

รายงานผลการดำเนินการจัดการความรู้ ประจำปีการศึกษา 2568  
ด้านพันธกิจอื่น

เรื่อง แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิด  
ข้อมูลส่วนบุคคล (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 สามารถนำไปประยุกต์ใช้ในการบริหารจัดการข้อมูลในระบบสารสนเทศ และสื่อสังคมออนไลน์ได้อย่างถูกต้อง ปลอดภัย และมีประสิทธิภาพ โดยมุ่งเป้าสูงสุดให้อัตรการรั่วไหลของข้อมูลส่วนบุคคลเป็นศูนย์ (Risk Zero)

ดังนั้น หวังเป็นอย่างยิ่งว่าองค์ความรู้และแนวทางปฏิบัตินี้ จะเป็นประโยชน์ในการสร้างความตระหนักรู้ปรับเปลี่ยนพฤติกรรมการทำงาน และสร้างมาตรฐานความมั่นคงปลอดภัยด้านข้อมูลส่วนบุคคลของมหาวิทยาลัยราชภัฏกำแพงเพชรให้เป็นไปตามที่กฎหมายกำหนดอย่างยั่งยืนต่อไป

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ  
มหาวิทยาลัยราชภัฏกำแพงเพชร

## สารบัญ

| รายการ   | หน้า |
|--|------|
| ชื่อแผนการจัดการความรู้ เรื่อง “แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)” ..... | 1    |
| ผู้รับผิดชอบ.....  | 1    |
| หลักการและเหตุผล.....  | 1    |
| วัตถุประสงค์.....  | 1    |
| ผู้เข้าร่วมโครงการ.....  | 1    |
| สถานที่ดำเนินการ.....  | 1    |
| วิธีดำเนินงาน (แผนการจัดการความรู้ 6 ขั้นตอน) .....  | 2    |
| ผลการดำเนินงาน(แผนการจัดการความรู้ 6 ขั้นตอน) .....  | 3    |
| ประโยชน์ที่คาดว่าจะได้รับ.....   | 23   |
| องค์ความรู้.....   | 23   |
| การนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้.....  | 23   |
| ช่องทางการเผยแพร่องค์ความรู้.....  | 23   |
| <b>ภาคผนวก</b>   |      |
| แผนการจัดการความรู้ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ปีการศึกษา 2568.....   | 25   |

## 1. ชื่อแผนการจัดการความรู้

แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)

## 2. ผู้รับผิดชอบ

นางสาวอรปรียา คำแพง

นางสาวสรลชนา น้ำเงินสุกณี

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 สามารถนำไปใช้ในการบริหารจัดการข้อมูลในระบบสารสนเทศ และสื่อสังคมออนไลน์ได้อย่างถูกต้อง 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                               | <b>กิจกรรมที่ 1 จัดตั้งคณะกรรมการ</b><br>1.1 จัดตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ<br>1.2 จัดตั้งคณะกรรมการดำเนินงาน และกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร  | 31 ต.ค.<br>2568<br><br>12 พ.ย.<br>2568 | 1. คำสั่ง แต่งตั้งคณะกรรมการจัดการความรู้ จำนวน 1 ฉบับ<br>2. คำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล จำนวน 1 ฉบับ   | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ<br>- บุคลากรของสำนักฯ<br>- ตัวแทนหน่วยงานที่เกี่ยวข้องกับการกำกับและการใช้ข้อมูลส่วนบุคคล ภายในมหาวิทยาลัย | - คณะกรรมการจัดการความรู้ สำนักฯ        |
|       |  | <b>กิจกรรมที่ 2 ประชุมคณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล</b>  | 5 พ.ย.<br>2568                         | 1. แผนการจัดการความรู้ จำนวน 1 เรื่อง<br>2. รายการความเสี่ยงที่เกี่ยวข้อง จำนวน 5 ประเด็น   | คณะกรรมการจัดการความรู้และคณะกรรมการความเสี่ยงสำนักฯ   | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ |
| 2     | การเสาะหาความรู้ที่ต้องการ   | <b>กิจกรรมที่ 3 รวบรวมและศึกษา</b><br>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                                   | <b>กิจกรรมที่ 4 จัดทำเครื่องมือ/แนวทางปฏิบัติ</b> เช่น คู่มือ, Checklist การใช้งานระบบที่ต้องระบุตัวตน หรือ Infographic สรุปข้อปฏิบัติของบุคลากร   | ธ.ค.68 -<br>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  | <b>กิจกรรมที่ 5 แลกเปลี่ยนเรียนรู้</b><br>(1) นำเครื่องมือ/แนวทางปฏิบัติจาก กิจกรรมที่ 4 ไปทดลองใช้ในหน่วยงาน/กลุ่มงานที่เกี่ยวข้องกับ 3 อันดับความเสี่ยงที่วิเคราะห์ไว้<br>(2) จัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล สำหรับผู้ที่มีหน้าที่และความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) | ก.พ. - มี.ค.<br>2569                   | - ร้อยละของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ร้อยละ 60)<br>- ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ระดับดี)<br>- จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต (เป้าหมาย 0 ครั้ง) | บุคลากรมหาวิทยาลัยฯ  | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ |
| 5     | การนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้และสกัดขุมความรู้ออกมาบันทึกไว้ | <b>กิจกรรมที่ 6 จัดตั้งชุมชนนักปฏิบัติ (CoP) ในกลุ่มผู้ใช้งาน</b> กิจกรรมที่ 5 เพื่อแลกเปลี่ยนประสบการณ์ ปัญหา และจุดที่ต้องปรับปรุง ในการนำแนวทางไปปฏิบัติจริง และสกัดบทเรียนที่ได้ออกมา  | เม.ย. - พ.ค.<br>2569                   | - ชุมชนนักปฏิบัติ (CoP) เพื่อแลกเปลี่ยนเรียนรู้ จำนวน 1 ชุมชน   | คณะกรรมการ PDPA  | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ |

| ลำดับ | วิธีการสู่ความสำเร็จที่คาดการณ์   | กิจกรรมการจัดการความรู้   | ระยะเวลา  | ตัวชี้วัดและค่าเป้าหมาย  | กลุ่มเป้าหมาย   | ผู้รับผิดชอบ                            |
|-------|---|---|-----------|--|-----------------|---|
| 6     | การจัดบันทึกข้อความรู้และแก่นความรู้สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น | กิจกรรมที่ 7 นำบทเรียนที่สกัดได้จากกิจกรรมที่ 6 มาปรับปรุงและจัดทำเป็นชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล (ฉบับร่าง) สรุปลงเป็นฉบับสมบูรณ์ 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 สังกัด ณ วันที่ 20 ตุลาคม 2568

1.2 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ สังกัด ณ วันที่ 31 ตุลาคม 2568

1.3 คำสั่งมหาวิทยาลัยราชภัฏกำแพงเพชร เรื่อง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร สังกัด ณ วันที่ 12 พฤศจิกายน 2568

1.4 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล สังกัด 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](https://arit.kpru.ac.th/page_id/1649/TH)

## 2. การเสาะหาความรู้ที่ต้องการ

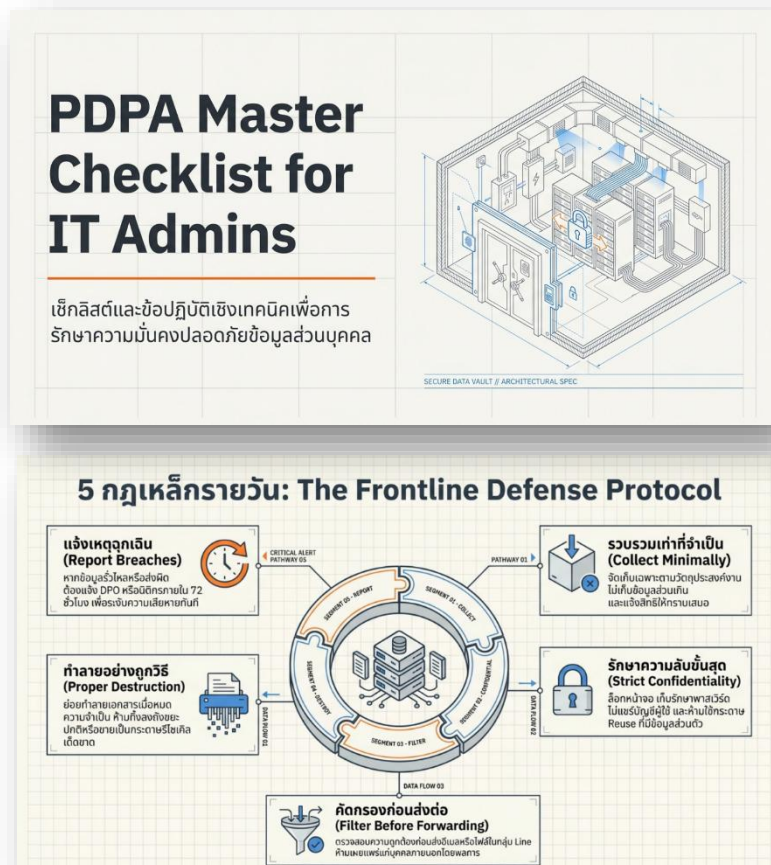
**กิจกรรมที่ 3** รวบรวมความรู้จากแหล่งต่าง ๆ ทั้งภายในและภายนอก คณะทำงานได้รวบรวมและศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA และตัวอย่าง Best Practice การลดความเสี่ยงและป้องกันการละเมิดข้อมูลส่วนบุคคลจากหน่วยงานที่ประสบความสำเร็จ ได้แก่ คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการณ์ละเมิดข้อมูล ของ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

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

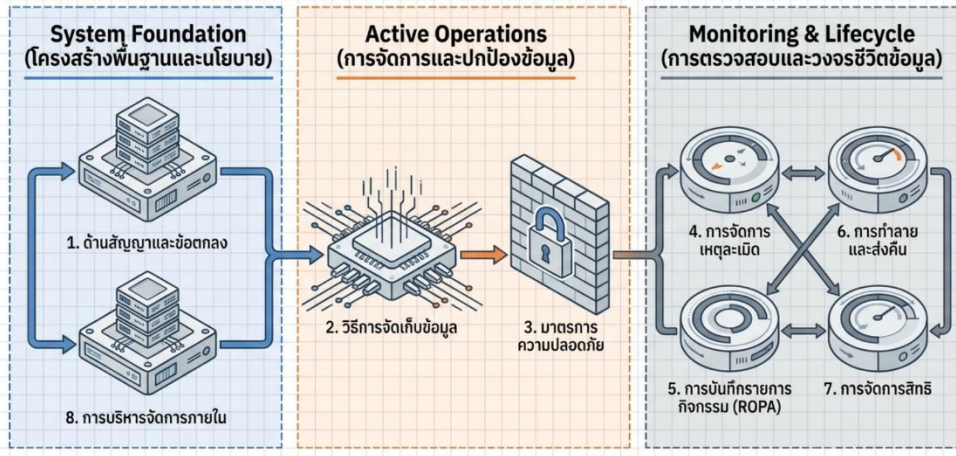
**3. ปรับปรุง ดัดแปลง หรือสร้างความรู้อย่างบางส่วนให้เหมาะสมต่อการใช้งานของตน** โดยการนำความรู้ที่ได้มาปรับให้เหมาะสมกับบริบทของมหาวิทยาลัย

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

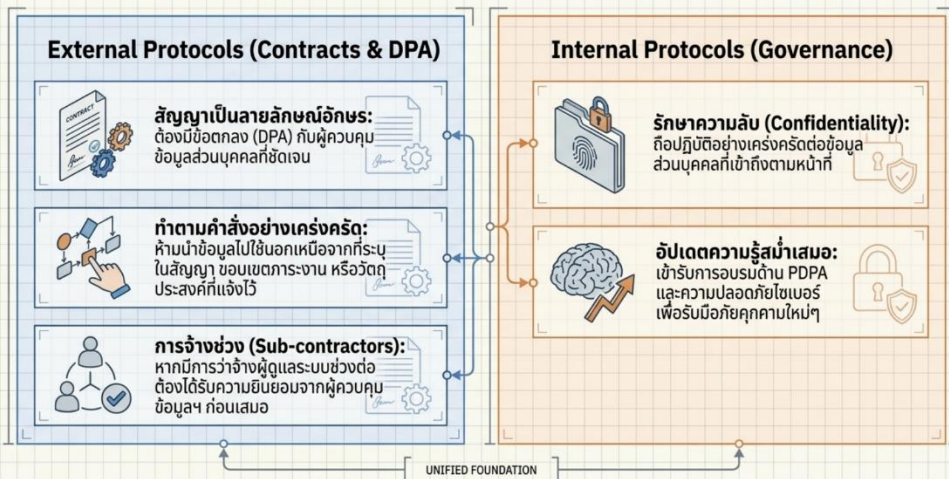
(1) PDPA Master Checklist for IT Admins เช็กลิสต์และข้อปฏิบัติเชิงเทคนิค เพื่อการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล สำหรับ Admin



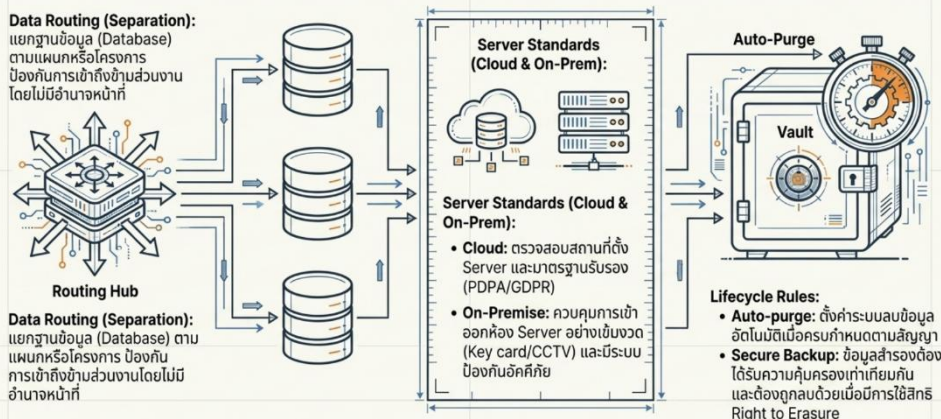
## The 8-Pillar Implementation Blueprint



## Foundation & Governance: ขอบเขตอำนาจหน้าที่

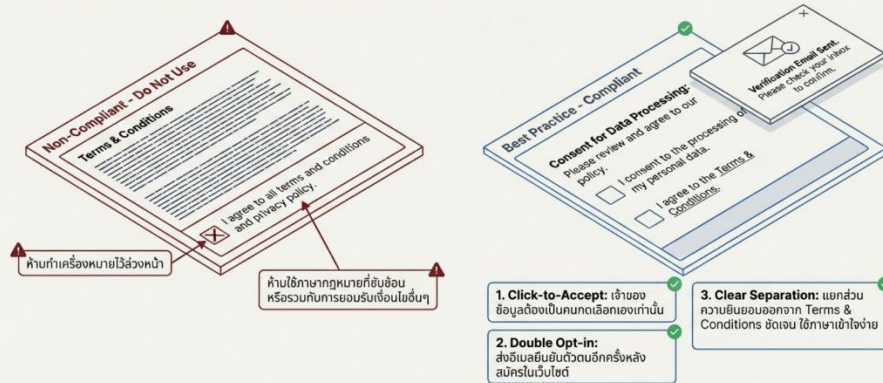


## Storage Architecture & Data Segregation

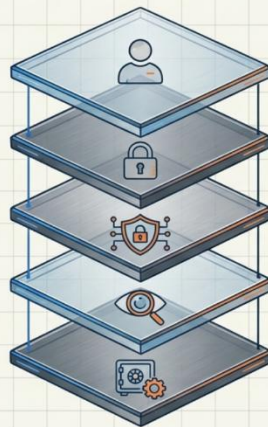


## Legal Consent Mechanisms in UI/UX

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)



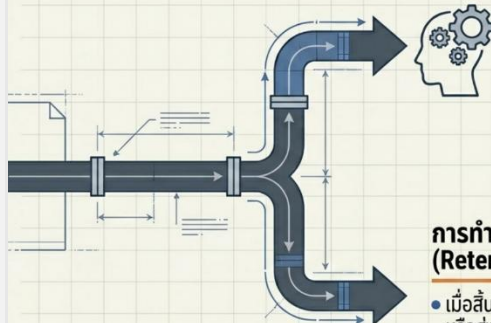
- จัดทำขั้นตอนการปฏิบัติงาน (SOP) สำหรับรับมือข้อมูลรั่วไหล
- เมื่อพบเหตุต้องสงสัย ต้องแจ้งผู้ควบคุมข้อมูลทันที (ภายใน 24-72 ชั่วโมง)

### Record of Processing (ROPA)

| Dashboard Matrix |         |                  |           |                  |         |                  |
|------------------|---------|------------------|-----------|------------------|---------|------------------|
| Data Category    | Purpose | Retention Period | Recipient | Data Used Matrix | Metrics | Technical Matrix |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |
|                  |         |                  |           |                  | ✓       |                  |

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

## Data Lifecycle Management & Subject Rights




**การจัดการสิทธิ์ (Data Subject Rights Readiness):**

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

**การทำลายและสัณฐาน (Retention & Disposal):**

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



## The Data Asset Radar

หมวดหมู่ข้อมูลที่ระบบ IT ต้องควบคุมดูแล

|   |   |
|---|---|
| <p><b>Quadrant 1: Digital Footprints (ร่องรอยดิจิทัล)</b></p> <ul style="list-style-type: none"> <li>หมายเลข IP Address, Cookies, Browser, Device ID, Time zone.</li> <li>การเข้าสู่ระบบ (Logins), Username/Password, PIN, App activity logs.</li> </ul>      | <p><b>Quadrant 2: Identity &amp; Profile (ข้อมูลระบุตัวตนบุคคล)</b></p> <ul style="list-style-type: none"> <li>ข้อมูลรายละเอียดส่วนบุคคล และการระบุ/ยืนยันตัวตน.</li> <li>ข้อมูลการติดต่อ, การทำงาน, การศึกษา.</li> </ul> |
| <p><b>Quadrant 3: Behavioral &amp; Commercial (พฤติกรรมและการทำธุรกรรม)</b></p> <ul style="list-style-type: none"> <li>ข้อมูลการเงิน และ การรับบริการ.</li> <li>ข้อมูลธุรกรรมมีประกัย.</li> <li>ข้อมูลวิจยตลาด และ ข้อมูลการสื่อสาร (บันทึกสนทนา).</li> </ul> | <p><b>Quadrant 4: Highly Sensitive (ข้อมูลอ่อนไหว - ควบคุมพิเศษ)</b></p> <p>ข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data) ต้องใช้มาตรการขั้นสูงสุดและบันทึก ROPA เสมอ.</p>  |

## Self-Audit Diagnostic Matrix

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

สถานะของระบบ IT ในปัจจุบันของคุณเป็นอย่างไร? นำเช็กลิสต์นี้ไปใช้ประเมินทันที

(2) สร้างกลไกการรับรื้อนโยบายการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) โดยเผยแพร่ ประกาศ นโยบายคุ้มครองข้อมูลส่วนบุคคล ประชาสัมพันธ์ไว้ที่หน้าหลักเว็บไซต์มหาวิทยาลัย ราชภัฏกำแพงเพชร ดังภาพ



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



(3) จัดทำ Infographic แนวปฏิบัติ แผนผังขั้นตอน และอื่นๆที่เกี่ยวข้อง เผยแพร่ผ่านเว็บไซต์ มหาวิทยาลัย และ เพจ ศูนย์คอมพิวเตอร์

**แนวปฏิบัติ** เมื่อตกเป็นเหยื่อถูกแอบอ้าง รูปภาพบน **FACEBOOK** ติดต่อบิดเบือนข้อเท็จจริง

**ขั้นตอนปฏิบัติ 5 ขั้นตอน** เมื่อตกเป็นเหยื่อ

- 1. เก็บหลักฐานให้ครบ**
  - ✓ แคปหน้าจอโพสต์/ข้อความ
  - ✓ คัดลอกลิงก์โปรไฟล์ & โพสต์
  - ✓ บันทึกวัน/เวลา
- 2. แจ้งความดำเนินคดี**
  - ✓ ไปสถานีตำรวจท้องที่
  - ✓ ขอใบแจ้งความ/ใบร้องทุกข์
- 3. รายงาน FACEBOOK**
  - แอบอ้างเป็นผู้อื่น
  - คุกคาม
- 4. ประกาศแจ้งหน้า FEED**

โพสต์หน้า Timeline ของตนเอง ยืนยันความบริสุทธิ์ & เตือนภัย
- 5. ตั้งค่าความเป็นส่วนตัว**

ปรับการมองเห็นรูปภาพ/โพสต์ เลือก 'เพื่อนเท่านั้น'

**ปกป้องตนเอง ดำเนินคดีให้ถึงที่สุด!** 1441

Computer Center - KPRU  
9 เมษายน เวลา 16:30 น.

**⚠️ แจ้งเตือนภัย! ถูกแอบอ้างรูปภาพบน FACEBOOK**  
ติดต่อและกล่าวหาหลอกลวง หากคุณหรือคนใกล้ชิดตกเป็นเหยื่อของการถูกนำรูปไปแอบอ้าง หรือใช้ในการกระทำความผิด นี่คือ 5 ขั้นตอนปฏิบัติเมื่อตกเป็นเหยื่อ ที่ควรทำทันที:

- 1. เก็บหลักฐานให้ครบ**  
แคปหน้าจอ โพสต์ หรือข้อความที่ใช้แอบอ้างคัดลอก ลิงก์โปรไฟล์ (URL) และลิงก์โพสต์ของมีจฉายืนยันที่กวันและเวลาที่พบเห็น
- 2. แจ้งความดำเนินคดี** 🚔 เดินทางไปยังสถานีตำรวจท้องที่เพื่อแจ้งความ ขอใบแจ้งความ หรือใบร้องทุกข์เพื่อใช้เป็นหลักฐานทางกฎหมาย
- 3. รายงาน FACEBOOK (Report)** ▶️ กระจายงาน โป้รไฟล์หรือโพสต์นั้นๆ เลือกหัวข้อ "แอบอ้างเป็นผู้อื่น" (Pretending to be someone) หรือ "คุกคาม" (Harassment)
- 4. ประกาศแจ้งหน้า FEED** 📣 โพสต์หน้า Timeline ของตนเองเพื่อยืนยันความบริสุทธิ์แจ้งเตือนภัยให้คนอื่นทราบ (เช่น "โดนแอบอ้าง! ไม่มีการกู้เงิน" หรือ "ระวังเพจปลอม")
- 5. ตั้งค่าความเป็นส่วนตัว** 🔒 ปรับการมองเห็นรูปภาพ หรือโพสต์ต่างๆ ในอดีตและอนาคตเลือกตั้งค่าเป็น "เพื่อนเท่านั้น" (Friends Only) เพื่อป้องกันมีจฉายื่นเข้าถึงรูปถ่ายได้ง่าย

ปกป้องตนเอง ดำเนินคดีให้ถึงที่สุด!  
สายด่วนอาชญากรรมทางเทคโนโลยี: 1441

#เตือนภัย #มีจฉายื่น #แอบอ้างรูปภาพ #ความปลอดภัยโซเชียล #1441 #ตำรวจไซเบอร์ คุ้น้อยลง

มหาวิทยาลัยราชภัฏกำแพงเพชร  
KAMPHAENG PHET RAJABHAT UNIVERSITY

รับสมัครนักศึกษาใหม่ 2569  
เปิดรับสมัครอยู่ชั้น วิชาเกษตรศาสตร์

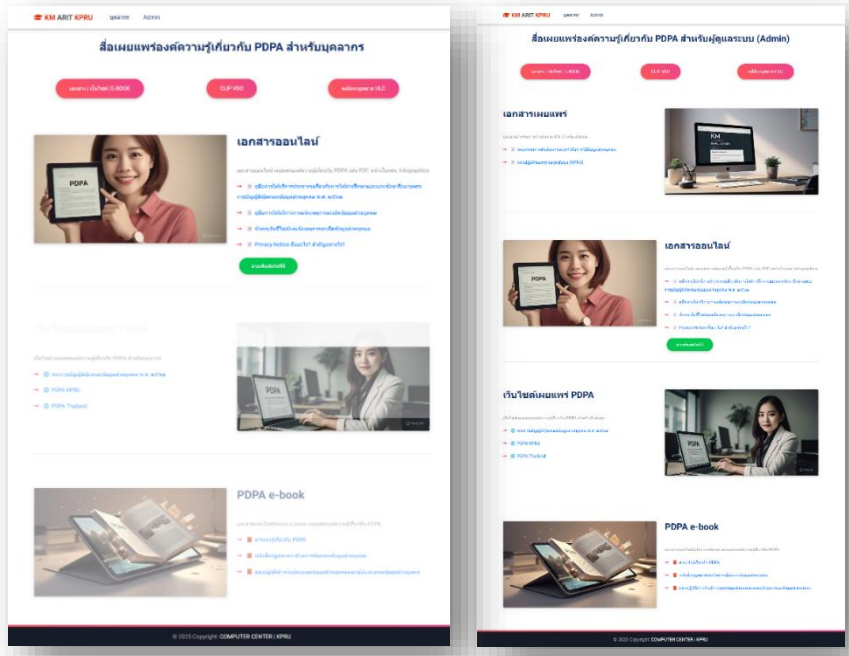
**แจ้งเตือนภัย! ถูกแอบอ้างรูปภาพบน Facebook ติดต่อและกล่าวหาหลอกลวง**

- 1. เก็บหลักฐาน**  
แคปหน้าจอ, ลิงก์ลิงก์, บันทึกวัน/เวลา
- 2. แจ้งความดำเนินคดี & ขอใบแจ้งความ**  
ไปสถานีตำรวจ & ขอใบแจ้งความ
- 3. รายงาน FACEBOOK**  
เลือก 'แอบอ้างเป็นผู้อื่น' หรือ 'คุกคาม'
- 4. ประกาศแจ้งหน้า FEED**  
โพสต์ Timeline ของตนเอง ยืนยันความบริสุทธิ์ & เตือนภัย
- 5. ตั้งค่าความเป็นส่วนตัว**  
ปรับการมองเห็น เลือก 'เพื่อนเท่านั้น'

**ปกป้องตนเอง ดำเนินคดีให้ถึงที่สุด!** 1441

ข่าวกิจกรรม

### (4) เผยแพร่องค์ความรู้เกี่ยวกับ PDPA ผ่านสื่อส่งเสริมการเรียนรู้ PDPA



### (5) เผยแพร่ มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (การตั้งค่าสื่อสังคมออนไลน์ จำกัดสิทธิ์การโพสต์และการแสดงความคิดเห็น) ประสานงาน Admin ผ่านกลุ่มผู้ดูแลเว็บภายใน KPRU

มหาวิทยาลัยราชภัฏกำแพงเพชร

## มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (ดำเนินการตามมาตรการเชิงเทคนิค) Facebook Page

- 1. ควบคุมการโพสต์และแสดงความคิดเห็น (Content Moderation)**
  - ดำเนินการจัดการลบขบวนการโพสต์บนหน้าเพจ (Disable Visitor Posts)
  - ตั้งค่าที่ตรงจุดความคิดเห็น (Comment Ranking/Filtering) ให้กรองด้วย Moderation Asses ใน Facebook เพื่อลดความถี่ที่ผู้โพสต์หรือผู้แสดงความคิดเห็นจะมองเห็น
- 2. การจัดการสิทธิ์และการเข้าถึง (Identity and Access Management)**
  - ตรวจสอบและจำกัดจำนวนผู้แสดง (Page Roles) ให้เฉพาะบุคคลที่จำเป็น และบังคับใช้การยืนยันตัวตนสองชั้น (Two-Factor Authentication: 2FA) สำหรับบัญชีผู้ดูแลระบบ เพื่อป้องกันการถูกแฮ็กหรือเข้าถึงโดยไม่ได้รับอนุญาต
- 3. การรายงานและระงับเนื้อหา (Reporting & Takedown)**
  - ใช้เครื่องมือรายงาน (Report) ของ Meta เพื่อแจ้งการฉ้อโกง (Impersonation) และการละเมิดมาตรฐานชุมชน (Community Standards) ที่สื่อทาง Facebook ดำเนินการสนับสนุนการดำเนินการระงับเนื้อหาละเมิด
- 4. การบันทึกและเก็บรวบรวมหลักฐานทางดิจิทัล (Digital Evidence Preservation)**
  - ใช้ฟังก์ชันการบันทึกกิจกรรม (Activity Log) และการจับภาพหน้าจอ (Screen Capture) ใ้ระบุ URL และเวลาที่เกิดเหตุอย่างชัดเจน เพื่อนำไปใช้เป็นหลักฐานในการดำเนินคดีตามกฎหมาย
- 5. การตรวจสอบความปลอดภัยของระบบ (Security Monitoring)**
  - หมั่นตรวจสอบกิจกรรมเข้าถึงบัญชีโซเชียลมีเดียใช้งาน (Active Sessions) ในการจำกัดความปลอดภัยของ Facebook เพื่อตรวจสอบว่าการเข้าถึงงานที่ผิดปกติหรือไม่

WWW.KPRU.AC.TH  
KAMPANGPHET RAJABHAT UNIVERSITY

Ao Kpru  
15 มีนาคม · ๑

ประกาศ!!  
ใช้วิธีมอบหมายจาก ผู้ว่าราชการจังหวัดกำแพงเพชรให้โดยมีคุณยศ นรค.ภ.พ. ให้ประสานทุกหน่วยงานดังนี้:

เพื่อเป็นแนวทางในการก่อกวนหรือการโจมตีของสื่อโซเชียลจากบุคคลภายนอก ระยะเวลาเริ่มแจ้ง Admin เพจ facebook ทุกหน่วย ดำเนินการดังนี้ให้เฉพาะ Admin (ผู้ดูแล) เท่านั้นที่สามารถโพสต์หรือแสดงความคิดเห็นได้

- การจำกัดสิทธิ์การโพสต์ (Visitor Posts)
- การควบคุมการแสดงความคิดเห็น (Comments)

เนื่องจากมีผู้ใช้โซเชียลมีเดียโพสต์ในเพจของหน่วยงาน และอาจกระทบภาพลักษณ์องค์กรในอนาคตได้ จะดำเนินการขอความร่วมมือทุกหน่วยงานในการแจ้งจับกุม หรือแจ้ง:

1. การจำกัดสิทธิ์การโพสต์ (VISITOR POSTS)

ตามปกติ Facebook จะมอบให้ทุกเพจโพสต์อย่างไรก็ได้ (ซึ่งจะไม่ปรากฏในเมนู "Community") แต่ควรเปิดส่วนนี้เพื่อใช้ควบคุมเนื้อหาที่ระบุบนหน้าเพจขององค์กร

- ไปที่ Settings (การตั้งค่า) > Privacy (ความเป็นส่วนตัว) > Page and Tagging (เพจและการแท็ก)
- ใต้หัวข้อ "Who can post on your Page?" ให้เลือกเป็น "Only Me" (ซึ่งในบริบทเพจหมายถึงเฉพาะ Admin/Editor เท่านั้น)

2. การควบคุมการแสดงความคิดเห็น (COMMENTS)

หากหน่วยงานต้องการควบคุมเนื้อหาโพสต์ใดโพสต์หนึ่ง หรือจำกัดสิทธิ์ สามารถทำได้หลายระดับ:

- เปิดคอมเมนต์ที่โพสต์นี้ เปิดทุกโพสต์นี้ทั้งหมด ไปที่จุดที่ 3 ข้างล่างของรายการโพสต์นี้ > เมื่อกำหนด "Who can comment on your post?" > เลือก "Profiles and Pages you mention" (ถ้าเราไม่แน่ใจโดยนัย ก็จะไม่ใคร่คอมเมนต์ได้ก็ออกจาก Admin)
- การกรองคำพยานแบบ (Content Moderation): ไปที่ Settings > Public Posts > Content Moderation สามารถใส่ Keyword ที่ไม่ต้องการ หรือเปิด "Profanity Filter" เพื่อใช้ระบบตรวจจับคอมเมนต์ที่ไม่เหมาะสมได้ทันที

## [ด่วนที่สุด]

# แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน

**เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล**

“ สืบเนื่องจากการนำภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้ ”

- ### 1. ปิดสิทธิ์โพสต์สาธารณะ

ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง
- ### 2. เปิดระบบคัดกรองอัตโนมัติ

ใช้งาน Moderation Assist เพื่อตั้งค่าข้อความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย

ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย

## การปิดสิทธิ์โพสต์บนเพจ Facebook ของหน่วยงาน

เพื่อความปลอดภัยและภาพลักษณ์ที่เป็นทางการ

- ### 1. เข้าสู่ระบบ

ด้วยบัญชีผู้ดูแล (Admin)
- ### 2. สลับไปเพจหน่วยงาน

เลือกสลับการใช้งานไปยังเพจ
- ### 3. ไปที่การตั้งค่า

คลิกเมนูโปรไฟล์ > การตั้งค่า และความเป็นส่วนตัว > การตั้งค่า
- ### 4. เลือกความเป็นส่วนตัว & เพจและการแก็ก

ในเมนูด้านซ้าย เลือก “ความเป็นส่วนตัว” > “เพจและการแก็ก”
- ### 5. ตั้งค่าใครสามารถโพสต์ได้

เลือก “เฉพาะฉัน”
- ### 6. บันทึกอัตโนมัติ

ระบบจะบันทึกการตั้งค่าให้โดยอัตโนมัติ

จัดการเพจอย่างมืออาชีพ

**Ao Kpru**  
ผู้ดูแล · 10 เมษายน เวลา 12:04 น. · 🌐

แจ้ง Admin ทุกหน่วยงานทราบ

1. [ด่วนที่สุด] แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล

สืบเนื่องจากการเมื่อวันที่ 8 เมษายน 2569 เกิดเหตุการณ์ภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin ทุกหน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้

(1) ปิดสิทธิ์โพสต์สาธารณะ ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง

(2) เปิดระบบคัดกรองอัตโนมัติ ใช้งาน Moderation Assist เพื่อตั้งค่าข้อความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย

ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย

2. นัดหมาย และแจ้งกำหนดจัดกิจกรรมแลกเปลี่ยนเรียนรู้สำหรับประมวลผลข้อมูลส่วนบุคคล วันพุธที่ 29 เมษายน 2569 เวลา 09.00-12.00 น. ณ ห้องประชุมดอกสีก สำหรับวิทยบริการและเทคโนโลยีสารสนเทศ

**Ao Kpru**  
ผู้ดูแล · 9 เมษายน เวลา 11:56 น. · 🌐

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์กระทำด้วยความผิดในลักษณะนำรูปภาพส่วนตัวจากสื่อสังคมออนไลน์มาดัดแปลงเพื่อบิดเบือนข้อเท็จจริง และเผยแพร่ผ่านช่องทางแสดงความคิดเห็น (Comment) ในหน้าเพจ Facebook ของหน่วยงานภายในมหาวิทยาลัย ซึ่งการกระทำดังกล่าวนี้ใช้ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ แต่มีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล นั้น

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ... ดูเพิ่มเติม

### แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศ และการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน

สืบเนื่องจากการละเมิดข้อมูลส่วนบุคคล เมื่อวันที่ 15 มีนาคม 2569 โดยการบิดเบือนรูปภาพและเผยแพร่ผ่านความคิดเห็นในหน้าเพจ Facebook

- #### 1. จำกัดสิทธิ์การโพสต์

  - ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง
- #### 2. ยกระดับการคัดกรอง

  - เปิดใช้งาน “ตัวช่วยการควบคุม” (Moderation Assist)
  - ตั้งค่าคัดกรองความคิดเห็น (Comment Filtering)
  - ซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญบิดเบือนอัตโนมัติ

อ้างอิง: หลักสูตรการบริหารมหาวิทยาลัย ครั้งที่ 4/2569 วันที่ 2 เมษายน 2569

## การตั้งค่าตัวกรองคำหยาบและคำเฉพาะ

เพื่อการควบคุมเนื้อหาและภาพลักษณ์ที่ดี

- ### 1. สลับโปรไฟล์ไปที่หน้าเพจ

เลือกสลับบัญชีเป็นผู้ดูแลเพจ
- ### 2. ไปที่การตั้งค่า (Settings)

คลิกเมนูโปรไฟล์ > การตั้งค่า และความเป็นส่วนตัว > ความเป็นส่วนตัว
- ### 3. เลือกโพสต์สาธารณะ (Public Posts)

ในเมนูด้านซ้าย เลือก “โพสต์สาธารณะ”
- ### 4. ตรวจสอบเนื้อหา (Content Moderation)

มองหาและคลิกหัวข้อ “การตรวจสอบเนื้อหา”
- ### 5. ซ่อนความคิดเห็น

ซ่อนความคิดเห็นที่มีคำบางคำ มี\_มี\_ , ู-ู- , คำไม่สุภาพ , คำต่ำ
- ### 6. บันทึก (Save)

กดปุ่ม “บันทึก” เพื่อสิ้นสุด

จัดการเพจอย่างมืออาชีพ

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

**รายงานสถานการณ์และการตรวจพบเหตุละเมิด**

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์การกระทำความผิด ดังนี้

- **ลักษณะการกระทำ** มีการนำรูปภาพของบุคลากรและบุคคลภายนอกไปตัดต่อโดยไม่ได้รับอนุญาต เพื่อสร้างสื่อบิดเบือนข้อเท็จจริงในลักษณะการทวงหนี้ และกล่าวหาว่าเป็นส่วนหนึ่งของขบวนการฉ้อโกง

- **ช่องทางที่เกิดเหตุ** การนำภาพตัดต่อดังกล่าวไปเผยแพร่ผ่านช่องการแสดงความคิดเห็น (Comment) ในเพจ Facebook "สโตนท์คนวิศวะ มหาวิทยาลัยราชภัฏกำแพงเพชร"

**การดำเนินการโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)**

ภายหลังตรวจพบเหตุ มหาวิทยาลัยฯ ได้ดำเนินการตามขั้นตอนมาตรฐานทางกฎหมาย (PDPA) อย่างเร่งด่วน ดังนี้

- **การรายงานเหตุ** รายงานสรุปเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อผู้บริหารระดับสูง (อธิการบดี/รองอธิการบดี) เพื่อทราบสถานการณ์

- **การแจ้งเหตุต่อหน่วยงานกำกับดูแล** ดำเนินการจัดทำหนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายในกรอบเวลา 72 ชั่วโมงตามที่กฎหมายกำหนด

- **การเยียวยาผู้ได้รับผลกระทบ** จัดทำบันทึกแจ้งเหตุให้แก่ผู้ที่ได้รับผลกระทบโดยตรง พร้อมให้คำแนะนำในการปฏิบัติตนและการคุ้มครองสิทธิรายบุคคล

**มาตรการตอบโต้ทางเทคนิคและทางกฎหมาย (สำนักวิทยบริการฯ)**

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) ที่เกี่ยวข้องกับบิดเบือนข้อมูล โดยอัตโนมัติ

จึงเรียนที่ประชุมทราบแนวทางการจัดการเหตุละเมิด และขอความร่วมมือทุกหน่วยงานตรวจสอบและรักษามาตรฐานการตั้งค่าสื่อสังคมออนไลน์โดยการ**จำกัดสิทธิ์การโพสต์และการแสดงความคิดเห็นอย่างเคร่งครัด** ทั้งนี้ สำนักวิทยบริการฯ ได้ดำเนินการจัดส่งบันทึกข้อความแจ้งเวียนไปในระบบ E-Office วันที่ 7 เมษายน 2569

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

| ที่ | เลขที่เรื่อง | เลขคดี            | วันที่     | เรื่อง   | เรื่อง  | จาก                              | หมายเหตุ | ปฏิบัติ | entry               | แก้ไข |
|-----|--------------|-------------------|------------|--|---|----------------------------------|----------|---------|---------------------|-------|
|     | ๒๕๖๐๖๓๖๔     | ๒๒๓.๒๒.๓.๐๒๑/๒๕๖๑ | 07/04/2569 | 1.ขอคืนเอกสาร<br>2.ขอคืนและนำเอกสาร<br>3.ขอคืนใบรายการ<br>4.ขอคืนและนำเอกสาร<br>คืนเอกสาร<br>5.ขอคืนและคืนใบ<br>ดูค่าทราบ<br>6.ขอคืนและนำเอกสาร<br>คืนใบ<br>7.ผู้ดำเนินการดำเนินการ<br>และคืนใบเอกสาร<br>8.ผู้ดำเนินการดำเนินการ<br>และคืนใบ<br>9.ผู้ดำเนินการดำเนินการ<br>รับทราบและขอคืน<br>10.ผู้ดำเนินการดำเนินการ<br>รับทราบ<br>11.ผู้ดำเนินการดำเนินการ<br>รับทราบ<br>12.ผู้ดำเนินการดำเนินการ<br>คืนเอกสาร<br>13.ผู้ดำเนินการดำเนินการ<br>และคืนเอกสาร<br>14.ผู้ดำเนินการดำเนินการ<br>และคืนเอกสาร<br>15.ผู้ดำเนินการดำเนินการ<br>รับทราบและคืน | แนวทางการปฏิบัติงานของบุคลากร<br>ที่สำนักงานอธิการบดีมหาวิทยาลัยราชภัฏวชิรเวศน์ | ผู้อำนวยการสำนักงาน<br>อธิการบดี |          |         | 08/04/2569<br>09:07 |       |



## บันทึกข้อความ

ส่วนราชการ งานพัฒนาสมรรถนะดิจิทัลและภาษาต่างประเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ  
ที่ สวท.งพ.ว ๐๐๖๑/๒๕๖๙ วันที่ ๗ เมษายน ๒๕๖๙

เรื่อง แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศและการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน

---

**เรียน** [เรียน]

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ ๑๕ มีนาคม ๒๕๖๙ โดยมีเหตุการณ์กระทำความผิดในลักษณะนำรูปภาพส่วนตัวจากสื่อสังคมออนไลน์ มาดัดแปลงเพื่อบิดเบือนข้อเท็จจริง และเผยแพร่ผ่านช่องทางแสดงความคิดเห็น (Comment) ในหน้าเพจ Facebook ของหน่วยงานภายในมหาวิทยาลัย ซึ่งการกระทำดังกล่าว **มิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัย จัดเก็บ** 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 : F๒๘AgKXUFAVKCtt๓JL๓

จากบันทึกข้อความข้างต้น เหตุการณ์ละเมิดข้อมูลส่วนบุคคลในวันดังกล่าว มิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ จึงสรุปได้ว่า **ไม่มีการได้รับรายงานการละเมิดข้อมูลส่วนบุคคล**

## (8) ขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (PDPA Response Plan)

ขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (PDPA Response Plan) เพื่อให้เข้าใจง่ายและพร้อมนำไปใช้งานจริงเมื่อเกิดเหตุฉุกเฉิน สรุป 4 ขั้นตอนหลัก ดังนี้

### ขั้นตอนที่ 1 ตรวจพบ & สกัดกั้น (Containment) — ภายใน 24 ชม. แรก

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

### ขั้นตอนที่ 2 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

### ขั้นตอนที่ 3 แจ้งเตือนตามกฎหมาย (Notification) — ต้องเสร็จสิ้นใน 72 ชม.

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

### ขั้นตอนที่ 4 อุดช่องโหว่ & เยียวยา (Recovery & Remediation) — หลังเกิดเหตุ

- **ซ่อมแซมระบบถาวร** ทีมไอทีทำการอุดช่องโหว่ อัปเดต Patch ปรับปรุงกฎ Web Application Firewall (WAF) และกู้คืนระบบที่ปลอดภัยจาก Backup
- **อนุมัติงบประมาณ** 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.) นี้ เป็นแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล ว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าว ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

| ตัวอย่างที่ | เหตุการณ์   | แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) | แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล | เหตุผล  |
|-------------|---|---|-----------------------------------|---|
| 1           | ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่นำเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป                                | ไม่ต้องแจ้ง   | ไม่ต้องแจ้ง                       | ความเสี่ยงต่ำ เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่นำเชื่อถือแล้วข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล    |
| 2           | ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล | ต้องแจ้ง  | ต้องแจ้ง                          | เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้ และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก |
| 3           | ระบบไฟฟ้าใน Call center ของ คณะ ส่วนงาน   | ไม่ต้องแจ้ง   | ไม่ต้องแจ้ง                       | ข้อมูลส่วนบุคคลดังกล่าว ไม่อยู่ในสภาพพร้อมใช้งานเนื่องจาก   |

| ตัวอย่างที่ | เหตุการณ์  | แจ้งเหตุแก่<br>สำนักงานคณะกรรมการ<br>คุ้มครองข้อมูล<br>ส่วนบุคคล (สคส.) | แจ้งเหตุแก่<br>เจ้าของข้อมูล<br>ส่วนบุคคล   | เหตุผล  |
|-------------|--|---|---|---|
|             | หน่วยงานในฐานะเป็นผู้<br>ควบคุมข้อมูลส่วนบุคคล<br>ขัดข้อง โดยไฟดับชั่วคราว<br>ส่งผลให้ระบบคอมพิวเตอร์<br>และอุปกรณ์คอมพิวเตอร์<br>ของคณะ ส่วนงาน<br>หน่วยงานในฐานะเป็นผู้<br>ควบคุมข้อมูลส่วนบุคคลไม่<br>สามารถให้บริการได้ชั่วคราว  |   |   | ปัญหาทางด้านเทคโนโลยีเมื่อ<br>ระบบไฟฟ้ากลับมาเหมือนเดิม<br>ข้อมูลส่วนบุคคลดังกล่าว ก็<br>สามารถใช้งานได้ จึงไม่ถือว่าเป็น<br>กรณีการละเมิดข้อมูลส่วน<br>บุคคลที่มีความเสี่ยงที่จะมี<br>ผลกระทบต่อสิทธิและเสรีภาพ<br>ของบุคคล  |
| 4           | ผู้ควบคุมข้อมูลส่วนบุคคล<br>ถูกภัยคุกคามทางไซเบอร์<br>โดยถูกโจมตีจากมัลแวร์<br>เรียกค่าไถ่ (Ransomware)<br>ข้อมูลส่วนบุคคลทั้งหมดของ<br>ผู้ควบคุมข้อมูล ส่วนบุคคล<br>ถูกเข้ารหัสโดยผู้โจมตี<br>(hacker) และไม่มีข้อมูล<br>สำรอง จึงไม่สามารถที่จะ<br>เข้าถึงและใช้งานข้อมูล<br>ดังกล่าวได้ | ต้องแจ้ง  | ต้องแจ้ง  | เนื่องจากข้อมูลส่วนบุคคล<br>ดังกล่าวอยู่ในสภาพที่สามารถ<br>ระบุตัวบุคคลได้และการถูก<br>โจมตีจากมัลแวร์เรียกค่าไถ่ ทำ<br>ให้ข้อมูลดังกล่าวไม่อยู่ในสภาพ<br>ที่พร้อมใช้งาน และไม่มีข้อมูล<br>สำรอง นอกจากนี้ยังอาจ<br>ก่อให้เกิดความเสียหายต่อธุรกิจ<br>ของผู้ควบคุมข้อมูลส่วนบุคคล<br>รวมถึงตัวเจ้าของข้อมูลส่วน<br>บุคคลจึงต้องแจ้งเหตุ |
| 5           | ธนาคารได้รับการติดต่อจาก<br>ลูกค้าธนาคาร 1 ราย ว่า<br>ได้รับใบแจ้งหนี้เรียกเก็บเงิน<br>ของบุคคลที่ไม่รู้จัก ผู้ควบคุม<br>ข้อมูลส่วนบุคคลทำการ<br>ตรวจสอบแล้วภายใน 24<br>ชั่วโมง พบว่ามีการรั่วไหล<br>ของข้อมูลส่วนบุคคลจำนวน<br>10 ราย   | ต้องแจ้ง  | ต้องแจ้งเฉพาะ<br>เจ้าของข้อมูลส่วน<br>บุคคล 10 ราย ที่<br>ถูกเรียกเก็บเงิน<br>ตาม ใบแจ้งหนี้<br>ของธนาคาร | เนื่องจากข้อมูลดังกล่าวเป็น<br>ข้อมูลที่รั่วไหลออกไปจริง ใน<br>เบื้องต้นมีผลกระทบเฉพาะผู้ที่<br>ถูกเรียกเก็บเงินตามใบแจ้งหนี้<br>อย่างไรก็ตามคณะ ส่วนงาน<br>หน่วยงานในฐานะผู้ควบคุม<br>ข้อมูลส่วนบุคคลจะต้อง<br>ดำเนินการตรวจสอบเพิ่มเติมว่า<br>มีบุคคลอื่นใดที่ข้อมูลรั่วไหล<br>ออกไปภายนอกหรือไม่<br>หากพบจะต้องแจ้งเพิ่มเติม         |
| 6           | ผู้ควบคุมข้อมูลส่วนบุคคล<br>ให้บริการซื้อขายสินค้า<br>ออนไลน์ทั่วประเทศ ต่อมาผู้<br>ควบคุมข้อมูลส่วนบุคคลถูก<br>โจมตีจากภัยคุกคามทาง   | ต้องแจ้ง  | ต้องแจ้งลูกค้าของ<br>ผู้ควบคุมข้อมูล<br>ส่วนบุคคลในส่วน<br>ที่มีข้อมูลรั่วไหล<br>บน อินเทอร์เน็ต          | ข้อมูลที่มีการรั่วไหลบน<br>อินเทอร์เน็ต ซึ่งถูกโจมตี เป็น<br>การกระทำความผิดตาม<br>กฎหมายว่าด้วยการกระทำ<br>ความผิดเกี่ยวกับคอมพิวเตอร์   |

| ตัวอย่างที่ | เหตุการณ์   | แจ้งเหตุแก่<br>สำนักงานคณะกรรมการ<br>คุ้มครองข้อมูล<br>ส่วนบุคคล (สคส.)   | แจ้งเหตุแก่<br>เจ้าของข้อมูล<br>ส่วนบุคคล  | เหตุผล  |
|-------------|---|---|--|---|
|             | ไซเบอร์ โดยข้อมูลรายชื่อ<br>ผู้ใช้บริการ รหัสผ่าน และ<br>ประวัติการซื้อสินค้าถูก<br>เข้าถึงและนำไปโพสต์บน<br>อินเทอร์เน็ต   |   |  | ข้อมูลที่รั่วไหลประกอบด้วย<br>รายชื่อและข้อมูลสำคัญของ<br>ผู้ใช้บริการ จึงจำเป็นต้องแจ้ง<br>เหตุแก่ เจ้าของข้อมูลส่วนบุคคล<br>เพราะมีความเสี่ยงสูงที่ข้อมูล<br>ดังกล่าวจะถูกนำไปทำธุรกรรมที่<br>ผิดกฎหมาย   |
| 7           | เว็บไซต์ผู้ให้บริการ Web<br>Hosting ที่รับจ้าง<br>ประมวลผลข้อมูลส่วนบุคคล<br>จากผู้ควบคุมข้อมูลส่วน<br>บุคคลเกิดปัญหาผิดพลาด<br>ของโปรแกรมในการ<br>ตรวจสอบสิทธิการเข้าถึง<br>ทำให้ผู้ใช้บริการไม่สามารถ<br>เข้าใช้บริการได้ | ต้องแจ้งผู้ควบคุมข้อมูล<br>ส่วนบุคคลเพื่อให้ผู้<br>ควบคุมข้อมูลส่วนบุคคล<br>แจ้งสำนักงานฯ<br>เนื่องจากมีผลกระทบต่อ<br>กลุ่มลูกค้าพอสมควร<br>เพราะปัญหาดังกล่าวทำให้<br>ให้กลุ่มลูกค้าไม่สามารถ<br>เข้าถึงข้อมูลส่วนบุคคล<br>ได้ | ผู้ควบคุมข้อมูลส่วน<br>บุคคลไม่ต้องแจ้ง<br>เจ้าของข้อมูลส่วนบุคคล<br>ที่ไม่ได้รับผลกระทบ<br>เนื่องจากยังไม่เกิด<br>ปัญหา   | ในเบื้องต้นเป็นเพียงข้อผิดพลาด<br>ของโปรแกรมที่ทำให้เข้าถึง<br>ข้อมูลส่วนบุคคลไม่ได้ซึ่งจากการ<br>สอบสวนยังไม่ปรากฏว่ามี<br>ภัยคุกคามทางไซเบอร์แต่อย่าง<br>ใด อย่างไรก็ตามผู้ควบคุมข้อมูล<br>ส่วนบุคคลและผู้ประมวลผล<br>ข้อมูลส่วนบุคคลต้องตรวจสอบ<br>ข้อเท็จจริงเพิ่มเติม หากพบว่า<br>ระบบถูกโจมตีจากภัยคุกคาม<br>ทางไซเบอร์เว็บไซต์ผู้ให้บริการ<br>Web Hosting ต้องรีบแจ้งผู้<br>ควบคุมข้อมูลส่วนบุคคล และผู้<br>ควบคุมข้อมูลส่วนบุคคลต้องรีบ<br>แจ้งทั้งสำนักงานฯ และเจ้าของ<br>ข้อมูลส่วนบุคคลต่อไป |
| 8           | โรงพยาบาลแห่งหนึ่งถูกภัย<br>คุกคามทางไซเบอร์ โดยการ<br>โจมตีระบบจาก hacker ทำ<br>ให้ประวัติของผู้ป่วยไม่<br>สามารถเข้าถึงได้เป็นเวลา<br>30 ชั่วโมง  | ต้องแจ้ง เนื่องจากข้อมูล<br>ประวัติของผู้ป่วยเป็น<br>ข้อมูลส่วนบุคคลที่มี<br>ความอ่อนไหวและ<br>สามารถระบุตัวบุคคลได้  | ต้องแจ้ง เนื่องจากข้อมูล<br>ส่วนบุคคลที่มี<br>ความอ่อนไหวผู้ที่ไม่หวัง<br>ดีอาจนำไปใช้ในการ<br>กระทำความผิด<br>หรือมีผลกระทบต่อสิทธิ<br>และเสรีภาพของ<br>เจ้าของข้อมูลส่วนบุคคล<br>ได้ | เนื่องจากข้อมูลที่ถูกละเมิด<br>ดังกล่าวรวมถึงข้อมูลสุขภาพ<br>ด้วย เป็นข้อมูลส่วนบุคคลที่มี<br>ความอ่อนไหว จึงจำเป็นต้อง<br>แจ้งเหตุและตรวจสอบข้อมูล<br>เพิ่มเติม  |
| 9           | โรงเรียนแห่งหนึ่งเกิดความ<br>ผิดพลาดในการส่งข้อมูลของ<br>นักเรียนจำนวนมากทาง  | ต้องแจ้ง  | ต้องแจ้ง   | เนื่องจากการส่งข้อมูลดังกล่าว<br>ไม่มีการเข้ารหัส และเป็นข้อมูล<br>ส่วนบุคคลของบุคคลจำนวนมาก  |

| ตัวอย่างที่ | เหตุการณ์  | แจ้งเหตุแก่<br>สำนักงานคณะกรรมการ<br>คุ้มครองข้อมูล<br>ส่วนบุคคล (สคส.)  | แจ้งเหตุแก่<br>เจ้าของข้อมูล<br>ส่วนบุคคล  | เหตุผล   |
|-------------|--|--|--|--|
|             | อีเมลไปยังผู้รับเหมาในการ<br>ให้บริการขนส่งสินค้าของ<br>โรงเรียน ไม่ใช่ผู้ปกครอง<br>นักเรียน   |  |  | มาก ซึ่งอาจมีทั้งข้อมูลส่วน<br>บุคคลทั่วไป และข้อมูลส่วน<br>บุคคลที่มีความอ่อนไหว ซึ่ง<br>ผู้รับเหมาอาจจะนำข้อมูล<br>ดังกล่าวไปใช้โดยมิชอบและ<br>ก่อให้เกิดความเสียหายได้  |
| 10          | บริษัทแห่งหนึ่งทำการตลาด<br>แบบตรง โดยการส่งข้อมูล<br>ส่วนบุคคลไปยังผู้รับข้อมูล<br>แต่ละราย แต่ด้วยความ<br>ผิดพลาด จึงมีการใส่ที่อยู่<br>ของบุคคลที่รับอีเมลทั้ง 100<br>คน เข้าไปในช่อง To หรือ<br>Cc ทำให้ผู้รับอีเมลเห็น<br>อีเมลที่มีข้อมูลส่วนบุคคล<br>ของบุคคลอื่น | ต้องแจ้ง เนื่องจาก<br>เป็นการส่งข้อมูล<br>ของเจ้าของข้อมูล<br>ส่วนบุคคลจำนวน<br>มาก จึงจำเป็นต้อง<br>แจ้งเหตุ แต่หาก<br>ข้อมูลดังกล่าวมีการ<br>เข้ารหัสโดยเทคโนโลยี<br>ที่น่าเชื่อถือ อาจได้รับ<br>ยกเว้นไม่ต้องแจ้งเหตุ | ต้องแจ้ง เนื่องจากข้อมูล<br>ส่วนบุคคลใน<br>อีเมลดังกล่าวอาจ<br>ถูกนำไปใช้และ<br>ก่อให้เกิดความ<br>เสียหายต่อเจ้าของ<br>ข้อมูลส่วนบุคคล<br>ภายหลังได้ | การพิจารณาว่าจะต้องแจ้งเหตุ<br>แก่เจ้าของข้อมูลส่วนบุคคล<br>หรือไม่ อาจขึ้นอยู่กับปริมาณ<br>ของข้อมูลส่วนบุคคลที่ส่งออกไป<br>และลักษณะของข้อมูลด้วยหาก<br>มีการเข้ารหัสข้อมูลดังกล่าว<br>ทั้งหมด อาจถือว่ามีความเสี่ยง<br>ต่ำไม่จำเป็นต้องแจ้งเหตุ |

**หมายเหตุ** ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลทั้ง 10 ตัวอย่าง ดังกล่าวข้างต้น เป็นเพียง  
แนวทางในการประเมินความเสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริง  
ตามปัจจัยที่เกี่ยวข้องเป็นกรณี ๆ ไป

### (10) Infographic อื่นๆที่เกี่ยวข้อง

**UNIVERSITY DATA SECURITY GUIDELINES**

### ข้อควรปฏิบัติและข้อห้าม (Do's & Don'ts) ในการจัดการข้อมูลส่วนบุคคลของมหาวิทยาลัย

**UNIVERSITY DATA SECURITY GUIDELINES**

**✓ ข้อควรปฏิบัติ (DO'S)**

1. ใช้ระบบองค์กรเท่านั้นในการกักข้อมูล  
USE UNIVERSITY SYSTEMS ONLY FOR DATA
2. ตรวจสอบสิทธิ์ก่อนเปิดเผยข้อมูล  
VERIFY PERMISSIONS BEFORE DISCLOSING
3. เก็บข้อมูลอย่างปลอดภัย  
STORE DATA SECURELY
4. รายงานเหตุผิดปกติทันที  
REPORT INCIDENTS IMMEDIATELY

**✗ ข้อห้าม (DON'TS)**

1. ใช้ LINE / Facebook ส่วนตัวส่งข้อมูล  
DO NOT USE PERSONAL LINE / FACEBOOK
2. พุดถึงข้อมูลกับบุคคลภายนอก  
DO NOT DISCUSS CONFIDENTIAL INFO WITH OUTSIDERS
3. เก็บเอกสารสำคัญไว้นอกระบบ  
DO NOT STORE IMPORTANT DOCS OUTSIDE SYSTEM

**SECURITY IS EVERYONE'S RESPONSIBILITY** **MARCORN UNIVERSITY**

## 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)

1.2 แจ้งต่อลูกค้าเพื่อขอความยินยอม (COOKIE CONSENT BANNER)

1.3 แนบฟอร์มสมัครที่เข้าระบบและมีลิงก์นโยบาย (NECESSARY FORMS & POLICY LINK)

**2. มาตรการรักษาความปลอดภัยเชิงเทคนิค (TECHNICAL SECURITY MEASURES)**

2.1 ทำการเข้ารหัสข้อมูลและการส่งผ่านข้อมูล (DATA ENCRYPTION: IN STORAGE & TRANSIT)

2.2 จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตนข้อมูล (ACCESS CONTROL & 2FA/MFA)

2.3 ตรวจสอบช่องโหว่และอัปเดตระบบอย่างสม่ำเสมอ (VULNERABILITY SCAN & PATCHING)

**3. การจัดการข้อมูลและการสำรองข้อมูล (DATA MANAGEMENT & SECURE BACKUP)**

3.1 เห็น LOG การเข้าถึงและเปลี่ยนแปลงข้อมูล

3.2 วางระบบข้อมูลอัตโนมัติเพื่อลบกำหนด (AUTOMATED DATA DELETION)

3.3 สำรองข้อมูลอย่างปลอดภัยและมีการเข้ารหัส (ENCRYPTED BACKUP STORAGE)

**4. การเตรียมความพร้อมเมื่อเกิดเหตุละเมิด (DATA BREACH RESPONSE PREPARATION)**

4.1 ขั้นตอนปฏิบัติเมื่อตรวจพบการบุกรุก (INCIDENT RESPONSE PLAN: DETECT -> CONTAIN -> ERADICATE -> RECOVER)

4.2 ประสานงานกับ DPO และแจ้ง สอ. (COORDINATE WITH DPO & NOTIFY AUTHORITY)

72 HOURS

ประสานงานกับ DPO และแจ้ง สอ. (COORDINATE WITH DPO & NOTIFY AUTHORITY)

FOR UNIT INFORMATION SYSTEM & WEBSITE ADMINISTRATORS  
สำหรับผู้ดูแลระบบสารสนเทศและเว็บไซต์หน่วยงาน

## กระบวนการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (PERSONAL DATA BREACH MANAGEMENT PROCESS)

- 1. การตรวจจับและยืนยันเหตุละเมิด**

  - ตรวจสอบบันทึก: ประเมินความน่าเชื่อถือของข้อมูลที่ได้รับ
  - ตรวจสอบมาตรการรักษาความปลอดภัยเบื้องต้น
  - ตรวจสอบที่มาการแจ้งเตือนหรือ เทคโนโลยี และภาษาภาพ
- 2. การประเมินความเสี่ยงและผลกระทบ**

  - หากยืนยันว่าการละเมิดจริง ต้องประเมินว่า:
    - ผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลมากน้อยเพียงใด
    - พิจารณาปัจจัยต่างๆ เช่น ประเภทของการละเมิด ประเภทของข้อมูล ปริมาณข้อมูล และความร้ายแรงของผลกระทบ
- 3. การดำเนินการมาตรการเพื่อบรรเทาผลกระทบ**

  - ดำเนินการทันทีเพื่อ:
    - หยุดยั้งการละเมิด: ปิดช่องโหว่ระบบ เปลี่ยนรหัสผ่าน หรือระงับการเข้าถึงชั่วคราว
    - บรรเทาผลกระทบ: ลดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูล
- 4. การแจ้งเหตุละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**

  - รายงานต่อ สอ. ภายใน 72 ชั่วโมง: เป็นรายงานเหตุละเมิด รายละเอียดข้อมูลละเมิด: ลักษณะของการละเมิด ข้อมูลที่กระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
- 5. การแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคล**

  - แจ้งโดยไม่มีค่าใช้จ่าย: หากมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
  - ข้อมูลที่ต้องแจ้ง: ลักษณะของการละเมิด ผลกระทบที่อาจเกิดขึ้น แนวทางเยียวยา และมาตรการที่ดำเนินการ
- 6. การดำเนินการมาตรการเยียวยา**

  - ชดเชยความเสียหาย: ทั้งทางการเงินและการให้บริการที่เกี่ยวข้องผลกระทบ
  - ให้ความปรึกษา: ช่วยเหลือเจ้าของข้อมูลในการจัดการกับผลกระทบที่เกิดขึ้น
  - แก้ไขข้อบกพร่อง: ดำเนินการแก้ไขหรือลบข้อมูลที่ถูกละเมิด
- 7. การปรับปรุงมาตรการรักษาความมั่นคงปลอดภัย**

  - ทบทวนและปรับปรุง: มาตรการป้องกันเพื่อป้องกันกรณีเกิดเหตุซ้ำในอนาคต

## แนวปฏิบัติที่ดีที่สุดสำหรับการจัดการเหตุการณ์ด้านความปลอดภัยทางไซเบอร์

เพื่อสร้างความพร้อมและลดผลกระทบต่อองค์กร

- 1. ทำให้แผนรับมือเหตุการณ์ฉุกเฉิน (IRP) เป็นเอกสารที่มีการพัฒนาอย่างต่อเนื่อง**

  - ทบทวนและปรับปรุงอย่างสม่ำเสมอ (อย่างน้อยปีละครั้ง)
  - หลีกเลี่ยงการเปลี่ยนแปลงที่สำคัญ
  - อิงจากทฤษฎีการเรียนรู้และการฝึกซ้อมและเหตุการณ์จริง
- 2. สื่อสารอย่างชัดเจน**

  - ทักท้วงที่ละชัดเจน
  - สื่อสารทั้งภายในและภายนอก (ผู้ได้รับผลกระทบ, หน่วยงาน, สาธารณชน)
  - กำหนดช่องทางและระเบียบปฏิบัติที่ชัดเจน
- 3. ใช้ระบบอัตโนมัติในส่วนที่ทำได้**

  - งานตรวจจับและการควบคุมที่ซ้ำซาก
  - เร่งความเร็วในการตอบสนอง
  - ใช้คู่มือและเครื่องมือการทำงานอัตโนมัติ (เช่น SOAR)
- 4. การมีส่วนร่วมของที่ปรึกษาด้านกฎหมาย**

  - ปรึกษาตั้งแต่เนิ่นๆ ในการวางแผนและระงับเหตุการณ์
  - โดยเฉพาะเหตุการณ์รั่วไหลของข้อมูล
  - ดูแลเรื่องการควบคุม, การแจ้งเตือน, และการจัดการหลักฐาน
- 5. รักษาหลักฐาน**

  - รักษาความสมบูรณ์ของหลักฐาน
  - เพื่อวิเคราะห์สาเหตุและทางกฎหมาย
  - ฝึกอบรบกับบุคลากรที่เกี่ยวข้อง

Chain of Custody

## เทคนิคการจัดการ LOG FILES ให้สอดคล้องกับ PDPA

รักษาสอดคล้องระหว่าง “เก็บหลักฐาน” และ “คุ้มครองความเป็นส่วนตัว”

|  |   |   |   |  |
|--|---|---|---|--|
| <p style="text-align: center; background-color: #003366; color: white; padding: 2px;"><b>DATA MINIMIZATION</b><br/>(เก็บเท่าที่จำเป็น)</p> <div style="text-align: center;"> </div> <ul style="list-style-type: none"> <li>✓ ตัดข้อมูลที่ไม่เกี่ยวข้อง (CUT IRRELEVANT DATA)</li> <li>✓ เลิกเก็บเฉพาะ METADATA ใคร ทำอะไร เมื่อไหร่ ที่ไหน (WHO, WHAT, WHEN, WHERE)</li> </ul> | <p style="text-align: center; background-color: #003366; color: white; padding: 2px;"><b>PSEUDONYMIZATION</b><br/>(การใช้นามแฝง)</p> <div style="text-align: center;"> </div> <ul style="list-style-type: none"> <li>✓ ใช้ ID แทนชื่อ (USE ID INSTEAD OF NAME)</li> <li>✓ HASHING IP ADDRESS</li> </ul> | <p style="text-align: center; background-color: #003366; color: white; padding: 2px;"><b>DATA MASKING</b><br/>(การปกปิดข้อมูล)</p> <div style="text-align: center;"> </div> <p style="text-align: center;">081-XXX-XXXX<br/>user_***@email.com</p> <ul style="list-style-type: none"> <li>✓ ซ่อนข้อมูลอ่อนไหว (SENSOR SENSITIVE DATA)</li> <li>✓ กรองรูปแบบ Credit Card ออ</li> </ul> | <p style="text-align: center; background-color: #003366; color: white; padding: 2px;"><b>ACCESS CONTROL</b><br/>(การจำกัดสิทธิ์)</p> <div style="text-align: center;"> </div> <p style="text-align: center;">Principle of Least Privilege</p> <ul style="list-style-type: none"> <li>✓ ให้สิทธิ์เฉพาะผู้จำเป็น (ONLY ESSENTIAL STAFF)</li> <li>✓ แยกคนมีสิทธิ์ดู Log กับแก้ไขระบบ (SEPARATE VIEWER &amp; SYSTEM ADMIN ROLES)</li> </ul> | <p style="text-align: center; background-color: #003366; color: white; padding: 2px;"><b>RETENTION POLICY</b><br/>(กำหนดอายุการเก็บ)</p> <div style="text-align: center;"> </div> <p style="text-align: center;">Auto-90 days</p> <ul style="list-style-type: none"> <li>✓ ตั้งระบบ Log ที่เก็บ (AUTO-DELETION)</li> <li>✓ Log การลบต้องเข้ารหัส (ENCRYPTION AT REST)</li> </ul> |
|--|---|---|---|--|

จุดที่มักพลาด

(COMMON PITFALLS)

GUG FILE LOGS

และ 'คุ้มครองความเป็นส่วนตัว'

DEBUG MODE

บันทึกข้อมูลทุกอย่าง

ERROR LOGS

เฉพาะข้อมูลลูกค้าอ่อนไหว

## 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 เพื่อยกระดับความมั่นคงปลอดภัยการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล

1. มาตรการด้านการบริหารจัดการ (Administrative Measures)

การขนานนกรักษาความลับ (Confidentiality)

ผู้ปฏิบัติงานที่รับผิดชอบการประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามสัญญาการรักษาข้อมูล (Non-Disclosure Agreement: NDA) หรือข้อตกลงการรักษาข้อมูลที่ไม่ได้ระบุชื่อ (Contractual Data Protection Agreement)

การกำหนดหน้าที่และสิทธิ์เข้าถึง (Role-based Access)

พนักงานมีข้อมูลความลับที่ตนเองเข้าถึงได้โดยต้องขออนุญาตจากผู้ดูแลระบบสารสนเทศระดับสูง (CIO) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

การตรวจสอบสถานะความเสี่ยง (Risk Review/KM)

มีการประเมินความเสี่ยงด้านความปลอดภัยสารสนเทศ (ISM) และวิเคราะห์ความเสี่ยงที่อาจส่งผลกระทบต่อชื่อเสียงของมหาวิทยาลัยอย่างสม่ำเสมอ

2. มาตรการเชิงเทคนิคและระบบสารสนเทศ (Technical Measures)

การแจ้งเตือนประสงค์และขอความยินยอม

การเผยแพร่เนื้อหาที่ผิดกฎหมายบนเว็บไซต์และโซเชียลมีเดียของมหาวิทยาลัย (Social Media) รวมถึงการขอความยินยอม (Consent) ก่อนมีการนำข้อมูลไปใช้

ความปลอดภัยของสื่อสังคมออนไลน์

สำหรับเพจ Facebook Page และเพจหน่วยงาน ต้องปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัว (Privacy Notice) รวมถึงการปิดกั้นการเข้าถึงข้อมูล (Restrict Audience) หรือการปิดกั้นการเข้าถึงข้อมูล (Restrict Audience)

การยึดถือเทคโนโลยีป้องกัน (Preventive Tech)

สิ่งอำนวยความสะดวกในการรักษาความปลอดภัย (เช่น การเข้ารหัส หรือ การกรองข้อมูล) สำหรับโซเชียลมีเดีย เพื่อลดความเสี่ยงจากการถูกแฮก การโจมตีด้วยไวรัส หรือการละเมิดข้อมูลส่วนบุคคล

3. มาตรการด้านบุคลากรและการสร้างวัฒนธรรม (Human Measures)

การเข้ารับการอบรม

ผู้ปฏิบัติงาน (รวมถึงบุคลากรบริหาร) ต้องเข้ารับการอบรมด้านข้อมูลส่วนบุคคล (ข้อมูลส่วนบุคคล: "Sensitive Data") ตามระดับความสำคัญที่กำหนด

โดยมีเป้าหมายให้ทราบร้อยละ 60 ของบุคลากรทั้งหมด

การแลกเปลี่ยนเรียนรู้ (KM)

มีการจัดสรรแหล่งเรียนรู้และการดำเนินการแก้ไขข้อผิดพลาด (Case Study) เพื่อป้องกันเหตุการณ์ซ้ำกันที่สอดคล้องกับ PDPA

4. มาตรการการตอบสนองต่อเหตุการณ์ (Incident Response)

ช่องทางการร้องเรียน

ผู้ปฏิบัติงานสามารถแจ้งเหตุการณ์ที่กระทบต่อความปลอดภัยของข้อมูลส่วนบุคคล (Data Breach) หรือการละเมิดข้อมูลส่วนบุคคล (Data Breach) ได้ผ่านช่องทางที่ระบุไว้ในนโยบายความเป็นส่วนตัว

แนวปฏิบัติเมื่อเกิดเหตุ

หากพบเหตุละเมิด ต้องดำเนินการตามแนวปฏิบัติที่ระบุไว้ในนโยบายความเป็นส่วนตัว และดำเนินการแก้ไขสถานการณ์โดยเร็วที่สุด

#### 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

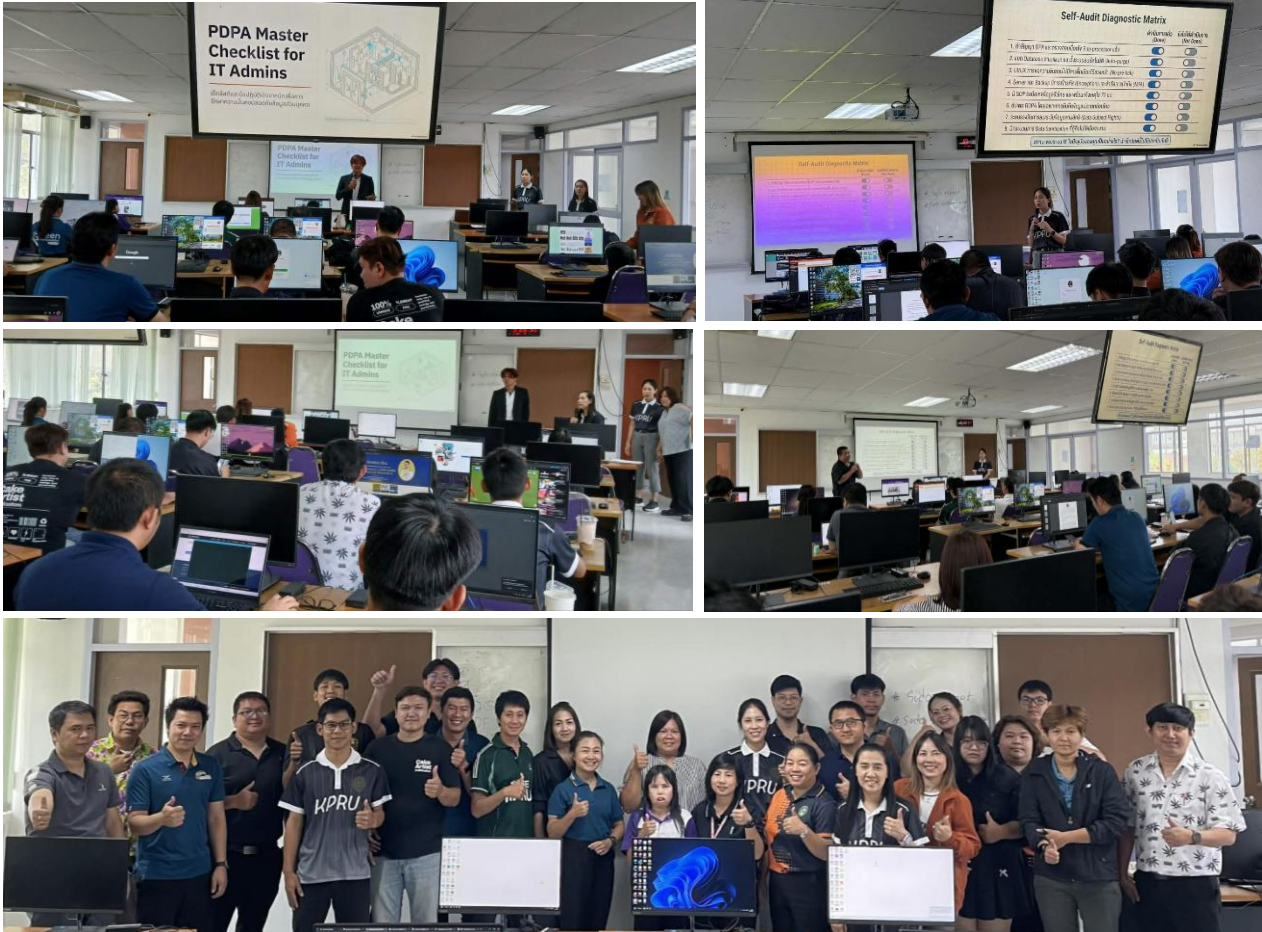


(3) กิจกรรมแลกเปลี่ยนเรียนรู้กลุ่มแอดมิน ร่วมกับ DPO และผู้ประมวลผลข้อมูลสำนักฯ วันที่ 27 กุมภาพันธ์ 2569 เวลา 09.00 น. ณ ห้องประชุมดอกสัก เพื่อแนะนำเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย และวางแผนจัดอบรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล 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 “ชุมชนความรู้” ออกมาบันทึกไว้ เพื่อสร้างชุมชนการเรียนรู้ (Learning Community) โดย สร้างกลุ่มสำหรับแลกเปลี่ยนเรียนรู้ทางโซเชียลมีเดีย ได้แก่ คลินิกกฎหมาย HLC

**6. จัดบันทึก “ชุมชนความรู้” 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 จัดบันทึก “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) แล้วจัดเก็บเป็นคลังความรู้ออนไลน์เผยแพร่ใน เว็บไซต์ให้ผู้เข้าถึงได้ง่าย นำไปใช้ประโยชน์ได้จริง สร้างสังคมเวทีแห่งการเรียนรู้ให้บุคลากร มีโอกาสพูดคุย แลกเปลี่ยน ความรู้ซึ่งกันและกัน

## 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 | วิธีการสู่ความสำเร็จที่คาดหวัง   | กิจกรรมการจัดการความรู้   | ระยะเวลา                         | ตัวชี้วัดและค่าเป้าหมาย   | กลุ่มเป้าหมาย  | ผู้รับผิดชอบ                            |
|-------|--|---|----------------------------------|---|--|---|
| 1     | การกำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร | <b>กิจกรรมที่ 1</b> จัดตั้งคณะทำงาน<br>1.1 จัดตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ<br>1.2 จัดตั้งคณะกรรมการดำเนินงาน และกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร | 31 ต.ค. 2568<br><br>12 พ.ย. 2568 | 1. คำสั่ง แต่งตั้งคณะกรรมการจัดการความรู้ จำนวน 1 ฉบับ<br>2. คำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล จำนวน 1 ฉบับ | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ<br>- บุคลากรของสำนักฯ<br>- ตัวแทนหน่วยงานที่เกี่ยวข้องกับการกำกับและการใช้ข้อมูลส่วนบุคคลภายในมหาวิทยาลัยฯ | คณะกรรมการจัดการความรู้ สำนักฯ          |
|       |  | <b>กิจกรรมที่ 2</b> ประชุมคณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล             | 5 พ.ย. 2568                      | 1. แผนการจัดการความรู้ จำนวน 1 เรื่อง<br>2. รายการความเสี่ยงที่เกี่ยวข้อง จำนวน 5 ประเด็น   | คณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ  | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ |



| ลำดับ | วิธีการสู่ความสำเร็จที่คาดหวัง   | กิจกรรมการจัดการความรู้  | ระยะเวลา          | ตัวชี้วัดและค่าเป้าหมาย   | กลุ่มเป้าหมาย                  | ผู้รับผิดชอบ                            |
|-------|--|--|-------------------|---|--------------------------------|---|
| 2     | การเสาะหาความรู้ที่ต้องการ   | <b>กิจกรรมที่ 3</b> รวบรวมและศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA, และตัวอย่าง Best Practice การลดความเสี่ยงจากมหาวิทยาลัยหรือหน่วยงานที่ประสบความสำเร็จ เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล  | พ.ย. 2568         | เอกสารที่เกี่ยวข้อง จำนวน 5 เรื่อง  | คณะกรรมการ KM, คณะกรรมการ PDPA | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ |
| 3     | การปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะสมต่อการใช้งานของตน | <b>กิจกรรมที่ 4</b> 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                                  | <b>กิจกรรมที่ 5</b> แลกเปลี่ยนเรียนรู้<br>(1) นำเครื่องมือ/แนวทางปฏิบัติจาก กิจกรรมที่ 4 ไปทดลองใช้ในหน่วยงาน/กลุ่มงานที่เกี่ยวข้องกับ 3 อันดับความเสี่ยงที่วิเคราะห์ไว้ พร้อมทั้งจัดอบรมสร้างความเข้าใจในการนำไปใช้<br>(2) จัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล สำหรับผู้ที่มีหน้าที่และความรับผิดชอบตาม | ก.พ. - มี.ค. 2569 | - ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคล (เป้าหมาย ร้อยละ 60)<br>- ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ระดับดี)<br>- ระดับความสำเร็จในการดำเนินการจัดการความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคล (เป้าหมาย 5 คะแนน)<br>- จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ ถูกนำไปเผยแพร่ โดยไม่ได้รับอนุญาต (เป้าหมาย 0 ครั้ง) | บุคลากรมหาวิทยาลัยฯ            | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ |



| ลำดับ | วิธีการสู่ความสำเร็จที่คาดหวัง   | กิจกรรมการจัดการความรู้   | ระยะเวลา          | ตัวชี้วัดและค่าเป้าหมาย  | กลุ่มเป้าหมาย   | ผู้รับผิดชอบ                            |
|-------|--|---|-------------------|--|-----------------|---|
|       |  | พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)  |                   |  |                 |   |
| 5     | การนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด “ขุมความรู้” ออกมาบันทึกไว้  | <b>กิจกรรมที่ 6</b> 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” สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น | <b>กิจกรรมที่ 7</b> นำบทเรียนที่สกัดได้จากกิจกรรมที่ 6 มา ปรับปรุงและจัดทำเป็น “ชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล” ฉบับร่าง สรุปลงเป็น ฉบับสมบูรณ์ เพื่อใช้ในการปฏิบัติงานที่เป็นทางการ | พ.ค. 2569         | - ชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล จำนวน 1 ชิ้น | คณะกรรมการ PDPA | - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ |

ลงชื่อ.....

(นางสาวอรปรียา คำแพง)  
ผู้รับผิดชอบงานการจัดการความรู้  
26 พฤศจิกายน 2568

ลงชื่อ.....

(ผู้ช่วยศาสตราจารย์พรหมเมศ วีระพันธ์)  
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ  
26 พฤศจิกายน 2568



## วงจรการเรียนรู้ (Learning Cycle)

| วงจรการเรียนรู้                                   | การประยุกต์ใช้   |
|---|--|
| 1. การมีองค์ความรู้                               | <ol style="list-style-type: none"><li>1. ทบทวนแผน วิเคราะห์ความเสี่ยง และศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA และ Best Practice เพื่อเป็นฐานความรู้ตั้งต้น</li><li>2. สร้างและจัดระบบ นำความรู้ที่ซับซ้อนมาย่อและแปลงให้เป็นเครื่องมือ/แนวทางปฏิบัติที่ใช้งานง่าย โดยเน้นแก้ปัญหาความเสี่ยง</li><li>3. อันดับแรก เช่น คู่มือจัดเก็บ/ทำลายเอกสาร, Checklist, Infographic เป็นการสร้างองค์ความรู้ที่เป็นรูปธรรม พร้อมใช้งาน</li></ol>  |
| 2. วิธีการส่งเสริมการเผยแพร่องค์ความรู้           | <ol style="list-style-type: none"><li>1. จัดอบรม/กิจกรรม เพื่อสร้างความตระหนักรู้และให้ความรู้ PDPA ในวงกว้าง</li><li>2. นำเครื่องมือ/แนวทางปฏิบัติที่สร้างขึ้น ไปทดลองใช้จริงในหน่วยงานที่มีความเสี่ยงสูง พร้อมจัดอบรมเพื่อสร้างความเข้าใจในการนำไปใช้</li><li>3. จัดตั้งชุมชนนักปฏิบัติ (CoP) เพื่อเป็นเวทีให้ผู้ใช้งานจริงมาแลกเปลี่ยนประสบการณ์ ปัญหา และแนวทางแก้ไขร่วมกันในกลุ่ม ถือเป็น การเผยแพร่และถ่ายทอดความรู้แบบมีปฏิสัมพันธ์ (Interactional Sharing)</li></ol>                     |
| 3. ผลการนำองค์ความรู้ไปใช้                        | <ol style="list-style-type: none"><li>1. ติดตามผลการใช้เครื่องมือ/แนวทางปฏิบัติ และผลการทดลองใช้จากผู้ปฏิบัติงานว่ามีความเข้าใจในการใช้งานมากน้อยเพียงใด</li><li>2. บทเรียนและข้อเสนอแนะที่สกัดได้จากเวที CoP สะท้อนให้เห็นว่าความรู้ที่ถ่ายทอดไป (เครื่องมือ/แนวทาง) สามารถลดความเสี่ยง</li><li>3. อันดับแรก ได้ตามที่คาดหวังหรือไม่</li><li>3. ข้อมูลจากการแลกเปลี่ยนเรียนรู้ใน CoP ถือเป็นผลลัพธ์ที่ใช้ในการปรับปรุงต่อไป</li></ol>   |
| 4. ติดตามปัญหาและอุปสรรคจากการนำองค์ความรู้ไปใช้  | <ol style="list-style-type: none"><li>1. ใช้การจัดตั้งชุมชนนักปฏิบัติ (CoP) เป็นกลไกในการติดตามปัญหาและอุปสรรคในการปฏิบัติงานจริง เช่น เครื่องมือใช้ยาก, ข้อกำหนดไม่ชัดเจน, การต่อต้านการเปลี่ยนแปลง</li></ol>   |
| 5. การนำความรู้มาปรับเป็นแนวปฏิบัติในการดำเนินงาน | <ol style="list-style-type: none"><li>1. นำบทเรียน ปัญหา และอุปสรรคที่สกัดได้จาก CoP มาใช้ในการปรับปรุงแก้ไของค์ความรู้เดิม</li><li>2. จัดทำเป็นชุดความรู้/คู่มือหรือแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคลฉบับสมบูรณ์ ซึ่งผ่านการทดลองใช้และปรับปรุงแล้ว</li><li>3. ประกาศใช้ชุดความรู้ฉบับสมบูรณ์ เป็นแนวปฏิบัติ ที่เป็นทางการ (Official Guideline) ของสำนักฯ/มหาวิทยาลัย เพื่อใช้เป็นมาตรฐานในการปฏิบัติงานจริง ถือเป็น การบรรจุความรู้เข้าสู่ระบบการดำเนินงานอย่างเป็นทางการ</li></ol> |