วารสาร Mahidol R2R e-Journal ปีที่ 8 ฉบับที่ 2 ประจำเดือนพฤษภาคม-สิงหาคม 2564
Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

ความมั่นคงปลอดภัยระบบสารสนเทศ (ISO27001: 2013) – มิติใหม่ของการบริหารจัดการโรงพยาบาล

The Information Security Management System (ISO27001: 2013) – A New Dimension in Hospital Management

กิตติศักดิ์ แก้วบุตรดี*
Kittisak Kaewbooddee*

บทคัดย่อ

การถือกำเนิดของเทคโนโลยีสารสนเทศได้นำไปสู่การเปลี่ยนแปลงในปัจจุบันเป็นอย่างมาก ในด้านของการบริหารจัดการ ทำให้การเข้าถึงการบริการ หรือการทำธุรกรรมต่าง ๆ สามารถทำได้ด้วยความรวดเร็วผ่านช่องทางออนไลน์ ในปัจจุบันมนุษย์กำลังสื่อสารผ่านช่องทางดิจิตอลมากกว่าโลกทางกายภาพ การสื่อสารกับผู้รับบริการหรือพันธมิตรทางธุรกิจ สามารถจัดการประชุมแบบดิจิทัลได้ทุกที่ทุกเวลาผ่านรูปแบบของการประชุมผ่านทางระบบวิดีโอ รวมไปถึงการดำเนินธุรกรรม สามารถชำระเงินให้กับผู้ให้บริการได้อย่างสะดวก โดยการโอนเงินหรือชำระเงินผ่านระบบอิเล็กทรอนิกส์หลังจากที่รับการบริการได้ด้วยระบบออนไลน์ผ่านโทรศัพท์มือถือได้ทันที

ความก้าวหน้าทางด้านเทคโนโลยีสารสนเทศส่งผลให้ข้อมูลการทำธุรกรรม ข้อมูลการใช้งาน และข้อมูลส่วนตัวถูกบันทึก และข้อมูลดังกล่าวถูกดูแลโดยผู้ให้บริการหรือผู้เก็บรักษาข้อมูล ส่งผลให้การเข้าถึงข้อมูลที่สำคัญต่าง ๆ เหล่านั้นทำได้ง่ายขึ้น ดังนั้นเพื่อความน่าเชื่อถือ สร้างความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลที่ให้บริการต่าง ๆ ในการดำเนินธุรกิจ การเพิ่มความน่าเชื่อถือให้แก่ลูกค้า และเพิ่มมูลค่าขององค์กรด้วยการออกมาตรการในการรักษาความปลอดภัยของระบบสารสนเทศเพิ่มมากขึ้น ด้วยกระบวนการพัฒนาให้ระบบสารสนเทศมีความมั่นคงปลอดภัยมากยิ่งขึ้น

การให้บริการแก่ผู้ป่วยของคณะแพทยศาสตร์ศิริราชพยาบาลมีการบันทึกข้อมูลส่วนตัว และข้อมูลของการรักษาพยาบาล รวมไปถึงข้อมูลการทำหัตถการต่าง ๆ ซึ่งข้อมูลเหล่านี้ถือเป็นข้อมูลส่วนบุคคลที่สำคัญ คณะแพทยศาสตร์ศิริราชพยาบาลมีภาระหน้าที่โดยตรงในการดูแลข้อมูลให้มีความมั่นคงปลอดภัยจึงดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) เพื่อกำกับดูแลระบบสารสนเทศ และข้อมูลต่าง ๆ ให้มีความมั่นคงและปลอดภัยตามมาตรฐานสากล

คำสำคัญ: ความมั่นคงปลอดภัยระบบสารสนเทศ; ความมั่นคงปลอดภัยของข้อมูล; การบริหารโรงพยาบาล

---

*ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล
*Siriraj Information Technology Department, Faculty of Medicine Siriraj Hospital, Mahidol University
*Corresponding Author: kittisak.kae@mahidol.ac.th

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

Abstract

The advent of information technology has brought dramatic changes in the field of management. Nowadays in the online world can be enabling access to the service, e-commerce and commercial just click away. Today humans are living in the digital world rather than the physical world and communicating with clients or business partners can conduct the digital meetings from anywhere at any time by video conferencing. The client can make online payment transactions via mobile phones instantly.

Advances in information technology systems had resulted in transactional data, usage information and personal information recorded by the service providers. Resulting in service providers more easily accessing important information. In order for credibility and data security in the field of business operations. Therefore, the service has taken measures to increase the reliability of customers and enhance corporate value. The service provider maintains information systems to be more secure.

The patient information and patient treatment information has been recorded during hospital services and all of the information considered personal. The Faculty of Medicine Siriraj Hospital was responsible for maintaining information to be secure according to international standards in order to information security. Faculty of Medicine Siriraj Hospital has implemented the Information Security Management System (ISO/IEC27001: 2013) in order to security according to international standards.

Key Words: Information security Management; Data security; Hospital Management

บทนำ

ยุคโลกาภิวัฒน์ความก้าวหน้าทางด้านระบบเทคโนโลยีสารสนเทศส่งผลให้การดำเนินธุรกิจต่าง ๆ มีการเปลี่ยนแปลงอย่างรวดเร็ว ทั้งในส่วนของผู้ให้บริการและผู้รับบริการต้องมีการปรับตัวให้ทันกับการเปลี่ยนแปลงอยู่เสมอ การให้บริการในส่วนต่าง ๆ ของคณะแพทยศาสตร์ศิริราชพยาบาลต้องมีความสะดวกและรวดเร็วเพื่อตอบสนองความต้องการของทุกฝ่ายที่เกี่ยวข้อง บนพื้นฐานของการให้บริการที่สะดวก และรวดเร็วนั้น คณะแพทยศาสตร์ศิริราชพยาบาลต้องมีความมั่นใจว่าระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพ และมีความมั่นคงปลอดภัย รวมไปถึงข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการให้บริการต้องมีความถูกต้องและสามารถตรวจสอบได้ เพื่อให้การให้บริการต่าง ๆ ทันต่อความต้องการ ระบบสารสนเทศและข้อมูลที่อยู่ในการดูแลต้องมีความพร้อมใช้งานอยู่เสมอ

การจู่โจมทางไซเบอร์ถือเป็นปัญหาใหญ่ในหลายองค์กร เป็นเรื่องที่สามารถเกิดขึ้นได้บ่อย ๆ ในปัจจุบัน และการป้องการจู่โจมก็สามารถทำได้ยากมากขึ้นอีกด้วย สิ่งที่คณะแพทยศาสตร์ศิริราชพยาบาลต้องทำอย่างสม่ำเสมอคือการทบทวนนโยบายเรื่องความมั่นคงปลอดภัยของระบบสารสนเทศ รวมไปถึงข้อมูลที่เกี่ยวข้องต่าง ๆ อย่างสม่ำเสมอ กระบวนการดังกล่าวยังถือเป็นกระบวนการที่มีความสำคัญที่มีส่วนสนับสนุนให้การดำเนินธุรกิจบรรลุวัตถุประสงค์ของคณะแพทยศาสตร์ศิริราชพยาบาล

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

ข้อมูลเป็นสินทรัพย์ที่มีค่ามากที่สุดของทุกองค์กร รวมทั้งคณะแพทยศาสตร์ศิริราชพยาบาลด้วย การละเมิดข้อมูลและการนำข้อมูลไปใช้ในด้านต่าง ๆ โดยผู้ที่ไม่ได้รับอนุญาตนั้นเป็นสาเหตุที่ก่อให้เกิดความเสียหายอย่างร้ายแรง อาจเกิดการฟ้องร้องจากเจ้าของข้อมูลหรือผู้รับบริการ ทำให้เกิดความเสียหาย ขาดความเชื่อมั่นจากผู้รับบริการรวมไปถึงพันธมิตรทางธุรกิจ ส่งผลให้เสียชื่อเสียงได้ ดังนั้น คณะแพทยศาสตร์ศิริราช-พยาบาลจำเป็นต้องสร้างมาตรฐานการควบคุมการเข้าถึงข้อมูล มีการประเมินและติดตามความเสี่ยงที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา เพื่อป้องกันมิให้มีการละเมิดข้อมูลเกิดขึ้น

การปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศเกี่ยวกับการใช้คอมพิวเตอร์และซอฟต์แวร์ที่เกี่ยวข้องกับการปฏิบัติงานถือเป็นความสำคัญของคณะแพทยศาสตร์ศิริราชพยาบาลเพื่อเป็นการป้องกันความเสียหายที่อาจจะเกิดขึ้นจากการปฏิบัติหน้าที่ ในปัจจุบันคณะแพทยศาสตร์ศิริราชพยาบาลได้ดำเนินการโครงการความมั่งคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) และส่งเสริมให้บุคลากรมีความตระหนักถึงความสำคัญของการรักษาความปลอดภัยระบบสารสนเทศ และข้อมูลที่เกี่ยวข้องในการให้บริการผู้ป่วย เพื่อให้องค์กรสามารถดำเนินการตามวิสัยทัศน์ที่ว่า “สถาบันทางการแพทย์ของแผ่นดินมุ่งสู่ความเป็นเลิศระดับสากล” (คณะแพทยศาสตร์ศิริราชพยาบาล, 2562) ทุกส่วนงานที่เกี่ยวข้องต้องปฏิบัติตามพื้นฐานของความมั่นคงปลอดภัยสารสนเทศอันได้แก่ ความลับ (Confidentiality) การรักษาความลับของข้อมูลผู้ป่วยและข้อมูลต่าง ๆ ที่เป็นความลับ ข้อมูลสารสนเทศจะต้องถูกกำหนดให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตให้สามารถเข้าถึงข้อมูลสารสนเทศ, ความถูกต้องสมบูรณ์ (Integrity) ข้อมูลจะต้องมีความถูกต้องสมบูรณ์อยู่เสมอและผู้ที่แก้ไขข้อมูลจะต้องเป็นผู้ที่ได้รับอนุญาตเท่านั้น และความพร้อมใช้ (Availability) ระบบสารสนเทศจะต้องมีความพร้อมที่จะให้บริการ และพร้อมที่จะเข้าถึงได้ตลอดเวลาที่ต้องการ (Vallabhaneni, 2018) ดังนั้นถ้าไม่ปฏิบัติตามพื้นฐานที่จำเป็นเหล่านี้อาจจะทำให้องค์กรมีความเสี่ยงที่จะถูกโจมตีทางไซเบอร์ และทำให้องค์เกิดเกิดความเสียหายได้

ความเป็นมาและความหมายของความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013)

ความมั่นคงปลอดภัยสารสนเทศ (ISO27001) เป็นมาตรฐานความปลอดภัยของระบบสารสนเทศซึ่งเป็นส่วนหนึ่งของมาตรฐาน ISO27000 ซึ่งเป็นรุ่นสุดท้ายมีการปรับปรุงเพียงเล็กน้อย และเผยแพร่ในปี พ.ศ. 2556 (ค.ศ. 2013) โดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization: ISO) และคณะกรรมการ Electrotechnical ระหว่างประเทศ (IEC) ภายใต้คณะอนุกรรมการร่วม ISO (The British Standards Institution, 2019) ดังรูปที่ 1

รูปที่ 1 ความเป็นมาของความมั่นคงปลอดภัยระบบสารสนเทศ

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

ความมั่นคงปลอดภัยระบบสารสนเทศ คือ การบริหารจัดการระบบสารสนเทศที่มีวัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และข้อมูลที่เกี่ยวข้องภายใต้การควบคุมที่เหมาะสม องค์กรใดที่ปฏิบัติตามข้อกำหนดจะได้รับการรับรองหลังจากการตรวจสอบเสร็จแล้วโดยหน่วยงานที่ออกใบรับรอง (Certificate) ประวัติของความมั่นคงปลอดภัยระบบสารสนเทศกำเนิดขึ้นเมื่อปี พ.ศ. 2535 (ค.ศ. 1992) โดยกรมการค้าและอุตสาหกรรม (DTI) ซึ่งเป็นส่วนหนึ่งของรัฐบาลสหราชอาณาจักรได้เผยแพร่ "หลักปฏิบัติสำหรับการจัดการความปลอดภัยของข้อมูล" เพื่อใช้เป็นหลักปฏิบัติในการกำกับดูแลความปลอดภัยของข้อมูล ในปี พ.ศ. 2538 (ค.ศ. 1995) สถาบันมาตรฐานอังกฤษ (British Standards Institute: BSI) ได้มีการปรับปรุง และแก้ไขเอกสาร “หลักปฏิบัติสำหรับการจัดการความปลอดภัยของข้อมูล” โดยใช้ชื่อใหม่ว่า BS7799 (Honan, 2014)

ในเดือนธันวาคม ปี พ.ศ. 2543 (ค.ศ. 2000) เอกสาร BS7799 ฉบับที่ถูกปรับปรุงโดยสถาบันมาตรฐานอังกฤษถูกเผยแพรในชื่อมาตรฐาน ISO/IEC 17799 ถือเป็นจุดกำเนิดของมาตรฐาน ISO อย่างจริงจังมากขึ้น จนถึงปี พ.ศ. 2548 (ค.ศ. 2005) ได้มีการเผยแพร่มาตรฐาน ISO/IEC27001: 2005 ซึ่งต่อมาได้เป็นข้อกำหนดสำหรับระบบการจัดการความปลอดภัยของระบบสารสนเทศ และมีความสอดคล้องกับมาตรฐาน ISO 17799 ในวันที่ 25 กันยายน พ.ศ. 2556 (ค.ศ. 2005) ได้มีการยกเลิก ISO27001: 2005 และได้มีการเผยแพร่มาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศฉบับใหม่คือ ISO/IEC27001: 2013 ซึ่งฉบับนี้ยังคงถูกใช้อยู่จนถึงปัจจุบัน (Honan, 2014)

แนวโน้มของการขอรับรองความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) ในปัจจุบัน

ความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) มีขอบเขตการควบคุมนโยบาย กระบวนการทำงาน และระบบสารสนเทศที่เกี่ยวข้องต่าง ๆ ซึ่งการปฏิบัติตามขอบเขตของโครงการนั้น องค์กรจะต้องพัฒนาวิธีคิด และนโยบายต่าง ๆ รวมไปถึงการปฏิบัติงานให้ครอบคลุมการบริหารงานโดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด (ศิริพร ชำนาญชาติ, 2561)

ความปลอดภัยของข้อมูล และข้อมูลของการรักษาพยาบาลของผู้ป่วยที่มารับการรักษาที่คณะแพทยศาสตร์ศิริราชพยาบาลเป็นข้อมูลที่เป็นความลับของผู้ป่วย คณะแพทยาสตร์ศิริราชพยาบาลได้ตระหนักและให้ความสำคัญกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างจริงจังเพื่อป้องกันความเสี่ยงที่ข้อมูลผู้ป่วยจะถูกโจรกรรม และอาจส่งผลกระทบต่อชื่อเสียงภาพลักษณ์ของคณะแพทย์ศาสตร์ศิริราชพยาบาล จากรายงานองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization: ISO) ทำให้ทราบว่าองค์กรในประเทศไทยได้ให้ความสำคัญในด้านการกำกับดูแลระบบสารสนเทศให้มีความมั่นคงปลอดภัยมากขึ้นเป็นลำดับโดยในปี พ.ศ. 2557 - พ.ศ. 2561 พบว่ามีองค์กรที่ได้รับรองมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) จำนวนมากถึง 1,076 องค์กร และจำนวนการขอรับรองมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ ในปี พ.ศ. 2557 –พ.ศ.2661 มีจำนวนเพิ่มขึ้น (International Organization for Standardization, 2019 ดังตารางที่ 1

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

ตารางที่ 1 แสดงจำนวนการขอรับรองมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC27001: 2013)

ปี พ.ศ.	2557	2558	2559	2560	2561	รวม
จำนวน	143	189	218	287	239	1,076

ที่มา: ดัดแปลงมาจากรายงานการรับรองมาตรฐานระบบการจัดการ องค์การมาตรฐานสากล (ISO)

พื้นฐานของความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013)

ความมั่นคงปลอดภัยระบบสารสนเทศมีพื้นฐานสำคัญที่ช่วยส่งเสริมให้การดำเนินงานของคณะแพทยศาสตร์ศิริราชพยาบาลสำเร็จลุล่วงตามเป้าหมาย การรักษาความมั่นคงปลอดภัยของทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือข้อมูลสารสนเทศให้มีความมั่นคงและปลอดภัยประกอบไปด้วยองค์ประกอบพื้นฐานที่สำคัญ 3 ข้อดังนี้

รูปที่ 2 องค์ประกอบพื้นฐานความมั่นคงปลอดภัยสารสนเทศ (CIA)

ความลับของข้อมูล (Confidentiality) เป็นองค์ประกอบที่สำคัญที่สุดของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ การป้องกันและรักษาความลับของข้อมูลหรือเอกสารต่าง ๆ ที่มีประสิทธิภาพ ผู้บริหารต้องมีต้องมีนโยบายและมาตรการตรวจสอบสิทธิในการเข้าถึงข้อมูล ผู้ปฏิบัติงานที่มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลเหล่านั้นได้ การยืนยันตัวตนในการเข้าถึงระบบสารสนเทศ และข้อมูลต่าง ๆ ที่ใช้กันอย่างแพร่หลายในปัจจุบันนี้ คือการใช้รหัสผ่าน (Password) ส่วนบุคคลในการเข้าถึงระบบสารสนเทศ (Srinivasan, 2016)

การกำหนดชั้นความลับ ของการเอกสารการดำเนินงานในโครงการความมั่นคงปลอดภัยระบบสารสนเทศเป็นอีกหนึ่งปัจจัยที่สำคัญที่ทำให้การดำเนินโครงการบรรลุผลสำเร็จ โดยได้กำหนดชั้นความลับแบ่งออกเป็น 3 ประเภทตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. 2544 (สำนักนายกรัฐมนตรี, 2544)

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

ประกอบด้วย ระดับชั้นลับที่สุด (Top Secret), ระดับชั้นลับมาก (Secret), ระดับชั้นลับ (Confidential) และระดับชั้นข้อมูลที่ถูกกำหนดขึ้นเพิ่มเติมประกอบด้วย ระดับชั้นข้อมูลสำหรับใช้ภายในองค์กร (Internal Use) และระดับชั้นสารธารณะ (Public) (ฝ่ายสารสนเทศ, 2562) ทั้งนี้ในปัจจุบันการปกป้องความลับ เช่น การเข้ารหัส (Encryption) ถูกนำมาใช้ในการปกป้องสารสนเทศที่ต้องการการดูแลอย่างเข้มงวดกันอย่างแพร่หลาย ตัวอย่างเช่น การเก็บรักษาเอกสารคุณภาพของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล เอกสารคุณภาพที่มีการขึ้นทะเบียน และถูกจัดให้เป็นเอการชั้นความลับต่าง ๆ นั้นเป็นหน้าที่ของเจ้าหน้าที่ผู้ดูแลเอกสารคุณภาพ (Document Control) ซึ่งได้รับมอบหมายในการดูแลเอกสารชั้นความลับ เอกสารเหล่านี้จะถูกเก็บไว้ในตู้อยู่ในห้องมั่นคง ซึ่งเป็นห้องที่มีลักษณะทนความร้อน กันไฟไหม้ ผู้ที่มีสิทธิสามารถเข้าถึงเอกสารเหล่านี้ได้คือเจ้าหน้าที่ผู้ดูเอกสารคุณภาพที่ถูกกำหนดไว้เท่านั้น

ในการรักษาความลับของข้อมูลการรักษาพยาบาลของผู้ป่วย รวมไปถึงข้อมูลต่าง ๆ ที่อยู่ในระบบสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้มีมาตรฐานในการป้องกันการเข้าถึงข้อมูล และการกำหนดสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ ตามภาระหน้าที่ความรับผิดชอบในแต่ละตำแหน่ง ในกรณีที่มีการแก้ไขข้อมูลที่สำคัญในระบบสารสนเทศจะมีการจัดเก็บประวัติของการแก้ไขข้อมูลต่าง ๆ ในระบบสารสนเทศเพื่อให้สามารถตรวจสอบในกรณีที่มีความจำเป็น โดยสาระสำคัญของการกำหนดสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ ในระบบสารสนเทศเพื่อป้องกันไม่ให้ข้อมูลที่สำคัญถูกแก้ไข หรือถูกทำสำเนาโดยผู้ที่ไม่ได้รับอนุญาต ซึ่งถ้าข้อมูลเหล่านี้ถูกแก้ไข หรือทำสำเนา และถูกนำไปใช้ในทางที่ผิดจะมาซึ่งความเสียหายอย่างร้ายแรงต่อคณะแพทยศาสตร์ศิริราชพยาบาลได้

ความถูกต้องสมบูรณ์ของข้อมูล (Integrity) ความถูกต้องสมบูรณ์ของข้อมูลเป็นสิ่งที่สะท้อนถึงความน่าเชื่อถือของระบบสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล และข้อมูลสารสนเทศ ส่งผลถึงความน่าเชื่อถือ ข้อมูลต้องไม่ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาตในระหว่างและหลังจากการบันทึก ทั้งนี้ข้อมูลมีความถูกต้องสมบูรณ์เพียงใดนั้น ต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใด ๆ ต่อข้อมูล เช่นการเก็บประวัติการแก้ไขข้อมูลเพื่อให้เจ้าหน้าที่ที่ปฏิบัติงานสามารถตรวจสอบ และติดตามการแก้ไขข้อมูลได้ หากข้อมูลถูกเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่ประสงค์ดีย่อมส่งผลเสียต่อเจ้าของข้อมูล ความน่าเชื่อถือต่อคณะแพทยศาสตร์ศิริราชพยาบาลลดน้อยลง และอาจจะนำไปสู่การฟ้องร้องทางกฎหมายได้ (AL-Zahawi, 2019)

ความพร้อมใช้งานของข้อมูลและระบบสารสนเทศต่าง ๆ (Availability) เป็นการสร้างความเชื่อมั่นที่แสดงให้เห็นถึงความพร้อมใช้ของระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการผู้ป่วย ระบบสารสนเทศต้องตอบสนองความต้องการของผู้ใช้งานให้สามารถเข้าถึงระบบได้เมื่อต้องการ คณะ-แพทยศาสตร์ศิริราชพยาบาลมีหน้าที่ให้บริการผู้ป่วยจำนวนมาก ปัจจุบันมีนโยบายและแผนการกู้คืนระบบจากความเสียหาย (Disaster Recovery Plan) ได้อย่างทันท่วงที การให้บริการผู้ป่วยในปัจจุบัน ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือแม้แต่ระบบไฟฟ้าที่เกี่ยวข้องมีความจำเป็นอย่างยิ่ง หากอุปกรณ์ใด ๆ เกิดความขัดข้อง และไม่สามารถกู้คืนให้กลับมาให้บริการได้ทันท่วงที ทำให้การให้บริการหยุดชะงักอาจส่งผลเสียต่อการให้บริการในวงกว้างได้ เหตุการณ์ที่ทำให้เกิดความไม่พร้อมใช้งานของระบบคอมพิวเตอร์มี 2 แบบใหญ่ๆ คือ ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service) และระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability) ดังนั้นต้องทำการตรวจสอบ ประเมินสมรรถนะการทำงานของระบบสารสนเทศ และอุปกรณ์สนับสนุนที่เกี่ยวข้อง เพื่อให้มั่นใจได้ว่าระบบต่าง ๆ นั้นพร้อมใช้งานอยู่เสมอ (Barrett, Weiss, Hausman, 2015)

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

ถึงแม้ในปัจจุบันจะยังไม่เกิดเหตุการณ์ฉุกเฉินที่ทำให้ศูนย์ข้อมูล (Data Center) และระบบสารสนเทศ ซึ่งเป็นหัวใจหลักของการให้บริการของคณะแพทยศาสตร์ศิริราชพยาบาลไม่สามารถกลับมาให้บริการได้ ทั้งนี้ผู้บริหารได้กำหนดให้ทำการซ้อมแผนกรณีที่เกิดเหตุการณ์ที่ไม่คาดคิดเป็นประจำทุกปี ทำให้เกิดการเตรียมความพร้อมในกรณีฉุกเฉินที่ศูนย์ข้อมูล (Data Center) เสียหาย การซักซ้อมแผนการกู้คืนระบบสารสนเทศกรณีที่เกิดเหตุการณ์ที่ไม่คาดคิดจะทำให้เกิดความคล่องตัว และสามารถกู้คืนระบบสารสนเทศเพื่อให้การบริการผู้ป่วยของคณะแพทยศาสตร์ศิริราชพยาบาลเป็นไปอย่างทันท่วงที

นโยบายและกระบวนการทำงานที่เกี่ยวข้องในการขับเคลื่อนเพื่อสนับสนุนความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013)

ความเข้าใจในนโยบาย ISO/IEC27001: 2013 ผู้บริหารและคณะกรรมการที่เกี่ยวข้อง รวมไปถึงผู้ที่มีส่วนสนับสนุนให้การดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศประสบความสำเร็จต้องศึกษาทำความเข้าใจของความต้องการ นโยบายที่เกี่ยวข้องกับการดำเนินโครงการ ผู้บริหารต้องให้การสนับสนุนเพื่อให้เกิดการพัฒนาอย่างต่อเนื่อง เสริมสร้างความรู้ความเข้าใจให้แก่ผู้ปฏิบัติงานให้ทราบ และปฏิบัติตามนโยบายที่กำหนดไว้ (Calder, 2017; Watkins, 2013)

นำหลักการวงจรบริหารงานคุณภาพ Plan-Do-Check-Act (PDCA) ย่อมาจาก Plan (การวางแผน), Do (การปฏิบัติ), Check (การตรวจสอบ, การประเมิน) และ Act (การปรับปรุง และการดำเนินการให้เหมาะสม) มาปรับใช้แนวทางการบริหารงานคุณภาพเพื่อให้สอดคล้องกับการดำเนินงานของคณะแพทยศาสตร์ศิริราชพยาบาลเพื่อให้เกิดกระบวนการทำงานที่มีคุณภาพ สะท้อนผลการปฏิบัติงานจริง สามารถตรวจสอบผลการดำเนินงานได้ สามารถอธิบายได้ดังนี้

การวางแผน (Plan) คือการวางแผน และกำหนดขอบเขตการดำเนินการจัดตั้งโครงการโครงการความมั่นคงปลอดภัยระบบสารสนเทศ รวมไปถึงการวางแผนการดำเนินงานต่าง ๆ เช่น การศึกษาเกี่ยวกับบริบทขององค์กร, ความเป็นผู้นำของผู้บริหาร ตลอดจนการสนับสนุนการดำเนินงานต่าง ๆ จากผู้บริการระดับสูงเพื่อให้การดำเนินงานสำเร็จลุล่วงตามวัตถุประสงค์

การปฏิบัติ (Do) คือการจัดทำเอกสารการดำเนินโครงการและการลงมือปฏิบัติเพื่อให้ครอบคลุมถูกต้องตามข้อกำหนดต่าง ๆ ภายใต้กรอบของการดำเนินงานตามมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) ไปประยุกต์ใช้ในการทำงานจริง เช่น กำหนดให้มีระเบียบวิธีการพัฒนาซอฟต์แวร์ หน่วยงานทีหน้าที่ปฏิบัติตามระเบียบวิธีปฏิบัติงานดังกล่าวเพื่อให้การพัฒนาซอฟต์แวร์มีมาตรฐาน และความมั่นคงปลอดภัยจากเหตุการณ์ที่ไม่พึงประสงค์ เป็นต้น

การประเมินหรือการตรวจสอบ (Check) คือการประเมินกิจกรรมต่าง ๆ เช่น การดำเนินการตรวจสอบภายใน, การตรวจสอบความพร้อมใช้ของระบบสารสนเทศ รวมไปถึงการตรวจสอบและทบทวนนโยบาย หรือแผนการดำเนินงานประจำปีภายใต้โครงการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) ยกตัวอย่างเช่น การตรวจประเมินภายใน (Internal Audit) เป็นการเตรียมความพร้อมสำหรับการตรวจประเมินภายนอก (Certification Body) เพื่อเป็นการตรวจประเมินผลการดำเนินโครงการความมั่นคงปลอดภัยสารสนเทศให้เป็นไปตามนโยบาย เอกสารหลักฐาน และข้อกำหนดต่าง ๆ หากการตรวจประเมินจากภายนอกไม่พบประเด็นที่ไม่สอดคล้อง หน่วยงานที่ตรวจประเมินจากภายนอกจึงจะสามารถออกใบรับรองให้แก่หน่วยงานที่ขอรับตรวจได้

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

การปรับปรุง (Act) คือ การติดตามปรับปรุงข้อบกพร่อง ทบทวนและพิจารณาข้อกำหนด, วิธีปฏิบัติและนโยบายความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการวางแผนการดำเนินงานภายใต้กรอบของการดำเนินงานโครงการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) เพื่อให้เกิดการปรับปรุงข้อบกพร่อง และเกิดการพัฒนาอย่างต่อเนื่อง (Matthews, 1999) ดังรูปที่ 3

รูปที่ 3 วงจรบริหารงานคุณภาพ (PDCA)

ประโยชน์ของความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001 :2013)

ความมั่นคงปลอดภัยระบบสารสนเทศทำให้ระบบสารสนเทศและข้อมูลมีความมั่นคงปลอดภัย ลดความเสี่ยงที่อาจจะทำให้เกิดเหตุการณ์ที่ไม่คาดคิด เช่น ระบบสารสนเทศถูกโจมตีทางไซเบอร์ ทำให้ข้อมูลสูญหาย หรือข้อมูลที่สำคัญ เช่น ข้อมูลผู้ป่วย ข้อมูลทางการเงินถูกแก้ไขจากเจ้าหน้าที่ภายใน เป็นต้น การดำเนินการตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO/ IEC27001: 2013) เป็นตัวชี้วัดว่าคณะแพทยศาสตร์ศิริราชพยาบาลได้ให้ความสำคัญกับความปลอดภัยของข้อมูลที่เก็บรักษาไว้อย่างจริงจัง ซึ่งจะเป็นส่วนที่ช่วยส่งเสริม และสร้างความมั่นใจให้แก่องค์กรและผู้ป่วยที่เข้ามารับบริการ องค์กรได้มีการประเมินและระบุถึงความเสี่ยงที่อาจจะเกิดขึ้นทั้งในด้านความปลอดภัยของคอมพิวเตอร์ ความปลอดภัยทางกายภาพ ความปลอดภัยทางไซเบอร์ที่มีมากขึ้นในปัจจุบัน ล้วนส่งผลให้คณะแพทยศาสตร์ศิริราชพยาบาลได้รับประโยชน์ดังนี้ (Lopes, Guarda, & Oliveira, 2019; Moh, 2019; Velasco, Ullauri, & Pilicita, 2018)

คงไว้ซึ่งฐานผู้ป่วยที่มารับการรักษาที่คณะแพทยศาสตร์ศิริราชพยาบาล และพันธมิตรทางธุรกิจ เนื่องจากมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ถือว่าเป็นแนวปฏิบัติที่ดีที่สุดในปัจจุบัน และได้รับการยอมรับในระดับสากล ทำให้ผู้ป่วยหรือพันธมิตรทางธุรกิจให้ความไว้วางใจในความปลอดภัยของข้อมูล เนื่องจากข้อมูลส่วนตัว และข้อมูลของการรักษาพยาบาลต่าง ๆ ถือเป็นข้อมูลที่เป็นความลับเฉพาะบุคคล

ประหยัดเวลาและต้นทุน เมื่อเกิดเหตุการณ์ที่ไม่คาดคิดขึ้น เช่น การสูญเสียข้อมูลอันเนื่องมาจากเหตุการณ์ที่ไม่คาดคิดหรือถูกโจมตีทางไซเบอร์ ถ้าข้อมูลของผู้ป่วยถูกโจรกรรม คณะแพทยศาสตร์ศิริราช

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

พยาบาลจะต้องสูญเสียทรัพยากรบุคคลและเกิดต้นทุนในด้านต่าง ๆ เพื่อทำการกู้คืนระบบและข้อมูลที่สำคัญเพื่อให้องค์กรสามารถกลับมาให้บริการได้ตามปกติ ดังนั้น การปฏิบัติตามหลักความมั่นคงปลอดภัยระบบสารสนเทศจึงเป็นเกราะป้องกันเหตุการณ์ไม่พึงประสงค์ที่จะก่อให้เกิดความเสียหายดังกล่าวได้

สร้างชื่อเสียงและเพิ่มความเชื่อมั่นทั้งภายในและภายนอกคณะแพทยศาสตร์ศิริราชพยาบาล การดำเนินการตามหลักความมั่นคงปลอดภัยสารสนเทศ รวมไปถึงการประเมินความเสี่ยงอย่างสม่ำเสมอให้ลดโอกาสที่จะเกิดเหตุการณ์ที่ไม่พึงประสงค์ และทำให้เกิดการพัฒนาอย่างต่อเนื่อง (Continuous Improvement) ระบบความมั่นคงปลอดภัยสารสนเทศเป็นมาตรฐานระดับสากลที่ได้รับการยอมรับ การที่คณะแพทยศาสตร์ศิริราชพยาบาลได้รับการรับรองส่งผลโดยตรงต่อผู้ป่วย พันธมิตรทางธุรกิจ และผู้ที่มีส่วนได้ส่วนเสียให้ความไว้วางใจในมาตรฐานการกำกับดูแลข้อมูลและระบบสารสนเทศที่เกี่ยวข้องกับการดำเนินงานต่าง ๆ ซึ่งส่งผลให้คณะแพทยศาสตร์ศิริราชพยาบาลมีมาตรฐานในการบริหารจัดการระบบความปลอดภัยข้อมูลเทียบเท่าระดับสากล อีกทั้งยังสามารถนำไปประยุกต์ใช้ในการวางแผนจัดการด้านการบริหารโครงการ และความเสี่ยงต่าง ๆ ที่อาจก่อให้เกิดความสูญเสีย ซึ่งการนำระบบการจัดการความมั่นคงปลอดภัยข้อมูลมาประยุกต์ใช้อย่างมีประสิทธิภาพตั้งแต่แรกเริ่มก็จะไม่ก่อให้เกิดการสูญเสียแก่องค์กรโดยไม่จำเป็น

ข้อเสียของความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013)

ความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) ถึงแม้ว่าจะมีข้อดีในหลายๆ ด้าน แต่ก็มีข้อเสียภายใต้ดำเนินการ เช่นถ้ามุ่งเน้นเพื่อจะได้รับการรับรองตามมาตรฐาน ถึงแม้ว่าการปรับปรุงกระบวนการต่าง ๆ จะนำไปสู่ระบบการบริการที่ดีกว่า องค์กรมีแนวโน้มที่จะมุ่งเน้นไปที่การตรวจสอบ และการประเมินผลเพื่อให้ได้รับการรับรองมาตรฐาน แต่กระบวนการต่าง ๆ ที่เกิดขึ้นภายใต้การดำเนินงานของโครงการทำให้เกิดความล่าช้า อันเนื่องมาจากมีการบันทึก จัดเก็บเอกสารที่มากขึ้นทำให้เจ้าหน้าที่ที่ปฏิบัติงานเกิดความเบื่อหน่าย และอาจจะนำไปสู่การละเลยการปฏิบัติตามข้อกำหนดต่าง ๆ ของโครงการทำให้เกิดความเสี่ยงต่อกระบวนการทำงานต่าง ๆ ในอนาคตได้

ปัญหาและอุปสรรคของการดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001: 2013) ของคณะแพทยศาสตร์ศิริราชพยาบาล

ตลอดระยะเวลาในการดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลแสดงให้เห็นว่าทุกส่วนงานที่เกี่ยวข้องมีความมุ่งมั่นเพื่อที่จะพัฒนาและสร้างความมั่นคงปลอดภัยของระบบสารสนเทศในการให้บริการแก่ผู้ป่วย ปัญหาและอุปสรรคหลัก ๆ ที่พบระหว่างการดำเนินโครงการมีดังนี้

ด้านซอฟต์แวร์ เมื่อมีการดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศ ในการพัฒนาระบบซอฟต์แวร์การให้บริการผู้ป่วยของคณะแพทยศาสตร์ศิริราชพยาบาลส่วนใหญ่ยังคำนึงถึงเรื่องความปลอดภัยไม่เพียงพอ ซึ่งอาจทำให้มีช่องโหว่ที่จะถูกกลุ่มมิจฉาชีพหรือผู้ที่มีความเชี่ยวชาญใช้โจมตีระบบที่ให้ที่ให้บริการผู้ป่วยเกิดความเสียหายได้ ดังนั้นการพัฒนาระบบซอฟต์แวร์ต่าง ๆ จึงมีความจำต้องปฏิบัติตามระเบียบวิธีปฏิบัติของการพัฒนาซอฟต์แวร์อย่างเคร่งครัด

ด้านบุคลากร ที่ปฏิบัติงานยังขาดความตระหนักรู้ในเรื่องความมั่นคงปลอดภัยระบบสารสนเทศอย่างจริงจัง ทำให้ส่งผลกระทบกับการนำมา

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

ประยุกต์ใช้และลงมือปฏิบัติจริง เพื่อให้เกิดประโยชน์สูงสุดต่อองค์กร เช่นการแจกจ่าย หรือเผยแพร่ชื่อผู้ใช้งานและรหัสผ่านสำหรับเข้าใช้ระบบต่าง ๆ ให้ผู้อื่นทราบ, ไม่ตั้งภาพพักหน้าจอและรหัสผ่านคอมพิวเตอร์ซึ่งอาจจะทำให้ผู้ที่ไม่เกี่ยวข้องสามารถเข้าถึงระบบและข้อมูลที่สำคัญขององค์กร และอาจจะทำให้เกิดความเสียหายอย่างร้ายแรงได้

ด้านการปฏิบัติงาน การพัฒนาโครงการความมั่นคงปลอดภัยสารสนเทศ ทำให้เกิดกระบวนการทำงานมีความซับซ้อนมากขึ้น ส่งผลให้ผู้ปฏิบัติงานมีภาระงานที่เพิ่มมากขึ้นตามไปด้วย ดังนั้นการบริหารจัดการเรื่องกำลังคน และภาระงานจึงเป็นเรื่องที่สำคัญที่ผู้บริหารควรนำมาพิจารณา เพื่อให้การดำเนินการต่าง ๆ ภายใต้โครงการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) มีประสิทธิภาพและคล่องตัวมากขึ้น

ด้านทุนทรัพย์ การเพิ่มความปลอดภัยแก่ระบบสารสนเทศ และการดำเนินการต่าง ๆ เพื่อให้สอดคล้องตามข้อกำหนด หรือนโยบายความมั่นคงปลอดภัยสารสนเทศที่คณะแพทยศาสตร์ศิริราชพยาบาลได้กำหนดไว้ ทำให้เกิดค่าใช้จ่ายที่เพิ่มมากขึ้นตามไปด้วย แต่การดำเนินงานภายใต้โครงการความมั่นคงปลอดภัยสารสนเทศส่งผลให้เกิดการพัฒนาอย่างต่อเนื่อง ดังนั้นจึงเป็นการปรับปปรุง และป้องกันเหตุการณ์อันไม่พึงประสงค์ที่อาจจะเกิดขึ้นในอนาคตได้เป็นอย่างดี

สรุป

การดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาล ส่งผลให้การดำเนินงานตามพันธกิจขององค์กรเกิดความน่าเชื่อถือ เป็นการเพิ่มมูลค่าและสร้างความมั่นคงให้แก่ระบบสารสนเทศที่เกี่ยวข้อง ภายใต้การดำเนินโครงการส่งผลให้บุคลากรได้รับความรู้สามารถนำไปปรับใช้ในการทำงาน และชีวิตประจำวันได้โดยตรง ถึงแม้ว่าคณะแพทยศาสตร์ศิริราชพยาบาลจะได้รับการรับรองตามมาตรฐาน ISO/IEC27001: 2013 แต่สิ่งที่จะทำให้ประสบความสำเร็จอย่างยั่งยืน ทุกหน่วยงานรวมถึงบุคลากรที่เกี่ยวข้องจะต้องให้ความสำคัญ มีความตระหนักรู้ และสร้างกระบวนการในการปรับปรุงอย่างต่อเนื่องเพื่อให้เกิดการพัฒนาอย่างต่อเนื่อง ซึ่งการดำเนินโครงการดังกล่าวทำให้คณะแพทยศาสตร์ศิริราชพยาบาลมีมาตรฐานในการบริหารจัดการระบบความปลอดภัยข้อมูลเทียบเท่าระดับสากลที่ได้รับการยอมรับทั่วโลก ทำให้คณะแพทยศาสตร์ศิริราชเป็นที่ยอมรับ และเป็นการสร้างความเชื่อมั่นให้แก่ผู้ป่วยที่มารับบริการ อีกทั้งการดำเนินการต่าง ๆ ตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศยังเป็นการป้องกันความเสียหายที่อาจจะเกิดขึ้นโดยไม่คาดคิดอีกด้วย

ข้อเสนอแนะ

การดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) ของคณะแพทยศาสตร์ศิริราชพยาบาล ซึ่งการได้รับการรับรองตามมาตรฐานดังกล่าวเป็นตัวชี้วัดที่แสดงให้เห็นถึงความมุ่งมั่นและตั้งใจในการบริหารจัดการระบบสารสนเทศเพื่อให้ได้รับการยอมรับตามมาตรฐานสากล มีส่วนอย่างมากในการสนับสนุนให้คณะแพทยศาสตร์ศิริราชพยาบาลมีความมั่นคงปลอดภัยทั้งระบบสารสนเทศและข้อมูลต่าง ๆ ในการให้บริการผู้ป่วย ด้วยพันธกิจหลักของคณะแพทยศาสตร์ศิริราชพยาบาลได้แก่ การเรียนการสอน การวิจัย และการรักษาพยาบาล คณะแพทยศาสตร์ศิริราชพยาบาลเป็นองค์กรที่มีขนาดใหญ่ทำให้บุคลากรเจ้าหน้าที่ นักศึกษา และผู้ที่มาใช้บริการเป็นจำนวนมาก เพื่อความสะดวกในการให้บริการ ระบบสารสนเทศมีบทบาทที่สำคัญ และเป็นส่วนสำคัญที่จะช่วยให้คณะแพทยศาสตร์ศิริราชพยาบาลบรรลุพันธกิจ ดังนั้นการสร้างความตระหนักให้แก่บุคลากรที่ปฏิบัติ

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

หน้าที่เกี่ยวกับระบบสารสนเทศของคณะแพทยศาสตร์ศิริราชพยาบาลถือเป็นเรื่องที่สำคัญ และเป็นการป้องกันให้ระบบมีความมั่นคงปลอดภัย รวมถึงลดความเสี่ยงจากเหตุการณ์ไม่พึงประสงค์ที่อาจจะเกิดขึ้นได้ ดังนั้น ผู้บริหารคือหัวใจหลักที่สำคัญในการสนับสนุน และกระตุ้นให้บุคลากรในหน่วยงานมีความเข้าใจในนโยบาย ตลอดจนการนำไปปฏิบัติให้เกิดความเคยชินในการปฏิบัติงาน และมีความตระหนักในด้านความมั่นคงปลอดภัยสารสนเทศมากขึ้น

กิตติกรรมประกาศ

บทความทางวิชาการฉบับนี้สำเร็จสมบูรณ์ได้จากการสนับสนุนจากฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ที่ได้มอบหมายให้ปฏิบัติหน้าที่ในโครงการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ และในโอกาสนี้ผู้เขียนได้ใช้ความรู้ และประสบการณ์จริงที่ได้ปฏิบัติหน้าที่ในโครงการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001: 2013) เพื่อถ่ายทอดความรู้และประสบการณ์ผ่านบทความทางวิชาการ ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

เอกสารอ้างอิง

คณะแพทยศาสตร์ศิริราชพยาบาล. (2562). *รู้จักองค์กร*. สืบค้นเมื่อ 28 พฤศจิกายน 2562 จาก https://www.si.mahidol.ac.th/th/history.asp.

ฝ่ายสารสนเทศ คณะแพทยาสตร์ศิริราชพยาบาล. (2562). *การจัดระดับชั้นความลับ และการจัดการข้อมูลตามระดับชั้นความลับ (Information Classification and Handling Procedure)*. สืบค้นเมื่อ 3 ธันวาคม 2562 จาก http://172.20.9.238/Department/SIIT/qd/document_files/2562000004.pdf.

สำนักนายกรัฐมนตรี. (2544). *ระเบียบว่าด้วยการรักษาความลับของทางราชการ*. สืบค้นเมื่อ 3 ธันวาคม 2562 จาก http://www.gad.moi.go.th/nsk-17-04-62-2366-2367-2368.pdf.

ศิริพร ชำนาญชาติ. (2561). *ISO/IEC 27001: 2013 เบื้องหลังสู่ความเป็นเลิศด้วยนวัตกรรมของ DBD.* กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์, 46-49.

AL-Zahawi, O. S. (2019). *Information Security Handbook For ISO 27001 Controls*. Helsinki, Finland: UR academy.

Barrett, D., Weiss, M. M., & Hausman, K. (2015). *CompTIA Security+ SYO-401 Exam Cram: Comp Secu SY04 Auth ePub _4*. (4thed.). Indianapolis, IN: Pearson Education.

Calder, A. (2017). *Nine Steps to Success: An ISO 27001 Implementation Overview, North American edition*. (North American Edition). Cambridge shire, United Kingdom: IT Governance Publishing.

Honan, B. (2014). *ISO27001 in a Windows Environment: The best practice handbook for a Microsoft Windows environment*. (3th ed.). Dublin, Ireland: IT Governance Publishing.

International Organization for Standardization. (2019). *ISO Survey of certifications to management system standards*. Retrieved from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.

Received: December 11, 2019, Revised: June 8,2020 , Accepted: October 12 2020
http://doi.org/

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. *14th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). Coimbra: Portugal.

Matthews, M. L. (1999). *Knowledge-Driven Profit Improvement: Implementing Assessment Feedback Using PDKAction Theory.* Boca Raton, Florida: CRC Press.

Moh, C. (2019). An ISO 27001 compliance project for a cyber security service team. *Cyber Security: A Peer-Reviewed Journal*, 2(4), 346-359.

Srinivasan, M. L. (2016). *CISSP in 21 Days*. (2nd ed.). Birmingham, England: Packt Publishing.

The British Standards Institution. (2019). *BS EN ISO/IEC 27001:2017 – what has changed?*. Retrieved from https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/.

Velasco, J., Ullauri, R., & Pilicita, L. (2018). Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. *3rd International Conference on Information Systems and Computer Science* (pp. 294 - 300). Quito: Ecuador.

Watkins, S. (2013). *An Introduction to Information Security and ISO27001:2013: A Pocket Guide*. (2nd ed.). Cambridge shire, United Kingdom: IT Governance Publishing.