แนวปฏิบัติการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
และการรายงานเหตุการละเมิดข้อมูลส่วนบุคคล
สำนักงานเศรษฐกิจการคลัง

จัดทำโดย

ศูนย์เทคโนโลยีสารสนเทศ

สำนักงานเศรษฐกิจการคลัง

สารบัญ

บทนำ

สำนักงานเศรษฐกิจการคลัง (สศค.) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เล็งเห็นถึงความสำคัญของข้อมูลส่วนบุคคลที่ สศค. จัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และตระหนักว่าในช่วงเวลาการประมวลผลข้อมูลส่วนบุคคล มีโอกาสที่จะเกิดเหตุการละเมิดข้อมูลส่วนบุคคลซึ่งต้องปฏิบัติให้เป็นไปตามหลักเกณฑ์และวิธีการที่กฎหมายกำหนด อย่างไรก็ตาม การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ) มีรายละเอียดค่อนข้างมากและมีหลายประเด็นที่เป็นเรื่องใหม่สำหรับการขับเคลื่อนเศรษฐกิจและยกระดับการคุ้มครองสิทธิของสังคมไทย ประกอบกับมาตรา ๓๗ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และแจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพ และตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ข้อ ๔ เหตุการละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยเหตุที่เกิดจากการละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใดซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่น โดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท

ดังนั้น สศค. จึงกำหนดกระบวนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลและแบบฟอร์มรายงานเหตุละเมิดข้อมูลส่วนบุคคลเพื่อแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลเพื่อใช้เป็นแนวทางในการปฏิบัติเมื่อเกิดเหตุต้องมีการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลที่เหมาะสม และสร้างความเชื่อมั่นต่อเจ้าของข้อมูลส่วนบุคคลที่ สศค. มีการนำข้อมูลส่วนบุคคลมาประมวลผล

วัตถุประสงค์

แนวปฏิบัติฉบับนี้จัดทำขึ้นเพื่อกำหนดขั้นตอนและกระบวนการตอบสนองเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ในการแก้ไขและลดผลกระทบต่อเจ้าของข้อมูลที่เกิดการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคลเพื่อให้มั่นใจว่าเจ้าของข้อมูลจะได้รับผลกระทบจากการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคลน้อยที่สุด รวมถึงการรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล

/ขอบเขต ...

ขอบเขต

กระบวนการปฏิบัติงานที่กำหนดไว้ในแนวปฏิบัติฉบับนี้ใช้กับการจัดการและการรายงานเหตุการละเมิดข้อมูลส่วนบุคคล ประกอบด้วยช่องทางการเฝ้าระวังและตรวจสอบกระบวนการตอบสนองเหตุการละเมิดข้อมูลส่วนบุคคล การรายงานเหตุการละเมิดข้อมูลส่วนบุคคล การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อผู้อำนวยการสำนักงานเศรษฐกิจการคลัง ภายใน ๒๔ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ หากเป็นกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล พร้อมแนวทางการเยียวยาเจ้าของข้อมูลส่วนบุคคลในการแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้าด้วย ทั้งนี้ สศค. จะดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

สศค. อาจดำเนินการทบทวนเพื่อปรับปรุง แก้ไขหรือเพิ่มเติมแนวปฏิบัตินี้เป็นครั้งคราว โดยจะแจ้งให้ผู้ปฏิบัติงานทราบตามความจำเป็นและเหมาะสมกับสถานการณ์ปัจจุบัน

คำนิยาม

คำศัพท์	ความหมาย
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต ที่อยู่อีเมล (email address) ทะเบียนรถยนต์ IP Address, Cookies, Log File เป็นต้น
การประมวลผลข้อมูลส่วนบุคคล (Processing of Personal Data)	การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล อันจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในลักษณะใดลักษณะหนึ่งได้ เช่น การจัดเก็บ รวบรวมการบันทึก การจัดระบบ จัดโครงสร้าง การปรับปรุง หรือ การแก้ไขข้อมูล การดึงข้อมูล การให้คำปรึกษาที่ต้องใช้ข้อมูลในการให้คำปรึกษา การใช้ข้อมูล การเปิดเผยด้วยการส่งต่อ การเผยแพร่ หรือ การกระทำใด ๆ เพื่อให้ข้อมูลสามารถเข้าถึงหรือใช้งานได้ การรวมข้อมูลเข้าด้วยกัน การดำเนินการเพื่อให้ข้อมูลสอดคล้องกัน การจำกัดการใช้งาน การลบ หรือการทำลายข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่สามารถระบุตัวตนได้จากข้อมูลส่วนบุคคล และให้หมายรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ รวมตลอดทั้งผู้ที่ถือว่าเป็นเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

/คำศัพท์ ...

คำศัพท์	ความหมาย
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	สำนักงานเศรษฐกิจการคลัง (บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล)
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	บุคคลหรือองค์กรใดที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
การละเมิดข้อมูลส่วนบุคคล (Data Breach)	การละเมิดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีการเก็บ รวบรวม ใช้ หรือเผยแพร่ ซึ่งนำไปสู่ผลกระทบของเจ้าของข้อมูลส่วนบุคคล เกิดความเสียหายและความไม่ชอบด้วยกฎหมาย เช่น เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ หรือเหตุอื่นใด เช่น ข้อมูลส่วนบุคคลสูญหายหรือถูกโจรกรรม การประมวลผลข้อมูลส่วนบุคคลผิดพลาด หรือไม่ถูกต้อง ผิดวัตถุประสงค์ที่กำหนดไว้
ประเภทของการละเมิดข้อมูลส่วนบุคคล	การละเมิดข้อมูลส่วนบุคคล ๓ ประเภท (๑) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ (๒) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ (๓) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO	เจ้าหน้าที่ที่จะเข้ามาดูแลและให้ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลทั้งในองค์กร ไม่ว่าจะเป็นข้อมูลภายในขององค์กร หรือจะเป็นข้อมูลภายนอก โดย DPO มีหน้าที่ (๑) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลและตรวจสอบการใช้ข้อมูลส่วนบุคคล (๒) ศึกษาและทำความเข้าใจกระบวนการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

คำศัพท์	ความหมาย
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO (ต่อ)	(๓) ติดต่อประสานงานภายในหน่วยงานให้มีการดำเนินงานที่ถูกต้องตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งให้คำแนะนำแก่หน่วยงาน ลูกจ้าง หรือผู้รับจ้างเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ (๔) ทบทวนกิจกรรมการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานให้ถูกต้องและเป็นปัจจุบัน
ทีมรับมือ CERT/IT/SOC (Security Operations Center)	เป็นทีมปฏิบัติการด้านความปลอดภัยทางไซเบอร์ ทำหน้าที่เฝ้าระวัง ป้องกัน ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์แบบเรียลไทม์ โดยใช้เทคโนโลยีและเครื่องมือที่ทันสมัยในการตรวจสอบเครือข่าย ระบบงาน และแอปพลิเคชันขององค์กร เพื่อให้แน่ใจว่าการดำเนินงานขององค์กรเป็นไปอย่างปลอดภัย รวมถึงสนับสนุนและประสานงานภายในหน่วยงาน ดังนี้ (๑) ประสานงานและให้ความร่วมมือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ สศค. (๒) ในกรณีพบเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหล ถูกละเมิด ให้แจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ สศค. โดยไม่ชักช้า ภายใน ๒๔ ชั่วโมง นับตั้งแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เนื่องจากจะต้องแจ้งต่อไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน ๗๒ ชั่วโมง (๓) รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาในการปฏิบัติหน้าที่ (๔) ประสานงานและให้ความร่วมมือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ สศค. ในการดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล หรือข้อร้องเรียนใด ๆ ตามกฎหมายว่าด้วยคุ้มครองข้อมูลส่วนบุคคลในกรณีที่หน่วยงานเป็นผู้เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
คทง. BCM	คณะทำงานดำเนินการตามแผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Management: BCM) หรืออาจเรียกชื่ออื่น
แผน BCP	แผนบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan: BCP) หรือแผนดำเนินธุรกิจอย่างต่อเนื่อง หรืออาจเรียกชื่ออื่น
แผน DRP	แผนกู้คืนระบบหรือ DRP (Disaster Recovery Plan)
หน่วยงาน	หน่วยงานภายใต้สังกัดสำนักงานเศรษฐกิจการคลัง รวมทั้งหน่วยงานตามภารกิจเฉพาะ

/แผนการรับมือ ...

แผนการรับมือเหตุการละเมิดข้อมูลส่วนบุคคล

ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ (ประกาศฯ) ข้อ ๔ มีขั้นตอนและหลักเกณฑ์ที่ต้องปฏิบัติตามอย่างเคร่งครัด เพื่อให้เป็นไปตามที่กฎหมายกำหนดและลดผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล

เมื่อหน่วยงานได้รับแจ้งข้อมูลเบื้องต้นว่าเกิดเหตุการณ์ไม่ปกติ เข้าข่ายเป็นเหตุการละเมิดข้อมูลส่วนบุคคล จะต้องดำเนินการตาม ๕ ขั้นตอนหลัก ๆ ดังต่อไปนี้

ขั้นตอนที่ ๑ ประเมินความน่าเชื่อถือของข้อมูลการละเมิดที่ได้รับแจ้งและตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถทำได้

หน่วยงานจะต้องดำเนินการประเมินว่าข้อมูลการละเมิดที่ได้รับแจ้งเบื้องต้นนั้น มีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลจริงหรือไม่ โดยหน่วยงานควรดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ประกอบด้วย

- มาตรการเชิงองค์กร (Organizational Measures) เช่น นโยบายความมั่นคงปลอดภัยของข้อมูล การประเมินความเสี่ยง การสร้างความตระหนักและการอบรมความรู้แก่บุคลากรภายในองค์กร เป็นต้น
- มาตรการเชิงเทคนิค (Technical Measures) เช่น ระบบการเข้ารหัสข้อมูล (encryption) การทำข้อมูลแฝง (Pseudonymisation) เป็นต้น
- มาตรการทางกายภาพ (Physical Measures) เช่น การมีระบบความปลอดภัย การติดตั้งกล้องวงจรปิด สอดส่องดูแลบริเวณที่มีการเก็บเซิร์ฟเวอร์ของหน่วยงาน เป็นต้น ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว

ทั้งนี้ หน่วยงานจะต้องดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับหน่วยงานเอง เพื่อยืนยันว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นรวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพื่อประกอบการพิจารณาในการดำเนินการขั้นตอนต่อไป

ขั้นตอนที่ ๒ ป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที

หน่วยงานได้ดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดรวมทั้งประเมินความเสี่ยงของเหตุการละเมิดข้อมูลส่วนบุคคลแล้ว พบว่าเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้หน่วยงานดำเนินการใช้มาตรการในการป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลนั้นสิ้นสุดลง หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมเท่าที่สามารถกระทำได้โดยทันที

/ขั้นตอน ...

ขั้นตอนที่ ๓ แจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

เมื่อพิจารณาจากข้อเท็จจริงแล้วเห็นว่ามีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง

- หน่วยงานจะต้องแจ้งผู้อำนวยการ สศค. ทราบภายใน ๒๔ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

- หากเหตุการละเมิดดังกล่าวมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และหน่วยงานไม่สามารถแจ้งเหตุละเมิดดังกล่าวได้ จะต้องดำเนินการชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องกับการแจ้งเหตุล่าช้าเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานเศรษฐกิจการคลังโดยเร็วไม่เกิน ๑๐ วันนับตั้งแต่ทราบเหตุ

สำนักงานเศรษฐกิจการคลังจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ กรณีมีเหตุจำเป็นที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถแจ้งเหตุการละเมิดที่มีความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลต้องรายงานโดยไม่ชักช้าแต่ไม่เกิน ๑๕ วันนับแต่ทราบเหตุ โดย สคส. จะพิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าตามที่เห็นสมควร (อ้างอิงประกาศฯ ข้อ ๗)

ขั้นตอนที่ ๔ แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หน่วยงานจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงนั้นให้แก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการละเมิดดังกล่าวโดยไม่ชักช้า พร้อมกับแจ้งแนวทางในการเยียวยาผลกระทบที่เกิดจากเหตุการละเมิดดังกล่าวไปด้วยให้สำนักงานเศรษฐกิจการคลังพร้อมรายงานตาม ขั้นตอนที่ ๓ เพื่อพิจารณาด้วย

วิธีการแจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลเป็นรายบุคคล หนังสือ หรือโดยวิธีการทางอิเล็กทรอนิกส์ หากโดยสภาพหน่วยงานไม่สามารถดำเนินการแจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลเป็นรายบุคคล เนื่องจากไม่มีวิธีการติดต่อหรือโดยเหตุจำเป็นอื่นใด หน่วยงานอาจแจ้งเหตุการละเมิดเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ หรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้ เช่น เว็บไซต์ที่ให้บริการแก่ผู้รับบริการ เป็นต้น ทั้งนี้ การแจ้งในลักษณะดังกล่าวจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ขั้นตอนที่ ๕ ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว

หน่วยงานจะต้องดำเนินการป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน

/การประเมิน ...

การประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ได้วางหลักการให้สำนักงานเศรษฐกิจการคลังในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ทั้งยังวางหลักให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ สคส. โดยไม่ชักช้าภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

ดังนั้น การประเมินความเสี่ยงเหตุการละเมิดข้อมูลส่วนบุคคล จึงแยกประเมินเป็นเหตุการละเมิดจากบุคคลและเหตุการละเมิดจากระบบการรักษาความมั่นคงปลอดภัยของข้อมูล ดังนี้

๑ การประเมินความเสี่ยงเหตุการละเมิดจากบุคคล ต้องประเมินจากผลกระทบที่อาจเกิดความร้ายแรง ละเมิดต่อเจ้าของข้อมูลส่วนบุคคล เช่น ถูกนำไปประจาน ดูถูก ดูหมิ่นเกลียดชัง ถูกหมิ่นประมาท ถูกเลือกปฏิบัติ ถูกสะกดรอยตาม ถูกทำร้ายร่างกาย การแบล็คเมล์เรียกค่าไถ่ ถูกสวมรอยบุคคล ขโมยรหัสผ่านหรือเข้าถึงข้อมูลอื่น ๆ ต่อไป

๒ การประเมินความเสี่ยงเหตุการละเมิดจากระบบการรักษาความมั่นคงปลอดภัย ต้องประเมินจากความร้ายแรงของผลกระทบ (Impact Levels) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ประกอบกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ทั้งนี้ สำนักงานเศรษฐกิจการคลังได้จัดทำปัจจัยความเสี่ยงเพื่อคำนวณคะแนนสำหรับระดับความเสี่ยง ดังนี้

การพิจารณาปัจจัยความเสี่ยง

เป็นการกำหนดเกณฑ์คะแนนความเสี่ยงในแต่ละหัวข้อประเมินปัจจัยความเสี่ยงที่เกี่ยวข้องหากเกิดเหตุการละเมิดข้อมูลส่วนบุคคล หรือเกิดการรั่วไหลของข้อมูล (Data Breach) และอาจมีผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลเพื่อนำมาคำนวณหาระดับความเสี่ยงตามเกณฑ์ดังต่อไปนี้

/คะแนน ...

คะแนนสำหรับระดับความเสี่ยง	ระดับความเสี่ยง
๐	ไม่มีความเสี่ยง
๑ – ๗	ความเสี่ยงต่ำ
๘ – ๑๔	ความเสี่ยงปานกลาง
๑๕ – ๒๑	ความเสี่ยงสูง

หัวข้อประเมินปัจจัยความเสี่ยง	**คะแนนความเสี่ยง**			
	๐	**๑**	**๒**	**๓**
๑. จำนวนเจ้าของข้อมูลที่อาจได้รับผลกระทบ	ไม่มีเจ้าของข้อมูลที่ได้รับผลกระทบ เช่น จำนวนข้อมูลที่รั่วไหลเป็นจำนวนสถิติ หรือข้อมูลที่ได้รับการแปลงแล้ว	ทราบจำนวนเจ้าของข้อมูลแน่นอน ซึ่งไม่เกิน ๕๐ คน	คาดหมายว่าอาจมีเจ้าของข้อมูลที่ได้รับผลกระทบไม่เกิน ๑๐๐ คน	มากกว่า ๑๐๐ คน หรือไม่สามารถระบุจำนวนเจ้าของข้อมูลได้
๒. ลักษณะของข้อมูลที่รั่วไหล	ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เช่น ข้อมูลนิรนาม และข้อมูลภาพรวมเชิงสถิติ เป็นต้น	ข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้ทันที (โดยไม่รวมถึงข้อมูลอ่อนไหว) ต้องประกอบกับข้อมูลอื่น เช่น รหัสพนักงาน ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น	ข้อมูลส่วนบุคคลที่สามารถระบุตัวเจ้าของข้อมูลได้ทันที เช่น ชื่อของเจ้าของข้อมูล ภาพถ่าย วิดีโอ เป็นต้น	ข้อมูลอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ ความเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลชีวภาพ เป็นต้น
๓. ระยะเวลาการพบการรั่วไหล	ทราบเหตุทันทีที่เกิดการรั่วไหล	ทราบเหตุภายใน ๒๔ ชั่วโมง นับแต่การรั่วไหล	ทราบเหตุภายหลัง ๒๔ ชั่วโมง แต่ไม่เกิน ๗๒ ชั่วโมง นับแต่การรั่วไหล	ทราบเหตุภายหลัง ๗๒ ชั่วโมง นับแต่การรั่วไหล
๔. การเข้าถึงข้อมูลของบุคลากรของหน่วยงานเมื่อถูกโจรกรรมข้อมูล	บุคลากรสามารถเข้าถึงข้อมูลได้ปกติ	บุคลากรไม่สามารถเข้าถึงข้อมูลบางส่วน เป็นการชั่วคราว	บุคลากรไม่สามารถเข้าถึงข้อมูลทั้งหมด เป็นการชั่วคราว	บุคลากรไม่สามารถเข้าถึงข้อมูลทั้งหมด เป็นการถาวร

/หัวข้อ ...

หัวข้อประเมินปัจจัยความเสี่ยง	คะแนนความเสี่ยง			
	๐	๑	๒	๓
๕. ความเสียหายต่อข้อมูลเมื่อถูกโจรกรรมข้อมูล หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือเกิดจากความผิดพลาดของบุคลากรที่เกี่ยวข้อง	ข้อมูลไม่ได้ถูกแก้ไข/เสียหายประการใด	ข้อมูลถูกแก้ไข แต่ยังไม่ถูกนำไปใช้งาน ซึ่งหน่วยงานคงมีข้อมูลสำรอง และสามารถใช้ข้อมูลสำรองได้	ข้อมูลถูกแก้ไข และอาจถูกนำไปใช้งาน โดยไม่ทราบว่ามีการแก้ไขข้อมูล ทั้งนี้ หน่วยงานคงมีข้อมูลสำรอง และสามารถใช้ข้อมูลสำรองได้	ข้อมูลถูกแก้ไข และอาจถูกนำไปใช้งาน โดยไม่ทราบว่ามีการแก้ไขข้อมูล ซึ่งหน่วยงานไม่มีข้อมูลสำรอง
๖. ขอบเขตในการรั่วไหลของข้อมูล	ข้อมูลไม่ได้ถูกเปิดเผยหรือถูกเข้าถึงโดยมิชอบโดยบุคคลที่ไม่ได้รับอนุญาต	ข้อมูลที่รั่วไหลอาจถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาตภายในหน่วยงาน แต่ยังไม่พบหลักฐานว่าบุคคลที่ไม่ได้รับอนุญาตดังกล่าวมีการประมวลผลโดยมิชอบ เช่น เอกสารหายภายในอาคารหน่วยงาน หรืออุปกรณ์อิเล็กทรอนิกส์ถูกเลิกใช้งานโดยไม่ลบทำลายข้อมูล	ข้อมูลถูกเปิดเผยต่อหรือเข้าถึงโดยบุคคลภายนอกโดยทราบบุคคลภายนอกดังกล่าว เช่น การส่งอีเมลผิดให้ผู้อื่นพร้อมเอกสารแนบซึ่งเป็นข้อมูลส่วนบุคคล แต่ผู้รับข้อมูลไม่สามารถเปิดหรืออ่านข้อมูลได้ ต้องใช้มาตรการทางเทคนิคจึงจะเข้าถึงข้อมูลได้	ข้อมูลถูกเปิดเผยหรือเข้าถึงโดยบุคคลภายนอกที่ไม่เกี่ยวข้องโดยไม่ทราบจำนวน เช่น ถูกเปิดเผยสาธารณะ หรือมีการขายข้อมูลลูกค้า/ผู้ใช้บริการให้บุคคลภายนอก
๗. ผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลจากการรั่วไหล	ไม่มีผลกระทบต่อเจ้าของข้อมูลเนื่องจากเป็นข้อมูลที่เป็นสาธารณะอยู่ก่อนการรั่วไหล หรือหน่วยงานสามารถป้องกันเหตุที่อาจเกิดขึ้นแล้ว	คาดว่าจะไม่เกิดผลกระทบต่อเจ้าของข้อมูล แต่อาจก่อให้เกิดความรำคาญต่อเจ้าของข้อมูล เช่น ต้องกรอกข้อมูลในระบบใหม่ หรือลักษณะของข้อมูลที่รั่วไหลไม่สามารถกระทบต่อการดำรงชีวิตของเจ้าของข้อมูลได้	อาจก่อให้เกิดผลกระทบโดยอ้อม ต่อสิทธิ ทรัพย์สิน และร่างกาย เช่น เกิดความกลัว หรือความกังวล	อาจก่อให้เกิดกระทบโดยตรงที่ไม่อาจแก้ไขได้โดยง่าย เช่น ได้รับความเสียหายต่อทรัพย์สิน ถูกเลิกจ้าง การถูกปฏิเสธในการรับบริการ ถูกดำเนินคดี เสียสุขภาพ หรือเจ็บป่วยรุนแรง หรือระยะยาว หรือเสียชีวิต

/การแจ้ง ...

การแจ้งเหตุภัยคุกคามไซเบอร์

เมื่อพบความพยายามในการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ หรือพบจุดอ่อนจากการตรวจสอบ หรือทดสอบ หรือเกิดจุดอ่อนของระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๑) ให้ผู้รับผิดชอบเทคโนโลยีสารสนเทศ หรือทีมรับมือ CERT/IT/SOC

๑.๑ ดำเนินการตรวจสอบยับยั้งการโจมตี หรือละเมิดโดยอาจพิจารณาปิดระบบถ้ามีความจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

๑.๒ เสนอผู้บริหารของหน่วยงาน และแจ้ง MOF CERT ช่วยดำเนินการตรวจสอบ

๑.๓ กรณีที่มีการรั่วไหลหรือคาดว่าจะเกิดเหตุละเมิดข้อมูลส่วนบุคคลให้รีบแจ้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO) พร้อมจัดทำรายงานภัยคุกคามทางไซเบอร์สรุปในเบื้องต้น นำเสนอผู้อำนวยการสำนักงานเศรษฐกิจการคลัง ภายใน ๒๔ ชั่วโมงนับตั้งแต่เมื่อทราบเหตุละเมิด เพื่อจัดทำสรุปผลเสนอสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมง

๑.๔ เมื่อสถานการณ์กลับสู่ภาวะปกติที่สามารถให้บริการได้ ให้หน่วยงานรีบจัดทำรายงานเสนอผู้อำนวยการสำนักงานเศรษฐกิจการคลังเพื่อส่งสรุปการดำเนินงานให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ต่อไป

๒) ให้หัวหน้าหน่วยงาน

๒.๑ หากเป็นผู้รับผิดชอบภายในหน่วยงานให้ดำเนินการสืบสวน และสอบสวน รวมถึงพิจารณาลงโทษทางวินัยตามระเบียบหรือกฎหมายที่เกี่ยวข้อง

๒.๒ หากเป็นบุคคลภายนอกให้ดำเนินการเก็บหลักฐานข้อมูลและพิจารณาดำเนินการตามกฎหมายที่เกี่ยวข้อง

๒.๓ ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

๒.๔ สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

ทั้งนี้ สำนักงานเศรษฐกิจการคลังได้จัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ ตามประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘ ซึ่งได้ประกาศ ณ วันที่ ๒๗ พฤษภาคม ๒๕๖๘ และได้แจ้งให้ถือปฏิบัติ ดังนั้น หน่วยงานที่เกิดเหตุภัยคุกคามทางไซเบอร์ สามารถรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามแบบบันทึกรายงานภัยคุกคามทางไซเบอร์ที่ สกมช. กำหนด โดยอ้างอิงจากแผนรับมือเหตุภัยคุกคามทางไซเบอร์ตามประกาศ สศค. ดังกล่าว

/กระบวน ...

กระบวนการตอบสนองเหตุการละเมิดข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๓๗ (๑) และ ๓๗ (๔) ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่จัดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า สำนักงานเศรษฐกิจการคลังจึงได้กำหนดกระบวนการตอบสนองเหตุละเมิดข้อมูลส่วนบุคคล ดังนี้

๑. การยับยั้งการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคล

เมื่อพบความพยายามในการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจ หรือพบจุดอ่อนที่อาจทำให้ข้อมูลรั่วไหลจากการตรวจสอบ หรือทดสอบ หรือเกิดจุดอ่อนของระบบ

๑) ให้ผู้รับผิดชอบของหน่วยงาน หรือทีมรับมือ CERT/IT/SOC

๑.๑ ดำเนินการยับยั้งการรั่วไหล หรือละเมิดโดยอาจพิจารณาปิดระบบถ้ามีความจำเป็น และแก้ไขจนกว่าจะแล้วเสร็จจึงเปิดใช้ข้อมูลนั้นอีกครั้ง

๑.๒ ให้หน่วยงานเสนอหัวหน้าหน่วยงาน เพื่อหน่วยงานเตรียมร่าง

๑.๒.๑ จัดทำรายงานในเบื้องต้นเสนอผู้อำนวยการสำนักงานเศรษฐกิจการคลังภายใน ๒๔ ชั่วโมง นับตั้งแต่เมื่อทราบเหตุละเมิด เพื่อ สศค. จัดสรุปผลเสนอสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมง

๑.๒.๒ แจ้งเจ้าข้อมูลข้อมูลส่วนบุคคล หากการละเมิดข้อมูลส่วนบุคคลมีระดับความเสี่ยงสูงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๑.๒.๓ ทำการสื่อสารเกี่ยวกับเหตุการณ์ทั้งภายในและภายนอก

๑.๓ เมื่อสถานการณ์กลับสู่ภาวะปกติที่สามารถให้บริการได้ ให้หน่วยงานรีบจัดทำรายงานเสนอผู้อำนวยการสำนักงานเศรษฐกิจการคลังเพื่อส่งสรุปการดำเนินงานให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ต่อไป

๒) ให้หัวหน้าหน่วยงาน

๒.๑ หากเป็นผู้รับผิดชอบภายในหน่วยงานให้ดำเนินการสืบสวน และสอบสวน รวมถึงพิจารณาลงโทษทางวินัยตามระเบียบหรือกฎหมายที่เกี่ยวข้อง

๒.๒ หากเป็นบุคคลภายนอกให้ดำเนินการเก็บหลักฐานข้อมูลและพิจารณาดำเนินการตามกฎหมายที่เกี่ยวข้อง

๒.๓ ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

๒.๔ สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

/๒. การแก้ไข ...

๒. การแก้ไขการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคล

ข้อ ๑ รับแจ้งเหตุ รายงานเหตุ การควบคุมความเสียหายและการแก้ไขสถานการณ์

๑) ผู้พบเหตุรายงานเหตุการณ์ พบการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลโดยผู้ไม่มีอำนาจให้รีบแจ้งทีมรับมือ CERT/IT/SOC/ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ (ผอ. ศทส.) ทราบโดยทันที

๒) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. รับแจ้งเหตุและตรวจสอบข้อมูลเบื้องต้นพร้อมบันทึกเหตุการณ์

๓) ประชุม และ/หรือ ยืนยันเหตุการณ์ (ภายใน ๒๔ ชม.) และจะต้องประเมินเหตุการณ์ ดังนี้

ก. กรณีที่ไม่พบต้นเหตุการละเมิด

(๑) จัดทำบันทึกเอกสาร

(๒) รายงานข้อมูลให้ผู้บริหารและสำเนาให้เจ้าหน้าที่ DPO รับทราบ

ข. กรณีที่พบต้นเหตุการละเมิด ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศจะต้องพิจารณาดังนี้

(๑) กรณีที่เกี่ยวข้องระบบ IT

ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ทำการหาสาเหตุ แก้ไข และควบคุม สถานการณ์ พร้อมทั้งวิเคราะห์ว่าเหตุการณ์นั้นจำเป็นต้องปิดระบบ IT หรือไม่

(๑.๑) กรณีที่ปิดระบบแล้ว

(๑.๑.๑) แจ้ง คณะทำงาน BCM

(๑.๑.๒) ทีม CERT/IT/SOC/ผอ. ศทส. ต้องดำเนินการตามขั้นตอนต่อไปนี้

๑) ประกาศใช้แผน BCP/DRP

๒) กระบวนการตามแผน BCP/DRP

๓) กู้คืนระบบ (DR-Site)

๔) กู้คืนกระบวนการสำคัญ

๕) ติดตามสถานการณ์

๖) ประกาศยกเลิกแผน BCP/DRP

(๑.๑.๓) กลับสู่ภาวะปกติ

(๑.๑.๔) **ดำเนินการตามข้อ ๒ ต่อไป**

(๑.๒) กรณีที่ไม่ปิดระบบ

(๑.๒.๑) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ตรวจสอบขอบเขตของการละเมิด หรือการรั่วไหลข้อมูล

(๑.๒.๒) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. พิจารณาว่าความเสี่ยงที่ก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล

(๑.๒.๓) **ดำเนินการตามข้อ ๒ ต่อไป**

/(๒) กรณี ...

(๒) กรณีที่ไม่เกี่ยวข้องกับระบบ IT

(๒.๑) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. รับทราบเหตุ ต้องดำเนินการ

(๒.๑.๑) ตรวจสอบขอบเขตของการละเมิดและการรั่วไหลของข้อมูล

(๒.๑.๒) พิจารณาว่าระดับความเสี่ยงที่มีผลต่อสิทธิเสรีภาพของเจ้าของข้อมูล

(๒.๒) **ดำเนินการตามข้อ ๒ ต่อไป**

ข้อ ๒ การวิเคราะห์ประเมินความเสี่ยงที่ก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล

ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ตรวจสอบขอบเขตของการละเมิดและการรั่วไหลของข้อมูล

ก. กรณีการละเมิดหรือรั่วไหลข้อมูลไม่ใช่ข้อมูลส่วนบุคคล

(๑) รายงานข้อมูลให้ผู้บริหารและสำเนาให้เจ้าหน้าที่ DPO รับทราบ

(๒) ไม่ต้องแจ้ง สคส. และหรือเจ้าของข้อมูลส่วนบุคคล

(๓) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ต้องจัดทำรายงานแจ้ง MOF CERT กระทรวงการคลัง

ข. กรณีการละเมิดหรือรั่วไหลข้อมูลเป็นข้อมูลส่วนบุคคล

(๑) คณะทำงาน BCM พิจารณามาตรการเยียวยาและบรรเทาผลกระทบ

(๒) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ต้องจัดทำรายงาน MOF CERT กระทรวงการคลัง

(๓) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. จัดเตรียมร่างการแจ้งเตือน (อนุมัติโดยผู้บริหาร)

(๔) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ดำเนินการวิเคราะห์ระดับความเสี่ยง

(๔.๑)กรณีมีระดับความเสี่ยงสูงต่อสิทธิของเจ้าของข้อมูล (ระดับความเสี่ยงสูง)

(๔.๑.๑) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. จัดทำรายงานและแนวทางเยียวยาแจ้งให้ผู้บริหารหน่วยงาน และเจ้าหน้าที่ DPO เพื่อเสนอให้ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง และส่งให้สำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) รับทราบภายใน ๗๒ ชม. ทั้งนี้ เพื่อให้การส่งรายงานทันกำหนดเวลา หน่วยงานอาจพิจารณานำเสนอรายงานเบื้องต้นต่อ สคส. และผู้อำนวยการสำนักงานเศรษฐกิจการคลังพร้อมกันได้

(๔.๑.๒) สำนักงานเศรษฐกิจการคลังและหน่วยงานแจ้งสาเหตุและแนวทางเยียวยาต่อเจ้าของข้อมูลส่วนบุคคล

(๔.๑.๓) สำนักงานเศรษฐกิจการคลังและหน่วยงานดำเนินการสื่อสารภายในและภายนอก

(๔.๑.๔) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ต้องดำเนินงาน

๑) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

๒) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

๓) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

/(๔.๒) กรณี ...

(๔.๒) กรณีมีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล (ระดับความเสี่ยงน้อย หรือปานกลาง)

(๔.๒.๑) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. แจ้งให้ผู้บริหาร และเจ้าหน้าที่ DPO เพื่อเสนอผู้อำนวยการสำนักงานเศรษฐกิจการคลัง และส่งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) รับทราบภายใน ๗๒ ชม. ทั้งนี้ เพื่อให้การส่งรายงานทันกำหนดเวลา หน่วยงานอาจพิจารณานำเสนอรายงานเบื้องต้นต่อ สคส. และผู้อำนวยการสำนักงานเศรษฐกิจการคลังพร้อมกันได้

(๔.๒.๒) หน่วยงานดำเนินการสื่อสารภายในและภายนอก

(๔.๒.๓) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ต้องดำเนินการ

๑) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

๒) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

๓) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

(๔.๓) กรณีไม่มีความเสี่ยงต่อสิทธิของเจ้าของข้อมูล

(๔.๓.๑) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. แจ้งให้ผู้บริหาร และ DPO รับทราบ

(๔.๓.๒) หน่วยงานดำเนินการสื่อสารภายใน

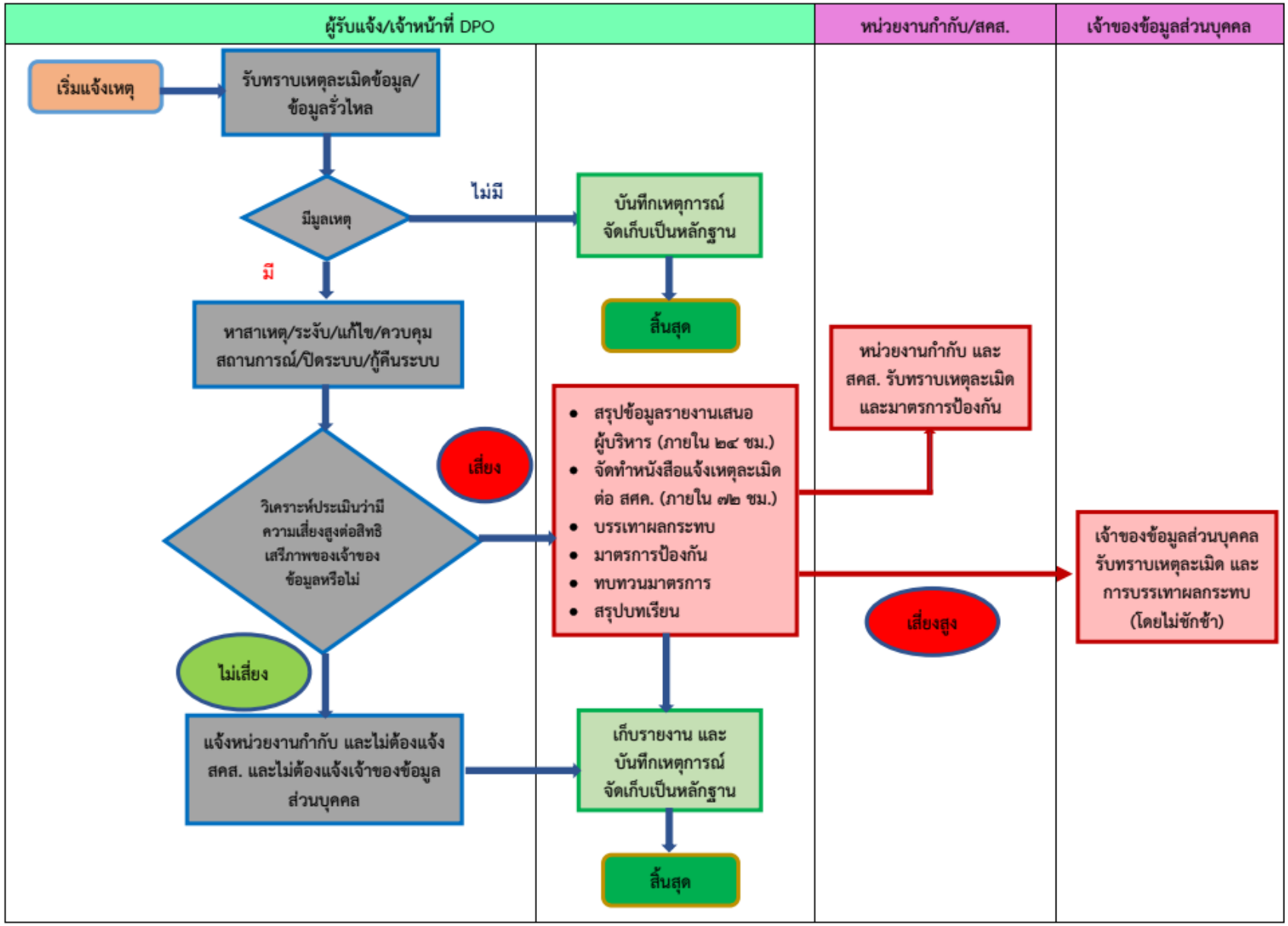
(๔.๓.๓) ทีมรับมือ CERT/IT/SOC/ผอ. ศทส. ต้องดำเนินการ

๑) จัดทำบันทึกเอกสารและจัดเก็บพยานหลักฐาน

๒) ทำการทบทวนปรับปรุงมาตรการ (มาตรการองค์กร/มาตรการเชิงเทคนิค)

๓) สรุปบทเรียนและสื่อสารความตระหนักให้กับผู้ที่เกี่ยวข้อง

สรุปขั้นตอนการดำเนินการ กรณีเกิดการละเมิดข้อมูลหรือข้อมูลรั่วไหล (Data Breach Response)



/การรายงาน ...

การรายงานเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ประเมินผลกระทบและความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจากเหตุการละเมิดข้อมูลส่วนบุคคล ในระดับความเสี่ยงต่ำ ปานกลาง สูง ที่มีต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ซึ่งนำมาพิจารณาดำเนินการแจ้งเหตุละเมิดต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) หรือแจ้งเหตุต่อเจ้าของข้อมูลส่วนบุคคลได้ ดังนี้

ระดับความเสี่ยง	ผลกระทบและความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล	การดำเนินการแจ้งเหตุการละเมิด / รายงานเหตุละเมิด		
สูง	ได้รับผลกระทบที่มีนัยสำคัญ และไม่สามารถแก้ไขปัญหาได้ เช่น เกิดความเสียหายด้านการเงิน ทำให้เกิดหนี้สิน ไม่สามารถชดใช้ได้ ไม่สามารถทำงานได้ ผลกระทบทางจิตใจ หรือร่างกาย หรือทำให้ถึงขั้นเสียชีวิต หรือมีปัญหาแต่สามารถแก้ไขปัญหาได้ เช่น ถูกยักยอกเงิน ถูกธนาคารปฏิเสธการทำธุรกรรม ทรัพย์สินเสียหาย ถูกเลิกจ้าง หรือได้รับหมายศาล สุขภาพทรุดโทรม	แจ้งเหตุต่อเจ้าของข้อมูลส่วนบุคคล	แจ้งเหตุต่อ สคส.	แจ้งเหตุต่อผู้บริหารที่เกี่ยวข้อง
ปานกลาง	ได้รับความไม่สะดวกอย่างมีนัยสำคัญ มีปัญหาความยุ่งยากเล็กน้อย แต่สามารถแก้ไขปัญหาได้ เช่น เกิดภาระค่าใช้จ่ายเพิ่มเติม ถูกปฏิเสธการเข้าถึงบริการทางธุรกิจ มีความกลัว มีความเครียด เกิดความไม่เข้าใจ หรือมีอาการเจ็บป่วยทางกายเล็กน้อย	ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล	แจ้งเหตุต่อ สคส.	แจ้งเหตุต่อผู้บริหารที่เกี่ยวข้อง
ต่ำ	ได้รับความไม่สะดวกเพียงเล็กน้อย เช่น เจ้าของข้อมูลส่วนบุคคลเสียเวลาในการป้อนข้อมูลใหม่ หรือมีความไม่พึงพอใจเล็กน้อย	ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล	แจ้งเหตุต่อ สคส.	แจ้งเหตุต่อผู้บริหารที่เกี่ยวข้อง
ไม่เสี่ยง	ไม่ได้รับผลกระทบ	ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล	ไม่ต้องแจ้งเหตุต่อ สคส.	จดบันทึกและรายงานเหตุละเมิดต่อผู้บริหาร/ (รายไตรมาส)

/ในการ ...

ในการรายงานเหตุการละเมิดข้อมูลส่วนบุคคลของหน่วยงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และต่อ สศค. รวมถึงการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล สามารถดำเนินการแจ้งโดยกรอกข้อมูลตามแบบฟอร์ม และตัวอย่างหนังสือการรายงาน ดังต่อไปนี้

แบบฟอร์มการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

เลขที่ ..... (ส่วนหน่วยงานผู้แจ้ง/รับแจ้ง)	**วันที่แจ้ง/รับแจ้ง**.....
แบบฟอร์มฉบับนี้ใช้สำหรับหน่วยงานที่เกิดเหตุการละเมิดข้อมูลส่วนบุคคลและต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล **ขอความกรุณาอย่ากรอกข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับเหตุการละเมิดข้อมูลส่วนบุคคลในแบบฟอร์มฉบับนี้** เช่น ห้ามใส่ชื่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล หาก สป กค. และ สคส. ต้องการข้อมูลดังกล่าว จะทำการติดต่อท่านไปในภายหลัง หน่วยงานควรตรวจสอบให้แน่ใจว่าข้อมูลที่ให้นั้นถูกต้องที่สุดและมีรายละเอียดครบถ้วนมากที่สุดเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล กรุณาตอบคำถามต่อไปนี้เพื่อช่วยให้ สป กค. และ สคส. ดำเนินการเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลของท่านอย่างมีประสิทธิภาพและเพื่อทำความเข้าใจหน่วยงานของท่านได้ดียิ่งขึ้น	
ส่วนที่ ๑ ผู้แจ้ง/ผู้รับแจ้งเหตุการณ์	
ชื่อ-นามสกุล:	ตำแหน่ง: .....
หน่วยงาน:	
เบอร์โทร:	เบอร์โทรสาร: .....
อีเมล:.....	หน่วยงาน/ผู้ประสานงานสำหรับติดต่อ
ที่อยู่เพื่อการติดต่อ	
ส่วนที่ ๒ รายละเอียดเหตุการณ์	
วันที่พบเหตุการละเมิด :	เวลาที่พบเหตุการละเมิด **.....** นาฬิกา
วันที่เกิดเหตุการละเมิดขึ้น :	เวลาที่เกิดเหตุการละเมิดขึ้น **.....** นาฬิกา
กิจกรรม/ระบบที่เกิดเหตุ:.....	
รายละเอียดเหตุการณ์: (๑) กรุณาอธิบายเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ..... (๒) กรุณาอธิบายว่าเหตุการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นได้อย่างไร ..... (๓) หน่วยงานพบเหตุการละเมิดข้อมูลส่วนบุคคลได้อย่างไร เช่น พบเหตุจากกระบวนการตรวจสอบภายใน ..... (๔) หน่วยงานมีมาตรการป้องกันอะไรบ้าง	

/(๕) ประเภท ...

(๕) ประเภทของการละเมิด

☐ รูปแบบเอกสาร ☐ รูปแบบอิเล็กทรอนิกส์ ☐ ระบบงาน

(๖) เหตุการละเมิดข้อมูลส่วนบุคคลเกิดจากสาเหตุทางไซเบอร์หรือไม่

☐ ใช่ ☐ ไม่ใช่ ☐ ไม่ทราบ

ส่วนที่ ๓ ผลกระทบ (ทำเครื่องหมายทุกข้อที่เกี่ยวข้อง ได้มากกว่า ๑ ข้อ)

ประเภทของข้อมูลที่ถูกละเมิด:	☐ข้อมูลเจ้าหน้าที่และผู้บริหาร ☐ข้อมูลผู้มารับบริการ เช่น ผู้มาติดต่อ ☐ข้อมูลผู้สมัครงาน ☐ข้อมูลผู้เข้าร่วมฝึกอบรมภายในหน่วยงาน ☐ที่ปรึกษา และบุคคลที่เกี่ยวข้อง ☐ลูกจ้างตามสัญญาจ้าง หรือผู้ที่ทำงาน หรือปฏิบัติงาน ☐กรรมการ และผู้บริหาร ☐ข้อมูลอื่น ๆ (ระบุ)..... ☐ข้อมูลอื่น ๆ (ระบุ)..... ☐ข้อมูลอื่น ๆ (ระบุ)..... ☐ไม่สามารถระบุได้ในขณะนี้
ข้อมูลที่ถูกละเมิด:	**ข้อมูลส่วนบุคคลทั่วไป** ☐ ข้อมูลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อีเมล วันเดือนปีเกิด การศึกษา ข้อมูลติดต่อ Username Password เป็นต้น ☐ ประวัติการทำงาน เช่น สถานะ วิชาชีพ ตำแหน่งงาน ผลการประเมินผลการปฏิบัติงาน ☐ ข้อมูลเอกสารราชการ บัตรประจำตัวประชาชน หนังสือเดินทาง ใบขับขี่ บัตรข้าราชการ ☐ ข้อมูลด้านการเงิน เช่น ธุรกรรมทางการเงิน ข้อมูลภาษี เลขที่บัญชี เลขบัตรเครดิต ☐ ข้อมูลภาพวิดีทัศน์กล้องวงจรปิด ☐ ข้อมูลที่เกี่ยวเนื่องกับบุคคล เช่น IP address บทสนทนา และการสื่อสารทางโทรศัพท์ หรือ อุปกรณ์อิเล็กทรอนิกส์ ☐ ข้อมูลอื่น ๆ (โปรดระบุ)..... ☐ ไม่สามารถระบุได้ในขณะนี้

/ข้อมูลส่วนบุคคล

	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ☐ ข้อมูลเกี่ยวกับเชื้อชาติ ☐ ข้อมูลเกี่ยวกับศาสนา ☐ ข้อมูลด้านความคิดเห็นทางการเมือง ☐ ประวัติอาชญากรรม ☐ ข้อมูลสุขภาพ/สุขภาพจิต ☐ ข้อมูลสหภาพแรงงาน ☐ ข้อมูลพันธุกรรม ☐ ข้อมูลเกี่ยวกับชีวิตทางด้านเพศ ☐ ข้อมูลเกี่ยวกับรสนิยมทางเพศ ☐ ข้อมูลการแปลงเพศ ☐ ข้อมูลตำแหน่ง เช่น พิกัด ☐ ข้อมูลชีวมิติ (อาทิ ภาพสแกนใบหน้า/ม่านตา ลายนิ้วมือ ฟิล์มเอกซเรย์ เสียง) ☐ข้อมูลอื่น ๆ (โปรดระบุ)..... ☐ไม่สามารถระบุได้ในขณะนี้
ปริมาณของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณ	☐ จำนวน **.....** คน/record ☐ ไม่สามารถระบุจำนวนได้ในขณะนี้
ลักษณะเหตุการละเมิดอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล	☐ กลุ่มของข้อมูลที่มีความเฉพาะข้อมูลที่เป็นความลับหรือข้อมูลที่มีความเสี่ยงสูงเมื่อเกิดเหตุละเมิด เช่น ข้อมูลทางการเงิน ประวัติสุขภาพ เป็นต้น ☐ จำนวนความหลากหลายของข้อมูลส่วนบุคคล เช่น กลุ่มของข้อมูลที่รั่วไหล ประกอบด้วย ชื่อ ที่อยู่ อาชีพ ประวัติการศึกษา อายุ ☐ ความยากง่ายในการระบุถึงตัวบคคล เช่น ข้อมูลที่ถูกละเมิดไม่ได้เป็นข้อมูลแฝง หรือเป็นข้อมูลที่เข้ารหัส ☐ ข้อมูลส่วนบุคคลของผู้ที่มีความเสี่ยงต่อการล่วงละเมิด หรืออาชญากรรม เช่น ข้อมูลของพยานในคดี ข้อมูลของเหยื่อผู้ถูกล่วงละเมิด ☐ การรั่วไหลที่มีสาเหตุมาจากการโจมตีโดยผู้ไม่ประสงค์ดีที่มุ่งเน้นในการเข้าถึงข้อมูลที่เป็นความลับ ☐ ข้อมูลอื่น ๆ (โปรดระบุ).....

/รายละเอียด ...

รายละเอียดของผลกระทบที่อาจจะเกิด หรือเกิดไปแล้วต่อเจ้าของข้อมูลส่วนบุคคล:	....
รายละเอียดของผลกระทบที่น่าจะเกิดจากการละเมิด:	....
การประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (ตามเกณฑ์ภาคผนวก ข้อ ๑. การพิจารณาปัจจัยความเสี่ยง)	☐ สูง - ส่งผลกระทบต่อสุขภาพ เสรีภาพ และชีวิตของเจ้าของข้อมูล ☐ ปานกลาง - ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของเจ้าของข้อมูล ☐ ต่ำ – ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลต่ำ ☐ ไม่มีความเสี่ยง - เป็นข้อมูลส่วนบุคคลที่เข้าถึงได้สาธารณะอยู่ก่อนแล้ว
ส่วนที่ ๔ การตอบสนองเพื่อระงับเหตุการณ์	
การตอบสนองเพื่อระงับเหตุการณ์ ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ข้อ ๕(๕)	....
แนวทางเยียวยาเจ้าของข้อมูล (กรณีผลกระทบสูง) ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ประกาศ สคส. ข้อ ๖(๔)	(โปรดระบุมาตรการการแก้ไขปัญหา เช่น ดำเนินการเปลี่ยนรหัสความปลอดภัย ดำเนินการค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น) สาเหตุของปัญหา..... ..... การแก้ไขระยะสั้น..... ..... การแก้ไขระยะยาว..... .....
ส่วนที่ ๕ การวิเคราะห์สาเหตุ และป้องกันการเกิดซ้ำ	
สาเหตุ	(โปรดอธิบาย เพื่อขยายความลักษณะเหตุละเมิด เพื่อให้เข้าใจเนื้อหาของการละเมิดข้อมูลส่วนบุคคล โดยอธิบายเนื้อหาเท่าที่สามารถระบุได้ รวมไปถึงคำขยายความประเภทข้อมูลที่ทราบโดยละเอียด) .....
การป้องกัน/ การขจัดสาเหตุ	(โปรดระบุแผนงาน และการป้องกัน การเกิดเหตุการณ์ซ้ำ) ....

หน่วยงานที่รับผิดชอบ	(โปรดระบุหน่วยงาน/กลุ่ม/ฝ่าย/ส่วน/งาน ที่รับผิดชอบในการดำเนินการตามแผนข้างต้น) ๑..... เบอร์โทร:.....e-Mail :..... ๒..... เบอร์โทร:.....e-Mail :.....

ส่วนที่ ๖ การแจ้งต่อหน่วยงานที่เกี่ยวข้อง

๑. แจ้งต่อผู้คุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวง ☐ แจ้งเรียบร้อยแล้ว ☐ ยังไม่แจ้ง

๒. แจ้งต่อผู้บริหารของหน่วยงาน ☐ แจ้งเรียบร้อยแล้ว ☐ ยังไม่แจ้ง

๓. แจ้งความ/ลงบันทึกประจำวันต่อเจ้าหน้าที่ตำรวจ ☐ แจ้งเรียบร้อยแล้ว ☐ ยังไม่แจ้ง

๔. แจ้งต่อเจ้าของข้อมูลส่วนบุคคล* ☐ ดำเนินการแจ้งเจ้าของข้อมูลเรียบร้อยแล้ว วันที่.....
ช่องทางที่ใช้ในการแจ้ง.....
☐ อยู่ระหว่างการดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล
☐ ไม่แจ้งเจ้าของข้อมูลส่วนบุคคล
☐ อยู่ระหว่างการพิจารณาของสำนักงานปลัดกระทรวง และ/หรือ หน่วยงาน
☐ อื่น ๆ (โปรดระบุ) _____

* หมายเหตุ หากเป็นกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมง

ผู้รายงาน (หัวหน้าหน่วยงานที่ถูกละเมิด)

ชื่อ-นามสกุล:	ตำแหน่ง:
ส่วนราชการ:	เบอร์โทร:
e-Mail :	

ส่วนที่ ๗ แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPO เป็นผู้บันทึกข้อมูล)

๕. แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล*

☐ แจ้งเรียบร้อยแล้ว ☐ ไม่ต้องแจ้งเพราะการละเมิดไม่ใช่ข้อมูลส่วนบุคคล หรือไม่มีข้อมูลรั่วไหล

☐ ยังไม่แจ้ง เนื่องจาก ... .

* หมายเหตุ หากเป็นกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมง

ผู้รายงาน (ผู้ควบคุมข้อมูลส่วนบุคคล)

ชื่อ-นามสกุล:	ตำแหน่ง: ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง
ส่วนราชการ: สำนักงานเศรษฐกิจการคลัง	เบอร์โทร: ๐๒ ๒๗๓ ๙๐๒๐ ต่อ XXXX
e-Mail :XXXXXX @fpo.go.th https : www.fpo.go.th	

ตัวอย่าง

หนังสือการรายงานเหตุการละเมิดข้อมูลส่วนบุคคลของหน่วยงาน
ต่อผู้อำนวยการสำนักงานเศรษฐกิจการคลัง

เรื่อง รายงานเหตุการละเมิดข้อมูลส่วนบุคคล
เรียน ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง
สิ่งที่ส่งมาด้วย: แบบฟอร์มการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล จำนวน ๑ ชุด

ด้วย.....ชื่อหน่วยงาน.....ได้ตรวจพบเหตุการละเมิดข้อมูลส่วนบุคคลที่....ชื่อหน่วยงาน..... ..... ทำการเก็บรักษาอยู่ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่ง.....ชื่อหน่วยงาน..... พิจารณาว่าเหตุดังกล่าวมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล เพื่อเป็นการปฏิบัติตามความของมาตรา ๓๗ (๔) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒. .....ชื่อหน่วยงาน..... ขอรายงานเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังเอกสารแนบ

ทั้งนี้ .....ชื่อหน่วยงาน.....ยินดีให้ความร่วมมือในการสอบสวนเหตุการละเมิดข้อมูลส่วนบุคคลนี้ โดยสามารถติดต่อ.....ชื่อหน่วยงาน..... ได้ที่.....โทร..... อีเมล.....

จึงเรียนมาเพื่อโปรดทราบและลงนามในหนังสือการรายงานเหตุการละเมิดข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลังต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(ลงชื่อ).....
ตำแหน่ง.....ผู้อำนวยการ กอง/ศูนย์/กลุ่ม.....

ตัวอย่าง

หนังสือการรายงานเหตุการละเมิดข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง
ต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง รายงานเหตุการละเมิดข้อมูลส่วนบุคคล
เรียน เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เอกสารแนบ แบบฟอร์มรายงานเหตุการละเมิดข้อมูลส่วนบุคคล

ด้วย สำนักงานเศรษฐกิจการคลัง ได้ตรวจพบเหตุการละเมิดข้อมูลส่วนบุคคลที่....ชื่อหน่วยงาน..... ทำการเก็บรักษาอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งสำนักงานเศรษฐกิจการคลัง พิจารณาว่าเหตุดังกล่าวมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล เพื่อเป็นการปฏิบัติตามความในมาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำนักงานเศรษฐกิจการคลังขอรายงานเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังเอกสารแนบ

ทั้งนี้ สำนักงานเศรษฐกิจการคลัง ยินดีให้ความร่วมมือในการสอบสวนเหตุการละเมิดข้อมูลส่วนบุคคลนี้ โดยสามารถติดต่อ.....ชื่อหน่วยงาน..... ได้ที่.....โทร..... อีเมล.....

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการต่อไปด้วย จักขอบคุณยิ่ง

(ลงชื่อ).....
ตำแหน่ง ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง.....

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประเมินผลกระทบของเหตุการละเมิดข้อมูลส่วนบุคคล ผลการพิจารณาระดับความรุนแรงระดับ ต่ำ, ปานกลาง, สูง ถ้าเหตุละเมิดข้อมูลส่วนบุคคลที่มีผลการพิจารณาระดับความเสี่ยงสูงต่อเจ้าของข้อมูลส่วนบุคคล ต้องดำเนินการแจ้งเจ้าของข้อมูล

ตัวอย่าง

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

เรื่อง รายงานเหตุการละเมิดข้อมูลส่วนบุคคล ....ชื่อหน่วยงาน.....

เรียน คุณ.....

จากการที่ สำนักงานเศรษฐกิจการคลัง โดย....ชื่อหน่วยงาน.....ได้ทำการเก็บรักษาข้อมูลส่วนบุคคลของท่านภายใต้มาตรการคุ้มครองข้อมูลส่วนบุคคล รวมถึงมาตรการในการตรวจสอบการละเมิดข้อมูลส่วนบุคคลอย่างต่อเนื่อง พบว่ามีเหตุละเมิดข้อมูลส่วนบุคคลที่.....ชื่อหน่วยงาน..... ทำการเก็บรักษาอยู่ โดยเหตุการณ์ที่ตรวจพบ คือ..... ตรวจพบเมื่อวันที่ .....เหตุ เกิดเมื่อวันที่.....
ประเภทของการละเมิด..ข้อมูลส่วนบุคคล/ข้อมูลอ่อนไหว.....ข้อมูลที่ถูกละเมิด.....
ความรุนแรงของผลกระทบ..... ซึ่งส่งผล (อาจส่งผล) ให้..... .....

....ชื่อหน่วยงาน..... ได้ดำเนินการระงับเหตุการณ์ดังกล่าว และวิเคราะห์หาสาเหตุ รวมถึงดำเนินการเพื่อป้องการการเกิดขึ้นซ้ำ

....ชื่อหน่วยงาน..... ขอแนะนำให้ท่านดำเนินการ ดังนี้

๑. .....

๒. .....

ทั้งนี้ ....ชื่อหน่วยงาน.....มีมาตรการเยียวยาสำหรับเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ดังนี้

๑. .....

๒. .....

หากท่านต้องการข้อมูลเพิ่มเติม สามารถติดต่อ ได้ที่:

เจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล โทร..... อีเมล.....
เจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ โทร..... อีเมล.....

ขออภัยเป็นอย่างสูง

(ลงชื่อ).....

ตำแหน่ง.....

คำแถลงข่าวเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์
ตัวอย่าง

คำแถลงข่าวเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์

สำนักงานเศรษฐกิจการคลัง **วันที่: [วัน/เดือน/ปี]**
คำแถลงข่าวเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์

สำนักงานเศรษฐกิจการคลัง ขอเรียนแจ้งให้สาธารณชนทราบว่า เมื่อวันที่ **[ระบุวันที่เกิดเหตุการณ์]** สำนักงานฯ ได้ตรวจพบเหตุการณ์ที่เข้าข่ายเป็น **ภัยคุกคามทางไซเบอร์** ซึ่งอาจส่งผลกระทบต่อระบบสารสนเทศบางส่วนของสำนักงานฯ ทันทีที่พบความผิดปกติ ทีมความปลอดภัยไซเบอร์ของสำนักงานฯ ได้ดำเนินการดังต่อไปนี้:

๑. **ระงับการทำงานของระบบที่เกี่ยวข้อง** เพื่อป้องกันความเสียหายเพิ่มเติม
๒. **ประสานงานผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ภายนอก** เพื่อทำการตรวจสอบ วิเคราะห์ และควบคุมสถานการณ์
๓. **ดำเนินการสอบสวนเชิงลึก** เพื่อระบุสาเหตุและขอบเขตของผลกระทบ
๔. **ปกป้องข้อมูลของผู้ใช้บริการและลูกค้า** โดยดำเนินมาตรการตามมาตรฐานสากลด้านความปลอดภัยข้อมูล

จากการประเมินเบื้องต้น ณ ขณะนี้

- **ข้อมูลที่ได้รับผลกระทบ:** [ระบุถ้าทราบ / “อยู่ระหว่างการตรวจสอบ”]
- **ระบบที่ได้รับผลกระทบ:** [ระบุระบบ / ฟังก์ชัน / “อยู่ระหว่างการตรวจสอบ”]
- **ผลกระทบต่อผู้ใช้บริการ:** [ระบุหรือแจ้งว่าอยู่ระหว่างประเมิน]

สำนักงานฯ ให้ความสำคัญอย่างยิ่งต่อความปลอดภัยของข้อมูล และกำลังดำเนินการอย่างเต็มที่เพื่อให้การบริการกลับสู่สภาวะปกติโดยเร็วที่สุด หากพบว่ามีข้อมูลของลูกค้าหรือผู้ใช้บริการได้รับผลกระทบ สำนักงานฯ จะ **แจ้งเตือนและให้คำแนะนำการป้องกันเพิ่มเติม** โดยตรงในช่องทางที่เหมาะสม

เราขออภัยเป็นอย่างสูงต่อความไม่สะดวกที่อาจเกิดขึ้นจากเหตุการณ์นี้ และเรามุ่งมั่นดำเนินมาตรการอย่างรัดกุมเพื่อป้องกันไม่ให้เหตุการณ์ลักษณะนี้เกิดขึ้นอีกในอนาคต

ช่องทางติดต่อสอบถาม

- โทร: [หมายเลขติดต่อ]
- อีเมล: [อีเมลฝ่ายสนับสนุน]
- เว็บไซต์: [URL สำนักงานเศรษฐกิจการคลัง]

[ชื่อผู้บริหาร / โฆษกสำนักงานเศรษฐกิจการคลัง]
ตำแหน่ง: [ตำแหน่ง]
สำนักงานเศรษฐกิจการคลัง