นโยบายการบริหารจัดการหากมีการละเมิด หรือข้อมูลรั่วไหล (Data Breach)

บริษัท ทเวนตี้ โฟร์ คอน แอนด์ ซัพพลาย จำกัด (มหาชน)

เลขที่เอกสาร : 24CS-PL-025
ฉบับที่ : A
แก้ไขครั้งที่ : 01
วันที่บังคับใช้ : 13 พฤษภาคม 2567

	ตำแหน่ง	ชื่อ - นามสกุล	ลายเซ็น	วันที่
จัดทำโดย	เลขานุการบริษัท	ดุลภาพร เปไธสง	*-ดุลภาพร-*	10/05/67
ทวนสอบโดย	กรรมการผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	นางสาวชุติกาญจน์ สง่า	*-ชุติกาญจน์-*	10/05/67
อนุมัติโดย	ประธานเจ้าหน้าที่บริหาร	นายยศวีย์ วัฒนธีระกิจจา	*-ยศวีย์-*	13/05/67

นโยบายการบริหารจัดการหากมีการละเมิดหรือข้อมูลรั่วไหล (Data Breach)

1. **วัตถุประสงค์**

   1) เพื่อเป็นแนวทางในการจัดการหากมีการละเมิดหรือข้อมูลรั่วไหล (Data Breach)

   2) เพื่อให้มั่นใจว่า การให้บริการ หรือการทำงานทั้งหลาย บริษัทนำข้อมูลดังกล่าวไปเก็บรวบรวม ประมวลผลใช้หรือเปิดเผยข้อมูลเท่าที่จะเป็น ด้วยความระมัดระวัง

2. **นโยบาย**

   ข้อมูลส่วนบุคคลรั่วไหล สามารถเกิดได้จากปัจจัยหลายประการ ทั้งในเชิงระบบและเชิงเทคนิค เช่น การไม่อัพเดทซอฟแวร์ที่ใช้ในการรักษาความปลอดภัย หรือความประมาทและรู้เท่าไม่ถึงการณ์ของผู้ดูแลข้อมูลส่วนบุคคล เช่น การเปิดอีเมลหรือลิงก์ที่ไม่เหมาะสม การดาวน์โหลดไฟล์ที่แฝงไปด้วยมัลแวร์ ดังนั้น แม้ว่าบริษัทฯ จะมีการรักษาความปลอดภัยที่เพียงพอเหมาะสม ก็สามารถเกิดการรั่วไหลหรือถูกโจมตีระบบได้เช่นเดียวกัน โดยเฉพาะระบบคอมพิวเตอร์ของบริษัทฯ นั้นจะมีข้อมูลสุขภาพผู้ป่วย ซึ่งถือเป็นข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ดังนั้นจึงจำเป็นต้องกำหนดแนวทางนโยบายการจัดการข้อมูลส่วนบุคคลรั่วไหล ให้เจ้าหน้าที่ทุกท่านรับทราบและนำไปปฏิบัติ เพื่อเป็นการป้องกันไม่ให้เกิดข้อมูลส่วนบุคคลรั่วไหล หรือหากมีการรั่วไหลจะมีการปฏิบัติตามขั้นตอนที่กฎหมายกำหนดได้อย่างถูกต้องเหมาะสม

3. **ขอบเขต**

   กรณีข้อมูลส่วนบุคคลรั่วไหลมีความหมายกว้างครอบคลุมการที่ข้อมูลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษาหรือถูกประมวลผลอย่างอื่น ไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ โดยใช้นโยบายนี้กับเจ้าหน้าที่ทุกท่านในบริษัทฯ รวมถึงเจ้าหน้าที่ชั่วคราวและตัวแทนและผู้รับเหมา ที่ปรึกษา ซัพพลายเออร์และผู้ประมวลผลข้อมูลที่ทำงานให้หรือในนามของบริษัทฯ

4. **คำนิยาม**

คำศัพท์	คำอธิบาย
การประมวลผลข้อมูล	การดำเนินการหรือชุดการดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่นการเก็บ บันทึก จัดระบบ จัดโครงสร้าง เก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการ

คำศัพท์	คำอธิบาย
	ส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย
ข้อมูลอ่อนไหว (Sensitive Personal Data)	เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลใดๆ ที่ระบุไปถึง “เจ้าของข้อมูล” (Data Subject)ได้
ข้อมูลส่วนบุคคลรั่วไหล (Personal Data Breach)	การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลทำให้เกิด ความเสียหาย,สูญหาย,เปลี่ยนแปลง, เปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคลที่ใช้งานอยู่
ผู้ควบคุมข้อมูล (Data Controller)	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ หน่วยงานหรือองค์กรใด ซึ่งเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูล (Data Processor)	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ หน่วยงานหรือองค์กรใด ซึ่งประมวลผลข้อมูลแทนผู้ควบคุมข้อมูล
เจ้าของข้อมูล (Data Subject)	มีความหมายในลักษณะเป็นบุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง ไม่ใช้เจ้าของในลักษณะทรัพย์สิทธิ หรือเป็นคนสร้างข้อมูลนั้นขึ้นมา มีความแตกต่างจาก Data owner ในกฎหมาย (บางตัว) ของสหรัฐอเมริกา
ผู้กำกับดูแล	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
Confidentiality Breach	การเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ เช่น ○ กำหนด User authorization ผิดพลาด ทำให้เข้าถึงข้อมูลที่ไม่ได้มีเพื่อไว้ตนเอง ○ ระบบความรักษาปลอดภัยข้อมูลไม่ดีเพียงพอ ทำให้ Hacker นำข้อมูลออกไปได้ ○ การส่งข้อมูลความลับออกไปโดย email หรือ Social media

คำศัพท์	คำอธิบาย
Integrity Breach	การแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ ○ ข้อมูลถูกผู้ที่ไม่ได้รับอนุญาตลบไป ○ ข้อมูลเดียวกันมน 2 ตารางไม่เท่ากัน หรือ ไม่ถูกต้อง ○ ใบแจ้งหนี้ของธนาคารของลูกค้ารายหนึ่งได้ส่งไปยังลูกค้าอีกรายหนึ่ง
Availability Breach	การทำให้เข้าถึงข้อมูลไม่ได้หรือการทำให้ข้อมูลสูญหายหรือทำลายไป ไม่ว่าโดยการกระทำโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ เช่น ○ ระบบล่ม ไม่สามารถใช้ข้อมูลได้หลายชั่วโมง ○ ระบบของบริษัทโดน Ransomware โจมตี ○ การถูกโจมตีด้วย DoS (Denial of Service) ทำให้ระบบไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้

5. **หน้าที่และความรับผิดชอบ**

ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (data breach)

1) หน้าที่แจ้งต่อผู้กำกับดูแล: ภายใน 72 ชั่วโมงนับแต่ได้ทราบ เว้นแต่เหตุที่เกิดนั้นไม่น่าจะก่อให้เกิดความเสี่ยงใดๆ ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล กรณีที่ไม่อาจแจ้งเหตุได้ภายใน 72 ชั่วโมง ผู้ควบคุมจะต้องแจ้งเหตุผลแห่งการแจ้งเหตุล่าช้าด้วย ข้อมูลที่ต้องแจ้งมีดังต่อไปนี้

1.1) คำอธิบายลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณและปริมาณข้อมูลที่เกี่ยวข้อง

1.2) ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม

1.3) คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว

1.4) คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น

2) หน้าที่แจ้งต่อเจ้าของข้อมูล: ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเจ้าของข้อมูลโดยไม่ชักช้าต่อเมื่อการรั่วไหลของข้อมูลนั้นก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูลในกรณีเช่นว่านี้จะต้องแจ้งให้เจ้าของข้อมูลทราบด้วยภาษาที่เข้าใจง่ายและมีความชัดเจนและมีรายละเอียดอย่างน้อยดังต่อไปนี้

2.1) คำอธิบายลักษณะของการรั่วไหลของข้อมูล

2.2) ชื่อหรือข้อมูลการติดต่อเจ้าหน้าที่ผู้รับผิดชอบหรือเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer)

2.3) ผลที่อาจจะเกิดขึ้นจากการที่ข้อมูลรั่วไหล ซึ่งรวมถึงความเสี่ยงต่อเจ้าของข้อมูล

2.4) มาตรการที่เสนอแนะหรือแนวทางเยียวยา ให้เจ้าของข้อมูลกระทำเพื่อรับมือกับกรณีดังกล่าวที่อาจจะลดผลร้ายที่อาจเกิดจากการที่ข้อมูลรั่วไหลได้

6. **การการจัดการและประเมินระดับความเสียหาย**

1) ไม่มีความเสี่ยง:

1.1) จดบันทึกการรั่วไหล

1.2) รายงาน ต่อประธานเจ้าหน้าที่บริหารทราบ (หลังจบเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล)

2) มีความเสี่ยงแต่ไม่มาก:

2.1) จดบันทึกการรั่วไหล

2.2) รายงาน ต่อประธานเจ้าหน้าที่บริหารทราบ (ภายใน 48 ชั่วโมงในวันทำการ นับจากทราบเหตุการณ์) และแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล(ภายใน 72 ชั่วโมงในวันทำการ นับจากทราบเหตุการณ์)

3) มีความเสี่ยงสูง:

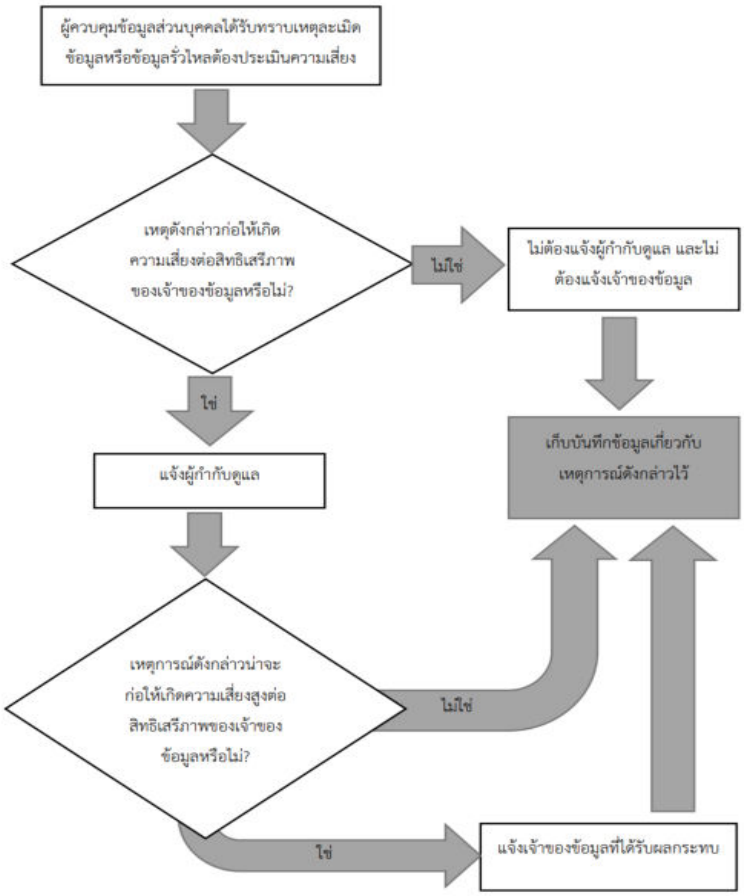
3.1) จดบันทึกการรั่วไหล

3.2) รายงานต่อประธานเจ้าหน้าที่บริหารทราบ (ภายใน 24 ชั่วโมงในวันทำการ นับจากทราบ เหตุการณ์) แจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ภายใน 48 ชั่วโมงในวันทำการ นับจากทราบ เหตุการณ์) และแจ้งเจ้าของข้อมูลส่วนบุคคล (ภายใน 72 ชั่วโมงในวันทำการ นับจากทราบเหตุการณ์)

7. **ขั้นตอนการปฏิบัติงาน**



8. **Flow Chart กระบวนการทำงาน**



9. **ช่องทางติดต่อ**

ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ตามช่องทาง ดังต่อไปนี้

อีเมล์ 24cs.dpo@24con-supply.com
ไปรษณีย์หรือส่งด้วยตนเองโดย ส่งถึง: Data Protection Officer
ที่อยู่: บริษัท ทเวนตี้ โฟร์ คอน แอนด์ ซัพพลาย จำกัด (มหาชน)
89 อาคาร เอไอเอ แคปปิตอล เซ็นเตอร์ ชั้น 9 ห้อง
901 ถนนรัชดาภิเษก เขต/แขวง ดินแดง จังหวัด กรุงเทพมหานคร
10400