กระบวนการรับมือเมื่อเกิดเหตุละเมิด
(Incident Management Procedure)[1]

บริษัท อรุณ พลัส จำกัด (**"บริษัทฯ"**) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่เกิดเหตุการณ์เกี่ยวกับการละเมิดข้อมูลส่วนบุคคลซึ่งอยู่ในความรับผิดชอบของบริษัทฯ เอกสารฉบับนี้มีวัตถุประสงค์เพื่อเป็นแนวทางการจัดการที่บริษัทฯ ควรปฏิบัติตามเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล (ตามที่นิยามด้านล่าง) ทั้งที่เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น ซึ่งอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล

1. ข้อกำหนดในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

(1) **การติดต่อฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูล:** บุคลากรรายใดที่พบเห็น สงสัย หรือทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่ได้เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น จะต้องรายงานประเด็นดังกล่าวให้ฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูลทราบ**โดยทันที** (สามารถดูข้อมูลการติดต่อของฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูลได้ที่ **ข้อ 1. (4)** ของเอกสารฉบับนี้) โดยใช้แบบฟอร์มการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่อยู่ใน **ภาคผนวก 1**

(2) **เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล:** เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล คือ เหตุการณ์การกระทำ ความขัดข้อง รวมถึงการละเมิดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลใด ๆ ทั้งที่เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ที่ก่อหรืออาจก่อให้เกิดความเสียหาย การทำลาย การสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยข้อมูลที่บริษัทฯ เป็นเจ้าของ ควบคุม หรือเก็บรักษาไว้ ไม่ว่าจะโดยตรงหรือโดยอ้อม (เช่น ข้อมูลที่อยู่ภายใต้การดูแลของพันธมิตรทางธุรกิจ หรือผู้ให้บริการภายนอกอื่นที่ให้บริการแก่บริษัทฯ) ทั้งนี้ ไม่ว่าข้อมูลดังกล่าวจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับหรือไม่ก็ตาม และไม่ว่าข้อมูลดังกล่าวจะอยู่ในแฟ้มเอกสารกระดาษ อีเมล ตาราง บันทึกบุคลากร บันทึกบัญชีเงินเดือน เครื่องแม่ข่าย (เซิร์ฟเวอร์) อุปกรณ์จัดเก็บข้อมูลแบบพกพา (เช่น คอมพิวเตอร์แล็ปท็อป หรือโทรศัพท์สมาร์ตโฟน) หรือฐานข้อมูลไอที เป็นต้น

โดยลักษณะของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งดังต่อไปนี้

- การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

[1] เอกสาร**กระบวนการรับมือเมื่อเกิดเหตุละเมิด (Incident Management Procedure)** ฉบับนี้ ถือเป็นส่วนหนึ่งของ**นโยบายการคุ้มครองข้อมูลส่วนบุคคล (PDPA Policy)** (**"นโยบายฯ"**) ของบริษัท อรุณ พลัส จำกัด ถ้อยคำใดที่ไม่ได้ให้ความหมายไว้โดยเฉพาะในเอกสารฉบับนี้ ให้มีความหมายตามที่ระบุไว้ในนโยบายฯ โปรดศึกษารายละเอียดที่เกี่ยวข้องในนโยบายฯ ควบคู่ไปกับการศึกษาและปรับใช้เอกสารฉบับนี้ด้วย

- การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
- การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

เหตุการณ์ต่อไปนี้เป็นเพียงตัวอย่างเหตุการณ์บางส่วน ซึ่งโดยลักษณะจะต้องรายงานให้ฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูลทราบ

- การโจรกรรมหรือการสูญหายของเครื่องคอมพิวเตอร์ คอมพิวเตอร์แล็ปท็อป โทรศัพท์สมาร์ทโฟน อุปกรณ์บันทึกข้อมูลแบบธัมบ์ไดรฟ์ อุปกรณ์บันทึกข้อมูลแบบพกพา (External Hard Drive) หรืออุปกรณ์บันทึกข้อมูลอื่นที่เป็นของบริษัทฯ หรือบุคลากรที่ใช้อุปกรณ์ดังกล่าวบันทึกข้อมูลที่เกี่ยวข้องกับบริษัทฯ
- การบุกรุก หรือการโจรกรรมภายในสถานที่ของบริษัทฯ
- ผู้โจมตีก่อให้เกิดความเสี่ยงต่อระบบของบริษัทฯ เช่น ฐานข้อมูล คอมพิวเตอร์ เครื่องข่าย การสื่อสารของบริษัทฯ
- เมื่อบุคลากรได้เห็น เข้าถึง หรือเปิดเผยข้อมูล แฟ้มข้อมูล หรือฐานข้อมูลที่อยู่นอกขอบเขตหน้าที่ที่ได้รับมอบหมาย
- เมื่อมีบุคคลภายนอกกระทำผิดสัญญาการห้ามเปิดเผยข้อมูล หรือสัญญาการรักษาความลับ
- เหตุการณ์ตามที่กล่าวมาข้างต้น ซึ่งเกี่ยวข้องกับพันธมิตรทางธุรกิจหรือผู้ให้บริการภายนอกของบริษัทฯ

(3) **ความร่วมมือ:** บุคลากรจะต้องให้ความร่วมมือกับบริษัทฯ และฝ่ายจัดการสถานการณ์ในการตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

(4) **ฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูล**

ฝ่ายจัดการสถานการณ์	
ข้อมูลการติดต่อ	ที่อยู่อีเมล: PDPA@arunplus.com หมายเลขโทรศัพท์: 02-095-5681
สมาชิก	
ผู้จัดการเหตุการณ์ลำดับแรก	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (นายกมลสุข ผาสุข)
สำนักกรรมการผู้จัดการและกฎหมาย	1. นายกมลสุข ผาสุข 2. นางสาวชวิศา วิสัยแสวง 3. นางสาวพัชรี จันทร์แรม
ฝ่ายทรัพยากรบุคคล	นางสาวชนานุช เจียมพาณิชยกิจ
ฝ่ายกลยุทธ์และวางแผน	นายธีระยุทธ พิบูลรุจนานนท์

ความพร้อมของฝ่ายจัดการสถานการณ์: ฝ่ายจัดการสถานการณ์จะต้องมีการเฝ้าสังเกตการณ์ เพื่อเฝ้าระวังตลอด 24 ชั่วโมง โดยสามารถติดต่อได้ที่อีเมล PDPA@arunplus.com และหมายเลขโทรศัพท์ 02-095-5681 เพื่อให้ผู้จัดการเหตุการณ์ลำดับแรกสามารถรับรายงานได้โดยทันที

2. ขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

ระยะที่ 1: การรายงานและยืนยันเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลภายในองค์กร

วัตถุประสงค์ของระยะที่ 1 คือ เพื่อระบุและยืนยันได้อย่างทันท่วงทีว่ามีเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลเกิดขึ้นจริงหรือไม่ และรายงานต่อไปยังฝ่ายจัดการสถานการณ์

(1) **การตรวจสอบเบื้องต้น:** ฝ่ายจัดการสถานการณ์จะระบุผู้ที่ได้รับมอบหมายให้ทำการสืบสวนและตรวจสอบในเบื้องต้นสำหรับแต่ละเหตุการณ์ที่ได้รับรายงาน (“**ผู้จัดการเหตุการณ์ลำดับแรก**”)

โดยผู้จัดการเหตุการณ์ลำดับแรกจะต้องประสานงานกับบุคลากรซึ่งเป็นผู้รายงานเหตุการณ์ และขอข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลให้ได้มากที่สุดเท่าที่มีอยู่ในเวลานั้น รวมถึงตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งในเชิงองค์กร (organizational measure) เชิงเทคนิค (technical measure) และเชิงกายภาพ (physical measure) ที่ใช้กับบริษัทฯ หรือบุคลากรที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล พิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง ตลอดจนประเมินความเสี่ยงที่เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ทั้งนี้ หากเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่เกิดขึ้นเกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือเกี่ยวกับความมั่นคงปลอดภัยของคอมพิวเตอร์อื่น ๆ ผู้จัดการเหตุการณ์ลำดับแรกจะต้องประสานงานกับฝ่ายที่เกี่ยวข้องด้วย นอกจากนี้ ผู้จัดการเหตุการณ์ลำดับแรกควรพิจารณาในเบื้องต้น**โดยเร็วที่สุดและภายในระยะเวลา 24 ชั่วโมงแรก**ว่าจากข้อมูลที่มีอยู่นั้นมีมูลเหตุอันควรเชื่อได้ว่าเหตุการณ์ดังกล่าวได้เกิดขึ้นจริงหรือไม่ หากขณะนั้นไม่มีมูลเหตุอันสมควร ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นการภายในโดยระบุข้อมูลดังนี้

- ชื่อของบุคลากรที่รายงานเหตุการณ์
- คำอธิบายสถานการณ์ของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่มีการรายงาน
- คำอธิบายถึงสาเหตุที่ผู้จัดการเหตุการณ์ลำดับแรกพิจารณาแล้วเห็นว่า เหตุการณ์ดังกล่าวไม่มีมูลเหตุอันควรเชื่อได้ว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลอาจเกิดขึ้น หรือได้เกิดขึ้นไปแล้ว

ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นลายลักษณ์อักษรไปยังสมาชิกรายอื่น ๆ ของฝ่ายจัดการสถานการณ์ทันทีที่ได้รับข้อมูลที่เพียงพอ

(2) **การยืนยันเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล:** หากผู้จัดการเหตุการณ์ลำดับแรกพิจารณาแล้วเห็นว่ามีมูลเหตุอันควรเชื่อได้ว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าวได้เกิดขึ้นจริง ผู้จัดการเหตุการณ์ลำดับแรกจะต้องแจ้งให้สมาชิกรายอื่น ๆ ของฝ่ายจัดการสถานการณ์ทราบโดย**ทันที** เพื่อเริ่มดำเนินการระยะที่ 2 **ต่อไปทันที**

ระยะที่ 2: การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

วัตถุประสงค์ของระยะที่ 2 คือ เพื่อจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลทั้งในระดับภายในและภายนอกองค์กร ในระยะนี้จะต้องมีการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลโดยเร็วที่สุดเท่าที่จะทำได้ เพื่อให้บริษัทฯ สามารถทำการแจ้งเตือนที่จำเป็นได้ทันเวลาในกรณีที่ฝ่ายจัดการสถานการณ์เห็นว่าต้อง

รายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้นให้หน่วยงานรัฐบาล บุคคล หรือผู้ใดก็ตามทราบตามที่กฎหมายกำหนด

ในขณะเดียวกัน ฝ่ายจัดการสถานการณ์จะต้องดำเนินการอื่น ๆ ที่จำเป็นไปพร้อม ๆ กันเพื่อควบคุมเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล และลดความเสี่ยง รวมทั้งความเสียหายลงให้ได้มากที่สุด

(3) **การควบคุมภัยคุกคาม:** เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลขึ้น ฝ่ายจัดการสถานการณ์จะต้องดำเนินการให้แน่ใจว่าบุคลากรที่เกี่ยวข้องดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

หากเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้นมีลักษณะเป็นภัยคุกคามถาวร หรือภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่อง (เช่น มีแฮกเกอร์หรือไวรัสทำการโจมตีระบบสารสนเทศของบริษัทฯ) หรือเป็นกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล นอกเหนือจากการดำเนินการข้างต้น ฝ่ายจัดการสถานการณ์จะต้องดำเนินการให้แน่ใจว่าบุคลากรที่เกี่ยวข้องกำหนดมาตรการที่เหมาะสมเพื่อป้องกัน ระงับ หรือแก้ไข เพื่อให้เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้นสิ้นสุด หรือไม่ให้เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้นส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีตามที่จำเป็นและเหมาะสม

(4) **การจัดทำบันทึกการจัดการเหตุการณ์:** ฝ่ายจัดการสถานการณ์ต้องจัดทำบันทึกขั้นตอนที่ตนได้ดำเนินการ ตั้งแต่มีการพบเหตุการณ์ ไปจนถึงการชี้แจง และการแก้ไขเหตุการณ์นั้น

(5) **การเก็บหลักฐาน:** ในการตรวจสอบนั้น ฝ่ายจัดการสถานการณ์จะต้องจัดให้มีมาตรการที่เหมาะสมในการเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้อง ซึ่งรวมถึง:

- การระงับ การลบ หรือทำลายข้อมูล (รวมทั้งแฟ้มบันทึกข้อมูลอัตโนมัติ การเขียนทับลงบนเทปสำรองข้อมูล หรือการนำข้อมูลกลับมาใช้ใหม่)
- การออกคำสั่งให้บุคลากรที่สามารถเข้าถึงระบบได้ ใช้ความระมัดระวังไม่ให้ลบ แก้ไข หรือทำให้ข้อมูล และหลักฐานที่เกี่ยวข้องได้รับความเสียหาย
- การเก็บรหัส หรือมัลแวร์ที่ต้องสงสัย และ
- การดำเนินการตามกฎหมายที่เกี่ยวข้องตามนโยบายหรือขั้นตอนปฏิบัติของบริษัทฯ (ในกรณีที่เกี่ยวข้อง)

(6) **ผู้ตรวจสอบทางนิติวิทยาศาสตร์:** ฝ่ายจัดการสถานการณ์จะพิจารณาเป็นรายกรณีว่าจำเป็นต้องให้ผู้ตรวจสอบ / บริษัทตรวจสอบทางนิติวิทยาศาสตร์ เข้ามาบันทึกภาพอุปกรณ์ที่ได้รับผลกระทบ ทำการตรวจสอบทางนิติวิทยาศาสตร์กับคอมพิวเตอร์ หรือให้บริการอื่น ๆ หรือไม่ ซึ่งการตรวจสอบทางนิติวิทยาศาสตร์จะถูกควบคุมการ

ดำเนินการโดยสำนักกรรมการผู้จัดการและกฎหมายหรือที่ปรึกษาทางกฎหมายจากภายนอกที่คอยให้คำปรึกษาและคำแนะนำทางกฎหมายแก่บริษัทฯ หากคาดว่าจะต้องมีการดำเนินคดี สืบสวนสอบสวนทางกฎหมาย หรือการตรวจสอบภายในองค์กร

(7) **การรักษาความลับ:** ฝ่ายจัดการสถานการณ์จะประสานงานร่วมกับฝ่ายอื่น ๆ เพื่อให้แน่ใจว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลจะถูกเก็บไว้เป็นความลับ จนกว่าจะมีการตัดสินใจเกี่ยวกับการชี้แจงหรือการเปิดเผยข้อมูล นอกจากนี้ จะต้องจำกัดจำนวนบุคลากรที่ทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลให้น้อยที่สุดเท่าที่จะทำได้ เพื่อป้องกันการรั่วไหลของข้อมูล

(8) **การตรวจสอบขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล:** ฝ่ายจัดการสถานการณ์จะตรวจสอบและรวบรวมข้อมูลที่เกี่ยวข้องกับขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล ซึ่งรวมถึงข้อมูลดังต่อไปนี้ตามความสมควร

- เวลา ลักษณะ และประเภทของการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล
- ลักษณะและจำนวนของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้น
- ข้อมูลเกี่ยวกับมาตรการที่บริษัทฯ ใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล หรือเยียวยาความเสียหาย ซึ่งอาจเป็นมาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใด
- รายชื่อผู้ที่ทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าว ไม่ว่าจะเป็นบุคลากรภายในหรือภายนอกบริษัทฯ

รายการตรวจสอบเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่ฝ่ายจัดการสถานการณ์อาจนำมาใช้ในการตรวจสอบ มีดังนี้

- ลักษณะของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่ทราบเป็นอย่างไร (เช่น การเจาะระบบข้อมูล การสูญหายของอุปกรณ์ การโจรกรรมโดยบุคคลภายใน หรือเหตุการณ์อื่น ๆ ที่มีลักษณะคล้ายกัน) และฝ่ายจัดการสถานการณ์ทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยทางข้อมูลนี้ได้อย่างไร
- ลักษณะของข้อมูลที่ได้รับผลกระทบเป็นอย่างไร ขอบข่ายของข้อมูลที่ได้รับผลกระทบ มีข้อมูลที่อาจก่อให้เกิดหน้าที่ในการแจ้งเตือนการละเมิด หรือหน้าที่อื่นตามกฎหมายหรือตามสัญญาหรือไม่
- บุคคลที่อาจได้รับผลกระทบเป็นบุคคลประเภทใดบ้าง (เช่น ลูกค้า พันธมิตรทางธุรกิจ พนักงาน หรือบุคคลประเภทอื่น ๆ)
- ที่อยู่ของผู้ที่อาจได้รับผลกระทบดังกล่าว (เช่น เฉพาะผู้ที่อยู่ในประเทศไทยเท่านั้น หรือรวมถึงผู้ที่อยู่ในประเทศอื่นด้วย)
- เราสามารถประเมินประเภทและจำนวนข้อมูลส่วนบุคคลที่ได้รับผลกระทบได้หรือไม่

- ขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลครอบคลุมเพียงใด หากเหตุการณ์ดังกล่าวเกี่ยวข้องกับการบุกรุกระบบสารสนเทศโดยไม่ได้รับอนุญาตแล้วนั้น มีเครื่องโฮสต์ใดบ้างที่อาจถูกเข้าถึง และมีข้อมูลใดบ้างที่อยู่ในเครื่องเหล่านั้น ตลอดจนผู้บุกรุกใช้วิธีการใดในการเข้าถึง
- สื่อได้รับทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลแล้วหรือไม่
- ขณะนี้มีมาตรการใดบ้างเพื่อรักษาความปลอดภัยของระบบโดยไม่ทำลายหลักฐานทางอิเล็กทรอนิกส์ที่สำคัญ (เช่น การตัดการเชื่อมต่อเครื่องแม่ข่าย (server) ที่มีข้อมูลส่วนบุคคลออกจากอินเทอร์เน็ตหรือกรณีอื่น ๆ ที่คล้ายกัน หรือมีการบันทึกภาพอุปกรณ์ที่อาจได้รับผลกระทบแล้วหรือไม่)
- ใครเป็นผู้ทำหน้าที่จัดการด้านเทคนิคและความมั่นคงปลอดภัยของเหตุการณ์ด้านความมั่นคงปลอดภัย และ บริษัทฯ ได้มีการว่าจ้างบริษัทเทคโนโลยีสารสนเทศ / นิติวิทยาศาสตร์เพื่อดำเนินการเช่นว่าแล้วหรือไม่
- มีบุคลากรอื่นใดในบริษัทฯ ที่ควรทราบเหตุการณ์ดังกล่าวหรือไม่ (เช่น ผู้บริหารอาวุโส ฝ่ายบริหารความสัมพันธ์ภายนอกองค์กร ฯลฯ)
- ได้มีการติดต่อหน่วยงานผู้บังคับใช้กฎหมายแล้วหรือไม่ หากได้มีการติดต่อแล้ว ติดต่อไปยังหน่วยงานใดบ้าง และใครเป็นผู้ที่ติดต่อไป

(9) **การรายงานต่อหน่วยงานผู้บังคับใช้กฎหมาย:** เพื่อเป็นส่วนหนึ่งของการตรวจสอบ ในกรณีที่มีการเข้าถึงข้อมูลหรือระบบสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาต ฝ่ายจัดการสถานการณ์จะต้องพิจารณาว่ามีความจำเป็น หรือสมควรต้องรายงานต่อหน่วยงานผู้บังคับใช้กฎหมายหรือไม่

(10) **การพิจารณาข้อกำหนดทางกฎหมายที่ใช้บังคับ**

สำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก จะต้องใช้ขั้นตอนปฏิบัติการวิเคราะห์ใน*ภาคผนวก 3* เพื่อให้คำแนะนำแก่ฝ่ายจัดการสถานการณ์ว่ามีกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลใดบ้างที่อาจใช้บังคับกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนี้ (“**สรุปสาระสำคัญของกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล**”) (ดู*ภาคผนวก 2*) และให้คำแนะนำว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าวถือว่าเป็นการละเมิดความมั่นคงปลอดภัยของข้อมูลจะที่ต้องแจ้งไปยังบุคคลผู้ได้รับผลกระทบ หน่วยงานรัฐบาล/หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูล หรือบุคคลอื่น ๆ หรือไม่

ฝ่ายจัดการสถานการณ์จะต้องให้ข้อมูลตามความเป็นจริง ตามที่ สำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก ร้องขอ เพื่อให้ สำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก สามารถทำการประเมินและให้ความเห็นทางกฎหมายที่จำเป็นได้

(11) **การพิจารณาข้อกำหนดอื่น ๆ**

นอกจากนี้ สำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก สามารถให้คำแนะนำแก่ฝ่ายจัดการสถานการณ์เกี่ยวกับข้อกำหนดอื่น ๆ ที่นอกเหนือจากกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่อาจกำหนดให้ต้องมีการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลก็ได้ ซึ่งรวมถึงข้อกำหนดดังนี้

- กฎหมาย และระเบียบเฉพาะของแต่ละภาคธุรกิจ / อุตสาหกรรมที่อาจนำมาใช้บังคับต่อเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

- หน้าที่ตามสัญญาที่มีต่อพันธมิตรทางธุรกิจ หรือบุคคลอื่น ๆ
- นโยบายความเป็นส่วนตัว ประกาศหรือแถลงการณ์อื่น ๆ ในเอกสารที่เกี่ยวข้องกับการชี้แจงทั้งภายในและนอกองค์กร
- คำมั่นที่ไม่มีผลผูกพัน นโยบายหรือขั้นตอนปฏิบัติของบริษัทฯ ที่มีการเผยแพร่ต่อสาธารณะ

(12) **การรายงานต่อหน่วยงานรัฐบาล บุคคล หรือฝ่ายอื่น ๆ**

ก.) **เนื้อหาในรายงาน คำชี้แจง และบทพูดสำหรับตอบคำถาม:** ฝ่ายจัดการสถานการณ์ควรประสานงานกับสำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก เพื่อกำหนดถ้อยคำและวิธีการเผยแพร่รายงาน คำชี้แจง และบทพูดสำหรับตอบคำถามเพื่อให้เป็นไปตามข้อกำหนด

หากฝ่ายจัดการสถานการณ์ตัดสินใจใช้บุคลากรของบริษัทฯ หรือให้ศูนย์คอลเซ็นเตอร์จากภายนอกเป็นผู้ตอบคำถาม ซึ่งเป็นคำถามจากผู้ได้รับผลกระทบที่อาจมีข้อสงสัยเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลหรือเรื่องอื่น ๆ ที่เกี่ยวข้อง ฝ่ายจัดการสถานการณ์ต้องจัดทำบทพูดให้บุคลากรประจำศูนย์คอลเซ็นเตอร์ หรือฝ่ายติดต่อของบริษัทฯ ที่ได้รับมอบหมาย ในการชี้แจงให้ผู้ที่ได้รับผลกระทบทราบ

ข.) **รูปแบบของคำชี้แจง** หากกฎหมายที่ใช้บังคับในขณะนั้นไม่ได้กำหนดรูปแบบการชี้แจงไปยังบุคคลผู้ได้รับผลกระทบไว้เป็นการเฉพาะ บริษัทฯ อาจพิจารณาวิธีการดังต่อไปนี้

- **สำหรับผู้ที่ได้ให้ที่อยู่อีเมลไว้แก่บริษัทฯ** ฝ่ายจัดการสถานการณ์จะต้องมีการส่งคำชี้แจงทางอีเมลไปยังผู้ที่ได้รับผลกระทบทุกราย พร้อมขอให้มีการตอบรับ
- **สำหรับผู้ที่ให้ที่อยู่ทางไปรษณีย์ไว้แก่บริษัทฯ** โดยไม่มีที่อยู่อีเมล ฝ่ายจัดการสถานการณ์จะต้องมีการส่งคำชี้แจงไปยังผู้ที่ได้รับผลกระทบดังกล่าวผ่านทางไปรษณีย์ลงทะเบียนตอบรับ
- **สำหรับผู้ที่ไม่ได้ให้ช่องทางการติดต่อใด ๆ ไว้แก่บริษัทฯ** ฝ่ายจัดการสถานการณ์จะต้องมีการส่งคำชี้แจงไปยังบุคคลผู้ได้รับผลกระทบเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่บุคคลผู้ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้ ทั้งนี้ ต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบเพิ่มเติมต่อบุคคลผู้ได้รับผลกระทบดังกล่าว

ฝ่ายจัดการสถานการณ์จะต้องประสานงานกับ สำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก เพื่อกำหนดรูปแบบที่เหมาะสมในการส่งคำชี้แจง โดยพิจารณาจากกฎหมายที่ใช้บังคับและค่าใช้จ่ายที่เกี่ยวข้อง

หากไม่สามารถทำการชี้แจงตามข้อนี้ได้ ฝ่ายจัดการสถานการณ์ควรปรึกษา สำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก โดยทันที เพื่อพิจารณาวิธีการชี้แจงอื่น ๆ แทน ทั้งนี้ ฝ่ายจัดการสถานการณ์อาจชะลอการส่งคำชี้แจงไว้หากหน่วยงานผู้บังคับใช้กฎหมายเห็นว่าการชี้แจงไปยังผู้ที่ได้รับผลกระทบนั้นอาจเป็นอุปสรรคต่อการสืบสวน

(13) **การตอบคำถาม:** ฝ่ายจัดการสถานการณ์ต้องมีการวางแผนว่าบริษัทฯ ควรมีวิธีการในการตอบข้อซักถามจากสื่อมวลชน รัฐบาล หรือบุคคลอื่น ๆ อย่างไร โดยในกรณีส่วนใหญ่ ฝ่ายจัดการสถานการณ์ควรส่งข้อซักถามนั้นไปยัง [ฝ่ายกฎหมาย หรือฝ่ายประชาสัมพันธ์] โดยตรงก่อน เพื่อวิเคราะห์และจัดเตรียมแนวทางในการตอบ

ระยะที่ 3: มาตรการหลังเกิดเหตุการณ์

(14) **ข้อกำหนดเรื่องการจัดทำบันทึกเอกสาร:** ไม่ว่าจะมีการพิจารณาให้นำกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลมาใช้บังคับกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลหรือไม่ก็ตาม ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำเอกสารบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่ง ควรมีการบันทึกผลการประเมินที่ทำให้บริษัทฯ พิจารณาไม่นำกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมาใช้บังคับ

(15) **มาตรการเพื่อการแก้ไข:** ฝ่ายจัดการสถานการณ์จะต้องประสานงานกับสำนักกรรมการผู้จัดการและกฎหมาย หรือที่ปรึกษาทางกฎหมายจากภายนอก เพื่อกำหนดมาตรการทางเทคนิค และทางองค์กรที่จำเป็น เพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลในลักษณะที่คล้ายกันอีกในอนาคต ซึ่งรวมถึงการพิจารณาทบทวนขั้นตอนปฏิบัติ การฝึกอบรมเพื่อสร้างความเข้าใจ การกำหนดกระบวนการสำหรับบุคลากร นอกจากนี้ ฝ่ายจัดการสถานการณ์ควรประเมินความสัมพันธ์กับบุคคลภายนอกที่อาจเกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล และดำเนินการต่าง ๆ ตามความเหมาะสม เช่น การแก้ไขสัญญา การแก้ไขกระบวนการต่าง ๆ การฝึกอบรม การปรับปรุงมาตรการความปลอดภัย และ/หรือ การเลือกพันธมิตรทางธุรกิจรายใหม่ เป็นต้น ขณะเดียวกันบุคคลภายนอกจะต้องมีหน้าที่ตามสัญญาที่จะต้องแจ้งให้บริษัทฯ ทราบโดยทันที ทั้งนี้ ภายในระยะเวลาและพร้อมด้วยรายละเอียดข้อมูลเบื้องต้นตามที่กฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลกำหนด หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล ไม่ว่าจะเป็นเหตุการณ์ที่เกิดขึ้นจริงหรือสงสัยว่าจะเกิดขึ้นก็ตาม และคู่สัญญาของบริษัทฯ ควรให้คำแนะนำแก่ สำนักกรรมการผู้จัดการและกฎหมาย หรือ ที่ปรึกษาทางกฎหมายจากภายนอก หากต้องมีการปรับเปลี่ยนกระบวนการต่าง ๆ ที่เกี่ยวข้องกับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

(16) **การทบทวนหน้าที่ตามกรมธรรม์ประกันภัย:** ฝ่ายจัดการสถานการณ์จะต้องทบทวนกรมธรรม์ประกันภัยที่เกี่ยวข้องของบริษัทฯ เพื่อพิจารณาว่าควรแจ้งให้บริษัทประกันภัยทราบตามข้อกำหนดในกรมธรรม์ประกันภัยที่ยังคงมีผลบังคับหรือไม่ รวมถึงข้อกำหนดในเรื่องเวลา เนื้อหา และรูปแบบของคำชี้แจงด้วย

วันที่มีผลบังคับ: 1 พฤศจิกายน 2568

ประกาศ ณ วันที่ 1 พฤศจิกายน พ.ศ. 2568

นายเอกชัย ยิ้มสกุล

กรรมการผู้จัดการ

ภาคผนวก 1

แบบฟอร์มการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

กรุณากรอกรายละเอียดด้านล่าง และส่งอีเมลไปยังฝ่ายจัดการสถานการณ์ที่ PDPA@arunplus.com

คำอธิบายลักษณะและประเภทของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล	
วันและเวลาที่พบเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล	
ผู้ที่ระบุเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล	ชื่อ: ตำแหน่ง: ส่วนงาน: ประเทศ: ที่อยู่อีเมล: หมายเลขโทรศัพท์:
บุคลากรที่รายงาน:	☐ เป็นบุคคลเดียวกับผู้ที่ระบุเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล ชื่อ: ตำแหน่ง: ส่วนงาน: ประเทศ: ที่อยู่อีเมล: หมายเลขโทรศัพท์:
ระบบที่อาจหรือได้รับผลกระทบ	
ลักษณะของบุคคลที่อาจหรือได้รับผลกระทบ (เช่น ลูกค้า พันธมิตรทางธุรกิจ บุคคลทั่วไป พนักงาน ผู้เยาว์ ผู้พิการ)	
จำนวนของบุคคลที่อาจหรือได้รับผลกระทบ	
ลักษณะของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	
จำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	
ผลกระทบที่เกิดขึ้นหรืออาจเกิดขึ้น	
รายชื่อผู้ที่ได้รับรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล	

มาตรการที่ได้ใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล หรือเยียวยาความเสียหาย ซึ่งอาจเป็นมาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใด	