นโยบายการจัดการในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลและแนวทางปฏิบัติที่เกี่ยวข้องของ บริษัท ลีซ อิท จำกัด (มหาชน) และบริษัทย่อย

1. วัตถุประสงค์

นโยบายการจัดการในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลและแนวทางปฏิบัติที่เกี่ยวข้องของบริษัท ลีซ อิท จำกัด (มหาชน) และบริษัทย่อย ("แนวทาง") ฉบับนี้ จัดทำขึ้นเพื่อแสดงถึงขั้นตอนที่บริษัท ลีซ อิท จำกัด (มหาชน) และบริษัทย่อย ("บริษัท") จะปฏิบัติเมื่อเกิดเหตุการณ์รั่วไหลของข้อมูล (ตามคำนิยามด้านล่าง) ทั้งที่เกิดขึ้นจริง หรือมีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น ซึ่งอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล

2. ขอบเขต

แนวทางนี้ใช้บังคับกับพนักงาน ผู้รับจ้าง ตัวแทน ตลอดจนบุคคลากรอื่น ๆ ของบริษัท นอกจากนี้บริษัทยังกำหนดให้พันธมิตรทางธุรกิจและผู้ให้บริการภายนอก ซึ่งรวมถึง พนักงาน ผู้รับจ้าง ตัวแทน และบุคคลากรอื่น ๆ ของพันธมิตรทางธุรกิจและผู้ให้บริการภายนอกดังกล่าว ที่ต้องเก็บรวบรวม เข้าถึง จัดเก็บ หรือจัดการข้อมูลส่วนบุคคลในนามของบริษัท (ต่อจากนี้ไปจะเรียกรวมกันว่า "พนักงานหรือผู้รับจ้าง") ต้องทำสัญญาเพื่อปฏิบัติตามแนวทางนี้ ทั้งนี้ แนวทางฉบับนี้จะไม่ก่อให้เกิดสิทธิใด ๆ แก่พนักงานหรือผู้รับจ้าง หรือสิทธิใด ๆ นอกเหนือหน้าที่ของบริษัทภายใต้กฎหมายที่ใช้บังคับแนวทางนี้เป็นเอกสารภายในของบริษัท และมิได้ก่อสิทธิหรือสิทธิพิเศษใด ๆ สำหรับบุคคลภายนอก

ผู้ใดฝ่าฝืนแนวทางฉบับนี้ อาจได้รับโทษทางวินัย ซึ่งรวมถึงการเลิกจ้าง หรืออาจส่งผลให้มีการบอกเลิกสัญญากับพันธมิตรทางธุรกิจ หรือผู้ให้บริการได้

บริษัทอาจแก้ไขเพิ่มเติมแนวทางนี้เป็นครั้งคราว โดยบริษัทจะแจ้งให้พนักงานหรือผู้รับจ้าง ทราบตามความเหมาะสม

3. ข้อกำหนดในการรายงานเหตุการณ์รั่วไหลของข้อมูล

3.1 การติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล

หากพนักงานหรือผู้รับจ้างใดพบ สงสัย หรือทราบถึงเหตุการณ์รั่วไหลของข้อมูลที่เกิดขึ้นจริง หรือมีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น จะต้องรายงานประเด็นดังกล่าวให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลทราบโดยทันที โดยใช้แบบฟอร์มการบันทึกการรั่วไหลของข้อมูลส่วนบุคคลภาคในภาคผนวก 1

3.2 เหตุการณ์รั่วไหลของข้อมูล

เหตุการณ์รั่วไหลของข้อมูล คือเหตุการณ์ที่เกิดขึ้นจริง หรือมีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น หรือเกิดเหตุขัดข้อง หรือเหตุการณ์อื่นที่ก่อให้เกิดการทำลาย การสูญหาย การเปลี่ยนแปลงของข้อมูลที่บริษัทเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือเก็บรักษาไว้ ไม่ว่าจะโดยทางตรงหรือโดยทางอ้อม (เช่น ข้อมูลที่อยู่

ภายใต้การดูแลของพันธมิตรทางธุรกิจหรือผู้ให้บริการภายนอกอื่นที่ให้บริการแก่บริษัท) ไม่ว่าจะโดยอุบัติเหตุ โดยเจตนา หรือโดยมิชอบด้วยกฎหมาย หรือก่อให้เกิดการได้รับ การเปิดเผย หรือการเข้าถึงเอกสารกระดาษหรือข้อมูลทางอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับหรือไม่ก็ตามซึ่งข้อมูลดังกล่าวอาจอยู่ในแฟ้มเอกสาร กระดาษ อีเมล ตาราง บันทึก เครื่องแม่ข่าย (เซิร์ฟเวอร์) อุปกรณ์จัดเก็บข้อมูลแบบพกพา (เช่น คอมพิวเตอร์แล็ปท็อป, โทรศัพท์สมาร์ตโฟน, ธัมบ์ไดรฟ์) และฐานข้อมูลไอที เป็นต้น

ตัวอย่างเหตุการณ์บางส่วนที่มีลักษณะต้องรายงาน เช่น

- การโจรกรรมหรือการสูญหายของคอมพิวเตอร์ คอมพิวเตอร์แล็ปท็อป โทรศัพท์สมาร์ตโฟน อุปกรณ์บันทึกข้อมูลแบบธัมบ์ไดรฟ์ หรืออุปกรณ์บันทึกข้อมูลอื่นที่เป็นของบริษัท หรือของพนักงานหรือผู้รับจ้างที่ใช้อุปกรณ์ดังกล่าว บันทึกข้อมูลที่เกี่ยวข้องกับบริษัท
- บุคคลภายนอกกระทำผิดสัญญาการไม่เปิดเผยข้อมูลหรือสัญญาการรักษาความลับ
- ผู้โจมตีก่อให้เกิดความเสี่ยงต่อระบบของบริษัท เช่น ฐานข้อมูล คอมพิวเตอร์ เครื่องแม่ข่าย การสื่อสารของบริษัท
- พนักงานหรือผู้รับจ้างทำการตรวจสอบ เข้าถึง หรือเปิดเผยข้อมูล แฟ้มข้อมูล หรือฐานข้อมูลนอกขอบเขตหน้าที่ที่ได้รับมอบหมาย

3.3 ความช่วยเหลือ

พนักงานหรือผู้รับจ้างจะต้องให้ความช่วยเหลือบริษัทและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลในการตรวจสอบเหตุการณ์รั่วไหลของข้อมูลอย่างเต็มความสามารถ

3.4 การติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลการติดต่อ

อีเมล : dpo@leaseit.co.th

เบอร์ติดต่อ : 02-163-4260

4. ขั้นตอนการจัดการเหตุการณ์รั่วไหลของข้อมูล

4.1 การตรวจสอบเบื้องต้น

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล จะมอบหมายให้สมาชิกหรือผู้ที่ได้รับมอบหมายทำการตรวจสอบในเบื้องต้นสำหรับเหตุการณ์รั่วไหลของข้อมูล

4.2 การยืนยันเหตุการณ์รั่วไหลของข้อมูล

หากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล พิจารณาแล้วเห็นว่า มีมูลฐานอันสมเหตุสมผลหรือน่าเชื่อถือที่ทำให้เชื่อได้ว่าเหตุการณ์รั่วไหลของข้อมูลดังกล่าวเกิดขึ้นจริงแล้วนั้น จะต้องแจ้งให้ผู้บริหารของตนทราบโดยทันที

4.3 การควบคุมภัยคุกคาม

หากเหตุการณ์รั่วไหลของข้อมูลนั้นเป็นภัยคุกคามถาวร หรือเกิดภัยคุกคามอย่างต่อเนื่อง (เช่น แฮกเกอร์หรือไวรัสในระบบสารสนเทศของบริษัท) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการให้บุคลากรในกลุ่มงานเทคโนโลยีสารสนเทศกำหนดมาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยและแยกภัยคุกคามออกไปไม่ให้สร้างความเสียหายต่อสภาพแวดล้อมทางเทคนิคของบริษัทต่อไป

4.4 การจัดเก็บบันทึกเอกสารที่เกี่ยวข้องกับการจัดการเหตุการณ์

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลต้องจัดเก็บบันทึกเอกสารต่าง ๆ ที่เกี่ยวข้องในช่วงขั้นตอนที่ดำเนินการ ตั้งแต่พบเหตุการณ์ไปจนถึงการแจ้งให้ทราบและการแก้ไข

4.5 การเก็บหลักฐาน

ในการตรวจสอบ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการที่เหมาะสมในการเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้อง ซึ่งรวมถึง

- ระงับการลบหรือทำลายข้อมูล (รวมทั้งแฟ้มบันทึกข้อมูลอัตโนมัติ การเขียนทับลงบนเทปสำรองข้อมูลหรือการรีไซเคิล)
- สั่งให้พนักงานหรือผู้รับจ้าง ตัวแทน หรือผู้แทนที่สามารถเข้าถึงระบบได้ใช้ความระมัดระวังไม่ให้ลบแก้ไข หรือทำให้ข้อมูลและหลักฐานที่เกี่ยวข้องได้รับความเสียหาย
- เก็บรักษารหัสหรือมัลแวร์ที่ต้องสงสัย และ
- ดำเนินการตามกฎหมายที่เกี่ยวข้องตามนโยบายของบริษัท (ในกรณีที่เกี่ยวข้อง)

4.6 การรักษาความลับ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะประสานงานร่วมกับฝ่ายอื่น ๆ เพื่อให้แน่ใจว่าเหตุการณ์รั่วไหลของข้อมูลจะถูกปิดเป็นความลับจนกว่าจะมีการตัดสินใจเกี่ยวกับการแจ้งให้ทราบหรือเปิดเผย นอกจากนี้จะต้องจำกัดจำนวนพนักงานหรือผู้รับจ้างที่ทราบเหตุการณ์รั่วไหลของข้อมูลให้น้อยที่สุดเท่าที่จะทำได้

4.7 การตรวจสอบขอบเขตของเหตุการณ์รั่วไหลของข้อมูล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะตรวจสอบและรวบรวมข้อมูลเกี่ยวกับขอบเขตของเหตุการณ์รั่วไหลของข้อมูล ซึ่งรวมถึงข้อมูลต่อไปนี้ (ในกรณีที่เกี่ยวข้อง)

- วันและเวลาที่เกิดเหตุการณ์รั่วไหลของข้อมูล
- ลักษณะการเกิดเหตุการณ์รั่วไหลของข้อมูล
- ประเภทของข้อมูล (เช่น ประเภทของข้อมูลส่วนบุคคล) ที่อาจเสี่ยงต่อการได้รับผลกระทบ
- ความเสี่ยงว่าจะเกิดความเสียหายหรือการใช้งานในทางที่ผิด และ
- ผู้ทราบเหตุการณ์รั่วไหลของข้อมูลดังกล่าว ไม่ว่าจะเป็นบุคลากรภายในหรือนอกบริษัท

- และข้อมูลอื่นๆ ที่มีความจำเป็นหรือเป็นไปได้ และข้อมูลดังกล่าวเป็นประโยชน์ต่อการตรวจสอบหรือหาผลกระทบ

4.8 การรายงานต่อหน่วยงานบังคับใช้กฎหมาย

ในฐานะส่วนหนึ่งของการตรวจสอบ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะต้องพิจารณาและประเมินความเสี่ยงก่อนว่าการรั่วไหลของข้อมูลนั้นมีความเสี่ยงเป็นอย่างไร หากมีความเสี่ยงสูง ก็จำเป็นที่จะต้องรายงานต่อหน่วยงานที่บังคับใช้กฎหมายที่เกี่ยวข้องรวมไปถึงเจ้าของข้อมูลส่วนบุคคลด้วย แต่ถ้าหากพิจารณาและประเมินความเสี่ยงออกมาแล้วมีความเสี่ยงต่ำ และสามารถดำเนินการแก้ไขได้ทันทีก็ไม่จำต้องรายงานต่อหน่วยงานที่บังคับใช้กฎหมาย

4.9 การพิจารณาข้อกำหนดทางกฎหมายที่ใช้บังคับ

ฝ่ายกฎหมาย และหรือที่ปรึกษาทางกฎหมายจากภายนอกจะใช้แนวทางการวิเคราะห์เพื่อให้คำแนะนำแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่จะนำมาใช้บังคับกับเหตุการณ์รั่วไหลของข้อมูลและให้คำแนะนำว่าเหตุการณ์รั่วไหลของข้อมูลดังกล่าวถือว่าเป็นการละเมิดความมั่นคงปลอดภัยของข้อมูลที่ต้องแจ้งหน่วยงานรัฐบาลหรือหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลหรือหน่วยงานอื่น ๆที่เกี่ยวข้องหรือไม่ รวมถึงต้องมีการแจ้งเตือนไปยังเจ้าของข้อมูลส่วนบุคคลผู้ที่ได้รับผลกระทบโดยตรงหรือไม่

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะต้องให้ข้อมูลตามความเป็นจริงตามที่ฝ่ายกฎหมายและหรือที่ปรึกษาทางกฎหมายจากภายนอกร้องขอเพื่อให้ฝ่ายกฎหมายและหรือที่ปรึกษาทางกฎหมายจากภายนอกทำการประเมินทางกฎหมายที่จำเป็นได้

4.10 ข้อกำหนดเรื่องการจัดทำบันทึกเอกสาร

ไม่ว่าจะมีการพิจารณาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมาใช้บังคับต่อเหตุการณ์รั่วไหลของข้อมูลหรือไม่ก็ตามนั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะต้องจัดทำเอกสารบันทึกเหตุการณ์รั่วไหลของข้อมูลให้เพียงพอ โดยเฉพาะอย่างยิ่งการประเมินทางกฎหมายที่ไม่ได้นำกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมาใช้บังคับ ทั้งนี้ ให้ใช้แบบฟอร์มบันทึกเหตุการณ์รั่วไหลของข้อมูลในภาคผนวก 1 เพื่อการบันทึกรายละเอียดที่เกี่ยวข้อง

4.11 มาตรการแก้ไข

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลจะต้องประสานงานกับฝ่ายกฎหมาย ฝ่ายเทคโนโลยีสารสนเทศ และผู้บริหารของบริษัท เพื่อกำหนดมาตรการทางเทคนิคและมาตรการทางองค์กรที่จำเป็นในการป้องกันไม่ให้เกิดเหตุการณ์รั่วไหลของข้อมูลที่คล้ายกันอีกในอนาคต ซึ่งรวมถึงแนวทางการฝึกอบรมเพื่อสร้างความเข้าใจกระบวนการสำหรับพนักงานหรือผู้รับจ้าง ทั้งนี้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลควรประเมินความสัมพันธ์กับบุคคลภายนอกที่อาจเกี่ยวข้องกับเหตุการณ์รั่วไหลของข้อมูล พร้อมดำเนินมาตรการที่เหมาะสม เช่น การแก้ไขสัญญาให้รัดกุมมากยิ่งขึ้น โดยการกำหนดหน้าที่ให้ชัดเจนว่าเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลหรือคาดว่ามีข้อมูลรั่วไหลจะต้องดำเนินการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอย่างไร หรือกำหนดมาตรฐานขั้นต่ำในการรักษาความมั่นคงปลอดภัยข้อมูลของบุคคลภายนอก หรือการเลือกผู้ให้บริการรายใหม่ เป็นต้น ขณะเดียวกันบุคคลภายนอกมีหน้าที่ตามสัญญาที่จะต้องแจ้งให้บริษัททราบโดยทันทีหากเกิดเหตุการณ์รั่วไหลของข้อมูล ไม่ว่าที่เกิดขึ้นจริงหรือสงสัยว่าจะเกิดขึ้นก็ตาม

ประกาศ เมื่อวันที่ 1 พฤศจิกายน 2567

ภาคผนวก 1

แบบฟอร์มการบันทึกการรั่วไหลของข้อมูลส่วนบุคคล

คำชี้แจง : โปรดระบุรายละเอียดเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

ส่วนของพนักงานผู้พบการรั่วไหลของข้อมูล

1. ชื่อผู้พบการรั่วไหล_____

สังกัด_____ฝ่าย/แผนก_____

2. ชื่อผู้บังคับบัญชา_____

3. วันและเวลาที่พบการรั่วไหล: _____

4. วันและเวลาที่การรั่วไหลเกิดขึ้น: _____

5. วันและเวลาที่แจ้งการรั่วไหลต่อผู้บังคับบัญชา_____

6. พบการรั่วไหลได้อย่างไร: _____

7. โปรดอธิบายอย่างละเอียดถึงเหตุการณ์ที่เกิดขึ้น

_____

_____

_____

8. ประเภทของเจ้าของข้อมูลที่เสียหายจากการรั่วไหลของข้อมูล (เลือกทุกข้อที่มีความเกี่ยวข้องกัน)

☐ ลูกค้า ☐ พนักงาน

☐ ผู้ติดต่อ ☐ ไม่ทราบแน่ชัด

☐ อื่น ๆ (โปรดระบุ)

9. ประเภทของข้อมูลที่เกิดการรั่วไหล (เลือกทุกข้อที่มีความเกี่ยวข้องกัน)

☐ ข้อมูลทั่วไป เช่น ชื่อ-นามสกุล, หมายเลขโทรศัพท์ ☐ เอกสารทางราชการ เช่น สำเนาบัตรประจำตัวประชาชน

☐ Username,Passwords ☐ ข้อมูลด้านการเงิน เช่น หมายเลขบัญชีธนาคาร

☐ ข้อมูล GPS Locations ☐ ข้อมูลเกี่ยวกับเชื้อชาติ หรือ สัญชาติ

☐ ข้อมูลด้านความคิดเห็นทางการเมือง ☐ ข้อมูลเกี่ยวกับศาสนา

☐ ข้อมูลเกี่ยวกับเพศ ☐ ข้อมูลเรื่องสุขภาพ

☐ ข้อมูลทางชีวภาพ เช่น ภาพสแกนใบหน้า ☐ ประวัติอาชญากรรม

☐ ยังไม่ทราบ

10. ปริมาณโดยคร่าวของข้อมูลที่รั่วไหล_____

11. ปริมาณโดยคร่าวของเจ้าของข้อมูลที่ได้รับผลกระทบ _____

12. โปรดอธิบายอย่างละเอียดถึงผบกระทบที่น่าจะเกิดจากการรั่วไหล

_____

_____

_____

13. ความน่าจะเป็นที่การรั่วไหลของข้อมูลส่วนบุคคลจะส่งผลกระทบที่เป็นการคุกคามต่อเจ้าของข้อมูลส่วนบุคคล

☐ เป็นไปได้สูง ☐ เป็นไปได้ต่ำ

☐ เป็นไปได้ ☐ เป็นไปไม่ได้

☐ เป็นไปได้ปานกลาง ☐ ไม่ทราบแน่ชัด

14. โปรดอธิบายอย่างละเอียดถึงผลกระทบที่อาจจะเกิด หรือ เกิดไปแล้วต่อเจ้าของข้อมูล:

_____

_____

_____

ลงชื่อ .....ผู้แจ้ง

(.....)

ส่วนของผู้บังคับบัญชา

1. ชื่อผู้บังคับบัญชา _____

สังกัด_____ฝ่าย/แผนก_____

2. วันและเวลาที่แจ้งการรั่วไหลต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล: _____

ลงชื่อ .....ผู้บังคับบัญชา

(.....)

ส่วนของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

1. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้มีการแจ้งเจ้าของข้อมูลถึงเหตุการณ์การรั่วไหลหรือไม่

☐ มีการแจ้งเจ้าของข้อมูลเรียบร้อย ☐ อยู่ระหว่างการตัดสินใจของบริษัท

☐ อยู่ระหว่างการดำเนินการแจ้งเจ้าของข้อมูล ☐ อื่น ๆ (โปรดระบุ_____)

☐ มีการตัดสินใจที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคล

2. หากไม่มีการแจ้งข้อมูลต่อเจ้าของข้อมูลส่วนบุคคล โปรดชี้แจงเหตุผล

_____

_____

_____

3. หากมีการล่าช้าในการแจ้งเหตุการณ์การรั่วไหลเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล โปรดชี้แจงเหตุผล

_____

_____

_____

4. วิธีการแก้ไขเยียวยาต่อเจ้าของข้อมูลส่วนบุคคล

_____

_____

_____

5. มีการแจ้งผู้บริหารซึ่งทำหน้าที่ควบคุมข้อมูลส่วนบุคคล ถึงเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลหรือไม่

☐ มีการแจ้งแล้ว ☐ ไม่มีการแจ้ง

6. มีการแจ้งสำนักคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ถึงเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลหรือไม่

☐ มีการแจ้งแล้ว ☐ ไม่มีการแจ้ง

7. วันและเวลาที่แจ้งการรั่วไหลของข้อมูลต่อสำนักคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล_____

_____

8. หากมีการแจ้ง โปรดชี้แจงรายละเอียด

_____

_____

_____

9. หากไม่มีการแจ้ง โปรดชี้แจงรายละเอียด

_____

_____

_____