สรุปกิจกรรมแลกเปลี่ยนเรียนรู้การพัฒนาเว็บไซต์ ครั้งที่ 1
วันที่ 1 ธันวาคม 2568 เวลา 09.00-12.00 น.
ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มรภ.กพ.

ประเด็นหัวข้อ

1. เกี่ยวกับ Webometrics
2. การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.
3. ความก้าวหน้าเกี่ยวกับการรักษาความปลอดภัยของเว็บไซต์

1.1 เกี่ยวกับ Webometrics

รอบที่ 1 ปี 2568

1. เว็บ www.webometrics.info ไม่สามารถเข้าถึงได้ และย้ายไปแสดงผลที่ www.figshare.com แทน
2. ไม่มีการแสดงอันดับของ Impact Rank, Openness Rank และ Excellence Rank โดยจะแสดงเพียงค่า WR (World Rank) อย่างเดียว
3. แสดงออกมาเป็นไฟล์ pdf ไม่มีการแสดงผลในรูปแบบข้อมูลในเว็บไซต์

รอบที่ 2 ปี 2568

1. ค่าการเปิดเผยข้อมูลอ้างอิงทั้งหมด (Total citations) จาก เกณฑ์ Openness จากเดิมใช้จาก Google Scholar แจ้งว่า เปลี่ยนมาใช้ OpenAlex แทน
2. เกณฑ์ IMPACT ใช้แหล่งข้อมูลเดียว คือ MAJESTIC
3. แสดงผลที่ www.figshare.com เป็นไฟล์ pdf ไม่มีการแสดงผลในรูปแบบข้อมูลในเว็บไซต์ อ้างอิงจาก https://figshare.com/articles/preprint/Ranking_Web_of_Universities_webometrics_info_July_2025_edition/ 29588921?file=56338199

ปัจจุบัน **Webometrics.org** คือแพลตฟอร์มการจัดอันดับมหาวิทยาลัยที่ได้รับการยอมรับทั่วโลก ซึ่งมุ่งเน้นการประเมินผลการดำเนินงานด้านดิจิทัลและวิชาการของสถาบันอุดมศึกษา การจัดอันดับของเราตั้งอยู่บนหลักการของความโปร่งใส ความเปิดกว้าง และการวิเคราะห์ข้อมูล นำเสนอมุมมองที่หลากหลายครอบคลุมสถาบันกว่า 30,000 แห่งทั่วโลก

Webometrics.org ส่งเสริมศักยภาพนักศึกษา นักวิจัย และผู้กำหนดนโยบาย ด้วยข้อมูลเชิงเปรียบเทียบที่เชื่อถือได้ ซึ่งสนับสนุนการตัดสินใจอย่างรอบรู้ในด้านการศึกษาและการวิจัย

การรวบรวมข้อมูล สถาบันมากกว่า 32,000 แห่ง จากกว่า 200 ประเทศ ประกาศผลเดือนมกราคมและกรกฎาคม

Ranking Indicators	เกณฑ์การจัดอันดับ
We use a composite scoring model combining normalized indicators to ensure fair and balanced evaluation: **Visibility**: Impact based on number of external referring domains *(Ahrefs.com)* – **50%** **Transparency**: Citations from top 310 cited researchers (excluding top 20 outliers) *(Google Scholar profiles)* – **10%** **Excellence**: Research papers in the top 10% most cited (2019–2023) *(Scopus / Scimago)* – **40%**	เราใช้แบบจำลองการให้คะแนนแบบผสมที่ผสมผสานตัวบ่งชี้มาตรฐาน เพื่อให้มั่นใจว่าการประเมินมีความยุติธรรม และสมดุล: **การมองเห็น:** ผลกระทบอ้างอิงจากจำนวนโดเมนที่อ้างอิงภายนอก (Ahrefs.com) – **50%** **ความโปร่งใส:** การอ้างอิงจากนักวิจัย 310 อันดับแรกที่ได้รับการอ้างอิง (ไม่รวม 20 อันดับแรก) (โปรไฟล์ Google Scholar) **– 10%** **ความเป็นเลิศ:** บทความวิจัยที่อยู่ใน 10% อันดับแรกที่ได้รับการอ้างอิงมากที่สุด (2019–2023) (Scopus / Scimago) **– 40%**
We Measure • Research and scholarly impact • Academic openness and visibility • Digital engagement and third-party references • Performance across all university missions: education, research, and public service **We Do Not Measure** • Website design or user experience • Visitor traffic or analytics • Marketing or advertising activity	**เราวัดผล** • งานวิจัยและผลกระทบทางวิชาการ • ความเปิดกว้างและการมองเห็นทางวิชาการ • การมีส่วนร่วมทางดิจิทัลและการอ้างอิงจากบุคคลที่สาม • ประสิทธิภาพในพันธกิจของมหาวิทยาลัยทั้งหมด ได้แก่ การศึกษา การวิจัย และการบริการสาธารณะ **เราไม่ได้วัดผล** • การออกแบบเว็บไซต์หรือประสบการณ์ผู้ใช้ • ปริมาณผู้เข้าชมหรือการวิเคราะห์ • กิจกรรมทางการตลาดหรือการโฆษณา

WEBOMETRICS
GLOBAL WEB RANKINGS FOR UNIVERSITIES

Thailand Ranking July 2025 – Webometrics Global Position

Explore Thailand's July 2025 Webometrics ranking across global visibility, research excellence, openness, and academic performance. See how it compares worldwide.

Webometrics.org เป็นแพลตฟอร์มการจัดอันดับมหาวิทยาลัยอิสระ และไม่มีส่วนเกี่ยวข้องกับเว็บไซต์ Webometrics[.]info เดิม หรือ Consejo Superior de Investigaciones Científicas (CSIC) การจัดอันดับบนเว็บไซต์นี้อ้างอิงจากข้อมูลที่เผยแพร่ต่อสาธารณะ ตัวชี้วัดที่โปร่งใส และวิธีการที่พัฒนาขึ้นโดยอิสระ

10 อันดับแรกในไทย

Ranking	World Rank	University	Country	Impact Rank	Openness Rank	Excellence Rank
1	317	Chulalongkorn University		501	591	458
2	399	Mahidol University		769	789	535
3	437	Chiang Mai University		650	920	697
4	609	Kasetsart University		608	1358	1270
5	623	Khon Kaen University		921	1099	977
6	664	Prince of Songkla University		1028	1264	1037
7	732	Thammasat University		914	1476	1380
8	759	King Mongkut's University of Technology Thonburi		1107	1398	1231
9	904	King Mongkut's University of Technology North Bangkok		1509	1671	1343
10	948	Asian Institute of Technology Thailand		1121	2640	2126

Kamphaeng Phet Rajabhat University Ranking July 2025 – Webometrics Global Position

Explore Kamphaeng Phet Rajabhat University's July 2025 Webometrics ranking across global visibility, research excellence, openness, and academic performance. See how it compares worldwide.

Year	Edition	World Rank	Continent Rank	Country Rank	Impact Rank	Openness Rank	Excellence Rank
2025	july	8461	2410	70	8198	6557	7461
2025	jan	8461	2583	67	8182	6569	7445
2024	jan	31340	2193	67	31541	6454	7505
2023	jan	7466	2571	66	6627	6175	7237
2022	jan	7226	2055	62	6276	5716	7216
2021	jan	7150	1923	49	9414	4934	6650
2020	jan	7479	1842	49	9673	5373	6084
2019	jan	7549	2132	49	9526	5813	6115
2018	jan	6569	1276	33	5648	4121	5824
2016	jan	6569	1276	33	5648	4121	5824
2015	jan	4242	432	67	3367	2529	5490

Webometrics Global Web Rankings for Universities: Measuring Global Academic Impact & Visibility

Webometrics ranks global universities by visibility, research excellence, and open access. Explore our transparent methodology and global coverage.

Ranking	World Rank	University	Country	Impact Rank	Openness Rank	Excellence Rank
1	3757	Kamphaeng Phet Rajabhat University		8189	6570	24242

ที่มา: https://www.webometrics.org/kamphaeng-phet-rajabhat-university

ข้อมูล ณ วันที่ 29 พฤศจิกายน 2568

ภาพกิจกรรม

สรุปกิจกรรมแลกเปลี่ยนเรียนรู้การพัฒนาเว็บไซต์ ครั้งที่ 2
วันที่ 18 ธันวาคม 2568 เวลา 09.00-12.00 น.
ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มรภ.กพ.

ประเด็นหัวข้อ

1. เกี่ยวกับ “การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.”
2. ความก้าวหน้าเกี่ยวกับการรักษาความปลอดภัยของเว็บไซต์

1. ผลการดำเนินงานเกี่ยวกับการถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.

- **ความเสี่ยง** การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ. https://kpru.ac.th/km-web/files/risk-kpru2569-v2.pdf
- **ควบคุมภายใน** การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ. https://kpru.ac.th/km-web/files/audit-pdpa-kpru.pdf
- **แผนการจัดการความรู้** สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จัดทำแผนการจัดการความรู้ (KM Action Plan) ประจำปีการศึกษา 2568 ด้านพันธกิจอื่นๆ
  ประเด็นการจัดการความรู้ **“แนวทางปฏิบัติงานเพื่อลดความเสี่ยงข้อมูลรั่วไหลและป้องกันการละเมิดข้อมูลส่วนบุคคล”**
  https://kpru.ac.th/km-web/files/ok-plankm-pdpa-risk-zero-final.pdf
- **คำสั่ง** แต่งตั้งคณะกรรมการดำเนินงานและกำกับการใช้ข้อมูลส่วนบุคคล https://www.kpru.ac.th/km-web/files/command-pdpa2569.pdf

ตาราง ประเด็นความเสี่ยง เรื่อง การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ผู้รับผิดชอบ/ผู้รับผิดชอบหลัก (6)	ระยะเวลาดำเนินการ (7)
O1/การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.	**(ปัจจัยภายนอก)** 1. ภัยคุกคามทางไซเบอร์ต่อมหาวิทยาลัย ซึ่งจะทำให้ข้อมูลถูกละเมิด **(ปัจจัยภายใน)** 1. บุคลากรและนักศึกษาขาดความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) และกฎหมายที่เกี่ยวข้อง 2. ผู้ควบคุม/ผู้ประมวลผล/เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) 3. บุคลากรในมหาวิทยาลัยฯ นำข้อมูลไปใช้ผิดวัตถุประสงค์	**KPI1** – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยข้อมูลส่วนบุคคล (เป้าหมาย ร้อยละ 60) **KPI2** – ระดับความรู้ความเข้าใจของบุคลากรที่เข้ารับการอบรม (เป้าหมาย ระดับดี) **KPI3** – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยของข้อมูลส่วนบุคคล (เป้าหมายอย่างน้อยร้อยละ 70) **KPI4** – ระดับความสำเร็จในการดำเนินการจัดการความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคล (เป้าหมาย 5 คะแนน) **KPI5** - จำนวนครั้งข้อมูลส่วนบุคคลที่มหาวิทยาลัยจัดเก็บถูกนำไปเผยแพร่โดยไม่ได้รับอนุญาต (เป้าหมาย 0 ครั้ง)	4(L1) x 4(C14) สูงมาก	1. จัดตั้งคณะทำงานและผู้รับผิดชอบ 2. ประชุมคณะกรรมการดำเนินงาน จัดทำนโยบาย วางแผนการดำเนินงาน 3. จัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล อย่างต่อเนื่อง โดยแยกประเภทของผู้ที่มีหน้าที่และความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) 4. กำหนดให้เจ้าหน้าที่ที่เกี่ยวข้องลงนามในสัญญารักษาความลับ 5. จัดกิจกรรมแลกเปลี่ยนเรียนรู้กลุ่มบุคลากรตามคำสั่งฯ เพื่อให้การปฏิบัติงานสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) 6. สรุปผลการจัดกิจกรรม 7. จัดทำมาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 8. จัดทำแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล และมีช่องทางการร้องเรียน กรณีที่มีเหตุการละเมิดข้อมูลส่วนบุคคล	- รองอธิการบดีฝ่ายวิชาการ - ผอ. สำนักวิทยบริการฯ - ผอ. สำนักส่งเสริมฯ - ผอ. กองพัฒนานักศึกษา - รอง ผอ. สำนักวิทยบริการฯ - รอง ผอ. สำนักส่งเสริมฯ - อาจารย์นฤชล เชื่อนยัง	ปีงบประมาณ 2569

การประเมินผลการควบคุมภายใน ด้านการดำเนินงาน(O) ความเสี่ยง “การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.”

กระดาษทำการ (Work Sheet)
เรื่อง การสอบทานแบบประเมินความเสี่ยงภารกิจเพื่อการควบคุมภายใน

(2) ภารกิจ/งาน	(3) วัตถุประสงค์ของภารกิจ/งาน	(4) ประเภท OBJ			(5) ความเสี่ยง	(6) ปัจจัยเสี่ยง		การประเมินความเสี่ยง						
		O ด้านการดำเนินงาน	R ด้านการรายงาน	C ด้านการปฏิบัติตามกฎระเบียบ		ภายใน	ภายนอก	(7) การควบคุมที่มีอยู่	(8) ความเสี่ยงที่เหลืออยู่	(9) ผลกระทบ	(10) ค่าคะแนนผลกระทบ	(11) ค่าคะแนนโอกาส	(12) ค่า/ระดับความเสี่ยง	(13) วิธีการตอบสนองความเสี่ยง
6) ด้านการบริหารจัดการ พัฒนาระบบ และกลไกการบริหารจัดการด้วยหลักธรรมาภิบาล มุ่งสู่การเป็นมหาวิทยาลัยสมรรถนะสูง	1. เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา 2. เพื่อยกระดับธรรมาภิบาลหน่วยงานให้มีมาตรการบริหารข้อมูลอย่างเป็นระบบและโปร่งใส	✓			การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากร และนักศึกษา มรภ.กพ.	1. บุคลากรและนักศึกษาขาดความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) และกฎหมายที่เกี่ยวข้อง 2. ผู้ควบคุม/ผู้ประมวลผล/เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) 3. บุคลากรในมหาวิทยาลัยฯ นำข้อมูลไปใช้ผิดวัตถุประสงค์	ภัยคุกคามทางไซเบอร์ต่อมหาวิทยาลัย ซึ่งจะทำให้ข้อมูลถูกละเมิด	1. จัดทำเว็บไซต์และป้ายประชาสัมพันธ์เชิญชวนเปลี่ยนรหัสผ่านและ ยกระดับความปลอดภัยบัญชี เพื่อเชิญชวนบุคลากรและนักศึกษา เปลี่ยน PASSWORD เพื่อความปลอดภัยของข้อมูลส่วนตัวและข้อมูลสำคัญของมหาวิทยาลัย 2. รวบรวมองค์ความรู้เกี่ยวกับ PDPA จัดเก็บในรูปแบบเว็บไซต์และเผยแพร่ในเว็บไซต์หลักมหาวิทยาลัย	มีการโจมตีทางไซเบอร์ในรูปแบบใหม่ๆเพื่อละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.	ข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ. รั่วไหลไปยังบุคคลอื่น/มิจฉาชีพ	C14=4	L1=4	16 สูงมาก	ควบคุมความเสี่ยง

กระดาษทำการ (Work Sheet)
เรื่อง การสอบทานรายงานการประเมินการควบคุมภายใน (แบบ ปค.5)

(2)ภารกิจตามกฎหมายที่จัดตั้งหน่วยงานของรัฐ หรือภารกิจตามแผนการดำเนินงาน หรือภารกิจอื่นๆ ที่สำคัญของหน่วยงานของรัฐ/วัตถุประสงค์	(3) ความเสี่ยง	(4) การควบคุมภายในที่มีอยู่	(5) การประเมินผลการควบคุมภายใน	(6) ความเสี่ยงที่ยังมีอยู่	(7) การปรับปรุงการควบคุมภายใน	(8) หน่วยงาน/ผู้รับผิดชอบ
ภารกิจ : ภารกิจตามกฎหมายที่จัดตั้งหน่วยงานของรัฐ **6) ด้านการบริหารจัดการ** พัฒนาระบบ และกลไกการบริหารจัดการด้วยหลักธรรมาภิบาล มุ่งสู่การเป็น มหาวิทยาลัย สมรรถนะสูง **วัตถุประสงค์** 1. เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา 2. เพื่อยกระดับธรรมาภิบาลหน่วยงานให้มีมาตรการบริหารข้อมูลอย่างเป็นระบบและโปร่งใส	การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.	1. จัดทำเว็บไซต์และป้ายประชาสัมพันธ์เชิญชวนเปลี่ยนรหัสผ่าน และยกระดับความปลอดภัยบัญชี เพื่อเชิญชวนบุคลากรและนักศึกษา เปลี่ยน PASSWORD เพื่อความปลอดภัยของข้อมูลส่วนตัวและข้อมูลสำคัญของมหาวิทยาลัย 2. รวบรวมองค์ความรู้เกี่ยวกับ PDPA จัดเก็บในรูปแบบเว็บไซต์และเผยแพร่ในเว็บไซต์หลักมหาวิทยาลัย	หน่วยงานมีการดำเนินการควบคุมตามที่กำหนดอย่างต่อเนื่อง อย่างไรก็ตามการควบคุมที่มีอยู่ยังไม่เพียงพอที่จะลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	มีการโจมตีทางไซเบอร์ในรูปแบบใหม่ๆเพื่อละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา มรภ.กพ.	1. จัดตั้งคณะทำงานและผู้รับผิดชอบ 2. ประชุมคณะกรรมการดำเนินงานจัดทำนโยบาย วางแผนการดำเนินงาน 3. จัดอบรม/กิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลส่วนบุคคล อย่างต่อเนื่อง โดยแยกประเภทของผู้ที่มีหน้าที่และความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) 4. กำหนดให้เจ้าหน้าที่ที่เกี่ยวข้องลงนามในสัญญารักษาความลับ 5. จัดกิจกรรมแลกเปลี่ยนเรียนรู้กลุ่มบุคลากรตามคำสั่งฯ เพื่อให้การปฏิบัติงานสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) 6. สรุปผลการจัดกิจกรรม 7. จัดทำมาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 8. จัดทำแนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล และมีช่องทางการร้องเรียนกรณีที่มีเหตุการละเมิดข้อมูลส่วนบุคคล	- รองอธิการบดีฝ่ายวิชาการ - สำนักวิทยบริการและเทคโนโลยีสารสนเทศ - สำนักส่งเสริมวิชาการและงานทะเบียน - กองพัฒนานักศึกษา - อาจารย์นฤชล เขื่อนยัง

1.2 รายงานการตรวจสอบและการรักษาความปลอดภัยระบบและเว็บไซต์

รายงานโครงการบริการตรวจสอบและป้องกันการโจมตีบนเว็บไซต์ API โมบายแอปพลิเคชัน และการปลอมแปลงเว็บที่ใช้ในการหลอกลวงประชาชน โดย สกมช.

รายงานเดือนพฤศจิกายน 2568

(1) บทสรุปผู้บริหาร

หน่วยงานเป็นมหาวิทยาลัยราชภัฏกำแพงเพชร (kpru.ac.th) ซึ่งมีการตรวจสอบกิจกรรมทางไซเบอร์อย่างต่อเนื่อง ในช่วงเวลาล่าสุด พบว่ามีการโจมตีจากแหล่งภายนอกจำนวนมาก โดยมีจุดมุ่งหมายหลักที่การเข้าถึงระบบล็อกอิน การสแกนช่องโหว่ และการพยายามทำการทดสอบช่องโหว่ประเภท SQL Injection และ Cross-site scripting อย่างไรก็ตาม ระบบ Web Application Firewall ของหน่วยงานได้ทำการบล็อกทุกเหตุการณ์ที่ตรวจจับได้อย่างสมบูรณ์ ไม่มีเหตุการณ์ใดที่ทำให้ข้อมูลสูญหายหรือความเสถียรของบริการได้รับผลกระทบใด ๆ ทั้งสิ้น

ข้อค้นพบที่สำคัญ (Key Findings)

- การโจมตีหลักเป็นรูปแบบ SQL Injection (185,807 เหตุการณ์) และ Illegal Resource Access (152,246 เหตุการณ์) ซึ่งเป็นเทคนิคการเจาะระบบที่พยายามเข้าถึงฐานข้อมูลหรือทรัพยากรที่ไม่ได้รับอนุญาต
- แหล่งที่มาของการโจมตีสูงสุดมาจาก Germany (142,212 เหตุการณ์), China (64,551 เหตุการณ์) และ United Kingdom (58,696 เหตุการณ์) แสดงให้เห็นว่าผู้โจมตีมีการกระจายตัวทั่วโลก
- เหตุการณ์ทั้งหมดเกิดขึ้นต่อเนื่องตลอดช่วงเวลาการตรวจสอบโดยไม่มีช่วงเวลาที่หยุดพักหรือการเพิ่มจำนวนโจมตีแบบพุ่งชนอย่างฉับพลัน
- หลังจากการบล็อกโดยระบบป้องกันทั้งหมด ไม่มีหลักฐานของการโจมตีที่สำเร็จหรือการละเมิดข้อมูลใด ๆ ทั้งสิ้น

(2) รายงานผลการป้องกันการโจมตีเว็บไซต์

หน่วยงานได้ทำการตรวจสอบและบล็อกการโจมตีที่มาจากหลายแหล่งโดยอิงจากข้อมูลที่บันทึกไว้ ในระบบรักษาความปลอดภัย รายงานต่อไปนี้แสดงรายละเอียดของแหล่งที่มาของการโจมตี ทั้งในระดับ IP,ประเทศ, ประเภทเครื่องมือการโจมตี รวมถึง URL เป้าหมายที่ได้รับการโจมตีอย่างต่อเนื่อง ทั้งนี้ระบบป้องกัน ได้ทำการบล็อกทุกเหตุการณ์โดยอัตโนมัติ และไม่มีการละเมิดใด ๆ เกิดขึ้น

2.1 ตารางแสดงข้อมูล IP Address ผู้โจมตี

No.	IP Address	Country	Attack Events	Attack Blocked
1	193.142.147.5	Germany	141,556	141,556
2	45.133.172.243	United Kingdom	58,236	58,236
3	120.245.128.166	China	53,699	53,699
4	159.65.156.21	India	26,359	26,359
5	45.80.184.66	Thailand	25,777	25,777
6	39.188.157.3	China	10,320	10,320
7	38.110.228.115	United States	7,661	7,661
8	Distributed	Distributed	3,996	3,996
9	104.145.210.130	United States	1,963	1,963
10	103.208.207.42	Indonesia	963	963

2.2 ตารางแสดงข้อมูล ประเทศของผู้โจมตี

No.	Country	Attack Events	Attack Blocked
1	Germany	142,212	142,212
2	China	64,551	64,551
3	United Kingdom	58,696	58,696
4	India	27,014	27,014
5	Thailand	26,161	26,161
6	United States	12,086	12,086
7	Distributed	3,996	3,996
8	Macao	1,801	1,801
9	Indonesia	1,730	1,730
10	Singapore	1,074	1,074

2.3 ตารางแสดงข้อมูล ประเภทของการโจมตี

No.	Attack Types	Attack Events	Attack Blocked
1	SQL Injection	185,807	185,807
2	Illegal Resource Access	152,246	152,246
3	Cross-site scripting	2,949	2,949
4	Bad Bots	387	387

2.4 ตารางแสดงข้อมูล Target URL ที่ถูกโจมตี

No.	Target URL	Requests
1	arit.kpru.ac.th/page_id/wp-login.php	141,556
2	arit.kpru.ac.th/ap/ir/index.php	71,608
3	kpru.ac.th	67,140
4	arit.kpru.ac.th	56,027
5	mooc.kpru.ac.th	2,570
6	www.kpru.ac.th/en/index.php/11-news/78-welcomed-honour-guest-from-bowling-green-state-university-usa-2/wp-login.php	760
7	www.kpru.ac.th	531
8	www.kpru.ac.th/en/index.php/11-news/87-covid-19-epidemics-vol13-3/wp-login.php	303
9	mooc.kpru.ac.th/course/index.php	277
10	arit.kpru.ac.th/ap/activityOnline/index.php	219

Target URL ที่ถูกโจมตี คือ ลิงก์หรือที่อยู่เว็บปลายทางที่ผู้โจมตีต้องการให้เหยื่อเข้าถึง เพื่อหลอกให้เปิดเผยข้อมูลส่วนตัว (เช่น รหัสผ่าน) หรือติดตั้งมัลแวร์ โดยมักใช้เทคนิคหลอกลวง เช่น การปลอมแปลง URL ให้เหมือนเว็บไซต์จริง (Phishing), การใช้ลิงก์ที่เปลี่ยนเส้นทางไปหน้าอันตรายโดยไม่รู้ตัว (Reverse Tabnabbing), หรือการฝัง URL ในอีเมล, ข้อความ, หรือภาพ เพื่อหลอกให้คลิกโดยไม่ตั้งใจ

2.5 ตารางการใช้งาน Total Requests

No.	Domain Name	Total Requests
1	kpru.ac.th	3,293,191

(3) รายงานผลการรั่วไหลของข้อมูล

หน่วยงานได้ทำการสแกนและวิเคราะห์บันทึกด้านความปลอดภัยเพื่อค้นหาหลักฐานของการรั่วไหลข้อมูลภายในระบบ ทั้งในส่วนของฐานข้อมูลเว็บเซิร์ฟเวอร์และระบบจัดเก็บข้อมูลภายในองค์กร ผลการตรวจสอบไม่พบเหตุการณ์ใดที่บ่งบอกถึงการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการโอนถ่ายข้อมูลที่ผิดปกติใด ๆ ทั้งนี้ระบบตรวจจับการละเมิดข้อมูล (Data Loss Prevention) ได้ทำงานร่วมกับ Web Application Firewall อย่างต่อเนื่องตั้งแต่เริ่มเก็บข้อมูล จึงสามารถระบุและบล็อกการพยายามดึงข้อมูลออกจากเครือข่ายได้ทันที การไม่มีเหตุการณ์รั่วไหลใด ๆ แสดงให้เห็นถึงประสิทธิภาพของการตั้งค่าและนโยบายการควบคุมการเข้าถึงข้อมูลที่หน่วยงานได้ดำเนินการอย่างเหมาะสม **สรุป** ไม่พบภัยคุกคาม

(4) รายงานผลการตรวจพบการลอกเลียนแบบเว็บไซต์

กระบวนการตรวจสอบได้ทำการสแกนหาหน้าเว็บหรือโดเมนที่อาจมีการทำลอกเลียนแบบ (phishing) หรือการโฮสต์เนื้อหาเทียบเคียงกับเว็บไซต์ของหน่วยงาน ผลการสแกนไม่พบโดเมนหรือที่อยู่ IP ใด ที่แสดงพฤติกรรมคล้ายคลึงกับการปลอมแปลงหรือพยายามหลอกลวงผู้ใช้ให้เข้าใจว่าเป็นเว็บไซต์ของมหาวิทยาลัยราชภัฏกำแพงเพชร การไม่มีข้อมูลลิงก์หรือเว็บไซต์ปลอมแปลงใด ๆ ปรากฏขึ้นเป็นสัญญาณที่ดี ว่าการดำเนินการด้านการจัดการชื่อโดเมนและการใช้ระบบ DNSSEC ของหน่วยงานได้ทำงานอย่างเต็มประสิทธิภาพและลดความเสี่ยงจากการลอกเลียนแบบอย่างมีนัยสำคัญ

สรุป ไม่พบภัยคุกคาม

อ่านรายละเอียดรายงานฉบับสมบูรณ์ได้ที่ https://www.kpru.ac.th/km-web/files/report-waf-nov25-kpru.pdf

ภาพกิจกรรม




กิจกรรมแลกเปลี่ยนเรียนรู้การพัฒนาเว็บไซต์ ครั้งที่ 3 (รูปแบบออนไลน์)
วันที่ 26 ธันวาคม 2568 เวลา 09.30 น. เป็นต้นไป

ประเด็นหัวข้อ

1. รับเรื่องจากมติการประชุมคณะกรรมการบริหารมหาวิทยาลัย
2. สร้างความเข้าใจแบบฟอร์มที่ทุกหน่วยงานต้องกรอกข้อมูล

สรุปกิจกรรม

การดำเนินงานของทีมแอดมินจะมีความเกี่ยวข้องกับแผนพัฒนาตามค่าเป้าหมายตัวชี้วัดผลลัพธ์ หมวด 7 ประจำปีการศึกษา 2568 (ดำเนินการในปี พ.ศ. 2569 – 2570) ดังนี้

ตัวชี้วัดที่ 48 ระดับความสำเร็จของการเปลี่ยนผ่านกระบวนการปฏิบัติงานและการให้บริการสู่รูปแบบ e-Service

ตัวชี้วัดที่ 49 ระดับความพึงพอใจของผู้รับบริการที่มีต่อระบบเทคโนโลยีและสารสนเทศที่สนับสนุนการบริหารจัดการ

ตัวชี้วัดที่ 50 ร้อยละของระดับความพร้อมใช้งานและเสถียรภาพของระบบสารสนเทศหลัก

ตัวชี้วัดที่ 56 ประสิทธิภาพการเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cybersecurity Defense & Response Efficiency Index)

จึงเป็นที่มาของการทำแบบฟอร์มเก็บข้อมูล เพื่อนำข้อมูลมาประมวลผล วิเคราะห์ สรุป บริหารจัดการงานที่เกี่ยวข้อง และพัฒนาต่อยอดเกี่ยวกับการจัดการ PDPA ของมหาวิทยาลัยฯ เพื่อให้การดำเนินงานเป็นไปด้วยความเรียบร้อยทีมงานส่วนกลาง จึงรวบรวมข้อมูลระบบสารสนเทศต่างๆ รวมถึงเว็บไซต์ที่ให้บริการทั้งภายใน ภายนอกมหาวิทยาลัยฯ เพื่อรวมเป็นศูนย์กลาง แหล่งรวมระบบการให้บริการต่างๆ ผู้ใช้งานสามารเรียกใช้ / ติดต่อ / แจ้งข้อมูล ปัญหา / ให้กับผู้ดูแล ได้ผ่านหน้าเว็บไซต์หลักของมหาวิทยาลัยฯ ได้อย่างสะดวก

กิจกรรมแลกเปลี่ยนเรียนรู้การพัฒนาเว็บไซต์ ครั้งที่ 4
วันที่ 8 มกราคม 2569 เวลา 09.00-12.00 น.
ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มรภ.กพ.

ประเด็นหัวข้อ

1. การรักษาความปลอดภัยเว็บไซต์และระบบสารสนเทศภายในมหาวิทยาลัย
2. ผลการดำเนินงานความเสี่ยง การถูกละเมิดหรือการละเมิดข้อมูลส่วนบุคคลของบุคลากรและนักศึกษา

สรุปกิจกรรม

ความก้าวหน้าและสร้างความเข้าใจเกี่ยวกับแบบฟอร์มสำรวจข้อมูลระบบสารสนเทศต่างๆ ของแต่ละหน่วยงานที่ได้รับผิดชอบ

1. ขณะนี้ทีมงานส่วนกลาง กำลังรวบรวมข้อมูลระบบสารสนเทศต่างๆ รวมถึงเว็บไซต์ที่ให้บริการทั้งภายใน ภายนอกมหาวิทยาลัยฯ เพื่อรวมเป็นศูนย์กลาง แหล่งรวมระบบการให้บริการต่างๆ ผู้ใช้งานสามารถเรียกใช้ / ติดต่อ / แจ้งข้อมูล ปัญหา / ให้กับผู้ดูแล ผ่านหน้าเว็บไซต์หลักของมหาวิทยาลัยฯ ของเราได้อย่างสะดวก
2. เพื่อนำข้อมูลมาสรุป และต่อยอดการบริหารจัดการเกี่ยวกับ PDPA ของมหาวิทยาลัยฯ

รายงานผลการดำเนินงานการตรวจสอบและป้องกันการโจมตีบนเว็บไซต์ เดือนมกราคม 2569 ฉบับสมบูรณ์ ได้ที่ https://kpru.ac.th/km-web/files/jan26_kpru.pdf

กิจกรรมแลกเปลี่ยนเรียนรู้การพัฒนาเว็บไซต์ ครั้งที่ 5
วันที่ 27 กุมภาพันธ 2569 เวลา 09.00-12.00 น.
ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ประเด็นหัวข้อ

1. แจ้งคำสั่งแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. หารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย
3. ประเด็นความเสี่ยงด้านความปลอดภัยทางไซเบอร์และสถิติการโจมตี
4. ข้อเสนอแนะและแนวทางการดำเนินงานในอนาคต

1. แจ้งคำสั่งแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ตามคำสั่งมหาวิทยาลัยราชภัฏกำแพงเพชรที่ 2363/2568 ลงวันที่ 24 ธันวาคม 2568 ได้แต่งตั้ง นางสาวนฤชล เขื่อนยัง อาจารย์ประจำหลักสูตรโปรแกรมวิชานิติศาสตร์ เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ เพื่อรองรับการเป็นมหาวิทยาลัยดิจิทัลและปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) อย่างถูกต้อง ซึ่งกำหนดให้มีหน้าที่และอำนาจในการให้คำแนะนำและวางแนวทางปฏิบัติ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในแต่ละหน่วยงาน ตรวจสอบการดำเนินงานด้านการคุ้มครองข้อมูลขององค์กรให้เป็นไปตามกฎหมาย การประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) กรณีมีเหตุละเมิดข้อมูล การรักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้จากการปฏิบัติหน้าที่

โดยสรุป แจ้งให้ทีมแอดมินเข้าใจถึงบทบาทหน้าที่ของ DPO และบทบาทของทีมแอดมินในฐานะผู้ประมวลข้อมูลส่วนบุคคล ซึ่งเป็นบุคลากรที่สำคัญจะต้องปฏิบัติหน้าที่ภายในกรอบของกฎหมาย PDPA

2. หารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย

จากการสอบถามและหารือระหว่างทีมแอดมินที่ปฏิบัติงานในหน่วยงานต่าง ๆ ภายในมหาวิทยาลัย เกี่ยวกับแนวทางการบริหารจัดการข้อมูลส่วนบุคคล (PDPA) มาตรการควบคุมการเข้าถึงข้อมูล และสถานะความปลอดภัยทางไซเบอร์ในปัจจุบัน สาระสำคัญครอบคลุมถึงระบบฐานข้อมูลนักศึกษาและบุคลากร แนวทางปฏิบัติเกี่ยวกับกล้องวงจรปิด (CCTV) และความเสี่ยงจากการตั้งรหัสผ่านที่คาดเดาง่าย ซึ่งเป็นช่องโหว่สำคัญในการโจมตีระบบโดยมหาวิทยาลัยมุ่งเน้นการสร้างมาตรฐานการปฏิบัติงานที่ชัดเจนเพื่อคุ้มครองเจ้าหน้าที่ผู้ปฏิบัติงานและป้องกันการละเมิดข้อมูลส่วนบุคคลในวาระนี้ อาจารย์นฤชล เขื่อนยัง (DPO) ได้กำหนดประเด็นในการแลกเปลี่ยนข้อมูล เพื่อที่จะนำไปออกแบบจัดอบรมเชิงปฏิบัติการให้กับบุคลากรกลุ่มที่เป็นทีมแอดมิน เกี่ยวกับบทบาทและหน้าที่ของเจ้าหน้าที่แอดมิภายใต้กรอบของกฎหมาย PDPA เพื่อสร้างความรู้และความเข้าใจ รวมถึงสอบถามปัญหาที่ทีมแอดมินเคยพบเจอจากการปฏิบัติงาน และส่วนสุดท้ายคือการสร้างความเข้าใจเกี่ยวกับการจัดทำสัญญา NDA โดยมีหัวข้อในการหารือ ดังนี้

2.1 วิธีการจัดเก็บข้อมูลส่วนบุคคลในแต่ละหน่วยงาน เพื่อเป็นการสำรวจความเสี่ยง พฤติกรรม และปัญหาที่อาจพบในการจัดเก็บข้อมูลของทีมแอดมิน การให้สิทธิเข้าถึงข้อมูล กรณีเจ้าหน้าที่แอดมิน โยกย้ายงาน หรือลาออกมีวิธีการจำกัดการเข้าถึงข้อมูล หรือทำลายข้อมูลหรือไม่ อย่างไร

2.2 การตรวจสอบความรับผิดชอบของเจ้าหน้าที่แอดมิน/มหาวิทยาลัย ระบบต่าง ๆ สามารถตรวจสอบย้อนหลังได้หรือไม่ว่า ใครเข้าไปดู / แก้ไขข้อมูล รวมถึงความพร้อมในการรับมือกรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล

มีการกำหนดเจ้าหน้าที่แอดมินที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลไว้ชัดเจนหรือไม่ หรือเจ้าหน้าที่แอดมินบางคนเป็นเพียงคณะทำงาน มีการจัดทำคำสั่ง หรือระบุหน้าที่ของทีมแอดมินไว้ชัดเจนหรือไม่ ว่าเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลอย่างไร

2.3 สอบถามประเด็นความเสี่ยงในการปฏิบัติงาน เพื่อที่จะนำไปออกแบบเป็น Case Study ในการจัดการอบรมให้ทีมแอดมินต่อไป จากประเด็นที่ อาจารยนฤชล เขื่อนยัง (DPO) กำหนดหัวขอในการประชุมวาระนี้ไว สามารถสรุปรายละเอียดพอสังเขปไดดังตอไปนี้

2.1 วิธีการจัดเก็บข้อมูลส่วนบุคคลในแต่ละหน่วยงาน

สำหรับการบริหารจัดการข้อมูลและระบบฐานข้อมูลในแต่ละหน่วยงาน จะมีฐานการจัดเก็บข้อมูลที่แตกต่างกัน กรณีตัวอย่างสำนักส่งเสริมวิชาการและงานทะเบียน มีการจัดเก็บข้อมูลตั้งแต่แรกเข้าจนถึงสำเร็จการศึกษา โดยแบ่งระดับการเข้าถึงและการจัดเก็บออกเป็น 2 ส่วนหลัก

- ฐานข้อมูลหลัก (ฐานดำ) เป็นระบบปิดที่ใช้งานภายใน (Offline) เก็บข้อมูลทุกอย่างที่เกี่ยวข้องกับการรายงานตัวและการส่งข้อมูลให้กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) จะไม่มีการเชื่อมต่ออออนไลน์เพื่อความปลอดภัย

- ระบบเผยแพร่ข้อมูลออนไลน์ แสดงผลเฉพาะข้อมูลเบื้องต้น เช่น รายชื่อและสถานะการศึกษา เพื่อให้บุคคลภายนอก ผู้ปกครอง หรือศิษย์เก่าสามารถตรวจสอบและยืนยันสถานะได้ โดยระบบมีการจัดเก็บ Log สามารถตรวจสอบได้ว่าใครเป็นผู้เข้ามาดูข้อมูล

- นโยบายการจัดเก็บและทำลายข้อมูล

(1) ข้อมูลนักศึกษา เก็บข้อมูลไว้จนสำเร็จการศึกษา หากพ้นสภาพนักศึกษาจะมีการ Disable บัญชีผู้ใช้งานเบื้องตัน โดยจะเก็บข้อมูลไว้ในระบบประมาณ 2 ปี ก่อนพิจารณาดำเนินการตามระเบียบ

(2) ข้อมูลบุคลากร สำหรับบุคลากรทั่วไปจะเก็บข้อมูลไว้ 2 ปีหลังลาออก แต่กรณีอาจารย์ที่เป็นข้าราชการจะคงบัญชีอีเมลไว้ตลอดชีวิต เนื่องจากมีความจำเป็นในการใช้เป็นชื่อผู้ประสานงานในผลงานวิจัย

นอกจากการจัดเก็บข้อมูลส่วนบุคคลผ่านระบบและฐานข้อมูลต่าง ๆ แล้ว ยังมีกรณีการจัดเก็บข้อมูลส่วนบุคคลจากกล้องวงจรปิด (CCTV) มหาวิทยาลัยฯ และมีมาตรการควบคุมและเข้าถึงกล้องวงจรปิด (CCTV) โดยการบริหารจัดการภาพจากกล้องวงจรปิดภายในมหาวิทยาลัย มีการแบ่งความรับผิดชอบระหว่างส่วนกลาง ซึ่งอยู่ภายใต้การกำกับและดูแล โดยทีมแอดมินของสำนักวิทยบริการฯ และส่วนงานคณะ/สำนัก/สถาบัน จะอยู่ภายใต้การดูแลของหน่วยงานนั้น ๆ เอง

(1) การจัดเก็บและระยะเวลา

การจัดเก็บภาพขึ้นอยู่กับความจุของ Hard Disk (NVR) เมื่อข้อมูลเต็มระบบจะทำการบันทึกวนทับอัตโนมัติ งานพัฒนาระบบเครือข่ายและการสื่อสาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ดูแลกล้องพื้นที่สาธารณะส่วนภายในอาคารเป็นความรับผิดชอบของแต่ละคณะ

(2) ขั้นตอนการขอเข้าถึงข้อมูลภาพ

แนวปฏิบัติดำเนินการขอตามประกาศมหาวิทยาลัยฯ ซึ่งมีแนวทาง ขั้นตอน และ วิธีการขอดูภาพ และขอสำเนาภาพไว้อย่างชัดเจน ซึ่งหน่วยงานภายในสามารถนำไปใช้ได้ สรุปแนวทางการขอดู ภาพและขอสำเนาภาพได้ดังนี้

- การขอดูภาพ ควรระบุวัตถุประสงค์และช่วงเวลาที่ชัดเจน (วินาที/นาที)

- การขอสำเนาภาพ (ไฟล์วิดีโอ) หากต้องการนำภาพออกไปประกอบคดี ต้องมีบันทึกประจำวัน หรือหลักฐานการแจ้งความจากสถานีตำรวจมาแนบ เพื่อป้องกันความรับผิดชอบของเจ้าหน้าที่แอดมินจากการเปิดเผยภาพบุคคลอื่นที่ไม่เกี่ยวข้อง

- หน่วยงานควรจัดทำป้ายเตือน "พื้นที่บันทึกภาพกล้องวงจรปิด" ตามกฎหมาย เพื่อแจ้งให้ผู้ใช้บริการทราบ ข้อสรุป ประเด็นนี้ จึงขอความอนุเคราะห์ให้แอดมินแต่ละหน่วยงาน นำส่งข้อมูลเกี่ยวกับวิธีการจัดเก็บข้อมูล ตามแบบฟอร์มการบันทึกข้อมูลระบบสารสนเทศ ประกอบไปด้วย ชื่อระบบ ข้อมูลที่จัดเก็บ ระยะเวลาการจัดเก็บ สิทธิการเข้าถึงข้อมูล เจ้าหน้าที่ประมวลผลข้อมูล เป็นต้น ภายในวันที่ 5 มีนาคม 2569

2.2 การตรวจสอบความรับผิดชอบของเจ้าหน้าที่แอดมิน/มหาวิทยาลัยจากการสอบถามทีมแอดมินในแตละหนวยงาน สามารถระบุตัวตนไดวาใครเขามา ดู/แกไข ในระบบตาง ๆ มหาวิทยาลัยฯ มีประกาศเชิงนโยบายเกี่ยวกับ

มาตรการคุมครองขอมูลสวนบุคคล แตยังไมมีแนวปฏิบัติกรณีเกิดเหตุละเมิดขอมูลสวนบุคคล และขั้นตอน/วิธีการรายงานมหาวิทยาลัย และแจงเหตุละเมิดมายัง DPO

ข้อสรุป

DPO ได้ให้ข้อเสนอแนะหน่วยงานว่า ควรกำหนดหน้าที่ของเจ้าหน้าที่แอดมินให้ชัดเจนว่าใครเป็น Data Processorหรือใครบ้างที่เป็นเพียงคณะทำงานช่วยเหลือ Data Processor เพื่อกำหนดกรอบหน้าที่และความรับผิดชอบให้ชัดเจนตามกฎหมาย PDPA

2.3 สอบถามประเด็นความเสี่ยงในการปฏิบัติงาน เพื่อนำมาเป็นกรณีศึกษาในการออกแบบกิจกรรมการจัดอบรมสำหรับแอดมิน โดยได้มีการแลกเปลี่ยนประสบการณ์การทำงาน และสอบถามวิธีการดำเนินการในประเด็นดังนี้

(1) การขอข้อมูลส่วนตัวจากบุคคลภายนอก มีกรณีผู้ปกครองโทรศัพท์ติดต่อมาขอเบอร์โทรศัพท์ และข้อมูลติดต่อของอาจารย์ เจ้าหน้าที่ไม่ให้ข้อมูลติดต่อส่วนตัว แต่ให้แจ้งขั้นตอนการติดตามงานหรือผลการเรียนตามระเบียบแทนแบบนี้ถูกต้องหรือไม่

(2) การยืนยันสถานะบุคลากรทางโทรศัพท์ การให้ข้อมูลว่าใครทำงานอยู่ที่ไหนผ่านทางโทรศัพท์ มีความเสี่ยงเจ้าหน้าที่ควรดำเนินการอย่างไร

(3) การจัดการข้อมูลที่ละเอียดอ่อน การฝากเจ้าหน้าที่ธุรการจัดการเรื่องการจัดทำบันทึกข้อความในระบบซึ่งต้องให้ข้อมูลส่วนตัวแก่เจ้าหน้าที่ กรณีนี้เจ้าหน้าที่รู้สึกลำบากใจที่ต้องรู้ข้อมูลส่วนบุคคล เป็นจุดเสี่ยงที่อาจทำให้ข้อมูลรั่วไหลได้ หากไม่มีการจัดการที่รัดกุม และเจ้าหน้าที่ที่ช่วยเหลือในการจัดทำเอกสารอาจจะต้องรับผิดชอบจึงเกิดความกังวลในการปฏิบัติงาน

(4) การใช้ข้อมูลเพื่อประกอบการเรียนการสอน/การเป็นวิทยากร การนำระบบที่มีข้อมูลนักศึกษาจริงไปแสดงเป็นตัวอย่าง โดยไม่ปิดบังรายชื่อหรือเกรด ถือเป็นพฤติกรรมสุ่มเสี่ยงที่อาจถูกร้องเรียนหรือไม่

(5) การที่มีบุคคลภายนอกมาขอใช้ server ของหน่วยงานในการประชาสัมพันธ์ ควรมีขอบเขตอย่างไร หากมีการประชาสัมพันธ์หรือใช้พื้นที่ทำเรื่องส่วนตัว ซึ่งอาจมีข้อมูลที่สุ่มเสี่ยง ควรมีแนวทางการป้องกัน อย่างไร

(6) การแจ้งให้บุคลากร/นักศึกษา เปลี่ยนรหัสผ่านแต่ไม่เปลี่ยนตามที่ประชาสัมพันธ์ ควรมีแนวทางการดำเนินการอย่างไร หากข้อมูลรั่วไหลหรือถูกละเมิด เจ้าหน้าที่จะต้องรับผิดชอบหรือไม่

ข้อสรุป

จากการรับฟังปัญหาและข้อกังวลในการปฏิบัติงานต่าง ๆ DPO ได้แนะนำวิธีการดำเนินการให้รัดกุมไปเบื้องต้น แต่เพื่อให้มีมาตรการและแนวทางที่ชัดเจน จึงจะนำเป็นกรณีศึกษาที่จะนำไปปรับใช้ในการออกแบบกิจกรรมที่จะจัดอบรมในทีมแอดมินต่อไป

3. ประเด็นความเสี่ยงด้านความปลอดภัยทางไซเบอร์และสถิติการโจมตี

รายงานสถิติความปลอดภัยทางไซเบอร์ (ช่วงเดือนมกราคม - กุมภาพันธ์) พบประเด็นที่น่ากังวลดังนี้

รายการความเสี่ยง	รายละเอียด
รายการความเสี่ยง	พบการโจมตีประมาณ 18.8 ล้านครั้ง (ระบบป้องกันได้ 100%)
จำนวนการโจมตี	พบ 54 รายการ โดยเป็นระดับสูง 30 รายการ
ช่องโหว่ที่เป็นอันตราย	ตรวจพบเครื่องในเครือข่ายถูกฝังมัลแวร์หรือเป็น "ซอมบี้" ประมาณ 800 เครื่อง
เครื่องที่ติดมัลแวร์	ส่วนใหญ่มาจากประเทศจีนและสวิตเซอร์แลนด์
แหล่งที่มาการโจมตี	98% ของผู้ใช้งานตั้งรหัสผ่านที่คาดเดาง่าย เช่น เบอร์โทรศัพท์ ชื่อ หรือวันเกิด

ข้อเสนอแนะ

ควรมีนโยบายบังคับเปลี่ยนรหัสผ่านทุก 3 เดือน หรือกำหนดรูปแบบรหัสผ่านที่ซับซ้อน (เช่น ผสมตัวอักษรพิเศษ หรือรหัสหน่วยงาน) ตั้งแต่การลงทะเบียนครั้งแรกเพื่อลดความเสี่ยงจากการถูกสุ่มรหัส (Brute Force)

4. ข้อเสนอแนะและแนวทางการดำเนินงานในอนาคต

4.1 ข้อเสนอแนะในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

จากการประชุมทีมแอดมิน มีประเด็นสำคัญที่เกี่ยวข้องกับการดำเนินการเพื่อคุ้มครองผู้ปฏิบัติงานเบื้องต้น และปฏิบัติตามกฎหมาย PDPA ดังนี้

(1) ทีมแอดมินมีลักษณะการปฏิบัติงานในบทบาทของผู้ประมวลผลข้อมูล (Data Processor) เจ้าหน้าที่แอดมินจึงมีสถานะเป็นผู้ประมวลผลข้อมูลตามกฎหมาย PDPA ดังนั้น จึงจำเป็นต้องมีคำสั่งแต่งตั้งหรือเอกสารที่กำหนดหน้าที่ความรับผิดชอบ ซึ่งระบุภาระงานและชื่อรายบุคคลที่ชัดเจน เพื่อให้มหาวิทยาลัยสามารถคุ้มครองทางกฎหมายแก่เจ้าหน้าที่ได้ หากเกิดเหตุละเมิดที่เกิดจากการปฏิบัติหน้าที่ตามปกติ

(2) การจัดทำข้อตกลงรักษาความลับ (NDA) อยู่ระหว่างการพิจารณาจัดทำสัญญาหรือข้อตกลงรักษาความลับเพิ่มเติม เพื่อเป็นเกราะป้องกันให้ทีมแอดมินและสร้างมาตรฐานการทำงานที่เป็นระบบ

4.2 แนวทางการดำเนินงานในอนาคต

(1) การจัดอบรมเชิงปฏิบัติการ (Workshop) สำหรับทีมแอดมิน ซึ่งมุ่งเน้นการจำลองเหตุการณ์จริง (Case Study) ให้ทีมแอดมินได้ทดลองแก้ปัญหามากกว่าการบรรยายข้อกฎหมายเพียงอย่างเดียว

(2) การจัดทำ Checklist เพื่อพัฒนาการประเมินความเสี่ยงและภาระงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลสำหรับแต่ละหน่วยงาน รวมถึงการจัดทำข้อตกลงรักษาความลับ (NDA) ให้ตรงตามบทบาทหน้าที่และมีความกระชับเพื่อไม่ให้เป็นภาระต่อผู้ปฏิบัติงานจนเกินไป

(3) การทบทวนคำสั่งแต่งตั้งคณะกรรมการ/คณะทำงานตามกฎหมาย PDPA เพื่อเป็นการปรับปรุงรายชื่อคณะกรรมการและผู้รับผิดชอบระบบให้เป็นปัจจุบัน และสอดคล้องตามกฎหมาย

ภาพกิจกรรม