ประกาศสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
เรื่อง นโยบายการดำเนินการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy)

สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (“**สำนักงาน**”) มุ่งมั่นที่จะคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลเพื่อให้ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำนักงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายในการกำหนดมาตรฐานและแนวทางในการประมวลผลข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะได้รับการคุ้มครองและถูกนำไปใช้ตรงตามวัตถุประสงค์ในการดำเนินงานของสำนักงาน สำนักงานจึงออกประกาศแนวทางการดำเนินการเพื่อให้เป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคล ดังนี้

๑. คำนิยาม

ในนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ คำหรือข้อความสามารถนิยามได้ดังนี้

คำจำกัดความ	ความหมาย
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และที่จะมีการแก้ไขเพิ่มเติม รวมถึงกฎ ระเบียบ และคำสั่งที่เกี่ยวข้อง
การเข้าถึงข้อมูล (Access)	หมายถึง สิทธิในการอ่าน/ดู บันทึก คัดลอก เก็บสำรอง จัดเก็บ สืบค้น ดาวน์โหลด หรือแก้ไข (อัพเดท แทรก/เพิ่ม ลบ) ข้อมูล รวมถึงการจัดการสิทธิการเข้าถึงนั้น ๆ
การบันทึก (Record)	ข้อมูลหรือสารสนเทศในรูปแบบเฉพาะ ซึ่งถูกสร้างขึ้นหรือได้มาจากกิจกรรมบุคคลหรือกิจกรรมองค์กร และได้สำรอง (เก็บรักษา) ไว้เป็นหลักฐานของกิจกรรมนั้น ๆ เพื่อใช้อ้างอิงในอนาคต
การประมวลผลข้อมูลส่วนบุคคล (Processing)	การดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้างเก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อม ใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย
ข้อมูล/สารสนเทศ	ข้อมูลในรูปแบบใดก็ตามทั้งในแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ เช่น ข้อมูลในสิ่งพิมพ์ซึ่งอยู่ในระบบภายในหรือระบบภายนอกที่นอกเหนือการควบคุมขององค์กรและปรากฏเงื่อนไขดังต่อไปนี้ ▪ ข้อมูลที่พนักงานและลูกจ้างขององค์กรหรือบุคคลที่ได้รับมอบหมายได้มาประมวลผล จัดการ และ/หรือ ดูแล (เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษา) เพื่อปฏิบัติหน้าที่ ▪ ข้อมูลที่เกี่ยวเนื่องกับการจัดการ การปฏิบัติงาน วางแผน รายงาน หรือการตรวจสอบการดำเนินงานขององค์กร ข้อมูลที่ใช้อ้างอิงหรือจำเป็นต่อการทำงานของหน่วยงานอย่างน้อยหนึ่งหน่วย

คำจำกัดความ	ความหมาย
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (มาตรา ๖ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒) เช่น ชื่อ นามสกุล อีเมล รูป ลายนิ้วมือ รหัสประชาชน ซึ่งสามารถระบุตัวบุคคลได้ในทางตรง หรือการเก็บ Location หรือ Cookie เป็นการเก็บข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้ในทางอ้อม นอกจากนี้ ข้อมูลที่โดยพื้นฐานแล้วไม่สามารถนำไประบุตัวบุคคลได้แต่เมื่อนำไปใช้ร่วมกับข้อมูลอื่นแล้วก่อให้เกิดชุดข้อมูลที่สามารถระบุข้อมูลส่วนบุคคลได้ ก็ถือเป็นข้อมูลส่วนบุคคลเช่นกัน เช่น ที่อยู่ เพศ และอายุ ที่เมื่อนำมารวมกันแล้วสามารถระบุตัวบุคคลได้
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคลนั้น ๆ ไม่ว่าโดยทางตรงหรือทางอ้อม
บุคคลภายนอก (Third Parties)	หมายถึง บุคคลธรรมดา หรือนิติบุคคล สำนักงานราชการ หน่วยงานราชการ หรือบุคคลอื่นที่มิใช่เจ้าของข้อมูลส่วนบุคคล มิใช่สำนักงาน มิใช่ผู้ประมวลผลข้อมูลส่วนบุคคล และมิใช่บุคคลผู้ได้รับอำนาจจากสำนักงาน หรือ ได้รับอำนาจจากผู้ประมวลผลข้อมูลส่วนบุคคลให้ทำการประมวลผลข้อมูลส่วนบุคคลโดยตรง
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	ผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	ผู้ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ให้บริการภายนอก (Outsource)	ผู้ประมวลผลข้อมูลส่วนบุคคล ที่เป็นบุคคลธรรมดาหรือนิติบุคคลซึ่งไม่ใช่พนักงานและลูกจ้างของสำนักงาน ทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของสำนักงาน หรือ ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานร่วมของสำนักงาน
ฝ่ายงานเจ้าของสารสนเทศ	สายงาน ฝ่ายงาน หรือหน่วยงานปฏิบัติงานภายใต้ความรับผิดชอบของสำนักงาน มีหน้าที่และความรับผิดชอบในการจัดระดับชั้นความลับของข้อมูล ควบคุมการเข้าถึงข้อมูล ดูแลรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูล

๒. วัตถุประสงค์

สำนักงานตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล อันเป็นส่วนหนึ่งของการรับผิดชอบต่อสังคมและเป็นรากฐานในการสร้างความสัมพันธ์ที่น่าเชื่อถือให้กับประชาชน สำนักงานจึงยึดมั่นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎเกณฑ์ ข้อบังคับอื่น ๆ ที่เกี่ยวข้อง

เอกสารฉบับนี้ได้รับการจัดทำขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

- เพื่อชี้แจงความรับผิดชอบของสำนักงานที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- เพื่อกำหนดมาตรฐานและแนวทางบริหารข้อมูลส่วนบุคคล โดยครอบคลุมถึงการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

๓. ขอบเขต

นโยบายฉบับนี้ใช้บังคับการจัดเก็บข้อมูลส่วนบุคคลซึ่งมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล โดยครอบคลุมถึงบุคลากรทั้งหมด ได้แก่ พนักงาน ลูกจ้าง บุคลากรภายใต้การควบคุมของสำนักงาน รวมถึงหน่วยงานร่วมในการเข้าถึงหรือประมวลผลข้อมูลของสำนักงานนอกจากนี้ยังครอบคลุมถึงการส่งต่อข้อมูลสู่องค์กรภายนอก หน่วยงานราชการ หรือบุคคลที่ได้รับอนุญาตตามกฎหมาย ระเบียบ หรือข้อบังคับกฎหมายอื่น ๆ และใช้บังคับกับข้อมูลทุกรูปแบบ ทั้งข้อมูลอิเล็กทรอนิกส์ และไม่ใช่อิเล็กทรอนิกส์

๔. คำแถลงนโยบาย

๔.๑ นโยบายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy)

▪ นโยบายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy) ดูแลโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งได้รับการอนุมัติจากสำนักงาน โดยต้องจัดให้มีการประกาศและสื่อสารไปยังพนักงาน ลูกจ้าง และหน่วยงานที่เกี่ยวข้อง โดยกำหนดให้มีการทบทวนและปรับปรุงนโยบายฉบับนี้ให้เป็นปัจจุบันอย่างสม่ำเสมอ

▪ การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะต้องเป็นไปตามกฎหมาย มีความเป็นธรรม และมีความโปร่งใส

▪ การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องมีความเหมาะสมตามวัตถุประสงค์ที่กำหนด เป็นไปตามฐานในการประมวลผลข้อมูลส่วนบุคคลที่กำหนด

▪ การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการประมวลผลข้อมูลส่วนบุคคลอย่างจำกัดและสอดคล้องตามวัตถุประสงค์ที่กำหนด

▪ การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการปรับปรุงอยู่เสมอ รวมทั้งจะต้องมีการกำหนดขั้นตอนในการตรวจสอบ เพื่อให้ข้อมูลส่วนบุคคลมีความถูกต้องเป็นไปตามกฎหมายหรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกำหนด

▪ สำนักงานอนุญาตให้จัดเก็บข้อมูลส่วนบุคคลภายในระยะเวลาที่สำนักงานกำหนดเท่านั้น ข้อมูลส่วนบุคคลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด ผู้รับผิดชอบจะต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

▪ การประมวลผลข้อมูลส่วนบุคคลจะต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีสิทธิ การลบหรือทำลายข้อมูลทั้งโดยความตั้งใจและไม่ตั้งใจ และการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่สำนักงานยอมรับได้

๔.๒ นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)

สำนักงานมีการกำหนดแนวทางในการจัดเก็บเอกสารที่มีข้อมูลส่วนบุคคลของสำนักงาน เพื่อให้มั่นใจว่าเอกสาร รวมถึงเอกสารในรูปแบบอิเล็กทรอนิกส์ ที่มีข้อมูลส่วนบุคคลจะไม่ถูกเก็บไว้นานเกินความจำเป็น และมีมาตรการในการจัดเก็บที่สอดคล้องกับข้อกำหนดทางธุรกิจและกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

๑. สถานที่จัดเก็บข้อมูล

๑.๑ เอกสารในรูปแบบอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ (อีเมล) และ บันทึกมัลติมีเดีย (Multimedia)

เอกสารในรูปแบบอิเล็กทรอนิกส์ อีเมล และบันทึกมัลติมีเดียทั้งหมดจะต้องจัดเก็บภายในสถานที่ที่เหมาะสมเพื่อให้แน่ใจว่ามีการใช้มาตรการรักษาความปลอดภัยที่เป็นไปตามมาตรฐานที่กำหนดโดยกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึง กฎหมายอื่น แนวปฏิบัติ และคำสั่งที่เกี่ยวข้อง

๑.๒ เอกสารในรูปแบบกระดาษ

การจัดเก็บเอกสารในรูปแบบกระดาษที่จำเป็นสำหรับการดำเนินการตามภารกิจในแต่ละวันต้องเก็บไว้ในตู้เก็บเอกสารและลิ้นชักโต๊ะทำงานเมื่อไม่ได้ใช้งาน และจะต้องล็อคกุญแจตู้เก็บเอกสารและลิ้นชักที่จัดเก็บเอกสารที่มีข้อมูลส่วนบุคคลเมื่อสิ้นเวลาทำการของสำนักงาน

๒. การปกป้องเอกสาร

เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยเอกสารที่มีข้อมูลส่วนบุคคลที่อยู่ในการควบคุมของสำนักงานโดยมิชอบหรือโดยปราศจากอำนาจ เอกสารทั้งในรูปแบบกระดาษและรูปแบบอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลจะถูกเก็บไว้ในที่ปลอดภัยจนกว่าจะถูกทำลาย สำนักงานจะใช้เทคโนโลยีและกระบวนการต่าง ๆ ที่ได้รับการตรวจสอบอย่างสม่ำเสมอเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล

๓. การทำลายเอกสาร

เมื่อพ้นกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลหรือหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลแล้ว เอกสารในรูปแบบประเภทกระดาษที่มีข้อมูลส่วนบุคคลจะถูกทำลายโดยการย่อยเอกสารโดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว ส่วนข้อมูลส่วนบุคคลที่จัดเก็บทางอิเล็กทรอนิกส์จะถูกลบออกจากสื่อที่ใช้เก็บข้อมูล เช่น ฮาร์ดดิสก์จะถูกทำลาย หรือ ถูกลบข้อมูลโดยวิธีที่ไม่สามารถกู้คืนข้อมูลได้ โดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว

๔. การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

สำนักงานจะกำหนดระยะเวลาการจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ในการเก็บรวบรวมสำหรับการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน โดยอาจเป็นไปตามระยะเวลาที่กำหนดตามกฎหมาย แนวปฏิบัติของธุรกิจ หรือมาตรฐานของการประมวลผล โดยสำนักงานจะดำเนินการกำหนดระยะเวลาไว้ในเอกสารรายการบันทึกการประมวลผลข้อมูลส่วนบุคคล (ROPA) ของสำนักงาน

สำนักงานจะจัดให้มีกระบวนการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษาที่ได้กำหนดไว้ หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเป็นไปตาม **นโยบายในการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)**

๔.๓ นโยบายการแยกประเภทของข้อมูลส่วนบุคคล (Personal Data Classification Policy)

๑. แนวทางการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล

๑.๑ สำนักงานมีการกำหนดชั้นความลับของสารสนเทศไว้ ๔ ระดับ ได้แก่ ข้อมูลทั่วไป (Public) ข้อมูลใช้ภายใน (Internal Use) ข้อมูลความลับ (Confidential) และข้อมูลความลับที่สุด (Secret) โดยมีการกำหนดนิยาม รวมทั้งแนวทางในการควบคุมและป้องกันสารสนเทศตามระดับชั้นความลับของข้อมูล ซึ่งผู้ที่เกี่ยวข้องจะต้องปฏิบัติตามโดยเคร่งครัด หากกลุ่มของสารสนเทศประกอบไปด้วยสารสนเทศหลายระดับชั้นความลับ ให้ฝ่ายงานเจ้าของสารสนเทศกำหนดระดับชั้นความลับของสารสนเทศนั้นตามระดับชั้นความลับของสารสนเทศ ระดับสูงสุดของกลุ่มสารสนเทศ

๑.๒ ฝ่ายงานเจ้าของสารสนเทศมีหน้าที่กำหนดและทบทวนระดับชั้นความลับของข้อมูลส่วนบุคคลที่อยู่ภายใต้ความรับผิดชอบของตนอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับระดับความสำคัญของสารสนเทศที่อาจมีการเปลี่ยนแปลงตามระยะเวลา รวมทั้งจัดให้มีการควบคุมที่เหมาะสมกับระดับชั้นความลับของข้อมูล โดยฝ่ายงานเจ้าของสารสนเทศอาจมอบหมายกิจกรรมการควบคุมข้างต้นให้กับผู้ดูแลสารสนเทศ และอาจขอการสนับสนุนและความช่วยเหลือทางด้านเทคนิคจากฝ่ายงานเทคโนโลยีสารสนเทศ อย่างไรก็ตามฝ่ายงานเจ้าของสารสนเทศก็ยังเป็นผู้รับผิดชอบที่แท้จริงในการจัดระดับชั้นความลับและการควบคุมความมั่นคงปลอดภัยของสารสนเทศที่ตนเป็นผู้รับผิดชอบ

๑.๓ ฝ่ายงานเจ้าของสารสนเทศควรเก็บข้อมูลส่วนบุคคลเป็นความลับและเปิดเผยต่อบุคคลที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมายและกฎเกณฑ์ที่บังคับใช้เท่านั้น

๑.๔ ฝ่ายงานเจ้าของสารสนเทศและหน่วยงานอื่นที่เกี่ยวข้อง ต้องร่วมดำเนินการให้มีมาตรการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็น และได้รับอนุญาตให้เข้าถึงข้อมูลในระยะเวลาที่เหมาะสมเท่านั้น

๑.๕ การขอสิทธิเพื่อเข้าถึงข้อมูลส่วนบุคคลนอกเหนือจากสิทธิที่กำหนดไว้จะต้องผ่านการพิจารณาจากฝ่ายงานเจ้าของสารสนเทศ

๑.๖ การดำเนินการทางเทคนิคในการให้สิทธิเข้าถึงข้อมูลต้องเป็นไปตามมาตรการการรักษาความมั่นคงปลอดภัยสารสนเทศที่สำนักงานกำหนด

๑.๗ การเก็บรักษาข้อมูลส่วนบุคคลต้องเก็บรักษาตามระยะเวลาเท่าที่จำเป็น เพื่อให้เป็นไปตามวัตถุประสงค์ในการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาที่ระบุไว้ใน**นโยบายการจัดเก็บข้อมูลส่วนบุคคล** (Data Retention Policy)

๑.๘ การลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม ให้เป็นไปตาม**นโยบายการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด** (Personal Data Disposal Policy)

๑.๙ หากมีการว่าจ้างผู้ให้บริการภายนอกที่ต้องมีการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องมีการปฏิบัติตาม**นโยบายในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล** (Outsourcing Policy for Personal Data Processing) และต้องมีการจัดระดับชั้นความลับของข้อมูลส่วนบุคคลโดยฝ่ายงานเจ้าของสารสนเทศที่ได้ทำการว่าจ้างผู้ให้บริการภายนอกนั้น ๆ

๑.๑๐ การจัดระดับชั้นความลับของข้อมูลส่วนบุคคล ต้องมีการกำหนดความเสี่ยงเพื่อจัดระดับชั้นความลับของข้อมูลส่วนบุคคล ดังนี้

ระดับชั้นความลับข้อมูลสารสนเทศ	คำนิยามระดับชั้นความลับข้อมูลสารสนเทศ
ความลับที่สุด (Secret)	เป็นข้อมูลที่มีการประเมินแล้วว่า หากมีการเปิดเผยโดยไม่ได้รับอนุญาตจะสามารถสร้างความเสียหายและมีผลกระทบต่อภารกิจของสำนักงานอย่างร้ายแรง ข้อมูลที่จัดอยู่ในกลุ่มนี้จะต้องได้รับการดูแลเป็นพิเศษ ทั้งจากฝ่ายงานเจ้าของสารสนเทศและผู้ที่จำเป็นต้องใช้ข้อมูลตามหน้าที่ของงานที่รับผิดชอบ ทุกคนที่สามารถเข้าถึงข้อมูลเหล่านี้จำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA)

ระดับชั้นความลับข้อมูลสารสนเทศ	คำนิยามระดับชั้นความลับข้อมูลสารสนเทศ
	ตัวอย่างข้อมูลความลับที่สุด *เช่น แผนการดำเนินงานของสำนักงานก่อนการประกาศ หรือแผนงานที่อาจมีผลกระทบต่อความมั่นคงภายในประเทศ*
ความลับ (Confidential)	ข้อมูลซึ่งหากเปิดเผยโดยไม่ได้รับอนุญาต จะเป็นการฝ่าฝืนกฎ ข้อบังคับของสำนักงาน ก่อให้เกิดความเสียหายและมีผลกระทบต่อภารกิจของสำนักงานผู้ที่สามารถเข้าถึงข้อมูลประเภทนี้ได้จึงถูกจำกัดเพียงพนักงานและลูกจ้างเป็นรายบุคคล ฝ่ายงานหรือบุคคลที่สามที่มีความสัมพันธ์กันตามสัญญา โดยกลุ่มคนที่ระบุจำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA) ในนามรายบุคคลหรือหน่วยงานต้นสังกัด ซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายทั้งสองฝ่าย ***ตัวอย่างข้อมูลความลับ*** *เช่น รหัสผ่าน คีย์การเข้ารหัส ข้อมูลทางการเงิน ข้อมูลงบประมาณ ข้อมูลลูกค้า ข้อมูลที่เกี่ยวข้องกับระบบความปลอดภัย ข้อมูลจำลองลายนิ้วมือ ข้อมูลเงินเดือน ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ข้อมูลพันธุกรรม ข้อมูลสุขภาพ ข้อมูลชีวภาพ เป็นต้น*
ใช้ภายใน (Internal Use)	ข้อมูลที่เปิดเผยได้เฉพาะภายในสำนักงานและบุคคลภายนอกที่มีความสัมพันธ์กันตามสัญญา ซึ่งได้รับสิทธิเท่านั้น ไม่เหมาะที่จะเปิดเผยต่อสาธารณชนเป็นการทั่วไป ***ตัวอย่างข้อมูลใช้ภายใน*** *เช่น เอกสารภายใน อีเมลภายในสำนักงาน นโยบายและมาตรฐานของสำนักงาน สมุดรายชื่อโทรศัพท์ ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ อีเมล เบอร์โทรศัพท์*
ทั่วไป (Public)	ข้อมูลสารสนเทศที่ไม่ได้กระทบอย่างมีนัยสำคัญต่อการดำเนินงาน และผู้บริหารอนุมัติให้เปิดเผยต่อสาธารณะได้ อย่างไรก็ดีข้อมูลสารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้กับประชาชน ***ตัวอย่างข้อมูลทั่วไป*** *เช่น ข้อมูลที่เป็นประโยชน์แก่ประชาชน แผ่นพับประชาสัมพันธ์ด้านการตลาด ข่าวประชาสัมพันธ์ ข่าวประกาศที่เกี่ยวข้องกับการดำเนินงานของสำนักงาน*

ตัวอย่างการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use)
ข้อมูลที่ใช้ในการพิสูจน์หรือยืนยันตัวตน	รหัสผ่าน	✓	
	คีย์การเข้ารหัสข้อมูล (Encryption keys)	✓	
	ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า (Face recognition) ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ	✓	
	บันทึกกิจกรรมการเข้าถึงระบบ (Authentication logs)	✓	
ข้อมูลบัตรอิเล็กทรอนิกส์	ชื่อผู้ถือบัตรอิเล็กทรอนิกส์	✓	
	เลขบัตรอิเล็กทรอนิกส์	✓	

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use)
(เช่น บัตรเดบิต บัตรเครดิต เป็นต้น)	PIN, PIN block	✓	
	CVV, CVV๒, CVC๒, CID	✓	
	ข้อมูลบัตรบนแถบแม่เหล็ก	✓	
ข้อมูลที่สามารถระบุตัวบุคคลได้ (Personally Identifiable Information (PII))	ชื่อ นามสกุล		✓
	เลขบัตรประชาชน		✓
	เลขหนังสือเดินทาง		✓
	เลขบัตรประกันสังคม		✓
	เลขใบอนุญาตขับขี่		✓
	เลขประจำตัวผู้เสียภาษี		✓
	รหัสพนักงานและลูกจ้าง		✓
	เลขบัญชีธนาคาร		✓
	เลขที่กรมธรรม์		✓
	วันเดือนปีเกิด		✓
	อายุ		✓
	เพศ		✓
	ที่อยู่		✓
	เบอร์โทรศัพท์		✓
	อีเมล		✓
	ข้อมูลเงินเดือน	✓	
	ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID		✓
	ข้อมูลชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม	✓	
	ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน		✓
	ข้อมูลการจ้างงาน		✓
	ประวัติการทำงาน		✓
	ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง		✓
	ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file		✓
ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว	ความเชื่อในลัทธิ ศาสนาหรือปรัชญา	✓	
	ความคิดเห็นทางการเมือง	✓	

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use)
	เชื้อชาติ เผ่าพันธุ์	✓	
	ข้อมูลพันธุกรรม	✓	
	ประวัติอาชญากรรม	✓	
	พฤติกรรมทางเพศ	✓	
	ข้อมูลประวัติทางการแพทย์ สุขภาพ หมู่เลือด ความพิการ หรือข้อมูลสุขภาพจิต	✓	
	ข้อมูลสหภาพแรงงาน	✓	

ในกรณีที่ไม่สามารถกำหนดระดับชั้นความลับของสารสนเทศบางประเภทตามคำนิยามหรือตัวอย่างที่ได้กล่าวไว้ข้างต้น ให้ฝ่ายงานเจ้าของสารสนเทศเป็นผู้ตัดสินใจในการกำหนดระดับชั้นความลับของสารสนเทศดังกล่าว โดยสามารถขอคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสำนักงาน

๒. แนวทางในการควบคุมและป้องกันสารสนเทศ

การควบคุมและป้องกันสารสนเทศครอบคลุมในด้านการจัดทำ การจัดเก็บ การจัดพิมพ์ และการทำสำเนา การจัดส่ง การทำลาย และการนำกลับมาใช้ใหม่ของสารสนเทศทั้งในรูปแบบของเอกสารและอิเล็กทรอนิกส์ โดยมีรายละเอียดการควบคุมที่จำเป็น ดังต่อไปนี้

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การจัดทำข้อมูล				
การทำเครื่องหมายหรือสัญลักษณ์แสดงชั้นความลับเอกสารฉบับพิมพ์ (Hard Copy) และอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ควรระบุคำว่า “ข้อมูลใช้ภายใน” หรือ “INTERNAL USE” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน ยกเว้นกรณีที่เป็นเทป backup จะไม่ทำเครื่องหมายสัญลักษณ์ เพื่อป้องกันข้อผิดพลาดทางเทคนิค	ระบุคำว่า “ลับ” หรือ “CONFIDENTIAL” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน กรณีทำได้ ควรระบุทุกหน้า ยกเว้นกรณีที่เป็นเทป backup จะไม่ทำเครื่องหมายสัญลักษณ์ เพื่อป้องกันข้อผิดพลาดทางเทคนิค	ระบุคำว่า “ลับที่สุด” หรือ “SECRET” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน กรณีทำได้ ควรระบุทุกหน้า และควรระบุชื่อหน่วยงานเจ้าของเรื่อง เลขที่ชุดของจำนวนชุดทั้งหมด และเลขที่หน้าของจำนวนหน้าทั้งหมดด้วย
		กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ข้อมูลใช้ภายใน [ชื่อหน่วยงาน] ” หรือ	กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ลับ [ชื่อหน่วยงาน]” หรือ “[ชื่อ	กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ลับที่สุด [ชื่อหน่วยงาน]” หรือ

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
		"[ชื่อหน่วยงาน] INTERNAL USE" หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น	หน่วยงาน] CONFIDENTIAL" หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น	"[ชื่อหน่วยงาน] SECRET" หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น
การพิมพ์ออกทางเครื่องพิมพ์ (Printer) เอกสารฉบับพิมพ์	ไม่มีข้อบังคับพิเศษ	เมื่อพิมพ์เอกสารเสร็จจะต้องเก็บทันทีโดยไม่ปล่อยเอกสารทิ้งไว้ที่เครื่องพิมพ์	๑) ตรวจสอบเครื่องพิมพ์ปลายทางให้แน่ใจว่าถูกต้องทุกครั้งก่อนสั่งพิมพ์ ๒) เมื่อพิมพ์เอกสารเสร็จจะต้องเก็บทันทีโดยไม่ปล่อยเอกสารทิ้งไว้ที่เครื่องพิมพ์ ๓) หากมีการพิมพ์ไปที่เครื่องพิมพ์ ซึ่งเชื่อมต่อกับระบบเครือข่ายที่มีการใช้งานโดยผู้ใช้หลายคน ผู้สั่งพิมพ์ต้องเป็นผู้ไปรับเอกสารด้วยตนเอง โดยรอเอกสารตั้งแต่เริ่มพิมพ์จนกระทั่งเอกสารพิมพ์เสร็จ ๔) ห้ามพิมพ์เอกสารภายนอกสำนักงาน เช่น โรงแรม ศูนย์ประชุม สนามบิน เป็นต้น	
การจัดเก็บข้อมูล				
เอกสารฉบับพิมพ์ (Hard Copy) หรือสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	เก็บไว้ในที่เหมาะสมกับการปฏิบัติงานและมีการจัดเก็บอย่างเป็นระบบ	เก็บไว้ในที่มิดชิดและสามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น การเก็บในตู้ใส่กุญแจเมื่อไม่ได้ใช้งาน หรือการเก็บในตู้นิรภัย	
การจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์ หรือเครื่องแม่ข่าย (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	ไม่จำเป็นต้องเข้ารหัส (Unencrypted) แต่ต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และมีการกำหนดสิทธิในการเข้าถึง	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และมีการกำหนดสิทธิในการเข้าถึง	
การจัด เก็บข้อมูลในระบบ Cloud (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	มีมาตรการในการควบคุม และมีการกำหนดสิทธิในการเข้าถึง	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และกำหนดสิทธิในการเข้าถึง	

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การจัดเก็บข้อมูลในโทรศัพท์เคลื่อนที่ (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	มีการตั้งค่าการพิสูจน์ตัวตนก่อนการเข้าถึง เช่น pin-code หรือรหัสผ่านเพื่อป้องกันการเข้าถึงข้อมูล กรณีโทรศัพท์สูญหายหรือถูกขโมย		
การจัดเก็บข้อมูลบนสื่อบันทึกข้อมูล (Media) เช่น USB, Memory Stick, SD Card, CD, DVD, External Hard Disk (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	มีการเข้ารหัส (Encrypted) แฟ้มข้อมูลหรือสื่อบันทึกข้อมูล เช่น • Zip file ด้วย AES-๒๕๖ • BitLocker • Utility ที่เจ้าของผลิตภัณฑ์มีให้	
การจัดเก็บข้อมูล (เมื่อนำข้อมูลออกนอกสถานที่)				
เมื่อนำข้อมูลไปด้วยระหว่างการเดินทาง เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	ข้อมูลจะต้องอยู่ภายใต้การดูแลตลอดเวลา หรือเก็บในที่ที่สามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น ใส่ซองปิดผนึกไว้ในห้องโรงแรมที่มีการใส่กุญแจ หรือเก็บในตู้นิรภัย		
เมื่อนำข้อมูลเอกสารฉบับพิมพ์ (Hard Copy) ไว้ในรถยนต์	ไม่มีข้อบังคับพิเศษ	เก็บไว้ในรถยนต์ที่มีการล็อคและไว้ในจุดที่ไม่สามารถมองเห็นได้จากภายนอก		
การส่ง/รับ และการโอนข้อมูล				
การจัดส่งผ่านทางไปรษณีย์ เอกสารฉบับพิมพ์ (Hard copy) หรือสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	ใส่เอกสารในซองทึบ ปิดผนึก	ใส่เอกสารในซองทึบ ปิดผนึก และประทับตราที่ระบุคำว่า “ลับ” หรือ “CONFIDENTIAL”	ไม่ควรส่งผ่านไปรษณีย์ หากจำเป็นจะต้องได้รับอนุญาตจากฝ่ายงานเจ้าของสารสนเทศก่อน โดยวิธีการปฏิบัติให้ปฏิบัติเช่นเดียวกับข้อมูลความลับ
การส่งด้วยมือ เอกสารฉบับพิมพ์ (Hard Copy) หรือ	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	๑) ใส่เอกสารในซองทึบ ปิดผนึก และประทับตราที่	๑) ต้องทำการปิดผนึกซองเอกสารก่อนจัดส่งให้ไม่สามารถสังเกตได้

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
สื่อบันทึกข้อมูล (Media)			ระบุคำว่า “ลับ” หรือ “CONFIDENTIAL” ๒) จัดทำบันทึกการส่งและการรับไว้เป็นหลักฐาน	จากภายนอกใส่เอกสารในซอง ๒ ชั้น ๒) ซองชั้นในให้ระบุระบุคำว่า “ลับที่สุด” หรือ “SECRET” และซองชั้นนอกห้ามระบุระดับชั้นความลับเอกสาร ๓) จัดทำบันทึกการส่งและรับไว้เป็นหลักฐาน ๔) จัดส่งให้บุคคลที่ได้รับมอบหมายเท่านั้น
การส่งผ่านเครื่องโทรสาร	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	๑) ต้องระบุชื่อรายละเอียดของผู้รับและผู้ส่งให้ชัดเจนครบถ้วน ๒) ตรวจสอบหมายเลขปลายทางให้แน่ใจว่าถูกต้องทุกครั้ง ๓) ต้องส่งโทรสารไปยังสถานที่ปลายทางที่มีความมั่นคงปลอดภัยเพียงพอ ๔) ผู้ส่งต้องอยู่รอจนการส่งเสร็จสิ้นแล้วจึงเก็บเอกสารกลับไปโดยไม่ลืมไว้ที่เครื่องโทรสาร ๕) ผู้รับเอกสารที่ปลายทางต้องเป็นผู้ได้รับอนุญาตเท่านั้น	ห้ามส่งผ่านเครื่องโทรสาร

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Email, FTP)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	ต้องแลกเปลี่ยนข้อมูลให้มีความมั่นคงปลอดภัย เช่น ต้องมีการเข้ารหัส หรือใส่รหัสผ่านโดยต้องไม่ส่งรหัสผ่านไปพร้อมกับข้อมูล หรือส่งรหัสผ่านคนละช่องทางกับการส่งข้อมูลครั้งนั้น เป็นต้น	ไม่ควรมีการแลกเปลี่ยนข้อมูลทาง Electronic หากจำเป็นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน โดยวิธีการปฏิบัติให้ปฏิบัติเช่นเดียวกับข้อมูลความลับ
การจัดการกรณีข้อมูลสูญหาย				
ข้อมูลอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	กรณีข้อมูลสูญหายหรือถูกขโมยให้รายงานต่อหัวหน้าฝ่ายงานเจ้าของสารสนเทศทันทีที่ทราบเหตุ เพื่อดำเนินการลดความเสียหายให้มากที่สุด เท่าที่จะเป็นไปได้ เช่น การเปลี่ยนรหัสผ่านหรือล็อคการเข้าสู่บัญชีผู้ใช้ กรณีเครื่องคอมพิวเตอร์ถูกขโมย หรือการลบข้อมูล (wipe data) ในโทรศัพท์เคลื่อนที่ กรณีโทรศัพท์เคลื่อนที่สูญหาย		
เอกสารฉบับพิมพ์ (Hard copy)	ไม่มีข้อบังคับพิเศษ	กรณีข้อมูลสูญหายหรือถูกขโมยให้รายงานหัวหน้าฝ่ายงานเจ้าของสารสนเทศทันทีที่ทราบเหตุ		
อื่น ๆ				
เอกสารฉบับพิมพ์ (hard copy) หรือข้อมูลอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	กรณีที่ข้อมูลลับหรือข้อมูลลับที่สุดไม่มีเครื่องหมายแสดงชั้นความลับไว้ แต่หากพนักงานและลูกจ้างรู้ หรือควรจะรู้ข้อเท็จจริงว่าข้อมูลนั้นได้มีการกำหนดชั้นความลับไว้แล้ว ให้ปฏิบัติกับข้อมูลนั้นเช่นเดียวกับข้อมูลที่มีเครื่องหมายแสดงชั้นความลับไว้ และให้พนักงานและลูกจ้างจัดทำหรือแจ้งฝ่ายงานเจ้าของสารสนเทศให้จัดทำเครื่องหมายแสดงชั้นความลับโดยเร็ว	

๔.๔ นโยบายการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)

สำนักงานตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล จึงกำหนดให้มีการลบ ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลตาม**นโยบาย**

ในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy) หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมและสอดคล้องกับการรักษาความลับของข้อมูลส่วนบุคคล

ทั้งนี้เพื่อป้องกันการสูญหาย การเข้าถึง การทำลาย การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย ให้ดำเนินการตามแนวทางในการควบคุมและป้องกันสารสนเทศที่กำหนดใน**นโยบายการแยกประเภทของข้อมูลส่วนบุคคล (Personal Data Classification Policy)**

๑. แนวทางในการลบหรือทำลายข้อมูล

สำนักงานมีการเก็บรักษาข้อมูลทั้งในรูปแบบกระดาษ สื่อบันทึกข้อมูลและอิเล็กทรอนิกส์ ซึ่งมีแนวทางการลบหรือทำลายด้วยวิธีที่มีความมั่นคงปลอดภัยอย่างเหมาะสมกับระดับชั้นความลับของข้อมูลและประเภทของข้อมูลแตกต่างกัน รายละเอียดดังนี้

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การทำลายข้อมูล				
เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	ฉีกทำลาย หรือใช้เครื่องย่อยเอกสาร หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร	ใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร	ต้องส่งเอกสารคืนกลับให้หน่วยงานเจ้าของข้อมูลเพื่อทำการทำลาย หรือใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) เท่านั้น ทั้งนี้ต้องได้รับอนุมัติจากระดับหัวหน้าฝ่ายขึ้นไปของฝ่ายงานเจ้าของสารสนเทศก่อนทำลาย
การทำลายข้อมูลอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ต้องดำเนินการลบข้อมูลด้วยการลบข้อมูลและ Clear ข้อมูลใน Recycle Bin หรือใช้โปรแกรมในการลบข้อมูล เช่น Eraser	ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ ๓ Passes หรือ Dumping ข้อมูล **กรณีที่มีการคืนอุปกรณ์ให้กับหน่วยงานภายนอกให้ใช้ซอฟต์แวร์ Low Level Format	
การทำลายข้อมูลค่า Configuration และข้อมูลที่จัดเก็บบนอุปกรณ์	ไม่มีข้อบังคับพิเศษ	Reset ค่า Configuration และข้อมูลที่จัดเก็บบนอุปกรณ์เป็นค่า Factory Default		

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การทำลายสื่อบันทึกข้อมูลชนิด CD/DVD	ไม่มีข้อบังคับพิเศษ	ทุบทำลาย หรือใช้เครื่องทำลายแผ่นบันทึกข้อมูลแบบ Strip-cut		
การทำลายสื่อบันทึกข้อมูลชนิด USB Flash Drive, Hard disk และ Tape	ไม่มีข้อบังคับพิเศษ	ทุบทำลาย หรือ วิธีการที่ฝ่ายงานเทคโนโลยีสารสนเทศพิจารณาว่ามีความมั่นคงปลอดภัย		

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงเมื่อมีกฎเกณฑ์เกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลเพิ่มเติมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภายหลัง

๒. แนวทางการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล

๒.๑ ในกรณีที่ไม่สามารถลบหรือทำลายข้อมูลส่วนบุคคลได้โดยตรง เนื่องจากอาจส่งผลกระทบต่อความถูกต้องในการปฏิบัติงาน เช่น อาจส่งผลให้การทำงานของฐานข้อมูลไม่ถูกต้อง หรือเป็นข้อจำกัดของระบบ สำนักงานจะใช้วิธีการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของข้อมูลส่วนบุคคลได้ ดังนี้

๑) การเปลี่ยนแปลงส่วนใดส่วนหนึ่งของข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่มหรือการทำให้เป็นข้อมูลอื่น ๆ หรือการใช้กระบวนการอื่นใดที่ได้รับการรับรองเป็นมาตรฐานในปัจจุบัน เช่น การใช้ Hash Function เพื่อเปลี่ยนข้อมูลเดิมให้ไม่สามารถที่จะให้ข้อมูลย้อนกลับมาระบุตัวตนของเจ้าของข้อมูลได้

๒) การลดความชัดเจนของข้อมูล (Blurring or Noising) โดยการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลเดิมเพื่อลดความเฉพาะเจาะจงของข้อมูลลง

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงเมื่อมีกฎเกณฑ์เกี่ยวกับการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวตนได้เพิ่มเติมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภายหลัง

๒.๒ สำนักงานจะดำเนินการลบข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ตามประเภทของข้อมูลส่วนบุคคล เมื่อมีกรณีดังต่อไปนี้

๑) ครบกำหนดระยะเวลาการจัดเก็บตามที่กำหนดไว้ใน**นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)**

๒) ข้อมูลส่วนบุคคลนั้นไม่มีความเกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

๓) ข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย

๔) เจ้าของข้อมูลส่วนบุคคลร้องขอการใช้สิทธิตามสิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคลที่มีการระบุไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อเจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

๒.๓ หากมีการขอให้ลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ สำนักงานจะดำเนินการตามกระบวนการดังนี้

๑) เมื่อได้รับแบบคำร้องขอใช้สิทธิในการลบหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ข้อมูลจะถูกส่งต่อไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและทำการบันทึกเอาไว้

๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการตรวจสอบข้อมูลส่วนบุคคลทั้งหมดที่เกี่ยวข้อง เพื่อหาความจำเป็นขั้นพื้นฐานทางกฎหมายและวัตถุประสงค์เดิม

๓) ตรวจสอบแบบคำร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ เพื่อให้แน่ใจว่าการขอลบข้อมูลนั้นจะไม่เกี่ยวกับวัตถุประสงค์ในการเก็บรวบรวม หรือการประมวลผลอย่างอื่น

๔) ดำเนินการลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ทั้งนี้ ต้องตรวจสอบเพื่อให้แน่ใจว่าได้มีการลบ/ทำลายข้อมูลส่วนบุคคลออกจากระบบหรือเอกสารที่ใช้งานอยู่ รวมถึงในระบบสำรอง หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้

๕) หากมีการปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลบันทึกการปฏิเสธดังกล่าวพร้อมเหตุผลในการปฏิเสธ และแจ้งเจ้าของข้อมูลส่วนบุคคลให้รับทราบ

๒.๔ สำนักงานสามารถปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคลที่ขอให้ลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ ตามมาตรา ๓๓ วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนี้

๑) มีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล

๒) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

๓) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๔) เป็นการจำเป็นในการปฏิบัติตามกฎหมายของสำนักงานเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

๕) การเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

๔.๕ นโยบายหรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดแนวทางการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่สำนักงานมีการเก็บรวบรวม ใช้ และเปิดเผยไปยังบุคคลอื่น ครอบคลุมทั้งข้อมูลส่วนบุคคลของพนักงานและลูกจ้างของสำนักงานและหน่วยงานร่วมให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑. แนวปฏิบัติ

แนวปฏิบัติการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

๑.๑ ต้องมีการทำข้อตกลงหรือสัญญาในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ระหว่างสำนักงานซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล และหน่วยงานอื่น และ/หรือผู้ให้บริการภายนอกรายนั้นซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล โดยข้อตกลงหรือสัญญาจะต้องเป็นไปตามรูปแบบที่สำนักงานกำหนดไว้

๑.๒ เนื้อหาของข้อตกลงหรือสัญญาระหว่างสำนักงาน และหน่วยงานอื่น และ/หรือ ผู้ให้บริการภายนอกดังกล่าวจะต้องมีการกำหนดมาตรการเกี่ยวกับ

๑.๒.๑ หน้าที่ในการประมวลผลข้อมูล โดยต้องมีข้อความเกี่ยวกับ

๑) คำสั่งในการประมวลผลข้อมูลส่วนบุคคล และไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งเป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลส่วนบุคคล และการให้การรับรองจากผู้ประมวลผลข้อมูลส่วนบุคคลว่าคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๒) การให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีการจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลให้กับบุคคลที่ได้รับมอบหมาย โดยให้เข้าถึงข้อมูลส่วนบุคคลได้เท่าที่จำเป็นภายในวัตถุประสงค์ที่กำหนด

๓) ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ประมวลผล รวมถึงมีมาตรการที่ทำให้มั่นใจว่าบุคคลที่ได้รับสิทธิเข้าถึงข้อมูลส่วนบุคคลได้ให้คำมั่นสัญญาหรือมีหน้าที่ตามสัญญาในการรักษาความลับของข้อมูลส่วนบุคคล

๔) ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อการปฏิบัติตามหน้าที่ตามสัญญาหรือตามที่ตกลงกัน รวมถึงยินยอมและให้ความร่วมมือในการตรวจสอบและสอบสวนโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ตรวจสอบซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมอบหมาย

๑.๒.๒ มาตรการในการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อความเกี่ยวกับ

ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดหามาตรการการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยอย่างน้อยต้องประกอบด้วยการดำเนินการดังนี้

๑) มาตราการรักษาความมั่นคงปลอดภัยจะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

๒) มาตรการรักษาความมั่นคงปลอดภัยจะต้องประกอบไปด้วยมาตรการเชิงองค์กร และมาตรการเชิงเทคนิคที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพที่จำเป็นด้วย

๓) มาตรการรักษาความมั่นคงปลอดภัยจะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละ เมิด

ข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย

๔) มาตรการรักษาความมั่นคงปลอดภัยจะต้องคำนึงความสามารถในการธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคล

๕) สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

๖) ในส่วนที่เกี่ยวข้องการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบหรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้

ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญที่มีการพิสูจน์และยืนยันตัวตน และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงหลักการให้สิทธิเท่าที่จำเป็น

ข) การบริหารจัดการการเข้าถึงของผู้ใช้งานที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน การจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไขหรือลบข้อมูลส่วนบุคคล

๗) การสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยให้ พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งานหรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ

๑.๒.๓ หน้าที่ในการดำเนินกิจกรรมที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

๑) หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการสนับสนุนผู้ควบคุมข้อมูลส่วนบุคคลในเรื่องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

๒) การแจ้งต่อผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

๑.๒.๔ การแจ้งเตือนหากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้า หากทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

๑.๒.๕ การเก็บรักษาข้อมูลส่วนบุคคล และการลบข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับ

๑) หน้าที่และระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็น เพื่อการปฏิบัติหน้าที่ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล

๒) วิธีในการลบ ทำลาย ส่งคืน หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

๓) การเก็บข้อมูลส่วนบุคคลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๑.๒.๖ การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยต้องมีข้อความเกี่ยวกับ

๑) การไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เว้นแต่จะได้รับอนุญาตจากสำนักงาน

๒) การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ จะต้องเป็นไปตามเงื่อนไขที่กำหนดในกฎหมายคุ้มครองข้อมูลส่วนบุคคลและประกาศที่เกี่ยวข้อง

๔.๖ นโยบายการส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก หรือการส่งข้อมูลส่วนบุคคลไปยังประเทศอื่น (Third Parties / Cross Border Data Transfer Policy)

สำนักงานได้มีการกำหนดนโยบายในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก หรือการส่งหรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศ โดยมีวัตถุประสงค์เพื่อชี้แจงข้อตกลงในการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก (หน่วยงานภายนอก) หรือการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ และกำหนดหลักเกณฑ์และมาตรการคุ้มครองในการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก (หน่วยงานภายนอก) หรือการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ

๑. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

สำนักงานจะเปิดเผยข้อมูลส่วนบุคคลให้แก่องค์กรหรือหน่วยงานภายนอกโดยมีแนวปฏิบัติดังนี้

๑.๑ หากจะมีการเปิดเผยข้อมูลส่วนบุคคลให้กับ สำนักงานคู่ค้า พันธมิตรทางธุรกิจ และ/หรือ ผู้ให้บริการภายนอก ควรมีการระบุรายชื่อของหน่วยงานอื่น และ/หรือ ผู้ให้บริการภายนอก ในแบบบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (ROPA) โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรให้คำปรึกษาและจะต้องพิจารณาฐานในการประมวลผลข้อมูลส่วนบุคคลและเงื่อนไขให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑.๒ กรณีส่งหรือโอนข้อมูลส่วนบุคคลไปยังนิติบุคคล จะต้องพิจารณาว่าในการส่งหรือโอนข้อมูลส่วนบุคคลนั้นมีมาตรการการรักษาความมั่นคงปลอดภัย และมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน

๑.๓ กรณีที่หน่วยงานรัฐ หรือองค์กรผู้ถืออำนาจรัฐ ร้องขอเข้าถึงข้อมูลส่วนบุคคลโดยการอ้างถึงกฎหมาย ระเบียบ หรือคำสั่งใด ๆ ที่สำนักงานจะต้องปฏิบัติตาม ผู้รับผิดชอบควรพิจารณาให้หน่วยงานเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่มีบทบัญญัติกฎหมาย หรือคำสั่ง หรือหนังสือแจ้งอย่างเป็นทางการ อย่างใดอย่างหนึ่งเป็นอย่างน้อยตามอำนาจทางกฎหมายเท่านั้น ยกเว้นกรณีที่เป็นการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation) ของสำนักงานที่แม้ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่สำนักงานจะต้องกระทำตามหน้าที่อยู่แล้ว

๒. การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ (Cross Border data Transfer Policy)

เพื่อให้การส่งหรือโอนข้อมูลส่วนบุคคลอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล การดำเนินการส่งหรือโอนข้อมูลส่วนบุคคลไปประเทศปลายทาง หรือองค์กรระหว่างประเทศจะต้องมีความมั่นคงปลอดภัย โดยสำนักงานสามารถพิจารณาทางเลือกดังต่อไปนี้

๒.๑ การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์กรระหว่างประเทศ สำนักงานจะดำเนินการส่งข้อมูลส่วนบุคคลไปยังประเทศที่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๒.๒ มีการจัดทำข้อตกลงเป็นไปตามข้อสัญญามาตรฐาน (Standard Data Protection Clauses) มาใช้เพื่อให้ข้อมูลส่วนบุคคลถูกส่งหรือโอนอย่างที่ควรจะเป็น เพื่อให้การให้บริการ รวมถึงการรักษามาตรฐาน

และการปรับปรุงบริการให้เป็นไปโดยถูกต้องตามกฎหมาย อย่างไรก็ตามข้อสัญญาคุ้มครองข้อมูลส่วนบุคคลจะต้องมีการกำหนดหน้าที่ทางสัญญาเกี่ยวกับการส่งข้อมูลส่วนบุคคลไปยังต่างประเทศตลอดจนการโอนย้ายข้อมูลส่วนบุคคล ซึ่งเจ้าข้อมูลส่วนบุคคลสามารถใช้สิทธิของตนเองในการส่งหรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศได้ โดยต้องมีมาตรการคุ้มครองที่เหมาะสม ดังนี้

๒.๒.๑ ในการตกลงส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศจะต้องมีรายละเอียดเกี่ยวกับ

๑) สำนักงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

๑.๑) รับรองว่าการเก็บรวบรวม ประมวล ส่งหรือโอนข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑.๒) พิจารณาว่าผู้รับโอนข้อมูลส่วนบุคคลสามารถปฏิบัติตามข้อกำหนดตามที่ระบุในนโยบายนี้ได้

๑.๓) ให้ข้อมูลเกี่ยวกับกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลซึ่งใช้บังคับอยู่ในประเทศปลายทางหรือบังคับแก่องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล

๑.๔) ตอบคำถามของเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยผู้รับการส่งหรือโอนข้อมูลส่วนบุคคล

๑.๕) ให้ข้อมูลเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นสิทธิเกี่ยวกับความรับผิดและสิทธิของบุคคลที่สามแก่เจ้าของข้อมูลส่วนบุคคล

๑.๖) ร่วมรับผิดกับผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายจากการฝ่าฝืนข้อกำหนด

๑.๗) ร่วมกับผู้รับการส่งหรือผู้รับโอนในการระงับข้อพิพาทที่เกิดขึ้นโดยเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผข้อมูลส่วนบุคคล โดยใช้วิธีการระงับข้อพิพาทโดยการไกล่เกลี่ยซึ่งไม่ได้มีผลบังคับผูกพันทางกฎหมาย

๑.๘) ในกรณีที่ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลฝ่าฝืนหน้าที่ตามที่ได้กำหนดสำนักงานมีสิทธิที่จะพักการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจนกว่าการฝ่าฝืนจะได้รับการแก้ไขหรือข้อกำหนดถูกยกเลิก

๒) บุคคลผู้รับส่งหรือรับโอนข้อมูลส่วนบุคคลที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

๒.๑) กำหนดว่ามีการจัดมาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา ๓๗ (๑) กฎหมายคุ้มครองข้อมูลส่วนบุคคล

๒.๒) ดำเนินการให้บุคคลภายนอกที่สามารถเข้าถึงข้อมูลส่วนบุคคลนั้นรักษาความลับของข้อมูลส่วนบุคคล

๒.๓) รับรองว่าตนไม่มีเหตุอันควรจะเชื่อได้ว่ามีกฎหมายใดที่ขัดขวางมิให้สามารถปฏิบัติหน้าที่เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามข้อกำหนดนี้ได้

๒.๔) ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่กำหนดเท่านั้น

๒.๕) แจ้งให้สำนักงานได้ทราบถึงส่วนงานภายในองค์กรซึ่งมีหน้าที่ในการตอบสนองต่อคำร้องเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและจะให้ความร่วมมือกับสำนักงานโดยสุจริต

๒.๖) ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบ ในกรณีที่ได้รับการร้องขอจากสำนักงาน

๒.๗) ประมวลผลข้อมูลส่วนบุคคลโดยสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๒.๘) ร่วมรับผิดกับสำนักงานในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายจากการฝ่าฝืนข้อกำหนด

๒.๙) ร่วมกับสำนักงานในการระงับข้อพิพาทที่เกิดขึ้นโดยเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยใช้วิธีการระงับข้อพิพาทโดยการไกล่เกลี่ยซึ่งไม่ได้มีผลบังคับผูกพันทางกฎหมาย

๒.๒.๒ ในการตกลงส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศ จะต้องมีรายละเอียดเกี่ยวกับข้อสัญญาที่กำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถบังคับสิทธิของตนต่อสำนักงาน ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

๑) สำนักงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

๑.๑) รับรองว่าการประมวลผลข้อมูลส่วนบุคคลซึ่งหมายรวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นไปโดยสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑.๒) รับรองว่าผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลจะประมวลผลข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนตามคำสั่งของสำนักงานในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมายที่บังคับใช้แก่กรณีและข้อกำหนดนี้

๑.๓) รับรองว่าผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะจัดหามาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา ๓๗ (๑) ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑.๔) รับรองว่าจะมีการจัดหามาตรการด้านความปลอดภัยเพื่อป้องกันคุ้มครองมิให้ข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนสูญหายโดยอุบัติเหตุหรือโดยการกระทำโดยมิชอบ หรือการถูกทำลายโดยอุบัติเหตุหรือการกระทำโดยมิชอบ การเปลี่ยนแปลงแก้ไข การถูกเปิดเผย หรือการเข้าถึงโดยมิชอบโดยเฉพาะอย่างยิ่งในกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลผ่านระบบโครงข่าย (Transmission of Data over a Network) และการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายใด ๆ

๑.๕) รับรองว่าจะมีการปฏิบัติตามมาตรการคุ้มครองความปลอดภัยของข้อมูล

๑.๖) รับรองว่าเจ้าของข้อมูลส่วนบุคคลจะได้รับการแจ้งว่ามีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลในกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมาตรา ๒๖ กฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑.๗) ดำเนินการส่งการแจ้งเตือนที่ได้รับจากผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่สำนักงานตัดสินใจว่าจะส่งหรือโอนข้อมูลส่วนบุคคลต่อไป หรือยกเลิกพักการส่งหรือโอนข้อมูลส่วนบุคคล

๑.๘) ส่งบทสรุปรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลช่วง

๑.๙) ร่วมกับสำนักงานรับผิดต่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการไม่ปฏิบัติตามหน้าที่ที่กำหนดในข้อกำหนดนี้ซึ่งไม่ว่าจะเป็นการกระทำของสำนักงานหรือผู้รับสิทธิการส่งหรือรับโอน

๑.๑๐) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถเรียกร้องค่าเสียหายจากสำนักงานตามข้อกำหนดได้เนื่องจากสำนักงานไม่สามารถถูกติดตามตัวได้ หรือล้มละลาย เจ้าของข้อมูลส่วนบุคคลสามารถเรียกค่าเสียหายได้จากการผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล

๑.๑๑) สำนักงานจะส่งสำเนาของข้อกำหนดนี้ให้สำนักงานคณะกรรมคุ้มครองข้อมูลส่วนบุคคลเก็บรักษาไว้

๒) บุคคลผู้รับส่งหรือรับโอนข้อมูลส่วนบุคคลที่มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

๒.๑) รับรองว่าจะประมวลผลข้อมูลส่วนบุคคลเฉพาะในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลและตามคำสั่งของสำนักงานเท่านั้น ในกรณีที่ไม่สามารถปฏิบัติการตามหน้าที่ดังกล่าวได้ จะต้องแจ้งสำนักงานทราบโดยไม่ชักช้า ในกรณีนี้สำนักงานสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้

๒.๒) รับรองว่าตนไม่มีเหตุอันควรจะเชื่อได้ว่ามีกฎหมายใดที่ขัดขวางมิให้สามารถประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของสำนักงาน และในกรณีที่มีการเปลี่ยนแปลงทางกฎหมายซึ่งจะส่งผลต่อการปฏิบัติหน้าที่ตามข้อกำหนดนี้ ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะแจ้งให้สำนักงานทราบถึงการเปลี่ยนแปลงดังกล่าวโดยไม่ชักช้า ในกรณีนี้สำนักงานสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้

๒.๓) รับรองว่าตนได้จัดหามาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา ๓๗ (๑) กฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว

๒.๔) แจ้งให้สำนักงานทราบโดยไม่ชักช้าเกี่ยวกับคำร้องให้เปิดเผยข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมาย เว้นแต่ กรณีไม่สามารถแจ้งได้เนื่องจากมีกฎหมายห้าม เช่น เป็นข้อห้ามตามกฎหมายอาญาเพื่อรักษาความลับของการดำเนินกระบวนการสืบสวนสอบสวน การเข้าถึงข้อมูลหรือโดยการกระทำที่มิชอบ และคำร้องที่ได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรงโดยไม่มีการตอบสนองต่อคำร้องดังกล่าว

๒.๕) สอบถามสำนักงานถึงการประมวลผลข้อมูลส่วนบุคคลซึ่งถูกส่งหรือโอน

๒.๖) ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบในกรณีที่ได้รับคำร้องขอจากสำนักงาน

๒.๗) ส่งบทสรุปรายละเอียดเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลตลอดจนสำเนาสัญญาให้บริการประมวลผลข้อมูลส่วนบุคคลช่วงโดยลบส่วนที่เป็นข้อมูลเชิงพาณิชย์ออก แต่มีการเติมรายละเอียดเกี่ยวกับมาตรการรักษาความปลอดภัยเข้าไปแทนในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถดำเนินการให้ได้รับรายละเอียดดังกล่าวจากสำนักงานได้

๒.๘) แจ้งสำนักงานให้ทราบถึงการประมวลผลข้อมูลส่วนบุคคลช่วงและได้รับความยินยอม

๒.๙) ร่วมกับสำนักงานรับผิดต่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการไม่ปฏิบัติตามหน้าที่ที่กำหนดในข้อกำหนดนี้ซึ่งไม่ว่าจะเป็นการกระทำของสำนักงานหรือผู้รับการส่งหรือรับโอน

๒.๑๐) การประมวลผลข้อมูลส่วนบุคคลช่วงจะเป็นไปตามข้อกำหนดนี้

๒.๑๑) ส่งสำเนาสัญญาประมวลผลข้อมูลส่วนบุคคลช่วงให้กับสำนักงาน

๒.๑๒) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนเพื่อเรียกร้องค่าสินไหม ทดแทนหรือค่าเสียหายจากผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล ผู้รับการส่งหรือรับโอนข้อมูล

ส่วนบุคคลตกลงว่าจะระงับข้อพิพาทดังกล่าวโดยการไกล่เกลี่ยซึ่งมีความเป็นอิสระหรือโดยองค์กรคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

๒.๓ ในกรณีที่ไม่สามารถใช้ทางเลือกการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในข้อ ๑) และ ๒) สามารถดำเนินการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ หากเป็นกรณีดังนี้

- เป็นการปฏิบัติตามกฎหมายของสำนักงาน
- สำนักงานได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
- สำนักงานมีความจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- เป็นการกระทำตามสัญญาระหว่างสำนักงานกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- สำนักงานมีความจำเป็นต้องป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
- สำนักงานมีความจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

๒.๔ ในกรณีที่มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้นไม่มีมาตรฐานเพียงพอ ให้เสนอต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัยเสียก่อน สำนักงานจะใช้คำรับรองที่ได้รับการยอมรับโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งประกอบกับคำมั่นสัญญาที่มีผลบังคับผูกพันผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศที่จะปรับใช้มาตรการที่เหมาะสมเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล เพื่อแสดงให้เห็นว่ามีการป้องกันที่เหมาะสมในการส่งหรือโอนข้อมูลส่วนบุคคลในระดับสากล

ประกาศ ณ วันที่ ๒๐ ธันวาคม พ.ศ. ๒๕๖๕

(นายวีระพงศ์ มาลัย)
ผู้อำนวยการ
สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม