รายงานผลการดำเนินการจัดการความรู้ ประจำปีการศึกษา 2568
ด้านการวิจัย/ด้านการเรียนการสอน/ด้านพันธกิจอื่น

เรื่อง แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏกำแพงเพชร

1. ชื่อแผนการจัดการความรู้

แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA Risk Zero)

2. ผู้รับผิดชอบ

นางสาวอรปรียา คำแพ่ง
นางสาวสรัลชนา น้ำเงินสกุณี
และบุคลากร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

3. หลักการและเหตุผล

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

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

4. วัตถุประสงค์

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

5. ผู้เข้าร่วมโครงการ

บุคลากรสายสนับสนุน และแอดมิน (Admin) ผู้ดูแลระบบ มหาวิทยาลัยราชภัฏกำแพงเพชร

6.สถานที่ดำเนินการ

มหาวิทยาลัยราชภัฏกำแพงเพชร

7. วิธีดำเนินงาน (แผนการจัดการความรู้ 6 ขั้นตอน)

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

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

8. ผลการดำเนินงานตามแผนการจัดการความรู้ 6 ขั้นตอน

1. กำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร

กิจกรรมที่ 1 จัดตั้งคณะทำงาน

1.1 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการวิเคราะห์ความเสี่ยงและการควบคุมภายใน สั่ง ณ วันที่ 20 ตุลาคม 2568

1.2 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการจัดการความรู้ ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ สั่ง ณ วันที่ 31 ตุลาคม 2568

1.3 คำสั่งมหาวิทยาลัยราชภัฏกำแพงเพชร เรื่อง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร สั่ง ณ วันที่ 12 พฤศจิกายน 2568

1.4 คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล สั่ง ณ วันที่ 22 พฤศจิกายน 2568

กิจกรรมที่ 2 ประชุมกรรมการ

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

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

2. การเสาะหาความรู้ที่ต้องการ

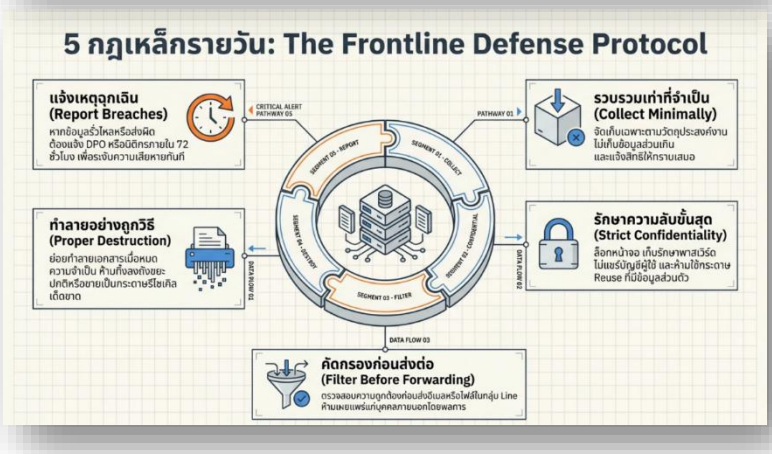
<u>กิจกรรมที่ 3</u> รวบรวมความรู้จากแหล่งต่าง ๆ ทั้งภายในและภายนอก คณะทำงานได้รวบรวมและศึกษาข้อกำหนด PDPA, แนวทางปฏิบัติจาก DGA และตัวอย่าง Best Practice การลดความเสี่ยงและป้องกันการละเมิดข้อมูลส่วนบุคคลจากหน่วยงานที่ประสบความสำเร็จ ได้แก่ คู่มือแนวทางการประเมินความเสี่ยง และแจ้งเหตุการณ์ละเมิดข้อมูล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

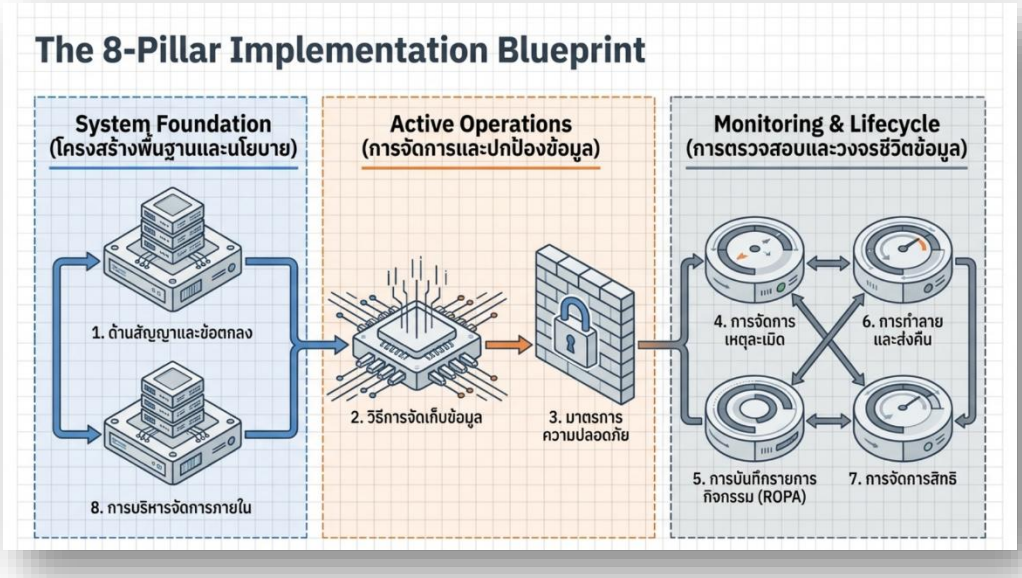
นอกจากนี้ได้อบรมออนไลน์ หลักสูตรการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) จำนวน 3 ชั่วโมง เพื่อนำชุดความรู้มาปรับปรุงให้เหมาะสมกับงาน การอบรมดังกล่าวจะได้รับประกาศนียบัตร

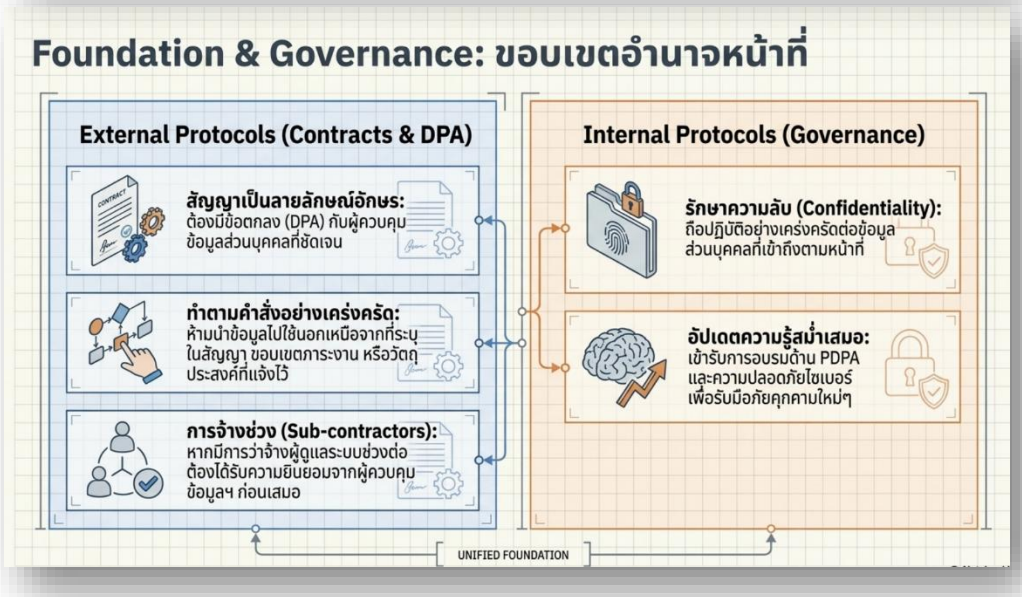
3. ปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน โดยการนำความรู้ที่ได้มาปรับให้เหมาะสมกับบริบทของมหาวิทยาลัย

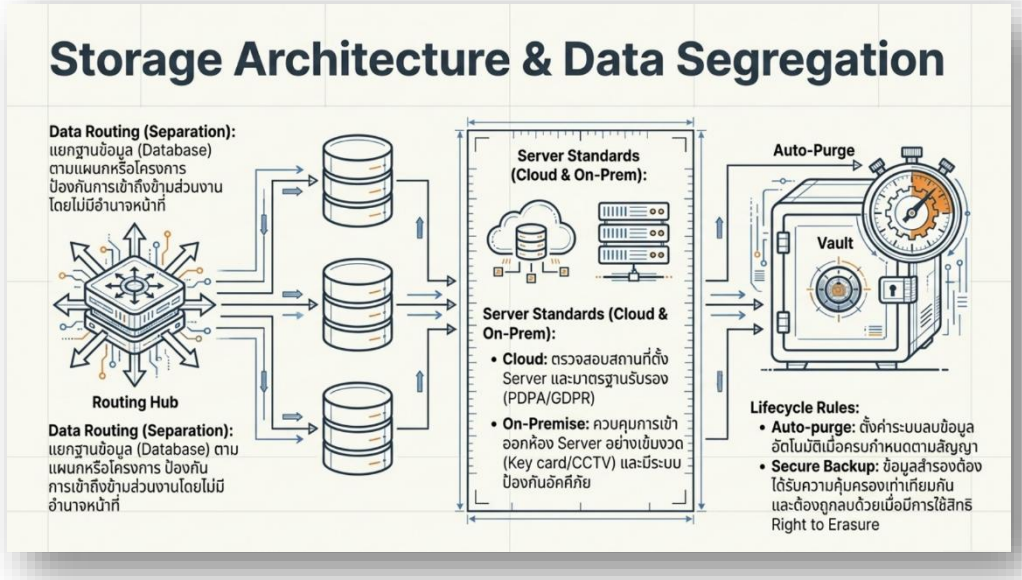
<u>กิจกรรมที่ 4</u> จัดทำเครื่องมือ/แนวทางปฏิบัติ เช่น คู่มือ, Checklist การใช้งานระบบที่ต้องระบุตัวตน หรือ Infographic สรุปข้อปฏิบัติของบุคลากร ทำให้ความรู้ PDPA ที่ซับซ้อนกลายเป็นเครื่องมือที่ใช้งานง่าย

(1) PDPA Master Checklist for IT Admins เช็กลิสต์และข้อปฏิบัติเชิงเทคนิคเพื่อการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล



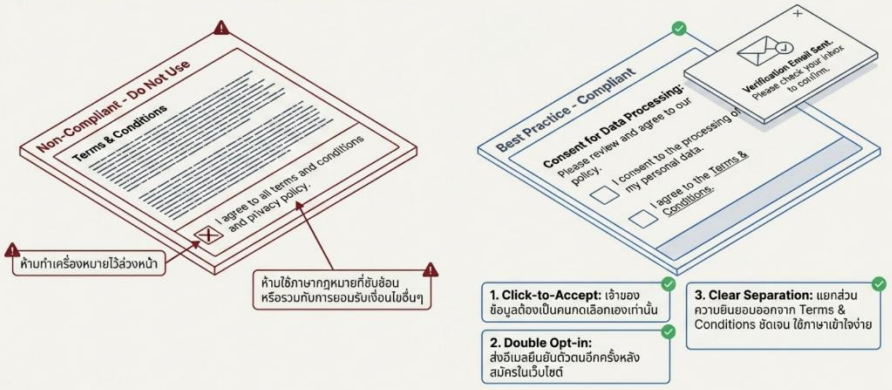

The 8-Pillar Implementation Blueprint
System Foundation
(โครงสร้างพื้นฐานและนโยบาย)
Active Operations
(การจัดการและปกป้องข้อมูล)
Monitoring & Lifecycle
(การตรวจสอบและวงจรชีวิตข้อมูล)
1. ด้านสัญญาและข้อตกลง
8. การบริหารจัดการภายใน
2. วิธีการจัดเก็บข้อมูล
3. มาตรการ
ความปลอดภัย
4. การจัดการ
เหตุละเมิด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


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

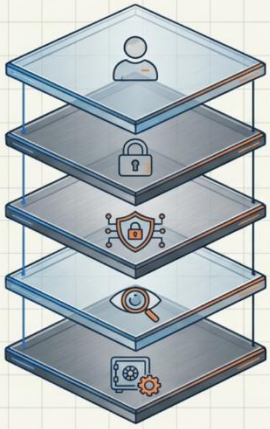

Storage Architecture & Data Segregation
Data Routing (Separation):
แยกฐานข้อมูล (Database)
ตามแผนกหรือโครงการ
ป้องกันการเข้าถึงข้ามส่วนงาน
โดยไม่มีอำนาจหน้าที่
Routing Hub
Data Routing (Separation):
แยกฐานข้อมูล (Database) ตาม
แผนกหรือโครงการ ป้องกัน
การเข้าถึงข้ามส่วนงานโดยไม่มี
อำนาจหน้าที่
Server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

Legal Consent Mechanisms in UI/UX

รูปแบบการขอความยินยอมที่ถูกต้องตามกฎหมาย



The Security Measures Framework (SOC Stack)



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

Active Monitoring: Breach Incident SOP & ROPA

Data Breach Management (SOP)

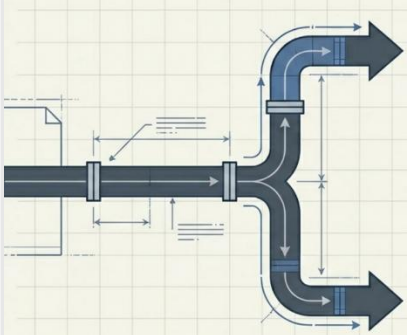
Detect → Alert → Report → 72 HOURS

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

Record of Processing (ROPA)

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

Data Lifecycle Management & Subject Rights

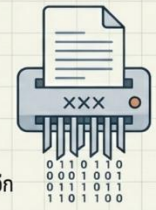


การจัดการสิทธิ
(Data Subject Rights Readiness):

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

การทำลายและส่งคืน
(Retention & Disposal):

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



The Data Asset Radar

หมวดหมู่ข้อมูลที่ระบบ IT ต้องควบคุมดูแล

Quadrant 1: Digital Footprints
(ร่องรอยดิจิทัล)

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

Quadrant 2: Identity & Profile
(ข้อมูลระบุตัวตนบุคคล)

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

Quadrant 3: Behavioral & Commercial
(พฤติกรรมและการทำธุรกรรม)

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

Quadrant 4: Highly Sensitive
(ข้อมูลอ่อนไหว - ควบคุมพิเศษ)

ข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data) ต้องใช้มาตรการขั้นสูงสุดและบันทึก ROPA เสมอ.

ROPA

Self-Audit Diagnostic Matrix

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

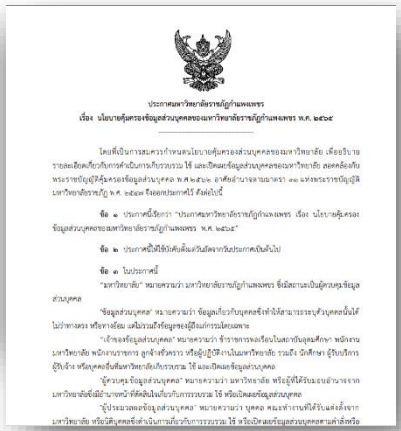
สถานะของระบบ IT ในปัจจุบันของคุณเป็นอย่างไร? นำเช็กลิสต์นี้ไปใช้ประเมินทันที

NotebookLM

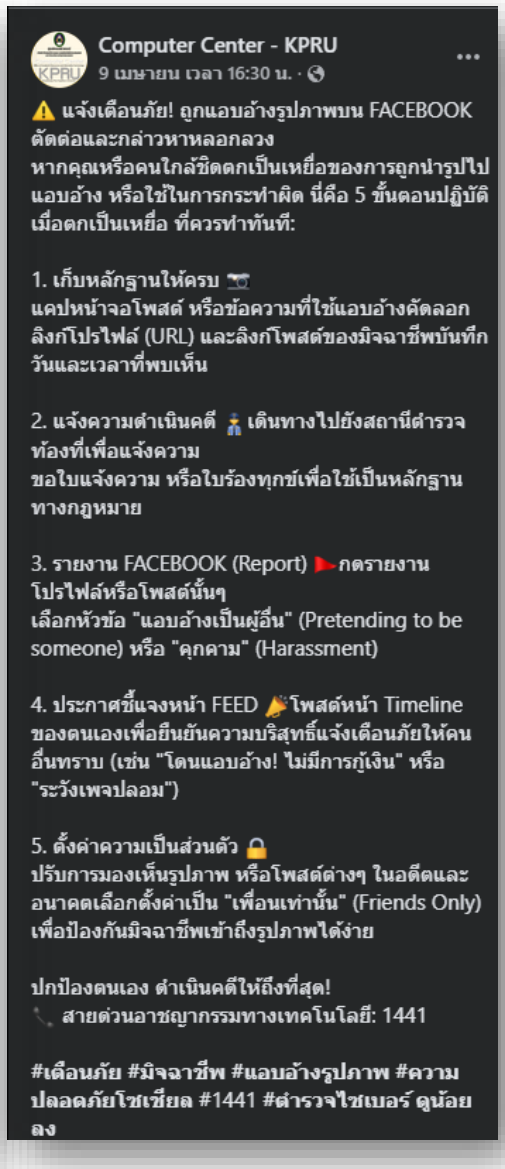
(2) สร้างกลไกการรับรู้นโยบายการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

โดยเผยแพร่ **ประกาศ นโยบายคุ้มครองข้อมูลส่วนบุคคล** ประชาสัมพันธ์ไว้ที่หน้าหลักเว็บไซต์มหาวิทยาลัยราชภัฏกำแพงเพชร ดังภาพ

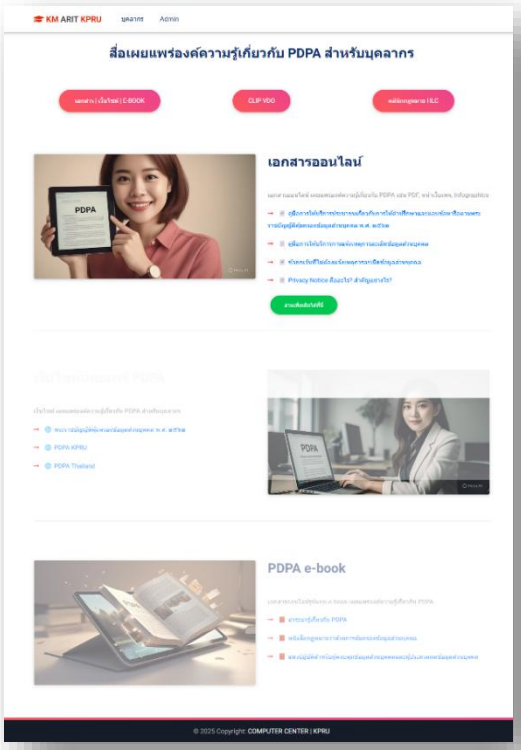
เมื่อคลิกอ่านนโยบาย จะแสดงหน้าเว็บไซต์ PDPA รวบรวมข้อมูลที่เกี่ยวข้อง ดังลิงค์ https://kpru.ac.th/pdpa/

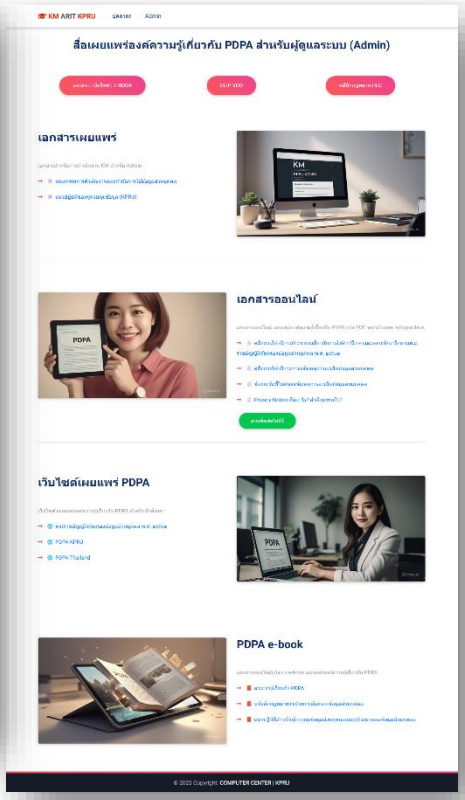


(3) จัดทำ Infographic แนวปฏิบัติ แผนผังขั้นตอน และอื่นๆที่เกี่ยวข้อง เผยแพร่ผ่านเว็บไซต์มหาวิทยาลัย และ เพจ ศูนย์คอมพิวเตอร์

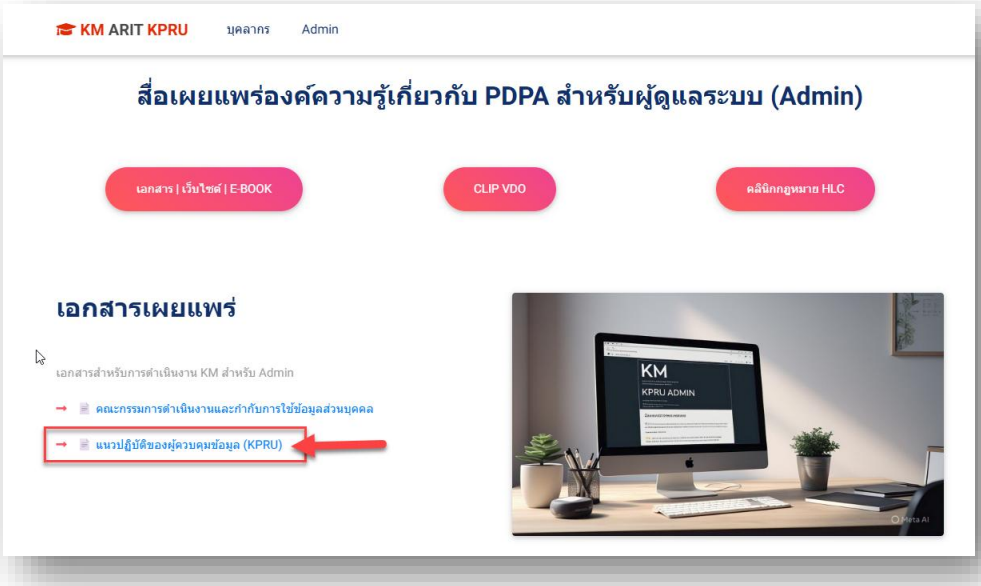


(4) เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผ่านสื่อส่งเสริมการเรียนรู้ PDPA แยกตามประเภทผู้ใช้

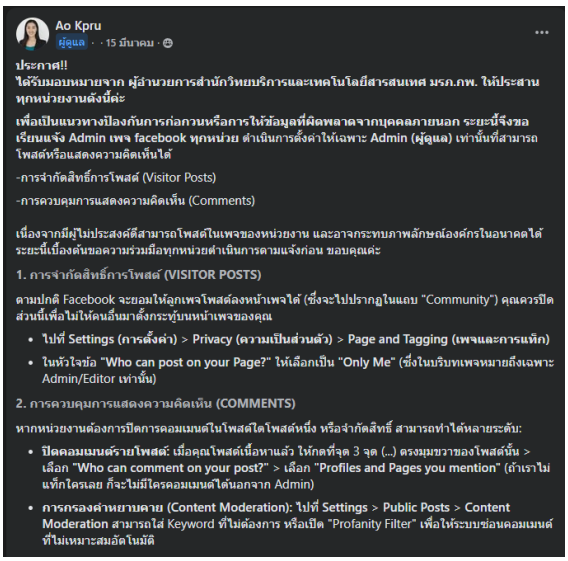




สำหรับกลุ่ม Admin เผยแพร่แนวปฏิบัติของผู้ควบคุมข้อมูล (KPRU)



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



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

<u>รายงานสถานการณ์และการตรวจพบเหตุละเมิด</u>

ตามที่ปรากฏเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของบุคลากรและบุคคลภายนอก เมื่อวันที่ 15 มีนาคม 2569 โดยมีพฤติการณ์การกระทำความผิด ดังนี้

- ลักษณะการกระทำ มีการนำรูปภาพของบุคลากรและบุคคลภายนอกไปตัดต่อโดยไม่ได้รับอนุญาต เพื่อสร้างสื่อบิดเบือนข้อเท็จจริงในลักษณะการทวงหนี้ และกล่าวหาว่าเป็นส่วนหนึ่งของขบวนการฉ้อโกง

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

<u>การดำเนินการโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)</u>

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

- การรายงานเหตุ รายงานสรุปเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อผู้บริหารระดับสูง (อธิการบดี/รองอธิการบดี) เพื่อทราบสถานการณ์

- การแจ้งเหตุต่อหน่วยงานกำกับดูแล ดำเนินการจัดทำหนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายในกรอบเวลา 72 ชั่วโมงตามที่กฎหมายกำหนด

- การเยียวยาผู้ได้รับผลกระทบ จัดทำบันทึกแจ้งเหตุให้แก่ผู้ที่ได้รับผลกระทบโดยตรง พร้อมให้คำแนะนำในการปฏิบัติตนและการคุ้มครองสิทธิ์รายบุคคล

<u>มาตรการตอบโต้ทางเทคนิคและทางกฎหมาย (สำนักวิทยบริการฯ)</u>

เพื่อให้เกิดการแก้ไขที่ต้นเหตุและป้องกันการขยายตัวของความเสียหาย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการ ดังนี้

- การรวบรวมพยานหลักฐาน เก็บรวบรวมหลักฐานทางดิจิทัลทั้งหมด และมอบหมายให้ผู้ดูแลเพจดำเนินการแจ้งความลงบันทึกประจำวันไว้เป็นหลักฐานทางกฎหมาย

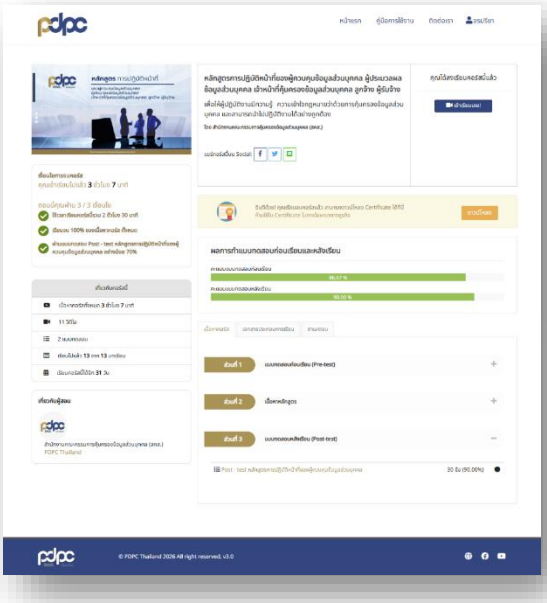
- มาตรการป้องกันเชิงรุกสำหรับทุกหน่วยงาน ประสานงานเครือข่ายผู้ดูแล (Admin) Facebook Page ทุกหน่วยงานภายในมหาวิทยาลัย ให้ยกระดับการตั้งค่าความปลอดภัย ดังนี้

1. จำกัดสิทธิ์การโพสต์ ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง (Disable Visitor Posts)

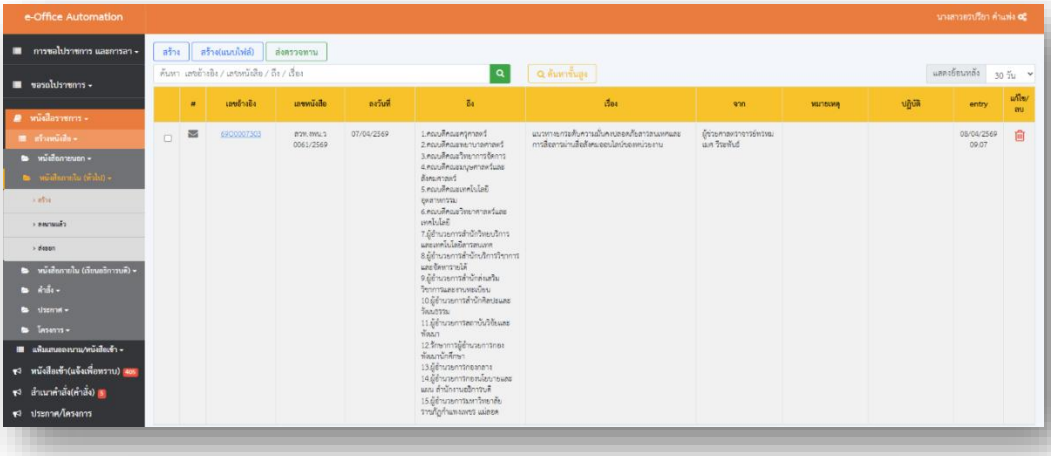
2. ยกระดับการคัดกรอง เปิดใช้งานเครื่องมือ Moderation Assist และตั้งค่าการคัดกรองความคิดเห็น (Comment Filtering) เพื่อซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญ (Keywords) ที่เกี่ยวข้องกับการบิดเบือนข้อมูล โดยอัตโนมัติ

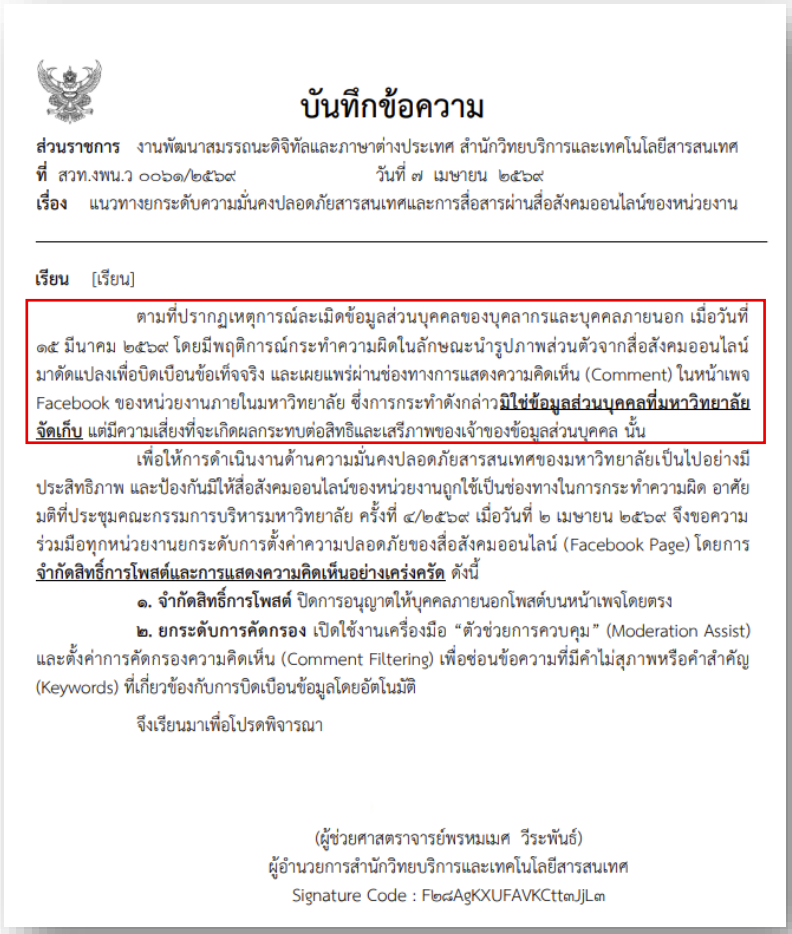
จึงเรียนที่ประชุมทราบแนวทางการจัดการเหตุละเมิด และขอความร่วมมือทุกหน่วยงานตรวจสอบและรักษามาตรฐานการตั้งค่าสื่อสังคมออนไลน์โดยการ**<u>จำกัดสิทธิ์การโพสต์และการแสดงความคิดเห็นอย่างเคร่งครัด</u>** ทั้งนี้ สำนักวิทยบริการฯ ได้ดำเนินการจัดส่งบันทึกข้อความแจ้งเวียนไปในระบบ E-Office วันที่ 7 เมษายน 2569

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



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





บันทึกข้อความ

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

เรียน [เรียน]

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

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

๑. จำกัดสิทธิ์การโพสต์ ปิดการอนุญาตให้บุคคลภายนอกโพสต์บนหน้าเพจโดยตรง

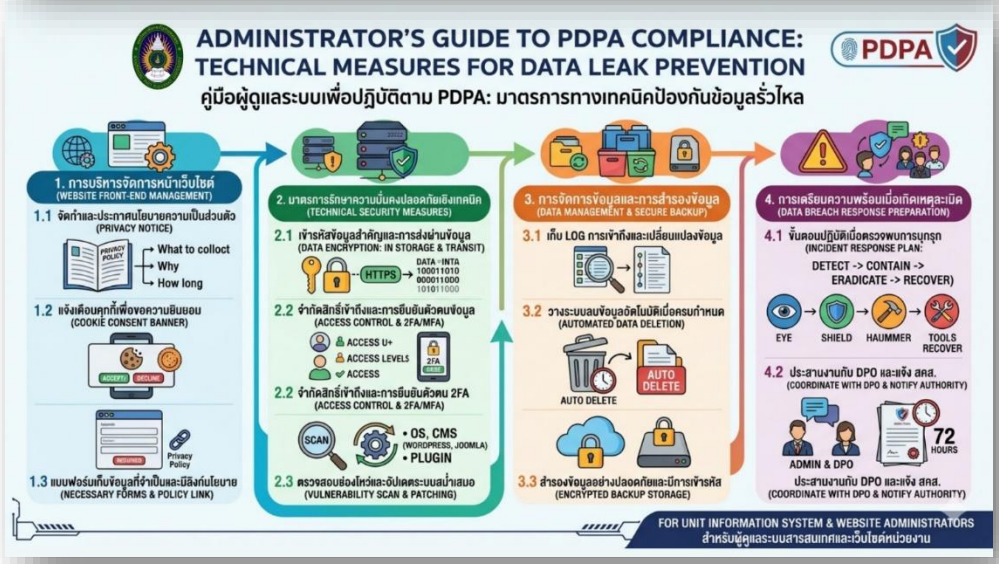
๒. ยกระดับการคัดกรอง เปิดใช้งานเครื่องมือ “ตัวช่วยการควบคุม” (Moderation Assist) และตั้งค่าการคัดกรองความคิดเห็น (Comment Filtering) เพื่อซ่อนข้อความที่มีคำไม่สุภาพหรือคำสำคัญ (Keywords) ที่เกี่ยวข้องกับการบิดเบือนข้อมูลโดยอัตโนมัติ

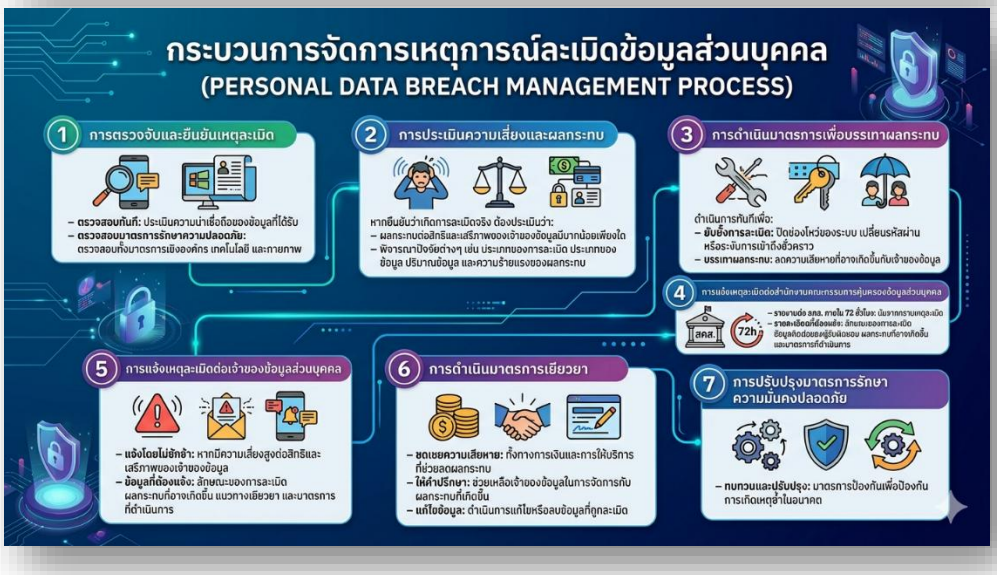
จึงเรียนมาเพื่อโปรดพิจารณา

(ผู้ช่วยศาสตราจารย์พรหมเมศ วีระพันธ์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
Signature Code : F๒๘AgKXUFAVKCttฅJjLฅ

จากบันทึกข้อความข้างต้น เหตุการณ์ละเมิดข้อมูลส่วนบุคคลในวันดังกล่าว มิใช่ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ **จึงสรุปได้ว่า ไม่มีการได้รับรายงานการละเมิดข้อมูลส่วนบุคคล**

(10) Infographic อื่นๆที่เกี่ยวข้อง






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


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


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

(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 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) **ภายใน 72 ชั่วโมง** นับแต่ทราบเหตุ	แจ้งเหตุยกเว้นการละเมิดพร้อมหลักฐานประกอบต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เพื่อให้ สคส. พิจารณา

หากประเมินแล้วพบว่า มีความเสี่ยงสูง ที่จะกระทบต่อสิทธิและเสรีภาพ ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบด้วยโดยไม่ชักช้า

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

แผนผัง (Flowchart) กระบวนการในการปฏิบัติงานกรณีที่มีการละเมิดข้อมูลส่วนบุคคล

แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล (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 ไม่สามารถชดใช้ได้ ไม่สามารถทำงานได้ ได้รับผลกระทบทางจิตใจหรือร่างกาย หรือทำให้ถึงขั้นเสียชีวิต
4 - สูง	ได้รับผลกระทบที่มีนัยสำคัญ ซึ่งมีปัญหา- ความยุ่งยากต่อเจ้าของข้อมูลส่วนบุคคล แต่สามารถแก้ไขปัญหาได้ เช่น ถูกยักยอกเงิน 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 จดบันทึกและรายงานเหตุละเมิดต่อผู้บริหาร/รายไตรมาส

ข้อกำหนดการแจ้งเหตุละเมิด

ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลนั้นแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง เว้นแต่การละเมิดดังกล่าวไม่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีความเสี่ยงสูงที่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งการละเมิดให้เจ้าของข้อมูลทราบพร้อมแนวทางเยียวยา

4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล ผู้ดูแลระบบสารสนเทศ เจ้าหน้าที่ IT

- หาสาเหตุและดำเนินการป้องกัน ระงับเหตุ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที เท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม (ควรซึ่งได้รับการอนุมัติจากผู้บริหาร พร้อมระบุระยะเวลาในการดำเนินการที่แน่นอน)
- ทบทวน ปรับปรุงมาตราการรักษาความปลอดภัยของข้อมูลให้รัดกุม
- หากการรั่วไหลของข้อมูลส่วนบุคคล ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (ในระดับ 2-5) DPO ต้องส่งเรื่องไปยังผู้บริหารที่เกี่ยวข้องทราบภายในระยะเวลาที่รวดเร็ว
- ผู้เกี่ยวข้องทุกฝ่าย รวมถึงผู้บริหาร ร่วมกำหนด**แนวทางเยียวยา**
- หามาตรการบรรเทาผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลอย่างเร่งด่วน

5. ผู้ควบคุมข้อมูล/เจ้าหน้าที่คุ้มครองข้อมูลแจ้งเหตุละเมิด ต่อ สคส. และเจ้าของข้อมูลส่วนบุคคล

6. ผู้เกี่ยวข้องทุกฝ่าย ทบทวนแนวทางการรับมือและหาวิธีการป้องกันไม่ให้เกิดซ้ำอีก

(12) ตัวอย่างการประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

ตัวอย่างเหตุการณ์ละเมิดข้อมูลส่วนบุคคลจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) นี้เป็นแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล ว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าว ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

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

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
4	ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูล ส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้และการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง นอกจากนี้ยังอาจก่อให้เกิดความเสียหายต่อธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงตัวเจ้าของข้อมูลส่วนบุคคลจึงต้องแจ้งเหตุ
5	ธนาคารได้รับการติดต่อจากลูกค้าธนาคาร 1 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้วภายใน 24 ชั่วโมง พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน 10 ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล 10 ราย ที่ถูกเรียกเก็บเงินตาม ใบแจ้งหนี้ของธนาคาร	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตามคณะ ส่วนงาน หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม
6	ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาผู้ควบคุมข้อมูลส่วนบุคคลถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลรายชื่อผู้ใช้บริการ รหัสผ่าน และประวัติการซื้อสินค้าถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต	ต้องแจ้ง	ต้องแจ้งลูกค้าของผู้ควบคุมข้อมูลส่วนบุคคลในส่วนที่มีข้อมูลรั้วไหลบน อินเทอร์เน็ต	ข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
7	เว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลเกิดปัญหาอผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง 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 เนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิดหรือมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าวรวมถึงข้อมูลสุขภาพด้วย เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุและตรวจสอบข้อมูลเพิ่มเติม
9	โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าวไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งผู้รับเหมาอาจจะนำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
10	บริษัทแห่งหนึ่งทำการตลาดแบบตรง โดยการส่งข้อมูล	ต้องแจ้ง เนื่องจากเป็นการส่งข้อมูล	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลใน	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
	ส่วนบุคคลไปยังผู้รับข้อมูลแต่ละราย แต่ด้วยความผิดพลาด จึงมีการใส่ที่อยู่ของบุคคลที่รับอีเมลทั้ง 100 คน เข้าไปในช่อง To หรือ Cc ทำให้ผู้รับอีเมลเห็นอีเมลที่มีข้อมูลส่วนบุคคลของบุคคลอื่น	ของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก จึงจำเป็นต้องแจ้งเหตุ แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ	อีเมลดังกล่าวอาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลภายหลังได้	หรือไม่ อาจขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไปและลักษณะของข้อมูลด้วยหากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด อาจถือว่ามีความเสี่ยงต่ำไม่จำเป็นต้องแจ้งเหตุ

หมายเหตุ ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลทั้ง 10 ตัวอย่าง ดังกล่าวข้างต้น เป็นเพียงแนวทางในการประเมินความสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณี 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 กุมภาพันธ 2569 เวลา 09.00 น. ณ ห้องประชุมดอกสัก เพื่อแนะนำเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย และวางแผนจัดอบรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล สำหรับผู้ที่มีหน้าที่และความรับผิดชอบตามกฎหมาย PDPA


5. นำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด“ขุมความรู้” ออกมาบันทึกไว้ เป็นการสรุปบทเรียนจากการใช้งานจริง

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


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

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

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

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

9. ประโยชน์ที่คาดว่าจะได้รับ

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

2. บุคลากรสายสนับสนุนของมหาวิทยาลัย สามารถนำความรู้ที่ได้ไปใช้ในการทำงาน ทำให้การคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องปกติของทุกๆ กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

3. ได้แนวปฏิบัติและเว็บไซต์เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากร มหาวิทยาลัยราชภัฏกำแพงเพชร

10. องค์ความรู้

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

11. การนำองค์ความรู้หรือแนวปฏิบัติที่ดีไปใช้

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	- **On-Premise** หน่วยงานเป็นผู้ควบคุมทั้งหมด เช่น Server ห้อง Data Center ของหน่วยงาน (ระบุชั้น/ตึก) **- Cloud Service** เช่น AWS (Region Singapore), Google Workspace หรือ Azure **- Backup Device** สำรองข้อมูลด้วยอุปกรณ์ใดบ้าง เช่น ฮาร์ดดิสก์ไดรฟ์ (HDD), โซลิดสเตทไดรฟ์ (SDD) หรือ External Drive ที่เก็บไว้ในตู้เซฟ ฯลฯ
การบันทึก Log ตาม พรบ. คอมพิวเตอร์	IP Address, หมายเลขเครื่อง (MAC), ประวัติการเข้าเว็บ, วันเวลาใช้งาน	**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)

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

แบบ RM-4

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)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
O1/การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.	**(ปัจจัยภายนอก)** 1. ภัยคุกคามทางไซเบอร์ต่อมหาวิทยาลัย ซึ่งจะทำให้ข้อมูลถูกละเมิด **(ปัจจัยภายใน)** 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 - อาจารย์นฤชล เขื่อนยัง	**1. จัดตั้งคณะทำงานและผู้รับผิดชอบ** 1.1 คำสั่ง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO : Chief Information Office) ของมหาวิทยาลัยราชภัฏกำแพงเพชร 1.2 คำสั่ง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ของมหาวิทยาลัยราชภัฏกำแพงเพชร 1.3 คำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล https://www.kpru.ac.th/km-web/files/command-pdpa2569.pdf	ร้อยละ 100	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
	2. ผู้ควบคุม/ผู้ประมวลผล/เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) 3. บุคลากรในมหาวิทยาลัยฯ นำข้อมูลไปใช้ผิดวัตถุประสงค์	**KPI4** – ระดับความสำเร็จในการดำเนินการจัดการความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคล (เป้าหมาย 5 คะแนน) **KPI5** - จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต (เป้าหมาย 0 ครั้ง)		2. ประชุมคณะกรรมการดำเนินงาน จัดทำนโยบาย วางแผนการดำเนินงาน	ปีงบประมาณ 2569		**2. ประชุมกรรมการ** 2.1 ประชุมคณะกรรมการจัดการความรู้ และคณะกรรมการความเสี่ยงสำนักฯ ทบทวนแผนการจัดการความรู้ และร่วมกันวิเคราะห์ความเสี่ยง เพื่อระบุ 3 อันดับความเสี่ยงที่มีโอกาสทำให้ข้อมูลรั่วไหล วันที่ 5 พฤศจิกายน 2568 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ 2.2 ประชุมวางแผนการจัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล โดยแยกประเภทของผู้ที่มีหน้าที่และความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) วันที่ 21 กุมภาพันธ์ 2569 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ 2.3 ประชุมทบทวนแผนการดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อกำหนดวันจัดกิจกรรมอบรม วันที่ 1 เมษายน	ร้อยละ 100 ร้อยละ 100 ร้อยละ 50	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
							2569 ณ ห้องสำนักงานศูนย์ภาษา อาคารศูนย์ภาษาและคอมพิวเตอร์ 2.4 กิจกรรมเสนอแผนการดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) สำหรับผู้บริหาร (คณะกรรมการบริหารประจำมหาวิทยาลัย) วันที่ 2 เมษายน 2569 ณ ห้องประชุมชั้น 8 อาคารเรียนรวมและอำนวยการ (ตึก 14)	ร้อยละ 100	
				3. จัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคลอย่างต่อเนื่อง โดยแยกประเภทของผู้ที่มีหน้าที่และความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - ผอ.กองพัฒนานักศึกษา - รอง ผอ. สำนักวิทยบริการ - รอง ผอ. สำนักส่งเสริมฯ - อาจารย์นฤชล เขื่อนยัง - นางสาวอรปรียา คำแพ่ง	3.1 กำหนดจัดกิจกรรมอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคลและวัคซีนไซเบอร์นักศึกษาชั้นปีที่ 1 วันปฐมนิเทศ วันที่ 27 พฤษภาคม 2569 เวลา 11.00 - 12.00 น. ณ อาคารทีปังกรรัศมีโชติ 3.2 กำหนดจัดกิจกรรมอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคลและวัคซีนไซเบอร์ สำหรับบุคลากร มหาวิทยาลัยราชภัฏกำแพงเพชร สายสนับสนุน วันที่ 5 มิถุนายน 2569 3.3 กำหนดจัดกิจกรรมอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคลและวัคซีนไซเบอร์ สำหรับ	N/A N/A N/A	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
							บุคลากร มหาวิทยาลัยราชภัฏกำแพงเพชร สายวิชาการ (แยกตามคณะ เดือนมิถุนายน 2569)		
				4. กำหนดให้เจ้าหน้าที่ที่เกี่ยวข้องลงนามในสัญญารักษาความลับ	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ. สำนักวิทยบริการฯ - อาจารย์นฤชล เขื่อนยัง - นางสาวอรปรียา คำแพ่ง	4.1 กำหนดจัดกิจกรรม (ร่าง) กรอบการจัดทำข้อตกลงการรักษาความลับ (NDA) วันที่ 21 เมษายน 2569 ณ ห้องประชุมเล็กชั้น 4 อาคารเรียนรวมและอำนวยการ 4.2 กำหนดจัดกิจกรรมอบรมเชิงปฏิบัติการผู้ประมวลผลข้อมูลและลงนามในสัญญารักษาความลับ (NDA) วันที่ 13 พฤษภาคม 2569	N/A N/A	
				5. จัดกิจกรรมแลกเปลี่ยนเรียนรู้กลุ่มบุคลากรตามคำสั่งฯ เพื่อให้การปฏิบัติงานสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ.สำนักวิทยบริการฯ - อาจารย์นฤชล เขื่อนยัง - นางสาวอรปรียา คำแพ่ง	5.1 กิจกรรมแลกเปลี่ยนเรียนรู้แนวทางการจัดเก็บข้อมูลส่วนบุคคลในระบบสารสนเทศ สำหรับ Admin หน่วยงานภายในมหาวิทยาลัย วันที่ 8 มกราคม 2569 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ผลการดำเนินงาน (1) มีการกำหนดแบบฟอร์มการจัดเก็บข้อมูลส่วนบุคคลในระบบสารสนเทศของทุกหน่วยงานภายในมหาวิทยาลัย	ร้อยละ 100	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
							(2) มีการกำหนดให้มีการแจ้งวัตถุประสงค์ของการเก็บ ใช้ รวบรวม และเปิดเผยข้อมูลส่วนบุคคล รวมถึงการขอความยินยอมในระบบสารสนเทศของมหาวิทยาลัย 5.2 กิจกรรมแลกเปลี่ยนเรียนรู้แนวทางการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย Admin หน่วยงานภายในมหาวิทยาลัย วันที่ 27 กุมภาพันธ์ 2569 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ผลการดำเนินงาน (1) มีการตรวจสอบประเด็นความเสี่ยง และความรับผิดชอบของ Admin ในการบริหารจัดการข้อมูลส่วนบุคคล เพื่อนำไปปรับปรุงคำสั่งผู้ประมวลผลข้อมูลส่วนบุคคล (2) ได้แผนการดำเนินงานอบรมเชิงปฏิบัติการสำหรับทีมแอดมิน ซึ่งจะมุ่งเน้นการจำลองเหตุการณ์จริง (Case Study)	ร้อยละ 100	
				6. สรุปผลการจัดกิจกรรม	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - อาจารย์นฤชล เชื่อนยัง	6.1 สรุปผลการจัดกิจกรรมแลกเปลี่ยนเรียนรู้การพัฒนา	N/A	

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
						- นางสาวอรปรียา คำแพ่ง	เว็บไซต์ สำหรับ Admin (ไตรมาส1-2)		
				7. จัดทำมาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ. สำนักวิทยบริการฯ - อาจารย์นฤชล เขื่อนยัง - นางสาวอรปรียา คำแพ่ง	7.1 จัดทำมาตรการแก้ไขปัญหาและแก้ไขสถานการณ์เบื้องต้นในการระงับเหตุการละเมิดข้อมูลส่วนบุคคล สำหรับ Facebook Page หน่วยงานภายในมหาวิทยาลัย 7.2 จัดทำมาตรการเชิงเทคนิคสำหรับแอดมิน Facebook Page หน่วยงานภายในมหาวิทยาลัย 7.3 อยู่ระหว่างการจัดทำ (ร่าง) มาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยไซเบอร์	100 100 N/A	
				8. จัดทำแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล และมีช่องทางการร้องเรียน กรณีที่มีเหตุการละเมิดข้อมูลส่วนบุคคล	ปีงบประมาณ 2569	- ผอ.สำนักวิทยบริการฯ - รอง ผอ. สำนักวิทยบริการฯ - อาจารย์นฤชล เขื่อนยัง - นางสาวอรปรียา คำแพ่ง	8.1 กิจกรรมจัดทำ (ร่าง) แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล 8.2 จัดทำช่องทางการร้องเรียนกรณีที่มีเหตุการละเมิดข้อมูลส่วนบุคคล	N/A N/A	

แบบ RM-5

แบบสรุปผลการประเมินความเสี่ยงภายหลังการดำเนินการตามแผนบริหารความเสี่ยง

ชื่อหน่วยงาน มหาวิทยาลัยราชภัฏกำแพงเพชร **ประจำปีงบประมาณ** 2569 **รอบ** 6 **เดือน**

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลงระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงานปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
O1/การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.	4	4	16 สูงมาก	N/A	N/A	N/A	N/A	**KPI1** – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคล	ร้อยละ 60	- ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ - ผอ.กองพัฒนานักศึกษา	☐ บรรลุ ☒ ไม่บรรลุ ผลดำเนินงาน กำหนดจัดกิจกรรมอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคลและวัคซีนไซเบอร์ สำหรับบุคลากรมหาวิทยาลัยราชภัฏกำแพงเพชร	-
								KPI2 – ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม	ระดับดี	- ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ - ผอ.กองพัฒนานักศึกษา - หัวหน้างาน บค.	☐ บรรลุ ☒ ไม่บรรลุ ผลดำเนินงาน กำหนดจัดกิจกรรมอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคลและวัคซีนไซเบอร์ สำหรับบุคลากรมหาวิทยาลัยราชภัฏกำแพงเพชร	-
								KPI3 - ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้าน	ร้อยละ 70	- ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ	☐ บรรลุ ☒ ไม่บรรลุ ผลดำเนินงาน กำหนดจัดอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคล	-

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลงระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงานปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
								ความปลอดภัยของข้อมูลส่วนบุคคล		- ผอ.กองพัฒนานักศึกษา	และวัคซีนไซเบอร์สำหรับนักศึกษาชั้นปีที่ 1 วันปฐมนิเทศ วันที่ 27 พฤษภาคม 2569 เวลา 11.00 - 12.00 น. ณ อาคารทีปังกรรัศมีโชติ	
								KPI4 – ระดับความสำเร็จในการดำเนินการจัดการความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคล <u>เกณฑ์การให้คะแนน</u> คะแนน 1 : มีการจัดตั้งคณะทำงานและผู้รับผิดชอบ คะแนน 2 : มีการประชุมคณะกรรมการดำเนินงาน จัดทำนโยบาย วาง	5 คะแนน	- ผอ.สำนักวิทยบริการฯ - DPO นิติกรและคณะทำงาน	☐ บรรลุ ☒ ไม่บรรลุ <u>ผลดำเนินงาน</u> ผลการดำเนินงาน รอบ 6 เดือน ปฏิบัติตามเกณฑ์ได้ 2 คะแนน ดังนี้ **1. จัดตั้งคณะทำงานและผู้รับผิดชอบ** 1.1 มีคำสั่ง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO: Chief Information Office) ของมหาวิทยาลัยราชภัฏกำแพงเพชร 1.2 มีคำสั่ง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ของมหาวิทยาลัยราชภัฏกำแพงเพชร	-

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลงระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงานปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
								แผนการดำเนินงาน คะแนน 3 : มีการจัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคลและกำหนดให้เจ้าหน้าที่ที่เกี่ยวข้องลงนามในสัญญารักษาความลับ คะแนน 4 : มีการจัดกิจกรรมแลกเปลี่ยนเรียนรู้ (KM) ระหว่างบุคลากร เพื่อให้การปฏิบัติงานสอดคล้องกับ PDPA จัดทำมาตรการด้านความมั่นคง			1.3 มีคำสั่ง แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล **2. ประชุมกรรมการ** 2.1 ประชุมคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล วันที่ 5 พฤศจิกายน 2568 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ 2.2 ประชุมทบทวนแผนการดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อกำหนดวันจัดกิจกรรมอบรม วันที่ 1 เมษายน 2569 ณ ห้องสำนักงานศูนย์ภาษาอาคารศูนย์ภาษาและคอมพิวเตอร์ 2.3 กิจกรรมเสนอแผนการดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) สำหรับผู้บริหาร	

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลงระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI				แนวทางดำเนินงานปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
								ปลอดภัยของข้อมูลส่วนบุคคล สรุปผลการจัดกิจกรรม และรายงานผลการดำเนินงานต่อผู้บริหาร คะแนน 5 : มีการจัดทำแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคลและช่องทางการร้องเรียน			(คณะกรรมการบริหารประจำมหาวิทยาลัย) วันที่ 2 เมษายน 2569 ณ ห้องประชุมชั้น 8 อาคารเรียนรวมและอำนวยการ (ตึก 14)	
								KPI5 - จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ ถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต	0 ครั้ง	- ผอ.สำนักวิทยบริการฯ - ผอ.สำนักส่งเสริมฯ	☑ บรรลุ ☐ ไม่บรรลุ <u>ผลดำเนินงาน</u> การดำเนินงานภาพรวมรอบ 6 เดือน ข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บ <u>ไม่มี</u> กรณีถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต	-