แนวปฏิบัติ

เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

จัดทำโดย
นิติกร หน่วยทรัพยากรบุคคล ฝ่ายบริหารงานทั่วไป

แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล
สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

1. วัตถุประสงค์

เพื่อใช้สำหรับเป็นแนวทางปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำของสถาบัน (DPO) ตลอดจนเป็นแนวทางในการปฏิบัติให้กับบุคลากรสถาบัน นักศึกษา หรือบุคคลอื่นใดที่พบเจอเหตุละเมิดข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสถาบัน และเป็นไปตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) กำหนดตามกฎหมาย

2. ขอบเขต

แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลนี้ ใช้ดำเนินการงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน ในกรณีที่อาจเกิดหรือเกิดเหตุละเมิดข้อมูลส่วนบุคคล ซึ่งอยู่ในความควบคุมดูแลของสถาบัน โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือนิติกร มีหน้าที่ต้องประเมินความเสี่ยงและแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลผู้เป็นเจ้าของข้อมูลเพียงใด

3. คำจำกัดความ

“สถาบัน” หมายความว่า สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า สถาบัน ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายความว่า รองอธิการบดีฝ่ายบริหาร ซึ่งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำสถาบัน

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคล ซึ่งมีหน้าที่ดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในนามของสถาบัน

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ กระทำโดยปราศจากอำนาจหรือโดยมิชอบ หรือกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่อง หรือเหตุอื่นใด

4. ประโยชน์ที่คาดว่าจะได้รับ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำสถาบัน (DPO) ตลอดจนบุคลากรสถาบัน นักศึกษา หรือบุคคลอื่นใดที่พบเจอเหตุละเมิดข้อมูลส่วนบุคคลซึ่งเกี่ยวข้องกับสถาบัน ทราบแนวทางในการปฏิบัติเมื่อพบเจอเหตุละเมิดข้อมูลส่วนบุคคล และสามารถแจ้งเหตุดังกล่าว ต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลตามระยะเวลาที่กฎหมายกำหนด

5. ช่องทางการรับเรื่อง/การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย มีช่องทางการรับเรื่อง/การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลรวม 4 ช่องทาง ดังนี้

1. กล่องรับความเห็น ณ ชั้น 1 อาคารเฉลิมพระเกียรติ 6 รอบ พระชนมพรรษา และชั้น G อาคารสิรินธรานุสรณ์ ๖๐ พรรษา
2. โทรศัพท์ งานนิติกร หน่วยทรัพยากรบุคคล ฝ่ายบริหารงานทั่วไป เบอร์ 02-256-4092 ต่อ 1154 หรือ 1199
3. มาพบนิติกรด้วยตนเอง ณ ห้องฝ่ายบริหารงานทั่วไป ชั้น 8 อาคารสิรินธรานุสรณ์ ๖๐ พรรษา
4. ไปรษณีย์อิเล็กทรอนิกส์ (อีเมล) ถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล : sarinrat.w@stin.ac.th หรือนิติกร : suradej.m@stin.ac.th, fa-is.y@stin.ac.th

หมายเหตุ : แบบฟอร์มการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล สามารถดาวน์โหลดได้ที่เว็บไซต์: https://stin.ac.th/ ไปที่ หัวข้อ “ข้อมูลส่วนบุคคล หรือ PDPA” เลือกหัวข้อ “แบบฟอร์ม” และเลือกหัวข้อ “แบบฟอร์มการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล” พร้อมหลักฐานประกอบการพิจารณา

6. แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

เมื่อได้รับเรื่อง แจ้ง หรือพบเจอเหตุละเมิดข้อมูลส่วนบุคคลให้ดำเนินการโดยอ้างอิงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 และประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ช่องทางอิเล็กทรอนิกส์ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลสำหรับผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2568 โดยมีขั้นตอน ดังนี้

6.1 เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลขึ้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนิติกรจะต้อง **ตรวจสอบความน่าเชื่อถือและข้อเท็จจริงการแจ้งเหตุละเมิดละเมิดข้อมูลส่วนบุคคลดังกล่าว** รวมทั้งต้องมี **การประเมินความเสี่ยงว่าเหตุละเมิดที่เกิดขึ้นนั้นมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลมากน้อยเพียงใด** โดยเหตุละเมิดข้อมูลส่วนบุคคลมีวิธีการได้มา 3 กรณี ดังนี้

6.1.1 บุคลากรสถาบัน นักศึกษา หรือบุคคลภายนอกแจ้งเหตุละเมิดข้อมูลส่วนบุคคลด้วยตนเอง

6.1.2 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพบเจอเหตุละเมิดด้วยตนเอง

6.1.3 ผู้ประมวลผลข้อมูลส่วนบุคคลพบเจอเหตุละเมิดข้อมูลส่วนบุคคล จะต้องดำเนินการแจ้งให้สถาบันทราบโดยเร็ว

6.2 เมื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนิติกรดำเนินการพิจารณาความน่าเชื่อถือและข้อเท็จจริงว่าเหตุละเมิดดังกล่าวเป็นความจริง รวมทั้งได้ประเมินความเสี่ยงเสร็จสิ้นแล้ว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนิติกรต้องดำเนินการแจ้งผลสรุปดังกล่าว แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) **ภายใน 72 ชั่วโมง หรือระยะเวลาท่าที่จะสามารถกระทำได้**

หากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนิติกรพิจารณาแล้วเห็นว่าเหตุละเมิด**ไม่เป็นความจริงและไม่มีความเสี่ยงใด ๆ** เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนิตกรต้องแจ้งเหตุยกเว้นดังกล่าว พร้อมหลักฐาน แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) พิจารณา

อนึ่ง ข้อมูลสาระสำคัญที่ต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตามวรรคแรก ได้แก่ **บทสรุปเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคล ช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผลกระทบที่อาจเกิดขึ้น และมาตรการเยียวยา**

6.3 เมื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนิตกรประเมินความเสี่ยงแล้วพบว่า**มีความเสี่ยงสูงต่อสิทธิและเสรีภาพ หรือมีความจำเป็น** เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนิติกรจะต้อง**แจ้งแก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ** โดยมีข้อมูลสาระสำคัญ ได้แก่ **บทสรุปเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคล ช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผลกระทบที่อาจเกิดขึ้น และมาตรการเยียวยา**

7. ตัวอย่างเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

7.1 เหตุการณ์ที่ไม่ถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล

หน่วยงานแห่งหนึ่ง ขอเบอร์ติดต่อเจ้าหน้าที่ทุกคน เพื่อจัดทำหนังสือโทรศัพท์ในที่ทำงาน เจ้าหน้าที่ ก ไม่ให้เบอร์ติดต่อกับผู้ประมวลผลข้อมูลในการจัดทำหนังสือโทรศัพท์ และอ้างว่าผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งในความจริงผู้ประมวลผลสามารถกระทำได้ เนื่องจากเป็นการใช้ในการดำเนินงานภายในหน่วยงาน เพื่อให้การปฏิบัติงานมีความสะดวกและมีประสิทธิภาพยิ่งขึ้น แต่ทั้งนี้ผู้ควบคุมข้อมูลยังคงมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่นำมาใช้ในการดำเนินงานภายในหน่วยงาน

7.2 เหตุการณ์ที่ถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล

เจ้าหน้าที่ในหน่วยงานแห่งหนึ่ง ได้ใช้กระดาษพิมพ์งานของตน ซึ่งด้านหลังเป็นสำเนาบัตรประจำตัวประชาชน ซึ่งเจ้าหน้าที่ดังกล่าวใช้กระดาษรียูสในการพิมพ์งานโดยที่ด้านหลังเป็นสำเนาบัตรประจำตัวประชาชน หากกรณีดังกล่าวพบเจอโดยบุคคลภายนอกอาจถือได้ว่าเป็นการละเมิดข้อมูลส่วนบุคคล ทำให้ข้อมูลรั่วไหลไปยังภายนอก อาจทำให้เจ้าของบัตรเสียหายได้

8. การประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

8.1 ปัจจัยที่อาจนำมาพิจารณาในการประเมินความเสี่ยง

โดยที่ข้อ 12 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ได้กำหนดปัจจัยในการประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล ซึ่งอาจพิจารณาจากปัจจัยดังต่อไปนี้

1. ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล
2. ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด
3. ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

4. ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจำกัดต่าง ๆ ด้วยหรือไม่ เพียงใด

5. ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

6. ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

7. ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)

8. สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคล รวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

8.2 ตัวอย่างการประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

รายละเอียดดังต่อไปนี้เป็นตัวอย่างแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด

โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าวต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
1	ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ความเสี่ยงต่ำ เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้ว ข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
2	ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก
3	ระบบไฟฟ้าใน Call center ของ คณะ ส่วนงาน หน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ขัดข้อง โดยไฟดับชั่วคราว ส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของคณะ ส่วนงาน หน่วยงาน ในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งานเนื่องจากปัญหาทางด้านเทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วนบุคคลดังกล่าวก็สามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
4	ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูล ส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้และการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง นอกจากนี้ยังอาจก่อให้เกิดความเสียหายต่อธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงตัวเจ้าของข้อมูลส่วนบุคคลจึงต้องแจ้งเหตุ

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
5	ธนาคารได้รับการติดต่อจากลูกค้าธนาคาร 1 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้วภายใน 24 ชั่วโมง พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน 10 ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล 10 ราย ที่ถูกเรียกเก็บเงินตาม ใบแจ้งหนี้ของธนาคาร	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตามคณะส่วนงาน หน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม
6	ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาผู้ควบคุมข้อมูลส่วนบุคคลถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลรายชื่อผู้ใช้บริการ รหัสผ่าน และประวัติการซื้อสินค้าถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต	ต้องแจ้ง	ต้องแจ้งลูกค้าของผู้ควบคุมข้อมูลส่วนบุคคลในส่วนที่มีข้อมูลรั้วไหลบน อินเทอร์เน็ต	ข้อมูลที่มการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
7	เว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้างประมวลผลข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลเกิดปัญหาข้อผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง ทำให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้	ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งสำนักงานฯ เนื่องจากมีผลกระทบต่อกลุ่มลูกค้าพอสมควร เพราะปัญหาดังกล่าวทำให้กลุ่มลูกค้าไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้	ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้ง เจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับผลกระทบ เนื่องจากยังไม่เกิดปัญหา	ในเบื้องต้นเป็นเพียงข้อผิดพลาดของโปรแกรมที่ทำให้เข้าถึงข้อมูลส่วนบุคคลไม่ได้ ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามี ภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบ ข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกคามทางไซเบอร์เว็บไซต์ผู้ให้บริการ Web Hosting ต้องรีบแจ้งผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลต้องรีบแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลต่อไป
8	โรงพยาบาลแห่งหนึ่งถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก hacker ทำให้ประวัติของผู้ป่วยไม่สามารถเข้าถึงได้เป็นเวลา 30 ชั่วโมง	ต้องแจ้ง เนื่องจากข้อมูลประวัติของผู้ป่วยเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและสามารถระบุตัวบุคคลได้	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหว ผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิดหรือมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าวรวมถึงข้อมูลสุขภาพด้วย เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุและตรวจสอบข้อมูลเพิ่มเติม

ตัวอย่างที่	เหตุการณ์	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
9	โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าวไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งผู้รับเหมาอาจจะนำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
10	บริษัทแห่งหนึ่งทำการตลาดแบบตรง โดยการส่งข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลแต่ละราย แต่ด้วยความผิดพลาด จึงมีการใส่ที่อยู่ของบุคคลที่รับอีเมลทั้ง 100 คน เข้าไปในช่อง To หรือ Cc ทำให้ผู้รับอีเมลเห็นอีเมลที่มีข้อมูลส่วนบุคคลของบุคคลอื่น	ต้องแจ้ง เนื่องจากเป็นการส่งข้อมูลของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก จึงจำเป็นต้องแจ้งเหตุ แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลในอีเมลดังกล่าวอาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ภายหลังได้	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ อาจขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไปและลักษณะของข้อมูลด้วย หากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด อาจถือว่ามีความเสี่ยงต่ำไม่จำเป็นต้องแจ้งเหตุ

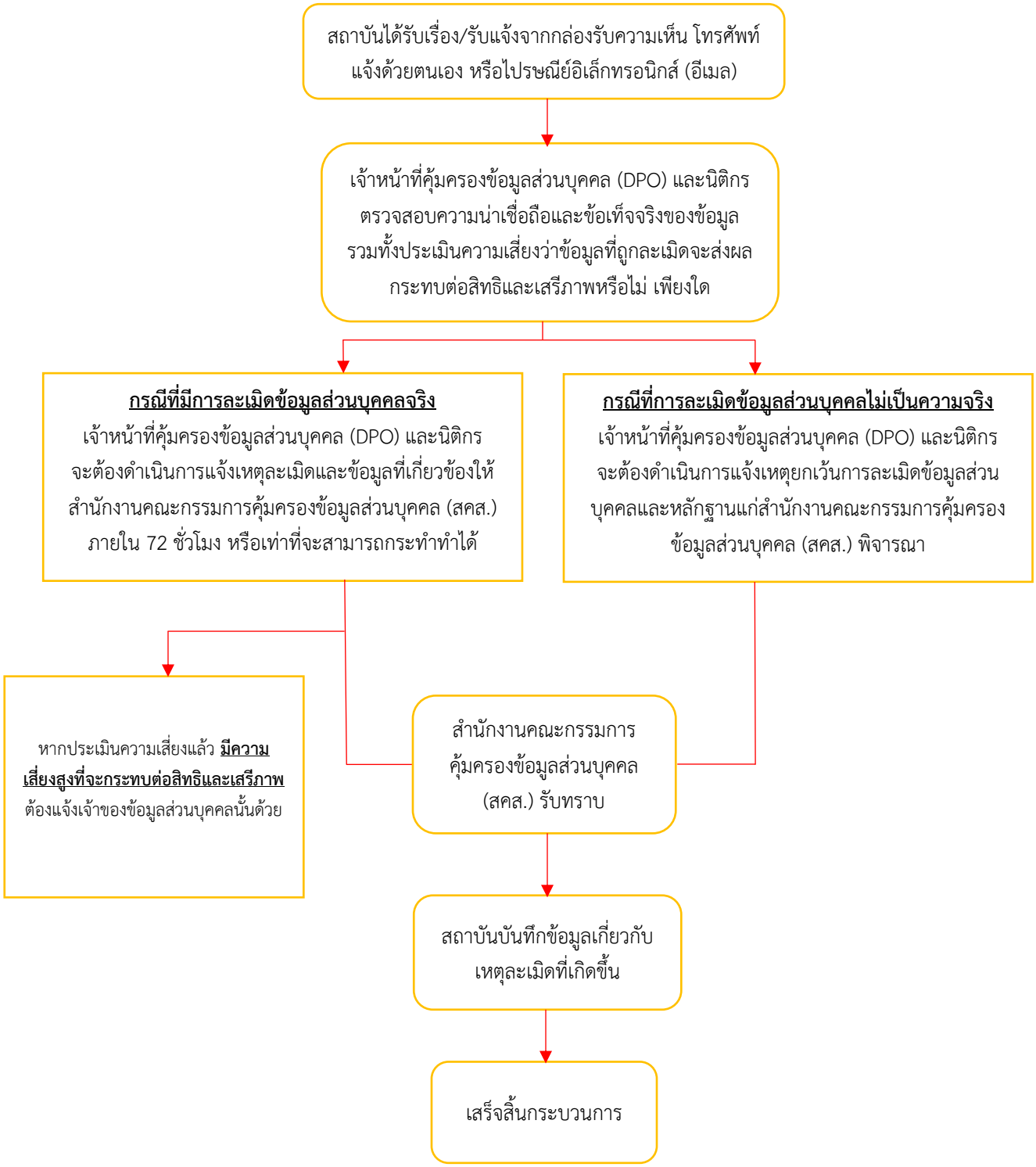
หมายเหตุ :

1. ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลทั้ง 10 ตัวอย่าง ดังกล่าวข้างต้นเป็นเพียงแนวทางในการประเมินความสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณี ๆ ไป

2. เป็นตัวอย่างเหตุการณ์ละเมิดข้อมูลส่วนบุคคลจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

9. แผนผัง (Flowchart) การปฏิบัติงาน

กระบวนการในการปฏิบัติงานกรณีที่มีการละเมิดข้อมูลส่วนบุคคลของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย



หมายเหตุ :

1. แผนผังการปฏิบัติงานนี้ไม่มีค่าใช้จ่าย
2. หน่วยงานที่รับผิดชอบ : นิติกร หน่วยทรัพยากรบุคคล ฝ่ายบริหารงานทั่วไป