การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา
Resources on Information System Security Management for Educational Organizations

สฤษดิ์พงษ์ ลิมปิษเฐียร*
Saritpong Limpisathian*
มหาวิทยาลัยสุโขทัยธรรมาธิราช*
Sukhothai Thammathirat Open University*

(Received: *November 20, 2018*; Revised: *January 09, 2019*; Accepted: *January 09, 2019*)

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อเสนอแนะแนวทางการบริหารความมั่นคงปลอดภัย ด้านทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา ซึ่งในปัจจุบันพบว่า องค์การทางการศึกษามีการใช้งานทรัพยากรระบบสารสนเทศเพิ่มขึ้นเป็นจำนวนมาก อย่างไรก็ตาม บุคลากรในองค์การทางการศึกษาจำนวนมาก ก็ยังมีการใช้อุปกรณ์ด้านระบบสารสนเทศอย่างไม่ถูกวิธี ขาดความรู้ ความเข้าใจ หรืออาจขาดการฝึกอบรมด้านการบริหารทรัพยากรระบบสารสนเทศในระดับที่เหมาะสมหรือเพียงพอ และส่งผลทำให้เกิดปัญหาในการใช้งานทรัพยากรระบบสารสนเทศในองค์การทางการศึกษาจนเป็นเรื่องปกติ การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา เป็นสถานการณ์หรือคุณภาพของการบริหารที่เกี่ยวกับชีวิตและทรัพย์สินในองค์การทางการศึกษา ในด้านที่เกี่ยวข้องกับทรัพยากรระบบสารสนเทศ เพื่อให้รอดพ้นจากภัยอันตราย ภัยคุกคาม ความกลัว หรือความกังวล ทั้งที่เกิดขึ้นโดยบังเอิญ หรือโดยการตั้งใจทั้งจากภายในและภายนอกองค์การ

องค์การธุรกิจ รัฐวิสาหกิจ และราชการต่าง ๆ จะดำเนินการตามองค์การระหว่างประเทศว่าด้วยมาตรฐาน (International Organization for Standardization) ด้านการบริหารความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศ (ISO 27001) ซึ่งต้องมีการปฏิบัติตามข้อกำหนด (Compliance) โดยมาตรฐานนี้เป็นมาตรฐานสากล อย่างไรก็ตาม เพื่อความเหมาะสมกับองค์การซึ่งมีขนาด และความรู้ความสามารถของบุคลากรแตกต่างกัน ดังนั้น การปฏิบัติตามข้อกำหนดของ ISO 27001 จึงอาจแตกต่างกันในรายละเอียดต่อไป

คำสำคัญ: ความมั่นคงปลอดภัย, ทรัพยากรระบบสารสนเทศ, องค์การทางการศึกษา

*ผู้ให้การติดต่อ (Corresponding e-mail: saritpong.lim@stou.ac.th เบอร์โทรศัพท์ 02-5048539)

Abstract

This article aims to present the concept of security management in information system resources for the benefit of educational organizations. Educational organizations are increasingly using information resources. However, many educational organizations use inadequate information systems, lack of knowledge or training at a sufficient level. These problems cause in the use of information system resources in educational organizations. Information Security Management in Educational Organizations is a situation in relation to information system resources, so that it is free of danger, threat, fear or anxiety, either accidentally or intentionally, both from within and outside the organization.

Businesses, enterprises, and government agencies should operate in accordance with the International Organization for Standardization of Information Security Management Systems, which should be compliant with ISO 27001. However the size of organization, and knowledge or competency of personnel are vary, so the compliance with ISO 27001 may also vary in details for more appropriateness.

Keywords: Security, Information System Management, Educational Organization

บทนำ

การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศ ถือเป็นอีกประเด็นหนึ่งที่น่ากังวลสำหรับองค์การทางการศึกษาในยุคปัจจุบัน เนื่องจากทรัพยากรระบบสารสนเทศในองค์การทางการศึกษาทุกวันนี้ มีจำนวนการใช้งานเพิ่มมากขึ้นจากเดิมเป็นอย่างมาก การใช้อุปกรณ์ต่าง ๆ ด้านระบบสารสนเทศในองค์การทางการศึกษาจึงถือเป็นปกติที่สามารถพบเห็นได้ทั่วไป อย่างไรก็ตาม บุคลากรในองค์การทางการศึกษาจำนวนมาก ก็ยังคงมีการใช้ทรัพยากรระบบสารสนเทศที่ไม่ถูกวิธี ขาดความรู้ ความเข้าใจ หรืออาจขาดการฝึกอบรมด้านการบริหารทรัพยากรระบบสารสนเทศในระดับที่เหมาะสมและเพียงพอ จากการเก็บข้อมูลที่ได้จากการวิจัยกับนักศึกษาระดับบัณฑิตศึกษาในสถาบันอุดมศึกษาแห่งหนึ่ง พบว่า นักศึกษาเหล่านี้มากกว่าร้อยละ 90 เป็นผู้ปฏิบัติหน้าที่ด้านการเรียนการสอนอยู่ในองค์การทางการศึกษาขั้นพื้นฐานทั่วประเทศ โดยกว่าร้อยละ 90 ทำหน้าที่ผู้ใช้และดูแลทรัพยากรระบบสารสนเทศด้วยตัวเอง และมากกว่าครึ่งหนึ่ง ก็ไม่มีการตั้งรหัสผ่านเพื่อป้องกันทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา นอกจากนี้ ผู้ให้ข้อมูลเหล่านี้ยังกล่าวว่า ปัญหามัลแวร์ (Malware) (“Malware,” nd.) ในเครื่องคอมพิวเตอร์ของผู้ให้ข้อมูลเหล่านี้ถือเรื่องปกติ และสามารถพบเห็นได้เสมอ และส่วนใหญ่ก็เข้าใจว่า การใช้โปรแกรมป้องกันคอมพิวเตอร์ไวรัสซึ่งสามารถดาวน์โหลดได้ฟรีมาจากเว็บไซด์ก็เพียงพอต่อการป้องกันปัญหานี้ได้แล้ว (Limpisathian, 2015) นอกจากนี้ จากการพูดคุยกับนักศึกษาจำนวนมาก ยังพบว่า นักศึกษาส่วนใหญ่ยังไม่เข้าใจปัญหามัลแวร์ทั้งบนเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และแบบเคลื่อนที่ (Mobile Computer) ได้แก่ คอมพิวเตอร์ประเภทโน๊ตบุ๊ค (Notebook Computer) แท็บเล็ต (Tablet PC) และสมาร์ทโฟน (Smart Phone) ซึ่งปัญหาในลักษณะนี้ ก็มักส่งผลทำให้เกิดปัญหาด้านทรัพยากรระบบสารสนเทศในองค์การตามมาอีกหลายประการ (“การกำจัด Malware Ads ที่แฝงตัวอยู่กับ Internet Browser,” nd.) บทความนี้ จึงเป็นการเสนอแนะแนวทางให้กับผู้บริหารและบุคลากรตามความรู้และความสามารถในการบริหารด้านความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศต่อไป

ทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา หมายถึงทรัพยากรต่าง ๆ ในองค์การทางการศึกษาที่เกี่ยวข้องกับระบบสารสนเทศ ได้แก่ ข้อมูลและสารสนเทศ ฮาร์ดแวร์คอมพิวเตอร์ ซอฟต์แวร์คอมพิวเตอร์ เครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง ได้แก่ เครื่องคอมพิวเตอร์ เครื่องเซิร์ฟเวอร์ เครื่องสำรองไฟฟ้าที่ใช้

งานอยู่ในองค์การ รวมถึงบุคลากรต่าง ๆ ที่เกี่ยวข้องกับงานในด้านนี้ เช่น นักโปรแกรม นักพัฒนาระบบ ผู้บริหารศูนย์คอมพิวเตอร์ หรือศูนย์สารสนเทศ ซึ่งหมายถึงผู้ใช้ระบบสารสนเทศทั้งหมด นั่นเอง

ความมั่นคงปลอดภัย (Security) หมายถึง สถานการณ์หรือคุณภาพของการรอดพ้นจากภัยอันตราย ภัยคุกคาม ความกลัว หรือความกังวลใดๆ ในชีวิตและทรัพย์สิน รวมทั้งการป้องกันของภัยต่าง ๆ เหล่านี้ ทั้งที่เกิดขึ้นโดยการตั้งใจหรือโดยบังเอิญ (Wankrirojana, 2013; Limpisathian, 2015) ดังนั้น การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา จึงเป็นสถานการณ์หรือคุณภาพของการบริหารด้านต่าง ๆ เช่น การตัดสินใจ การวางแผน และการควบคุม กำกับ และติดตามการปฏิบัติงาน หรือความเป็นไปได้เกี่ยวกับชีวิตและทรัพย์สินในองค์การทางการศึกษาในด้านที่เกี่ยวข้องกับทรัพยากรระบบสารสนเทศให้รอดพ้นจากภัยอันตราย ภัยคุกคาม ความกลัว หรือความกังวล ทั้งที่เกิดขึ้นโดยบังเอิญหรือโดยการตั้งใจทั้งจากภายในและภายนอกองค์การ ดังนั้น บทความนี้จึงมีวัตถุประสงค์เพื่อเสนอแนะแนวทางการบริหารความมั่นคงปลอดภัยด้านทรัพยากรระบบสารสนเทศให้เหมาะสมกับองค์การทางการศึกษาต่าง ๆ เพื่อความยั่งยืนต่อไป

การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา

ในอดีตที่ผ่านมา การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษาส่วนใหญ่จะดำเนินการในลักษณะที่ขาดความแน่นอน และเป็นไปตามความรู้หรือความสามารถของผู้บริหารและบุคลากรในองค์การเป็นหลัก หรืออาจไม่มีการบริหารด้านนี้ในองค์การก็เป็นได้ ซึ่งเป็นผลทำให้เกิดความเสี่ยงต่อทรัพยากรระบบสารสนเทศในองค์การเป็นอย่างมาก จากการวิจัยในองค์การทางการศึกษาพบว่า ในปัจจุบันบุคลากรในองค์การกว่าร้อยละ 80 ทำหน้าที่จัดหาทรัพยากรระบบสารสนเทศมาใช้ด้วยตนเอง โดยขาดการศึกษาหรือการอบรมด้านการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศ หรือมีการฝึกอบรมในระดับน้อยมาก (Limpisathian, 2015) อย่างไรก็ตาม การศึกษาความรู้ด้านการบริหารความมั่นคงปลอดภัยทรัพยากรสารสนเทศในยุคปัจจุบันได้มีการพัฒนาไปมาก จนมีการกำหนดแนวคิดและแนวทางการปฏิบัติที่มีความชัดเจนแบ่งการทำงานออกเป็นขั้นเป็นตอน เพื่อให้เกิดความมั่นใจแก่องค์การในทุกภาคส่วนต่อไป โดยจะพบว่า องค์การธุรกิจ รัฐวิสาหกิจ และราชการต่าง ๆ จะดำเนินการตามองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization) ด้านการบริหารความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศ (ISO 27001) ซึ่งต้องมีการปฏิบัติตามข้อกำหนด (Compliance) โดยมาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นการรักษาความมั่นคงปลอดภัยให้กับทรัพยากรระบบสารสนเทศขององค์การ และยังนิยมใช้เป็นมาตรฐานเพื่อการอ้างอิงในการเสริมสร้างความมั่นคงปลอดภัยให้กับทรัพยากรระบบสารสนเทศขององค์การ โดยมาตรฐานนี้จะกล่าวถึงข้อกำหนดด้านต่าง ๆ ในการจัดทำระบบบริหารความมั่นคงปลอดภัยขององค์การทั่วโลก (ISO/IEC 27000-Series, n.d.)

อย่างไรก็ตาม เป็นที่ทราบกันโดยทั่วไปว่า องค์การทางการศึกษาไทยแต่ละแห่งจะมีความแตกต่างกันเป็นจำนวนมาก โดยเฉพาะในด้านขนาดขององค์การ ดังนั้น การบริหารความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศตามข้อกำหนดมาตรฐาน ISO 27001 ซึ่งต้องมีการปฏิบัติตามข้อกำหนดในองค์การทางการศึกษาที่มีขนาด และความรู้ความสามารถของบุคลากรแตกต่างกัน จึงไม่สามารถดำเนินการตามข้อกำหนดเดียวกันได้แม้จะใช้มาตรฐาน ISO 27001 เดียวกันก็ตาม ดังนั้น เพื่อให้องค์การทางการศึกษาแต่ละแห่งสามารถดำเนินการตามมาตรฐาน ISO 27001 ให้เหมาะสมกับขนาด การปฏิบัติงาน และจำนวนบุคลากรในองค์การทางการศึกษาที่มีขนาดต่างกัน องค์การทางการศึกษาจึงควรมีการแบ่งแนวทางการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การออกเป็น 2 กลุ่มตามขนาดขององค์การ คือ กลุ่มองค์การขนาดใหญ่ ซึ่งเป็นองค์การทางการศึกษาที่มีการทำงาน จำนวนบุคลากร รวมถึงจำนวนนักเรียน/นักศึกษาเป็นจำนวนมาก และกลุ่มองค์การขนาดกลาง และขนาดเล็ก ซึ่งมีการทำงาน จำนวนบุคลากร และนักเรียน/นักศึกษาพอประมาณหรือมีจำนวนไม่มากนัก ทั้งนี้ การกำหนดขนาดขององค์การทางการศึกษา ในกรณีที่เป็นสถานศึกษา และมหาวิทยาลัยจะนิยมใช้จำนวนนักเรียน/นักศึกษาเป็นหลัก ซึ่งเป็นการสะท้อนให้เห็นถึงจำนวนผู้ใช้ทรัพยากรระบบสารสนเทศในองค์การ

แต่หากเป็นองค์การทางการศึกษาอื่น ๆ เช่น สำนักงานในกระทรวงศึกษาธิการ สำนักงานศึกษาธิการระดับภาค หรือจังหวัด และสำนักเขตการศึกษา ขนาดขององค์การจะขึ้นอยู่กับระดับของหน่วยราชการ และจำนวนของบุคลากรในองค์การเป็นหลัก ซึ่งสะท้อนให้เห็นจำนวนทรัพยากรระบบสารสนเทศที่ใช้งานในองค์การ นั่นเอง

กลุ่มองค์การทางการศึกษาขนาดใหญ่ เป็นองค์การที่มีการใช้ทรัพยากรระบบสารสนเทศในปริมาณที่มาก มีความสลับซับซ้อนในองค์การมาก และมีจำนวนบุคลากรและผู้ใช้ทรัพยากรสารสนเทศมาก ยกตัวอย่าง เช่น องค์การขนาดใหญ่ มักมีการแบ่งหน่วยงานย่อยออกเป็นหลายฝ่าย การใช้ทรัพยากรระบบสารสนเทศจึงมีการแบ่งแยกไปตามหน่วยงานย่อยเหล่านี้ และมีบุคลากรและผู้ใช้ระบบสารสนเทศเป็นจำนวนมาก การบริหารความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศตามข้อกำหนดมาตรฐาน ISO 27001 ทุกประเด็นจึงควรต้องดำเนินการตามข้อกำหนดอย่างครบถ้วน เพื่อให้องค์การมั่นใจว่า การใช้ทรัพยากรระบบสารสนเทศในองค์การมีความถูกต้อง

ในขณะที่ กลุ่มองค์การทางการศึกษาขนาดกลาง และขนาดเล็ก ซึ่งมักมีปริมาณการใช้ทรัพยากรระบบสารสนเทศไม่มาก มีการปฏิบัติงานด้านระบบสารสนเทศที่มีไม่ความสลับซับซ้อน และมีจำนวนผู้ใช้ทรัพยากรจำกัด การบริหารความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศตามมาตรฐาน ISO 27001 เต็มรูปแบบจึงอาจไม่เหมาะสม และเป็นการสร้างภาระด้านการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศให้กับองค์การเกินความจำเป็น การบริหารความมั่นคงปลอดภัยเพื่อให้เหมาะสมกับองค์การศึกษาขนาดกลางและขนาดเล็ก จึงควรเลือกพิจารณาเน้นคุณสมบัติที่สำคัญ 3 ด้านของความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศ คือ การรักษาความลับ (Confidentiality) ความคงสภาพ (Integrity) และความพร้อมใช้ (Availability) ของทรัพยากรระบบสารสนเทศ ซึ่งสามารถเรียกรวมกันสั้น ๆ ว่า CIA Triad (Limpisathian, 2015 as cited in Information Security, n.d.) นั่นเอง

การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศตามมาตรฐาน ISO 27001 สำหรับองค์การขนาดใหญ่

วัตถุประสงค์ของมาตรฐาน ISO 27001 เป็นข้อกำหนดมาตรฐานการปฏิบัติเพื่อนำไปสู่ระบบบริหารความมั่นคงปลอดภัยเพื่อให้องค์การสามารถบริหารความมั่นคงปลอดภัยได้อย่างมีระบบ และเพียงพอเหมาะสมต่อการดำเนินการขององค์กร ดังนั้น ผู้บริหารองค์การจึงควรเน้นประเด็นในการปฏิบัติต่าง ๆ 16 ประเด็น (Limpisathian, & Passonsiri, 2014) คือ

1. การให้การสนับสนุนด้านการจัดการทรัพยากรระบบสารสนเทศ เป็นประเด็นที่เกี่ยวข้องกับการสนับสนุนงานด้านการจัดการระบบ การดูแลเอาใจใส่เกี่ยวกับการจัดงบประมาณ ด้านบุคลากร อุปกรณ์ เครื่องไม้เครื่องมือต่าง ๆ รวมถึงการป้องกันปัญหาความล้มเหลวของทรัพยากรระบบสารสนเทศในองค์การเหล่านี้

2. การพัฒนาโครงการการดูแลรักษาทรัพยากรระบบสารสนเทศ เป็นเรื่องที่เกี่ยวกับการพัฒนาโครงการเพื่อการดูแลรักษากิจกรรมเกี่ยวกับทรัพยากรระบบสารสนเทศในองค์การทางการศึกษาขนาดใหญ่ ซึ่งมีความสลับซับซ้อน มีความต่อเนื่องในการทำงานตลอดเวลา และใช้เวลาในการดูแลเป็นหลัก

3. การกำหนดขอบเขตของระบบ เนื่องจากเป็นองค์การทางการศึกษาขนาดใหญ่ หรือใหญ่พิเศษ องค์การจึงจำเป็นต้องดำเนินการในด้านทรัพยากรระบบสารสนเทศให้ครอบคลุมในทุกด้าน ทุกฝ่าย หรือทุกกิจกรรมในองค์การ การกำหนดขอบเขตของระบบจึงต้องเกี่ยวข้องกับโครงการด้านการจัดการองค์การ และความเสี่ยงอย่างแนบแน่น และต้องเป็นบทบาทหน้าที่โดยตรงของผู้บริหารองค์การเป็นหลัก

4. การพัฒนาเอกสารนโยบายการจัดการความมั่นคงปลอดภัยของระบบ นโยบายระบบการบริหารความมั่นคงปลอดภัยเป็นเรื่องที่มีความสำคัญ และจะต้องทำเป็นเอกสารที่แสดงให้เห็นรายละเอียดอย่างชัดเจนเข้าใจง่าย นโยบายเหล่านี้ควรประกอบไปด้วยพื้นฐานเกี่ยวกับความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศในองค์การ เพื่อช่วยให้ผู้บริหารเข้าใจเป้าหมาย และความสำเร็จของการมีและใช้ทรัพยากรระบบ

สารสนเทศในองค์การ รวมทั้งแนวทางในการควบคุมและการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การ

5. การกำหนดวิธีการประเมินความเสี่ยงของระบบ การประเมินความเสี่ยงด้านทรัพยากรระบบสารสนเทศเป็นงานที่มีความซับซ้อนและเกี่ยวข้องกับโครงการดูแลรักษาทรัพยากรระบบสารสนเทศในองค์การ โดยเป็นการพิจารณาถึงกฎด้านทรัพย์สิน ช่องว่าง การคุมคาม และผลกระทบที่เกี่ยวข้องด้านทรัพยากรระบบสารสนเทศในองค์การ รวมทั้งระดับความเสี่ยงที่สามารถเกิดขึ้นได้ในองค์การเพื่อแสวงหาแนวทางในการป้องกันต่อไป

6. การดำเนินการประเมินและดูแลรักษาระบบ เป็นการดำเนินการตามวิธีการประเมินความเสี่ยงของทรัพยากรระบบสารสนเทศตามที่กำหมนดไว้ รวมทั้งการดูแลรักษาระบบให้คงอยู่ต่อไป โดยการประเมินเหล่านี้ควรทำเป็นรายงานเพื่อเสนอต่อผู้บริหารต่อไป

7. การทำคำสั่งเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการ คำสั่งดังกล่าวควรทำเป็นเอกสารที่ชัดเจน หลีกเลี่ยงการสั่งด้วยวาจา หรือฝ่ายระบบสื่อสังคม (Social Media) ซึ่งสามารถค้นคืนได้ยากเมื่อเวลาผ่านไปนาน เพื่อให้ผู้ที่เกี่ยวข้องได้ทราบเป้าหมาย และความต้องการทรัพยากรระบบสารสนเทศและแอปพลิเคชันที่เกี่ยวข้องเพื่อการใช้ทำงานในองค์การ รวมทั้งการควบคุมแอปพลิเคชันที่มีอยู่หรือควรจะมีในอนาคตเพื่อให้เครื่องมือให้ผู้บริหารได้ตัดสินใจต่อไป

8. การจัดทำแผนการดูแลรักษาด้านความเสี่ยงของระบบ โดยทั่วไป บุคลากรในองค์การมักจะคิดว่าเราทำงานได้ เราแก้ไขปัญหาที่เกิดขึ้นได้ เพราะเราทราบเรื่องต่าง ๆ ที่เราเกี่ยวข้อง แต่ในความเป็นจริง อาจไม่เป็นเช่นนั้น แผนการดูแลรักษาด้านความเสี่ยงของระบบจึงเป็นเรื่องที่มีความสำคัญ แผนดังกล่าวนี้จึงต้องทำเป็นเอกสารตามเป้าหมายของการดูแลรักษาด้านความเสี่ยงของระบบ และกำหนดรูปแบบและแนวทางการควบคุมให้ชัดเจนเป็นขั้น ๆ เพื่อสามารถนำไปใช้ได้อย่างถูกต้อง

9. การกำหนดแนวทางเพื่อการวัดวิธีการควบคุมประสิทธิภาพของระบบ เมื่อมีการจัดทำแผน ก็จะต้องกำหนดแนวทางการประเมินแผนด้วยวิธีการประเมินที่ถูกต้องตามหลักการประเมินเพื่อให้สามารถควบคุมดูแลด้านความเสี่ยงต่าง ๆ ได้อย่างมีประสิทธิภาพ

10. การทำงานตามกระบวนการควบคุมและบังคับด้านความมั่นคงปลอดภัยของระบบ เป็นขั้นตอนที่จะต้องดำเนินการตามสิ่งที่กำหนดไว้ตามคำสั่ง แผน และแนวทางในการปฏิบัติ ดังนั้น เพียงการมีคำสั่ง แผน และแนวทางการปฏิบัติ แต่ไม่มีการทำจริง จึงเป็นเรื่องไร้ค่า องค์การจึงจะเป็นจะต้องมีการบังคับให้ผู้ที่เกี่ยวข้องลงมือปฏิบัติอย่างสม่ำเสมอจะเกิดเป็นนิสัย หากมีการเปลี่ยนแปลงใด ๆ ในทรัพยากรระบบสารสนเทศ องค์การก็จะต้องประเมิน แก้ไข และลงมือทำอย่างถูกต้องตามเอกสารใหม่อย่างเคร่งครัด

11. การฝึกอบรบและโปรแกรมความตระหนักด้านความมั่นคงปลอดภัย การฝึกอบรม และความตระหนักถือเป็นมาตรฐานสำคัญใน ISO 27001 หากต้องการกำหนดนโยบายหรือขั้นตอนด้านความมั่นคงปลอดภัยใหม่ในองค์การ ผู้บริหารจำเป็นจะต้องอธิบาย และฝึกอบรมให้ผู้ที่เกี่ยวข้องเข้าใจความสำคัญของความมั่นคงปลอดภัยในองค์การตามมาตรฐาน ISO 27001 เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อไป

12. การดำเนินการระบบการจัดการความมั่นคงปลอดภัยของระบบ การดำเนินการเกี่ยวกับความมั่นคงปลอดภัยถือเป็นส่วนหนึ่งชีวิตประจำวัน ดังนั้น ระบบการจัดการความมั่นคงปลอดภัยจึงเป็นเรื่องที่ผู้เกี่ยวข้องกับทรัพยากรระบบสารสนเทศจะต้องให้ความสนใจ โดยจะต้องมีการจดบันทึกสิ่งที่เกิดขึ้นเสมอ รวมทั้งจะต้องมีการตรวจสอบโดยผู้ที่ประเมินเพื่อให้มีการยืนยันว่า ทุกอย่างถูกต้อง ทั้งในเรื่องที่เกี่ยวกับบุคคลและอุปกรณ์

13. การควบคุมระบบการจัดการความมั่นคงปลอดภัยของระบบ การจัดการความมั่นคงปลอดภัยในองค์การเป็นประเด็นที่มีความสำคัญ วัตถุประสงค์ของการควบคุมระบบการจัดการความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศในองค์การคือการดูแลและวิธีการวัดการดำเนินการด้านความมั่นคงปลอดภัยของ

องค์การ หากพบความผิดปกติ ผู้ที่เกี่ยวข้องจะต้องรีบทำการแก้ไข และป้องกันไม่ให้ปัญหาด้านความมั่นคงปลอดภัยเกิดขึ้นอีกในองค์การ

14. การตรวจสอบภายในด้านความมั่นคงปลอดภัยของระบบ โดยทั่วไป การตรวจสอบภายในด้านความมั่นคงปลอดภัยในทรัพยากรระบบสารสนเทศในองค์การจะมีแนวคิดเช่นเดียวกับการประเมินการประกันในองค์การ อย่างไรก็ตาม บุคคลากรส่วนใหญ่มักไม่ตระหนักว่า ตัวเองได้ทำอะไรด้านความมั่นคงปลอดภัยไปบ้างและมีความผิดพลาดไปบ้างหรือไม่ ทั้งโดยตั้งใจหรือไม่ก็ตาม การตรวจสอบภายในด้านความมั่นคงปลอดภัยจึงเป็นเรื่องที่จำเป็น เพราะหากมีความผิดพลาดเกิดขึ้นในองค์การ ปัญหาใหญ่อาจตามมา เช่น ข้อมูลสำคัญในองค์การหายไป หรือโดนไวรัสเข้าทำลายจนไม่สามารถเรียกคืนกลับมาได้

15. การตรวจสอบเชิงบริหารจากผู้บริหาร บทบาทหน้าของผู้บริหารองค์การ เป็นเรื่องของการดูแลและตรวจสอบว่า มีปัญหาอะไรเกิดขึ้นบ้าง เช่นเดียวกัน ในทรัพยากรระบบสารสนเทศในองค์การ การตรวจสอบเชิงบริหารจากผู้บริหารก็เป็นเรื่องที่มีความจำเป็นเช่นเดียวกัน ผู้บริหารองค์การไม่จำเป็นจะต้องรู้ เข้าใจ หรือทำงานกับอุปกรณ์ด้านสารสนเทศ แต่ผู้บริหารองค์การจำเป็นจะต้องรู้ว่า หากเกิดปัญหาขึ้น เจ้าหน้าที่ผู้ใดจะเป็นผู้ที่จะต้องทำหน้าที่ดูแลรับผิดชอบ หรือแก้ไขปัญหาที่เกิดขึ้นนี้ ดังนั้น ผู้บริหารองค์การจึงจำเป็นจะต้องทำหน้าที่กำกับตรวจตราการทำงานของเจ้าหน้าที่ให้สามารถทำงานอยู่ได้อย่างเป็นปกติ

16. การแก้ไขและการป้องกันเกี่ยวกับความมั่นคงปลอดภัยของระบบ เป้าหมายของระบบการจัดการในองค์การ ก็คือการสร้างความมั่นใจว่าการทุกอย่างในองค์การดำเนินไปด้วยความถูกต้อง ระบบการจัดการมาตรฐาน ISO 27001 ในองค์การก็เป็นเช่นเดียวกัน คือควรมีการดูแล ควบคุมงานเกี่ยวกับระบบสารสนเทศอย่างถูกต้องและเป็นระบบ รวมทั้งจะต้องมีการปรับแก้และตรวจสอบงานความมั่นคงปลอดภัย ทรัพยากรระบบสารสนเทศในองค์การเป็นอย่างดี

ประเด็นทั้ง 16 ข้อเหล่านี้ จึงเป็นเรื่องสำคัญที่ผู้บริหารองค์การทางการศึกษาจะต้องตระหนัก และดำเนินการตามข้อกำหนดต่อไป ซึ่งองค์การขนาดใหญ่สามารถดำเนินการได้ไม่ยาก

การบริหารทรัพยากรระบบสารสนเทศตามมาตรฐาน CIA Triad สำหรับองค์การขนาดกลาง และขนาดเล็ก

ในองค์การขนาดกลาง และขนาดเล็ก ซึ่งมีการใช้ทรัพยากรระบบสารสนเทศใช้งานไม่มากนัก และไม่มีความสลับซับซ้อน ดังนั้น ความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศเพื่อให้เหมาะสมกับองค์การขนาดกลางและขนาดเล็ก จึงควรเลือกพิจารณาถึงคุณสมบัติ 3 ด้านของความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศ ซึ่งสามารถเรียกรวมกันสั้น ๆ ว่า CIA Triad ได้แก่

1. การรักษาความลับ (Confidentiality) เป็นเรื่องของการป้องกันไม่ให้ผู้ไม่มีสิทธิ์ได้มีโอกาสเข้าไปดำเนินการใด ๆ กับทรัพยากรระบบสารสนเทศในองค์การได้ ดังนั้น การรักษาความลับของทรัพยากรระบบสารสนเทศ จึงเป็นการอนุญาตและไม่อนุญาตให้ผู้ที่ได้รับสิทธิ์ในการเข้าถึง เปิดเผย และดำเนินการกับทรัพยากรระบบสารสนเทศเท่านั้น เนื่องจากสารสนเทศในทรัพยากรระบบสารสนเทศบางประการ มีความสำคัญและจำเป็นต้องเก็บไว้เป็นความลับ เช่น ข้อสอบ เกรดนักเรียน/นักศึกษาในเอกสารสำคัญ เป็นต้น หากถูกเปิดเผยออกไปโดยเจ้าของสารสนเทศไม่ทราบเรื่อง ก็อาจจะมีผลเสียหรือเป็นอันตรายต่อการทำงานในองค์การ เนื่องจากปัจจุบันบุคลากรในองค์การส่วนใหญ่ นิยมเก็บสารสนเทศไว้ในทรัพยากรระบบสารสนเทศ เช่น เครื่องคอมพิวเตอร์ขององค์การเอง หรือเครื่องส่วนบุคคล แต่เก็บสารสนเทศของโรงเรียนไว้ประกอบในการทำงาน

2. ความคงสภาพของทรัพยากร (Integrity) เป็นเรื่องที่เกี่ยวกับความถูกต้อง ความมั่นคง รวมถึงความสมบูรณ์ของสารสนเทศในระบบในองค์การ ดังนั้น ความคงสภาพของสารสนเทศในองค์การ จึงหมายความถึง ความถูกต้องของสารสนเทศในระบบ ได้แก่ ซอฟต์แวร์ ฮาร์ดแวร์ เครือข่าย และฐานข้อมูล ซึ่งจะต้องมีการกำหนดกฎเกณฑ์ของระบบทั้งระบบ เพื่อรักษาความถูกต้องของซอฟต์แวร์ ฮาร์ดแวร์ เครือข่าย และ

ฐานข้อมูล และความสัมพันธ์ระหว่างสารสนเทศต่าง ๆ และเป็นการป้องกันความเสียหายที่อาจเกิดกับฐานข้อมูลขององค์การ นั่นเอง

3. ความพร้อมใช้ (Availability) เป็นคุณสมบัติขององค์ประกอบด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ การรักษาคุณสมบัติด้านความพร้อมใช้งานของสารสนเทศ เป็นการทำให้บุคลากรในหน่วยงานที่ได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือทรัพยากรระบบสารสนเทศ สามารถเข้าถึงสารสนเทศเหล่านั้นได้เมื่อต้องการ ความพร้อมใช้งาน จึงเป็นส่วนหนึ่งของความน่าเชื่อถือ (Reliability) ของระบบ เนื่องจากการที่ระบบไม่พร้อมใช้งานในเวลา ย่อมจะมีค่าเท่ากับการไม่มีระบบใช้งานเลย

คุณสมบัติด้านความมั่นคงปลอดภัย ของทรัพยากรระบบสารสนเทศ 3 ประการ (CIA Triad) ถือเป็นมาตรฐานในการบริหารด้านความมั่นคงปลอดภัย ของทรัพยากรระบบสารสนเทศที่กระทัดรัด และเข้าใจง่าย เป็นแนวทางที่เหมาะสมกับการดำเนินงานในองค์การ ทางการศึกษาขนาดกลาง และขนาดเล็กที่ไม่สร้างความยุ่งยากในการดำนเนินการและการควบคุมของผู้บริหารในองค์การโดยยังคงไว้ซึ่งการ รักษาความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศตามมาตรฐานสากลต่อไป

สรุป

การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศ ในองค์การทางการศึกษา ถือเป็นเรื่องที่มีความสำคัญในการทำงานในยุคปัจจุบัน การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การธุรกิจ รัฐวิสาหกิจ และหน่วยงานราชการต่าง ๆ มีการดำเนินการตามองค์การระหว่างประเทศ ว่าด้วยการมาตรฐาน (International Organization for Standardization) ด้านการบริหารความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศ (ISO 27001) ซึ่งต้องมีการปฏิบัติตามข้อกำหนด (Compliance) โดยมาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นการรักษาความมั่นคงปลอดภัยให้กับทรัพยากรระบบสารสนเทศขององค์การ อย่างไรก็ตาม ในอดีตที่ผ่านมาการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษามีการศึกษาและให้ความสนใจน้อยมาก ปัญหาด้านความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษาเป็นเรื่องที่สามารถพบเห็นอยู่เสมอ ผู้บริหารและบุคลากรในองค์การส่วนใหญ่มักยังมีการใช้งานทรัพยากรระบบสารสนเทศไม่ถูกหลัก หรือขาดความสนใจในประเด็นต่าง ๆ เหล่านี้ เหตุผลประการหนึ่งที่ผู้บริหารและบุคลากรมักกล่าวคือ การขาดความรู้และบุคลากรที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา ด้วยเหตุนี้ ผู้เขียนจึงได้แบ่งกลุ่มการบริหารด้านนี้ออกเป็น 2 กลุ่ม เพื่อให้เหมาะสมกับการใช้ทรัพยากรระบบสารสนเทศ การทำงาน จำนวน และความสามารถของบุคลากรในองค์การทางการศึกษาต่อไปโดยยังคงไว้ซึ่งข้อกำหนดด้านความมั่นคงปลอดภัยของทรัพยากรระบบสารสนเทศในระบบสากลทั่วโลก คือมาตรฐาน ISO 27001 ต่อไป

ข้อเสนอแนะ

การบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศ ในองค์การทางการศึกษา ถือเป็นประเด็นหนึ่งที่น่าเป็นห่วงในยุคปัจจุบัน เนื่องจากการใช้งานทรัพยากรระบบสารสนเทศในองค์การทางการศึกษาทุกวันนี้มีจำนวนเพิ่มมากขึ้นจากอดีตเป็นอย่างมาก ดังนั้น เพื่อให้ทันต่อปัญหาด้านความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษาในอนาคต ดังนั้น ผู้เขียนขอเสนอแนะในด้านการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา โดยการเน้นบุคลากรไว้เป็น 2 กลุ่ม คือ

1. ผู้บริหาร ในฐานะผู้มีบทบาทสำคัญในด้านการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การ ควรจะต้องให้ความสำคัญกับประเด็นด้านความมั่นคงปลอดภัย ทรัพยากรระบบสารสนเทศในองค์การด้วยสนับสนุนให้บุคลากรทุกคนในองค์การให้ความสนใจเกี่ยวกับความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การ และจัดให้มีการฝึกอบรมด้านการบริหารความมั่นคงปลอดภัยทรัพยากร

ระบบสารสนเทศด้วยมาตรฐานในระบบสากลทั่วโลก คือมาตรฐาน ISO 27001 อย่างสม่ำเสมอ เพราะเท่ากับเป็นการช่วยป้องกันปัญหาที่อาจเกิดในองค์การต่อไป

2. กลุ่มบุคลากร ในฐานะผู้ใช้ทรัพยากรระบบสารสนเทศในองค์การทางการศึกษา จำเป็นจะต้องให้ความสนใจเกี่ยวกับการบริหารความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การ และควรถือเป็นเรื่องที่สำคัญสำหรับการปฏิบัติงานตามข้อกำหนดด้านความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การอย่างเคร่งครัด ไม่ว่าองค์การของเราจะมีขนาดเล็กหรือใหญ่เพียงใด เนื่องจากปัญหาด้านความมั่นคงปลอดภัยทรัพยากรระบบสารสนเทศในองค์การ แม้จะเกิดขึ้นเพียงครั้งเดียว หรือจากบุคลากรเพียงคนเดียวก็อาจส่งผลทำให้องค์การโดยส่วนรวมมีปัญหาที่แก้ไขได้ยากมาก

References

Information Security. (n.d.). In *Wikipedia*. Retrieved January 10, 2015, from https://en.wikipedia.org/wiki/ Information_security

ISO/IEC 27000-series. (n.d.). In *Wikipedia.* Retrieved September 28, 2017 from https://en.wikipedia.org/wiki/ISO/IEC_27000-series

Limpisathian, S. (2015). Information Security of STOU Graduate Diploma Students in Educational Administration. *Journal of Education in Thaksin University*, *15*(1), 152-167. (in Thai)

Limpisathian, S., & Passonsiri, N. (2014). *Information Systems for Educational Administration*. Nonthaburi: Textbook Promotion Project, Sukhothai Thammathirat Open University. (in Thai)

Malware. (nd.). In *Wikipedia.* Retrieved September 28, 2017 from https://en.wikipedia.org/wiki/Malware

Wankrirojana, S. (2013). *Technology for Information Management*. School of Liberal Arts. Nonthaburi: Sukhothai Thammathirat Open University Press Office. (in Thai)

การกำจัด Malware Ads ที่แฝงตัวอยู่กับ Internet Browser. (nd.). *In CAT Cyfence*. Retrieved September 30, 2018 from https://www.catcyfence.com/it-security/article/howto-remove-malware-ads-from-browser/ (in Thai)