สภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาของรัฐ[1]

แววตา เตชาทวีวรรณ[2]

received 07/06/2020 Revised 12/10/2020 Accepted 13/10/2020

บทคัดย่อ

ห้องสมุดมีหน้าที่จัดเก็บและให้บริการสารสนเทศซึ่งเปรียบเสมือนสินทรัพย์ที่สำคัญ ความมั่นคงปลอดภัยของสารสนเทศจึงเป็นภารกิจที่สำคัญของห้องสมุด การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตาม “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553” ของห้องสมุดสถาบันอุดมศึกษาของรัฐ โดยใช้วิธีวิจัยเชิงคุณภาพ เก็บรวบรวมข้อมูลด้วยแบบสัมภาษณ์จากผู้ให้ข้อมูลหลักที่เกี่ยวข้องกับระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษา จำนวน 11 คน โดยวิธีเลือกแบบเจาะจง ผลการวิจัยพบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศโดยมีการปฏิบัติตามแนวนโยบายและแนวปฏิบัติครบทั้ง 11 ข้อ โดยมีการรับรู้และวิธีปฏิบัติที่หลากหลาย ซึ่งขึ้นอยู่กับการจัดการและทรัพยากรทั้งด้านกำลังคนและงบประมาณ ส่วนปัญหาที่ประสบ ได้แก่ การใช้ซอฟต์แวร์โรบอติกส์และซอฟต์แวร์ไม่ถูกต้องลิขสิทธิ์ ระบบไฟฟ้าที่ไม่เสถียร ความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล และการขาดแคลนงบประมาณ ผลการวิจัยนี้จะถูกนำไปใช้ในการสร้างเครื่องมือวิจัยในการวิจัยระยะต่อไป

คำสำคัญ: ความมั่นคงปลอดภัยระบบสารสนเทศ; ห้องสมุดสถาบันอุดมศึกษา; ความปลอดภัยของข้อมูล; งานเทคโนโลยีห้องสมุด

---

[1]บทความส่วนหนึ่งของโครงการวิจัยเรื่อง การประเมินความต้องการจำเป็นในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาของรัฐ ได้รับทุนอุดหนุนการวิจัยจากเงินงบประมาณคณะมนุษยศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ปีงบประมาณ 2563

[2]รองศาสตราจารย์ โปรแกรมสารสนเทศศึกษา คณะมนุษยศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ อีเมล walta@g.swu.ac.th

The Condition and Problems of Information Systems Security of Public Universities' Libraries [1]

Wawta Techataweewan[2]

received 07/06/2020 Revised 12/10/2020 Accepted 13/10/2020

Abstract

The library is responsible for storing and providing information which is an important asset. Therefore, data security is a library mission. The purpose of this research was to study the condition and problems of information security systems according to "Government Information Security Policy and Practice Guidelines 2010" of academic libraries using qualitative research methods Data were collected using interview forms from 11 key informants related to the information systems of seven academic libraries selected by specific sampling method. The result of the research shows that the public university libraries focus on the security of information systems by following the 11 policies and guidelines that have a variety of perceptions and operations, depending on the management and resources, both manpower and Budget. The encountered problems of this mission are the use of robotics software and illegal software, unstable electrical systems, risk of violating personal information, and budget shortage. The results of this research will be used to create research tools for the next phase of research.

Abstract Information systems security, Academic library, data security, library technology

---

1An article in the research project "Need Assessments of Information Systems Security of Public Academic Universities" funded from the Faculty of Humanities, Srinakharinwirot University, fiscal year 2020

[2]Associate Professor, Information Studies Program, Faculty of Humanities, Srinakharinwirot University, E-mail: walta@g.swu.ac.th

บทนำ

ยุคสารสนเทศในปัจจุบันทำให้บุคคลคุ้นเคยกับเทคโนโลยีสารสนเทศและอินเทอร์เน็ต เพื่อการเข้าถึงสารสนเทศอย่างรวดเร็วและครอบคลุม บุคคลใช้สารสนเทศในการตัดสินใจทั้งด้านการศึกษา การทำงาน และชีวิตประจำวัน สารสนเทศมีความสำคัญต่อองค์กรเช่นกัน ซึ่งองค์กรต่าง ๆ ให้ความสำคัญต่อสารสนเทศ การดำเนินธุรกิจหรือธุรกรรมต่าง ๆ ขององค์กรล้วนขับเคลื่อนด้วยสารสนเทศ จนกล่าวได้ว่า สารสนเทศเป็นเสมือนสินทรัพย์ (Asset) ที่มีค่าอย่างหนึ่งขององค์กร โดยนำมาใช้ในการวางแผนดำเนินการธุรกิจและตอบสนองการเปลี่ยนแปลงสถานการณ์ต่าง ๆ ทั้งภายในและภายนอกองค์กร เช่น พฤติกรรมองค์กร เทคโนโลยี เศรษฐกิจ สังคม การเมือง เป็นต้น สารสนเทศจึงจำเป็นต้องได้รับการดูแลรักษาและจัดการอย่างเหมาะสม โดยการนำเทคโนโลยีสารสนเทศและอินเทอร์เน็ตเข้ามาจัดการ เพื่อให้สามารถจัดเก็บและค้นคืนได้อย่างมีประสิทธิภาพ ทำให้บุคคลและองค์กรดำรงอยู่อย่างมีคุณภาพและมีศักยภาพที่จะพัฒนาให้เจริญก้าวหน้าต่อไป

สารสนเทศเป็นทรัพย์สินที่มีค่าขององค์กร ระบบสารสนเทศขององค์กรจึงต้องได้รับการรักษาความปลอดภัยเพื่อไม่ให้เกิดการสูญเสียสารสนเทศหรือทำให้สารสนเทศนั้นด้อยประโยชน์ จากการสำรวจความเสียหายของระบบสารสนเทศของศูนย์รับเรื่องร้องเรียนอาชญากรรมทางอินเทอร์เน็ต ประเทศสหรัฐอเมริกา หรือที่เรียกอย่างย่อว่า IC3 (Internet Crime Compliant Center, 2015, p. 3) พบว่า ความเสียหายที่เกิดจากอาชญากรรมทางอินเทอร์เน็ตในขณะนั้นมีถึง 275,000,000 ดอลลาร์สหรัฐ ในประเทศไทยมีผลสำรวจของอาชญากรรมทางเศรษฐกิจของ PwC Thailand (2016) เรื่อง Global Economic Crime Survey: Economic crime in Thailand ประจำปี 2559 พบว่า ประเทศไทยมีอัตราการก่ออาชญากรรมทางไซเบอร์ (Cybercrime) อยู่ในอันดับสอง หรือร้อยละ 24 จากทั่วโลกมีอัตราการก่ออาชญากรรมที่ร้อยละ 32 โดยระบุว่าการจารกรรมข้อมูลส่วนบุคคล (Personal identity information) และข้อมูลที่เป็นทรัพย์สินทางปัญญา (Intellectual property) ถือเป็นอาชญากรรมทางคอมพิวเตอร์ที่สร้างผลกระทบร้ายแรงที่สุดขององค์กร เพราะนอกจากจะสูญเสียข้อมูลและทรัพย์สินแล้ว องค์กรยังสูญเสียด้านชื่อเสียงด้วย (Reputational damage) นอกจากนี้ยังพบข่าวอย่างต่อเนื่องเกี่ยวกับการโจรกรรมข้อมูลบนอินเทอร์เน็ต บางข่าวมีผลกระทบต่อบุคคลและองค์กรทั่วโลก เช่น ข่าวการรั่วไหลของข้อมูลผู้ใช้เฟซบุ๊ก ข้อมูลธนาคาร ข้อมูลส่วนบุคคลของหน่วยงานราชการ เป็นต้น

ระบบสารสนเทศขององค์กรมีสินทรัพย์ จำแนกเป็น 2 ประเภท คือ สินทรัพย์ทางกายภาพ (Physical asset) ได้แก่ ระบบคอมพิวเตอร์ อุปกรณ์ บุคลากร และเอกสารที่เกี่ยวข้อง และสินทรัพย์ทางตรรกะ (logical asset) ได้แก่ ซอฟต์แวร์และสารสนเทศ โดยสารสนเทศเป็นสินทรัพย์ที่สำคัญที่สุด การป้องกันและรักษาความปลอดภัยระบบสารสนเทศขององค์กรมีวัตถุประสงค์เพื่อรักษาความลับของสารสนเทศ (Confidentiality) ความถูกต้องครบถ้วนของสารสนเทศ (Integrity) และความสามารถทำงานได้ตามปกติ (Availability) (Talapphet, 2010, pp. 199-210: Phanitkul & Pongsakulchai, 2009, p. 7) จึงมีการกำหนดแนวทางป้องกันและรักษาความปลอดภัยของระบบสารสนเทศ หลายแนวทางถูกใช้เป็นมาตรฐานในการปฏิบัติ เช่น มาตรฐานโคบิต (CoBit) มาตรฐานสมุดสีส้ม (Orange book / TCSEC) มาตรฐาน ISO เป็นต้น มาตรฐานที่ได้รับการยอมรับและถูกนำมาใช้งานอย่างแพร่หลายทั้งองค์กรภาครัฐและภาคเอกชนทั่วโลก คือ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบ

สารสนเทศ ISO/IEC 27001 (International Organization for Standardization/International Electrotechnical Commission) กำหนดโดยองค์กรมาตรฐานสากล (International Organization for Standardization) ซึ่งเป็นมาตรฐานสากลที่เกี่ยวข้องโดยตรงกับการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบสารสนเทศมากที่สุด โดยมีรายละเอียดครอบคลุมตั้งแต่การกำหนดนโยบาย การดำเนินงานตามองค์ประกอบของระบบสารสนเทศ การควบคุมและจัดการความปลอดภัยของระบบ รวมทั้งเกณฑ์การประเมินที่ระบุลำดับการควบคุมตามมาตรฐาน (International Organization for Standardization, 2013) นอกจากนี้คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ ภายใต้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center, 2007, preface) กำหนดใช้มาตรฐาน ISO/IEC 207001 เป็นแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย ต่อมาได้กำหนดเป็น “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ” (“Announcement of the Electronic Transactions Commission...”, 2010, pp. 131-138; 2013, p. 8) โดยประกาศในราชกิจจานุเบกษาให้มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2553 เป็นต้นไป และต่อมามีประกาศฉบับที่ 2 ใน พ.ศ. 2556 ที่แก้ไขในบางมาตรา

ห้องสมุดมหาวิทยาลัยเป็นหน่วยงานการศึกษาระดับอุดมศึกษาที่ให้บริการสารสนเทศแก่นิสิตนักศึกษาและคณาจารย์ โดยมีวัตถุประสงค์ให้บริการทรัพยากรสารสนเทศครอบคลุมทุกสาขาวิชาตามหลักสูตรการเรียนการสอนของมหาวิทยาลัย อำนวยความสะดวกในการศึกษาค้นคว้าและวิจัย ส่งเสริมให้นิสิตนักศึกษาและคณาจารย์สามารถแสวงหาความรู้ได้ด้วยตนเอง และเป็นแหล่งเพิ่มพูนความรู้สำหรับนิสิตนักศึกษาในการประกอบอาชีพเมื่อจบการศึกษาไปแล้ว นอกจากนี้ยังเป็นหน่วยงานบริการวิชาการแก่ชุมชน และส่งเสริมการทำนุบำรุงศิลปวัฒนธรรม (Burapha University, 2007, p. 7) ห้องสมุดมหาวิทยาลัยจึงเป็นองค์กรที่เกี่ยวข้องกับสารสนเทศโดยตรง โดยเป็นแหล่งรวบรวมและจัดเก็บสารสนเทศสำหรับให้บริการแก่ผู้ใช้ นอกจากนี้ห้องสมุดมหาวิทยาลัยบางแห่งดำเนินการจัดเก็บและรวบรวมภูมิปัญญาท้องถิ่น เนื่องจากความก้าวหน้าของเทคโนโลยี ห้องสมุดมหาวิทยาลัยได้จัดทำระบบสารสนเทศเพื่อใช้งานผ่านระบบคอมพิวเตอร์และเครือข่าย ระบบสารสนเทศของห้องสมุดที่สำคัญ ได้แก่ ฐานข้อมูลบรรณานุกรมทรัพยากรสารสนเทศ ฐานข้อมูลทรัพยากรสารสนเทศอิเล็กทรอนิกส์/ดิจิทัล และฐานข้อมูลการบริหารห้องสมุด ซึ่งหากข้อมูลในระบบสารสนเทศของห้องสมุดถูกคุกคามหรือเสียหาย ย่อมส่งผลต่อการดำเนินงานและการบริการสารสนเทศแก่นิสิตนักศึกษาและคณาจารย์ รวมทั้งอาจส่งผลต่อการบริการวิชาการแก่ชุมชนและการรักษาองค์ความรู้ที่เป็นภูมิปัญญาของท้องถิ่นด้วย

ห้องสมุดสถาบันอุดมศึกษาในประเทศไทยจัดว่าเป็นห้องสมุดที่มีความพร้อมด้านเทคโนโลยีสารสนเทศ ปัจจุบันห้องสมุดสถาบันอุดมศึกษาทุกแห่งมีการใช้ระบบคอมพิวเตอร์ในการจัดเก็บและให้บริการสารสนเทศทั้งที่เป็นข้อมูลทางบรรณานุกรมและเอกสารฉบับเต็ม บางห้องสมุดทำหน้าที่จัดเก็บสารสนเทศที่เป็นภูมิปัญญาท้องถิ่น ซึ่งจัดทำเป็นระบบสารสนเทศและให้บริการบนเครือข่ายอินเทอร์เน็ต นอกจากนี้จากการสำรวจงานวิจัยที่เกี่ยวข้องไม่พบงานวิจัยเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศห้องสมุดต่าง ๆ ในประเทศไทย แต่พบงานวิจัยในประเทศมาเลเซีย คือ งานวิจัยของอิสเมลและไซแน็บ (Ismail & Zainab, 2011) ศึกษาระบบสารสนเทศ

ของห้องสมุดในประเทศมาเลเซีย ซึ่งพบว่า ห้องสมุดส่วนใหญ่มีการดำเนินงานรักษาความปลอดภัยของระบบสารสนเทศในด้านเทคนิคอยู่ในระดับดี แต่มีการดำเนินงานในด้านบริหารองค์กรอยู่ในระดับต่ำ เนื่องจากขาดแคลนระเบียบปฏิบัติด้านความปลอดภัย (Security procedure) เครื่องมือที่ใช้ในการบริหารจัดการความปลอดภัย (Administrative tools) และกิจกรรมที่เสริมสร้างความตระหนักรู้เกี่ยวกับการรักษาความปลอดภัย ดังนั้นผู้วิจัยจึงสนใจที่จะศึกษามาตรการการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาในประเทศไทย เพื่อประเมินความต้องการจำเป็นในการปฏิบัติตามแนวทางประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (“Announcement of the Electronic Transactions Commission...”, 2010, pp. 131-138) ผลการวิจัยนี้จะทำให้ทราบสภาพและปัญหาด้านนโยบายและการปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาที่แสดงลำดับความจำเป็นหรือสำคัญในการปรับปรุงแก้ไข รวมทั้งสามารถนำมาพัฒนาเป็นแนวทางปฏิบัติเพื่อธำรงระบบสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น ตลอดจนใช้เป็นแนวทางสำหรับห้องสมุดประเภทอื่นในประเทศไทยให้สามารถรักษาความมั่นคงปลอดภัยของระบบสารสนเทศได้ตามมาตรฐานของภาครัฐ

วัตถุประสงค์ของการวิจัย

เพื่อศึกษาสภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตาม “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553” ของห้องสมุดสถาบันอุดมศึกษาของรัฐ

วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นการวิจัยระยะที่ 1 ของโครงการวิจัย ซึ่งใช้วิธีวิจัยเชิงคุณภาพแบบวิธีศึกษาเฉพาะกรณีแบบมุ่งการค้นหา (Case study approach: Exploratory) (Phosita, 2011, pp. 151-157; Savin-Baden & Major, 2013, pp. 154-155) เพื่อศึกษาทำความเข้าใจเกี่ยวกับนโยบาย การปฏิบัติ และปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยดำเนินการตามขั้นตอน ดังนี้

1. การกำหนดกลุ่มผู้ให้ข้อมูลหลัก (Key informants) กลุ่มผู้ให้ข้อมูลหลักสำหรับวิธีวิจัยเชิงคุณภาพ ได้แก่ ผู้อำนวยการ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ และผู้ปฏิบัติงานที่เกี่ยวข้องของห้องสมุดสถาบันอุดมศึกษาของรัฐ จำนวน 7 แห่ง ซึ่งเป็นห้องสมุดของมหาวิทยาลัยในกำกับของรัฐ 3 แห่ง (จุฬาลงกรณ์มหาวิทยาลัย มหาวิทยาลัยธรรมศาสตร์ มหาวิทยาลัยสวนดุสิต) ห้องสมุดมหาวิทยาลัยเทคโนโลยีราชมงคล 2 แห่ง (มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ) และห้องสมุดมหาวิทยาลัยราชภัฏ 2 แห่ง (มหาวิทยาลัยราชภัฏสวนสุนันทา และมหาวิทยาลัยราชภัฏบ้านสมเด็จ) รวมจำนวนทั้งสิ้น 11 คน โดยวิธีเลือกแบบเจาะจง

2. การสร้างเครื่องมือที่ใช้ในการวิจัย เครื่องมือที่ใช้ในการวิจัยครั้งนี้ คือ แบบสัมภาษณ์กึ่งโครงสร้าง โดยการศึกษาวรรณกรรมและงานวิจัยที่เกี่ยวข้อง นำมาสร้างข้อคำถามเกี่ยวกับสภาพ ปัญหาและแนวโน้มการ

ดำเนินงานตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ("Announcement of the Electronic Transactions Commission ..., 2010", pp.131-138) ซึ่งมีประเด็นหลัก 11 ข้อ ได้แก่

2.1 นโยบายในการรักษาความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร

2.2. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.3 การกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access control)

2.4 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

2.5 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

2.6 การควบคุมการเข้าถึงเครือข่าย (Network access control)

2.7 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

2.8 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control)

2.9 การจัดทำระบบสำรอง

2.10 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.11 การกำหนดความรับผิดชอบที่ชัดเจนแก่บุคลากรที่เกี่ยวข้อง

3. การเก็บและรวบรวมข้อมูลโดยการสัมภาษณ์ ผู้วิจัยทาบทามและนัดหมายผู้เชี่ยวชาญเพื่อสัมภาษณ์ทางอีเมลและโทรศัพท์ โดยมีหนังสือเชิญเป็นผู้เชี่ยวชาญและขอความอนุเคราะห์ข้อมูลวิจัย ซึ่งออกโดยคณบดีคณะมนุษยศาสตร์ ผู้วิจัยชี้แจงเกี่ยวกับวัตถุประสงค์ของการวิจัย สาเหตุที่ได้รับเชิญเข้าร่วมการวิจัย และเงื่อนไขการให้สัมภาษณ์ ซึ่งผู้เชี่ยวชาญทุกคนรับทราบและยินดีเข้าร่วมการวิจัย การสัมภาษณ์เริ่มตั้งแต่เดือนกุมภาพันธ์ ถึงเดือนเมษายน 2563 เป็นการสัมภาษณ์แบบเผชิญหน้า (Face-to-face interview) และการสัมภาษณ์ทางโทรศัพท์ ใช้เวลารายละประมาณ 1 ชั่วโมง เมื่อการสัมภาษณ์เสร็จสิ้นแต่ละครั้ง ผู้วิจัยสรุปและวิเคราะห์ข้อมูลเพื่อประเมินข้อมูลที่ได้รับว่าสมบูรณ์เพียงพอหรือไม่ หากไม่สมบูรณ์หรือไม่ชัดเจน ก็จะขอสัมภาษณ์เพิ่มเติม และปรับข้อคำถามให้เหมาะสมเพื่อให้ได้ข้อมูลครบถ้วนสมบูรณ์มากที่สุด

4. การจัดกระทำและวิเคราะห์ข้อมูล ผู้วิจัยวิเคราะห์ข้อมูลโดยวิธีวิเคราะห์เนื้อหา (Content analysis) เพื่อให้ได้ข้อมูลตามวัตถุประสงค์ของการวิจัย นำเสนอข้อมูลในรูปแบบการสังเคราะห์สรุปความพร้อมคำสัมภาษณ์ในแต่ละประเด็น และนำไปใช้ในการออกแบบแบบสอบถามสำหรับการวิจัยในระยะที่ 2 ต่อไป

ผลการวิจัย

สภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตาม “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553” ของห้องสมุดสถาบันอุดมศึกษาของรัฐ

ผลการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง และสัมภาษณ์ผู้ให้ข้อมูลหลัก จำนวน 11 คน เพื่อศึกษาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตาม “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553” ของห้องสมุดสถาบันอุดมศึกษา พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศโดยมีการปฏิบัติครบ 11 ข้อ โดยมีการรับรู้และวิธีปฏิบัติที่หลากหลาย ซึ่งขึ้นอยู่กับการจัดการและทรัพยากรทั้งด้านกำลังคนและงบประมาณ ดังนี้

1. นโยบายในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดอย่างเป็นลายลักษณ์อักษร พบว่า นโยบายรักษาความมั่นคงระบบสารสนเทศถูกกำหนดอย่างเป็นลายลักษณ์อักษรโดยห้องสมุดหรือสำนักคอมพิวเตอร์ของมหาวิทยาลัยเพื่อให้บุคลากรทุกคนปฏิบัติตาม ซึ่งนโยบายที่เป็นลายลักษณ์อักษรดังกล่าวมีเพียงบางห้องสมุดเท่านั้น การรับรู้ของบุคลากรเกี่ยวกับนโยบายดังกล่าวขึ้นกับกฎระเบียบและความเข้มงวดของแต่ละห้องสมุด ห้องสมุดที่กำหนดนโยบายเองเนื่องจากเป็นหน่วยงานรับผิดชอบเทคโนโลยีสารสนเทศของมหาวิทยาลัยด้วย ได้แก่ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สังกัดมหาวิทยาลัยราชภัฏและมหาวิทยาลัยเทคโนโลยีราชมงคล ส่วนห้องสมุดที่ไม่ได้กำหนดเองแต่ต้องรับนโยบายนี้จากหน่วยงานที่รับผิดชอบของมหาวิทยาลัย เช่น สำนักคอมพิวเตอร์ สำนักเทคโนโลยีสารสนเทศ เป็นต้น แต่การรับรู้เกี่ยวกับนโยบายดังกล่าวของบุคลากรห้องสมุดขึ้นกับกฎระเบียบและความเข้มงวดของแต่ละมหาวิทยาลัย บางมหาวิทยาลัยที่ไม่เข้มงวดทำให้ผู้บริหารและผู้ปฏิบัติงานเทคโนโลยีสารสนเทศห้องสมุดไม่เคยรับรู้หรือพบเห็นนโยบายที่เป็นลายลักษณ์อักษร บางมหาวิทยาลัยประกาศเป็นข้อกำหนดให้บุคลากรที่เข้ามาทำงานใหม่ทุกคนเซ็นสัญญารับทราบเกี่ยวกับนโยบายดังกล่าว รวมทั้งการจัดปฐมนิเทศหรือฝึกอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยแก่บุคลากรของมหาวิทยาลัย ดังคำสัมภาษณ์

“มีนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ปี 2560 อธิการบดีลงนามและประกาศส่งไปตามหัวหน้าหน่วยงานเพื่อแจ้งบุคลากรในหน่วยงานอีกที... มหาวิทยาลัยทำนโยบายการรักษาความมั่นคงปลอดภัยแล้วส่งให้สำนักงานคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ตรวจสอบ เมื่อผ่านก็นำมาประกาศ... บุคลากรที่เข้ามาใหม่ต้องเซ็นรับทราบประกาศนี้ทุกคน”

“ทำงานมาหลายสิบปีแล้ว แต่ไม่เคยเห็นหรือรับรู้ว่ามีนโยบายเรื่องนี้อย่างเป็นลายลักษณ์อักษร ไม่มีนโยบายที่เป็นลายลักษณ์อักษร ไม่เคยเห็นนะ”

2. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ นอกเหนือจากข้อปฏิบัติตามประกาศของมหาวิทยาลัย เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยห้องสมุดนำนโยบาย กฎหมาย และพระราชบัญญัติต่าง ๆ ที่เกี่ยวข้องมากำหนดเป็นประกาศและข้อปฏิบัติสำหรับบุคลากรและผู้ใช้ห้องสมุด เช่น การติดตั้งซอฟต์แวร์โดยไม่ได้รับอนุญาต การใช้งานฐานข้อมูลออนไลน์ที่ผิดปกติที่กระทบต่อข้อ

สัญญาการเป็นสมาชิกฐานข้อมูลออนไลน์ เช่น การใช้โปรแกรม Robotic ดาวน์โหลดข้อมูลจำนวนมาก เป็นต้น การแจ้งเตือนเกี่ยวกับไวรัสคอมพิวเตอร์ การดาวน์โหลดข้อมูลจำนวนมากซึ่งกระทบต่อการใช้งานเครือข่ายส่วนรวม เช่น Bit Torrent เกมออนไลน์ เป็นต้น ดังคำสัมภาษณ์

“มีการแจ้งเตือนเกี่ยวกับไวรัส ถึงแม้เครื่องคอมฯ ที่ให้นักศึกษาใช้ติดตั้ง recovery แต่แต่ละวันมีคนใช้เครื่องนั้นซ้ำ ใช้ flash drive ซึ่งไม่มีการ boot เครื่องใหม่ ทำให้ติดไวรัส นักศึกษามาร้องเรียนว่าข้อมูลหายติดไวรัสบ้าง ต้องประกาศแจ้งเป็นกฎระเบียบให้ปฏิบัติ”

“กำลังจะมีระเบียบกับคนทำงานเรื่องการลงซอฟต์แวร์โดยไม่ได้รับอนุญาต โดยเรา Lock account ไม่ให้ติดตั้งได้เอง มีการคุยกันในที่ประชุมแต่ยังไม่ประกาศ.. ส่วนนักศึกษาอาจารย์เราห้ามใช้ Robot download ประกาศบนเว็บห้องสมุด”

“มีประกาศคณะกรรมการดำเนินงานห้องสมุด ว่าห้องสุมดจะใช้โปรแกรมลิขสิทธิ์เท่านั้น เช่น Adobe ทั้ง set สำหรับคนที่ทำงาน PR (ประชาสัมพันธ์) ทำสื่อมีเดียต่าง ๆ ก็ต้องใช้โปรแกรมที่มี license รวมทั้งโปรแกรม antivirus”

“มีมาตรการ set (ติดตั้ง) firewall ห้ามเล่นเกมออนไลน์ โหลดบิท (BitTorrent) เราบล็อกไว้ นักศึกษาที่โหลดจะทำเป็นช่วงเวลาต่อเนื่องจนครบ ทำให้ traffic เน็ตใช้มากผิดปกติ ซึ่งกระทบการใช้งานของคนอื่นด้วย”

3. การกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access control) พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐมีการกำหนดสิทธิและระดับของบุคคลทั้งทางกายภาพและทางอิเล็กทรอนิกส์ ในทางกายภาพเป็นการป้องกันการเข้าถึงอุปกรณ์ ฮาร์ดแวร์ และเครื่องคอมพิวเตอร์แม่ข่ายต่าง ๆ ภายในห้องควบคุมระบบโดยจำกัดการเข้าถึงจากผู้ที่ไม่เกี่ยวข้องและอนุญาตเฉพาะผู้ปฏิบัติงานที่เกี่ยวข้องเท่านั้น ซึ่งเข้าถึงด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น การ์ด RFID ปุ่มกดรหัส การสแกนลายนิ้วมือ เป็นต้น รวมทั้งการจัดห้องควบคุมอยู่ในสถานที่ที่เข้าถึงยาก ไม่ตั้งอยู่ในสถานที่ส่วนกลางที่ผู้คนเดินผ่านไปมาหรือเข้าถึงได้ง่าย ส่วนทางอิเล็กทรอนิกส์เป็นการเข้าถึงระบบสารสนเทศผ่านระบบเครือข่าย โดยกำหนดสิทธิการเข้าถึงตามหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานของ แต่ละระบบสารสนเทศ ซึ่งส่วนใหญ่แยกเป็น 3 กลุ่ม คือ ผู้ใช้ (User) ผู้ควบคุม (Supervisor) และผู้จัดการ (Administrator) ซึ่งห้องสมุดส่วนใหญ่มีผู้จัดการระบบของแต่ละงานหรือหน่วยงานเป็นผู้กำหนดบัญชีผู้ใช้และสิทธิในการเข้าใช้งานระบบตามภาระหน้าที่ ดังคำสัมภาษณ์

“ห้อง Server เข้าได้เฉพาะ staff ที่ปฏิบัติงาน คนเข้ามาทำงานใหม่ในฝ่ายเทคโนฯ ต้องผ่านการประเมินแล้วจึงจะเข้าได้”

“การเข้าไปในห้องควบคุมและเซิฟเวอร์ต้องมีบัตรสแกนแถบแม่เหล็กหรือ RFID เฉพาะผู้ที่เกี่ยวข้องเท่านั้น คือ เฉพาะ system admin ถ้าห้องสำนักงานจะใช้การสแกนนิ้วมือ ผู้ที่มีบัตรหรือสแกนนิ้วมือเท่านั้นมีสิทธิเข้าห้องทำงานตามสิทธิของตัวเอง”

“มีการแยกสิทธิ User/Supervisor/Admin ซึ่ง admin กับ supervisor แยกสิทธิกัน admin ดูแลระบบที่ตนรับผิดชอบ ส่วน supervisor ดูแล Server ข้อมูลในฐานข้อมูลไม่ยุ่งเกี่ยวกับระบบสารสนเทศ”

“งานไอทีดูแลโครงสร้างพื้นฐานเท่านั้น ไม่มีสิทธิเข้าใช้งานในระบบสารสนเทศของแต่ละงาน เพราะเป็นงานของเขาเราไม่ยุ่งเกี่ยว แต่ละงานแต่ละระบบจะมี username/password มี admin ของเขาเอง”

4. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) พบว่า ห้องสมุดสถาบันอุดมศึกษากำหนดให้บุคลากรและผู้ใช้ห้องสมุดสามารถเข้าถึงระบบสารสนเทศได้ตลอดเวลา แต่มีการตัดการเชื่อมต่อหรือการล๊อกอินหากไม่มีการเคลื่อนไหวของหน้าจอคอมพิวเตอร์ หรือหยุดใช้งานนานตามระยะเวลาที่กำหนด เช่น 15 นาที 20 นาที ครึ่งชั่วโมง เป็นต้น รวมทั้งจำนวนเครื่องหรืออุปกรณ์คอมพิวเตอร์ที่ล๊อกอินใช้งานระบบสารสนเทศพร้อมกัน ซึ่งการใช้งานอินเทอร์เน็ตของมหาวิทยาลัยมีการกำหนดบัญชีผู้ใช้ประจำแต่ละบุคคล และส่วนใหญ่แต่ละบัญชีผู้ใช้สามารถใช้งานอุปกรณ์คอมพิวเตอร์ได้พร้อมกันเพียง 2 เครื่อง เชื่อมต่อได้นานต่อเนื่องสูงสุด 8 ชั่วโมง แต่หากไม่มีการเคลื่อนไหวของหน้าจอหรือใช้งานนานเกินระยะเวลาที่กำหนดก็จะตัดการเชื่อมต่ออินเทอร์เน็ตนั้น ดังคำสัมภาษณ์

“ระบบ... (ห้องสมุดอัตโนมัติ) จะกำหนดการเข้าใช้งาน account ใคร account มัน เข้าใช้งานแล้วต้องทำงานต่อเนื่อง หากหยุดไปทำธุระอย่างอื่นนานเกิน 15 นาที ระบบ...ก็จะตัดออก ต้อง login เข้ามาใหม่ ซึ่งดีเพราะเราลุกไปไหนใครอาจมาใช้งาน account เราได้”

“การใช้งานอินเทอร์เน็ตและสืบค้นฐานข้อมูลออนไลน์ต้องผ่าน authen (authentication) ของมหาวิทยาลัย สำหรับบุคคลภายนอก แต่ละห้องสมุดจะมีเครื่องคอมสำหรับบุคคลภายนอกใช้ได้โดยไม่ต้องผ่าน authen”

“มีการให้ username และ password บุคลากรใหม่และนักศึกษาที่เข้ามาใหม่ทุกคน สำหรับการใช้งานอินเทอร์เน็ต กรณีบุคลากรลาออกหรือเกษียณ กองบริหารงานบุคคลจะเป็นคนตัด user ออกจากระบบเอง disable account ไปทำให้ไม่สามารถใช้งานได้อีก”

5. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐจัดทำการพรรณนางาน (Job description) กำหนดหน้าที่ความรับผิดชอบของบุคลากรแต่ละตำแหน่งอย่างชัดเจนโดยเฉพาะผู้ที่มีตำแหน่งด้านระบบคอมพิวเตอร์หรือเทคโนโลยีห้องสมุด แต่ตำแหน่งบรรณารักษ์และตำแหน่งอื่น ๆ ไม่มีรายละเอียดเกี่ยวกับการปฏิบัติงานด้านเทคโนโลยีห้องสมุด ทั้งนี้ผู้ใช้แต่ละคนต้องรับผิดชอบบัญชีผู้ใช้ของตนเองในการปฏิบัติงานตามหน้าที่ความรับผิดชอบ โดยแต่ละระบบสารสนเทศสามารถตรวจสอบการใช้งานของผู้ใช้แต่ละคนได้จากข้อมูลบันทึกการใช้งานคอมพิวเตอร์ (Log file) ของระบบในกรณีที่มีเหตุการณ์ผิดปกติ ดังคำสัมภาษณ์

“ห้องสมุดมีการจัดทำเป็น job description, job assignment สำหรับทุกคนทุกตำแหน่งงาน หากเป็นงานบรรณารักษ์ไม่มีกล่าวถึงงานคอมพิวเตอร์หรืองานระบบนะ เพราะแต่เดิมไม่เกี่ยวข้อง มุ่งงานเทคนิคงานบริการอะไรพวกนี้มากกว่า”

“ห้องสมุดมีระบุชัดเจนว่าใครเป็น admin ระบบ ดูแลเซิฟเวอร์ ระบบเครือข่าย ซึ่งใน job description ของพวกเทคโนฯ จะบอกว่าใครทำอะไรบ้าง เรามีตามมาตรฐาน ISO9001 version 2015 และในแต่ละระบบฐานข้อมูลมีการกำหนดสิทธิอยู่แล้วว่าใครเข้าถึง level ไหนได้บ้าง”

“ทุกคนต้องใช้ username/password ของตนเองในการทำงาน ต้องระวังไม่ให้ใครใช้ หากมีอะไรเกิดขึ้นหรือผิดพลาดก็สามารถตรวจสอบได้จาก log file ของระบบว่าใครทำอะไรไปบ้าง”

6. การควบคุมการเข้าถึงเครือข่าย (Network access control) พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐควบคุมการเข้าถึงระบบเครือข่ายสำหรับการใช้งานระบบสารสนเทศทั้งเครือข่ายภายในมหาวิทยาลัย (Local area network) และอินเทอร์เน็ต แบบใช้สายสัญญาณเครือข่ายและแบบไร้สาย โดยมีการป้องกันการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาตด้วยใช้วิธียืนยันตัวตนของผู้ใช้ (User authentication) ในการใช้งานระบบสารสนเทศต่าง ๆ ของห้องสมุดและอินเทอร์เน็ต หากเป็นการใช้ระบบสารสนเทศจากภายนอกมหาวิทยาลัย เช่น การสืบค้นฐานข้อมูลออนไลน์ที่ห้องสมุดบอกรับ ฐานข้อมูลห้องสมุดดิจิทัล เป็นต้น ต้องใช้งานผ่านระบบเครือข่ายส่วนตัวเสมือน (VPN: Virtual Private Network) ที่ห้องสมุดติดตั้งโดยฮาร์ดแวร์หรือซอฟต์แวร์ นอกจากนี้มีการจำกัดจำนวนอุปกรณ์และระยะเวลาที่ใช้เครือข่ายสำหรับบัญชีผู้ใช้งานแต่ละคน ดังคำสัมภาษณ์

“ใช้ net authentication ของสำนักไอทีมหาวิทยาลัย ผู้ใช้สามารถใช้ VPN ของมหาวิทยาลัย แต่ห้องสมุดใช้ (ซื่อซอฟต์แวร์) เป็น VPN หากใช้อินเทอร์เน็ตของมหาวิทยาลัย ต้องผ่าน authen (authentication) สามารถใช้งานได้ต่อเนื่อง แต่ตั้งเวลาไว้ 45 นาทีหากทิ้งเครื่องนานกว่านี้จะตัดออก”

“การใช้งานจากภายนอกใช้ VPN ส่วนใช้เครือข่ายหรือ Wifi ในมหาวิทยาลัย ใช้ authen ให้ใช้งานได้ 5 เครื่องพร้อมกัน”

7. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐมีการป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยให้บุคลากรกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์ที่ตนใช้ปฏิบัติงาน ซึ่งบัญชีผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ที่ห้องสมุดกำหนด มี 2 ระดับ คือ ผู้ดูแล (Administrator) และผู้ใช้งานปกติ (Standard user) หากเป็นเครื่องคอมพิวเตอร์สืบค้นโอแพคหรือฐานข้อมูลออนไลน์ต่าง ๆ เครื่องคอมพิวเตอร์สำหรับผู้ใช้ห้องสมุดที่เป็นบุคคลภายนอกซึ่งไม่มีบัญชีผู้ใช้งานระบบเครือข่ายของห้องสมุดและมหาวิทยาลัย จะไม่มีการกำหนดรหัสผ่านในการเปิดใช้เพื่อสืบค้นโอแพค ดังคำสัมภาษณ์

“คอมพิวเตอร์แต่ละเครื่องให้สิทธิ user แต่ไม่ให้สิทธิลงโปรแกรม, config network, แก้ไข ip ไม่ได้, add ฮาร์ดแวร์ เช่น printer ไม่ได้, แต่ลงภาษาได้เปลี่ยนภาษาได้”

“แต่ละเครื่องมี password ของแต่ละคน ตั้งกันเอง ยกเว้นบางคนขี้เกียจไม่ทำก็ไม่บังคับ การใช้ username/password ในการเปิดวินโดว์แต่ละคนยังไม่เข้มงวด แล้วแต่ว่าเขาจะมีหรือไม่มีก็ได้ ส่วนเครื่องสาธารณะก็เปิดใช้งานได้เลย”

“เครื่องคอมพิวเตอร์ที่ใช้ทำงานเป็นการใช้ร่วมกัน ไม่มีเฉพาะของใครของมัน จึงไม่มีการ login เข้า Windows บางคนก็นำเครื่องโน้ตบุ๊กส่วนตัวมาใช้ที่ทำงาน เราก็ไม่ว่าอะไร”

“เราจัดเครื่องคอมพิวเตอร์สำหรับบุคคลภายนอกจำนวนหนึ่ง เขาสามารถเปิดใช้งานได้โดยไม่ต้องมี username/password เขาสามารถค้นได้ทั้งโอแพคและออกอินเทอร์เน็ต”

8. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control) พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐติดตั้งโปรแกรมคอมพิวเตอร์ลิขสิทธิ์สำหรับใช้ในการปฏิบัติงานตามความจำเป็น ได้แก่ ระบบปฏิบัติการวินโดวส์ โปรแกรมออฟฟิศ โปรแกรมกราฟิก และโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ส่วนเครื่องคอมพิวเตอร์สำหรับผู้ใช้บริการมีการติดตั้งโปรแกรมประยุกต์ตามความจำเป็น เช่น SPSS, Endnote, Turnit-in เป็นต้น โดยจัดซื้อลิขสิทธิ์สำหรับติดตั้งโปรแกรมบนเครื่องแบบทั่วไปและการใช้งานผ่านคลาวด์ นอกจากนี้มีการเข้มงวดเรื่องการติดตั้งโปรแกรมไม่มีลิขสิทธิ์ลงในเครื่องคอมพิวเตอร์ของห้องสมุดทั้งเครื่องคอมพิวเตอร์สำหรับบุคลากรและสำหรับผู้ใช้ห้องสมุด ดังคำสัมภาษณ์

“เรื่องติดตั้งโปรแกรมโดยไม่ได้รับอนุญาตกระทำไม่ได้ กำหนดให้ใช้ซอฟต์แวร์พื้นฐานเท่านั้น ถ้าต้องการเพิ่มต้องแจ้ง”

“การ download app ต่าง ๆ เช่น tulip app, Endnote จะตั้งให้ผูกติดกับ authen ต้องระบุ username/password ในการดาวน์โหลดหรือใช้งานทุกครั้ง”

9. การจัดทำระบบสำรอง (Backup) พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐสำรองข้อมูลของระบบสารสนเทศต่าง ๆ มากกว่าวิธี ได้แก่ 1) การสำรองข้อมูลแบบอัตโนมัติในช่วงเวลาที่กำหนด คือ หลังเลิกงานหรือหลังเที่ยงคืน ซึ่งข้อมูลสำรองจะถูกจัดเก็บในระบบจัดเก็บข้อมูลบนเครือข่ายที่เรียกว่า NAS (Network attached storage และระบบจัดเก็บข้อมูลแบบเชื่อมโยงเป็นเครือข่ายที่เรียกว่า SAN (Storage area network) 2) การทำสำรองข้อมูลแบบมือ (Manual backup) เป็นการทำสำรองโดยผู้ดูแลระบบแต่ละระบบสารสนเทศที่ทำสำรองข้อมูลเก็บไว้ในเทปแม่เหล็กและนำไปเก็บในที่ที่ปลอดภัย เช่น ตู้เซฟกันไฟของห้องสมุด ตู้เซฟในอาคารอื่นของมหาวิทยาลัยหรือต่างวิทยาเขต ตู้นิรภัยของธนาคารพาณิชย์ เป็นต้น 3) การสำรองข้อมูลแบบคลาวด์ ซึ่งเป็นระบบคลาวด์ของห้องสมุด/สำนักคอมพิวเตอร์ของมหาวิทยาลัย หรือระบบคลาวด์ของเอกชนโดยเช่าพื้นที่จัดเก็บข้อมูล

และดูแลเครื่องแม่ข่ายของระบบสารสนเทศ และ 4) การสำรองข้อมูลบนระบบคลาวด์ที่ไม่เสียค่าใช้จ่าย เช่น Google drive, cloud drive ของมหาวิทยาลัย เป็นต้น ดังคำสัมภาษณ์

"มีการ backup ข้อมูลเวลาเที่ยงคืนแบบอัตโนมัติ จัดเก็บใน NAS ทำ Mirror site ข้อมูลไว้ที่สำนักไอที และนำเทปบันทึกข้อมูลที่ backup เก็บไว้ที่ธนาคารพาณิชย์แห่งหนึ่ง 2 สัปดาห์ครั้ง ส่วนข้อมูลการทำงานของบุคลากรต่าง ๆ ให้จัดเก็บที่ Google Cloud"

"การสำรองข้อมูลทุก server หลักไปเก็บที่คลาวด์ทั้งหมด เป็นบริการคลาวด์ของเอกชน จ่ายปีละเกือบล้าน แต่ดีกว่าทำเองเพราะประหยัดกว่า เสถียรกว่า มั่นใจกว่าสำรองอยู่ในตึกเราหรือทำเอง"

"สำรองเก็บข้อมูล มีใช้ SAN และ NAS ทำ backup แบบ manual เพราะ end of sale ของบริษัทหมด support จากบริษัท ถ้าต่อสัญญาจะแพงมาก จึงทำ manual ไปก่อน ใช้วิธี remote login เข้ามาทำ backup ตอนกลางคืน ข้อมูลทุกอย่างอยู่ที่ Data Center นี้ เราทำให้ทั้งหมด บางหน่วยงานเขาก็ backup ส่วนงานของเขาเองลงเทปหรือฮาร์ดดิสต์สำรองไป เครื่อง server ส่วนกลางหากมีปัญหาก็สามารถกู้คืนข้อมูลได้บางส่วนตาม run time การทำงานของมัน"

10. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ เนื่องจากมีการปฏิบัติตามหลักการประกันคุณภาพของห้องสมุด และเป็นหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานที่เกี่ยวข้องโดยเฉพาะฝ่ายเทคโนโลยีห้องสมุด โดยมีการป้องกันทางกายภาพด้วยอุปกรณ์และอาคารสถานที่ และการตรวจสอบความเสี่ยงเป็นระยะ จนถึงการตรวจสอบก่อนการบริการหรือห้องสมุดเปิดเพื่อให้มั่นใจว่าผู้ใช้สามารถใช้บริการได้ทันที ดังคำสัมภาษณ์

"ปฏิบัติตาม ISO9001 version 2015 มีการลำดับความสำคัญของอุปกรณ์ในกรณีที่ไฟฟ้าขัดข้องเนื่องจากกำลังไฟไม่เพียงพอในการบู๊ทเครื่องทั้งหมดพร้อมกัน"

"ระบบดับเพลิงใช้แบบ CO2 แบบควัน มีการซ้อมแผนดับเพลิงทุกปี และอาคารมีระบบกันไฟในหลายจุด ห้องระบบฯ จะซีลด์กันความร้อน เพราะเป็นห้องกระจก และใช้แอร์ 3 ตัว เปิดสลับวันละ 2 ตัว"

"ห้องสมุดมีแผน PM (Prevention maintenance) ฝ่ายเทคโนฯ มีการประเมินความเสี่ยงเป็นแผนรายปี เช่น downtime ต้องใช้งานได้ไม่น้อยกว่า 98%เรามีคณะกรรมการจัดการความเสี่ยง และทุกปีจะมีการตรวจสอบภายในจากหน่วยงานของมหาวิทยาลัย"

"ฐานข้อมูลทุกฐาน ฝ่ายเทคโนฯ จะตรวจสอบความพร้อมใช้ก่อนเวลาห้องสมุดเปิดทุกวัน โดยใช้วิธีรีโมท โปรแกร bot ยิงไปที่ฐานข้อมูลว่าใช้งานได้ปกติหรือไม่ เพราะเดิมเรารู้ทีหลังผู้ใช้ จึงให้มีการตรวจสอบก่อน"

"มีการบำรุงรักษาระบบเป็นระยะ ๆ มีตารางเวลา Checklist รวมทั้งการ maintainance ของบริษัทต่าง ๆ"

11. การกำหนดความรับผิดชอบที่ชัดเจนแก่บุคลากรที่เกี่ยวข้องพบว่าห้องสมุดสถาบันอุดมศึกษาของรัฐกำหนดความรับผิดชอบต่อเหตุการณ์ความเสียหายที่อาจเกิดขึ้นแก่ผู้ปฏิบัติงานตามการพรรณนางานของแต่ละตำแหน่ง ทั้งนี้ความรับผิดชอบโดยรวมของระบบสารสนเทศขึ้นกับหัวหน้าฝ่ายเทคโนโลยีห้องสมุดและผู้บริหารห้องสมุดตามแต่ละนโยบายของห้องสมุด ดังคำสัมภาษณ์

"ผู้บริหารห้องสมุดต้องรับผิดชอบต่อความเสียหายโดยรวม โดยเฉพาะ ผอ. (ผู้อำนวยการ) ห้องสมุด ซึ่งทั้งโดยหน้าที่ความรับผิดชอบและกฎระเบียบต้องเป็นเช่นนั้น ส่วนผู้บริหารอื่น รอง ผอ. หัวหน้าฝ่าย ก็ต้องรับผิดชอบในงานของตัวเองเหมือนกัน"

"เรื่องหัวหน้างานต้องรับผิดชอบหากเกิดความเสียหา ยังไม่เคยเห็นคำสั่งนะ แต่โดยหน้าที่เราก็ต้องรับผิดชอบเป็นหลักอยู่แล้ว การแบ่งงาน มอบหมายงานชัดเจน ทำให้ควบคุมการทำงานของเด็ก ๆ ได้ง่าย ทุกคนรู้หน้าที่ของตัวเองและช่วยเหลือกัน การทำงานไม่มีปัญหา"

12. ปัญหาความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศของห้องสมุด ปัจจัยสนับสนุนและวิธีแก้ปัญหา พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐประสบปัญหาทางตรงและทางอ้อมที่เป็นความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศของห้องสมุด ได้แก่ 1) ผู้ใช้ใช้ซอฟต์แวร์ประเภท Robotic เพื่อดาวน์โหลดข้อมูลจากฐานข้อมูลออนไลน์ ซึ่งเสี่ยงต่อการถูกฟ้องร้องและระงับการใช้งานจากสำนักพิมพ์หรือเจ้าของฐานข้อมูล ซึ่งแก้ไขโดยการออกประกาศหรือระเบียบข้อบังคับ และใช้ระบบตรวจตราการใช้งานเครือข่าย 2) การใช้ซอฟต์แวร์ที่ไม่ถูกต้องเรื่องลิขสิทธิ์ ซึ่งเสี่ยงต่อไวรัสคอมพิวเตอร์และการถูกฟ้องร้องจากบริษัทเจ้าของลิขสิทธิ์ซอฟต์แวร์ ซึ่งแก้ไขโดยการออกประกาศหรือระเบียบข้อบังคับ และการกำหนดสิทธิการเข้าถึงระบบระบบปฏิบัติการของเครื่องคอมพิวเตอร์ที่ใช้งาน 3) ระบบไฟฟ้าที่ไม่เสถียร เช่น ไฟดับ ไฟกระชาก เป็นต้น ทำให้เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไม่สามารถให้บริการได้ รวมทั้งอาจทำให้เสียหายด้วย ซึ่งแก้ไขโดยการใช้อุปกรณ์สำรองไฟฟ้า (UPS) และการจัดตารางงานสำหรับบุคลากรดูแลระบบตลอดเวลา 4) ความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลทั้งของบุคลากรและผู้ใช้ห้องสมุด ซึ่งอาจขัดต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำลังประกาศใช้ ซึ่งแก้ไขโดยการฝึกอบรมให้ความรู้แก่บุคลากรทุกคน และการกำหนดระเบียบข้อบังคับเพื่อป้องกันการกระทำดังกล่าว และ 5) การขาดแคลนงบประมาณ ทำให้ไม่สามารถขยายการบริการได้ทั่วถึง รวมทั้งการจัดซื้อฮาร์ดแวร์และซอฟต์แวร์ ดังคำสัมภาษณ์

"Publisher แจ้งว่า มีการใช้งานข้อมูลผิดปกติ เช่น download ข้อมูลจำนวนมาก ตั้ง auto download เอาไว้ หรือใช้ bot อย่างนี้ ซึ่งสำนักคอมฯ track ไม่ได้ ระบุได้เฉพาะว่ามาจากคณะไหน ตึกไหน น้อยครั้งมากที่จะ track ได้ บางตึก เช่น ตึกแพทย์ ตึกบัญชี มี lease line ของตัวเอง ก็ track ไม่ได้"

“พบว่า บางเครื่องที่ใช้งานมีการใช้ซอฟต์แวร์ไม่ถูกต้องเรื่องลิขสิทธิ์ ซึ่งผู้ใช้ติดตั้งเอง ก็ว่ากล่าวตักเตือนและให้ถอนออก หากจำเป็นต้องใช้งานจริง ๆ ให้ทำบันทึกแจ้งมาอย่างเป็นทางการ ก็จะพิจารณาเป็นราย ๆ ไป”

“ถ้าเกิดไฟฟ้าดับ ห้องสมุดมี UPS สำรองได้ 10 ชั่วโมง เพราะระบบห้องสมุดอัตโนมัติเป็นแบบ centralized ให้ห้องสมุดคณะต่าง ๆ ทำให้ใช้งานไม่ได้ทั้งหมด เมื่อไฟฟ้ากลับมาปกติ พบว่ากำลังไฟไม่สามารถบู๊ตเครื่องและระบบต่าง ๆ ได้ทั้งหมด จึงมีการจัดลำดับความสำคัญของอุปกรณ์เพื่อให้รองรับกำลังไฟได้”

“ตอนนี้มีประกาศพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มหาวิทยาลัย หน่วยงานต่าง ๆ รวมทั้งห้องสมุดต้องปฏิบัติ ต้องมีการกำหนดนโยบายป้องกันเพื่อไม่ให้เกิดเหตุฟ้องร้อง แต่ตอนนี้ห้องสมุดยังไม่มีมาตรการหรือแนวปฏิบัติใด ๆ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จะมีการจัดอบรมบรรยายให้บุคลากรของมหาวิทยาลัย เรื่อง กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการพัฒนาระบบบริหารงานบุคคล เร็ว ๆ นี้”

“Wifi ไม่เพียงพอ เนื่องจากงบประมาณน้อย ติดตั้ง access point ได้ไม่ทั่วถึง ต้องเลือกเฉพาะจุดที่ใช้งานมากหรือจุดสำคัญจริง ๆ โดยใช้วิธีตรวจ traffic การใช้งาน”

“การนำโน้ตบุ๊คส่วนตัวจากบ้านมาใช้งานที่ทำงาน ก็เคยเกิดเรื่องทำให้แพร่ไวรัส ซึ่งแก้ไขตามอาการ เพราะมหาวิทยาลัยเป็นไซส์ขนาดเล็ก และงบประมาณน้อย ไม่ได้ซื้อ antivirus แบบ license มาใช้ ยิ่งถ้าห้องสมุดไม่มี Web application firewall ก็ไม่มีตัวช่วย ทำให้เว็บไซต์โดนแฮ็กค์ได้ง่าย”

“ห้องสมุดขาดแคลนงบประมาณ เนื่องจากจำนวนนักศึกษาน้อยลงทำให้งบประมาณที่ได้รับลดลงด้วย ต้องแก้ปัญหาเฉพาะหน้า เช่น ไม่ซื้ออุปกรณ์ใหม่ ซ่อมแซมเองเพื่อใช้งานไปก่อน”

อภิปรายผล

ผลการวิจัยสภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาของรัฐ มีประเด็นที่น่าสนใจนำมาอภิปรายผล ดังนี้

1. ห้องสมุดสถาบันอุดมศึกษาของรัฐมีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตาม “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553” ทั้ง 11 ข้อ เนื่องจากห้องสมุดสังกัดมหาวิทยาลัยที่เป็นหน่วยงานของรัฐที่ที่หน้าที่ต้องปฏิบัติตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553” ("Announcement of the Electronic Transactions Commission ...", 2010) ซึ่งกำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้สามารถดำเนินการต่าง ๆ ด้วยวิธีทางอิเล็กทรอนิกส์ โดยให้หน่วยงานของรัฐมีการดำเนินการทางอิเล็กทรอนิกส์อย่างมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล โดยอาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 (“Royal decree prescribing rules and procedures…”, 2007, pp. 2-3) ที่กำหนดให้มีผลโดยชอบด้วยกฎหมาย

นโยบายรักษาความมั่นคงระบบสารสนเทศถูกกำหนดอย่างเป็นลายลักษณ์อักษรโดยห้องสมุดหรือสำนักคอมพิวเตอร์ของมหาวิทยาลัยเพื่อให้บุคลากรทุกคนปฏิบัติตาม ซึ่งนโยบายที่เป็นลายลักษณ์อักษรดังกล่าวมีเพียงบางห้องสมุดเท่านั้น เนื่องจากการกำหนดนโยบายดังกล่าวต้องดำเนินการโดยคณะกรรมการของมหาวิทยาลัยและมีอธิการบดีเป็นประธาน เมื่อร่างนโยบายเสร็จต้องนำเสนอต่อสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อพิจารณา ซึ่งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Development Agency, 2020) จัดทำประกาศรายชื่อหน่วยงานที่ผ่านการความเห็นชอบการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐผ่านเว็บไซต์ ซึ่งล่าสุดเมื่อวันที่ 14 เมษายน 2563 มีมหาวิทยาลัยที่ผ่านการพิจารณาเห็นชอบ ตั้งแต่ พ.ศ. 2555-2563 มีจำนวน 14 แห่ง นอกจากนี้มีการประกาศในราชกิจจานุเบกษา เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559 (Announcement of the Electronic Transactions Commission, 2016) หน่วยงานที่สังกัดกระทรวงศึกษาธิการ ได้แก่ มหาวิทยาลัย ซึ่งมีเพียง 7 แห่งที่ผ่านเกณฑ์ดังกล่าว ได้แก่ มหาวิทยาลัยขอนแก่น มหาวิทยาลัยเชียงใหม่ มหาวิทยาลัยธรรมศาสตร์ มหาวิทยาลัยนเรศวร มหาวิทยาลัยมหิดล มหาวิทยาลัยศรีนครินทรวิโรฒ และมหาวิทยาลัยสงขลานครินทร์ ซึ่งแสดงว่า รัฐบาลเข้มงวดและให้ความสำคัญต่อนโยบายดังกล่าว รวมทั้งการปฏิบัติต้องเป็นไปอย่างเคร่งครัด มีมหาวิทยาลัยที่ผ่านความเห็นชอบจำนวนน้อยมาก จึงทำให้บุคลากรห้องสมุดสถาบันอุดมศึกษาของรัฐบางแห่งไม่ทราบหรือพบเห็นนโยบายดังกล่าวที่เป็นลายลักษณ์อักษร ดังนั้นผลการวิจัยจึงพบว่า ห้องสมุดทุกแห่งกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของห้องสมุดขึ้นมาเอง โดยนำนโยบาย กฎหมาย และพระราชบัญญัติต่าง ๆ ที่เกี่ยวข้องมากำหนดเป็นประกาศและข้อปฏิบัติสำหรับบุคลากรและผู้ใช้ห้องสมุดเพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ผลการวิจัยนี้สอดคล้องกับงานวิจัยของพีรพันธ์ รุจิพงษ์กุล (Ruchiphongkun, 2015) ที่พบว่า มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือมีการกำหนดนโยบายการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ที่ชัดเจนและเป็นลายลักษณ์อักษร งานวิจัยของยาสดันมีห์รและวอง (Yazdanmehr & Wang, 2016) ที่ให้ความสำคัญต่อการนำนโยบายความมั่นคงปลอดภัยสารสนเทศไปใช้ในองค์กรเพื่อให้เกิดผลในทางปฏิบัติโดยเกิดจากความรับผิดชอบส่วนบุคคลและบรรทัดฐานทางสังคมที่มาจากบรรยากาศทางจริยธรรมขององค์กร

ห้องสมุดสถาบันอุดมศึกษาของรัฐกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ การบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน และการควบคุมการเข้าถึงเครือข่าย โดยกำหนดสิทธิและระดับของบุคคลทั้งทางกายภาพและทางอิเล็กทรอนิกส์ เนื่องจากระบบสารสนเทศประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล เครือข่าย และบุคคล (Zwass, 2020) การดำเนินธุรกรรมต่าง ๆ ผ่านระบบเครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์แม่ข่ายกับเครื่องลูกข่าย ซึ่งมีห้องควบคุมส่วนกลางที่จัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ เช่น เครื่องแม่ข่ายฐานข้อมูล เครื่องแม่ข่ายระบบเครือข่าย เครื่องแม่ข่ายเว็บไซต์ อุปกรณ์ระบบเครือข่าย เป็นต้น จึงต้องมีการป้องกันการเข้าถึงอุปกรณ์ต่าง ๆ ทางกายภาพโดยอนุญาตเฉพาะผู้ที่เกี่ยวข้องเข้าถึงอุปกรณ์ต่าง ๆ ได้ โดยกำหนดกฎระเบียบและใช้อุปกรณ์ป้องกันบุคคลอื่นเข้าถึงโดยไม่ได้รับอนุญาต นอกจากนี้การคุกคามทางระบบ

เครือข่ายสามารถกระทำได้โดยแฮคเกอร์ (Hacker) ซึ่งกระทำได้หลายรูปแบบ ได้แก่ การขโมยข้อมูล ทำให้ข้อมูลเสียหาย หรือรบกวนการทำงาน โดยใช้ซอฟต์แวร์ เช่น ไวรัสคอมพิวเตอร์ มัลแวร์ (Malware) รันซัมแวร์ (Ransomware) สนิฟเฟอร์ (Sniffer) เป็นต้น ผู้ปฏิบัติงานต้องระมัดระวังเรื่องการใช้ซอฟต์แวร์ คอมพิวเตอร์ และอินเทอร์เน็ต เพื่อเลี่ยงความเสี่ยงที่จะเกิดขึ้น (Rhee, Kim, & Ryu, 2009) ห้องสมุดจึงจำเป็นต้องมีมาตรการป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ชอบดังกล่าว ผลการวิจัยนี้สอดคล้องกับงานวิจัยของวศิน รำพึงกิจ (Ramphungkit, 2009) ที่พบว่า ประเด็นที่มีความเสี่ยงสูงต่อการรักษาความปลอดภัยสารสนเทศของธนาคารพาณิชย์ ได้แก่ การเข้าใช้งานอินเทอร์เน็ตและการใช้ระบบเครือไร้สายที่ไม่เกี่ยวกับการปฏิบัติงานของพนักงาน การเปลี่ยนหน้าเว็บโดยไม่ได้รับอนุญาต และการเจาะระบบโดยผู้ไม่ประสงค์ดีงานวิจัยฮู (Hou, 2020) ที่พบว่าการโจมตีทางเครือข่ายโดยเฉพาะปัจจุบันที่เป็นสังคมอินเทอร์เน็ตของทุกสิ่ง (Internet of Things) ก่อให้เกิดความเสียหายทั้งการใช้งานเครือข่ายและข้อมูลขององค์กร และงานวิจัยของค็อค (Cox, 2012) ที่พบว่าพฤติกรรมไม่ใส่ใจในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้ใช้เป็นสาเหตุหลักของการเกิดความเสี่ยงต่อความปลอดภัยของระบบ

ห้องสมุดสถาบันอุดมศึกษาของรัฐมีการป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต รวมทั้งการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ โดยให้บุคลากรกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์ที่ตนใช้ปฏิบัติงาน รวมทั้งติดตั้งโปรแกรมคอมพิวเตอร์ลิขสิทธิ์สำหรับใช้ในการปฏิบัติงานตามความจำเป็น เนื่องจากซอฟต์แวร์ระบบปฏิบัติการวินโดวส์สามารถตั้งรหัสป้องกันการเปิดใช้เครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต รวมทั้งกำหนดผู้ใช้ที่เป็น Administrator ที่สามารถติดตั้งและตั้งค่าต่าง ๆ ของคอมพิวเตอร์ได้ และ Guest เป็นเพียงผู้ใช้งานเท่านั้นโดยถูกจำกัดสิทธิในการติดตั้งโปรแกรมและตั้งค่าระบบ ซึ่งเป็นไปตามมาตรฐานความปลอดภัย Orange Book ระดับ C2 ของกระทรวงกลาโหม ประเทศสหรัฐอเมริกา ซึ่งเป็นต้นแบบของเกณฑ์ความมั่นคงปลอดภัย (U.S. Department of Defense, 1985, p. 17) โดยป้องกันการลักลอบใช้โปรแกรมประยุกต์เพื่อเข้าสู่ฐานข้อมูลของห้องสมุดและเข้าถึงข้อมูลที่จัดเก็บภายในเครื่องคอมพิวเตอร์ ส่วนการติดตั้งซอฟต์แวร์ที่ได้มาโดยไม่เสียค่าใช้จ่ายหรือดาวน์โหลดจากเว็บไซต์นั้นเสี่ยงต่อการติดไวรัสคอมพิวเตอร์ประเภทสปายแวร์ (Spyware or malicious software) ที่ซ่อนตัวอยู่ในคอมพิวเตอร์ คอยตรวจสอบกิจกรรมการทำงาน ขโมยข้อมูลหรือกระทำการที่สร้างความเสียหายทำให้เกิดความไม่มั่นคงปลอดภัยต่อระบบสารสนเทศ (Malwarebytes Ltd, 2020; Safa, von Solms, & Futcher, 2016) ผลการวิจัยนี้สอดคล้องกับงานวิจัยของถนอมศรี เตมานุวัตร์ และไสว ศิริทองถาวร (Temanuwat & Sirithongthavorn, 2011) พบว่า การใช้โปรแกรมละเมิดลิขสิทธิ์เป็นความเสี่ยงต่อความมั่นคงปลอดภัยระบบสารสนเทศ และงานวิจัยของนฤมล รุ่งสาย (Rungsai, 2013) พบว่าการนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาใช้ปฏิบัติงานในองค์กร การใช้งานโดยไม่ได้รับอนุญาต และการขาดการรักษาความปลอดภัยจากอันตรายที่มาจากอินเทอร์เน็ตเป็นความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

ห้องสมุดสถาบันอุดมศึกษาของรัฐกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานและกำหนดความรับผิดชอบที่ชัดเจนแก่บุคลากรที่เกี่ยวข้อง เนื่องจากการปฏิบัติงานในหน่วยงานของรัฐมีการกำหนดหน้าที่ความ

รับผิดชอบทุกตำแหน่งงานอย่างชัดเจน แต่ตำแหน่งบรรณารักษ์และเจ้าหน้าที่ห้องสมุดยกเว้นตำแหน่งที่เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศไม่พบการกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุด ทั้งที่ห้องสมุดเป็นแหล่งรวบรวมและให้บริการสารสนเทศ ซึ่งอาจเป็นเพราะเดิมการปฏิบัติงานห้องสมุดไม่มีการใช้เทคโนโลยีคอมพิวเตอร์หรือใช้น้อยมาก ทำให้ไม่มีการปรับปรุงการพรรณนางานตำแหน่งบรรณารักษ์และเจ้าหน้าที่ห้องสมุดให้สอดคล้องกับการปฏิบัติงานในปัจจุบันที่การปฏิบัติงานส่วนใหญ่ต้องใช้ระบบเทคโนโลยีสารสนเทศเป็นหลัก นอกจากนี้ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 (“Announcement of the Electronic Transactions Commission...”, 2010, pp. 131-138) ข้อ 3 “หน่วยงานของรัฐกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน ให้หัวหน้าหน่วยงานรับผิดชอบ” และข้อ 14 ตามประกาศฯ ฉบับที่ 2 พ.ศ. 2556 “หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ... ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น”

ห้องสมุดสถาบันอุดมศึกษาของรัฐสำรองข้อมูลของระบบสารสนเทศต่าง ๆ มากกว่าวิธี ซึ่งนอกเหนือจากการปฏิบัติตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ (“Announcement of the Electronic Transactions Commission...”, 2010, p. 132) ข้อ 2 (2) แล้ว ห้องสมุดจำเป็นต้องสร้างความมั่นคงและปลอดภัยแก่ข้อมูลในระบบสารสนเทศที่เป็นสินทรัพย์ในงานบริการที่สำคัญของห้องสมุด การสำรองข้อมูลในระบบสารสนเทศของทุกห้องสมุดทั้งระบบมือหรือระบบอัตโนมัติมีกระทำมากกว่า 1 วิธี เพื่อสร้างความมั่นใจและประกันความเสียหาย (Linli, 2004) รวมทั้งมีการทำซ้ำ (Redundancy) ในกรณีที่ระบบใดระบบหนึ่งเกิดความเสียหายก็สามารถใช้อีกระบบแทนได้ นอกจากนี้ห้องสมุดมีการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ ซึ่งเป็นการปฏิบัติตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (“Announcement of the Electronic Transactions Commission...”, 2010, p. 132) ข้อ 2 (3) “จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน...” และเป็นการปฏิบัติตามหลักการประกันคุณภาพของห้องสมุดสถาบันอุดมศึกษา รวมทั้งเป็นหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานที่เกี่ยวข้องโดยเฉพาะฝ่ายเทคโนโลยีห้องสมุด ซึ่งเป็นมาตรฐานสากลที่ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Governance Institute, 2007, p. 12) ผลวิจัยนี้สอดคล้องกับงานวิจัยของถนอมศรี เตมานุวัตร์ และไสว ศิริทองถาวร (Temanuwat & Sirithongthavorn, 2011) พบว่า การปฏิบัติงานระบบสารสนเทศหน่วยงานของรัฐมีความเสี่ยงเรื่องข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์แม่ขายสูญหาย ระบบไม่สามารถให้บริการได้ต่อเนื่องนานกว่า 1 ชั่วโมง และโปรแกรมระบบปฏิบัติการไม่สามารถทำงานได้ตามปกติ งานวิจัยของธิดา ลิ่มทองวิรัตน์ (Limthongwiwat, 2011) พบว่า การบำรุงรักษาอุปกรณ์ต่าง ๆ ให้อยู่ในสภาพสมบูรณ์ เป็นมาตรการหนึ่งในการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และงานวิจัยของอิสเมลและไซแน็บ (Ismail & Zainab, 2011) พบว่า ห้องสมุดส่วนใหญ่ร้อยละ 95 มีการดำเนินงานรักษาความปลอดภัยของระบบสารสนเทศในด้านเทคนิคอยู่ในระดับดี

เอกสารอ้างอิง

[Announcement of the Electronic Transactions Commission on government agencies' information security policy and practice guidelines]. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 (2010, 23 June). *Ratchakitchanubeksa*. Book 127 special Part 78 Ngo, pp. 131-138. [In Thai]

[Announcement of the Electronic Transactions Commission on list of departments or organizations, or sections of departments or organizations considered as an important structure of the country, which must be done in accordance with strict safety procedures in 2016]. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559 (2016, 25 August). *Ratchakitchanubeksa*, Book 133 Special part 189 Ngor p. 8. [In Thai]

Burapha University, Department of Library Science. (2007). *สารสนเทศและการศึกษาค้นคว้า [Information and research]*. Chonburi: Author. [In Thai]

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior, 28*, 1849-1858.

Electronic Transactions Development Agency. (2020). *รายชื่อหน่วยงานผ่านความเห็นชอบการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ปรับปรุง ณ วันที่ 17-04-2563) [List of agencies through approval of establishing policy guidelines and guidelines for information security of government agencies (updated 17-04-2020).* Retrieved from https://etcommission.go.th/etc-annoucement-sp-p2.html [In Thai]

Hou, R., Ren, G., Zhou, C., Yue, H., Liu, H., & Liu, J. (2020). Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things. *Computer Communications*, 158, 64-72.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013*. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

Internet Crime Compliant Center. (2015). *2015 Internet crime report. Washington, DC: Federal Bureau of Investigation*. Retrieved from http://www.ic3.gov/media/annualreport/ 2015_ic3report.pdf

Ismail, R. & Zainab, A. N. (2011, August). Information systems security in special and public libraries: An assessment of status. *Malaysian Journal of Library & Information Science, 16*(2), 45-62.

IT Governance Institute. (2007). *CoBit 4.1 excerpt*. Meadows, IL: Author.

Limthongwiwat, T. (2011). *Evaluation of the effectiveness of the internal control for information security according to ISO27001: A case study of Business Online Public Co. Ltd.* (Master's Independent study). University of the Thai Chamber of Commerce, Bangkok. [In Thai]

Linli, G. (2004). The data's backup of automatic system in library. *New Technology of Library and Information Service*, 20(8), 81-83. doi: 10.11925/infotech.1003-3513.2004.08.22

Malwarebytes Ltd. (2020). *Spyware*. Retrieved from https://www.malwarebytes.com/spyware

National Electronics and Computer Technology Center. (2007). *มาตรการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550 [Security measures for electronic transactions (Version 2.5) for the year 2007].* Bangkok: Author. [In Thai]

Phanitkul, P., & Pongsakulchai, S. (2009). *ระบบสารสนเทศเพื่อการจัดการ [Management information system].* Bangkok: KTP Comp & Consult. [In Thai]

Phosita, C. (2011). *ศาสตร์และศิลป์แห่งการวิจัยเชิงคุณภาพ [The sciences and arts of qualitative research]* (5th ed.). Bangkok: Amarin Printing and Publishing. [In Thai]

PwC Thailand. (2016). *Economic crime in Thailand: PwC's 2016 global economic crime survey.* Bangkok: Author. Retrieved from https://www.pwc.com/th/en/publications/2016/economic-crime-thailand2016.pdf

Ramphungkit, W. (2009). *การสำรวจภัยคุกคามทางคอมพิวเตอร์และการรักษาความปลอดภัยข้อมูลสารสนเทศของธนาคารพาณิชย์ในประเทศไทย [Computer crime and security survey of the commercial banks in Thailand*] (Master's independent study). Thammasat University, Bangkok. [In Thai]

Rhee, H. –S, Kim, C., & Ryu, Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computer & Security, 28*(8), 816-826.

[Royal decree prescribing rules and procedures for government electronic transactions 2006 (B.E. 2549)] พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ. (2007, 10 January). *Ratchakitchanubeksa*. Book 124 Part 4 Ko, pp. 1-4. [In Thai]

Ruchiphongkun, P. (2015). *การศึกษาแนวโน้มของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยใช้เทคนิคเดลฟาย [Study on trends of security systems on computer networks within King Mongkut's University of Technology North Bangkok using the delphi technique*] (Master's thesis). King Mongkut's University of Technology North Bangkok, Bangkok. [In Thai]

Rungsai, N. (2013*). แนวทางในการป้องกันและแก้ไขความเสี่ยงในการนำอุปกรณ์ส่วนตัวมาใช้ในองค์กร [An approach to prevent and mitigate risk of using personal device at workplace]* (Master's thesis). King Mongkut's University of Technology North Bangkok, Bangkok. [In Thai]

Safa, N. S., von Solms, R., & Futcher, L. (2016, February). Human aspects of information security in organizations. *Computer Fraud & Security*. Retrieved from https://www.researchgate.net

Savin-Baden, M., & Major, C. (2013). *Qualitative research: The essential guide to theory and practice*. London, UK: Routledge.

Talapphet, K. (2010). Meaning and objectives of security control of information systems. In *การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน [Computer systems and internal control]* (10th ed., pp. 199-210). Nonthaburi: Sukhothai Thammathirat Open University. [In Thai]

Temanuwat, T, & Sirithongthavorn, S. (2011). การปรับปรุงกระบวนการให้บริการงานสารสนเทศ โดยการประยุกต์ใช้มาตรฐานบริหารความปลอดภัยของข้อมูลสารสนเทศ ISO/IEC27001 [Improvement of information services process by applying safety management standard of ISO/IEC27001]. In *the 1st Graduate Education Conference. Bangkok: Bangkok University.* Retrieved from http://proceedings.bu.ac.th/index.php/com-phocadownload-controlpanel/grc?start=20 [In Thai]

TNet Co. Ltd. (2013). *มาตรฐาน ISO/IEC 27001: 2013 [Standard ISO/IEC 27001: 2013].* Retrieved from http://www.rtna.ac.th/download/27001-2013.pdf [In Thai]

U.S. Department of Defense. (1985). *Department of Defense standard: Department of Defense Trusted Computer System Evaluation Criteria*. Washington, D.C.: Author. Retrieved from https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

Yazdanmehr, A., & Wang, J. (2016, December). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*, 36-46.

Zwass, V. (2020). Information system. In *Encyclopedia Britannica*. Retrieved form https://www.britannica.com/topic/information-system