

รายงานผลการดำเนินการจัดการความรู้ ประจำปีการศึกษา 2568  
ด้านการวิจัย/ด้านการเรียนการสอน/ด้านพันธกิจอื่น

เรื่อง แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ  
มหาวิทยาลัยราชภัฏกำแพงเพชร

## 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> 1.1 จัดตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ 1.2 จัดตั้งคณะกรรมการดำเนินงาน และกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร	31 ต.ค. 2568  12 พ.ย. 2568	1. คำสั่ง แต่งตั้งคณะกรรมการจัดการความรู้ จำนวน 1 ฉบับ 2. คำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล จำนวน 1 ฉบับ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ - บุคลากรของสำนักฯ - ตัวแทนหน่วยงานที่เกี่ยวข้องกับการกำกับและการใช้ข้อมูลส่วนบุคคล ภายในมหาวิทยาลัย	- คณะกรรมการจัดการความรู้ สำนักฯ
		<b>กิจกรรมที่ 2 ประชุมคณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล</b>	5 พ.ย. 2568	1. แผนการจัดการความรู้ จำนวน 1 เรื่อง 2. รายการความเสี่ยงที่เกี่ยวข้อง จำนวน 5 ประเด็น	คณะกรรมการจัดการความรู้และคณะกรรมการความเสี่ยงสำนักฯ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
2	การเสาะหาความรู้ที่ต้องการ	<b>กิจกรรมที่ 3 รวบรวมและศึกษา</b> 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 - 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> (1) นำเครื่องมือ/แนวทางปฏิบัติ จาก 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	<b>กิจกรรมที่ 6 จัดตั้งชุมชนนักปฏิบัติ (CoP) ในกลุ่มผู้ใช้งาน</b> กิจกรรมที่ 5 และจุดที่ต้องปรับปรุง ในการนำแนวทางไปปฏิบัติจริง และสกัดบทเรียนที่ได้ออกมา	เม.ย. - พ.ค. 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) สรุปลงให้เป็นฉบับสมบูรณ์ 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 อันดับความเสี่ยงที่มีโอกาสทำให้อิทธิพลร้ายแรง 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

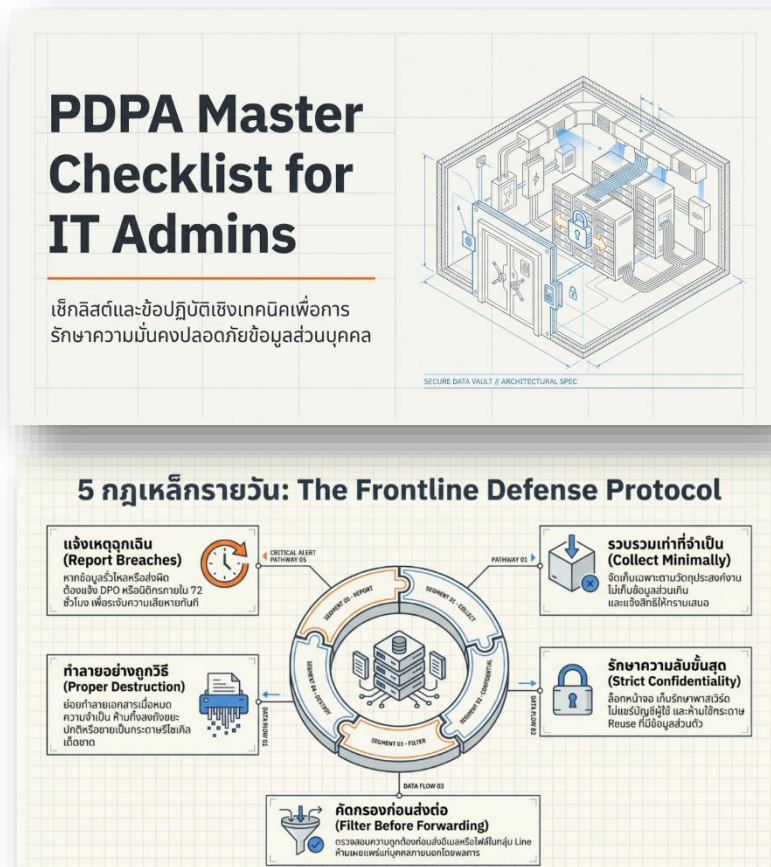
**กิจกรรมที่ 3** รวบรวมความรู้จากแหล่งต่าง ๆ ทั้งภายในและภายนอก คณะทำงานได้รวบรวมและศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA และตัวอย่าง Best Practice การลดความเสี่ยงและป้องกันการละเมิดข้อมูลส่วนบุคคลจากหน่วยงานที่ประสบความสำเร็จ ได้แก่ คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการณ์ละเมิดข้อมูล ของ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

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

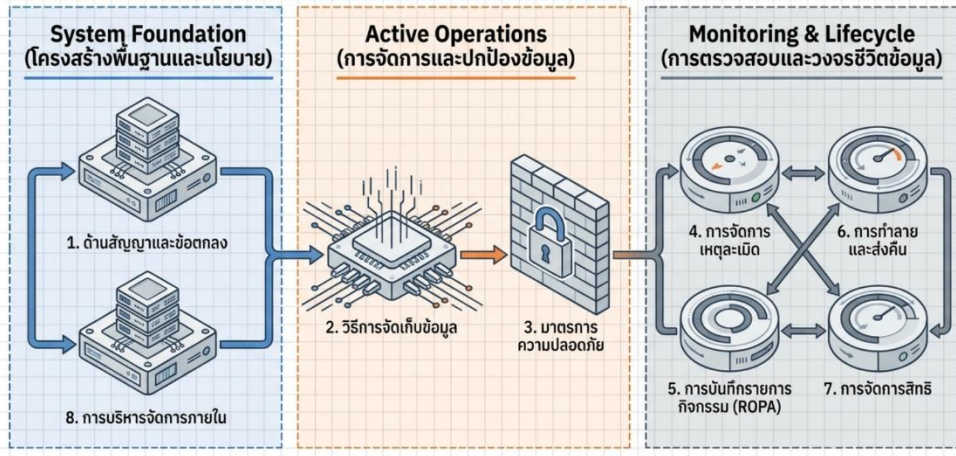
**3. ปรับปรุง ดัดแปลง หรือสร้างความรู้อย่างบางส่วนให้เหมาะต่อการใช้งานของตน** โดยการนำความรู้ที่ได้มาปรับให้เหมาะสมกับบริบทของมหาวิทยาลัย

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

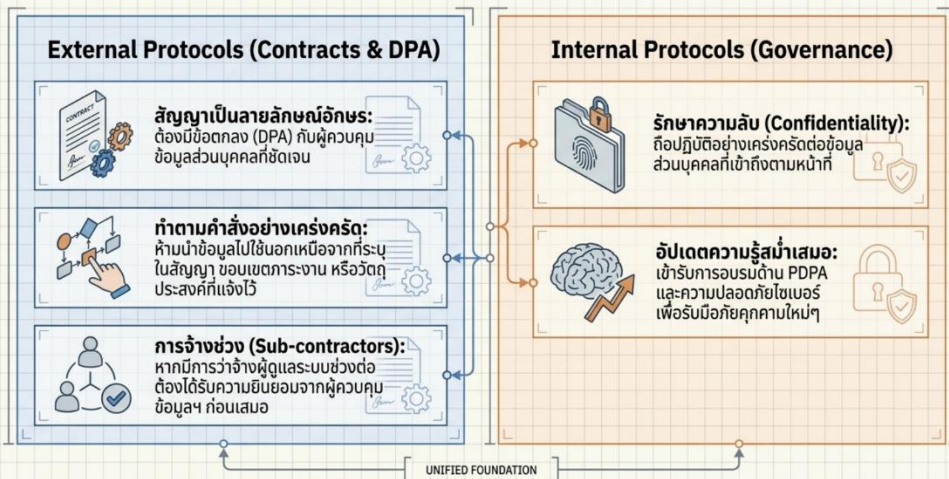
(1) PDPA Master Checklist for IT Admins เช็กลิสต์และข้อปฏิบัติเชิงเทคนิคเพื่อการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล



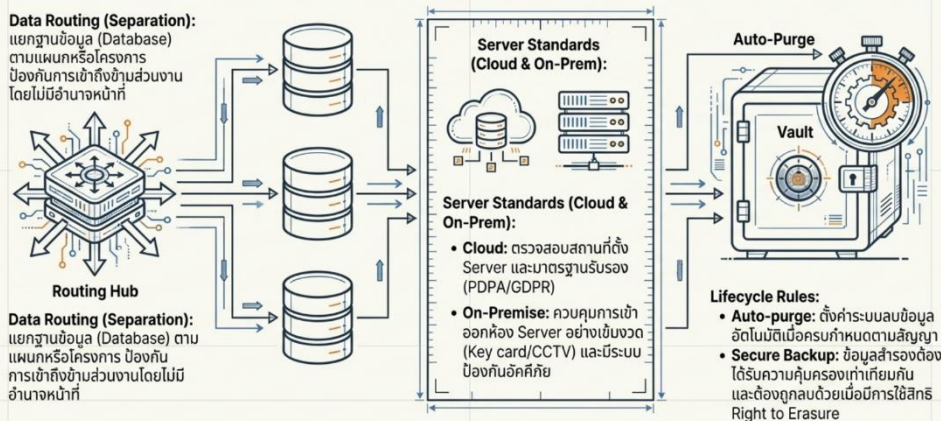
## The 8-Pillar Implementation Blueprint



## Foundation & Governance: ขอบเขตอำนาจหน้าที่

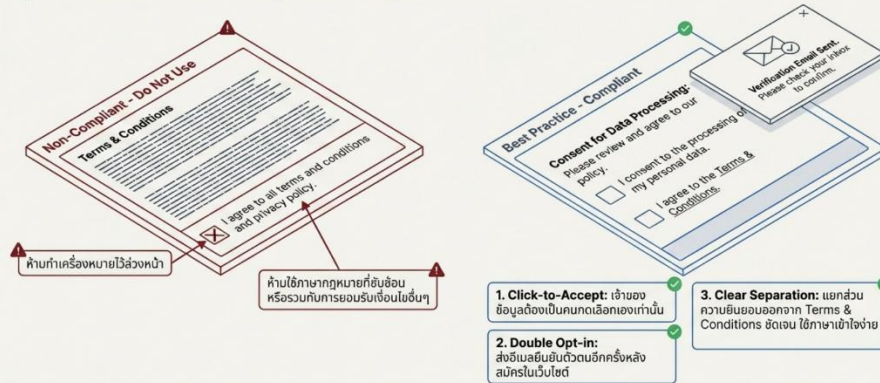


## Storage Architecture & Data Segregation

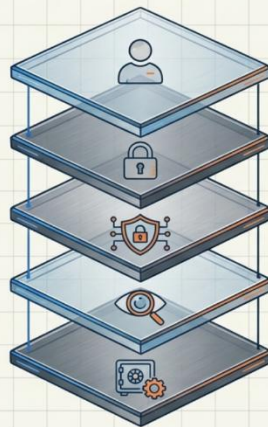


## Legal Consent Mechanisms in UI/UX

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

<h3>Quadrant 1: Digital Footprints (ร่องรอยดิจิทัล)</h3> <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>	<h3>Quadrant 2: Identity &amp; Profile (ข้อมูลระบุตัวตนบุคคล)</h3> <ul style="list-style-type: none"> <li>ข้อมูลรายละเอียดส่วนบุคคล และการระบุ/ยืนยันตัวตน.</li> <li>ข้อมูลการติดต่อ, การทำงาน, การศึกษา.</li> </ul>
<h3>Quadrant 3: Behavioral &amp; Commercial (พฤติกรรมและการทำธุรกรรม)</h3> <ul style="list-style-type: none"> <li>ข้อมูลการเงิน และ การรับบริการ.</li> <li>ข้อมูลธุรกรรมมีประกกันภัย.</li> <li>ข้อมูลวิจยตลาด และ ข้อมูลการสื่อสาร (บันทึกสนทนา).</li> </ul>	<h3>Quadrant 4: Highly Sensitive (ข้อมูลอ่อนไหว - ควบคุมพิเศษ)</h3> <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** เมื่อตกเป็นเหยื่อถูกแอบอ้างรูปภาพบน **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**  
 เดินทางไปยังสถานีตำรวจท้องที่เพื่อแจ้งความขอใบแจ้งความ หรือใบร้องทุกข์เพื่อใช้เป็นหลักฐานทางกฎหมาย
- 3. รายงาน FACEBOOK (Report)**  
 ติตรายงาน 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) เพื่อป้องกันมีจฉายื่นเข้าถึงรูปภาพได้ง่าย

ปกป้องตนเอง ดำเนินคดีให้ถึงที่สุด!  
 สายด่วนอาชญากรรมทางเทคโนโลยี: 1441

#เตือนภัย #มีจฉายื่น #แอบอ้างรูปภาพ #ความปลอดภัยโซเชียล #1441 #ตำรวจไซเบอร์ อนุมัติ

มหาวิทยาลัยราชภัฏกำแพงเพชร  
KAMPHAENG PHET RAJABHAT UNIVERSITY

รับสมัครนักศึกษาใหม่ 2569  
 เปิดรับสมัครสอบเข้า วิชาการศึกษา

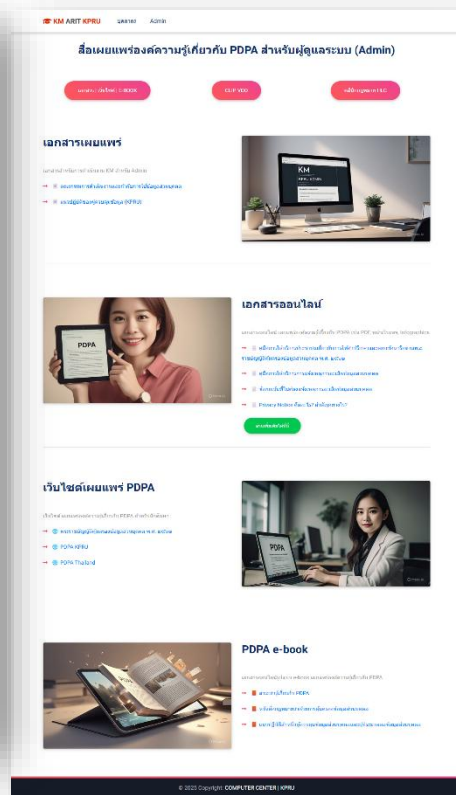
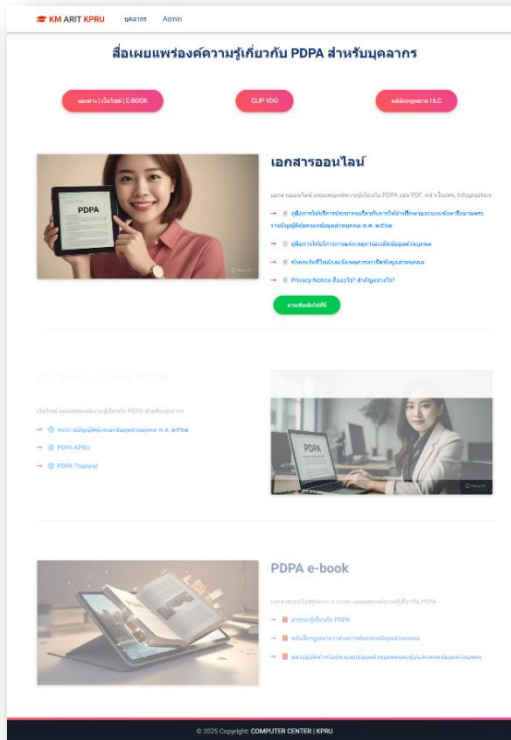
**แจ้งเตือนภัย! ถูกแอบอ้างรูปภาพบน Facebook ติดต่อและกล่าวหาหลอกลวง**

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

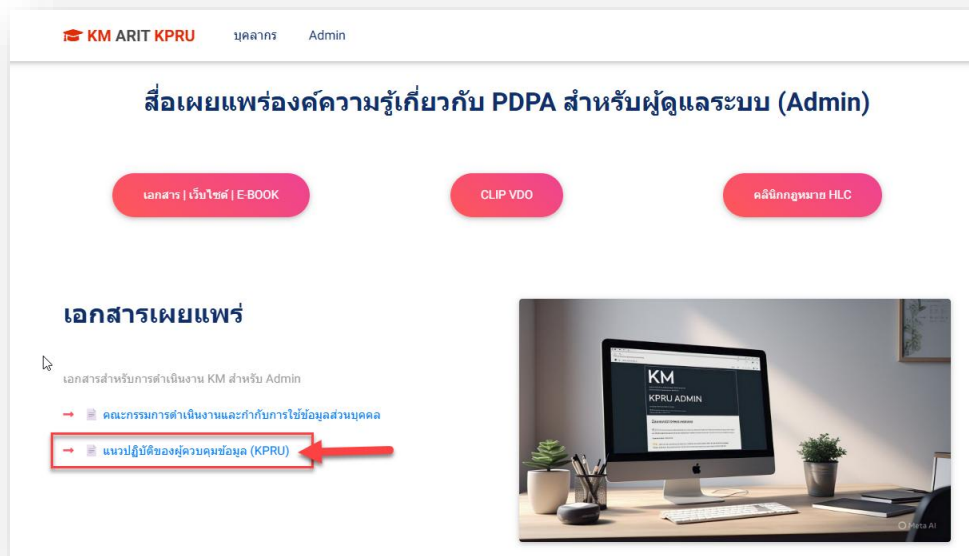
**ปกป้องตนเอง ดำเนินคดีให้ถึงที่สุด!** 1441

ข่าวกิจกรรม

(4) เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผ่านสื่อส่งเสริมการเรียนรู้ PDPA แยกตามประเภทผู้ใช้



สำหรับกลุ่ม Admin เผยแพร่แนวปฏิบัติของผู้ควบคุมข้อมูล (KPRU)



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

**มาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (ดำเนินการตามมาตรการเชิงเทคนิค) Facebook Page**

- 1. ควบคุมการโพสต์และแสดงความคิดเห็น (Content Moderation)**
  - ดำเนินการปิดการอนุญาตให้บุคคลนอกโพสต์บนหน้าเพจ (Disable Visitor Posts)
  - ตั้งค่าการกรองความคิดเห็น (Comment Ranking/Filtering)
  - ใช้เครื่องมือ Moderation Assist ใน Facebook เพื่อซ่อนความคิดเห็นที่ไม่สุภาพหรือเกี่ยวข้องกับการบิดเบือนข้อมูลอัตโนมัติ
- 2. การจัดการสิทธิ์และการเข้าถึง (Identity and Access Management)**
  - ตรวจสอบและจำกัดจำนวนผู้ดูแลเพจ (Page Roles) ให้เฉพาะบุคคลที่จำเป็น, และบังคับใช้การยืนยันตัวตนแบบสองชั้น (Two-Factor Authentication: 2FA) สำหรับบัญชีผู้ดูแลเพจ เพื่อป้องกันการถูกแฮกหรือเข้าถึงโดยไม่ได้รับอนุญาต
- 3. การรายงานและระงับเนื้อหา (Reporting & Takedown)**
  - ใช้เครื่องมือการรายงาน (Report) ของ Meta เพื่อแจ้งการแอบอ้างบุคคล (Impersonation) และการละเมิดมาตรฐานชุมชน (Community Standards) เพื่อให้ทาง Facebook ดำเนินการลบบัญชีผู้กระทำผิดและเนื้อหาที่เกี่ยวข้อง
- 4. การบันทึกและเก็บรวบรวมหลักฐานทางดิจิทัล (Digital Evidence Preservation)**
  - ใช้ฟังก์ชันบันทึกกิจกรรม (Activity Log) และการถ่ายภาพหน้าจอ (Screen Capture) ที่ระบุ URL และวันที่เกิดเหตุอย่างชัดเจน เพื่อนำไปใช้เป็นหลักฐานในการดำเนินคดีตามกฎหมาย
- 5. การตรวจสอบความปลอดภัยของระบบ (Security Monitoring)**
  - หมั่นตรวจสอบการเข้าถึงบัญชีผ่านเซสชันที่ใช้งานอยู่ (Active Sessions) ในการตั้งค่าความปลอดภัยของ Facebook เพื่อตรวจสอบว่ามีการเข้าถึงโดยไม่ปกติหรือไม่

WWW.KPRU.AC.TH  
KAMPHAENG PHET RAJABHAT UNIVERSITY

**Ao Kpru**  
ผู้ดูแล · 15 มีนาคม

ประกาศ!!  
ได้รับมอบหมายจาก ผู้อำนวยการสำนักบริหารการและเทคโนโลยีสารสนเทศ มร.ภ.พ. ให้ประสานหน่วยงานดังนี้:

เพื่อเป็นแนวทางป้องกันการกลั่นแกล้งหรือการใช้เครื่องมือที่ผิดเพี้ยนจากบุคคลภายนอก ระยะเวลาที่แจ้งขอเรียนแจ้ง Admin เพจ facebook ทุกหน่วย ดำเนินการตั้งค่าให้เฉพาะ Admin (ผู้ดูแล) เท่านั้นที่สามารถโพสต์หรือแสดงความคิดเห็นได้

- การจำกัดสิทธิ์การโพสต์ (Visitor Posts)
- การควบคุมการแสดงความคิดเห็น (Comments)

เนื่องจากมีโปรแกรมที่สามารถโพสต์ในเพจของหน่วยงาน และอาจกระทบภาพลักษณ์องค์กรในอนาคตได้ ระยะเวลาที่แจ้งขอความร่วมมือทุกหน่วยงานดำเนินการตามแจ้งกล่าว ขอมุขคณะ:

1. การจำกัดสิทธิ์การโพสต์ (VISITOR POSTS)  
ตามปกติ Facebook จะยอมให้ใครโพสต์ลงหน้าเพจได้ (ซึ่งจะไปปรากฏในแถบ "Community") คุณควรปิดส่วนนี้เพื่อไม่ให้คนอื่นมาส่งกระทู้บนหน้าเพจของคุณ
  - ไปที่ Settings (การตั้งค่า) > Privacy (ความเป็นส่วนตัว) > Page and Tagging (เพจและการแท็ก)
  - ในหัวข้อ "Who can post on your Page?" ให้เลือกเป็น "Only Me" (ซึ่งในบริบทเพจหมายถึงเฉพาะ Admin/Editor เท่านั้น)
2. การควบคุมการแสดงความคิดเห็น (COMMENTS)  
หากหน่วยงานต้องการจัดการคอมเมนต์ในโพสต์ใดโพสต์หนึ่ง หรือจำกัดสิทธิ์ สามารถทำได้หลายระดับ:
  - ปิดคอมเมนต์รายโพสต์: เมื่อคุณโพสต์เนื้อหาแล้ว ไปที่จุดที่จุด 3 จุด (...) ตรงมุมขวาของโพสต์นั้น > เลือก "Who can comment on your post?" > เลือก "Profiles and Pages you mention" (ถ้าเราไม่แท็กใครเลย ก็จะไม่มีใครคอมเมนต์ได้นอกจาก Admin)
  - การกรองคำขายนาม (Content Moderation): ไปที่ Settings > Public Posts > Content Moderation สามารถใส่ Keyword ที่ไม่ต้องการ หรือเปิด "Profanity Filter" เพื่อให้ระบบซ่อนคอมเมนต์ที่ไม่น่าเหมาะสมอัตโนมัติ

**"มาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (สำหรับผู้ปฏิบัติงาน)"**

อ้างอิงตามแผนดำเนินงานรอบ 6 เดือนของมหาวิทยาลัย เพื่อยกระดับความคืบหน้าของการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล

- 1. มาตรการด้านการบริหารจัดการ (Administrative Measures)**
  - การสงวนรักษาความลับ (Confidentiality)**: มีบัญชีรายชื่อที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย (Non-Disclosure Agreement: NDA) หรือข้อตกลงการปกป้องข้อมูล (Data Protection Agreement)
  - การกำหนดหน้าที่และสิทธิ์เข้าถึง (Role-based Access)**: นำหน้าที่และอำนาจหน้าที่ในแผนกต่างๆ มาใช้เพื่อตรวจสอบว่าพนักงานหรือผู้ปฏิบัติงานที่เกี่ยวข้องสามารถเข้าถึงข้อมูลส่วนบุคคล (DPO)
  - การตรวจสอบสถานะความเสี่ยง (Risk Review/KM)**: มีการประเมินความเสี่ยงตามวิธีการควบคุม (KM) และวิเคราะห์ความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของหน่วยงาน
- 2. มาตรการเชิงเทคนิคและระบบสารสนเทศ (Technical Measures)**
  - การแจ้งวัตถุประสงค์และขอความยินยอม**: การประมวลผลข้อมูลส่วนบุคคลเป็นการดำเนินการที่โปร่งใสและแจ้งวัตถุประสงค์ (Privacy Notice) รวมถึงการขอความยินยอม (Consent) ที่สามารถคืนใจ หรือลบข้อมูลได้
  - ความปลอดภัยของสื่อสังคมออนไลน์**: จำกัดสิทธิ์บน Facebook Page ของหน่วยงาน ด้วยบัญชีผู้ดูแลเพจที่เฉพาะเจาะจง
  - การใช้เทคโนโลยีเชิงป้องกัน (Preventive Tech)**: ดำเนินการในการรักษาความปลอดภัย (เช่น การกรอง IP หรือระบบตรวจสอบสิทธิ์) เพื่อลดความเสี่ยงจากการถูกแฮกหรือการละเมิดข้อมูลส่วนบุคคล
- 3. มาตรการด้านบุคลากรและการสร้างความตระหนัก (Human Measures)**
  - การเข้ารับการสอน**: มีบัญชีรายชื่อ (รายชื่อและเนื้อหาการเรียน) ด้วยตัวชี้วัดการประเมินผลตามผลสัมฤทธิ์ของบุคลากร "วัดผลโดย" อบรมหรือเข้ารับการฝึกอบรม
  - โดยมีเป้าหมายว่า "ร้อยละ: 60" ของบุคลากรทั้งหมด**
  - การแลกเปลี่ยนเรียนรู้ (KM)**: มีบันทึกกรณีศึกษาและผลการเรียนรู้จากการดำเนินงาน (Case Study) เพื่อปรับปรุงกระบวนการทำงานให้สอดคล้องกับ PDPA
- 4. มาตรการการตอบสนองและรายงานเหตุละเมิด (Incident Response)**
  - ช่องทางการร้องเรียน**: มีบัญชีรายชื่อหรือช่องทางติดต่อเหตุหรือแจ้งการร้องเรียน กรณีพบเหตุการรั่วไหลเป็นการละเมิดข้อมูลส่วนบุคคล
  - แบบปฏิบัติงานเมื่อเกิดเหตุ**: หากพบเหตุละเมิด ต้องดำเนินการตามแบบปฏิบัติงานกรณีเกิดเหตุเมื่อ มาตรการที่สถานการณณ์เบื้องต้นเพื่อระงับเหตุ

**[ด่วนที่สุด]**  
**แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน**  
**เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล**

สืบเนื่องจากการนำภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin หน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้

- 1. ปิดสิทธิ์โพสต์สาธารณะ:**  
ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง
- 2. เปิดระบบคัดกรองอัตโนมัติ**  
ใช้งาน Moderation Assist เพื่อตั้งค่าข้อความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย

ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย

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

แจ้ง Admin หน่วยงานทราบ  
1. [ด่วนที่สุด] แนวทางยกระดับความปลอดภัย Facebook Page หน่วยงาน เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล

สืบเนื่องจากการนำภาพบุคคลมาดัดแปลงและบิดเบือนข้อเท็จจริงในช่องทาง Comment ของเพจหน่วยงาน เพื่อเป็นการป้องกันเชิงรุกและรักษามาตรฐานความปลอดภัยสารสนเทศ ขอให้ Admin หน่วยงานดำเนินการตั้งค่า Facebook Page ดังนี้

(1) ปิดสิทธิ์โพสต์สาธารณะ: ไม่อนุญาตให้บุคคลภายนอกโพสต์เนื้อหาบน Timeline ของเพจโดยตรง  
(2) เปิดระบบคัดกรองอัตโนมัติ: ใช้งาน Moderation Assist เพื่อตั้งค่าข้อความเห็นที่มีคำไม่สุภาพ หรือ Keywords ที่เข้าข่ายบิดเบือนข้อมูล/สร้างความเสียหาย

ทั้งนี้ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลและป้องกันมิให้พื้นที่ของมหาวิทยาลัยถูกใช้ในทางที่ผิดกฎหมาย

2. นัดหมาย และแจ้งกำหนดจัดกิจกรรมแลกเปลี่ยนเรียนรู้สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล วันพุธที่ 29 เมษายน 2569 เวลา 09.00-12.00 น. ณ ห้องประชุมดอกสัก สำหรับวิทยากรและเทคโนโลยีสารสนเทศ

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

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์การกระทำความคิดในลักษณะนำรูปภาพส่วนตัวจากสื่อสังคมออนไลน์มาดัดแปลงเพื่อบิดเบือนข้อเท็จจริง และเผยแพร่ผ่านช่องทางแสดงความคิดเห็น (Comment) ในหน้าเพจ Facebook ของหน่วยงานภายในมหาวิทยาลัย ซึ่งการกระทำดังกล่าวนี้ใช้ข้อมูลส่วนบุคคลของมหาวิทยาลัยจู่โจม แต่มีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล นั้น

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ... ดูเพิ่มเติม

**แนวทางยกระดับความมั่นคงปลอดภัยสารสนเทศ และการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน**

สืบเนื่องจากการเกิดเหตุละเมิดข้อมูลส่วนบุคคล เมื่อวันที่ 15 มีนาคม 2569 โดยการบิดเบือนรูปภาพและเผยแพร่ผ่านความคิดเห็นในหน้าเพจ Facebook

- 1. จำกัดสิทธิ์การโพสต์**
  - ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง
- 2. ยกระดับการคัดกรอง**
  - เปิดใช้งาน "ตัวช่วยการกรอง" (Moderation Assist)
  - ตั้งค่าคัดกรองความคิดเห็น (Comment Filtering)
  - ข้อความที่เข้าข่ายบิดเบือนข้อมูล

อ้างอิง: มติคณะกรรมการบริหารมหาวิทยาลัย ครั้งที่ 4/2569 วันที่ 2 เมษายน 2569

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

#### รายงานสถานการณ์และการตรวจพบเหตุละเมิด

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์การกระทำความคิด ดังนี้

- **ลักษณะการกระทำ** มีการนำรูปภาพของบุคลากรและบุคคลภายนอกไปตัดต่อโดยไม่ได้รับอนุญาต เพื่อสร้างสื่อบิดเบือนข้อเท็จจริงในลักษณะการทวงหนี้ และกล่าวหาว่าเป็นส่วนหนึ่งของขบวนการฉ้อโกง

- **ช่องทางที่เกิดเหตุ** การนำภาพตัดต่อดังกล่าวไปเผยแพร่ผ่านช่องทางการแสดงความคิดเห็น (Comment) ในเพจ Facebook "โสตทัศนวัสดุ มหาวิทยาลัยราชภัฏกำแพงเพชร"

#### การดำเนินการโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ภายหลังตรวจพบเหตุ มหาวิทยาลัยฯ ได้ดำเนินการตามขั้นตอนมาตรฐานทางกฎหมาย (PDPA) อย่างเร่งด่วน ดังนี้

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

- การแจ้งเหตุต่อหน่วยงานกำกับดูแล ดำเนินการจัดทำหนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายในกรอบเวลา 72 ชั่วโมงตามที่กฎหมายกำหนด
- การเยียวยาผู้ได้รับผลกระทบ จัดทำบันทึกแจ้งเหตุให้แก่ผู้ที่ได้รับผลกระทบโดยตรง พร้อมให้คำแนะนำในการปฏิบัติตนและการคุ้มครองสิทธิส่วนบุคคล

**มาตรการตอบโต้ทางเทคนิคและทางกฎหมาย (สำนักวิทยบริการฯ)**

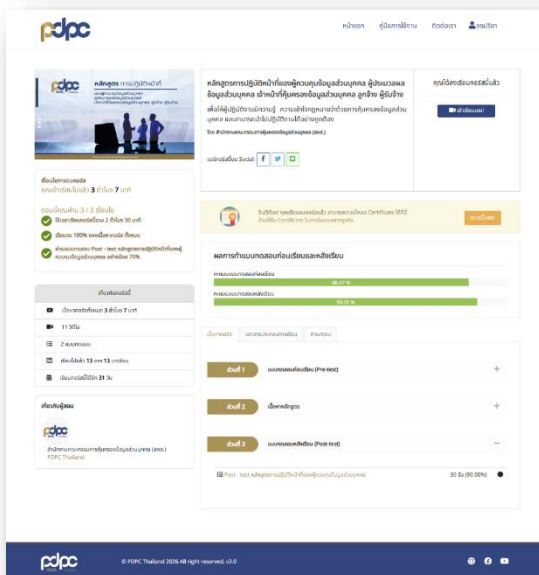
เพื่อให้เกิดการแก้ไขที่ต้นเหตุและป้องกันการขยายตัวของความเสียหาย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการ ดังนี้

- 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) ที่เกี่ยวข้องกับการบิดเบือนข้อมูล โดยอัตโนมัติ

จึงเรียนที่ประชุมทราบแนวทางการจัดการเหตุละเมิด และขอความร่วมมือทุกหน่วยงานตรวจสอบและรักษามาตรฐานการตั้งค่าสื่อสังคมออนไลน์โดยการจำกัดสิทธิ์การโพสต์และการแสดงความคิดเห็นอย่างเคร่งครัด ทั้งนี้ สำนักวิทยบริการฯ ได้ดำเนินการจัดส่งบันทึกข้อความแจ้งเวียนไปในระบบ E-Office วันที่ 7 เมษายน 2569

(8) อบรมหลักสูตรการเรียนรู้ออนไลน์ หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง โดย สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) จำนวน 3 ชั่วโมง และเมื่อผ่านจะได้รับประกาศนียบัตร เพื่อคัดเลือกหลักสูตรสำหรับบุคลากร ขั้วเคลื่อนที่กระบวนการของมหาวิทยาลัยต่อซึ่งอยู่ระหว่างนำเรียนคณะกรรมการบริหารมหาวิทยาลัย พิจารณา



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

ที่	เลขที่แจ้ง	เลขที่แจ้ง	วันที่	ถึง	เรื่อง	จาก	หมายเลข	ปฏิทิน	entry	แก้ไข
	5820007263	๕๗๓.๗๗.๑ 0061/2569	07/04/2569	1.คณบดีและคณาจารย์ 2.คณบดีและบุคลากร 3.คณบดีและบุคลากร 4.คณบดีและบุคลากร 5.คณบดีและบุคลากร 6.คณบดีและบุคลากร 7.คณบดีและบุคลากร 8.คณบดีและบุคลากร 9.คณบดีและบุคลากร 10.คณบดีและบุคลากร 11.คณบดีและบุคลากร 12.คณบดีและบุคลากร 13.คณบดีและบุคลากร 14.คณบดีและบุคลากร 15.คณบดีและบุคลากร	แนวทางการยกระดับความมั่นคงปลอดภัยสารสนเทศและการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยงาน	ผู้อำนวยการสำนักสถาบันเทคโนโลยีสารสนเทศ มหาวิทยาลัย			08/04/2569 09:07	



## บันทึกข้อความ

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

เรียน [เรียน]

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ ๑๕ มีนาคม ๒๕๖๙ โดยมีเหตุการณ์กระทำความผิดในลักษณะนำรูปภาพส่วนตัวจากสื่อสังคมออนไลน์ มาตัดแปลงเพื่อบิดเบือนข้อเท็จจริง และเผยแพร่ผ่านช่องทางการแสดงความคิดเห็น (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

1. จำกัดสิทธิ์การโพสต์ ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง
2. ยกระดับการคัดกรอง เปิดใช้งานเครื่องมือ “ตัวช่วยการควบคุม” (Moderation Assist) และตั้งค่าการคัดกรองความคิดเห็น (Comment Filtering) เพื่อซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญ (Keywords) ที่เกี่ยวข้องกับการบิดเบือนข้อมูลโดยอัตโนมัติ

จึงเรียนมาเพื่อโปรดพิจารณา

(ผู้ช่วยศาสตราจารย์พรหมเมศ วีระพันธ์)  
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ  
Signature Code : FlobAgKXUFVAKCttmJLm

จากบันทึกข้อความข้างต้น เหตุการณ์ละเมิดข้อมูลส่วนบุคคลในวันดังกล่าว มิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ จึงสรุปได้ว่า **ไม่มีการได้รับรายงานการละเมิดข้อมูลส่วนบุคคล**

(10) Infographic อื่นๆที่เกี่ยวข้อง

**UNIVERSITY DATA SECURITY GUIDELINES** **UNIVERSITY DATA SECURITY GUIDELINES**

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

**✓ ข้อควรปฏิบัติ (DO'S)**

- ใช้ระบบองค์กรเท่านั้นในการกักข้อมูล**  
USE UNIVERSITY SYSTEMS ONLY FOR DATA
- ตรวจสอบสิทธิ์ก่อนเปิดเผยข้อมูล**  
VERIFY PERMISSIONS BEFORE DISCLOSING
- เก็บข้อมูลอย่างปลอดภัย**  
STORE DATA SECURELY
- รายงานเหตุผิดปกติทันที**  
REPORT INCIDENTS IMMEDIATELY

**✗ ข้อห้าม (DON'TS)**

- ใช้ LINE / Facebook ส่วนตัวส่งข้อมูล**  
DO NOT USE PERSONAL LINE / FACEBOOK
- พูดถึงข้อมูลกับบุคคลภายนอก**  
DO NOT DISCUSS CONFIDENTIAL INFO WITH OUTSIDERS
- 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)**

- จัดทำและประกาศนโยบายความเป็นส่วนตัว (PRIVACY NOTICE)
- แจ้งข้อตกลงที่ขอความยินยอม (COOKIE CONSENT BANNER)
- แนบฟอร์มรับข้อมูลจำเป็นและลิงก์นโยบาย (NECESSARY FORMS & POLICY LINK)

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

- เข้ารหัสข้อมูลสำคัญและการส่งผ่านข้อมูล (DATA ENCRYPTION: IN STORAGE & TRANSIT)
- จำกัดสิทธิ์เข้าถึงและการยืนยันตัวตนข้อมูล (ACCESS CONTROL & 2FA/MFA)
- ตรวจสอบช่องโหว่และอัปเดตระบบอย่างสม่ำเสมอ (VULNERABILITY SCAN & PATCHING)

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

- เก็บ LOG การทำงานและเปลี่ยนแปลงข้อมูล
- วางแผนลบข้อมูลอัตโนมัติโดยคอมพิวเตอร์ (AUTOMATED DATA DELETION)
- สำรองข้อมูลอย่างปลอดภัยและมีการเข้ารหัส (ENCRYPTED BACKUP STORAGE)

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

- ขั้นตอนปฏิบัติเมื่อตรวจพบการบุกรุก (INCIDENT RESPONSE PLAN)
- ประสานงานกับ DPO และแจ้ง ส.ส. (COORDINATE WITH DPO & NOTIFY AUTHORITY)

FOR UNIT INFORMATION SYSTEM & WEBSITE ADMINISTRATORS สำหรับผู้ดูแลระบบสารสนเทศและเว็บไซต์หน่วยงาน

### กระบวนการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (PERSONAL DATA BREACH MANAGEMENT PROCESS)

- การตรวจสอบและยืนยันเหตุการณ์**
  - ตรวจสอบทันที: ประเมินความน่าเชื่อถือของข้อมูลที่ได้รับ
  - ตรวจสอบมาตรการรักษาความปลอดภัย: ตรวจสอบเส้นทางการเข้าถึงที่ผิดปกติ และภาษาภาพ
- การประเมินความเสี่ยงและผลกระทบ**
  - หากยืนยันว่าเกิดการละเมิดจริง ต้องประเมินว่า:
    - ผลกระทบของข้อมูลรั่วไหลมีระดับความเสี่ยงสูงหรือไม่
    - ข้อมูลรั่วไหลมีลักษณะเป็นประเภทของข้อมูล ซึ่งสูง เช่นนามข้อมูล หมายเลขบัญชีธนาคาร
- การดำเนินการจัดการเพื่อบรรเทาผลกระทบ**
  - ดำเนินการแก้ไข:
    - ตัดการเชื่อมต่อ: ปิดช่องโหว่ของระบบ แก้ไขรหัสผ่าน หรือระงับการเข้าถึงชั่วคราว
    - บรรเทาผลกระทบ: ลดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูล
- การแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคล**
  - รายงาน ส.ส. ภายใน 72 ชั่วโมง: ปรึกษาทางเทคนิค
  - รายละเอียดข้อมูล: ลักษณะของการละเมิด ข้อมูลที่รั่วไหล มีลักษณะอย่างไร และระดับความเสียหายที่ประเมินได้
- การดำเนินการมาตรการเยียวยา**
  - ขอความเสียหาย: กับการแจ้งเตือนและการให้บริการที่ช่วยลดผลกระทบ
  - ให้คำปรึกษา: ช่วยเหลือเจ้าของข้อมูลในการจัดการกับผลกระทบที่เกิดขึ้น
  - แก้ไขข้อบกพร่อง: ดำเนินการแก้ไขหรือขจัดข้อมูลที่ถูกละเมิด
- การปรับปรุงมาตรการรักษาความมั่นคงปลอดภัย**
  - ทบทวนและปรับปรุง: มาตรการป้องกันเพื่อป้องกันเหตุการณ์ซ้ำในอนาคต

## แนวปฏิบัติที่ดีที่สุดสำหรับการจัดการเหตุการณ์ด้านความปลอดภัยทางไซเบอร์

### เพื่อสร้างความพร้อมและลดผลกระทบต่อองค์กร

- 1** ทำให้แผนรับมือเหตุการณ์ฉุกเฉิน (IRP) เป็นเอกสารที่มีการพัฒนาอย่างต่อเนื่อง
  - ทบทวนและปรับปรุงอย่างสม่ำเสมอ (อย่างน้อยปีละครั้ง)
  - หลีกเลี่ยงการเปลี่ยนแปลงที่สำคัญ
  - อิงจากบทเรียนการฝึกซ้อมและเหตุการณ์จริง
- 2** สื่อสารอย่างชัดเจน
  - กันทั่วทั้งทีและชัดเจน
  - สื่อสารทั้งภายในและภายนอก (ผู้ได้รับผลกระทบ, หน่วยงาน, สาธารณชน)
  - กำหนดช่องทางและระเบียบปฏิบัติก่อนวิกฤต
- 3** ใช้ระบบอัตโนมัติในส่วนที่ทำได้
  - งานตรวจจับและการควบคุมที่ซ้ำซาก
  - เร่งความเร็วในการตอบสนอง
  - ใช้คู่มือและเครื่องมือการทำงานอัตโนมัติ (เช่น SOAR)
- 4** การมีส่วนร่วมของที่ปรึกษาด้านกฎหมาย
  - ปรึกษาดังแต่เนิ่นๆ ในการวางแผนและระหว่างเหตุการณ์
  - โดยเฉพาะเหตุการณ์รั่วไหลของข้อมูล
  - ดูแลเรื่องการควบคุม, การแจ้งเตือน, และการจัดการหลักฐาน
- 5** รักษาหลักฐาน
  - รักษาความสมบูรณ์ของหลักฐาน
  - เพื่อวิเคราะห์สาเหตุทางกฎหมาย
  - พิสูจน์ระบบกันชนในการที่รวบรวมที่ถูกต้อง

Chain of Custody

## เทคนิคการจัดการ LOG FILES ให้สอดคล้องกับ PDPA

### รักษาสมดุลระหว่าง “เก็บหลักฐาน” และ “คุ้มครองความเป็นส่วนตัว”

<b>DATA MINIMIZATION</b> (เก็บเท่าที่จำเป็น) <ul style="list-style-type: none"> <li>✓ ตัดข้อมูลที่ไม่เกี่ยวข้องออก (CUT IRRELEVANT DATA)</li> <li>✓ เลิกเก็บเฉพาะ METADATA ไร้ ท่าอะไร เมื่อไหร่ ที่ไหน (WHO, WHAT, WHEN, WHERE)</li> </ul>	<b>PSEUDONYMIZATION</b> (การใช้นามแฝง) <ul style="list-style-type: none"> <li>✓ ใช้ ID แทนชื่อ (USE ID INSTEAD OF NAME)</li> <li>✓ HASHING IP ADDRESS</li> </ul>	<b>DATA MASKING</b> (การปกปิดข้อมูล) <ul style="list-style-type: none"> <li>✓ ซ่อนเซอร์ข้อมูลอ่อนไหว (SENSOR SENSITIVE DATA)</li> <li>✓ กรองรูปแบบ Credit Card ออ</li> </ul>	<b>ACCESS CONTROL</b> (การจำกัดสิทธิ์) <ul style="list-style-type: none"> <li>✓ ให้สิทธิ์เฉพาะผู้จำเป็น (ONLY ESSENTIAL STAFF)</li> <li>✓ แยกคนมีสิทธิ์ดู Log กับแก้ไขระบบ (SEPARATE VIEWER &amp; SYSTEM ADMIN ROLES)</li> </ul>	<b>RETENTION POLICY</b> (กำหนดอายุการเก็บ) <ul style="list-style-type: none"> <li>✓ ตั้งระบบ Log ที่เก็บ (AUTO-DELETION)</li> <li>✓ Log รักษาแบบต้องเข้ารหัส (ENCRYPTION AT REST)</li> </ul>
--	---	---	---	---

**จุดที่มักพลาด**  
(COMMON PITFALLS)

GUG FILE LOGS และ “คุ้มครองความเป็นส่วนตัว”

DEBUG MODE บันทึกข้อมูลทุกอย่าง

ERROR LOGS เหลือพื้นที่ข้อมูลลูกค้าออกมา

## 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

### (11) ขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (PDPA Response Plan) และแนวปฏิบัติ

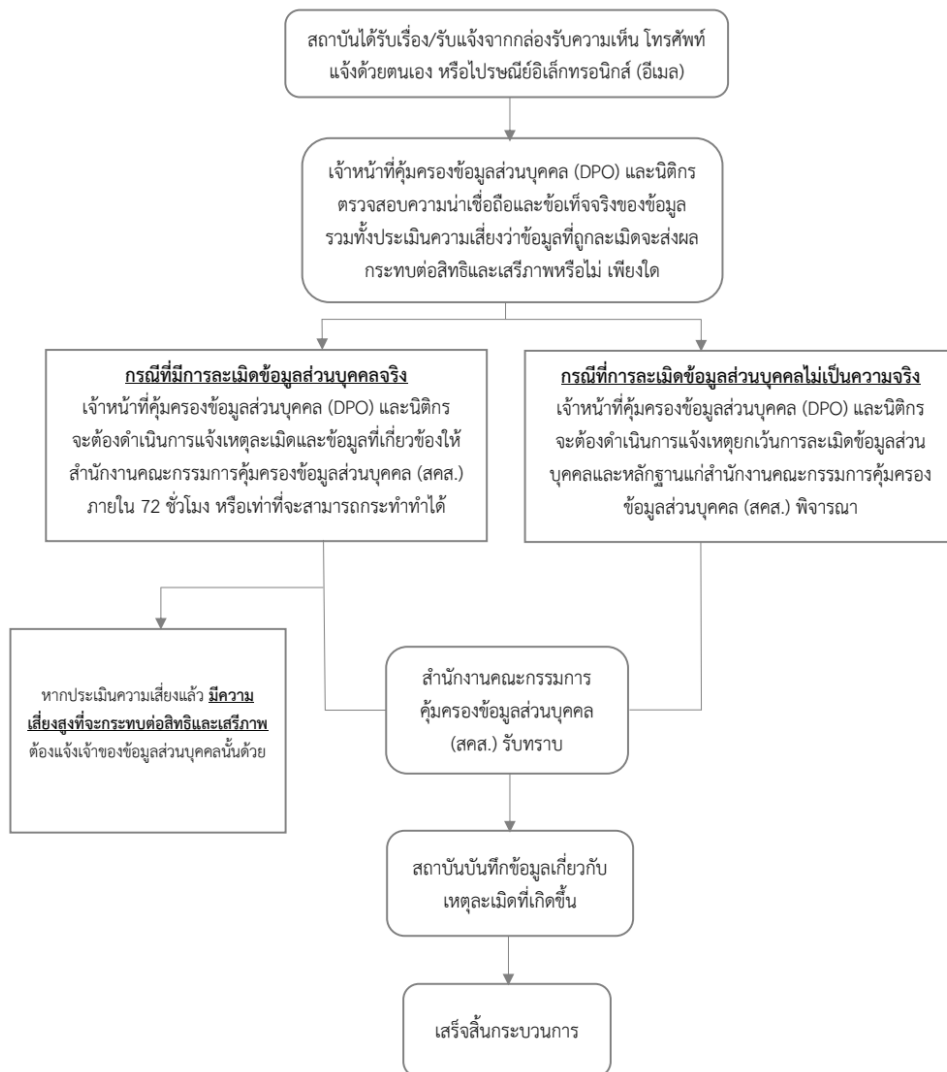
1. การรับแจ้งเหตุ หน่วยงาน/สถาบัน รับเรื่องจากกล่องรับความคิดเห็น, โทรศัพท์, แจ้งด้วยตนเอง หรืออีเมล
2. การตรวจสอบและประเมิน เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และนิติกร ดำเนินการ
  - ตรวจสอบความน่าเชื่อถือและข้อเท็จจริงของข้อมูล
  - ประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

กรณีที่ 1 มีการละเมิดจริง	กรณีที่ 2 ไม่มีการละเมิดจริง
แจ้งเหตุและข้อมูลที่เกี่ยวข้องต่อ สำนักงาน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ	แจ้งเหตุยกเว้นการละเมิดพร้อมหลักฐานประกอบต่อ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เพื่อให้ สคส. พิจารณา

หากประเมินแล้วพบว่า มีความเสี่ยงสูง ที่จะกระทบต่อสิทธิและเสรีภาพ ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบด้วยโดยไม่ชักช้า

3. การบันทึก สคส. รับเรื่องเข้าสู่กระบวนการของเจ้าหน้าที่รัฐ สถาบันทำการบันทึกรายละเอียดเกี่ยวกับเหตุ ละเมิดที่เกิดขึ้น (Log/Record of Processing) เป็นอันเสร็จสิ้นกระบวนการจัดการเหตุละเมิด

#### แผนผัง (Flowchart) กระบวนการในการปฏิบัติงานกรณีที่มีการละเมิดข้อมูลส่วนบุคคล





**แนวปฏิบัติการรับมือเหตุการณ์ข้อมูลส่วนบุคคล (Data Breach Incident Response Plan)**  
**มหาวิทยาลัยราชภัฏกำแพงเพชร**

**1. เจ้าของข้อมูลส่วนบุคคล** แจ้งเหตุละเมิดข้อมูลส่วนบุคคล ในระบบรับรองสิทธิ หรือช่องทางอื่นใดที่มหาวิทยาลัยจัดเตรียมไว้

**2. ผู้ควบคุมข้อมูลส่วนบุคคล/เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** ตรวจสอบเหตุละเมิด

- ตรวจสอบข้อมูลส่วนบุคคลตามที่เจ้าของข้อมูลส่วนบุคคลได้แจ้งไว้ ถูกทำให้สูญเสียการเป็นความลับ ความถูกต้อง หรือความพร้อมใช้ หรือไม่

- ตรวจสอบตัวตนของเจ้าของข้อมูลว่า เป็นบุคคลเดียวกันที่เป็นเจ้าของข้อมูลหรือไม่ โดยสามารถแจ้งให้เจ้าของข้อมูลส่งรายละเอียดเพิ่มเติม เพื่อยืนยันตัวตนได้ (เริ่มนับระยะเวลาดำเนินการแจ้งเหตุละเมิดแก่ สคส. ภายใน 72 ชม.)

- กรณีผู้ประมวลผลข้อมูลทราบเหตุละเมิด ให้แจ้งผู้ควบคุมข้อมูลภายใน 24 ชม.

- กรณีผู้ควบคุมข้อมูลทราบเหตุละเมิด ให้แจ้ง DPO ภายใน 24 ชม.

- ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเชิงองค์กร (organizational measures) และ มาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว

**3. ผู้ควบคุมข้อมูล/เจ้าหน้าที่คุ้มครองข้อมูล** ประเมินผลกระทบต่อความเสียหายของเจ้าของข้อมูลส่วนบุคคล

- พิจารณาผลของเหตุการณ์ข้อมูลรั่วไหลนั้น ได้ส่งผลกระทบต่อความเสี่ยงหรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่

- ประเมินระดับความรุนแรงและผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ระดับความรุนแรง	ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล
5 - สูงมาก	ได้รับผลกระทบที่มีนัยสำคัญ และไม่สามารถแก้ไขปัญหาได้ เช่น เกิดความเสียหายด้านการเงิน ทำให้เกิดหนี้สิน ไม่สามารถชดเชยได้ ไม่สามารถทำงานได้ ได้รับผลกระทบทางจิตใจหรือร่างกาย หรือทำให้ถึงขั้นเสียชีวิต
4 - สูง	ได้รับผลกระทบที่มีนัยสำคัญ ซึ่งมีปัญหา- ความยุ่งยากต่อเจ้าของข้อมูลส่วนบุคคล แต่สามารถแก้ไขปัญหาได้ เช่น ถูกยึดยกยอกเงิน ถูกธนาคารปฏิเสธการทำธุรกรรม ทรัพย์สินเสียหาย ถูกเลิกจ้าง ได้รับหมายศาล สุขภาพทรุดโทรม
3 - ปานกลาง	ได้รับความไม่สะดวกอย่างมีนัยสำคัญ ซึ่งมีปัญหา-ความยุ่งยากเล็กน้อย แต่สามารถแก้ไขปัญหาได้ เช่น เจ้าของข้อมูลส่วนบุคคลมีภาระค่าใช้จ่ายเพิ่มเติม ถูกปฏิเสธการเข้าถึงบริการทางธุรกิจ มีความกลัว มีความเครียด เกิดความไม่เข้าใจ หรือมีอาการเจ็บป่วยทางกายเล็กน้อย
2 - ต่ำ	ได้รับความไม่สะดวกเพียงเล็กน้อย เช่น เจ้าของข้อมูลส่วนบุคคลเสียเวลาในการป้อนข้อมูลใหม่ หรือ มีความไม่พึงพอใจเล็กน้อย
1 - ต่ำมาก	ไม่ได้รับผลกระทบ

**หมายเหตุ** ระดับความรุนแรง 5 - สูงมาก และ 4 - สูง แจ้งเจ้าของข้อมูลส่วนบุคคล  
ระดับความรุนแรง 2 - ต่ำ จนถึง 5 - สูงมาก แจ้งสำนักงาน (สคส.)  
ระดับความรุนแรง 1 - ต่ำมาก จัดบันทึกและรายงานเหตุละเมิดต่อผู้บริหาร/รายไตรมาส



### ข้อกำหนดการแจ้งเหตุละเมิด

ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลนั้นแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง เว้นแต่การละเมิดดังกล่าวไม่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีความเสี่ยงสูง ที่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งการละเมิดให้เจ้าของข้อมูลทราบพร้อมแนวทางเยียวยา



### 4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล ผู้ดูแลระบบสารสนเทศ เจ้าหน้าที่ IT

- หาสาเหตุและดำเนินการป้องกัน ระวังเหตุ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที เท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม (ควรซึ่งได้รับการอนุมัติจากผู้บริหาร พร้อมระยะเวลาในการดำเนินการที่แน่นอน)

- ทบทวน ปรับปรุงมาตรการการรักษาความปลอดภัยของข้อมูลให้รัดกุม
- หากการรั่วไหลของข้อมูลส่วนบุคคล ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (ในระดับ 2-5) DPO ต้องส่งเรื่องไปยังผู้บริหารที่เกี่ยวข้องทราบภายในระยะเวลาที่รวดเร็ว
- ผู้เกี่ยวข้องทุกฝ่าย รวมถึงผู้บริหาร ร่วมกำหนดแนวทางเยียวยา
- หามาตรการบรรเทาผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลอย่างเร่งด่วน

### 5. ผู้ควบคุมข้อมูล/เจ้าหน้าที่คุ้มครองข้อมูลแจ้งเหตุละเมิด ต่อ สคส. และเจ้าของข้อมูลส่วนบุคคล

### 6. ผู้เกี่ยวข้องทุกฝ่าย ทบทวนแนวทางการรับมือและหาวิธีการป้องกันไม่ให้เกิดขึ้นอีก

### (12) 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 ส่วนงานหน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลขัดข้อง โดยไฟดับชั่วคราวส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของคณะ ส่วนงานหน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าว ไม่อยู่ในสภาพพร้อมใช้งานเนื่องจากปัญหาทางด้านเทคโนโลยีเมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วนบุคคลดังกล่าว ก็ยังสามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
4	ผู้ควบคุมข้อมูลส่วนบุคคล ถูกภัยคุกคามทางไซเบอร์ โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูล ส่วนบุคคล ถูกเข้ารหัสโดยผู้โจมตี (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 อย่างไรก็ตามตามคณะ ส่วนงานหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม
6	ผู้ควบคุมข้อมูลส่วนบุคคล ให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาผู้ควบคุมข้อมูลส่วนบุคคลถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลรายชื่อผู้ใช้บริการ รหัสผ่าน และประวัติการซื้อสินค้าถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต	ต้องแจ้ง	ต้องแจ้งลูกค้าของผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของที่มีข้อมูลรั่วไหลบน อินเทอร์เน็ต	ข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
7	เว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้าง ประมวลผลข้อมูลส่วนบุคคล จากผู้ควบคุมข้อมูลส่วนบุคคลเกิดปัญหาผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง ทำให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้	ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งสำนักงานฯ เนื่องจากมีผลกระทบต่อกลุ่มลูกค้าพอสมควร เพราะปัญหาดังกล่าวทำให้กลุ่มลูกค้าไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้	ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้ง เจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับผลกระทบ เนื่องจากยังไม่เกิดปัญหา	ในเบื้องต้นเป็นเพียงข้อผิดพลาดของโปรแกรมที่ทำให้เข้าถึงข้อมูลส่วนบุคคลไม่ได้ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามีภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกคามทางไซเบอร์เว็บไซต์ผู้ให้บริการ Web Hosting ต้องรีบแจ้งผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลต้องรีบแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลต่อไป
8	โรงพยาบาลแห่งหนึ่งถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก hacker ทำให้ประวัติของผู้ป่วยไม่สามารถเข้าถึงได้เป็นเวลา 30 ชั่วโมง	ต้องแจ้ง เนื่องจากข้อมูลประวัติของผู้ป่วยเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและสามารถระบุตัวบุคคลได้	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิด หรือมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าวรวมถึงข้อมูลสุขภาพด้วย เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุและตรวจสอบข้อมูลเพิ่มเติม
9	โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าวไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งผู้รับเหมาอาจจะนำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
10	บริษัทแห่งหนึ่งทำการตลาดแบบตรง โดยการส่งข้อมูล	ต้องแจ้ง เนื่องจากเป็นการส่งข้อมูล	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลใน	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
	ส่วนบุคคลไปยังผู้รับข้อมูล แต่ละราย แต่ด้วยความ ผิดพลาด จึงมีการใส่ที่อยู่ ของบุคคลที่รับอีเมลทั้ง 100 คน เข้าไปในช่อง To หรือ Cc ทำให้ผู้รับอีเมลเห็น อีเมลที่มีข้อมูลส่วนบุคคล ของบุคคลอื่น	ของเจ้าของข้อมูล ส่วนบุคคลจำนวนมาก จึงจำเป็นต้อง แจ้งเหตุ แต่หาก ข้อมูลดังกล่าวมีการ เข้ารหัสโดยเทคโนโลยี ที่น่าเชื่อถือ อาจได้รับ ยกเว้นไม่ต้องแจ้งเหตุ	อีเมลดังกล่าวอาจ ถูกนำไปใช้และ ก่อให้เกิดความ เสียหายต่อเจ้าของ ข้อมูลส่วนบุคคล ภายหลังได้	หรือไม่ อาจขึ้นอยู่กับปริมาณ ของข้อมูลส่วนบุคคลที่ส่งออกไป และลักษณะของข้อมูลด้วยหาก มีการเข้ารหัสข้อมูลดังกล่าว ทั้งหมด อาจถือว่ามีความเสี่ยง ต่ำไม่จำเป็นต้องแจ้งเหตุ

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

#### 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

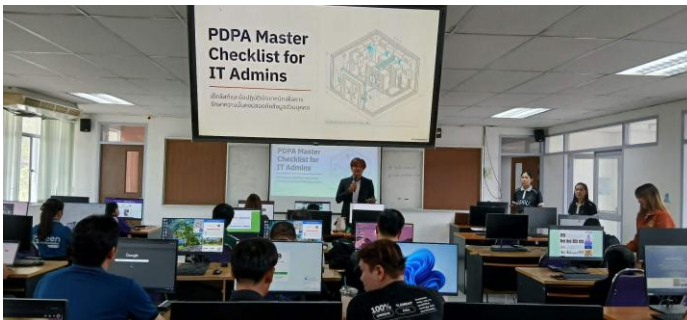


(3) กิจกรรมแลกเปลี่ยนเรียนรู้กลุ่มแอดมิน ร่วมกับ DPO และผู้ประมวลผลข้อมูลสำนักฯ วันที่ 27 กุมภาพันธ์ 2569 เวลา 09.00 น. ณ ห้องประชุมดอกสัก เพื่อแนะนำเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย และวางแผนจัดอบรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล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



**5. นำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด“ขุมความรู้” ออกมาบันทึกไว้** เป็นการสรุปบทเรียนจากการทำงานจริง

กิจกรรมที่ 6 จัดตั้งชุมชนนักปฏิบัติ (CoP) ในกลุ่มผู้ใช้งาน กิจกรรมที่ 5 เพื่อแลกเปลี่ยนประสบการณ์ปัญหา และจุดที่ต้องปรับปรุงในการนำ แนวทางไปปฏิบัติจริง และสกัด บทเรียนที่ได้ออกมา โดยจัดกิจกรรมแลกเปลี่ยนเรียนรู้ เมื่อวันที่ 29 เมษายน 2569 เวลา 09.00 น. ณ ห้องปฏิบัติการคอมพิวเตอร์ ชั้น 5 อาคารศูนย์ภาษา และคอมพิวเตอร์





จากขั้นตอนการนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด “ชุมชนความรู้” ออกมาบันทึกไว้ เพื่อสร้างชุมชนการเรียนรู้ (Learning Community) โดย สร้างกลุ่มสำหรับแลกเปลี่ยนเรียนรู้ทางโซเซียลมีเดีย 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 ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และแหล่งอื่นๆ ที่มีความน่าเชื่อถือ คัดเลือก จัดบันทึก “ชุมชนความรู้” 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 สรุปลงเป็นประเด็นสาระสำคัญของงาน เป็นชุดความรู้ แบบ Explicit Knowledge และรวบรวมความรู้ที่มีประโยชน์ อ้างอิงจากแหล่งความรู้ (References) แล้วจัดเก็บเป็นคลังความรู้ออนไลน์เผยแพร่ในเว็บไซต์ให้ผู้เข้าเข้าถึงได้ง่าย 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. องค์กรความรู้

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

## 11. การนำองค์ความรู้หรือแนวปฏิบัติที่ดีที่สุดไปใช้

อยู่ระหว่างรอการส่งกลับจากผู้มีส่วนเกี่ยวข้อง

## 12. ช่องทางการเผยแพร่องค์ความรู้

- เผยแพร่ผ่านช่องทาง Website มหาวิทยาลัย และ Facebook ศูนย์คอมพิวเตอร์
- ชุดความรู้เฉพาะกลุ่ม เผยแพร่ผ่านเพจ Facebook กลุ่มผู้ดูแลเว็บไซต์ และเว็บไซต์

<https://kpru.ac.th/km-web/>

# ภาคผนวก

ตัวอย่างการกรอก RoPA แผนก IT

กิจกรรม	ประเภทข้อมูล	ฐานทางกฎหมาย	ระยะเวลาจัดเก็บ	สถานที่จัดเก็บ
การจัดการสิทธิ์เข้าถึงระบบ	ชื่อ-นามสกุล, อีเมลมหาวิทยาลัย, เลขบัตรประจำตัวประชาชน, รหัสบุคลากร, Log การใช้งาน	ฐานสัญญา (Contract) เพื่อให้บุคลากรสามารถปฏิบัติงานได้ตามสัญญาจ้าง	ตลอดอายุการทำงาน + 30 วันหลังลาออก	<ul style="list-style-type: none"> <li>- On-Premise หน่วยงานเป็นผู้ควบคุมทั้งหมด เช่น Server ห้อง Data Center ของหน่วยงาน (ระบุชั้น/ตึก)</li> <li>- Cloud Service เช่น AWS (Region Singapore), Google Workspace หรือ Azure</li> <li>- Backup Device สำรองข้อมูลด้วยอุปกรณ์ใดบ้าง เช่น ฮาร์ดดิสก์ไดรฟ์ (HDD), โซลิดสเตทไดรฟ์ (SSD) หรือ External Drive ที่เก็บไว้ในตู้เซฟ ฯลฯ</li> </ul>
การบันทึก Log ตาม พรบ. คอมพิวเตอร์	IP Address, หมายเลขเครื่อง (MAC), ประวัติการเข้าเว็บ, ระยะเวลาใช้งาน	ฐานหน้าที่ตามกฎหมาย (Legal Obligation) ปฏิบัติตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	ไม่น้อยกว่า 90 วัน (ตามที่กฎหมายกำหนด)	
การให้ยืม-คืน อุปกรณ์ (IT Asset)	ชื่อ, หมายเลขโทรศัพท์, รายการอุปกรณ์ที่ถือครอง	ฐานประโยชน์โดยชอบธรรม (Legitimate Interest) เพื่อติดตามและป้องกันทรัพย์สินบริษัทสูญหาย	ตลอดอายุการใช้งานอุปกรณ์ + 1 ปี	
การแก้ไขปัญหาทางเทคนิค (IT Support/Helpdesk)	ชื่อ, รหัสพนักงาน, รายละเอียดปัญหา, ภาพหน้าจอ (ถ้ามี)	ฐานสัญญา/ประโยชน์โดยชอบธรรม เพื่อสนับสนุนการทำงานและปรับปรุงบริการ	1-2 ปี เพื่อดูสถิติการเกิดปัญหาซ้ำ	
การตรวจสอบความมั่นคงปลอดภัย (Security Audit)	Log การเข้าถึงไฟล์, กิจกรรมที่ผิดปกติ, ข้อมูลระบุตัวตน	ฐานประโยชน์โดยชอบธรรม เพื่อป้องกันการจารกรรมข้อมูลและภัยคุกคามไซเบอร์	1-5 ปี (ตามนโยบายบริษัท)	

ตัวอย่างการกรอก RoPA แผนก HR

กิจกรรม	ประเภทข้อมูล	ฐานทางกฎหมาย	ระยะเวลาจัดเก็บ
สรรหาพนักงาน	ชื่อ, เบอร์โทร, ประวัติการศึกษา, ผลทดสอบ	ฐานสัญญา เพื่อดำเนินการตามคำขอของเจ้าของข้อมูลก่อนเข้าทำสัญญา	1 ปี (กรณีไม่รับเข้าทำงาน)
จัดทำเงินเดือน	ชื่อ, เลขบัญชีธนาคาร, เลขบัตรประชาชน	ฐานสัญญา (Contract) เพื่อปฏิบัติตามสัญญาจ้างงาน	ตลอดอายุงาน + 10 ปี (ตามกฎหมายบัญชี/ภาษี)
สวัสดิการประกันกลุ่ม	ชื่อ, ข้อมูลสุขภาพ, ผู้รับผลประโยชน์	ฐานสัญญา + ความยินยอม (Consent) ข้อมูลสุขภาพเป็นข้อมูลอ่อนไหว ต้องขอความยินยอมแยกต่างหาก	ตลอดอายุงาน + 2 ปี
ลงเวลาทำงาน/CCTV	ภาพใบหน้า, เวลาเข้า-ออก	ฐานประโยชน์โดยชอบธรรม (Legitimate Interest) เพื่อความปลอดภัยและวินัยการทำงาน	30-90 วัน (แล้วแต่ความจุระบบ)

**ข้อควรระวัง** ข้อมูลใน **หน้าบัตรประชาชน** มีทั้งศาสนาและหมู่เลือด (Sensitive Data) หาก HR สแกนเก็บไว้โดยไม่ขีดฆ่าส่วนนี้ออก ต้องขอ **ความยินยอม (Consent)** เสมอ

## แบบติดตามผลการจัดการความเสี่ยง

ชื่อหน่วยงาน มหาวิทยาลัยราชภัฏกำแพงเพชร ประจำปีงบประมาณ 2569 ผลดำเนินงานรอบ 6 เดือน  
 ผู้รับผิดชอบหลัก รองอธิการบดีฝ่ายวิชาการ / ผอ. สำนักวิทยบริการฯ / ผอ. สำนักส่งเสริมฯ / ผอ. กองพัฒนานักศึกษา

( ) ด้านกลยุทธ์ (✓) ด้านการปฏิบัติงาน ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ  
 ( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับ ความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลา ดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงาน ของกิจกรรม (8)	ร้อยละความ คืบหน้า (9)	ปัญหา/ อุปสรรค (10)
<b>O1/การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.</b>	<b>(ปัจจัยภายนอก)</b> 1. ภัยคุกคามทางไซเบอร์ต่อมหาวิทยาลัย ซึ่งจะทำให้ข้อมูลถูกละเมิด  <b>(ปัจจัยภายใน)</b> 1. บุคลากรและนักศึกษาขาดความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) และกฎหมายที่เกี่ยวข้อง	KPI1 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคล (เป้าหมาย ร้อยละ 60)  KPI2 – ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ระดับดี)  KPI3 – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคล (เป้าหมาย อย่างน้อยร้อยละ 70)	16 สูงมาก	1. จัดตั้งคณะทำงานและผู้รับผิดชอบ	ปีงบประมาณ 2569	- รองอธิการบดีฝ่ายวิชาการ - ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ - ผอ.กองพัฒนานักศึกษา - รอง ผอ. สำนักวิทยบริการ - รอง ผอ. สำนักส่งเสริมฯ - อาจารย์ณฤชล เชื้อนยัง	<b>1. จัดตั้งคณะทำงานและผู้รับผิดชอบ</b> 1.1 คำสั่ง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO : Chief Information Office) ของมหาวิทยาลัยราชภัฏกำแพงเพชร 1.2 คำสั่ง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ของมหาวิทยาลัยราชภัฏกำแพงเพชร 1.3 คำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล  <a href="https://www.kpru.ac.th/km-web/files/command-pdpa2569.pdf">https://www.kpru.ac.th/km-web/files/command-pdpa2569.pdf</a>	ร้อยละ 100	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับ ความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลา ดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงาน ของกิจกรรม (8)	ร้อยละความ คืบหน้า (9)	ปัญหา/ อุปสรรค (10)
	<p>2. ผู้ควบคุม/ผู้ประมวลผล/เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)</p> <p>3. บุคลากรในมหาวิทยาลัยฯ นำข้อมูลไปใช้ผิดวัตถุประสงค์</p>	<p>KPI4 - ระดับความสำเร็จในการดำเนินการจัดการความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคล (เป้าหมาย 5 คะแนน)</p> <p>KPI5 - จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต (เป้าหมาย 0 ครั้ง)</p>		<p>2. ประชุมคณะกรรมการดำเนินงาน จัดทำนโยบาย วางแผนการดำเนินงาน</p>	<p>ปีงบประมาณ 2569</p>		<p><b>2. ประชุมกรรมการ</b></p> <p>2.1 ประชุมคณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล วันที่ 5 พฤศจิกายน 2568 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ</p> <p>2.2 ประชุมวางแผนการจัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล โดยแยกประเภทของผู้ที่มีหน้าที่และความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) วันที่ 21 กุมภาพันธ์ 2569 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ</p> <p>2.3 ประชุมทบทวนแผนการดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อกำหนดวันจัดกิจกรรมอบรม วันที่ 1 เมษายน</p>	<p>ร้อยละ 100</p> <p>ร้อยละ 100</p> <p>ร้อยละ 50</p>	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับ ความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลา ดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงาน ของกิจกรรม (8)	ร้อยละความ คืบหน้า (9)	ปัญหา/ อุปสรรค (10)
							2569 ณ ห้องสำนักงานศูนย์ภาษา อาคารศูนย์ภาษาและคอมพิวเตอร์ 2.4 กิจกรรมเสนอแผนการ ดำเนินงานตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) สำหรับผู้บริหาร (คณะกรรมการบริหารประจำ มหาวิทยาลัย) วันที่ 2 เมษายน 2569 ณ ห้องประชุมชั้น 8 อาคาร เรียนรวมและอำนวยการ (ตึก 14)	ร้อยละ 100	
				3. จัดอบรม/กิจกรรม สร้างความตระหนักรู้ ด้านความปลอดภัย ของข้อมูลส่วนบุคคล อย่างต่อเนื่อง โดยแยก ประเภทของผู้ที่มี หน้าที่และความ รับผิดชอบตาม พระราชบัญญัติ คุ้มครองข้อมูลส่วน บุคคล พ.ศ.2562 (PDPA)	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - ผอ.กองพัฒนานักศึกษา - รอง ผอ. สำนักวิทย บริการ - รอง ผอ. สำนักส่งเสริมฯ - อาจารย์ณฤชล เชื้อนัยัง - นางสาวอรปรียา คำแพง	3.1 กำหนดจัดกิจกรรมอบรมด้าน ความปลอดภัยของข้อมูลส่วน บุคคลและวัคซีนไซเบอร์นักศึกษา ชั้นปีที่ 1 วันปฐมนิเทศ วันที่ 27 พฤษภาคม 2569 เวลา 11.00 - 12.00 น. ณ อาคารที่ปิงกรังศรีมี โชติ 3.2 กำหนดจัดกิจกรรมอบรมด้าน ความปลอดภัยของข้อมูลส่วน บุคคลและวัคซีนไซเบอร์ สำหรับ บุคลากร มหาวิทยาลัยราชภัฏ กำแพงเพชร สายสนับสนุน วันที่ 5 มิถุนายน 2569 3.3 กำหนดจัดกิจกรรมอบรมด้าน ความปลอดภัยของข้อมูลส่วน บุคคลและวัคซีนไซเบอร์ สำหรับ	N/A  N/A  N/A	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับ ความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลา ดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงาน ของกิจกรรม (8)	ร้อยละความ คืบหน้า (9)	ปัญหา/ อุปสรรค (10)
							บุคลากร มหาวิทยาลัยราชภัฏ กำแพงเพชร สายวิชาการ (แยก ตามคณะ เดือนมิถุนายน 2569)		
				4. กำหนดให้เจ้าหน้าที่ ที่เกี่ยวข้องลงนามใน สัญญารักษาความลับ	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ. สำนักวิทย บริการฯ - อาจารย์นฤชล เชื้อนยัง - นางสาวอรปรียา คำแพ่ง	4.1 กำหนดจัดกิจกรรม (ร่าง) กรอบการจัดทำข้อตกลงการรักษา ความลับ (NDA) วันที่ 21 เมษายน 2569 ณ ห้องประชุมเล็กชั้น 4 อาคารเรียนรวมและอำนวยการ 4.2 กำหนดจัดกิจกรรมอบรมเชิง ปฏิบัติการผู้ประมวลผลข้อมูลและ ลงนามในสัญญารักษาความลับ (NDA) วันที่ 13 พฤษภาคม 2569	N/A  N/A	
				5. จัดกิจกรรม แลกเปลี่ยนเรียนรู้กลุ่ม บุคลากรตามคำสั่งฯ เพื่อให้การปฏิบัติงาน สอดคล้องกับ พระราชบัญญัติ คุ้มครองข้อมูลส่วน บุคคล พ.ศ.2562 (PDPA)	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ.สำนักวิทย บริการฯ - อาจารย์นฤชล เชื้อนยัง - นางสาวอรปรียา คำแพ่ง	5.1 กิจกรรมแลกเปลี่ยนเรียนรู้ แนวทางการจัดเก็บข้อมูลส่วน บุคคลในระบบสารสนเทศ สำหรับ Admin หน่วยงานภายใน มหาวิทยาลัย วันที่ 8 มกราคม 2569 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยี สารสนเทศ ผลการดำเนินงาน (1) มีการกำหนดแบบฟอร์มการ จัดเก็บข้อมูลส่วนบุคคลในระบบ สารสนเทศของทุกหน่วยงาน ภายในมหาวิทยาลัย	ร้อยละ 100	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับ ความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลา ดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงาน ของกิจกรรม (8)	ร้อยละความ คืบหน้า (9)	ปัญหา/ อุปสรรค (10)
							<p>(2) มีการกำหนดให้มีการแจ้ง วัตถุประสงค์ของการเก็บ ใช้ รวบรวม และเปิดเผยข้อมูล ส่วนบุคคล รวมถึงการขอความ ยินยอมในระบบสารสนเทศของ มหาวิทยาลัย</p> <p>5.2 กิจกรรมแลกเปลี่ยนเรียนรู้ แนวทางการบริหารจัดการข้อมูล ส่วนบุคคลในมหาวิทยาลัย Admin หน่วยงานภายในมหาวิทยาลัย วันที่ 27 กุมภาพันธ์ 2569 ณ ห้อง ประชุมดอกสัก สำนักวิทยบริการ และเทคโนโลยีสารสนเทศ</p> <p>ผลการดำเนินงาน</p> <p>(1) มีการตรวจสอบประเด็นความ เสี่ยง และความรับผิดชอบของ Admin ในการบริหารจัดการข้อมูล ส่วนบุคคล เพื่อนำไปปรับปรุง คำสั่งผู้ประมวลผลข้อมูลส่วน บุคคล</p> <p>(2) ได้แผนการดำเนินงานอบรมเชิง ปฏิบัติการสำหรับทีมแอดมิน ซึ่งจะ มุ่งเน้นการจำลองเหตุการณ์จริง (Case Study)</p>	ร้อยละ 100	
				6. สรุปผลการจัด กิจกรรม	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - อาจารย์นฤชล เชื้อนยัง	6.1 สรุปผลการจัดกิจกรรม แลกเปลี่ยนเรียนรู้การพัฒนา	N/A	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับ ความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลา ดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงาน ของกิจกรรม (8)	ร้อยละความ คืบหน้า (9)	ปัญหา/ อุปสรรค (10)
						- นางสาวอรปรียา คำแพง	เว็บไซต์ สำหรับ Admin (ไตรมาส1-2)		
				7. จัดทำมาตรการด้าน ความมั่นคงปลอดภัย ของข้อมูลส่วนบุคคล	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ. สำนักวิทย บริการฯ - อาจารย์นฤชล เชื้อนยัง - นางสาวอรปรียา คำแพง	7.1 จัดทำมาตรการแก้ไขปัญหา และแก้ไขสถานการณ์เบื้องต้นใน การระงับเหตุการณ์ละเมิดข้อมูลส่วน บุคคล สำหรับ Facebook Page หน่วยงานภายในมหาวิทยาลัย 7.2 จัดทำมาตรการเชิงเทคนิค สำหรับแอดมิน Facebook Page หน่วยงานภายในมหาวิทยาลัย 7.3 อยู่ระหว่างการจัดทำ (ร่าง) มาตรการด้านความมั่นคงปลอดภัย ของข้อมูลส่วนบุคคล และการ รักษาความมั่นคงปลอดภัยไซเบอร์	100  100  N/A	
				8. จัดทำแนว ปฏิบัติการรับมือเหตุ ละเมิดข้อมูลส่วน บุคคล และมีช่องทาง การร้องเรียน กรณีที่มี เหตุการณ์ละเมิดข้อมูล ส่วนบุคคล	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ. สำนักวิทย บริการฯ - อาจารย์นฤชล เชื้อนยัง - นางสาวอรปรียา คำแพง	8.1 กิจกรรมจัดทำ (ร่าง) แนว ปฏิบัติการรับมือเหตุละเมิดข้อมูล ส่วนบุคคล 8.2 จัดทำช่องทางกรรณการร้องเรียน กรณีที่มีเหตุการณ์ละเมิดข้อมูล ส่วนบุคคล	N/A  N/A	

## แบบสรุปผลการประเมินความเสี่ยงภายหลังการดำเนินการตามแผนบริหารความเสี่ยง

ชื่อหน่วยงาน.....มหาวิทยาลัยราชภัฏกำแพงเพชร..... ประจำปีงบประมาณ..... 2569..... รอบ..... 6..... เดือน

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลง ระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงาน ปิดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
01/การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.	4	4	16 สูง มาก	N/A	N/A	N/A	N/A	KPI1 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคล	ร้อยละ 60	- ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ - ผอ.กองพัฒนานักศึกษา	<input type="checkbox"/> บรรลุ <input checked="" type="checkbox"/> ไม่บรรลุ <u>ผลดำเนินงาน</u> กำหนดจัดกิจกรรมอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคลและวัคซีนไซเบอร์ สำหรับบุคลากรมหาวิทยาลัยราชภัฏกำแพงเพชร	-
								KPI2 – ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม	ระดับดี	- ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ - ผอ.กองพัฒนานักศึกษา - หัวหน้างาน บค.	<input type="checkbox"/> บรรลุ <input checked="" type="checkbox"/> ไม่บรรลุ <u>ผลดำเนินงาน</u> กำหนดจัดกิจกรรมอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคลและวัคซีนไซเบอร์ สำหรับบุคลากรมหาวิทยาลัยราชภัฏกำแพงเพชร	-
								KPI3 - ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้าน	ร้อยละ 70	- ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ	<input type="checkbox"/> บรรลุ <input checked="" type="checkbox"/> ไม่บรรลุ <u>ผลดำเนินงาน</u> กำหนดจัดอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคล	-

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลง ระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงาน ปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
								ความปลอดภัย ของข้อมูลส่วนบุคคล		- ผอ.กองพัฒนา นักศึกษา	และวัคซีนไซเบอร์สำหรับ นักศึกษาชั้นปีที่ 1 วันพุธนิเทศ วันที่ 27 พฤษภาคม 2569 เวลา 11.00 - 12.00 น. ณ อาคารที่ปิงกรรัศมีโชติ	
								KPI4 – ระดับ ความสำเร็จใน การดำเนินการ จัดการความ เสี่ยงด้านการ ละเมิดข้อมูล ส่วนบุคคล <u>เกณฑ์การให้ คะแนน</u> คะแนน 1 : มี การจัดตั้ง คณะทำงานและ ผู้รับผิดชอบ คะแนน 2 : มี การประชุม คณะกรรมการ ดำเนินงาน จัดทำ นโยบาย วาง	5 คะแนน	- ผอ.สำนักวิทย บริการฯ - DPO นิติกรและ คณะทำงาน	<input type="checkbox"/> บรรลุ <input checked="" type="checkbox"/> ไม่บรรลุ <u>ผลดำเนินงาน</u> ผลการดำเนินงาน รอบ 6 เดือน ปฏิบัติตามเกณฑ์ได้ 2 คะแนน ดังนี้ <b>1. จัดตั้งคณะทำงานและ ผู้รับผิดชอบ</b> 1.1 มีคำสั่ง แต่งตั้งผู้บริหาร เทคโนโลยีสารสนเทศระดับสูง (CIO: Chief Information Office) ของมหาวิทยาลัย ราชภัฏกำแพงเพชร 1.2 มีคำสั่ง แต่งตั้งเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ของมหาวิทยาลัยราชภัฏ กำแพงเพชร	-

ความเสี่ยง	ระดับความเสี่ยง			การเปลี่ยนแปลง ระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงาน ปีถัดไป	
	ก่อนการประเมิน		หลังการประเมิน		KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์		
					แผนการดำเนินงาน คะแนน 3 : มี การจัดอบรม/ กิจกรรมสร้าง ความตระหนักรู้ ด้านความ ปลอดภัยของ ข้อมูลส่วนบุคคล และกำหนดให้ เจ้าหน้าที่ที่ เกี่ยวข้องลงนาม ในสัญญารักษา ความลับ คะแนน 4 : มี การจัดกิจกรรม แลกเปลี่ยนเรียนรู้ (KM) ระหว่าง บุคลากร เพื่อให้ การปฏิบัติงาน สอดคล้องกับ PDPA จัดทำ มาตรการด้าน ความมั่นคง				<p>1.3 มีคำสั่ง แต่งตั้ง คณะกรรมการดำเนินงานและ กำกับการใช้ข้อมูลส่วนบุคคล</p> <p><b>2. ประชุมกรรมการ</b></p> <p>2.1 ประชุมคณะกรรมการ ดำเนินงานและกำกับการใช้ ข้อมูลส่วนบุคคล วันที่ 5 พฤศจิกายน 2568 ณ ห้อง ประชุมดอกสัก สำนักวิทย บริการและเทคโนโลยี สารสนเทศ</p> <p>2.2 ประชุมทบทวนแผนการ ดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อกำหนดวัน จัดกิจกรรมอบรม วันที่ 1 เมษายน 2569 ณ ห้อง สำนักงานศูนย์ภาษาอาคารศูนย์ ภาษาและคอมพิวเตอร์</p> <p>2.3 กิจกรรมเสนอแผนการ ดำเนินงานตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) สำหรับผู้บริหาร</p>	

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลง ระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงาน ปีถัดไป	
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์		
								ปลอดภัยของ ข้อมูลส่วนบุคคล สรุปผลการจัด กิจกรรม และ รายงานผลการ ดำเนินงานต่อ ผู้บริหาร คะแนน 5 : มี การจัดทำแนว ปฏิบัติการรับมือ เหตุละเมิดข้อมูล ส่วนบุคคลและ ช่องทางการ ร้องเรียน				(คณะกรรมการบริหารประจำ มหาวิทยาลัย) วันที่ 2 เมษายน 2569 ณ ห้องประชุมชั้น 8 อาคารเรียนรวมและอำนวยการ (ตึก 14)	
								KPI5 - จำนวน ครั้งข้อมูลส่วน บุคคลที่ มหาวิทยาลัย จัดเก็บ ถูกนำไป เผยแพร่โดยไม่ได้ รับอนุญาต	0 ครั้ง	- ผอ.สำนักวิทย บริการฯ - ผอ.สำนัก ส่งเสริมฯ	<input checked="" type="checkbox"/> บรรลุ <input type="checkbox"/> ไม่บรรลุ <u>ผลดำเนินงาน</u> การดำเนินงานภาพรวม รอบ 6 เดือน ข้อมูลส่วนบุคคล ที่มหาวิทยาลัยจัดเก็บ <u>ไม่มี</u> กรณีถูกนำไปเผยแพร่โดยไม่ได้ รับอนุญาต	-	