แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

1. เจ้าของข้อมูลส่วนบุคคล แจ้งเหตุละเมิดข้อมูลส่วนบุคคล ในระบบรับรองสิทธิ –หรือช่องทางอื่นใดที่มหาวิทยาลัยจัดเตรียมไว้

2. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตรวจสอบเหตุละเมิด

- DPO ต้องตรวจสอบข้อมูลส่วนบุคคลตามที่เจ้าของข้อมูลส่วนบุคคลได้แจ้งไว้ ถูกทำให้สูญเสียการเป็นความลับ ความถูกต้อง หรือความพร้อมใช้หรือไม่
- DPO ตรวจสอบตัวตนของเจ้าของข้อมูลว่า เป็นบุคคลเดียวกันที่เป็นเจ้าของข้อมูลหรือไม่ โดยสามารถแจ้งให้เจ้าของข้อมูลส่งรายละเอียดเพิ่มเติมเพื่อยืนยันตัวตนได้ (*เริ่มนับระยะเวลาดำเนินการแจ้งเหตุละเมิดแก่ สคส. ภายใน 72 ชม.)

*กรณีผู้ประมวลผลข้อมูลทราบเหตุละเมิด ให้แจ้งผู้ควบคุมข้อมูลภายใน 24 ชม.

*กรณีผู้ควบคุมข้อมูลทราบเหตุละเมิด ให้แจ้ง DPO ภายใน 24 ชม.

- DPO ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเชิงองค์กร (organizational measures) และ มาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว

แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

PDPA Personal Data Protection Act พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

3. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประเมินผลกระทบต่อความเสียหายของเจ้าของข้อมูลส่วนบุคคล

- DPO พิจารณาผลของเหตุการณ์ข้อมูลรั่วไหลนั้น ได้ส่งผลกระทบต่อความเสี่ยงหรือความไม่มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่
- DPO 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 หรือมีความไม่พึงพอใจเล็กน้อย
1 - ต่ำมาก	ไม่ได้รับผลกระทบ

แจ้งเจ้าของข้อมูลส่วนบุคคล

แจ้งสำนักงาน (สคส)

ข้อกำหนดการแจ้งเหตุละเมิด

- ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลนั้นแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง เว้นแต่การละเมิดดังกล่าวไม่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีความเสี่ยงสูงที่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งการละเมิดให้เจ้าของข้อมูลทราบพร้อมแนวทางเยียวยา

จดบันทึกและรายงานเหตุละเมิดต่อผู้บริหาร/รายไตรมาส

แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูล ผู้ดูแลระบบสารสนเทศ เจ้าหน้าที่ IT

- **หาสาเหตุและดำเนินการป้องกัน ระงับเหตุ หรือแก้ไข** เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที เท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม (ควรซึ่งได้รับการอนุมัติจากผู้บริหาร พร้อมระบุระยะเวลาในการดำเนินการที่แน่นอน)
- ทบทวน-ปรับปรุงมาตราการรักษาความปลอดภัยของข้อมูลให้รัดกุม
- หากการรั่วไหลของข้อมูลส่วนบุคคล ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (ในระดับ2-5) DPO ต้องส่งเรื่องไปยังผู้บริหารที่เกี่ยวข้องทราบภายในระยะเวลาที่รวดเร็ว
- *ผู้เกี่ยวข้องทุกฝ่าย รวมถึงผู้บริหาร ร่วมกำหนด**แนวทางเยียวยา** - หามาตรการบรรเทาผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลอย่างเร่งด่วน

5. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแจ้งเหตุละเมิด ต่อ สคส.-เจ้าของข้อมูลส่วนบุคคล

6. ผู้เกี่ยวข้องทุกฝ่าย ทบทวนแนวทางการรับมือและหาวิธีการป้องกันไม่ให้เกิดขึ้นอีก

แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

PDPA Personal Data Protection Act พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

รายการที่ต้องแจ้งต่อ สคส.	รายการที่ต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคล
1. คำอธิบายลักษณะของการรั่วไหลของข้อมูล ประเภทของข้อมูล และจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณ 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

แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

ข้อ ๗ ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่าเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานพิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานโดยเร็ว ทั้งนี้ ต้องไม่เกินสิบห้าวันนับแต่ทราบเหตุ

ข้อ ๘ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือมอบหมายหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของตนเอง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุไว้ในข้อตกลงหรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน

แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

ข้อ ๑๑ ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ หากโดยสภาพไม่สามารถดำเนินการแจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้

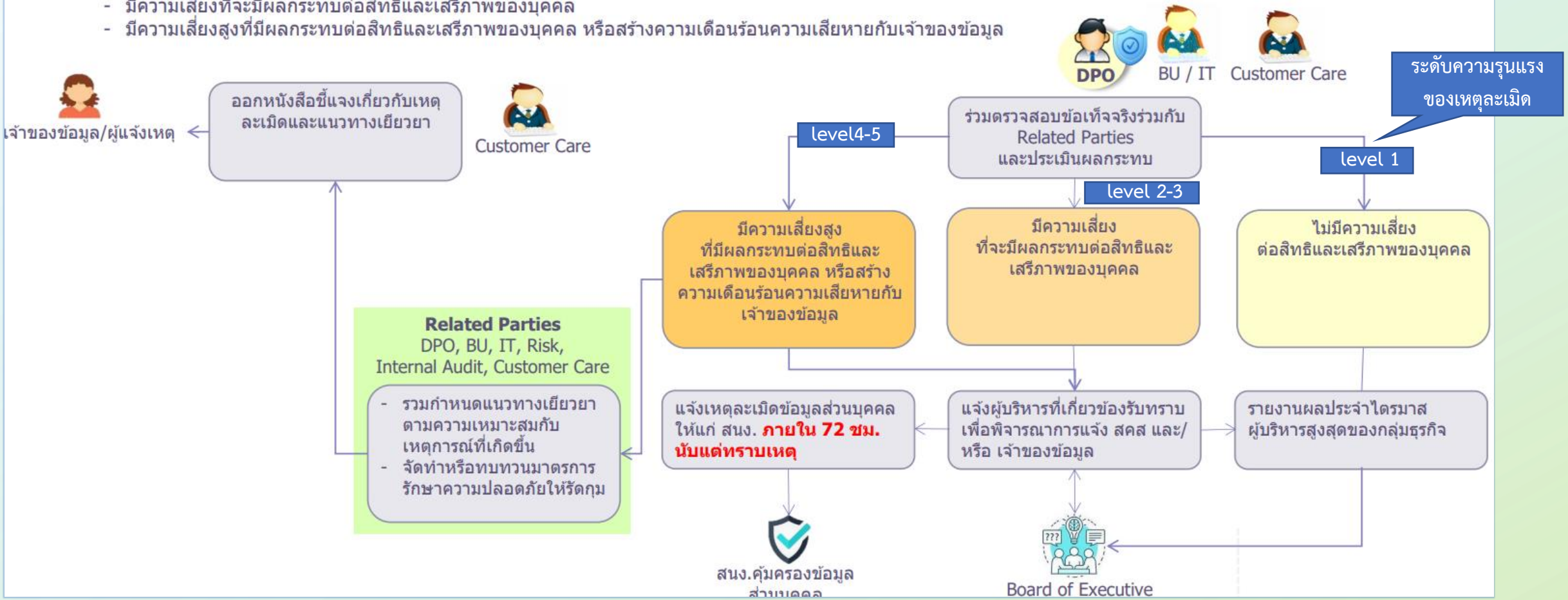
การแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไป จะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

แนวปฏิบัติการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

Data Breach / Data Leaks Process การจัดการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

การการแจ้งเหตุละเมิดตามการพิจารณาผลกระทบและระดับความรุนแรง

- พิจารณาเหตุการณ์ว่าเป็นเหตุละเมิดข้อมูลส่วนบุคคลหรือไม่
- พิจารณาผลกระทบตามระดับความรุนแรง
  - ไม่มีความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล
  - มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
  - มีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือสร้างความเดือนร้อนความเสียหายกับเจ้าของข้อมูล



เอกสารที่เกี่ยวข้อง

สำหรับเจ้าของข้อมูล/ผู้ควบคุมข้อมูล เพื่อแจ้งเหตุละเมิด

แบบการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ส่วนที่ 1 ข้อมูลของผู้แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

เพื่อการยืนยันตัวตนของผู้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ขอให้ท่านกรอกข้อมูลของท่านตามที่ระบุไว้ดังต่อไปนี้ ชื่อ.....นามสกุล.....

ที่อยู่.....

เบอร์โทรศัพท์ที่ติดต่อได้..... อีเมล .....

ส่วนที่ 2 รายละเอียดของเหตุการละเมิดข้อมูลส่วนบุคคล (พร้อมแนบหลักฐาน (หากมี))

.....

.....

.....

ส่วนที่ 3 การดำเนินงานของมหาวิทยาลัย ภายหลังจากที่ได้รับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

มหาวิทยาลัยขอขอบคุณที่ท่านกรุณาแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลพร้อมทั้งเอกสารและรายละเอียดที่เกี่ยวข้อง ทั้งนี้มหาวิทยาลัยจะรีบดำเนินการพิจารณาเรื่องดังกล่าวโดยเร็ว หากมีกรณีที่มหาวิทยาลัยอาจต้องการการอธิบายเพิ่มเติมจากท่าน มหาวิทยาลัยจะดำเนินการติดต่อท่านกลับไปตามรายละเอียดที่ท่านได้ให้ไว้ในส่วนที่ 1

ส่วนที่ 4 คำรับรอง

ข้าพเจ้าขอยืนยันว่าข้าพเจ้าได้อ่านและเข้าใจเนื้อหาและข้อกำหนดตามที่ระบุไว้ในแบบการแจ้งเหตุฉบับนี้ พร้อมทั้งรับรอง ว่าข้อมูลดังกล่าวที่ข้าพเจ้าให้ไว้ตามเอกสารฉบับนี้ถูกต้อง ครบถ้วนและสมบูรณ์ ข้าพเจ้าขอยืนยันและรับประกันว่า ข้าพเจ้าไม่มีเจตนาดำเนินการเพื่อก่อให้เกิดความเสียหายกับบุคคลใด ข้าพเจ้าจึงได้ลงลายมือชื่อตามที่ระบุด้านล่างนี้

ลายมือชื่อ.....

(.....)

วันที่.....

เอกสารประกอบการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

-สำหรับ DPO เพื่อบันทึกเหตุ
-สำหรับผู้ควบคุมข้อมูล เพื่อแจ้งเหตุต่อ DPO

สำหรับ DPO หรือ ผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล ที่ทบข้อมูลส่วนบุคคลรั่วไหลแล้วแต่กรณีและจะต้องแจ้งแก่ DPO ทราบถึงเหตุการณ์การรั่วไหล

แบบฟอร์มการบันทึกการรั่วไหลของข้อมูลส่วนบุคคล

โปรดระบุรายละเอียดเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

วันและเวลาที่พบการรั่วไหล : .....

โปรดอธิบายอย่างละเอียดถึงเหตุการณ์ที่เกิดขึ้น :

.....

.....

พบการรั่วไหลได้อย่างไร : ..... วัน

และเวลาที่การรั่วไหลเกิดขึ้น : .....

ประเภทของเจ้าของข้อมูลส่วนบุคคล (เลือกทุกข้อที่มีความเกี่ยวข้อง)

☐ นักเรียน/ นักศึกษา ☐ บุคลากร ☐ ผู้เยาว์ ☐ ไม่ทราบแน่ชัด

☐ อื่น ๆ (โปรดระบุ) .....

ประเภทของข้อมูลที่เกิดการรั่วไหล (เลือกทุกข้อที่มีความเกี่ยวข้อง)

☐ ข้อมูลทั่วไป เช่น ชื่อ ข้อมูลติดต่อ
☐ เอกสารทางการ เช่น บัตรประชาชน
☐ Usernames, Passwords
☐ ข้อมูลด้านการเงิน เช่น เลขบัตรเครดิต ❐
☐ ข้อมูล GPS locations
☐ ข้อมูลเกี่ยวกับเชื้อชาติ หรือ สัญชาติ
☐ ข้อมูลด้านความคิดเห็นทางการเมือง
☐ ข้อมูลเกี่ยวกับศาสนา
☐ ข้อมูลเกี่ยวกับเพศ
☐ ข้อมูลเรื่องสุขภาพ
☐ ข้อมูลทางชีวภาพ
☐ ประวัติอาชญากรรม
☐ ยังไม่ทราบ
☐ อื่น ๆ (โปรดระบุ) .....

ปริมาณโดยสังเขปของข้อมูลที่รั่วไหล : .....

ปริมาณโดยสังเขปของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ :

.....

โปรดอธิบายอย่างละเอียดถึงผลกระทบที่น่าจะเกิดจากการรั่วไหล :

.....

สำหรับDPO
-แจ้งเหตุละเมิดต่อสคส.
-แจ้งเหตุละเมิดต่อเจ้าของข้อมูล

(ร่าง) หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

Personal Data Breach Notification

วันที่ .....

เรียน สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ด้วยมหาวิทยาลัยเทคโนโลยีสุรนารี ได้ตรวจพบเหตุการณ์ละเมิดในข้อมูลส่วนบุคคลที่มหาวิทยาลัยฯ เก็บรักษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งมหาวิทยาลัยพิจารณาว่าเหตุดังกล่าว มีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

เพื่อเป็นการปฏิบัติตามความของมาตรา 37(4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มหาวิทยาลัยจึงขอนำเรียนหนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังต่อไปนี้

รายละเอียดของเหตุละเมิดข้อมูลส่วนบุคคล	ระบุรายละเอียดเหตุการณ์ที่เป็นภัยคุกคามข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะละเมิดสิทธิเสรีภาพของบุคคล เช่น 1. ข้อมูลถูกลักลอบคัดลอกออกไปภายนอกโดยอดีตพนักงาน 2. ฐานข้อมูลขององค์กรถูกโจมตีและเข้าถึงโดยมิชอบ 3. ฐานข้อมูลขององค์กรถูกโจมตีโดย Ransomware ทำให้ไม่สามารถให้บริการประชาชน/ลูกค้า ได้ในช่วงระยะเวลาหนึ่ง หรือ ทำให้บริการเกิดล่าช้า 4. เอกสาร (กระดาษ) ที่มีรายการข้อมูลส่วนบุคคลถูกโจรกรรม
วันเวลาที่ทราบเหตุ	ระบุวันเวลาที่ทราบเหตุ เช่น วันที่ 1 มกราคม 2564 เวลา 15.00 น.
ผู้ที่รายงานเหตุให้ทราบ (หากมี)	ระบุชื่อผู้ที่แจ้ง/พบเหตุการณ์ เป็นคนแรก
รายการข้อมูลส่วนบุคคล	ระบุรายการข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการณ์ เช่น