เลขที่.....

แบบรายงานการเข้าอบรม / สัมมนา / ศึกษาดูงาน

❑รายบุคคล ☑กลุ่มบุคคล

ชื่อ - สกุล : นายกันตพงศ์ พุ่มอยู่ ตำแหน่ง : นักวิชาการคอมพิวเตอร์	
งาน : ผู้บริหารสำนักหอสมุดกลาง	
ชื่อ - สกุล : นายอดินันท์ เจะตีแม ตำแหน่ง : นักวิชาการคอมพิวเตอร์	
งาน : ฝ่ายเทคโนโลยีห้องสมุด	
ชื่อ - สกุล : นายธนวัฒน์ เสริฐสุวรรณกุล ตำแหน่ง : นักวิชาการคอมพิวเตอร์	
งาน : ฝ่ายเทคโนโลยีห้องสมุด	
ชื่อหลักสูตร : ความมั่นคงปลอดภัยและภัยคุกคาม (นโยบาย/กฎหมาย/PDPA)	
วันเดือนปี : 23 กรกฎาคม 2564	
สถานที่จัด : อบรมออนไลน์ผ่าน Microsoft Teams	
หน่วยงานผู้จัด : สำนักคอมพิวเตอร์มหาวิทยาลัยศรีนครินทรวิโรฒ	
ค่าใช้จ่าย	☑ไม่มี ❑มี เบิกจ่ายจากงบประมาณ ❑แผ่นดิน ❑เงินรายได้ ❑งบอื่นๆ (ระบุ).....
ใบเกียรติบัตร/วุฒิบัตร	☑ได้รับ ❑ไม่ได้รับ เนื่องจาก..... ❑ไม่มี

สำนักคอมพิวเตอร์มหาวิทยาลัยศรีนครินทรวิโรฒ ได้จัดอบรมออนไลน์ ในวันที่ 23 กรกฎาคม 2564 ภายใต้หัวข้อความมั่นคงปลอดภัยและภัยคุกคาม (นโยบาย/กฎหมาย/PDPA) ในการอบรมครั้งนี้จัดเพื่อให้เรารู้และเข้าใจความเสี่ยง ภัยคุกคาม และผลกระทบของภัยทางออนไลน์ เพราะปัจจุบันในช่วงที่เราไม่สามารถหลีกเลี่ยงที่จะทำธุรกรรมต่างๆ ผ่านระบบออนไลน์และแน่นอนว่าส่วนงานที่ได้รับผลกระทบด้านความปลอดภัยมากที่สุดคือ ภาคอุตสาหกรรม ทั่วโลกที่โดนโจมตีทางไซเบอร์มากที่สุดเมื่อเทียบกับด้านอื่นๆ

โดยรูปแบบการโจมตีนั้นมีหลากหลายไม่ว่าจะเป็น การขโมยข้อมูล การเจาะข้อมูล การทำให้ระบบไม่สามารถใช้งานได้หรือทำงานผิดพลาด เป็นต้น แน่นอนว่าผลกระทบที่เราได้รับนั้น เกี่ยวข้องถึงข้อมูลส่วนตัวที่เราทำการระบุไว้ในโลกไซเบอร์ ไม่ว่าจะเป็นไม่ว่าจะเป็น email เบอร์ติดต่อ ที่อยู่ ทุกๆข้อมูลนี้สามารถสร้างภัยคุกคามและผลกระทบกับเราได้มากมาย

ทั้งนี้เราควรเรียนรู้รูปแบบภัยคุกคามที่คนทั่วไปมักจะพบปัญหาโดยมี 2 รูปแบบคือ

1. Malware

Malicious Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ไม่ว่าจะเป็น ไวรัส (Virus), วอร์ม (Worm), โทรจัน (Trojan), สปายแวร์ (Spyware) เป็นต้น ดังนั้น ผู้ใช้งานคอมพิวเตอร์ทุกคนควรรู้ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในทุกรูปแบบ รวมถึงการป้องกันตัวเองจากมัลแวร์ง่าย ๆ ที่ใคร ๆ ก็สามารถทำได้

ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท

- Virus: มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น
- Worm: สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์
- Trojan: หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้งโดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย
- Backdoor: เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว
- Rootkit: เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)
- Spyware: แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย
- Ransomware: ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

ข้อแนะนำในการป้องกันการติดมัลแวร์

- อัพเดทคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ
- ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์
- ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดร์ฟ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน
- ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์-โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ
- ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่
- หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

2. Phishing

Phishing คือคำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น

รูปแบบของ Phishing มีดังนี้

- Phishing ทั่วไป
- SMS-Phishing หรือ Smishing

ข้อแนะนำเพื่อป้องกันตัวเองจาก Phishing

- ไม่มีการร้องขอข้อมูลส่วนบุคคลผ่านทาง Application หรือ SMS จากหน่วยงานต่างๆ
- ตรวจสอบ Link ที่ส่งมา โดยเฉพาะ Shorted URL หากไม่แน่ใจ ติดต่อหน่วยงานที่ส่ง link นั้น
- ห้ามเปิดเผยข้อมูลส่วนบุคคล หากพบการร้องของข้อมูล

- หากส่งรหัสไปแล้ว ให้เปลี่ยนรหัสใหม่ทันที

ซึ่งสิ่งสำคัญคือเราต้องรู้จักภัยคุกคามเพื่อป้องกันและรู้เท่าทันอันตรายจากการใช้บริการโลกไซเบอร์ ทั้งนี้เราสามารถป้องกันภัยคุกคามในระดับรายบุคคลได้ด้วยการ

- การจัดการไฟล์ข้อมูลและการสำรองข้อมูล
- การจัดเก็บข้อมูลบนฐานข้อมูลออนไลน์ในรูปแบบ “คลาวด์”
- การใช้และแบ่งปันข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ในขณะที่สามารถปกป้องตนเองและผู้อื่นจากความเสียหาย
- การใช้บริการดิจิทัล “ความเป็นส่วนตัวและความเป็นสาธารณะ”
- การตั้งรหัสผ่านที่ยากหรือใช้ 2FA (Two Factor Authentication)
- ไม่ควร jail break หรือ root ระบบปฏิบัติการเป็นต้น

พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)

ข้อมูลส่วนบุคคล แบ่งเป็น ข้อมูลส่วนบุคคล และ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ข้อมูลส่วนบุคคล (Personal Data) ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวตนบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม
1. ชื่อ-นามสกุล หรือ ชื่อเล่น 2. ที่อยู่, e-mail, เบอร์โทรศัพท์ 3. รหัสต่างๆที่สามารถบ่งบอกถึงเจ้าตัวของ ข้อมูลส่วนบุคคล เช่น เลขบัตรประชาชน , เลขหนังสือเดินทาง, เลขใบอนุญาติขับขี่, เลขบัญชีธนาคาร, เลขบัตรเครดิต, บัวศรีไอดี เป็นต้น 4. ข้อมูลของอุปกรณ์ที่ใช้งานเครือข่าย เช่น IP Address, Cookie ID 5. ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลส่วนบุคคลได้ เช่น สัญชาติ ส่วนสูง น้ำหนัก สถานที่ทำงาน ข้อมูลการศึกษา ข้อมูลการเงิน 6. ข้อมูลการประเมินผลพนักงาน 7. ข้อมูลที่บันทึกการใช้งาน เช่น Log file	1. เชื้อชาติ หรือ เผ่าพันธุ์ 2. ความคิดเห็นทางการเมือง 3. ความเชื่อในศาสนา 4. พฤติกรรมทางเพศ 5. ประวัติอาชญากรรม 6. ข้อมูลสุขภาพ, ความพิการ หรือข้อมูลพันธุกรรม เช่น DNA 7. ข้อมูลชีวภาพ เช่น ข้อมูลลายนิ้วมือ ข้อมูลสแกนม่านตา 8. ข้อมูลอื่นใดตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

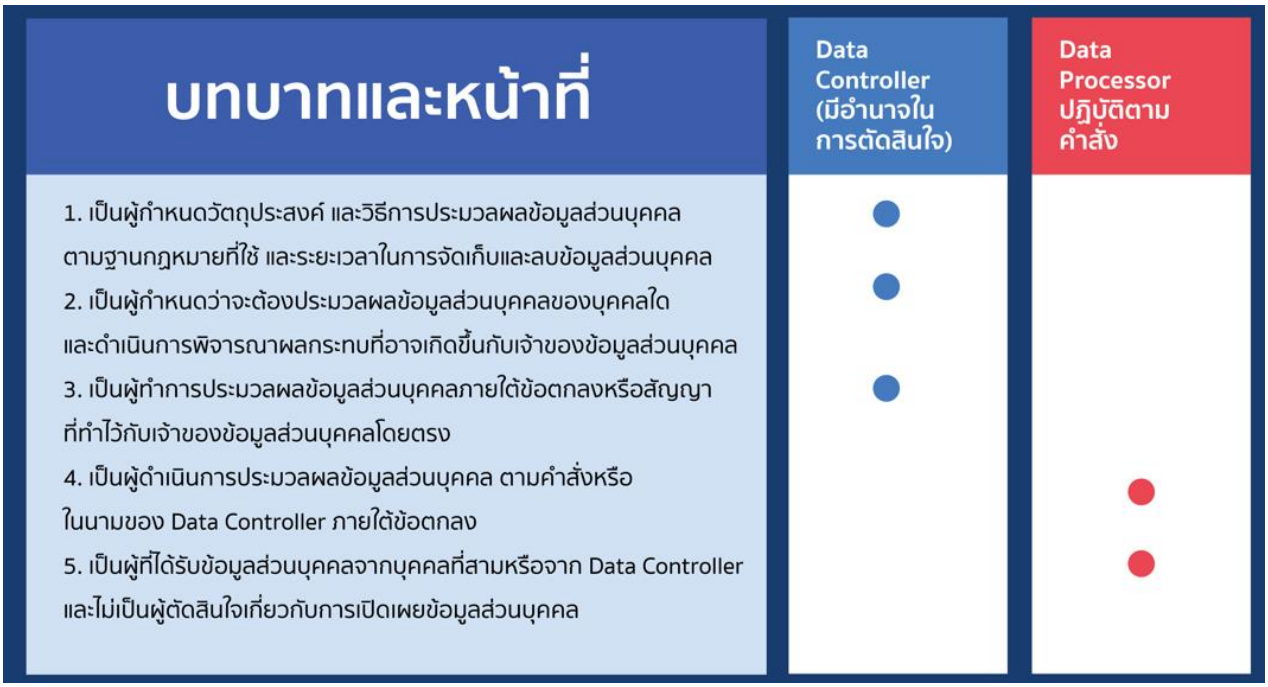
ผู้เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

- เจ้าข้องข้อมูลส่วนบุคคล (Data subject) – บุคคลที่ข้อมูลชี้ไปถึงหรือเป็นคนสร้างข้อมูล
- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) – บุคคลหรือคณะกรรมการซึ่งมีอำนาจตัดสินใจเก็บ รวมรวบ ใช้หรือเผยข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) – บุคคลหรือคณะกรรมการซึ่งดำเนินการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

หลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย

1. ความโปร่งใส่ของกิจกรรมการประมวลผลต่างๆ และสามารถอธิบายได้ว่ามีความชอบธรรมในการประมวลผล
2. มีการตรวจสอบว่ามีการใช้ตามวัตถุประสงค์หรือไม่
3. มีการตรวจสอบว่ามีการเก็บเท่าที่จำเป็นตามวัตถุประสงค์เท่านั้น
4. ข้อมูลมีความเป็นปัจจุบัน ครบถ้วนถูกต้อง
5. ลบหรือทำลายตามระยะเวลาที่กำหนด
6. เก็บรักษาข้อมูลให้เป็นความลับและไม่เปิดเผยข้อมูลส่วนบุคคลแก่ผู้ที่ไม่ได้รับอนุญาต
7. มีความรับผิดชอบและมีหน้าที่ในการดูแลการประมวลผลข้อมูล

ความแตกต่างระหว่าง Data Controller และ Data Processor



DPO

DPO (Data Protection Officer) คือคนที่เข้าดูแลรักษาข้อมูลส่วนบุคคลทั้งหมดในองค์กรไม่ว่าจะเป็นองค์กรข้อมูลภายใน (ข้อมูลพนักงาน) หรือภายนอก (ข้อมูลลูกค้า) หน้าที่ที่สำคัญของตำแหน่งนี้ก็จะรวมไปถึงการกำหนดทิศทาง ซึ่งแน่นอนว่าในตัวกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น DPO นั้นมีหน้าที่ บริหารจัดการ, ให้คำแนะนำ, ประสานงานกับ ส.ค.ส., ตรวจสอบการปฏิบัติการกฎหมาย PDPA, รายงานผลต่อกรรมการบริหารมหาวิทยาลัย

หลักการจัดเก็บข้อมูล

- Necessity เก็บรวบรวมข้อมูลเท่าที่จำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูล
- Relevance เก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะที่เกี่ยวข้องกับวัตถุประสงค์ในการในการประมวลผลข้อมูล
- Limitation เก็บรวมรวมข้อมูลส่วนบุคคลในปริมาณที่จำกัดเฉพาะสำหรับการใช้ประมลผลข้อมูลเท่านั้นและเก็บตามเวลาที่จำเป็นหรือตามกฎหมาย

วงจรการบริหารจัดการข้อมูลส่วนบุคคล

การประมวลผลโดยชอบด้วยกฎหมาย (Lawful Basic)

Historical document and research
ฐานเอกสารประวัติศาสตร์ จดหมายเหตุ หรือการศึกษาวิจัย หรือ วิธีการทางสถิติ

Vital Interest
ฐานการป้องกันหรืออันตรายที่เกี่ยวข้องกับชีวิต ร่างกาย หรือ สุขภาพของบุคคล

Contract
ฐานการปฏิบัติตามสัญญา หรือดำเนินการคำร้องขอของเจ้าของข้อมูลส่วนบุคคลที่ได้ทำสัญญากับมหาวิทยาลัยในการเข้ามาปฏิบัติงาน

Public Task
ฐานภารกิจภาครัฐ หรือการดำเนินการตามนโยบายภาครัฐ

Legitimate Interest
ฐานประโยชน์โดยชอบด้วยกฎหมาย เช่นใช้เพื่อการเรียนการสอน หรือใช้เพื่อการบริหารงานของมหาวิทยาลัย เช่น การขึ้นเงินเดือน

Legal Obligation
ฐานการปฏิบัติตามกฎหมาย เช่นทำตามบทบัญญัติใดของกฎหมาย หรือ หน่วยงานใดของรัฐที่มีอำนาจ

ทั้งนี้ในการขอข้อมูลควรปฏิบัติตามข้อกำหนดและควรทำเอกสารของความยินยอม (Consent) ตามกฎหมายกรณีที่มีการเก็บข้อมูลส่วนบุคคล

หัวข้อในการบันทึกข้อมูลใน ROPA (Record of Processing Activities)

1. ชื่อระบบสารสนเทศที่มีการประมวลผลข้อมูล
2. วัตถุประสงของการเก็บรวมรวมข้อมูลส่วนบุคคลแต่ละประเภท
3. ประเภทเจ้าของข้อมูลส่วนบุคคล เช่น บุคลากร นิสิต หรือผู้ที่มีส่วนเกี่ยวข้อง

4. ประเภทของข้อมูล เช่น ข้อมูลระบุตัวตน ข้อมูลสำหรับการติดต่อ ข้อมูลทางการเงิน เป็นต้น

5. แหล่งที่มาของข้อมูลส่วนบุคคล

6. ฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล

7. มีการเก็บ ใช้ และแก้ไข ข้อมูลส่วนบุคคล เมื่อใด เช่น มีการปรับปรุงข้อมูลเมื่อใดและระยะเวลาในการจัดเก็บเท่าใด

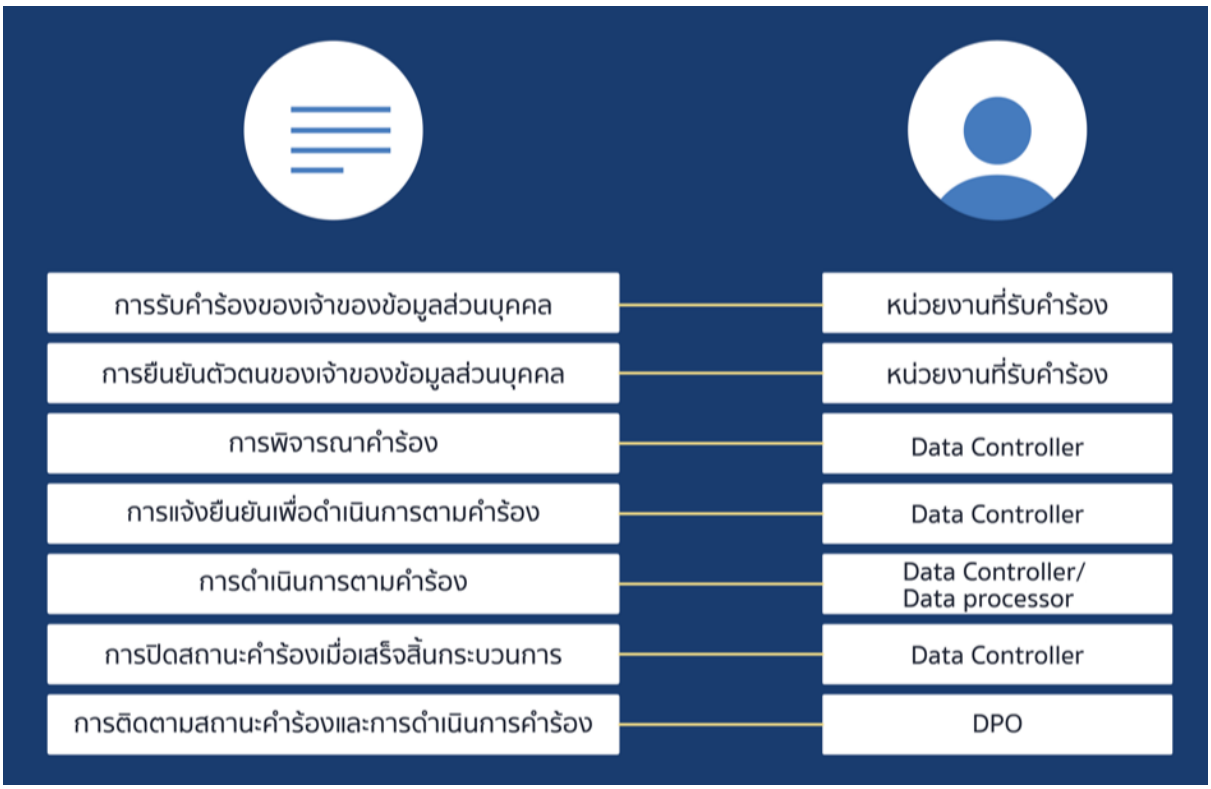
8. มีการเก็บข้อมูลไว้ในลักษณะใด เช่นรูปแบบที่เป็นเอกสารหรือรูปแบบที่เป็นอิเล็กทรอนิกส์

9. มีการโอนย้ายข้อมูลส่วนบุคคลไปยังภายนอกหรือไม่ และโอนไปด้วยวิธีใด

10. มีมาตรการในการรักษาความมั่นคงปลอดภัยอย่างไร

7 สิทธิของเจ้าของข้อมูลส่วนบุคคล Data Subject Right Request (DSSR)

DSSR Procedures



การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล

หน่วยงานหรือมหาวิทยาลัยต้องรับคำร้องของเจ้าของข้อมูลส่วนบุคคลซึ่งอาจจะมีพิจารณาปฏิเสธคำรองข้องเจ้าของข้อมูลได้กรณีที่คำร้องมีลักษณะดังต่อไปนี้

- คำร้องไม่สมเหตุสมผล
- คำร้องที่มีซ้ำๆ หรือมีจำนวนมากเกินไป
- คำร้องที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่มหาวิทยาลัยไม่ได้มีการจัดเก็บ
- คำร้องที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีความจำเป็นสำหรับการประมวลผล
- ตามฐานกฎหมาย หรือเพื่อวัตถุประสงค์ตามสัญญา ตามกฎระเบียบหรือตามที่กฎหมายกำหนด

มาตรการการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ข้อปฏิบัติในการเตรียมความพร้อมในการปฏิบัติตาม PDPD 10 ข้อ มีดังต่อไปนี้

1. ตั้งงบประมาณ
2. จัดตั้งคณะกรรมการหรือคณะทำงาน
3. กำหนดประเภทของข้อมูลและวัตถุประสงค์
4. ดำเนินการจัดทำ Data Protection Policy
5. Security Awareness training ในองค์กร
6. จัดทำการบวนการแจ้งเตือน Breach Notification
7. จัดทำเอกสารเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย (privacy and security Policy)
8. จัดเตรียมข้อกำหนดและแนวทางปฏิบัติ
9. พัฒนาทักษะกระบวนการ audit
10. จัดทำ security and privacy by design

ประโยชน์ที่ได้รับ

1. ได้เรียนรู้เกี่ยวกับเรื่องที่ควรระวังเกี่ยวกับภัยคุกคามทางไซเบอร์และกฎหมายเกี่ยวกับ PDPA เพื่อเตรียมรับมือกับรูปแบบการทำงานที่เปลี่ยนไปตามข้อกำหนดทางกฎหมาย

หัวข้อการปรับปรุง / พัฒนา	รายงานผลการปรับปรุง / พัฒนา ภายในวันที่

ข้อเสนอแนะอื่นๆ

.....

.....

.....

ผู้รายงาน.....

(นายอดินันท์ เจะตีแม)

ตำแหน่งนักวิชาการคอมพิวเตอร์

ผู้รายงาน..... .....

(นายกันตพงศ์ พุ่มอยู่)

ตำแหน่งนักวิชาการคอมพิวเตอร์

ผู้รายงาน..... .....

(นายธนวัฒน์ เสริฐสุวรรณกุล)

ตำแหน่งนักวิชาการคอมพิวเตอร์

วันที่ 2 กันยายน 2564

ความคิดเห็นของหัวหน้าหน่วยงาน

.....

.....

ลงชื่อ..... .....

(นายทรงยศ ขันบุตรศรี)

ตำแหน่งหัวหน้าฝ่ายเทคโนโลยีห้องสมุด

วันที่ 2 กันยายน 2564

ความคิดเห็นของผู้บริหารที่กำกับดูแลหน่วยงาน

.....

.....

ลงชื่อ.. .....

(ผศ.นพ.วิศาล มหาสิทธิวัฒน์)

ผู้อำนวยการสำนักหอสมุดกลาง

วันที่ - 6 ก.ย. 2564 /...../.....

หมายเหตุ : 1. จัดทำรายงานฯ หลังจากเข้าร่วมประชุม/ อบรม/สัมมนา /ศึกษาดูงาน ภายใน 7 วันทำการเสนอหัวหน้าฝ่าย

2. หัวหน้าฝ่ายเสนอความเห็น ภายใน 3 วันทำการ และเสนอต่อผู้อำนวยการสำนักหอสมุดกลาง

3. แจ้งผู้รายงานทราบ และจัดเก็บเข้าแฟ้มรายงานการเข้าประชุม/ อบรม/สัมมนา /ศึกษาดูงาน

4. หัวหน้าฝ่ายติดตามผลการปรับปรุงพัฒนา

5. หัวหน้าฝ่ายรายงานผลการปรับปรุงพัฒนาให้ผู้อำนวยการสำนักหอสมุดกลางได้ทราบ