคำถามที่ได้ค่า IOC ต่ำกว่า 0.5 พิจารณาแก้ไขหรือตัดทิ้ง

1.3. ตรวจสอบความเชื่อมั่น (reliability) ของเครื่องมือในการเก็บข้อมูล โดยนำแบบสอบถามที่ผ่านความเห็นชอบของผู้เชี่ยวชาญไปทดลองใช้กับเจ้าหน้าที่ในโรงพยาบาลที่มีคุณสมบัติคล้ายกัน และไม่ใช่กลุ่มตัวอย่างที่ใช้ในการวิเคราะห์ ด้วยการสุ่มอย่างอย่างง่ายจำนวน 30 คน และนำคำตอบที่ได้มาหาความเชื่อมั่น (reliability) ด้วยวิธีการของครอนบาค ได้ค่าเท่ากับ 0.98 โดยค่าความเชื่อมั่นของแบบสอบถามที่อยู่ในเกณฑ์ยอมรับได้คือ 0.70 ขึ้นไป

3. การเก็บรวบรวมข้อมูล

การวิจัยนี้ใช้การเก็บข้อมูลโดยใช้แบบสอบถาม โดยเก็บข้อมูลด้วยตนเอง กลุ่มอาสาสมัคร/ผู้เข้าร่วมวิจัยสามารถร่วมตอบแบบสอบถามด้วยความสมัครใจและไม่มีการบังคับ การเก็บข้อมูลจะเริ่มหลังจากได้รับการรับรอง

4. การวิเคราะห์ข้อมูล

วิเคราะห์ข้อมูลทั่วไป คำถามตรวจสอบรายการ (Check list) วัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ แบบมาตราส่วนประมาณค่า 5 ระดับ โดยใช้สถิติเชิงพรรณนาได้แก่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน วิเคราะห์เปรียบเทียบวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ โดยใช้สถิติ T-Test สำหรับเปรียบเทียบค่าเฉลี่ยของตัวแปรอิสระซึ่งจำแนกเป็น 2 กลุ่ม และการทดสอบความแปรปรวนทางเดียวใช้ One-Way ANOVA หรือ F-Test สำหรับตัวแปรที่แบ่งกลุ่มมากกว่า 2 กลุ่ม ในกลุ่มกรณีข้อมูลมีการแจกแจงปกติ กรณีข้อมูลมีการแจกแจงไม่ปกติ ใช้สถิติทดสอบเลือกใช้สถิติทดสอบตามจำนวนกลุ่มเปรียบเทียบ ได้แก่ การทดสอบเปรียบเทียบ 2 กลุ่ม ใช้สถิติ Mann-Whitney U test หรือ มากกว่า 2 กลุ่มใช้สถิติ Kruskal-Wallis one-way ANOVA ในการทดสอบการแปลผลความหมายของค่าเฉลี่ยระดับวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ คะแนนระหว่าง 1.00 – 2.99 หมายถึง ไม่ผ่าน/ควรปรับปรุงเร่งด่วน คะแนน 3.00 – 3.99 หมายถึง ไม่ผ่าน/ควรปรับปรุง คะแนน 4.00 – 5.00 หมายถึง ผ่าน

5. จริยธรรมการวิจัย

การศึกษาวิจัยครั้งนี้ได้ผ่านการพิจารณาจริยธรรมการวิจัยในคน จากคณะกรรมการจริยธรรมการวิจัยในคน คณะแพทยศาสตร์ศิริราชพยาบาล รหัสโครงการ 245/2565 (IRB3) COA NO. SI 302/2022

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

ผลการศึกษา

จากการส่งแบบสอบถามไปยังแต่ละหน่วยงาน ได้รับกลับคืนจำนวน 312 ฉบับ พบว่าไม่เข้าเกณฑ์ 4 ฉบับ แบ่งเป็นบุคลากรของหน่วยงานในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ 90 ฉบับ และเป็นหน่วยงานที่ไม่อยู่ในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ 218 ฉบับ คิดเป็นร้อยละ 81.81 และ 77.11 ของจำนวนแบบสอบถามที่ส่งออกไปในแต่ละกลุ่มตามลำดับ ซึ่งเป็นอัตราการตอบกลับที่ยอมรับได้

ข้อมูลทั่วไปของกลุ่มตัวอย่างทั้งหมด 308 เป็นบุคลากรในหน่วยงานในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ 90 คน (ร้อยละ 29.22) และเป็นหน่วยงานที่ไม่อยู่ในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ 218 คน (ร้อยละ 70.78) ข้อมูลอื่น ๆ แสดงดังตารางที่ 2

ตารางที่ 2 ข้อมูลผู้ตอบแบบสอบถามจำแนกตามปัจจัยส่วนบุคคล

ปัจจัย	จำนวน	ร้อยละ
เพศ		
- ชาย	63	20.39
- หญิง	241	77.99
- ไม่ระบุ	5	1.62
ช่วงอายุ		
- 20 - 30 ปี	87	28.16
- 31 - 40 ปี	127	41.10
- 41 - 50 ปี	79	25.57
- 51 - 60 ปี	16	5.18
การศึกษา		
- ประถมศึกษาหรือต่ำกว่า	8	2.59
- มัธยมศึกษา หรืออนุปริญญา	81	26.21
- ปริญญาตรี	189	61.17
- การศึกษาหลังปริญญาตรี	31	10.03
ตำแหน่ง		
- ระดับปฏิบัติการ	294	95.15
- หัวหน้าหน่วย/หัวหน้างาน	12	3.88
- ผู้บริหาร	3	0.97
ระยะเวลาในการทำงานในศูนย์การแพทย์ฯ	38	12.30
- มากกว่า 6 เดือน – 1 ปี	92	29.77
- 1 – 5 ปี	179	57.93
- มากกว่า 5 ปี		

จากการศึกษาวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรศูนย์การแพทย์กาญจนาภิเษก ทั้งหมด 8 ด้าน พบว่าในภาพรวมบุคลากรมีวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศในระดับที่ผ่าน

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

เกณฑ์ ($\bar{x}$ = 4.03, SD = 0.62) โดยพบว่าด้าน ความรู้และการรับรู้ข้อมูลพื้นฐาน (Background questions) ซึ่งมีวัตถุประสงค์เพื่อประเมินความรู้ และการรับรู้ข้อมูลพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ มีค่าเฉลี่ยสูงที่สุด ($\bar{x}$ = 4.21, SD = 0.13) รองลงมาเป็นด้านการจัดการทรัพย์สินสารสนเทศ(Information asset management) ซึ่งมีวัตถุประสงค์ เพื่อประเมินการรับรู้ของบุคลากรในการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ มีค่าเฉลี่ย $\bar{x}$ = 4.06, SD = 0.60 รองลงมาเป็นด้านนโยบาย และระเบียบปฏิบัติ (Information security policies), ด้านการนำองค์กร (Information security leadership), ด้านการจัดการผู้ใช้งาน (User management) , ด้านความเชื่อมั่นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการรักษาความเป็นส่วนตัว (Trust and privacy protection), ด้านการบริหารการเปลี่ยนแปลง (Change management) และด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security program) ตามลำดับ รายละเอียดดังแสดงในตารางที่ 3

ตารางที่ 3 ผลการศึกษาวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก

	ISCA dimensions	วัตถุประสงค์	$\bar{X}$	SD	ความหมาย
1.	ความรู้ และการรับรู้ข้อมูลพื้นฐาน (Background questions)	เพื่อประเมินความรู้ และการรับรู้ข้อมูลพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ	4.21	0.13	ผ่าน
2.	นโยบาย และระเบียบปฏิบัติ (Information security policies)	เพื่อประเมินการรับรู้ และความเข้าใจของบุคลากรเกี่ยวกับนโยบายความมั่นคงปลอดภัยสารสนเทศตลอดจนความสำเร็จในการสื่อสารนโยบาย	4.02	0.64	ผ่าน
3.	การนำองค์กร (Information security leadership)	เพื่อประเมินการรับรู้ของบุคลากรต่อการธรรมาภิบาลข้อมูล, การติดตาม ตลอดจนการให้ความสำคัญด้านความมั่นคงปลอดภัยสารสนเทศของผู้บริหาร	4.00	0.57	ผ่าน
4.	การจัดการทรัพย์สินสารสนเทศ (Information asset management)	เพื่อประเมินการรับรู้ของบุคลากรในการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ	4.06	0.60	ผ่าน
5.	การจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security program)	เพื่อประเมินการรับรู้ประสิทธิผลการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ	3.98	0.60	ไม่ผ่าน
6.	การบริหารการเปลี่ยนแปลง (Change management)	เพื่อประเมินทัศนคติของบุคลากรในการดำเนินการเพื่อให้เกิดความมั่นคงปลอดภัยสารสนเทศ	3.99	0.67	ไม่ผ่าน
7.	ความเชื่อมั่นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการรักษาความเป็นส่วนตัว (Trust and privacy protection)	เพื่อประเมินการรับรู้ และความเชื่อมั่นของบุคลากรต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการรักษาความเป็นส่วนตัวของข้อมูล	3.99	0.63	ไม่ผ่าน
8.	การจัดการผู้ใช้งาน (User management)	เพื่อประเมินความตระหนักรู้ การบริหารจัดการ user และอื่น ๆ	4.00	0.59	ผ่าน
	ภาพรวม (Overall)	ภาพรวม	4.03	0.62	ผ่าน

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

จากผลการศึกษาพบว่ามีวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 3 ด้านที่ไม่ผ่านเกณฑ์การประเมิน โดยได้กำหนดเกณฑ์การผ่านการประเมินไว้ที่ระดับคะแนน 4.00 ขึ้นไป ได้แก่ 1) ด้านความเชื่อมั่นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการรักษาความเป็นส่วนตัว (Trust and privacy protection) ซึ่งมีวัตถุประสงค์ เพื่อประเมินการ รับรู้ และความเชื่อมั่นของบุคลากรต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล มีค่าเฉลี่ย $\bar{x}$ = 3.99, SD = 0.63 2) ด้านการบริหารการเปลี่ยนแปลง (Change management) ที่มีวัตถุประสงค์เพื่อประเมินทัศนคติของบุคลากรในการดำเนินการเพื่อให้เกิดความมั่นคงปลอดภัยสารสนเทศ มีค่าเฉลี่ย $\bar{x}$ = 3.99, SD = 0.67 และ 3) ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security program) ซึ่งมีวัตถุประสงค์เพื่อประเมินการรับรู้ประสิทธิผลการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ มีค่าเฉลี่ย $\bar{x}$ = 3.98, SD = 0.60

จากการศึกษาเพื่อเปรียบเทียบวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ ระหว่างบุคลากรในขอบเขตและบุคลากรที่อยู่นอกขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก คณะแพทยศาสตร์ศิริราชพยาบาล พบว่าค่าเฉลี่ยระดับวัฒนธรรมองค์กรของบุคลากรในหน่วยงานที่อยู่ในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ มีค่าเฉลี่ย $\bar{x}$ = 4.11, SD = 0.55 ส่วนบุคลากรในหน่วยงานที่ไม่อยู่ในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ มีค่าเฉลี่ย $\bar{x}$ = 3.98, SD = 0.56 รายละเอียดดังตารางที่ 4

ตารางที่ 4. แสดงผลการประเมินวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ เปรียบเทียบระหว่างกลุ่มบุคลากรในขอบเขตและบุคลากรที่อยู่นอกขอบเขต การบริหารความมั่นคงปลอดภัยสารสนเทศ

ISCA dimensions		หน่วยงาน				p-value
		ในขอบเขต (n = 90)		นอกขอบเขต (n = 218)		
		$\bar{x}$	SD	$\bar{x}$	SD	
1.	ความรู้ และการรับรู้ข้อมูลพื้นฐาน	4.30	0.10	4.13	0.14	0.194
2.	นโยบาย และระเบียบปฏิบัติ	4.18	0.61	3.98	0.66	0.443
3.	การนำองค์กร	4.00	0.62	3.96	0.58	0.142
4.	การจัดการทรัพย์สินสารสนเทศ	4.13	0.61	4.03	0.61	0.303
5.	การจัดการความมั่นคงปลอดภัยสารสนเทศ	4.06	0.57	3.95	0.62	0.478
6.	การบริหารการเปลี่ยนแปลง	4.09	0.66	3.95	0.68	0.473
7.	ความเชื่อมั่นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการรักษาความเป็นส่วนตัว	4.09	0.65	3.94	0.64	0.324
8.	การจัดการผู้ใช้งาน	4.10	0.59	3.96	0.60	0.393
	ภาพรวม	4.11	0.55	3.98	0.56	0.344

จากตารางที่ 4 เมื่อเปรียบเทียบผล โดยใช้สถิติเปรียบเทียบระหว่างกลุ่มบุคลากรในขอบเขตและบุคลากรที่อยู่นอกขอบเขต การบริหารความมั่นคงปลอดภัยสารสนเทศ ศูนย์การแพทย์กาญจนาภิเษก พบว่าทั้งภาพรวมและผลในแต่ละด้านไม่มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($p > .05$)

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

อภิปรายและสรุปผลการวิจัย

จากการวิเคราะห์ข้อมูลวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรศูนย์การแพทย์กาญจนาภิเษก โดยแบ่งออกเป็น 8 ด้านได้แก่ 1) ด้านความรู้ และการรับรู้ข้อมูลพื้นฐาน (Background questions) 2) ด้านการรับรู้ และความเข้าใจเกี่ยวกับนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information security policies) 3) ด้านการนำองค์กรของผู้บริหารระดับสูง (Information security leadership) 4) ด้านการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ (Information asset management) 5) ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security program) 6) ด้านการบริหารการเปลี่ยนแปลง (Change management) 7) ด้านการรับรู้และความเชื่อมั่นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการรักษาความเป็นส่วนตัว (Trust and privacy protection) และ 8) ด้านการจัดการผู้ใช้งาน (User management)

จากผลการศึกษาพบว่าในภาพรวมบุคลากรศูนย์การแพทย์กาญจนาภิเษกมีวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศอยู่ในระดับที่ผ่านเกณฑ์ ทั้งนี้เมื่อพิจารณาเปรียบเทียบระหว่างบุคลากรในขอบเขตและบุคลากรที่อยู่นอกขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศ พบว่าไม่มีความแตกต่างกันอย่างมีนัยสำคัญ อย่างไรก็ตามเมื่อใช้เกณฑ์ระดับคะแนนเฉลี่ยผ่านเกณฑ์ที่ 4.00 พบว่าบุคลากรที่อยู่ในขอบเขตการบริหารความมั่นคงปลอดภัยสารสนเทศมีระดับคะแนนเฉลี่ยที่ผ่านเกณฑ์ในทุกด้านของการประเมิน ในขณะที่บุคลากรที่ไม่อยู่ในขอบเขตฯ มีระดับคะแนนเฉลี่ยที่ผ่านเกณฑ์เพียง 2 ด้าน คือ ด้านความรู้ และการรับรู้ข้อมูลพื้นฐาน และด้านการจัดการทรัพย์สินสารสนเทศ

เมื่อจำแนกผลการประเมินวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศตามเพศ อายุ ตำแหน่ง และระยะเวลาที่ปฏิบัติงานในศูนย์การแพทย์ฯ ทั้งภาพรวมและผลในแต่ละด้านไม่มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($p > .05$) อย่างไรก็ตามพบว่าเมื่อจำแนกผลตามระดับการศึกษาพบว่าผู้ที่มีระดับการศึกษาระดับประถมศึกษาหรือต่ำกว่ามีระดับวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ ในภาพรวมไม่แตกต่างจากกลุ่มอื่น ($p > .05$) แต่ด้าน Background questions ซึ่งมีวัตถุประสงค์เพื่อประเมินความรู้ และการรับรู้ข้อมูลพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศแตกต่างกับกลุ่มอื่นอย่างมีนัยสำคัญ ($p < .05$) โดยมีค่าเฉลี่ย $\bar{x} = 2.59$, SD = 0.28 โดยเมื่อพิจารณาจากตำแหน่งงาน และหน่วยงานที่สังกัดพบว่าเป็นตำแหน่งงานที่ไม่เกี่ยวข้องกับระบบคอมพิวเตอร์หรือข้อมูล

จากผลการวิเคราะห์ข้อมูลวัฒนธรรมองค์กรในแต่ละด้าน สอดคล้องกับการศึกษาของ เมธาพร ธรรมสิริ และ ศิริภัสสรศ์ วงศ์ทองดี (2565) พบว่าเพศ อายุ และประสบการณ์ในการทำงานของบุคลากรที่แตกต่างกัน มีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่แตกต่างกัน อย่างไรก็ตามพบว่าระดับการศึกษา และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศมีผลต่อความตระหนักรู้ดังกล่าว และสอดคล้องกับการศึกษาของ อภิญญา รัตนาตรานุรักษ์ (2561) ซึ่งพบว่าการรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติที่มีต่อการปฏิบัติตามนโยบาย การรับรู้ถึงความรับผิดชอบ และการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศส่งผลต่อความตั้งใจ และพฤติกรรมในการปฏิบัติตามนโยบาย และระเบียบปฏิบัติการที่เกี่ยวข้องในการรักษาความมั่นคงปลอดภัยสารสนเทศ การศึกษาของ Bulgurcu et al. (2010) และ Shropshire et al. (2015) พบว่าการที่พนักงานรับรู้และตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นกับสารสนเทศขององค์กรส่งผลต่อความตั้งใจที่จะปฏิบัติตามนโยบาย ดังนั้นหากองค์กรต้องการให้พนักงานปฏิบัติตามนโยบาย และระเบียบปฏิบัติที่เกี่ยวข้ององค์การต้องส่งเสริมให้บุคลากรมีการรับรู้ถึงภัยคุกคาม การรับรู้ถึงหน้าที่ความรับผิดชอบ และตระหนักถึงความสำคัญ เพื่อกระตุ้นและเป็นแรงจูงใจให้กับพนักงานในองค์กร ซึ่ง

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

สอดคล้องกับการศึกษาของ Ifinedo (2012) และ Vance et al. (2015)

ทั้งนี้จากผลการศึกษาถึงแม้ศูนย์การแพทย์ฯ จะมีภาพรวมระดับคะแนนเฉลี่ยของวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศที่ผ่านเกณฑ์ แต่เมื่อพิจารณาแต่ละด้านของการประเมินพบว่ามีด้านที่ไม่ผ่านเกณฑ์ถึง 3 ด้าน ได้แก่ 1) ด้านความเชื่อมั่นต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และการรักษาความเป็นส่วนตัว 2) ด้านการบริหารการเปลี่ยนแปลงและ 3) ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนั้นองค์กรจึงควรพัฒนา และส่งเสริมให้เกิดการรับรู้ และสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

ข้อเสนอแนะจากการศึกษา

ศูนย์การแพทย์กาญจนาภิเษก ได้นำระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC27001 มาใช้เพื่อการรักษาความลับ (confidentiality), ความถูกต้อง ครบถ้วน สมบูรณ์ (integrity), และความพร้อมใช้ของข้อมูล (availability), ทั้งนี้โดยส่วนใหญ่จะเน้นที่กระบวนการทางเทคนิค โดยใช้เครื่องมือทางคอมพิวเตอร์ และระบบเน็ตเวิร์ค อย่างไรก็ตามการจัดการเชิงพฤติกรรมของพนักงาน/เจ้าหน้าที่ ที่มีปฏิสัมพันธ์โดยตรงกับข้อมูลมักไม่ถูกกล่าวถึง และเป็นความท้าทายในเชิงการบริหารจัดการ การศึกษาวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศจะเป็นจุดเริ่มต้นที่ช่วยให้ทราบถึงจุดพัฒนา เพื่อส่งเสริมให้บุคลากรมีความรู้ เกิดการรับรู้ และสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ แล้วประเมินความเปลี่ยนแปลงของระดับคะแนนวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศอีกครั้งเพื่อเปรียบเทียบ

เอกสารอ้างอิง

เมธาพร ธรรมสิริ และ ศิริภัสสรศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. *วารสารวิชาการไทยและการจัดการ. 3*(2), 1-17

อภิญญา รัตนาตรานุรักษ์. (2561). ปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ. *วารสารระบบสารสนเทศด้านธุรกิจ (JISB). 4*(3), 40-65.

AlHogail, A. & Mirza, A. (2014, October 1). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, pp. 1-7. DOI: 10.1109/WCCAIS.2014.6916579.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review, 31*(2), 243-256. doi: 10.1016/j.clsr.2015.01.005

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security, 31*, 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding transition towards information security culture change. *In Proceedings of 3rd Australian Information*

Received: August 4, 2022, Revised: June 27, 2023, Accepted: August 7, 2023
http://doi.org/10.14456/jmu.

Security Management Conference, pp. 67-73. https://ro.ecu.edu.au/ecuworks/7317/

Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2020). Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal, 34*(2), 340-357. https://doi.org/10.1057/s41284-020-00228-4

Schlienger, T. & Teufel, S., (2003, September 1-5). Analyzing information security culture: increased trust by an appropriate information security culture*, 14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings*, pp. 405-409. DOI: 10.1109/DEXA.2003.1232055

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computer and Security, 49*, 177-191.

Vance, A., Lowry, P. B., & Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface, *MIS Quarterly*, *39*(2), 345-366