คู่มือ

การสร้างความมั่นคงปลอดภัยทางไซเบอร์ส่วนบุคคล

บนระบบการเรียนรู้ด้วยตนเอง (Self-learning)

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ปีการศึกษา 2566

คำนำ

เอกสารคู่มือการจัดการองค์ความรู้ เรื่อง การสร้างความมั่นคงปลอดภัยทางไซเบอร์ส่วนบุคคล บนระบบการเรียนรู้ด้วยตนเอง (Self-learning) จัดทำขึ้นเพื่อรวบรวมองค์ความรู้ ความเข้าใจ ที่ได้จากกิจกรรมการแลกเปลี่ยนรู้เรียนภายในหน่วยงาน เพื่อนำองค์ความรู้ที่ได้มาพัฒนาให้เป็นระบบการเรียนรู้ด้วยตนเอง (Self-learning) เพื่อให้บุคลากรสามารถเข้าถึงองค์ความรู้และพัฒนาตนเองให้เป็นผู้รู้ได้ และเพื่อใช้เป็นแนวทางการปฏิบัติที่เหมาะสมในเรื่องของการสร้างความมั่นคงด้านความปลอดภัยของข้อมูลและการป้องกันภัยคุกคามที่อาจเกิดขึ้นในชีวิตประจำวันกับบุคลากรได้

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี หวังเป็นอย่างยิ่งว่าการจัดองค์ความรู้ในครั้งนี้ที่ได้จากการรวบรวม และการถ่ายทอดองค์ความรู้ผ่านวิธีการต่าง ๆ จะช่วยพัฒนาความรู้และทักษะให้กับบุคลากรสามารถนำไปใช้ให้เกิดประโยชน์ได้จริง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
กรกฎาคม 2567

สารบัญ

หน้า

สารบัญภาพ

บทนำ

การจัดการความรู้ในองค์กร คือ การรวบรวมองค์ความรู้ที่มีอยู่ภายในองค์กรจากตัวบุคคลหรือเอกสารเพื่อถ่ายทอดแลกเปลี่ยนความรู้ฝังลึก สร้างความรู้ และความเข้าใจให้คนในองค์กรสามารถเรียนรู้และพัฒนาตนเอง รวมถึงทำให้การปฏิบัติงานมีประสิทธิภาพที่ดียิ่งขึ้น ด้วยสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีพันธกิจที่สำคัญในการขับเคลื่อนเทคโนโลยีสารสนเทศและทรัพยากรการเรียนรู้ในรูปแบบบริการออนไลน์ต่าง ๆ การตอบสนองความต้องการทางด้านเทคโนโลยีการเรียนรู้ให้กับผู้ใช้บริการจึงจำเป็นต้องมีการปรับเปลี่ยนรูปแบบบริการต่าง ๆ ให้ทันกับความเปลี่ยนแปลงก้าวหน้าด้านเทคโนโลยีด้วยเช่นกัน ซึ่งการเข้าใช้บริการด้านเทคโนโลยีปัจจุบันผู้ใช้บริการจำเป็นต้องมีความรู้ความเข้าใจในการถึงข้อมูลอย่างปลอดภัยเบื้อนต้น เพื่อป้องกันภัยคุมคามที่อาจแฝงมาขณะใช้บริการทางออนไลน์ผ่านช่องทางต่าง ๆ ที่พยายามจะเข้าถึงข้อมูลได้ ไม่ว่าจะเป็นข้อมูลความเป็นส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลการปฏิบัติงาน เป็นต้น ซึ่งในชีวิตประจำวันไม่สามารถหลีกเลี่ยงการทำงานผ่านระบบออนไลน์ในรูปแบบต่าง ๆ การมีความรู้และทักษะทางเทคโนโลยีถือมีความจำเป็นที่จะต้องเรียนรู้ถึงวิธีการป้องกันภัยคุมคามที่อาจเกิดขึ้นอยู่เสมอได้ อีกทั้งทางสำนักฯ ได้พบเจอกับปัญหาการถูกลักลอกการเข้าถึงข้อมูลจากเครือข่ายภายนอกอยู่บ่อยครั้ง และการเร่งแก้ไขปัญหาเพื่อให้สามารถใช้งานระบบได้ปกติตามสถานการณ์ที่เกิดขึ้นนั้นเป็นการแก้ไขปัญหาที่ปลายเหตุ สำนักฯ เป็นหนึ่งในองค์กรที่ขับเคลื่อนทางด้านเทคโนโลยีสารสนเทศ และเพื่อให้การดำเนินงานของฝ่ายงานระบบเครือข่ายและความปลอดภัยข้อมูลเป็นไปตามวัตถุประสงค์ของการปฏิบัติงานอย่างแท้จริง การจัดการองค์ความรู้ภายในองค์กรตามกระบวนการแลกเปลี่ยนเรียนรู้จะช่วยให้งานสามารถดำเนินการเดินหน้าไปได้อย่างมีประสิทธิภาพและประสิทธิผลเพิ่มยิ่งขึ้น ดังนั้นหากองค์กรต้องการจะพัฒนาตนเองให้เป็นองค์กรแห่งการเรียนรู้ก็จำเป็นจะต้องบริหารจัดการความรู้ภายในองค์กรให้เป็นระบบอย่างสม่ำเสมอ และเพื่อส่งเสริมให้บุคลากรเกิดการเรียนรู้ได้อย่างต่อเนื่องและสามารถพัฒนาตนเองได้

ดังนั้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงได้รวบรวมองค์ความรู้เกี่ยวกับการสร้างความมั่นคงปลอดภัยทางไซเบอร์เพื่อเพิ่มองค์ความรู้และทักษะให้กับบุคลากร โดยได้จัดทำเป็นหลักสูตรเรียนผ่านระบบ D-Learn เพื่อใช้บริหารจัดการเรียนการสอนออนไลน์ให้ผู้เรียนสามารถเข้าถึงองค์ความรู้ได้ตลอดเวลา ซึ่งผู้เรียนเมื่อเข้าสู่ระบบแล้วต้องทำแบบทดสอบวัดความรู้ก่อนเรียน และเมื่อเรียนจบหลักสูตร ผู้เรียนต้องทำแบบทดสอบเพื่อทดสอบความรู้หลังจากที่ได้เรียนจบแล้วตามเกณฑ์ข้อกำหนด รวมถึงได้สร้างห้องสนทนากระดานถาม-ตอบสำหรับตั้งกระทู้หัวข้อแลกเปลี่ยนการเรียนรู้ กรณีศึกษา Best Practice เพื่อสร้างเป็น CoP: Community of Practice ผ่านการเรียนรู้จากสมาชิกด้วยกันเองที่ต้องการจะแบ่งปันแลกเปลี่ยนความรู้ ประสบการณ์ที่พบเจอจากการปฏิบัติงาน

การแลกเปลี่ยนเรียนรู้การสร้างความมั่นคงปลอดภัยทางไซเบอร์ส่วนบุคคล

สำนักฯ ปฏิบัติงานหลักส่วนใหญ่ผ่านการเชื่อมต่อระบบอินเทอร์เน็ตเป็นปัจจัยหลัก ซึ่งปัจจุบันมีภัยคุกคามที่เข้าโจมตีทางไซเบอร์ (Cyber Attack) เป็นภัยอันตรายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ เครือข่าย และข้อมูลทางอิเล็กทรอนิกส์ โดยสามารถก่อให้เกิดความเสียหายกับองค์กร เช่น การสูญหายของข้อมูล การเรียกค่าไถ่ การถูกขโมยข้อมูลส่วนตัว การถูกแฮ็กบัญชี การติดมัลแวร์ เป็นต้น

โดยในปัจจุบันมีการโจมตีทางไซเบอร์หลายรูปแบบด้วยกัน การรักษาความปลอดภัยทางไซเบอร์จึงเป็นสิ่งสำคัญอย่างยิ่ง เพราะภัยคุกคามทางไซเบอร์สามารถเกิดขึ้นได้ตลอดเวลา ดังนั้น จึงควรศึกษาและเรียนรู้วิธีการป้องกันเพื่อปกป้องข้อมูลส่วนตัวและทรัพย์สินส่วนบุคคลและองค์กร จึงได้แบ่งหัวข้อการเรียนรู้เป็น 4 ประเด็น ดังนี้

1. ภัยคุกคามทางไซเบอร์ที่ทุกองค์กรต้องระวัง

ประเภทและแนวทางวิธีการป้องกันของภัยคุกคาม

ปัจจุบันภัยไซเบอร์มีการเปลี่ยนแปลงอย่างต่อเนื่อง และพยายามหากลอุบายต่าง ๆ มาเพื่อทำร้ายคนและองค์กรทั่วโลก ปัจจุบันภัยไซเบอร์ที่อาจจะทวีความรุนแรงมากขึ้น ซึ่งควรต้องระมัดระวัง ดังต่อไปนี้ (เอซิส โปรเฟสชั่นนัล เซ็นเตอร์, 2566ก)

1.1 การโจมตีแบบ Ransomware เป็นปัญหาที่ยังคงรุนแรงและมีผลกระทบมากต่อองค์กรและบุคคลทั่วไปได้อย่างต่อเนื่อง โดยลักษณะของ Ransomware คือ โปรแกรมคอมพิวเตอร์ที่ทำการเข้ารหัสข้อมูลบนเครื่องคอมพิวเตอร์ของเหยื่อ แล้วขอเงินค่าไถ่ในรูปแบบของเงินที่เป็นบิทคอยน์หรือเงินสกุลที่ไม่สามารถติดตามได้ง่าย โดยที่เหยื่อจะไม่สามารถเข้าถึงข้อมูลของตัวเองได้จนกว่าจะจ่ายเงินที่ถูกขอไว้ โดยในปี 2024 ลักษณะการโจมตี Ransomware มีการพัฒนาและปรับปรุงขึ้นอย่างต่อเนื่อง เทคนิคต่าง ๆ ที่มักพบได้ ดังนี้

<u>รูปแบบของการโจมตี</u>

1) **การเข้าถึงผ่านช่องโหว่ในระบบ** การโจมตีบางครั้งสามารถเข้าถึงผ่านช่องโหว่ในซอฟต์แวร์หรือระบบปฏิบัติการที่ไม่ได้รับการอัปเดตหรือมีช่องโหว่ที่ทรัพยากรแก้ไขได้แล้ว ซึ่งทำให้เป็นช่องทางที่น่าสนใจสำหรับผู้โจมตี
2) **การใช้เทคโนโลยีการเข้ารหัสขั้นสูง** จากการโจมตี Ransomware ในปัจจุบันมักใช้เทคโนโลยีการเข้ารหัสขั้นสูงที่ยากต่อการถอดรหัส ทำให้เหยื่อที่ถูกโจมตีมีความยากลำบากในการกู้คืนข้อมูลโดยไม่ต้องจ่ายเงินค่าไถ่
3) **การแฝงตัวเข้าไปในระบบ** ในบางครั้ง Ransomware อาจแฝงตัวเข้าไปในระบบของเหยื่อโดยไม่รู้ตัว เพื่อทำให้การตรวจจับและกำจัดเป็นไปได้ยาก

4) **การเรียกเงินค่าไถ่ที่สูงขึ้น** โดยผู้โจมตีอาจเรียกเงินค่าไถ่ในปริมาณที่สูงขึ้นเมื่อเทียบกับการโจมตีในอดีต นอกจากนี้ยังมีการใช้เทคนิคการเรียกเงินค่าไถ่แบบการจ่ายบางส่วนก่อนเพื่อแสดงความจริงจากการโจมตี

<u>มาตรการป้องกัน</u>

1) **การอัปเดตและแก้ไขช่องโหว่** การอัปเดตซอฟต์แวร์หรือระบบปฏิบัติการเป็นประจำจะช่วยป้องกันช่องโหว่ที่อาจถูกแฮกเกอร์ใช้โจมตีได้
2) **การสำรองข้อมูล** การสำรองข้อมูลอย่างสม่ำเสมอและแยกเก็บไว้ในสถานที่ที่ปลอดภัย เช่น ในคลาวด์ จะช่วยให้สามารถกู้คืนข้อมูลได้โดยไม่ต้องจ่ายค่าไถ่
3) **การใช้เครื่องมือป้องกันภัยขั้นสูง** การใช้เครื่องมือป้องกันภัยที่ใช้เทคโนโลยี AI และการเรียนรู้ของเครื่องในการตรวจจับและป้องกันการโจมตีจะช่วยเพิ่มประสิทธิภาพในการป้องกันภัย
4) **การฝึกอบรมพนักงาน** ในการฝึกอบรมพนักงานให้รู้จักและระมัดระวังต่อภัยคุกคามไซเบอร์ เช่น การหลอกลวงแบบฟิชชิ่ง จะช่วยลดความเสี่ยงในการถูกโจมตี เป็นต้น
5) **การจำกัดการเข้าถึงของผู้ใช้** การให้สิทธิ์การเข้าถึงข้อมูลเฉพาะผู้ที่จำเป็นเท่านั้นจะช่วยลดโอกาสที่มัลแวร์จะกระจายตัวในเครือข่าย

1.2 การขโมยข้อมูลส่วนบุคคลและการรั่วไหลข้อมูล การขโมยข้อมูลส่วนบุคคลและการรั่วไหลของข้อมูลยังคงเป็นภัยคุกคามที่สำคัญต่อทั้งบุคคลและองค์กร โดยมีลักษณะและรูปแบบที่พัฒนามากขึ้น รวมถึงเทคโนโลยีใหม่ ๆ ที่เพิ่มความซับซ้อนในการโจมตีและการป้องกัน ดังนี้

<u>รูปแบบของการขโมยข้อมูลส่วนบุคคล</u>

1) **Phishing และ Social Engineering** เป็นการโจมตีผ่านทางอีเมล ปลอมแปลงเว็บไซต์ และการใช้เทคนิคทางจิตวิทยาเพื่อหลอกลวงเหยื่อให้เปิดเผยข้อมูลส่วนบุคคล เช่น รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูลการเข้าสู่ระบบ
2) **Malware และ Spyware** เป็นซอฟต์แวร์ที่เป็นอันตรายที่ติดตั้งบนอุปกรณ์ของเหยื่อโดยไม่รู้ตัว เพื่อลักลอบเก็บข้อมูลส่วนบุคคล เช่น การกดแป้นพิมพ์ (Keylogging) การบันทึกหน้าจอ หรือการดักจับข้อมูลจากหน่วยความจำ เป็นต้น
3) **การโจมตีผ่านเครือข่ายไร้สาย** เป็นการโจมตีผ่านเครือข่าย Wi-Fi ที่ไม่ปลอดภัย เช่น การดักฟังข้อมูลที่ส่งผ่านเครือข่าย (Sniffing) หรือ การทำ Man-in-the-Middle (MitM) ดักฟังอยู่ระหว่างคอมพิวเตอร์สองเครื่อง และสามารถดักจับการรับส่งข้อมูลต่าง ๆ ได้ เป็นต้น

ลักษณะและรูปแบบของการรั่วไหลของข้อมูล

1) **การเจาะระบบ** การแฮ็กระบบคอมพิวเตอร์หรือเครือข่ายขององค์กรเพื่อเข้าถึงข้อมูลสำคัญ เช่น ข้อมูลลูกค้า ข้อมูลการเงิน หรือข้อมูลสำคัญทางธุรกิจ เป็นต้น
2) **การรั่วไหลจากภายใน** พนักงานหรือผู้มีสิทธิ์เข้าถึงข้อมูลภายในองค์กรที่นำข้อมูลออกไปใช้ผิดวัตถุประสงค์ เช่น การขายข้อมูลให้กับคู่แข่งหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น
3) **การกำจัดข้อมูลไม่ถูกวิธี** การทิ้งอุปกรณ์ที่มีข้อมูลสำคัญโดยไม่ลบข้อมูลอย่างปลอดภัย หรือการขายอุปกรณ์ที่ยังมีข้อมูลส่วนตัวอยู่

ผลกระทบของการขโมยและรั่วไหลของข้อมูล

1) **ความเสียหายทางการเงิน** การสูญเสียเงินจากการขโมยข้อมูลบัตรเครดิตหรือการถูกขโมยเงินในบัญชี รวมถึงค่าใช้จ่ายในการแก้ไขปัญหาและการป้องกันการรั่วไหลในอนาคต
2) **ความเสียหายทางชื่อเสียง** การสูญเสียความไว้วางใจจากลูกค้าหรือคู่ค้า เนื่องจากข้อมูลของพวกเขาถูกขโมยหรือรั่วไหล
3) **ความเสี่ยงทางกฎหมาย** การถูกฟ้องร้องหรือถูกลงโทษตามกฎหมายเนื่องจากการจัดการข้อมูลไม่ดี เช่น การไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

มาตรการป้องกัน

1) **การฝึกอบรมและการให้ความรู้** การให้ความรู้แก่พนักงานและผู้ใช้งานในองค์กรเกี่ยวกับวิธีการป้องกันการขโมยข้อมูล เช่น การหลีกเลี่ยงการเปิดอีเมลที่ไม่รู้จัก การตั้งรหัสผ่านที่แข็งแรง และการใช้เทคนิคการยืนยันตัวตนสองชั้น (2FA) เป็นต้น
2) **การใช้เทคโนโลยีป้องกัน** การใช้ซอฟต์แวร์ป้องกันมัลแวร์และไฟร์วอลล์ การเข้ารหัสข้อมูล และการตรวจสอบและบันทึกกิจกรรมในระบบ (Logging and monitoring)
3) **การจัดการสิทธิ์เข้าถึงข้อมูล** การกำหนดสิทธิ์เข้าถึงข้อมูลให้เหมาะสมกับหน้าที่ของพนักงาน การตรวจสอบสิทธิ์เข้าถึงข้อมูลอย่างสม่ำเสมอ และการใช้หลักการ “Least privilege” ในการจัดการสิทธิ์
4) **การสร้างและทดสอบแผนตอบสนองต่อเหตุการณ์** การสร้างแผนการตอบสนองต่อการรั่วไหลของข้อมูลและการทดสอบแผนดังกล่าวอย่างสม่ำเสมอ เพื่อให้สามารถรับมือกับเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ

1.3 การโจมตีภายในองค์กร (Insider Threats) การกระทำที่เป็นอันตรายหรือเป็นการละเมิดความปลอดภัยขององค์กรที่กระทำโดยบุคคลภายในองค์กรเอง เช่น พนักงาน เจ้าหน้าที่ หรือผู้รับจ้างที่มีสิทธิ์

เข้าถึงข้อมูลและระบบขององค์กร โดยมีวัตถุประสงค์ที่จะขโมย ข้อมูล ทำลายทรัพย์สิน หรือก่อให้เกิดความเสียหายต่อองค์กร โดยแบ่งออกตามประเภท ดังนี้

<u>ประเภทของการโจมตีภายในองค์กร</u>

1) **ความผิดพลาดที่เกิดจากความไม่รู้** การกระทำที่ไม่ตั้งใจให้เกิดความเสียหาย เช่น การคลิกที่ลิงก์ฟิชชิง การเผยแพร่ข้อมูลสำคัญโดยไม่ตั้งใจ
2) **การโจมตีที่ตั้งใจ** การกระทำที่มีเจตนาร้าย เช่น การขโมยข้อมูล การขายข้อมูลสำคัญให้กับคู่แข่ง การทำลายระบบหรือข้อมูล
3) **การใช้สิทธิ์อย่างผิดวัตถุประสงค์** การเข้าถึงข้อมูลหรือระบบที่เกินกว่าที่ได้รับอนุญาต เช่น การดูข้อมูลส่วนบุคคลของเพื่อนร่วมงานโดยไม่มีเหตุผล
4) **การสมรู้ร่วมคิดกับบุคคลภายนอก** การร่วมมือกับบุคคลภายนอกในการโจมตีองค์กร เช่น การให้ข้อมูลหรือช่วยเหลือในการเข้าถึงระบบขององค์กร

<u>มาตรการป้องกัน</u>

1) **การจัดการสิทธิ์การเข้าถึง (Access Control Management)** จำกัดการเข้าถึงข้อมูลและระบบให้เฉพาะบุคคลที่จำเป็นต้องใช้
2) **การตรวจสอบและเฝ้าระวัง (Monitoring and Surveillance)** ใช้ระบบตรวจสอบและเฝ้าระวังการใช้งานข้อมูลและระบบ เพื่อตรวจจับการกระทำที่ผิดปกติ
3) **การฝึกอบรมและการสร้างความตระหนัก (Training and Awareness Programs)** จัดฝึกอบรมให้พนักงานเกี่ยวกับความปลอดภัยไซเบอร์และการป้องกันการโจมตีภายใน
4) **การจัดการเหตุการณ์ (Incident Response Plan)** วางแผนการจัดการเมื่อเกิดเหตุการณ์โจมตี เช่น การแจ้งเตือน การสืบสวน และการฟื้นฟู เป็นต้น
5) **การจัดการกับอุปกรณ์และข้อมูลที่ถูกทิ้ง (Device and Data Disposal Management)** การจัดการอุปกรณ์และข้อมูลที่ไม่ใช้แล้วอย่างปลอดภัย เพื่อป้องกันการนำข้อมูลออกไปใช้งานโดยไม่ได้รับอนุญาต
6) **การใช้เครื่องมือและเทคโนโลยีป้องกัน (Security Tools and Technologies)** ใช้เทคโนโลยีและเครื่องมือในการป้องกัน เช่น ระบบการตรวจจับการบุกรุก (IDS/IPS) และการเข้ารหัสข้อมูล (Data Encryption) เป็นต้น

1.4 การโจมตีเทคโนโลยีด้านความปลอดภัย (Security Technology Attack) การพยายามเจาะระบบหรือทำลายความปลอดภัยของระบบเทคโนโลยีสารสนเทศ อาจเกิดขึ้นในหลายรูปแบบ ตั้งแต่การโจมตีทางไซเบอร์ การเจาะข้อมูลส่วนตัว การกระจายไวรัส และมัลแวร์ จนถึงการโจมตีทางกายภาพ เช่น การขโมยอุปกรณ์คอมพิวเตอร์หรือข้อมูลที่เก็บอยู่ในอุปกรณ์นั้น เป็นต้น โดยมีรูปแบบการโจมตี ดังนี้

<u>รูปแบบของการโจมตี</u>

1) **การโจมตีแบบ Phishing** การหลอกลวงให้ผู้ใช้เปิดเผยข้อมูลส่วนตัวหรือข้อมูลสำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต ผ่านทางอีเมลหรือเว็บไซต์ปลอม เป็นต้น
2) **การโจมตีแบบ Malware** การใช้โปรแกรมที่เป็นอันตราย เช่น ไวรัส เวิร์ม สปายแวร์ เพื่อทำลายระบบหรือขโมยข้อมูล เป็นต้น
3) **การโจมตีแบบ DDoS (Distributed Denial of Service)** การส่งคำขอข้อมูลจำนวนมากไปยังเซิร์ฟเวอร์เพื่อทำให้ระบบล่มและไม่สามารถให้บริการได้
4) **การโจมตีแบบ SQL Injection** การใส่คำสั่ง SQL ที่เป็นอันตรายเข้าไปในช่องกรอกข้อมูลบนเว็บไซต์เพื่อเจาะฐานข้อมูล
5) **การโจมตีแบบ Man-in-the-Middle** การสอดแนมและดักฟังการสื่อสารระหว่างสองฝ่ายเพื่อขโมยข้อมูล

<u>มาตรการป้องกัน</u>

1) **การใช้ Firewall** ติดตั้งและปรับปรุง Firewall เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่หวังดี
2) **การเข้ารหัสข้อมูล (Encryption)** การเข้ารหัสข้อมูลที่สำคัญเพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงได้
3) **การอัพเดทซอฟต์แวร์และแพตช์** ทำการอัพเดทระบบปฏิบัติการและซอฟต์แวร์ต่าง ๆ ให้ทันสมัยอยู่เสมอ เพื่อปิดช่องโหว่ที่อาจถูกใช้ในการโจมตี
4) **การใช้การยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication)** เพิ่มความปลอดภัยในการเข้าสู่ระบบด้วยการยืนยันตัวตนเพิ่มเติม เช่น รหัส OTP ที่ส่งไปยังโทรศัพท์มือถือ เป็นต้น
5) **การอบรมและให้ความรู้แก่ผู้ใช้** การให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และการป้องกันตัวเองจากการโจมตี เช่น การระวังการเปิดอีเมลจากแหล่งที่ไม่รู้จัก เป็นต้น

1.5 การแฮ็กระบบ IoT (Internet of Things) การเจาะเข้าสู่ระบบที่เชื่อมต่ออุปกรณ์ต่าง ๆ ผ่านอินเทอร์เน็ต ซึ่งอาจมีผลกระทบทั้งต่อข้อมูลส่วนบุคคลและการทำงานของอุปกรณ์เหล่านั้น การแฮ็กระบบ IoT สามารถเกิดขึ้นได้หลายรูปแบบ ดังนี้

<u>รูปแบบของการโจมตี</u>

1) **การแฮ็กผ่านเครือข่าย** แฮ็กเกอร์สามารถเจาะเข้าสู่เครือข่ายที่เชื่อมต่ออุปกรณ์ IoT โดยใช้ช่องโหว่ในโปรโตคอลหรือการตั้งค่าเครือข่ายที่ไม่ปลอดภัย

2) **การเจาะเข้าสู่ตัวอุปกรณ์** แฮ็กเกอร์สามารถเจาะเข้าสู่ตัวอุปกรณ์ IoT ได้โดยตรงผ่านการใช้ช่องโหว่ในซอฟต์แวร์หรือเฟิร์มแวร์ของอุปกรณ์
3) **การใช้มัลแวร์** แฮ็กเกอร์สามารถใช้มัลแวร์เพื่อควบคุมหรือทำลายอุปกรณ์ IoT และขโมยข้อมูลที่ส่งผ่านอุปกรณ์เหล่านั้น
4) **การโจมตีแบบ DDoS** แฮ็กเกอร์สามารถใช้เครือข่ายของอุปกรณ์ IoT ที่ถูกแฮ็กเพื่อทำการโจมตีแบบ Distributed Denial of Service (DDoS) กับระบบหรือเว็บไซต์เป้าหมาย

<u>มาตรการป้องกัน</u>

1) **การใช้รหัสผ่านที่แข็งแรงและเปลี่ยนเป็นประจำ** การใช้รหัสผ่านที่มีความซับซ้อนและการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอจะช่วยลดความเสี่ยงในการถูกแฮ็ก
2) **การอัปเดตซอฟต์แวร์และเฟิร์มแวร์** การอัปเดตซอฟต์แวร์และเฟิร์มแวร์ของอุปกรณ์ IoT อย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่อาจเกิดขึ้น
3) **การใช้เครือข่ายที่ปลอดภัย** การตั้งค่าเครือข่ายให้มีความปลอดภัยโดยใช้การเข้ารหัสและการตรวจสอบตัวตน
4) **การแยกเครือข่าย** การแยกเครือข่ายสำหรับอุปกรณ์ IoT ออกจากเครือข่ายหลักขององค์กรหรือบ้านจะช่วยลดความเสี่ยงในการถูกเจาะเข้าสู่ระบบหลัก
5) **การติดตั้งและใช้งานซอฟต์แวร์ป้องกันมัลแวร์** การติดตั้งและใช้งานซอฟต์แวร์ป้องกันมัลแวร์เพื่อป้องกันการโจมตีจากมัลแวร์

1.6 การละเมิดความเป็นส่วนตัวในการใช้งานข้อมูลบนโซเชียลมีเดีย เป็นปัญหาที่สำคัญและซับซ้อน โดยมีลักษณะการละเมิดที่หลากหลายและเกิดขึ้นได้ในหลายรูปแบบ ดังนี้

<u>รูปแบบของการละเมิดความเป็นส่วนตัว</u>

1) **การเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต** บางบริษัทหรือบุคคลอาจเก็บข้อมูลส่วนตัวของผู้ใช้โดยไม่ได้รับอนุญาต เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ และข้อมูลการใช้งานอื่น ๆ เป็นต้น
2) **การใช้ข้อมูลเพื่อการโฆษณาและการตลาด** ข้อมูลส่วนบุคคลมักถูกนำไปใช้ในการสร้างโฆษณาที่ตรงกลุ่มเป้าหมาย ซึ่งบางครั้งทำให้ผู้ใช้รู้สึกว่าเป็นการล่วงล้ำ
3) **การขายข้อมูลให้บุคคลที่สาม** บางครั้งข้อมูลผู้ใช้อาจถูกขายให้กับบริษัทอื่น ๆ โดยที่ผู้ใช้ไม่ทราบหรือไม่ได้ให้ความยินยอม
4) **การโจรกรรมข้อมูลส่วนบุคคล** การแฮ็กหรือการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตเพื่อใช้ในการขโมยข้อมูลประจำตัวหรือกิจกรรมทางอาญาอื่น ๆ

มาตรการป้องกัน

1) **การตั้งค่าความเป็นส่วนตัว** ตรวจสอบและปรับการตั้งค่าความเป็นส่วนตัวในแพลตฟอร์มโซเชียลมีเดียให้เหมาะสมจำกัดการแชร์ข้อมูลส่วนบุคคลเฉพาะกับเพื่อนหรือคนรู้จักเท่านั้น
2) **การใช้รหัสผ่านที่แข็งแรง** ใช้รหัสผ่านที่มีความยาวและมีตัวอักษรหลากหลายประเภท เปลี่ยนรหัสผ่านอย่างสม่ำเสมอและไม่ใช้รหัสผ่านเดียวกันในหลายบัญชี
3) **การใช้การยืนยันตัวตนแบบสองขั้นตอน** เปิดใช้งานการยืนยันตัวตนแบบสองขั้นตอนเพื่อเพิ่มความปลอดภัยในการเข้าถึงบัญชี
4) **การระมัดระวังในการคลิกลิงก์** หลีกเลี่ยงการคลิกลิงก์ที่ไม่น่าเชื่อถือหรือมาจากแหล่งที่ไม่รู้จัก
5) **การใช้ซอฟต์แวร์รักษาความปลอดภัย** ติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัสและมัลแวร์อย่างสม่ำเสมอ
6) **การให้ความรู้และการฝึกอบรม** ให้ความรู้เกี่ยวกับความปลอดภัยในโลกออนไลน์แก่ผู้ใช้ และจัดอบรมเรื่องการป้องกันการละเมิดความเป็นส่วนตัว
7) **การเฝ้าระวังและตรวจสอบการใช้งาน** ตรวจสอบกิจกรรมที่ผิดปกติในบัญชีของตนเองและรายงานเหตุการณ์ที่น่าสงสัยให้กับแพลตฟอร์มโซเชียลมีเดีย
8) **การติดต่อกับผู้ให้บริการโซเชียลมีเดีย** หากพบว่ามีการละเมิดความเป็นส่วนตัว ควรติดต่อผู้ให้บริการโซเชียลมีเดียทันทีเพื่อขอความช่วยเหลือ

1.7 การโจมตีในโลกเสมือน (Virtual World Attacks) เป็นการโจมตีที่เกิดขึ้นในสภาพแวดล้อมที่สร้างขึ้นโดยคอมพิวเตอร์ ซึ่งเป็นโลกเสมือนที่ผู้ใช้งานสามารถเข้าไปทำกิจกรรมต่าง ๆ ได้เช่นเดียวกับในโลกจริง โดยโลกเสมือนนี้สามารถเป็นเกมออนไลน์ โซเชียลมีเดียแบบสามมิติ หรือแพลตฟอร์มที่ใช้เทคโนโลยีเสมือนจริง (VR) และเสมือนผสาน (AR) การโจมตีในโลกเสมือนสามารถมีหลายรูปแบบ ดังนี้

รูปแบบการโจมตีในโลกเสมือน

1) **การแฮ็กบัญชีผู้ใช้ (Account Hacking)** การโจมตีแบบนี้มักจะเกิดขึ้นเมื่อผู้โจมตีสามารถเข้าถึงบัญชีผู้ใช้ในโลกเสมือน และใช้ข้อมูลส่วนตัวหรือทรัพย์สินดิจิทัลของผู้ใช้ไปในทางที่ไม่เหมาะสม
2) **การโจมตีทางด้านสังคม (Social Engineering)** การโจมตีที่ใช้เทคนิคในการหลอกลวงผู้ใช้ให้เปิดเผยข้อมูลสำคัญหรือทำการกระทำบางอย่างที่เป็นประโยชน์ต่อผู้โจมตี

3) **การโจมตีทางเครือข่าย (Network Attacks)** การโจมตีที่มุ่งเป้าไปที่เครือข่ายที่ใช้ในการเชื่อมต่อผู้ใช้งานเข้ากับโลกเสมือน เช่น การโจมตีแบบ DDoS (Distributed Denial of Service) ที่ทำให้เครือข่ายล่มหรือทำงานช้าลง
4) **การโจมตีผ่านมัลแวร์ (Malware Attacks)** การใช้ซอฟต์แวร์ที่เป็นอันตรายเพื่อแทรกซึมเข้ามาในโลกเสมือน เช่น การติดตั้งมัลแวร์ที่สามารถขโมยข้อมูลหรือควบคุมอุปกรณ์ของผู้ใช้
5) **การขโมยทรัพย์สินดิจิทัล (Digital Asset Theft)** การโจรกรรมทรัพย์สินดิจิทัลที่มีค่าในโลกเสมือน เช่น ไอเท็มในเกม หรือสกุลเงินดิจิทัล

<u>มาตรการป้องกัน</u>

1) **การใช้การยืนยันตัวตนสองขั้นตอน (Two-Factor Authentication)** การใช้การยืนยันตัวตนสองขั้นตอนช่วยเพิ่มความปลอดภัยให้กับบัญชีผู้ใช้ โดยต้องมีการยืนยันตัวตนผ่านสองวิธี เช่น รหัสผ่านและการยืนยันผ่านโทรศัพท์มือถือ เป็นต้น
2) **การใช้รหัสผ่านที่แข็งแรงและเปลี่ยนรหัสผ่านบ่อย ๆ** การใช้รหัสผ่านที่ยาวและซับซ้อน และการเปลี่ยนรหัสผ่านเป็นประจำช่วยลดความเสี่ยงในการถูกแฮ็ก
3) **การติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัสและมัลแวร์** การใช้ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่ทันสมัยช่วยป้องกันการโจมตีจากซอฟต์แวร์ที่เป็นอันตราย
4) **การฝึกอบรมด้านความปลอดภัยไซเบอร์** การให้ความรู้และฝึกอบรมด้านความปลอดภัยไซเบอร์แก่ผู้ใช้งาน เพื่อให้รู้เท่าทันและสามารถระวังการโจมตีทางด้านสังคมได้
5) **การสำรองข้อมูลเป็นประจำ** การสำรองข้อมูลช่วยให้สามารถกู้คืนข้อมูลได้ในกรณีที่เกิดการโจมตีหรือข้อมูลสูญหาย
6) **การเฝ้าระวังและตรวจสอบกิจกรรมที่ผิดปกติ** การใช้เครื่องมือในการตรวจสอบและเฝ้าระวังการกระทำที่ผิดปกติในโลกเสมือน เพื่อสามารถตอบสนองและจัดการกับการโจมตีได้ทันท่วงที
7) **การใช้เทคโนโลยีการเข้ารหัส (Encryption)** การเข้ารหัสข้อมูลที่ถูกส่งและเก็บในโลกเสมือนช่วยป้องกันการถูกดักจับและอ่านข้อมูลโดยไม่ได้รับอนุญาต

1.8 การใช้งานเทคโนโลยี AI หรือการใช้งานปัญญาประดิษฐ์ในการโจมตีทางไซเบอร์มีหลายรูปแบบ ซึ่งสามารถแบ่งออกเป็นประเภทต่าง ๆ ตามวิธีการและวัตถุประสงค์ของการโจมตี ดังนี้

<u>รูปแบบการใช้งานเทคโนโลยี AI</u>

1) **การโจมตีโดยใช้ AI เพื่อสร้างมัลแวร์หรือไวรัส** AI สามารถใช้ในการสร้างมัลแวร์ที่ซับซ้อนมากขึ้น ซึ่งสามารถปรับตัวและหลีกเลี่ยงการตรวจจับจากระบบป้องกันได้ มัลแวร์ที่ขับเคลื่อนด้วย AI สามารถเรียนรู้จากการตอบสนองของระบบป้องกันและปรับปรุงตัวเองเพื่อทำให้การโจมตีมีประสิทธิภาพมากขึ้น
2) **การโจมตีโดยใช้ AI เพื่อทำการโจมตีแบบ Phishing** AI สามารถสร้างอีเมลหรือข้อความปลอมที่เหมือนจริงมากขึ้น ทำให้เหยื่อตกหลุมพรางได้ง่าย การใช้ Natural Language Processing (NLP) ในการสร้างข้อความที่เหมือนจริง และการใช้ Machine Learning เพื่อวิเคราะห์ข้อมูลของเหยื่อและปรับแต่งข้อความเพื่อเพิ่มโอกาสในการโจมตี
3) **การโจมตีโดยใช้ AI เพื่อทำการโจมตีแบบ DDoS** AI สามารถใช้ในการวิเคราะห์และปรับปรุงการโจมตีแบบ Distributed Denial of Service (DDoS) เพื่อเพิ่มประสิทธิภาพในการโจมตี AI สามารถใช้ในการสร้าง botnet ที่มีการควบคุมอย่างชาญฉลาด และสามารถเปลี่ยนแปลงพฤติกรรมเพื่อหลีกเลี่ยงการตรวจจับ
4) **การโจมตีโดยใช้ AI เพื่อทำการเจาะข้อมูล (Data Breach)** AI สามารถใช้ในการวิเคราะห์และเจาะระบบเครือข่ายเพื่อค้นหาจุดอ่อนและช่องโหว่ การใช้ Machine Learning ในการวิเคราะห์ปริมาณข้อมูลขนาดใหญ่เพื่อหาข้อมูลที่มีค่าหรือข้อมูลที่อ่อนไหว

<u>มาตรการป้องกัน</u>

1) **การใช้ AI ในการป้องกัน** การใช้ AI เพื่อสร้างระบบตรวจจับและตอบสนองต่อการโจมตีทางไซเบอร์อย่างรวดเร็ว เช่น ระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) ที่ขับเคลื่อนด้วย AI การใช้ Machine Learning ในการวิเคราะห์และเรียนรู้พฤติกรรมของเครือข่ายเพื่อค้นหาการโจมตีที่อาจเกิดขึ้น
2) **การอบรมและการเพิ่มความรู้ให้กับบุคลากร** การฝึกอบรมให้พนักงานมีความรู้เกี่ยวกับการโจมตีทางไซเบอร์และวิธีการป้องกันตนเอง การสร้างความเข้าใจในเรื่องการรักษาความปลอดภัยของข้อมูลและการใช้เทคโนโลยีอย่างปลอดภัย
3) **การอัพเดตและการรักษาความปลอดภัยของระบบ** การอัพเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดเสมอ การใช้มาตรการรักษาความปลอดภัยขั้นสูง

เช่น การใช้การเข้ารหัสข้อมูล การตรวจสอบสิทธิ์หลายขั้นตอน (Multi-Factor Authentication) เป็นต้น

4) **การตรวจสอบและการประเมินความเสี่ยง** การทำการตรวจสอบความเสี่ยงอย่างต่อเนื่องเพื่อหาช่องโหว่และจุดอ่อนของระบบการทำ penetration testing เพื่อทดสอบความปลอดภัยของระบบ

5) **การสร้างนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจน** การสร้างและปรับปรุงนโยบายความปลอดภัยทางไซเบอร์ให้เหมาะสมกับสถานการณ์ปัจจุบัน การกำหนดแนวทางการตอบสนองต่อเหตุการณ์การโจมตีทางไซเบอร์อย่างมีระบบ

2. แนวทางในการปฏิบัติและกรณีศึกษา

การป้องกันตัวเองจากภัยคุกคามทางไซเบอร์ต้องการความรู้และการปฏิบัติตามแนวทางที่เหมาะสม ซึ่งแนวทางปฏิบัติและกรณีศึกษาที่สามารถช่วยลดความเสี่ยงในการตกเป็นเหยื่อจากภัยคุกคามทางไซเบอร์ ดังนี้

<u>แนวทางปฏิบัติ</u>

1) ใช้รหัสผ่านที่แข็งแรงและไม่ซ้ำกัน ใช้รหัสผ่านที่มีความยาวอย่างน้อย 12 ตัวอักษร ประกอบด้วยตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และสัญลักษณ์

2) ใช้รหัสผ่านที่แตกต่างกันสำหรับแต่ละบัญชี ใช้ตัวจัดการรหัสผ่าน (Password Manager) เพื่อจัดการและเก็บรักษารหัสผ่านอย่างปลอดภัย

3) เปิดใช้งานการยืนยันตัวตนสองขั้นตอน (2FA) เพิ่มการยืนยันตัวตนอีกขั้นตอนหนึ่ง เช่น การใช้รหัสที่ส่งไปยังโทรศัพท์มือถือหรือแอปพลิเคชันการยืนยันตัวตน

4) อัพเดตซอฟต์แวร์และระบบปฏิบัติการ ติดตั้งการอัพเดตล่าสุดสำหรับระบบปฏิบัติการ ซอฟต์แวร์ และแอปพลิเคชันที่ใช้งาน เพื่อปิดช่องโหว่ที่อาจถูกโจมตีระวังการคลิกลิงก์และเปิดไฟล์แนบ ตรวจสอบความถูกต้องของลิงก์และไฟล์แนบในอีเมลก่อนคลิก หลีกเลี่ยงการคลิกลิงก์ที่มาจากแหล่งที่ไม่น่าเชื่อถือ

5) ใช้โปรแกรมป้องกันไวรัสและมัลแวร์ ติดตั้งและอัพเดตโปรแกรมป้องกันไวรัสและมัลแวร์เป็นประจำ ใช้โปรแกรมสแกนมัลแวร์เพื่อตรวจสอบและลบภัยคุกคาม

6) สำรองข้อมูลเป็นประจำ สำรองข้อมูลสำคัญเก็บไว้ในที่ปลอดภัย เช่น ฮาร์ดดิสก์ภายนอกหรือบริการคลาวด์ ตรวจสอบการสำรองข้อมูลให้แน่ใจว่าทำงานถูกต้อง

<u>กรณีศึกษา</u>

กรณีศึกษา: การโจมตีฟิชชิ่ง

บริษัท A ได้รับอีเมลที่ดูเหมือนมาจากธนาคารของตน โดยขอให้พนักงานคลิกลิงก์และกรอกข้อมูลเข้าสู่ระบบ

พนักงานคลิกลิงก์และกรอกข้อมูลเข้าไป ทำให้ข้อมูลการเข้าสู่ระบบถูกขโมย

ธนาคารตรวจพบการเข้าสู่ระบบที่น่าสงสัยและทำการแจ้งเตือน

บริษัท A ปรับปรุงนโยบายการฝึกอบรมพนักงานเกี่ยวกับการรับรู้และป้องกันการโจมตีฟิชชิ่ง

กรณีศึกษา: การโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware)

โรงพยาบาล B ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ โดยที่ข้อมูลคนไข้ทั้งหมดถูกเข้ารหัส

โรงพยาบาลไม่สามารถเข้าถึงข้อมูลคนไข้ได้ และผู้โจมตีเรียกร้องค่าไถ่เป็นเงินดิจิตอล

โรงพยาบาลเลือกไม่จ่ายค่าไถ่และทำการกู้คืนข้อมูลจากการสำรองข้อมูลที่มี

โรงพยาบาลเสริมสร้างการป้องกันเพิ่มเติมด้วยการติดตั้งซอฟต์แวร์ป้องกันมัลแวร์และฝึกอบรมพนักงานเรื่องการป้องกันภัยคุกคามไซเบอร์

กรณีศึกษา: การโจมตี DDoS (Distributed Denial of Service)

เว็บไซต์ C ถูกโจมตีด้วย DDoS ทำให้ระบบไม่สามารถให้บริการได้ชั่วคราว

ทีม IT ของเว็บไซต์ทำการตรวจสอบและบล็อกที่อยู่ IP ที่โจมตี

เว็บไซต์ C ปรับปรุงระบบป้องกัน DDoS ด้วยการใช้บริการคลาวด์ที่มีความสามารถในการป้องกันการโจมตี DDoS การป้องกันภัยคุกคามทางไซเบอร์ต้องการความตระหนักรู้และการปฏิบัติตามแนวทางที่เหมาะสมเพื่อให้ระบบและข้อมูลมีความปลอดภัยอยู่เสมอ

3. การใช้เครื่องมือในการทำงานแบบดิจิทัลให้ปลอดภัยจากภัยคุกคามทางไซเบอร์

การทำงานในโลกดิจิทัลในปัจจุบันมีความสะดวกและมีประสิทธิภาพมากขึ้น แต่ก็มีความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นเช่นกัน การป้องกันและทำงานให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ต้องใช้เครื่องมือและวิธีการที่หลากหลาย (เอซิส โปรเฟสชั่นนัล เซ็นเตอร์, 2566ข)

วิธีการ	เครื่องมือ
1. การใช้ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์	• ซอฟต์แวร์ป้องกันไวรัส เช่น Norton, McAfee, Bitdefender ช่วยตรวจจับและลบไวรัสและมัลแวร์ที่อาจทำลายระบบ • ซอฟต์แวร์ป้องกันมัลแวร์ เช่น Malwarebytes ช่วยตรวจจับและป้องกันมัลแวร์ที่อาจไม่ได้ถูกตรวจจับโดยซอฟต์แวร์ป้องกันไวรัส
2. การใช้ไฟร์วอลล์ (Firewall)	• ไฟร์วอลล์ที่ใช้ในระบบปฏิบัติการ เช่น Windows Defender Firewall ช่วยป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตจากภายนอก • ไฟร์วอลล์ฮาร์ดแวร์ ใช้เพื่อป้องกันเครือข่ายโดยรวม เช่น Cisco ASA, Fortinet FortiGate เป็นต้น
3. การใช้ระบบป้องกันการบุกรุก (IDS/IPS)	• ระบบตรวจจับการบุกรุก (IDS) เช่น Snort, Suricata ตรวจสอบและเตือนภัยเมื่อมีการพยายามโจมตี • ระบบป้องกันการบุกรุก (IPS) เช่น Cisco Firepower, Palo Alto Networks ทำการป้องกันและบล็อกการโจมตีที่ตรวจพบ
4. การใช้การเข้ารหัสข้อมูล	• การเข้ารหัสข้อมูลในขณะส่งผ่าน (Encryption in Transit) ใช้โปรโตคอล HTTPS, TLS เพื่อปกป้องข้อมูลขณะส่งผ่านเครือข่าย • การเข้ารหัสข้อมูลในขณะเก็บรักษา (Encryption at Rest) ใช้เทคนิคการเข้ารหัสเพื่อปกป้องข้อมูลที่เก็บอยู่ในฐานข้อมูลหรือสื่อบันทึก
5. การใช้การตรวจสอบสิทธิ์หลายปัจจัย (MFA)	• การตรวจสอบสิทธิ์หลายปัจจัย ใช้หลายวิธีในการยืนยันตัวตน เช่น การใช้รหัสผ่านพร้อมกับรหัส OTP ที่ส่งมาทางโทรศัพท์มือถือ
6. การอัปเดตและแพตช์	• การอัปเดตซอฟต์แวร์ ตรวจสอบและติดตั้งอัปเดตความปลอดภัยอย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่อาจถูกโจมตี • แพตช์ระบบปฏิบัติการและซอฟต์แวร์ ทำการติดตั้งแพตช์ที่ออกมาใหม่เพื่อแก้ไขปัญหาความปลอดภัย
7. การจัดการสิทธิ์การเข้าถึง (Access Control)	• สิทธิ์การเข้าถึงที่ถูกต้อง ให้สิทธิ์การเข้าถึงข้อมูลและระบบเฉพาะผู้ที่จำเป็นเท่านั้น • การตรวจสอบสิทธิ์การเข้าถึง ตรวจสอบและปรับปรุงสิทธิ์การเข้าถึงตามความจำเป็น

วิธีการ	เครื่องมือ
8. การฝึกอบรมและการศึกษา	• การฝึกอบรมพนักงาน ให้พนักงานมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกัน เช่น การระวังฟิชชิ่ง (Phishing) • การทดสอบความปลอดภัย การทำการทดสอบการเจาะระบบ (Penetration Testing) เพื่อประเมินความปลอดภัยของระบบ
9. การสำรองข้อมูล (Backup)	• การสำรองข้อมูลอย่างสม่ำเสมอ ทำการสำรองข้อมูลที่สำคัญเป็นประจำและเก็บสำรองไว้ในสถานที่ที่ปลอดภัย • การทดสอบการกู้คืนข้อมูล ตรวจสอบให้แน่ใจว่าข้อมูลสำรองสามารถกู้คืนได้ในกรณีที่เกิดปัญหา

การใช้เครื่องมือและวิธีการเหล่านี้ช่วยให้ระบบดิจิทัลของคุณปลอดภัยจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยรวมแล้ว การรักษาความปลอดภัยทางไซเบอร์เป็นกระบวนการที่ต้องใช้ความพยายามและการดูแลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าข้อมูลและระบบของคุณปลอดภัยจากการโจมตีต่าง ๆ

4. การตอบสนองต่ออุบัติการณ์ (Incident Responses)

การตอบสนองต่ออุบัติการณ์ (Incident Response) เป็นกระบวนการที่สำคัญในการจัดการกับภัยคุกคามทางไซเบอร์ เพื่อช่วยป้องกัน ลดผลกระทบ และฟื้นฟูระบบหลังจากเหตุการณ์การละเมิดความปลอดภัยหรือการโจมตีทางไซเบอร์ กระบวนการนี้ประกอบด้วยหลายขั้นตอนหลักที่สำคัญ ได้แก่ (ไซเบอร์ อีลีท, 2566)

กระบวนการ	รายละเอียด
1. การเตรียมการ (Preparation)	• การวางแผน จัดทำแผนตอบสนองต่ออุบัติการณ์ที่ชัดเจน รวมถึงการระบุทีมตอบสนอง การกำหนดหน้าที่ และการจัดเตรียมเครื่องมือและทรัพยากรที่จำเป็น • การฝึกอบรม ฝึกอบรมทีมตอบสนองและพนักงานทั่วไปให้มีความรู้และทักษะในการจัดการกับเหตุการณ์ทางไซเบอร์ • การทดสอบ ทดสอบแผนการตอบสนองเพื่อให้แน่ใจว่าสามารถทำงานได้อย่างมีประสิทธิภาพ
2. การตรวจจับและการรายงาน (Detection and Reporting)	• การตรวจจับ ใช้เครื่องมือและเทคนิคในการตรวจจับการละเมิดหรือกิจกรรมที่ผิดปกติ เช่น การใช้ซอฟต์แวร์ตรวจจับภัยคุกคาม (IDS/IPS) หรือระบบการจัดการบันทึก (SIEM) • การรายงาน แจ้งเตือนทีมตอบสนองเกี่ยวกับเหตุการณ์ที่เกิดขึ้นอย่างรวดเร็วและถูกต้อง

กระบวนการ	รายละเอียด
3. การตอบสนอง (Containment, Eradication, and Recovery)	• การควบคุม (Containment) ดำเนินการเพื่อจำกัดการแพร่กระจายของภัยคุกคามและป้องกันไม่ให้เหตุการณ์เกิดขึ้นอีกในระยะสั้นและระยะยาว • การกำจัด (Eradication) กำจัดสาเหตุของภัยคุกคามออกจากระบบ เช่น การลบมัลแวร์หรือการปิดช่องโหว่ที่ถูกใช้ในการโจมตี • การฟื้นฟู (Recovery) ฟื้นฟูระบบให้กลับสู่สถานะปกติ ตรวจสอบให้แน่ใจว่าระบบทำงานได้อย่างถูกต้อง และพิจารณาการตรวจสอบและการแก้ไขหลังการฟื้นฟู
4. การเรียนรู้และการปรับปรุง (Lessons Learned)	• การวิเคราะห์ วิเคราะห์เหตุการณ์เพื่อเข้าใจสิ่งที่เกิดขึ้นและเหตุผลที่เป็นสาเหตุ • การรายงาน สร้างรายงานสรุปเหตุการณ์พร้อมกับข้อเสนอแนะสำหรับการปรับปรุงในอนาคต • การปรับปรุง ปรับปรุงแผนการตอบสนองและมาตรการด้านความปลอดภัยเพื่อป้องกันเหตุการณ์ในอนาคต

การตอบสนองต่ออุบัติการณ์ที่มีประสิทธิภาพสามารถช่วยลดผลกระทบของการโจมตีทางไซเบอร์และช่วยให้องค์กรฟื้นฟูได้อย่างรวดเร็วและปลอดภัยมากขึ้น

แนวทางการปฏิบัติพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

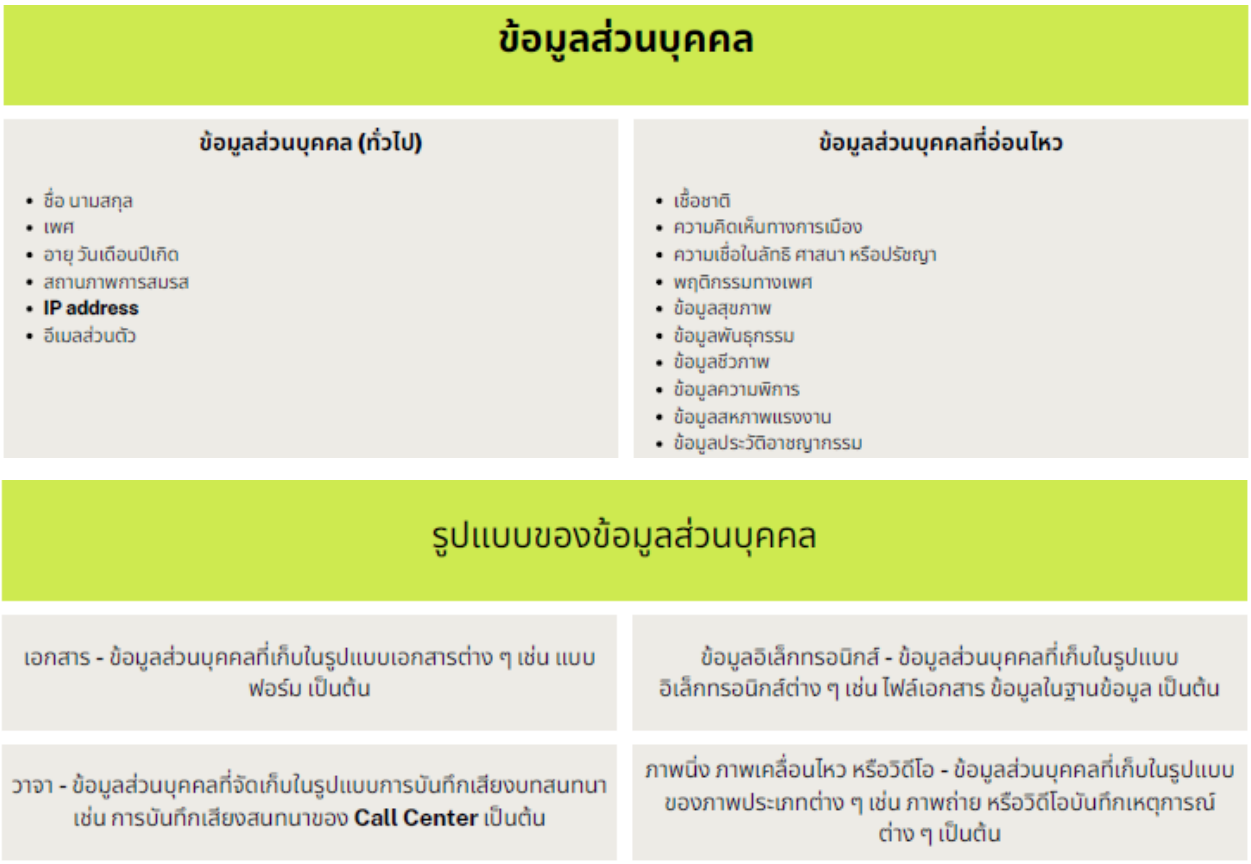
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นกฎหมายที่ถูกสร้างมาเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล และเพื่อสร้างความปลอดภัยให้แก่เจ้าของข้อมูล โดยผู้เป็นเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่สำคัญ คือ สิทธิการรับทราบและยิมยอมการเก็บข้อมูลส่วนตัว สิทธิได้รับการแจ้งให้ทราบ สิทธิในการขอเข้าถึงข้อมูลส่วนตัว สิทธิเคลื่อนย้ายโอนข้อมูล สิทธิคัดค้าน สิทธิเพิกถอนการเก็บและนำข้อมูลไปใช้ สิทธิขอให้ระงับการใช้ข้อมูล สิทธิขอแก้ไขข้อมูล และสิทธิขอให้ลบหรือทำลายข้อมูลส่วนตัว โดยมีแนวทางปฏิบัติตามมาตรการด้านความปลอดภัยของข้อมูลส่วนบุคคล ดังต่อไปนี้ (อรรถศิษฐ์ พัฒนะศิริ, 2566)

แนวทางการปฏิบัติของสถาบันการศึกษาแหล่งข้อมูล

PDPA คือ กฎหมายที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล โดยห้ามมิให้ผู้อื่นนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในด้านใดด้านหนึ่งโดยที่เจ้าของข้อมูลไม่ยินยอม

ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ ถึงแก่กรรมโดยเฉพาะ

การคุ้มครองข้อมูลส่วนบุคคล คือ 1. สร้างความเชื่อมั่น (Trust) 2. ยกระดับการธรรมาภิบาลข้อมูล (Better data governance) และ 3. ยกระดับสู่มาตรฐานสากล (Connecting with global standards)



ผู้ที่เกี่ยวข้องกับ PDPA

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทาให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคล หรือ นิติบุคคล ซึ่งมีอำนาจหน้าที่ ตัดสินใจ และควบคุมเกี่ยวกับวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล”

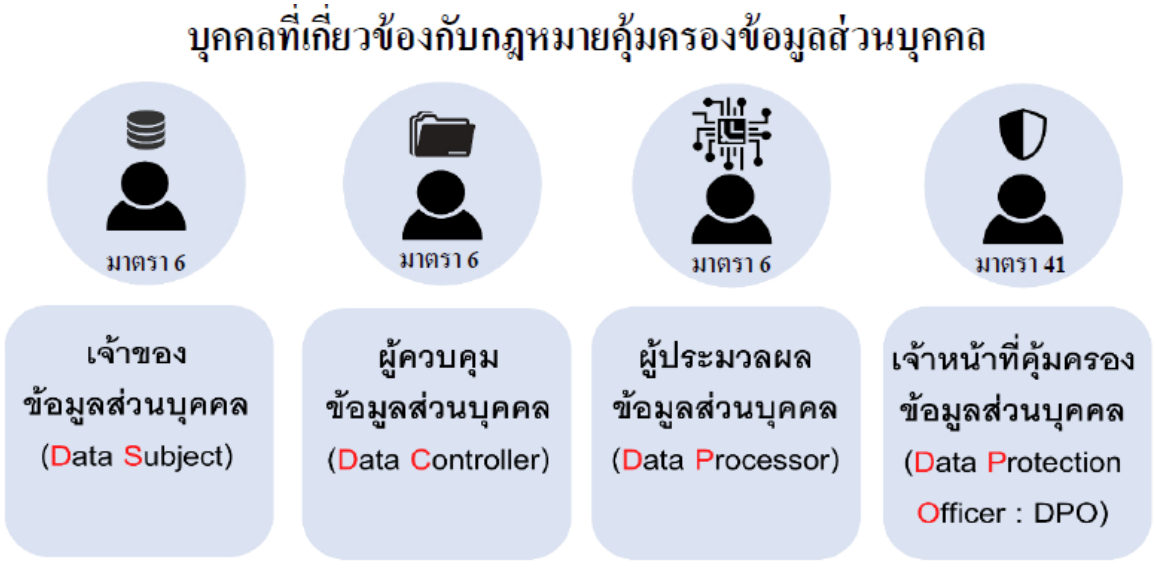
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

<u>การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล</u>

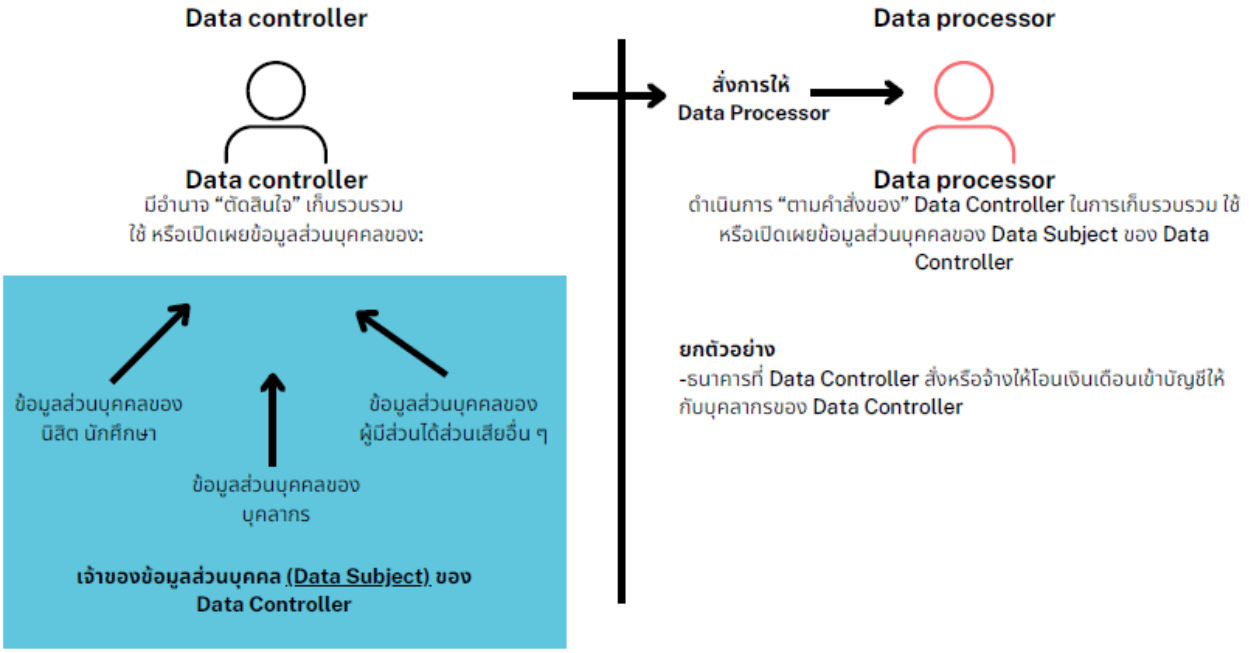
(1) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(2) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

(3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 (อุดมธิปก ไพรเกษตร, 2567)



หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล



หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ตามกฎหมาย PDPA

1	แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล Privacy notice (ม.23)	Lawful and transparency
2	มีความชอบธรรมในการประมวลผล Lawful basis (ม.24, 26)	
3	เก็บ ใช้ เปิดเผยเท่าที่จำเป็นและตามวัตถุประสงค์ Purpose limitation (ม.22, 27)	Only collect, use, and share what's necessary
4	ทำข้อมูลส่วนบุคคลให้ถูกต้อง Data accuracy (ม.35)	
5	ป้องกันมิให้บุคคลหรือองค์กรอื่นที่รับข้อมูลจาก Data controller นำข้อมูลไปใช้หรือเปิดเผยโดยมิชอบ Preventing others from unlawful use or disclosure: (ม.37(2))	Security
6	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม Appropriate security (ม.37 (1))	
7	แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้กำกับดูแลทราบภายใน 72 ชั่วโมง Breach notification: (ม.37 (4))	
8	มีการตรวจสอบเพื่อลบข้อมูลที่ไม่จำเป็น และมีการจัดการสิทธิเจ้าของข้อมูลส่วนบุคคล Data check and Data subject rights management: (ม.37(3))	Governance and management
9	ทำบันทึกรายการกิจกรรมที่ใช้ข้อมูลส่วนบุคคล Records of Processing Activity (RoPA) (ม.39)	
10	แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO (ม.41)	

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ตามกฎหมาย PDPA

1	ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล
2	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
3	แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ **Data controller** ทราบ
4	ทำบันทึกรายการการประมวลผลข้อมูล **(RoPA)** (ถ้าเป็นไปตามเกณฑ์ต้องจัดทำ)
5	แต่งตั้ง **DPO** (ถ้าเป็นไปตามเกณฑ์ต้องแต่งตั้ง)

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามกฎหมาย PDPA

DATA PROTECTION OFFICER (DPO)

หน่วยงานใดต้องจัดให้มี DPO

1 - หน่วยงานของรัฐ

2 - หน่วยงานที่การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด

3 - หน่วยงานที่มีกิจกรรมหลักเป็นการเก็บ รวบรวม ใช้ หรือเปิดเผย **Sensitive Personal Data**

หน้าที่ของ DPO

1 - ให้คำแนะนำ **Data controller**

2 - ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล

3 - ประสานงานและให้ความร่วมมือกับสำนักงานฯ

4 - รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

หลักการของ PDPA

หลักการของ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

1	**Lawful Processing and Transparency** มีความชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลและมีความโปร่งใส
2	**Necessity and Purpose Limitation** ใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์และเท่าที่จำเป็น
3	**Data Accuracy** ต้องทำข้อมูลส่วนบุคคลให้ถูกต้องและเป็นปัจจุบัน
4	**Limitation of Storage** มีระยะเวลาในการเก็บข้อมูลส่วนบุคคลที่แน่นอน
5	**Security** มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
6	เคารพสิทธิของ **Data Subject** ดำเนินการตามคำร้องขอของ **Data Subject** ตามขอบเขตที่กฎหมายกำหนด

ข้อยกเว้นของ PDPA ตาม พรบ.

1	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
2	การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
3	บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น
4	สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
5	การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา
6	การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

หลักการขอความยินยอมตาม PDPA

ฐานความยินยอม (Consent)

เจ้าของข้อมูลยินยอมให้ใช้ข้อมูลส่วนบุคคล (ไม่ว่าจะเก็บรวบรวม ใช้ หรือเปิดเผย) (ม.**24** และ ม.**26**)
- มาตรา **24** (การยินยอมในกรณีทั่วไป)
- มาตรา **26** (การยินยอมโดยชัดแจ้ง ในกรณีใช้ข้อมูลอ่อนไหว)

หลักการใช้

PDPA ม.**19** กำหนดให้
- การขอความยินยอมต้องแจ้งให้ชัดเจนว่าขอไปเพื่ออะไร
- การขอความยินยอมต้องให้อิสระกับเจ้าของข้อมูลในการให้หรือไม่ให้ความยินยอม
- การขอความยินยอม ต้องแยกส่วนการขอความยินยอมจากส่วนอื่นโดยชัดเจน
- ถ้าการถอนความยินยอมกระทบการใช้งานในเรื่องใด ให้แจ้งผลกระทบนั้นกับเจ้าของข้อมูลส่วนบุคคลด้วย

การขอความยินยอมจากเจ้าของข้อมูลกรณีพิเศษ

A

การขอความยินยอมผู้เยาว์

ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา **22** มาตรา **23** หรือมาตรา **24** แห่งประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อานาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

B

การขอความยินยอมผู้ไร้ความสามารถ

ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

C

การขอความยินยอมผู้เสมือนไร้ความสามารถ

ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

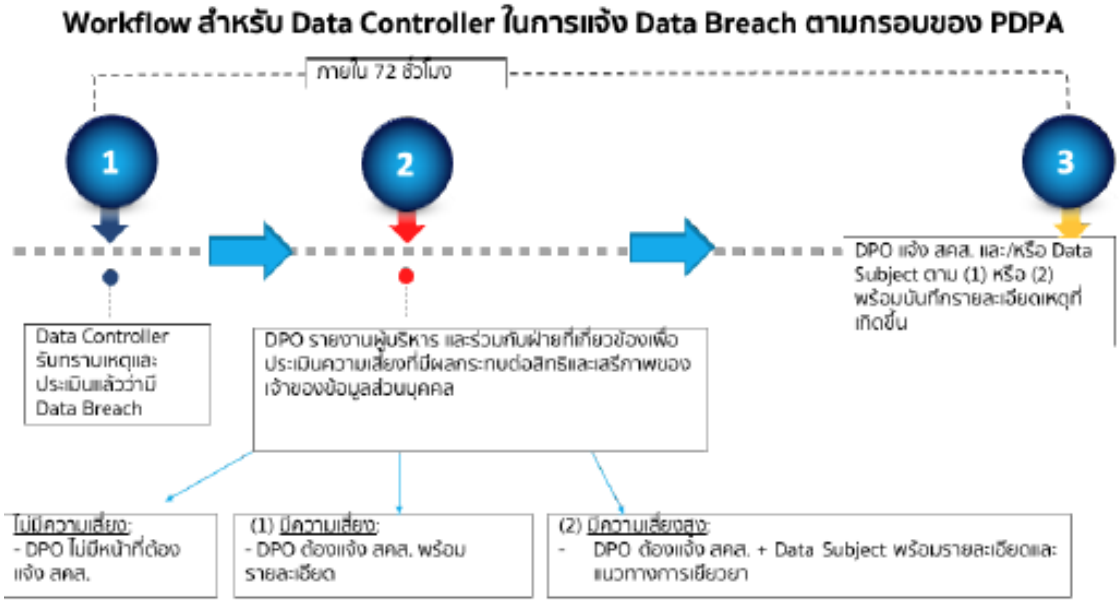
การจัดการกับข้อมูลส่วนบุคคลเดิม

1. ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลต่อไปได้ตามวัตถุประสงค์เดิม
2. ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย
3. การเปิดเผยและดำเนินการอื่นที่มิใช่การเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ให้เป็นไปตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นี้

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1	สิทธิในการเพิกถอนความยินยอมที่เคยให้ไว้ เมื่อใดก็ได้
2	สิทธิขอเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล (Right of access)
3	สิทธิในการขอแก้ไขให้ข้อมูลส่วนบุคคลมีความถูกต้อง (Right to Rectification)
4	สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure)
5	สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restrict processing)
6	สิทธิในการขอให้โอนข้อมูลส่วนบุคคลไปยัง data controller อื่น (Right to data portability)
7	สิทธิขอคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)

สิ่งที่องค์กรต้องดำเนินการเพื่อให้เป็นไปตาม PDPA



การจัดการความปลอดภัยของข้อมูลและการตระหนักถึงความเป็นส่วนตัว

หลักการสำคัญของ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายอื่น ๆ ที่เกี่ยวกับคุ้มครองข้อมูลส่วนบุคคล เพื่อนำมาใช้เป็นแนวการปฏิบัติตาม และจัดการความปลอดภัยของข้อมูลส่วนบุคคลและการตระหนักถึงความเป็นส่วนตัว ความสอดคล้องของการคุ้มครองข้อมูลส่วนบุคคล และการปฏิบัติงานให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล สำหรับมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี (อุดมธิปก ไพรเกษตร, 2567)

การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประกอบด้วย 1. ฐานกฎหมายของการประมวลผลข้อมูลส่วนบุคคล 2. สิทธิของเจ้าของข้อมูลส่วนบุคคล และ 3. การคุ้มครองข้อมูลส่วนบุคคล ซึ่งมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีมีกฎหมายและประเภทข้อมูลส่วนบุคคลที่เกี่ยวข้องและบังคับใช้ ดังนี้

กฎหมาย	การบังคับใช้
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	**บทนำ** ม1 - ม7 **หมวด 1** คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ม8 - ม18 **หมวด 2** การคุ้มครองข้อมูลส่วนบุคคล • ส่วนที่ 1 บททั่วไป ม19 - ม21 • ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล ม22 - ม26 • ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ม27 - ม29 **หมวด 3** สิทธิของเจ้าของข้อมูลส่วนบุคคล ม30 - ม42 **หมวด 4** สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ม43 - ม70 **หมวด 5** การร้องเรียน ม71 - ม76 **หมวด 7** บทกำหนดโทษ • ส่วนที่ 1 โทษอาญา ม79 - ม81 • ส่วนที่ 2 โทษทางปกครอง ม82 - ม90 **บทเฉพาะกาล** ม91 - ม96

การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

กฎหมาย	มาตรา
รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560	**มาตรา 32** “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนาข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”
ประมวลกฎหมายแพ่งและพาณิชย์	**มาตรา 420** “ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น”

กฎหมายที่เกี่ยวข้องกับมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ดังนี้

กฎหมาย	พระราชบัญญัติ
กฎหมายเกี่ยวกับสถาบันอุดมศึกษา	• พระราชบัญญัติระเบียบบริหารราชการกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม พ.ศ. 2562 • พระราชบัญญัติการอุดมศึกษา พ.ศ. 2562 • พระราชบัญญัติสภานโยบายการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม พ.ศ. 2562 • พระราชบัญญัติระเบียบข้าราชการพลเรือนในสถาบันอุดมศึกษา พ.ศ. 2547 • พระราชบัญญัติการบริหารส่วนงานภายในของสถาบันอุดมศึกษา พ.ศ. 2550 • กฎหมายเกี่ยวกับมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
กฎหมายเฉพาะมหาวิทยาลัยเทคโนโลยีราชมงคล	• พระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. 2548 • พระราชกฤษฎีกาว่าด้วยปริญญาในสาขาวิชา อักษรย่อสำหรับสาขาวิชาครุยวิทยฐานะ เข็มวิทยฐานะ และครุยประจำตำแหน่งของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี พ.ศ. 2553 • กฎกระทรวงจัดตั้งส่วนราชการในมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีกระทรวงศึกษาธิการ พ.ศ. 2549

กฎหมาย	พระราชบัญญัติ
	• ประกาศกระทรวงศึกษาธิการ เรื่อง การแบ่งส่วนราชการในมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี พ.ศ. 2550

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

กฎหมาย	มาตรา
ข้อมูลข่าวสารส่วนบุคคล	**มาตรา 4** “ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”

ประเภทข้อมูลของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ข้อมูลของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี คือ ข้อมูลข่าวสารของราชการ ได้แก่

ประเภทข้อมูล	รายละเอียด
ข้อมูลที่อยู่ในมหาวิทยาลัย	1. ข้อมูลเฉพาะของมหาวิทยาลัย 2. ข้อมูลสาธารณะ 3. ข้อมูลส่วนบุคคล • ข้อมูลข่าวสารส่วนบุคคล
ข้อมูลส่วนบุคคลของมหาวิทยาลัย	1. บุคลากร ได้แก่ • ผู้บริหาร คณาจารย์ นักวิจัย เจ้าหน้าที่ พนักงาน ลูกจ้าง • อาจารย์พิเศษ วิทยากร • อดีตผู้สมัคร • อดีตบุคลากร • กรรมการ..... 2. นิสิต 3. นักเรียนสาธิต

ประเภทข้อมูล	รายละเอียด
	4. ศิษย์เก่า 5. ผู้ปกครอง 6. อดีตผู้ปกครอง 7. ผู้สมัคร และผู้เข้าอบรม 8. อดีตผู้เข้าอบรม 9. ผู้ตอบแบบสอบถาม 10. ผู้ที่เป็นกลุ่มตัวอย่างในการวิจัย 11. ผู้ป่วยในและผู้ป่วยนอก 12. ผู้เข้าพักโรงแรมของมหาวิทยาลัย 13. ผู้เสนอขายและผู้ขาย 14. ผู้เสนอซื้อ / ผู้เสนอเช่า / ผู้ซื้อ / ผู้เช่า 15. ผู้จะเข้าร่วมหรือผู้เข้าร่วมกิจกรรมต่าง ๆ ของมหาวิทยาลัย 16. ผู้มาติดต่อ 17. อดีตของ 7-14 18. อื่น ๆ
บุคลากรของมหาวิทยาลัยในกฎหมายคุ้มครองข้อมูลส่วนบุคคล	1. เป็นเจ้าของข้อมูลส่วนบุคคล 2. ปฏิบัติตามที่องค์กรสั่ง หรือมอบหมายให้ทำเพื่อประโยชน์ขององค์กร 3. ปฏิบัตินอกเหนือจากที่องค์กรสั่ง หรือมอบหมายให้ทำเพื่อประโยชน์องค์กร 4. ปฏิบัตินอกเหนือจากที่องค์กรสั่ง หรือมอบหมายให้ทำเพื่อประโยชน์ตนเอง 5. ทำในนามส่วนตัว เพื่อประโยชน์ตนเอง

มาตรา 5 : PDPA บังคับใช้กับใคร

1. ผู้ควบคุมฯ หรือ ผู้ประมวลผลฯ “อยู่ในประเทศไทย” ไม่ว่าการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล จะกระทำ “ใน” หรือ “นอก” ประเทศไทยก็ตาม

2. ผู้ควบคุมฯ หรือ ผู้ประมวลผลฯ “อยู่นอกประเทศไทย” แต่ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลฯ ของเจ้าของข้อมูลฯ ซึ่ง อยู่ในราชอาณาจักร.... เมื่อเป็นกิจกรรม ดังต่อไปนี้

- มีการเสนอสินค้าหรือบริการ ให้แก่เจ้าของข้อมูล (ไม่ว่าจะมีการชา ระเงินหรือไม่)
- มีการเฝ้าติดตามพฤติกรรม ของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้น ในราชอาณาจักร

การปฏิบัติตาม PDPA

สิ่งที่ควรรู้เกี่ยวกับ PDPA ซึ่งได้ครอบคลุม 4 เรื่องสำคัญ ได้แก่

1. หลักการคุ้มครองข้อมูลส่วนบุคคล

1) ชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness, and Transparency)
   - ข้อมูลส่วนบุคคลจะต้องได้รับการประมวลผลอย่างถูกต้องตามกฎหมาย เป็นธรรม และอย่างโปร่งใสต่อเจ้าของข้อมูล
   - การประมวลผลข้อมูลส่วนบุคคลจะเกิดขึ้นได้กรณีเดียวเท่านั้น คือ เมื่อมีฐานทางกฎหมายรองรับ และเจ้าของข้อมูลจะต้องรู้ว่าข้อมูลส่วนตัวของตนถูกนาไปใช้อย่างไร
   - การประมวลผลข้อมูลส่วนบุคคลควรโปร่งใสต่อบุคคลธรรมดาที่ข้อมูลส่วนบุคคลนั้นได้ถูกรวบรวม ถูกใช้ประโยชน์ หรือประมวลผลในรูปแบบอื่น ๆ และรวมถึงขอบเขตที่ข้อมูลส่วนบุคคลถูกประมวลผลหรืออาจถูกประมวลผลต่อไป
2) การจำกัดวัตถุประสงค์ (Purpose Limitation)
   - ข้อมูลส่วนบุคคลจะถูกรวบรวมเพื่อวัตถุประสงค์ที่ระบุไว้ชัดเจนและถูกต้องตามกฎหมาย และจะต้องไม่ดำเนินการต่อจากนั้นในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว
   - เมื่อแชร์ข้อมูลส่วนบุคคลให้กับผู้อื่น ผู้แชร์ข้อมูลย่อมคาดหวังว่าข้อมูลจะถูกใช้ตามวัตถุประสงค์ การระบุวัตถุประสงค์ของการใช้ข้อมูลในเบื้องต้นเป็นสิ่งจำเป็นสำหรับการบังคับใช้กฎหมายคุ้มครองข้อมูล
   - วัตถุประสงค์เฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลต้องมีความชัดเจนและถูกต้องตามกฎหมาย และสิ้นสุดตามกำหนดของการรวบรวมข้อมูลส่วนบุคคล
   - หลักการของการจำกัดวัตถุประสงค์เป็นการป้องกันไม่ให้ข้อมูลส่วนบุคคลถูกนำไปดำเนินการอย่างอื่นนอกเหนือจากวัตถุประสงค์ของการรวบรวมข้อมูลในเบื้องต้น
3) ใช้เท่าที่จำเป็นเกี่ยวข้อง (Data Minimization)
   - ผู้ควบคุมข้อมูลต้องสามารถอธิบายอย่างชัดเจน และแสดงเหตุผลอันสมควรถึงความต้องการรวบรวมและเก็บข้อมูลส่วนบุคคล ทั้งนี้ต้องสอดคล้องกับวัตถุประสงค์ที่กำหนดไว้
   - การเก็บข้อมูลส่วนบุคคล ควรจะทำเท่าที่จำเป็นเกี่ยวข้องและจำกัดเฉพาะความจำเป็นตามวัตถุประสงค์ที่จะนำไปประมวลผล
   - ผู้ควบคุมข้อมูลต้องไม่รวบรวมข้อมูลแบบเผื่อไว้สำหรับวัตถุประสงค์จำเป็นที่อาจเกิดขึ้นในอนาคต ข้อมูลส่วนบุคคลควรถูกประมวลผลเพียงเพราะว่าวัตถุประสงค์ที่ต้องทำการประมวลผลไม่สามารถบรรลุด้วยวิธีการอื่น

4) ความแม่นยำ ถูกต้อง เป็นปัจจุบัน (Accuracy)
   - การประมวลผลข้อมูลส่วนบุคคล ควรดำเนินไปในแต่ละขั้นตอนอย่างเหมาะสม เพื่อให้แน่ใจว่าข้อมูลที่ไม่ถูกต้องจะได้รับการแก้ไข หรือถูกลบ
   - ข้อมูลส่วนบุคคลจะต้องถูกต้องและปรับปรุงให้ทันสมัยตามความจำเป็น โดยแต่ละขั้นตอนต้องดำเนินการอย่างเหมาะสมเพื่อให้แน่ใจว่าข้อมูลที่ไม่ถูกต้องตามวัตถุประสงค์ของการประมวลผล ต้องได้รับการแก้ไข หรือถูกลบโดยทันที
   - ข้อมูลส่วนบุคคลที่จะถูกนำไปประมวลผลสำหรับวัตถุประสงค์ใดโดยเฉพาะ จะต้องเป็นข้อมูลที่ถูกต้องและเป็นปัจจุบัน ถ้าข้อมูลที่นำไปใช้สำหรับวัตถุประสงค์นั้นต้องการความเป็นปัจจุบัน เพื่อเป็นไปตามหลักการ"ความแม่นยำ"นั้น ทำให้ต้องมีเก็บข้อมูลที่เป็นปัจจุบัน ซึ่งกรณีนี้ผู้ควบคุมข้อมูลจะต้องรับประกันว่ามีระบบสำหรับการแก้ไขและลบข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่เป็นปัจจุบัน
5) การจำกัดระยะเวลาการจัดเก็บข้อมูล ไม่เก็บนานเกินความจำเป็น (Storage Limitation)
   - ข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาในรูปแบบที่อนุญาตให้การระบุตัวตนของเจ้าของข้อมูลไม่นานกว่าความจำเป็นสำหรับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลนั้น
   - จะต้องมีการรับประกันว่าช่วงเวลาในการจัดเก็บข้อมูลส่วนบุคคลนั้นจะต้องเป็นเวลาที่สั้นที่สุด เพื่อรับประกันว่าข้อมูลส่วนบุคคลนั้นจะไม่ถูกนำไปใช้เกินความจำเป็น และผู้ควบคุมข้อมูลควรเป็นผู้กำหนดระยะเวลาที่จำกัดนี้สำหรับการลบข้อมูลหรือการทบทวนอย่างสม่ำเสมอ
   - ผู้ควบคุมข้อมูลจำเป็นต้อง กำหนดระยะเวลาที่จำเป็นสำหรับการเก็บรักษาข้อมูลส่วนบุคคล ทบทวนข้อมูลส่วนบุคคลที่เก็บไว้อย่างสม่ำเสมอ ลบข้อมูลส่วนบุคคลที่วัตถุประสงค์ของการจัดเก็บไม่สมเหตุสมผลอีกต่อไปออก
6) ความสมบูรณ์ และเก็บรักษาเป็นความลับ (Integrity and Confidentiality)
   - ต้องพยายามเก็บรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัยตลอดเวลา มีการป้องกันการประมวลผลที่ไม่ได้รับอนุญาต หรือไม่ชอบด้วยกฎหมายทำให้ข้อมูลสูญหาย ถูกทำลายหรือเสียหายโดยบังเอิญ
   - ทั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องกำหนดมาตรการทางเทคนิค และการบริหารจัดการองค์กรที่เหมาะสม เพื่อให้มั่นใจได้ว่าระดับของระบบรักษาความปลอดภัยของข้อมูลสามารถรับมือกับความเสี่ยงได้
   - การคุ้มครองข้อมูลส่วนบุคคลให้ปลอดภัยจากการประมวลผลโดยไม่ชอบหรืออย่างไม่ถูกต้องตามกฎหมายเป็นสิ่งที่จะต้องพิจารณาด้วยมุมมองหลาย ๆ ด้าน
7) ความรับผิดชอบ (Accountability)
   - ผู้ควบคุมข้อมูลต้องมีความรับผิดชอบ ที่จะต้องปฏิบัติตามหลักการแห่งการประมวลผลข้อมูลโดยมีมาตรการเหมาะสมและมีประสิทธิภาพ และต้องสามารถแสดงให้เห็นถึงมาตรการที่ชัดแจ้งที่ปฏิบัติเมื่อมีการร้องขอ

2. ฐานทางกฎหมายของการประมวลผลข้อมูลส่วนบุคคลตาม PDPA

1) ฐานการปฏิบัติตามสัญญา (Contract)
   - เฉพาะข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอ่อนไหวไม่สามารถใช้ฐานสัญญาได้
   - เมื่อใช้ฐานสัญญาแล้ว ไม่ต้องขอความยินยอม
   - เมื่อไม่ต้องขอความยินยอม จึงไม่อาจถอนความยินยอมได้
   - จำกัดเฉพาะข้อมูลของเจ้าของข้อมูลผู้เป็นคู่สัญญาเท่านั้น
   - ภายใต้ขอบเขตของสัญญาตามที่ตกลงกัน
2) ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)
   - ปฏิบัติตามกฎหมาย ไม่ต้องขอความยินยอม
   - เป็นการดำเนินการบทบัญญัติแห่งกฎหมาย
   - เป็นการทำหน้าที่ตามคำสั่งของหน่วยงานรัฐที่มีอำนาจ
3) ฐานการป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest)
4) ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public Interest)
5) ฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล (Legitimate Interest)
6) ฐานความยินยอม มาตรา 19, 24
   - ลักษณะการให้ความยินยอมที่ชอบด้วยกฎหมาย
     - ก่อน หรือขณะเก็บข้อมูล
     - ชัดแจ้ง แจ้งวัตถุประสงค์
     - ไม่หลอกลวง หรือทำให้เข้าใจผิด
     - แยกส่วนจากข้อความอื่นชัดเจน
     - อ่านเข้าใจได้ง่าย
     - ไม่มีเงื่อนไข
     - ให้อิสระในการตัดสินใจ
     - ถอนความยินยอมได้ง่าย เมื่อใดก็ได้ และต้องแจ้งผลกระทบจากการถอน

3. สิทธิของเจ้าของข้อมูลส่วนบุคคล

1) สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)

   มาตรา 23
   - ต้องเป็นการแจ้งให้ทราบ ก่อน หรือ ขณะ เก็บรวบรวมข้อมูล ในเรื่อง ต่อไปนี้
     - วัตถุประสงค์และฐานทางกฎหมาย
     - เงื่อนไขในการใช้บริการ
     - ประเภทของข้อมูลและระยะเวลาเก็บ

- การโอนข้อมูลส่วนบุคคล
- ข้อมูลการติดต่อผู้ควบคุมข้อมูล
- สิทธิของเจ้าของข้อมูลส่วนบุคคล

2) สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right to Access)

มาตรา 30

- เป็นการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคล ที่เกี่ยวกับตนเอง
- เมื่อมีการใช้สิทธิ ถือเป็นหน้าที่โดยปริยายของผู้ควบคุมข้อมูลที่จะต้องค้นหา ต้องดำเนินการโดยไม่ชักช้า ไม่เกิน 30 วัน นับแต่มีการร้องขอ
- กรณีติดขัดไม่ทำตามที่ขอ ต้องมีการทำบันทึกคำร้องขอ และระบุเหตุผล
- เป็นสิทธิไม่เด็ดขาด ผู้ควบคุมข้อมูลสามารถปฏิเสธได้ หากเป็นกรณี
  - ตามกฎหมาย หรือตามคำสั่งศาล
  - หากให้ไป อาจก่อให้เกิดความเสียหายแก่สิทธิของผู้อื่น

3) สิทธิในการเคลื่อนย้ายโอนข้อมูล (Right to Data Portability)

มาตรา 28, 31

- มีสิทธิขอรับข้อมูลที่เกี่ยวกับตน
- ขอให้ส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลอื่น
- ขอรับข้อมูลที่ส่งหรือโอนไปยังผู้ควบคุมข้อมูลอื่น
- ทั้งนี้ การส่งหรือโอนข้อมูลไปยังต่างประเทศ ต้องมีมาตรฐานการคุ้มครองข้อมูลที่เหมาะสมและเพียงพอ

4) สิทธิคัดค้านไม่ให้เก็บรวบรวม ใช้ ประมวลผล (Right to Object)

มาตรา 32

- คัดค้านการเก็บรวบรวม ใช้ เปิดเผยข้อมูลที่เกี่ยวกับตนเมื่อใดก็ได้
- กรณีการตลาดแบบตรง หรือกรณีการเก็บเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ เว้นแต่เป็นการดำเนินการไปเพื่อประโยชน์สาธารณะ เป็นต้น

5) สิทธิขอให้ลบหรือทาลาย (Right to erasure/Right to be Forgotten)

มาตรา 33

- เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา
- เมื่อข้อมูลส่วนบุคคลไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม
- เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ ยกเว้นมีเหตุตามที่กฎหมายกำหนด
- เมื่อเจ้าของข้อมูลได้ถอนความยินยอม
- เมื่อเจ้าของข้อมูลใช้สิทธิคัดค้าน ตามมาตรา 32 และไม่เข้าข้อยกเว้น
- เมื่อข้อมูลถูกเก็บรวบรวม ใช้ เปิดเผยโดยไม่ชอบด้วยกฎหมาย

6) สิทธิขอเพิกถอนความยินยอม (Right to withdraw consent)

มาตรา 19

- การเก็บรวบรวม ใช้ หรือเปิดเผย ไม่ได้ เว้นแต่ขอความยินยอม
  - ความยินยอมต้องได้รับก่อนหรือขณะนั้น โดยชัดแจ้ง
  - เป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์
  - แจ้งวัตถุประสงค์
  - ภาษา ไม่คลุมเครือ อ่านง่าย เข้าใจง่าย
  - ไม่ก่อให้เกิดการหลอกลวง ทำให้เข้าใจผิดวัตถุประสงค์
  - อิสระในการให้ความยินยอม ไม่มีเงื่อนไข
  - ถอนเมื่อใดก็ได้ และต้องถอนได้ง่าย

7) สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)

มาตรา 34 เงื่อนไข

- ต้องอยู่ระหว่างตรวจสอบตามที่เจ้าของข้อมูลร้องขอ
- เป็นข้อมูลที่ต้องลบหรือทำลายตามมาตรา 33(4) แต่เจ้าของให้ระงับการใช้แทน
- เมื่อข้อมูลหมดความจำเป็นที่จะต้องเก็บตามวัตถุประสงค์ แต่เจ้าของขอให้เก็บรักษาไว้เพื่อการก่อตั้งสิทธิเรียกร้อง
- เมื่อข้อมูลอยู่ในระหว่างการพิสูจน์ หรือตรวจสอบเพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูล

8) สิทธิขอแก้ไขข้อมูล (Right to rectification)

มาตรา 35

- เจ้าของข้อมูลแจ้งขอต่อผู้ควบคุมข้อมูล
  - ให้ดำเนินการแก้ไขข้อมูลที่ไม่ถูกต้อง ทำให้สมบูรณ์ ให้รายละเอียดเพิ่มเติม
  - หากผู้ควบคุมข้อมูล ไม่สามารถดำเนินการตามคำร้องขอ ให้ทำบันทึกคำร้องขอของเจ้าของข้อมูล และระบุเหตุผลในบันทึกรายการกิจกรรมการประมวลผล (RoPA)

4. การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

<u>ผู้รับผิดชอบต่อการถูกลงโทษตามกฎหมาย</u>

*องค์กรเป็นผู้รับผิดชอบต่อการถูกลงโทษทั้งทางแพ่งและทางปกครอง

**กรณีลงโทษทางอาญา ถ้าผู้กระทำผิดเป็นนิติบุคคลกรรมการผู้มีอำนาจสั่งการ / บุคคลที่รับผิดชอบในการดำเนินงานของนิติบุคคล / บุคคลที่มีหน้าที่สั่งการ หรือละเว้นการสั่งการต้องระวางโทษในความผิดนั้นด้วย (มาตรา 81)

***กรณีที่มีความผิดตาม PDPA เกิดในระดับพนักงาน เจ้าหน้าที่ ที่ปฏิบัติหน้าที่ตามที่นายจ้างสั่ง ทางผู้เสียหายไม่ฟ้องร้องค่าเสียหายจากบุคคลเหล่านี้ได้ แต่องค์กรสามารถฟ้องร้อง หรือลงโทษฐานที่ทำให้องค์กรได้รับความเสียหายได้

<u>การแจ้งเหตุละเมิด</u>

• กรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ให้ปฏิบัติตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 https://www.pdpc.or.th/2405

• “การละเมิดข้อมูลส่วนบุคคล ” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดย ปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

• กรณีเหตุการละเมิดมีแนวโน้มที่จะสร้างความเสี่ยงหรือกระทบสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงที่ทราบ และแจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า

<u>มาตรการจัดการการละเมิดข้อมูลส่วนบุคคล</u>

1. กิจกรรมที่เข้าข่ายละเมิด
2. ทราบเมื่อไร
3. สอบสวน
   1) สาเหตุการละเมิด
   2) ผลกระทบ ได้แก่ 1. ต่อองค์กร และ 2. ต่อเจ้าของข้อมูลส่วนบุคคล น้อย / มาก
4. ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล
   1) ไม่ต้องเยียวยา 2) ต้องเยียวยา
5. แจ้ง PDPC ภายใน 72 ชั่วโมง
6. มีมาตรการป้องกันไม่ให้เกิดเหตุอีกในครั้งต่อไป

ความรับผิดและบทลงโทษ

มาตรการจัดการการละเมิดข้อมูล	บทกำหนดโทษ
ความรับผิดทางแพ่ง	• ผู้กระทำละเมิดข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนให้กับเจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม • ศาลมีอำนาจสั่งให้ชดใช้ค่าสินไหมทดแทนเพิ่มเติมได้สองเท่าของค่าสินไหมทดแทนที่แท้จริง
โทษอาญา	• กำหนดบทลงโทษทางอาญาไว้สำหรับความผิดร้ายแรง เช่น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยมิชอบ ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นแล้วนำไปเปิดเผยแก่ผู้อื่นโดยมิชอบ • ระวางโทษสูงสุดจำคุกไม่เกิน 1 ปีหรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ • ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล กรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นอาจต้องร่วมรับผิดในความผิดอาญาที่เกิดขึ้น
โทษทางปกครอง	• กำหนดโทษปรับทางปกครองสำหรับการกระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด เช่น ไม่แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคล ไม่แต่งตั้ง DPO เป็นต้น • โทษปรับทางปกครองสูงสุด 5,000,000 บาท

มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

การรักษาความมั่นคงปลอดความภัยข้อมูล

การเก็บ ประมวลผล ใช้ และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะได้รับการยกเว้นไม่ต้องปฏิบัติตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ จะต้องมีมาตรการรักษาความปลอดภัยข้อมูลตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 https://www.pdpc.or.th/2971

2. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้รับการยกเว้นไม่ให้นำ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาใช้บังคับ พ.ศ. 2566 https://www.pdpc.or.th/2271 ซึ่งมีทั้ง 2 ประกาศ มีการระบุ

1. มาตรการเชิงองค์กร (organizational measures)
2. มาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม
3. มาตรการทางกายภาพ (physical measures)

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ มทร.ธัญบุรี

- ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ มทร.ธัญบุรี

- เป็นการสมควรกำหนดนโยบายด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ Information Technology Security Policy ของ มทร.ธัญบุรี โดยมีวัตถุประสงค์เพื่อให้เกิดความมั่นคงและปลอดภัยในกิจการด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย เพื่อให้สอดคล้องและรองรับกับมาตรา 5 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

- อาศัยอำนาจตามความในมาตรา 24 และมาตรา 27 แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. 2548 และมาตรา 5 มาตรา 6 และมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 จึงออกประกาศไว้

คู่มือระบบการเรียนรู้ด้วยตนเอง (Self-learning)

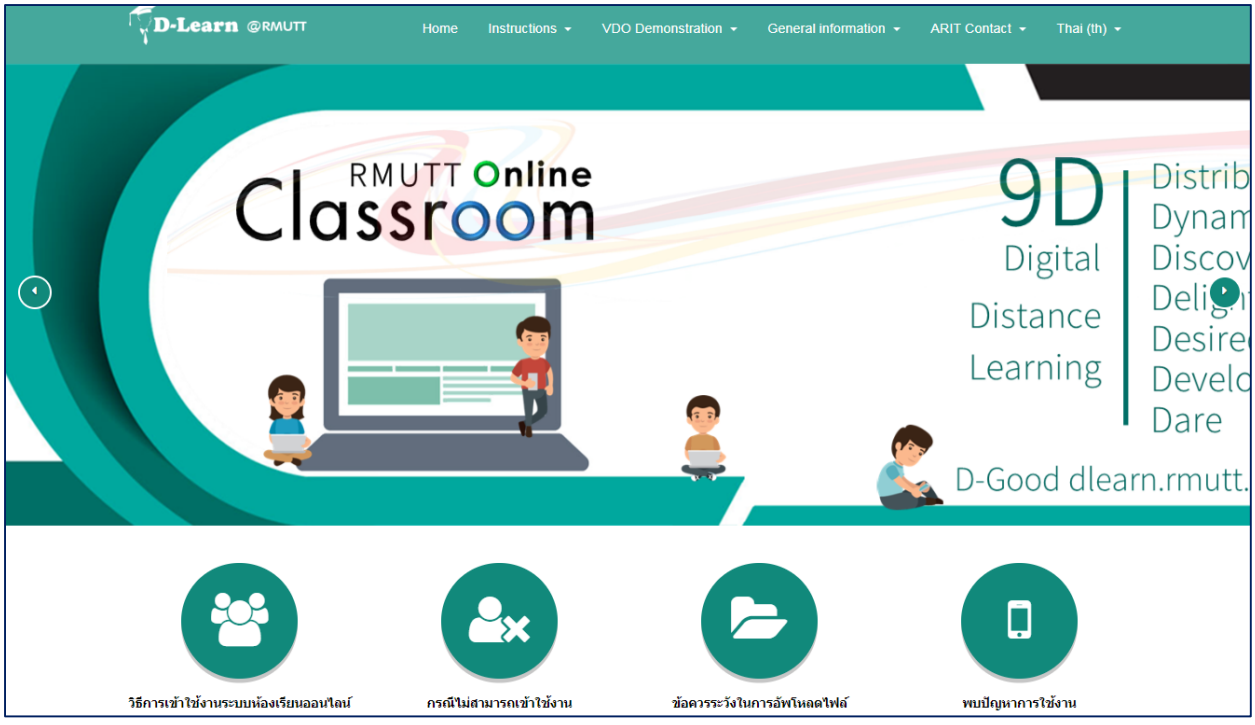
ผู้ใช้งานระบบสามารถเข้าห้องเรียนออนไลน์ สำหรับเรียนรู้ เรื่อง “การสร้างความมั่นคงปลอดภัยทางไซเบอร์ส่วนบุคคล” ผ่านทางเว็บไซต์ที่หน่วยงานให้บริการ โดยมีรูปแบบการเรียนรู้ที่ไม่จำกัดเรื่องของสถานที่และเวลาเรียน ผู้ใช้งานสามารถเข้าเรียนเวลาใดก็ได้ผ่านการเรียนรู้ตนเอง ดังขั้นตอนการใช้งานต่อไป

สิทธิการใช้งานระบบ

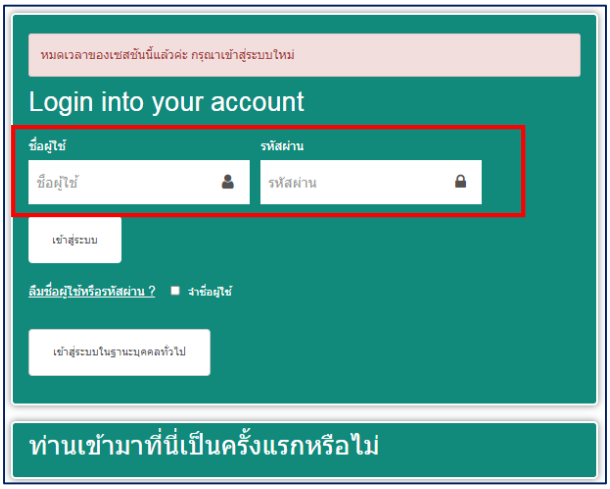
กลุ่มผู้ใช้งาน	สิทธิการใช้งานระบบ
ผู้ใช้งาน (User)	1. การแก้ไขข้อมูลส่วนบุคคลได้ 2. การร้องขอรหัสผ่านใหม่ได้ 3. จัดเก็บเอกสารส่วนตัวได้ 4. ลงทะเบียนเรียนหลักสูตรในหน่วยงานสังกัดได้ 5. ตรวจสอบคะแนนของตนเองได้ 6. ตั้งกระทู้ในห้องสนทนาได้ 7. ตั้งค่าการแจ้งเตือนของตนเองได้

การใช้งานห้องเรียนออนไลน์ (D-Learn)

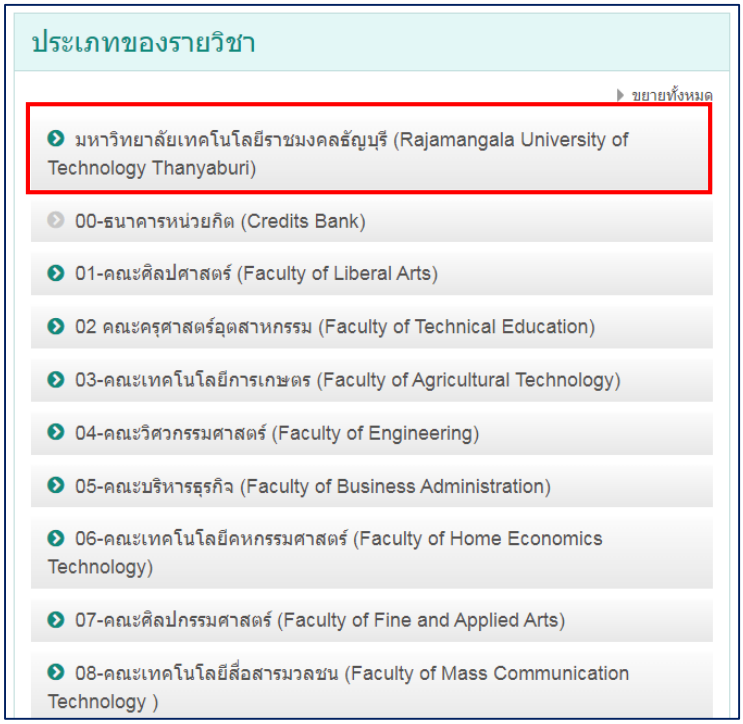
1. หน้าหลักของห้องเรียนออนไลน์ โดยเข้าระบบผ่านเว็บไซต์ https://dlearn.rmutt.ac.th



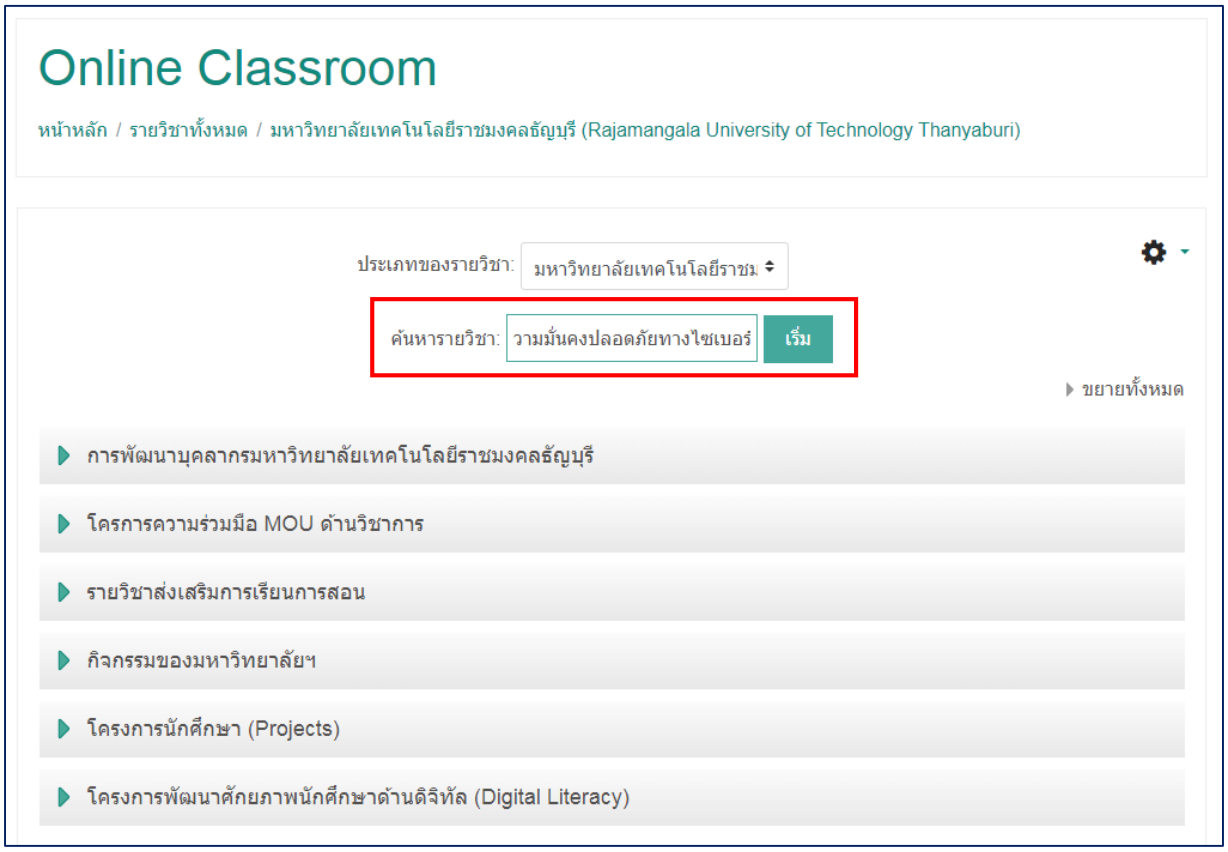
2. เข้าสู่ระบบด้วย Internet Account WiFi ของมหาวิทยาลัย



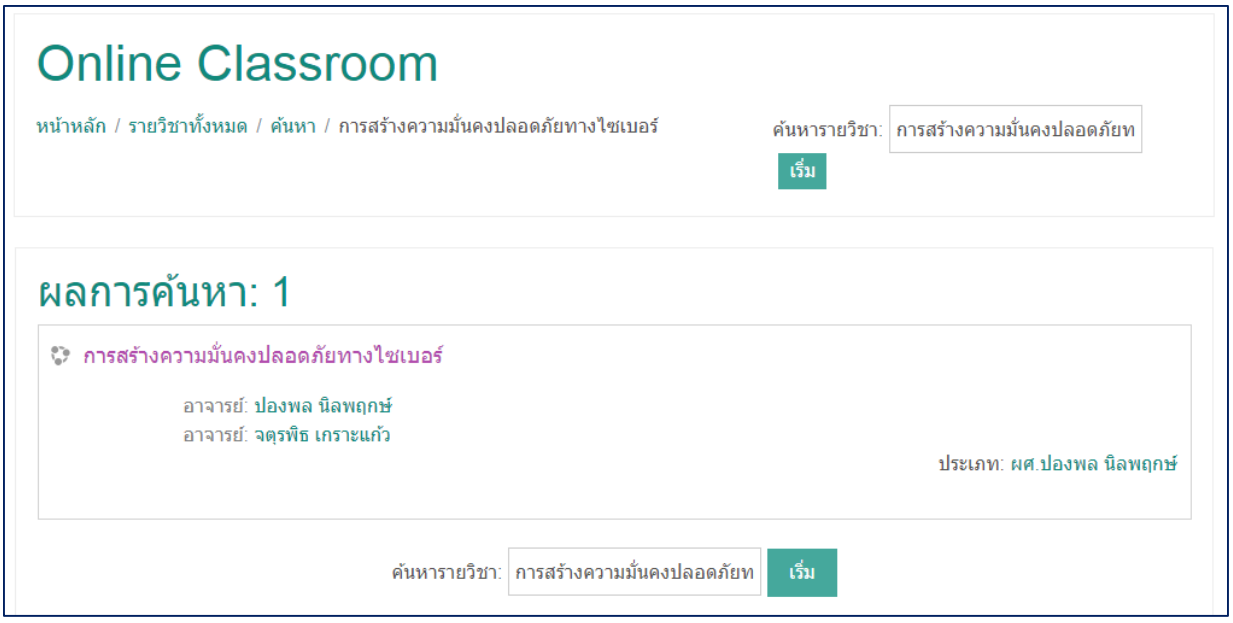
3. เลือกรายวิชา/กรอกรหัสที่ได้รับ > เลือก มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี (Rajamangala University of Technology Thanyaburi)



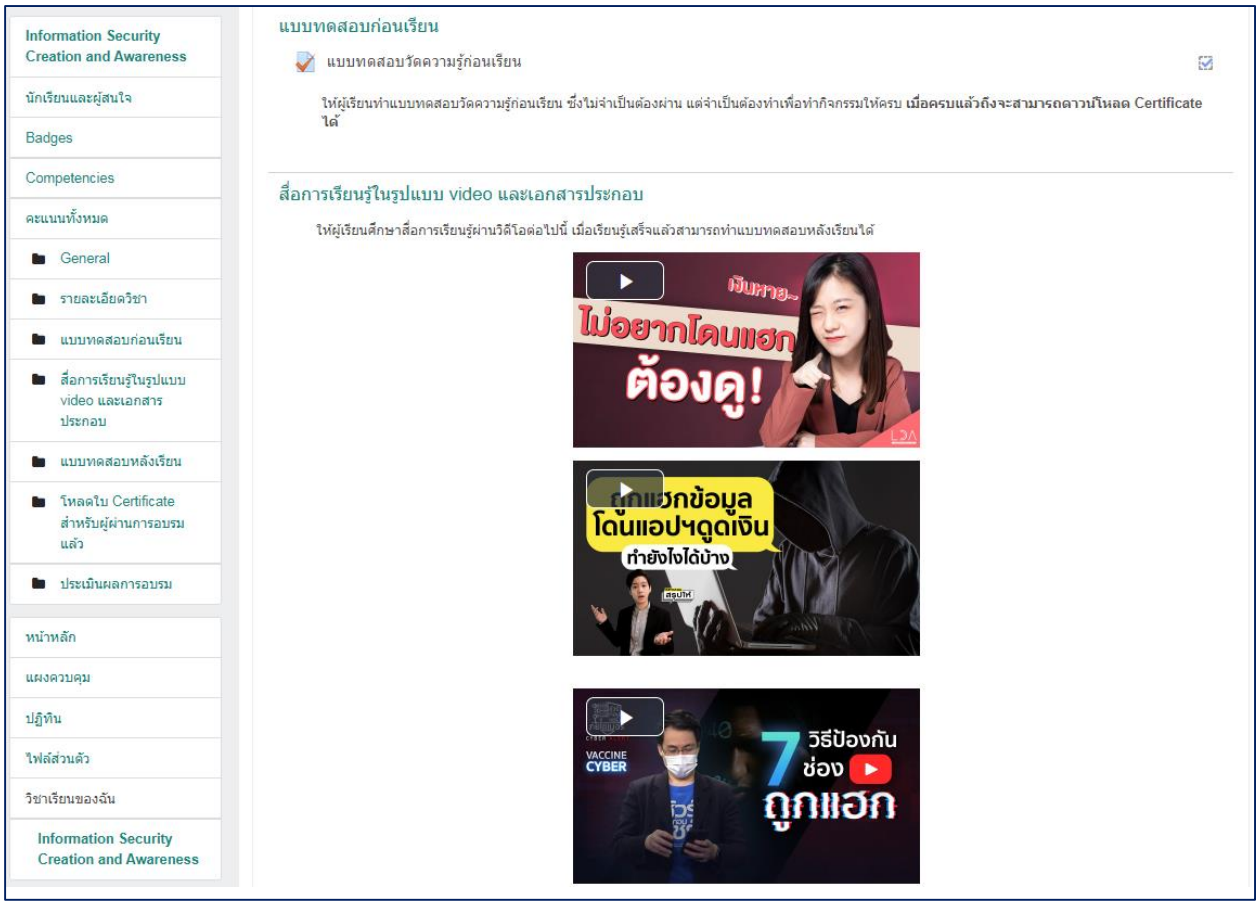
4. ค้นหารายวิชา “การสร้างความมั่นคงปลอดภัยทางไซเบอร์”



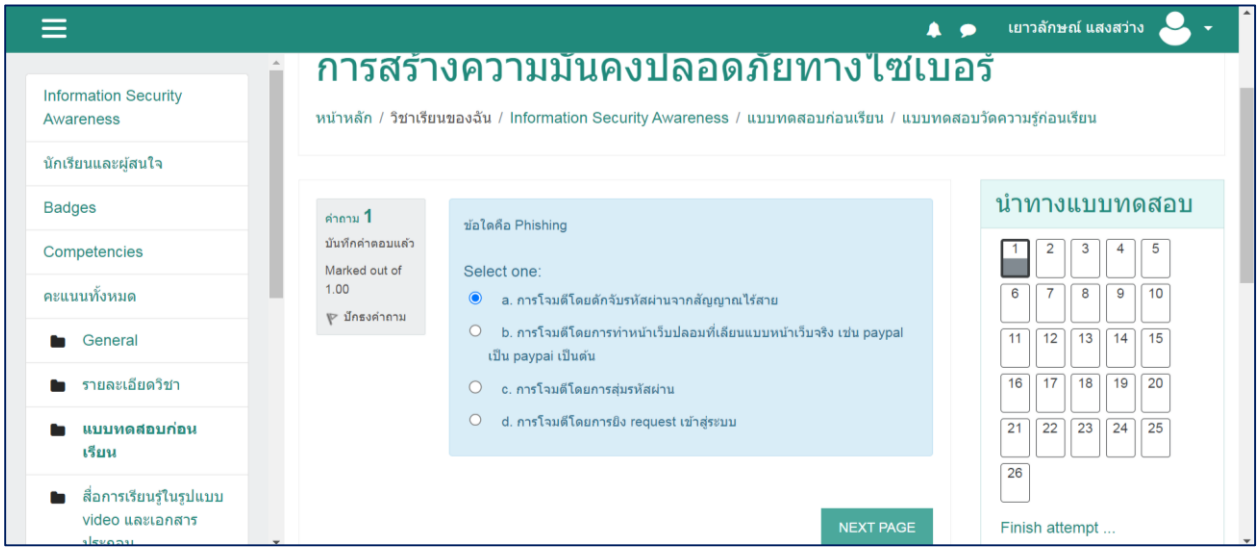
5. คลิกที่ชื่อรายวิชาเพื่อเข้าบทเรียน



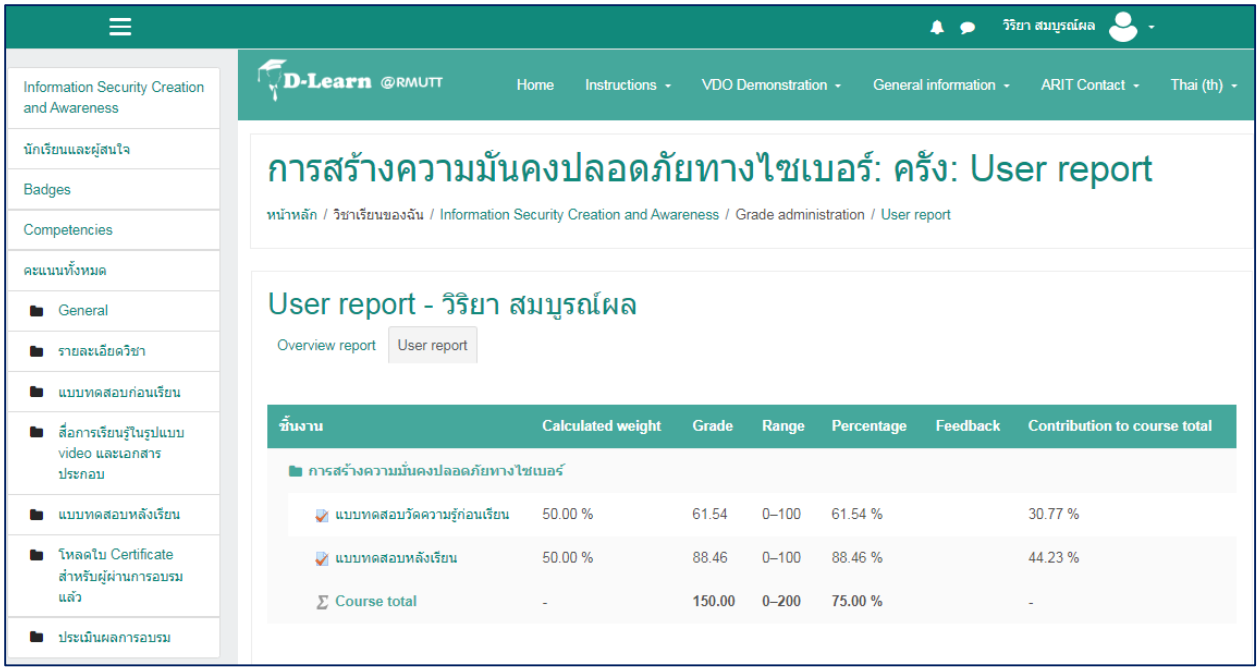
6. หน้าจอแสดงรายวิชาหลักสูตร และแสดงแถบสถานะรายวิชาหลักสูตร



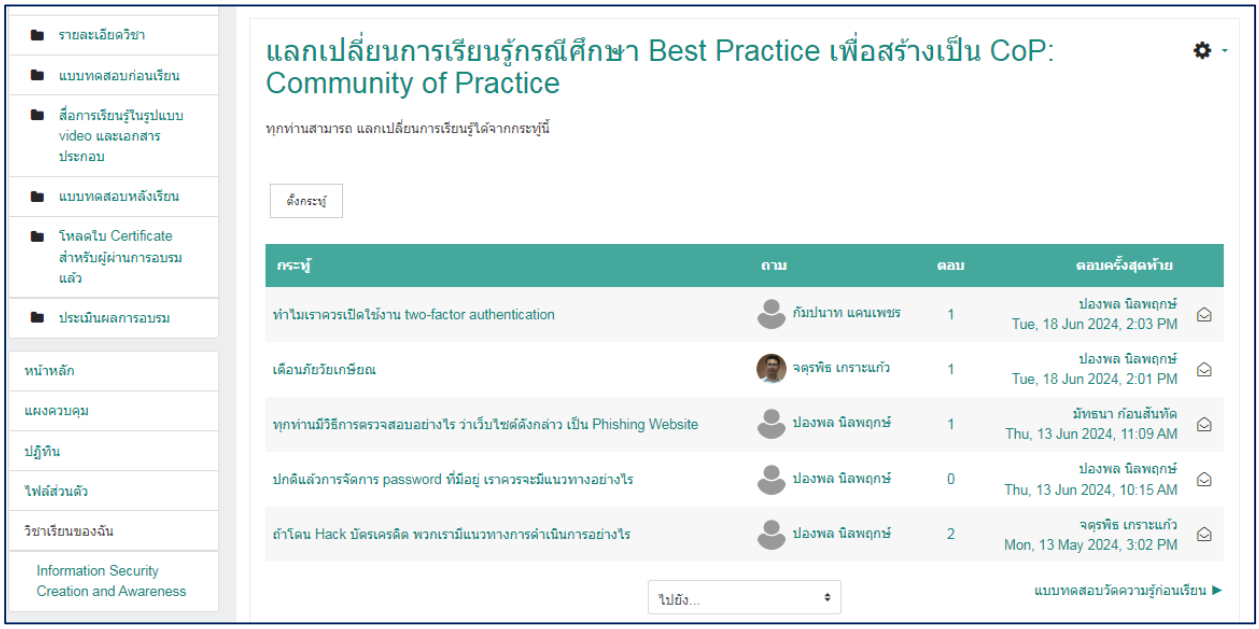
7. ทำแบบทดสอบการเรียน และหลังเรียนเสร็จ



8. รายละเอียดคะแนนในบทเรียน

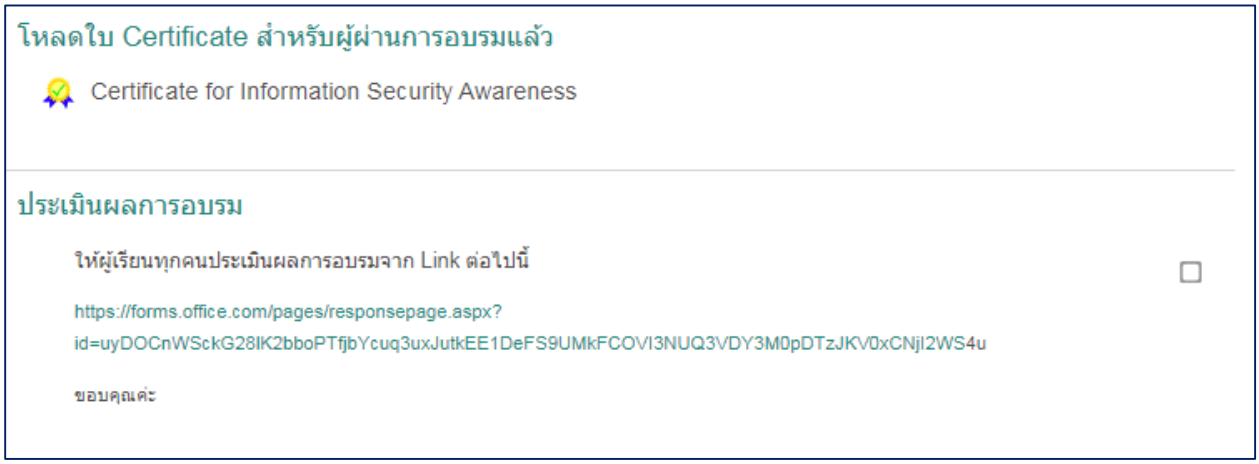


9. ห้องสนทนากระดานถาม-ตอม



10. กระทู้แสดงความคิดเห็นสำหรับแลกเปลี่ยนเรียนรู้ระหว่างกัน

11. ระบบทำการสร้างใบประกาศนียบัตร เพื่อให้ผู้เรียนกดดาวน์โหลดไฟล์ที่ระบบสร้าง



12. ใบประกาศนียบัตร

บรรณานุกรม

ไซเบอร์ อีลีท. (2566). **Incident Response (IR) รับมืออย่างไร เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์** สืบค้นจาก https://www.cyberelite.co.th/blog/incident-response/

สำนักวิทยบริการและเทคโนโนโลยีสารสนเทศ. (2563). **ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ มทร. ธัญบุรี**. สืบค้นจาก www.arit.rmutt.ac.th/2020/01/10/4392

อรรถศิษฐ์ พัฒนะศิริ. (2566, พฤษภาคม). **แนวทางการปฏิบัติ PDPA ของสถาบันอุดมศึกษาไทย**. เอกสารนำเสนอโครงการอบรม สำนักวิทยบริการและเทคโนโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี. ปทุมธานี

อุดมธิปก ไพรเกษตร. (2567, กรกฎาคม). **โครงการการจัดการความปลอดภัยของข้อมูลและการตระหนักถึงความเป็นส่วนตัว (PDPA)**. เอกสารนำเสนอโครงการอบรม สำนักวิทยบริการและเทคโนโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี. ปทุมธานี

เอซิส โปรเฟสชั่นนัล เซ็นเตอร์. (2566ก). **เตือนภัยไซเบอร์ที่อาจจะทวีความรุนแรงมากขึ้นในปี 2024**. สืบค้นจาก https://www.acisonline.net/?p=10648

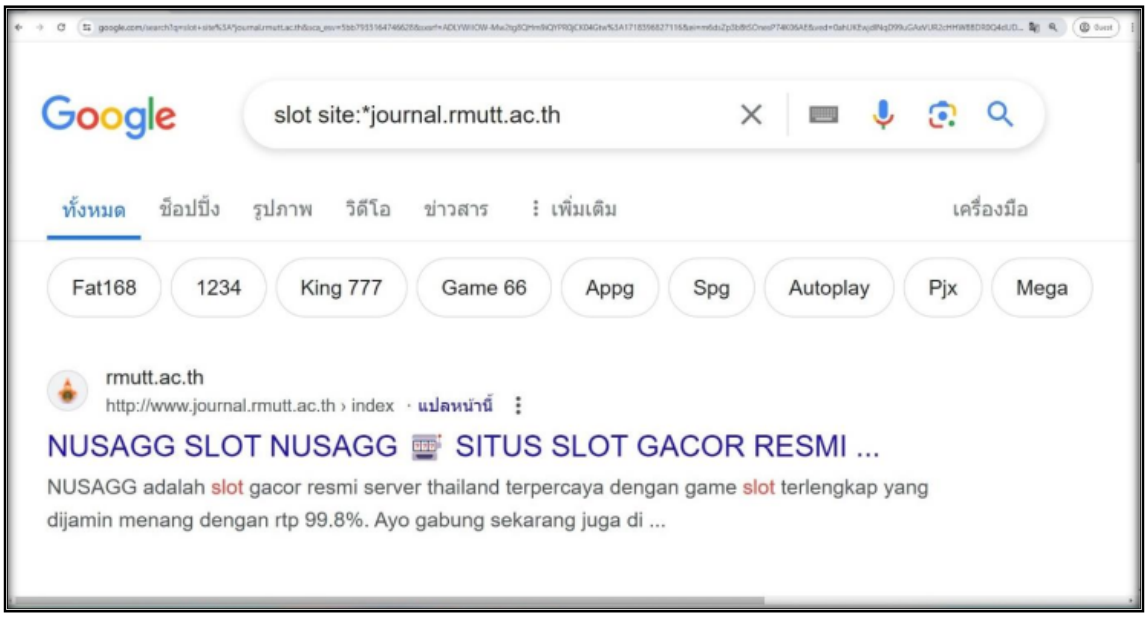
เอซิส โปรเฟสชั่นนัล เซ็นเตอร์. (2566ข). **5 วิธีรับมือภัยคุกคามความปลอดภัยทางไซเบอร์ในปี 2024**. สืบค้นจาก https://www.acisonline.net/?p=10694

ภาคผนวก

กรณีตัวอย่าง การถูกโจมตีบนเว็บไซต์

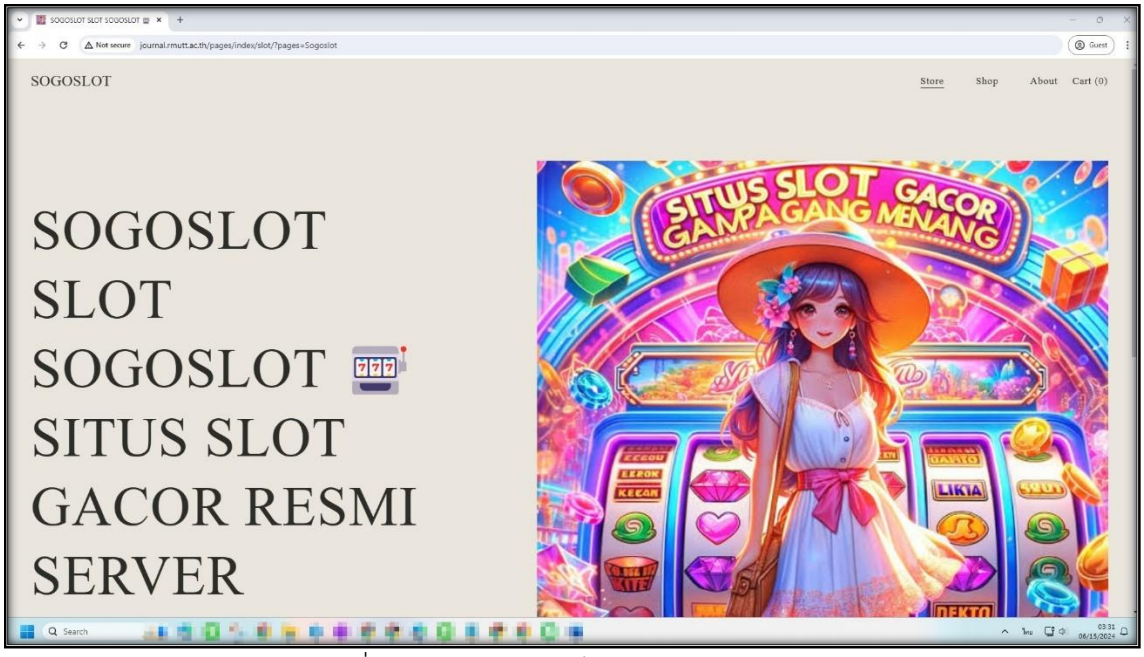
กรณีตัวอย่าง การแจ้งเตือนตรวจพบการโจมตีเว็บไซต์หน่วยงานการศึกษา

1. เมื่อวันที่ 14 มิถุนายน 2567 เวลาประมาณ 23.00 น. ได้ตรวจพบลิงก์โฆษณาเว็บไซต์การพนันออนไลน์บนอินเทอร์เน็ต



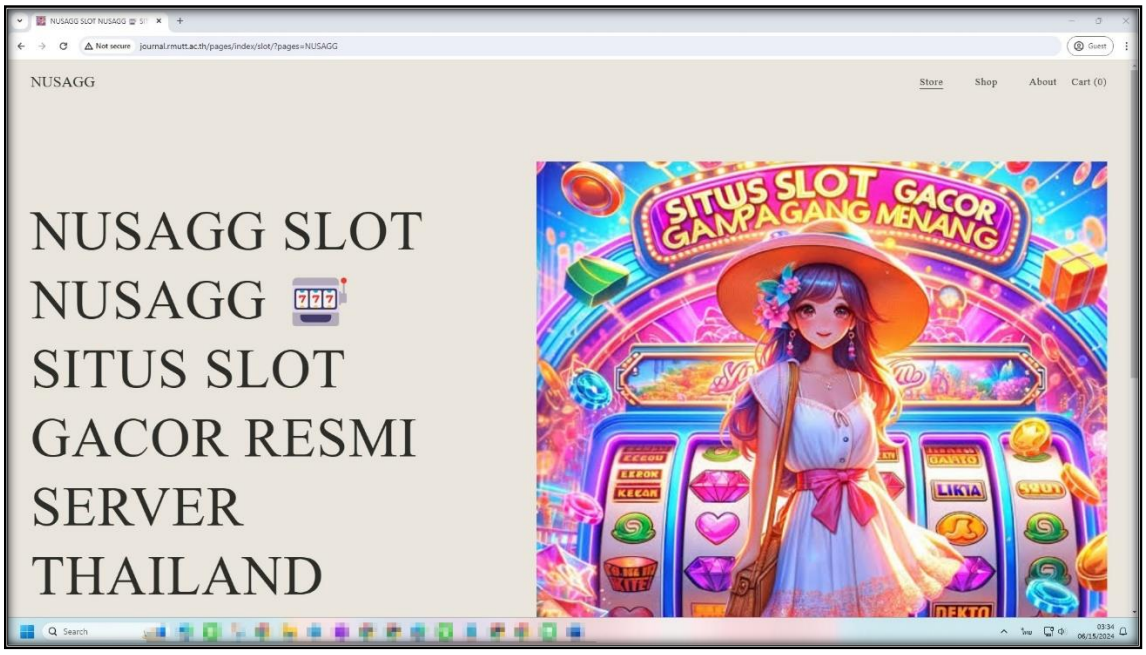
ภาพที่ 1 แสดงภาพเว็บไซต์ที่ตรวจพบ

2. พบหน้าเว็บไซต์เป็นลิงก์เว็บไซต์การพนันออนไลน์ ที่ URL: hxxp://www.journal.rmutt.ac[.]th/pages/index/slot/?pages=Sogoslot



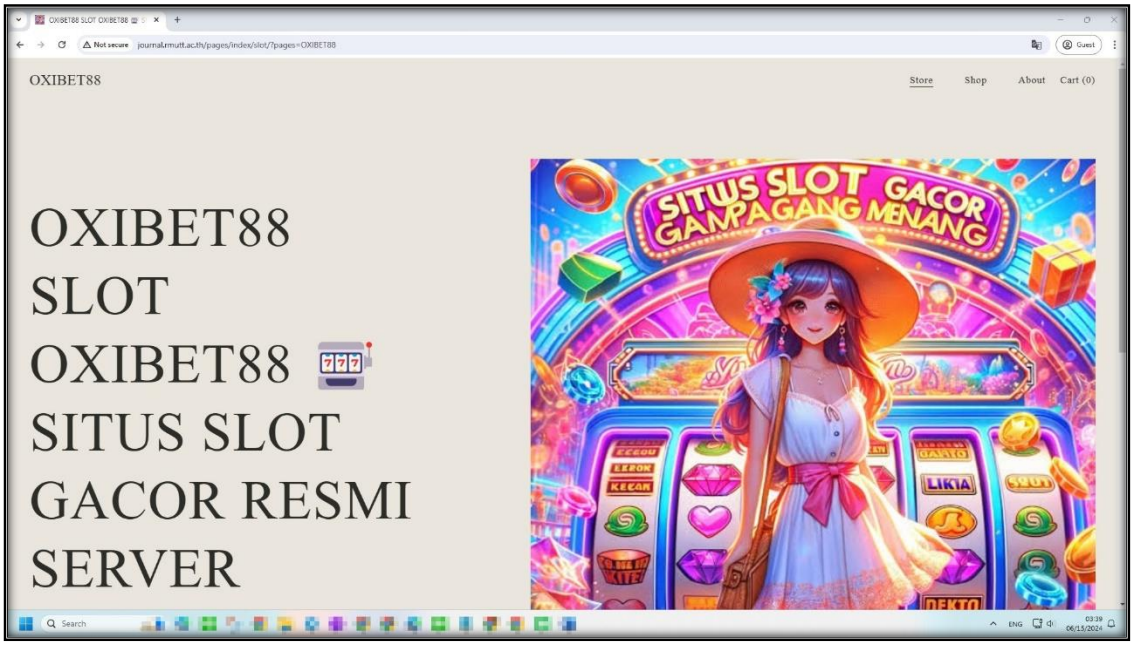
ภาพที่ 2 แสดงภาพหน้าเว็บไซต์การพนันออนไลน์

3. พบหน้าเว็บไซต์เป็นลิงก์เว็บไซต์การพนันออนไลน์ ที่ URL: hxxp://www.journal.rmutt.ac[.]th /pages/index/slot/?pages=NUSAGG



ภาพที่ 3 แสดงภาพหน้าเว็บไซต์การพนันออนไลน์

4. พบหน้าเว็บไซต์เป็นลิงก์เว็บไซต์การพนันออนไลน์ ที่ URL: hxxp://www.journal.rmutt.ac[.]th /pages/index/slot/?pages=OXIBET88



ภาพที่ 4 แสดงภาพหน้าเว็บไซต์การพนันออนไลน์

5. ทำการตรวจสอบพบว่าเป็นเว็บไซต์วารสารวิชาการ ของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ภาพที่ 5 แสดงภาพเว็บไซต์วารสารวิชาการ ของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

แนวทางการแก้ไข

1. ตรวจสอบไฟล์ทุกไฟล์และลบไฟล์ที่ไม่เกี่ยวข้องออกจาก เครื่องแม่ข่าย
2. ปิดการใช้งานฟังก์ชั่นการอัปโหลดไฟล์
3. ปิดการใช้งานระบบดังกล่าวเนื่องจากไม่ได้ถูกใช้งานแล้ว
4. เปลี่ยน Password ในการเข้าถึงเครื่องแม่ข่าย
5. เปลี่ยน Password ในการเข้าถึงระบบฐานข้อมูล และใช้บัญชีผู้ใช้งานเฉพาะผู้ที่มีสิทธิ์ในการเข้าถึงระบบฐานข้อมูลเท่านั้น
6. ดำเนินการทบทวนและกำหนดสิทธิ์ในการเข้าถึงใหม่ทั้งหมด
7. วางแผนการดำเนินงานในการทำ VA Scan สำหรับ OWASP TOP 10 ในระบบอื่น ๆ ที่เกี่ยวข้อง เช่น การใช้คำค้นหาเฉพาะบน search engine เพื่อหาข้อมูลที่เกี่ยวข้องกับเว็บไซต์การพนันออนไลน์ และ keyword อื่น ๆ ที่เกี่ยวข้อง
8. วางแผนการดำเนินการปิดระบบทั้งหมดที่ไม่ได้ถูกใช้งาน หรือระบบที่มีความถี่ในการใช้งานน้อย ให้เปิดเฉพาะช่วงเวลาที่ดำเนินการ เป็นต้น
9. วางแผนปรับปรุงระบบเก่าโดยใช้ Framework ที่มีมาตรฐานด้านความปลอดภัยสำหรับการพัฒนาระบบทดแทนระบบเดิม