เอกสารบันทึกแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Incident Report)

แนวปฏิบัติการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

บทที่ ๑ บททั่วไป

- ❖ แนวปฏิบัตินี้ใช้บังคับเป็นการทั่วไปกับส่วนงานและพนักงานทุกระดับ
- ❖ แนวปฏิบัตินี้ไม่ถือเป็นส่วนหนึ่งของสัญญาจ้าง แต่เป็นการกำหนดแนวทางการทำงานที่พนักงานต้องปฏิบัติ การไม่ดำเนินการตามแนวปฏิบัตินี้จะมีผลทางวินัยพนักงาน
- ❖ แนวปฏิบัตินี้จะได้รับการทบทวนและปรับปรุงอยู่ตลอด ซึ่งจะได้แจ้งให้พนักงานทุกคนทราบทุกครั้ง

๑. **[ขอบเขตและความหมาย]** แนวปฏิบัตินี้วางกรอบแนวทางในการดำเนินการที่สำคัญสำหรับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (**"สพฐ."**) โดยสอดคล้องและเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (**"พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ฯ"**) ทั้งนี้รายละเอียด แนวปฏิบัติ และความหมายต่าง ๆ ให้ใช้อ้างอิงตาม TDPG ๓.๐ Extension (Thailand Data Protection Guidelines ๓.๐ Extension) และแนวปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

๒. **[ขั้นตอนการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล]** พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ (มาตรา ๓๗ (๔)) กำหนดให้เมื่อบุคลากรของ สพฐ. ทราบถึงการละเมิดข้อมูลส่วนบุคคลต้องแจ้งเหตุดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่เหตุละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดข้อมูลส่วนบุคคลที่**มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล (High Risk)** ให้แจ้งเหตุละเมิดนั้นให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมแนวทางการเยียวยาโดยไม่ช้า ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๓. **[การละเมิดข้อมูลส่วนบุคคล]** การละเมิดข้อมูลส่วนบุคคล หมายความว่า การละเมิดต่อความปลอดภัย (Breach of security) ที่นำไปสู่การทำลาย การทำให้สูญหาย การแก้ไข การเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึงข้อมูลส่วนบุคคล ที่เกิดขึ้นโดยตั้งใจและไม่ตั้งใจ[๑]

[๑] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ไม่ได้ระบุคำนิยามของ "การละเมิดข้อมูลส่วนบุคคล" ไว้ จึงนำคำนิยาม "personal data breach" ตาม Article ๔ ของกฎหมาย GDPR ของสหภาพยุโรปที่มีความใกล้เคียงกับกฎหมายของประเทศไทยมาใช้ ซึ่งให้คำนิยามว่า "a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

ตัวอย่างของการละเมิดข้อมูลส่วนบุคคล ได้แก่

- อนุมัติสิทธิการเข้าถึงข้อมูลส่วนบุคคลแก่บุคคลที่สามที่ไม่สมควรได้รับอนุญาต
- การส่งข้อมูลส่วนบุคคลไปยังผู้รับที่ไม่มีหน้าที่หรือไม่มีความรับผิดชอบในเรื่องนั้น
- อุปกรณ์คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคลสูญหายหรือถูกขโมย
- การแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- เหตุการณ์ใด ๆ ข้างต้นเกิดขึ้นกับบุคคลที่สามซึ่งประมวลผลข้อมูลส่วนบุคคลให้กับ สพฐ.

๔. [กระบวนการในการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล]

เมื่อทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคล สพฐ. จะต้องดำเนินการดังต่อไปนี้

๔.๑ ให้ผู้ปฏิบัติงานซึ่งเป็นผู้รับทราบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลจะต้องรายงานต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) **ทันที** เพื่อร่วมกันพิจารณากำหนดแนวทาง และวิธีการระงับหรือบรรเทาผลเสียหายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้นโดยสามารถแจ้งได้ทั้งช่องทางปกติ และ ช่องทางออนไลน์ โดยให้แจ้งเหตุโดยใช้ <u>เอกสารแนบที่ ๒</u> ผ่านช่องทางดังนี้

๔.๑.๑ ช่องทางที่ ๑ ผ่านอีเมล กระบวนการ คือ ส่งไปที่อีเมล [*]

๔.๑.๒ ช่องทางที่ ๒ ผ่าน [*] กระบวนการ คือ

๔.๑.๓ ช่องทางที่ ๓ ผ่าน [*] กระบวนการ คือ

๔.๒ หลังจากได้รับแจ้งตาม ๔.๑ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสอบสวนและควบคุมการละเมิดข้อมูลส่วนบุคคล รวมถึง กู้คืนข้อมูลส่วนบุคคลที่ถูกละเมิด และ/หรือ บริการที่ได้รับผลกระทบ

๔.๓ หลังจากได้รับแจ้งตาม ๔.๑ และ ปฏิบัติตาม ๔.๒ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแจ้งคณะกรรมการบริหารถึงเหตุดังกล่าว และร่วมกับฝ่ายเทคโนโลยี หรือฝ่ายประเมินความเสี่ยงของ สพฐ. ในการประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (โดยใช้หลักเกณฑ์การประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ในบทที่ ๒) ประเมินระดับของความเสี่ยง

๔.๓.๑ ในกรณีที่ผลประเมินชี้ว่า**มีความเสี่ยง**ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนั้นต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๔.๓.๒ ในกรณีที่ผลประเมินชี้ว่า**มีความเสี่ยงสูง (High Risk)** ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล **พร้อมกับแนวทางเยียวยา** ให้ทั้งเจ้าของข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ

๔.๔ ระยะเวลาดำเนินงานในข้อ ๔.๑ และ ๔.๒ ต้องดำเนินการภายใน ๗๒ ชั่วโมง

๔.๕ การแจ้งเหตุตาม ๔.๑ และ ๔.๒ ต้องแจ้งเตือนไปยังหน่วยงานที่กำกับดูแลและเจ้าของข้อมูลที่ได้รับผลกระทบ ในแต่ละกรณีต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

๔.๕.๑ <u>การแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (โดยใช้แบบฟอร์มตามเอกสารแนบที่ ๑)</u>

๔.๕.๑.๑ คำอธิบายลักษณะของเหตุการณ์เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล ประเภทและปริมาณข้อมูลส่วนบุคคลที่เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล จำนวนเจ้าของข้อมูลส่วนบุคคลและผลกระทบที่เกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล

๔.๕.๑.๒ ชื่อ-สกุล และข้อมูลสำหรับการติดต่อของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และผู้ปฏิบัติงานที่เกี่ยวข้อง เพื่อการประสานงานและติดต่อสอบถามข้อมูลเพิ่มเติม

๔.๕.๑.๓ ลักษณะของความเสียหายที่เกิดหรืออาจจะเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคลนั้น

๔.๕.๒ <u>การแจ้งเจ้าของข้อมูลส่วนบุคคล (ในกรณีที่**เหตุการละเมิดมีความเสี่ยงสูง (High Risk)** ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล จะต้องแจ้งแนวทางและวิธีการระงับหรือบรรเทาผลเสียหายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้นด้วย)</u>

๔.๕.๒.๑ คำอธิบายลักษณะของเหตุการณ์เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล ประเภทและปริมาณข้อมูลส่วนบุคคลที่เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล รวมทั้งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

๔.๕.๒.๒ ชื่อ-สกุล รวมทั้งข้อมูลสำหรับการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและผู้ปฏิบัติงานที่เกี่ยวข้อง

๔.๕.๒.๓ ลักษณะของความเสียหายที่เกิดหรืออาจจะเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล รวมทั้งแนวทางและวิธีการระงับหรือบรรเทาผลเสียหายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้น

๔.๕.๒.๔ คำวินิจฉัยหรือข้อสั่งการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (ถ้ามี)

๔.๖ เมื่อปัญหาการละเมิดข้อมูลส่วนบุคคลได้รับการแก้ไขเรียบร้อยแล้ว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึกรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น รวมทั้งสรุปผลวิเคราะห์เหตุการละเมิด สิ่งที่ได้เรียนรู้และแนวทางการแก้ไขเหตุการณ์ดังกล่าว เพื่อทำแนวทางป้องกันไม่ให้เกิดความเสียหายที่เพิ่มมากขึ้น รวมไปถึงการระบุหรือส่งมอบหน้าที่ต่าง ๆ ให้กับผู้รับผิดชอบเพื่อดำเนินการตามแผนต่าง ๆ ตามที่กำหนดไว้

บทที่ ๒ หลักเกณฑ์การประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

๑. หลักการประเมินความเสี่ยง

๑.๑ เนื่องจากลักษณะของเหตุแห่งการละเมิดข้อมูลส่วนบุคคลอาจเกิดขึ้นโดยมีลักษณะเฉพาะและมีความหลากหลาย จึงจำเป็นต้องทำการประเมินความเสี่ยงเป็นรายกรณี

๑.๒ ต้องพิจารณาประเมินความเสี่ยงจากระดับความรุนแรงของเหตุ (Severity of Incident) ร่วมกับการประเมินผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคลด้วย เนื่องจากการละเมิดข้อมูลส่วนบุคคลที่สำคัญของเจ้าของข้อมูลส่วนบุคคลจำนวนน้อยอาจมีความเสี่ยงหรือผลกระทบสูงกว่าการละเมิดข้อมูลส่วนบุคคลที่ไม่สำคัญของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก โดยใช้เกณฑ์การประเมินความเสี่ยงตามที่กำหนดไว้ในข้อ ๒

๒. เกณฑ์การประเมินความเสี่ยงจากระดับความรุนแรงของเหตุ (Severity of Incident)

๒.๑ ระดับต่ำ: สำหรับกรณีดังต่อไปนี้

๒.๑.๑ เป็นการละเมิดข้อมูลส่วนบุคคลทั่วไป (เช่น ชื่อ-นามสกุล)

- เป็นการละเมิดข้อมูลส่วนบุคคลที่มีระบบป้องกันการเข้าถึงข้อมูล (Security) ในระดับดี เช่น ข้อมูลส่วนบุคคลที่เข้ารหัสไว้อย่างดี
- เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นพนักงานหรือลูกจ้างหรือผู้รับบริการ ของ สพฐ. ที่มีจำนวนน้อย

๒.๑.๒ ระดับปานกลาง: สำหรับกรณีดังต่อไปนี้

- เป็นการละเมิดข้อมูลส่วนบุคคลที่เป็นกลุ่มของข้อมูล เช่น ชุดข้อมูลที่ประกอบด้วย ชื่อ-นามสกุล วันเกิด ที่อยู่ ฯลฯ
- เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นพนักงานหรือลูกจ้างหรือผู้รับบริการ ของ สพฐ. หลายราย

๒.๑.๓ ระดับสูง: สำหรับกรณีดังต่อไปนี้

- เป็นการละเมิดข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น ข้อมูลด้านสุขภาพ
- เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นสมาชิกหรือเป็นพนักงานหรือลูกจ้างหรือผู้รับบริการทั้งหมดของ สพฐ.
- เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นบุคคลที่มีชื่อเสียง
- เป็นการละเมิดต่อข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่มีการรายงานข่าวเหตุการณ์ออกสู่สาธารณะโดยสื่อมวลชน

สำหรับการพิจารณาประเมินความเสี่ยงต้องประเมินจากปริมาณข้อมูลส่วนบุคคลที่ถูกละเมิดกับผลกระทบที่คาดว่าจะเกิดขึ้น ดังต่อไปนี้

ปริมาณข้อมูลส่วนบุคคลที่ถูกละเมิด X ผลกระทบที่คาดว่าจะเกิดขึ้น

ปริมาณข้อมูลส่วนบุคคลที่ถูกละเมิด

หัวข้อ	ระดับความเสี่ยง		
	ต่ำ	ปานกลาง	สูง
ปริมาณข้อมูลที่ถูกละเมิด	ข้อมูลส่วนบุคคลที่ถูกละเมิดมีปริมาณน้อยและมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไว้เป็นอย่างดีทำให้ยากที่จะเข้าถึงได้	ข้อมูลส่วนบุคคลที่ถูกละเมิดมีปริมาณน้อยและมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไว้บางส่วน ทำให้มีความเป็นไปได้ที่จะเข้าถึงได้	ข้อมูลส่วนบุคคลที่ถูกละเมิดมีปริมาณมากและไม่มีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทำให้สามารถเข้าถึงได้โดยง่าย

ผลกระทบที่คาดว่าจะเกิดขึ้น

หัวข้อ	ระดับความเสี่ยง		
	ต่ำ	ปานกลาง	สูง
ผลกระทบที่คาดว่าจะเกิดขึ้น	ข้อมูลส่วนบุคคลมีการเปิดเผยเป็นการทั่วไปและไม่มีผลกระทบต่อความปลอดภัยหรือชื่อเสียงของเจ้าของข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่มีลักษณะพิเศษเฉพาะ เช่น ข้อมูลการเงิน หรือข้อมูลที่โดยปกติจะต้องเก็บเป็นความลับ ซึ่งมีแนวโน้มส่งผลกระทบต่อความปลอดภัยหรือชื่อเสียงของเจ้าของข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่มีลักษณะพิเศษเฉพาะ เช่น ข้อมูลการเงิน ข้อมูลสุขภาพจิตหรือข้อมูลที่โดยปกติจะต้องเก็บเป็นความลับ ซึ่งมีผลกระทบต่อความปลอดภัยหรือชื่อเสียงของเจ้าของข้อมูลส่วนบุคคลอย่างร้ายแรง

ตารางแสดงระดับความเสี่ยง

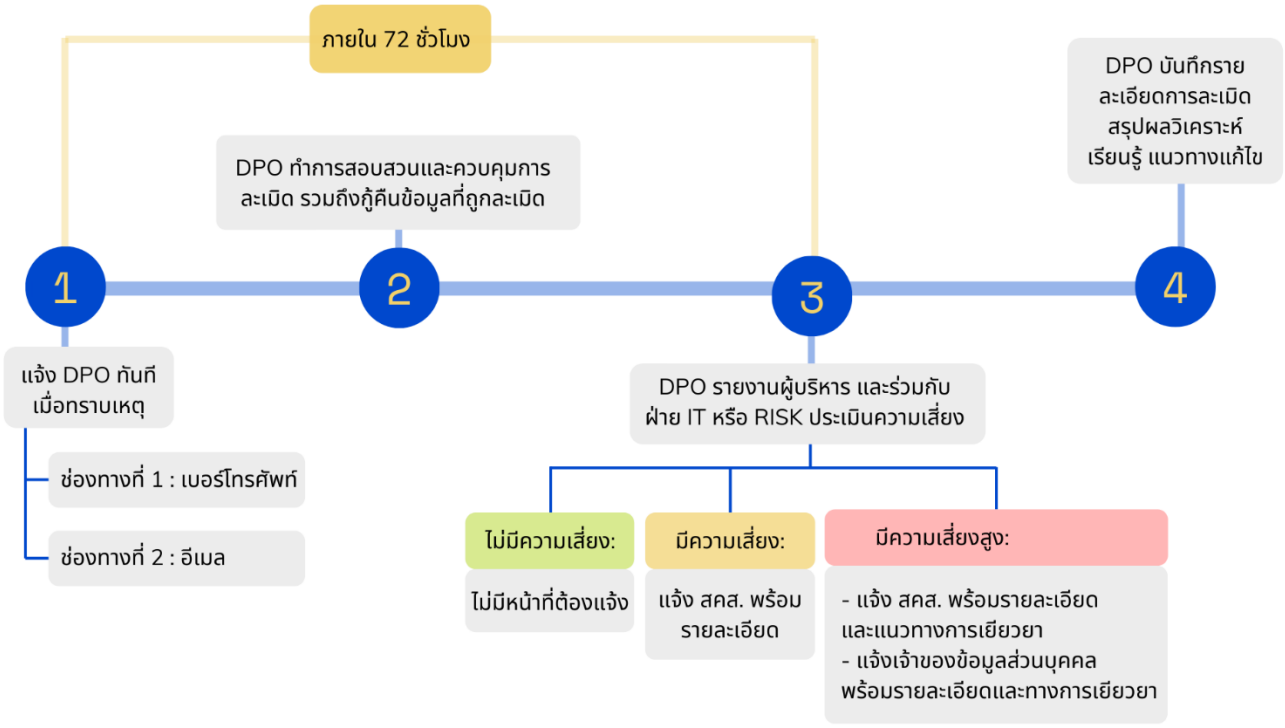
ปริมาณ ข้อมูลส่วนบุคคลที่ถูกละเมิด				
มาก	ปานกลาง	สูง	สูง	
ปานกลาง	ต่ำ	ปานกลาง	สูง	
น้อย	ต่ำ	ต่ำ	ปานกลาง	
	ต่ำ	ปานกลาง	สูง	ผลกระทบ ที่คาดว่าจะเกิดขึ้น

- **ปัจจัยเสริมประกอบการพิจารณาระดับความเสี่ยง**

การพิจารณาประเมินความเสี่ยงตามข้อ ๒ ควรพิจารณาปัจจัยเสริมที่มีผลต่อระดับความเสี่ยง ดังต่อไปนี้

- ระดับความยากในการบ่งชี้ตัวตนของเจ้าของข้อมูลส่วนบุคคล : แม้ว่าข้อมูลส่วนบุคคลจะเป็นข้อมูลนิรนาม แต่ถ้าสามารถบ่งชี้ตัวตนขอเจ้าของข้อมูลส่วนบุคคลได้ ก็อาจมีความเสี่ยงด้วยเช่นกัน เช่น ข้อมูลตำแหน่งของบุคคลในที่ทำงานซึ่งฝ่ายบริหารทรัพยากรบุคคลสามารถบ่งชี้ตัวตนได้
- ลักษณะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ : ถ้าบุคคลที่ได้รับผลกระทบเป็นกลุ่มที่อ่อนแอ (Vulnerable) เช่น ผู้ป่วยโรคติดต่อร้ายแรง หรือผู้ป่วยที่เป็นคนพิการ เป็นต้น จะถือว่ามีความเสี่ยงสูง
- ลักษณะของผู้ควบคุมข้อมูลส่วนบุคคล : ถ้าผู้ควบคุมข้อมูลส่วนบุคคลเป็นหน่วยงานที่มีหน้าที่เก็บข้อมูลของบุคคลที่มีปัญหาที่อ่อนไหว เช่น ปัญหาทางสุขภาพกายหรือสุขภาพจิต การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีความเสี่ยงมากกว่าข้อมูลของหน่วยงานทั่วไป
- การละเมิดข้อมูลส่วนบุคคลที่เจาะจงเป้าหมายเฉพาะ : การละเมิดข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เฉพาะเจาะจง เช่น การต้องการเข้าถึงข้อมูลส่วนบุคคลที่เป็นความลับที่สุดจะมีความเสี่ยงสูงกว่าการละเมิดข้อมูลส่วนบุคคลโดยไม่ได้ตั้งใจ

บทที่ ๓ สรุปขั้นตอนการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล



เอกสารแนบที่ ๑

เอกสารบันทึกแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Incident Report) สำหรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

วันที่ [*]

เรื่อง แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

เรียน สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

สิ่งที่แนบมาด้วย แบบบันทึกการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวข้อง

เมื่อวันที่ [*] [ชื่อผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล] พบว่า [ลักษณะเหตุละเมิด เช่น ระบบเทคโนโลยีสารสนเทศของ [*]] ได้ถูกผู้ไม่ประสงค์ดี [*รูปแบบการโจมตีด้านความปลอดภัยทางไซเบอร์*] ซึ่งส่งผลให้มีการเข้าถึงข้อมูลภายในระบบเทคโนโลยีสารสนเทศของ [*] ซึ่งประกอบไปด้วยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ [*ระบุประเภทของเจ้าของข้อมูลส่วนบุคคล*] โดยมิชอบด้วยกฎหมาย และโดยไม่ได้รับอนุญาต

ทั้งนี้ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งจากการตรวจสอบเบื้องต้น [*] พบว่าอาจมีข้อมูลส่วนบุคคลที่ถูกเข้าถึงโดยไม่ชอบด้วยกฎหมายและไม่ได้รับอนุญาต รายละเอียดดังต่อไปนี้

๑. รายละเอียดของเหตุละเมิดข้อมูลส่วนบุคคล

รายละเอียดของเหตุการณ์	
วันและเวลาการแจ้งเหตุละเมิด * วัน/เดือน/ปี เวลา [*] น.	
วันและเวลาที่พบเหตุละเมิด * วัน/เดือน/ปี เวลา [*] น.	
วันและเวลาที่เริ่มต้นของเหตุละเมิด * วัน/เดือน/ปี เวลา [*] น.	
ลักษณะเหตุละเมิดข้อมูล * เช่น การโจรกรรมข้อมูลส่วนบุคคล / การเข้าถึงข้อมูลโดยบุคคลไม่ได้รับอนุญาต / การจัดส่งข้อมูลต่อบุคคลอื่นที่ไม่มีสิทธิรับข้อมูล / อุปกรณ์	

รายละเอียดของเหตุการณ์	
อิเล็กทรอนิกส์ที่บรรจุข้อมูลส่วนบุคคลสูญหาย / การแก้ไขข้อมูลโดยไม่ได้รับความยินยอม	
สถานที่เกิดเหตุละเมิดข้อมูล * เช่น ภายในฝ่ายงาน / หน้าสำนักงาน / ระบบ เป็นต้น	
ประเภทของเจ้าของข้อมูล * อ้างอิงตามแบบบันทึกการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมดังกล่าว	
ประมาณการจำนวนผู้เสียหาย * เช่น ๑ คน ๑๐ คน ๑๐๐ คน / อย่างน้อย ๕๐ คน / ไม่สามารถประมาณการยอดได้	
ประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด * ระบุรายการข้อมูลเป็นประเภทหรือในกรณีที่ยังไม่สามารถระบุได้ในขณะที่แจ้งให้ระบุว่า “อยู่ระหว่างการพิจารณาและจะแจ้งให้ สคส. ต่อไป”	
การพบเหตุละเมิด * เช่น ได้รับแจ้งจากเจ้าของข้อมูลถึงการละเมิด / พบการเข้าถึงระบบใน Log File ว่าถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ / ทำอุปกรณ์สูญหาย	
รายละเอียดโดยสรุปของเหตุละเมิด * เพื่อขยายความลักษณะเหตุละเมิด เพื่อให้เข้าใจเนื้อหาของการละเมิดข้อมูลส่วนบุคคล โดยอธิบายเนื้อหาเท่าที่สามารถระบุได้ รวมไปถึงคำขยายความประเภทข้อมูลที่ทราบโดยละเอียด	
รายละเอียดระบบเทคโนโลยีสารสนเทศและอุปกรณ์อิเล็กทรอนิกส์ที่เกี่ยวข้อง (ถ้ามี) * เช่น ระบบ / มือถือส่วนบุคคล รวมถึงอธิบายถึงการรักษาความปลอดภัยของข้อมูลในระบบดังกล่าว โดยสรุป เช่น มีการเข้ารหัสข้อมูล หรือมีการสำรองไฟล์ไว้ในระบบ	

๒. ผลกระทบที่อาจเกิดขึ้นจากเหตุละเมิดส่วนบุคคล

ความเสี่ยง อธิบายหัวข้อความเสี่ยงต่อข้อมูลส่วนบุคคล * เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	**อธิบายความเสี่ยงและผลกระทบต่อข้อมูลส่วนบุคคล** อธิบายรายละเอียดผลกระทบที่อาจเกิดขึ้นต่อข้อมูลส่วนบุคคล * เช่น ผู้พบเห็นอาจสามารถเข้าถึงข้อมูลดังกล่าวและสามารถใช้ข้อมูลดังกล่าวโดยมิชอบ	**ประมาณการความเสี่ยงต่อเจ้าของข้อมูล** * สูง / กลาง / ต่ำ / ไม่มีความเสี่ยง / ไม่สามารถประเมินได้
ความเสี่ยงที่ (๑)		
ความเสี่ยงที่ (๒)		
ความเสี่ยงที่ (๓)		

๓. มาตรการในการรับมือกับเหตุละเมิดที่เกิดขึ้นเพื่อลดผลกระทบและการดำเนินการในการเยียวยา

ความเสี่ยง	**มาตรการในการรับมือกับความเสี่ยงที่เกิดจากเหตุเหตุละเมิด** * อธิบายรายละเอียดมาตรการที่จะดำเนินการกับความเสี่ยงแต่ละรูปแบบที่เกิดขึ้น	**รายละเอียดการกระทำที่ได้ดำเนินการเพื่อเยียวยาการละเมิด** * เช่น ดำเนินการเปลี่ยนรหัสความปลอดภัย ดำเนินการค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น
ความเสี่ยงที่ (๑)		
ความเสี่ยงที่ (๒)		
ความเสี่ยงที่ (๓)		

๔. ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๕. ข้อมูลติดต่อขององค์กร

ชื่อองค์กร	
ที่อยู่ขององค์กร	
ชื่อ-สกุล ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	
ที่อยู่ที่ติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	โทรศัพท์: อีเมล:
ชื่อ-สกุล ของเจ้าหน้าที่ประสานงาน	
ที่อยู่ที่ติดต่อของเจ้าหน้าที่ประสานงาน	โทรศัพท์: อีเมล:

จึงเรียนมาเพื่อทราบ และโปรดดำเนินการตามที่เห็นสมควร ในกรณีที่สำนักงานฯ มีข้อสงสัยหรือต้องการข้อมูลเกี่ยวกับเหตุละเมิดดังกล่าวเพิ่มเติม สำนักงานฯ สามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ เจ้าหน้าที่ประสานงาน ของ [*] ได้ตามข้อมูลข้างต้น

ขอแสดงความนับถือ

_____

(*ชื่อ-นามสกุล*)

(*ตำแหน่ง*)

สิ่งที่แนบมาด้วย : **แบบบันทึกการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวข้อง**

เอกสารแนบที่ ๒

แบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ดังนั้น เพื่อให้ทางเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถดำเนินการตามบทบัญญัติดังกล่าว โปรดระบุรายละเอียดเหตุละเมิดข้อมูลส่วนบุคคลเท่าที่ท่านสามารถระบุได้ตามแบบฟอร์มต่อไปนี้ ทั้งนี้ ภายในระยะเวลายี่สิบสี่ชั่วโมงนับแต่ทราบเหตุละเมิดดังกล่าว

- ให้ผู้แจ้งเหตุส่งเอกสารหลักฐานเท่าที่มีต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อประกอบการพิจารณาความเสี่ยงของเหตุละเมิดดังกล่าวกรณีที่ประเมินว่าไม่มีความเสี่ยง ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลบันทึกเหตุละเมิดไว้ และเสนอแนวทางแก้ไขไม่ให้มีเหตุการณ์เช่นเดียวกันนี้เกิดขึ้นอีกในอนาคต
- กรณีที่ประเมินว่ามีความเสี่ยง ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเสนอเรื่องแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้แล้วเสร็จภายในเจ็ดสิบสองชั่วโมง
- กรณีที่ประเมินว่ามีความเสี่ยงสูง ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเสนอแนวทางการแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคลเพื่ออนุมัติโดยทันที

๑. ข้อมูลของผู้แจ้งเหตุ

ชื่อ-สกุล	
ที่อยู่ที่ติดต่อ * โทรศัพท์ * อีเมล	
หน่วยงานที่สังกัด * ส่วนงานหรือฝ่ายงาน	

๒. รายละเอียดของเหตุละเมิดข้อมูลส่วนบุคคล

รายละเอียดของเหตุการณ์	
วันและเวลาการแจ้งเหตุละเมิด * DD/MM/YY เวลา [*] น.	
วันและเวลาที่พบเหตุละเมิด * DD/MM/YY เวลา [*] น.	
วันและเวลาที่เริ่มต้นของเหตุละเมิด * DD/MM/YY เวลา [*] น.	
ลักษณะเหตุละเมิดข้อมูล * เช่น การโจรกรรมข้อมูลส่วนบุคคล / การเข้าถึงข้อมูลโดยบุคคลไม่ได้รับอนุญาต / การจัดส่งข้อมูลต่อบุคคลอื่นที่ไม่มีสิทธิรับข้อมูล / อุปกรณ์อิเล็กทรอนิกส์ที่บรรจุข้อมูลส่วนบุคคลสูญหาย / การแก้ไขข้อมูลโดยไม่ได้รับความยินยอม	
สถานที่เกิดเหตุละเมิดข้อมูล * เช่น ภายในฝ่ายงาน / หน้าสำนักงาน / ระบบ Mango เป็นต้น	
ประเภทของเจ้าของข้อมูล * อ้างอิงตาม ROP	
ประมาณการจำนวนผู้เสียหาย * เช่น ๑ คน ๑๐ คน ๑๐๐ คน / อย่างน้อย ๕๐ คน / ไม่สามารถประมาณการยอดได้	
ประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด * ระบุรายการข้อมูลเป็น field หรือไม่สามารถระบุได้ในขณะที่แจ้ง	
คุณทราบเหตุละเมิดได้อย่างไร * เช่น ได้รับแจ้งจากเจ้าของข้อมูลถึงการละเมิด / พบการเข้าถึงระบบใน Log File ว่าถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ / ทำอุปกรณ์สูญหาย	

รายละเอียดโดยสรุปของเหตุละเมิด * เพื่อขยายความลักษณะเหตุละเมิด เพื่อให้เข้าใจเนื้อหาของการละเมิดข้อมูลส่วนบุคคล โดยอธิบายเนื้อหาเท่าที่สามารถระบุได้ รวมไปถึงคำขยายความประเภทข้อมูลที่ทราบโดยละเอียด	
รายละเอียดระบบเทคโนโลยีสารสนเทศและอุปกรณ์อิเล็กทรอนิกส์ที่เกี่ยวข้อง (ถ้ามี) * เช่น ระบบ Mango / มือถือส่วนบุคคล รวมถึงอธิบายถึงการรักษาความปลอดภัยของข้อมูลในระบบดังกล่าวโดยสรุป เช่น มีการเข้ารหัสข้อมูล หรือมีการสำรองไฟล์ไว้ในระบบ	
อธิบายความเสี่ยงต่อข้อมูลส่วนบุคคล * เช่น ผู้พบเห็นอาจสามารถเข้าถึงข้อมูลดังกล่าว และสามารถใช้ข้อมูลดังกล่าวโดยมิชอบ	
ประมาณการความเสี่ยงต่อเจ้าของข้อมูล * สูง / กลาง / ต่ำ / ไม่มีความเสี่ยง / ไม่สามารถประเมินได้	
รายละเอียดการกระทำที่ได้ดำเนินการเพื่อเยียวยาการละเมิด * เช่น ดำเนินการเปลี่ยนรหัสความปลอดภัย ดำเนินการค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น	
ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	