แนวปฏิบัติในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

แนวปฏิบัตินี้ ได้แบ่งหัวข้อต่าง ๆ ออกเป็นจำนวน 3 บท ได้แก่

บทที่ 1: บททั่วไป

บทที่ 2: หลักเกณฑ์การประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

บทที่ 3: สรุปขั้นตอนการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล

1. บทที่ 1: บททั่วไป

1.1. วัตถุประสงค์ของนโยบาย

1.1.1. เพื่อมีผลบังคับใช้ภายในบริษัท วานา นาวา จำกัด (บริษัท) โดยครอบคลุมถึงการดำเนินงานในธุรกิจที่บริษัทฯ ดูแลรับผิดชอบ อันมีสวนน้ำ วานา นาวา วอเตอร์ จังเกิ้ล เป็นอาทิ

1.1.2. เพื่อใช้บังคับเป็นการทั่วไปกับส่วนงานและพนักงานทุกระดับ

1.1.3. นโยบายนี้ไม่ถือเป็นส่วนหนึ่งของสัญญาจ้าง แต่เป็นการกำหนดแนวทางการทำงานที่พนักงานต้องปฏิบัติ การไม่ดำเนินการตามนโยบายนี้จะมีผลทางวินัยพนักงาน

1.1.4. นโยบายนี้จะได้รับการทบทวนและปรับปรุงเป็นประจำ ซึ่งจะได้แจ้งให้พนักงานทุกคนทราบทุกครั้ง

1.2. ขอบข่าย

1.2.1. นโยบายนี้วางกรอบหลักการและแนวทางในการดำเนินการที่สำคัญบการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล โดยสอดคล้องและเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.2.2. การปฏิบัติตามแนวทางนี้ รวมถึงรายละเอียด แนวปฏิบัติ และความหมายต่างๆ ให้ใช้อ้างอิงตาม TDPG3.0 (Thailand Data Protection Guidelines 3.0) และแนวปฏิบัติอื่นๆที่เกี่ยวข้อง

1.3. หน้าที่และความรับผิดชอบ

1.3.1. ในการปฏิบัติตามขั้นตอนการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 37 (4)) กำหนดให้เมื่อบุคลากรของ บริษัท วานา นาวา จำกัด (“วานา นาวา” หรือ “บริษัท”) ทราบถึงการละเมิดข้อมูลส่วนบุคคล ต้องแจ้งเหตุดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่เหตุละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล (High Risk) ให้แจ้งเหตุละเมิดนั้นให้เจ้าของ

ข้อมูลส่วนบุคคลทราบ พร้อมแนวทางการเยียวยาโดยไม่ช้า ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

1.4. **นิยามศัพท์**

1.4.1. การละเมิดข้อมูลส่วนบุคคล หมายความว่า การละเมิดต่อความปลอดภัย (Breach of security) ที่นำไปสู่การทำลาย การทำให้สูญหาย การแก้ไข การเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึงข้อมูลส่วนบุคคล ที่เกิดขึ้นโดยตั้งใจและไม่ตั้งใจ[1]

1.4.2. ตัวอย่างของการละเมิดข้อมูลส่วนบุคคล ได้แก่

1.4.2.1. อนุมัติสิทธิการเข้าถึงข้อมูลส่วนบุคคลแก่บุคคลที่สามที่ไม่สมควรได้รับอนุญาต

1.4.2.2. การส่งข้อมูลส่วนบุคคลไปยังผู้รับที่ไม่มีหน้าที่หรือไม่มีความรับผิดชอบในเรื่องนั้น

1.4.2.3. อุปกรณ์คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคลสูญหายหรือถูกขโมย

1.4.2.4. การแก้ไขข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

1.4.2.5. เหตุการณ์ใด ๆ ข้างต้นเกิดขึ้นกับบุคคลที่สามซึ่งประมวลผลข้อมูลส่วนบุคคลให้กับ บริษัท

1.5. **ขั้นตอนการดำเนินงาน**

เมื่อทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคล บริษัท จะต้องดำเนินการดังต่อไปนี้

1.5.1. ให้ผู้ปฏิบัติงานซึ่งเป็นผู้รับทราบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล จะต้องรายงานต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) **ทันที** เพื่อร่วมกันพิจารณากำหนดแนวทาง และวิธีการระงับหรือบรรเทาผลเสียหายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้น โดยสามารถได้แจ้งทั้งช่องทางปกติและ ช่องทางออนไลน์ โดยดำเนินการดังนี้

1.5.1.1. ช่องทางที่ 1 ผ่านการแจ้งทางโทรศัพท์ กระบวนการ คือ แจ้งเรื่องไปที่เจ้าหน้าที่ [โทร. 032 909606]

1.5.1.2. ช่องทางที่ 2 ผ่านอีเมล กระบวนการ คือ ส่งไปที่อีเมล [info@vananava.com]

1.5.2. หลังจากได้รับแจ้งตาม 5.1. ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สอบสวนและควบคุมการละเมิดข้อมูลส่วนบุคคล รวมถึง กู้คืนข้อมูลส่วนบุคคลที่ถูกละเมิด และ/หรือ บริการที่ได้รับผลกระทบ

---

[1] *พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้ระบุคำนิยามของ "การละเมิดข้อมูลส่วนบุคคล" ไว้ จึงนำคำนิยาม "personal data breach" ตาม Article 4 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."*

1.6. หลังจากได้รับแจ้งตาม 5.1. และปฏิบัติตาม 5.2. ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล แจ้งคณะกรรมการบริหาร ถึงเหตุดังกล่าว และร่วมกับฝ่ายเทคโนโลยีสารสนเทศ (IT) และแผนกความปลอดภัย ในการประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (โดยใช้หลักเกณฑ์การประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ในบทที่ 2) ประเมินระดับของความเสี่ยง

1.6.1. ในกรณีที่ผลประเมินชี้ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหาร แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนั้นต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

1.6.2. ในกรณีที่ผลประเมินชี้ว่ามีความเสี่ยงสูง (High Risk) ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พร้อมกับแนวทางเยียวยา ให้ทั้งเจ้าของข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ

1.7. ระยะเวลาดำเนินงานในข้อ 5.1. และ 5.2. ต้องดำเนินการภายใน 72 ชั่วโมง

1.8. การแจ้งเหตุตาม 5.1. และ 5.2. ต้องแจ้งเตือนไปยังหน่วยงานที่กำกับดูแลและเจ้าของข้อมูลที่ได้รับผลกระทบ ในแต่ละกรณีต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

1.8.1. การแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (โดยใช้แบบฟอร์มตามเอกสารแนบที่ 1)

1.8.1.1. คำอธิบายลักษณะของเหตุการณ์เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล ประเภทและปริมาณข้อมูลส่วนบุคคลที่เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล จำนวนเจ้าของข้อมูลส่วนบุคคลและผลกระทบที่เกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล

1.8.1.2. ชื่อสกุล รวมทั้งข้อมูลสำหรับการติดต่อเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และผู้ปฏิบัติงานที่เกี่ยวข้อง เพื่อการประสานงานและติดต่อสอบถามข้อมูลเพิ่มเติม

1.8.1.3. ลักษณะของความเสียหายที่เกิดหรืออาจจะเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคลนั้น

1.8.1.4. **ในกรณีที่เหตุการละเมิดมีความเสี่ยงสูง (High Risk)** ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล จะต้องแจ้งแนวทางและวิธีการระงับหรือบรรเทาผลเสียหายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้นด้วย

1.8.2. การแจ้งเจ้าของข้อมูลส่วนบุคคล

1.8.2.1. คำอธิบายลักษณะของเหตุการณ์เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล ประเภทและปริมาณข้อมูลส่วนบุคคลที่เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล รวมทั้งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

1.8.2.2. ชื่อสกุล รวมทั้งข้อมูลสำหรับการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและผู้ปฏิบัติงานที่เกี่ยวข้อง

1.8.2.3. ลักษณะของความเสียหายที่เกิดหรืออาจจะเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล รวมทั้งแนวทางและวิธีการระงับหรือบรรเทาผลเสียหายเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้น

1.8.2.4. คำวินิจฉัยหรือข้อสั่งการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (ถ้ามี)

1.9. เมื่อปัญหาการละเมิดข้อมูลส่วนบุคคลได้รับการแก้ไขเรียบร้อยแล้ว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึกรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น รวมทั้งสรุปผลวิเคราะห์เหตุการละเมิด สิ่งที่ได้เรียนรู้และแนวทางการแก้ไขเหตุการณ์ดังกล่าว เพื่อทำแนวทางป้องกันไม่ให้เกิดความเสียหายที่เพิ่มมากขึ้น รวมไปถึงการระบุหรือส่งมอบหน้าที่ต่าง ๆ ให้กับผู้รับผิดชอบเพื่อดำเนินการตามแผนต่าง ๆ ตามที่กำหนดไว้

นโยบายการเก็บรักษาข้อมูล

1. วัตถุประสงค์ของนโยบาย

1.1. เพื่อมีผลบังคับใช้ภายในบริษัท วานา นาวา จำกัด (บริษัท) โดยครอบคลุมถึงการดำเนินงานในธุรกิจที่บริษัท ดูแลรับผิดชอบ อันมีสวนน้ำ วานา นาวา วอเตอร์ จังเกิ้ล เป็นอาทิ

1.2. เพื่อใช้บังคับเป็นการทั่วไปกับส่วนงานและพนักงานทุกระดับ

1.3. นโยบายนี้ไม่ถือเป็นส่วนหนึ่งของสัญญาจ้าง แต่เป็นการกำหนดแนวทางการทำงานที่พนักงานต้องปฏิบัติ การไม่ดำเนินการตามนโยบายนี้จะมีผลทางวินัยพนักงาน

1.4. นโยบายนี้จะได้รับการทบทวนและปรับปรุงเป็นประจำ ซึ่งจะได้แจ้งให้พนักงานทุกคนทราบทุกครั้ง

2. ขอบข่าย

2.1. เมื่อมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล บริษัท วานา นาวา จำกัด ("วานา นาวา" หรือ "บริษัท") มีหน้าที่จะต้องปฏิบัติตามมาตรา 23 (3) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยบริษัทจะไม่ทำการเก็บข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็นที่จะต้องมีการดำเนินการตามนโยบายนี้

2.2. นโยบายนี้กำหนดระยะเวลาการเก็บรักษาและเงื่อนไขในการทำลายข้อมูลส่วนบุคคลซึ่ง วานา นาวา ครอบครองอยู่ ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์ หรือเอกสารอื่นใด ซึ่งหมายรวมถึง (แต่ไม่จำกัดเพียง) จดหมาย อีเมล การจดข้อความ ข้อมูลการเงิน รายงาน เอกสารทางกฎหมาย หรือรูปภาพใด ๆ ที่มีข้อมูลส่วนบุคคลอยู่

3. ขอบเขตการใช้และการกักเก็บข้อมูล

ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (ของบุคลากร/บุคคลภายนอก)		
ประเภทของข้อมูลส่วนบุคคล	ระยะเวลาการเก็บรักษา	ระดับการลบข้อมูล
ข้อมูลส่วนบุคคล ข้อมูลการเงินและการทำธุรกรรมด้านการเงินและการบัญชี	ปีปัจจุบัน +10 ปี	ต้องได้รับพิจารณาจากคณะกรรมการบริหารก่อนลบข้อมูล
ข้อมูลส่วนบุคคลและข้อมูลการติดต่อของคู่ค้า/คู่สัญญา ด้านการจัดซื้อจัดจ้าง	ปีปัจจุบัน +10 ปี	ลบด้วยการทำให้ข้อมูลไม่อาจถูกเข้าถึงได้อีก
ข้อมูลด้านการบริหาร	ปีปัจจุบัน +10 ปี	ต้องได้รับพิจารณาจากคณะกรรมการบริหารก่อนลบข้อมูล
ข้อมูลส่วนบุคคลและข้อมูลการติดต่อของลูกค้าด้านการตลาด	ปีปัจจุบัน +10 ปี	ลบด้วยการทำให้ข้อมูลไม่อาจถูกเข้าถึงได้อีก
ข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวของพนักงาน ด้านทรัพยากรบุคคล	ปีปัจจุบัน +10 ปี	ลบด้วยการทำให้ข้อมูลไม่อาจถูกเข้าถึงได้อีก
ข้อมูลบนเว็บไซต์	ปีปัจจุบัน +2 ปี	ลบด้วยการทำให้ข้อมูลไม่อาจถูกเข้าถึงได้อีก

4. การลบ ทำลาย หรือทำให้ข้อมูลนั้นไม่อาจระบุตัวบุคคลได้

เมื่อหมดความจำเป็นที่จะต้องเก็บข้อมูลตามระยะเวลาที่ระบุในเอกสารนี้แล้ว บริษัท มีหน้าที่จะต้อง ลบ หรือทำลายข้อมูลส่วนบุคคลนั้นอย่างถาวร (permanently) หรือทำให้ข้อมูลนั้นไม่อาจระบุตัวบุคคลได้ โดย บริษัท อาจเลือกที่จะดำเนินกระบวนการดังต่อไปนี้

4.1. เอกสารในรูปแบบอิเล็กทรอนิกส์จะต้องถูกลบด้วยวิธีการที่ทำให้ข้อมูลนั้นไม่อาจถูกเข้าถึงได้อีกเลย

4.2. ข้อมูลส่วนบุคคลที่ถูกเก็บอยู่ในอุปกรณ์ที่เก็บข้อมูลหรือวัตถุใด ๆ จะต้องถูกลบออกจากอุปกรณ์ดังกล่าวก่อนที่จะมีการทิ้งอุปกรณ์นั้น

4.3. ในกรณีที่ข้อมูลส่วนบุคคลนั้นไม่สามารถถูกลบจากอุปกรณ์ได้ จะต้องมีการทำลายตัวอุปกรณ์นั้นโดยบุคคลที่มีสิทธิหรือองค์กรที่ได้รับอนุญาตให้ประกอบกิจการทำลาย

4.4. กระดาษจะต้องถูกทำลายโดยเครื่องย่อยกระดาษ

2. <u>บทที่ 2: หลักเกณฑ์การประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล</u>

2.1. หลักการประเมินความเสี่ยง

2.1.1. เนื่องจากลักษณะของเหตุแห่งการละเมิดข้อมูลส่วนบุคคลอาจเกิดขึ้นโดยมีลักษณะเฉพาะและมีความหลากหลาย จึงจำเป็นต้องทำการประเมินความเสี่ยงเป็นรายกรณี

2.1.2. ต้องพิจารณาประเมินความเสี่ยงจากระดับความรุนแรงของเหตุ (Severity of Incident) ร่วมกับการประเมินผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคลด้วย เนื่องจากการละเมิดข้อมูลส่วนบุคคลที่สำคัญของเจ้าของข้อมูลส่วนบุคคลจำนวนน้อยอาจมีความเสี่ยงหรือผลกระทบสูงกว่าการละเมิดข้อมูลส่วนบุคคลที่ไม่สำคัญของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก โดยใช้เกณฑ์การประเมินความเสี่ยงตามที่กำหนดไว้ในข้อ 2.2

2.2. เกณฑ์การประเมินความเสี่ยงจากระดับความรุนแรงของเหตุ (Severity of Incident)

2.2.1. ระดับต่ำ: สำหรับกรณีดังต่อไปนี้

2.2.1.1. เป็นการละเมิดข้อมูลส่วนบุคคลทั่วไป (เช่น ชื่อ นามสกุล)

2.2.1.2. เป็นการละเมิดข้อมูลส่วนบุคคลที่มีระบบป้องกันการเข้าถึงข้อมูล (Security) ในระดับดี เช่น ข้อมูลส่วนบุคคลที่เข้ารหัสไว้อย่างดี

2.2.1.3. เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นพนักงาน หรือลูกจ้าง หรือผู้รับบริการ ของ วานา นาวา ที่มีจำนวนน้อย

2.3. ระดับปานกลาง: สำหรับกรณีดังต่อไปนี้

2.3.1. เป็นการละเมิดข้อมูลส่วนบุคคลที่เป็นกลุ่มของข้อมูล เช่น ชุดข้อมูลที่ประกอบด้วย ชื่อ นามสกุล วันเกิด ที่อยู่ ฯลฯ

2.3.2. เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นพนักงาน หรือลูกจ้าง หรือผู้รับบริการของ วานา นาวา หลายราย

2.3.3. ระดับสูง: สำหรับกรณีดังต่อไปนี้

2.3.3.1. เป็นการละเมิดข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น ข้อมูลด้านสุขภาพ

2.3.3.2. เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นสมาชิก หรือเป็นพนักงาน หรือลูกจ้างหรือผู้รับบริการทั้งหมดของ วานา นาวา

2.3.3.3. เป็นการละเมิดข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นบุคคลที่มีชื่อเสียง

2.3.3.4. เป็นการละเมิดต่อข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ที่มีการรายงานข่าวเหตุการณ์ออกสู่สาธารณะโดยสื่อมวลชน

สำหรับการพิจารณาประเมินความเสี่ยงต้องประเมินจากปริมาณข้อมูลส่วนบุคคลที่ถูกละเมิดกับผลกระทบที่คาดว่าจะเกิดขึ้น ดังต่อไปนี้

ปริมาณข้อมูลส่วนบุคคลที่ถูกละเมิด X ผลกระทบที่คาดว่าจะเกิดขึ้น

ปริมาณข้อมูลส่วนบุคคลที่ถูกละเมิด

หัวข้อ	ระดับความเสี่ยง		
	ต่ำ	ปานกลาง	สูง
ปริมาณข้อมูลที่ถูกละเมิด	ข้อมูลส่วนบุคคลที่ถูกละเมิดมีปริมาณน้อยและมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไว้เป็นอย่างดีทำให้ยากที่จะเข้าถึงได้	ข้อมูลส่วนบุคคลที่ถูกละเมิดมีปริมาณน้อยและมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไว้บางส่วนทำให้มีความเป็นไปได้ที่จะเข้าถึงได้	ข้อมูลส่วนบุคคลที่ถูกละเมิดมีปริมาณมากและไม่มีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทำให้สามารถเข้าถึงได้โดยง่าย

ผลกระทบที่คาดว่าจะเกิดขึ้น

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

ตารางแสดงระดับความเสี่ยง

ปริมาณข้อมูลส่วนบุคคลที่ถูกละเมิด				
มาก	ปานกลาง	สูง	สูง	
ปานกลาง	ต่ำ	ปานกลาง	สูง	
น้อย	ต่ำ	ต่ำ	ปานกลาง	
	ต่ำ	ปานกลาง	สูง	ผลกระทบที่คาดว่าจะเกิดขึ้น

2.4. **ปัจจัยเสริมประกอบการพิจารณาระดับความเสี่ยง**

การพิจารณาประเมินความเสี่ยงตามข้อ 2 ควรพิจารณาปัจจัยเสริมที่มีผลต่อระดับความเสี่ยง ดังต่อไปนี้

2.5. ระดับความยากในการบ่งชี้ตัวตนของเจ้าของข้อมูลส่วนบุคคล:

แม้ว่าข้อมูลส่วนบุคคลจะเป็นข้อมูลนิรนาม แต่ถ้าสามารถบ่งชี้ตัวตนขอเจ้าของข้อมูลส่วนบุคคลได้ ก็อาจมีความเสี่ยงด้วยเช่นกัน เช่น ข้อมูลตำแหน่งของบุคคลในที่ทำงาน ซึ่งฝ่ายทรัพยากรบุคคลสามารถบ่งชี้ตัวตนได้

2.6. ลักษณะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ:

ถ้าบุคคลที่ได้รับผลกระทบเป็นกลุ่มที่อ่อนแอ (Vulnerable) เช่น ผู้ป่วยโรคติดต่อร้ายแรง หรือผู้ป่วยที่เป็นคนพิการ เป็นต้น จะถือว่ามีความเสี่ยงสูง

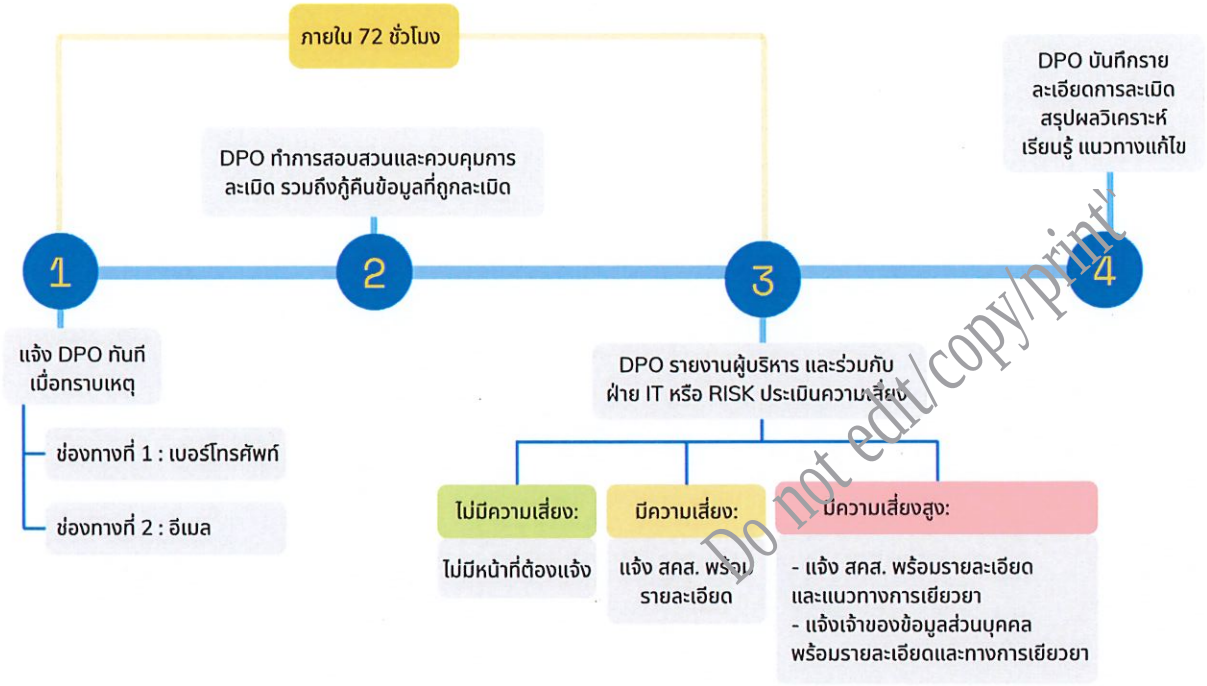
2.7. ลักษณะของผู้ควบคุมข้อมูลส่วนบุคคล

ถ้าผู้ควบคุมข้อมูลส่วนบุคคลเป็นหน่วยงานที่มีหน้าที่เก็บข้อมูลของบุคคลที่มีปัญหาที่อ่อนไหว เช่น ปัญหาทางสุขภาพกายหรือสุขภาพจิต การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีความเสี่ยงมากกว่าข้อมูลของหน่วยงานทั่วไป

2.8. การละเมิดข้อมูลส่วนบุคคลที่เจาะจงเป้าหมายเฉพาะ:

การละเมิดข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เฉพาะเจาะจง เช่น การต้องการเข้าถึงข้อมูลส่วนบุคคลที่เป็นความลับที่สุด จะมีความเสี่ยงสูงกว่าการละเมิดข้อมูลส่วนบุคคลโดยไม่ได้ตั้งใจ

3. บทที่ 3: สรุปขั้นตอนการดำเนินการเมื่อทราบเหตุละเมิดข้อมูลส่วนบุคคล



3.1. เอกสารที่เกี่ยวข้อง

3.1.1. แบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3.1.2. แบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

3.1 แบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

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. 2562 กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า ภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งจากการตรวจสอบเบื้องต้น [*] พบว่าอาจมีข้อมูลส่วนบุคคลที่ถูกเข้าถึงโดยไม่ชอบด้วยกฎหมายและไม่ได้รับอนุญาต รายละเอียดดังต่อไปนี้

1. 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 / อุปกรณ์อิเล็กทรอนิกส์ที่บรรจุข้อมูลส่วนบุคคลสูญหาย / การแก้ไขข้อมูลโดยไม่ได้รับความยินยอม	

รายละเอียดของเหตุการณ์	
สถานที่เกิดเหตุละเมิดข้อมูล * เช่น ภายในฝ่ายงาน / หน้าสำนักงาน / ระบบ เป็นต้น	
ประเภทของเจ้าของข้อมูล * อ้างอิงตามแบบบันทึกการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมดังกล่าว	
ประมาณการจำนวนผู้เสียหาย * เช่น 1 คน 10 คน 100 คน / อย่างน้อย 50 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 รวมถึงอธิบายถึงการรักษาความปลอดภัยของข้อมูลในระบบดังกล่าวโดยสรุป เช่น มีการเข้ารหัสข้อมูล หรือมีการสำรองไฟล์ไว้ในระบบ	

2. ผลกระทบที่อาจเกิดขึ้นจากเหตุละเมิดส่วนบุคคล

ความเสี่ยง อธิบายหัวข้อความเสี่ยงต่อข้อมูลส่วนบุคคล * เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	อธิบายความเสี่ยงและผลกระทบต่อข้อมูลส่วนบุคคล อธิบายรายละเอียดผลกระทบที่อาจเกิดขึ้นต่อข้อมูลส่วนบุคคล * เช่น ผู้พบเห็นอาจสามารถเข้าถึงข้อมูลดังกล่าวและสามารถใช้ข้อมูลดังกล่าวโดยมิชอบ	ประมาณการความเสี่ยงต่อเจ้าของข้อมูล * สูง / กลาง / ต่ำ / ไม่มีความเสี่ยง / ไม่สามารถประเมินได้
ความเสี่ยงที่ (1)		
ความเสี่ยงที่ (2)		
ความเสี่ยงที่ (3)		

3. มาตรการในการรับมือกับเหตุละเมิดที่เกิดขึ้นเพื่อลดผลกระทบและการดำเนินการในการเยียวยา

ความเสี่ยง	มาตรการในการรับมือกับความเสี่ยงที่เกิดจากเหตุเหตุละเมิด * อธิบายรายละเอียดมาตรการที่จะดำเนินการกับความเสี่ยงแต่ละรูปแบบที่เกิดขึ้น	รายละเอียดการกระทำที่ได้ดำเนินการเพื่อเยียวยาการละเมิด * เช่น ดำเนินการเปลี่ยนรหัสความปลอดภัย ดำเนินการค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น
ความเสี่ยงที่ (1)		
ความเสี่ยงที่ (2)		
ความเสี่ยงที่ (3)		

4. ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

5. ข้อมูลติดต่อขององค์กร

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

จึงเรียนมาเพื่อทราบ และโปรดดำเนินการตามที่เห็นสมควร ในกรณีที่สำนักงานฯ มีข้อสงสัยหรือต้องการข้อมูลเกี่ยวกับเหตุละเมิดดังกล่าวเพิ่มเติม สำนักงานฯ สามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ เจ้าหน้าที่ประสานงานของ [*] ได้ตามข้อมูลข้างต้น

ขอแสดงความนับถือ

_____

(ชื่อ-นามสกุล)

(ตำแหน่ง)

สิ่งที่แนบมาด้วย : แบบบันทึกการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวข้อง

3.2 แบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

แบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า ภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ดังนั้น เพื่อให้ทางเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถดำเนินการตามบทบัญญัติดังกล่าว โปรดระบุรายละเอียดเหตุละเมิดข้อมูลส่วนบุคคลเท่าที่ท่านสามารถระบุได้ตามแบบฟอร์มต่อไปนี้ ทั้งนี้ ภายในระยะเวลายี่สิบสี่ชั่วโมงนับแต่ทราบเหตุละเมิดดังกล่าว

- ให้ผู้แจ้งเหตุส่งเอกสารหลักฐานเท่าที่มีต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อประกอบการพิจารณาความเสี่ยงของเหตุละเมิดดังกล่าวกรณีที่ประเมินว่าไม่มีความเสี่ยง ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลบันทึกเหตุละเมิดไว้และเสนอแนวทางแก้ไขไม่ให้มีเหตุการณ์เช่นเดียวกันนี้เกิดขึ้นอีกในอนาคต
- กรณีที่ประเมินว่ามีความเสี่ยง ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเสนอเร่งแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้แล้วเสร็จภายในเจ็ดสิบสองชั่วโมง
- กรณีที่ประเมินว่ามีความเสี่ยงสูง ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเสนอแนวทางการแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคลเพื่ออนุมัติโดยทันที

1. ข้อมูลของผู้แจ้งเหตุ

ชื่อ-สกุล	
ที่อยู่ที่ติดต่อ * โทรศัพท์ * อีเมล	
หน่วยงานที่สังกัด * ส่วนงานหรือฝ่ายงาน	

2. 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 / ระบบปฏิบัติการด้านการเก็บข้อมูล เป็นต้น	
ประเภทของเจ้าของข้อมูล * อ้างอิงตาม ROP	
ประมาณการจำนวนผู้เสียหาย * เช่น 1 คน 10 คน 100 คน / อย่างน้อย 50 คน / ไม่สามารถประมาณการยอดได้	
ประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด * ระบุรายการข้อมูลเป็น field หรือไม่สามารถระบุได้ในขณะที่แจ้ง	
คุณทราบเหตุละเมิดได้อย่างไร * เช่น ได้รับแจ้งจากเจ้าของข้อมูลถึงการละเมิด / พบการเข้าถึงระบบใน Log File ว่าถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ / ทำอุปกรณ์สูญหาย	
รายละเอียดโดยสรุปของเหตุละเมิด * เพื่อขยายความลักษณะเหตุละเมิด เพื่อให้เข้าใจเนื้อหาของการละเมิดข้อมูลส่วนบุคคล โดยอธิบายเนื้อหาเท่าที่สามารถระบุได้ รวมไปถึงคำขยายความประเภทข้อมูลที่ทราบโดยละเอียด	

รายละเอียดระบบเทคโนโลยีสารสนเทศและอุปกรณ์อิเล็กทรอนิกส์ที่เกี่ยวข้อง (ถ้ามี) * เช่น ระบบปฏิบัติการด้านการเก็บข้อมูล/ มือถือส่วนบุคคล รวมถึงอธิบายถึงการรักษาความปลอดภัยของข้อมูลในระบบดังกล่าวโดยสรุป เช่น มีการเข้ารหัสข้อมูล หรือมีการสำรองไฟล์ไว้ในระบบ	
อธิบายความเสี่ยงต่อข้อมูลส่วนบุคคล * เช่น ผู้พบเห็นอาจสามารถเข้าถึงข้อมูลดังกล่าว และสามารถใช้ข้อมูลดังกล่าวโดยมิชอบ	
ประมาณการความเสี่ยงต่อเจ้าของข้อมูล * สูง / กลาง / ต่ำ / ไม่มีความเสี่ยง / ไม่สามารถประเมินได้	
รายละเอียดการกระทำที่ได้ดำเนินการเพื่อเยียวยาการละเมิด * เช่น ดำเนินการเปลี่ยนรหัสความปลอดภัย ดำเนินการค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น	
ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	