แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Incident Response Plan)
มหาวิทยาลัยราชภัฏกำแพงเพชร

1. เจ้าของข้อมูลส่วนบุคคล แจ้งเหตุละเมิดข้อมูลส่วนบุคคล ในระบบรับรองสิทธิ หรือช่องทางอื่นใดที่มหาวิทยาลัยจัดเตรียมไว้

2. ผู้ควบคุมข้อมูลส่วนบุคคล/เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตรวจสอบเหตุละเมิด

- ตรวจสอบข้อมูลส่วนบุคคลตามที่เจ้าของข้อมูลส่วนบุคคลได้แจ้งไว้ ถูกทำให้สูญเสียการเป็นความลับ ความถูกต้อง หรือความพร้อมใช้ หรือไม่
- ตรวจสอบตัวตนของเจ้าของข้อมูลว่า เป็นบุคคลเดียวกันที่เป็นเจ้าของข้อมูลหรือไม่ โดยสามารถแจ้งให้เจ้าของข้อมูลส่งรายละเอียดเพิ่มเติม เพื่อยืนยันตัวตนได้ (เริ่มนับระยะเวลาดำเนินการแจ้งเหตุละเมิดแก่ สคส. ภายใน 72 ชม.)
    - กรณีผู้ประมวลผลข้อมูลทราบเหตุละเมิด ให้แจ้งผู้ควบคุมข้อมูลภายใน 24 ชม.
    - กรณีผู้ควบคุมข้อมูลทราบเหตุละเมิด ให้แจ้ง DPO ภายใน 24 ชม.
- ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเชิงองค์กร (organizational measures) และ มาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว

3. ผู้ควบคุมข้อมูล/เจ้าหน้าที่คุ้มครองข้อมูล ประเมินผลกระทบต่อความเสียหายของเจ้าของข้อมูลส่วนบุคคล

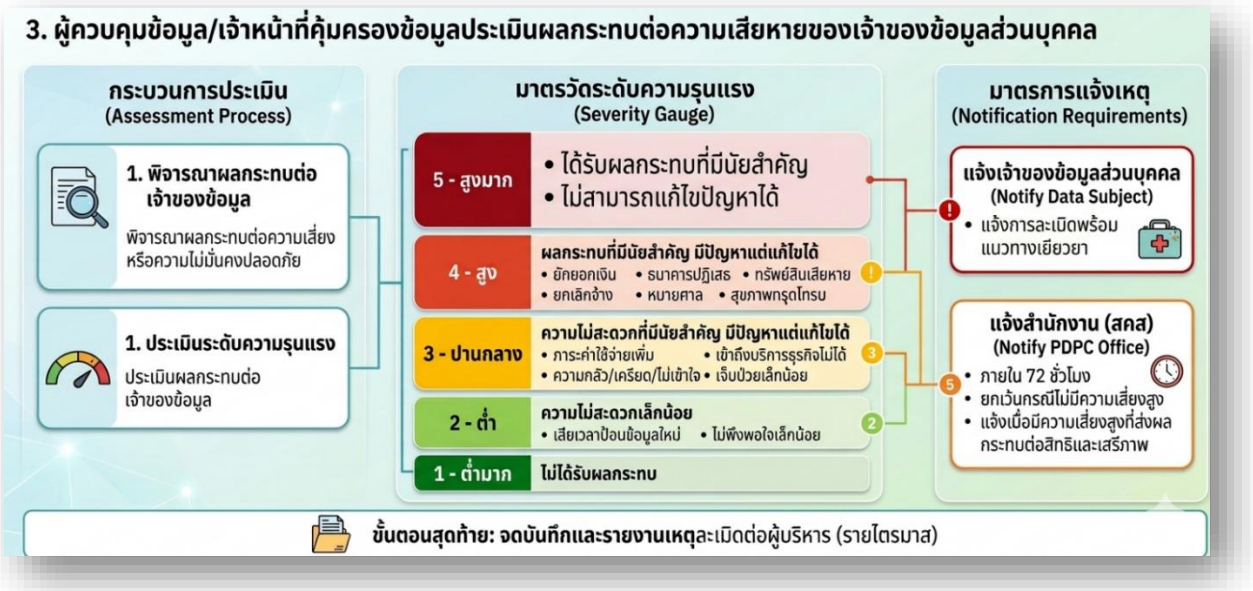
- พิจารณาผลของเหตุการณ์ข้อมูลรั่วไหลนั้น ได้ส่งผลกระทบต่อความเสี่ยงหรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่
- ประเมินระดับความรุนแรงและผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ระดับความรุนแรง	ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล
5 - สูงมาก	ได้รับผลกระทบที่มีนัยสำคัญ และไม่สามารถแก้ไขปัญหาได้ เช่น เกิดความเสียหายด้านการเงิน ทำให้เกิดหนี้สิน ไม่สามารถชดใช้ได้ ไม่สามารถทำงานได้ ได้รับผลกระทบทางจิตใจหรือร่างกาย หรือทำให้ถึงขั้นเสียชีวิต
4 - สูง	ได้รับผลกระทบที่มีนัยสำคัญ ซึ่งมีปัญหา- ความยุ่งยากต่อเจ้าของข้อมูลส่วนบุคคล แต่สามารถแก้ไขปัญหาได้ เช่น ถูกยักยอกเงิน ถูกธนาคารปฏิเสธการทำธุรกรรม ทรัพย์สินเสียหาย ถูกเลิกจ้าง ได้รับหมายศาล สุขภาพทรุดโทรม
3 - ปานกลาง	ได้รับความไม่สะดวกอย่างมีนัยสำคัญ ซึ่งมีปัญหา-ความยุ่งยากเล็กน้อย แต่สามารถแก้ไขปัญหาได้ เช่น เจ้าของข้อมูลส่วนบุคคลมีภาระค่าใช้จ่ายเพิ่มเติม ถูกปฏิเสธการเข้าถึงบริการทางธุรกิจ มีความกลัว มีความเครียด เกิดความไม่เข้าใจ หรือมีอาการเจ็บป่วยทางกายเล็กน้อย
2 - ต่ำ	ได้รับความไม่สะดวกเพียงเล็กน้อย เช่น เจ้าของข้อมูลส่วนบุคคลเสียเวลาในการป้อนข้อมูลใหม่ หรือ มีความไม่พึงพอใจเล็กน้อย
1 - ต่ำมาก	ไม่ได้รับผลกระทบ

หมายเหตุ ระดับความรุนแรง 5 - สูงมาก และ 4 - สูง แจ้งเจ้าของข้อมูลส่วนบุคคล
ระดับความรุนแรง 2 - ต่ำ จนถึง 5 - สูงมาก แจ้งสำนักงาน (สคส.)
ระดับความรุนแรง 1 - ต่ำมาก จดบันทึกและรายงานเหตุละเมิดต่อผู้บริหาร/รายไตรมาส

ข้อกำหนดการแจ้งเหตุละเมิด

ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลนั้นแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง เว้นแต่การละเมิดดังกล่าวไม่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีความเสี่ยงสูงที่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งการละเมิดให้เจ้าของข้อมูลทราบพร้อมแนวทางเยียวยา



4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล ผู้ดูแลระบบสารสนเทศ เจ้าหน้าที่ IT

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

5. ผู้ควบคุมข้อมูล/เจ้าหน้าที่คุ้มครองข้อมูลแจ้งเหตุละเมิด ต่อ สคส. และเจ้าของข้อมูลส่วนบุคคล

6. ผู้เกี่ยวข้องทุกฝ่าย ทบทวนแนวทางการรับมือและหาวิธีการป้องกันไม่ให้เกิดขึ้นอีก

รายการที่ต้องแจ้งต่อ สคส.	รายการที่ต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคล
1. คำอธิบายลักษณะของการรั่วไหลของข้อมูล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง 2. ประเภทเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคล 3. วิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) 4. คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว 5. คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น 6. รายละเอียดอื่น ๆ เพิ่มเติมตามความเหมาะสม	1. คำอธิบายลักษณะของการรั่วไหลของข้อมูลส่วนบุคคล 2. วิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของสำนักงาน 3. ผลที่อาจจะเกิดขึ้นจากการที่ข้อมูลส่วนบุคคลรั่วไหล ซึ่งรวมถึงความเสี่ยง ต่อเจ้าของข้อมูลส่วนบุคคล 4. มาตรการที่เสนอแนะหรือแนวทางเยียวยาให้เจ้าของข้อมูลส่วนบุคคลกระทำเพื่อรับมือกับกรณีดังกล่าว ซึ่งอาจจะลดผลร้ายที่เกิดจากการมีข้อมูลส่วนบุคคลรั่วไหลได้