ปธ.๐๐๑/๖๓

บันทึกข้อความ

ส่วนงาน คณะวิทยาศาสตร์ หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ โทร ๓๘๙๐
ที่ อว ๖๙.๕.๑.๑/๕๐๙ **วันที่** ๒๕ พฤษภาคม ๒๕๖๕
เรื่อง ขอรายงานสรุปเนื้อหาและการนำไปใช้ประโยชน์

เรียน คณบดีคณะวิทยาศาสตร์

ตามที่ คณะวิทยาศาสตร์ ได้อนุญาตให้ข้าพเจ้าเข้าร่วมการสัมมนา เรื่อง โครงการเตรียมความพร้อมรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล(PDPA) เมื่อวันที่ ๒๖ เมษายน ๒๕๖๕ ผ่านระบบการประชุมออนไลน์ด้วยโปรแกรม Microsoft Teams จัดโดยกองเทคโนโลยีดิจิทัล สำนักงานมหาวิทยาลัย นั้น

บัดนี้ ข้าพเจ้าได้เข้าร่วมการสัมมนา เป็นที่เรียบร้อยแล้ว ดังนั้น จึงขอรายงานสรุปเนื้อหาและประโยชน์ที่ได้รับ ดังนี้

๑. <u>สรุปเนื้อหาที่ได้รับจากการเข้าประชุม/อบรม ฯลฯ</u>

รายงานสรุปเนื้อหา การสัมมนา เรื่อง โครงการเตรียมความพร้อมรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล(PDPA) เมื่อวันที่ ๒๖ เมษายน ๒๕๖๕ ผ่านระบบการประชุมออนไลน์ด้วยโปรแกรม Microsoft Teams จัดโดยกองเทคโนโลยีดิจิทัล สำนักงานมหาวิทยาลัย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือกฎหมาย PDPA ที่ย่อมาจาก Personal Data Protection Act จะเริ่มบังคับใช้เต็มรูปแบบในวันที่ ๑ มิถุนายน ๒๕๖๕ กฎหมาย PDPA นี้ให้ความคุ้มครองข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ บัญชีธนาคาร อีเมล ไอดีไลน์ บัญชีผู้ใช้ของเว็บไซต์ ลายนิ้วมือ ประวัติสุขภาพ เป็นต้น ซึ่งข้อมูลเหล่านี้สามารถระบุถึงตัวเจ้าของข้อมูลนั้นได้ อาจเป็นได้ทั้งข้อมูลในรูปแบบเอกสาร กระดาษ หนังสือ หรือจัดเก็บในรูปแบบอิเล็กทรอนิกส์ก็ได้

กฎหมาย PDPA ถอดแบบมาจากกฎหมายต้นแบบอย่างกฎหมาย GDPR (General Data Protection Regulation) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป วัตถุประสงค์ของการเก็บรักษาข้อมูลส่วนบุคคลของกฎหมายทั้ง ๒ ฉบับ เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีทำการแฮ็กข้อมูลหรือละเมิดความเป็นส่วนตัวเพื่อข่มขู่หวังผลประโยชน์จากทั้งจากตัวเจ้าของข้อมูลเอง หรือจากบุคคลที่ดูแลข้อมูล

เตรียมความพร้อมตาม PDPA

บุคคลที่สำคัญตามกฎหมาย PDPA คือ เจ้าของข้อมูลส่วนบุคคล (Data Subject) และผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ผู้ควบคุมข้อมูลส่วนบุคคลเปรียบเสมือนผู้ดูแลระบบ เป็นฝ่ายปฏิบัติงาน มีหน้าที่เก็บรวบรวม และนำข้อมูลส่วนบุคคลที่ขอความยินยอม (Consent) จากเจ้าของข้อมูลไปใช้ ตัวอย่างเช่น เว็บไซต์ขายของออนไลน์ ผู้จัดทำเว็บไซต์ก็จะต้องขอข้อมูลทั้งชื่อ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลการจ่ายเงิน เพื่อนำไปดำเนินการสั่งซื้อและจัดส่งสินค้าไปยังที่อยู่ของเจ้าของข้อมูล ซึ่ง PDPA เมื่อได้ข้อมูลมาแล้วก็ต้องจัดให้มีมาตรการรักษาความปลอดภัยข้อมูลด้วย ขั้นตอนดังนี้

ขั้นตอนที่ ๑. การเก็บรวบรวมข้อมูลส่วนบุคคล

๑.๑) จัดทำ Privacy Policy แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ องค์กรหรือเจ้าของเว็บไซต์สามารถแจ้งเจ้าของข้อมูลผ่าน Privacy Policy บนเว็บไซต์หรือแอปพลิเคชัน หรือช่องทางการติดต่ออื่นๆ เช่น การลงทะเบียนผ่านเว็บไซต์ หรือทางโซเชียลมีเดีย

- แจ้งว่าจะขอเก็บข้อมูลอะไรบ้าง เพื่อวัตถุประสงค์ใด
- แจ้งสิทธิของเจ้าของข้อมูล โดยสามารถถอนความยินยอมได้ทุกเมื่อ
- ข้อความอ่านเข้าใจง่าย ชัดเจน ใช้ภาษาไม่กำกวม ไม่มีเงื่อนไขในการยินยอม คลิก PDPA Pro เพื่อสร้าง Privacy Policy ที่ถูกต้องตาม PDPA

๑.๒) การจัดการเว็บไซต์ แอปพลิเคชัน และ Third-party นอกจากการจัดทำ Privacy Policy ผ่านเว็บไซต์หรือแอปพลิเคชันแล้ว การขอจัดเก็บ Cookie ต้องแจ้งเพื่อขอความยินยอมให้ใช้ข้อมูลส่วนบุคคลจากผู้ใช้งานด้วย ซึ่งที่พบเห็นทั่วไป มักแจ้งขอเก็บ Cookie เป็น Pop up เล็ก ๆ ทางด้านล่างเว็บไซต์ คลิก Cookiewow เพื่อจัดทำ Cookie Consent Banner เพียงไม่กี่นาที ส่วน Third Party ที่เก็บข้อมูลส่วนบุคคล เช่น เว็บไซต์โฆษณาที่ทำการตลาด ก็ต้องระบุวัตถุประสงค์และขอความยินยอมการเก็บรวบรวมข้อมูลไว้ใน Privacy Policy ด้วย

๑.๓) การเก็บข้อมูลพนักงาน สำหรับการเก็บข้อมูลส่วนบุคคลของพนักงานนั้นก็ต้องจัดทำนโยบายความเป็นส่วนตัวสำหรับพนักงานหรือ HR Privacy Policy เพื่อแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของพนักงานเช่นเดียวกัน แนะนำว่าสำหรับพนักงานเก่า ให้แจ้ง Privacy Policy เป็นเอกสารใหม่ ส่วนพนักงานใหม่ ให้แจ้งในใบสมัคร ๑ ครั้ง และแจ้งในสัญญาจ้าง ๑ ครั้ง คลิก PDPA Pro เพื่อสร้าง Privacy Policy สร้าง HR Privacy Policy ถูกต้องตาม PDPA

ขั้นตอนที่ ๒. การใช้หรือประมวลผลข้อมูลส่วนบุคคล

แต่ละฝ่ายในองค์กรควรร่วมกำหนดแนวทางหรือนโยบายในการดำเนินการด้านข้อมูลส่วนบุคคล (Standard Operating Procedure) และบันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บหรือใช้ (Records of Processing Activity: ROPA) ทั้งข้อมูลที่จัดเก็บในฐานข้อมูลอิเล็กทรอนิกส์ ข้อมูลเอกสารที่จับต้องได้ ข้อมูลส่วนบุคคลทั่วไป ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ซึ่งเป็นข้อมูลที่ระบุตัวบุคคลได้เฉพาะเจาะจงมากขึ้น เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (face ID, ลายนิ้วมือ) รวมถึงห้ามเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่ไม่มีความรับผิดชอบโดยตรง

สิ่งที่ควรทำ

- แอด line เจ้าของข้อมูลส่วนบุคคล หลังจากขออนุญาตแล้ว
- ส่ง Direct Marketing ให้ลูกค้าหลังจากที่ลูกค้ายินยอมแล้ว
- ส่งข้อมูลลูกค้าจาก Cookie ไป Target Advertising ต่อ หลังจากที่ลูกค้ายินยอมแล้ว
- ส่งข้อมูลให้ Vendor หลังจากบริษัทได้ทำความตกลงกับ Vendor ที่มีข้อกำหนดเรื่องความคุ้มครองข้อมูลส่วนบุคคลแล้ว

- การให้บริการที่ต้องวิเคราะห์ข้อมูลส่วนบุคคลจำนวนมากหรือใช้ Sensitive Personal Data เช่น การสแกนใบหน้า จะต้องขอความยินยอมก่อน
- รวบรวมสถิติลูกค้าเพื่อพัฒนาบริการ โดยไม่ใช้ข้อมูลส่วนบุคคลของลูกค้า

ขั้นตอนที่ ๓. มาตรการด้านความปลอดภัยของข้อมูลส่วนบุคคล

- กำหนดแนวทางอย่างน้อยตามมาตรฐานขั้นต่ำด้านการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Minimum Security Requirements) ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- กำหนดนโยบายรักษาระยะเวลาการเก็บข้อมูล และการทำลายเอกสารที่มีข้อมูลส่วนบุคคล (Data Rentention)
- มีกระบวนการ Breach Notification Protocol ซึ่งเป็นระบบแจ้งเตือนเพื่อปกป้องข้อมูลจากการโจมตีจากผู้ไม่หวังดี

ขั้นตอนที่ ๔. การส่งหรือเปิดเผยข้อมูลส่วนบุคคล

- ทำสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอก หรือทำ Data Processing Agreement เพื่อคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานกฎหมาย PDPA
- ในกรณีโอนข้อมูลไปต่างประเทศ ให้ทำสัญญากับบริษัทปลายทางเพื่อคุ้มครองข้อมูลตามมาตรฐาน PDPA
- มีกระบวนการรับคำร้องจากเจ้าของข้อมูลส่วนบุคคล ควรเป็นวิธีที่ง่ายไม่ซับซ้อน และไม่กำหนดเงื่อนไข อาจผ่านการยื่นแบบฟอร์ม ส่งคำร้องผ่านช่อง Chat หรือส่งอีเมลก็ได้

ขั้นตอนที่ ๕. การกำกับดูแลข้อมูลส่วนบุคคล

ในประเทศไทย มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานภาครัฐเป็นผู้กำกับดูแลกฎหมาย PDPA ให้แต่ละองค์กรต้องปฏิบัติตาม โดย PDPA กำหนดให้องค์กรต้องมีเจ้าหน้าที่คุ้มครองข้อมูล หรือ DPO (Data Protection Officer) ซึ่งเป็นผู้มีความรู้ด้านกฎหมายPDPA ด้านเทคโนโลยี และเข้าใจบริบทขององค์กรมีหน้าที่ให้คำปรึกษากับองค์กร และดูแลการดำเนินการให้เป็นไปตามกฎหมาย ยิ่งไปกว่านั้น องค์กรควรจัดอบรมแนวปฏิบัติหรือข้อกฎหมาย PDPA เพื่อสร้างความตระหนักรู้ และให้พนักงานมีความรู้ความเข้าใจในการปฏิบัติงานได้อย่างถูกต้อง

ถึงเวลาปฏิบัติตาม PDPA แล้ว จะเห็นได้ว่าถ้าศึกษารายละเอียดของกฎหมายให้เข้าใจ องค์กรของเราก็สามารถปฏิบัติตาม PDPA ได้ไม่ยาก ทั้งนี้ก็มีผู้เชี่ยวชาญที่จะช่วยสร้างนโยบายการเก็บรักษาข้อมูลส่วนบุคคลของลูกค้าให้เกิดความปลอดภัย และที่สำคัญหากผู้ควบคุมข้อมูลส่วนบุคคลและบุคลากรในองค์กรมีความรู้ความเข้าใจและปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูลตาม PDPA แล้ว ความเสี่ยงกรณีข้อมูลถูกละเมิดก็จะน้อยลง ซึ่งจะสร้างความเชื่อมั่นต่อองค์กรให้กับผู้ใช้งานได้เป็นอย่างดี

พ.ร.บ.คอมพิวเตอร์

คือพระราชบัญญัติที่ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ทั้งคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์โน้ตบุ๊ค สมาร์ตโฟน รวมถึงระบบต่างๆ ที่ถูกควบคุมด้วยระบบคอมพิวเตอร์ ซึ่งเป็นพ.ร.บ.ที่ตั้งขึ้นมาเพื่อป้องกัน ควบคุมการกระทำผิดที่จะเกิดขึ้นได้จากการใช้คอมพิวเตอร์ หากใครกระทำความผิดตามพ.ร.บ. คอมพิวเตอร์นี้ ต้องได้รับการลงโทษตามที่พ.ร.บ.กำหนดไว้

๘ เรื่องที่ห้ามทำ ผิดกฎหมาย พ.ร.บ.คอมพิวเตอร์

๑. เข้าถึงระบบ หรือข้อมูลของผู้อื่นโดยไม่ชอบ (มาตรา ๕-๘)

หากเข้าไปเจาะข้อมูลทางคอมพิวเตอร์ของคนอื่น โดยที่เจ้าของข้อมูลไม่ได้อนุญาต (ละเมิด Privacy) หรือในเคสที่รู้จักดีก็คือ การปล่อยไวรัส มัลแวร์เข้าคอมพิวเตอร์คนอื่น เพื่อเจาะข้อมูลบางอย่าง หรือพวกแฮคเกอร์ ที่เข้าไปขโมยข้อมูลของคนอื่นก็มีความผิดตามพ.ร.บ. คอมพิวเตอร์

๒. แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย (มาตรา ๙-๑๐)

ในข้อนี้จะรวมหมายถึงการทำให้ข้อมูลเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลของผู้อื่นโดยมิชอบ หรือจะเป็นในกรณีที่ทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ อย่างเช่น กรณีของกลุ่มคนที่ไม่ชอบใจกับการกระทำของอีกฝ่าย แล้วต่อต้านด้วยการเข้าไปขัดขวาง ทำร้ายระบบเว็บไซต์ของฝ่ายตรงข้าม ให้บุคคลอื่นๆ ใช้งานไม่ได้

๓. ส่งข้อมูลหรืออีเมลก่อกวนผู้อื่น หรือส่งอีเมลสแปม (มาตรา ๑๑)

พ.ร.บ.คอมพิวเตอร์ข้อนี้ก็เข้ากับประเด็นพ่อค้า แม่ค้าออนไลน์ หรือนักการตลาดที่ส่งอีเมลขายของที่ลูกค้าไม่ยินดีที่จะรับ หรือที่รู้จักกันว่า อีเมลสแปม หรือแม้แต่การฝากร้านตาม Facebook กับ IG ก็เป็นสิ่งที่ไม่ควรทำ และยังรวมถึงคนที่ขโมย Database ลูกค้าจากคนอื่น แล้วส่งอีเมลขายของตัวเอง

๔. เข้าถึงระบบ หรือข้อมูลทางด้านความมั่นคงโดยมิชอบ (มาตรา ๑๒)

โพสต์เกี่ยวกับเรื่องการเมืองที่ส่งผลให้เกิดความเสียหายหรือความมั่นคงต่อประเทศ หรือโพสต์ที่เป็นการก่อกวน หรือการก่อการร้ายขึ้น ก็มีความผิดค่ะ เพราะมาตรา ๑๒ ได้บอกไว้ว่าการเข้าถึงระบบหรือข้อมูลทางด้านความมั่งคงโดยมิชอบ หรือการโพสต์ข้อความในโลกออนไลน์ที่เข่าข่ายข้อมูลเท็จที่น่าจะเกิดความ

เสียหายต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ หรือทำให้ประชาชนเกิดอาการตื่นตระหนก และล่วงรู้ถึงมาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์และนำไปเปิดเผย

๕. จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด (มาตรา ๑๓)

กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์ตามมาตรา ๕-๑๑ (หรือข้อ ๑-๓) ต้องจำคุกไม่เกิน ๑ ปี ปรับไม่เกิน ๒ หมื่นบาท หรือทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้องรับผิดชอบร่วมด้วย กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์ มาตรา ๑๒ ต้องจำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๔ หมื่นบาท หรือทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้องรับผิดชอบร่วมด้วย

๖. นำข้อมูลที่ผิดพ.ร.บ.เข้าสู่ระบบคอมพิวเตอร์ (มาตรา ๑๔)

โทษการนำข้อมูลที่เปิดพ.ร.บ.เข้าสู่ระบบคอมพิวเตอร์ ซึ่งแบ่งออกเป็น ๕ ข้อความผิด คือ

- โพสต์ข้อมูลปลอม ทุจริต หลอกลวง (อย่างเช่น ข่าวปลอม โฆษณาธุรกิจลูกโซ่ที่หลอกลวงเอาเงินลูกค้า และไม่มีการส่งมอบของให้จริงๆ เป็นต้น)
- โพสต์ข้อมูลความผิดเกี่ยวกับความมั่งคงปลอดภัย
- โพสต์ข้อมูลความผิดเกี่ยวกับความมั่นคง ก่อการร้าย
- โพสต์ข้อมูลลามก ที่ประชาชนเข้าถึงได้
- เผยแพร่ ส่งต่อข้อมูล ที่รู้แล้วว่าผิด (อย่างเช่น กด Share ข้อมูลที่มีเนื้อหาเข้าข่ายความผิดพ.ร.บ.คอมพิวเตอร์)

๗. ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจกับผู้ร่วมกระทำความผิด (มาตรา ๑๕)

เพจต่างๆ ที่เปิดให้มีการแสดงความคิดเห็น แล้วมีความคิดเห็นที่มีเนื้อหาผิดกฎหมายก็มีความผิด แต่ถ้าหากแอดมินเพจตรวจสอบแล้วพบเจอ และลบออก จะถือว่าเป็นผู้ที่พ้นความผิด

๘. ตัดต่อ เติม หรือดัดแปลงภาพ (มาตรา ๑๖)

ความผิดข้อนี้ แบ่งออกเป็น ๒ ประเด็นหลักคือ

• การโพสต์ภาพของผู้อื่นที่เกิดจากการสร้าง ตัดต่อ หรือดัดแปลง ที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง อย่างเช่นกรณีที่เอาภาพดาราไปตัดต่อ และตกแต่งเรื่องขึ้นมา จนทำให้บุคคลนั้นเกิดความเสียหาย ก็ถือว่ามีความผิดตามพ.ร.บ.คอมพิวเตอร์

• การโพสต์ภาพผู้เสียชีวิต หากเป็นการโพสต์ที่ทำให้บิดามารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอาย

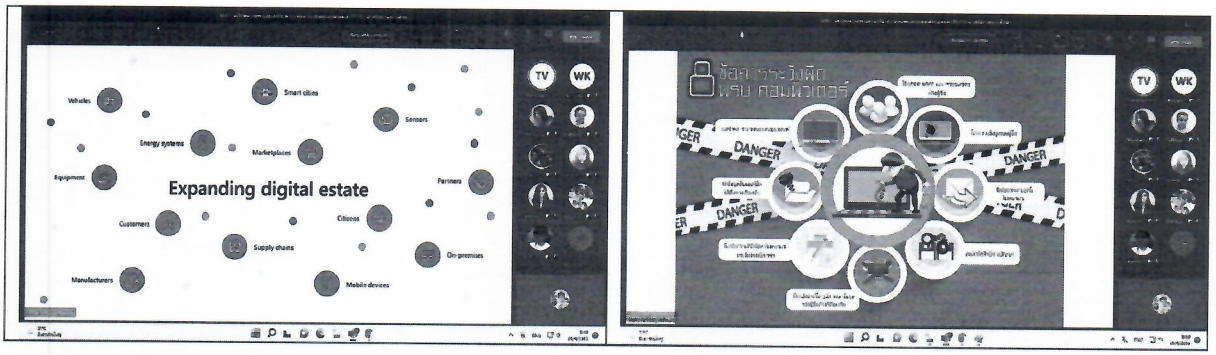
๒. <u>ประโยชน์ต่อการปฏิบัติงานในตำแหน่งหน้าที่</u>

๑. เพื่อเตรียมความพร้อมรองรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)
๒. เพื่อทำให้ทราบและเข้าใจเกี่ยวกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)
๓. เนื่องจากในหน้าที่ปฏิบัติงานมีภาระงานเกี่ยวกับควบคุมดูแลข้อมูลกล้องวงจรปิดหลักสูตร เป็นการเก็บข้อมูลของหน่วยงานเป็นความลับ ไม่มีการเผยแพร่คลิปภาพของหน่วยงาน
๔. ทำให้ทราบและระมัดระวังการเก็บและคุ้มครองข้อมูลส่วนบุคคล

๓. <u>ประโยชน์ต่อหน่วยงาน (ระดับงาน/หลักสูตร/คณะ)</u>

๑. เพื่อเตรียมความพร้อมรองรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) สำหรับหลักสูตร
๒. เพื่อทำให้ทราบและเข้าใจเกี่ยวกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) สำหรับหลักสูตร
๓. หลักสูตรลดความเสี่ยงจากการถูกละเมิดข้อมูลส่วนบุคคลได้
๔. หลักสูตรเพิ่มความเสี่ยงและจากการเก็บข้อมูลของหน่วยงานเป็นความลับ ไม่มีการเผยแพร่คลิปภาพของหน่วยงาน

พร้อมนี้ได้แนบภาพถ่าย จากการเข้าประชุม/อบรมฯลฯ มาพร้อมนี้แล้ว จำนวน ๒ ภาพ



จึงเรียนมาเพื่อโปรดทราบ

ประทีป สุขสมัย

(นายประทีป สุขสมัย)
นักวิชาการโสตทัศนศึกษา

ความคิดเห็นของผู้บังคับบัญชาชั้นต้น (ประธานอาจารย์ผู้รับผิดชอบหลักสูตร)
บุคลากรดังกล่าวไปนำความรู้ไปใช้ประโยชน์ ดังนี้(โปรดระบุรายละเอียด)

.....
สามารถนำข้อมูลส่วนบุคคลของหลักสูตรได้
.....

.....

(อาจารย์อรรถวิท ชังคมานนท์)
ประธานอาจารย์ผู้รับผิดชอบหลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์
๒๕/พ.ค./๒๕๖๕

บันทึกข้อความ

ส่วนงาน สำนักงานมหาวิทยาลัย กองเทคโนโลยีดิจิทัล โทร. ๓๒๖๙
ที่ อว ๖๙.๒.๑๑/ ว๑๐ **วันที่** ๔ เมษายน ๒๕๖๕
เรื่อง ขอเชิญเข้าร่วมโครงการเตรียมความพร้อมรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

เรียน ทุกหน่วยงาน

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ จะมีผลบังคับใช้อย่างเต็มรูปแบบในทุกหน่วยงาน ในวันที่ ๑ มิถุนายน ๒๕๖๕ ซึ่งส่งผลกระทบต่อองค์กรทั้งภาครัฐ ภาครัฐวิสาหกิจ และภาคเอกชนจำนวนมาก โดยเฉพาะอย่างยิ่งหน่วยงานในมหาวิทยาลัยแม่โจ้ มีการเก็บข้อมูลส่วนบุคคลของผู้รับบริการจำนวนมากที่อยู่ในระบบงานต่างๆ ซึ่งยังไม่มีการกำกับดูแลข้อมูลอย่างถูกต้อง ชัดเจน ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ นั้น

ในการนี้ กองเทคโนโลยีดิจิทัล สำนักงานมหาวิทยาลัย ได้เห็นความสำคัญของการสื่อสารให้บุคลากร มีความรู้ ความเข้าใจ ตลอดจนทักษะที่จำเป็นเบื้องต้น เพื่อให้สามารถปฏิบัติงานได้อย่างสอดคล้องกับพรบ.คุ้มครองข้อมูลส่วนบุคคล **จึงได้จัดโครงการเตรียมความพร้อมรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในวันอังคารที่ ๑๙ เมษายน ๒๕๖๕ เวลา ๙.๓๐-๑๑.๓๐ น. ผ่านระบบประชุมออนไลน์ MS Teams สามารถลงทะเบียนได้ที่** https://forms.office.com/r/RiRCjpqafs หากมีข้อสงสัยประการใดสามารถสอบถามรายละเอียดเพิ่มเติมได้ที่ คุณบรรพต โตสิตารัตน์ นักวิชาการคอมพิวเตอร์ งานระบบเครือข่ายและบริการอินเทอร์เน็ต หมายเลขโทรศัพท์ ๓๒๖๙

จึงเรียนมาเพื่อโปรดทราบ

(นายวุฒิพล คล้ายทิพย์)
ผู้อำนวยการกองเทคโนโลยีดิจิทัล

Link ลงทะเบียนสัมมนา
https://forms.office.com/r/RiRCjpqafs

บันทึกข้อความ

ส่วนงาน สำนักงานมหาวิทยาลัย กองเทคโนโลยีดิจิทัล โทร. ๓๒๖๙
ที่ อว ๖๙.๒.๑๑/ ว๑๒ **วันที่** ๗ เมษายน ๒๕๖๕
เรื่อง ขอเลื่อนการเข้าร่วมโครงการเตรียมความพร้อมรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

เรียน ทุกหน่วยงาน

ตามหนังสือที่ อว ๖๙.๒.๑๑/ว๑๐ ลงวันที่ ๔ เมษายน ๒๕๖๕ ได้เชิญเข้าร่วมโครงการเตรียมความพร้อมรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในวันที่ ๑๙ เมษายน ๒๕๖๕ เวลา ๙.๓๐-๑๑.๓๐ น. ผ่านระบบประชุมออนไลน์ MS Teams นั้น

เนื่องจากวิทยากรภายนอกติดภารกิจสำคัญในวันดังกล่าว ในการนี้ กองเทคโนโลยีดิจิทัล สำนักงานมหาวิทยาลัย จึงขอเลื่อนการจัดโครงการเตรียมความพร้อมรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) **จากเดิม** ในวันอังคารที่ ๑๙ เมษายน ๒๕๖๕ เวลา ๙.๓๐-๑๑.๓๐ น. **เป็น วันอังคารที่ ๒๖ เมษายน ๒๕๖๕ เวลา ๙.๓๐-๑๑.๓๐ น. ผ่านระบบประชุมออนไลน์ MS Teams สามารถลงทะเบียนได้ที่** https://forms.office.com/r/RiRCjpqafs หากมีข้อสงสัยประการใดสามารถสอบถามรายละเอียดเพิ่มเติมได้ที่ คุณบรรพต โตสิตารัตน์ นักวิชาการคอมพิวเตอร์ งานระบบเครือข่ายและบริการอินเทอร์เน็ต หมายเลขโทรศัพท์ ๓๒๖๙

จึงเรียนมาเพื่อโปรดทราบ

(นายวุฒิพล คล้ายทิพย์)
ผู้อำนวยการกองเทคโนโลยีดิจิทัล

Link ลงทะเบียนสัมมนา
https://forms.office.com/r/RiRCjpqafs

กำหนดการ

“โครงการเตรียมความพร้อมรองรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) สำหรับภาคการศึกษา”

วันอังคารที่ ๒๖ เมษายน ๒๕๖๕ เวลา ๙.๓๐-๑๑.๓๐ น.

ผ่านระบบประชุมออนไลน์ MS Teams

Time	Session
9:30 – 9:35	**พิธีเปิดการการบรรยายในหัวข้อ “เตรียมความพร้อมรองรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) สำหรับภาคการศึกษา”**
9:35 – 10:45	**ทำความรู้จักและเข้าใจ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) สำหรับภาคการศึกษา** คุณธนชาติ วิวัฒนภูติ – หัวหน้าฝ่ายกลยุทธ์โซลูชั่นซอฟต์แวร์การศึกษา บริษัท ลานนาคอม จำกัด
10:45 – 11:15	**แบ่งปันประสบการณ์การเตรียมความพร้อม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)** คุณพงศธร บุญนิธิพัฒน์ – หัวหน้าฝ่ายงานบริการลูกค้า และ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล บริษัท ลานนาคอม จำกัด
11:15 – 11:30	**ถาม-ตอบข้อสงสัย**