รายงานผลการดำเนินการจัดการความรู้ ประจำปีการศึกษา 2568
ด้านพันธกิจอื่น

เรื่อง แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏกำแพงเพชร

คำนำ

ในยุคปัจจุบันที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการบริหารจัดการและการดำเนินงานในสถาบันอุดมศึกษา ข้อมูลส่วนบุคคลของบุคลากรและนักศึกษาถือเป็นสินทรัพย์ที่มีค่ายิ่ง แต่ในขณะเดียวกันก็มีความเสี่ยงสูงที่จะถูกคุกคามทางไซเบอร์ หรือเกิดการรั่วไหลอันเนื่องมาจากความเท่าไม่ถึงการณ์และการขาดความรู้ความเข้าใจที่เพียงพอเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งจากการประเมินของมหาวิทยาลัยราชภัฏกำแพงเพชร พบว่าความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคลในปัจจุบันจัดอยู่ในระดับที่สูงมาก (ระดับ 16) ซึ่งเป็นเรื่องเร่งด่วนที่ต้องได้รับการบริหารจัดการอย่างเป็นระบบ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ในฐานะหน่วยงานหลักที่มีบทบาทหน้าที่ในการดูแลระบบเทคโนโลยีสารสนเทศและความปลอดภัยทางไซเบอร์ของมหาวิทยาลัย ได้เล็งเห็นถึงความจำเป็นในการแก้ไขปัญหาดังกล่าวอย่างยั่งยืน จึงได้จัดทำการจัดการความรู้ (Knowledge Management: KM) ประจำปีการศึกษา 2568 ภายใต้หัวข้อ แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero) ขึ้น โดยมีวัตถุประสงค์เพื่อเป็นศูนย์รวมองค์ความรู้ แปรรูปข้อกำหนดทางกฎหมายที่ซับซ้อนให้กลายเป็นแนวทางปฏิบัติที่เข้าใจง่าย พร้อมทั้งพัฒนาเครื่องมือสนับสนุนการทำงาน เช่น รายการตรวจสอบ (Checklist) และสื่ออินโฟกราฟิก (Infographic) เพื่อให้บุคลากรสายสนับสนุน และแอดมิน (Admin) ผู้ดูแลระบบของหน่วยงานต่างๆ ภายในมหาวิทยาลัย สามารถนำไปประยุกต์ใช้ในการบริหารจัดการข้อมูลในระบบสารสนเทศและสื่อสังคมออนไลน์ได้อย่างถูกต้อง ปลอดภัย และมีประสิทธิภาพ โดยมุ่งเป้าสูงสุดให้อัตราการรั่วไหลของข้อมูลส่วนบุคคลเป็นศูนย์ (Risk Zero)

ดังนั้น หวังเป็นอย่างยิ่งว่าองค์ความรู้และแนวทางปฏิบัตินี้ จะเป็นประโยชน์ในการสร้างความตระหนักรู้ ปรับเปลี่ยนพฤติกรรมการทำงาน และสร้างมาตรฐานความมั่นคงปลอดภัยด้านข้อมูลส่วนบุคคลของมหาวิทยาลัยราชภัฏกำแพงเพชรให้เป็นไปตามที่กฎหมายกำหนดอย่างยั่งยืนต่อไป

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏกำแพงเพชร

สารบัญ

1. ชื่อแผนการจัดการความรู้

แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)

2. ผู้รับผิดชอบ

นางสาวอรปรียา คำแพ่ง
นางสาวสรัลชนา น้ำเงินสกุณี
และบุคลากร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

3. หลักการและเหตุผล

มหาวิทยาลัยราชภัฏกำแพงเพชร เล็งเห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ซึ่งปัจจุบันมีความเสี่ยงจากการถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษาในระดับสูงมาก (ระดับ 16) โดยมีปัจจัยเสี่ยงสำคัญทั้งจากภายนอก เช่น ภัยคุกคามทางไซเบอร์ และปัจจัยภายใน เช่น บุคลากรและนักศึกษาบางส่วนยังขาดความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) รวมถึงความเสี่ยงที่เจ้าหน้าที่ผู้เกี่ยวข้องอาจละเลยหรือไม่ปฏิบัติตามกฎหมายจนนำไปสู่การนำข้อมูลไปใช้ผิดวัตถุประสงค์

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ในฐานะหน่วยงานผู้รับผิดชอบหลักด้านการจัดการความเสี่ยงดังกล่าว ในปีการศึกษา 2568 จึงเลือกประเด็นการจัดการความรู้ เรื่อง “แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)” ช่วยขับเคลื่อนการดำเนินงานด้าน PDPA ของมหาวิทยาลัย เพื่อรวบรวมและสร้างแนวทางปฏิบัติงานที่ชัดเจน โดยมุ่งเน้นการเปลี่ยนข้อกำหนดทางกฎหมายที่ซับซ้อนให้เป็นเครื่องมือที่ใช้งานง่าย เช่น รายการตรวจสอบ (Checklist) และสื่ออินโฟกราฟิก (Infographic) เพื่อให้ผู้ปฏิบัติงานและแอดมิน (Admin) ของหน่วยงานต่าง ๆ สามารถนำไปใช้ในการบริหารจัดการข้อมูลในระบบสารสนเทศและสื่อสังคมออนไลน์ได้อย่างถูกต้อง ทั้งนี้ เพื่อลดโอกาสการเกิดเหตุการณ์ข้อมูลรั่วไหลให้เป็นศูนย์ และสร้างความมั่นคงปลอดภัยด้านข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กฎหมายกำหนดอย่างยั่งยืน

4. วัตถุประสงค์

1. เพื่อสร้างและรวบรวมองค์ความรู้ด้านแนวทางปฏิบัติงานในการลดความเสี่ยงการถูกละเมิดและป้องกันการรั่วไหลของข้อมูลส่วนบุคคลภายในมหาวิทยาลัย
2. เพื่อพัฒนาเครื่องมือสนับสนุนการปฏิบัติงานสำหรับบุคลากรสายสนับสนุน และแอดมิน (Admin) ผู้ดูแลระบบ ของหน่วยงานภายในมหาวิทยาลัย
3. เพื่อส่งเสริมความรู้ ความเข้าใจ และสร้างความตระหนักรู้ด้าน PDPA และความปลอดภัยไซเบอร์ให้แก่บุคลากรสายสนับสนุน และแอดมิน (Admin) ผู้ดูแลระบบ ของหน่วยงานภายในมหาวิทยาลัย

5. ผู้เข้าร่วมโครงการ

บุคลากรสายสนับสนุน และแอดมิน (Admin) ผู้ดูแลระบบ มหาวิทยาลัยราชภัฏกำแพงเพชร

6.สถานที่ดำเนินการ

มหาวิทยาลัยราชภัฏกำแพงเพชร

7. วิธีดำเนินงาน (แผนการจัดการความรู้ 6 ขั้นตอน)

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
1	การกำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร	**กิจกรรมที่ 1 จัดตั้งคณะทำงาน** 1.1 จัดตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ 1.2 จัดตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร	31 ต.ค. 2568 12 พ.ย. 2568	1. คำสั่ง แต่งตั้งคณะกรรมการจัดการความรู้ จำนวน 1 ฉบับ 2. คำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล จำนวน 1 ฉบับ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ - บุคลากรของสำนักฯ - ตัวแทนหน่วยงานที่เกี่ยวข้องกับการกำกับและการใช้ข้อมูลส่วนบุคคลภายในมหาวิทยาลัย	- คณะกรรมการจัดการความรู้สำนักฯ
		กิจกรรมที่ 2 ประชุมคณะกรรมการ จัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล	5 พ.ย. 2568	1. แผนการจัดการความรู้ จำนวน 1 เรื่อง 2. รายการความเสี่ยงที่เกี่ยวข้อง จำนวน 5 ประเด็น	คณะกรรมการจัดการความรู้และคณะกรรมการความเสี่ยงสำนักฯ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
2	การเสาะหาความรู้ที่ต้องการ	**กิจกรรมที่ 3 รวบรวมและศึกษา** ข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA, และตัวอย่าง Best Practice การลดความเสี่ยงจากมหาวิทยาลัยหรือหน่วยงานที่ประสบความสำเร็จ เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล	พ.ย. 2568	เอกสารที่เกี่ยวข้อง จำนวน 5 เรื่อง	คณะกรรมการ KM, คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
3	การปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน	**กิจกรรมที่ 4 จัดทำเครื่องมือ/แนวทางปฏิบัติ** เช่น คู่มือ, Checklist การใช้งานระบบที่ต้องระบุตัวตน หรือ Infographic สรุปข้อปฏิบัติของบุคลากร	ธ.ค.68 - ม.ค.69	เครื่องมือ/แนวทางปฏิบัติ (ฉบับร่าง) 3 รายการ เช่น คู่มือหรือแนวปฏิบัติ 1 รายการ, Checklist 1 รายการ, Infographic 1 รายการ	คณะกรรมการ KM, คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
4	การประยุกต์ใช้ความรู้ในกิจการงานของตน	**กิจกรรมที่ 5 แลกเปลี่ยนเรียนรู้** (1) นำเครื่องมือ/แนวทางปฏิบัติจาก กิจกรรมที่ 4 ไปทดลองใช้ในหน่วยงาน/กลุ่มงานที่เกี่ยวข้องกับ 3 อันดับความเสี่ยงที่วิเคราะห์ไว้ (2) จัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล สำหรับผู้ที่มีหน้าที่และความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)	ก.พ. - มี.ค. 2569	- ร้อยละของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ร้อยละ 60) - ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ระดับดี) - จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต (เป้าหมาย 0 ครั้ง)	บุคลากรมหาวิทยาลัยฯ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
5	การนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้และสกัดขุมความรู้ออกมาบันทึกไว้	**กิจกรรมที่ 6 จัดตั้งชุมชนนักปฏิบัติ (CoP) ในกลุ่มผู้ใช้งาน** กิจกรรมที่ 5 เพื่อแลกเปลี่ยนประสบการณ์ ปัญหาและจุดที่ต้องปรับปรุง ในการนำแนวทางไปปฏิบัติจริง และสกัดบทเรียนที่ได้ออกมา	เม.ย. - พ.ค. 2569	- ชุมชนนักปฏิบัติ (CoP) เพื่อแลกเปลี่ยนเรียนรู้ จำนวน 1 ชุมชน	คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
6	การจดบันทึกขุมความรู้และแก่นความรู้ สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น	**กิจกรรมที่ 7** นำบทเรียนที่สกัดได้จากกิจกรรมที่ 6 มาปรับปรุงและจัดทำเป็นชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล (ฉบับร่าง) สรุปให้เป็นฉบับสมบูรณ์ เพื่อใช้ในการปฏิบัติงานที่เป็นทางการ	พ.ค. 2569	- ชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล จำนวน 1 ชิ้น	คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

8. ผลการดำเนินงานตามแผนการจัดการความรู้ 6 ขั้นตอน

1. กำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร

กิจกรรมที่ 1 จัดตั้งคณะทำงาน

1.1 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการวิเคราะห์ความเสี่ยงและการควบคุมภายใน สั่ง ณ วันที่ 20 ตุลาคม 2568

1.2 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ สั่ง ณ วันที่ 31 ตุลาคม 2568

1.3 คำสั่งมหาวิทยาลัยราชภัฏกำแพงเพชร เรื่อง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร สั่ง ณ วันที่ 12 พฤศจิกายน 2568

1.4 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล สั่ง ณ วันที่ 22 พฤศจิกายน 2568

กิจกรรมที่ 2 ประชุมกรรมการ

ประชุมคณะกรรมการจัดการความรู้และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล เมื่อวันที่ 5 พฤศจิกายน 2568 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มติที่ประชุมกำหนด **ประเด็นการจัดการความรู้ เรื่อง แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)** และร่วมกันเขียนแผนการจัดการความรู้ในประเด็นดังกล่าว

ที่มา https//arit.kpru.ac.th/page_id/1649/TH

2. การเสาะหาความรู้ที่ต้องการ

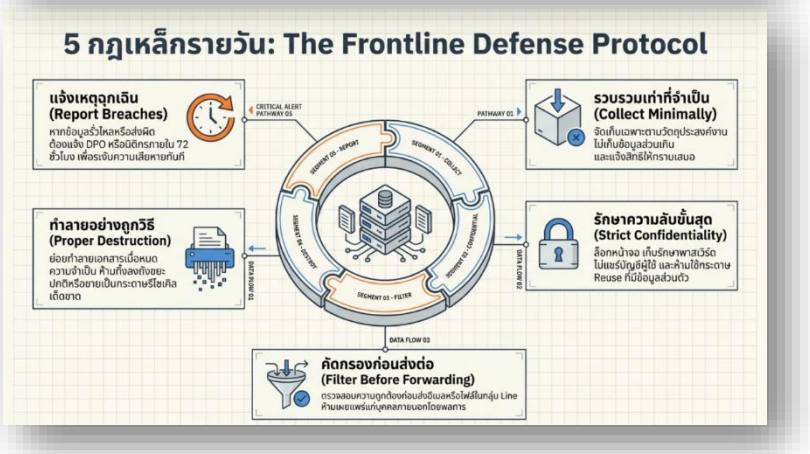
<u>กิจกรรมที่ 3</u> รวบรวมความรู้จากแหล่งต่าง ๆ ทั้งภายในและภายนอก คณะทำงานได้รวบรวมและศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA และตัวอย่าง Best Practice การลดความเสี่ยงและป้องกันการละเมิดข้อมูลส่วนบุคคลจากหน่วยงานที่ประสบความสำเร็จ ได้แก่ คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการณ์ละเมิดข้อมูล ของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ DGA เป็นหน่วยงานภาครัฐที่มีบทบาทกำหนดมาตรฐานบริการดิจิทัลภาครัฐ, แนวปฏิบัติพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (ภาคส่วนทั่วไป), การรักษาความมั่นคงปลอดภัยของข้อมูลและการแจ้งเหตุการณ์ละเมิด ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล(สคส.), และแนวปฏิบัติการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและรายงานของสำนักงานปลัดกระทรวงสาธารณสุข

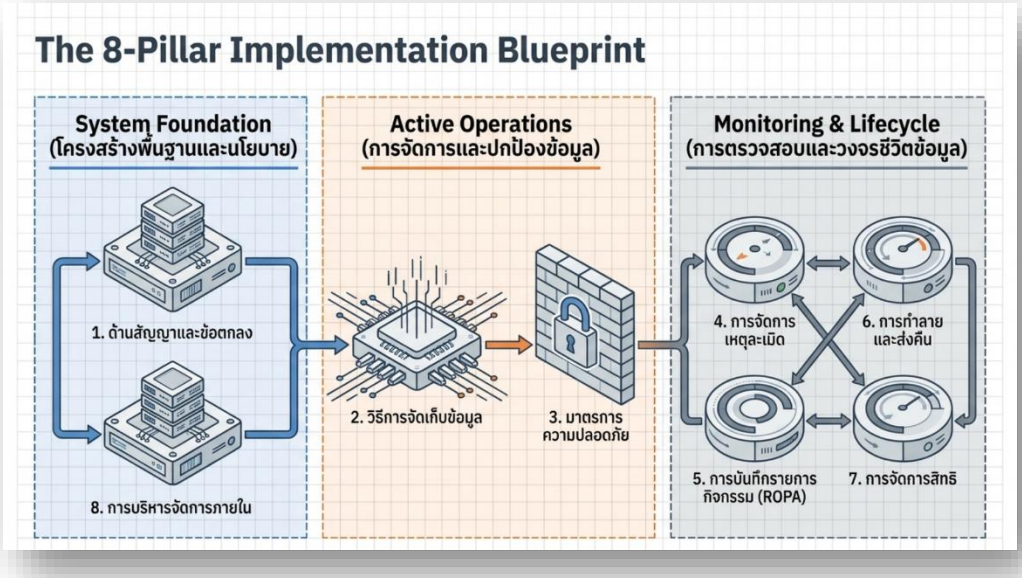
นอกจากนี้ได้อบรมออนไลน์ หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) จำนวน 3 ชั่วโมง เพื่อนำชุดความรู้มาปรับปรุงให้เหมาะสมกับงาน และคัดเลือกเผยแพร่ในสื่อส่งเสริมการเรียนรู้

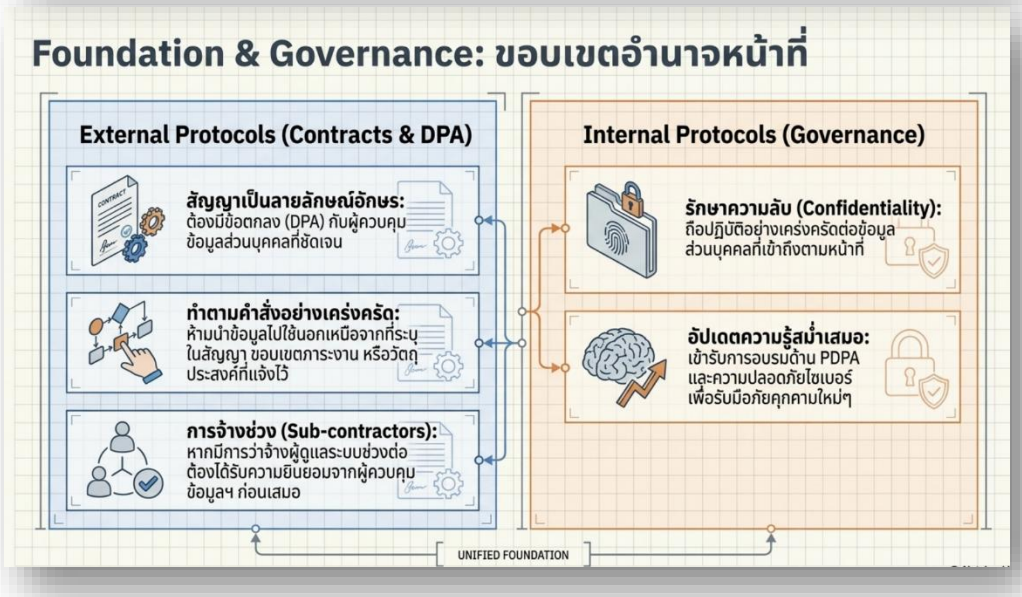
3. ปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน โดยการนำความรู้ที่ได้มาปรับให้เหมาะสมกับบริบทของมหาวิทยาลัย

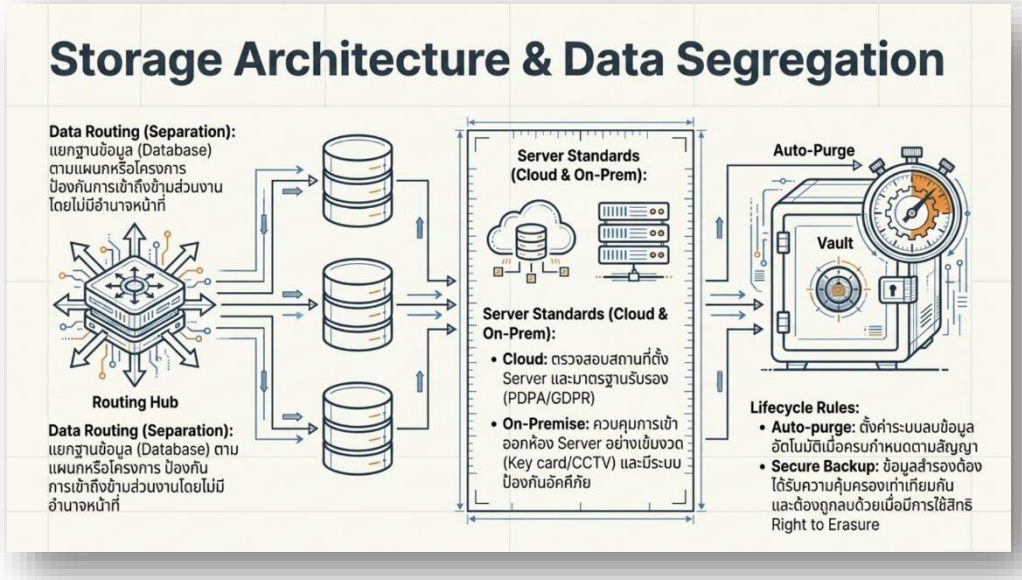
<u>กิจกรรมที่ 4</u> จัดทำเครื่องมือ/แนวทางปฏิบัติ เช่น คู่มือ, Checklist การใช้งานระบบที่ต้องระบุตัวตน หรือ Infographic สรุปข้อปฏิบัติของบุคลากร ทำให้ความรู้ PDPA ที่ซับซ้อนกลายเป็นเครื่องมือที่ใช้งานง่าย

(1) PDPA Master Checklist for IT Admins เช็กลิสต์และข้อปฏิบัติเชิงเทคนิค เพื่อการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล สำหรับ Admin



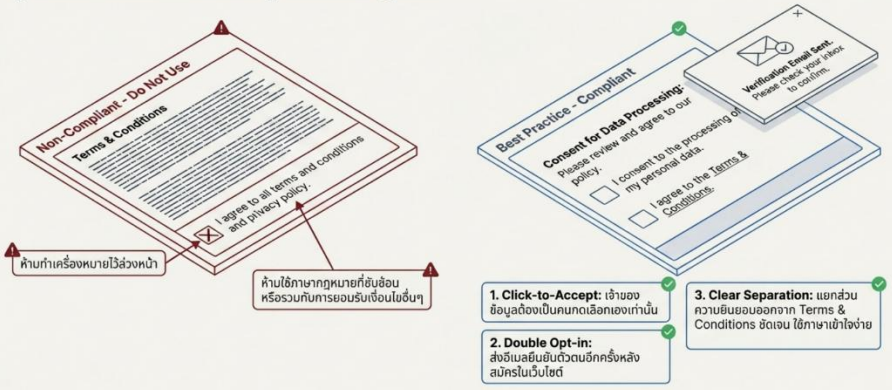

The 8-Pillar Implementation Blueprint
System Foundation
(โครงสร้างพื้นฐานและนโยบาย)
Active Operations
(การจัดการและปกป้องข้อมูล)
Monitoring & Lifecycle
(การตรวจสอบและวงจรชีวิตข้อมูล)
1. ด้านสัญญาและข้อตกลง
8. การบริหารจัดการภายใน
2. วิธีการจัดเก็บข้อมูล
3. มาตรการ
ความปลอดภัย
4. การจัดการ
เหตุละเมิด
6. การทำลาย
และส่งคืน
5. การบันทึกรายการ
กิจกรรม (ROPA)
7. การจัดการสิทธิ


Foundation & Governance: ขอบเขตอำนาจหน้าที่
External Protocols (Contracts & DPA)
สัญญาเป็นลายลักษณ์อักษร:
ต้องมีข้อตกลง (DPA) กับผู้ควบคุม
ข้อมูลส่วนบุคคลที่ชัดเจน
ทำตามคำสั่งอย่างเคร่งครัด:
ห้ามนำข้อมูลไปใช้นอกเหนือจากที่ระบุ
ในสัญญา ขอบเขตภาระงาน หรือวัตถุ
ประสงค์ที่แจ้งไว้
การจ้างช่วง (Sub-contractors):
หากมีการว่าจ้างผู้ดูแลระบบช่วงต่อ
ต้องได้รับความยินยอมจากผู้ควบคุม
ข้อมูลฯ ก่อนเสมอ
Internal Protocols (Governance)
รักษาความลับ (Confidentiality):
ถือปฏิบัติอย่างเคร่งครัดต่อข้อมูล
ส่วนบุคคลที่เข้าถึงตามหน้าที่
อัปเดตความรู้สม่ำเสมอ:
เข้ารับการอบรมด้าน PDPA
และความปลอดภัยไซเบอร์
เพื่อรับมือภัยคุกคามใหม่ๆ
UNIFIED FOUNDATION

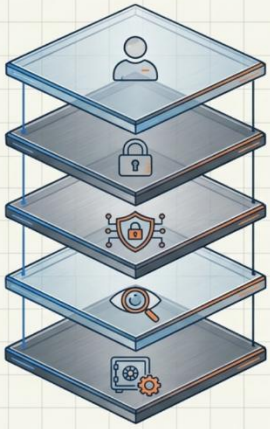

Storage Architecture & Data Segregation
Data Routing (Separation):
แยกฐานข้อมูล (Database)
ตามแผนกหรือโครงการ
ป้องกันการเข้าถึงข้ามส่วนงาน
โดยไม่มีอำนาจหน้าที่
Routing Hub
Data Routing (Separation):
แยกฐานข้อมูล (Database) ตาม
แผนกหรือโครงการ ป้องกัน
การเข้าถึงข้ามส่วนงานโดยไม่มี
อำนาจหน้าที่
Server Standards
(Cloud & On-Prem):
Server Standards (Cloud &
On-Prem):
• Cloud: ตรวจสอบสถานที่ตั้ง
Server และมาตรฐานรับรอง
(PDPA/GDPR)
• On-Premise: ควบคุมการเข้า
ออกห้อง Server อย่างเข้มงวด
(Key card/CCTV) และมีระบบ
ป้องกันอัคคีภัย
Auto-Purge
Vault
Lifecycle Rules:
• Auto-purge: ตั้งค่าระบบลบข้อมูล
อัตโนมัติเมื่อครบกำหนดตามสัญญา
• Secure Backup: ข้อมูลสำรองต้อง
ได้รับความคุ้มครองเท่าเทียมกัน
และต้องถูกลบด้วยเมื่อมีการใช้สิทธิ
Right to Erasure

Legal Consent Mechanisms in UI/UX

รูปแบบการขอความยินยอมที่ถูกต้องตามกฎหมาย



The Security Measures Framework (SOC Stack)



- **Layer 1: Authentication -** ใช้ระบบยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) สำหรับการเข้าถึงระบบฐานข้อมูล
- **Layer 2: Access Control -** กำหนดสิทธิ์ตามหลัก Least Privilege (ให้สิทธิ์เฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น)
- **Layer 3: Encryption -** เข้ารหัสข้อมูลทั้งขณะรับส่งข้อมูล (In transit) และขณะจัดเก็บ (At rest)
- **Layer 4: Logging & Monitoring -** บันทึก Log files เพื่อตรวจสอบย้อนหลัง (ใคร, เข้าถึงอะไร, เมื่อใด)
- **Layer 5: Backup & Recovery -** สำรองข้อมูลสม่ำเสมอ และทดสอบแผนการกู้คืนเพื่อให้ระบบพร้อมใช้งาน (Availability) เสมอ

Active Monitoring: Breach Incident SOP & ROPA

Data Breach Management (SOP)

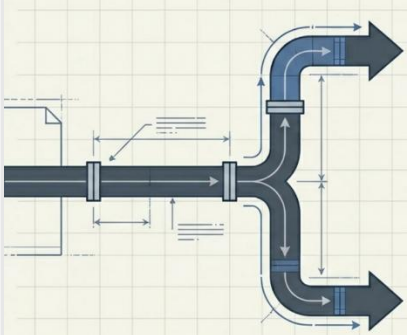
Detect → Alert → Report → 72 HOURS

- จัดทำขั้นตอนการปฏิบัติงาน (SOP) สำหรับรับมือข้อมูลรั่วไหล
- เมื่อพบเหตุต้องสงสัย ต้องแจ้งผู้ควบคุมข้อมูลทันที (ภายใน 24-72 ชั่วโมง)

Record of Processing (ROPA)

- จัดทำและอัปเดตบัญชีรายการกิจกรรม (ROPA) ให้เป็นปัจจุบัน
- ระบุ: ประเภทข้อมูล, วัตถุประสงค์, และระยะเวลาจัดเก็บ
- Special Requirement: ข้อมูลอ่อนไหว/อาชญากรรม ต้องมีการบันทึกการประมวลผลเป็นหนังสือหรือระบบอิเล็กทรอนิกส์อย่างเคร่งครัด

Data Lifecycle Management & Subject Rights

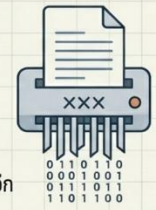


การจัดการสิทธิ
(Data Subject Rights Readiness):

- เตรียมระบบให้พร้อมสนับสนุนผู้ควบคุมข้อมูล
- รองรับการขอใช้สิทธิของเจ้าของข้อมูล (เช่น ขอเข้าถึง, ขอระงับการใช้, ขอลบ) ภายในเวลาที่กฎหมายกำหนด

การทำลายและส่งคืน
(Retention & Disposal):

- เมื่อสิ้นสุดสัญญา/ภารกิจ ต้องลบ ทำลาย หรือส่งคืนข้อมูลทั้งหมด
- ใช้วิธี Data Sanitization ที่ได้มาตรฐาน เพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้อีก



The Data Asset Radar

หมวดหมู่ข้อมูลที่ระบบ IT ต้องควบคุมดูแล

Quadrant 1: Digital Footprints
(ร่องรอยดิจิทัล)

- หมายเลข IP Address, Cookies, Browser, Device ID, Time zone.
- การเข้าสู่ระบบ (Logins), Username/ Password, PIN, App activity logs.

Quadrant 2: Identity & Profile
(ข้อมูลระบุตัวตนบุคคล)

- ข้อมูลรายละเอียดส่วนบุคคล และการระบุ/ยืนยันตัวตน.
- ข้อมูลการติดต่อ, การทำงาน, การศึกษา.

Quadrant 3: Behavioral & Commercial
(พฤติกรรมและการทำธุรกรรม)

- ข้อมูลการเงิน และ การรับบริการ.
- ข้อมูลกรมธรรม์ประกันภัย.
- ข้อมูลวิจัยตลาด และ ข้อมูลการสื่อสาร (บันทึกสนทนา).

Quadrant 4: Highly Sensitive
(ข้อมูลอ่อนไหว - ควบคุมพิเศษ)

ข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data) ต้องใช้มาตรการขั้นสูงสุดและบันทึก ROPA เสมอ.

ROPA

Self-Audit Diagnostic Matrix

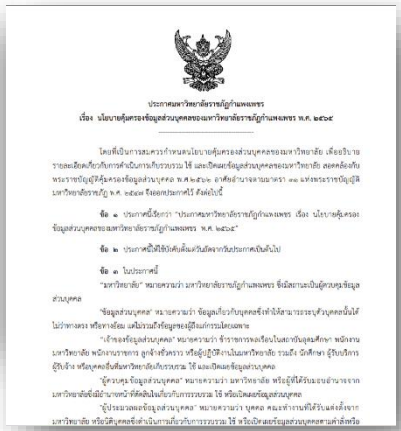
	ดำเนินการแล้ว (Done)	ยังไม่ได้ดำเนินการ (Not Done)
1. ทำสัญญา DPA และตรวจสอบเงื่อนไข Sub-processor แล้ว	☐	☐
2. แยก Database ตามแผนก และตั้งระบบลบอัตโนมัติ (Auto-purge)	☐	☐
3. UI/UX การขอความยินยอมไม่มีการติ๊กเลือกไว้ล่วงหน้า (No pre-tick)	☐	☐
4. Server และ Backup มีการเข้ารหัส (Encryption) และจำกัดการเข้าถึง (MFA)	☐	☐
5. มี SOP รับมือเหตุข้อมูลรั่วไหล และพร้อมแจ้งเหตุใน 72 ชม.	☐	☐
6. อัปเดต ROPA โดยเฉพาะการบันทึกข้อมูลประเภทอ่อนไหว	☐	☐
7. ระบบรองรับการลบ/ระงับข้อมูลตามสิทธิ (Data Subject Rights)	☐	☐
8. มีกระบวนการ Data Sanitization ที่กู้คืนไม่ได้เมื่อจบงาน	☐	☐

สถานะของระบบ IT ในปัจจุบันของคุณเป็นอย่างไร? นำเช็กลิสต์นี้ไปใช้ประเมินทันที

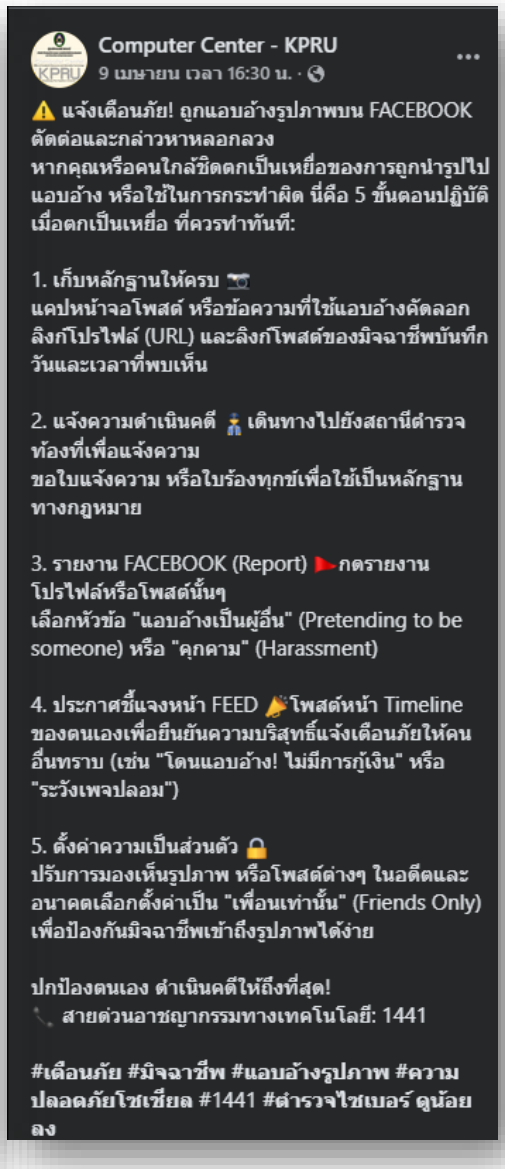
(2) สร้างกลไกการรับรู้นโยบายการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

โดยเผยแพร่ **ประกาศ นโยบายคุ้มครองข้อมูลส่วนบุคคล** ประชาสัมพันธ์ไว้ที่หน้าหลักเว็บไซต์มหาวิทยาลัยราชภัฏกำแพงเพชร ดังภาพ

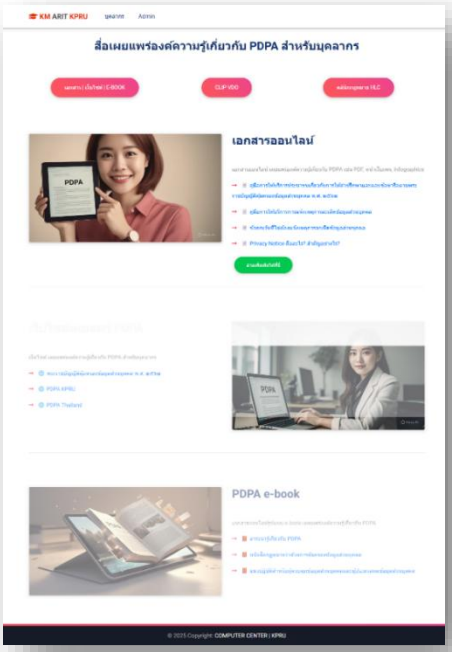
เมื่อคลิกอ่านนโยบาย จะแสดงหน้าเว็บไซต์ PDPA รวบรวมข้อมูลที่เกี่ยวข้อง ดังลิงค์ https://kpru.ac.th/pdpa/

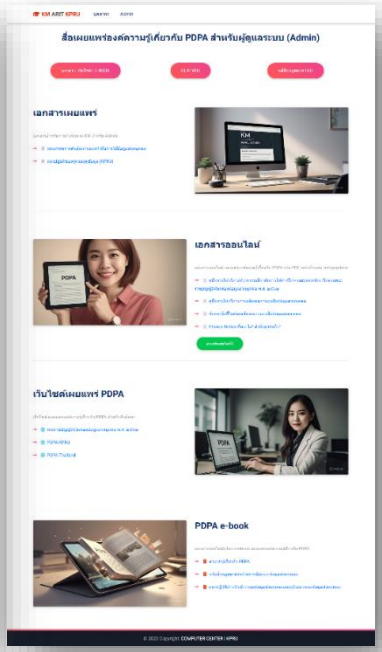


(3) จัดทำ Infographic แนวปฏิบัติ แผนผังขั้นตอน และอื่นๆที่เกี่ยวข้อง เผยแพร่ผ่านเว็บไซต์มหาวิทยาลัย และ เพจ ศูนย์คอมพิวเตอร์

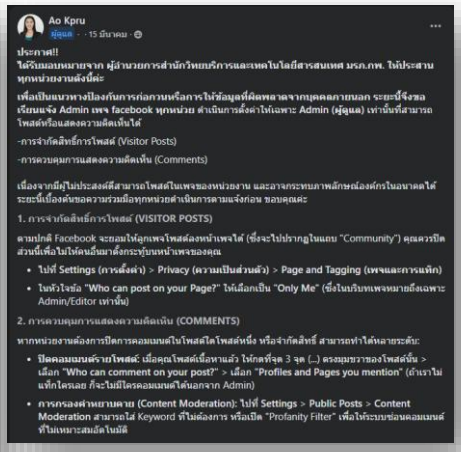


(4) เผยแพร่องค์ความรู้เกี่ยวกับ PDPA ผ่านสื่อส่งเสริมการเรียนรู้ PDPA





(5) เผยแพร่ มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการละเมิดข้อมูลส่วนบุคคล(การตั้งค่าสื่อสังคมออนไลน์ จำกัดสิทธิ์การโพสต์และการแสดงความคิดเห็น) ประสานงาน Admin ผ่านกลุ่มผู้ดูแลเว็บภายใน KPRU




[ด่วนที่สุด]
แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน
เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล
สืบเนื่องจากกรณีการนำภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้
1
1. ปิดสิทธิ์โพสต์สาธารณะ
ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง
2
2. เปิดระบบคัดกรองอัตโนมัติ
ใช้งาน Moderation Assist เพื่อตั้งค่าซ่อนความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย
ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย


Ao Kpru
ผู้ดูแล · 10 เมษายน เวลา 12:04 น.
แจ้ง Admin ทุกหน่วยงานทราบ
1. [ด่วนที่สุด] แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล
สืบเนื่องจากกรณีเมื่อวันที่ 8 เมษายน 2569 เกิดเหตุมีการนำภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้
(1) ปิดสิทธิ์โพสต์สาธารณะ ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง
(2) เปิดระบบคัดกรองอัตโนมัติ ใช้งาน Moderation Assist เพื่อตั้งค่าซ่อนความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย
ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย
2. นัดหมาย และแจ้งกำหนดจัดกิจกรรมแลกเปลี่ยนเรียนรู้สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล วันพุธที่ 29 เมษายน 2569 เวลา 09.00-12.00 น. ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
Ao Kpru
ผู้ดูแล · 9 เมษายน เวลา 11:56 น.
ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์กระทำความผิดในลักษณะนำรูปภาพส่วนตัวจากสื่อสังคมออนไลน์มาดัดแปลงเพื่อบิดเบือนข้อเท็จจริง และเผยแพร่ผ่านช่องทางการแสดงความคิดเห็น (Comment) ในหน้าเพจ Facebook ของหน่วยงานภายในมหาวิทยาลัย ซึ่งการกระทำดังกล่าวมิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ แต่มีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล นั้น
เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเ... ดูเพิ่มเติม
แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศ และการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน
สืบเนื่องจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เมื่อวันที่ 15 มีนาคม 2569 โดยการบิดเบือนรูปภาพและเผยแพร่ผ่านความคิดเห็นในหน้าเพจ Facebook
1. จำกัดสิทธิ์การโพสต์
ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง
2. ยกระดับการคัดกรอง
เปิดใช้งาน 'ตัวช่วยการควบคุม' (Moderation Assist)
ตั้งค่าคัดกรองความคิดเห็น (Comment Filtering)
ซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญบิดเบือนอัตโนมัติ
อ้างอิง: มติคณะกรรมการบริหารมหาวิทยาลัย ครั้งที่ 4/2569 วันที่ 2 เมษายน 2569


การปิดสิทธิ์โพสต์บนเพจ Facebook ของหน่วยงาน
เพื่อความปลอดภัยและภาพลักษณ์ที่เป็นทางการ
1. เข้าสู่ระบบ
ด้วยบัญชีผู้ดูแล (Admin)
2. สลับไปเพจหน่วยงาน
เลือกสลับการใช้งานไปยังเพจ
3. ไปที่การตั้งค่า
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > การตั้งค่า
4. เลือกความเป็นส่วนตัว & เพจและการแท็ก
ในเมนูด้านซ้าย เลือก "ความเป็นส่วนตัว" > "เพจและการแท็ก"
5. ตั้งค่าใครสามารถโพสต์ได้
เลือก "เฉพาะฉัน"
6. บันทึกอัตโนมัติ
ระบบจะบันทึกการตั้งค่าให้โดยอัตโนมัติ
จัดการเพจอย่างมืออาชีพ


การตั้งค่าตัวกรองคำหยาบและคำเฉพาะ
เพื่อการควบคุมเนื้อหาและภาพลักษณ์ที่ดี
1. สลับโปรไฟล์ไปที่หน้าเพจ
เลือกสลับบัญชีเป็นผู้ดูแลเพจ
2. ไปที่การตั้งค่า (Settings)
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > ความเป็นส่วนตัว
3. เลือกโพสต์สาธารณะ (Public Posts)
ในเมนูด้านซ้าย เลือก "โพสต์สาธารณะ"
4. ตรวจสอบเนื้อหา (Content Moderation)
มองหาและคลิกหัวข้อ "การตรวจสอบเนื้อหา"
5. ซ่อนความคิดเห็น
ซ่อนความคิดเห็นที่มีคำบางคำ
มี_มี_, ฎ_ฎ_, คำไม่สุภาพ, คำด่า
6. บันทึก (Save)
กดปุ่ม "บันทึก" เพื่อสิ้นสุด
จัดการเพจอย่างมืออาชีพ

(6) รายงานผลการป้องกันและรับมือเหตุละเมิดของข้อมูลส่วนบุคคล นำเสนอการประชุมคณะกรรมการบริหารมหาวิทยาลัย (วาระเพื่อพิจารณา 5.2 ประเด็นที่ 3) รายละเอียดโดยสรุปดังนี้

<u>รายงานสถานการณ์และการตรวจพบเหตุละเมิด</u>

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์การกระทำความผิด ดังนี้

- ลักษณะการกระทำ มีการนำรูปภาพของบุคลากรและบุคคลภายนอกไปตัดต่อโดยไม่ได้รับอนุญาต เพื่อสร้างสื่อบิดเบือนข้อเท็จจริงในลักษณะการทวงหนี้ และกล่าวหาว่าเป็นส่วนหนึ่งของขบวนการฉ้อโกง

- ช่องทางที่เกิดเหตุ การนำภาพตัดต่อดังกล่าวไปเผยแพร่ผ่านช่องการแสดงความคิดเห็น (Comment) ในเพจ Facebook "โสตทัศนวัสดุ มหาวิทยาลัยราชภัฏกำแพงเพชร"

<u>การดำเนินการโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)</u>

ภายหลังตรวจพบเหตุ มหาวิทยาลัยฯ **<u>ได้ดำเนินการตามขั้นตอนมาตรฐานทางกฎหมาย (PDPA) อย่างเร่งด่วน</u>** ดังนี้

- การรายงานเหตุ รายงานสรุปเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อผู้บริหารระดับสูง (อธิการบดี/รองอธิการบดี) เพื่อทราบสถานการณ์

- การแจ้งเหตุต่อหน่วยงานกำกับดูแล ดำเนินการจัดทำหนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายในกรอบเวลา 72 ชั่วโมงตามที่กฎหมายกำหนด

- การเยียวยาผู้ได้รับผลกระทบ จัดทำบันทึกแจ้งเหตุให้แก่ผู้ที่ได้รับผลกระทบโดยตรง พร้อมให้คำแนะนำในการปฏิบัติตนและการคุ้มครองสิทธิ์รายบุคคล

<u>มาตรการตอบโต้ทางเทคนิคและทางกฎหมาย (สำนักวิทยบริการฯ)</u>

เพื่อให้เกิดการแก้ไขที่ต้นเหตุและป้องกันการขยายตัวของความเสียหาย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการ ดังนี้

- การรวบรวมพยานหลักฐาน เก็บรวบรวมหลักฐานทางดิจิทัลทั้งหมด และมอบหมายให้ผู้ดูแลเพจดำเนินการแจ้งความลงบันทึกประจำวันไว้เป็นหลักฐานทางกฎหมาย

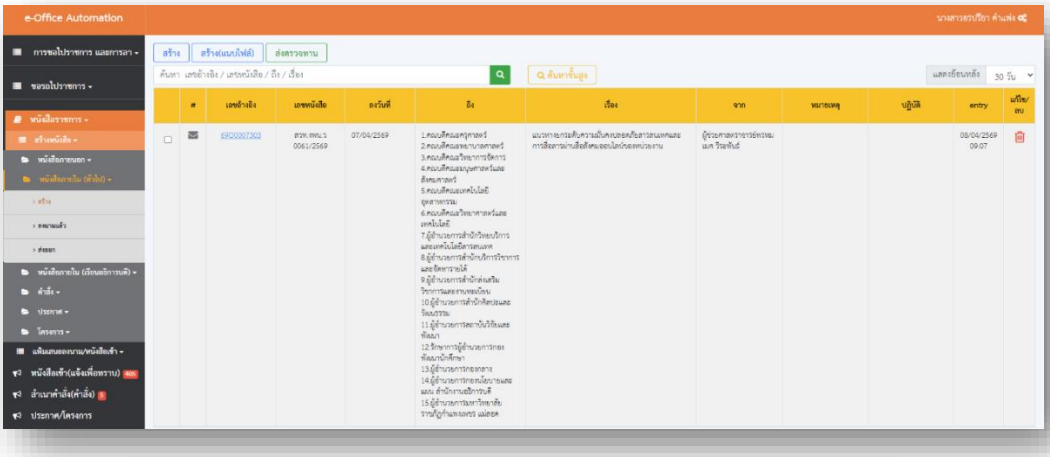
- มาตรการป้องกันเชิงรุกสำหรับทุกหน่วยงาน ประสานงานเครือข่ายผู้ดูแล (Admin) Facebook Page ทุกหน่วยงานภายในมหาวิทยาลัย ให้ยกระดับการตั้งค่าความปลอดภัย ดังนี้

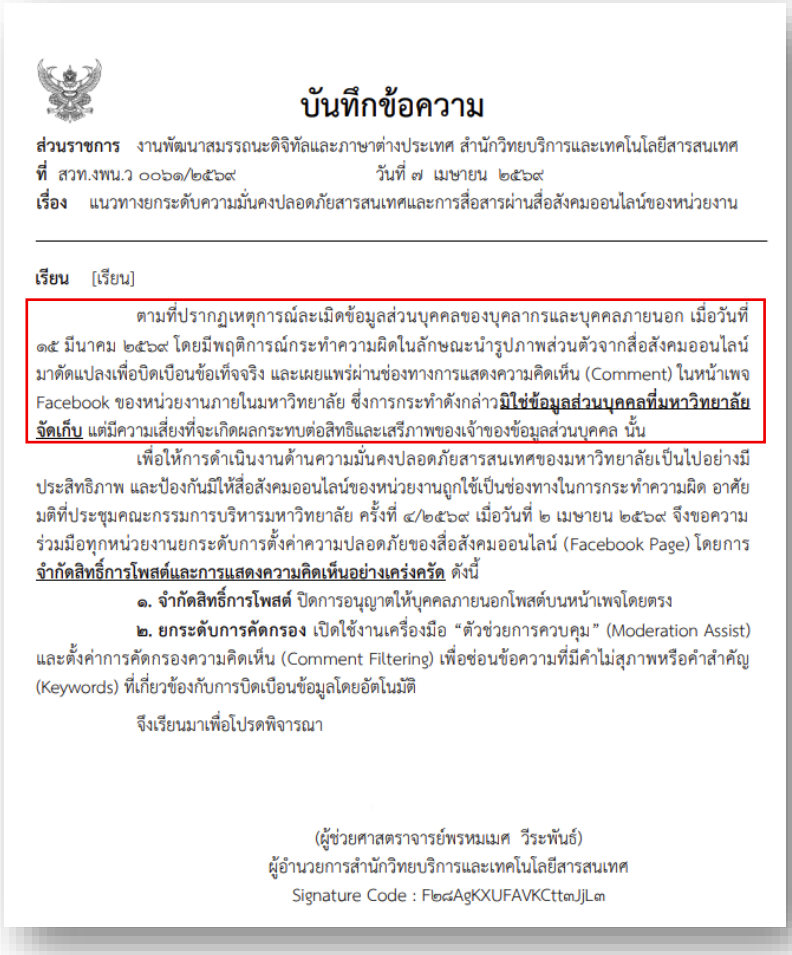
1. จำกัดสิทธิ์การโพสต์ ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง (Disable Visitor Posts)

2. ยกระดับการคัดกรอง เปิดใช้งานเครื่องมือ Moderation Assist และตั้งค่าการคัดกรองความคิดเห็น (Comment Filtering) เพื่อซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญ (Keywords) ที่เกี่ยวข้องกับการบิดเบือนข้อมูล โดยอัตโนมัติ

จึงเรียนที่ประชุมทราบแนวทางการจัดการเหตุละเมิด และขอความร่วมมือทุกหน่วยงานตรวจสอบและรักษามาตรฐานการตั้งค่าสื่อสังคมออนไลน์โดยการ**<u>จำกัดสิทธิ์การโพสต์และการแสดงความคิดเห็นอย่างเคร่งครัด</u>** ทั้งนี้ สำนักวิทยบริการฯ ได้ดำเนินการจัดส่งบันทึกข้อความแจ้งเวียนไปในระบบ E-Office วันที่ 7 เมษายน 2569

(7) จัดส่งบันทึกข้อความ แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศและการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน แจ้งเวียนไปในยัง คณบดี/ผู้อำนวยการสำนัก สถาบัย ผ่านระบบ E-Office วันที่ 7 เมษายน 2569





บันทึกข้อความ

ส่วนราชการ งานพัฒนาสมรรถนะดิจิทัลและภาษาต่างประเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
ที่ สวท.งพน.ว ๐๐๖๑/๒๕๖๙ **วันที่** ๗ เมษายน ๒๕๖๙
เรื่อง แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศและการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน

เรียน [เรียน]

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ ๑๕ มีนาคม ๒๕๖๙ โดยมีพฤติการณ์กระทำความผิดในลักษณะนำรูปภาพส่วนตัวจากสื่อสังคมออนไลน์มาดัดแปลงเพื่อบิดเบือนข้อเท็จจริง และเผยแพร่ผ่านช่องทางการแสดงความคิดเห็น (Comment) ในหน้าเพจ Facebook ของหน่วยงานภายในมหาวิทยาลัย ซึ่งการกระทำดังกล่าว**มิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ** แต่มีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล นั้น

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยเป็นไปอย่างมีประสิทธิภาพ และป้องกันมิให้สื่อสังคมออนไลน์ของหน่วยงานถูกใช้เป็นช่องทางในการกระทำความผิด อาศัยมติที่ประชุมคณะกรรมการบริหารมหาวิทยาลัย ครั้งที่ ๔/๒๕๖๙ เมื่อวันที่ ๒ เมษายน ๒๕๖๙ จึงขอความร่วมมือทุกหน่วยงานยกระดับการตั้งค่าความปลอดภัยของสื่อสังคมออนไลน์ (Facebook Page) โดยการ**จำกัดสิทธิ์การโพสต์และการแสดงความคิดเห็นอย่างเคร่งครัด** ดังนี้

๑. จำกัดสิทธิ์การโพสต์ ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง

๒. ยกระดับการคัดกรอง เปิดใช้งานเครื่องมือ “ตัวช่วยการควบคุม” (Moderation Assist) และตั้งค่าการคัดกรองความคิดเห็น (Comment Filtering) เพื่อซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญ (Keywords) ที่เกี่ยวข้องกับการบิดเบือนข้อมูลโดยอัตโนมัติ

จึงเรียนมาเพื่อโปรดพิจารณา

(ผู้ช่วยศาสตราจารย์พรหมเมศ วีระพันธ์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
Signature Code : Fb๔AgKXUFAVKCttaJjLa

จากบันทึกข้อความข้างต้น เหตุการณ์ละเมิดข้อมูลส่วนบุคคลในวันดังกล่าว มิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ **จึงสรุปได้ว่า ไม่มีการได้รับรายงานการละเมิดข้อมูลส่วนบุคคล**

(8) ขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (PDPA Response Plan)

ขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (PDPA Response Plan) เพื่อให้เข้าใจง่ายและพร้อมนำไปใช้งานจริงเมื่อเกิดเหตุฉุกเฉิน สรุป 4 ขั้นตอนหลัก ดังนี้

<u>ขั้นตอนที่ 1</u> ตรวจพบ & สกัดกั้น (Containment) — *ภายใน 24 ชม. แรก*

- **ตัดวงจรการรั่วไหล** สั่งปิดระบบ ย้ายเซิร์ฟเวอร์ หรือตัดการเชื่อมต่อเครือข่ายของระบบที่เกิดเหตุทันที เพื่อหยุดไม่ให้ข้อมูลไหลออกเพิ่ม
- **เก็บหลักฐานทางดิจิทัล** บันทึก Log ไฟล์ และถ่ายภาพหน้าจอจุดที่เกิดช่องโหว่ (ห้ามลบหรือแก้ไข)
- **รายงานด่วน** ผู้ดูแลระบบหรือผู้พบเหตุแจ้งเรื่องไปยัง **DPO (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล) ของมหาวิทยาลัย** ทันที

<u>ขั้นตอนที่ 2</u> ประเมินความเสี่ยง (Risk Assessment) — *ภายใน 48 ชม.*

- **วิเคราะห์ข้อมูล** DPO ร่วมกับทีม IT ตรวจสอบว่าข้อมูลที่หลุดเป็นประเภทใด (ข้อมูลทั่วไป หรือข้อมูลอ่อนไหว) และส่งผลกระทบต่อนักศึกษาหรือบุคลากรจำนวนเท่าใด
- **แบ่งระดับความรุนแรง**
  - *มีความเสี่ยง* ต้องแจ้ง สคส. (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล)
  - *มีความเสี่ยงสูง* ต้องแจ้งทั้ง สคส. และส่งข้อความเตือนเจ้าของข้อมูลทุกคน
- **สรุปเรื่องเสนอต่ออธิการบดี** เพื่ออนุมัติมาตรการขั้นต่อไป

<u>ขั้นตอนที่ 3</u> แจ้งเตือนตามกฎหมาย (Notification) — *ต้องเสร็จสิ้นใน 72 ชม.*

- **แจ้งหน่วยงานกำกับดูแล** DPO ส่งหนังสือรายงานเหตุละเมิดอย่างเป็นทางการให้สำนักงาน สคส. ทันที ตามกรอบเวลาทางกฎหมาย 72 ชั่วโมง
- **แจ้งผู้เสียหาย** ส่งอีเมลและ SMS แจ้งเตือนนักศึกษาและบุคลากรที่ได้รับผลกระทบโดยตรง เพื่อเตือนให้ระวังมิจฉาชีพ แนะนำให้รีบเปลี่ยนรหัสผ่าน KPRU Account และเฝ้าระวังการหลอกลวง
- **ควบคุมการให้ข่าว** ให้งานประชาสัมพันธ์เป็นสื่อกลางหลักช่องทางเดียวเพื่อป้องกันข้อมูลคลาดเคลื่อน

<u>ขั้นตอนที่ 4</u> อุดช่องโหว่ & เยียวยา (Recovery & Remediation) — *หลังเกิดเหตุ*

- **ซ่อมแซมระบบถาวร** ทีมไอทีทำการอุดช่องโหว่ อัปเดต Patch ปรับปรุงกฎ Web Application Firewall (WAF) และกู้คืนระบบที่ปลอดภัยจาก Backup
- **อนุมัติงบฉุกเฉิน** อธิการบดีอนุมัติงบกลางในการจัดหาซอฟต์แวร์ความปลอดภัยเพิ่มเติม หรือจ้างผู้เชี่ยวชาญภายนอกเข้ามาช่วยสืบสวนเชิงลึก
- **ตั้งศูนย์เยียวยา** จัดตั้งทีมให้คำปรึกษาทางกฎหมาย กรณีถูกแอบอ้างสิทธิ์ และดูแลสภาพจิตใจ กรณีเป็นข้อมูลอ่อนไหวที่กระทบต่อชื่อเสียง
- **บันทึกและถอดบทเรียน** บันทึกประวัติลงใน **Breach Log** ตามกฎหมาย และประชุมสรุปแนวทางเพื่อป้องกันการเกิดเหตุซ้ำ

สรุปแนวปฏิบัติสำคัญ

- ความเร็วคือหัวใจ ทุกขั้นตอนมีเงื่อนไขเวลาควบคุม โดยเฉพาะกรอบเวลา 72 ชั่วโมง ของกฎหมาย PDPA ดังนั้นการประสานงานภายในต้องกระชับและรวดเร็ว

- ความลับและการเก็บหลักฐาน ขณะระงับเหตุ เจ้าหน้าที่ห้ามทำการใดๆ ที่เป็นการทำลายหลักฐาน (Log) และต้องควบคุมการสื่อสารภายในไม่ให้เกิดความตื่นตระหนกก่อนจะประเมินสถานการณ์เสร็จสิ้น

- รับผิดชอบและจริงใจ การแจ้งเหตุแก่ผู้เสียหายด้วยข้อความที่ชัดเจน พร้อมแนวทางแก้ไขและการดูแลเยียวยา ทั้งทางระบบและทางจิตใจ จะช่วยรักษาความน่าเชื่อถือของมหาวิทยาลัยได้ดีที่สุด

(9) ตัวอย่างการประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

ตัวอย่างเหตุการณ์ละเมิดข้อมูลส่วนบุคคลจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) นี้เป็นแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล ว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าว ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
1	ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ความเสี่ยงต่ำ เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้วข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
2	ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก
3	ระบบไฟฟ้าใน Call center ของ คณะ ส่วนงาน	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าว ไม่อยู่ในสภาพพร้อมใช้งานเนื่องจาก

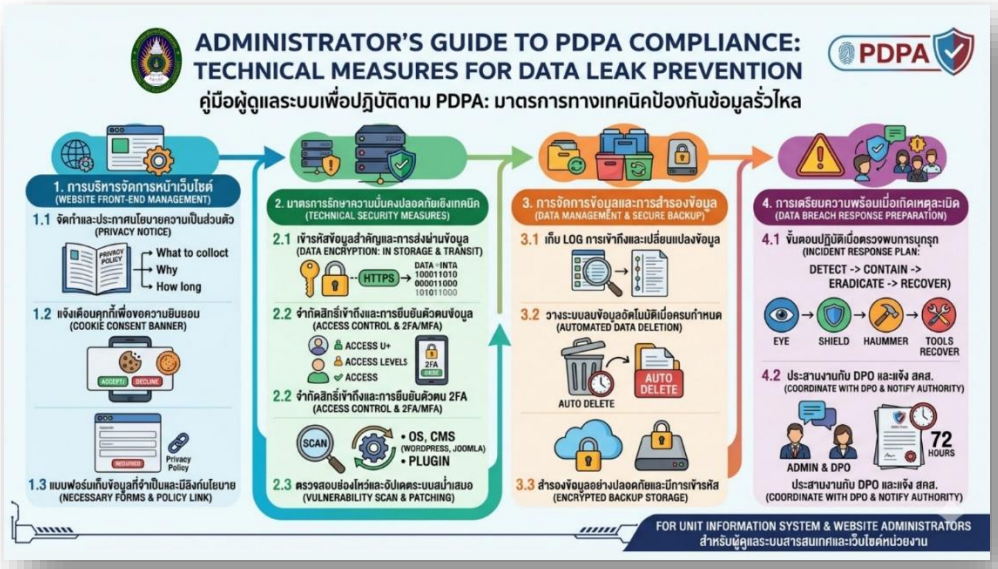
ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
	หน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ขัดข้อง โดยไฟดับชั่วคราว ส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของคณะ ส่วนงาน หน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว			ปัญหาทางด้านเทคโนโลยีเมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วนบุคคลดังกล่าว ก็สามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบคคล
4	ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์ โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูล ส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้และการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง นอกจากนี้ยังอาจก่อให้เกิดความเสียหายต่อธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงตัวเจ้าของข้อมูลส่วนบุคคลจึงต้องแจ้งเหตุ
5	ธนาคารได้รับการติดต่อจากลูกค้าธนาคาร 1 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้วภายใน 24 ชั่วโมง พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน 10 ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล 10 ราย ที่ถูกเรียกเก็บเงินตาม ใบแจ้งหนี้ของธนาคาร	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตามคณะ ส่วนงาน หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม
6	ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาผู้ควบคุมข้อมูลส่วนบุคคลถูกโจมตีจากภัยคุกคามทาง	ต้องแจ้ง	ต้องแจ้งลูกค้าของผู้ควบคุมข้อมูลส่วนบุคคลในส่วนที่มีข้อมูลรั้วไหลบน อินเทอร์เน็ต	ข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

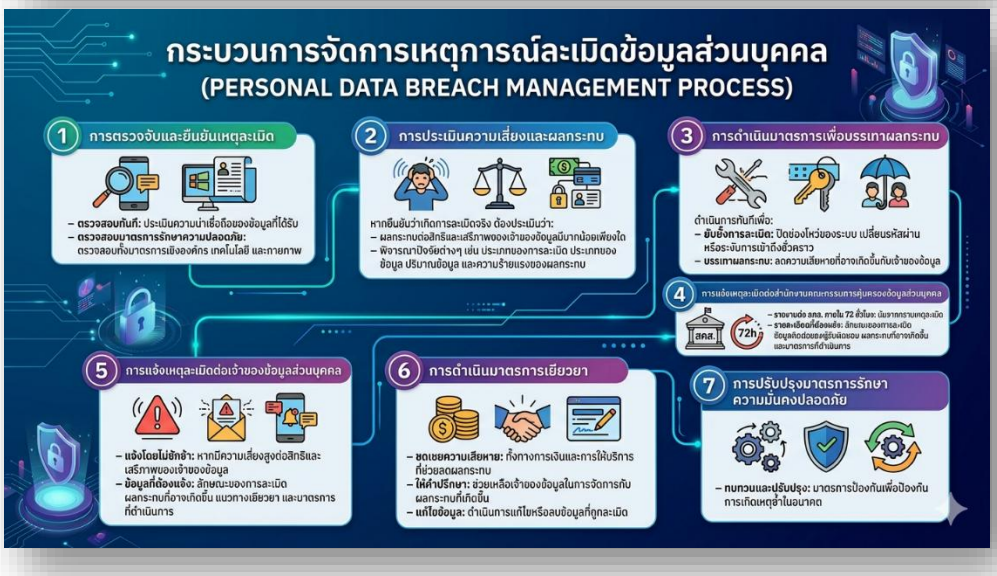
ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
	ไซเบอร์ โดยข้อมูลรายชื่อผู้ใช้บริการ รหัสผ่าน และประวัติการซื้อสินค้าถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต			ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย
7	เว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลเกิดปัญหาอผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง ทำให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้	ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งสำนักงานฯ เนื่องจากมีผลกระทบต่อกลุ่มลูกค้าพอสมควร เพราะปัญหาดังกล่าวทำให้กลุ่มลูกค้าไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้	ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับผลกระทบ เนื่องจากยังไม่เกิดปัญหา	ในเบื้องต้นเป็นเพียงข้อผิดพลาดของโปรแกรมที่ทำให้เข้าถึงข้อมูลส่วนบุคคลไม่ได้ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามีภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกคามทางไซเบอร์เว็บไซต์ผู้ให้บริการ Web Hosting ต้องรีบแจ้งผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลต้องรีบแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลต่อไป
8	โรงพยาบาลแห่งหนึ่งถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก hacker ทำให้ประวัติของผู้ป่วยไม่สามารถเข้าถึงได้เป็นเวลา 30 ชั่วโมง	ต้องแจ้ง เนื่องจากข้อมูลประวัติของผู้ป่วยเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและสามารถระบุตัวบุคคลได้	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิดหรือมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าวรวมถึงข้อมูลสุขภาพด้วย เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุและตรวจสอบข้อมูลเพิ่มเติม
9	โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทาง	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าวไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวน

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
	อีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน			มาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งผู้รับเหมาอาจจะนำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
10	บริษัทแห่งหนึ่งทำการตลาดแบบตรง โดยการส่งข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลแต่ละราย แต่ด้วยความผิดพลาด จึงมีการใส่ที่อยู่ของบุคคลที่รับอีเมลทั้ง 100 คน เข้าไปในช่อง To หรือ Cc ทำให้ผู้รับอีเมลเห็นอีเมลที่มีข้อมูลส่วนบุคคลของบุคคลอื่น	ต้องแจ้ง เนื่องจากเป็นการส่งข้อมูลของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก จึงจำเป็นต้องแจ้งเหตุ แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลในอีเมลดังกล่าวอาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลภายหลังได้	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ อาจขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไปและลักษณะของข้อมูลด้วยหากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด อาจถือว่ามีความเสี่ยงต่ำไม่จำเป็นต้องแจ้งเหตุ

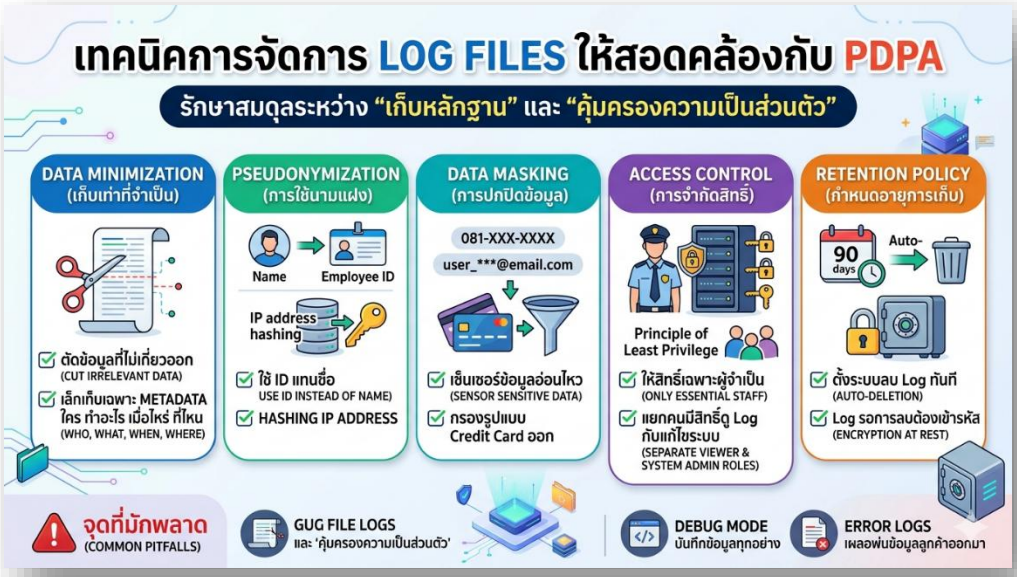
หมายเหตุ ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลทั้ง 10 ตัวอย่าง ดังกล่าวข้างต้น เป็นเพียงแนวทางในการประเมินความสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณี ๆ ไป

(10) Infographic อื่นๆที่เกี่ยวข้อง


ADMINISTRATOR'S GUIDE TO PDPA COMPLIANCE:
TECHNICAL MEASURES FOR DATA LEAK PREVENTION
คู่มือผู้ดูแลระบบเพื่อปฏิบัติตาม PDPA: มาตรการทางเทคนิคป้องกันข้อมูลรั่วไหล
PDPA
1. การบริหารจัดการหน้าเว็บไซต์
(WEBSITE FRONT-END MANAGEMENT)
1.1 จัดทำและประกาศนโยบายความเป็นส่วนตัว
(PRIVACY NOTICE)
What to collect
Why
How long
1.2 แจ้งเตือนคุกกี้เพื่อขอความยินยอม
(COOKIE CONSENT BANNER)
ACCEPT
DECLINE
1.3 แบบฟอร์มเก็บข้อมูลที่จำเป็นและมีลิงก์นโยบาย
(NECESSARY FORMS & POLICY LINK)
REQUIRED
Privacy Policy
2. มาตรการรักษาความมั่นคงปลอดภัยเชิงเทคนิค
(TECHNICAL SECURITY MEASURES)
2.1 เข้ารหัสข้อมูลสำคัญและการส่งผ่านข้อมูล
(DATA ENCRYPTION: IN STORAGE & TRANSIT)
HTTPS
DATA =INTA
100011010
000011000
2.2 จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตนข้อมูล
(ACCESS CONTROL & 2FA/MFA)
ACCESS U+
ACCESS LEVELS
ACCESS
2FA
2.2 จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตน 2FA
(ACCESS CONTROL & 2FA/MFA)
SCAN
• OS, CMS
(WORDPRESS, JOOMLA)
• PLUGIN
2.3 ตรวจสอบช่องโหว่และอัปเดตระบบสม่ำเสมอ
(VULNERABILITY SCAN & PATCHING)
3. การจัดการข้อมูลและการสำรองข้อมูล
(DATA MANAGEMENT & SECURE BACKUP)
3.1 เก็บ LOG การเข้าถึงและเปลี่ยนแปลงข้อมูล
3.2 วางระบบลบข้อมูลอัตโนมัติเมื่อครบกำหนด
(AUTOMATED DATA DELETION)
AUTO DELETE
AUTO DELETE
3.3 สำรองข้อมูลอย่างปลอดภัยและมีการเข้ารหัส
(ENCRYPTED BACKUP STORAGE)
4. การเตรียมความพร้อมเมื่อเกิดเหตุละเมิด
(DATA BREACH RESPONSE PREPARATION)
4.1 ขั้นตอนปฏิบัติเมื่อตรวจพบการบุกรุก
(INCIDENT RESPONSE PLAN:
DETECT -> CONTAIN ->
ERADICATE -> RECOVER)
EYE
SHIELD
HAUMMER
TOOLS
RECOVER
4.2 ประสานงานกับ DPO และแจ้ง สคส.
(COORDINATE WITH DPO & NOTIFY AUTHORITY)
ADMIN & DPO
72
HOURS
ประสานงานกับ DPO และแจ้ง สคส.
(COORDINATE WITH DPO & NOTIFY AUTHORITY)
FOR UNIT INFORMATION SYSTEM & WEBSITE ADMINISTRATORS
สำหรับผู้ดูแลระบบสารสนเทศและเว็บไซต์หน่วยงาน


กระบวนการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
(PERSONAL DATA BREACH MANAGEMENT PROCESS)
1 การตรวจจับและยืนยันเหตุละเมิด
– ตรวจสอบทันที: ประเมินความน่าเชื่อถือของข้อมูลที่ได้รับ
– ตรวจสอบมาตรการรักษาความปลอดภัย:
ตรวจสอบทั้งมาตรการเชิงองค์กร เทคโนโลยี และกายภาพ
2 การประเมินความเสี่ยงและผลกระทบ
หากยืนยันว่าเกิดการละเมิดจริง ต้องประเมินว่า:
– ผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลมีมากน้อยเพียงใด
– พิจารณาปัจจัยต่างๆ เช่น ประเภทของการละเมิด ประเภทของ
ข้อมูล ปริมาณข้อมูล และความร้ายแรงของผลกระทบ
3 การดำเนินมาตรการเพื่อบรรเทาผลกระทบ
ดำเนินการทันทีเพื่อ:
– ยับยั้งการละเมิด: ปิดช่องโหว่ของระบบ เปลี่ยนรหัสผ่าน
หรือระงับการเข้าถึงชั่วคราว
– บรรเทาผลกระทบ: ลดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูล
4 การแจ้งเหตุละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
สคส.
72h
– รายงานต่อ สคส. ภายใน 72 ชั่วโมง: นับจากทราบเหตุละเมิด
– รายละเอียดที่ต้องแจ้ง: ลักษณะของการละเมิด
ข้อมูลติดต่อเจ้าหน้าที่คุ้มครองข้อมูล ผลกระทบที่อาจเกิดขึ้น
และมาตรการที่ดำเนินการ
5 การแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคล
– แจ้งโดยไม่ชักช้า: หากมีความเสี่ยงสูงต่อสิทธิและ
เสรีภาพของเจ้าของข้อมูล
– ข้อมูลที่ต้องแจ้ง: ลักษณะของการละเมิด
ผลกระทบที่อาจเกิดขึ้น แนวทางเยียวยา และมาตรการ
ที่ดำเนินการ
6 การดำเนินมาตรการเยียวยา
– ชดเชยความเสียหาย: ทั้งทางการเงินและการให้บริการ
ที่ช่วยลดผลกระทบ
– ให้คำปรึกษา: ช่วยเหลือเจ้าของข้อมูลในการจัดการกับ
ผลกระทบที่เกิดขึ้น
– แก้ไขข้อมูล: ดำเนินการแก้ไขหรือลบข้อมูลที่ถูกละเมิด
7 การปรับปรุงมาตรการรักษา
ความมั่นคงปลอดภัย
– ทบทวนและปรับปรุง: มาตรการป้องกันเพื่อป้องกัน
การเกิดเหตุซ้ำในอนาคต


แนวปฏิบัติที่ดีที่สุดสำหรับการจัดการเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
เพื่อสร้างความพร้อมและลดผลกระทบต่อองค์กร
NEWS
NEWS
Chain of Custody
POLICE
POLICE
1 ทำให้แผนรับมือเหตุการณ์ฉุกเฉิน (IRP) เป็นเอกสารที่มีการพัฒนาอย่างต่อเนื่อง
• ทบทวนและปรับปรุงอย่างสม่ำเสมอ (อย่างน้อยปีละครั้ง)
• หลังจากมีการเปลี่ยนแปลงที่สำคัญ
• อิงจากบทเรียนการฝึกซ้อมและเหตุการณ์จริง
2 สื่อสารอย่างชัดเจน
• ทันท่วงทีและชัดเจน
• สื่อสารทั้งภายในและภายนอก (ผู้ได้รับผลกระทบ, หน่วยงาน, สาธารณชน)
• กำหนดช่องทางและระเบียบปฏิบัติก่อนวิกฤต
3 ใช้ระบบอัตโนมัติในส่วนที่ทำได้
• งานตรวจจับและการควบคุมที่ซ้ำซาก
• เร่งความเร็วในการตอบสนอง
• ใช้คู่มือและเครื่องมือการทำงานอัตโนมัติ (เช่น SOAR)
4 การมีส่วนร่วมของที่ปรึกษาด้านกฎหมาย
• ปรึกษาตั้งแต่เนิ่นๆ ในการวางแผนและระหว่างเหตุการณ์
• โดยเฉพาะเหตุการณ์รั่วไหลของข้อมูล
• ดูแลเรื่องการควบคุม, การแจ้งเตือน, และการจัดการหลักฐาน
5 รักษาหลักฐาน
• รักษาความสมบูรณ์ของหลักฐาน
• เพื่อวิเคราะห์สาเหตุและทางกฎหมาย
• ฝึกอบรมทีมงานในการเก็บรวบรวมที่ถูกต้อง
Chain of Custody


เทคนิคการจัดการ LOG FILES ให้สอดคล้องกับ PDPA
รักษาสมดุลระหว่าง "เก็บหลักฐาน" และ "คุ้มครองความเป็นส่วนตัว"
DATA MINIMIZATION (เก็บเท่าที่จำเป็น)
ตัดข้อมูลที่ไม่เกี่ยวออก (CUT IRRELEVANT DATA)
เล็กเก็บเฉพาะ METADATA ใคร ทำอะไร เมื่อไหร่ ที่ไหน (WHO, WHAT, WHEN, WHERE)
PSEUDONYMIZATION (การใช้นามแฝง)
Name
Employee ID
IP address hashing
ใช้ ID แทนชื่อ USE ID INSTEAD OF NAME)
HASHING IP ADDRESS
DATA MASKING (การปกปิดข้อมูล)
081-XXX-XXXX
user_***@email.com
เซ็นเซอร์ข้อมูลอ่อนไหว (SENSOR SENSITIVE DATA)
กรองรูปแบบ Credit Card ออก
ACCESS CONTROL (การจำกัดสิทธิ์)
Principle of Least Privilege
ให้สิทธิ์เฉพาะผู้จำเป็น (ONLY ESSENTIAL STAFF)
แยกคนมีสิทธิ์ดู Log กับแก้ไขระบบ (SEPARATE VIEWER & SYSTEM ADMIN ROLES)
RETENTION POLICY (กำหนดอายุการเก็บ)
90 days
Auto-
ตั้งระบบลบ Log ทันที (AUTO-DELETION)
Log รอการลบต้องเข้ารหัส (ENCRYPTION AT REST)
จุดที่มักพลาด (COMMON PITFALLS)
GUG FILE LOGS และ 'คุ้มครองความเป็นส่วนตัว'
DEBUG MODE บันทึกข้อมูลทุกอย่าง
ERROR LOGS เผลอพ่นข้อมูลลูกค้าออกมา


แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศ
และการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน
สืบเนื่องจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เมื่อวันที่ 15 มีนาคม 2569
โดยการบิดเบือนรูปภาพและเผยแพร่ผ่านความคิดเห็นในหน้าเพจ Facebook
1. จำกัดสิทธิ์การโพสต์
ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง
2. ยกระดับการคัดกรอง
เปิดใช้งาน 'ตัวช่วยการควบคุม' (Moderation Assist)
ตั้งค่าคัดกรองความคิดเห็น (Comment Filtering)
ซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญบิดเบือนอัตโนมัติ
อ้างอิง: มติคณะกรรมการบริหารมหาวิทยาลัย ครั้งที่ 4/2569 วันที่ 2 เมษายน 2569


"มาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (สำหรับผู้ปฏิบัติงาน)
อ้างอิงตามแผนดำเนินงานรอบ 6 เดือนของมหาวิทยาลัย
เพื่อยกระดับความคืบหน้าของการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล
1. มาตรการด้านการบริหารจัดการ (Administrative Measures)
CIO &
DPO
การลงนามรักษาความลับ Confidentiality
การกำหนดหน้าที่และสิทธิเข้าถึง Role-based Access
การตรวจสอบสถานะความเสี่ยง Risk Review/KM
2. มาตรการเชิงเทคนิคและระบบสารสนเทศ (Technical Measures)
การแจ้งวัตถุประสงค์และขอความยินยอม
ความปลอดภัยของสื่อสังคมออนไลน์
การใช้เทคโนโลยีป้องกัน Preventive Tech
PDPA
3. มาตรการด้านบุคลากรและการสร้างความตระหนัก (Human Measures)
การเข้ารับการอบรม
ร้อยละ 60
การแลกเปลี่ยนเรียนรู้ (KM)
4. มาตรการการตอบสนองและรายงานเหตุละเมิด (Incident Response)
ช่องทางการร้องเรียน
แนวปฏิบัติเมื่อเกิดเหตุ

4. ประยุกต์ใช้ความรู้ในกิจการงานของตน เป็นการนำความรู้และเครื่องมือไปทดลองใช้จริงในหน่วยงาน

กิจกรรมที่ 5 แลกเปลี่ยนเรียนรู้

(1) จัดกิจกรรมแลกเปลี่ยนเรียนรู้กับกลุ่มแอดมิน (Admin) เว็บไซต์และสื่อออนไลน์ (1 ธันวาคม 2568 และ 18 ธันวาคม 2568) เพื่อสร้างความเข้าใจในการเผยแพร่ข้อมูลอย่างปลอดภัย รับทราบขั้นตอน ประเด็นความเสี่ยง เรื่อง “การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.” ของมหาวิทยาลัย


(2) นำเครื่องมือ/แนวทางปฏิบัติจาก กิจกรรมที่ 4 ไปทดลองใช้ในหน่วยงาน/กลุ่มงานที่เกี่ยวข้อง (วันที่ 8 มกราคม 2569 เวลา 09.00 น. ณ ห้องประชุมดอกสัก

(3) กิจกรรมแลกเปลี่ยนเรียนรู้กลุ่มแอดมิน ร่วมกับ DPO และผู้ประมวลผลข้อมูลสำนักฯ วันที่ 27 กุมภาพันธ 2569 เวลา 09.00 น. ณ ห้องประชุมดอกสัก เพื่อแนะนำเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย และวางแผนจัดอบรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล สำหรับผู้ที่มีหน้าที่และความรับผิดชอบตามกฎหมาย PDPA


5. นำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด“ขุมความรู้” ออกมาบันทึกไว้ เป็นการสรุปบทเรียนจากการใช้งานจริง

กิจกรรมที่ 6 จัดตั้งชุมชนนักปฏิบัติ (CoP) ในกลุ่มผู้ใช้งาน กิจกรรมที่ 5 เพื่อแลกเปลี่ยนประสบการณ์ ปัญหา และจุดที่ต้องปรับปรุงในการนำแนวทางไปปฏิบัติจริง และสกัดบทเรียนที่ได้ออกมา โดยจัดกิจกรรมแลกเปลี่ยนเรียนรู้ เมื่อวันที่ 29 เมษายน 2569 เวลา 09.00 น. ณ ห้องปฏิบัติการคอมพิวเตอร์ ชั้น 5 อาคารศูนย์ภาษาและคอมพิวเตอร์

จากขั้นตอนการนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด “ขุมความรู้” ออกมาบันทึกไว้ เพื่อสร้างชุมชนการเรียนรู้ (Learning Community) โดย สร้างกลุ่มสำหรับแลกเปลี่ยนเรียนรู้ทางโซเชียลมีเดีย ได้แก่ **คลินิกกฎหมาย HLC**

6. จดบันทึก “ขุมความรู้” และ “แก่นความรู้” สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น เป็นการรวบรวมความรู้ให้เป็นชุดข้อมูลที่สมบูรณ์

กิจกรรมที่ 7 การจัดทำชุดความรู้ฉบับสมบูรณ์ นำบทเรียนที่สกัดได้มาปรับปรุงร่างแนวปฏิบัติเดิมให้กลายเป็น “ชุดความรู้/คู่มือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล” ฉบับสมบูรณ์ เผยแพร่ผลงานผ่านเล่มรายงานและ Infographic เพื่อให้เป็นมาตรฐานการทำงานที่เป็นทางการของมหาวิทยาลัย

ในขั้นตอนนี้ ได้ใช้ประสบการณ์การทำงานและการเรียนรู้ผ่านการเรียนรู้ออนไลน์ หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง ของ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และแหล่งอื่นๆ ที่มีความน่าเชื่อถือ คัดเลือก จดบันทึก “ขุมความรู้” และ “แก่นความรู้” สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน และเชื่อมโยงเหมาะต่อการใช้งาน จัดทำเป็นเว็บไซต์เผยแพร่การจัดการความรู้ PDPA (Personal Data Privacy Policy) รวบรวม สื่อส่งเสริมการเรียนรู้ PDPA สำหรับบุคลากร ที่เว็บไซต์ https//kpru.ac.th/km-pdpa/ กิจกรรมทั้งหมดที่สำนักฯ จัดขึ้น ได้รวบรวม Knowledge Asset (KA) โดยบันทึกความรู้ สรุปเป็นประเด็นสาระสำคัญของงาน เป็นชุดความรู้ แบบ Explicit Knowledge และรวบรวมความรู้ที่มีประโยชน์ อ้างอิงจากแหล่งความรู้ (References) แล้วจัดเก็บเป็นคลังความรู้ออนไลน์เผยแพร่ในเว็บไซต์ให้ผู้ใช้เข้าถึงได้ง่าย นำไปใช้ประโยชน์ได้จริง สร้างสังคมเวทีแห่งการเรียนรู้ให้บุคลากร มีโอกาสพูดคุย แลกเปลี่ยนความรู้ซึ่งกันและกัน

9. ประโยชน์ที่คาดว่าจะได้รับ

1. บุคลากร ผู้ปฏิบัติงานได้รับความรู้ มีความเข้าใจ และตระหนักถึงการรักษาความปลอดภัยข้อมูลส่วนบุคคล สามารถ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้อย่างถูกต้อง เหมาะสม เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

2. บุคลากรสายสนับสนุนของมหาวิทยาลัย สามารถนำความรู้ที่ได้ไปใช้ในการทำงาน ทำให้การคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องปกติของทุกๆ กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

3. ได้แนวปฏิบัติและเว็บไซต์เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากร มหาวิทยาลัยราชภัฏกำแพงเพชร

10. องค์ความรู้

- ชุดความรู้/คู่มือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล และ Infographic ที่เกี่ยวข้อง เช่น มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล, แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล

11. การนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้

นำองค์ความรู้เผยแพร่ลงเว็บไซต์ https//kpru.ac.th/km-pdpa/ และให้ผู้มีส่วนเกี่ยวข้องนำไปใช้ประโยชน์ตามประเด็นที่เห็นว่าเกิดประโยชน์ต่อการปฏิบัติงาน

12. ช่องทางการเผยแพร่องค์ความรู้

- เผยแพร่ผ่านช่องทาง Website มหาวิทยาลัย นำองค์ความรู้เผยแพร่ลงเว็บไซต์ https//kpru.ac.th/km-pdpa/ และ Facebook ศูนย์คอมพิวเตอร์

- ชุดความรู้เฉพาะกลุ่ม เผยแพร่ผ่านเพจ Facebook กลุ่มผู้ดูแลเว็บไซต์ และเว็บไซต์ https://kpru.ac.th/km-web/

ภาคผนวก

แผนการจัดการความรู้ (KM Action Plan)

หน่วยงาน : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร

ประจำปีการศึกษา 2568 (1 มิถุนายน พ.ศ. 2568 ถึง 31 พฤษภาคม พ.ศ. 2569)

ประเด็นการจัดการความรู้ “แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)”

☐ การเรียนการสอน ☐ การวิจัย ☑ พันธกิจอื่นๆ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
1	การกำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร	**กิจกรรมที่ 1** จัดตั้งคณะทำงาน 1.1 จัดตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ 1.2 จัดตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร	31 ต.ค. 2568 12 พ.ย. 2568	1. คำสั่ง แต่งตั้งคณะกรรมการจัดการความรู้ จำนวน 1 ฉบับ 2. คำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล จำนวน 1 ฉบับ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ - บุคลากรของสำนักฯ - ตัวแทนหน่วยงานที่เกี่ยวข้องกับการกำกับและการใช้ข้อมูลส่วนบุคคลภายในมหาวิทยาลัยฯ	คณะกรรมการจัดการความรู้ สำนักฯ
		กิจกรรมที่ 2 ประชุมคณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล	5 พ.ย. 2568	1. แผนการจัดการความรู้ จำนวน 1 เรื่อง 2. รายการความเสี่ยงที่เกี่ยวข้อง จำนวน 5 ประเด็น	คณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
2	การเสาะหาความรู้ที่ต้องการ	**กิจกรรมที่ 3** รวบรวมและศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA, และตัวอย่าง Best Practice การลดความเสี่ยงจากมหาวิทยาลัยหรือหน่วยงานที่ประสบความสำเร็จ เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล	พ.ย. 2568	เอกสารที่เกี่ยวข้อง จำนวน 5 เรื่อง	คณะกรรมการ KM, คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
3	การปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน	**กิจกรรมที่ 4** จัดทำเครื่องมือ/แนวทางปฏิบัติ โดยเฉพาะ 3 อันดับความเสี่ยงที่ระบุไว้ เช่น คู่มือการจัดเก็บ/ทำลายเอกสารข้อมูลส่วนบุคคล, Checklist การใช้งานระบบที่ต้องระบุตัวตน หรือ Infographic สรุปข้อปฏิบัติของบุคลากร ทำให้ความรู้ PDPA ที่ซับซ้อนกลายเป็นเครื่องมือที่ใช้งานง่าย	ธ.ค.68 - ม.ค.69	เครื่องมือ/แนวทางปฏิบัติ (ฉบับร่าง) 3 รายการ เช่น คู่มือ 1 รายการ, Checklist 1 รายการ, Infographic 1 รายการ	คณะกรรมการ KM, คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
4	การประยุกต์ใช้ความรู้ในกิจการงานของตน	**กิจกรรมที่ 5** แลกเปลี่ยนเรียนรู้ (1) นำเครื่องมือ/แนวทางปฏิบัติ จาก กิจกรรมที่ 4 ไปทดลองใช้ในหน่วยงาน/กลุ่มงานที่เกี่ยวข้องกับ 3 อันดับความเสี่ยงที่วิเคราะห์ไว้ พร้อมทั้งจัดอบรมสร้างความเข้าใจในการนำไปใช้ (2) จัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล สำหรับผู้ที่มีหน้าที่และความรับผิดชอบตาม	ก.พ. - มี.ค. 2569	- ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคล (เป้าหมาย ร้อยละ 60) - ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ระดับดี) - ระดับความสำเร็จในการดำเนินการจัดการความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคล (เป้าหมาย 5 คะแนน) - จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ ถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต (เป้าหมาย 0 ครั้ง)	บุคลากรมหาวิทยาลัยฯ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
		พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)				
5	การนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้และสกัด“ขุมความรู้” ออกมาบันทึกไว้	**กิจกรรมที่ 6** จัดตั้งชุมชนนักปฏิบัติ (CoP) ในกลุ่มผู้ใช้งาน กิจกรรมที่ 5 เพื่อแลกเปลี่ยนประสบการณ์ ปัญหา และจุดที่ต้องปรับปรุง ในการนำแนวทางไปปฏิบัติจริง และสกัดบทเรียนที่ได้ออกมา	เม.ย. - พ.ค. 2569	- ชุมชนนักปฏิบัติ (CoP) เพื่อแลกเปลี่ยนเรียนรู้ จำนวน 1 ชุมชน	คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
6	การจดบันทึก “ขุมความรู้” และ “แก่นความรู้” สำหรับไว้ใช้งานและปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น	**กิจกรรมที่ 7** นำบทเรียนที่สกัดได้จากกิจกรรมที่ 6 มา ปรับปรุงและจัดทำเป็น “ชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล” ฉบับร่าง สรุปให้เป็น ฉบับสมบูรณ์ เพื่อใช้ในการปฏิบัติงานที่เป็นทางการ	พ.ค. 2569	- ชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล จำนวน 1 ชิ้น	คณะกรรมการ PDPA	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลงชื่อ.....
(นางสาวอรปรียา คำแพ่ง)
ผู้รับผิดชอบงานการจัดการความรู้
26 พฤศจิกายน 2568

ลงชื่อ.....
(ผู้ช่วยศาสตราจารย์พรหมเมศ วีระพันธ์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
26 พฤศจิกายน 2568

วงจรการเรียนรู้ (Learning Cycle)

วงจรการเรียนรู้	การประยุกต์ใช้
1. การมีองค์ความรู้	1. ทบทวนแผน วิเคราะห์ความเสี่ยง และศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA และ Best Practice เพื่อเป็นฐานความรู้ตั้งต้น 2. สร้างและจัดระบบ นำความรู้ที่ซับซ้อนมาย่อยและแปลงให้เป็นเครื่องมือ/แนวทางปฏิบัติที่ใช้งานง่าย โดยเน้นแก้ปัญหาความเสี่ยง 3 อันดับแรก เช่น คู่มือจัดเก็บ/ทำลายเอกสาร, Checklist, Infographic เป็นการสร้างองค์ความรู้ที่เป็นรูปธรรม พร้อมใช้งาน
2. วิธีการส่งเสริมการเผยแพร่องค์ความรู้	1. จัดอบรม/กิจกรรม เพื่อสร้างความตระหนักรู้และให้ความรู้ PDPA ในวงกว้าง 2. นำเครื่องมือ/แนวทางปฏิบัติที่สร้างขึ้น ไปทดลองใช้จริงในหน่วยงานที่มีความเสี่ยงสูง พร้อมจัดอบรมเพื่อสร้างความเข้าใจในการนำไปใช้ 3. จัดตั้งชุมชนนักปฏิบัติ (CoP) เพื่อเป็นเวทีให้ผู้ใช้งานจริงมาแลกเปลี่ยนประสบการณ์ ปัญหา และแนวทางแก้ไขร่วมกันในกลุ่ม ถือเป็นการเผยแพร่และถ่ายทอดความรู้แบบมีปฏิสัมพันธ์ (Interactional Sharing)
3. ผลการนำองค์ความรู้ไปใช้	1. ติดตามผลการใช้เครื่องมือ/แนวทางปฏิบัติ และผลการทดลองใช้จากผู้ปฏิบัติงานว่ามีความเข้าใจในการใช้งานมากน้อยเพียงใด 2. บทเรียนและข้อเสนอแนะที่สกัดได้จากเวที CoP สะท้อนให้เห็นว่าความรู้ที่ถ่ายทอดไป (เครื่องมือ/แนวทาง) สามารถลดความเสี่ยง 3 อันดับแรก ได้ตามที่คาดหวังหรือไม่ 3. ข้อมูลจากการแลกเปลี่ยนเรียนรู้ใน CoP ถือเป็นผลลัพธ์ที่ใช้ในการปรับปรุงต่อไป
4. ติดตามปัญหาและอุปสรรคจากการนำองค์ความรู้ไปใช้	1. ใช้การจัดตั้งชุมชนนักปฏิบัติ (CoP) เป็นกลไกในการติดตามปัญหาและอุปสรรคในการปฏิบัติงานจริง เช่น เครื่องมือใช้ยาก, ข้อกำหนดไม่ชัดเจน, การต่อต้านการเปลี่ยนแปลง
5. การนำความรู้มาปรับเป็นแนวปฏิบัติในการดำเนินงาน	1. นำบทเรียน ปัญหา และอุปสรรคที่สกัดได้จาก CoP มาใช้ในการปรับปรุงแก้ไของค์ความรู้เดิม 2. จัดทำเป็นชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคลฉบับสมบูรณ์ ซึ่งผ่านการทดลองใช้และปรับปรุงแล้ว 3. ประกาศใช้ชุดความรู้ฉบับสมบูรณ์ เป็นแนวปฏิบัติ ที่เป็นทางการ (Official Guideline) ของสำนักฯ/มหาวิทยาลัย เพื่อใช้เป็นมาตรฐานในการปฏิบัติงานจริง ถือเป็นการบรรจุความรู้เข้าสู่ระบบการดำเนินงานอย่างเป็นทางการ

Infographic แนวปฏิบัติเมื่อตกเป็นเหยื่อถูกแอบอ้าง
รูปภาพบน Facebook ตัดต่อบิดเบือนข้อเท็จจริง

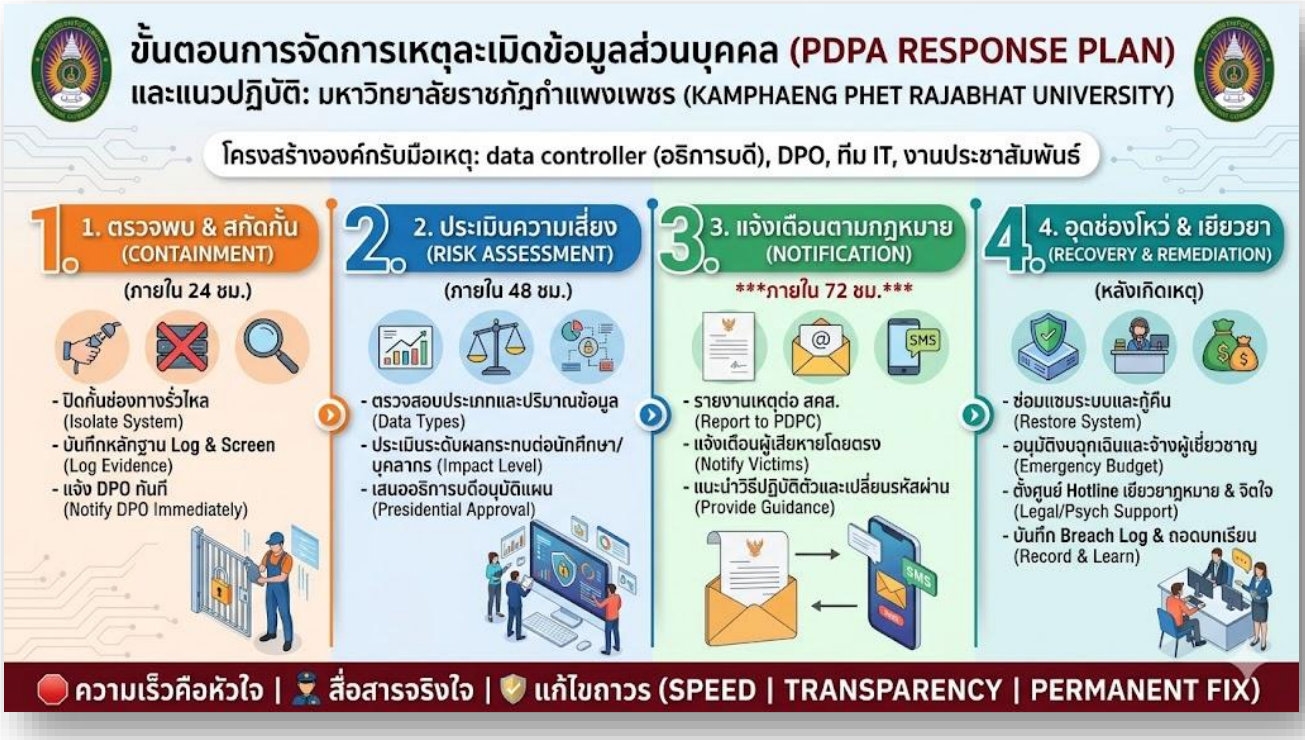
มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการละเมิดข้อมูลส่วนบุคคล

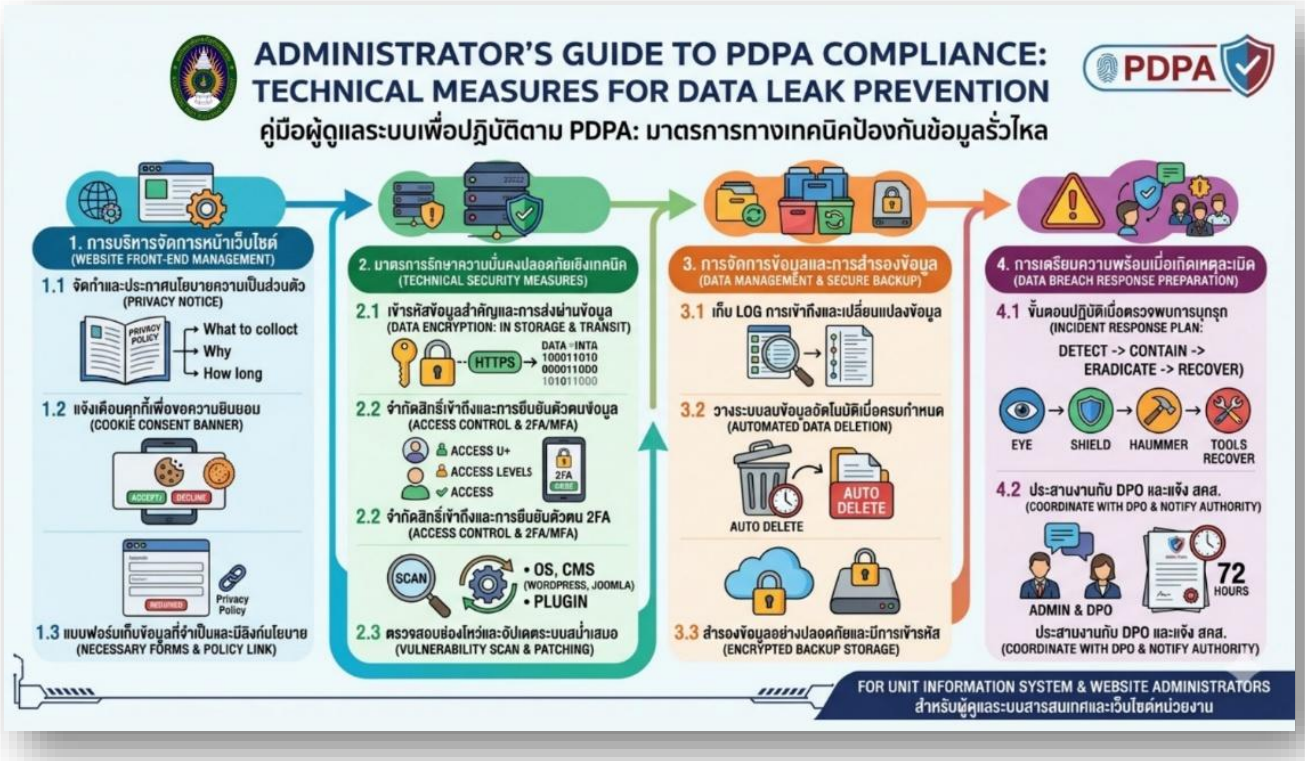

[ด่วนที่สุด]
แนวทางยกระดับความปลอดภัย
Facebook Page หน่วยงาน
เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล
สืบเนื่องจากกรณีการนำภาพบุคคลมาดัดแปลงและบิดเบือน
ข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน
เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความ
ปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการ
ตั้งค่า Facebook Page ดังนี้
1
1. ปิดสิทธิ์โพสต์สาธารณะ
ไม่อนุญาตให้บุคคลภายนอกโพสต์
เนื้อหาบน Timeline ของเพจโดยตรง
2
2. เปิดระบบคัดกรองอัตโนมัติ
ใช้งาน Moderation Assist
เพื่อตั้งค่าซ่อนความเห็นที่มีคำไม่สุภาพ
หรือ Keywords ที่เข้าข่ายบิดเบือน
ข้อมูล/สร้างความเสียหาย
ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้
พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย


แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศ
และการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน
สืบเนื่องจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เมื่อวันที่ 15 มีนาคม 2569
โดยการบิดเบือนรูปภาพและเผยแพร่ผ่านความคิดเห็นในหน้าเพจ Facebook
1. จำกัดสิทธิ์การโพสต์
• ปิดการอนุญาตให้บุคคลภายนอก
โพสต์บนหน้าเพจโดยตรง
2. ยกระดับการคัดกรอง
• เปิดใช้งาน 'ตัวช่วยการควบคุม' (Moderation Assist)
• ตั้งค่าคัดกรองความคิดเห็น (Comment Filtering)
• ซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญบิดเบือนอัตโนมัติ
อ้างอิง: มติคณะกรรมการบริหารมหาวิทยาลัย ครั้งที่ 4/2569 วันที่ 2 เมษายน 2569


การปิดสิทธิ์โพสต์บนเพจ Facebook ของหน่วยงาน
เพื่อความปลอดภัยและภาพลักษณ์ที่เป็นทางการ
Username
Password
Log in
1. เข้าสู่ระบบ
ด้วยบัญชีผู้ดูแล (Admin)
2. สลับไปเพจหน่วยงาน
เลือกสลับการใช้งานไปยังเพจ
การตั้งค่าและความเป็นส่วนตัว
การตั้งค่า
3. ไปที่การตั้งค่า
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > การตั้งค่า
ความเป็นส่วนตัว
เพจและการแท็ก
4. เลือกความเป็นส่วนตัว & เพจและการแท็ก
ในเมนูด้านซ้าย เลือก “ความเป็นส่วนตัว” > “เพจและการแท็ก”
ใครสามารถโพสต์บนเพจของคุณได้บ้าง
เฉพาะฉัน
เฉพาะฉัน
5. ตั้งค่าใครสามารถโพสต์ได้
เลือก “เฉพาะฉัน”
6. บันทึกอัตโนมัติ
ระบบจะบันทึกการตั้งค่าให้โดยอัตโนมัติ
จัดการเพจอย่างมืออาชีพ


การตั้งค่าตัวกรองคำหยาบและคำเฉพาะ
เพื่อการควบคุมเนื้อหาและภาพลักษณ์ที่ดี
Username
Password
Log in
1. สลับโปรไฟล์ไปที่หน้าเพจ
เลือกสลับบัญชีเป็นผู้ดูแลเพจ
2. ไปที่การตั้งค่า (Settings)
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > ความเป็นส่วนตัว
3. เลือกโพสต์สาธารณะ (Public Posts)
ในเมนูด้านซ้าย เลือก “โพสต์สาธารณะ”
4. ตรวจสอบเนื้อหา (Content Moderation)
มองหาและคลิกหัวข้อ “การตรวจสอบเนื้อหา”
5. ซ่อนความคิดเห็น
ซ่อนความคิดเห็นที่มีคำบางคำ
มึ_มึ_ , กู_กู_ , คำไม่สุภาพ , คำด่า
6. บันทึก (Save)
กดปุ่ม “บันทึก” เพื่อสิ้นสุด
จัดการเพจอย่างมืออาชีพ


ขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (PDPA RESPONSE PLAN)
และแนวปฏิบัติ: มหาวิทยาลัยราชภัฏกำแพงเพชร (KAMPHAENG PHET RAJABHAT UNIVERSITY)
โครงสร้างองค์กรรับมือเหตุ: data controller (อธิการบดี), DPO, ทีม IT, งานประชาสัมพันธ์
1. ตรวจพบ & สกัดกั้น (CONTAINMENT)
(ภายใน 24 ชม.)
- ปิดกั้นช่องทางรั่วไหล (Isolate System)
- บันทึกหลักฐาน Log & Screen (Log Evidence)
- แจ้ง DPO ทันที (Notify DPO Immediately)
2. ประเมินความเสี่ยง (RISK ASSESSMENT)
(ภายใน 48 ชม.)
- ตรวจสอบประเภทและปริมาณข้อมูล (Data Types)
- ประเมินระดับผลกระทบต่อนักศึกษา/บุคลากร (Impact Level)
- เสนออธิการบดีอนุมัติแผน (Presidential Approval)
3. แจ้งเตือนตามกฎหมาย (NOTIFICATION)
ภายใน 72 ชม.
SMS
- รายงานเหตุต่อ สคส. (Report to PDPC)
- แจ้งเตือนผู้เสียหายโดยตรง (Notify Victims)
- แนะนำวิธีปฏิบัติตัวและเปลี่ยนรหัสผ่าน (Provide Guidance)
4. อุดช่องโหว่ & เยียวยา (RECOVERY & REMEDIATION)
(หลังเกิดเหตุ)
- ซ่อมแซมระบบและกู้คืน (Restore System)
- อนุมัติงบฉุกเฉินและจ้างผู้เชี่ยวชาญ (Emergency Budget)
- ตั้งศูนย์ Hotline เยียวยากฎหมาย & จิตใจ (Legal/Psych Support)
- บันทึก Breach Log & ถอดบทเรียน (Record & Learn)
ความเร็วคือหัวใจ | สื่อสารจริงใจ | แก้ไขถาวร (SPEED | TRANSPARENCY | PERMANENT FIX)


ADMINISTRATOR'S GUIDE TO PDPA COMPLIANCE:
TECHNICAL MEASURES FOR DATA LEAK PREVENTION
PDPA
คู่มือผู้ดูแลระบบเพื่อปฏิบัติตาม PDPA: มาตรการทางเทคนิคป้องกันข้อมูลรั่วไหล
1. การบริหารจัดการหน้าเว็บไซต์
(WEBSITE FRONT-END MANAGEMENT)
1.1 จัดทำและประกาศนโยบายความเป็นส่วนตัว
(PRIVACY NOTICE)
What to collect
Why
How long
1.2 แจ้งเตือนคุกกี้เพื่อขอความยินยอม
(COOKIE CONSENT BANNER)
ACCEPT
DECLINE
1.3 แบบฟอร์มเก็บข้อมูลที่จำเป็นและมีลิงก์นโยบาย
(NECESSARY FORMS & POLICY LINK)
REQUIRED
Privacy Policy
2. มาตรการรักษาความมั่นคงปลอดภัยเชิงเทคนิค
(TECHNICAL SECURITY MEASURES)
2.1 เข้ารหัสข้อมูลสำคัญและการส่งผ่านข้อมูล
(DATA ENCRYPTION: IN STORAGE & TRANSIT)
HTTPS
DATA→INTA
100011010
000011000
1010111000
2.2 จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตนข้อมูล
(ACCESS CONTROL & 2FA/MFA)
ACCESS U+
ACCESS LEVELS
ACCESS
2FA
2.2 จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตน 2FA
(ACCESS CONTROL & 2FA/MFA)
SCAN
• OS, CMS
(WORDPRESS, JOOMLA)
• PLUGIN
2.3 ตรวจสอบช่องโหว่และอัปเดตระบบสม่ำเสมอ
(VULNERABILITY SCAN & PATCHING)
3. การจัดการข้อมูลและการสำรองข้อมูล
(DATA MANAGEMENT & SECURE BACKUP)
3.1 เก็บ LOG การเข้าถึงและเปลี่ยนแปลงข้อมูล
3.2 วางระบบลบข้อมูลอัตโนมัติเมื่อครบกำหนด
(AUTOMATED DATA DELETION)
AUTO DELETE
AUTO DELETE
3.3 สำรองข้อมูลอย่างปลอดภัยและมีการเข้ารหัส
(ENCRYPTED BACKUP STORAGE)
4. การเตรียมความพร้อมเมื่อเกิดเหตุละเมิด
(DATA BREACH RESPONSE PREPARATION)
4.1 ขั้นตอนปฏิบัติเมื่อตรวจพบการบุกรุก
(INCIDENT RESPONSE PLAN:
DETECT -> CONTAIN ->
ERADICATE -> RECOVER)
EYE
SHIELD
HAUMMER
TOOLS
RECOVER
4.2 ประสานงานกับ DPO และแจ้ง สคส.
(COORDINATE WITH DPO & NOTIFY AUTHORITY)
ADMIN & DPO
72
HOURS
ประสานงานกับ DPO และแจ้ง สคส.
(COORDINATE WITH DPO & NOTIFY AUTHORITY)
FOR UNIT INFORMATION SYSTEM & WEBSITE ADMINISTRATORS
สำหรับผู้ดูแลระบบสารสนเทศและเว็บไซต์หน่วยงาน


"มาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (สำหรับผู้ปฏิบัติงาน)
อ้างอิงตามแผนดำเนินงานรอบ 6 เดือนของมหาวิทยาลัย
เพื่อยกระดับความคืบหน้าของการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล
1. มาตรการด้านการบริหารจัดการ
(Administrative Measures)
CIO &
DPO
การลงนามรักษาความลับ
Confidentiality
ผู้ปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลทุกคน ต้องลงนามในสัญญารักษาความลับ (Non-Disclosure Agreement: NDA) เพื่อป้องกันการนำข้อมูลไปใช้ผิดวัตถุประสงค์
การกำหนดหน้าที่และสิทธิเข้าถึง
Role-based Access
เจ้าถึงข้อมูลตามความจำเป็นของงานภาคหน้าที่ โดยมีโครงสร้างการทำงานดูแลห่านผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
การตรวจสอบสถานะความเสี่ยง
Risk Review/KM
มีการจัดประชุมเพื่อทบทวนแผนจัดการความรู้ (KM) และวิเคราะห์ความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหลอย่างอย่างสม่ำเสมอ
2. มาตรการเชิงเทคนิคและระบบสารสนเทศ
(Technical Measures)
การแจ้งวัตถุประสงค์และขอความยินยอม
กระบบสารสนเทศต้องมีแบบฟอร์มการจัดเก็บข้อมูลที่ชัดเจน และต้องมีการกล่าววัตถุประสงค์ (Privacy Notice) รวมถึงการขอความยินยอม (Consent) ก่อนการเก็บ ใช้ หรือเปิดเผยข้อมูล
ความปลอดภัยของสื่อสังคมออนไลน์
สำหรับแอดมิน Facebook Page ของหน่วยงาน ต้องปฏิบัติตามมาตรการเชิงเทคนิคเพื่อป้องกันการถูกโจมตี หรือการโพสต์รูปภาพ/ข้อมูลที่อาจเป็นการเผยแพร่ข้อมูลส่วนบุคคล
การใช้เทคโนโลยีป้องกัน
Preventive Tech
สนับสนุนการใช้มาตรการเชิงเทคนิค (เช่น การคัดกรอง IP หรือระบบตรวจสอบสิทธิ์) เพื่อลดความเสี่ยงจากการคุกคามทางไซเบอร์ที่อาจส่งผลต่อข้อมูลของบุคลากรและนักศึกษา
PDPA
3. มาตรการด้านบุคลากรและการสร้างความตระหนัก
(Human Measures)
การเข้ารับการอบรม
ผู้ปฏิบัติงาน (ลายสนับสนุนและสายวิชาการ) ต้องเข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคลและ: 'วัคซีนไซเบอร์' ตามรอบที่มหาวิทยาลัยกำหนด
โดยมีเป้าหมายไม่ต่ำกว่า
ร้อยละ 60
ของบุคลากรทั้งหมด
การแลกเปลี่ยนเรียนรู้ (KM)
เข้าร่วมกิจกรรมแลกเปลี่ยนแนวทางการบริหารจัดการข้อมูลส่วนบุคคล (Case Study) เพื่อปรับปรุงกระบวนการทำงานให้ลอดคล้องกับ PDPA
4. มาตรการการตอบสนองและรายงานเหตุละเมิด
(Incident Response)
ช่องทางการร้องเรียน
ผู้ปฏิบัติงานต้องทราบช่องทางการแจ้งเหตุหรือช่องทางการร้องเรียน กรณีพบเห็นเหตุการณ์ที่อาจเป็นการละเมิดข้อมูลส่วนบุคคล
แนวปฏิบัติเมื่อเกิดเหตุ
หากพบเหตุละเมิด ต้องดำเนินการตาม 'หมวดปฏิบัติการรับมือเหตุละเมิด' และมาตรการแก้ไขสถานการณ์เบื้องต้นเพื่อระงับเหตุทันที


แนวปฏิบัติที่ดีที่สุดสำหรับการจัดการเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
เพื่อสร้างความพร้อมและลดผลกระทบต่อองค์กร
NEWS
NEWS
Chain of Custody
POLICE
POLICE
1 ทำให้แผนรับมือเหตุการณ์ฉุกเฉิน (IRP) เป็นเอกสารที่มีการพัฒนาอย่างต่อเนื่อง
ทบทวนและปรับปรุงอย่างสม่ำเสมอ (อย่างน้อยปีละครั้ง)
หลังจากมีการเปลี่ยนแปลงที่สำคัญ
อิงจากบทเรียนการฝึกซ้อมและเหตุการณ์จริง
2 สื่อสารอย่างชัดเจน
ทันท่วงทีและชัดเจน
สื่อสารทั้งภายในและภายนอก (ผู้ได้รับผลกระทบ, หน่วยงาน, สาธารณชน)
กำหนดช่องทางและระเบียบปฏิบัติก่อนวิกฤต
3 ใช้ระบบอัตโนมัติในส่วนที่ทำได้
งานตรวจจับและการควบคุมที่ซ้ำซาก
เร่งความเร็วในการตอบสนอง
ใช้คู่มือและเครื่องมือการทำงานอัตโนมัติ (เช่น SOAR)
4 การมีส่วนร่วมของที่ปรึกษาด้านกฎหมาย
ปรึกษาตั้งแต่เนิ่นๆ ในการวางแผนและระหว่างเหตุการณ์
โดยเฉพาะเหตุการณ์รั่วไหลของข้อมูล
ดูแลเรื่องการควบคุม, การแจ้งเตือน, และการจัดการหลักฐาน
5 รักษาหลักฐาน
รักษาความสมบูรณ์ของหลักฐาน
เพื่อวิเคราะห์สาเหตุและทางกฎหมาย
ฝึกอบรมทีมงานในการเก็บรวบรวมที่ถูกต้อง
Chain of Custody


เทคนิคการจัดการ LOG FILES ให้สอดคล้องกับ PDPA
รักษาสมดุลระหว่าง “เก็บหลักฐาน” และ “คุ้มครองความเป็นส่วนตัว”
DATA MINIMIZATION
(เก็บเท่าที่จำเป็น)
ตัดข้อมูลที่ไม่เกี่ยวออก
(CUT IRRELEVANT DATA)
เล็กเก็บเฉพาะ METADATA
ใคร ทำอะไร เมื่อไหร่ ที่ไหน
(WHO, WHAT, WHEN, WHERE)
PSEUDONYMIZATION
(การใช้นามแฝง)
Name
Employee ID
IP address hashing
ใช้ ID แทนชื่อ
USE ID INSTEAD OF NAME)
HASHING IP ADDRESS
DATA MASKING
(การปกปิดข้อมูล)
081-XXX-XXXX
user_***@email.com
เซ็นเซอร์ข้อมูลอ่อนไหว
(SENSOR SENSITIVE DATA)
กรองรูปแบบ
Credit Card ออก
ACCESS CONTROL
(การจำกัดสิทธิ์)
Principle of
Least Privilege
ให้สิทธิ์เฉพาะผู้จำเป็น
(ONLY ESSENTIAL STAFF)
แยกคนมีสิทธิ์ดู Log
กับแก้ไขระบบ
(SEPARATE VIEWER &
SYSTEM ADMIN ROLES)
RETENTION POLICY
(กำหนดอายุการเก็บ)
90
days
Auto-
ตั้งระบบลบ Log ทันที
(AUTO-DELETION)
Log รอการลบต้องเข้ารหัส
(ENCRYPTION AT REST)
จุดที่มักพลาด
(COMMON PITFALLS)
GUG FILE LOGS
และ 'คุ้มครองความเป็นส่วนตัว'
DEBUG MODE
บันทึกข้อมูลทุกอย่าง
ERROR LOGS
เผลอพ่นข้อมูลลูกค้าออกมา


UNIVERSITY
DATA SECURITY
GUIDELINES
ข้อควรปฏิบัติและข้อห้าม (Do’s & Don’ts)
ในการจัดการข้อมูลส่วนบุคคลของมหาวิทยาลัย
UNIVERSITY DATA
SECURITY GUIDELINES
ข้อควรปฏิบัติ (DO’S)
1
ใช้ระบบขององค์กรเท่านั้นในการทีข้อมูล
USE UNIVERSITY SYSTEMS
ONLY FOR DATA
2
Checked
ตรวจสอบสิทธิ์ก่อนเปิดเผยข้อมูล
VERIFY PERMISSIONS
BEFORE DISCLOSING
3
SECURE
เก็บข้อมูลอย่างปลอดภัย
STORE DATA SECURELY
4
HELP DESK
รายงานเหตุผิดปกติทันที
REPORT INCIDENTS IMMEDIATELY
ข้อห้าม (DON’TS)
1
LINE
ใช้ LINE / Facebook
ส่วนตัวส่งข้อมูล
DO NOT USE PERSONAL
LINE / FACEBOOK
2
NO TALK
พูดถึงข้อมูลกับบุคคลภายนอก
DO NOT DISCUSS CONFIDENTIAL
INFO WITH OUTSIDERS
3
NOT SECURE
เก็บเอกสารสำคัญไว้นอกระบบ
DO NOT STORE IMPORTANT DOCS OUTSIDE SYSTEM
SECURITY IS EVERYONE’S RESPONSIBILITY
MARCORN UNIVERSITY

แบบฟอร์มการนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์
มหาวิทยาลัยราชภัฏกำแพงเพชร

ข้าพเจ้า (นามบุคคลหรือหน่วยงาน) : นางเกศรินทร์ เมฆโพธิ์
ที่อยู่ : 69 หมู่ 1 ต.นครชุม อ.เมือง จ.กำแพงเพชร
หมายเลขโทรศัพท์ : ..... E-Mail Address : .....
ได้ใช้ประโยชน์จากผลงาน ☑ องค์ความรู้ ☐ แนวปฏิบัติที่ดี เรื่อง : แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหล และป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)
เป็นผลงานของ (ระบุชื่อเจ้าของผลงาน) : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และคลินิกกฎหมาย HLC
ตำแหน่ง : - สังกัดหน่วยงาน : -
โดยนำไปใช้ประโยชน์ในด้าน : ☐ ด้านการผลิตบัณฑิต ☐ ด้านการวิจัย ☐ ด้านสิ่งแวดล้อม
☐ ด้านการบริการวิชาการ ☐ ด้านการทำนุบำรุงศิลปวัฒนธรรม
☐ ด้านการบริหารจัดการ ☑ ด้านอื่นๆ (ระบุ) .....
วัน / เดือน / ปี ที่นำไปใช้ประโยชน์ : วันที่ 9 เดือน เมษายน พ.ศ. 2569
วิธีการที่นำไปใช้ประโยชน์ : นำองค์ความรู้ส่วนของแนวปฏิบัติถูกแอบอ้างรูปภาพบน Facebook ติดต่อและกล่าวหาหลอกลวง และทบทวนเอกสารประกอบการอบรมจากเว็บไซต์ https://kpru.ac.th/km-pdpa/ ไปใช้ประกอบการปฏิบัติงาน
.....
.....
ผลที่ได้รับจากการนำไปใช้ประโยชน์ : สามารถปฏิบัติตามขั้นตอนได้อย่างถูกต้อง
.....
.....
.....

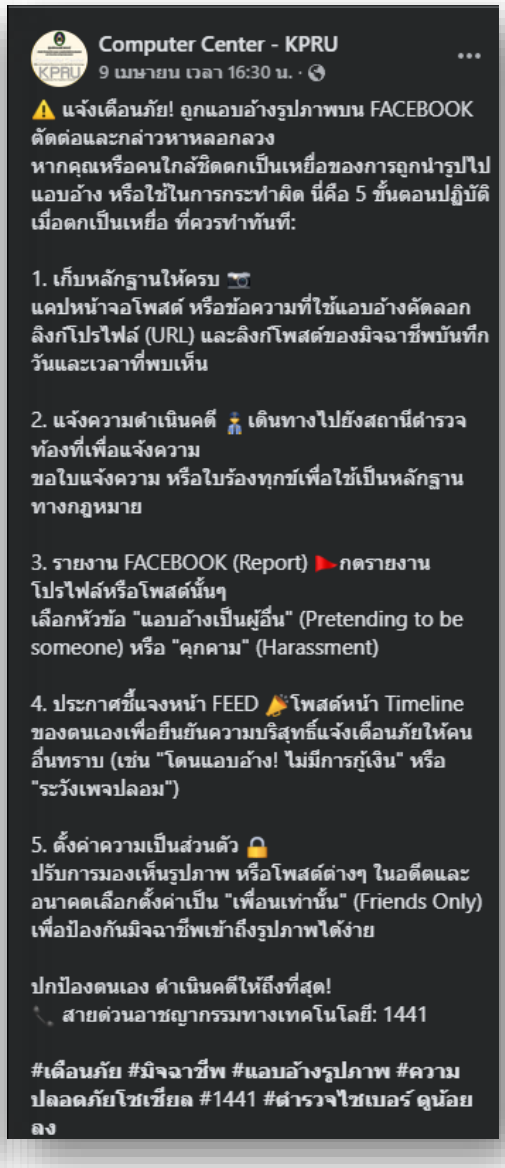
โดยแนบรายการเอกสาร / หลักฐาน ประกอบการนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์ เป็น

☐ เอกสารหลักฐาน / รายงานผลการดำเนินงาน
☑ ภาพถ่าย / ไฟล์วีดีโอ
☐ เว็บไซต์ ที่ URL : .....
☐ อื่นๆ (ระบุ) .....
รายละเอียดดังเอกสารที่แนบมาพร้อมแบบฟอร์มนี้

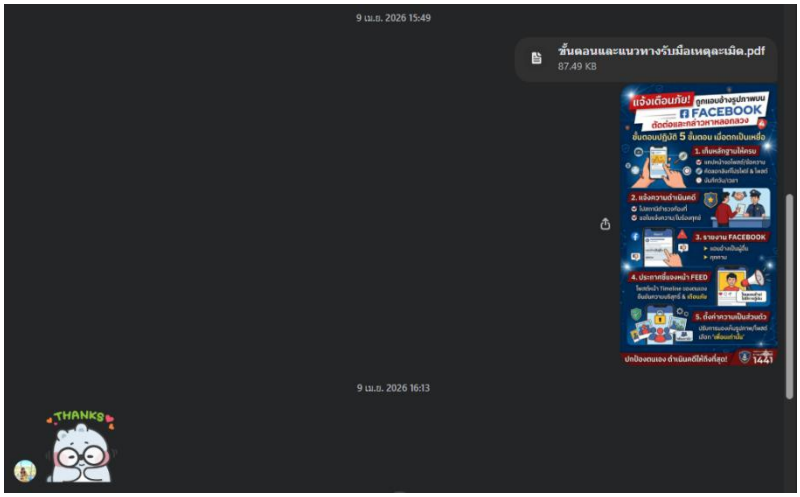
ข้าพเจ้าขอรับรองว่า การนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์ตามรายละเอียดในแบบฟอร์มฉบับนี้ เป็นการนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์ที่เกิดขึ้นจริงและมีผลที่ได้รับเป็นรูปธรรมตามที่รายงานในแบบฟอร์มฉบับนี้ ทุกประการ

ลงชื่อ เกศรินทร์ ผู้ใช้ประโยชน์
(นางเกศรินทร์ เมฆโพธิ์)
ตำแหน่ง เจ้าหน้าที่บริหารงานทั่วไป
วันที่ 20 เดือน กรกฎาคม พ.ศ. 2569

แนวปฏิบัติสำหรับผู้ที่ตกเป็นเหยื่อถูกละเมิดข้อมูลส่วนบุคคล
(กรณีแอบอ้างรูปภาพบน FACEBOOK)



เนื่องจากในช่วงเดือนมีนาคม - เมษายน 2569 ที่ผ่านมา บุคลากรภายในมหาวิทยาลัย และบุคคลภายนอก ตกเป็นเหยื่อถูกละเมิดข้อมูลส่วนบุคคล โดยแอบอ้างรูปภาพบน FACEBOOK จึงจัดทำและแนะนำเพื่อนบุคลากรที่ตกเป็นเหยื่อ



แบบฟอร์มการนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์
มหาวิทยาลัยราชภัฏกำแพงเพชร

ข้าพเจ้า (นามบุคคลหรือหน่วยงาน) : นางสาวอนันตพร อรุณฉาย

ที่อยู่ : 69 หมู่ 1 ต.นครชุม อ.เมือง จ.กำแพงเพชร

หมายเลขโทรศัพท์ : ..... E-Mail Address : .....

ได้ใช้ประโยชน์จากผลงาน ☑ องค์ความรู้ ☐ แนวปฏิบัติที่ดี เรื่อง : แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหล และป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)

เป็นผลงานของ (ระบุชื่อเจ้าของผลงาน) : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และคลินิกกฎหมาย HLC

ตำแหน่ง : - ..... สังกัดหน่วยงาน : -

โดยนำไปใช้ประโยชน์ในด้าน : ☐ ด้านการผลิตบัณฑิต ☐ ด้านการวิจัย ☐ ด้านสิ่งแวดล้อม
☐ ด้านการบริการวิชาการ ☐ ด้านการทำนุบำรุงศิลปวัฒนธรรม
☑ ด้านการบริหารจัดการ ☐ ด้านอื่นๆ (ระบุ) .....

วัน / เดือน / ปี ที่นำไปใช้ประโยชน์ : วันที่ 10 เดือน เมษายน พ.ศ. 2569

วิธีการที่นำไปใช้ประโยชน์ : นำองค์ความรู้ส่วนของแนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ไปใช้ในการดำเนินงานตั้งค่า Facebook Page ของศูนย์คอมพิวเตอร์

ผลที่ได้รับจากการนำไปใช้ประโยชน์ : ช่วยให้ผู้ปฏิบัติงานทำตามขั้นตอนได้อย่างถูกต้อง ชัดเจน รวดเร็วขึ้น

โดยแนบรายการเอกสาร / หลักฐาน ประกอบการนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์ เป็น

☐ เอกสารหลักฐาน / รายงานผลการดำเนินงาน
☑ ภาพถ่าย / ไฟล์วีดีโอ
☐ เว็บไซต์ ที่ URL : .....
☐ อื่นๆ (ระบุ) .....

รายละเอียดดังเอกสารที่แนบมาพร้อมแบบฟอร์มนี้

ข้าพเจ้าขอรับรองว่า การนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์ตามรายละเอียดในแบบฟอร์มฉบับนี้ เป็นการนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้ประโยชน์ที่เกิดขึ้นจริงและมีผลที่ได้รับเป็นรูปธรรมตามที่รายงานในแบบฟอร์มฉบับนี้ ทุกประการ

ลงชื่อ อนันตพร ผู้ใช้ประโยชน์
(นางสาวอนันตพร อรุณฉาย)
ตำแหน่ง นักวิชาการคอมพิวเตอร์
วันที่ 10 เดือน เมษายน พ.ศ. 2569


[ด่วนที่สุด]
แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน
เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล
สืบเนื่องจากกรณีการนำภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้
1
1. ปิดสิทธิ์โพสต์สาธารณะ
ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง
2
2. เปิดระบบคัดกรองอัตโนมัติ
ใช้งาน Moderation Assist เพื่อตั้งค่าซ่อนความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย
ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย


Ao Kpru
ผู้ดูแล · 10 เมษายน เวลา 12:04 น.
แจ้ง Admin ทุกหน่วยงานทราบ
1. [ด่วนที่สุด] แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล
สืบเนื่องจากกรณีเมื่อวันที่ 8 เมษายน 2569 เกิดเหตุมีการนำภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้
(1) ปิดสิทธิ์โพสต์สาธารณะ ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง
(2) เปิดระบบคัดกรองอัตโนมัติ ใช้งาน Moderation Assist เพื่อตั้งค่าซ่อนความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย
ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย
2. นัดหมาย และแจ้งกำหนดจัดกิจกรรมแลกเปลี่ยนเรียนรู้สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล วันพุธที่ 29 เมษายน 2569 เวลา 09.00-12.00 น. ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

Ao Kpru
ผู้ดูแล · 9 เมษายน เวลา 11:56 น.
ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์กระทำความผิดในลักษณะนำรูปภาพส่วนตัวจากสื่อสังคมออนไลน์มาดัดแปลงเพื่อบิดเบือนข้อเท็จจริง และเผยแพร่ผ่านช่องทางการแสดงความคิดเห็น (Comment) ในหน้าเพจ Facebook ของหน่วยงานภายในมหาวิทยาลัย ซึ่งการกระทำดังกล่าวมิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ แต่มีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล นั้น
เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเ... ดูเพิ่มเติม
แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศ และการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน
สืบเนื่องจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เมื่อวันที่ 15 มีนาคม 2569 โดยการบิดเบือนรูปภาพและเผยแพร่ผ่านความคิดเห็นในหน้าเพจ Facebook
1. จำกัดสิทธิ์การโพสต์
• ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง
2. ยกระดับการคัดกรอง
• เปิดใช้งาน 'ตัวช่วยการควบคุม' (Moderation Assist)
• ตั้งค่าคัดกรองความคิดเห็น (Comment Filtering)
• ซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญบิดเบือนอัตโนมัติ
อ้างอิง: มติคณะกรรมการบริหารมหาวิทยาลัย ครั้งที่ 4/2569 วันที่ 2 เมษายน 2569


การปิดสิทธิ์โพสต์บนเพจ Facebook ของหน่วยงาน
เพื่อความปลอดภัยและภาพลักษณ์ที่เป็นทางการ
1. เข้าสู่ระบบ
ด้วยบัญชีผู้ดูแล (Admin)
2. สลับไปเพจหน่วยงาน
เลือกสลับการใช้งานไปยังเพจ
3. ไปที่การตั้งค่า
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > การตั้งค่า
4. เลือกความเป็นส่วนตัว & เพจและการแท็ก
ในเมนูด้านซ้าย เลือก "ความเป็นส่วนตัว" > "เพจและการแท็ก"
5. ตั้งค่าใครสามารถโพสต์ได้
เลือก "เฉพาะฉัน"
6. บันทึกอัตโนมัติ
ระบบจะบันทึกการตั้งค่าให้โดยอัตโนมัติ
จัดการเพจอย่างมืออาชีพ


การตั้งค่าตัวกรองคำหยาบและคำเฉพาะ
เพื่อการควบคุมเนื้อหาและภาพลักษณ์ที่ดี
1. สลับโปรไฟล์ไปที่หน้าเพจ
เลือกสลับบัญชีเป็นผู้ดูแลเพจ
2. ไปที่การตั้งค่า (Settings)
คลิกรูปโปรไฟล์ > การตั้งค่าและความเป็นส่วนตัว > ความเป็นส่วนตัว
3. เลือกโพสต์สาธารณะ (Public Posts)
ในเมนูด้านซ้าย เลือก "โพสต์สาธารณะ"
4. ตรวจสอบเนื้อหา (Content Moderation)
มองหาและคลิกหัวข้อ "การตรวจสอบเนื้อหา"
5. ซ่อนความคิดเห็น
ซ่อนความคิดเห็นที่มีคำบางคำ
มึ_มึ_ , กู_กู_ ,
คำไม่สุภาพ , คำด่า
6. บันทึก (Save)
กดปุ่ม "บันทึก" เพื่อสิ้นสุด
จัดการเพจอย่างมืออาชีพ