แนวปฏิบัติว่าด้วยเรื่องการรายงานและ

การรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

บริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน)

ฉบับลงวันที่ 1 กันยายน 2565

1. วัตถุประสงค์

แนวปฏิบัติว่าด้วยเรื่องการรายงานและการรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ฉบับนี้ ("**แนวปฏิบัติ**") มีไว้เพื่อช่วยอธิบายขั้นตอนที่บริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน) และบริษัทย่อย (รวมกันว่า "**บริษัทฯ**")[1] ควรปฏิบัติตามเมื่อเกิดสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล (ตามคำนิยามเกี่ยวที่เกี่ยวข้องด้านล่าง) ทั้งที่เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดสถานการณ์เช่นว่านั้นขึ้น

2. ขอบเขตของแนวปฏิบัติ

แนวปฏิบัตินี้ใช้บังคับกับพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน ผู้แทน และบุคคลอื่นที่กระทำการแทนบริษัทฯ นอกจากนี้ บริษัทฯ ยังกำหนดให้ผู้ขายและผู้ให้บริการอื่น รวมถึงพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน ผู้แทน และและบุคคลอื่นที่กระทำการแทนผู้ขายและผู้ให้บริการดังกล่าวที่ต้องเก็บรวบรวม ใช้ เข้าถึง จัดเก็บ เปิดเผย หรือรับมือข้อมูลในนามบริษัทฯ (เรียกรวมกันว่า "**พนักงาน**") ต้องทำสัญญาเพื่อปฏิบัติตามแนวปฏิบัตินี้ ทั้งนี้ แนวปฏิบัตินี้จะไม่ก่อสิทธิใด ๆ แก่พนักงาน หรือสิทธิใด ๆ นอกเหนือหน้าที่ของบริษัทฯ ภายใต้กฎหมายที่ใช้บังคับ แนวปฏิบัตินี้เป็นความลับและเป็นแนวปฏิบัติภายในของบริษัทฯ อันจะไม่ก่อสิทธิหรือสิทธิพิเศษใด ๆ สำหรับบุคคลภายนอก

ผู้ฝ่าฝืนแนวปฏิบัตินี้อาจได้รับโทษทางวินัย ซึ่งรวมถึงการเลิกจ้าง หรืออาจส่งผลให้มีการบอกเลิกสัญญากับผู้ขาย หรือสัญญาบริการใด ๆ

บริษัทฯ อาจแก้ไขเพิ่มเติม หรือทบทวนแนวปฏิบัตินี้เป็นครั้งคราว หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยบริษัทฯ จะแจ้งให้พนักงาน ผู้ขาย และผู้ให้บริการทุกรายทราบตามความเหมาะสม

3. ข้อกำหนดในการรายงานสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

3.1 การติดต่อฝ่ายรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ("ฝ่ายรับมือสถานการณ์")

พนักงานใดที่พบเห็น สงสัย หรือทราบถึงสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลที่ได้เกิดขึ้นจริง หรือมีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น จะต้องรายงานประเด็นดังกล่าวให้แก่ผู้บังคับบัญชาฝ่ายงานของตน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยทันที เพื่อดำเนินการตรวจสอบเบื้องต้นร่วมกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายกฎหมาย (รวมเรียกว่า "**ผู้รับมือสถานการณ์ลำดับแรก**") และรายงานแก่ฝ่ายรับมือสถานการณ์ให้ทราบในลำดับต่อไป (โปรดดูข้อ 3.4 ของแนวปฏิบัติฉบับนี้สำหรับเรื่องข้อมูลติดต่อฝ่ายรับมือสถานการณ์) และโปรดดูภาคผนวก 1 สำหรับแบบฟอร์มการรายงานสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

---

[1]**บริษัทฯ**" หมายถึง บริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน) และบริษัทย่อย ซึ่งไม่ได้ประกอบธุรกิจโรงแรม และธุรกิจประกันชีวิต

3.2 สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล หมายถึง สถานการณ์ การกระทำ ความผิดพลาด หรือกรณีอื่นใดที่เกิดขึ้นจริง หรือมีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น ที่ก่อให้เกิดการทำลาย การสูญหาย การเปลี่ยนแปลงของข้อมูลที่บริษัทฯ เป็นเจ้าของ ควบคุม หรือเก็บรักษาไว้ ไม่ว่าจะโดยตรงหรือโดยอ้อม (เช่น ข้อมูลที่อยู่ภายใต้การดูแลของผู้ขายหรือผู้ให้บริการอื่นที่ให้บริการแก่บริษัทฯ) ไม่ว่าจะโดยอุบัติเหตุ โดยเจตนา หรือโดยมิชอบด้วยกฎหมาย หรือที่ได้รับมา ถูกเปิดเผย หรือเข้าถึงโดยไม่ได้รับอนุญาต ไม่ว่าที่อยู่ในรูปแบบของกระดาษหรือข้อมูลทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับหรือไม่ก็ตาม ทั้งนี้ ข้อมูลดังกล่าวอาจอยู่ในแฟ้มเอกสารกระดาษ อีเมล ตารางข้อมูล บันทึกข้อมูลพนักงาน บันทึกบัญชีเงินเดือน เซิร์ฟเวอร์ อุปกรณ์จัดเก็บข้อมูลแบบพกพา (เช่น คอมพิวเตอร์แล็ปท็อป โทรศัพท์สมาร์ตโฟน) หรือฐานข้อมูลเทคโนโลยีสารสนเทศใด ๆ (โปรดดู ภาคผนวก 5 สำหรับตัวอย่างสถานการณ์ที่จะต้องรายงานแก่ฝ่ายรับมือสถานการณ์)

3.3 ความช่วยเหลือ

พนักงานจะต้องให้ความช่วยเหลือแก่บริษัทฯ และฝ่ายรับมือสถานการณ์ในการตรวจสอบสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

3.4 ความพร้อมของฝ่ายรับมือสถานการณ์

ฝ่ายรับมือสถานการณ์จะต้องจัดให้มีการเฝ้าติดตามการติดต่อประสานงานเกี่ยวกับสถานการณ์ผ่านทางบัญชีอีเมล และหมายเลขโทรศัพท์ เพื่อการเฝ้าระวังตลอด 24 ชั่วโมง โดยไม่มีวันหยุด เพื่อให้ผู้รับมือสถานการณ์ลำดับแรกสามารถดำเนินการใด ๆ ได้ทันทีเมื่อได้รับการรายงาน

4. ขั้นตอนการรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

โปรดดูภาคผนวก 4 สำหรับ Diagram สรุปแผนผังขั้นตอนการรายงานและรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ดังต่อไปนี้

ระยะที่ 1 : การรายงานและการยืนยันสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลภายในองค์กร

วัตถุประสงค์ของระยะที่ 1 คือเพื่อระบุและยืนยันได้อย่างทันท่วงทีว่า มีสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลเกิดขึ้นจริงหรือไม่ เพื่อที่จะได้รายงานต่อไปยังฝ่ายรับมือสถานการณ์

4.1 การตรวจสอบเบื้องต้น

ให้พนักงาน/บุคคลที่เกี่ยวข้องรายงานต่อผู้บังคับบัญชาสายงานของตน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยทันที และร่วมกับผู้รับมือสถานการณ์ลำดับแรกในการสืบสวนและตรวจสอบแต่ละสถานการณ์ที่ได้รับการรายงานในเบื้องต้น โดยผู้รับมือสถานการณ์ลำดับแรกจะต้องรวบรวมข้อมูลจากพนักงานซึ่งเป็นผู้รายงานสถานการณ์อย่างทันท่วงที และขอข้อมูลเกี่ยวกับสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลดังกล่าวให้ได้มากที่สุดเท่าที่มีอยู่ในเวลานั้น และร่วมกันตรวจสอบยืนยันเหตุการณ์ร่วมกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายกฎหมาย ในการร่วมกันพิจารณาตัดสินใจเบื้องต้นโดยเร็วที่สุดและภายใน 24 ชั่วโมงแรกนับจากทราบเหตุการณ์ดังกล่าวว่า จากข้อมูลที่มีอยู่นั้นมีมูลฐานอันควรเชื่อและน่าเชื่อถือว่าได้มีสถานการณ์ดังกล่าวเกิดขึ้นจริงหรือไม่ ผู้รับมือสถานการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นการภายในโดยระบุข้อมูลต่อไปนี้ หากตรวจสอบแล้วขณะนั้นยังไม่มีมูลฐานอันควรเชื่อว่าสถานการณ์ดังกล่าวอาจเกิดขึ้นได้ หรือเกิดขึ้นแล้ว

- ข้อมูลตัวตนของพนักงานที่รายงานสถานการณ์ (หรือพนักงานท่านอื่น)
- คำอธิบายสถานการณ์แวดล้อมของสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลที่มีการรายงาน
- คำอธิบายถึงสาเหตุที่ผู้รับมือสถานการณ์ลำดับแรกพิจารณาว่า สถานการณ์ดังกล่าวไม่มีมูลเหตุอันควรเชื่อหรือน่าเชื่อถือได้ว่าสถานการณ์ดังกล่าวอาจเกิดขึ้นได้หรือเกิดขึ้นไปแล้ว

โดยผู้รับมือสถานการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นลายลักษณ์อักษรไปยังฝ่ายรับมือสถานการณ์โดยทันที

4.2 การยืนยันสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

หากผู้รับมือสถานการณ์ลำดับแรกพิจารณาแล้วว่า มีมูลฐานอันควรเชื่อและน่าเชื่อถือได้ว่า สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลดังกล่าวได้เกิดขึ้นจริง ผู้รับมือสถานการณ์ลำดับแรกจะต้องแจ้งให้ฝ่ายรับมือสถานการณ์ ทราบโดยทันที เพื่อดำเนินการระยะที่ 2 ต่อไปทันที

ระยะที่ 2 : การรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

วัตถุประสงค์ของระยะที่ 2 คือเพื่อรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลทั้งในระดับภายในและภายนอกองค์กร ในระยะนี้จะต้องมีการประเมินสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลโดยไม่ล่าช้าและเร็วที่สุดเท่าที่จะทำได้ เพื่อให้บริษัทฯ สามารถทำการแจ้งเตือนที่จำเป็นได้ทันเวลา หากฝ่ายรับมือสถานการณ์เห็นว่าต้องรายงานสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลนั้นให้หน่วยงานรัฐบาล บุคคล

หรือผู้ใดก็ตาม ทราบตามที่กฎหมายกำหนด ในขณะเดียวกัน ฝ่ายรับมือสถานการณ์จะต้องดำเนินการอื่น ๆ ที่จำเป็นไปพร้อมๆ กันเพื่อควบคุมสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลและเพื่อลดความเสี่ยงและความเสียหายลงให้ได้มากที่สุด

4.3 การควบคุมภัยคุกคาม

หากสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลนั้นมีลักษณะเป็นภัยคุกคามถาวร หรือเป็นภัยคุกคามอย่างต่อเนื่อง (เช่น มีแฮกเกอร์หรือไวรัสทำการโจมตีระบบสารสนเทศของบริษัทฯ) ฝ่ายรับมือสถานการณ์จะต้องดำเนินการ

4.4 จัดทำบันทึกการรับมือสถานการณ์

ฝ่ายรับมือสถานการณ์ต้องจัดเก็บบันทึกขั้นตอนที่ตนได้ดำเนินการ ตั้งแต่มีการพบสถานการณ์ ไปจนถึงการชี้แจง และการแก้ไขสถานการณ์นั้น

4.5 เก็บรักษาหลักฐาน

ในการทำการสืบสวนเพื่อตรวจสอบ ฝ่ายรับมือสถานการณ์จะต้องจัดให้มีมาตรการที่เหมาะสมในการเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้อง ซึ่งรวมถึงกรณีดังต่อไปนี้

- การระงับข้อมูลไม่ให้ถูกลบหรือทำลาย (รวมทั้งแฟ้มบันทึกข้อมูลอัตโนมัติ การเขียนทับลงบนเทปสำรองข้อมูล หรือการนำข้อมูลกลับมาใช้ใหม่)
- การออกคำสั่งให้พนักงาน ผู้รับจ้าง ตัวแทน หรือผู้แทนที่สามารถเข้าถึงระบบได้ใช้ความระมัดระวังไม่ให้ลบ แก้ไข หรือทำให้ข้อมูลและหลักฐานที่เกี่ยวข้องได้รับความเสียหาย
- การเก็บรักษารหัส หรือบันทึกกิจกรรมของมัลแวร์ที่ต้องสงสัย และ
- การอายัดข้อมูลไว้เพื่อวัตถุประสงค์ในการดำเนินคดีตามกฎหมายตามนโยบายของบริษัทฯ (ถ้าจำเป็น)

4.6 ผู้ตรวจสอบทางนิติวิทยาศาสตร์

ฝ่ายรับมือสถานการณ์จะพิจารณาเป็นรายกรณีไปว่า จำเป็นต้องให้ผู้ตรวจสอบ/หน่วยงานตรวจสอบทางนิติวิทยาศาสตร์ที่ได้รับอนุญาต เข้ามาบันทึกภาพอุปกรณ์ที่ได้รับผลกระทบ หรือทำการตรวจสอบคอมพิวเตอร์ด้วยวิธีการทางนิติวิทยาศาสตร์ หรือให้บริการอื่น ๆ หรือไม่ การตรวจสอบด้วยวิธีการทางนิติวิทยาศาสตร์จะดำเนินการโดยฝ่ายกฎหมาย (หรืออาจจัดหาผู้เชี่ยวชาญ) เพื่อให้คำปรึกษาและคำแนะนำทางกฎหมายแก่บริษัทฯ หากคาดว่าจะต้องมีการดำเนินคดี การสืบสวนสอบสวนทางกฎหมาย หรือการตรวจสอบภายในองค์กร

4.7 การรักษาความลับ

ฝ่ายรับมือสถานการณ์จะดำเนินการประสานงานร่วมกับฝ่ายอื่น ๆ เพื่อให้แน่ใจว่าสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลจะถูกเก็บเป็นความลับ จนกว่าจะมีการตัดสินใจเกี่ยวกับการชี้แจงหรือเปิดเผย นอกจากนี้ จะต้องจำกัดจำนวนพนักงานที่ทราบสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลให้น้อยที่สุดเท่าที่จะทำได้ เพื่อป้องกันมิให้ข้อมูลรั่วไหล

4.8 การตรวจสอบขอบเขตของสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล

ฝ่ายรับมือสถานการณ์จะตรวจสอบและรวบรวมข้อมูลเกี่ยวกับขอบเขตของสถานการณ์ที่สงสัยว่าจะเป็นสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ซึ่งรวมถึงข้อมูลต่อไปนี้ตามความเหมาะสม (ในกรณีที่เกี่ยวข้อง)

- วัน เวลาและลักษณะสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลที่เกิดขึ้นและเวลาที่พบสถานการณ์นั้น
- ประเภท และจำนวนของข้อมูลส่วนบุคคลที่อาจเสี่ยงต่อการได้รับผลกระทบ
- ระดับความเสี่ยงว่าจะเกิดความเสียหายหรือการใช้งานในทางที่ผิด และ
- รายชื่อผู้ที่ทราบถึงสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลดังกล่าว ไม่ว่าจะเป็นบุคลากรภายในหรือบุคคลภายนอกบริษัทฯ

ฝ่ายรับมือสถานการณ์อาจนำกระบวนการตรวจสอบสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลดังนี้มาใช้

- ลักษณะของสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลที่ทราบเป็นอย่างไร (เช่น การเจาะระบบ การสูญหายของอุปกรณ์ การโจรกรรมโดยบุคคลภายใน หรือสถานการณ์อื่น ๆ ที่มีลักษณะคล้ายคลึงกัน) และฝ่ายรับมือสถานการณ์ทราบสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยทางข้อมูลนี้ได้อย่างไร
- ลักษณะของข้อมูลที่ได้รับผลกระทบเป็นอย่างไร ขอบข่ายของข้อมูลที่ได้รับผลกระทบมีข้อมูลที่อาจก่อให้เกิดหน้าที่ในการแจ้งเตือน หรือหน้าที่อื่นตามกฎหมายหรือตามสัญญาหรือไม่
- บุคคลที่อาจได้รับผลกระทบเป็นบุคคลประเภทใดบ้าง (เช่น พนักงาน ผู้บริโภค หรือบุคคลอื่น ๆ)

- ที่อยู่ของผู้ที่อาจได้รับผลกระทบดังกล่าว (เช่น เฉพาะผู้ที่อยู่ในประเทศไทยเท่านั้น หรือรวมถึงผู้ที่อยู่ในประเทศอื่นด้วย)

- บริษัทฯ สามารถเข้าถึงประเภทและจำนวนข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณจากบันทึกได้หรือไม่

- ขอบเขตของสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลครอบคลุมแค่ไหน หากสถานการณ์ดังกล่าวเกี่ยวข้องกับการบุกรุกระบบสารสนเทศโดยไม่ได้รับอนุญาตแล้วนั้น มีเครื่องโฮสต์ใดที่อาจถูกเข้าถึงและมีข้อมูลใดบ้างที่อยู่ในเครื่องเหล่านั้น ตลอดจนผู้บุกรุกใช้วิธีการใดในการเข้าถึง

- สื่อได้รับทราบถึงสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลดังกล่าวแล้วหรือไม่

- มีมาตรการใดบ้างเพื่อรักษาความมั่นคงปลอดภัยของระบบโดยไม่ทำลายหลักฐานทางอิเล็กทรอนิกส์ที่สำคัญ (เช่น การตัดการเชื่อมต่อเซิร์ฟเวอร์ที่มีข้อมูลส่วนบุคคลออกจากอินเทอร์เน็ต หรือมาตรการอื่น ๆ ที่คล้ายคลึงกัน หรือมีความน่าจะเป็นที่การบันทึกภาพอุปกรณ์อาจได้รับผลกระทบแล้วหรือไม่)

- ใครเป็นผู้ทำหน้าที่รับมือเกี่ยวกับเทคนิคและความมั่นคงปลอดภัยของสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลบริษัทฯ และบริษัทฯ ได้มีการว่าจ้างให้บริษัทเทคโนโลยีสารสนเทศ/นิติวิทยาศาสตร์เพื่อดำเนินการดังกล่าวแล้วหรือไม่

- มีบุคลากรอื่นใดในบริษัทฯ ที่ควรทราบสถานการณ์ดังกล่าวหรือไม่ (เช่น ผู้บริหารอาวุโส ฝ่ายรับมือความสัมพันธ์นอกองค์กร ฯลฯ)

- ได้มีการติดต่อหน่วยงานบังคับใช้กฎหมายแล้วหรือไม่ หากติดต่อแล้ว ได้มีการติดต่อไปยังหน่วยงานใดบ้าง และใครเป็นผู้ที่ติดต่อไป

4.9 การรายงานต่อหน่วยงานบังคับใช้กฎหมาย

เพื่อเป็นส่วนหนึ่งของการตรวจสอบ ในกรณีที่มีการเข้าถึงข้อมูลหรือระบบสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาต ฝ่ายรับมือสถานการณ์จะต้องพิจารณาว่า มีความจำเป็นหรือสมควรต้องรายงานต่อหน่วยงานบังคับใช้กฎหมายหรือไม่

4.10 การพิจารณาข้อกำหนดทางกฎหมายที่ใช้บังคับ

ฝ่ายรับมือสถานการณ์จะใช้แนวทางการวิเคราะห์ในภาคผนวก 3 ว่ามีกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลใดบ้างที่อาจใช้บังคับกับสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลนี้ ("กฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล") (โปรดดูภาคผนวก 2) และพิจารณาว่า สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลดังกล่าวถือว่าเป็นการละเมิดความมั่นคงปลอดภัยของข้อมูลที่ต้องแจ้งไปยังผู้ที่ได้รับผลกระทบหน่วยงานรัฐบาล/หน่วยงานกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูล หรือบุคคลอื่น ๆ หรือไม่

ทั้งนี้ ฝ่ายรับมือสถานการณ์อาจพิจารณาขอคำแนะนำหรือคำปรึกษาจากผู้เชี่ยวชาญเป็นรายกรณี

4.11 การพิจารณาข้อกำหนดอื่น ๆ

นอกจากนี้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะให้คำแนะนำแก่ฝ่ายรับมือสถานการณ์ในเรื่องข้อกำหนดอื่น ๆ นอกเหนือจากกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ที่อาจกำหนดให้ต้องมีการรายงานสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ซึ่งรวมถึงข้อกำหนดดังนี้

- กฎหมายและระเบียบเฉพาะรายธุรกิจ/อุตสาหกรรมที่อาจนำมาใช้บังคับต่อสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล
- หน้าที่ตามสัญญาที่มีต่อพันธมิตรทางธุรกิจหรืออื่น ๆ
- นโยบายความเป็นส่วนตัว ประกาศหรือแถลงการณ์อื่น ๆ ในเอกสารเกี่ยวกับการชี้แจงทั้งของภายในและนอกองค์กร
- คำสัญญาที่ไม่ได้มีผลผูกพันหรือนโยบายบริษัทที่มีการเผยแพร่ต่อสาธารณะ

4.12 การรายงานต่อหน่วยงานรัฐบาล บุคคล หรือบุคคลอื่นๆ

(ก) เนื้อหาในคำชี้แจงและบทพูดสำหรับตอบคำถาม : ฝ่ายรับมือสถานการณ์ควรประสานงานกับฝ่ายสื่อสารองค์กรเพื่อกำหนดถ้อยคำและวิธีการเผยแพร่คำชี้แจงดังกล่าวให้เป็นไปตามข้อกำหนดเกี่ยวกับการชี้แจง

(ข) รูปแบบของคำชี้แจง: หากกฎหมายที่ใช้บังคับในขณะนั้นไม่ได้ระบุรูปแบบการชี้แจงไว้เป็นการเฉพาะ ในการบอกกล่าวไปยังผู้ที่ได้รับผลกระทบ (ที่ได้ให้ที่อยู่อีเมล ที่อยู่ติดต่ออื่นๆ ไว้ให้แก่บริษัทฯ) บริษัทฯ จะต้องส่งคำชี้แจงทางอีเมลให้กับผู้ที่ได้รับผลกระทบทุกราย พร้อมขอให้มีการตอบรับ ทั้งนี้ สำหรับผู้ที่ให้ที่อยู่ไปรษณีย์ไว้ให้แก่บริษัทฯ โดยไม่มีที่อยู่อีเมล จะต้องส่งคำชี้แจงผ่านทางไปรษณีย์ลงทะเบียน

ฝ่ายรับมือสถานการณ์จะต้องประสานงานกับฝ่ายสื่อสารองค์กรเพื่อกำหนดรูปแบบที่เหมาะสมในการส่งคำชี้แจง โดยพิจารณาจากข้อกฎหมายที่ใช้บังคับและต้นทุนที่ต้องใช้ หากไม่สามารถทำการชี้แจงได้ตามข้อนี้

ฝ่ายรับมือสถานการณ์ควรพิจารณาใช้วิธีการชี้แจงอื่นๆ แทน โดยอาจชะลอการส่งคำชี้แจงไว้หากหน่วยงานบังคับใช้กฎหมายเห็นว่า การชี้แจงไปยังผู้ที่ได้รับผลกระทบนั้นอาจเป็นอุปสรรคต่อกระบวนการสืบสวนสอบสวนทางอาญา

แนวปฏิบัตินี้ไม่ได้กำหนดให้ต้องชี้แจงผ่านช่องทางสาธารณะอื่น ๆ ด้วย เว้นแต่ กรณีที่มีกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่มีอยู่ในขณะนั้นกำหนด ทั้งนี้ ฝ่ายรับมือสถานการณ์ควรประสานงานกับฝ่ายการสื่อสารหรือประชาสัมพันธ์ของบริษัทฯ เพื่อพิจารณาผลกระทบและความจำเป็นในการชี้แจงผ่านต่อทางสาธารณะด้วย เช่น ผ่านทางเว็บไซต์หรือชี้แจงต่อสื่อมวลชนระดับประเทศ) ในกรณีที่บริษัทฯ พิจารณาแล้วว่า จะเป็นประโยชน์เกี่ยวกับลูกค้าสัมพันธ์หรือวัตถุประสงค์อื่นในบางกรณี

4.13 การตอบคำถาม

ฝ่ายรับมือสถานการณ์จะต้องวางแผนว่า บริษัทฯ ควรมีวิธีการในการตอบข้อซักถามของสื่อมวลชน รัฐบาล หรือฝ่ายอื่น ๆ อย่างไรบ้าง ในกรณีส่วนใหญ่แล้ว ควรพิจารณาข้อซักถามนั้นโดยตรวจสอบข้อกฎหมายและประสานงานกับฝ่ายสื่อสารองค์กรโดยตรงก่อน

ระยะที่ 3 : **มาตรการหลังเกิดสถานการณ์**

วัตถุประสงค์ของระยะที่ 3 คือ การจัดการกับผลกระทบของสถานการณ์ โดยฝ่ายรับมือสถานการณ์จะต้องจัดทำเอกสารบันทึกสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล และปรับปรุงมาตรการเชิงเทคนิคและเชิงองค์กร เพื่อป้องกันไม่ให้เกิดสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลในลักษณะที่คล้ายคลึงกันอีกในอนาคต พร้อมกระบวนการในการทบทวนและพิจารณารายละเอียดกรมธรรม์ประกันภัยที่เกี่ยวข้อง (หากมี) ด้วย

4.14 ข้อกำหนดเรื่องการจัดทำบันทึกเอกสาร

ไม่ว่าจะมีการพิจารณาให้นำกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลมาใช้บังคับกับสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลหรือไม่ก็ตาม ผู้รับมือสถานการณ์ลำดับแรกจะต้องจัดทำเอกสารบันทึกสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่ง การประเมินทางกฎหมายซึ่งกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไม่ใช้บังคับ

4.15 มาตรการเพื่อการแก้ไข

ฝ่ายรับมือสถานการณ์ คณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกัน กำหนดมาตรการ ที่จำเป็นเพื่อป้องกันไม่ให้เกิดสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลในลักษณะที่คล้ายคลึงกันอีกในอนาคต ซึ่งรวมถึงนโยบาย การฝึกอบรมเพื่อสร้างความเข้าใจ กระบวนการสำหรับพนักงาน ฝ่ายรับมือสถานการณ์ควรประเมินความสัมพันธ์กับบุคคลภายนอกที่อาจเกี่ยวข้องกับสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล พร้อมดำเนินการต่างๆ ตามความเหมาะสม เช่น การแก้ไขสัญญา การ

แก้ไขกระบวนการต่าง ๆ และ/หรือ การฝึกอบรม การปรับปรุงมาตรการความปลอดภัย การเลือกผู้ให้บริการรายใหม่ เป็นต้น ขณะเดียวกันบุคคลภายนอกจะต้องมีหน้าที่ตามสัญญาที่จะต้องแจ้งให้คู่สัญญาอีกฝ่ายในบริษัทฯ ทราบโดยทันที หากเกิดสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล ไม่ว่าจะเป็นสถานการณ์ที่เกิดขึ้นจริงหรือสงสัยว่าจะเกิดขึ้นก็ตาม และคู่สัญญานั้นควรแนะนำให้ฝ่ายกฎหมายและฝ่ายเทคโนโลยีสารสนเทศขององค์กรตน ทำการปรับเปลี่ยนกระบวนการต่าง ๆ ด้วย

4.16 กรมธรรม์ประกันภัย

ฝ่ายรับมือสถานการณ์จะต้องพิจารณากรมธรรม์ประกันภัยที่เกี่ยวข้องกับบริษัทฯ (หากมี) เพื่อพิจารณาเงื่อนไขตามข้อกำหนดในกรมธรรม์ประกันภัยที่ยังคงมีผลบังคับ รวมถึงดูข้อกำหนดในเรื่องเวลา เนื้อหา และรูปแบบของคำชี้แจงอีกด้วย

ภาคผนวก 1

แบบฟอร์มรายงานสถานการณ์เกี่ยวกับความมั่นคงปลอดภัย

คำอธิบายสถานการณ์เกี่ยวกับความมั่นคงปลอดภัย	....
วันและเวลาที่ได้มีการระบุการพบสถานการณ์เกี่ยวกับความมั่นคงปลอดภัย	....
ผู้ที่ระบุเหตุการละเมิดข้อมูลส่วนบุคคล	ชื่อ..... ตำแหน่ง..... ฝ่าย..... ประเทศ..... ที่อยู่อีเมล..... หมายเลขโทรศัพท์.....
พนักงานที่รายงาน:	ชื่อ..... ตำแหน่ง..... ฝ่าย..... ประเทศ..... ที่อยู่อีเมล..... หมายเลขโทรศัพท์.....
ระบบที่ได้รับผลกระทบ	....

ประเภทบุคคลที่ได้รับผลกระทบ เช่น ลูกค้า พันธมิตรทางธุรกิจ พนักงาน ผู้ติดต่อในกรณีฉุกเฉินสำหรับพนักงาน ผู้เยาว์ ผู้พิการ	....
ประเภทของข้อมูลที่ได้รับผลกระทบ	....
รายชื่อผู้ที่ได้รับรายงานสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลแล้ว	....

กรุณาส่งอีเมลไปยังที่อยู่อีเมลสำหรับติดต่อฝ่ายรับมือสถานการณ์ที่ให้ไว้ในแนวปฏิบัตินี้

ภาคผนวก 2

สรุปสาระสำคัญของกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล - ประเทศไทย

<table>
<tr><th>ลำดับที่</th><th>กฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล</th><th>รายละเอียด</th></tr>
<tr><td>1.</td><td>พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พรบ. คุ้มครองข้อมูลส่วนบุคคล”)</td><td>
ข้อกำหนดว่าด้วยการแจ้งเตือนตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมีอยู่ 2 ประเภทด้วยกัน
<table>
<tr><th>1. หน้าที่ในการแจ้งต่อหน่วยงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล</th><th>2 .หน้าที่ในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ</th></tr>
<tr><td>โดยไม่ล่าช้าภายใน 72 ชั่วโมงนับตั้งแต่ผู้รับมือสถานการณ์ลำดับแรกทราบสถานการณ์[1]</td><td>โดยไม่ล่าช้า</td></tr>
<tr><td>แจ้งการเกิดเหตุการละเมิดข้อมูลส่วนบุคคล</td><td>แจ้งให้ทราบเรื่องการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลและมาตรการแก้ไขเยียวยา</td></tr>
<tr><td>มีแนวโน้มก่อให้เกิดความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล</td><td>มีแนวโน้มก่อให้เกิดความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล</td></tr>
<tr><td>ข้อยกเว้นไม่ต้องแจ้งเหตุการละเมิดข้อมูล</td><td>ข้อยกเว้นไม่ต้องแจ้งเหตุการละเมิดข้อมูลส่วน</td></tr>
</table>
</td></tr>
</table>

[1] แนะนำให้ปฏิบัติตามข้อกำหนดในพรบ. คุ้มครองข้อมูลส่วนบุคคล กล่าวคือ แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยถือว่าขณะที่ผู้จัดการเหตุการณ์ลำดับแรกทราบเหตุการณ์เป็นขณะเดียวกันกับที่ผู้ควบคุมข้อมูลส่วนบุคคล (บริษัท) ทราบเหตุการณ์ ทั้งนี้ หลักเกณฑ์การนับเวลาตั้งแต่ทราบเหตุสามารถติดตามการเปลี่ยนแปลงวิธีการนับเวลาหรือหลักเกณฑ์เพิ่มเติมใด ๆ ได้จากหลักเกณฑ์หรือวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจประกาศกำหนดในภายหลัง

ส่วนบุคคลและวิธีการแจ้งสถานการณ์จะมีกำหนดไว้ในกฎหมายลำดับรองต่อไป	บุคคลและวิธีการแจ้งสถานการณ์จะมีกำหนดไว้ในกฎหมายลำดับรองต่อไป

- *"ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้:*

  *(4)...**แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ**เท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล **ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย** ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด(37 มาตรา) "*

- *"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(83 มาตรา) "*

- *"ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้:*

  (2)...จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น(40 มาตรา) "

		• *"ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 40โดยไม่มีเหตุอันควร หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตราซึ่งได้นำมาใช้บังคับโดย (5) 37 38 อนุโลมตามมาตราวรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท (86 มาตรา) "*
2.	พระราชบัญญัติการรักษาความปลอดภัยมั่นคงไซเบอร์ พ.ศ. 2562 "**พ.ร.บ.การรักษาความปลอดภัยมั่นคงไซเบอร์**("	• พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์กำหนดให้มีการรายงานต่อหน่วยงานที่มีอำนาจ โดยเป็นข้อกำหนดที่นำมาใช้บังคับกับองค์กรที่มีโครงสร้างพื้นฐานสำคัญทาง "สารสนเทศตามกฎหมายลำดับรองที่ออกตามมาตราของพระราชบัญญัตินี้ 49และสำหรับภัยคุกคามไซเบอร์ที่มีผลกระทบสำคัญ • *"เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ 4 ทั้งนี้ คณะกรรมการกำกับดูแลเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (กฎหมายอาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้)" (มาตรา 57)* • *" หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา 57 โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท" (มาตรา 37)*

ภาคผนวก 3

แนวทางกฎหมายว่าด้วยการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

1. แนวทางในการพิจารณากำหนด - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ฝ่ายรับมือสถานการณ์จะต้องวิเคราะห์ลักษณะ ขอบข่าย และความรุนแรงของสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลตามทิศทางและแนวทางที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้คำแนะนำ ซึ่งควรทำเป็นรายกรณีไป โดยพิจารณาจากชุดคำถามต่อไปนี้

<u>หมายเหตุ</u>: ในทุกกรณี ฝ่ายรับมือสถานการณ์จะต้องตรวจสอบว่า หน่วยงานที่มีอำนาจได้ออกกฎหมายลำดับรองหรือแนวทางปฏิบัติเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลและการประเมินความเสี่ยงแล้วหรือไม่ หากมีการออกออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้วจะต้องนำมาพิจารณาร่วมกับชุดคำถามต่อไปนี้

***คำถามที่ 1**: สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลนี้เกี่ยวข้องกับ "ข้อมูลส่วนบุคคล" ตามคำนิยามในพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่*

(หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 2: *สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลเกี่ยวกับการทำลาย สูญหาย หรือแก้ไขโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย หรือการเปิดเผยหรือเข้าถึงข้อมูลส่วนบุคคลที่รับส่ง จัดเก็บ หรือประมวลผล โดยการเปิดเผยหรือเข้าถึงนั้นไม่ได้รับอนุญาตใช่หรือไม่ (การ "ละเมิดข้อมูลส่วนบุคคล")*

(หากใช่ กรุณาอ่านคำถามต่อไป)

***คำถามที่ 3**: การละเมิดข้อมูลส่วนบุคคลดังกล่าวอาจก่อให้เกิดความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลตามแนวทางดังกล่าวหรือไม่*

(หมายเหตุ: การประเมินความเสี่ยงควรพิจารณาจากกฎหมายลำดับรองหรือแนวทางปฏิบัติหากมีการออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้ว เช่น การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น)

(หากใช่ กรุณาอ่านคำถามต่อไป)

***คำถามที่ 4**: มีกฎหมายลำดับรองใดที่ยกเว้นให้ไม่ต้องรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ หากมี ข้อยกเว้นนั้นนำมาใช้บังคับได้หรือไม่*

(หากคำตอบข้อ 4 คือไม่มีข้อยกเว้นหรือข้อยกเว้นที่มีไม่สามารถนำมาใช้บังคับแก่กรณีได้ ฝ่ายรับมือสถานการณ์จะต้องพิจารณาจัดทำ<u>รายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล</u>)

ฝ่ายรับมือสถานการณ์ดำเนินการตามคำถามข้อถัดไป เพื่อพิจารณาว่าจำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลด้วยหรือไม่

คำถามที่ 5*: มีความเป็นไปได้ที่ความเสี่ยงนั้นจะพิจารณาได้ว่าเป็นความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลหรือไม่*

แนวทางการประเมินความเสี่ยง – ในการพิจารณาว่ามีความเสี่ยงสูงนั้นจะต้องพิจารณาตามรายการต่อไปนี้เป็นรายกรณีไป

- ประเภท (ความละเอียดอ่อน) ของข้อมูลส่วนบุคคลที่เกี่ยวกับสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลนั้น
- ปริมาณข้อมูลส่วนบุคคล
- จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
- ประเภทของการละเมิดข้อมูล
- ความสามารถในการระบุถึงตัวตนของบุคคลได้โดยง่าย
- ลักษณะพิเศษของผู้ที่ได้รับผลกระทบ (เช่น กลุ่มที่มีความอ่อนไหว)
- ลักษณะพิเศษของผู้ควบคุมข้อมูลส่วนบุคคล

(หมายเหตุ: การประเมินความเสี่ยงควรพิจารณาจากกฎหมายลำดับรองหรือแนวทางปฏิบัติหากมีการออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้ว)

คำถามที่ 6 *: มีกฎหมายลำดับรองใดที่ยกเว้นให้ไม่ต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคลหรือไม่ หากมีข้อยกเว้นนั้นนำมาใช้บังคับได้หรือไม่*

(หากคำตอบข้อ 6 คือไม่มีข้อยกเว้น หรือข้อยกเว้นที่มีไม่สามารถบังคับใช้แก่กรณีได้ ฝ่ายรับมือสถานการณ์จะต้องพิจารณา (1) รายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ (2) แจ้งต่อเจ้าของข้อมูลส่วนบุคคล

2. แนวทางในการพิจารณากำหนด – พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์

ฝ่ายรับมือสถานการณ์จะต้องวิเคราะห์ลักษณะ ขอบข่าย และความรุนแรงของสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลตามทิศทางและแนวทางตามที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้คำแนะนำ ซึ่งควรทำเป็นรายกรณีไป โดยพิจารณาจากชุดคำถามต่อไปนี้

หมายเหตุ: ในทุกกรณี จะต้องตรวจสอบว่า หน่วยงานที่มีอำนาจได้ออกกฎหมายลำดับรองหรือแนวทางปฏิบัติเกี่ยวกับโครงสร้างพื้นฐานสำคัญ การละเมิดข้อมูลส่วนบุคคล และการประเมินความเสี่ยงแล้วหรือไม่ หากมีการออกออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้วจะต้องนำมาพิจารณาร่วมกับชุดคำถามต่อไปนี้

***คำถามที่ 1**: มีกฎหมายลำดับรองใดที่กำหนดหลักเกณฑ์ของหน่วยงานโครงสร้างพื้นฐานสำคัญหรือไม่ หากมีบริษัทฯ เป็นไปตามหลักเกณฑ์ใด*

(หากใช่ กรุณาอ่านคำถามต่อไป)

***คำถามที่ 2**: สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลถือนี้เป็น "ภัยคุกคามทางไซเบอร์" ตามคำนิยามในพ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์หรือไม่*

(หากใช่ กรุณาอ่านคำถามต่อไป)

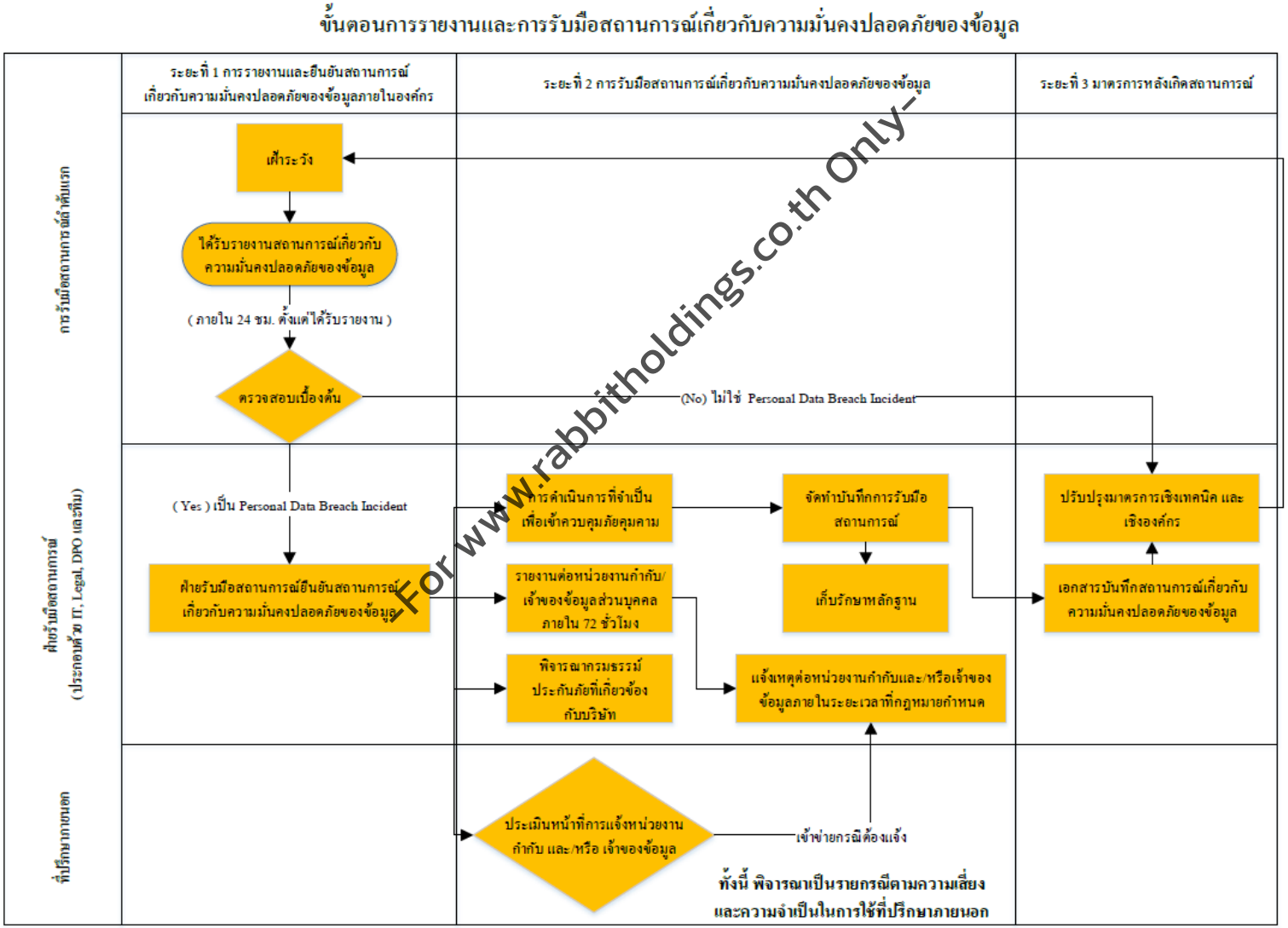
***คำถามที่ 3**: มีกฎหมายลำดับรองใดที่กำหนดหลักเกณฑ์ภัยคุกคามทางไซเบอร์ที่มี "นัยสำคัญ" หรือไม่ หากมี สถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลนี้เป็นไปตามหลักเกณฑ์ใด*

(หากมี ฝ่ายรับมือสถานการณ์จะต้องพิจารณาจัดทำรายงานต่อคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) และคณะกรรมการกำกับดูแลเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (กกม.) ตามกฎหมาย

หมายเหตุ: ควรระบุแนวทางการประเมินความเสี่ยงตามกฎหมายหรือระเบียบเฉพาะส่วนธุรกิจ (ถ้ามี) เพิ่มเติม และควรปรับปรุงแนวทางการประเมินความเสี่ยงนี้ให้เป็นข้อมูลล่าสุดเป็นครั้งคราว

ภาคผนวก 4

แผนผังขั้นตอนการรายงานและรับมือสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูล



ภาคผนวก 5

ตัวอย่างสถานการณ์ที่จะต้องรายงานแก่ฝ่ายรับมือสถานการณ์

สถานการณ์ต่อไปนี้เป็นเพียงตัวอย่างบางส่วนซึ่งมีลักษณะจะต้องรายงานแก่ฝ่ายรับมือสถานการณ์

- การโจรกรรมหรือสูญหายของคอมพิวเตอร์ คอมพิวเตอร์แล็ปท็อป โทรศัพท์สมาร์ตโฟน อุปกรณ์บันทึกข้อมูลแบบพกพา (Thumb Drive) หรืออุปกรณ์บันทึกข้อมูลอื่นที่เป็นของบริษัทฯ หรือของพนักงานที่ใช้อุปกรณ์ดังกล่าวบันทึกข้อมูลที่เกี่ยวข้องกับบริษัทฯ
- การบุกรุกหรือโจรกรรมภายในสถานที่ทำงานของบริษัทฯ
- เมื่อมีการโจมตีซึ่งอาจกระทำผ่านระบบคอมพิวเตอร์หรือด้วยวิธีการอื่นที่ก่อให้เกิดความเสี่ยงต่อฐานข้อมูล คอมพิวเตอร์ เครือข่าย การติดต่อสื่อสารของบริษัทฯ ฯลฯ
- เมื่อพนักงานได้เห็น ใช้ เข้าถึง หรือเปิดเผยข้อมูล แฟ้มข้อมูล หรือฐานข้อมูลนอกเหนือจากขอบเขตหน้าที่ที่ได้รับมอบหมาย
- เมื่อมีบุคคลภายนอก/ผู้ให้บริการภายนอก (Third Party/Outsourcing) กระทำผิดสัญญาห้ามเปิดเผยข้อมูลหรือสัญญาการรักษาความลับ
- สถานการณ์ใดที่กล่าวมาข้างต้นซึ่งเกี่ยวเนื่องกับผู้ขายหรือผู้ให้บริการอื่นของบริษัทฯ

ภาคผนวก 6

รายละเอียดการติดต่อผู้รับมือสถานการณ์ลำดับแรก

บุคคลที่เกี่ยวข้อง	
ฝ่ายงานที่เกิดเหตุสงสัยว่าเกิดเหตุ	(1) ผู้บังคับบัญชาสูงสุดตามสายงาน (2) พนักงานผู้ที่เกี่ยวข้อง
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	(1) นางสาวหัสยา นุ่นแจ้ง ตำแหน่งรองผู้อำนวยการฝ่ายกฎหมายและกำกับดูแล อีเมล : hassaya.n@ucity.co.th โทรศัพท์ : 02-2738838 (2) นายชัยกฤษ มงคลสักวานนท์ ตำแหน่งผู้จัดการอาวุโสฝ่ายเทคโนโลยีสารสนเทศ อีเมล : chaikrit.m@ucity.co.th โทรศัพท์ : 02-2738838
ฝ่ายเทคโนโลยีสารสนเทศ	นายชัยกฤษ มงคลสักวานนท์ ตำแหน่งผู้จัดการอาวุโสฝ่ายเทคโนโลยีสารสนเทศ อีเมล : chaikrit.m@ucity.co.th โทรศัพท์ : 02-2738838
ฝ่ายกฎหมาย	นางสาวหัสยา นุ่นแจ้ง ตำแหน่งรองผู้อำนวยการฝ่ายกฎหมายและกำกับดูแล อีเมล : hassaya.n@ucity.co.th โทรศัพท์ : 02-2738838
คณะทำงานข้อมูลส่วนบุคคล	(1) นายอภินันท์ อู่ทอง ตำแหน่งผู้อำนวยการ - ฝ่ายบริหารทรัพย์สิน อีเมล : apinant.u@ucity.co.th โทรศัพท์ : 02-2738838

	(2) นางสาวณัฐิตา มาปัด ตำแหน่งผู้จัดการอาวุโส - ฝ่ายทรัพยากรมนุษย์ อีเมล : nattita.m@ucity.co.th โทรศัพท์ : 02-2738838 (3) นางสาวทัศลียา สังขสุวรรณ์ ตำแหน่งผู้จัดการอาวุโส - ฝ่ายบัญชี อีเมล : thatsaleya.s@ucity.co.th โทรศัพท์ : 02-2738838 (4) นายธันว์ เชาวน์นิรัติศัย ตำแหน่งผู้จัดการ - ฝ่ายจัดซื้อจัดจ้าง อีเมล : thun.c@ucity.co.th โทรศัพท์ : 02-2738838

ภาคผนวก 7

รายละเอียดการติดต่อฝ่ายรับมือสถานการณ์

บุคคลที่เกี่ยวข้อง	
ผู้รับมือสถานการณ์ลำดับแรก	
ฝ่ายเทคโนโลยีสารสนเทศ	นายชัยกฤษ มงคลสักวานนท์ ตำแหน่งผู้จัดการอาวุโสฝ่ายเทคโนโลยีสารสนเทศ อีเมล : chaikrit.m@ucity.co.th โทรศัพท์ 02-2738838
ฝ่ายกฎหมาย	นางสาวหัสยา นุ่นแจ้ง ตำแหน่งรองผู้อำนวยการฝ่ายกฎหมายและกำกับดูแล อีเมล : hassaya.n@ucity.co.th โทรศัพท์ 02-2738838
คณะทำงานข้อมูลส่วนบุคคล	(1)นายอภินันท์ อู่ทอง ตำแหน่งผู้อำนวยการ - ฝ่ายบริหารทรัพย์สิน อีเมล : apinant.u@ucity.co.th โทรศัพท์ : 02-2738838 (2)นางสาวณัฐิตา มาปัด ตำแหน่งผู้จัดการอาวุโส - ฝ่ายทรัพยากรมนุษย์ อีเมล : nattita.m@ucity.co.th โทรศัพท์ : 02-2738838 (3) นางสาวทัศลียา สังขสุวรรณ์ ตำแหน่งผู้จัดการอาวุโส - ฝ่ายบัญชี อีเมล : thatsaleya.s@ucity.co.th โทรศัพท์ : 02-2738838 (4) นายธันว์ เชาวน์นิรัติศัย ตำแหน่งผู้จัดการ - ฝ่ายจัดซื้อจัดจ้าง อีเมล : thun.c@ucity.co.th โทรศัพท์ : 02-2738838

ภาคผนวก 8

การพิจารณาระดับความรุนแรงของเหตุการละเมิดข้อมูลส่วนบุคคลและการรับมือ

ฝ่ายรับมือสถานการณ์พิจารณาระดับความรุนแรงของเหตุการละเมิดข้อมูลส่วนบุคคลจากระดับความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล (“**ความเสี่ยง**”)

ความเสี่ยง	การแจ้ง
ไม่มีความเสี่ยง	ไม่ต้องแจ้ง
มีความเสี่ยง	แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล
มีความเสี่ยงสูง	แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล แจ้งเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างกรณีเหตุการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง

ได้แก่ กรณีที่เหตุการละเมิดข้อมูลส่วนบุคคลนั้น ส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ไม่ว่าเหตุการละเมิดดังกล่าวจะส่งผลให้เกิดความเสียหายทางกายภาพ ความเสียหายต่อทรัพย์สิน หรือความเสียหายที่ไม่ใช่ทรัพย์สิน เช่น ก่อให้เกิดการเลือกปฏิบัติ การขโมยอัตลักษณ์หรือการฉ้อโกง การสูญเสียทางการเงิน หรือความเสียหายต่อชื่อเสียง

ในการพิจารณาว่ามีความเสี่ยงสูงนั้นจะต้องพิจารณาตามรายการต่อไปนี้เป็นรายกรณีไป

- เหตุการละเมิดข้อมูลส่วนบุคคลเกี่ยวข้องต่อข้อมูลส่วนบุคคลที่อ่อนไหว[2] (Sensitive Data) ซึ่งรวมถึงข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ เป็นต้น ก็จะถือว่าเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูง

- ปริมาณข้อมูลส่วนบุคคล

[2] ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

- จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
- ประเภทของการละเมิดข้อมูล
- ความสามารถในการระบุถึงตัวตนของบุคคลได้โดยง่าย
- ลักษณะพิเศษของผู้ที่ได้รับผลกระทบ) เช่น กลุ่มที่มีความอ่อนไหว ได้แก่ ผู้เยาว์ หรือผู้ไร้ความสามารถหรือเสมือนไร้ความสามารถ)
- ลักษณะพิเศษของผู้ควบคุมข้อมูลส่วนบุคคล

(หมายเหตุ: การประเมินความเสี่ยงสามารถพิจารณาจากกฎหมายลำดับรองหรือแนวทางปฏิบัติ หากมีการออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้ว)

ภาคผนวก 9

ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคล

รายละเอียดดังต่อไปนี้เป็นตัวอย่างแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล เพื่อพิจารณาว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด และความเสี่ยงในระดับใดที่ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือความเสี่ยงในระดับใดที่ต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคล

ลำดับ	ตัวอย่าง	แจ้งเหตุแก่ สคส.	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
1.	พนักงานจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ความเสี่ยงต่ำ เนื่องจากเมื่อ มีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้ว ข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
2.	บริษัทให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของบริษัท	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก
3.	ระบบไฟฟ้าใน call center ของบริษัทขัดข้อง โดยไฟดับชั่วคราว ส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัทไม่สามารถให้บริการได้ชั่วคราว	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งาน เนื่องจากปัญหาทางด้านเทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วนบุคคลดังกล่าวก็สามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ลำดับ	ตัวอย่าง	แจ้งเหตุแก่ สคส.	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
4.	บริษัทถูกภัยคุกคามทางไซเบอร์โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของบริษัทถูกเข้ารหัสโดย ผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้ และการถูก โจมตีจากมัลแวร์เรียกค่าไถ่ ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และไม่มีข้อมูลสำรอง นอกจากนี้ ยังอาจ ก่อให้เกิดความเสียหายต่อธุรกิจของบริษัท รวมถึงตัวเจ้าของข้อมูลส่วนบุคคล จึงต้องแจ้งเหตุ
5.	บริษัทได้รับการติดต่อจากลูกค้า 1 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก บริษัททำการตรวจสอบแล้วภายใน 24 ชั่วโมง พบว่า มีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน 10 ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล 10 รายที่ข้อมูลได้มีการรั่วไหล	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตาม บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม
6.	บริษัทให้บริการซื้อขายสินค้าออนไลน์ทั่วประเทศ ต่อมาบริษัทถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลรายชื่อลูกค้า รหัสผ่าน และประวัติการซื้อสินค้าถูกเข้าถึงและนำไปโพสต์บนอินเทอร์เน็ต	ต้องแจ้ง	ต้องแจ้งลูกค้าของบริษัทในส่วนที่มีข้อมูลรั่วไหลบนอินเทอร์เน็ต	ข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของลูกค้า จึงจำเป็นต้องแจ้งเหตุแก่ลูกค้า เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย
7.	บริษัทเป็นเว็บไซต์ผู้ให้บริการ Web Hosting ที่รับจ้าง	ต้องแจ้งผู้ว่าจ้างซึ่งเป็นผู้ควบคุมข้อมูล	ผู้ว่าจ้างซึ่งเป็นผู้ควบคุมข้อมูลส่วน	ในเบื้องต้นเป็นเพียงข้อผิดพลาดของโปรแกรมที่ทำให้เข้าถึงข้อมูลส่วน

ลำดับ	ตัวอย่าง	แจ้งเหตุแก่ สคส.	แจ้งเหตุแก่ เจ้าของข้อมูลส่วนบุคคล	เหตุผล
	ประมวลผลข้อมูลส่วนบุคคลจากผู้ว่าจ้าง เกิดปัญหาข้อผิดพลาดของโปรแกรมในการตรวจสอบสิทธิการเข้าถึง ทำให้ลูกค้าไม่สามารถเข้าใช้บริการได้ *(ข้อสังเกต: ในกรณีนี้บริษัทเป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่ทำตามคำสั่งของผู้ว่าจ้างซึ่งเป็นผู้ควบคุมส่วนบุคคล)*	ส่วนบุคคล เพื่อให้ผู้ว่าจ้างได้แจ้งสำนักงานฯ ต่อไป เนื่องจากมีผลกระทบต่อกลุ่มลูกค้าพอสมควร เพราะปัญหาดังกล่าวทำให้ กลุ่มลูกค้าไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้	บุคคล ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับผลกระทบ เนื่องจากยังไม่เกิดปัญหา	บุคคลไม่ได้ ซึ่งจากการสอบสวนยังไม่ปรากฏว่ามี ภัยคุกคามทางไซเบอร์แต่อย่างใด อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคล (ผู้ว่าจ้าง) และผู้ประมวลผลข้อมูลส่วนบุคคล (บริษัท) ต้องตรวจสอบข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกคามทางไซเบอร์ บริษัทซึ่งเป็นเว็บไซต์ผู้ให้บริการ Web Hosting ต้องรีบแจ้งผู้ว่าจ้างซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล และผู้ว่าจ้างต้องรีบแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลต่อไป
8.	ฝ่าย HR ของบริษัทถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก hacker ทำให้ผลตรวจสุขภาพประจำปีของพนักงานไม่สามารถเข้าถึงได้เป็นเวลา 30 ชั่วโมง	ต้องแจ้ง เนื่องจากข้อมูลผลตรวจสุขภาพของพนักงานเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว และสามารถระบุตัวบุคคลได้	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลที่มีความอ่อนไหว ผู้ที่ไม่หวังดีอาจนำไปใช้ในการกระทำความผิดหรือมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้	เนื่องจากข้อมูลที่ถูกละเมิดดังกล่าว รวมถึงข้อมูลสุขภาพด้วย เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องแจ้งเหตุ และตรวจสอบข้อมูลเพิ่มเติม
9.	โรงเรียนแห่งหนึ่งเกิดความผิดพลาดในการส่งข้อมูลของนักเรียนจำนวนมากทางอีเมลไปยังผู้รับเหมาในการให้บริการขนส่งสินค้าของโรงเรียน ไม่ใช่ผู้ปกครองนักเรียน	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าวไม่มีการเข้ารหัส และเป็นข้อมูลส่วนบุคคลของบุคคลจำนวนมาก ซึ่งอาจมีทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งผู้รับเหมาอาจจะ

ลำดับ	ตัวอย่าง	แจ้งเหตุแก่ สคส.	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
				นำข้อมูลดังกล่าวไปใช้โดยมิชอบและก่อให้เกิดความเสียหายได้
10.	บริษัททำการตลาดแบบตรงโดยการส่งข้อมูลส่วนบุคคลไปยังลูกค้าแต่ละราย แต่ด้วยความผิดพลาด จึงมีการใส่ที่อยู่ของบุคคลที่รับอีเมลทั้ง 100 คน เข้าไปในช่อง To หรือ Cc ทำให้ผู้รับอีเมลเห็นอีเมลที่มีข้อมูลส่วนบุคคลของลูกค้าคนอื่น	ต้องแจ้ง เนื่องจากเป็นการส่งข้อมูลของเจ้าของข้อมูลส่วนบุคคลจำนวนมาก จึงจำเป็นต้องแจ้งเหตุ แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลในอีเมลดังกล่าวอาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลภายหลังได้	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลหรือไม่ อาจขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไป และลักษณะของข้อมูลด้วย หากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด อาจถือว่ามีความเสี่ยงต่ำ ไม่จำเป็นต้องแจ้งเหตุ