แนวปฏิบัติงานของเจ้าหน้าที่
กรณีการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Management)
ของสถาบันคุ้มครองเงินฝาก

---

1. **ชื่องาน :** แนวปฏิบัติงานของเจ้าหน้าที่ กรณีการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Management) ของสถาบันคุ้มครองเงินฝาก
2. **วิธีการขั้นตอนการปฏิบัติงาน :** หน้าที่ 4 – 8
3. **ระยะเวลาที่ใช้ในการปฏิบัติงาน :** ภายใน 72 ชั่วโมงนับแต่เวลาที่ทราบเหตุละเมิด
4. **กฎหมายที่เกี่ยวข้อง :**
    a. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
    b. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

1. การจัดการเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Management)

1.1 กฎหมายที่เกี่ยวข้อง และประเภทเหตุละเมิด

(1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ (4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า ภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยง ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิ และเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้ไปเป็นตามหลักเกณฑ์และวิธีการที่คณะกรรมการ ประกาศกำหนด

(2) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 (ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ) โดยประกาศในราชกิจจานุเบกษา ณ วันที่ 6 ธันวาคม พ.ศ. 2565 ได้กำหนดคำนิยามศัพท์ “การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการ สูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำอันเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด โดยตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดเหตุละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

(2.1) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality breach: C) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(2.2) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity breach: I) ซึ่งมีการเปลี่ยนแปลง แก้ไข ข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจาก ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

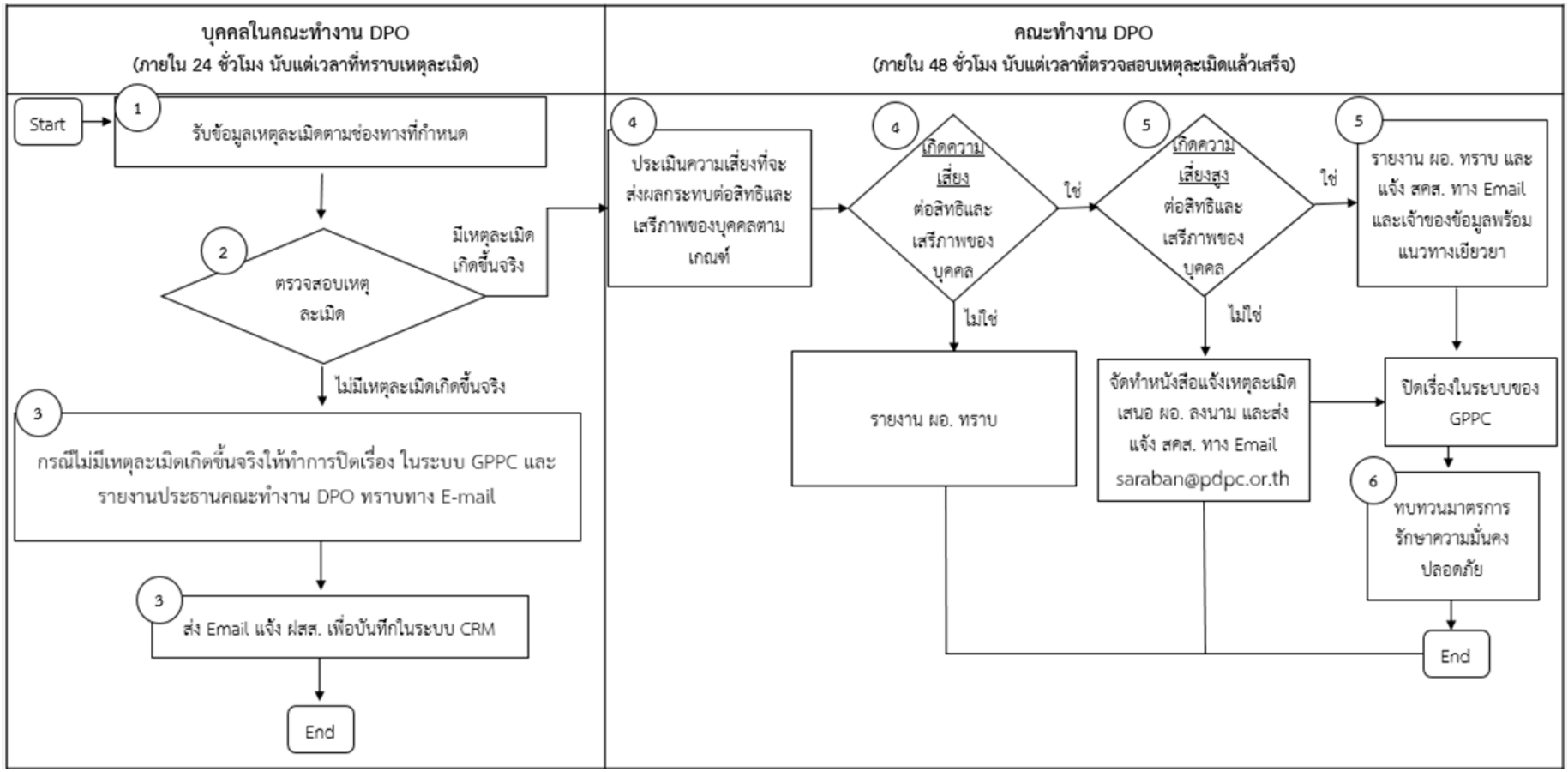
(2.3) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability breach: A) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ ตามปกติ

1.2 ช่องทางการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลของสถาบันคุ้มครองเงินฝาก

ช่องทางการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	**ฝ่ายงานที่ได้รับข้อมูลตามช่องทางแจ้งเหตุการละเมิด**	**การส่งต่อเรื่องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ฝ่ายงานที่เกี่ยวข้อง**
1. แบบฟอร์มแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลในระบบ GPPC ทาง Website สถาบัน 2. Email คณะทำงาน DPO (DPO@dpa.or.th)	ผู้แทนในคณะทำงาน DPO (ฝคส. ฝกม. และ ฝทส.)	• ฝคส. ฝกม. และ ฝทส. ดำเนินการตรวจสอบเหตุละเมิดและความเสี่ยงเบื้องต้น หากพบว่าเหตุละเมิดมีมูลและมีความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล ให้ดำเนินการส่งเรื่องไปยังคณะ DPO เพื่อพิจารณาประเมินความเสี่ยงตามเกณฑ์เพื่อแจ้ง สคส. และ/หรือเจ้าของข้อมูลส่วนบุคคล ต่อไป
3. จดหมาย (เอกสาร) และ Walk-in	ฝสน.	• ฝสน. ส่งจดหมาย (เอกสาร) และข้อมูลที่ได้รับแจ้งจากประชาชน มายัง ฝคส. ฝกม. และ ฝทส. เพื่อดำเนินการตรวจสอบเหตุละเมิดและความเสี่ยงเบื้องต้น หากพบว่าเหตุละเมิดมีมูลและมีความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล ให้ดำเนินการส่งเรื่องไปยังคณะ DPO เพื่อพิจารณาประเมินความเสี่ยงตามเกณฑ์เพื่อแจ้ง สคส. และ/หรือเจ้าของข้อมูลส่วนบุคคล ต่อไป

ช่องทางการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	ฝ่ายงานที่ได้รับข้อมูลตามช่องทางแจ้งเหตุการละเมิด	การส่งต่อเรื่องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ฝ่ายงานที่เกี่ยวข้อง
4. Call Center 1158	ฝสส.	• Call Center แนะนำให้ประชาชน กรอกข้อมูลแบบฟอร์มแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลในระบบ GPPC ทาง Website สถาบัน โดยเข้าไปที่เมนูติดต่อสถาบัน → แจ้งเหตุละเมิดข้อมูลส่วนบุคคล และปิด Case ที่ Call center • ฝคส. ฝกม. และ ฝทส. ได้รับ E-mail แจ้งเหตุละเมิดในระบบ GPPC จากทาง Website สถาบันแล้ว ดำเนินการตรวจสอบเหตุละเมิดและความเสี่ยงเบื้องต้น หากพบว่าเหตุละเมิดมีมูลและมีความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล ให้ดำเนินการส่งเรื่องไปยังคณะ DPO เพื่อพิจารณาประเมินความเสี่ยงตามเกณฑ์เพื่อแจ้ง สคส. และ/หรือ เจ้าของข้อมูลส่วนบุคคลต่อไป

1.3 ขั้นตอนการดำเนินการกรณีมีเหตุการละเมิดข้อมูลส่วนบุคคล (Flow chart)



รายละเอียดขั้นตอนการดำเนินการกรณีมีเหตุการละเมิดข้อมูลส่วนบุคคล

ขั้นตอน	ผู้รับผิดชอบ	แบบฟอร์ม/ ระบบงานที่เกี่ยวข้อง	กฎหมาย/ประกาศและหลักเกณฑ์ที่เกี่ยวข้อง
ดำเนินการให้แล้วเสร็จภายใน 24 ชั่วโมง นับแต่เวลาที่ทราบเหตุละเมิด			
1. รับข้อมูลการแจ้งเหตุละเมิด 1.1 รับข้อมูลการแจ้งเหตุละเมิดผ่านทางระบบ GPPC กรณีที่รับข้อมูลการแจ้งเหตุละเมิดทางเอกสาร/จดหมายและ Email กลาง (dpo@dpa.or.th) ให้นำข้อมูลมาบันทึกในระบบ GPPC เพื่อให้มีข้อมูลอยู่ในฐานข้อมูลเดียวกัน	ฝคส. ฝกม. และ ฝทส.	ระบบ GPPC	-
2. การตรวจสอบเหตุละเมิด 2.1 ตรวจสอบเหตุละเมิดว่ามีเหตุการณ์เกิดขึ้นจริงตามที่ได้รับแจ้ง โดยอาจประสานงานขอข้อมูลกับฝ่ายงานที่เกี่ยวข้อง เพื่อตรวจสอบข้อเท็จจริงของเหตุละเมิดที่ได้รับแจ้ง 2.2 หากระหว่างการตรวจสอบข้อเท็จจริงพบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้แจ้งผู้อำนวยการและประธาน DPO เพื่อพิจารณาสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้	ฝคส. ฝกม. และ ฝทส.	-	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ข้อ 5 (1) และข้อ 5 (2)
3. กรณีไม่มีเหตุละเมิดเกิดขึ้นจริง 3.1 กรณีที่ตรวจสอบแล้วพบว่า ไม่มีเหตุละเมิดเกิดขึ้นจริงตามข้อมูลที่ได้รับแจ้ง ให้ดำเนินการปิดเรื่องในระบบ GPPC 3.2 ส่ง E-mail ถึงประธานคณะ DPO และสำเนาเรียนคณะ DPO และผู้เกี่ยวข้อง เพื่อทราบ 3.3 ส่ง E-mail แจ้ง ฝสส. เพื่อบันทึกข้อมูลที่ประชาชนแจ้งในระบบ CRM เพื่อให้ข้อมูลที่ประชาชนติดต่อเข้ามาอยู่ในระบบเดียวกัน เพื่อ ฝสส. จะดำเนินการในส่วนที่เกี่ยวข้อง	ฝคส. ฝกม. ฝทส. และ ฝสส.	ระบบ GPPC และ E-mail	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ข้อ 5 (1) และข้อ 9

ขั้นตอน	ผู้รับผิดชอบ	แบบฟอร์ม/ ระบบงานที่ เกี่ยวข้อง	กฎหมาย/ประกาศ และหลักเกณฑ์ที่ เกี่ยวข้อง
ดำเนินการให้แล้วเสร็จภายใน 48 ชั่วโมง นับแต่เวลาที่ตรวจสอบเหตุละเมิดแล้วเสร็จ			
4. ประเมินความเสี่ยงที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลตามเกณฑ์การประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล 4.1 กรณีเหตุละเมิดข้อมูลส่วนบุคคลเกิดขึ้นจริงให้ดำเนินการประเมินความเสี่ยงตามเกณฑ์ฯ ในส่วนที่ 1 ท้ายตาราง 4.2 กรณีที่เหตุละเมิดข้อมูลส่วนบุคคลไม่เกิดความเสี่ยง (ไม่เข้าเกณฑ์การประเมินความเสี่ยงข้อ 5 ในส่วนที่ 1 ทั้ง 2 ข้อ) ให้ส่ง E-mail ถึงผู้อำนวยการสถาบันเพื่อทราบ โดยสำเนาเรียนผู้บริหารระดับสูงและคณะ DPO	คณะ DPO	ระบบ GPPC และ E-mail	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ข้อ 4(1) (2) และ (3) และข้อ 12 (7)
5. เหตุละเมิดเกิดความเสี่ยงที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลตามเกณฑ์การประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล 5.1 กรณีที่เหตุละเมิดข้อมูลส่วนบุคคลเกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (เข้าเกณฑ์การประเมินความเสี่ยงข้อ 5 ในส่วนที่ 1 ทั้ง 2 ข้อ) ให้ประเมินความเสี่ยงตามเกณฑ์เข้าเกณฑ์การประเมินความเสี่ยงข้อ 5 ในส่วนที่ 2 จำนวน 7 ข้อท้ายตาราง 5.2 หากการประเมินความเสี่ยงในส่วนที่ 2 ไม่เข้าเกณฑ์ข้อใดข้อหนึ่งใน 7 ข้อ แสดงว่าเหตุละเมิดข้อมูลส่วนบุคคลเกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้ดำเนินการถึงผู้เกี่ยวข้อง (อ้างอิงประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ข้อ 5 (3)) ดังนี้ 1) จัดทำหนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเสนอผู้อำนวยการสถาบัน (ผอ.) ลงนาม (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) ส่งถึง	คณะ DPO / ผอ.	-หนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคลถึง สคส. -หนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคลถึงเจ้าของข้อมูลส่วนบุคคล พร้อมแนวทางการเยียวยา -ตัวอย่างแถลงเหตุการละเมิดข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปของบริษัทเอกชน	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ข้อ 6, 10, 11 และ 12

ขั้นตอน	ผู้รับผิดชอบ	แบบฟอร์ม/ระบบงานที่เกี่ยวข้อง	กฎหมาย/ประกาศและหลักเกณฑ์ที่เกี่ยวข้อง
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยสำเนาเรียนผู้บริหารระดับสูงและคณะ DPO 2) ส่งหนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคลถึง สคส. ที่ saraban@pdpc.or.th 3) ดำเนินการปิดเรื่องในระบบ GPPC 5.3 หากการประเมินความเสี่ยงในส่วนที่ 2 จำนวน 7 ข้อ เข้าข้อใดข้อหนึ่งใน 7 ข้อ ถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล**<u>ที่มีความเสี่ยงสูง</u>** ให้ดำเนินการถึงผู้เกี่ยวข้อง (อ้างอิงประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ข้อ 5 (3) และ (4)) ดังนี้ 1) จัดทำหนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเสนอผู้อำนวยการสถาบัน (ผอ.) ลงนาม (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) ส่งถึง สคส. และเจ้าของข้อมูลส่วนบุคคลพร้อมแนวทางการเยียวยา โดยสำเนาเรียนผู้บริหารระดับสูงและคณะ DPO 2) ส่งหนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคลถึง สคส. ที่ saraban@pdpc.or.th 3) ส่งหนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคลถึงเจ้าของข้อมูลส่วนบุคคลพร้อมแนวทางการเยียวยาทราบ หากไม่สามารถดำเนินการแจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้เนื่องจากไม่มีวิธีการติดต่อหรือโดยเหตุจำเป็นอื่นใด อาจแจ้งเหตุละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้ โดยการแจ้งเหตุละเมิดแก่			

ขั้นตอน	ผู้รับผิดชอบ	แบบฟอร์ม/ระบบงานที่เกี่ยวข้อง	กฎหมาย/ประกาศและหลักเกณฑ์ที่เกี่ยวข้อง
เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล 4) ดำเนินการปิดเรื่องในระบบ GPPC			
6. การทบทวนมาตรการรักษาความมั่นคงปลอดภัย 6.1 คณะ DPO ประชุมหารือร่วมกับฝ่ายงานที่เกี่ยวข้อง (ถ้ามี) เพื่อดำเนินการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เพียงพอที่จะป้องกันเหตุละเมิดข้อมูลส่วนบุคคลที่อาจเกิดขึ้น 6.2 รายงานผู้อำนวยการสถาบันและผู้บริหารระดับสูงทราบผลการทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัย เพื่อป้องกันเหตุการละเมิดข้อมูลส่วนบุคคลที่อาจเกิดขึ้น	คณะ DPO/ฝ่ายงานที่เกี่ยวข้อง (ถ้ามี)	-	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ข้อ 5 (5)