ORNSIRIN

นโยบายการรายงานและจัดการกรณีเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

1. วัตถุประสงค์

นโยบายการรายงานและจัดการกรณีเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล (“นโยบาย”) ฉบับนี้มีวัตถุประสงค์เพื่อเป็นแนวทางการจัดการที่บริษัท อรสิริน โฮลดิ้ง จำกัด (มหาชน) และกลุ่มบริษัทย่อย (รวมเรียกว่า “กลุ่มบริษัทอรสิริน”) ควรปฏิบัติตามเมื่อเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล (ตามคำนิยามด้านล่าง) ทั้งที่เกิดขึ้นจริงมีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น ซึ่งอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล

2. ขอบเขตของนโยบาย

นโยบายฉบับนี้ใช้บังคับกับพนักงาน ผู้รับจ้าง ตัวแทน ผู้แทน นักศึกษาฝึกงาน ตลอดจนบุคลากรประเภทอื่น ๆ ของกลุ่มบริษัทอรสิริน นอกจากนี้ กลุ่มบริษัทอรสิริน ยังกำหนดให้พันธมิตรทางธุรกิจ คู่ค้า หรือผู้ให้บริการ ซึ่งรวมถึงพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน ผู้แทน และบุคลากรอื่น ๆ ของพันธมิตรทางธุรกิจ คู่ค้า หรือผู้ให้บริการดังกล่าว ซึ่งต้องเก็บรวบรวม เข้าถึง จัดเก็บ หรือจัดการข้อมูลส่วนบุคคลในนามของกลุ่มบริษัทอรสิริน (ซึ่งต่อไปนี้จะเรียกรวมกันว่า “พนักงาน / ผู้รับจ้าง”) ต้องปฏิบัติตามนโยบายนี้ด้วย ทั้งนี้ นโยบายฉบับนี้จะไม่ก่อให้เกิดสิทธิใดๆ แก่พนักงาน / ผู้รับจ้าง หรือสิทธิใดๆ นอกเหนือหน้าที่ของกลุ่มบริษัทอรสิริน ภายใต้กฎหมายที่ใช้บังคับ นโยบายนี้เป็นเอกสารภายในของกลุ่มบริษัทอรสิริน และมิได้ก่อให้เกิดสิทธิหรือสิทธิพิเศษใด ๆ แก่บุคคลภายนอก

ผู้ที่ฝ่าฝืนนโยบายฉบับนี้อาจได้รับโทษทางวินัย ซึ่งอาจรวมถึงการเลิกจ้าง หรืออาจส่งผลให้มีการเลิกสัญญากับพันธมิตรทางธุรกิจ คู่ค้า หรือผู้ให้บริการได้

กลุ่มบริษัทอรสิรินอาจปรับปรุงแก้ไขนโยบายนี้เป็นครั้งคราว โดยจะแจ้งให้พนักงาน / ผู้รับจ้างทราบตามความเหมาะสม

3. ข้อกำหนดในการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

3.1 การติดต่อฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูล: พนักงาน / ผู้รับจ้างรายใดที่พบเห็น สงสัย หรือทราบถึงเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลที่ได้เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น จะต้องรายงานประเด็นดังกล่าวให้ฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูลทราบโดยทันที (สามารถดูข้อมูลการติดต่อของฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูลได้ที่ ข้อ 3.4 ของนโยบายฉบับนี้) โดยใช้แบบฟอร์มการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ที่อยู่ใน ภาคผนวก 1

3.2 เหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล: เหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลคือเหตุการณ์ใด ๆ ทั้งที่เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น หรือการกระทำ ความขัดข้อง หรือเหตุการณ์อื่นใดที่ก่อให้เกิดการทำลาย การสูญหาย การเปลี่ยนแปลงของข้อมูลที่กลุ่มบริษัทอรสิริน เป็นเจ้าของ ควบคุม หรือเก็บรักษาไว้ ไม่ว่าจะโดยตรงหรือโดยอ้อม (เช่น ข้อมูลที่อยู่ภายใต้การดูแลของคู่ค้า / พันธมิตรทางธุรกิจ หรือผู้ให้บริการภายนอกอื่นที่ให้บริการแก่กลุ่มบริษัทอรสิริน) ไม่ว่าจะโดยอุบัติเหตุ โดยเจตนา หรือโดยมิชอบด้วยกฎหมาย หรือก่อให้เกิดการได้รับ การเปิดเผย หรือการเข้าถึงเอกสารกระดาษหรือข้อมูลทางอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับหรือไม่ก็ตาม ซึ่งข้อมูลดังกล่าวอาจอยู่ในแฟ้มเอกสารกระดาษ อีเมล ตาราง บันทึกบุคลากร บันทึกบัญชีเงินเดือน เครื่องแม่ข่าย (เซิร์ฟเวอร์) อุปกรณ์จัดเก็บข้อมูลแบบพกพา (เช่น คอมพิวเตอร์ แล็ปท็อป หรือโทรศัพท์สมาร์ทโฟน) และฐานข้อมูลไอที เป็นต้น

เหตุการณ์ต่อไปนี้เป็นเพียงตัวอย่างเหตุการณ์บางส่วน ซึ่งโดยลักษณะจะต้องรายงานให้ฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูลทราบ

- การโจรกรรมหรือการสูญหายของเครื่องคอมพิวเตอร์ คอมพิวเตอร์ แล็ปท็อป โทรศัพท์สมาร์ทโฟน อุปกรณ์บันทึกข้อมูลแบบธัมบ์ไดรฟ์ อุปกรณ์บันทึกข้อมูลแบบพกพา (External Hard Drive) หรืออุปกรณ์บันทึกข้อมูลอื่นที่เป็นของกลุ่มบริษัทอรสิริน หรือพนักงาน / ผู้รับจ้างที่ใช้อุปกรณ์ดังกล่าวบันทึกข้อมูลที่เกี่ยวข้องกับกลุ่มบริษัทอรสิริน
- การบุกรุกหรือการโจรกรรมภายในสถานที่ของกลุ่มบริษัทอรสิริน

• ผู้โจมตีก่อให้เกิดความเสี่ยงต่อระบบของกลุ่มบริษัทอรสิริน เช่น ฐานข้อมูล คอมพิวเตอร์ เครือข่ายการสื่อสารของกลุ่มบริษัทอรสิริน

• เมื่อพนักงาน / ผู้รับจ้างได้เห็น เข้าถึง หรือเปิดเผยข้อมูล แฟ้มข้อมูล หรือฐานข้อมูลที่อยู่นอกขอบเขตหน้าที่ที่ได้รับมอบหมาย

• เมื่อมีบุคคลภายนอกกระทำผิดสัญญาการห้ามเปิดเผยข้อมูล หรือสัญญาการรักษาความลับ

• เหตุการณ์ตามที่กล่าวมาข้างต้น ซึ่งเกี่ยวข้องกับคู่ค้าหรือผู้ให้บริการอื่น ๆ ของกลุ่มบริษัทอรสิริน

3.3 ความร่วมมือ: พนักงาน / ผู้รับจ้างจะต้องให้ความร่วมมือกับกลุ่มบริษัทอรสิริน และฝ่ายจัดการสถานการณ์ในการตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

3.4 ฝ่ายจัดการสถานการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

ฝ่ายจัดการณ์สถานการณ์	
ข้อมูลการติดต่อ	ที่อยู่อีเมล: PDPA@ornsiril.co.th หมายเลขโทรศัพท์: 053-295709
สมาชิก	
ผู้จัดการเหตุการณ์ลำดับแรก	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คุณนงนุช เกษร เบอร์โทรศัพท์ 085-7047235
ฝ่ายเทคโนโลยีสารสนเทศ	คุณกาญจนา ศรีวิชัย เบอร์โทรศัพท์ 094-6344490
ฝ่ายกฎหมาย	
ฝ่ายทรัพยากรบุคคล	คุณชาญณรงค์ ตุ่นแก้ว เบอร์โทรศัพท์ 085-9519995
ฝ่ายบัญชี	คุณฉัตรชัยยงค์ บุญขวาง เบอร์โทรศัพท์ 087-7270324

3.5 ความพร้อมของฝ่ายจัดการสถานการณ์: ฝ่ายจัดการสถานการณ์จะต้องมีการเฝ้าสังเกตการณ์ เพื่อเฝ้าระวังตลอด 24 ชั่วโมง โดยสามารถติดต่อได้ที่ Email : Nongnuch.t@ornsirin.co.th หมายเลขโทรศัพท์ 097-9695164 เพื่อให้ผู้จัดการเหตุการณ์ลำดับแรกสามารถรับรายงานได้โดยทันที

4. ขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

ระยะที่ 1: การรายงานและยืนยันเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลภายในองค์กร

วัตถุประสงค์ของระยะที่ 1 คือ เพื่อระบุและยืนยันได้อย่างทันท่วงทีว่ามีเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลเกิดขึ้นจริงหรือไม่ และรายงานต่อไปยังฝ่ายจัดการสถานการณ์

4.1 การตรวจสอบเบื้องต้น: ฝ่ายจัดการสถานการณ์จะระบุผู้ที่ได้รับมอบหมายให้ทำการสืบสวนและตรวจสอบในเบื้องต้นสำหรับแต่ละเหตุการณ์ที่ได้รับรายงาน (“ผู้จัดการเหตุการณ์ลำดับแรก”)

โดยผู้จัดการเหตุการณ์ลำดับแรกจะต้องประสานงานกับพนักงาน / ผู้รับจ้าง ซึ่งเป็นผู้รายงานเหตุการณ์ และขอข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลให้ได้มากที่สุดเท่าที่มีอยู่ในเวลานั้น ทั้งนี้ หากเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่เกิดขึ้นเกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือเกี่ยวกับความมั่นคงปลอดภัยของคอมพิวเตอร์อื่น ๆ ผู้จัดการเหตุการณ์ลำดับแรกจะต้องประสานงานกับฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายจัดการสถานการณ์ด้วย นอกจากนี้ ผู้จัดการเหตุการณ์ลำดับแรกควรพิจารณาในเบื้องต้นโดยเร็วที่สุดและภายในระยะเวลา 24 ชั่วโมงแรกว่าจากข้อมูลที่มีอยู่นั้นมีมูลเหตุอันควรเชื่อได้ว่าเหตุการณ์ดังกล่าวได้เกิดขึ้นจริงหรือไม่ หากขณะนั้นไม่มีมูลเหตุอันสมควร ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นการภายในโดยระบุข้อมูลดังนี้

- ชื่อของพนักงาน / ผู้รับจ้างที่รายงานเหตุการณ์
- คำอธิบายสถานการณ์ของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่มีการรายงาน
- คำอธิบายถึงสาเหตุที่ผู้จัดการเหตุการณ์ลำดับแรกพิจารณาแล้วเห็นว่า เหตุการณ์ดังกล่าวไม่มีมูลเหตุอันควรเชื่อได้ว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลอาจเกิดขึ้น หรือได้เกิดขึ้นไปแล้ว

ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นลายลักษณ์อักษรไปยังสมาชิกรายอื่น ๆ ของฝ่ายจัดการสถานการณ์ทันทีที่ได้รับข้อมูลที่เพียงพอ

4.2 การยืนยันเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล: หากผู้จัดการเหตุการณ์ลำดับแรกพิจารณาแล้วเห็นว่า มีมูลเหตุอันควรเชื่อได้ว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าวได้เกิดขึ้นจริง ผู้จัดการเหตุการณ์ลำดับแรกจะต้องแจ้งให้สมาชิกรายอื่น ๆ ของฝ่ายจัดการสถานการณ์ทราบโดยทันที เพื่อเริ่มดำเนินการระยะที่ 2 ต่อไปทันที

ระยะที่ 2: การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

วัตถุประสงค์ของระยะที่ 2 คือ เพื่อจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลทั้งในระดับภายในและภายนอกองค์กร ในระยะนี้จะต้องมีการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลโดยเร็วที่สุดเท่าที่จะทำได้ เพื่อให้กลุ่มบริษัทอรสิริน สามารถทำการแจ้งเตือนที่จำเป็นได้ทันเวลาในกรณีที่ฝ่ายจัดการสถานการณ์เห็นว่าต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้นให้หน่วยงานรัฐบาล บุคคล หรือผู้ใดก็ตามทราบตามที่กฎหมายกำหนด

ในขณะเดียวกัน ฝ่ายจัดการสถานการณ์จะต้องดำเนินการอื่น ๆ ที่จำเป็นไปพร้อม ๆ กันเพื่อควบคุมเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล และลดความเสี่ยง รวมทั้งความเสียหายลงให้ได้มากที่สุด

4.3. การควบคุมภัยคุกคาม: หากเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้นมีลักษณะเป็นภัยคุกคามถาวร หรือภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่อง (เช่น มีแฮกเกอร์หรือไวรัสทำการโจมตีระบบสารสนเทศของกลุ่มบริษัทอรสิริน) ฝ่ายจัดการสถานการณ์จะต้องดำเนินการให้แน่ใจว่าบุคลากร ฝ่ายเทคโนโลยีสารสนเทศ กำหนดมาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัย และแยกภัยคุกคามออกไปไม่ให้สร้างความเสียหายต่อสภาพแวดล้อมทางเทคนิคของกลุ่มบริษัท
อรสิริน ต่อไปได้

4.4 การจัดทำบันทึกการจัดการเหตุการณ์: ฝ่ายจัดการสถานการณ์ต้องจัดทำบันทึกขั้นตอนที่ตนได้ดำเนินการ ตั้งแต่มีการพบเหตุการณ์ ไปจนถึงการชี้แจง และการแก้ไขเหตุการณ์นั้น

4.5 การเก็บหลักฐาน: ในการตรวจสอบนั้น ฝ่ายจัดการสถานการณ์จะต้องจัดให้มีมาตรการที่เหมาะสมในการเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้อง ซึ่งรวมถึง:

- การระงับ การลบ หรือทำลายข้อมูล (รวมทั้งแฟ้มบันทึกข้อมูลอัตโนมัติ การเขียนทับลงบนเทปสำรองข้อมูล หรือการนำข้อมูลกลับมาใช้ใหม่)
- การออกคำสั่งให้พนักงาน / ผู้รับจ้างที่สามารถเข้าถึงระบบได้ ใช้ความระมัดระวังไม่ให้ลบ แก้ไข หรือทำให้ข้อมูลและหลักฐานที่เกี่ยวข้องได้รับความเสียหาย
- การเก็บรหัส หรือมัลแวร์ที่ต้องสงสัย และ
- การดำเนินการตามกฎหมายที่เกี่ยวข้องตามนโยบายของกลุ่มบริษัทอรสิริน (ในกรณีที่เกี่ยวข้อง)

4.6 ผู้ตรวจสอบทางนิติวิทยาศาสตร์: ฝ่ายจัดการสถานการณ์จะพิจารณาเป็นรายกรณีว่าจำเป็นต้องให้ผู้ตรวจสอบ / บริษัทตรวจสอบทางนิติวิทยาศาสตร์ เข้ามาบันทึกภาพอุปกรณ์ที่ได้รับผลกระทบ ทำการตรวจสอบทางนิติวิทยาศาสตร์กับคอมพิวเตอร์ หรือให้บริการอื่น ๆ หรือไม่ ซึ่งการตรวจสอบทางนิติวิทยาศาสตร์จะถูกควบคุมการดำเนินการโดย ฝ่ายกฎหมาย หรือที่ปรึกษาทางกฎหมายจากภายนอกที่คอยให้คำปรึกษาและคำแนะนำทางกฎหมายแก่กลุ่มบริษัทอรสิริน หากคาดว่าจะต้องมีการดำเนินคดี สืบสวนสอบสวนทางกฎหมาย หรือการตรวจสอบภายในองค์กร

4.7 การรักษาความลับ: ฝ่ายจัดการสถานการณ์จะประสานงานร่วมกับฝ่ายอื่น ๆ เพื่อให้แน่ใจว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลจะถูกเก็บไว้เป็นความลับ จนกว่าจะมีการตัดสินใจเกี่ยวกับการชี้แจงหรือการเปิดเผยข้อมูล นอกจากนี้จะต้องจำกัดจำนวนพนักงาน / ผู้รับจ้างที่ทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลให้น้อยที่สุดเท่าที่จะทำได้ เพื่อป้องกันการรั่วไหลของข้อมูล

4.8 การตรวจสอบขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล: ฝ่ายจัดการสถานการณ์จะตรวจสอบและรวบรวมข้อมูลที่เกี่ยวข้องกับขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล ซึ่งรวมถึงข้อมูลดังต่อไปนี้ตามความสมควร

- เวลาและลักษณะการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล
- ประเภทของข้อมูลส่วนบุคคลที่อาจเสี่ยงต่อการได้รับผลกระทบ
- ความเสี่ยงที่จะเกิดความเสียหายหรือการใช้งานในทางที่ผิด และ
- รายชื่อผู้ที่ทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าว ไม่ว่าจะเป็นบุคลากรภายในหรือภายนอกกลุ่มบริษัทอรสิริน

รายการตรวจสอบเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่ฝ่ายจัดการสถานการณ์อาจนำมาใช้ในการตรวจสอบ มีดังนี้

- ลักษณะของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลที่ทราบเป็นอย่างไร (เช่น การเจาะระบบข้อมูล การสูญหายของอุปกรณ์ การโจรกรรมโดยบุคคลภายใน หรือเหตุการณ์อื่น ๆ ที่มีลักษณะคล้ายกัน) และฝ่ายจัดการสถานการณ์ทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยทางข้อมูลนี้ได้อย่างไร
- ลักษณะของข้อมูลที่ได้รับผลกระทบเป็นอย่างไร ขอบข่ายของข้อมูลที่ได้รับผลกระทบ มีข้อมูลที่อาจก่อให้เกิดหน้าที่ในการแจ้งเตือนการละเมิด หรือหน้าที่อื่นตามกฎหมายหรือตามสัญญาหรือไม่
- บุคคลที่อาจได้รับผลกระทบเป็นบุคคลประเภทใดบ้าง (เช่น ลูกค้า ลูกจ้าง หรือบุคคลประเภทอื่น ๆ)
- ที่อยู่ของผู้ที่อาจได้รับผลกระทบดังกล่าว (เช่น เฉพาะผู้ที่อยู่ในประเทศไทยเท่านั้น หรือรวมถึงผู้ที่อยู่ในประเทศอื่นด้วย)
- เราสามารถประเมินประเภทและจำนวนข้อมูลส่วนบุคคลที่ได้รับผลกระทบได้หรือไม่
- ขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลครอบคลุมเพียงใด หากเหตุการณ์ดังกล่าวเกี่ยวข้องกับการบุกรุกระบบสารสนเทศโดยไม่ได้รับอนุญาตแล้วนั้น มีเครื่องโฮสต์ใดบ้างที่อาจถูกเข้าถึง และมีข้อมูลใดบ้างที่อยู่ในเครื่องเหล่านั้น ตลอดจนผู้บุกรุกใช้วิธีการใดในการเข้าถึง
- สื่อได้รับทราบถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลแล้วหรือไม่
- ขณะนี้มีมาตรการใดบ้างเพื่อรักษาความปลอดภัยของระบบโดยไม่ทำลายหลักฐานทางอิเล็กทรอนิกส์ที่สำคัญ (เช่น การตัดการเชื่อมต่อเครื่องแม่ข่าย (server) ที่มีข้อมูลส่วนบุคคลออกจากอินเทอร์เน็ต หรือกรณีอื่น ๆ ที่คล้ายกัน หรือมีการบันทึกภาพอุปกรณ์ที่อาจได้รับผลกระทบแล้วหรือไม่)
- ใครเป็นผู้ทำหน้าที่จัดการด้านเทคนิคและความมั่นคงปลอดภัยของเหตุการณ์ด้านความมั่นคงปลอดภัย และกลุ่มบริษัทอรสิรินได้มีการว่าจ้างบริษัทเทคโนโลยีสารสนเทศ / นิติวิทยาศาสตร์เพื่อดำเนินการเช่นว่าแล้วหรือไม่
- มีบุคลากรอื่นใดในกลุ่มบริษัทอรสิริน ที่ควรทราบเหตุการณ์ดังกล่าวหรือไม่ (เช่น ผู้บริหารอาวุโส ฝ่ายบริหารความสัมพันธ์ภายนอกองค์กร ฯลฯ)
- ได้มีการติดต่อหน่วยงานผู้บังคับใช้กฎหมายแล้วหรือไม่ หากได้มีการติดต่อแล้ว ติดต่อไปยังหน่วยงานใดบ้างและใครเป็นผู้ที่ติดต่อไป

4.9 การรายงานต่อหน่วยงานผู้บังคับใช้กฎหมาย: เพื่อเป็นส่วนหนึ่งของการตรวจสอบ ในกรณีที่มีการเข้าถึงข้อมูลหรือระบบสารสนเทศของกลุ่มบริษัทอรสิริน โดยไม่ได้รับอนุญาต ฝ่ายจัดการสถานการณ์จะต้องพิจารณาว่ามีความจำเป็น หรือสมควรต้องรายงานต่อหน่วยงานผู้บังคับใช้กฎหมายหรือไม่

4.10 การพิจารณาข้อกำหนดทางกฎหมายที่ใช้บังคับ ฝ่ายกฎหมายจะต้องใช้แนวทางการวิเคราะห์ในภาคผนวก 3 เพื่อให้คำแนะนำแก่ฝ่ายจัดการสถานการณ์ว่ามีกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลใดบ้างที่อาจใช้บังคับกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนี้ (“สรุปสาระสำคัญของกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล”) (ดูภาคผนวก 2) และให้คำแนะนำว่าเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลดังกล่าวถือว่าเป็นการละเมิดความมั่นคงปลอดภัยของข้อมูลจะที่ต้องแจ้งไปยังบุคคลผู้ได้รับผลกระทบ หน่วยงานรัฐบาล / หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูล หรือบุคคลอื่น ๆ หรือไม่

ฝ่ายจัดการสถานการณ์จะต้องให้ข้อมูลตามความเป็นจริง ตามที่ ฝ่ายกฎหมาย ร้องขอ เพื่อให้ ฝ่ายกฎหมายสามารถทำการประเมินและให้ความเห็นทางกฎหมายที่จำเป็นได้

4.11 การพิจารณาข้อกำหนดอื่น ๆ

นอกจากนี้ ฝ่ายกฎหมายสามารถให้คำแนะนำแก่ฝ่ายจัดการสถานการณ์เกี่ยวกับข้อกำหนดอื่น ๆ ที่นอกเหนือจากกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่อาจกำหนดให้ต้องมีการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลก็ได้ ซึ่งรวมถึงข้อกำหนดดังนี้

- กฎหมาย และระเบียบเฉพาะของแต่ละภาคธุรกิจ / อุตสาหกรรมที่อาจนำมาใช้บังคับต่อเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล
- หน้าที่ตามสัญญาที่มีต่อพันธมิตรทางธุรกิจ หรือบุคคลอื่น ๆ
- นโยบายการคุ้มครองข้อมูลส่วนบุคคล ประกาศหรือแถลงการณ์อื่น ๆ ในเอกสารที่เกี่ยวข้องกับการชี้แจงทั้งภายในและนอกองค์กร
- คำมั่นที่ไม่มีผลผูกพัน หรือนโยบายของกลุ่มบริษัทอรสิริน ที่มีการเผยแพร่ต่อสาธารณะ

4.12 การรายงานต่อหน่วยงานรัฐบาล บุคคล หรือฝ่ายอื่น ๆ

(ก) เนื้อหาในรายงาน คำชี้แจง และบทพูดสำหรับตอบคำถาม: ฝ่ายจัดการสถานการณ์ควรประสานงานกับฝ่ายกฎหมาย เพื่อกำหนดถ้อยคำและวิธีการเผยแพร่รายงาน คำชี้แจง และบทพูดสำหรับตอบคำถามเพื่อให้เป็นไปตามข้อกำหนด

หากฝ่ายจัดการสถานการณ์ตัดสินใจใช้บุคลากรของกลุ่มบริษัทอรสิริน หรือให้ศูนย์คอลเซ็นเตอร์จากภายนอกเป็นผู้ตอบคำถาม ซึ่งเป็นคำถามจากผู้ได้รับผลกระทบที่อาจมีข้อสงสัยเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลหรือเรื่องอื่น ๆ ที่เกี่ยวข้อง ฝ่ายจัดการสถานการณ์ต้องจัดทำบทพูดให้บุคลากรประจำศูนย์คอลเซ็นเตอร์ หรือฝ่ายติดต่อของกลุ่มบริษัทอรสิริน ที่ได้รับมอบหมาย ในการชี้แจงให้ผู้ที่ได้รับผลกระทบทราบ

(ข) รูปแบบของคำชี้แจง หากกฎหมายที่ใช้บังคับในขณะนั้นไม่ได้กำหนดรูปแบบการชี้แจงไปยังบุคคลผู้ได้รับผลกระทบไว้เป็นการเฉพาะ กลุ่มบริษัทอรสิริน อาจพิจารณาวิธีการดังต่อไปนี้

- สำหรับผู้ที่ได้ให้ที่อยู่อีเมลไว้แก่กลุ่มบริษัทอรสิริน ฝ่ายจัดการสถานการณ์จะต้องมีการส่งคำชี้แจงทางอีเมลไปยังผู้ที่ได้รับผลกระทบทุกราย พร้อมขอให้มีการตอบรับ
- สำหรับผู้ที่ให้ที่อยู่ทางไปรษณีย์ไว้แก่กลุ่มบริษัทอรสิริน โดยไม่มีที่อยู่อีเมล ฝ่ายจัดการสถานการณ์จะต้องมีการส่งคำชี้แจงไปยังผู้ที่ได้รับผลกระทบดังกล่าวผ่านทางไปรษณีย์ลงทะเบียนตอบรับ

ฝ่ายจัดการสถานการณ์จะต้องประสานงานกับ ฝ่ายกฎหมาย เพื่อกำหนดรูปแบบที่เหมาะสมในการส่งคำชี้แจงโดยพิจารณาจากกฎหมายที่ใช้บังคับและค่าใช้จ่ายที่เกี่ยวข้อง อย่างไรก็ตาม นโยบายนี้ไม่ได้บังคับให้ต้องชี้แจงผ่านช่องทางสาธารณะอื่น ๆ ด้วย (เช่น ผ่านทางเว็บไซต์หรือสื่อมวลชนระดับประเทศ) เว้นแต่ กรณีที่กฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่มีอยู่ในขณะนั้นกำหนด หรือกรณีที่กลุ่มบริษัทอรสิริน พิจารณาแล้วเห็นว่าจะเป็นประโยชน์ในด้านลูกค้าสัมพันธ์ หรือเพื่อวัตถุประสงค์อื่นโดยพิจารณาเป็นรายกรณี

หากไม่สามารถทำการชี้แจงตามข้อนี้ได้ ฝ่ายจัดการสถานการณ์ควรปรึกษา ฝ่ายกฎหมาย โดยทันที เพื่อพิจารณาวิธีการชี้แจงอื่น ๆ แทน ทั้งนี้ ฝ่ายจัดการสถานการณ์อาจชะลอการส่งคำชี้แจงไว้หากหน่วยงานผู้บังคับใช้กฎหมายเห็นว่าการชี้แจงไปยังผู้ที่ได้รับผลกระทบนั้นอาจเป็นอุปสรรคต่อการสืบสวน

4.13 การตอบคำถาม: ฝ่ายจัดการสถานการณ์ต้องมีการวางแผนว่ากลุ่มบริษัทอรสิริน ควรมีวิธีการในการตอบข้อซักถามจากสื่อมวลชน รัฐบาล หรือบุคคลอื่น ๆ อย่างไร โดยในกรณีส่วนใหญ่ ฝ่ายจัดการสถานการณ์ควรส่งข้อซักถามนั้นไปยังฝ่ายกฎหมาย หรือฝ่ายประชาสัมพันธ์ โดยตรงก่อน เพื่อวิเคราะห์และจัดเตรียมแนวทางในการตอบ

ระยะที่ 3: มาตรการหลังเกิดเหตุการณ์

4.14 ข้อกำหนดเรื่องการจัดทำบันทึกเอกสาร: ไม่ว่าจะมีการพิจารณาให้นำกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลมาใช้บังคับกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลหรือไม่ก็ตาม ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำเอกสารบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่ง ควรมีการบันทึกผลการประเมินที่ทำให้กลุ่มบริษัทอรสิริน พิจารณาไม่นำกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมาใช้บังคับ

4.15 มาตรการเพื่อการแก้ไข: ฝ่ายจัดการสถานการณ์จะต้องประสานงานกับฝ่ายกฎหมาย และฝ่ายเทคโนโลยีสารสนเทศ เพื่อกำหนดมาตรการทางเทคนิค และทางองค์กรที่จำเป็น เพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลในลักษณะที่คล้ายกันอีกในอนาคต ซึ่งรวมถึงการพิจารณาทบทวนนโยบาย การฝึกอบรมเพื่อสร้างความเข้าใจ การกำหนดกระบวนการสำหรับพนักงาน / ผู้รับจ้าง นอกจากนี้ ฝ่ายจัดการสถานการณ์ควรประเมินความสัมพันธ์กับบุคคลภายนอกที่อาจเกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล และดำเนินการต่าง ๆ ตามความเหมาะสม เช่น การแก้ไขสัญญา การแก้ไขกระบวนการต่าง ๆ การฝึกอบรม

การปรับปรุงมาตรการความปลอดภัย และ/หรือ การเลือกคู่ค้ารายใหม่ เป็นต้น ขณะเดียวกันบุคคลภายนอกจะต้องมีหน้าที่ตามสัญญาที่จะต้องแจ้งให้กลุ่มบริษัทอรสิรินทราบโดยทันทีหากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล ไม่ว่าจะเป็นเหตุการณ์ที่เกิดขึ้นจริงหรือสงสัยว่าจะเกิดขึ้นก็ตาม และคู่สัญญาของกลุ่มบริษัทอรสิริน ควรให้คำแนะนำแก่ ฝ่ายกฎหมาย และฝ่ายเทคโนโลยีสารสนเทศ หากต้องมีการปรับเปลี่ยนกระบวนการต่าง ๆ ที่เกี่ยวข้องกับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

4.16 การทบทวนหน้าที่ตามกรมธรรม์ประกันภัย: ฝ่ายจัดการสถานการณ์จะต้องทบทวนกรมธรรม์ประกันภัยที่เกี่ยวข้องของกลุ่มบริษัทอรสิริน เพื่อพิจารณาว่าควรแจ้งให้บริษัทประกันภัยทราบตามข้อกำหนดในกรมธรรม์ประกันภัยที่ยังคงมีผลบังคับหรือไม่ รวมถึงข้อกำหนดในเรื่องเวลา เนื้อหา และรูปแบบของคำชี้แจงด้วย

ORNSIRIN

ภาคผนวก 1

แบบฟอร์มการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

กรุณากรอกรายละเอียดด้านล่าง และส่งอีเมลไปยังฝ่ายจัดการสถานการณ์ที่ [PDPA@ornsirin.co.th]

คำอธิบายเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล	
วันและเวลาที่พบเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล	
ผู้ที่ระบุเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล	ชื่อ: ตำแหน่ง: ฝ่าย: ประเทศ: ที่อยู่อีเมล: หมายเลขโทรศัพท์:
พนักงาน / ผู้รับจ้างที่รายงาน:	☐ เป็นบุคคลเดียวกับผู้ที่ระบุเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ชื่อ: ตำแหน่ง: ฝ่าย: ประเทศ: ที่อยู่อีเมล: หมายเลขโทรศัพท์:
ระบบที่อาจหรือได้รับผลกระทบ	
ประเภทบุคคลที่อาจหรือได้รับผลกระทบ (เช่น ลูกค้า พันธมิตรทางธุรกิจ พนักงาน / ผู้รับจ้าง / ผู้ติดต่อในกรณีฉุกเฉินสำหรับพนักงาน / ผู้รับจ้าง ผู้เยาว์ ผู้พิการ)	
ประเภทของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	
รายชื่อผู้ที่ได้รับรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล	

ภาคผนวก 2
สรุปสาระสำคัญของกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

<table>
<tr><th>ลำดับ</th><th>กฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</th><th>รายละเอียด</th></tr>
<tr><td>1.</td><td>พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”)</td><td>
• ข้อกำหนดว่าด้วยการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมีอยู่ 2 ประเภทด้วยกัน
<table>
<tr><th>1. หน้าที่ในการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล</th><th>2. หน้าที่ในการแจ้งให้เจ้าของข้อมูลทราบ</th></tr>
<tr><td>โดยไม่ชักช้า ภายใน 72 ชั่วโมง นับตั้งแต่ผู้จัดการเหตุการณ์ลำดับแรกทราบถึงเหตุการณ์ ด้านความมั่นคงปลอดภัยของข้อมูล</td><td>โดยไม่ชักช้า</td></tr>
<tr><td>แจ้งการเกิดเหตุการละเมิดข้อมูลส่วนบุคคล</td><td>แจ้งการเกิดเหตุการละเมิดข้อมูลส่วนบุคคล และมาตรการแก้ไขเยียวยา</td></tr>
<tr><td>มีแนวโน้มที่จะก่อให้เกิดความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล</td><td>มีแนวโน้มที่จะก่อให้เกิดความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล</td></tr>
<tr><td>ข้อยกเว้นการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและวิธีการแจ้งเหตุการณ์จะมีกำหนดไว้ในกฎหมายลำดับรองต่อไป</td><td>ข้อยกเว้นการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและวิธีการแจ้งเหตุการณ์จะมีกำหนดไว้ในกฎหมายลำดับรองต่อไป</td></tr>
</table>
• “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้:
...(4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ เท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด” (มาตรา 37)
• “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 21 มาตรา 22 มาตรา 24 มาตรา 25 วรรคหนึ่ง มาตรา 27 วรรคหนึ่งหรือวรรคสอง มาตรา 28 มาตรา 32 วรรคสอง หรือมาตรา 37 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา 21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสามต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท” (มาตรา 83)
• “ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้:
...(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น” (มาตรา 40)
</td></tr>
</table>

ลำดับ	กฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	รายละเอียด
		• “ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 40 โดยไม่มีเหตุอันควร หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 37 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 38 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท” (มาตรา 86)
3.	พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (“พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์”)	• พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์กำหนดให้มีการรายงานต่อหน่วยงานผู้มีอำนาจ โดยข้อกำหนดการแจ้งดังกล่าวจะใช้บังคับกับองค์กรที่มี “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” ตามกฎหมายลำดับรองที่ออกตามมาตรา 49 แห่งพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ และในกรณีที่มีภัยคุกคามไซเบอร์ที่มีผลกระทบสำคัญ • “เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ 4 ทั้งนี้ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) อาจกำหนดหลักเกณฑ์ และวิธีการการรายงานด้วยก็ได้” (มาตรา 57) • “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา 57 โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท” (มาตรา 73)

ภาคผนวก 3
แนวทางกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

1. แนวทางในการพิจารณา – พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ฝ่ายจัดการสถานการณ์จะต้องวิเคราะห์ลักษณะ ขอบเขต และความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลตามทิศทางและแนวทางของ ฝ่ายกฎหมาย ซึ่งควรประเมินเป็นรายกรณีไป โดยพิจารณาจากชุดคำถามต่อไปนี้

หมายเหตุ: ฝ่ายกฎหมาย จะต้องตรวจสอบว่า หน่วยงานผู้มีอำนาจได้ออกกฎหมายลำดับรองหรือแนวทางปฏิบัติที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลและการประเมินความเสี่ยงแล้วหรือไม่ ในทุกกรณี หากมีการออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้ว กลุ่มบริษัทอรสิริน จะต้องนำมาพิจารณาร่วมกับชุดคำถามต่อไปนี้

คำถามที่ 1: เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนี้เกี่ยวข้องกับ “ข้อมูลส่วนบุคคล” ตามคำนิยามในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่ (หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 2: เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนี้เกี่ยวข้องกับการทำลาย สูญหาย หรือแก้ไข โดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย หรือเกี่ยวข้องกับการเปิดเผยหรือเข้าถึงข้อมูลส่วนบุคคลที่รับส่ง จัดเก็บ หรือประมวลผล โดยไม่ได้รับอนุญาตใช่หรือไม่ (การ “ละเมิดข้อมูลส่วนบุคคล”) (หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 3: การละเมิดข้อมูลส่วนบุคคลดังกล่าวอาจก่อให้เกิดความเสี่ยงที่จะกระทบต่อสิทธิ และเสรีภาพของบุคคลตามแนวปฏิบัติดังกล่าวหรือไม่

(หมายเหตุ: การประเมินความเสี่ยงควรพิจารณาจากกฎหมายลำดับรอง / แนวทางปฏิบัติ เมื่อมีการออกกฎหมายลำดับรอง หรือแนวทางปฏิบัติแล้ว) (หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 4: มีกฎหมายลำดับรอง หรือแนวทางปฏิบัติใดที่ยกเว้นหน้าที่ในการรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ หากมี ข้อยกเว้นนั้นนำมาใช้บังคับได้หรือไม่

หากคำตอบข้อ 4 คือ ไม่มี ฝ่ายจัดการสถานการณ์ควรพิจารณาว่ามีหน้าที่จะต้องรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ ฝ่ายจัดการสถานการณ์ดำเนินการตามคำถามข้อถัดไป

คำถามที่ 5: มีความเป็นไปได้ที่ความเสี่ยงนั้นจะเรียกได้ว่าเป็นความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลหรือไม่

แนวทางการประเมินความเสี่ยง – ในการพิจารณาว่ามีความเสี่ยง หรือมีความเสี่ยงสูงหรือไม่นั้น จะต้องพิจารณาตามรายการต่อไปนี้เป็นรายกรณีไป

- ประเภท (ความละเอียดอ่อน) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้น
- ปริมาณข้อมูลส่วนบุคคล
- จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
- ประเภทของการละเมิดข้อมูลส่วนบุคคล (เช่น เป็นการสูญหายของเครื่องคอมพิวเตอร์ หรือเป็นการโจรกรรฐานข้อมูลของกลุ่มบริษัทอรสิริน)
- ข้อมูลที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนั้น สามารถระบุตัวบุคคลได้ยากง่ายเพียงใด
- ลักษณะพิเศษของบุคคลที่ได้รับผลกระทบ (เช่น กลุ่มบุคคลที่มีความอ่อนไหว ตัวอย่างเช่น ผู้เยาว์ คนพิการ)
- ลักษณะพิเศษของผู้ควบคุมข้อมูลส่วนบุคคล (เช่น ประกอบธุรกิจที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลที่ละเอียดอ่อนเป็นจำนวนมาก ตัวอย่างเช่น โรงพยาบาล หรือบริษัทประกันภัย)

(หมายเหตุ: การประเมินความเสี่ยงควรพิจารณาจากกฎหมายลำดับรองหรือแนวปฏิบัติ เมื่อมีการออกกฎหมายลำดับรอง หรือแนวทางปฏิบัติแล้ว)

คำถามที่ 6: มีกฎหมายลำดับรองใดที่ยกเว้นหน้าที่ในการแจ้งเจ้าของข้อมูลส่วนบุคคลหรือไม่ หากมี ข้อยกเว้นนั้นนำมาใช้บังคับได้หรือไม่

หากคำตอบข้อ 6 คือไม่มี ฝ่ายจัดการสถานการณ์ควรพิจารณาว่ามีหน้าที่ (1) จะต้องรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ และ (2) จะต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคลหรือไม่

2. แนวทางในการพิจารณา – พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์

ฝ่ายจัดการสถานการณ์จะต้องวิเคราะห์ลักษณะ ขอบเขต และความรุนแรงของเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล ตามทิศทางและแนวทางของ ฝ่ายกฎหมาย ซึ่งควรประเมินเป็นรายกรณีไป โดยพิจารณาจากชุดคำถามต่อไปนี้

หมายเหตุ: ฝ่ายกฎหมาย จะต้องตรวจสอบว่า หน่วยงานผู้มีอำนาจได้ออกกฎหมายลำดับรองหรือแนวทางปฏิบัติที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญ การละเมิดข้อมูลส่วนบุคคล และการประเมินความเสี่ยงแล้วหรือไม่ ในทุกกรณี หากมีการออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้ว กลุ่มบริษัทอรสิริน จะต้องนำมาพิจารณาร่วมกับชุดคำถามต่อไปนี้

คำถามที่ 1: มีกฎหมายลำดับรอง หรือแนวทางปฏิบัติใดที่กำหนดหลักเกณฑ์ของหน่วยงานโครงสร้างพื้นฐานสำคัญหรือไม่ หากมี กลุ่มบริษัทอรสิริน เป็นไปตามหลักเกณฑ์ใด (หากมี กรุณาอ่านคำถามต่อไป)

คำถามที่ 2: เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลถือนี้เป็น “ภัยคุกคามทางไซเบอร์” ตามคำนิยามใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์หรือไม่ (หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 3: มีกฎหมายลำดับรอง หรือแนวทางปฏิบัติใดที่กำหนดหลักเกณฑ์ภัยคุกคามทางไซเบอร์ที่มี “นัยสำคัญ” หรือไม่ หากมี เหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลนี้เป็นไปตามหลักเกณฑ์ใด

หากคำตอบข้อ 3 คือมี ฝ่ายจัดการสถานการณ์จะต้องพิจารณาว่ากลุ่มบริษัทอรสิริน มีหน้าที่ต้องรายงานต่อคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) และคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) หรือไม่ย

ประกาศใช้ ณ วันที่ 15 พฤศจิกายน 2567 เป็นต้นไป