รายงานผลการดำเนินการจัดการความรู้ ประจำปีการศึกษา 2567
ด้านพันธกิจอื่นๆ

เรื่อง การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏกำแพงเพชร

คำนำ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร ตระหนักและเห็นความสำคัญของข้อมูลส่วนบุคคล หรือ (PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ทั้งข้อมูลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งหากมีการละเมิด ตามกฎหมายอาจถูกดำเนินคดีทั้งอาญา แพ่ง และปกครอง อีกทั้งอาจจะนำไปสู่ความเสียหายด้านภาพลักษณ์และความเป็นมืออาชีพขององค์กร เพื่อให้ข้อมูลส่วนบุคคล ถูกนำไปใช้ในทางที่เหมาะสมและเป็นประโยชน์มากกว่าโทษ ดังนั้น แผนการจัดการความรู้ด้านการบริหารตามพันธกิจอื่นๆ ของมหาวิทยาลัยราชภัฏกำแพงเพชร ในปีการศึกษา 2567 จึงเลือกประเด็นการจัดการความรู้ เรื่อง “การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร” ช่วยขับเคลื่อนการดำเนินงานด้าน PDPA ของมหาวิทยาลัย ทั้งในกลุ่มบุคลากร นักศึกษา รวมทั้งมีการขยายผลการส่งเสริมความรู้ความเข้าใจด้าน PDPA สู่ประชาชน ให้ขยายวงกว้างออกไป และเกิดความยั่งยืน

คณะผู้จัดทำ หวังเป็นอย่างยิ่งว่าเว็บไซต์การจัดการความรู้การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากร และนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร จะเป็นประโยชน์สำหรับผู้ที่สนใจทั้งบุคลากร และนักศึกษา จะเพิ่มพูนความรู้ ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 สามารถนำความรู้ที่ได้ไปใช้ประยุกต์ในการเรียน การสอน และการทำงาน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

สารบัญ

1.ชื่อแผนการจัดการความรู้

การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

2.ผู้รับผิดชอบ

นางสาวอรปรียา คำแพ่ง
นางสาวสรัลชนา น้ำเงินสกุณี
และบุคลากร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

3.หลักการและเหตุผล

การให้ความคุ้มครองข้อมูลส่วนบุคคล ถือเป็นการสร้างความเคารพในสิทธิส่วนบุคคล ซึ่งเป็นพื้นฐานสำคัญของหลักสิทธิมนุษยชนของผู้เจริญแล้ว ซึ่งความเจริญของเทคโนโลยีในโลกยุคดิจิทัลที่ยั่งยืน จะต้องมาพร้อมกับ "ความรับผิดชอบ" จึงเป็นที่มาของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Personal Data Protection Act: PDPA) ซึ่งกฎหมายมีผลบังคับใช้ทั่วประเทศตั้งแต่วันที่ 1 มิถุนายน 2565 การมีผลบังคับใช้ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้น มีการกำหนดหลักเกณฑ์และวิธีการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมไปถึงกำหนดบทบาทหน้าที่ต่าง ๆ ให้กับผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล ส่วนหนึ่งในหน้าที่ที่กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติคือ การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล โดยมาตรการดังกล่าว ต้องรวมถึงการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัย แก่บุคลากร ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน หรือเกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร ตระหนักและเห็นความสำคัญของข้อมูลส่วนบุคคล หรือ (PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ทั้งข้อมูลทั่วไป เช่น ชื่อ-นามสกุล วันเดือนปีเกิด เลขบัตรประจำตัวประชาชน ที่อยู่ รูปถ่าย ฯลฯ และข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลอัตลักษณ์บุคคล (Biometrics) ได้แก่ ลายนิ้วมือ และลักษณะทางพันธุกรรม (DNA) ที่ใช้ยืนยันตัวบุคคล และต้องใช้ความระมัดระวังเป็นพิเศษ โดยจะต้องมีวัตถุประสงค์ในการนำไปใช้ที่ชัดเจน และตรวจสอบได้ว่ามีการนำเอาไปใช้ในเรื่องใดบ้าง ซึ่งหากมีการละเมิด ตามกฎหมายอาจถูกดำเนินคดีทั้งอาญา แพ่ง และปกครอง อีกทั้งอาจจะนำไปสู่ความเสียหายด้านภาพลักษณ์และความเป็นมืออาชีพขององค์กรด้วยเช่นกัน เพื่อให้ข้อมูลส่วนบุคคล ถูกนำไปใช้ในทางที่เหมาะสมและเป็นประโยชน์มากกว่าโทษ ดังนั้น ความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร สำนักฯ จึงเลือกจัดทำแผนการจัดการความรู้ด้านการบริหารตามพันธกิจอื่นๆ ของมหาวิทยาลัยราชภัฏกำแพงเพชร ในปีการศึกษา 2566 เรื่อง “การตระหนักถึงการกระทำความผิดการเผยแพร่ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของ Website หน่วยงานภายในมหาวิทยาลัยราชภัฏกำแพงเพชร” และเพื่อให้ครอบคลุมและเป็นการต่อยอดความรู้ ในปีการศึกษา 2567 จึงเลือกประเด็นการจัดการความรู้ เรื่อง “การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร” ช่วยขับเคลื่อนการดำเนินงานด้าน PDPA ของมหาวิทยาลัย ทั้งในกลุ่มบุคลากร นักศึกษา รวมทั้งมีการขยายผลการส่งเสริมความรู้ความเข้าใจด้าน PDPA สู่ประชาชน ให้ขยายวงกว้างออกไป และเกิดความยั่งยืน

4.วัตถุประสงค์

1. เพื่อเพิ่มพูนความรู้ ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ให้แก่ บุคลากร และนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

2. เพื่อให้ผู้ที่เข้าอบรมและเรียนรู้ผ่านเว็บไซต์การจัดการความรู้ เรื่อง “การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษา มหาวิทยาลัยราชภัฏกำแพงเพชร” สามารถนำความรู้ที่ได้ไปใช้ประยุกต์ในการเรียน การสอน และการทำงาน

3. เพื่อเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากร และนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

5.ผู้เข้าร่วมโครงการ

บุคลากรสายสนับสนุน และนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

6.สถานที่ดำเนินการ

มหาวิทยาลัยราชภัฏกำแพงเพชร

7.วิธีดำเนินงาน (แผนการจัดการความรู้ 6 ขั้นตอน)

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
1	การกำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร	**กิจกรรมที่ 1** จัดตั้งคณะทำงานและผู้รับผิดชอบการจัดการความรู้ของภายในมหาวิทยาลัยราชภัฏกำแพงเพชร	ต.ค. 2567	1. คำสั่งแต่งตั้งคณะกรรมการ จำนวน 1 ฉบับ	- ผู้บริหารของสำนักฯ - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ - บุคลากรของสำนักฯ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
		กิจกรรมที่ 2 จัดการประชุมนำเสนอและทบทวนแผนการจัดการความรู้เพื่อเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร	พ.ย. 2567	1. แผนการจัดการความรู้ จำนวน 1 เรื่อง	- บุคลากรตามคำสั่งในกิจกรรมที่ 1	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
2	การเสาะหาความรู้ที่ต้องการ	**กิจกรรมที่ 3** จัดประชุมแลกเปลี่ยนเรียนรู้เพื่อกำหนดขอบเขตขององค์ความรู้ให้แก่กลุ่มเป้าหมาย - บุคลากรสายสนับสนุน - นักศึกษา	ธ.ค. 2567	1. หัวข้อขององค์ความรู้ที่ต้องการเผยแพร่ให้กลุ่มเป้าหมาย - บุคลากรสายสนับสนุน จำนวน 13 หน่วยงาน - นักศึกษา จำนวน 6 คณะ	- รองอธิการบดีฝ่ายวิชาการ - ผู้ดูแลเว็บไซต์ (Admin) - อาจารย์ผู้สอนรายวิชาความฉลาดรู้ทางดิจิทัล สารสนเทศ และสื่อ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
3	การปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน	**กิจกรรมที่ 4** จัดกิจกรรมเพื่อหาแนวปฏิบัติเพื่อการเผยแพร่องค์ความรู้จากกิจกรรมที่ 3 เพื่อให้เหมาะสมกับกลุ่มเป้าหมาย - บุคลากรสายสนับสนุน	ม.ค. 2568	1. แนวปฏิบัติหรือนวัตกรรมการเผยแพร่องค์ความรู้ที่ต้องการเผยแพร่ให้กลุ่มเป้าหมาย จำนวน 1 เรื่อง	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
		- นักศึกษา				
4	การประยุกต์ใช้ความรู้ในกิจการงานของตน	**กิจกรรมที่ 5** นำความรู้ที่ได้จากกิจกรรมที่ 4 ไปดำเนินงานในหน่วยงานของตน	ม.ค. - เม.ย. 2568	1. บันทึกความรู้การร่วมกิจกรรม จำนวน 1 กิจกรรม 2. องค์ความรู้การร่วมกิจกรรม จำนวน 1 องค์ความรู้	- บุคลากรสายสนับสนุน	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
5	การนำประสบการณ์จากการทำงาน และการประยุกต์ ใช้ความรู้มาแลกเปลี่ยนเรียนรู้และสกัด“ขุมความรู้” ออกมาบันทึกไว้	**กิจกรรมที่ 6** นำองค์ความรู้ที่ได้มาเผยแพร่ผ่าน Website, และช่องทางอื่นๆ	พ.ค. 2568	1. จำนวนช่องทางการเผยแพร่องค์ความรู้อย่างน้อย 2 ช่องทาง	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
		กิจกรรมที่ 7 สร้างชุมชนการเรียนรู้	พ.ค. 2568	1. กลุ่มที่ใช้สำหรับแลกเปลี่ยนเรียนรู้ทางโซเชียลมีเดีย อย่างน้อย 1 กลุ่ม 2. สื่อส่งเสริมการเรียนรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จำนวนอย่างน้อย 5 ชิ้น	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
6	การจดบันทึก “ขุมความรู้” และ “แก่นความรู้” สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น	**กิจกรรมที่ 8** จัดทำแนวปฏิบัติหรือนวัตกรรม เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร	พ.ค. 2568	แนวปฏิบัติหรือนวัตกรรมเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างน้อย 1 ชิ้น	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

8.ขั้นตอนการดำเนินงาน

ขั้นตอนที่ 1 กำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร

สำนักวิทยบริการและเทคโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร เป็นหน่วยงานที่มีการเผยแพร่ข้อมูลในรูปแบบออนไลน์บน Website ทั้งเว็บไซต์มหาวิทยาลัย เว็บไซต์สำนักฯ และระบบสารสนเทศที่มีการให้บริการอื่นในรูปแบบเว็บไซต์ และมีหน้าที่กำกับติดตามงานพัฒนาเว็บไซต์หน่วยงานภายในมหาวิทยาลัย ทั้ง 13 หน่วยงาน ที่ผ่านมาได้มีการขับเคลื่อนการดำเนินงานด้าน PDPA ของมหาวิทยาลัย อีกทั้งช่วยสื่อสารเพื่อสร้างความตระหนักรู้เรื่อง PDPA ทั้งในนักศึกษา บุคลากร และได้มีแนวคิดขยายผลการส่งเสริมความรู้ความเข้าใจด้าน PDPA สู่ประชาชนทั่วไป เพื่อการสร้างความตระหนักรู้ให้ขยายวงกว้างออกไป และให้เกิดความยั่งยืน ดังนั้น เพื่อให้ข้อมูลส่วนบุคคล หรือ (PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ถูกนำไปใช้ในทางที่เหมาะสมและเป็นประโยชน์มากกว่าโทษ ในขั้นตอนการกำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร สำนักฯ จึงกำหนดการจัดทำแผนการจัดการความรู้ ดังนี้

(1) จัดทำคำสั่งคณะกรรมการทำงานและรับผิดชอบการจัดการความรู้ของสำนักฯ

(2) ประชุมคณะกรรมการการจัดการความรู้ ประจำปีการศึกษา 2567 ทบทวนแผนการจัดการความรู้เพื่อกำหนดความรู้หลักที่จำเป็น เมื่อวันที่ 21 พฤศจิกายน 2567 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จากการประชุม มติที่ประชุมกำหนดให้จัดทำ ***“ประเด็นการจัดการความรู้ เรื่อง การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร”*** และร่วมกันเขียนแผนการจัดการความรู้ในประเด็นดังกล่าว

ที่มา: ภาพกิจกรรม https://arit.kpru.ac.th/page_id/1479/TH

ขั้นตอนที่ 2 การเสาะหาความรู้ที่ต้องการ

ในส่วนของขั้นตอนที่ 2 ผู้อำนวยการสำนักฯ ได้มอบหมายให้คณะกรรมการผู้รับผิดชอบการจัดการความรู้ของสำนักฯ ทบทวน เสาะหาความรู้ที่เกี่ยวข้องและจำเป็น โดยค้นคว้าด้วยตนเอง จากเว็บไซต์ที่น่าเชื่อถือ เพื่อกำหนดขอบเขตขององค์ความรู้ให้แก่กลุ่มเป้าหมาย และประชุมแลกเปลี่ยนเรียนรู้ ครั้งที่ 1 เมื่อวันที่ 23 มกราคม 2568 เวลา 09.00-10.00 น. ณ ห้องประชุมลูกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

จากการประชุมได้เชิญผู้มีความรู้และประสบการณ์ด้านกฎหมาย ได้แก่ อาจารย์นฤชล เขื่อนยัง อาจารย์ประจำสาขานิติศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์ เพื่อร่วมวางแผนการดำเนินงานที่เกี่ยวข้อง 3 ประเด็น ดังนี้

(1) การอบรมให้ความรู้สำหรับกลุ่มเป้าหมาย บุคลากรสายสนับสนุน 13 หน่วยงาน และนักศึกษา 6 คณะ รวมถึงวิทยากรบรรยายให้ความรู้ ภายใต้โครงการชุมชนดิจิทัล (Digital Community) เพื่อรองรับสังคมศตวรรษที่ 21

(2) วางแผนรวบรวมสื่อส่งเสริมการเรียนรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จากแหล่งข้อมูลที่น่าเชื่อถือ และจากสื่อที่จัดทำขึ้นในระบบ KPRU MOOC

(3) วางแผนกำหนดขอบเขตเนื้อหาสำหรับจัดทำแนวปฏิบัติ หรือนวัตกรรมเพื่อเผยแพร่องค์ความรู้ PDPA ให้กับกลุ่มบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

ขั้นตอนที่ 3 ปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน

ในปัจจุบัน องค์กรต้องพึ่งพาเทคโนโลยีสารสนเทศและข้อมูลดิจิทัลอย่างมากในการดำเนินงาน เช่น ระบบปฏิบัติการ ฐานข้อมูล แอปพลิเคชัน หรือแม้แต่ซอฟต์แวร์บริหารจัดการข้อมูลต่างๆ เนื่องจากภัยคุกคามในโลกไซเบอร์มีการพัฒนาอย่างต่อเนื่องและสามารถสร้างความเสียหายร้ายแรง องค์กรควรต้องมีการบริหารจัดการความเสี่ยง ซึ่งจะเป็นกระบวนการที่ช่วยให้องค์กรสามารถระบุ ประเมิน วิเคราะห์ สามารถรับมือ และจัดการความเสี่ยงต่างๆ ที่เกี่ยวข้องกับภัยคุกคามไซเบอร์ได้อย่างทันท่วงที รวมถึงเหตุการณ์การรั่วไหลข้อมูล(Data Breaches) ความเสียหายของการรั่วไหลข้อมูลที่เกิดขึ้น เป็นผลมาจากปริมาณข้อมูลที่เพิ่มขึ้นตามความก้าวหน้าของเทคโนโลยี โดยเฉพาะเทคโนโลยี 5G และมนุษย์เป็นสาเหตุใหญ่ในการรั่วไหลของข้อมูล (Human Factor) ในปี 2024 มนุษย์เป็นสาเหตุของการรั่วไหลของข้อมูลมากถึง 90%

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีบทบาทสำคัญในการปกป้องค์กรจากเหตุการณ์ภัยคุกคามทางไซเบอร์ จึงต้องเฝ้าระวังและติดตามเทรนด์ภัยคุกคามรูปแบบใหม่ๆ อยู่เสมอ เพื่อนำมาพัฒนากลยุทธ์ในการป้องกันภัยคุกคามทางไซเบอร์อย่างเหมาะสม ด้วยเหตุผลดังกล่าว สำนักฯ จึงกำหนดให้จัดอบรมให้กับบุคลากรเกิดความตระหนักด้านความปลอดภัยทางไซเบอร์ที่ทันสมัยและต่อเนื่อง เพื่อสร้างวัฒนธรรมความปลอดภัยที่แข็งแกร่งทั่วทั้งองค์กร

3.1 ประชุมคณะกรรมการบริหารความเสี่ยงและการตรวจสอบควบคุมภายในของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ จากการประชุมคณะกรรมการการจัดการความรู้ ประจำปีการศึกษา 2567 เมื่อวันที่ 21 พฤศจิกายน 2567 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เนื่องจากการประชุมดังกล่าว คณะกรรมการเป็นทีมเดียวกับคณะกรรมการบริหารความเสี่ยงและการตรวจสอบควบคุมภายในของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หลังพิจารณา “ประเด็นการจัดการความรู้ เรื่อง การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร” และร่วมกันเขียนแผนการจัดการความรู้

ในขั้นตอนนี้ สำนักฯ เล็งเห็นว่าประเด็นการจัดการความรู้ ควรทำควบคู่กับแผนบริหารความเสี่ยง จึงได้ปรับปรุง และสร้างความรู้บางส่วนจากแผนการจัดการความรู้ มาต่อยอดจัดทำเป็นแผนบริหารความเสี่ยงของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568 **ประเด็นความเสี่ยงเรื่อง การโจมตีความปลอดภัยทางไซเบอร์** และถูกคัดเลือกเป็นความเสี่ยงมหาวิทยาลัยด้วย เนื่องด้วย (1) นโยบายและการดำเนินงานของสำนักงาน

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานที่กำหนด (2) การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอที อาจส่งผลให้ไม่สามารถให้บริการตามปกติได้

รายละเอียด RM1-RM3 ดังลิงค์ https://www.kpru.ac.th/km-web/files/rm1-3-arit2025.pdf

3.2 ส่งเสริมการใช้สื่อ PDPA e-Learning แบ่งเป็น 2 ส่วน ได้แก่ PDPA Thailand และ GE Online รายวิชากฎหมายชีวิตประจำวันในยุคดิจิทัล หัวข้อ PDPA โดยสร้างเว็บไซต์รวบรวมรายละเอียดการเข้าร่วมโครงการเรียนรู้ PDPA e-Learning

(1) PDPA Thailand

เมื่อวันที่ 4 มิถุนายน 2567 มหาวิทยาลัยฯ ได้รับหนังสือจาก สมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA) เชิญชวนเข้าร่วมโครงการ 5 ปี ประกาศ 2 ปีบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 สำหรับสถาบันอุดมศึกษา เพื่อส่งเสริมให้บุคลากรทางการศึกษา ตลอดจนนิสิตนักศึกษาได้เรียนรู้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ผ่านระบบ e-learning จาก PDPA Thailand ฟรี จึงได้ประสานสอบถามข้อมูลเพื่อเติม และมหาวิทยาลัยราชภัฏกำแพงเพชร ได้รับการพิจารณาให้สิทธิ์สถาบันอุดมศึกษาที่สมัครเข้าร่วมโครงการ สำนักฯ ได้ขอคำแนะนำจากรองอธิการบดีฝ่ายวิชาการ ผศ.ดร.ฆัมภิชา ตันติสันติสม และประสานตัวแทนอาจารย์ผู้สอนประจำรายวิชา ความฉลาดรู้ทางดิจิทัล สารสนเทศ และสื่อ เพื่อคัดเลือกผู้ใช้สื่อฯ

ขั้นตอนนี้ ได้จัดทำเว็บไซต์รวบรวมรายละเอียด การเข้าร่วมโครงการเรียนรู้ PDPA e-Learning ดังลิงค์ https://sites.google.com/view/tpdpa-kpru/

(2) GE Online ในระบบ KPRU MOOC

GE Online รายวิชากฎหมายชีวิตประจำวันในยุคดิจิทัล
หัวข้อ PDPA โดย อาจารย์นฤชล เขื่อนยัง
อาจารย์ประจำสาขานิติศาสตร์
คณะมนุษยศาสตร์และสังคมศาสตร์

ขั้นตอนที่ 4 ประยุกต์ใช้ความรู้ในกิจการงานของตน

ในขั้นตอนนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้นำองค์ความรู้เกี่ยวกับ PDPA และ Cyber Security นำมาดำเนินงานของหน่วยงาน ดังนี้

กลุ่มบุคลากร

4.1 จัดกิจกรรมแลกเปลี่ยนเรียนรู้กลุ่มผู้ดูแลเว็บไซต์หน่วยงาน จำนวน 6 ครั้ง จากกิจกรรมนี้ ได้ปรับปรุงดัดแปลง สร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน ได้ประเด็นหัวข้อที่มีความสอดคล้องกับงาน ดังนี้

กิจกรรม KM WEBSITE ครั้งที่ 1 เมื่อวันที่ 31 มกราคม 2568 เวลา 09.00 - 12.00 น. ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

สำนักฯ ได้ประสานขอคำแนะนำจาก สกมช. เกี่ยวกับเครื่องมือสำหรับตรวจสอบความปลอดภัยของเว็บไซต์ ได้รับคำแนะนำให้ใช้แพลตฟอร์มแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ MISP โดย นายอนุชา พวงผกา รองผู้อำนวยการสำนักฯ ได้แสดงตัวอย่างวิธีขั้นตอนและผลการตรวจสอบของแต่ละหน่วยงาน และสร้างข้อตกลงร่วมกันว่าจะตรวจสอบภัยคุกคามทางไซเบอร์ ทุกวันที่ 1 ของเดือน เช่นเดียวกับ backlink




กิจกรรม KM WEBSITE ครั้งที่ 2 เมื่อวันที่ 6 กุมภาพันธ์ 2568 เวลา 09.00 - 12.00 น. ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

1. แนวทางการปรับปรุงข้อมูล การเผยแพร่ข้อมูลของหน่วยงานในระบบสารสนเทศ และเว็บไซต์หน่วยงาน ให้มีความสอดคล้อง ถูกต้อง และเป็นปัจจุบัน

2. อัปเดตข้อมูลจากงาน "การดำเนินกิจกรรมบนระบบเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา" ครั้งที่ 44 | Workshop on UniNet Network and Computer Application (44th WUNCA)

3. รายละเอียดโครงการสื่อการเรียนรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA e-Learning) โดย สมาคมผู้ตรวจสอบและให้คำปรึกษาด้านการคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA) ใช้งานได้ถึง 19 สิงหาคม 2568

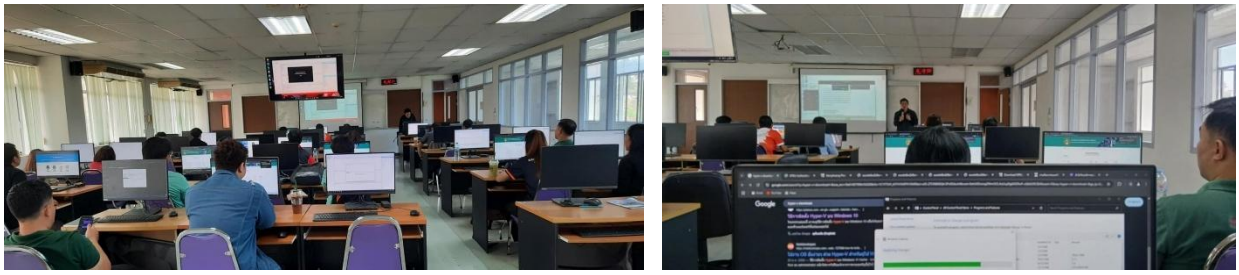
4. ปัญหาและอุปสรรคในการพัฒนาเว็บไซต์ของหน่วยงาน

มีประเด็นซักถามเกี่ยวกับเว็บไซต์คณะ/หน่วยงาน ในรูปแบบภาษาอังกฤษ จึงให้ข้อมูลโดยอ้างอิงจากคำสั่งคณะกรรมการดำเนินงานการพัฒนาเว็บไซต์หน่วยงานภายในมรภ.กำแพงเพชร ให้สอดคล้องตามเกณฑ์ของ Webometrics ดังลิงค์ https://www.kpru.ac.th/km-web/files/officer-command-admin2025.pdf

โดยสรุป คณะกรรมการพัฒนาระบบเว็บไซต์ มีหน้าที่ นำข้อมูลและสารสนเทศมาจัดทำเว็บไซต์ให้เหมาะสมกับวัตถุประสงค์การใช้ประโยชน์ พัฒนาเว็บไซต์ทั้งในรูปแบบภาษาไทยและภาษาอังกฤษ ที่มีคุณภาพ มีความถูกต้องเป็นปัจจุบันและได้รับการปรับปรุงข้อมูลอย่างต่อเนื่อง รวมถึงบำรุงรักษาและตรวจตราความปลอดภัยของเว็บไซต์

กิจกรรม KM WEBSITE ครั้งที่ 3 เมื่อวันที่ 26 กุมภาพันธ์ 2568 เวลา 09.00 - 12.00 น. ณ ห้องปฏิบัติการคอมพิวเตอร์ ชั้น 5 อาคารศูนย์ภาษาและคอมพิวเตอร์

1. อบรมแลกเปลี่ยนเทคนิคการบริหารจัดการ Hyper-V สำหรับการสำรองข้อมูลระบบสารสนเทศและเว็บไซต์ให้มีความปลอดภัย โดย นายประทีป เพ็ญแจ้ง (Admin คณะวิทยาศาสตร์และเทคโนโลยี)



2. อบรมแลกเปลี่ยนเทคนิคการใช้ Strapi สำหรับสร้างและจัดการ API โดย นายคมกริช กลิ่นอาจ (Admin สำนักส่งเสริมวิชาการและงานทะเบียน)

กิจกรรม KM WEBSITE ครั้งที่ 4 เมื่อวันที่ 5 มีนาคม 2568 เวลา เวลา 09.00 - 12.00 น. ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สรุปประเด็นสำคัญ ได้ดังนี้

1. ผลการจัดอันดับ Webometrics Ranking : January 2025 edition

มหาวิทยาลัยราชภัฏกำแพงเพชร ได้รับการจัดอันดับเป็นอันดับที่ 8461 ของโลก (เดิมอันดับที่ 31331), และเป็นอันดับที่ 26 ในกลุ่มมหาวิทยาลัยราชภัฏ (เดิมอันดับที่ 38)

2. ความก้าวหน้าเกี่ยวกับหลักสูตร AI เรียนฟรีของ Microsoft ภายใต้โครงการ Microsoft AI Academy for University เมื่อวันที่ 4 มีนาคม 2568 ได้มีการประชุมวางแผนการติดตั้งร่วมกับบริษัท Microsoft ใน KPRU MOOC หลังการประชุมบริษัท Microsoft ได้นำส่งไฟล์คลิปวิดีโอเนื้อหา Course AI จำนวน 5 หลักสูตร พร้อมคลังข้อสอบสำหรับนำเข้าระบบ KPRU MOOC ขณะนี้ได้ดำเนินการปรับตั้งค่าเครื่องแม่ข่ายให้พร้อมใช้งานมากขึ้น และได้ดำเนินการนำเข้าสมบูรณ์แล้ว 1 หลักสูตร ได้แก่ หลักสูตร AI Skills for All และอยู่ระหว่างการเตรียมข้อสอบสำหรับนำเข้าอีก 2 หลักสูตร ได้แก่ หลักสูตร AI Basic Copilot และ หลักสูตร Microsoft 365 Copilot

3. ประเด็นความเสี่ยงของมหาวิทยาลัย ประจำปีงบประมาณ 2568 ที่มีความเกี่ยวข้องกับ Admin ได้แก่ เรื่อง การโจมตีความปลอดภัยทางไซเบอร์

4. ผลการตรวจสอบเครื่องคอมพิวเตอร์ ของหน่วยงานภายในทั้งหมด จำนวน 1,602 เครื่อง มีเครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรม Adobe ที่ไม่มีลิขสิทธิ์ทั้งหมด จำนวน 743 เครื่อง

5. ความก้าวหน้าเรื่องระบบพิสูจน์และยืนยันตัวตนทางดิจิทัลของกรมการปกครอง (มหาวิทยาลัยราชภัฏกำแพงเพชร) Thai ID อยู่ระหว่างการพัฒนาระบบเชื่อมต่อข้อมูล และอบรมการเชื่อมต่อข้อมูลกับมหาวิทยาลัยนำร่อง

6. ความก้าวหน้าเรื่องการติดตั้ง WiFi จำนวน 166 ตัว ปรับเปลี่ยนแทนที่ในทุกๆ อาคารตามอายุการใช้งาน, จุดที่มีการใช้บริการหนาแน่น และอุปกรณ์ที่มีอายุเกิน 10 ปี ทดสอบและให้บริการทุกจุด วันที่ 11 มีนาคม 2568

7. ความก้าวหน้าเรื่องการติดตั้งอุปกรณ์เชื่อมต่อสัญญาณระหว่างตึก Switch จำนวน 17 ตัว ดำเนินการติดตั้งเสร็จเรียบร้อยและเปิดให้บริการ

8. ความก้าวหน้าเรื่องการติดตั้งเครื่องแม่ข่าย (Cloud) จำนวน 1 Node เพิ่มประสิทธิภาพการให้บริการเว็บไซต์ ดำเนินการติดตั้งเสร็จเรียบร้อย

9. ความก้าวหน้าเรื่องการปรับปรุง Switch หลักของมหาวิทยาลัย จำนวน 2 ตัว เพื่อเพิ่มประสิทธิภาพการเชื่อมต่อสัญญาณอินเทอร์เน็ต ดำเนินการติดตั้งอุปกรณ์เรียบร้อย และจะดำเนินการทดสอบระบบในวันที่ 11 มีนาคม 2568 เวลา 18.00 เป็นต้นไป


กิจกรรม KM WEBSITE ครั้งที่ 5 เมื่อวันที่ 14 มีนาคม 2568 เวลา 09.30 น. ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สรุปประเด็นสำคัญ ได้ดังนี้

1. **อัปเดตความรู้ด้าน Cybersecurity**
2. **แลกเปลี่ยนแนวทางการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ต่อระบบสารสนเทศ และข้อมูลดิจิทัล**
3. **ระบบบริหารจัดการสื่อการเรียนการสอนออนไลน์**
4. **ระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล ของกรมการปกครอง (มหาวิทยาลัยราชภัฏกำแพงเพชร)**
5. **การปรับเปลี่ยนอุปกรณ์เครือข่ายอินเทอร์และ Cloud**
6. **การใช้งานโปรแกรมลิขสิทธิ์**

กิจกรรม KM WEBSITE ครั้งที่ 6

เมื่อวันที่ 19 มีนาคม 2568 เวลา 09.30 น. น.ได้จัดกิจกรรม KM WEBSITE ครั้งที่ 6 ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สรุปประเด็นสำคัญ ได้ดังนี้

1. สรุปยอดจำนวนการใช้งานโปรแกรมลิขสิทธิ์

2. เรียนรู้การใช้งานระบบ MISP (Malware Information Sharing Platform) ตามที่ สกมช. แนะนำ

MISP เป็นซอฟต์แวร์โอเพ่นซอร์สที่ช่วยในการรวบรวม จัดเก็บ แจกจ่าย และแบ่งปันข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์และภัยคุกคามต่าง ๆ ที่เกี่ยวข้องกับการวิเคราะห์เหตุการณ์ความปลอดภัยทางไซเบอร์และมัลแวร์

3. ความก้าวหน้าเกี่ยวกับหลักสูตร AI เรียนฟรีของ Microsoft ในระบบ KPRU MOOC

สรุปรายงานและภาพกิจกรรม เผยแพร่ไว้ที่เว็บไซต์ https://www.kpru.ac.th/km-web/files/report-webometrics1-6-2025.pdf

<u>กลุ่มนักศึกษา</u>

1) จัดกิจกรรมบรรยายในหัวข้อ *"ความรู้ทางกฎหมาย PDPA และ IP Law สำหรับนักศึกษา IT"* พร้อมเทคนิควิธีการรับมือกับการหลอกลวงทางไซเบอร์ โดยเฉพาะการปลอมตัวเป็นเจ้าหน้าที่รัฐ เพื่อให้นักศึกษาโปรแกรมวิชาเทคโนโลยีสารสนเทศ ได้รู้เท่าทัน เข้าใจวิธีการป้องกัน และตระหนักถึงอาชญากรรมทางไซเบอร์ เมื่อวันที่ 3 มีนาคม 2568 ณ ห้องประชุมชั้น 8 อาคารศูนย์ภาษาและคอมพิวเตอร์ รูปแบบกิจกรรมแบ่งออกเป็น 3 ส่วน:

Section 1: ทดสอบความรู้ - นักศึกษาได้ลองตอบวิธีการรับมือจากสถานการณ์ที่อาจมีพฤติกรรมเสี่ยงต่อการกระทำผิดกฎหมาย เพื่อวัดความรู้พื้นฐานทางกฎหมาย

Section 2: บรรยายเกี่ยวกับ Digital Law for IT student - เรียนรู้เกี่ยวกับ PDPA, กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายลิขสิทธิ์ในเบื้องต้นที่นักศึกษาไอทีจำเป็นต้องรู้!

Section 3: Workshop - นักศึกษาไอทีร่วมระดมความคิดว่าหากเจอสถานการณ์ที่เป็นภัยทางไซเบอร์จะมีวิธีรับมือและแก้ไขปัญหาอย่างไร พร้อมการบรรยายสรุปโดย อาจารย์ศรัณย์ จงรักษ์ เกี่ยวกับการรับมือและวิธีการแก้ไขปัญหาเมื่อพบเจออาชญากรที่แฝงตัวเป็นเจ้าหน้าที่รัฐ

2) นักศึกษาชั้นปีที่ 1 ที่เรียนรายวิชา ความฉลาดรู้ทางดิจิทัล สารสนเทศ และสื่อ แบ่งเป็น นักศึกษา 649 คน อาจารย์ 13 คน และบุคลากร 38 คน จำนวนรวมทั้งสิ้น 700 คน ได้สิทธิ์ในการเรียนรู้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ผ่านระบบ e-learning จาก PDPA Thailand ฟรี (ใช้ได้ตั้งแต่ บัดนี้ - 19 สิงหาคม 2568)

3) กำหนดตารางจัดกิจกรรมบรรยายเรื่อง วัคซีนไซเบอร์และการตระหนักรู้เกี่ยวกับ PDPA กับนักศึกษาชั้นปีที่ 1 ในกิจกรรมวันปฐมนิเทศนักศึกษาใหม่ วันที่ 28 พฤษภาคม 2568 พร้อมกับแนะนำช่องทางการเข้าถึงแนวปฏิบัติหรือนวัตกรรมส่งเสริมการเรียนรู้เกี่ยวกับ PDPA ให้กับนักศึกษารับทราบด้วย

4) เพิ่มความรู้เกี่ยวกับ PDPA ในการจัดกิจกรรม เรื่อง วัคซีนไซเบอร์ การป้องกันภัยอาชญากรรมทางเทคโนโลยี สำหรับประชาชน ภายใต้โครงการชุมชนดิจิทัล (Digital Community) เพื่อรองรับศตวรรษที่ 21 จำนวน 17 ครั้ง ผู้เข้าร่วมอบรม 760 คน

ครั้งที่	วันที่จัดกิจกรรม	จำนวนผู้เข้าร่วมกิจกรรม (คน)	สถานที่
1	17 กุมภาพันธ์ 2568	40	หมู่ 1 หมู่บ้านบ้านคลองน้ำไหลเหนือ
2	18 กุมภาพันธ์ 2568	50	หมู่ 2 หมู่บ้านคลองน้ำไหล
3	20 กุมภาพันธ์ 2568	40	หมู่ 3 หมู่บ้านแม่สอด
4	21 กุมภาพันธ์ 2568	40	หมู่ 4 หมู่บ้านท่าช้าง
5	24 กุมภาพันธ์ 2568	100	หมู่ 5 / 7 / 10 / 14 / 24 หมู่บ้านมอมะปรางทอง
6	25 กุมภาพันธ์ 2568	60	หมู่ 8 / 20 / 23 หมู่บ้านใหม่วงศ์เจริญ
7	27 กุมภาพันธ์ 2568	60	หมู่ 9 / 12 /18 หมู่บ้านคลองพลู
8	28 กุมภาพันธ์ 2568	30	หมู่ 13 หมู่บ้านคลองหัวแหวน
9	3 มีนาคม 2568	30	หมู่ 15 หมู่บ้านศรีดอนชัย

ครั้งที่	วันที่จัดกิจกรรม	จำนวนผู้เข้าร่วมกิจกรรม (คน)	สถานที่
10	4 มีนาคม 2568	40	หมู่ 16 หมู่บ้านสามัคคีธรรม
11	6 มีนาคม 2568	30	หมู่ 19 หมู่บ้านชัยมงคล
12	7 มีนาคม 2568	40	หมู่ 21 หมู่บ้านคลองน้ำไหลเหนือพัฒนา
13	10 มีนาคม 2568	40	หมู่ 22 หมู่บ้านหนองปลาไหล
14	13 มีนาคม 2568	40	หมู่ 25 หมู่บ้านใหม่ศรีสุวรรณ
15	14 มีนาคม 2568	40	หมู่ 26 หมู่บ้านบึงทรัพย์เจริญ
16	17 มีนาคม 2568	40	หมู่ 27 หมู่บ้านร่มโพธิ์ทอง
17	18 มีนาคม 2568	40	หมู่ 28 หมู่บ้านคลองด้วน


COMPUTER CENTER


ศูนย์คอมพิวเตอร์
COMPUTER CENTER
ห้องสมุด
ARIT LIBRARY


ศูนย์คอมพิวเตอร์
COMPUTER CENTER
ห้องสมุด
ARIT LIBRARY


ห้องสมุด
ARIT
LIBRARY
ศูนย์คอมพิวเตอร์
COMPUTER
CENTER
วัคซีนไซเบอร์
POLICE


ห้องสมุด
ARIT
LIBRARY
ศูนย์คอมพิวเตอร์
COMPUTER
CENTER


ห้องสมุด
ARIT
LIBRARY


ศูนย์คอมพิวเตอร์
COMPUTER CENTER
ห้องสมุด
ARIT
LIBRARY


ศูนย์คอมพิวเตอร์
COMPUTER
CENTER


ศูนย์คอมพิวเตอร์
COMPUTER
CENTER


COMPUTER CENTER


ศูนย์คอมพิวเตอร์
COMPUTER
CENTER


ห้องสมุด
ARIT LIBRARY


ห้องสมุด
ARIT
LIBRARY


ห้องสมุด
ARIT
LIBRARY


ศูนย์คอมพิวเตอร์
COMPUTER
CENTER


ห้องสมุด
ARIT LIBRARY

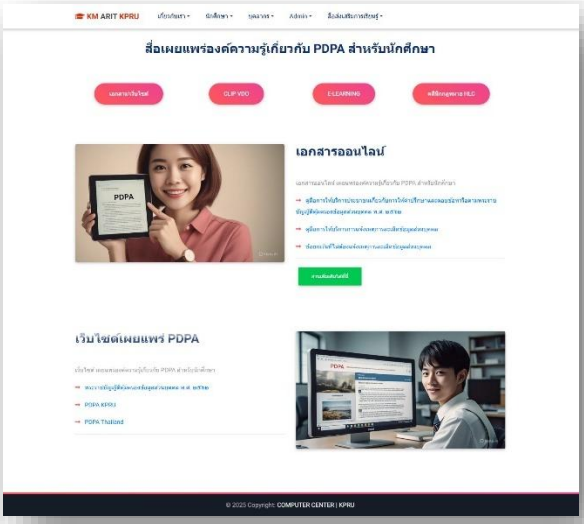

ห้องสมุด
ARIT LIBRARY
ศูนย์คอมพิวเตอร์
COMPUTER CENTER

ขั้นตอนที่ 5 นำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด “ขุมความรู้” ออกมาบันทึกไว้

5.1 กิจกรรมนำองค์ความรู้ที่ได้มาเผยแพร่ Website และช่องทางอื่นๆ

จากขั้นตอนการนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด “ขุมความรู้” ออกมาบันทึกไว้ แยกเป็น 2 กิจกรรม กิจกรรมนี้นำองค์ความรู้ที่ได้มาเผยแพร่ Website และช่องทางอื่นๆ จัดเก็บความรู้พัฒนาเป็นเว็บไซต์ “การจัดการความรู้ PDPA” โดยรวบรวมสื่อส่งเสริมการเรียนรู้เกี่ยวกับ PDPA อย่างน้อย 5 ชิ้น แยกตามประเภทผู้ใช้ เผยแพร่ 2 ช่องทาง ได้แก่ (1) ช่องทาง Website มหาวิทยาลัย และ (2) ช่องทาง Facebook มหาวิทยาลัย

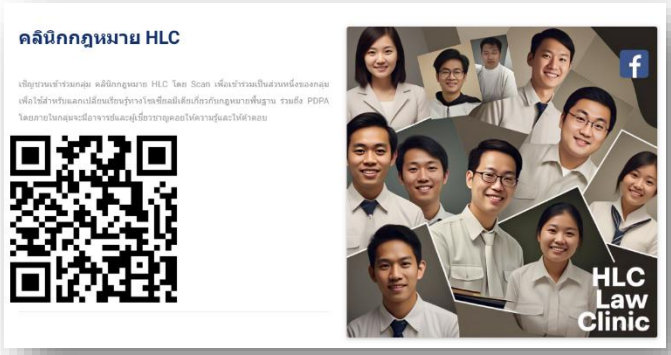
ตัวอย่าง หน้าหลักเว็บไซต์การจัดการความรู้ PDPA https://www.kpru.ac.th/km-pdpa/



สื่อส่งเสริมการเรียนรู้ PDPA แยกตามประเภทผู้ใช้

5.2 กิจกรรม สร้างชุมชนการเรียนรู้

จากขั้นตอนการนำประสบการณ์จากการทำงาน และการประยุกต์ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด “ขุมความรู้” ออกมาบันทึกไว้ เพื่อสร้างชุมชนการเรียนรู้ (Learning Community) โดย สร้างกลุ่มสำหรับแลกเปลี่ยนเรียนรู้ทางโซเชียลมีเดีย อย่างน้อย 1 กลุ่ม ได้แก่ **คลินิกกฎหมาย HLC**



ขั้นตอนที่ 6 จดบันทึก “ขุมความรู้” และ “แก่นความรู้” สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น

ในขั้นตอนนี้ ได้ใช้ประสบการณ์การทำงานและการเรียนรู้ผ่านคลิปวิดีโอของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) จาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และแหล่งอื่นๆ ที่มีความน่าเชื่อถือ คัดเลือก จดบันทึก “ขุมความรู้” และ “แก่นความรู้” สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น จัดทำเป็นเว็บไซต์เผยแพร่การจัดการความรู้ PDPA (Personal Data Privacy Policy) เรื่อง "การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษา มหาวิทยาลัยราชภัฏกำแพงเพชร" รวบรวม สื่อส่งเสริมการเรียนรู้ PDPA แยกตามประเภทผู้ใช้ ที่เว็บไซต์ https://kpru.ac.th/km-pdpa/ เพื่อเป็นการส่งเสริมและสนับสนุนความรู้เกี่ยวกับนโยบายด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ การรับมือภัยคุกคามในยุคดิจิทัล และการเสริมสร้างความตระหนักรู้ในการปกป้องตนเองและองค์กรจากภัยไซเบอร์ ด้วยการเข้าใจเรียนรู้กระบวนการเครื่องมือทางเทคโนโลยีเพื่อป้องกันและรับมือจากภัยคุกคาม เข้าใจสิทธิทางดิจิทัล กฎหมายที่คุ้มครองสิทธิของตนเอง ขอบเขตสิทธิเสรีภาพส่วนบุคคล เพื่อให้บุคลากร ผู้ปฏิบัติงาน นักศึกษา รู้เท่าทันภัยไซเบอร์รูปแบบต่างๆ ที่ทุกคนมีโอกาสพบเจอได้ในชีวิตประจำวัน และสำหรับหน่วยงาน ยิ่งจำเป็นต้องหาแนวทางรักษาป้องกันความปลอดภัยของระบบและข้อมูล เพื่อรักษาผลประโยชน์สูงสุดให้กับองค์กรและผู้รับบริการ กิจกรรมทั้งหมดที่สำนักฯ จัดขึ้น ได้รวบรวม Knowledge Asset (KA) โดยบันทึกความรู้ สรุปเป็นประเด็นสาระสำคัญของงาน เป็นชุดความรู้ แบบ Explicit Knowledge และรวบรวมความรู้ที่มีประโยชน์ อ้างอิงจากแหล่งความรู้ (References) แล้วจัดเก็บเป็นคลังความรู้ออนไลน์เผยแพร่ในเว็บไซต์ให้ผู้ใช้เข้าถึงได้ง่าย นำไปใช้ประโยชน์ได้จริง สร้างสังคมเวทีแห่งการเรียนรู้ให้บุคลากร นักศึกษา มีโอกาสพูดคุย แลกเปลี่ยนความรู้ซึ่งกันและกัน

9. ประโยชน์ที่คาดว่าจะได้รับ

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

2. บุคลากรและนักศึกษาของมหาวิทยาลัย สามารถนำความรู้ที่ได้ไปใช้ประยุกต์ในการเรียนการสอน และการทำงาน ทำให้การคุ้มครองข้อมูลส่วนบุคคคลเป็นเรื่องปกติของทุกๆ กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

3. ได้เว็บไซต์เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

10.องค์ความรู้

1. แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

2. แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ (Website Security)

3. แนวปฏิบัติพื้นฐานด้านความปลอดภัยทางไซเบอร์ ป้องกันเหตุการณ์ข้อมูลรั่วไหล

11.ช่องทางการเผยแพร่องค์ความรู้

- เผยแพร่ผ่านช่องทาง Website และ Facebook

ภาคผนวก

แผนการจัดการความรู้ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ปีการศึกษา 2567

แผนการจัดการความรู้ (KM Action Plan)

หน่วยงาน : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร

ประจำปีการศึกษา 2567 (1 มิถุนายน พ.ศ. 2567 ถึง 31 พฤษภาคม พ.ศ. 2568)

ประเด็นการจัดการความรู้ : การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร

☐ การเรียนการสอน ☐ การวิจัย ☑ พันธกิจอื่นๆ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
1	การกำหนดความรู้หลักที่จำเป็นหรือสำคัญต่องานหรือกิจกรรมของกลุ่มหรือองค์กร	**กิจกรรมที่ 1** จัดตั้งคณะทำงานและผู้รับผิดชอบการจัดการความรู้ของภายในมหาวิทยาลัยราชภัฏกำแพงเพชร	ต.ค. 2567	1. คำสั่งแต่งตั้งคณะกรรมการ จำนวน 1 ฉบับ	- ผู้บริหารของสำนักฯ - ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ - บุคลากรของสำนักฯ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
		กิจกรรมที่ 2 จัดการประชุมนำเสนอและทบทวนแผนการจัดการความรู้เพื่อเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร	พ.ย. 2567	1. แผนการจัดการความรู้ จำนวน 1 เรื่อง	- บุคลากรตามคำสั่งในกิจกรรมที่ 1	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
2	การเสาะหาความรู้ที่ต้องการ	**กิจกรรมที่ 3** จัดประชุมแลกเปลี่ยนเรียนรู้เพื่อกำหนดขอบเขตขององค์ความรู้ให้แก่กลุ่มเป้าหมาย - บุคลากรสายสนับสนุน - นักศึกษา	ธ.ค. 2567	1. หัวข้อขององค์ความรู้ที่ต้องการเผยแพร่ให้กลุ่มเป้าหมาย - บุคลากรสายสนับสนุน จำนวน 13 หน่วยงาน - นักศึกษา จำนวน 6 คณะ	- รองอธิการบดีฝ่ายวิชาการ - Admin - อาจารย์ผู้สอนรายวิชาความฉลาดรู้ทางดิจิทัล สารสนเทศและสื่อ	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
3	การปรับปรุง ดัดแปลง หรือสร้างความรู้บางส่วนให้เหมาะต่อการใช้งานของตน	**กิจกรรมที่ 4** นำขอบเขตขององค์ความรู้จากกิจกรรมที่ 3 จัดกิจกรรมแลกเปลี่ยนเรียนรู้ให้เหมาะสมกับกลุ่มเป้าหมาย - บุคลากรสายสนับสนุน - นักศึกษา	ม.ค. 2568	1. แนวปฏิบัติ หรือนวัตกรรมการเผยแพร่องค์ความรู้ที่ต้องการให้กลุ่มเป้าหมาย จำนวน 1 เรื่อง	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
4	การประยุกต์ใช้ความรู้ในกิจการงานของตน	**กิจกรรมที่ 5** นำความรู้ที่ได้จากกิจกรรมที่ 4 ไปดำเนินงานในหน่วยงานของตน	ม.ค. - เม.ย. 2568	1. บันทึกความรู้การร่วมกิจกรรม จำนวน 1 กิจกรรม 2. องค์ความรู้การร่วมกิจกรรม จำนวน 1 องค์ความรู้	- บุคลากรสายสนับสนุน	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
5	การนำประสบการณ์จากการทำงาน และการประยุกต์ ใช้ความรู้มาแลกเปลี่ยนเรียนรู้ และสกัด“ขุมความรู้” ออกมาบันทึกไว้	**กิจกรรมที่ 6** นำองค์ความรู้ที่ได้มาเผยแพร่ผ่าน Website และช่องทางอื่นๆ	พ.ค. 2568	1. จำนวนช่องทางการเผยแพร่องค์ความรู้ จำนวนอย่างน้อย 2 ช่องทาง	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ
		กิจกรรมที่ 7 สร้างชุมชนการเรียนรู้	พ.ค. 2568	1. กลุ่มที่ใช้สำหรับแลกเปลี่ยนเรียนรู้ทางโซเชียลมีเดีย อย่างน้อย 1 กลุ่ม 2. สื่อส่งเสริมการเรียนรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จำนวนอย่างน้อย 5 ชิ้น	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลำดับ	วิธีการสู่ความสำเร็จที่คาดการณ์	กิจกรรมการจัดการความรู้	ระยะเวลา	ตัวชี้วัดและค่าเป้าหมาย	กลุ่มเป้าหมาย	ผู้รับผิดชอบ
6	การจดบันทึก “ขุมความรู้” และ “แก่นความรู้” สำหรับไว้ใช้งาน และปรับปรุงเป็นชุดความรู้ที่ครบถ้วน ลุ่มลึกและเชื่อมโยงมากขึ้น เหมาะต่อการใช้งานมากยิ่งขึ้น	**กิจกรรมที่ 8** จัดทำแนวปฏิบัติ หรือนวัตกรรม เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษามหาวิทยาลัยราชภัฏกำแพงเพชร	พ.ค. 2568	1. แนวปฏิบัติ หรือนวัตกรรม เผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างน้อย 1 ชิ้น	- บุคลากรสายสนับสนุน - นักศึกษา	- ผู้รับผิดชอบการจัดการความรู้ของสำนักฯ

ลงชื่อ.....
(นางสาวอรปรียา คำแพ่ง)
ผู้รับผิดชอบงานการจัดการความรู้
วัน เดือน ปี .....2.....ธันวาคม.....พ.ศ.2567.....

ลงชื่อ.....
(ผู้ช่วยศาสตราจารย์พรหมเมศ วีระพันธ์)
คณบดี/ผู้อำนวยการ/หัวหน้างาน
วัน เดือน ปี .....2.....ธันวาคม.....พ.ศ.2567.....

วงจรการเรียนรู้ (Learning Cycle)

วงจรการเรียนรู้	การประยุกต์ใช้
1. การมีคลังความรู้	มีคลังความรู้ที่ชัดแจ้ง (Explicit Knowledge) จากบทความ วิดีโอ สื่อส่งเสริมการเรียนรู้รูปแบบต่างๆ และความรู้ที่อยู่ในคน (Tacit Knowledge) จากผู้เชี่ยวชาญ
2. การผลักดันให้นำความรู้ไปใช้	ผู้บริหารของสำนักฯ ช่วยผลักดันให้บุคลากรได้พัฒนาความรู้และนำความรู้ไปใช้ โดยจัดกิจกรรมแลกเปลี่ยนเรียนรู้ ทั้งในภาคทฤษฎีและเชิงปฏิบัติการให้กับกลุ่มเป้าหมาย - เผยแพร่องค์ความรู้ในรูปแบบต่างๆ ผ่านเวทีการนำเสนอความรู้
3. การนำความรู้ไปใช้	บุคลากรและนักศึกษา สามารถนำความรู้ที่ได้ไปปรับใช้ร่วมกับการดำเนินงานที่ได้รับมอบหมาย หรือประยุกต์ใช้ในชีวิตประจำวันได้อย่างถูกต้อง เหมาะสมตามตามเจตนารมณ์ของกฎหมาย
4. การสรุปความรู้ที่ได้จากการทำกิจกรรม ปัญหาและอุปสรรคจากการทำกิจกรรมเก็บเข้าคลังความรู้	สรุปองค์ความรู้เข้าคลังความรู้ เพื่อให้บุคคลอื่นสามารถเรียนรู้และนำไปปรับใช้ให้การปฏิบัติงานมีคุณภาพยิ่งขึ้น
5. การนำความรู้มาปรับเป็นแนวปฏิบัติในการดำเนินงาน	นำความรู้ และข้อเสนอแนะมาปรับปรุงการดำเนินงาน หรือปรับปรุงให้แนวปฏิบัติ หรือนวัตกรรมครบถ้วน สมบูรณ์มากขึ้น

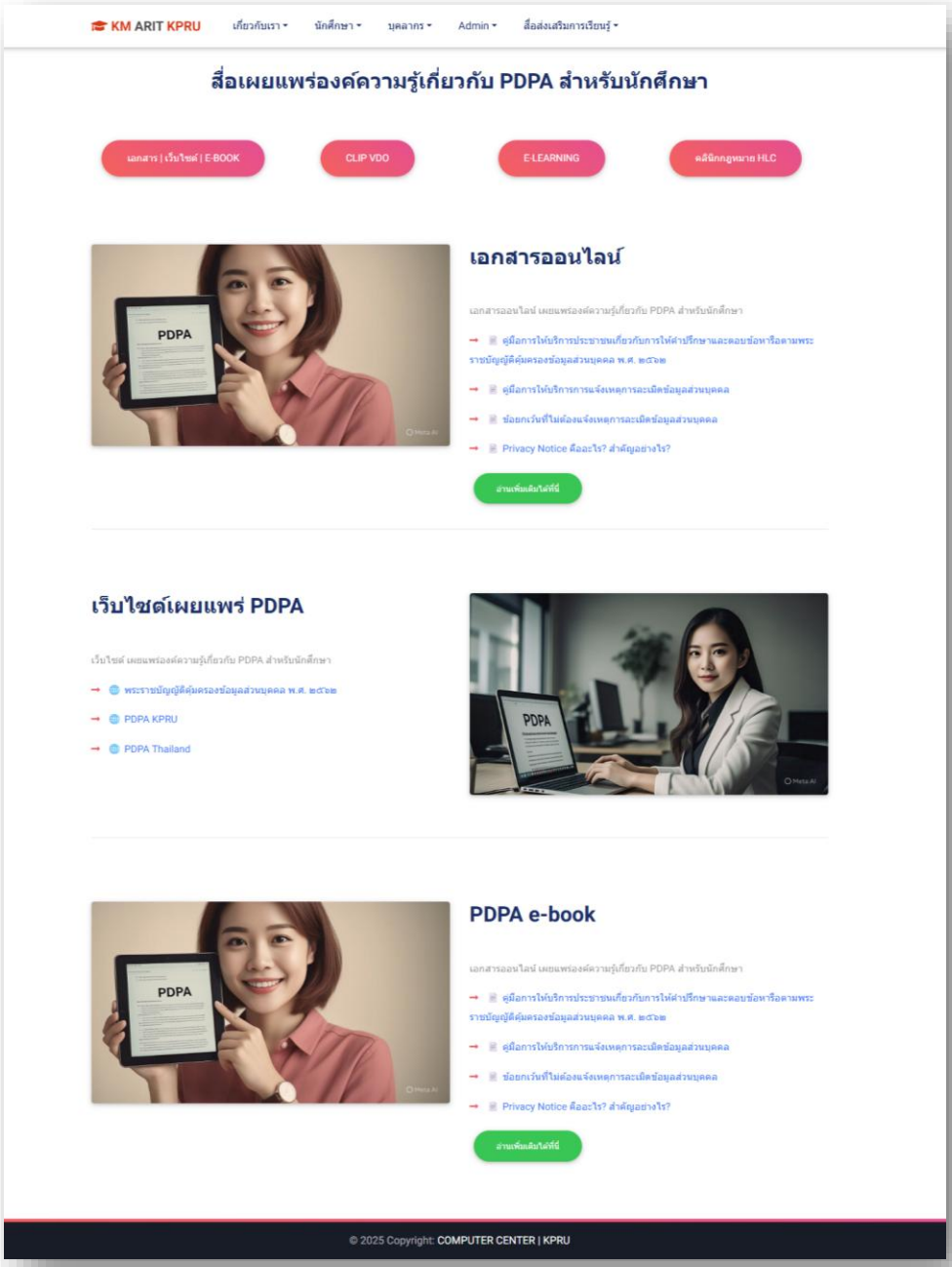
เว็บไซต์การจัดการความรู้

PDPA (Personal Data Privacy Policy)

เรื่อง "การเผยแพร่องค์ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับบุคลากรและนักศึกษา มหาวิทยาลัยราชภัฏกำแพงเพชร"

https://kpru.ac.th/km-pdpa/

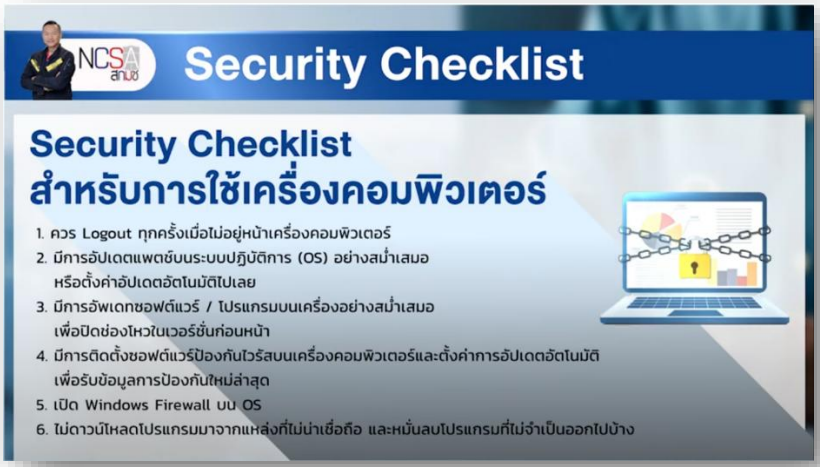
เอกสาร/เว็บไซต์/e-book
เผยแพร่องค์ความรู้เกี่ยวกับ PDPA

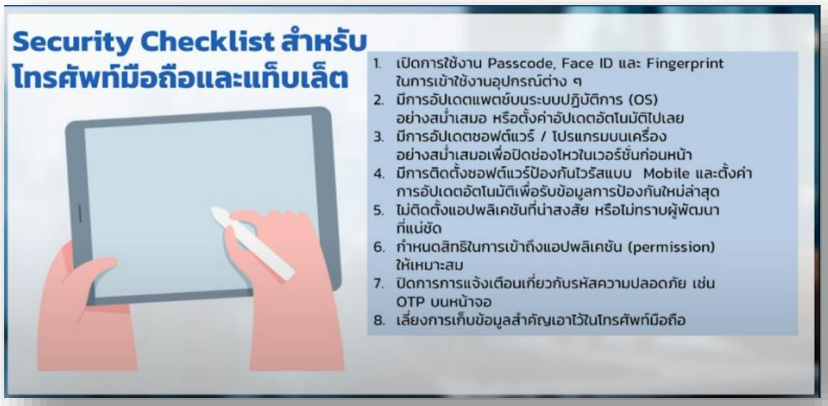


Clip VDO สื่อเผยแพร่องค์ความรู้เกี่ยวกับ PDPA

สื่อการเรียนรู้เกี่ยวกับ PDPA รูปแบบ e-Learning

ตัวอย่างสื่อส่งเสริมการเรียนรู้จากภายนอก





Security Checklist สำหรับการใช้งาน Wi-Fi

1. เปลี่ยนรหัสผ่านของอุปกรณ์ Wi-Fi router ที่บ้าน ไม่ใช้ค่าตั้งต้นที่กำหนดมาจากโรงงานผู้ผลิต (Default)
2. เปลี่ยน SSID และรหัสผ่านของ Wi-Fi ที่กำหนดมาจากผู้ให้บริการและซ่อน SSID ถ้าหากเป็นไปได้
3. กำหนดผู้ที่สามารถเชื่อมต่อ Wi-Fi ที่บ้านของเราได้ เช่น การล็อกให้เฉพาะเครื่องที่มี Mac address ที่กำหนดไว้ เข้าใช้งานได้เท่านั้น
4. ไม่เชื่อมต่อ Public Wi-Fi หรือ Free hotspot ที่เปิดให้ใช้งานได้ฟรีแบบไม่มีรหัสผ่าน
5. หลีกเลี่ยงการใช้งาน Public Wi-Fi ที่ไม่ทราบแหล่งที่มาในการเปิดให้บริการ
6. เมื่อออกจากบ้านควรปิดสัญญาณ Wi-Fi เพื่อป้องกันการเชื่อมต่อ Public Wi-Fi อัตโนมัติ

ข้อควรปฏิบัติเมื่อเจอ "อีเมลฟิชชิ่ง"

1. ระวังหากจุดประสงค์ของลิงค์คือ
   - ยืนยันตัวตนของเรา
   - ให้ตรวจสอบบัญชีของคุณ
   - ให้ Update บัญชีของเรา
   - ระบุหมายบัตรเครดิต หรือเลขประกันสังคมของเรา ดาวน์โหลดซอฟต์แวร์

2. ปฏิบัติต่ออีเมลใด ๆ ที่ขอให้เราคลิกลิงค์ด้วยความระมัดระวัง
   - อย่าตอบกลับคำขอล็อคอินเข้าสู่ระบบ/รีเซ็ตรหัสผ่านที่มาจากอีเมล์ซึ่งเราไม่ได้เป็นผู้ริเริ่มหรือคาดหวัง
   - อย่าให้รายละเอียดส่วนตัวของเราผ่านทางอีเมลหรือลิงค์ในอีเมลใดๆ โดยเฉพาะอย่างยิ่งหากอีเมลนั้นไม่พึงประสงค์
3. บริษัทขนาดใหญ่มักไม่ส่งอีเมลพร้อมลิงค์แนบมาเพื่อให้ลูกค้าของบริษัทยืนยันรายละเอียดส่วนบุคคล
   - หากมีข้อกังวลใด ๆ ควรโทรศัพท์ถึงบริษัทนั้นเป็นการส่วนตัวหรือไปที่สาขา และอธิบายรายละเอียดให้ทราบ

Password management

รหัสผ่านที่พบบ่อยที่สุด

1. 123456 – 2,543,285 คน
2. 123456789 – 961,435 คน
3. picture1 – 371,612 คน
4. password – 360,467 คน
5. 12345678 – 322,187 คน
6. 111111 – 230,507 คน
7. 123123 – 189,327 คน
8. 12345 – 188,268 คน
9. 1234567890 – 171,724 คน
10. senha – 167,728 คน
11. 1234567 – 165,909 คน
12. qwerty – 156,765 คน
13. abc123 – 151,804 คน
14. Million2 – 143,664 คน
15. 000000 – 122,982
16. 1234 – 112,297 คน
17. iloveyou – 106,327 คน
18. qqww1122 – 85,476 คน

วิธีตั้งรหัสผ่านที่ปลอดภัย

1. รหัสผ่านต้องประกอบไปด้วย ตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก และตัวเลข ที่สลับลำดับกันหรืออาจจะผสมอักขระพิเศษลงไปด้วยก็ได้ (ยิ่งหลากหลายยิ่งถอดรหัสได้ยากขึ้น)
2. ควรตั้งรหัสผ่านให้มีความยาวอย่างน้อย 8 ตัวอักษรขึ้นไป
3. ไม่ควรตั้งรหัสผ่านเป็นเบอร์โทรศัพท์หอถ้อยคำใด ๆ ที่เกี่ยวกับเรา เช่น ตั้งรหัสผ่านโดยใช้ชื่อ เบอร์โทร และข้อมูลอื่น ๆ เกี่ยวกับตัวเราหรือญาติพี่น้อง เป็นต้น
4. การตั้งรหัสผ่านเป็นคำไม่มีความหมาย มีความปลอดภัยกว่าการตั้งรหัสเป็นคำที่มีความหมาย เช่น do&12sS@d2 เป็นต้น
5. รหัสผ่านควรมีการเปลี่ยนอย่างน้อย 1 ครั้งภายใน 2-3 เดือน
6. หลีกเลี่ยงการตั้งรหัสผ่านหลาย ๆ บัญชีเป็นรหัสผ่านเดียวกัน เพื่อเป็นการลดความเสี่ยงที่จะโดนเจาะเข้าบัญชีอื่น ๆ ด้วย
7. ไม่ควรเลือกการจดจำรหัสผ่านอันมัติในเบราว์เซอร์ เพราะอย่าลืมว่ามันสามารถข้ามาดูได้โดยง่ายๆเลย


14 ประเภท คดีออนไลน์
จำนวน
คิดเป็น
ความเสียหาย
1 หลอกลวงซื้อขายสินค้าหรือบริการ ไม่เป็นขบวนการ 365,075 47.22% 5,035,793,009
2 หลอกให้โอนเงินเพื่อทำงานฯ 98,139 12.69% 12,859,745,775
3 หลอกให้กู้เงิน 74,147 9.59% 3,586,095,339
4 หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ 51,881 6.71% 28,441,508,012
5 ข่มขู่ทางโทรศัพท์ (Call Center) 51,678 6.68% 10,761,310,285
กลัว โลภ หลง
NCSA สกมช
National Cyber Security Agency
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ


แฉ!! กลโกงมิจฉาชีพแจกไอโฟน
NCSA สกมช
มิจฉาชีพแอบอ้างโดยใช้กลอุบาย แจกฟรี!! มือถือไอโฟนหลังจากนั้นจะให้แอดเข้าไปที่ไลน์แอดเพื่อทำการหลอกให้โอนเงิน โดยจะแอบแฝงโพสตามกลุ่มผู้เสียหายทุกเพศทุกวัยโดยเน้นไปที่กลุ่มนักเรียนเป็นส่วนใหญ่ และแอบแฝงด้วยการสร้างโปรไฟล์ปลอมเป็นบุคคลอื่น
กลโกงมิจฉาชีพที่ใช้หลอกเหยื่อ
เสียทั้งเงินและข้อมูลส่วนตัว
NCSA สกมช
National Cyber Security Agency
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ


จัดการคอลเซ็นเตอร์แสบ แอบอ้างเป็นเจ้าหน้าที่
เจ้าหน้าที่
1. อ้างเป็นเจ้าหน้าที่ธนาคาร : ให้ติดต่อสอบถาม call center ของธนาคารโดยตรง
2. อ้างเป็นหน่วยงานรัฐ : ให้โทรสอบถามจากหน่วยงานนั้น ๆ
3. อ้างว่า รับแจ้งความสอบสวนทางโทรศัพท์ : ให้นัดเจ้าหน้าที่เพื่อแจ้งความ ณ สถานที่ราชการด้วยตนเอง
4. หากสนทนาทาง Video call : มีสติ สังเกต ภาพ เสียง ปาก และท่าทางว่ามีความผิดปกติหรือไม่
NCSA สกมช
National Cyber Security Agency
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ


ศูนย์ AOC 1441
แก้ปัญหาหลอกลวงออนไลน์
#NCSA
NCSA
สกมช
National Cyber Security Agency
สำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ


ป้องกัน
โจร ONLINE
หลอกให้ท่าน ....
กลัว
โลภ
หลง
หลีกการสัมผัสโจร
ไม่รับ
เบอร์แปลก
ไม่ CLICK LINK
ใน SMS
ไม่รับเพื่อนแปลกหน้า
ใน SOCIAL
โดนหลอกออนไลน์ ! 24hr
ไม่รู้ทำอย่างไร โทรเลย
AOC 1441
NCSA Thailand
www.ncsa.or.th
saraban@ncsa.or.th

แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล
มหาวิทยาลัยราชภัฏกำแพงเพชร
เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล
มหาวิทยาลัยราชภัฏกำแพงเพชร
เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

มหาวิทยาลัยราชภัฏกำแพงเพชร กำหนดแนวปฏิบัติสำหรับการดำเนินการของหน่วยงานภายในมหาวิทยาลัยราชภัฏกำแพงเพชร ที่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งมีทั้งหมด 5 ข้อ ดังนี้

มาตรา 37 (1) *จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด*

แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา 37 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 "จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด"

หน่วยงานต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล อย่างน้อยดังต่อไปนี้

1. มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

1.1 ให้มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย มีการกำหนดให้มีบันทึกการเข้าออกพื้นที่ ให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง ทั้งนี้ความเข้มข้นของมาตรการ เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

1.2 ให้มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) แบ่งเป็น รูปแบบต่างๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

2. มาตรการป้องกันด้านเทคนิค (technical safeguard)

2.1 จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

2.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

2.3 จัดให้มีระบบสำรองและกู้คืนข้อมูลอย่างเหมาะสม เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

3. มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

3.1 มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น

- มีบันทึกการเข้าออกพื้นที่
- มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่
- มีระบบกล้องวงจรปิดติดตั้ง
- มีการล็อคประตูทุกครั้ง
- มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก

ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

3.2 กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

มาตรา 37 (2) *ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ*

แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา 37 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 "ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ"

หน่วยงานต้องจัดให้มีมาตรการดำเนินการ อย่างน้อยดังต่อไปนี้

1. การประเมินก่อนส่งมอบข้อมูล

1.1 ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล

1.2 ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด (เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่ หรือเพียงปี พ.ศ. เกิด และ รหัสไปรษณีย์ ก็เพียงพอ) และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคล (เช่น ชื่อ-นามสกุล เลขประจำตัว 13 หลัก) หรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงต่อการนำไปใช้ประโยชน์หรือไม่

2. เมื่อส่งมอบข้อมูล

2.1 จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

2.2 ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

2.3 แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

3. หลังส่งมอบข้อมูล

3.1 ติดตามการใช้งานเป็นครั้งคราว เช่น ทุก 3 เดือน 6 เดือน หรือ 1 ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือนิติบุคคลนั้น ลบทำลายข้อมูล

2.4 กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา

มาตรา 37 (3) *จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้ เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม*

แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา 37 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 "จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม"

หน่วยงานต้องจัดให้มีมาตรการดำเนินการ อย่างน้อยดังต่อไปนี้

1. ติดตามอย่างสม่ำเสมอ (เช่น ทุกสัปดาห์ หรือ ทุกเดือน) ว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรอไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือ ตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

2. กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

3. การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ทั้งนี้ ต้องจัดให้มีมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

มาตรา 37 (4) *แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการ ประกาศกำหนด*

แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา 37 (4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 "แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการ ประกาศกำหนด"

หน่วยงานต้องจัดให้มีมาตรการดำเนินการ อย่างน้อยดังต่อไปนี้

1. แจ้งให้บุคลากรผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏกำแพงเพชร ในฐานะตัวแทนของสถาบันให้ชัดเจน เช่น การส่งอีเมลล์ และแจ้งทางโทรศัพท์ กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

2. กำหนดวิธีปฏิบัติให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสถาบันต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน 72 ชั่วโมง (นับแต่ทราบเหตุ)

3. การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น

3.1 ตัวอย่างกรณีความเสี่ยงต่ำ: ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

3.2 ตัวอย่างกรณีความเสี่ยงสูง: เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์(ตรวจพบ 1 เดือนหลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน 72 ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

3.3 ตัวอย่างกรณีความเสี่ยงต่ำ: เจ้าหน้าที่ของหน่วยงานส่งอีเมลลิไปยังผู้รับผิดพลาด ซึ่งแนบไฟล์รายชื่อผู้เข้าอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่อีเมลล์ และข้อจำกัดในการทานอาหาร ซึ่งมีเพียง 2 คน ใน 15 คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลล์ถูกส่งไปยังผู้เข้าอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตามแม้ข้อมูลสุขภาพ จะถูกเผยแพร่ไปยังผู้ไม่เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

> ***มาตรา 37 (5)*** *ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล*

แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา 37 (5) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 "ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล"

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในข้อนี้ ยังไม่มีความจำเป็นที่ มหาวิทยาลัย ต้องดำเนินการใด ๆ

หมายเหตุ แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ดำเนินการภายใต้นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏกำแพงเพชร

แผนบริหารความเสี่ยง สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

แบบ RM-1

แบบกำหนดขอบเขตความรับผิดชอบตามประเด็นยุทธศาสตร์
ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

ประเด็นยุทธศาสตร์มหาวิทยาลัยที่ตอบสนอง	กลยุทธ์/ประเภทความเสี่ยง/โครงการ/งานประจำ	วัตถุประสงค์	ตัวชี้วัด	เป้าหมาย	ผู้รับผิดชอบ
4. การพัฒนาสู่มหาวิทยาลัยสมรรถนะสูง	4.1 พัฒนาระบบและกลไกการบริหารจัดการด้วยหลักธรรมาภิบาล มุ่งสู่การเป็นมหาวิทยาลัยสมรรถนะสูง	เพื่อบำรุงรักษาระบบเครือข่ายให้มีประสิทธิภาพในการให้บริการภายในมหาวิทยาลัยฯ	KPI13 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมาย คะแนน 5) KPI14 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80) KPI15 – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย อย่างน้อยร้อยละ 80)	(เป้าหมาย คะแนน 5)	ผศ.พรหมเมศ วีระพันธ์ ผศ.ศิลป์ณรงค์ ฉวีพัฒน์

แบบ RM-2

แบบฟอร์มการวิเคราะห์ความเสี่ยง

ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

งานหลักของฝ่าย (1)	ความเสี่ยง (2)	สถานะปัจจุบัน (3)	ปัจจัยเสี่ยง (4)		ผลกระทบ (5)	KPI (6)	โอกาสที่จะเกิด (L) (7)	ผลกระทบ (C) (8)	ระดับความเสี่ยง (9)	ระดับความเสี่ยงที่คาดหวัง (10)	แนวทางการตอบสนอง (11)
			ภายนอก	ภายใน							
งานประจำ (Routine : R)											
4.1 พัฒนาระบบและกลไกการบริหารจัดการด้วยหลักธรรมาภิบาลมุ่งสู่การเป็นมหาวิทยาลัยสมรรถนะสูง	O1/การโจมตีความปลอดภัยทางไซเบอร์	1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด 2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้	1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด 2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตี	1. บุคลากรและนักศึกษายังขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกหลอกผ่านอีเมลฟิชชิ่ง (Phishing) การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงเว็บไซต์ที่ไม่น่าเชื่อถือ 2. มาตรการรักษาความปลอดภัยด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยยังไม่ครอบคลุม โดยเฉพาะการปกป้องข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมไปถึง	1. การหยุดชะงักของระบบสารสนเทศสำคัญของมหาวิทยาลัย (เช่น ระบบทะเบียน การเงิน ระบบการเรียนการสอนออนไลน์) ส่งผลต่อภาพลักษณ์ ความน่าเชื่อถือ และมีค่าใช้จ่ายสูงในการแก้ไขฟื้นฟูระบบ 2. การรั่วไหลของข้อมูลส่วนบุคคลของนักศึกษาและบุคลากร นำไปสู่การละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจส่งผลให้มหาวิทยาลัยได้รับบทลงโทษทางกฎหมาย	KPI13 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมายคะแนน 5) KPI14 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80) KPI15 – ร้อยละของ	L2=2	C6=5	10 สูง	ต่ำ	ควบคุมความเสี่ยง

งานหลักของฝ่าย (1)	ความเสี่ยง (2)	สถานะปัจจุบัน (3)	ปัจจัยเสี่ยง (4)		ผลกระทบ (5)	KPI (6)	โอกาสที่จะเกิด (L) (7)	ผลกระทบ (C) (8)	ระดับความเสี่ยง (9)	ระดับความเสี่ยงที่คาดหวัง (10)	แนวทางการตอบสนอง (11)
			ภายนอก	ภายใน							
			แบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้	การสูญหายและความเสียหายของข้อมูลสารสนเทศที่สำคัญจากกรณีของการถูกไวรัสเรียกค่าไถ่โจมตี		นักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายอย่างน้อยร้อยละ 80)					

โครงการตามยุทธศาสตร์/ประเภทความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (4)	ผู้รับผิดชอบ/ผู้รับผิดชอบหลัก (5)	ระยะเวลาดำเนินการ (6)
	2. มาตรการรักษาความปลอดภัยด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยยังไม่ครอบคลุม โดยเฉพาะการปกป้องข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมไปถึงการสูญหายและความเสียหายของข้อมูลสารสนเทศที่สำคัญจากกรณีของการถูกไวรัสเรียกค่าไถ่โจมตี 3. บุคลากรยังขาดความรู้ความเข้าใจในการป้องกันการโจมตีรูปแบบใหม่ผ่านระบบเครือข่ายอินเตอร์เน็ต 4. บุคลากรขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน					

แบบ RM 3

แบบแสดงแนวทางตอบสนองความเสี่ยง/แผนบริหารความเสี่ยง
ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

โครงการตามยุทธศาสตร์/ประเภทความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (4)	ผู้รับผิดชอบ/ผู้รับผิดชอบหลัก (5)	ระยะเวลาดำเนินการ (6)
O3/การโจมตีความปลอดภัยทางไซเบอร์	**ภายนอก** 1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด 2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้ **ภายใน** 1. บุคลากรและนักศึกษายังขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกหลอกผ่านอีเมลฟิชชิ่ง (Phishing) การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงเว็บไซต์ที่ไม่น่าเชื่อถือ	KPI13 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมาย คะแนน 5) KPI14 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย ร้อยละ 80) KPI15 – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย อย่างน้อยร้อยละ 80)	ระดับสูง	1. ดำเนินการจัดตั้งคณะทำงานและผู้รับผิดชอบ 2. ประชุมคณะกรรมการดำเนินงาน จัดทำนโยบายวางแผนการดำเนินงาน 3. จัดอบรมเกี่ยวกับ เรื่อง การป้องกันความมั่นคงปลอดภัยไซเบอร์ 4. สรุปผลการจัดกิจกรรม 5. จัดทำแผนรักษาความมั่นคงปลอดภัยไซเบอร์ 6. จัดทำแนวปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 7. แบบประเมินความสอดคล้อง ของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 8. จัดทำนโยบายการรักษาความมั่นคงปลอดภัย	1. ผศ.พรหมเมศ วีระพันธ์ 2. ผศ.ศิลป์ณรงค์ ฉวีพัฒน์	ปีงบประมาณ 2568