ประกาศกรมการปกครอง

เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๘

ตามที่กรมการปกครองมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานของรัฐตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงเป็นการสมควรกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของกรมการปกครอง เพื่อถือเป็นหลักเกณฑ์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล และกำหนดมาตรการในการบริหารจัดการการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลที่มีประสิทธิภาพและเหมาะสม สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และได้มีประกาศกรมการปกครอง เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๗ ฉบับวันที่ ๑๐ กรกฎาคม ๒๕๖๗ ไว้แล้ว นั้น

เพื่อให้นโยบายการคุ้มครองข้อมูลส่วนบุคคลของกรมการปกครองมีประสิทธิภาพเหมาะสมและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูล พ.ศ. ๒๕๖๒ ยิ่งขึ้น อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ แก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ อธิบดีกรมการปกครอง จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศกรมการปกครองเรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๗ ฉบับวันที่ ๑๐ กรกฎาคม ๒๕๖๗

ข้อ ๒ ให้ใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ดังนี้

(๑) นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของกรมการปกครอง ตามเอกสารแนบท้ายประกาศนี้ (นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) หมายเลข ๑)

(๒) นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสำนักบริหารการทะเบียน ตามเอกสารแนบท้ายประกาศนี้ (นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) หมายเลข ๒) ประกาศนี้

ข้อ ๓ ให้ใช้นโยบายคุกกี้ (Cookies Policy) ของกรมการปกครอง ตามเอกสารแนบท้าย

ข้อ ๔ ให้ใช้คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ดังนี้

(๑) คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ของกรมการปกครอง ตามเอกสารแนบท้ายประกาศนี้ (คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) หมายเลข ๑)

(๒) คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ของสำนักบริหารการทะเบียน ตามเอกสารแนบท้ายประกาศนี้ (คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) หมายเลข ๒)

/ข้อ ๕ เพื่อให้การ ...

ข้อ ๕ เพื่อให้การดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลของกรมการปกครอง เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงให้ถือปฏิบัติตามแนวทางปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของกรมการปกครอง พ.ศ. ๒๕๖๗ ตามเอกสารแนบท้ายประกาศนี้

ข้อ ๖ ในการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ระหว่างกรมการปกครองกับหน่วยงานหรือบุคคลภายนอกให้ใช้แบบฟอร์มข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ตามเอกสารแนบท้ายประกาศนี้

ข้อ ๗ กรณีที่ต้องมีการดำเนินการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากผู้รับบริการ ให้ใช้แบบฟอร์มแสดงความยินยอม (Consent Form) กรมการปกครอง ตามเอกสารแนบท้ายประกาศนี้

ข้อ ๘ ให้ใช้ประกาศความเป็นส่วนตัวเกี่ยวกับการใช้กล้องวงจรปิด ตามเอกสารแนบท้ายประกาศนี้

ข้อ ๙ เพื่อให้การดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลของกรมการปกครอง เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงให้ถือปฏิบัติตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กรมการปกครอง ตามเอกสารแนบท้ายประกาศนี้

ข้อ ๑๐ ในการจัดทำข้อตกลงการแลกเปลี่ยนข้อมูลข่าวสาร (Data sharing Agreement) ระหว่างกรมการปกครองกับหน่วยงานหรือบุคคลภายนอกให้ใช้แบบฟอร์มจัดทำข้อตกลงการแลกเปลี่ยนข้อมูลข่าวสาร (Data sharing Agreement) ตามเอกสารแนบท้ายประกาศนี้

ข้อ ๑๑ ในการจัดทำรายการประเมินคู่ค้า/คู่สัญญาประกอบการจัดซื้อจัดจ้างให้ใช้แบบฟอร์มรายการประเมินคู่ค้าคู่สัญญา (Vendor/Contractor Assessment) ระหว่างกรมการปกครองกับผู้ประมวลผลข้อมูลส่วนบุคคล ตามเอกสารแนบท้ายประกาศนี้

ข้อ ๑๒ ในการจัดทำข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller Agreement) ระหว่างกรมการปกครองกับหน่วยงานหรือบุคคลภายนอกให้ใช้แบบฟอร์มจัดทำข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller Agreement) ตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๓๐ มิถุนายน พ.ศ. ๒๕๖๘

(นายไชยวัฒน์ จุนถิระพงศ์)
อธิบดีกรมการปกครอง

นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
กรมการปกครอง

.....

๑. บทนำ

กรมการปกครอง ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่นอันเกี่ยวกับท่าน (รวมเรียกว่า "**ข้อมูล**") เพื่อให้ท่านสามารถเชื่อมั่นได้ว่า กรมการปกครอง มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ("**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**") รวมถึงกฎหมายอื่นที่เกี่ยวข้อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล ("**นโยบาย**") นี้จึงได้ถูกจัดทำขึ้นเพื่อชี้แจงแก่ท่านถึงรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า "**ประมวลผล**") ข้อมูลส่วนบุคคลซึ่งดำเนินการโดย กรมการปกครอง รวมถึงเจ้าหน้าที่และบุคคลที่เกี่ยวข้องผู้ดำเนินการแทนหรือในนามของ กรมการปกครอง โดยมีเนื้อหาสาระดังต่อไปนี้

๒. ขอบเขตการบังคับใช้นโยบาย

กรมการปกครอง จะเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมายที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลเท่านั้น เพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตามภารกิจในอำนาจหน้าที่ของกรมการปกครอง นโยบายนี้ใช้บังคับกับข้อมูลส่วนบุคคล ของบุคคลซึ่งมีความสัมพันธ์กับกรมการปกครอง ในปัจจุบันและที่อาจมีในอนาคต ซึ่งถูกประมวลผลข้อมูลส่วนบุคคลโดยกรมการปกครอง รวมถึงคู่สัญญาหรือบุคคลภายนอกที่ประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของ กรมการปกครอง ("**ผู้ประมวลผลข้อมูลส่วนบุคคล**") ภายใต้บริการต่าง ๆ เช่น เว็บไซต์ ระบบ แอปพลิเคชัน เอกสาร หรือ บริการในรูปแบบอื่นที่ควบคุมดูแลโดย กรมการปกครอง (รวมเรียกว่า "**บริการ**") นอกจากนโยบายฉบับนี้แล้ว กรมการปกครอง อาจกำหนดให้มีคำประกาศเกี่ยวกับความเป็นส่วนตัว ("**ประกาศ**") สำหรับบริการของกรมการปกครอง เพื่อชี้แจงให้เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้ใช้บริการได้ทราบถึงข้อมูลส่วนบุคคลที่ถูกประมวลผล วัตถุประสงค์และเหตุผลอันชอบด้วยกฎหมายในการประมวลผล ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล รวมถึงสิทธิในข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลพึงมีในบริการนั้นเป็นการเฉพาะเจาะจง

สำหรับข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ใช้บังคับกรมการปกครอง จะเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปตามวัตถุประสงค์เดิม โดยการเปิดเผย และการดำเนินการอื่นที่ไม่ใช่การเก็บรวบรวม และการใช้ข้อมูลส่วนบุคคลข้างต้น กรมการปกครอง จะปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

/๓. คำนิยาม

๓. คำนิยาม

๓.๑ ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

๓.๒ การประมวลผลข้อมูลส่วนบุคคล หมายถึง การดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล ซึ่งกระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๓ ประกาศเกี่ยวกับความเป็นส่วนตัว (privacy notice) หมายถึง ประกาศสำหรับแสดงรายละเอียดของการเก็บรวบรวม ข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียด ดังกล่าวก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

๓.๔ บันทึกการให้ความยินยอม (consent receipt หรือ consent record) หมายถึง บันทึกที่มีสาระสำคัญของการ ให้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลส่งให้เจ้าของข้อมูลส่วนบุคคลใช้ ตรวจสอบได้

๓.๕ ผู้ควบคุมข้อมูลส่วนบุคคล (data controller) หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๓.๖ ผู้ประมวลผลข้อมูลส่วนบุคคล (data processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคล หรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

๓.๗ ข้อมูลส่วนบุคคลอ่อนไหว หมายถึง ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๓.๘ เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่กรมการปกครอง เก็บรวบรวม ใช้ หรือเปิดเผย

๓.๙ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่ให้คำแนะนำและตรวจสอบการดำเนินงาน ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๓.๑๐ ผู้ปฏิบัติงาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง เจ้าหน้าที่ของรัฐ และผู้ที่ได้มอบหมายให้ปฏิบัติหน้าที่ ของกรมการปกครอง

๓.๑๑ ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ

๓.๑๒ สิทธิการเข้าถึง หมายถึง กระบวนการตรวจสอบตัวตนโดยใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) หรือระบบการกำหนดสิทธิ์ของระบบสารสนเทศ เพื่อตรวจสอบสิทธิผู้ใช้งานในการเข้าใช้งาน

/๔. แหล่งที่มา...

๔. แหล่งที่มาของข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวม

กรมการปกครอง เก็บรวบรวมหรือได้มาซึ่งข้อมูลส่วนบุคคลประเภทต่าง ๆ จากแหล่งข้อมูลดังต่อไปนี้

๔.๑ ข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรงในช่องทางให้บริการต่าง ๆ เช่น ขั้นตอนการสมัคร ลงทะเบียน สมัครงาน ลงนามในสัญญา เอกสาร ทำแบบสำรวจ การยื่นคำขอ การพิจารณาอนุญาต หรือ บริการ หรือช่องทางให้บริการอื่นที่ควบคุมดูแลโดย กรมการปกครอง หรือเมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อสื่อสารกับ กรมการปกครอง ณ ที่ทำการหรือผ่านช่องทางติดต่ออื่นที่ควบคุมดูแลโดยกรมการปกครอง เป็นต้น

๔.๒ ข้อมูลที่ กรมการปกครอง เก็บรวบรวมจากการที่เจ้าของข้อมูลส่วนบุคคลเข้าใช้งานเว็บไซต์ หรือบริการอื่นๆ ตามสัญญาหรือตามพันธกิจในความรับผิดชอบของกรมการปกครอง เช่น การติดตามพฤติกรรมการใช้งานเว็บไซต์ ผลิตภัณฑ์หรือบริการของ กรมการปกครอง ด้วยการใช้คุกกี้ (Cookies) หรือจากซอฟต์แวร์บนอุปกรณ์ของเจ้าของข้อมูลส่วนบุคคล เป็นต้น

๔.๓ ข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวมจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล โดยที่แหล่งข้อมูลดังกล่าวมีอำนาจหน้าที่ มีเหตุผลที่ชอบด้วยกฎหมายหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้วในการเปิดเผยข้อมูลแก่กรมการปกครอง เช่น การเชื่อมโยงบริการดิจิทัลของหน่วยงานของรัฐในการให้บริการเพื่อประโยชน์สาธารณะแบบเบ็ดเสร็จแก่เจ้าของข้อมูลส่วนบุคคลเอง การรับข้อมูลส่วนบุคคลจากหน่วยงานของรัฐแห่งอื่นในฐานะที่ กรมการปกครอง มีหน้าที่ตามพันธกิจในการดำเนินการจัดให้มีศูนย์แลกเปลี่ยนข้อมูลกลางเพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล รวมถึงจากความจำเป็นเพื่อให้บริการตามสัญญาที่อาจมีการแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานคู่สัญญาได้

นอกจากนี้ ยังหมายความรวมถึงกรณีที่ท่านเป็นผู้ให้ข้อมูลส่วนบุคคลของบุคคลภายนอกแก่ กรมการปกครอง ดังนี้ ท่านมีหน้าที่รับผิดชอบในการแจ้งรายละเอียดตามนโยบายนี้หรือประกาศของผลิตภัณฑ์หรือบริการ ตามแต่กรณี ให้บุคคลดังกล่าวทราบ ตลอดจนขอความยินยอมจากบุคคลนั้นหากเป็นกรณีที่ต้องได้รับความยินยอมในการเปิดเผยข้อมูลแก่ กรมการปกครอง

๕. ประเภทของข้อมูลส่วนบุคคลที่กรมการปกครองเก็บรวบรวม

กรมการปกครองอาจเก็บรวบรวมหรือได้มาซึ่งข้อมูลดังต่อไปนี้ ซึ่งอาจรวมถึงข้อมูลส่วนบุคคลของท่าน ทั้งนี้ ขึ้นอยู่กับงานบริการที่ท่านขอรับบริการหรือบริบทความสัมพันธ์ที่ท่านมีกับกรมการปกครอง รวมถึงข้อพิจารณาอื่นที่มีผลกับการเก็บรวบรวมข้อมูลส่วนบุคคล โดยประเภทของข้อมูลที่ระบุไว้ดังต่อไปนี้เป็นเพียงกรอบการเก็บรวบรวมข้อมูลส่วนบุคคลของกรมการปกครองเป็นการทั่วไป ทั้งนี้ เฉพาะข้อมูลที่เกี่ยวข้องกับบริการที่ท่านใช้งานหรือมีความสัมพันธ์ด้วยเท่านั้นที่จะมีผลบังคับใช้

๕.๑ ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลระบุชื่อเรียกของท่านหรือข้อมูลจากเอกสารราชการที่ระบุข้อมูลเฉพาะตัวของท่าน เช่น คำนำหน้าชื่อ ชื่อ นามสกุล ชื่อกลาง ชื่อเล่น ลายมือชื่อ เลขที่บัตรประจำตัวประชาชน สัญชาติ เลขที่ใบขับขี่ เลขที่หนังสือเดินทาง ข้อมูลทะเบียนบ้าน หมายเลขใบประกอบการ หมายเลขใบอนุญาตการประกอบวิชาชีพ (สำหรับแต่ละอาชีพ) หมายเลขประจำตัวผู้ประกันตน หมายเลขประกันสังคม เป็นต้น

/๕.๒ ข้อมูลส่วนบุคคล...

๕.๒ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ได้แก่ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนของท่าน เช่น เชื้อชาติ ข้อมูลศาสนา ข้อมูลความพิการ ข้อมูลความเห็นทางการเมือง ประวัติอาชญากรรม ข้อมูลชีวภาพ (ข้อมูลภาพจำลองใบหน้า) ข้อมูลพันธุกรรม ข้อมูลเกี่ยวกับสุขภาพ เป็นต้น ทั้งนี้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลปฏิเสธไม่ให้ข้อมูลที่มีความจำเป็นในการให้บริการของ กรมการปกครอง อาจเป็นผลให้ กรมการปกครอง ไม่สามารถให้บริการนั้นแก่เจ้าของข้อมูลส่วนบุคคลดังกล่าวได้ทั้งหมดหรือบางส่วน

๖. คุกกี้

กรมการปกครอง เก็บรวบรวมและใช้คุกกี้รวมถึงเทคโนโลยีอื่นในลักษณะเดียวกันในเว็บไซต์ที่อยู่ภายใต้ความดูแลของกรมการปกครอง หรือบนอุปกรณ์ของท่านตามแต่บริการที่ท่านใช้งาน ทั้งนี้ เพื่อการดำเนินการด้านความปลอดภัยในการให้บริการของ กรมการปกครอง และเพื่อให้ท่านซึ่งเป็นผู้ใช้งานได้รับความสะดวกและประสบการณ์ที่ดีในการใช้งานบริการของ กรมการปกครอง และข้อมูลเหล่านี้จะถูกนำไปเพื่อปรับปรุงเว็บไซต์ของ กรมการปกครอง ให้ตรงกับความต้องการของท่านมากยิ่งขึ้น โดยท่านสามารถตั้งค่าหรือลบการใช้งานคุกกี้ได้ด้วยตนเองจากการตั้งค่าในเว็บเบราว์เซอร์ (Web Browser) ของท่าน

๗. ข้อมูลส่วนบุคคลของผู้เยาว์ คนไร้ความสามารถและคนเสมือนไร้ความสามารถ

กรณีที่ กรมการปกครอง ทราบว่าข้อมูลส่วนบุคคลที่จำเป็นต้องได้รับความยินยอมในการเก็บรวบรวม เป็นของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้เยาว์ คนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ ต่อเมื่อได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ หรือผู้อนุบาล หรือผู้พิทักษ์ตามแต่กรณี ยกเว้นเป็นกรณีที่กรมการปกครองมีอำนาจดำเนินการได้ตามที่กฎหมายกำหนด

กรณีที่ กรมการปกครอง ไม่ทราบมาก่อนว่าเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ และมาพบในภายหลังว่า กรมการปกครอง ได้เก็บรวบรวมข้อมูลของเจ้าของข้อมูลส่วนบุคคลดังกล่าวโดยยังมิได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ หรือผู้อนุบาล หรือผู้พิทักษ์ตามแต่กรณี ดังนี้ กรมการปกครอง จะดำเนินการลบทำลายข้อมูลส่วนบุคคลนั้น เว้นแต่มีกฎหมายให้อำนาจดำเนินการในเรื่องนั้นไว้

๘. วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล

กรมการปกครอง ดำเนินการเก็บรวบรวมข้อมูลเพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตามภารกิจในอำนาจหน้าที่ของกรมการปกครอง เพื่อประโยชน์ในการให้บริการ เพื่อปรับปรุงคุณภาพการให้บริการให้มีประสิทธิภาพมากยิ่งขึ้น และเพื่อบริหารจัดการด้านทรัพยากรบุคคลของ กรมการปกครอง โดย กรมการปกครอง จะขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล

ยกเว้น แต่ในกรณีดังต่อไปนี้ กรมการปกครอง สามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องขอความยินยอม

๑. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติ โดย กรมการปกครอง จะจัดให้มีมาตรการป้องกันที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

๒. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๓. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา

/๔. เป็นการจำเป็น...

๔. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๕. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของ ผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

๖. เป็นการปฏิบัติตามกฎหมายของ กรมการปกครอง

เนื่องจากข้อมูลส่วนบุคคลที่กรมการปกครองจะดำเนินการประมวลผลเพื่อวัตถุประสงค์ที่กำหนด ในส่วนที่มีความเกี่ยวเนื่องกับการปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นเพื่อเข้าทำสัญญากับท่าน ซึ่งข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่จำเป็นต่อการบรรลุวัตถุประสงค์ดังกล่าว หากท่านไม่ให้ข้อมูลส่วนบุคคลดังกล่าวแก่กรมการปกครอง อาจมีผลกระทบทางกฎหมาย หรือกรมการปกครองอาจจะไม่สามารถปฏิบัติหน้าที่ภายใต้สัญญาที่ได้เข้าทำกับท่าน หรือไม่สามารถข้าทำสัญญากับท่านได้ (แล้วแต่กรณี) ในกรณีดังกล่าว กรมการปกครองอาจมีความจำเป็นต้องปฏิเสธการเข้าทำสัญญากับท่านหรือยกเลิกการให้บริการที่เกี่ยวข้อง ต่อท่านไม่ว่าทั้งหมดหรือบางส่วน

๙. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ในบางกรณี กรมการปกครอง อาจจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังต่างประเทศเพื่อดำเนินการตามวัตถุประสงค์ในการให้บริการแก่ท่าน เช่น เพื่อส่งข้อมูลส่วนบุคคลไปยังระบบคลาวด์ (Cloud) ที่มีแพลตฟอร์มหรือเครื่องแม่ข่าย (Server) อยู่ต่างประเทศ (เช่น ประเทศสิงคโปร์ หรือสหรัฐอเมริกา เป็นต้น) เพื่อสนับสนุนระบบเทคโนโลยีสารสนเทศที่ตั้งอยู่นอกประเทศไทย ทั้งนี้ ขึ้นอยู่กับบริการของ กรมการปกครอง ที่ท่านใช้งานหรือมีส่วนเกี่ยวข้องเป็นรายกิจกรรม อย่างไรก็ตาม ในขณะที่จัดทำนโยบายฉบับนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมิได้มีประกาศกำหนดรายการประเทศปลายทางที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ดังนั้น เมื่อ กรมการปกครอง มีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังประเทศปลายทาง กรมการปกครอง จะดำเนินการเพื่อให้ข้อมูลส่วนบุคคลที่ส่งหรือโอนไปมีมาตรการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอตามมาตรฐานสากล หรือดำเนินการตามเงื่อนไขเพื่อให้สามารถส่งหรือโอนข้อมูลนั้นได้ตามกฎหมาย ได้แก่

๑. เป็นการปฏิบัติตามกฎหมายที่กำหนดให้กรมการปกครองต้องส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

๒. ได้แจ้งให้ท่านทราบและได้รับความยินยอมจากท่านในกรณีที่ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ ทั้งนี้ตามประกาศรายชื่อประเทศที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๓. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาที่ท่านเป็นคู่สัญญากับ กรมการปกครอง หรือเป็นการทำตามคำขอของท่านก่อนการเข้าทำสัญญานั้น

๔. เป็นการกระทำตามสัญญาของ กรมการปกครอง กับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของท่าน

๕. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของท่านหรือของบุคคลอื่น เมื่อท่านไม่สามารถให้ความยินยอมในขณะนั้นได้

๖. เป็นการจำเป็นเพื่อดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

/๑๐. ระยะเวลา...

๑๐. ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน

กรมการปกครอง จะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ในระยะเวลาเท่าที่ข้อมูลนั้นยังมีความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเท่านั้น ตามรายละเอียดที่ได้กำหนดไว้ในนโยบายประกาศหรือตามกฎหมายที่เกี่ยวข้อง ทั้งนี้ เมื่อพ้นระยะเวลาและข้อมูลส่วนบุคคลของท่านสิ้นความจำเป็นตามวัตถุประสงค์ดังกล่าวแล้ว กรมการปกครอง จะทำการลบ ทำลายข้อมูลส่วนบุคคลของท่าน หรือทำให้ข้อมูลส่วนบุคคลของท่านไม่สามารถระบุตัวตนได้ต่อไป ตามรูปแบบและมาตรฐานการลบทำลายข้อมูลส่วนบุคคลที่คณะกรรมการหรือกฎหมายประกาศกำหนดหรือตามมาตรฐานสากลอย่างไรก็ดี ในกรณีที่มีข้อพิพาท การใช้สิทธิหรือคดีความอันเกี่ยวข้องกับข้อมูลส่วนบุคคลของท่าน กรมการปกครอง ขอสงวนสิทธิในการเก็บรักษาข้อมูลนั้นต่อไปจนกว่าข้อพิพาทนั้นจะได้มีคำสั่งหรือคำพิพากษาถึงที่สุด

๑๑. การให้บริการโดยบุคคลที่สามหรือผู้ให้บริการช่วง

กรมการปกครอง อาจมีการมอบหมายหรือจัดซื้อจัดจ้างบุคคลที่สาม (ผู้ประมวลผลข้อมูลส่วนบุคคล) ให้ทำการประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของกรมการปกครอง ซึ่งบุคคลที่สามดังกล่าวอาจเสนอบริการในลักษณะต่าง ๆ เช่น การเป็นผู้ดูแล (Hosting) รับงานบริการช่วง (Outsourcing) หรือเป็นผู้ให้บริการคลาวด์ (Cloud computing service/provider) หรือเป็นงานในลักษณะการจ้างทำของในรูปแบบอื่น การมอบหมายให้บุคคลที่สามทำการประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลนั้น กรมการปกครอง จะจัดให้มีข้อตกลงระบุสิทธิและหน้าที่ของ กรมการปกครอง ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและของบุคคลที่ กรมการปกครอง มอบหมายในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งรวมถึงกำหนดรายละเอียดประเภทข้อมูลส่วนบุคคลที่ กรมการปกครอง มอบหมายให้ประมวลผล รวมถึงวัตถุประสงค์ ขอบเขตในการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงอื่น ๆ ที่เกี่ยวข้อง ซึ่งผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามขอบเขตที่ระบุในข้อตกลงและตามคำสั่งของกรมการปกครอง เท่านั้นโดยไม่สามารถประมวลผลเพื่อวัตถุประสงค์อื่นได้ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคล มีการมอบหมายผู้ให้บริการช่วง (ผู้ประมวลผลช่วง) เพื่อทำการประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้ กรมการปกครอง จะกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเอกสารข้อตกลงระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผลช่วง ในรูปแบบและมาตรฐานที่ไม่ต่ำกว่าข้อตกลงระหว่าง กรมการปกครอง กับผู้ประมวลผลข้อมูลส่วนบุคคล

๑๒. การเปิดเผยข้อมูลส่วนบุคคล

การเปิดเผยข้อมูลส่วนบุคคล กรมการปกครอง จะดำเนินการตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล โดยกรมการปกครอง อาจเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นอย่างจำกัดให้แก่หน่วยงานหรือบุคคลภายนอก ทั้งนี้ กรมการปกครองห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้น โดยไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือ มาตรา ๒๖ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

/๑๓. การรักษาความมั่นคง...

๑๓. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กรมการปกครอง จะจัดให้มีมาตรการปกป้องข้อมูลส่วนบุคคล โดยกำหนดมาตรการการยืนยันตัวตน (Authentication) กำหนดสิทธิ (Authorization) ในการเข้าถึง การใช้ การเปิดเผย การประมวลผลข้อมูลส่วนบุคคลตามมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการปกครอง โดยการจำกัดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลให้สามารถเข้าถึงได้โดยเจ้าหน้าที่เฉพาะรายหรือบุคคลที่มีอำนาจหน้าที่หรือได้รับมอบหมายที่มีความจำเป็นต้องใช้ข้อมูลดังกล่าวตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้แล้ว หรือตามที่ระเบียบกฎหมายกำหนดเท่านั้น ซึ่งบุคคลดังกล่าวจะต้องยึดมั่นและปฏิบัติตามมาตรการปกป้องข้อมูลส่วนบุคคล ของกรมการปกครอง อย่างเคร่งครัด ตลอดจนมีหน้าที่รักษาความลับของข้อมูลส่วนบุคคลที่ตนเองรับรู้จากการปฏิบัติการตามอำนาจหน้าที่ นอกจากนี้ เมื่อ กรมการปกครอง มีการส่งโอนหรือเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สาม ไม่ว่าเพื่อการให้บริการตามพันธกิจ ตามสัญญา หรือข้อตกลงในรูปแบบอื่น กรมการปกครอง จะกำหนดมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลและการรักษาความลับที่เหมาะสมและเป็นไปตามที่กฎหมายกำหนด

๑๔. ป้องกันการสูญหายของข้อมูลส่วนบุคคล

๑๔.๑ กรมการปกครองได้เลือกใช้บริการระบบคลาวด์กลางภารรัฐ ซึ่งผู้ให้บริการระบบคลาวด์กลางภาครัฐได้มีแนวทางการสำรองข้อมูลเป็นประจำทุกวัน ๆ ละ ๑ ครั้ง โดยเก็บไว้บนระบบสำรองข้อมูลเฉพาะและในสถานที่เก็บที่เป็นห้องมั่นคงปลอดภัย

๑๔.๒ กรมการปกครอง จะจัดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๗ โดยได้ดำเนินการตามมาตรการอย่างเคร่งครัด

๑๕. การเชื่อมต่อเว็บไซต์หรือบริการภายนอก

๑๕.๑ การเชื่อมโยงยังเว็บไซต์หรือบริการอื่นเป็นเพียงการให้บริการเพื่ออำนวยความสะดวกแก่ผู้ใช้บริการเท่านั้น กรมการปกครองมิได้มีส่วนเกี่ยวข้องหรือมีอำนาจควบคุมรับรองความถูกต้องความน่าเชื่อถือตลอดจนความรับผิดชอบในเนื้อหาข้อมูลของเว็บไซต์หรือบริการนั้น ๆ และกรมการปกครองไม่รับผิดชอบต่อเนื้อหาใดๆ ที่แสดงบนเว็บไซต์หรือบริการอื่นที่เชื่อมโยงมายังเว็บไซต์หรือบริการของกรมการปกครองหรือต่อความเสียหายใด ๆ ที่เกิดขึ้นจากการเข้าเยี่ยมชมเว็บไซต์หรือบริการดังกล่าว

๑๕.๒ กรณีต้องการเชื่อมโยงมายังเว็บไซต์ของกรมการปกครอง ผู้ใช้บริการสามารถเชื่อมโยงมายังหน้าแรกของเว็บไซต์กรมการปกครองได้ โดยแจ้งความประสงค์เป็นหนังสือ แต่หากต้องการเชื่อมโยงมายังหน้าภายในของเว็บไซต์นี้จะต้องได้รับความยินยอมเป็นหนังสือจากกรมการปกครองเท่านั้น และในการให้ความยินยอมดังกล่าว กรมการปกครองขอสงวนสิทธิที่จะกำหนดเงื่อนไขใด ๆ ไว้ด้วยก็ได้ ในการที่เว็บไซต์ที่เชื่อมโยงมายังเว็บไซต์ของกรมการปกครอง กรมการปกครองจะไม่รับผิดชอบต่อเนื้อหาใด ๆ ที่แสดงบนเว็บไซต์ที่เชื่อมโยงมายังเว็บไซต์ของกรมการปกครอง หรือต่อความเสียหายใด ๆ ที่เกิดขึ้นจากการใช้เว็บไซต์นั้น

๑๖. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

กรมการปกครอง ได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อทำหน้าที่ตรวจสอบ กำกับและให้คำแนะนำในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

/๑๗. สิทธิของท่าน...

๑๗. สิทธิของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ ทั้งนี้ สิทธิดังกล่าวจะเริ่มมีผลบังคับใช้เมื่อกฎหมายในส่วนของสิทธินี้มีผลใช้บังคับ โดยรายละเอียดของสิทธิต่าง ๆ ประกอบด้วย

๑. สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล ท่านมีสิทธิขอเข้าถึง รับสำเนาและขอให้เปิดเผยที่มาของข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวมไว้โดยปราศจากความยินยอมของท่าน เว้นแต่กรณีที่ กรมการปกครอง มีสิทธิปฏิเสธคำขอของท่านด้วยเหตุตามกฎหมายหรือคำสั่งศาล หรือกรณีที่การใช้สิทธิของท่านจะมีผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

๒. สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์และเป็นปัจจุบัน หากท่านพบว่าข้อมูลส่วนบุคคลของท่านไม่ถูกต้อง ไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ท่านมีสิทธิขอให้แก้ไขเพื่อให้มีความถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิดได้

๓. สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล ท่านมีสิทธิขอให้ กรมการปกครอง ลบหรือทำลายข้อมูลส่วนบุคคลของท่าน หรือทำให้ข้อมูลส่วนบุคคลของท่านไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ต่อไป ทั้งนี้ การใช้สิทธิลบหรือทำลายข้อมูลส่วนบุคคลนี้จะต้องอยู่ภายใต้เงื่อนไขตามที่กฎหมายกำหนด

๔. สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล ท่านมีสิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลของท่าน ทั้งนี้ ในกรณีดังต่อไปนี้

ก. เมื่ออยู่ในช่วงเวลาที่ กรมการปกครอง ทำการตรวจสอบตามคำร้องขอขอเจ้าของข้อมูลส่วนบุคคลให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้องสมบูรณ์และเป็นปัจจุบัน

ข. ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้หรือเปิดเผยโดยมิชอบด้วยกฎหมาย

ค. เมื่อข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ที่ กรมการปกครอง ได้แจ้งในการเก็บรวบรวมแต่เจ้าของข้อมูลส่วนบุคคลประสงค์ให้ กรมการปกครอง เก็บรักษาข้อมูลนั้นต่อไปเพื่อประกอบการใช้สิทธิตามกฎหมาย

ง. เมื่ออยู่ในช่วงเวลาที่ กรมการปกครอง กำลังพิสูจน์ถึงเหตุอันชอบด้วยกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล หรือตรวจสอบความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะ อันเนื่องมาจากการที่เจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๕. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล ท่านมีสิทธิคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับท่าน เว้นแต่กรณีที่ กรมการปกครอง มีเหตุในการปฏิเสธคำขอโดยชอบด้วยกฎหมาย (เช่น กรมการปกครอง สามารถแสดงให้เห็นว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่านมีเหตุอันชอบด้วยกฎหมายยิ่งกว่า หรือเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องทางกฎหมาย หรือเพื่อประโยชน์สาธารณะของ กรมการปกครอง)

๖. สิทธิในการขอถอนความยินยอม ในกรณีที่ท่านได้ให้ความยินยอมแก่ กรมการปกครอง ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ไม่ว่าความยินยอมนั้นจะได้ให้ไว้ก่อนหรือหลังพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลใช้บังคับ)

/ท่านมีสิทธิ...

ท่านมีสิทธิถอนความยินยอมเมื่อใดก็ได้ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของท่านถูกเก็บรักษาโดย กรมการปกครอง เว้นแต่มีข้อจำกัดสิทธิโดยกฎหมายให้ กรมการปกครอง จำเป็นต้องเก็บรักษาข้อมูลต่อไป หรือยังคงมีสัญญาระหว่างท่านกับกรมการปกครอง ที่ให้ประโยชน์แก่ท่านอยู่

๗. สิทธิในการขอรับ ส่งหรือโอนข้อมูลส่วนบุคคล ท่านมีสิทธิในการขอรับข้อมูลส่วนบุคคลของท่านจาก กรมการปกครอง ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยวิธีการอัตโนมัติ รวมถึงอาจขอให้ กรมการปกครอง ส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น ทั้งนี้ การใช้สิทธินี้จะต้องอยู่ภายใต้เงื่อนไขตามที่กฎหมายกำหนด

๑๘. การร้องขอให้ลบหรือทำลายข้อมูลส่วนบุคคล

ท่านสามารถแจ้งให้กรมการปกครองลบหรือทำลายข้อมูลส่วนบุคคลของท่าน รวมถึงสิทธิในการขอถอนความยินยอม เมื่อใดก็ได้ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของท่านถูกเก็บรักษาโดย กรมการปกครอง เว้นแต่มีขอจำกัดสิทธิโดยกฎหมายให้กรมการปกครองจำเป็นต้องเก็บรักษาข้อมูลต่อไป

๑๙. โทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล

การไม่ปฏิบัติตามนโยบายอาจมีผลเป็นความผิดและถูกลงโทษทางวินัยตามกฎเกณฑ์ของ กรมการปกครอง (สำหรับเจ้าหน้าที่หรือผู้ปฏิบัติงานของ กรมการปกครอง) หรือตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล) ทั้งนี้ ตามแต่กรณีและความสัมพันธ์ที่ท่านมีต่อ กรมการปกครอง และอาจได้รับโทษตามที่กำหนดโดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งกฎหมายลำดับรอง กฎ ระเบียบ คำสั่งที่เกี่ยวข้อง

๒๐. การร้องเรียนต่อหน่วยงานผู้มีอำนาจกำกับดูแล

ในกรณีที่ท่านพบว่า กรมการปกครอง มิได้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านมีสิทธิร้องเรียนไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือหน่วยงานที่มีอำนาจกำกับดูแลที่ได้รับการแต่งตั้งโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือตามกฎหมาย ทั้งนี้ ก่อนการร้องเรียนดังกล่าว กรมการปกครอง ขอให้ท่านโปรดติดต่อมายัง กรมการปกครอง เพื่อให้ กรมการปกครอง มีโอกาสได้รับทราบข้อเท็จจริงและได้ชี้แจงในประเด็นต่าง ๆ รวมถึงจัดการแก้ไขข้อกังวลของท่านก่อนในโอกาสแรก

๒๑. การปรับปรุงแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล

กรมการปกครอง อาจพิจารณาปรับปรุง แก้ไขหรือเปลี่ยนแปลงนโยบายนี้ตามที่เห็นสมควร และจะทำการแจ้งให้ท่านทราบผ่านช่องทางเว็บไซต์ www.dopa.go.th โดยมีวันที่มีผลบังคับใช้ของแต่ละฉบับแก้ไขกำกับอยู่ อย่างไรก็ดี กรมการปกครอง ขอแนะนำให้ท่านโปรดตรวจสอบเพื่อรับทราบนโยบายฉบับใหม่อย่างสม่ำเสมอ ผ่านแอปพลิเคชัน หรือช่องทางเฉพาะกิจกรรมที่ กรมการปกครอง ดำเนินการ โดยเฉพาะก่อนที่ท่านจะทำการเปิดเผยข้อมูลส่วนบุคคลแก่ กรมการปกครอง

การรับบริการของ กรมการปกครอง ภายหลังการบังคับใช้นโยบายใหม่ ถือเป็นการรับทราบตามข้อตกลงในนโยบายใหม่แล้ว ทั้งนี้ โปรดหยุดการเข้าใช้งานหากท่านไม่เห็นด้วยกับรายละเอียดในนโยบายฉบับนี้และโปรดติดต่อมายัง กรมการปกครอง เพื่อชี้แจงข้อเท็จจริงต่อไป

/๒๒. การติดต่อ...

๒๒. การติดต่อสอบถามหรือใช้สิทธิ

หากท่านมีข้อสงสัย ข้อเสนอแนะหรือข้อกังวลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของ กรมการปกครอง หรือเกี่ยวกับนโยบายนี้ หรือท่านต้องการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านสามารถติดต่อสอบถามได้ที่

๑. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

รองอธิบดีกรมการปกครอง ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ
๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : dpo@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๘๒-๑๐๔๗

๒. ผู้ควบคุมข้อมูลส่วนบุคคล กรมการปกครอง

๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : webmaster@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๒๔๑-๐๑๕๑-๘

ประกาศสำนักบริหารการทะเบียน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักบริหารการทะเบียน
พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ผู้อำนวยการสำนักบริหารการทะเบียน จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักบริหารการทะเบียน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน พ.ศ. ๒๕๖๕”

ข้อ ๒ ในประกาศนี้

(๑) **หน่วยงาน** หมายความว่า สำนักบริหารการทะเบียน

(๒) **ผู้บริหาร** หมายความว่า ผู้อำนวยการสำนักบริหารการทะเบียนหรือผู้ที่ผู้อำนวยการสำนักบริหารการทะเบียนมอบหมายให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศของหน่วยงาน

(๓) **ผู้บริหารระดับสูงสุด** หมายความว่า ผู้อำนวยการสำนักบริหารการทะเบียน

(๔) **คณะกรรมการ** หมายความว่า คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๕) **คณะทำงาน** หมายความว่า คณะทำงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๖) **นโยบาย** (Policy) หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๗) **ผู้ใช้งาน** (User) หมายความว่า ข้าราชการ พนักงานราชการ เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของหน่วยงาน รวมถึงบุคคลภายนอกที่สังกัดส่วนราชการหรือหน่วยงานของรัฐ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

(๘) **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๙) **สินทรัพย์** (Asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

(๑๐) **สินทรัพย์สารสนเทศ** หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล อุปกรณ์อื่นที่เกี่ยวข้องกับสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

/(๑๐) **การเข้าถึง**...

(๑๑) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๑๒) **ความมั่นคงปลอดภัยด้านสารสนเทศ** (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๑๓) **เหตุการณ์ด้านความมั่นคงปลอดภัย** (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๔) **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๔

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕ ถึงข้อ ๑๑

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้มี ๒ ส่วน ดังนี้

(๑) ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑.๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานมีส่วนร่วมในการทำนโยบาย

(๑.๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของหน่วยงาน

(๑.๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๑.๔) ต้องทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

(๒) ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๒.๑) การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ มีนโยบายให้บริการระบบสารสนเทศแก่ผู้ดูแลระบบ ผู้ใช้งาน โดยสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย ภายใต้บทบัญญัติของกฎหมาย

(๒.๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีระบบแยกประเภทและจัดเก็บเป็นหมวดหมู่ มีระบบสำรองของสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

/(๒.๓) การตรวจสอบ...

(๒.๓) การตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศอย่างสม่ำเสมอ มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๒.๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือการใช้งาน และการจัดการฝึกอบรมหรือเผยแพร่การใช้งานระบบสารสนเทศทางเว็บไซต์ภายใน (Intranet) และเว็บไซต์ภายนอก (Internet) ของหน่วยงานแก่ผู้ดูแลระบบ และผู้ใช้งาน

ข้อ ๕ ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

(๑) ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ

(๒) กำหนดหลักเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง

(๔) มีวิธีการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศของผู้ใช้งานแต่ละประเภทที่เหมาะสมและตรวจสอบได้ เพื่อป้องกันการเข้าถึงผู้ไม่ได้รับอนุญาต โดยครอบคลุมการลงทะเบียน การจัดการสิทธิผู้ใช้งาน รหัสผ่าน การทบทวนสิทธิการใช้งาน เพื่อให้มั่นใจว่าสอดคล้องกับภาระหน้าที่และความจำเป็นในการใช้งาน

(๕) ต้องควบคุมการเข้าถึงเครือข่ายและการใช้บริการผ่านเครือข่าย รวมทั้งการเชื่อมต่อเครือข่ายทั้งจากภายในหน่วยงานและจากภายนอกหน่วยงาน เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศหรือระบบสารสนเทศโดยไม่ได้รับอนุญาต

(๖) ต้องควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการใช้งานอุปกรณ์เพื่อการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

(๗) ต้องควบคุมการเข้าถึงโปรแกรมและระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๖ ต้องบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อต้องอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อยกเลิกการอนุญาตดังกล่าว

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัยโดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

/ข้อ ๗ ต้องกำหนด...

ข้อ ๗ ต้องกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหา ดังนี้

(๑) การใช้งานรหัสผ่าน กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน ต้องกำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อไม่ใช้งาน

ข้อ ๘ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองของสารสนเทศ ให้อยู่ในสภาพพร้อมใช้งาน

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการทำงานตามภารกิจ

(๓) ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๔) ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองของสารสนเทศและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) ต้องปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรองของสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ การตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ โดยมีเนื้อหา ดังนี้

(๑) ต้องกำหนดวิธีการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ

(๒) ต้องกำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ ๑ ครั้ง

(๓) ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบในการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ

(๔) ต้องมีการรายงานผลการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๐ ต้องประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติ ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

(๑) หนังสือเวียนภายในหน่วยงาน

(๒) เว็บไซต์ของหน่วยงาน

ข้อ ๑๑ ส่วนงานภายในหน่วยงานที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานได้เอง ทั้งนี้ ต้องให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน พ.ศ. ๒๕๖๕

/**ข้อ ๑๒** กำหนดให้...

ข้อ ๑๒ กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศที่มีความสำคัญเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงาน หรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๓ กำหนดบทบาทหน้าที่ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติ ดังนี้

(๑) คณะกรรมการ มีหน้าที่กำกับดูแลการใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) คณะทำงาน มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบ มีหน้าที่ดูแล ติดตาม และตรวจสอบ การใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของสำนักบริหารการทะเบียน ตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ ๑๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๕

(นายสุชาติ ธานีรัตน์)
ผู้อำนวยการสำนักบริหารการทะเบียน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักบริหารการทะเบียน
พ.ศ. ๒๕๖๕

เอกสารหมายเลข ๑	**คำนิยาม**
เอกสารหมายเลข ๒	**นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักบริหารการทะเบียน**
เอกสารหมายเลข ๓	**แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) สำนักบริหารการทะเบียน**

คำนิยาม

๑. **หน่วยงาน** หมายความว่า สำนักบริหารการทะเบียน

๒. **หน่วยงานภายใน** หมายความว่า สำนักงานผู้เชี่ยวชาญ ส่วน กลุ่มงานบริหารทั่วไป ศูนย์บริหารการทะเบียนภาค ศูนย์บริหารการทะเบียนภาค สาขาจังหวัด หรือหน่วยงานที่เรียกชื่อเป็นอย่างอื่นในสังกัดสำนักบริหารการทะเบียน

๓. **หน่วยงานภายนอก** หมายความว่า หน่วยงานราชการ รัฐวิสาหกิจ หรือองค์กรที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๔. **ผู้ใช้งาน (User)** หมายความว่า ข้าราชการ พนักงานราชการ เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของหน่วยงาน รวมถึงบุคคลภายนอกที่สังกัดส่วนราชการหรือหน่วยงานของรัฐ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

๕. **ชื่อผู้ใช้ (Username)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่ได้กำหนดสิทธิการใช้งานไว้

๖. **รหัสผ่าน (Password)** หมายความว่า กลุ่มตัวอักษรหรือตัวเลขหรืออักขระ รวมถึงรหัสลับ (PINCODE) ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

๗. **บัญชีผู้ใช้ (Account)** หมายความว่า รายชื่อผู้ใช้และรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๘. **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๙. **อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่** หมายความว่า อุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์สื่อสารที่สามารถนำไปติดตั้งนอกสถานที่ได้ อุปกรณ์สื่อสารแบบพกพา เช่น สมาร์ทโฟน แท็บเล็ต รวมถึงอุปกรณ์อิเล็กทรอนิกส์ที่ทำหน้าที่ได้เหมือนคอมพิวเตอร์ และอุปกรณ์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์โดยอาจใช้ทำหน้าที่เป็นอุปกรณ์สื่อสาร หรือใช้บันทึกข้อมูล เช่น เครื่องพิมพ์ สแกนเนอร์ หน่วยความจำภายนอก โทรศัพท์ กล้องดิจิทัล โทรทัศน์อัจฉริยะ และอุปกรณ์เครือข่ายต่าง ๆ เป็นต้น

๑๐. **ข้อมูล (Data)** หมายความว่า ข้อเท็จจริงที่เป็นตัวเลข ข้อความ ภาพ เสียง วิดีโอ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๑. **สารสนเทศ (Information)** หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๒. **ระบบสารสนเทศ (Information System)** หมายความว่า ระบบที่ประกอบด้วยส่วนต่างๆ ได้แก่ ระบบคอมพิวเตอร์ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้งานระบบ พนักงานที่เกี่ยวข้อง และผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูล เพื่อสร้างสารสนเทศและส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม

๑๓. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายความว่า เครื่องคอมพิวเตอร์ระบบงาน เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายและ/หรือ ระบบหรืออุปกรณ์สนับสนุนการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

๑๔. **การเข้าถึง (Access)** หมายความว่า การอนุญาต หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงระบบสารสนเทศและระบบเครือข่าย

๑๕. **การควบคุมการใช้งาน (Access Control)** หมายความว่า การกำหนดสิทธิในการเข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

๑๖. **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ โดยทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้งาน รหัสผ่าน หรือระบบการพิสูจน์ยืนยันตัวตนอื่นใดตามที่หน่วยงานกำหนด

๑๗. **ลงบันทึกการเข้า (Login)** หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์หรือระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้งาน และรหัสผ่านให้ถูกต้อง

๑๘. **ลงบันทึกการออก (Logout)** หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่าย

๑๙. **การเข้ารหัส (Encryption)** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๐. **ผู้ดูแลระบบ (System Administrator)** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บริหารให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๒๑. **สื่อบันทึกข้อมูล** หมายความว่า สื่อทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, Flash Drive, Handy Drive, Thumb Drive, Hard Drive, Portable Hard Drive, โทรศัพท์มือถือ กล้องถ่ายรูปดิจิตอล กล้องวิดีโอ หรือ เครื่องบันทึกเสียง เป็นต้น

๒๒. **จดหมายอิเล็กทรอนิกส์ (Electronic Mail: E-Mail)** หมายความว่า ระบบรับส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยีสารสนเทศ ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพนิ่ง ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

๒๓. **อุปกรณ์จัดเส้นทาง (Router)** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๒๔. **อุปกรณ์กระจายสัญญาณ (Access Point)** หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๒๕. **หมายเลขไอพีแอดเดรส (IP Address)** หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

๒๖. **อัพเดท (Update)** หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของระบบสารสนเทศให้ทันสมัยอยู่เสมอ

๒๗. **ช่องโหว่ (Vulnerability)** หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒๘. **VPN (Virtual Private Network)** หมายความว่า เครือข่ายส่วนตัวเสมือน โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๒๙. **SSID (Service Set Identifier)** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๓๐. **WEP (Wire Equivalent Privacy)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

๓๑. **WPA (Wi-Fi Protected Access)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๓๒. **MAC Address (Media Access Control Address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เน็ตการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๓๓. **ไฟร์วอลล์ (Firewall)** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๓๔. **เครือข่าย (Network)** หมายความว่า โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกองค์กรสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในองค์กร และโครงข่ายบนอินเทอร์เน็ตซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ขององค์กรหนึ่งได้

๓๕. **อินเทอร์เน็ต (Internet)** หมายความว่า เครือข่ายของคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกเข้าด้วยกัน โดยอาศัยเครือข่ายโทรคมนาคมเป็นตัวเชื่อมโยง

๓๖. **อินทราเน็ต (Intranet)** หมายความว่า ระบบเครือข่ายภายในองค์กร เป็นบริการและการเชื่อมต่อคอมพิวเตอร์เหมือนกันอินเทอร์เน็ต แต่จะเปิดให้ใช้เฉพาะสมาชิกในองค์กรเท่านั้น

๓๗. **แผนผังระบบเครือข่าย (Network Diagram)** หมายความว่า แผนผังหรือแผนภาพที่แสดงรูปแบบการจัดวางอุปกรณ์เครือข่ายในระบบเครือข่ายที่แสดงการเชื่อมโยง เพื่อให้เห็นเส้นทางการไหลเวียนของข้อมูลในเครือข่าย

๓๘. **ข้อมูลจราจรทางคอมพิวเตอร์ (Log)** หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๓๙. **เครือข่ายสังคมออนไลน์ (Social Network)** หมายความว่า เว็บไซต์หรือแอพพลิเคชันที่ผู้ใช้งานสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่าง ๆ

๔๐. **ระบบสำรอง (Disaster Recovery Site: DR Site)** หมายความว่า ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็น ที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

๔๑. **การสำรองข้อมูล (Backup)** หมายความว่า การคัดลอกแฟ้มข้อมูลเพื่อทำสำเนา เพื่อหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย โดยสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้ทันที

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักบริหารการทะเบียน

พ.ศ. ๒๕๖๕

สารบัญ

หน้า

ความเป็นมา

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

๒. การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๘. การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless LAN Access Control)

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๑๐. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

๑๑. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๔. การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

๑๕. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)

๑๖. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log Management)

ส่วนที่ ๒ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

๑. การคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒. การดำเนินการตรวจสอบและประเมินความเสี่ยง

๓. การบริหารความต่อเนื่องของระบบสารสนเทศ

๔. การแจ้งเหตุด้านความมั่นคงปลอดภัย

ส่วนที่ ๔ นโยบายสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน

ความเป็นมา

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือหน่วยงานที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมายก่อน จึงมีผลใช้บังคับได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๓ กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ และกำหนดให้หน่วยงานภาครัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

สำนักบริหารการทะเบียน จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์ การปฏิบัติงานและบริหารราชการได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยเชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง

๒. วัตถุประสงค์

เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด สำนักบริหารการทะเบียน ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังนี้

๒.๑ เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้บุคลากรและบุคคลที่ปฏิบัติงานให้กับสำนักบริหารการทะเบียน ในการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

๒.๓ เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ รักษาความถูกต้องสมบูรณ์ความพร้อมใช้อยู่เสมอของระบบสารสนเทศ และมีแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๔ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

๒.๕ เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ สร้างความเข้าใจและให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน มีรายละเอียดดังนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของสำนักบริหารการทะเบียน

๓.๒ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๓ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๓.๔ เผยแพร่ความรู้ความเข้าใจ เพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับในส่วนของสำนักบริหารการทะเบียน หน่วยงานภายในและหน่วยงานภายนอกที่เกี่ยวข้อง

๔. องค์ประกอบนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

๒. การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๘. การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless LAN Access Control)

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๑๐. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

๑๑. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๔. การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

๑๕. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)

๑๖. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log Management)

ส่วนที่ ๒ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

๑. การคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒. การดำเนินการตรวจสอบและประเมินความเสี่ยง

๓. การบริหารความต่อเนื่องของระบบสารสนเทศ

๔. การแจ้งเหตุด้านความมั่นคงปลอดภัย

ส่วนที่ ๔ นโยบายสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน

ส่วนที่ ๑

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการบัญชีผู้ใช้สารสนเทศของหน่วยงานและถือปฏิบัติโดยเคร่งครัด รวมทั้งสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ใช้งาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

- อ่านได้อย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไขข้อมูล
- อนุมัติการใช้ข้อมูล
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามแนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักหรือผู้อำนวยการส่วนที่ได้รับมอบหมาย

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล แบ่งออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรองการปฏิบัติราชการ ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงินและบัญชี ข้อมูลสถิติการทะเบียน เป็นต้น
- ข้อมูลสารสนเทศด้านการบริการ เช่น ข้อกฎหมายน่ารู้ กฎหมายและกฎระเบียบข้อมูลกฎหมายทางการทะเบียน เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล แบ่งออกเป็น

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล แบ่งออกเป็น

- ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง แบ่งออกเป็น

- เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ
- เข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับอนุมัติสิทธิจากเจ้าของระบบงานแล้วเท่านั้น
- เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง
- เข้าถึงได้ทุกกลุ่มผู้ใช้งานที่กำหนดไว้แล้ว

(๕) การกำหนดเวลาที่เข้าถึงได้ แบ่งออกเป็น

- ในเวลาราชการ ได้แก่ จันทร์ – ศุกร์ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.
- นอกเวลาราชการที่ได้รับอนุญาต ได้แก่ จันทร์ – ศุกร์ เวลา ๑๖.๓๐ – ๒๐.๓๐ น.
- วันหยุดราชการและวันหยุดนักขัตฤกษ์ที่ได้รับอนุญาต ได้แก่ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.
- เวลาอื่นตามที่ระบุไว้ให้เข้าถึงได้

(๖) การกำหนดช่องทางที่สามารถเข้าถึงได้ แบ่งออกเป็น

- อินทราเน็ต (Intranet)
- อินเทอร์เน็ต (Internet)
- จดหมายอิเล็กทรอนิกส์ (E-Mail)

๒. การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

เพื่อควบคุมการเข้าถึงสารสนเทศตามภารกิจให้ปฏิบัติ ดังนี้

๒.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๒.๒ มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้ ต้องมีการบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ให้ดำเนินการดังนี้

๓.๑ มีการประชาสัมพันธ์เผยแพร่ความรู้เกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)

๓.๒ มีการฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งานเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Training) เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึง การณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓.๓ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ดังนี้

(๑) ผู้ดูแลระบบจัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม โดยระบุข้อมูลพื้นฐาน เช่น ชื่อ-นามสกุล ตำแหน่ง หน่วยงาน

(๒) ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มขอใช้ระบบงานสารสนเทศแล้ว ต้องให้ผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่าให้ความเห็นชอบ

(๓) ผู้ดูแลระบบต้องตรวจสอบและกำหนดสิทธิที่เหมาะสมในการเข้าถึงตามหน้าที่ความรับผิดชอบ

(๔) ผู้ดูแลระบบจัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งผู้ขอใช้งานต้องลงนามรับทราบด้วย

(๕) ผู้ดูแลระบบกำหนดชื่อผู้ใช้ (Username) จากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๖) ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้งานระบบสารสนเทศและให้เก็บย้อนหลังอย่างน้อย ๑ ปี

(๗) ผู้ดูแลระบบกำหนดให้มีการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศเมื่อได้รับแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

๓.๔ มีการกำหนดการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๒) ผู้ดูแลระบบต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(๓) ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศให้เหมาะสมตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

(๔) ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานเป็นลายลักษณ์อักษรและให้เก็บย้อนหลังอย่างน้อย ๑ ปี

(๕) ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ดูแลระบบ หรือผู้ใช้งานอื่นใดที่มีสิทธิในระดับสูง ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกว่าวหรือพ้นจากตำแหน่ง และกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงในระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

๓.๕ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราวที่ยากต่อการเดา และต้องมีความแตกต่างกัน

(๓) ผู้ดูแลระบบต้องกำหนดวันหมดอายุอย่างน้อยทุก ๒ เดือน สำหรับรหัสผ่านของผู้ใช้งานทุกคน

(๔) ผู้ดูแลระบบต้องส่งมอบบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๕) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๖) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนาม เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเข้าถึงระบบสารสนเทศ

(๗) ผู้ดูแลระบบต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๓.๖ ข้อกำหนดการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศหรือการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๔.๑ มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีความมั่นคงปลอดภัย ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๕) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๕ นาที โดยต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๕) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๖) ผู้ใช้งานต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๔.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ดังนี้

(๑) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

- โปรแกรมที่ได้ถูกติดตั้งลงเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย โดยห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้บุคคลอื่นใช้งานโดยผิดกฎหมาย
- ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน
- ปิดเครื่องคอมพิวเตอร์ (Log Off) ทุกครั้งหลังเลิกงานหรือไม่ใช้งาน
- ออกจากระบบ (Log Out) ออกจากระบบสารสนเทศหรือระบบคอมพิวเตอร์ทันที เมื่อใช้งานเสร็จหรือจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงานไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน คู่สัญญาเช่าหรือผู้รับจ้างในการบำรุงรักษาหรือซ่อมแซมเครื่องคอมพิวเตอร์และอุปกรณ์ โดยมีข้อตกลงเป็นหนังสือกับหน่วยงานเท่านั้น
- ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive
- การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานอีกครั้ง
- ไม่วางของทับบนหน้าจอหรือแป้นพิมพ์
- ให้ติดตั้งหรือจัดเก็บอุปกรณ์คอมพิวเตอร์บนชั้นวางคอมพิวเตอร์ ตู้ติดตั้งอุปกรณ์เครือข่าย กล่องใส่แผ่น CD/DVD หรือสิ่งอื่นใดที่เป็นอุปกรณ์เฉพาะสำหรับติดตั้งหรือเก็บรักษาที่มั่นคงแข็งแรง

- ตรวจสอบ สายไฟ สายเมาส์ สายแป้นพิมพ์ หรือสายสัญญาณของอุปกรณ์คอมพิวเตอร์อื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์คอมพิวเตอร์ได้รับความเสียหาย

- ทำความสะอาดอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละอองที่จะทำให้เครื่องคอมพิวเตอร์เกิดการขัดข้องหรือเสียหาย

- ควรใช้วิธีการทางเทคนิคในการเข้ารหัสข้อมูล เพื่อเข้ารหัสข้อมูลสำคัญในเครื่องคอมพิวเตอร์

- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันเครื่องคอมพิวเตอร์มิให้ถูกขโมยหรือสูญหาย ไม่วางเครื่องไว้ในที่สาธารณะหรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

- ห้ามนำเครื่องคอมพิวเตอร์ที่ไม่ใช่ของหน่วยงานมาใช้งานกับเครือข่ายของหน่วยงาน เว้นแต่ได้รับการตรวจสอบจากผู้ดูแลระบบที่เกี่ยวข้องก่อนการใช้งาน

- ห้ามเปลี่ยนแปลงหมายเลขไอพีแอดเดรส (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงาน

- ต้องทำการสำรองข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

- ผู้ใช้งานมีหน้าที่รับผิดชอบในการการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกแบบภายนอก หรืออื่น ๆ ที่เหมาะสม

- ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๒) ผู้ใช้งานต้องป้องกันและแก้ไขไวรัสคอมพิวเตอร์หรือซอฟต์แวร์ไม่ประสงค์ดี (Antivirus)

- ตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานมีซอฟต์แวร์ป้องกันไวรัส ติดตั้งอยู่และต้องเปิดใช้งานตลอดเวลาที่ใช้งาน

- ปรับปรุงฐานข้อมูลป้องกันไวรัส (Updating Virus Signature Database) ให้เป็นปัจจุบัน

- ห้ามทำการใดเพื่อขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

- ควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสาร ที่น่าจะเป็นไปได้เท่านั้น

- ทำการตรวจหาไวรัสทุกครั้งหลังจากรับไฟล์จากแหล่งใด ๆ ก็ตาม มาใช้ที่เครื่องคอมพิวเตอร์

- ใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง โดยไม่เปิดเว็บไซต์เกมส์ออนไลน์ เว็บไซต์ลามกอนาจาร เว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมหรือไฟล์ต่าง ๆ หรือพฤติการณ์อื่นใดที่มีความเสี่ยงต่อการติดไวรัส

- ห้ามติดตั้งโปรแกรม Java, ActiveX หรือโปรแกรมประเภท Active Code อื่นใดจากแหล่งที่ไม่น่าเชื่อถือ

- ไม่เปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่ไม่รู้จักหรือชื่อเรื่องที่ไม่เคยติดต่อกันมาก่อน หรือสงสัยว่าไม่ปลอดภัย

- ไม่เปิดการแบ่งปันข้อมูลแบบ Share Drive หรือหากมีความจำเป็นให้เปิดการแบ่งปันข้อมูลแบบ Share Folder โดยต้องอนุญาตใช้รหัสผ่าน และอนุญาตให้อ่านอย่างเดียว

- ให้ความสำคัญกับการแจ้งเตือนจากซอฟต์แวร์ป้องกันไวรัส หากมีข้อสงสัยหรือพบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติหรือซอฟต์แวร์ป้องกันไวรัสมีการแจ้งเตือนมากผิดปกติ ให้แจ้งเจ้าหน้าที่ของส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน คู่สัญญาเช่าหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

(๓) การยับยั้งหรือจำกัดความเสียหาย เมื่อเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์หรือซอฟต์แวร์ไม่ประสงค์ดี ให้ผู้ที่มีหน้าที่ป้องกันและแก้ไขไวรัสปฏิบัติ ดังนี้

- ให้แยกเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติออกจากเครือข่ายของหน่วยงาน โดยการถอดสาย LAN หรือปิดอุปกรณ์ไร้สาย (Wireless LAN)

- สำรองข้อมูลสำคัญในเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติ

- ให้ทำการตรวจหาไวรัสคอมพิวเตอร์ที่อาจจะฝังตัวอยู่กับข้อมูลที่สำรองไว้ก่อนนำข้อมูลไปใช้กับเครื่องคอมพิวเตอร์อื่น

- ในกรณีที่พบไฟล์ที่ติดไวรัสคอมพิวเตอร์หรือไฟล์ที่เป็นซอฟต์แวร์ไม่ประสงค์ดี และซอฟต์แวร์ป้องกันไวรัสสามารถแก้ไขไวรัสคอมพิวเตอร์ที่ติดได้ ให้ดำเนินการแก้ไขโดยซอฟต์แวร์ป้องกันไวรัส หากซอฟต์แวร์ป้องกันไวรัสไม่สามารถแก้ไขไวรัสคอมพิวเตอร์ที่ติดได้ ให้ลบไฟล์ที่ติดไวรัสคอมพิวเตอร์หรือลบไฟล์ที่เป็นซอฟต์แวร์ไม่ประสงค์ดีทิ้ง

- ให้ติดตั้งโปรแกรมส่วนแก้ไข (Update Patch) ตามความเหมาะสม ปรับปรุงเวอร์ชันซอฟต์แวร์ป้องกันไวรัส และปรับปรุงฐานข้อมูลป้องกันไวรัส (Updating Virus Signature Database) ให้เป็นปัจจุบัน เพื่อเพิ่มประสิทธิภาพในการป้องกันไวรัส

(๔) การจัดทำเอกสารลับบนกระดาษหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

- มีการจัดหมวดหมู่เอกสารลับไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างเพียงพอ

- จำกัดการสำเนาเอกสารลับเท่าที่จำเป็นต้องใช้งานเท่านั้น

- ระมัดระวังการกระจาย ส่ง หรือการแจกจ่ายเอกสารลับไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับทราบ หรือใช้งานเอกสารนั้นเท่านั้น

- ใช้วิธีการตามกฎหมายที่หน่วยงานได้ถือปฏิบัติอยู่แล้วสำหรับการจัดส่งเอกสารลับทางไปรษณีย์

(๕) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

(๖) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๗) เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลายสื่อหรือข้อมูลอิเล็กทรอนิกส์ ดังนี้

- Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย

- กระดาษ หรือ แผ่น CD/DVD ใช้วิธีการหั่นด้วยเครื่องทำลายเอกสาร

- เทป ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย

- ฮาร์ดดิสก์ ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม ประเทศสหรัฐอเมริกา DOD ๕๒๒๐.๒๒-M (ซึ่งเป็นการลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับ โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ ซึ่งทำการลบข้อมูล ๓ รอบ รอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลไบต์สุ่ม)

(๘) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานการรักษาความปลอดภัยของข้อมูลที่รับส่งผ่านอินเทอร์เน็ต (Secure Sockets Layer: SSL) และเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

(๙) ผู้ใช้งานอาจนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่ม (ฉบับที่ ๒) พ.ศ. ๒๕๖๑

(๑๐) ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เพื่อส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมหรือจำหน่าย หรือเพื่อการอื่นให้มีการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

(๑๑) ป้องกันไม่ให้บุคคลภายนอกเข้าถึงหรือใช้งานกล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้ โดยไม่ได้รับอนุญาต

(๑๒) ให้นำเอกสารออกจากเครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้ทันทีที่ใช้งานเสร็จ

(๑๓) ในกรณีที่ต้องการนำสินทรัพย์สารสนเทศต่าง ๆ ออกจากพื้นที่ใช้งาน ต้องขออนุญาตจากผู้บังคับบัญชา

(๑๔) ผู้ใช้งานต้องคืนสินทรัพย์ทั้งหมดที่เกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ เมื่อพ้นการปฏิบัติหน้าที่

(๑๕) ผู้ดูแลระบบต้องระงับสิทธิ หรือถอดถอนสิทธิ หรือเรียกคืนสินทรัพย์ตามเห็นควร หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

(๑๖) การเผยแพร่ข้อมูลข่าวสารบนเว็บไซต์

- ข้อมูลที่จะนำขึ้นเว็บไซต์ ต้องไม่ก่อให้เกิดความเสียหาย ละเมิดสิทธิ หรือสร้างความรำคาญแก่ผู้อื่น หรือผิดกฎหมาย หรือขัดต่อศีลธรรมอันดีของประชาชน

- ในการนำข้อมูลขึ้นเว็บไซต์ ให้ใช้แบบฟอร์มตามที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนกำหนด ซึ่งลงนาม โดยผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่า

- ข้อมูลที่จะนำขึ้นเว็บไซต์ ต้องได้รับความเห็นชอบจากผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนหรือผู้ที่ได้รับมอบหมาย

- ให้ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน พิจารณากำหนดระยะเวลาการเผยแพร่ข้อมูลตามความเหมาะสมของข้อมูลที่ต้องเผยแพร่

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้ปฏิบัติดังนี้

๕.๑ การใช้บริการเครือข่าย กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) มีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องยืนยันตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username) ทุกครั้ง

(๒) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด (Smart Card) เป็นต้น

(๓) การใช้งานระบบสารสนเทศของหน่วยงานผ่านอินเทอร์เน็ต ต้องมีการเข้ารหัสที่เป็นมาตรฐานสากล เพื่อความมั่นคงปลอดภัยด้วยเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

(๔) การเข้าสู่ระบบสารสนเทศของหน่วยงานผ่านอินเทอร์เน็ต ต้องได้รับอนุญาตจากส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) มีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) ระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลขไอพีแอดเดรส (IP Address) และ MAC Address

(๒) ผู้ดูแลระบบจัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่เชื่อมต่อกับเครือข่าย ได้แก่ รายละเอียดเครื่องคอมพิวเตอร์ หมายเลขไอพีแอดเดรส (IP Address) MAC Address สถานที่ติดตั้งและชื่อผู้ใช้งาน

(๓) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนหรือผู้ที่ได้รับอนุญาตเท่านั้น

(๔) ต้องใช้ไฟร์วอลล์ (Firewall) กำหนดหมายเลขอุปกรณ์ ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

(๕) จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

(๖) ทำการทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันเสมอ อย่างน้อยปีละ ๑ ครับ

๕.๔ การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ดังนี้

(๑) การเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่าน (Password) และให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๒) มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่ายและเปิดเฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(๔) ทำการติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่าย โดยให้แยกเป็น

(๑) Management Zone เป็นระบบเครือข่ายที่ใช้ในการควบคุมการบริหารจัดการระบบคอมพิวเตอร์และเครือข่าย

(๒) Demilitarized Zone เป็นระบบคอมพิวเตอร์และเครือข่ายที่ให้บริการข้อมูลข่าวสารทั้งภายในหน่วยงาน (Intranet Zone) และภายนอกหน่วยงาน (Extranet Zone)

(๓) Intranet Zone เป็นระบบเครือข่ายภายในหน่วยงาน สำหรับการใช้งานข้อมูลสารสนเทศที่มีความสำคัญและเข้าถึงได้เฉพาะบุคลากรของหน่วยงานที่ได้รับอนุญาตเท่านั้น

(๔) Extranet Zone เป็นระบบเครือข่ายเชื่อมต่อกับภายนอกหน่วยงานสำหรับการรับ-ส่งข้อมูลกับหน่วยงานภายนอก

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

(๒) ระดับเครือข่ายทั้งหมดต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Intrusion Detection System: IDS/Intrusion Prevention System: IPS, ไฟร์วอลล์ (Firewall))

(๓) การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยเพื่อยืนยันตัวตน

(๔) ควบคุมการเชื่อมต่อทางเครือข่ายของผู้ใช้งานตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ดังนี้

(๑) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๒) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขไอพีแอดเดรส (IP Address)

(๓) กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน (Domain Name) เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

(๔) ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๕.๘ ข้อกำหนดการป้องกันการบุกรุก (Firewall Policy)

(๑) ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Firewall)

(๒) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

(๓) ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อกโดยไฟร์วอลล์ (Firewall)

(๔) ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการลงบันทึกการเข้า (Login) ก่อนการใช้งานทุกครั้ง

(๕) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ (Firewall) เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

(๖) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น

(๗) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

(๘) การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ต (Port) การเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ต (Port) การเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากทางส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๙) การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

(๑๐) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์ (Firewall) เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

(๑๑) ค่ารายการการป้องกันการเข้าถึง (Access Control Lists/Firewall Rules) ควรมีการปรับปรุงและทสบทวนให้สอดคล้องกับสถานภาพปัจจุบันด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

(๑๒) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

(๑๓) ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมีสิทธิที่จะระงับหรือบล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีการเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(๑๔) การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการ ตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๑๕) ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall) จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

๕.๙ ข้อกำหนดการตรวจจับการบุกรุก (IDS/IPS Policy)

(๑) กำหนดให้มีการบันทึกและการบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์และที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลสำหรับการตรวจจับการบุกรุก

(๒) ต้องมีการเฝ้าตรวจสอบหรือเรียนรู้พฤติกรรมที่อาจเป็นความเสี่ยงหรือส่งผลกระทบต่อระบบสารสนเทศและเครือข่ายที่มีอยู่ของหน่วยงาน และสามารถยับยั้งการทำงานนั้นได้ทันที โดยในกรณีที่ตรวจสอบและพบว่ามีเหตุการณ์ของการบุกรุกและโจมตี จะต้องกำหนดวิธีการปฏิบัติหรือกิจกรรม และมีผู้รับผิดชอบที่ชัดเจนในการแก้ไขหรือปรับปรุงเหตุการณ์ดังกล่าว

(๓) ระบบตรวจจับการบุกรุกระบบเครือข่าย จะต้องกำหนดให้มีการป้องกันการบุกรุกและโจมตีจากเครือข่ายภายนอก โดยการเรียนรู้พฤติกรรมการบุกรุกและโจมตีระบบ

(๔) ระบบตรวจจับการบุกรุกระบบเครือข่าย จะต้องกำหนดให้มีการปรับปรุงการกำหนดค่าด้านความมั่นคงปลอดภัยที่สามารถเรียนรู้พฤติกรรมการบุกรุกและโจมตี เพื่อให้สามารถเรียนรู้พฤติกรรมการบุกรุกและโจมตีระบบรูปแบบใหม่ ๆ ได้

(๕) ระบบตรวจจับการบุกรุกระบบเครือข่าย จะต้องกำหนดให้มีมาตรการในการป้องกันการโจมตีการทำงานของระบบตรวจจับการบุกรุกระบบเครือข่ายไม่ให้ทำงานผิดพลาด โดยต้องไม่เปิดเผยให้สามารถตรวจสอบหมายเลขไอพีแอดเดรส (IP Address) หรือเส้นทาง (Path) ในระบบเครือข่าย หรือมาตรการอื่นใดในการป้องกันการโจมตี ทั้งนี้ให้มีการตรวจสอบและทบทวนมาตรการให้มีความสอดคล้องกับสถานภาพด้านเครือข่ายในปัจจุบัน อย่างน้องปีละ ๒ ครั้ง หรือมีการเปลี่ยนแปลงสถานภาพด้านเครือข่ายที่มีผลกระทบ

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ให้ดำเนินการ ดังนี้

๖.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องมีการยืนยันตัวตนที่มีความมั่นคงปลอดภัย ดังนี้

(๑) ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๖.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านด้านเทคนิค หรือความสอดคล้องกับการปฏิบัติงาน

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น สมาร์ทการ์ด (Smart Card)

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ดังนี้

(๑) ให้มีการใช้เทคนิคการตรวจสอบการกำหนดรหัสผ่านซึ่งประกอบด้วยอักขระ ตัวเลข และอักขระพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๒) เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๖.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ที่ไม่ได้ใช้งานเป็นประจำไว้ในสื่อภายนอก

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) ให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) ห้ามติดตั้งหรือใช้งานโปรแกรมละเมิดลิขสิทธิ์หรือโปรแกรมที่มีนโยบายห้ามไม่ให้เข้าถึงหรือติดตั้งหรือใช้งาน รวมไปถึงใช้วิธีการในการหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดหรือที่มีอยู่แล้วด้วย

(๗) หน่วยงานไม่สนับสนุนการติดตั้งและ/หรือใช้งานโปรแกรมละเมิดลิขสิทธิ์ หากเกิดข้อพิพาทผู้ที่ติดตั้งและ/หรือใช้งานโปรแกรมดังกล่าวต้องเป็นผู้รับผิดชอบ

๖.๕ การกำหนดเวลาเพื่อยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน (Session Tine-Out) ดังนี้

(๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานรวมถึงปิดการใช้งานหลังจากที่ว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที

(๒) ระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง ต้องมีการตัดและหมดเวลาในการใช้งานที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ดังนี้

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชัน (Application) ที่มีความเสี่ยงหรือมีความสำคัญสูง แต่ละครั้งไม่เกิน ๓ ชั่วโมง โดยจะต้องระบุและพิสูจน์ยืนยันตัวตนเพื่อเข้าใช้งานใหม่

(๒) กำหนดให้ระบบระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง มีการจำกัดช่วงระยะเวลาการเชื่อมต่อให้ใช้งานได้เฉพาะช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น และมีการจำกัดระยะเวลาการเชื่อมต่อที่สั้นขึ้น

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ต้องมีการควบคุม ดังนี้

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงาน ตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูลต่าง ๆ

(๒) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด ต้องยกเลิกการเชื่อมต่อระบบ

(๓) ผู้ให้บริการภายนอก (Outsource) ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของหน่วยงาน

(๔) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(๕) ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ทุกครั้ง

๗.๒ การบริหารจัดการระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ดังนี้

(๑) ต้องมีการระบุความสำคัญของระบบงานซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อหน่วยงาน

(๒) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

(๓) ต้องมีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่น ๆ ที่มีความสำคัญน้อยกว่า

(๔) ต้องมีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(๕) ต้องมีการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๖) ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Mobile Computing) เพื่อควบคุมการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต จากการเสียหาย สูญหาย ถูกขโมย ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

- การป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ครอบคลุมการใช้งานอุปกรณ์สื่อสารแบบพกพาประเภทโทรศัพท์มือถือ สมาร์ทโฟน (Smartphone) เครื่องช่วยงานส่วนบุคคลแบบดิจิทัล (Personal Digital Assistants: PDA) โน้ตบุ๊ก (Notebook) แล็ปท็อป (Laptop) แท็บเล็ต (Tablet) หรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้
- ต้องกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือลับในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- ให้ใช้วิธีการทางเทคนิคในการเข้ารหัสข้อมูล เพื่อเข้ารหัสข้อมูลสำคัญในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- เมื่อพบซอฟต์แวร์ไม่ประสงค์ดีในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ปฏิบัติตามข้อปฏิบัติในการป้องกันซอฟต์แวร์ไม่ประสงค์ดีและที่เกี่ยวข้อง
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ มิให้ถูกขโมยหรือสูญหาย โดยการล็อกเครื่องขณะไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหายโดยทำการล็อกอุปกรณ์ไว้กับโต๊ะ หรือนำไปเก็บไว้ในที่ตู้ที่สามารถล็อกได้ หรือวิธีการอื่นใดที่เหมาะสม
- ให้ทำการสำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่อย่างสม่ำเสมอ
- กำหนดให้มีการป้องกันการเชื่อมต่ออุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เข้ากับเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต
- ให้ใส่ซองกันกระแทกหรือกระเป๋าสำหรับอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือนจากการตกหล่น หรือพฤติกรรมอื่นใด
- ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่
- ให้ติดตั้งหรือจัดเก็บอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่บนโต๊ะ ชั้นวางของหรือสิ่งอื่นใดที่เป็นอุปกรณ์เฉพาะสำหรับติดตั้งหรือเก็บรักษาที่มั่นคงแข็งแรง
- เพื่อความเป็นระเบียบและปลอดภัยสำหรับอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ให้จัดเก็บสายชาร์ต สายเชื่อมต่อกับระบบคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องอื่นใด ไว้ในสถานที่หรืออุปกรณ์เฉพาะที่สามารถปิดล็อกได้เพื่อป้องกันการสูญหาย
- ตรวจสอบสายสัญญาณของอุปกรณ์ สายชาร์ต สายเชื่อมต่อกับระบบคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องอื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์สื่อสารได้รับความเสียหาย
- ทำความสะอาดอุปกรณ์สื่อสารอย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละอองที่จะทำให้อุปกรณ์สื่อสารเกิดการขัดข้องเสียหาย

(๒) การควบคุมการติดตั้งระบบหรืออุปกรณ์ต่าง ๆ เพิ่มเติม

- ห้ามติดตั้งโปรแกรมเพิ่มเติมนอกเหนือจากที่หน่วยงานได้ติดตั้งไว้ให้ใช้งาน
- ห้ามติดตั้งโปรแกรมที่สามารถตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นติดตั้งเพื่อปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง
- ห้ามติดตั้งโปรแกรมหรืออุปกรณ์อื่นใดเพิ่มเติม เพื่อให้บุคคลอื่นสามารถใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ หรือเครือข่ายของหน่วยงานได้
- ห้ามนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ไม่ใช่ของหน่วยงานมาใช้กับเครือข่ายหน่วยงาน เว้นแต่ได้รับการตรวจสอบความปลอดภัยและตั้งค่าการใช้งานจากผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องก่อนการใช้งาน

(๓) ข้อกำหนดในการสำรองข้อมูลและการกู้คืน

- ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกประเภท CD, DVD, External Hard Disk หรือสื่อบันทึกอื่นใดที่เหมาะสม ในการใช้สำรองข้อมูลจากเครื่องคอมพิวเตอร์
- ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) เพื่อป้องกันการใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาตจากการปฏิบัติงานจากภายนอกหน่วยงาน ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ให้มีการเข้ารหัส (Encryption) ด้วย SSL VPN, XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่าง ๆ ภายในหน่วยงาน ทั้งนี้ให้มีความเหมาะสมกับรูปแบบการสื่อสารของความสำคัญของข้อมูล

(๒) การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับอนุญาตจากส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๓) การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษรและมีความเห็นชอบของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน โดยระบุรายละเอียดดังนี้

- เหตุผลความจำเป็นที่ต้องการให้สามารถปฏิบัติงานจากภายนอกหน่วยงาน
- รายละเอียดและ/หรือลักษณะของระบบงาน
- ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก
- รายชื่อผู้ใช้งาน หรือกลุ่มผู้ใช้งาน
- ช่วงเวลาและระยะเวลาในการใช้ปฏิบัติงานจากภายนอกหน่วยงาน

(๔) ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

(๕) ให้ผู้ที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงาน โดยห้ามมิให้สมาชิกในครอบครัวหรือบุคคลใด ๆ ที่ไม่ได้รับอนุญาต และขอสงวนสิทธิในการระงับหรือยกเลิกสิทธิหากพบว่าไม่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง

(๖) การยกเลิกสิทธิในการปฏิบัติงานจากภายนอกหน่วยงาน ให้มีหนังสือเป็นลายลักษณ์อักษรขอยกเลิกต่อผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน ทันทีที่ครบระยะเวลาหรือเมื่อหมดความจำเป็นในการใช้ปฏิบัติงานจากภายนอกหน่วยงาน

(๗) ให้มีการทบทวนปรับปรุงสิทธิการอนุญาตให้ใช้ปฏิบัติงานจากภายนอกหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

๘. การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless LAN Access Control)

๘.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการส่วนหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๘.๒ ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการดังนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๔) ต้องเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๕) ต้องกำหนดค่าใช้ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากที่สุด

(๖) ต้องเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

(๗) ต้องมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๘) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนทราบโดยทันที

๘.๓ ข้อกำหนดในการขอใช้เครือข่ายไร้สาย

(๑) เป็นบุคลากรในสังกัดสำนักบริหารการทะเบียน จะต้องได้รับการพิจารณาจากผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่า

(๒) ผู้ขอใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน ต้องทำการลงทะเบียนกับส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน และต้องได้รับอนุญาตจากผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนอย่างเป็นลายลักษณ์อักษรทุกครั้ง

(๓) ห้ามผู้ใช้งานติดตั้งอุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) โดยไม่ได้รับอนุญาต

(๔) การใช้บริการทางอินเทอร์เน็ต ให้ปฏิบัติตามข้อ ๑๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๘.๔ ขั้นตอนการขอใช้เครือข่ายไร้สาย

(๑) ผู้ขอใช้งาน ต้องมีคุณสมบัติตามข้อกำหนดในการขอใช้เครือข่ายไร้สาย

(๒) ผู้ขอใช้งาน ต้องกรอกรายละเอียดลงในแบบขอใช้งานเครือข่ายไร้สายที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนกำหนด พร้อมทั้งให้ผู้บังคับบัญชาลงนามรับรอง

(๓) เมื่อส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนได้รับหนังสือ ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนพิจารณาอนุมัติ ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายดำเนินการต่อไป

(๔) ในกรณีที่ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนพิจารณาไม่อนุมัติ ให้มีหนังสือแจ้งเหตุผลของการไม่อนุมัติกลับไปยังต้นเรื่อง

(๕) ผู้ดูแลระบบสามารถระงับหรือยกเลิกสิทธิการใช้เครือข่ายไร้สายได้ทันที เมื่อพบว่าผู้ใช้งานมีการกระทำเข้าข่ายไม่ปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

เพื่อให้มีการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม ไม่ก่อให้เกิดความเสี่ยงในการเข้าถึงระบบสารสนเทศและเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต และให้เครื่องคอมพิวเตอร์แม่ข่ายทำงานได้อย่างมีประสิทธิภาพ มีความถูกต้อง น่าเชื่อถือ และพร้อมใช้งานให้ปฏิบัติ ดังนี้

๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ที่อาจกระทบต่อการให้บริการของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) ไม่ติดตั้งซอร์สโค้ด (Source Code) คอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

(๕) ให้มีการจัดเก็บซอร์สโค้ด (Source Code) และไลบรารี่ (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) ให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ หรือซอฟต์แวร์หรือระบบสารสนเทศอื่นใด ตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๗) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(๘) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้นตามระยะเวลาที่เหมาะสม

(๙) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๙.๒ ข้อกำหนดในการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในสินทรัพย์ทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบซอฟต์แวร์ไม่ประสงค์ดี ในซอฟต์แวร์ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) ให้มีการจัดทำบัญชีของระบบสารสนเทศ เพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟแวร์นั้น ๆ

(๒) ให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบการดำเนินการดังนี้

- มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
- ให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๙.๔ ข้อกำหนดในการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) และการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการลงบันทึกการเข้า (Login) ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนการกำหนดค่า (Configuration) ของระบบ

(๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)

(๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๑๐) ข้อมูลหมายเลขไอพีแอดเดรส (IP Address) ที่เข้าถึง

(๑๑) ข้อมูลโปรโตคอลเครือข่าย (Network Protocol) ที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๐. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

เพื่อรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

๑๐.๑ การรักษาความมั่นคงปลอดภัยห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร มีดังนี้

(๑) พื้นที่ใช้งานระบบสารสนเทศและการสื่อสารแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย และพื้นที่สำหรับผู้มาติดต่อ

(๒) จัดทำแผนผังพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๓) กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๔) การควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ให้ปฏิบัติตามข้อ ๑๔. การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๕) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

(๖) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำ ระบบดับเพลิง ระบบปรับอากาศ ระบบควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านี้อย่างสม่ำเสมอ

(๗) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

(๘) เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก และสำนักงานหรือห้องจะต้องมีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๙) เจ้าหน้าที่ผู้ได้รับมอบหมายต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ที่ตนได้รับมอบหมายเป็นประจำ เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก อุปกรณ์ต่าง ๆ สื่อบันทึกข้อมูลที่สำคัญถูกจัดเก็บหรือได้รับการปิดล็อกอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๑๐.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security) มีดังนี้

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ให้มีการป้องกันการเข้าถึงจากบุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก (Fiber Optic) แทนสายสัญญาณสื่อสารแบบเดิมสำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๑๐.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) มีดังนี้

(๑) ให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ให้ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๐.๔ การนำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน (Removal of Property) มีดังนี้

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์นั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑๐.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises) มีดังนี้

(๑) ให้มีการป้องกันอุปกรณ์มิให้โดนกระแทก แตกหักในระหว่างการขนส่งหรือเคลื่อนย้าย

(๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

๑๐.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment) มีดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) ให้มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

๑๐.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ มีดังนี้

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ

๑๑. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๑.๑ ขั้นตอนการขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องเป็นบุคลากรสังกัดในหน่วยงาน

(๒) ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ดาวน์โหลดหรือรับแบบฟอร์มการขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงาน

(๓) ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) กรอกข้อมูลลงในแบบฟอร์มฯ ให้ครบถ้วน และให้ผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่าให้ความเห็นชอบ

(๔) มีหนังสือขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) พร้อมแนบแบบฟอร์มฯ ถึงผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๕) เมื่อได้รับการอนุมัติ ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนจะทำการส่งชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) กลับไปให้ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๑.๒ การใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ทั้งหมดของหน่วยงาน ต้องมีบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) เป็นของตนเอง

(๒) ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องเปลี่ยนรหัสผ่าน (Password) ทันทีหลังจากการเข้าสู่ระบบเป็นครั้งแรก

(๓) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ต้องได้รับการปกป้องด้วยรหัสผ่าน (Password) เพื่อป้องกันการถูกล่วงละเมิดและการนำไปใช้ในทางที่ผิด

(๔) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ที่มีวัตถุประสงค์พิเศษ เช่น webmaster@bora.dopa.go.th ที่สร้างขึ้นเพื่อเป็นบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) นั้น

(๕) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ทั้งหมด และจดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับ (รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ส่วนตัว) ที่ถูกสร้างและเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของหน่วยงาน ถือเป็นสินทรัพย์ของหน่วยงาน

(๖) ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงาน

(๗) พื้นที่เก็บจดหมายอิเล็กทรอนิกส์ (E-Mail) บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณจดหมายอิเล็กทรอนิกส์ (E-Mail) มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ

(๘) ต้องใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของหน่วยงานเพื่อติดต่องานของราชการเท่านั้น ห้ามใช้เพื่อการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย

(๙) ห้ามใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของหน่วยงานในการประกาศข้อมูลใด ๆ ในเว็บบอร์ด บล็อก กระดานข่าว หรือสื่อสังคมออนไลน์อื่นใด เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับหน่วยงาน

(๑๐) ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในจดหมายอิเล็กทรอนิกส์ (E-Mail) หัวจดหมายอิเล็กทรอนิกส์ (E-Mail) ลายเซ็นในจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของบุคคลอื่นโดยเด็ดขาด

(๑๑) การแจ้งที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของหน่วยงานให้บุคคลอื่นให้ใช้เพื่อการผลประโยชน์ทางราชการ

(๑๒) ห้ามใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงานในการติดต่อเรื่องส่วนตัวกับบุคคลหรือหน่วยงานที่ไม่รู้จักหรือไม่น่าเชื่อถือ

(๑๓) ขอสงวนสิทธิในการเพิกถอนสิทธิการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) หากพบว่าจดหมายอิเล็กทรอนิกส์ (E-Mail) ดังกล่าวถูกนำไปใช้งานขัดต่อนโยบายของหน่วยงาน ระเบียบปฏิบัติ หรือกฎหมายที่เกี่ยวข้อง

๑๑.๓ การส่งจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อหน่วยงาน

(๒) ซอฟต์แวร์สำหรับใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องได้รับการตั้งค่าให้จดหมายอิเล็กทรอนิกส์ (E-Mail) ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-นามสกุล ตำแหน่ง ชื่อหน่วยงานและเบอร์โทรศัพท์ติดต่อ

(๓) ห้ามผู้ใช้งานส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศหรือจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนาและจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีผลกระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

(๔) ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) หลอกลวงหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ในลักษณะลูกโซ่โดยเด็ดขาด

(๕) ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ขยะ (Junk Mail) โฆษณาสินค้าต่าง ๆ (Spam Mail) หรือจดหมายอิเล็กทรอนิกส์ (E-Mail) อื่นใดที่ผู้รับไม่ได้ต้องการ

(๖) ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใด ก็ตาม

(๗) ผู้ใช้งานต้องร่างเนื้อหาของจดหมายอิเล็กทรอนิกส์ (E-Mail) ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกจดหมายอิเล็กทรอนิกส์ (E-Mail) นั้นในนามตัวแทนของหน่วยงาน

(๘) ไฟล์เอกสารที่แนบมาพร้อมกับจดหมายอิเล็กทรอนิกส์ (E-Mail) จะต้องอยู่ในรูปแบบ .pdf, .doc, .xls, .ppt, .txt, csv, jpg, gif, html หรือในรูปแบบตามมาตรฐานอื่นใด ซึ่งผู้รับสามารถเปิดอ่านได้ด้วยซอฟต์แวร์พื้นฐานบนทุกระบบปฏิบัติการ

(๙) ห้ามส่งข้อมูลลับแนบกับจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นแต่กรณีที่มีความจำเป็นซึ่งต้องเข้ารหัสก่อน

(๑๐) การส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไฟล์แนบขนาดใหญ่เกิน ๑๐ MB ควรบีบอัดไฟล์แนบให้เล็กลงก่อนส่ง และหากจดหมายอิเล็กทรอนิกส์ (E-Mail) ดังกล่าวไม่เกี่ยวข้องกับงาน ให้ส่งนอกเวลาราชการ

๑๑.๔ การรับจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

(๒) ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัสจดหมายอิเล็กทรอนิกส์ (E-Mail) บอมม์ หรือซอฟต์แวร์ไม่ประสงค์ดีต่าง ๆ

(๓) ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่จำเป็นออกจากกล่องจดหมาย (Mailbox) ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้เป็นไปตามขนาดที่หน่วยงานกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่เกี่ยวข้องกับการทำงาน และจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่ขัดต่อกฎหมายเท่านั้น

(๔) ไม่ควรเปิดไฟล์แนบสกุล .exe, .com, .bat หรือไฟล์ประเภทโปรแกรมกระทำการอื่นใดที่ไม่เกี่ยวข้องกับงาน

(๕) ในกรณีที่ได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) ฉบับเดียวกันซ้ำหลายครั้งหรือได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่ไม่รู้จักเป็นประจำ หรือลักษณะอื่นใดที่สงสัยว่ามีการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ผิดปกติขึ้น ให้รีบแจ้งส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนดำเนินการตรวจสอบ

๑๑.๕ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

(๑) กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๖ ครั้ง

(๓) มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น ลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๔) มีการควบคุมการเข้าถึงระบบตามแนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๒.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบอินเทอร์เน็ตจะต้องทำการลงทะเบียนผู้ใช้งาน

๑๒.๒ ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้หน่วยงาน และบุคคลผู้ที่เกี่ยวข้องกับหน่วยงาน เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือว่าเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

๑๒.๓ การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านทางช่องทาง (Gateway) ที่ได้รับอนุญาตหรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ หน่วยงานขอสงวนสิทธิในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

๑๒.๔ ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบ Pop-up หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม (Spam) เนื่องจากเว็บไซต์เหล่านี้อาจมีซอฟต์แวร์ไม่ประสงค์ดีแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๑๒.๕ ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

๑๒.๖ หน่วยงานไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวผ่านทางเว็บบอร์ด บล็อก หรือสื่อสังคมออนไลน์อื่นใด ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจาการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของผู้นั้น

๑๒.๗ ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์จากเว็บไซต์ หรือแหล่งข้อมูลที่ไม่น่าเชื่อถือหรือไม่ปลอดภัยต่อระบบสารสนเทศ เว้นแต่ในกรณีที่มีความจำเป็นให้แจ้งส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน เพื่อพิจารณาความปลอดภัยและความเหมาะสม

๑๒.๘ กรณีที่มีความจำเป็นต้องดาวน์โหลดข้อมูลหรือไฟล์ขนาดใหญ่เกิน ๑๐ MB ผ่านอินเทอร์เน็ต ควรกระทำนอกเวลาราชการ เพื่อป้องกันผลกระทบต่อปริมาณข้อมูลในเครือข่าย

๑๒.๙ ตรวจสอบไวรัสในข้อมูลหรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตทุกครั้ง ก่อนติดตั้งหรือใช้งาน

๑๒.๑๐ ผู้ใช้งานมีหน้าที่ระมัดระวังการใช้งาน และต้องรับผิดชอบต่องานหรือผลที่เกิดจากการเรียกใช้บริการบนอินเทอร์เน็ตดังต่อไปนี้

(๑) ไม่ใช้เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อสิทธิ เสรีภาพหรือสินทรัพย์ของผู้อื่น

(๒) ไม่ใช้เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๓) ไม่ใช้เพื่อการกระทำอันเป็นการละเมิดเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๔) ไม่ใช้เพื่อการกระทำอันมีลักษณะเป็นการละเมิดสินทรัพย์ทางปัญญาของหน่วยงานหรือของบุคคลอื่น

(๕) ไม่ใช่เพื่อการค้า หรือผลประโยชน์ทางธุรกิจ

(๖) ไม่ใช้เพื่อเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่หน่วยงาน ไม่ว่าจะเป็นข้อมูลของหน่วยงาน หรือบุคคลภายนอกก็ตาม

(๗) ไม่ใช้เพื่อรบกวน หรือขัดขวางการใช้งานระบบเครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ทั้งในและนอกหน่วยงาน ไม่ให้สามารถใช้งานได้ตามปกติ

(๘) ไม่ใช้เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน ไปยังที่เว็บไซต์ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง หรือก่อให้เกิดความขัดแย้งในสังคม

(๙) ไม่ใช้เพื่อการอื่นใดที่อาจก่อให้เกิดความเสียหายแก่หน่วยงาน

๑๒.๑๑ ผู้ดูแลระบบสามารถระงับหรือยกเลิกสิทธิในการเรียกใช้บริการบนอินเทอร์เน็ตได้ทันที เมื่อพบว่าผู้ใช้งานมีการกระทำเข้าข่ายไม่ปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๓.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๑๓.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๔. การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

เพื่อควบคุมการเข้าถึงทางกายภาพและป้องกันสินทรัพย์จากการสูญหาย เสียหาย รวมถึงการเข้าถึงระบบโดยไม่ได้รับอนุญาต ผู้ที่สามารถเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารได้ ต้องเป็นผู้ที่ได้รับอนุญาตเท่านั้น

๑๔.๑ การขออนุญาตเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๑) หน่วยงานที่ขอเข้าปฏิบัติงานต้องทำหนังสือขออนุญาตเพื่อให้ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนเป็นผู้พิจารณาอนุญาต ได้แก่

- หน่วยงานในสังกัดสำนักบริหารการทะเบียน
- หน่วยงานระดับส่วนหรือเทียบเท่าในสังกัดสำนักบริหารการทะเบียน
- บริษัทที่เป็นผู้รับจ้างดำเนินงานโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารของสำนักบริหารการทะเบียน
- บริษัทหรือหน่วยงานที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน เห็นควรให้เข้าดำเนินการทดสอบระบบเพื่อเป็นประโยชน์ทางราชการ

(๒) หน่วยงานที่ขอเข้าปฏิบัติงานต้องทำหนังสือขออนุญาตถึงสำนักบริหารการทะเบียนเป็นผู้พิจารณาอนุญาต ได้แก่

- หน่วยงานราชการอื่นที่ไม่สังกัดสำนักบริหารการทะเบียน
- บริษัทที่เป็นผู้รับจ้างดำเนินงานโครงการของหน่วยงานราชการอื่นที่ไม่ได้สังกัดในสำนักบริหารการทะเบียน

(๓) ให้ระบุรายละเอียดการขอเข้าปฏิบัติงานในหนังสือขออนุญาตเข้าปฏิบัติงาน ดังนี้

- วัน – ช่วงเวลาในการเข้าปฏิบัติงาน
- รายชื่อเจ้าหน้าที่ประสานงาน
- รายชื่อเจ้าหน้าที่ที่จะเข้าปฏิบัติงาน
- วัตถุประสงค์การเข้าปฏิบัติงาน

(๔) หากมีการติดตั้งอุปกรณ์ให้แนบรายละเอียดอุปกรณ์ พร้อมรายละเอียดโครงการที่เกี่ยวข้องกับการติดตั้งอุปกรณ์

๑๔.๒ การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ให้ปฏิบัติดังนี้

(๑) ให้ลงทะเบียนชื่อตามแบบฟอร์มทะเบียนผู้เข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ก่อนเข้าห้อง

(๒) ห้ามเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ก่อนได้รับอนุญาตจากผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมาย

(๓) ห้ามเปิดประตูห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในห้องโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมาย และได้ลงทะเบียนชื่อตามแบบฟอร์มทะเบียนผู้เข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร เรียบร้อยแล้ว

(๔) ต้องแต่งกายให้สุภาพ

(๕) ห้ามสวมรองเท้าเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๖) ห้ามนำกระเป๋าเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๗) ห้ามสูบบุหรี่ หรือกระทำการอื่นใดที่อาจก่อให้เกิดฝุ่นละออง หรืออัคคีภัย

(๘) ห้ามนำอาหารหรือเครื่องดื่มเข้ามาในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๙) ห้ามนำกล่องเครื่องมือหรือหีบห่อเข้าและออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ก่อนได้รับอนุญาตจากผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมาย

(๑๐) ก่อนนำอุปกรณ์เข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ต้องให้ผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมายตรวจสอบก่อน

(๑๑) การนำอุปกรณ์เข้าติดตั้งชั่วคราวให้กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ ก่อนและต้องได้รับอนุมัติก่อนจึงจะสามารถนำอุปกรณ์เข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร และขอสำเนาแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์เพื่อใช้เป็นหลักฐานในกรณีนำอุปกรณ์ออก

(๑๒) การนำอุปกรณ์ออกต้องแสดงสำเนาแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ที่เคยอนุมัติในข้อ ๑๔.๒ (๑๑) ให้ผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมายตรวจสอบก่อน ในกรณีที่ไม่มีให้กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ก่อนและต้องได้รับการอนุมัติ จึงจะสามารถนำอุปกรณ์ออกจากห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารได้

(๑๓) เมื่อปฏิบัติงานเสร็จแล้วให้กรอกแบบรายงนการเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร แล้วให้ผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมายตรวจสอบก่อน

(๑๔) เวลาในการเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

- ในเวลาราชการ ตอนเช้า เวลา ๐๘.๓๐ – ๑๒.๐๐ น.

ตอนบ่าย เวลา ๑๓.๐๐ – ๑๖.๓๐ น.

- นอกเวลาราชการให้มีคำสั่งหรือทำหนังสือขออนุญาต ตามขั้นตอนการขออนุญาตเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ตามข้อ ๑๔.๑

๑๔.๓ ข้อกำหนดในการดูแลห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ให้ปฏิบัติดังนี้

(๑) บันทึกและจัดเก็บภาพของกล้องโทรทัศน์วงจรปิด (CCTV) ไว้อย่างน้อย ๑ เดือน เพื่อใช้ในการตรวจสอบภายหลัง

(๒) ตรวจสอบประตูเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารให้ปิดล็อกอยู่เสมอ

(๓) ต้องระมัดระวังดูแลสินทรัพย์สารสนเทศและให้มีการการบำรุงรักษาวัสดุอุปกรณ์ รวมทั้งระบบไฟฟ้า ระบบดับเพลิง ระบบปรับอากาศ หรือระบบอื่นใดที่ติดตั้งในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารตามระยะเวลาที่เหมาะสม ให้มีสภาพพร้อมใช้งานอยู่เสมอ

(๔) ต้องดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารอย่างสม่ำเสมอ

๑๕. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)

๑๕.๑ ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม ดังนี้

(๑) ผู้ดูแลระบบเครือข่าย (Network Administrator) มีหน้าที่และความรับผิดชอบดังนี้

- ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

- เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้นับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย

(๒) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server Administrator) มีหน้าที่และความรับผิดชอบดังนี้

- ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าว

เกิดขึ้นจากการใช้งานของผู้ใช้ที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานนั้นให้ยุติการกระทำในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้ทันที

- ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

- ติดตั้งโปรแกรมสำหรับจัดการซอฟต์แวร์ไม่ประสงค์ดีต่าง ๆ ให้เหมาะสม

- ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

- ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

(๓) ผู้ดูแลระบบสารสนเทศ (Application Administrator) มีหน้าที่และความรับผิดชอบดังนี้

- ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศ ให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

- ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๑๕.๒ หลักธรรมาภิบาลของผู้ดูแลระบบ มีดังนี้

(๑) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้โดยไม่มีเหตุผลอันสมควร

(๒) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

(๓) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๖. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log Management)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังนี้

๑๖.๑ ต้องกำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจำหน่วยงาน และมี Log Server ของหน่วยงาน สำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษาข้อมูลจราจรคอมพิวเตอร์ของหน่วยงานเมื่อมีการร้องขอ

๑๖.๒ กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงาน

๑๖.๓ บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ บันทึกการเข้า-ออกระบบ ซึ่งประกอบด้วย บัญชีผู้ใช้ (Account) หมายเลขไอพีแอดเดรส (IP Address) ต้นทาง หมายเลขไอพีแอดเดรส (IP Address) ปลายทาง โปรโตคอล (Protocol) และหมายเลขพอร์ต (Port Number) เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑๖.๔ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๖.๕ กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่าง ๆ และจำกัดสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๒

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถใช้งานได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑.๑ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ชนิดข้อมูลที่ต้องสำรองอย่างน้อยต้องประกอบด้วย

(๑) ค่า Configuration สำหรับระบบ

(๒) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ

(๓) ฐานข้อมูลของระบบสารสนเทศของหน่วยงาน

(๔) ซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่นใดที่เห็นควรทำการสำรอง

๑.๓ กำหนดขั้นตอนและความถี่ในการสำรองและกู้คืนข้อมูลอย่างถูกต้องและชัดเจน

๑.๔ กำหนดรูปแบบการสำรองข้อมูล การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) ให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

๑.๕ ต้องบันทึกข้อมูล ผู้ดำเนินการ วันที่ เวลา ชื่อข้อมูลที่สำรอง สถานะการสำรองข้อมูล

๑.๖ จัดเก็บข้อมูลที่สำรองนั้นในสื่อบันทึกข้อมูล โดยพิมพ์ชื่อบนสื่อบันทึกข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๑.๗ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ และดำเนินการป้องกันทางกายภายอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

๑.๘ กำหนดให้มีการใช้งานการเข้ารหัส (Encryption) กับข้อมูลลับที่ได้สำรองเก็บไว้

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

๒.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๒ ต้องประเมินสถานการณ์ความเสี่ยงสำหรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ

๒.๓ กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๔ กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอกที่จะต้องติดต่อเมื่อเกิดเหตุจำเป็นฉุกเฉิน

๒.๕ สร้างความตระหนัก ให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ สิ่งที่ต้องดำเนินการเมื่อเกิดเหตุเร่งด่วน หรือความรู้อื่นใดในการเตรียมความพร้อมกรณีฉุกเฉิน

๒.๖ ต้องทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ตรวจสอบ (Audit)

แนวปฏิบัติ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑.๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๓ มีการตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบ (Audit) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๒. การดำเนินการตรวจสอบและประเมินความเสี่ยง

๒.๑ ผู้ตรวจสอบ (Audit) สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว

๒.๒ ในกรณีจำเป็นต้องเข้าถึงข้อมูลแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบ (Audit) ใช้งาน รวมทั้งให้มีการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๒.๓ มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๔ มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ (Audit) รวมทั้งบันทึกประวัติแสดงการเข้าถึง (Logs) นั้น ซึ่งรวมถึงวันที่และเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๒.๕ ในกรณีที่มีเครื่องมือสำหรับตรวจประเมินระบบสารสนเทศ แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. การบริหารความต่อเนื่องของระบบสารสนเทศ

๓.๑ มีระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) สอดคล้องกับการใช้งานตามภารกิจของหน่วยงาน

๓.๒ มีการปรับปรุงระบบสารสนเทศ ระบบสำรอง และแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) อย่างน้อยปีละ ๑ ครั้ง ทั้งนี้ให้ความถี่เพียงพอสภาพความเสี่ยงที่ยอมรับได้

๓.๓ มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) อย่างน้อยปีละ ๑ ครั้ง ทั้งนี้ให้ความถี่เพียงพอสภาพความเสี่ยงที่ยอมรับได้

๓.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๓.๕ ในการสำรองข้อมูลให้มีการคัดเลือกและจัดทำระบบสำรองที่เหมาะสม

๓.๖ จัดทำคู่มือที่เกี่ยวข้องกับการปฏิบัติงานตามแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๔. การแจ้งเหตุด้านความมั่นคงปลอดภัย

๔.๑ แจ้งไปยังผู้ดูแลระบบของส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนโดยทันที เมื่อพบเหตุ

(๑) การกระทำผิดที่ขัดต่อกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

(๒) การกระทำผิดที่ขัดต่อความมั่นคงของชาติ

(๓) การใช้ทรัพยากรสารสนเทศของหน่วยงานไม่เหมาะสม ผิดวัตถุประสงค์

(๔) หน้าเว็บไซต์หลัก หรือระบบงานของหน่วยงานถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดี

(๕) ข้อมูลเว็บไซต์หลัก หรือระบบงานของหน่วยงานไม่ถูกต้อง หรือคลาดเคลื่อนจากความเป็นจริง

(๖) ข้อมูลสารสนเทศสำคัญของหน่วยงานหรือส่วนตัวถูกเปิดเผย เปลี่ยนแปลง ลบ หรือสูญหายโดยไม่ได้รับอนุญาต

(๗) มีการนำข้อมูลสารสนเทศสำคัญของหน่วยงานไปใช้ผิดวัตถุประสงค์

(๘) ทรัพยากรสารสนเทศถูกขโมย หรือสูญหาย

(๙) มีบุคลาการภายนอกเข้าใช้งานระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

(๑๐) มีการแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักฟัง ดักดูข้อมูลในระบบเครือข่ายของหน่วยงาน

(๑๑) มีการใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม

(๑๒) มีการบุกรุกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารของหน่วยงาน

(๑๓) มีการบุกรุกหรือการใช้โปรแกรมของผู้ไม่ประสงค์ดี

(๑๔) เหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๔.๒ การจัดการกับเหตุด้านความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับรายงานเหตุด้านความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้ดูแลระบบที่ได้รับมอบหมายปฏิบัติตามแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๔.๓ ให้ความร่วมมือและให้ความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลระบบที่เกี่ยวข้องในการตรวจเหตุการณ์ทางด้านความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาและผู้ดูแลระบบที่เกี่ยวข้อง

ส่วนที่ ๔

นโยบายสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศให้กับผู้ใช้งานของหน่วยงาน

๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการ

๓. เพื่อให้การใช้งานระบบสารสนเทศมีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

การฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน

๑.๑ จัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๑.๒ จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๑.๓ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๑.๔ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดให้ความรู้

๑.๕ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๑.๖ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
สำนักบริหารการทะเบียน

๑. หลักการและเหตุผล

ข้อมูลสารสนเทศซึ่งจัดเก็บไว้ที่ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ถือเป็นสินทรัพย์ทางการบริหารที่สำคัญของสำนักบริหารการทะเบียน จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนด้านการบริหารและการให้บริการ ดังนั้น เพื่อป้องกันปัจจัยจากภายนอกและปัจจัยภายในมากระทบ และทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งอุปกรณ์ต่าง ๆ เกิดความเสียหายได้ สำนักบริหารการทะเบียนจึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ ป้องกันและแก้ไขปัญหาที่อาจกระทบต่อระบบเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน

๒. วัตถุประสงค์

๒.๑ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงาน ในการดูแลระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน ให้มีเสถียรภาพและมีความพร้อมใช้งาน

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินและลดความเสียหายที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน

๓. เหตุภัยพิบัติ

ภัยพิบัติเป็นภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน ซึ่งสามารถจำแนกประเภทได้ ดังนี้

๓.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ได้แก่ อัคคีภัย อุทกภัย เป็นต้น

๓.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓.๓ ระบบสื่อสารของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

๓.๔ กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๓.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล

๓.๖ ไวรัสคอมพิวเตอร์

๓.๗ ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๓.๘ ระบบเทคโนโลยีสารสนเทศหลักเสียหาย หรือข้อมูลถูกทำลาย

๓.๙ การบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

๓.๑๐ ผลกระทบจากความชื้นและอุณหภูมิที่ไม่เหมาะสม

๔. แนวทางการป้องกันและแก้ไขความเสียหายจากภัยพิบัติ

๔.๑ ภัยธรรมชาติ

ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ได้แก่ อัคคีภัย อุทกภัย เป็นต้น

(๑) การป้องกันอัคคีภัย

- กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนให้มองเห็นชัดเจน
- จัดอบรมแผนป้องกันและระงับอัคคีภัย ซ้อมดับเพลิงและการหนีไฟขั้นต้นให้แก่บุคลากรในหน่วยงานทุกคน อย่างน้อยปีละ ๑ ครั้ง
- จัดทำระบบดับเพลิงอัตโนมัติสำหรับห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๒) การป้องกันอุทกภัย

- ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

๔.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

(๑) ควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้อง หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้รับผิดชอบนำเข้าไป

(๒) จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตนด้วยลายนิ้วมือ (Finger Scan)

(๓) มีเวรเฝ้าระวังและตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

(๔) ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๔.๓ ระบบสื่อสารของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

(๑) ตรวจสอบและเฝ้าระวังระบบเครือข่ายทั้งภายในและภายนอกให้สามารถใช้งานได้ตลอดเวลา

(๒) ต้องจัดให้มีเครือข่ายสำรอง กำหนดให้ใช้งานได้ในกรณีที่ระบบสื่อสารเส้นทางหลักไม่สามารถใช้งานได้

๔.๔ กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

(๑) มีระบบสำรองไฟฟ้าและปรับแรงดันอัตโนมัติเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

(๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาให้บริการ ตรวจสอบการทำงานของระบบทุกวัน และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอย่างน้อยเดือนละ ๑ ครั้ง

๔.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล

(๑) ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อตรวจสอบและป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) สามารถเข้าสู่ระบบตลอดเวลา

(๒) จัดเวรเฝ้าระวังระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือมีความถี่ในการเรียกใช้งานผิดปกติเพื่อจะได้สรุปหาสาเหตุและป้องกัน

(๓) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และปรับปรุงอย่างสม่ำเสมอ และปิดพอร์ต (Port) ที่ไม่มีการใช้งาน

(๔) กำหนดรหัสผ่าน (Password) เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

(๕) ป้องกันการปลอมแปลงหมายเลขไอพีแอดเดรส (IP Address) โดยการกรองแพ็คเกท (Package) ที่มาจากภายนอก

๔.๖ ไวรัสคอมพิวเตอร์

(๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดท (Update) ข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

(๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ

(๓) ใช้ความระมัดระวังในการเปิดจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๔) ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต (Internet)

๔.๗ ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากภัยดังกล่าวเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ สามารถป้องกันได้โดยการจัดทำระบบคอมพิวเตอร์กลางและระบบสื่อสารสำรอง และมีระบบสำรองข้อมูลโดยแยกสถานที่จัดเก็บมากกว่า ๑ แห่ง หากเกิดความเสียหายกับข้อมูล สามารถนำข้อมูลที่มีในระบบคอมพิวเตอร์กลางและระบบสื่อสารสำรองหรือข้อมูลในระบบสำรองที่จัดเก็บไว้มาใช้แทนได้ทันที

๔.๘ ระบบเทคโนโลยีสารสนเทศหลักเสียหาย หรือข้อมูลถูกทำลาย

(๑) กำหนดให้มีการสำรองข้อมูลอัตโนมัติไปยังฮาร์ดดิสก์ภายนอก (External Hard Disk) และเครื่องคอมพิวเตอร์แม่ข่ายที่ไซต์สำรอง (Disaster Recovery Site: DR Site) ซึ่งเครื่องจะบันทึกประวัติการทำงานไว้

(๒) ทดสอบกู้คืนข้อมูลและฐานข้อมูล ที่ได้สำรองไว้อย่างสม่ำเสมอทุกระบบอย่างน้อยปีละ ๑ ครั้ง

(๓) บำรุงรักษาข้อมูลและระบบสำรอง เพื่อลดความเสียหายของข้อมูล

๔.๙ การบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๑) มีระบบยืนยันตัวตน (Identification) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ต (Internet) และอินทราเน็ต (Intranet) หรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

(๒) กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

(๓) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร จะต้องให้เจ้าหน้าที่ผู้ดูแลห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารเป็นผู้รับผิดชอบนำเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้า-ออกมีการติดตั้งระบบสแกนลายนิ้วมือ (Finger Scan) และติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพื่อป้องกันการโจรกรรม

(๔) ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อตรวจสอบและป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) สามารถเข้าสู่ระบบตลอดเวลา

(๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือมีความถี่ในการเรียกใช้งานผิดปกติเพื่อจะได้สรุปหาสาเหตุและป้องกัน

๔.๑๐ การป้องกัน ความชื้นและอุณหภูมิที่ไม่เหมาะสม

เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น และติดตั้งระบบอัตโนมัติตรวจสอบการทำงานตลอด ๒๔ ชั่วโมง

๕. การกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติ

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ต้องอยู่ในสภาพพร้อมให้บริการได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเกิดความเสียหายหรือหยุดทำงาน ต้องดำเนินการ ดังนี้

๕.๑ ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

๕.๒ จัดหาอุปกรณ์หรือชิ้นส่วนเพื่อทดแทน

๕.๓ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๕.๔ นำข้อมูลจากสื่อบันทึกข้อมูลสำรองหรือจากระบบสำรองข้อมูลกลับมาใช้งานโดยเร็วภายใน ๔๘ ชั่วโมง

๖. ผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

หน่วยงานต้องจัดเตรียมผู้รับผิดชอบและมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๖.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่

(๑) ผู้บริหารระดับสูงสุดของหน่วยงาน

(๒) ผู้เชี่ยวชาญเฉพาะด้านเทคโนโลยีสารสนเทศและระบบข้อมูล

(๓) ผู้เชี่ยวชาญเฉพาะด้านการบริหารงานทะเบียน

(๔) ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๖.๒ ระดับปฏิบัติการ

(๑) ผู้ดูแลระบบเครือข่าย (Network Administrator) โดย กลุ่มงานควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารงานทะเบียน ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน ทำหน้าที่

- กู้คืนระบบเครือข่ายและสื่อสารให้ทำงานได้ปกติ
- หาสาเหตุและอุดช่องโหว่ระบบเครือข่าย เพื่อป้องกันภัยคุกคามทางคอมพิวเตอร์
- จัดเตรียมสถานที่สำหรับไซต์สำรอง (Disaster Recovery Site: DR Site) รวมถึงระบบไฟฟ้า ระบบสื่อสาร ระบบปรับอากาศให้พร้อมใช้งาน

(๒) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server Administrator) โดย กลุ่มงานควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารงานทะเบียน ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน ทำหน้าที่

- กู้คืนเมื่อเครื่องคอมพิวเตอร์แม่ข่ายไม่ทำงาน
- เฝ้าระวังการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศของหน่วยงาน
- ดูแลการสำรองและกู้คืนข้อมูลและฐานข้อมูลจากความเสียหายให้กลับมาใช้งานตามปกติ

(๓) ผู้ดูแลระบบไฟฟ้า (Electrical Administration) ประกอบด้วย กลุ่มงานควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารงานทะเบียน ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน และกลุ่มงานบริหารทั่วไป ทำหน้าที่

- ติดตั้งระบบดับเพลิงอัตโนมัติในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

- ดูแลและบำรุงรักษาอุปกรณ์ในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารไซต์สำรอง (Disaster Recovery Site: DR Site)

- ดูแลและบำรุงรักษาระบบไฟฟ้า ระบบปรับอากาศ การควบคุมความชื้นห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารและห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารไซต์สำรอง (Disaster Recovery Site: DR Site)

- ดูแลระบบแจ้งเตือนระบบไฟฟ้าขัดข้องนอกเวลาราชการ เพื่อให้เจ้าหน้าที่ผู้รับผิดชอบสามารถเข้าไปแก้ไขปัญหาได้อย่างรวดเร็ว

- ตรวจสอบและเตรียมน้ำมันสำรองสำหรับเครื่องกำเนิดไฟฟ้า เพื่อให้เครื่องพร้อมใช้งานเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

- รับผิดชอบการเปิดเครื่องกำเนิดไฟฟ้าเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

- จัดเวรเฝ้าระวังระบบไฟฟ้า

๗. การทบทวนและปรับปรุงแผน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ต้องได้รับการปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจตามที่ระบุ อย่างน้อยปีละ ๑ ครั้ง

๘. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บริหารทราบตามลำดับชั้นเป็นประจำทุกเดือน เพื่อรายงานสรุปให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบ และหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบทันที

ประกาศการใช้คุกกี้ (Cookies Policy)

นโยบายคุกกี้

เมื่อท่านได้เข้าสู่เว็บไซต์ (https://www.dopa.go.th) ข้อมูลที่เกี่ยวข้องกับการเข้าสู่เว็บไซต์ของท่านจะถูกบันทึกไว้ในรูปแบบของคุกกี้ โดยนโยบายคุกกี้นี้จะอธิบายถึงความหมาย การทำงาน วัตถุประสงค์ รวมถึงการลบและการปฏิเสธการเก็บคุกกี้ เพื่อความเป็นส่วนตัวของท่าน โดยการเข้าสู่เว็บไซต์นี้ถือว่าท่านได้อนุญาตให้เราใช้คุกกี้ตามนโยบายคุกกี้ที่มีรายละเอียดดังต่อไปนี้

คุกกี้คืออะไร

คุกกี้ คือ ไฟล์เล็ก ๆ เพื่อจัดเก็บข้อมูลการเข้าใช้งานเว็บไซต์ เช่น วันเวลา ลิงค์ที่คลิก หน้าที่เข้าชม เงื่อนไขการตั้งค่าต่าง ๆ โดยจะบันทึกลงไปในอุปกรณ์คอมพิวเตอร์ และ/หรือ เครื่องมือสื่อสารที่เข้าใช้งานของท่าน เช่น โน๊ตบุ๊ค แท็บเล็ต หรือ สมาร์ทโฟน ผ่านทางเว็บเบราว์เซอร์ในขณะที่ท่านเข้าสู่เว็บไซต์ โดยคุกกี้จะไม่ก่อให้เกิดอันตรายต่ออุปกรณ์คอมพิวเตอร์ และ/หรือ เครื่องมือสื่อสารของท่าน ในกรณีดังต่อไปนี้ ข้อมูลส่วนบุคคลของท่านอาจถูกจัดเก็บเพื่อใช้เพิ่มประสบการณ์การใช้งานบริการทางออนไลน์ โดยจะจำเอกลักษณ์ของภาษาและปรับแต่งข้อมูลการใช้งานตามความต้องการของท่าน เป็นการยืนยันคุณลักษณะเฉพาะตัว ข้อมูลความปลอดภัยของท่าน รวมถึงบริการที่ท่านสนใจ นอกจากนี้คุกกี้ยังถูกใช้เพื่อวัดปริมาณการเข้าใช้งานบริการทางออนไลน์ การปรับเปลี่ยนเนื้อหาตามการใช้งานของท่านโดยพิจารณาจากพฤติกรรมการเข้าใช้งานครั้งก่อนและ ณ ปัจจุบัน และอาจมีวัตถุประสงค์เพื่อการโฆษณาประชาสัมพันธ์ ทั้งนี้ท่านสามารถค้นหาข้อมูลเพิ่มเติมเกี่ยวกับคุกกี้ได้ที่ www.allaboutcookies.org

กรมการปกครอง ใช้คุกกี้อย่างไร

กรมการปกครอง ใช้คุกกี้ เพื่อบันทึกการเข้าเยี่ยมชมและสมัครเข้าใช้งานเว็บไซต์ของท่าน โดยทำให้กรมการปกครอง สามารถจดจำการใช้งานเว็บไซต์ของท่านได้ง่ายขึ้น และข้อมูลเหล่านี้จะถูกนำไปเพื่อปรับปรุงเว็บไซต์ของกรมการปกครองให้ตรงกับความต้องการของท่านมากยิ่งขึ้น เพื่ออำนวยความสะดวกให้เกิดความรวดเร็วในการใช้งานเว็บไซต์ของท่าน และในบางกรณี กรมการปกครองจำเป็นต้องให้บุคคลที่สามช่วยดำเนินการดังกล่าว ซึ่งอาจจะต้องใช้ อินเตอร์เน็ตโปรโตคอลแอดเดรส (IP Address) และคุกกี้เพื่อวิเคราะห์ทางสถิติ ตลอดจนเชื่อมโยงข้อมูล และประมวลผลตามวัตถุประสงค์ทางการตลาด

คุกกี้ที่ กรมการปกครอง ใช้ อาจจะแบ่งได้ ๒ ประเภทตามการจัดเก็บ ดังนี้

๑. Session Cookies เป็นคุกกี้ที่จะอยู่ชั่วคราวเพื่อจดจำท่านในระหว่างที่ท่านเข้าเยี่ยมชมเว็บไซต์ของกรมการปกครอง เช่น เฝ้าติดตามภาษาที่ท่านได้ตั้งค่าและเลือกใช้ เป็นต้น และจะมีการลบออกจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ของท่าน เมื่อท่านออกจากเว็บไซต์หรือได้ทำการปิดเว็บเบราว์เซอร์

๒. Persistent Cookie เป็นคุกกี้ที่จะอยู่ตามระยะเวลาที่กำหนดหรือจนกว่าท่านจะลบออก คุกกี้ประเภทนี้จะช่วยให้เว็บไซต์ของ กรมการปกครอง จดจำท่านและการตั้งค่าต่าง ๆ ของท่านเมื่อท่านกลับมาใช้บริการเว็บไซต์อีกครั้ง ซึ่งจะช่วยให้ท่านเข้าใช้บริการเว็บไซต์ได้สะดวกรวดเร็วยิ่งขึ้น

/วัตถุประสงค์...

วัตถุประสงค์ในการใช้งานคุกกี้ที่ กรมการปกครอง ใช้ มีรายละเอียดดังนี้

- คุกกี้ที่มีความจำเป็น (Strictly Necessary Cookies)
  คุกกี้ประเภทนี้มีความจำเป็นต่อการให้บริการเว็บไซต์ของกรมการปกครอง เพื่อให้ท่านสามารถเข้าใช้งานในส่วนต่าง ๆ ของเว็บไซต์ได้ รวมถึงช่วยจดจำข้อมูลที่ท่านเคยให้ไว้ผ่านเว็บไซต์ การปิดการใช้งานคุกกี้ประเภทนี้จะส่งผลให้ท่านไม่สามารถใช้บริการในสาระสำคัญของกรมการปกครอง ซึ่งจำเป็นต้องเรียกใช้คุกกี้ได้
- คุกกี้เพื่อการวิเคราะห์และประเมินผลการใช้งาน (Performance Cookies)
  คุกกี้ประเภทนี้ช่วยให้กรมการปกครอง ทราบถึงการปฏิสัมพันธ์ของผู้ใช้งานในการใช้บริการเว็บไซต์ของกรมการปกครอง รวมถึงหน้าเพจหรือพื้นที่ใดของเว็บไซต์ที่ได้รับความนิยมตลอดจนการวิเคราะห์ข้อมูลด้านอื่น ๆ กรมการปกครอง ยังใช้ข้อมูลนี้เพื่อการปรับปรุงการทำงานของเว็บไซต์ และเพื่อเข้าใจพฤติกรรมของผู้ใช้งานมากขึ้น ถึงแม้ว่าข้อมูลที่คุกกี้นี้เก็บรวบรวมจะเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ และนำมาใช้วิเคราะห์ทางสถิติเท่านั้น การปิด การใช้งานคุกกี้ประเภทนี้จะส่งผลให้ กรมการปกครอง ไม่สามารถทราบปริมาณผู้เข้าเยี่ยมชมเว็บไซต์ และไม่สามารถประเมินคุณภาพการให้บริการได้
- คุกกี้เพื่อการใช้งานเว็บไซต์ (Functional Cookies)
  คุกกี้ประเภทนี้จะช่วยให้เว็บไซต์ของกรมการปกครอง จดจำตัวเลือกต่าง ๆ ที่ท่านได้ตั้งค่าไว้และช่วยให้เว็บไซต์ส่งมอบคุณสมบัติและเนื้อหาเพิ่มเติมให้ตรงกับการใช้งานของท่านได้ เช่น ช่วยจดจำชื่อบัญชีผู้ใช้งานของท่าน หรือจดจำการเปลี่ยนแปลงการตั้งค่าขนาดฟอนต์หรือการตั้งค่าต่าง ๆ ของหน้าเพจซึ่งท่านสามารถปรับแต่งได้ การปิดการใช้งานคุกกี้ประเภทนี้อาจส่งผลให้เว็บไซต์ไม่สามารถทำงานได้อย่างสมบูรณ์

ประเภทของคุกกี้	รายละเอียด	ตัวอย่าง
คุกกี้ที่มีความจำเป็น (Strictly Necessary Cookies)	คุกกี้ประเภทนี้มีความจำเป็นต่อการให้บริการเว็บไซต์ของกรมการปกครอง เพื่อให้ท่านสามารถเข้าใช้งานในส่วนต่าง ๆ ของเว็บไซต์ได้ รวมถึงช่วยจดจำข้อมูลที่ท่านเคยให้ไว้ผ่านเว็บไซต์ การปิดการใช้งานคุกกี้ประเภทนี้จะส่งผลให้ท่านไม่สามารถใช้บริการในสาระสำคัญของกรมการปกครอง ซึ่งจำเป็นต้องเรียกใช้คุกกี้ได้	PHPSESSID JSESSIONID

ประเภทของคุกกี้	รายละเอียด	ตัวอย่าง
คุกกี้เพื่อการวิเคราะห์และประเมินผลการใช้งาน (Performance Cookies)	คุกกี้ประเภทนี้ช่วยให้ กรมการปกครอง ทราบถึงการปฏิสัมพันธ์ของผู้ใช้งานในการใช้บริการเว็บไซต์ของกรมการปกครอง รวมถึงหน้าเพจหรือพื้นที่ใดของเว็บไซต์ที่ได้รับความนิยม ตลอดจนการวิเคราะห์ข้อมูลด้านอื่น ๆ กรมการปกครอง ยังใช้ข้อมูลนี้เพื่อการปรับปรุงการทำงานของเว็บไซต์และเพื่อเข้าใจพฤติกรรมของผู้ใช้งานมากขึ้น ถึงแม้ว่า ข้อมูลที่คุกกี้นี้เก็บรวบรวมจะเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ และนำมาใช้วิเคราะห์ทางสถิติเท่านั้น การปิดการใช้งานคุกกี้ประเภทนี้จะส่งผลให้ กรมการปกครอง ไม่สามารถทราบปริมาณผู้เข้าเยี่ยมชมเว็บไซต์ และไม่สามารถประเมินคุณภาพการให้บริการได้	_utmc _hjIncludedInPageviewSample _hjTLDTest _gid __utma __utmb __utmt __utmz _hjid _ga _hjAbsoluteSessionInProgress _hjFirstSeen
คุกกี้เพื่อการใช้งานเว็บไซต์ (Functional Cookies)	คุกกี้ประเภทนี้จะช่วยให้เว็บไซต์ของ กรมการปกครอง จดจำตัวเลือกต่าง ๆ ที่ท่านได้ตั้งค่าไว้ และช่วยให้เว็บไซต์ส่งมอบคุณสมบัติและเนื้อหาเพิ่มเติมให้ตรงกับการใช้งานของท่านได้ เช่น ช่วยจดจำชื่อบัญชีผู้ใช้งานของทาน หรือจดจำการเปลี่ยนแปลงการตั้งค่าขนาดฟอนต์หรือการตั้งค่าต่าง ๆ ของหน้าเพจซึ่งท่านสามารถปรับแต่งได้ การปิดการใช้งานคุกกี้ประเภทนี้อาจส่งผลให้เว็บไซต์ไม่สามารถทำงานได้อย่างสมบูรณ์	fbsr_๓๔๐๔๘๖๖๔๒๖๔๕๗๖๑

/ท่านจะจัดการ

ท่านจะจัดการคุกกี้ได้อย่างไร

บราวเซอร์ส่วนใหญ่จะมีการตั้งค่าให้มีการยอมรับคุกกี้เป็นค่าเริ่มต้น อย่างไรก็ตาม ท่านสามารถปฏิเสธการใช้งานหรือลบคุกกี้ในหน้าการตั้งค่าของบราวเซอร์ที่ท่านใช้งานอยู่ ทั้งนี้ หากท่านทำการปรับเปลี่ยนการตั้งค่าบราวเซอร์ของท่านอาจส่งผลกระทบต่อรูปแบบและการใช้งานบนหน้าเว็บไซต์ของเราได้ หากท่านประสงค์ที่จะทำการปรับเปลี่ยนการตั้งค่า ท่านสามารถตรวจสอบรายละเอียดเพิ่มเติมได้ตามลิงก์ที่ได้ระบุไว้ข้างล่าง

- Android (Chrome)

https://support.google.com/chrome/answer/๙๕๖๔๗?co=GENIE.Platform%๓DAndroid&hl=en&oco=๑

- Apple Safari

https://support.apple.com/en-gb/guide/safari/sfri๑๑๔๗๑/mac

- Blackberry

https://docs.blackberry.com/content/dam/docs-blackberry-com/release-pdfs/en/device-user-guides/BlackBerry-Classic-Smartphone-๑๐.๓.๓-User-Guide-en.pdf

- Google Chrome

https://support.google.com/chrome/answer/๙๕๖๔๗?co=GENIE.Platform%๓DDesktop&hl=en

- Microsoft Edge

https://support.microsoft.com/en-us/windows/microsoft-edge-browsing-data-and-privacy-bb๘๑๗๔ba-๙d๗๓-dcf๒-๙b๔a-c๕๘๒b๔e๖๔๐dd

- Microsoft Internet Explorer

https://support.microsoft.com/en-us/topic/delete-and-manage-cookies-๑๖๘dab๑๑-๐๗๕๓-๐๔๓d-๗c๑๖-ede๕๙๔๗fc๖๔d

- Mozilla Firefox

https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop?redirectslug=enable-and-disable-cookies-website-preferences&redirectlocale=en-US

- Opera

https://help.opera.com/en/latest/web-preferences/

- Iphone or Ipad (Chrome)

https://support.google.com/chrome/answer/๙๕๖๔๗?co=GENIE.Platform%๓DiOS&hl=en&oco=๑

- Iphone or Ipad (Safari)

https://support.apple.com/en-us/HT๒๐๑๒๖๕

ทั้งนี้ โปรดทราบว่า หากท่านเลือกที่จะปิดการใช้งานคุกกี้บนเบราว์เซอร์หรืออุปกรณ์ของท่านอาจส่งผลกระทบกับการทำงานบางส่วนของเว็บไซต์ของกรมการปกครองที่ไม่สามารถทำงานหรือให้บริการได้เป็นปกติกรมการปกครองจะไม่รับผิดชอบ และกรมการปกครองไม่ได้มีความเกี่ยวข้องกับเว็บไซต์ รวมทั้งเนื้อหาในเว็บไซต์ต่าง ๆ ที่กล่าวมาข้างบนสำหรับข้อมูลอื่น ๆ เพิ่มเติมในเรื่องนี้ ท่านสามารถเข้าไปอ่านได้ที่ https://www.aboutcookies.org/how-to-delete-cookies

/การเชื่อมโยง...

การเชื่อมโยงข้อมูลกับเว็บไซต์อื่น

เว็บไซต์ของ กรมการปกครอง อาจมีการเชื่อมโยงไปยังเว็บไซต์หรือโซเชียลมีเดียของบุคคลภายนอก รวมถึงอาจมีการฝังเนื้อหาหรือวีดีโอที่มาจากโซเชียลมีเดีย เช่น YouTube หรือ Facebook เป็นต้น ซึ่งจะช่วยให้ท่านเข้าถึงเนื้อหาและสร้างการปฏิสัมพันธ์กับบุคคลอื่นบนโซเชียลมีเดียจากเว็บไซต์ของกรมการปกครองได้ ซึ่งเว็บไซต์หรือโซเชียลมีเดียของบุคคลภายนอกจะมีการกำหนดและตั้งค่าคุกกี้ขึ้นมาเองโดยที่ กรมการปกครองไม่สามารถควบคุมหรือรับผิดชอบต่อคุกกี้เหล่านั้นได้ และขอแนะนำให้ท่านควรเข้าไปอ่านและศึกษานโยบายหรือประกาศการใช้คุกกี้ของบุคคลภายนอกเหล่านั้นด้วย

การเปลี่ยนแปลงประกาศ

ประกาศนี้อาจมีการปรับปรุงให้เหมาะสมและสอดคล้องกับสถานการณ์และตามการให้บริการจริงโดยกรมการปกครอง จะมีการแจ้งประกาศที่มีการปรับปรุงใหม่บนเว็บไซต์นี้ ดังนั้น กรมการปกครองขอแนะนำให้ท่านตรวจสอบให้แน่ใจว่าท่านได้เข้าใจการเปลี่ยนแปลงตามข้อกำหนดดังกล่าว

การติดต่อสอบถามหรือใช้สิทธิ

หากท่านมีข้อสงสัย ข้อเสนอแนะหรือข้อกังวลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของ กรมการปกครอง หรือเกี่ยวกับนโยบายนี้ หรือท่านต้องการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านสามารถติดต่อสอบถามได้ที่

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
รองอธิบดีกรมการปกครอง ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ
๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : dpo@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๘๒-๑๐๔๗

ผู้ควบคุมข้อมูลส่วนบุคคล กรมการปกครอง
๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : webmaster@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๒๔๑-๐๑๕๑-๘

คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)

กรมการปกครอง

.....

๑. บทนำ

กรมการปกครองตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่นอันเกี่ยวกับท่าน (รวมเรียกว่า "**ข้อมูล**") เพื่อให้ท่านสามารถเชื่อมั่นได้ว่า กรมการปกครอง มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ("**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**") รวมถึงกฎหมายอื่นที่เกี่ยวข้อง คำประกาศเกี่ยวกับความเป็นส่วนตัว ("**คำประกาศ**") นี้ จึงได้ถูกจัดทำขึ้นเพื่อชี้แจงแก่ท่านถึงรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า "**ประมวลผล**") ข้อมูลส่วนบุคคลซึ่งดำเนินการโดย กรมการปกครอง รวมถึงเจ้าหน้าที่และบุคคลที่เกี่ยวข้องผู้ดำเนินการแทนหรือในนามของ กรมการปกครอง โดยมีเนื้อหาสาระดังต่อไปนี้

๒. ขอบเขตการบังคับใช้คำประกาศ

กรมการปกครอง จะเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมายที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลเท่านั้น เพื่อให้บรรลุวัตถุประสงค์ในการปฏิบัติตามภารกิจในอำนาจหน้าที่ของกรมการปกครอง คำประกาศนี้ใช้บังคับกับข้อมูลส่วนบุคคลของบุคคลซึ่งมีความสัมพันธ์กับกรมการปกครอง ในปัจจุบันและที่อาจมีในอนาคต ซึ่งถูกประมวลผลข้อมูลส่วนบุคคลโดยกรมการปกครอง รวมถึงคู่สัญญาหรือบุคคลภายนอกที่ประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของ กรมการปกครอง ("**ผู้ประมวลผลข้อมูลส่วนบุคคล**") ภายใต้บริการต่าง ๆ เช่น เว็บไซต์ ระบบแอปพลิเคชัน เอกสาร หรือ บริการในรูปแบบอื่นที่ควบคุมดูแลโดย กรมการปกครอง (รวมเรียกว่า "**บริการ**") นอกจากคำประกาศฉบับนี้แล้ว กรมการปกครอง อาจกำหนดให้มีคำประกาศเกี่ยวกับความเป็นส่วนตัว ("**ประกาศ**") สำหรับบริการของกรมการปกครอง เพื่อชี้แจงให้เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้ใช้บริการได้ทราบถึงข้อมูลส่วนบุคคลที่ถูกประมวลผล วัตถุประสงค์และเหตุผลอันชอบด้วยกฎหมายในการประมวลผล ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล รวมถึงสิทธิในข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลพึงมีในบริการนั้นเป็นการเฉพาะเจาะจง ทั้งนี้ ในกรณีที่มีความขัดแย้งกันในสาระสำคัญในประกาศเกี่ยวกับความเป็นส่วนตัวนี้ ให้ถือตามความในประกาศเกี่ยวกับความเป็นส่วนตัวของบริการนั้น

ประกาศเกี่ยวกับความเป็นส่วนตัวนี้จัดทำขึ้นเพื่อแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังต่อไปนี้

/๓. คำนิยาม

๓. คำนิยาม

๓.๑ ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

๓.๒ การประมวลผลข้อมูลส่วนบุคคล หมายถึง การดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล ซึ่งกระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

๓.๓ ประกาศเกี่ยวกับความเป็นส่วนตัว (privacy notice) หมายถึง ประกาศสำหรับแสดงรายละเอียดของการเก็บรวบรวม ข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียด ดังกล่าวก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

๓.๔ บันทึกการให้ความยินยอม (consent receipt หรือ consent record) หมายถึง บันทึกที่มีสาระสำคัญของการ ให้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลส่งให้เจ้าของข้อมูลส่วนบุคคลใช้ ตรวจสอบได้

๓.๕ ผู้ควบคุมข้อมูลส่วนบุคคล (data controller) หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๓.๖ ผู้ประมวลผลข้อมูลส่วนบุคคล (data processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคล หรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

๓.๗ ข้อมูลส่วนบุคคลอ่อนไหว หมายถึง ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล ในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๓.๘ เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวม ใช้ หรือเปิดเผย

๓.๙ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่ให้คำแนะนำและตรวจสอบการดำเนินงาน ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๓.๑๐ ผู้ปฏิบัติงาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง เจ้าหน้าที่ของรัฐ และผู้ที่ได้มอบหมายให้ปฏิบัติหน้าที่ ของกรมการปกครอง

๓.๑๑ ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

๓.๑๒ สิทธิการเข้าถึง หมายถึง กระบวนการตรวจสอบตัวตนโดยใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) หรือระบบการกำหนดสิทธิ์ของระบบสารสนเทศ เพื่อตรวจสอบสิทธิผู้ใช้งานในการเข้าใช้งาน

/๔. คุกกี้

๔. คุกกี้

กรมการปกครอง เก็บรวบรวมและใช้คุกกี้รวมถึงเทคโนโลยีอื่นในลักษณะเดียวกันในเว็บไซต์ที่อยู่ภายใต้ความดูแลของกรมการปกครองหรือบนอุปกรณ์ของท่านตามแต่บริการที่ท่านใช้งาน ทั้งนี้ เพื่อการดำเนินการด้านความปลอดภัยในการให้บริการของ กรมการปกครอง และเพื่อให้ท่านซึ่งเป็นผู้ใช้งานได้รับความสะดวกและประสบการณ์ที่ดีในการใช้งานบริการของ กรมการปกครอง และข้อมูลเหล่านี้จะถูกนำไปเพื่อปรับปรุงเว็บไซต์ของ กรมการปกครอง ให้ตรงกับความต้องการของท่านมากยิ่งขึ้น โดยท่านสามารถตั้งค่าหรือลบการใช้งานคุกกี้ได้ด้วยตนเองจากการตั้งค่าในเว็บเบราว์เซอร์ (Web Browser) ของท่าน

๕. ข้อมูลส่วนบุคคลของผู้เยาว์ คนไร้ความสามารถและคนเสมือนไร้ความสามารถ

กรณีที่กรมการปกครอง ทราบว่าข้อมูลส่วนบุคคลที่จำเป็นต้องได้รับความยินยอมในการเก็บรวบรวม เป็นของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้เยาว์ คนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ ต่อเมื่อได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ หรือผู้อนุบาล หรือผู้พิทักษ์ตามแต่กรณี ยกเว้นเป็นกรณีที่กรมการปกครองมีอำนาจดำเนินการได้ตามที่กฎหมายกำหนด

กรณีที่กรมการปกครอง ไม่ทราบมาก่อนว่าเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ และมาพบในภายหลังว่า กรมการปกครอง ได้เก็บรวบรวมข้อมูลของเจ้าของข้อมูลส่วนบุคคลดังกล่าวโดยยังมิได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ หรือผู้อนุบาล หรือผู้พิทักษ์ตามแต่กรณี ดังนี้ กรมการปกครอง จะดำเนินการลบทำลายข้อมูลส่วนบุคคลนั้น เว้นแต่มีกฎหมายให้อำนาจดำเนินการในเรื่องนั้นไว้

๖. วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

กรมการปกครองจะเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย โดยกรมการปกครองจะขอความยินยอม โดยชัดแจ้งจากท่านก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน เพื่อวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือการใช้อำนาจรัฐของกรมการปกครอง ซึ่งกำหนดไว้ตามกฎหมาย รวมถึง กฎ ระเบียบ คำสั่งและมติคณะรัฐมนตรีที่เกี่ยวข้อง

๒. เพื่อการปฏิบัติหน้าที่ตามกฎหมาย กรมการปกครอง ในกรณีที่มีกฎหมายกำหนดให้ต้องปฏิบัติเพื่อให้กรมการปกครอง สามารถปฏิบัติตามที่กฎหมายที่ควบคุม กรมการปกครอง

๓. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายระหว่างเจ้าของข้อมูลส่วนบุคคลกับกรมการปกครอง โดยประโยชน์ดังกล่าวมีความสำคัญไม่น้อยไปกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล เช่น ในช่วงที่เจ้าของข้อมูลส่วนบุคคลสมัครลงทะเบียนขอรหัสผู้ใช้งานเพื่อขอรับบริการบนระบบสารสนเทศที่ให้บริการ

๔. เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตาม คำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้นกับกรมการปกครอง

ยกเว้น แต่ในกรณีดังต่อไปนี้ กรมการปกครองสามารถเก็บรวบรวมข้อมูลส่วนบุคคลของท่านได้โดยไม่ต้องขอความยินยอม

๑. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์ สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครอง สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

/๒. เพื่อป้องกัน...

๒. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๓. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

๔. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๕. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือ นิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

๖. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

เนื่องจากข้อมูลส่วนบุคคลที่กรมการปกครองจะดำเนินการประมวลผลเพื่อวัตถุประสงค์ที่กำหนด ในส่วนที่มีความเกี่ยวเนื่องกับการปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นเพื่อเข้าทำสัญญากับท่าน ซึ่งข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่จำเป็นต่อการบรรลุวัตถุประสงค์ดังกล่าว หากท่านไม่ให้ข้อมูลส่วนบุคคลดังกล่าวแก่ กรมการปกครอง อาจมีผลกระทบทางกฎหมาย หรือ กรมการปกครองอาจจะไม่สามารถปฏิบัติหน้าที่ภายใต้สัญญาที่ได้เข้าทำกับท่าน หรือไม่สามารถเข้าทำสัญญากับท่านได้ (แล้วแต่กรณี) ในกรณีดังกล่าว กรมการปกครองอาจมีความจำเป็นต้องปฏิเสธการเข้าทำสัญญากับท่าน หรือยกเลิกการให้บริการที่เกี่ยวข้องต่อท่านไม่ว่าทั้งหมดหรือบางส่วน

๗. แหล่งที่มาของข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวม

กรมการปกครอง เก็บรวบรวมหรือได้มาซึ่งข้อมูลส่วนบุคคลประเภทต่าง ๆ จากแหล่งข้อมูลดังต่อไปนี้

๗.๑ ข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรงในช่องทางให้บริการต่าง ๆ เช่น ขั้นตอนการสมัคร ลงทะเบียน สมัครงาน ลงนามในสัญญา เอกสาร ทำแบบสำรวจ การยื่นคำขอ การพิจารณาอนุญาต หรือ บริการ หรือช่องทางให้บริการอื่นที่ควบคุมดูแลโดย กรมการปกครอง หรือเมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อสื่อสารกับ กรมการปกครอง ณ ที่ทำการหรือผ่านช่องทางติดต่ออื่นที่ควบคุมดูแลโดยกรมการปกครอง เป็นต้น

๗.๒ ข้อมูลที่ กรมการปกครอง เก็บรวบรวมจากการที่เจ้าของข้อมูลส่วนบุคคลเข้าใช้งานเว็บไซต์ หรือบริการอื่นๆ ตามสัญญาหรือตามพันธกิจในความรับผิดชอบของกรมการปกครอง เช่น การติดตามพฤติกรรมการใช้งานเว็บไซต์ ผลิตภัณฑ์หรือบริการของ กรมการปกครอง ด้วยการใช้คุกกี้ (Cookies) หรือจากซอฟต์แวร์บนอุปกรณ์ของเจ้าของข้อมูลส่วนบุคคล เป็นต้น

๗.๓ ข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวมจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล โดยที่แหล่งข้อมูลดังกล่าวมีอำนาจหน้าที่ มีเหตุผลที่ชอบด้วยกฎหมายหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้วในการเปิดเผยข้อมูลแก่กรมการปกครอง เช่น การเชื่อมโยงบริการดิจิทัลของหน่วยงานของรัฐในการให้บริการเพื่อประโยชน์สาธารณะแบบเบ็ดเสร็จแก่เจ้าของข้อมูลส่วนบุคคลเอง การรับข้อมูลส่วนบุคคลจากหน่วยงานของรัฐแห่งอื่นในฐานะที่ กรมการปกครอง มีหน้าที่ตามพันธกิจในการดำเนินการจัดให้มีศูนย์แลกเปลี่ยนข้อมูลกลางเพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล รวมถึงจากความจำเป็นเพื่อให้บริการตามสัญญาที่อาจมีการแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานคู่สัญญาได้

/นอกจากนี้...

นอกจากนี้ ยังหมายความรวมถึงกรณีที่ท่านเป็นผู้ให้ข้อมูลส่วนบุคคลของบุคคลภายนอกแก่กรมการปกครอง ดังนี้ ท่านมีหน้าที่รับผิดชอบในการแจ้งรายละเอียดตามนโยบายนี้หรือประกาศของผลิตภัณฑ์หรือบริการ ตามแต่กรณี ให้บุคคลดังกล่าวทราบ ตลอดจนขอความยินยอมจากบุคคลนั้นหากเป็นกรณีที่ต้องได้รับความยินยอมในการเปิดเผยข้อมูลแก่ กรมการปกครอง

๘. ประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม

กรมการปกครองอาจเก็บรวบรวมหรือได้มาซึ่งข้อมูลดังต่อไปนี้ ซึ่งอาจรวมถึงข้อมูลส่วนบุคคลของท่าน ทั้งนี้ขึ้นอยู่กับงานบริการที่ท่านขอรับบริการหรือบริบทความสัมพันธ์ที่ท่านมีกับกรมการปกครอง รวมถึงข้อพิจารณาอื่นที่มีผลกับการเก็บรวบรวมข้อมูลส่วนบุคคล โดยประเภทของข้อมูล ที่ระบุไว้ดังต่อไปนี้เป็นเพียงกรอบการเก็บรวบรวมข้อมูลส่วนบุคคลของกรมการปกครองเป็นการทั่วไป ทั้งนี้ เฉพาะข้อมูลที่เกี่ยวข้องกับบริการที่ท่านใช้งานหรือมีความสัมพันธ์ด้วยเท่านั้นที่จะมีผลบังคับใช้

๘.๑ ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลระบุชื่อเรียกของท่านหรือข้อมูลจากเอกสารราชการที่ระบุข้อมูลเฉพาะตัวของท่าน เช่น คำนำหน้าชื่อ ชื่อ นามสกุล ชื่อกลาง ชื่อเล่น ลายมือชื่อ เลขที่บัตรประจำตัวประชาชน สัญชาติ เลขที่ใบขับขี่ เลขที่หนังสือเดินทาง ข้อมูลทะเบียนบ้าน หมายเลขใบประกอบการ หมายเลขใบอนุญาตการประกอบวิชาชีพ (สำหรับแต่ละอาชีพ) หมายเลขประจำตัวผู้ประกันตน หมายเลขประกันสังคม เป็นต้น

๘.๒ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ได้แก่ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนของท่าน เช่น เชื้อชาติ ข้อมูลศาสนา ข้อมูลความพิการ ข้อมูลความเห็นทางการเมือง ประวัติอาชญากรรม ข้อมูลชีวภาพ (ข้อมูลภาพจำลองใบหน้า) ข้อมูลพันธุกรรม ข้อมูลเกี่ยวกับสุขภาพ เป็นต้น ทั้งนี้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลปฏิเสธไม่ให้ข้อมูลที่มีความจำเป็นในการให้บริการของ กรมการปกครอง อาจเป็นผลให้กรมการปกครองไม่สามารถให้บริการนั้นแก่เจ้าของข้อมูลส่วนบุคคลดังกล่าวได้ทั้งหมดหรือบางส่วน

๙. ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

กรมการปกครอง เก็บรวบรวมข้อมูลส่วนบุคคลของท่านตามความเหมาะสมและตามบริบทของการให้บริการ ทั้งนี้ ตามอำนาจหน้าที่ตามที่กฎหมายให้อำนาจไว้ เช่น ฐานทางกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคลที่กรมการปกครองใช้ ประกอบด้วย

๙.๑ เพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือการใช้อำนาจรัฐของกรมการปกครอง

๙.๒ เพื่อการปฏิบัติหน้าที่ตามกฎหมาย

๙.๓ เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย

๙.๔ เป็นการจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๙.๕ เพื่อการปฏิบัติตามสัญญา

๙.๖ เพื่อการจัดทำเอกสารประวัติศาสตร์ วิจัยหรือสถิติที่สำคัญ

๙.๗ ความยินยอมของท่าน

ในกรณีที่กรมการปกครองมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อการปฏิบัติตามสัญญา การปฏิบัติหน้าที่ตามกฎหมาย หรือเพื่อความจำเป็นในการเข้าทำสัญญา หากท่านปฏิเสธไม่ให้ข้อมูลส่วนบุคคลหรือ คัดค้านการดำเนินการประมวลผลตามวัตถุประสงค์ของกิจกรรม อาจมีผลทำให้กรมการปกครองไม่สามารถดำเนินการหรือให้บริการตามที่ท่านร้องขอได้ทั้งหมดหรือบางส่วน

/๑๐. ระยะเวลา...

๑๐. ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน

กรมการปกครอง จะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ในระยะเวลาเท่าที่ข้อมูลนั้นยังมีความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเท่านั้น ตามรายละเอียดที่ได้กำหนดไว้ในนโยบายประกาศหรือตามกฎหมายที่เกี่ยวข้อง ทั้งนี้ เมื่อพ้นระยะเวลาและข้อมูลส่วนบุคคลของท่านสิ้นความจำเป็นตามวัตถุประสงค์ดังกล่าวแล้ว กรมการปกครอง จะทำการลบ ทำลายข้อมูลส่วนบุคคลของท่าน หรือทำให้ข้อมูลส่วนบุคคลของท่านไม่สามารถระบุตัวตนได้ต่อไป ตามรูปแบบและมาตรฐานการลบทำลายข้อมูลส่วนบุคคลที่คณะกรรมการหรือกฎหมายประกาศกำหนดหรือตามมาตรฐานสากลอย่างไรก็ดี ในกรณีที่มีข้อพิพาทการใช้สิทธิหรือคดีความอันเกี่ยวข้องกับข้อมูลส่วนบุคคลของท่าน กรมการปกครอง ขอสงวนสิทธิในการเก็บรักษาข้อมูลนั้นต่อไปจนกว่าข้อพิพาทนั้นจะได้มีคำสั่งหรือคำพิพากษาถึงที่สุด

๑๑. การเปิดเผยข้อมูลส่วนบุคคล

การเปิดเผยข้อมูลส่วนบุคคล กรมการปกครอง จะดำเนินการตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล โดยกรมการปกครอง อาจเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นอย่างจำกัดให้แก่หน่วยงานหรือบุคคลภายนอก ทั้งนี้กรมการปกครองห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้น โดยไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือ มาตรา ๒๖ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

การนำข้อมูลส่วนบุคคลไปใช้ประโยชน์หรือเปิดเผย กรมการปกครอง อาจใช้ประโยชน์หรือเปิดเผยข้อมูลส่วนบุคคลให้แก่ผู้ปฏิบัติงานของ กรมการปกครอง หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลของกรมการปกครอง ได้ เพื่อการใช้ประโยชน์หรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่นนอกเหนือจากกรณีดังกล่าวจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน เว้นแต่เป็นกรณีที่ กรมการปกครอง จะต้องปฏิบัติให้เป็นไปตามกฎหมายหรือมีกฎหมายบัญญัติให้กระทำได้ดำเนินการให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้ ซึ่งอาจรวมถึงการเปิดเผยข้อมูลส่วนบุคคลให้กับหน่วยงานต่อไปนี้

๑. หน่วยงานของรัฐซึ่งมีอำนาจหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. หน่วยงานกำกับดูแลเรื่องข้อมูลส่วนบุคคล เช่น สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

๓. บุคคลหรือหน่วยงานที่ กรมการปกครอง จ้างให้เก็บข้อมูลหรือประมวลผลข้อมูลส่วนบุคคล

๔. หน่วยงานที่มีอำนาจตามกฎหมายอื่น ๆ เพื่อดำเนินวัตถุประสงค์ ด้านการตรวจสอบการดำเนินงานของกรมการปกครอง

๕. กรมการปกครอง จะดูแลไม่ให้ผู้ปฏิบัติงานของ กรมการปกครอง หรือผู้ประมวลผลข้อมูลส่วนบุคคลนำข้อมูลส่วนบุคคลไปใช้ประโยชน์หรือเปิดเผยแก่บุคคลอื่นนอกเหนือไปจากวัตถุประสงค์ในการดำเนินงานตามภารกิจของ กรมการปกครอง เว้นแต่ จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน หรือเป็นกรณีที่ กรมการปกครอง จะต้องปฏิบัติให้เป็นไปตามกฎหมายหรือมีกฎหมายบัญญัติให้กระทำได้

๖. ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นบุคคลภายนอก กรมการปกครอง จะจัดให้มีข้อตกลงระหว่างกรมการปกครอง กับผู้ประมวลผลข้อมูล เพื่อกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัย การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามที่กรมการปกครองกำหนดเท่านั้น ทั้งนี้ กรมการปกครอง จะจัดให้มีการควบคุมและตรวจสอบการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายและข้อตกลงดังกล่าวอย่างเคร่งครัดด้วย

/๑๒. การส่งหรือ...

๑๒. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ในบางกรณี กรมการปกครอง อาจจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังต่างประเทศเพื่อดำเนินการตามวัตถุประสงค์ในการให้บริการแก่ท่าน เช่น เพื่อส่งข้อมูลส่วนบุคคลไปยังระบบคลาวด์ (Cloud) ที่มีแพลตฟอร์มหรือเครื่องแม่ข่าย (Server) อยู่ต่างประเทศ (เช่น ประเทศสิงคโปร์ หรือสหรัฐอเมริกา เป็นต้น) เพื่อสนับสนุนระบบเทคโนโลยีสารสนเทศที่ตั้งอยู่นอกประเทศไทย ทั้งนี้ ขึ้นอยู่กับบริการของ กรมการปกครอง ที่ท่านใช้งานหรือมีส่วนเกี่ยวข้องเป็นรายกิจกรรม อย่างไรก็ตาม ในขณะที่จัดทำนโยบายฉบับนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมิได้มีประกาศกำหนดรายการประเทศปลายทางที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ดังนั้นเมื่อ กรมการปกครอง มีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังประเทศปลายทาง กรมการปกครอง จะดำเนินการเพื่อให้ข้อมูลส่วนบุคคลที่ส่งหรือโอนไปมีมาตรการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอตามมาตรฐานสากล หรือดำเนินการตามเงื่อนไขเพื่อให้สามารถส่งหรือโอนข้อมูลนั้นได้ตามกฎหมาย ได้แก่

๑. เป็นการปฏิบัติตามกฎหมายที่กำหนดให้กรมการปกครองต้องส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

๒. ได้แจ้งให้ท่านทราบและได้รับความยินยอมจากท่านในกรณีที่ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ ทั้งนี้ตามประกาศรายชื่อประเทศที่คณะกรรมการคุ้มครองส่วนบุคคลประกาศกำหนด

๓. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาที่ท่านเป็นคู่สัญญากับ กรมการปกครอง หรือเป็นการทำตามคำขอของท่านก่อนการเข้าทำสัญญานั้น

๔. เป็นการกระทำตามสัญญาของ กรมการปกครอง กับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของท่าน

๕. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของท่านหรือของบุคคลอื่น เมื่อท่านไม่สามารถให้ความยินยอมในขณะนั้นได้

๖. เป็นการจำเป็นเพื่อดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

๑๓. สิทธิของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ ทั้งนี้ สิทธิดังกล่าวจะเริ่มมีผลบังคับใช้เมื่อกฎหมายในส่วนของสิทธินี้มีผลใช้บังคับ โดยรายละเอียดของสิทธิต่าง ๆ ประกอบด้วย

๑. สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล ท่านมีสิทธิขอเข้าถึง รับสำเนาและขอให้เปิดเผยที่มาของข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวมไว้โดยปราศจากความยินยอมของท่าน เว้นแต่กรณีที่ กรมการปกครอง มีสิทธิปฏิเสธคำขอของท่านด้วยเหตุตามกฎหมายหรือคำสั่งศาล หรือกรณีที่การใช้สิทธิของท่านจะมีผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

๒. สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์และเป็นปัจจุบัน หากท่านพบว่าข้อมูลส่วนบุคคลของท่านไม่ถูกต้อง ไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ท่านมีสิทธิขอให้แก้ไขเพื่อให้มีความถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิดได้

/๓. สิทธิในการ...

๓. สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล ท่านมีสิทธิขอให้ กรมการปกครอง ลบหรือทำลายข้อมูลส่วนบุคคลของท่าน หรือทำให้ข้อมูลส่วนบุคคลของท่านไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ต่อไป ทั้งนี้ การใช้สิทธิลบหรือทำลายข้อมูลส่วนบุคคลนี้จะต้องอยู่ภายใต้เงื่อนไขตามที่กฎหมายกำหนด

๔. สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล ท่านมีสิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลของท่าน ทั้งนี้ ในกรณีดังต่อไปนี้

ก. เมื่ออยู่ในช่วงเวลาที่ กรมการปกครอง ทำการตรวจสอบตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สมบูรณ์และเป็นปัจจุบัน

ข. ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้หรือเปิดเผยโดยมิชอบด้วยกฎหมาย

ค. เมื่อข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ที่ กรมการปกครอง ได้แจ้งในการเก็บรวบรวม แต่เจ้าของข้อมูลส่วนบุคคลประสงค์ให้กรมการปกครอง เก็บรักษาข้อมูลนั้นต่อไปเพื่อประกอบการใช้สิทธิตามกฎหมาย

ง. เมื่ออยู่ในช่วงเวลาที่ กรมการปกครอง กำลังพิสูจน์ถึงเหตุอันชอบด้วยกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล หรือตรวจสอบความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะ อันเนื่องมาจากการที่เจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๕. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล ท่านมีสิทธิคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับท่าน เว้นแต่กรณีที่ กรมการปกครอง มีเหตุในการปฏิเสธคำขอโดยชอบด้วยกฎหมาย (เช่น กรมการปกครอง สามารถแสดงให้เห็นว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่านมีเหตุอันชอบด้วยกฎหมายยิ่งกว่า หรือเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องทางกฎหมาย หรือเพื่อประโยชน์สาธารณะของ กรมการปกครอง)

๖. สิทธิในการขอถอนความยินยอม ในกรณีที่ท่านได้ให้ความยินยอมแก่ กรมการปกครองในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ไม่ว่าความยินยอมนั้นจะได้ให้ไว้ก่อนหรือหลังพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลใช้บังคับ) ท่านมีสิทธิถอนความยินยอมเมื่อใดก็ได้ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของท่านถูกเก็บรักษาโดย กรมการปกครอง เว้นแต่มีข้อจำกัดสิทธิโดยกฎหมายให้กรมการปกครองจำเป็นต้องเก็บรักษาข้อมูลต่อไปหรือยังคงมีสัญญาระหว่างท่านกับ กรมการปกครองที่ให้ประโยชน์แก่ท่านอยู่

๗) สิทธิในการขอรับ ส่งหรือโอนข้อมูลส่วนบุคคล ท่านมีสิทธิในการขอรับข้อมูลส่วนบุคคลของท่านจาก กรมการปกครอง ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยวิธีการอัตโนมัติ รวมถึงอาจขอให้กรมการปกครอง ส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น ทั้งนี้ การใช้สิทธินี้จะต้องอยู่ภายใต้เงื่อนไขตามที่กฎหมายกำหนด

/๑๔. การรักษาความมั่นคง...

๑๔. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กรมการปกครอง จะจัดให้มีมาตรการปกป้องข้อมูลส่วนบุคคล โดยกำหนดมาตรการการยืนยันตัวตน (Authentication) กำหนดสิทธิ (Authorization) ในการเข้าถึง การใช้ การเปิดเผย การประมวลผลข้อมูลส่วนบุคคลตามมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการปกครอง โดยการจำกัดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลให้สามารถเข้าถึงได้โดยเจ้าหน้าที่เฉพาะรายหรือบุคคลที่มีอำนาจหน้าที่หรือได้รับมอบหมายที่มีความจำเป็นต้องใช้ข้อมูลดังกล่าวตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้แล้ว หรือตามที่ระเบียบกฎหมายกำหนดเท่านั้น ซึ่งบุคคลดังกล่าวจะต้องยึดมั่นและปฏิบัติตามมาตรการปกป้องข้อมูลส่วนบุคคล ของกรมการปกครอง อย่างเคร่งครัด ตลอดจนมีหน้าที่รักษาความลับของข้อมูลส่วนบุคคลที่ตนเองรับรู้จากการปฏิบัติการตามอำนาจหน้าที่ นอกจากนี้ เมื่อ กรมการปกครองมีการส่ง โอนหรือเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สาม ไม่ว่าเพื่อการให้บริการตามพันธกิจ ตามสัญญา หรือข้อตกลงในรูปแบบอื่นกรมการปกครอง จะกำหนดมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลและ การรักษาความลับที่เหมาะสมและเป็นไปตามที่กฎหมายกำหนด

๑๕. การให้บริการโดยบุคคลที่สามหรือผู้ให้บริการช่วง

กรมการปกครอง อาจมีการมอบหมายหรือจัดซื้อจัดจ้างบุคคลที่สาม (ผู้ประมวลผลข้อมูลส่วนบุคคล) ให้ทำการประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของกรมการปกครองซึ่งบุคคลที่สามดังกล่าวอาจเสนอบริการในลักษณะต่าง ๆ เช่น การเป็นผู้ดูแล (Hosting) รับงานบริการช่วง (Outsourcing) หรือเป็นผู้ให้บริการคลาวด์ (Cloud computing service/provider) หรือเป็นงานในลักษณะการจ้างทำของในรูปแบบอื่น การมอบหมายให้บุคคลที่สามทำการประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลนั้น กรมการปกครอง จะจัดให้มีข้อตกลงระบุสิทธิและหน้าที่ของ กรมการปกครอง ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและของบุคคลที่ กรมการปกครอง มอบหมายในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งรวมถึงกำหนดรายละเอียดประเภทข้อมูลส่วนบุคคลที่ กรมการปกครอง มอบหมายให้ประมวลผล รวมถึงวัตถุประสงค์ ขอบเขตในการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงอื่น ๆ ที่เกี่ยวข้อง ซึ่งผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามขอบเขตที่ระบุในข้อตกลงและตามคำสั่งของกรมการปกครอง เท่านั้นโดยไม่สามารถประมวลผลเพื่อวัตถุประสงค์อื่นได้ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลมีการมอบหมายผู้ให้บริการช่วง (ผู้ประมวลผลช่วง) เพื่อทำการประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้ กรมการปกครอง จะกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเอกสารข้อตกลงระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผลช่วง ในรูปแบบและมาตรฐานที่ไม่ต่ำกว่าข้อตกลงระหว่าง กรมการปกครอง กับผู้ประมวลผลข้อมูลส่วนบุคคล

๑๖. การเข้าถึงข้อมูลส่วนบุคคล

กรมการปกครอง ได้กำหนดให้ผู้ปฏิบัติงาน กรมการปกครอง ที่มีอานาจหน้าที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามประกาศนี้เท่านั้นที่จะสามารถเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ โดยกรมการปกครอง จะดำเนินการให้ผู้ปฏิบัติงานดังกล่าวปฏิบัติตามประกาศนี้อย่างเคร่งครัด

๑๗. ป้องกันการสูญหายของข้อมูลส่วนบุคคล

๑๗.๑ กรมการปกครองได้เลือกใช้บริการระบบคลาวด์กลางภารัฐ ซึ่งผู้ให้บริการระบบคลาวด์กลางภาครัฐได้มีแนวทางการสำรองข้อมูลเป็นประจำทุกวัน ๆ ละ ๑ ครั้ง โดยเก็บไว้บนระบบสำรองข้อมูลเฉพาะและในสถานที่เก็บที่เป็นห้องมั่นคงปลอดภัย

/๒. กรมการปกครอง...

๑๗.๒ กรมการปกครอง จะจัดให้มีมาตรฐานการักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๗ โดยได้ดำเนินการตามมาตการอย่างเคร่งครัด

๑๘. การเชื่อมต่อเว็บไซต์หรือบริการภายนอก

๑๘.๑ การเชื่อมโยงยังเว็บไซต์หรือบริการอื่นเป็นเพียงการให้บริการเพื่ออำนวยความสะดวกแก่ผู้ใช้บริการเท่านั้น กรมการปกครองมิได้มีส่วนเกี่ยวข้องหรือมีอำนาจควบคุมรับรองความถูกต้อง ความน่าเชื่อถือตลอดจนความรับผิดชอบในเนื้อหาข้อมูลของเว็บไซต์หรือบริการนั้น ๆ และกรมการปกครองไม่รับผิดชอบต่อเนื้อหาใด ๆ ที่แสดงบนเว็บไซต์หรือบริการอื่นที่เชื่อมโยงมายังเว็บไซต์หรือบริการของกรมการปกครอง หรือต่อความเสียหายใด ๆ ที่เกิดขึ้นจากการเข้าเยี่ยมชมเว็บไซต์หรือบริการดังกล่าว

๑๘.๒ กรณีต้องการเชื่อมโยงมายังเว็บไซต์ของกรมการปกครอง ผู้ใช้บริการสามารถเชื่อมโยงมายังหน้าแรกของเว็บไซต์กรมการปกครองได้ โดยแจ้งความประสงค์เป็นหนังสือ แต่หากต้องการเชื่อมโยงมายังหน้าภายในของเว็บไซต์นี้จะต้องได้รับความยินยอมเป็นหนังสือจากกรมการปกครองเท่านั้น และในการให้ความยินยอมดังกล่าว กรมการปกครองขอสงวนสิทธิที่จะกำหนดเงื่อนไขใด ๆ ไว้ด้วยก็ได้ ในการที่เว็บไซต์ที่เชื่อมโยงมายังเว็บไซต์ของกรมการปกครอง กรมการปกครองจะไม่รับผิดชอบต่อเนื้อหาใด ๆ ที่แสดงบนเว็บไซต์ที่เชื่อมโยงมายังเว็บไซต์ของกรมการปกครอง หรือต่อความเสียหายใด ๆ ที่เกิดขึ้นจากการใช้เว็บไซต์นั้น

๑๙. การร้องขอให้ลบหรือทำลายข้อมูลส่วนบุคคล

ท่านสามารถแจ้งให้กรมการปกครองลบหรือทำลายข้อมูลส่วนบุคคลของท่าน รวมถึงสิทธิในการขอถอนความยินยอม เมื่อใดก็ได้ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของท่านถูกเก็บรักษาโดยกรมการปกครอง เว้นแต่มีขอจำกัดสิทธิโดยกฎหมายให้กรมการปกครองจำเป็นต้องเก็บรักษาข้อมูลต่อไป

๒๐. โทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล

การไม่ปฏิบัติตามนโยบายอาจมีผลเป็นความผิดและถูกลงโทษทางวินัยตามกฎเกณฑ์ของกรมการปกครอง (สำหรับเจ้าหน้าที่หรือผู้ปฏิบัติงานของ กรมการปกครอง) หรือตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล) ทั้งนี้ ตามแต่กรณีและความสัมพันธ์ที่ท่านมีต่อกรมการปกครอง และอาจได้รับโทษตามที่กำหนดโดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งกฎหมายลำดับรอง กฎ ระเบียบ คำสั่งที่เกี่ยวข้อง

๒๑. การร้องเรียนต่อหน่วยงานผู้มีอำนาจกำกับดูแล

ในกรณีที่ท่านพบว่า กรมการปกครอง มิได้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านมีสิทธิร้องเรียนไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือหน่วยงานที่มีอำนาจกำกับดูแลที่ได้รับการแต่งตั้งโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือตามกฎหมาย ทั้งนี้ ก่อนการร้องเรียนดังกล่าว กรมการปกครอง ขอให้ท่านโปรดติดต่อมายัง กรมการปกครอง เพื่อให้ กรมการปกครอง มีโอกาสได้รับทราบข้อเท็จจริงและได้ชี้แจงในประเด็นต่าง ๆ รวมถึงจัดการแก้ไขข้อกังวลของท่านก่อนในโอกาสแรก

๒๒. การปรับปรุงแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล

กรมการปกครอง อาจพิจารณาปรับปรุง แก้ไขหรือเปลี่ยนแปลงนโยบายนี้ตามที่เห็นสมควร และจะทำการแจ้งให้ท่านทราบผ่านช่องทางเว็บไซต์ www.dopa.go.th โดยมีวันที่มีผลบังคับใช้ของแต่ละฉบับแก้ไขกำกับอยู่ อย่างไรก็ดี กรมการปกครอง ขอแนะนำให้ท่านโปรดตรวจสอบเพื่อรับทราบนโยบายฉบับใหม่อย่างสม่ำเสมอ ผ่านแอปพลิเคชัน หรือช่องทางเฉพาะกิจกรรมที่ กรมการปกครอง ดำเนินการ โดยเฉพาะก่อนที่ท่านจะทำการเปิดเผยข้อมูลส่วนบุคคลแก่กรมการปกครอง

/การรับบริการ...

การรับบริการของ กรมการปกครอง ภายหลังการบังคับใช้นโยบายใหม่ ถือเป็นการรับทราบตามข้อตกลงในนโยบายใหม่แล้ว ทั้งนี้ โปรดหยุดการเข้าใช้งานหากท่านไม่เห็นด้วยกับรายละเอียดในนโยบายฉบับนี้และโปรดติดต่อมายัง กรมการปกครอง เพื่อชี้แจงข้อเท็จจริงต่อไป

๒๓. การติดต่อสอบถามหรือใช้สิทธิ

หากท่านมีข้อสงสัย ข้อเสนอแนะหรือข้อกังวลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของ กรมการปกครอง หรือเกี่ยวกับนโยบายนี้ หรือท่านต้องการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านสามารถติดต่อสอบถามได้ที่

๑. **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** กรมการปกครอง
รองอธิบดีกรมการปกครอง ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ
๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : dpo@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๘๒-๑๐๔๗

๒. **ผู้ควบคุมข้อมูลส่วนบุคคล** กรมการปกครอง
๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : webmaster@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๒๔๑-๐๑๕๑-๘

ประกาศสำนักบริหารการทะเบียน
เรื่อง นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
ของสำนักบริหารการทะเบียน
พ.ศ. ๒๕๖๕

โดยที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ประกาศกำหนดนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ. ๒๕๕๓ เพื่อให้หน่วยงานของรัฐที่มีการจัดเก็บ รวบรวม และเผยแพร่ข้อมูลส่วนบุคคล ได้กำหนดแนวทางและแนวปฏิบัติที่ชัดเจน มีความมั่นคง ปลอดภัย น่าเชื่อถือ และมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๖ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ผู้อำนวยการสำนักบริหารการทะเบียน จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักบริหารการทะเบียน เรื่อง นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักบริหารการทะเบียน พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ นโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล มีรายละเอียดปรากฏตามที่แนบท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๕

(นายสุชาติ ธานีรัตน์)
ผู้อำนวยการสำนักบริหารการทะเบียน

นโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

คำนิยาม

"ข้อมูลทะเบียนราษฎร" หมายความว่า ข้อมูลของบุคคลที่แสดงออกในรูปของเอกสาร ภาพ หรือข้อมูลดิจิทัลโดยมีรายการตามที่ปรากฏในทะเบียนบ้าน เช่น ชื่อตัว ชื่อรอง ชื่อสกุล วันเดือนปีเกิด เลขประจำตัวประชาชน สัญชาติ สถานะเจ้าบ้าน ชื่อบิดา ชื่อมารดา ที่อยู่ตามทะเบียนบ้าน เป็นต้น ทะเบียนการเกิด ทะเบียนการตาย รวมถึงทะเบียนประวัติของคนซึ่งไม่มีสัญชาติไทย"

"ข้อมูลทะเบียนประวัติราษฎร" หมายความว่า ข้อมูลของบุคคลที่แสดงออกในรูปของเอกสาร ภาพหรือข้อมูลดิจิทัลโดยมีรายการตามที่ปรากฏในข้อมูลทะเบียนราษฎรและข้อมูลอื่นที่บ่งบอกถึงสถานภาพและตัวบุคคลที่เป็นเจ้าของทะเบียนประวัติ เช่น ภาพใบหน้า ลายพิมพ์นิ้วมือ สถานภาพการสมรส ชื่อคู่สมรส ชื่อบุตร ชื่อบุตรบุญธรรมหรือผู้รับบุตรบุญธรรม ศาสนา วุฒิการศึกษา อาชีพ ภูมิลำเนาตามทะเบียนบ้าน ผลการตรวจสารพันธุกรรม หรือ ดีเอ็นเอ เป็นต้น

"บุคคล" หมายความว่า บุคคลธรรมดา

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลธรรมดาที่ทำให้ระบุตัวเจ้าของข้อมูลได้ ไม่ว่าทางตรงหรือทางอ้อม ซึ่งเป็นข้อมูลที่สามารถแยกแยะตัวเจ้าของข้อมูลออกจากบุคคลอื่น สามารถติดตามพฤติกรรมของเจ้าของข้อมูล หรือสามารถเชื่อมโยงกับชุดข้อมูลอื่นแล้วทำให้สามารถระบุตัวเจ้าของข้อมูลได้ ทั้งนี้ ให้รวมถึงข้อมูลทะเบียนราษฎรและข้อมูลทะเบียนประวัติราษฎร ด้วย

"เจ้าของข้อมูล" หมายความว่า บุคคลที่เป็นเจ้าของข้อมูลที่สามารถระบุตัวตนไปถึงได้

"ผู้ควบคุมข้อมูลส่วนบุคคล" หมายความว่า สำนักทะเบียนกลาง รวมถึง สำนักทะเบียนจังหวัด สำนักทะเบียนกรุงเทพมหานคร สำนักทะเบียนอำเภอ สำนักทะเบียนท้องถิ่น และส่วนราชการหรือหน่วยงานของรัฐ ซึ่งเป็นผู้จัดทำ เก็บ รวบรวม และใช้ข้อมูลเกี่ยวกับบุคคล รวมถึงการใช้ข้อมูลทะเบียนราษฎรหรือข้อมูลทะเบียนประวัติราษฎรจากผู้ควบคุมข้อมูล และนำข้อมูลนั้นไปใช้ประโยชน์

"ผู้รับข้อมูล" หมายความว่า บุคคลหรือนิติบุคคลที่ได้รับข้อมูลจากผู้ควบคุมข้อมูล และนำข้อมูลนั้นไปใช้ประโยชน์

"เชื่อมโยงคอมพิวเตอร์" หมายความว่า การเชื่อมระบบคอมพิวเตอร์ของส่วนราชการหรือหน่วยงานของรัฐกับสำนักทะเบียนกลางเพื่อใช้ประโยชน์จากฐานข้อมูลทะเบียนกลางและฐานข้อมูลประชาชนของส่วนราชการหรือหน่วยงานของรัฐนั้น

"ฐานข้อมูลทะเบียนกลาง" หมายความว่า ฐานข้อมูลทะเบียนราษฎร ฐานข้อมูลทะเบียนครอบครัว ฐานข้อมูลทะเบียนชื่อบุคคล และฐานข้อมูลทะเบียนบัตรประจำตัวประชาชน

"Log files" หมายความว่า ข้อมูลจราจรคอมพิวเตอร์ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

๑. ข้อมูลทั่วไป

สำนักบริหารการทะเบียน มีอำนาจหน้าที่เกี่ยวกับการดำเนินงานตามกฎหมายว่าด้วยการทะเบียนราษฎร บัตรประจำตัวประชาชน ทะเบียนครอบครัว และการทะเบียนอื่น ๆ ที่อยู่ในความรับผิดชอบของกรมการปกครอง ทั้งนี้ ในการเก็บรวบรวมข้อมูลส่วนบุคคลได้ดำเนินการตามบทบัญญัติภายใต้พระราชบัญญัติ

/การทะเบียน...

การทะเบียนราษฎร พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม โดยใช้เลขประจำตัวประชาชน ๑๓ หลัก เป็นดัชนีในการจัดเก็บข้อมูลเพื่อการบริการประชาชน ณ สำนักทะเบียนอำเภอ สำนักทะเบียนท้องถิ่น สำนักทะเบียนไทยในต่างประเทศ และหน่วยบริการประชาชนอื่นที่ต้องมีงานบริการประชาชน เช่น หน่วยบริการเคลื่อนที่ หน่วยบริการ “อำเภอ..ยิ้ม” และหน่วยบริการอื่นๆ ทั้งนี้ นอกจากการให้บริการประชาชนโดยตรงแล้ว สำนักทะเบียนกลางยังอนุญาตให้ส่วนราชการหรือหน่วยงานของรัฐเชื่อมโยงข้อมูล เพื่อใช้ประโยชน์จากฐานข้อมูลทะเบียนกลางในการนำข้อมูลส่วนบุคคลไปบริการประชาชนหรือการปฏิบัติงานตามหน้าที่อีกด้วย โดยภายใต้บทบัญญัติแห่งพระราชบัญญัติการทะเบียนราษฎร พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติมทุกฉบับ และการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (Linkage Center) ตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๕ มีนาคม ๒๕๕๙ รวมทั้งการอนุญาตให้ส่วนราชการและหน่วยงานเอกชนใช้โปรแกรมอ่านข้อมูลจากบัตรประจำตัวประชาชนแบบอเนกประสงค์ (Smart Card) ตามประกาศกรมการปกครอง ลงวันที่ ๘ ตุลาคม ๒๕๖๑ ด้วย

๒. การเก็บรวบรวมข้อมูลส่วนบุคคล

๒.๑ สำนักบริหารการทะเบียนจะเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็น และภายใต้กรอบของกฎหมาย ซึ่งประกอบด้วยพระราชบัญญัติการทะเบียนราษฎร พระราชบัญญัติบัตรประจำตัวประชาชน พระราชบัญญัติชื่อบุคคล กฎหมายที่เกี่ยวข้องกับทะเบียนครอบครัว และระเบียบอื่นๆ ที่เกี่ยวข้อง เพื่อประโยชน์ต่อการบริการประชาชนด้านการทะเบียน สำนักบริหารการทะเบียนอาจเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง เฉพาะกรณีที่มีความจำเป็น เพื่อปรับปรุงข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน และหรือปรับปรุงคุณภาพและประสิทธิภาพการให้บริการของสำนักบริหารการทะเบียน โดยจะแจ้งถึงการจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ

๒.๒ ในกรณีการให้บริการทางเว็บไซต์ สำนักบริหารการทะเบียน จะจัดเก็บบันทึกข้อมูลการเข้าออกเว็บไซต์โดยระบบอัตโนมัติเพื่อวัตถุประสงค์ในการวิเคราะห์และติดตามการใช้บริการทางเว็บไซต์และการตรวจสอบย้อนหลัง ในกรณีที่เกิดปัญหาการใช้งาน โดยจะจัดเก็บรักษาข้อมูลดังกล่าวไว้ตามระยะเวลาเท่าที่จำเป็น

๒.๓ ในกรณีการให้บริการผ่านช่องทางอื่น เช่น โมบายแอปพลิเคชั่น เป็นต้น จะเก็บข้อมูลส่วนบุคคลเฉพาะที่ได้รับความยินยอมจากเจ้าของข้อมูลเท่านั้น ส่วนแนวทางหรือวิธีการยินยอมให้เป็นไปตามที่สำนักบริหารการทะเบียนกำหนด

๒.๔ สำนักบริหารการทะเบียน จะไม่จัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกัน เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดเจนเท่านั้น หรือข้อยกเว้นตามที่กฎหมายกำหนด

๓. คุณภาพของข้อมูลส่วนบุคคลหรือธรรมาภิบาลข้อมูล

ข้อมูลส่วนบุคคลที่สำนักบริหารการทะเบียนจัดเก็บไว้ในฐานข้อมูลทะเบียนกลาง เป็นข้อมูลที่เจ้าของข้อมูลมีอยู่แล้วส่วนหนึ่งที่ปรากฏตามเอกสารของประชาชน เช่น สำเนาทะเบียนบ้าน บัตรประจำตัวประชาชน ทะเบียนสมรส สูติบัตร เป็นต้น ซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลถืออยู่จะตรงกับข้อมูลส่วนบุคคลที่สำนักบริหารการทะเบียนจัดเก็บไว้ในฐานข้อมูลทะเบียนกลาง หากจะมีการแก้ไขข้อมูล เช่น การเปลี่ยนชื่อตัว

/ชื่อสกุล...

ชื่อสกุล แจ้งการย้ายที่อยู่ เป็นต้น และข้อมูลที่มีการแก้ไขจะถูกแก้ไขด้วยระบบคอมพิวเตอร์ออนไลน์แบบทันทีทันใด ประกอบกับข้อมูลส่วนบุคคลได้มีการเชื่อมโยงข้อมูลไปยังหลายหน่วยงานเพื่อบริการประชาชน ทำให้เกิดการตรวจสอบข้อมูลจากหลายแหล่ง ข้อมูลจึงมีความถูกต้องและเป็นปัจจุบันเสมอ ทั้งนี้ สำนักบริหารการทะเบียน ได้มีการออกประกาศกระทรวงมหาดไทย เรื่อง จรรยาบรรณข้าราชการและผู้ปฏิบัติงานทะเบียน พ.ศ. ๒๕๔๕

๔. การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

๔.๑ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล เป็นไปตามระเบียบสำนักทะเบียนกลางว่าด้วยการคุ้มครองและจัดการข้อมูลทะเบียนประวัติราษฎร พ.ศ. ๒๕๖๑ ลงวันที่ ๘ ตุลาคม ๒๕๖๑

ทั้งนี้ สำนักบริหารการทะเบียนจะรักษาข้อมูลของการใช้บริการดังกล่าวข้างต้นไว้เป็นความลับ เว้นแต่กรณีที่กฎหมายกำหนด และ/หรือในกรณีอื่น ๆ ตามที่กำหนดไว้ในนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

๔.๒ การให้บริการเว็บไซต์ สำนักบริหารการทะเบียน (https://www.bora.dopa.go.th/) มีการเก็บบันทึกเข้าออกเว็บไซต์ของผู้ใช้บริการ (Log Files) โดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคลได้ เช่น หมายเลขไอพี (IP Address) เว็บไซต์ที่เข้าออกก่อนและหลัง และประเภทของโปรแกรมบราวเซอร์ (Browser) เป็นต้น ทั้งนี้ เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๑) การใช้คุกกี้ (Cookies) หมายถึงไฟล์ข้อมูลขนาดเล็กที่จะถูกส่งไปเก็บไว้ยังโปรแกรมค้นดูเว็บ (Web browser) ของผู้รับบริการ เพื่อเก็บข้อมูลที่ผู้ใช้บริการเข้าเยี่ยมชมไว้ เมื่อผู้ใช้บริการมีการเข้าไปเยี่ยมชมเว็บไซต์ต่าง ๆ อีกครั้งในภายหลัง โปรแกรมค้นดูเว็บจะจดจำได้ว่าผู้ใช้บริการเคยเข้าเยี่ยมชมแล้วจนกว่าผู้รับบริการจะออกจากโปรแกรมค้นดูเว็บไซต์ หรือจนกว่าผู้ใช้บริการจะลบ “คุกกี้” นั้น หรือไม่อนุญาตให้ “คุกกี้” นั้น ทำงานอีกต่อไป เว็บไซต์ของสำนักบริหารการทะเบียน (https://www.bora.dopa.go.th/) ไม่มีการใช้คุกกี้ (Cookies) เชื่อมโยงข้อมูลส่วนบุคคลของผู้ใช้บริการ แต่จะนำข้อมูลคุกกี้ (Cookies) ได้บันทึกหรือเก็บรวบรวมไว้ไปใช้ในการวิเคราะห์เชิงสถิติหรือในกิจกรรมอื่นของเว็บไซต์ เพื่อปรับปรุงคุณภาพให้บริการของเว็บไซต์ต่อไป

(๒) บันทึกข้อมูลผู้เข้าชมเว็บไซต์ (Log Files) หมายถึงไฟล์ข้อมูลจราจรคอมพิวเตอร์แสดงถึงแหล่งกำเนิดต้นทางปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

(๓) การจัดเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information) เว็บไซต์ของสำนักบริหารการทะเบียน (https://www.bora.dopa.go.th/) ไม่มีการจัดเก็บข้อมูลทางสถิติเกี่ยวกับประชากร (Demographic Information) ที่สามารถเชื่อมโยงกับข้อมูลส่วนบุคคลได้

๕. การรักษาความมั่นคงปลอดภัย

สำนักบริหารการทะเบียน จะรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย การเข้าถึง การใช้การเปลี่ยนแปลง การแก้ไข รวมถึงการเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิ

/หรือไม่ชอบ...

หรือไม่ชอบด้วยกฎหมายด้วยการกำหนดมาตรการเชิงเทคนิคและเชิงบริหารจัดการ วิธีปฏิบัติ และสิทธิในการเข้าถึงข้อมูลส่วนบุคคลให้เป็นไปตามที่กฎหมายกำหนด และหรือสอดคล้องกับมาตรฐานสากล

สำนักบริหารการทะเบียน จะมีการกำหนดมาตรการต่าง ๆ เพื่อคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพและปลอดภัยตามมาตรฐานที่กฎหมายกำหนด ดังนี้

๕.๑ เงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคล เช่น การกำหนดชั้นความลับ วิธีการเข้าถึงข้อมูล และการจำกัดการเข้าถึงข้อมูล เป็นต้น

๕.๒ กระบวนการรองรับการเก็บรักษาข้อมูลส่วนบุคคลทางกายภาพ จัดให้มีสถานที่ที่เหมาะสมและปลอดภัยในการจัดเก็บข้อมูลหรือเอกสารต่าง ๆ และกำหนดกระบวนการลบหรือทำลายข้อมูลและอุปกรณ์เมื่อหมดความจำเป็นหรือได้รับการร้องขอจากเจ้าของข้อมูล

๕.๓ กระบวนการรองรับการเก็บรักษาข้อมูลส่วนบุคคลด้วยระบบเทคโนโลยีสารสนเทศ เช่น การแฝงข้อมูล (Pseudonymization) การจัดทำข้อมูลนิรนาม (Anonymization) และการเข้ารหัสข้อมูล (Encryption) เป็นต้น

๕.๔ กำหนดแผนการรับมือและแก้ไข กรณีการรั่วไหล หรือการละเมิดข้อมูลส่วนบุคคล

๕.๕ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการ เพื่อรักษาความมั่นคงปลอดภัยในการดำเนินงานที่เกี่ยวกับข้อมูลส่วนบุคคลให้เหมาะสมกับการบริหารความเสี่ยงของสำนักบริหารการทะเบียน ตามมาตรฐานสากล

๖. สิทธิของเจ้าของข้อมูล

เจ้าของข้อมูลสามารถร้องขอให้สำนักบริหารการทะเบียน ดำเนินการตามสิทธิของเจ้าของข้อมูล ดังนี้

๖.๑ สิทธิในการเข้าถึงข้อมูลส่วนบุคคล เจ้าของข้อมูลสามารถยื่นคำร้องขอเข้าถึงข้อมูลส่วนบุคคลหรือชี้แจงถึงการได้มาของข้อมูลส่วนบุคคลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม โดยสำนักบริหารการทะเบียนจะจัดเตรียมหรือจัดทำสำเนาข้อมูลส่วนบุคคลและข้อมูลที่เกี่ยวข้องตามช่องทางการสื่อสารของสำนักบริหารการทะเบียน ทั้งนี้ สำนักบริหารการทะเบียน ขอสงวนสิทธิ์ในการปฏิเสธคำร้องขอ หากไม่เป็นไปตามที่กฎหมายกำหนด หรือตามคำสั่งศาลหรือการเข้าถึงข้อมูลส่วนบุคคลนั้นอาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

๖.๒ สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เจ้าของข้อมูลสามารถยื่นคำร้องขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องตรงกับความเป็นจริงเป็นปัจจุบัน ครบถ้วนสมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด โดยจะต้องนำหลักฐานหรือเอกสารที่เกี่ยวข้องมาแสดง หากสำนักบริหารการทะเบียน เห็นว่าการขอแก้ไขข้อมูลนั้นไม่มีเหตุผลเพียงพอ สำนักบริหารการทะเบียน จะปฏิเสธคำร้องขอของเจ้าของข้อมูลและจะบันทึกเหตุผลในการปฏิเสธคำร้องขอไว้เป็นหลักฐาน

๖.๓ สิทธิในการลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวเจ้าของข้อมูลได้ เจ้าของข้อมูลสามารถยื่นคำร้องขอลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนเจ้าของข้อมูลได้โดย สำนักบริหารการทะเบียนจะดำเนินการตามคำร้องขอภายใต้เงื่อนไข ดังนี้

(๑) เมื่อหมดความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลตามวัตถุประสงค์

/(๒) เจ้าของข้อมูล...

(๒) เจ้าของข้อมูลเพิกถอนความยินยอม และสำนักบริหารการทะเบียน ไม่มีอำนาจตามกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๓) เจ้าของข้อมูลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการปฏิบัติภารกิจของรัฐและเพื่อประโยชน์อันชอบธรรม และสำนักบริหารการทะเบียน ไม่สามารถปฏิเสธการคัดค้านได้

(๔) ข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้ เปิดเผย โดยไม่ชอบด้วยกฎหมาย

๖.๔ ความในข้อ ๖.๓ มิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือหอจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ หรือเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสาธารณสุขหรือสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์หรือประโยชน์สาธารณะด้านการสาธารณสุข หรือการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมายซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

๖.๕ สิทธิในการเพิกถอนความยินยอม กรณีเจ้าของข้อมูลได้ให้ความยินยอมไว้กับ สำนักบริหารการทะเบียน เจ้าของข้อมูลสามารถยื่นคำร้องขอเพิกถอนความยินยอมนั้นได้ โดยสำนักบริหารการทะเบียนจะดำเนินการตามคำร้องขอของเจ้าของข้อมูล แต่ไม่รวมถึงการดำเนินการอื่นใดที่ได้กระทำก่อนที่จะมีการใช้สิทธิเพิกถอนความยินยอม ทั้งนี้ สำนักบริหารการทะเบียน มีสิทธิปฏิเสธคำร้องขอ หากมีข้อจำกัดสิทธิในการเพิกถอนความยินยอมโดยกฎหมาย

๗. ข้อสงวนสิทธิ

สำนักบริหารการทะเบียน ขอสงวนสิทธิในการปฏิเสธคำร้องขอตามข้อ ๖. กรณีดังต่อไปนี้

(๑) กฎหมายกำหนดให้สามารถดำเนินการได้

(๒) ข้อมูลส่วนบุคคลถูกทำให้ ไม่ปรากฏชื่อ หรือบอกลักษณะอันสามารถระบุตัวเจ้าของข้อมูลได้

(๓) ผู้ยื่นคำร้องไม่มีหลักฐานยืนยันว่าเป็นเจ้าของข้อมูลหรือเป็นผู้มีอำนาจในการยื่นคำร้องขอดังกล่าว

(๔) คำร้องขอดังกล่าวไม่สมเหตุสมผล เช่น กรณีที่ผู้ร้องขอไม่มีสิทธิตามกฎหมาย หรือไม่มีข้อมูลส่วนบุคคลนั้นอยู่ที่สำนักบริหารการทะเบียน เป็นต้น

(๕) คำร้องขอดังกล่าวเป็นคำร้องขอฟุ่มเฟือย เช่น เป็นคำร้องขอที่มีลักษณะเดียวกัน หรือมีเนื้อหาเดียวกันซ้ำ ๆ กันโดยไม่มีเหตุอันสมควร เป็นต้น

/๘. การปรับปรุง...

๘. การปรับปรุงนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

(๑) สำนักบริหารการทะเบียนจะปรับปรุงนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของกฎหมายและการดำเนินงานของสำนักบริหารการทะเบียน โดยจะประกาศแจ้งให้ทราบอย่างชัดเจน

(๒) ช่องทางการติดต่อ

การติดต่อระหว่างหน่วยงานของรัฐ สำนักบริหารการทะเบียนจะติดต่อไปยังผู้ใช้บริการ โดยที่ผู้ใช้บริการสามารถเลือกช่องทางการติดต่อกลับได้ เช่น หมายเลขโทรศัพท์สายด่วน (Call Center) ๑๕๔๘ หมายเลขโทรศัพท์ จดหมาย หรืออีเมล (E-mail) ของหน่วยงานที่เกี่ยวข้อง เป็นต้น

สำนักบริหารการทะเบียน เลขที่ ๕๙ หมู่ ๑๑ ถนนลำลูกกาคลอง ๙ ตำบลบึงทองหลาง อำเภอลำลูกกา จังหวัดปทุมธานี ๑๒๑๕๐ โทร ๐ ๒๗๙๑ ๗๐๐๐ เว็บไซต์ (https://www.bora.dopa.go.th/) หรือ Call Center ๑๕๔๘

.....

แนวทางปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล
เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
กรมการปกครอง พ.ศ. ๒๕๖๗

กรมการปกครอง กำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูล (Data Controller) โดยอ้างอิงจากมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีทั้งหมด ๕ ข้อ ดังนี้

มาตรา ๓๗ (๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

แนวทางดังกล่าว กำหนดรายละเอียดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เพื่อให้ข้อมูลส่วนบุคคลมีความปลอดภัยบนพื้นฐาน

๑. การธำรงไว้ซึ่งความลับ (Confidentiallity)
๒. ความถูกต้องครบถ้วน (Integrity) และ
๓. สภาพพร้อมใช้งาน (Availlabillity)

ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยดำเนินการ ดังนี้

๑. มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)
   ๑.๑ มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง
   ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ
   ๑.๒ มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) แบ่งเป็น รูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย
   ๑.๓ ดำเนินการอบรมและสร้างความตระหนักรู้ให้กับบุคลากรในสังกัด
   ๑.๔ แจ้งนโยบายความเป็นส่วนตัว และนโยบายคุ้มครองข้อมูลส่วนบุคคลให้บุคลากรในสังกัดรับทราบและปฏิบัติ
๒. มาตรการป้องกันด้านเทคนิค (technical safeguard)

/๒.๑ จัดให้มี...

๒.๑ จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือ ถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

๒.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการ เข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

๒.๓ จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

๓. มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

๓.๑ มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล้อมรั้วและล็อคประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๓.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

มาตรา ๓๗ (๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

๑. การประเมินก่อนส่งมอบข้อมูล

๑.๑ ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้นใช้เพื่อร้องขอข้อมูลส่วนบุคคล

๑.๒ ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด (เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่ หรือเพียงปี พ.ศ. เกิด และ รหัสไปรษณีย์ ก็เพียงพอ) และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคล (เช่น ชื่อ-นามสกุล เลขประจำตัว ๑๓ หลัก) หรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงต่อการนำไปใช้ประโยชน์หรือไม่

๒. เมื่อส่งมอบข้อมูล

๒.๑ จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

๒.๒ ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

๒.๓ แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

๓. หลังส่งมอบข้อมูล

๓.๑ ติดตามการใช้งานเป็นครั้งคราว เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือ นิติบุคคลนั้น ลบทำลายข้อมูล

๓.๒ กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา

มาตรา ๓๗ (๓) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

๑. มีการติดตามสม่ำเสมอเป็นระยะว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

๒. กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

๓. การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ทั้งนี้ ต้องจัดให้มีมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

มาตรา ๓๗ (๔) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

๑. แจ้งให้พนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ตัวแทนของสำนักงานให้ชัดเจน เช่น การส่งอีเมลล์ และ แจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน
๒. กำหนดวิธีปฏิบัติให้ตัวแทนสำนักงานต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน ๗๒ ชั่วโมง (นับแต่ทราบเหตุ)
๓. การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น
    ๓.๑ ตัวอย่างกรณีความเสี่ยงต่ำ: ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ
    ๓.๒ ตัวอย่างกรณีความเสี่ยงสูง: เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำ การฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์(ตรวจพบ ๑ เดือนหลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน ๗๒ ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย
    ๓.๓ ตัวอย่างกรณีความเสี่ยงต่ำ: เจ้าหน้าที่ของหน่วยงานส่งอีเมลล์ไปยังผู้รับผิดพลาด ซึ่งแนบไฟล์รายชื่อผู้เข้าอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่อีเมลล์ และข้อจำกัดในการทานอาหาร ซึ่งมีเพียง ๒ คน ใน ๑๕ คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลล์ถูกส่งไปยังผู้เข้าอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตาม แม้ข้อมูลสุขภาพ จะถูกเผยแพร่ไปยังผู้ไม่เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิ

และเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

มาตรา ๓๗ (๕) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในข้อนี้ ยังไม่มีความจำเป็นที่ กรมการปกครอง ต้องดำเนินการใด ๆ

หมายเหตุ แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ดำเนินการภายใต้นโยบายรักษาความมั่งคงปลอดภัยระบบสารสนเทศ กรมการปกครอง

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ของกรมการปกครอง พ.ศ. ๒๕๖๗

โดยที่มาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้มีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ เพื่อกำหนดมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับแล้ว ดังนั้น เพื่อให้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของกรมการปกครองสามารถดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ กรมการปกครอง จึงออกมาตรการไว้ ดังต่อไปนี้

ข้อ ๑ ในมาตรการนี้

“เจ้าหน้าที่” หมายความว่า ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างเหมาบริการ และสมาชิกกองอาสารักษาดินแดน ในสังกัดกรมการปกครองไม่ว่าจะมีหน้าที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้มาหรือไม่ก็ตาม ทั้งนี้ ให้รวมถึงบุคคลอื่นใดซึ่งปฏิบัติหน้าที่หรือมีหน้าที่เก็บรักษาข้อมูลส่วนบุคคล ที่ได้มาตามกฎหมายในความรับผิดชอบกรมการปกครอง ด้วย

“ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

ข้อ ๒ เจ้าหน้าที่ต้องตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัย (Privacy and Security Awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล ส่วนบุคคล ระดับความเสี่ยง และทรัพยากรที่ต้องใช้ให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และตามประกาศนี้อย่างเคร่งครัด

ข้อ ๓ เจ้าหน้าที่อาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในมาตรการนี้

/หมวด ๑

หมวด ๑

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ข้อ ๔ เจ้าหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึง หรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อย ต้องประกอบด้วยการดำเนินการ ดังต่อไปนี้

(๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุค

หมวด ๒

มาตรการการป้องกันรั่วไหลข้อมูลส่วนบุคคล

ข้อ ๕ ห้ามทำสำเนาเอกสารระบุตัวตนของผู้รับบริการโดยไม่จำเป็น เช่น บัตรประจำตัวประชาชน หรือ passport ไม่ว่าจะด้วยวิธีการ Xerox , Scan File , Email , Save File , Download , Print , ถ่ายรูปด้วยมือถือ เว้นแต่เป็นการการเก็บเข้าระบบหรือ Storage ของกรมการปกครอง ตามกระบวนการทำงานปกติ หรือเป็นไปตามหลักเกณฑ์ที่กรมการปกครองกำหนด

ข้อ ๖ ให้จัดทำใบรับส่งเอกสาร หรือ Checklist สำหรับการรับส่งเอกสารภายในและภายนอกองค์กรรวมถึงระบุประเภทเอกสารที่ต้องขอจากผู้รับบริการ ให้ผู้รับบริการลงนามต้องมีกระบวนการตรวจสอบความถูกต้อง และปิดผนึกให้เรียบร้อย เพื่อป้องกันการละเมิดหรือล่วงรู้ข้อมูลระหว่างทาง

ข้อ ๗ การจัดส่งเอกสารผ่านช่องทางต่างๆ ให้ดำเนินการ ดังนี้

(๑) ใส่ซองปิดผนึก ระบุผู้รับให้ชัดเจน

(๒) นำส่งด้วยตนเอง หรือผู้ได้รับมอบหมายจาก กรมการปกครอง โดยส่งถึงผู้รับบริการเท่านั้น เว้นแต่จะได้รับอนุญาตเป็นกรณี ๆ ไป

(๓) กรณีผู้ให้บริการภายนอก ต้องเป็นผู้ที่ให้บริการที่ กรมการปกครอง กำหนดเท่านั้น

(๔) กรณีส่งผ่านไปรษณีย์ ต้องส่งแบบปิดผนึก ระบุผู้รับอย่างเจาะจงและต้องมีมาตรการป้องกันการรั่วไหลของข้อมูลอื่นเพิ่มเติม เช่น การปิดบังข้อมูลสำคัญบางส่วนหรือใช้ผู้ให้บริการส่งไปรษณีย์ที่กรมการปกครองกำหนดเท่านั้น

(๕) ต้องมีการติดตามสถานการณ์จัดส่ง โดยเฉพาะกรณีที่เจ้าของข้อมูลมิได้เป็นผู้รับเอง

(๖) ไม่ควรใช้ Line หรือ Email ส่วนตัว ในการปฏิบัติงานหรือการรับทำธุรกรรมใด ๆ ที่มีข้อมูลบุคคล และข้อมูลลับหรือลับมากของกรมการปกครอง

/ข้อ ๘ ให้จัดทำ...

ข้อ ๘ ให้จัดทำทะเบียนการให้ข้อมูลลับหรือลับมาก เพื่อให้สามารถระบุ ติดตาม ตรวจสอบข้อมูลผู้รับได้

ข้อ ๙ ให้ระบุชั้นความลับของเอกสาร ได้แก่ การจัดทำป้ายเพื่อระบุชั้นความลับที่เอกสารแฟ้มและจัดเก็บให้สอดคล้องกับแนวทาง หรือมาตรการบริหารจัดการข้อมูลตามระดับชั้นความลับ

ข้อ ๑๐ ให้จัดทำทะเบียนบันทึก การทำลายเอกสาร และข้อมูลตามทะเบียนซึ่งอาจอยู่ในรูปแบบเอกสารหรือไฟล์ทะเบียน

ข้อ ๑๑ วิธีการทำลายข้อมูลให้ดำเนินการ ดังนี้

(๑) การทำลายเอกสาร ให้ใช้เครื่องย่อยเอกสารชนิดที่ไม่สามารถนำกลับมาประกอบใหม่หรือฉีกเอกสารก่อนหย่อนลงกล่อง

(๒) การลบข้อมูล หรือทำลายข้อมูลตามประเภทสื่อบันทึกข้อมูล จะต้องลบหรือทำลายข้อมูลนั้น ๆ ให้ไม่สามารถกู้คืนข้อมูลกลับมาใช้ได้อีก

ข้อ ๑๒ การบันทึกไฟล์งานให้บันทึกใน CLOUD DRIVE หรือระบบงานที่กรมการปกครองจัดเตรียมไว้ให้เท่านั้น โดยจะต้องมีการดำเนินการจัดเก็บ ดังนี้

(๑) จัดเก็บโดยต้องมีการกำหนดวันที่บันทึกไฟล์

(๒) กำหนดสิทธิการเข้าถึงไฟล์ใน Folder หรือข้อมูลในระบบเฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง

(๓) ต้องมีการเข้ารหัส (Encrypt) ด้วยสำหรับข้อมูลที่มีชั้นความลับ

ข้อ ๑๓ ในกรณีการส่งไฟล์ที่มีข้อมูลที่มีชั้นความลับ หรือลับมากระหว่างกันภายในองค์กรให้ดำเนินการ ดังนี้

(๑) ให้จัดทำเป็น link และส่งให้ผู้ที่ต้องใช้ข้อมูลเข้ามาดูผ่าน link ดังกล่าว

(๒) หากไม่สามารถดำเนินการตาม (๑) ได้ และมีความจำเป็นจะต้องส่งเป็นไฟล์ให้ดำเนินการ Encrypt ไฟล์ก่อนส่งทุกครั้ง โดยขอให้พิจารณาปิดบังข้อมูลบางส่วน และส่งเฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้นกรณีเป็นผู้รับไฟล์ให้ปฏิบัติตามข้อ ๕ คือห้ามทำสำเนาหรือบันทึกข้อมูลเก็บไว้หลายแห่งเกินความจำเป็น

ข้อ ๑๔ การใช้และและบันทึกไฟล์ข้อมูลลับ ให้ดำเนินการ ดังนี้

(๑) กรณีมีความจำเป็นต้องใช้ข้อมูล ให้ย้ายไปเก็บอยู่ใน CLOUD DRIVE หรือระบบงานที่กรมการปกครองจัดเตรียมไว้ให้

(๒) กรณีต้องการเก็บไฟล์งานไว้ใช้อ้างอิงใน Folder ส่วนตัว ให้ดำเนินการนำข้อมูลส่วนบุคคลออกก่อน และให้จัดเก็บได้ตามระยะเวลาที่ฝ่ายงานกำหนดหรือลบทิ้งเมื่อไม่ต้องใช้งานแล้ว

(๓) กรณีมีความจำเป็นต้องบันทึกไฟล์ที่มีข้อมูลส่วนบุคคล ออกมาใช้งานบน Drive C , Drive D เช่น กรณีการทำงานบน Microsoft Office Online ให้ทำได้เฉพาะกับกรณีใช้เครื่องคอมพิวเตอร์ของกรมการปกครองเท่านั้น

(๔) เมื่อทำงานเสร็จ และได้บันทึกไฟล์เข้าไปใน CLOUD DRIVE แล้วต้องลบไฟล์ที่บันทึกไว้ในเครื่องคอมพิวเตอร์ทุกครั้งและหมั่นลบไฟล์ที่อยู่ในเครื่องทุกปี

Logo คู่สัญญา

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล กรมการปกครอง

โครงการ.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือหรือสัญญาฉบับหลัก)....

ระหว่าง

กรมการปกครอง กับ.....(ชื่อคู่สัญญา).....

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ทำขึ้น เมื่อวันที่.... (ระบุวันที่ลงนามในข้อตกลง)..... ณ กรมการปกครอง กระทรวงมหาดไทย

โดยที่ กรมการปกครอง ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “ปค.” ฝ่ายหนึ่ง ได้ตกลงใน....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).... ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “(บันทึกความร่วมมือ/สัญญา)” กับ ..... (ระบุชื่อคู่สัญญา)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “.....(ระบุชื่อเรียกคู่สัญญา.....” อีกฝ่ายหนึ่ง

ตาม (ระบุชื่อบันทึกความร่วมมือ/สัญญาหลัก) ดังกล่าวกำหนดให้ ปค. มีหน้าที่และความรับผิดชอบในส่วนของการ.....(ระบุขอบเขต สิทธิ หน้าที่ของ ปค. ตามบันทึกความร่วมมือ/สัญญาหลัก)..... ซึ่งในการดำเนินการดังกล่าวประกอบด้วยการมอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา).....เป็นผู้ดำเนินการกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคลแทนหรือในนามของ ปค.

ปค. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีอำนาจตัดสินใจ กำหนดรูปแบบและกำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ได้.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้..... (ระบุชื่อคู่สัญญา).....ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. ..... (ระบุวัตถุประสงค์ที่ ปค. มอบหมายให้คู่สัญญาดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล เช่น เพื่อการรับจ้างทำระบบยืนยันตัวตน เพื่อการรับทำ Survey เพื่อการลงทะเบียนผู้เข้าร่วมอบรม เพื่อการรับจ้างพิมพ์บัตรพนักงาน เพื่อการรับส่งเอกสาร เป็นต้น).....

โดยข้อมูลส่วนบุคคลที่ ปค. มอบหมาย.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้.... (ระบุชื่อคู่สัญญา).....ประมวลผล ประกอบด้วย

๑. ..... (ระบุรายการข้อมูลส่วนบุคคลที่ ปค. มอบหมาย/เปิดเผยให้คู่สัญญาประมวลผล เช่น ชื่อ นามสกุลของเจ้าหน้าที่ เบอร์โทรศัพท์ ข้อมูลผู้ใช้งานแอปพลิเคชั่น รายชื่อผู้เข้าร่วมงานสัมมนา เป็นต้น).....

ด้วยเหตุนี้ ทั้งสองฝ่ายจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือข้อตกลงฉบับนี้เป็นส่วนหนึ่ง....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....เพื่อเป็นหลักฐานการควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่ ปค. มอบหมายหรือแต่งตั้งให้.....(ระบุชื่อคู่สัญญา)..... ดำเนินการ อันเนื่องมาจากการดำเนินการตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... และเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๑. ..... (ระบุชื่อคู่สัญญา)..... รับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดย..... (ระบุชื่อคู่สัญญา)..... จะดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

โดยในการดำเนินการตามข้อตกลงนี้ ..... (ระบุชื่อคู่สัญญา).....จะประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก ปค. แล้วเท่านั้น ทั้งนี้ เพื่อให้ปราศจากข้อสงสัย การดำเนินการประมวลผลข้อมูลส่วนบุคคลโดย..... (ระบุชื่อคู่สัญญา).....ตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....ถือเป็นการได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก ปค. แล้ว

๒. ..... (ระบุชื่อคู่สัญญา).....จะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น และจะดำเนินการเพื่อให้พนักงานและ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมายจาก..... (ระบุชื่อคู่สัญญา).....ทำการประมวลผลและรักษาความลับของข้อมูลส่วนบุคคลด้วยมาตรฐานเดียวกัน

๓. ..... (ระบุชื่อคู่สัญญา).....จะควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของการดำเนินการตามข้อตกลงฉบับนี้เท่านั้น โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของบันทึกความร่วมมือหรือสัญญา หรือกฎหมายที่เกี่ยวข้องจะระบุหรือบัญญัติไว้เป็นประการอื่น

๔. ..... (ระบุชื่อคู่สัญญา).....จะดำเนินการเพื่อช่วยเหลือหรือสนับสนุน ปค. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อ ปค. อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตของข้อตกลงฉบับนี้

อย่างไรก็ดี ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อ... (ระบุชื่อคู่สัญญา)..... โดยตรง ..... (ระบุชื่อคู่สัญญา).....จะดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่ ปค. ทันที โดย..... (ระบุชื่อคู่สัญญา).....จะไม่เป็นผู้ตอบสนองต่อคำร้องดังกล่าว เว้นแต่ ปค. จะได้มอบหมายให้..... (ระบุชื่อคู่สัญญา).....ดำเนินการเฉพาะเรื่องที่เกี่ยวข้องกับคำร้องดังกล่าว

๕. ..... (ระบุชื่อคู่สัญญา).....จะจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่..... (ระบุชื่อคู่สัญญา).....ประมวลผลในขอบเขตของข้อตกลงฉบับนี้ และจะดำเนินการส่งมอบบันทึกรายการดังกล่าวให้แก่ ปค. ทุก.....(ระบุความถี่ของการส่งมอบบันทึกรายการ เช่น ทุกสัปดาห์หรือทุกเดือน).... และ/หรือทันทีที่ ปค. ร้องขอ

๖. ..... (ระบุชื่อคู่สัญญา).....จะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศกำหนดและ/หรือตามมาตรฐานสากล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลตามที่กำหนดในข้อตกลงฉบับนี้เป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย เป็นต้น

๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ..... (ระบุชื่อคู่สัญญา)....จะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ทำการประมวลผลภายใต้ข้อตกลงฉบับนี้ภายใน....(ระบุจำนวนวันที่จะทำการลบทำลายข้อมูล)..วันนับแต่วันที่ดำเนินการประมวลผลเสร็จสิ้น หรือวันที่ ปค. และ.... (ระบุชื่อคู่สัญญา).....ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิก....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....แล้วแต่กรณีใดจะเกิดขึ้นก่อน

นอกจากนี้ ในกรณีปรากฏว่า..... (ระบุชื่อคู่สัญญา).....หมดความจำเป็นจะต้องเก็บรักษาข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ก่อนสิ้นระยะเวลาตามวรรคหนึ่ง ..... (ระบุชื่อคู่สัญญา).....จะทำการลบหรือทำลายข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ทันที

๘. กรณีที่..... (ระบุชื่อคู่สัญญา).....พบพฤติการณ์ใด ๆ ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่..... (ระบุชื่อคู่สัญญา).....ประมวลผลภายใต้ข้อตกลงฉบับนี้ ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย แล้ว..... (ระบุชื่อคู่สัญญา).....จะดำเนินการแจ้งให้ ปค. ทราบโดยทันทีภายในเวลาไม่เกิน....(ระบุเวลาเป็นหน่วยชั่วโมงที่คู่สัญญาต้องแจ้งเหตุแก่ ปค. เช่น ภายใน ๒๔ ชั่วโมงหรือ ๔๘ ชั่วโมง ทั้งนี้ไม่ควรเกิน ๔๘ ชั่วโมงเนื่องจาก ปค. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุดังกล่าวแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน ๗๒ ชั่วโมง).... ชั่วโมง

๙. การแจ้งถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นภายใต้ข้อตกลงนี้..... (ระบุชื่อคู่สัญญา)..... จะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่ ปค. ภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนด ดังต่อไปนี้

- รายละเอียดของลักษณะและผลกระทบที่อาจเกิดขึ้นของการละเมิด
- มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด
- ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด หากมีปรากฏ
- ข้อมูลอื่น ๆ เกี่ยวข้องกับการละเมิด

๑๐. หน้าที่และความรับผิดของ..... (ระบุชื่อคู่สัญญา).....ในการปฏิบัติตามข้อตกลงจะสิ้นสุดลงนับแต่วันที่ปฏิบัติงานที่ตกลงเสร็จสิ้น หรือ วันที่..... (ระบุชื่อคู่สัญญา).....และ ปค. ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิก....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....แล้วแต่กรณีใดจะเกิดขึ้นก่อน อย่างไรก็ดี การสิ้นผลลงของข้อตกลงนี้ ไม่กระทบต่อหน้าที่ของ..... (ระบุชื่อคู่สัญญา).....ในการลบหรือทำลายข้อมูลส่วนบุคคลตามที่ได้กำหนดในข้อ ๗ ของข้อตกลงฉบับนี้

ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว เพื่อเป็นหลักฐานแห่งการนี้ ทั้งสองฝ่ายจึงได้ลงนามไว้เป็นหลักฐานต่อหน้าพยาน ณ วัน เดือน ปี ที่ระบุข้างต้น

ลงชื่อ .....
(.....)
ผู้อำนวยการชื่อหน่วยงาน

ลงชื่อ .....
(.....)
ผู้มีอำนาจลงนามของผู้ประมวลผล

ลงชื่อ ..... พยาน
(.....)

ลงชื่อ ..... พยาน
(.....)

ข้อสัญญาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

๑. การใช้และการเก็บรักษาข้อมูล

ผู้ยื่นข้อเสนอตกลงจะเก็บรวบรวมและใช้ข้อมูลใด ๆ ซึ่งรวมถึงข้อมูลของผู้บุคคลซึ่งมีความสัมพันธ์กับกรมการปกครองในปัจจุบัน และอาจมีในอนาคต และข้อมูลที่เป็นความลับของกรมการปกครอง ตลอดจนเอกสารและรายงานต่าง ๆ ไม่ว่าจะจัดทำในรูปแบบใด ที่ผู้ยื่นข้อเสนอได้รับจากกรมการปกครองหรือให้แก่กรมการปกครอง อันเนื่องมาจากการเข้าเสนอราคาหรือประกวดราคาตามขอบเขตการจ้างงานฉบับนี้ และการปฏิบัติตามสัญญาจ้างเฉพาะเพื่อการปฏิบัติตามขอบเขตการจ้างงานและสัญญาจ้างที่ว่าจ้างในครั้งนี้เท่านั้น และจะไม่เปิดเผย เผยแพร่ หรือกระทำด้วยประการ ใด ๆ เพื่อให้ข้อมูลดังกล่าวแก่บุคคลภายนอก หรือใช้ประโยชน์เพื่อการอื่น หรือยินยอมให้ผู้อื่นใช้ประโยชน์จากข้อมูลดังกล่าว ไม่ว่าส่วนหนึ่งส่วนใดหรือทั้งหมด โดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากกรมการปกครอง ทั้งนี้ หน้าที่ดังกล่าวข้างต้นให้มีผลบังคับรวมถึงพนักงาน ลูกจ้าง เจ้าหน้าที่ และ/หรือตัวแทนของผู้ยื่นข้อเสนอด้วย

๒. การส่งคืนหรือทำลายข้อมูล

๒.๑ ผู้ยื่นข้อเสนอตกลงที่จะลบหรือทำลายข้อมูลที่ผู้ยื่นข้อเสนอได้รับจากกรมการปกครอง อันเนื่องมาจากการเข้าเสนอราคาหรือ ประกวดราคาตามขอบเขตการจ้างงานฉบับนี้และการปฏิบัติตามสัญญาจ้าง เพื่อไม่ให้สามารถนำกลับมาใช้ได้อีก รวมถึงสำเนาของข้อมูลที่อาจสื่อความหมายข้อมูลได้ ไม่ว่าจะจัดทำขึ้นหรือถูกเก็บในรูปแบบใด ๆ ภายใน ๗ วัน นับถัดจากวันที่ประกาศผล การคัดเลือกผู้ยื่นข้อเสนอหรือวันที่สัญญาจ้างสิ้นสุดลง ทั้งนี้ ผู้ยื่นข้อเสนอตกลงจะทำหนังสือรับรองว่าผู้ยื่นข้อเสนอได้ ดำเนินการลบหรือทำลายข้อมูลดังกล่าวทั้งหมดแล้ว รวมทั้งตกลงให้กรมการปกครองมีสิทธิในการเข้าตรวจสอบสถานที่ทำการของผู้ยื่นข้อเสนอว่ามีการดำเนินการดังกล่าวแล้ว

๒.๒ ในกรณีที่ผู้ยื่นข้อเสนอได้รับคำบอกกล่าวจากกรมการปกครองให้ส่งลบหรือทำลายข้อมูลก่อนวันที่ประกาศผลการคัดเลือก ผู้ยื่นข้อเสนอหรือวันที่สัญญาจ้างสิ้นสุดลง ผู้ยื่นข้อเสนอตกลงที่จะลบหรือทำลายข้อมูล ภายในระยะเวลาที่กำหนดในคำบอกกล่าว เว้นแต่ในกรณีที่คำบอกกล่าวไม่ได้มีการระบุระยะเวลาไว้ ผู้ยื่นข้อเสนอตกลงที่จะดำเนินการให้แล้วเสร็จภายใน ๗ วัน นับถัดจากวันที่ได้รับคำบอกกล่าวจากกรมการปกครอง

๒.๓ กรมการปกครองมีสิทธิแจ้งให้ผู้ยื่นข้อเสนอทำการส่งคืนข้อมูลแทนการลบหรือทำลายข้อมูลตามข้อ ๒.๑ ได้ โดยผู้ยื่นข้อเสนอ จะต้องดำเนินการส่งคืนข้อมูลให้แก่กรมการปกครองภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้งจากกรมการปกครอง

๓. ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้ยื่นข้อเสนอตกลงที่จะปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของกรมการปกครองรวมถึงนโยบาย คำสั่งและวิธี ปฏิบัติที่เกี่ยวข้องตามที่กำหนดไว้ใน TOR

หมายเหตุ : สามารถ download แบบฟอร์มการประมวลผลข้อมูลส่วนบุคคล ได้ที่ www.dopa.go.th/pdpa

เอกสารแสดงความยินยอม (Consent Form) กรมการปกครอง

วันที่_____

ชื่อบริการ _____

ข้าพเจ้า นาย/นาง/นางสาว _____

❒ “ให้” ความยินยอม ❒ “ไม่ให้” ความยินยอม

ในการ.....(ระบุวัตถุประสงค์ในการขอความยินยอม เช่น กรมการปกครอง เปิดเผยข้อมูลส่วนบุคคลให้คู่ค้าและ/หรือพันธมิตรทางธุรกิจ เพื่อการวิเคราะห์ คัดสรรและนำเสนอผลิตภัณฑ์หรือบริการ สิทธิประโยชน์ รายการส่งเสริมการขาย หรือข้อเสนอต่าง ๆ ของคู่ค้าและ/หรือพันธมิตรนั้น).....

ทั้งนี้ ก่อนการแสดงเจตนา ข้าพเจ้าได้อ่านรายละเอียดจากเอกสารชี้แจงข้อมูล หรือได้รับคำอธิบายจากกรมการปกครอง ถึง**วัตถุประสงค์**ในการเก็บรวบรวม ใช้หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคล และมีความเข้าใจดีแล้ว

ข้าพเจ้าให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารนี้ด้วยความสมัครใจ ปราศจากการบังคับหรือชักจูง และข้าพเจ้าทราบว่าข้าพเจ้าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้เว้นแต่ในกรณีมีข้อจำกัดสิทธิตามกฎหมายหรือยังมีสัญญาระหว่างข้าพเจ้ากับกรมการปกครอง ที่ให้ประโยชน์แก่ข้าพเจ้าอยู่

กรณีที่ข้าพเจ้าประสงค์จะขอถอนความยินยอม ข้าพเจ้าทราบว่าการถอนความยินยอมจะมีผลทำให้ .....(ระบุผลกระทบจากการถอนความยินยอม เช่น ข้าพเจ้าอาจได้รับความสะดวกในการใช้บริการน้อยลง หรือไม่สามารถเข้าถึงฟังก์ชันการใช้งานบางอย่างได้ เป็นต้น)..... และข้าพเจ้าทราบว่าการถอนความยินยอมดังกล่าวไม่มีผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่ได้ดำเนินการเสร็จสิ้นไปแล้วก่อนการถอนความยินยอม

ลงชื่อ.....

(.....)

บริเวณนี้มีการจับภาพ

QR Code

ท่านอาจศึกษาข้อมูลเพิ่มเติมได้ที่

- ณ จุดต้อนรับ/ลงทะเบียน
- ผ่าน Link ประกาศความเป็นส่วนตัวเกี่ยวกับการใช้กล้องวงจรปิด

รายละเอียดและช่องทางการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล:
กรมการปกครอง
ที่อยู่ : ๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
โทรศัพท์ : ๐๒-๒๘๒๑๐๔๗
อีเมล : webmaster@dopa.go.th

ช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล : รองอธิบดีกรมการปกครอง
ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ
ที่อยู่ : ๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
โทรศัพท์ : ๐๒-๒๘๒๑๐๔๗
อีเมล : dpo@dopa.go.th

วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล และฐานทางกฎหมายที่เกี่ยวข้อง:
สำนัก/กอง กรมการปกครอง บันทึกและจัดเก็บข้อมูลภาพจากกล้องวงจรปิด (CCTV) ซึ่งติดตั้งอยู่บริเวณอาคารและสถานที่ เพื่อวัตถุประสงค์
- การป้องกันเหตุอันตรายอันอาจเกิดขึ้นในบริเวณที่ทำการของสำนักบริหารการทะเบียน
- การปฏิบัติตามกฎหมายที่เกี่ยวข้อง
- ฐานทางกฎหมายที่เกี่ยวข้อง: ฐานหน้าที่ตามกฎหมาย (Legal Obligation) และ ฐานความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)

สิทธิของเจ้าของข้อมูล : ในฐานะเจ้าของข้อมูลส่วนบุคคล ท่านมีสิทธิต่อกรมการปกครองซึ่งเป็นผู้ควบคุมข้อมูลหลายประการด้วยกัน โดยเฉพาะสิทธิในการเข้าถึงข้อมูลส่วนบุคคล และสิทธิในการขอให้กรมการปกครองลบข้อมูลส่วนบุคคลของท่าน

อนึ่ง ท่านอาจศึกษารายละเอียดเพิ่มเติมเกี่ยวกับกิจกรรมการประมวลผลนี้ รวมถึงสิทธิของท่านผ่านช่องทางซึ่งเราได้จัดเตรียมไว้ให้ในด้านซ้าย

ประกาศความเป็นส่วนตัวเกี่ยวกับการใช้กล้องวงจรปิด

ปรับปรุงล่าสุด: [•]

๑. ขอบเขตและวัตถุประสงค์

กรมการปกครอง (“กรมการปกครอง” หรือ“เรา”) ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลของท่านที่ได้มอบให้แก่เราด้วยความไว้วางใจ และเรามีความจำเป็นต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อเป็นการรับรองสิทธิของท่านเกี่ยวกับการเก็บรวมรวม การใช้ การจัดเก็บ การเปิดเผย และการลบข้อมูลส่วนบุคคล (“ประมวลผล”) ทั้งนี้ เราจะทำการเก็บรวบรวมข้อมูลส่วนบุคคลของบุคลากรภายในผู้มาติดต่อบุคคลภายนอก หรือบุคคลใด ๆ (“ท่าน”) ที่เข้ามายังพื้นที่เฝ้าระวังสังเกตการณ์ภายในและรอบบริเวณอาคารและสถานที่ต่าง ๆ (“พื้นที่”) อันอยู่ในความดูแลของกรมการปกครอง ผ่านอุปกรณ์กล้องวงจรปิด (CCTV)

รายละเอียดและช่องทางการติดต่อผู้ควบคุมข้อมูล:	**ช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล:**รองอธิบดีกรมการปกครอง
กรมการปกครอง ที่อยู่ : 666 อาคารธนาลงกรณ์ทาวเวอร์ ชั้น 11 ถนนบรมราชชนนี แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ 10700 โทรศัพท์: 02-2821047 อีเมล: webmaster@dopa.go.th	ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ ที่อยู่ : 666 อาคารธนาลงกรณ์ทาวเวอร์ ชั้น 11 ถนนบ รมราชชนนี แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ 10700 โทรศัพท์: 02-2821047 อีเมล: dpo@dopa.go.th

วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล:

- เพื่อการป้องกันอันตรายแก่ชีวิต สุขภาพ และความปลอดภัยส่วนตัว ซึ่งรวมไปถึงทรัพย์สินของท่านด้วย
- เพื่อการปกป้องอาคาร สิ่งอำนวยความสะดวกและทรัพย์สินจากความเสียหาย การขัดขวาง การทำลาย ซึ่งทรัพย์สินหรืออาชญากรรมอื่น
- เพื่อสนับสนุนหน่วยงานที่เกี่ยวข้องในการบังคับใช้กฎหมายเพื่อการยับยั้ง ป้องกัน สืบค้น และดำเนินคดีทางกฎหมายทางกฎหมาย
- เพื่อการให้ความช่วยเหลือในกระบวนการระงับข้อพิพาทที่เกิดขึ้นในกระบวนการทางวินัยหรือกระบวนการยุติเรื่องร้องทุกข์อย่างมีประสิทธิภาพ
- เพื่อช่วยเหลือในการสอบสวนหรือกระบวนพิจารณาที่เกี่ยวข้องกับการแจ้งเบาะแส
- เพื่อสนับสนุนในการก่อตั้งสิทธิหรือยกขึ้นเป็นข้อต่อสู้ในการดำเนินการทางกฎหมาย ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะคดีทางแพ่ง และคดีแรงงาน

• เพื่อปฏิบัติตามกฎหมายที่ใช้บังคับ

ฐานในการประมวลผลข้อมูล: “ฐานการประมวลผล” หมายถึง เหตุผลความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๒๔ และมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยกรมการปกครองดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านภายใต้ฐานทางกฎหมาย ดังต่อไปนี้

- ฐานประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) : เรานำข้อมูลส่วนบุคคลของท่านไปใช้ในการประมวลผลเพื่อดูแลรักษาความปลอดภัยให้แก่บุคคลที่เข้ามาในพื้นที่ รวมถึงการดูแลทรัพย์สินของเรา ไม่ให้ผู้ที่ไม่เกี่ยวข้องสามารถเข้าออกเขตหวงห้าม และใช้ในการสอบสวนเหตุต่าง ๆ ที่เกิดขึ้นภายในพื้นที่
- ฐานหน้าที่ตามกฎหมาย (Legal Obligation) : เราอาจนำข้อมูลส่วนบุคคลของท่านไปใช้ในการประมวลผลเพื่อการปฏิบัติตามกฎหมายตามที่หน่วยงานรัฐที่มีอำนาจตามกฎหมายร้องขอหรือใช้เพื่อเป็นพยานหลักฐาน กรณีเกิดเหตุอาชญากรรม หรืออุบัติเหตุที่เกิดขึ้นภายใน หรือบริเวณอาคารและสถานที่

๒. เราประมวลผลข้อมูลส่วนบุคคลใดบ้าง?

เราประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้

• ข้อมูลอัตลักษณ์ เช่น รูปภาพบุคคล ภาพเคลื่อนไหว เป็นต้น

๓. เราเก็บรวบรวมข้อมูลส่วนบุคคลอย่างไร?

เราเก็บรวบรวมข้อมูลส่วนบุคคลของท่านโดยตรงผ่านกล้องวงจรปิด

๔. เราใช้ข้อมูลส่วนบุคคลอย่างไร?

เราใช้ข้อมูลส่วนบุคคลเพื่อการดำเนินการตามวัตถุประสงค์ของเรา ที่เกี่ยวข้องกับพื้นที่เฝ้าระวังสังเกตการณ์ตามฐานการประมวลผลข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

เราจะประมวลผลข้อมูลส่วนบุคคลของท่านตามวัตถุประสงค์ที่ได้แจ้งไว้เท่านั้น และในบางกรณีเราอาจพิจารณาประมวลผลข้อมูลส่วนบุคคลของท่านด้วยเหตุผลอื่นที่เกี่ยวข้องและไม่ขัดหรือนอกเหนือไปจากวัตถุประสงค์เดิม อย่างไรก็ตาม ในกรณีที่เราจำเป็นต้องประมวลผลข้อมูลด้วยวัตถุประสงค์อื่น ที่ไม่เกี่ยวข้องกับวัตถุประสงค์เดิมและการประมวลผลดังกล่าวไม่สามารถอ้างอิงฐานการประมวลผลอื่นได้ เช่นนี้เราจะขอความยินยอมจากท่านเพื่อการใช้ข้อมูลตามวัตถุประสงค์ใหม่นั้น

๕. การใช้ข้อมูลส่วนบุคคลร่วมกันกับหน่วยงานภายนอก

เราอาจมีความจำเป็นต้องส่งข้อมูลไปยังหน่วยงานภายนอก ดังต่อไปนี้

• หน่วยงานของรัฐ เช่น สำนักงานตำรวจแห่งชาติ สำนักงานอัยการ ศาล หรือเจ้าหน้าที่ของรัฐ เช่น พนักงานสอบสวน อัยการ เป็นต้น

ในกรณีที่เราใช้หรือส่งข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก เราจะดำเนินการเท่าที่จำเป็นโดยใช้หรือส่งข้อมูลให้น้อยที่สุด และอาจพิจารณาใช้วิธีจัดทำข้อมูลนิรนาม (Anonymisation) และการแฝงข้อมูล (Pseudonymisation) เพื่อความปลอดภัยของข้อมูล ทั้งนี้ สำหรับบุคคลภายนอกที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลให้กับเราจะต้องจัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมตามประกาศนี้ และเราจะไม่อนุญาตให้ผู้ประมวลผลข้อมูลใช้ข้อมูลเพื่อวัตถุประสงค์อื่นนอกจากที่เรากำหนด

๖. การส่งหรือโอนข้อมูลไปยังต่างประเทศ

ในกิจกรรมการประมวลผลนี้ เรามิได้ส่งหรือโอนข้อมูลส่วนบุคคลจากกล้องวงจรปิดไปยังต่างประเทศแต่ประการใด

๗. การส่งหรือโอนข้อมูลไปยังต่างประเทศ

เราได้กำหนดให้มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลขึ้นโดยประกาศให้ทราบและบังคับใช้โดยทั่วทั้งองค์กร พร้อมแนวทางปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคล โดยธำรงไว้ซึ่งความเป็นความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ซึ่งเราได้จัดให้มีการทบทวนนโยบายดังกล่าวในระยะเวลาตามที่เหมาะสม (ดูรายละเอียดได้ที่ [โปรดระบุ “DOPA IT Security Policy and Measurement Control” [ถ้ามี])

๘. ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล

เราจะจัดเก็บข้อมูลส่วนบุคคลตลอดระยะเวลาที่จำเป็นในการดำเนินการตามวัตถุประสงค์ของเรารวมถึงงานต่าง ๆ ที่จำเป็น เช่น การดำเนินงานเกี่ยวกับด้านกฎหมาย, บัญชี และการติดตามตรวจสอบต่าง ๆ (ดูรายละเอียดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลเพิ่มเติมได้ที่ [โปรดระบุลิงก์สำหรับ “Data Retention Schedule” (ถ้ามี)])

๙. ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล

ท่านมีสิทธิในข้อมูลส่วนบุคคลดังต่อไปนี้

- สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of Access) โดยท่านสามารถขอรับสำเนาข้อมูลของท่านและตรวจสอบว่าเราได้ประมวลผลข้อมูลของท่านตามกฎหมายหรือไม่
- สิทธิในการโอนข้อมูลส่วนบุคคล (Right to Data Portability) ในกรณีที่เราได้จัดทำข้อมูลส่วนบุคคลในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ ท่านสามารถขอให้ส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานอื่นได้ด้วยวิธีการอัตโนมัติ หรือขอรับข้อมูลส่วนบุคคลที่เราส่งหรือโอนไปยังหน่วยงานอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้
- สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object) โดยท่านสามารถคัดค้าน ในกรณีที่เราประมวลผลข้อมูลของท่าน
    - ตามฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)
- สิทธิในการลบข้อมูลส่วนบุคคล (Right to Erasure) โดยท่านสามารถขอให้ลบข้อมูล หรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวท่านได้ ในกรณีดังต่อไปนี้
    - เมื่อหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล
    - เมื่อท่านคัดค้านการประมวลผลข้อมูลส่วนบุคคลของท่านแล้ว
    - เมื่อข้อมูลส่วนบุคคลได้ถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย
- สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (Right to Restrict Processing) โดยท่านสามารถขอให้ระงับการใช้ข้อมูลส่วนบุคคลของท่านได้ ในกรณีดังต่อไปนี้
    - เมื่ออยู่ในระหว่างการตรวจสอบตามที่ท่านขอให้แก้ไขข้อมูลส่วนบุคคล
    - เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลาย แต่ท่านขอให้ระงับการใช้แทน
    - เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ แต่ท่านมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมายการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

o เมื่ออยู่ในระหว่างการพิสูจน์ หรือตรวจสอบ ตามคำขอใช้สิทธิในการคัดค้านของท่าน

- สิทธิในการแก้ไขข้อมูลส่วนบุคคล (Right to Rectification) โดยท่านสามารถขอแก้ไขข้อมูลของท่านให้ถูกต้อง สมบูรณ์ และเป็นปัจจุบันได้ หากท่านพบว่าข้อมูลของท่านไม่ถูกต้อง สมบูรณ์และเป็นปัจจุบัน ทั้งนี้ เราไม่สามารถตรวจสอบและแก้ไขข้อมูลดังกล่าวได้ด้วยตนเอง

ในบางกรณีตามสภาพของการดำเนินการ เราอาจไม่สามารถดำเนินการได้ตามที่ท่านขอได้ เช่น มีความจำเป็นต้องดำเนินการตามหน้าที่ตามกฎหมาย เป็นต้น

ขอให้ท่านรับทราบว่าเราจะบันทึกรายการต่าง ๆ ที่ได้ดำเนินการเกี่ยวกับคำร้องของท่านเอาไว้เพื่อใช้ในการแก้ไขปัญหาที่เกิดขึ้น หากมีข้อสงสัยในรายละเอียดทางปฏิบัติของการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (ท่านอาจศึกษาได้จากแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (TDPG ๓.๐ Extension) ได้ที่ https://www.law.chula.ac.th/wp-content/uploads/๒๐๒๑/๐๔/TDPG๓.๐-Extension-๒๐๒๑๐๔๑๓-๑.pdf)

ในกรณีที่ท่านประสงค์จะใช้สิทธิดังกล่าวข้างต้น หรือมีข้อร้องเรียนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โปรดติดต่อที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลผ่านช่องทางตามรายละเอียดที่แจ้งไว้ข้างต้น เราจะรีบดำเนินการตามคำร้องของท่านโดยเร็ว และสอดคล้องกับที่กฎหมายกำหนด อย่างไรก็ดี ท่านมีสิทธิร้องเรียนเกี่ยวกับการไม่คุ้มครองข้อมูลส่วนบุคคลตามกฎหมายได้ที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผ่านช่องทางอีเมล saraban@pdpc.or.th ตามแบบคำร้องเรียนที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๑๐. การทบทวนและปรับปรุงประกาศ

ประกาศความเป็นส่วนตัวเกี่ยวกับการใช้กล้องวงจรปิดฉบับนี้ ได้รับการปรับปรุงล่าสุดเมื่อวันที่ [•] ซึ่งอาจมีการแก้ไขเปลี่ยนแปลงในแต่ละคราว โดยจะแจ้งให้ท่านทราบถึงการเปลี่ยนแปลงที่สำคัญของประกาศนี้และอาจแจ้งเตือนท่านเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของท่านเป็นระยะ

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กรมการปกครอง

กรมการปกครองในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กรมการปกครองจึงได้กำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล ไว้ดังต่อไปนี้

ส่วนที่ ๑. ผู้มีหน้าที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานภายใต้กรมการปกครองซึ่งประกอบ หน่วยงานในส่วนกลางและส่วนภูมิภาค ดังนี้

๑.๑ ราชการบริหารส่วนกลาง ๑๗ หน่วยงาน

๑) กลุ่มพัฒนาระบบบริหาร
๒) กองการสื่อสาร
๓) กองการเจ้าหน้าที่
๔) กองคลัง
๕) กองวิชาการและแผนงาน
๖) วิทยาลัยการปกครอง
๗) ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง
๘) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้
๙) สำนักการสอบสวนและนิติการ
๑๐) สำนักกิจการความมั่นคงภายใน
๑๑) สำนักผู้เชี่ยวชาญเฉพาะด้านกฎหมาย
๑๒) สำนักผู้เชี่ยวชาญเฉพาะด้านความมั่นคงภายใน
๑๓) สำนักงานเลขานุการกรม กรมการปกครอง
๑๔) สำนักบริหารการทะเบียน
๑๕) สำนักบริหารการปกครองท้องที่
๑๖) สำนักอำนวยการกองอาสารักษาดินแดน
๑๗) ศูนย์ปฏิบัติการต่อต้านการทุจริต กรมการปกครอง

๑.๒ ราชการบริหารส่วนภูมิภาค ๙๕๔ หน่วยงาน

ที่ทำการปกครองจังหวัด ๗๖ จังหวัด
ที่ทำการปกครองอำเภอ ๘๗๘ อำเภอ

มีผลบังคับใช้กับข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างเหมาบริการ อาสาสมัครรักษาดินแดน รวมถึงบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้ กรมการปกครอง

ส่วนที่ ๒. ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง

๒.๑ ข้อมูลส่วนบุคคลของบุคลากรหน่วยงานของกรมการปกครอง

เป็นข้อมูลส่วนบุคคลของ ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างเหมาบริการ อาสาสมัครรักษาดินแดน ในสังกัดกรมการปกครองรวมถึง ผู้มาสมัครงาน ฝึกงาน หรือทดลองปฏิบัติงานในหน่วยงานกรมการปกครอง

๒.๒ ข้อมูลส่วนบุคคลของผู้มาติดต่องาน

เป็นข้อมูลส่วนบุคลคล ของผู้มาติดต่องาน สมัครงาน การทำธุรกรรม เช่น การขอใบอนุญาตต่าง ๆ การทำนิติกรรม เช่น การทำสัญญาว่าจ้าง สัญญาซื้อขาย รวมถึงข้อมูลส่วนบุคคลของพนักงานหรือลูกจ้างของหน่วยงานที่ทำสัญญา หรือทำงานให้กับกรมการปกครอง

๒.๓ ข้อมูลส่วนบุคคลของผู้รับบริการ

เป็นข้อมูลส่วนบุคคลของผู้มาติดต่อเพื่อรับบริการ ของกรมการปกครองรวมถึงข้อมูลส่วนบุคคลของผู้รับบริการกรณีที่บุคลากรของกรมการปกครอง ออกไปให้บริการนอกหน่วยบริการในพื้นที่ที่รับผิดชอบ

ส่วนที่ ๓. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

กรมการปกครองจะเก็บรวบรวมข้อมูลส่วนบุคคล “เท่าที่จำเป็น” สำหรับการให้บริการตามวัตถุประสงค์ในการดำเนินงานของกรมการปกครองอย่างเคร่งครัด เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่กรมการปกครองหรือเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการทะเบียนและบัตร หรือประโยชน์สาธารณะที่สำคัญอื่น ๆ เป็นต้น โดยกรมการปกครองจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และจะทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานของกรมการปกครอง

ส่วนที่ ๔. วัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล

๔.๑ กรมการปกครองจะเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย โดยกรมการปกครองจะขอความยินยอม โดยชัดแจ้งจากท่านก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือการใช้อำนาจรัฐของกรมการปกครอง ซึ่งกำหนดไว้ตามกฎหมาย รวมถึง กฎ ระเบียบ คำสั่งและมติคณะรัฐมนตรีที่เกี่ยวข้อง

๒. เพื่อการปฏิบัติหน้าที่ตามกฎหมาย กรมการปกครอง ในกรณีที่มีกฎหมายกำหนดให้ต้องปฏิบัติเพื่อให้กรมการปกครอง สามารถปฏิบัติตามที่กฎหมายที่ควบคุม กรมการปกครอง

๓. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายระหว่างเจ้าของข้อมูลส่วนบุคคลกับกรมการปกครอง โดยประโยชน์ดังกล่าวมีความสำคัญไม่น้อยไปกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล เช่น ในช่วงที่เจ้าของข้อมูลส่วนบุคคลสมัครลงทะเบียนขอรหัสผู้ใช้งานเพื่อขอรับบริการบนระบบสารสนเทศที่ให้บริการ

๔. เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้นกับกรมการปกครอง

ยกเว้น แต่ในกรณีดังต่อไปนี้ กรมการปกครองสามารถเก็บรวบรวมข้อมูลส่วนบุคคลของท่านได้โดยไม่ต้องขอความยินยอม

๑. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์ สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

๒. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๓. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

๔. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๕. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือ นิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

๖. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลเนื่องจากข้อมูลส่วนบุคคลที่กรมการปกครองจะดำเนินการประมวลผลเพื่อวัตถุประสงค์ที่กำหนด ในส่วนที่มีความเกี่ยวเนื่องกับการปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นเพื่อเข้าทำสัญญากับท่าน ซึ่งข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่จำเป็นต่อการบรรลุวัตถุประสงค์ดังกล่าว หากท่านไม่ให้ข้อมูลส่วนบุคคลดังกล่าวแก่กรมการปกครอง อาจมีผลกระทบทางกฎหมาย หรือกรมการปกครองอาจจะไม่สามารถปฏิบัติหน้าที่ภายใต้สัญญาที่ได้เข้าทำกับท่าน หรือไม่สามารถเข้าทำสัญญากับท่านได้ (แล้วแต่กรณี) ในกรณีดังกล่าว กรมการปกครองอาจมีความจำเป็นต้องปฏิเสธการเข้าทำสัญญากับท่าน หรือยกเลิกการให้บริการที่เกี่ยวข้องต่อท่านไม่ว่าทั้งหมดหรือบางส่วน

ส่วนที่ ๕. การใช้และเปิดเผยข้อมูลส่วนบุคคล

หลังจากที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลแล้ว กรมการปกครองอาจมีความจำเป็นต้องใช้หรือเปิดเผยข้อมูลไปยังบุคคลอื่นที่เกี่ยวข้อง ซึ่งการใช้หรือเปิดเผยข้อมูลนั้น จะเป็นการทำเพื่อให้บรรลุวัตถุประสงค์ในการประมวลผลข้อมูลหรือการเปิดเผยที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าวหรือเป็นการเปิดเผยเพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานอื่นใด

๕.๑ การใช้และเปิดเผยข้อมูลส่วนบุคคลมี ๒ ลักษณะ

๕.๑.๑. ใช้และเปิดเผยข้อมูลภายในหน่วยงาน จะต้องจัดทำโดยเจ้าหน้าที่ที่ได้รับการแต่งตั้งและเป็นการใช้ตามวัตถุประสงค์ของการเก็บรวบรวม จัดเก็บ ข้อมูลที่ได้แจ้งและ/หรือขอความยินยอมไว้ตามที่หน่วยงานระบุไว้ในหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคลและแบบหนังสือยินยอม เท่านั้น ผู้บริหารหรือผู้ที่ได้รับมอบหมายของหน่วยงานต้องกำกับดูแลบุคลากรให้ปฏิบัติตามอย่างเคร่งครัด ในกรณีที่หน่วยงานใช้ข้อมูลเพื่อดำเนินธุรกรรมนอกเหนือจากที่ระบุไว้ หน่วยงานจะต้องให้เจ้าของข้อมูลลงลายมือชื่อในหนังสือยินยอมที่ระบุธุรกรรมที่จะมีเพิ่มเติม

๕.๑.๒ การส่ง การโอน หรือการเปิดเผยขอต่อบุคคลภายนอกหรือหน่วยงานภายนอกรวมทั้งการเบิกใช้เอกสารจะต้องจัดทำโดยเจ้าหน้าที่ที่ได้รับมอบหมาย และได้รับอนุมัติจากผู้อนุมัติจากหัวหน้าหน่วยงานก่อนการส่ง โอน หรือเปิดเผยต่อหน่วยงานหรือบุคคลภายนอก

หน่วยงานหรือบุคคลภายนอก ได้แก่

(๑) หน่วยงานราชการตาม พ.ร.บ. ระเบียบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ที่มีอำนาจหน้าที่ตามกฎหมาย เช่น กรมสรรพากร (มีอำนาจหน้าที่เกี่ยวกับด้านภาษีอากร) ศาล (มีอำนาจหน้าที่เฉพาะที่เกี่ยวข้องกับคดีความ) พนักงานสอบสวน (มีอำนาจหน้าที่เฉพาะที่เกี่ยวกับคดีในความรับผิดชอบ)

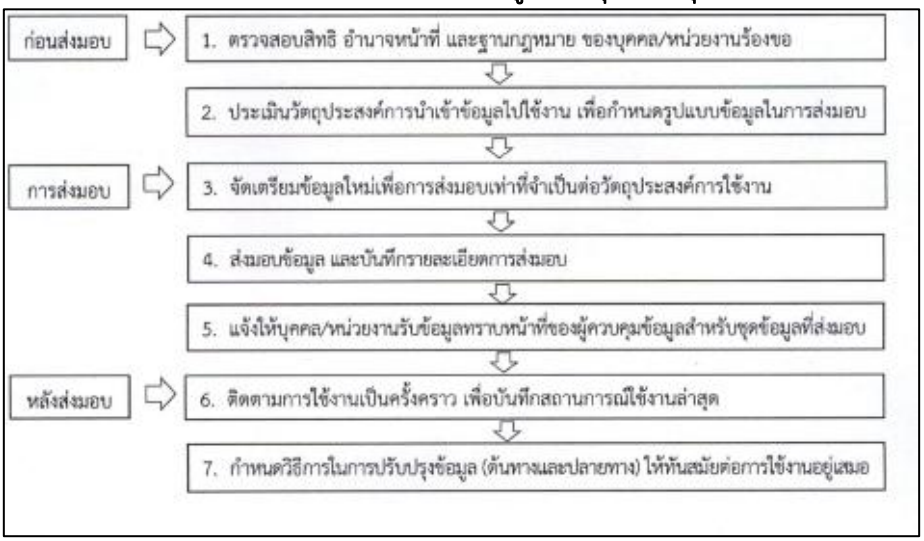
(๒) หน่วยงานราชการทั่วไป ที่ไม่มีอำนาจหน้าที่ตามกฎหมายในเรื่องนั้นๆ

(๓) นิติบุคคลในประเทศ ที่ไม่ต้องใช้สัญญาประมวลผลข้อมูล

(๔) นิติบุคคลต่างประเทศ ซึ่งต้องมีกฎหมาย PDPA ทัดเทียมกับประเทศไทย

(๕) คู่สัญญาที่เป็นผู้ประมวลผลข้อมูล

ขั้นตอนการใช้และเปิดเผยข้อมูลส่วนบุคคล สรุปได้ดังนี้



๕.๒ การโอนข้อมูลไปต่างประเทศ

ในบางกรณี กรมการปกครองอาจจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังต่างประเทศเพื่อดำเนินการตามวัตถุประสงค์ในการให้บริการแก่ท่าน เช่น เพื่อส่งข้อมูลส่วนบุคคลไปยังระบบคลาวด์ (Cloud) ที่มีแพลตฟอร์มหรือเครื่องแม่ข่าย (Server) อยู่ต่างประเทศ (เช่น ประเทศสิงคโปร์ หรือสหรัฐอเมริกา เป็นต้น) เพื่อสนับสนุนระบบเทคโนโลยีสารสนเทศที่ตั้งอยู่นอกประเทศไทย ทั้งนี้ ขึ้นอยู่กับบริการของ กรมการปกครอง ที่ท่านใช้งานหรือมีส่วนเกี่ยวข้องเป็นรายกิจกรรม อย่างไรก็ตาม ในขณะที่จัดทำนโยบายฉบับนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมิได้มีประกาศกำหนดรายการประเทศปลายทางที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ดังนั้นเมื่อ กรมการปกครอง มีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังประเทศปลายทาง กรมการปกครองจะดำเนินการเพื่อให้ข้อมูลส่วนบุคคลที่ส่งหรือโอนไปมีมาตรการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอตามมาตรฐานสากล หรือดำเนินการตามเงื่อนไขเพื่อให้สามารถส่งหรือโอนข้อมูลนั้นได้ตามกฎหมาย ได้แก่

๑. เป็นการปฏิบัติตามกฎหมายที่กำหนดให้กรมการปกครองต้องส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

๒. ได้แจ้งให้ท่านทราบและได้รับความยินยอมจากท่านในกรณีที่ประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ ทั้งนี้ตามประกาศรายชื่อประเทศที่คณะกรรมการคุ้มครองส่วนบุคคลประกาศกำหนด

๓. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาที่ท่านเป็นคู่สัญญากับ กรมการปกครอง หรือเป็นการทำตามคำขอของท่านก่อนการเข้าทำสัญญานั้น

๔. เป็นการกระทำตามสัญญาของ กรมการปกครอง กับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของท่าน

๕. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของท่านหรือของบุคคลอื่น เมื่อท่านไม่สามารถให้ความยินยอมในขณะนั้นได้

๖. เป็นการจำเป็นเพื่อดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

๕.๓ แนวทางปฏิบัติข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล Data Sharing Agreement เพื่อเป็นเครื่องมือและมาตรการในการกำกับดูแลการใช้และการเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๗ วรรคสอง กำหนดว่า บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น”และมาตรา ๓๗(๒) กำหนดว่า “ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น ที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ

วัตถุประสงค์ของการจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล Data Sharing Agreement มีดังต่อไปนี้

๑) ช่วยให้คู่สัญญารู้บทบาทและหน้าที่ของตนเองในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

๒) กำหนดวัตถุประสงค์ในการเปิดเผยข้อมูลส่วนบุคคล

๓) ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลในแต่ละขั้นตอน

๔) กำหนดมาตรฐานและวิธีการแบ่งปันข้อมูล

กรณีที่ควรจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล Data Sharing Agreement

๑) การโอนข้อมูลระหว่างองค์กรไม่ว่าทางเดียวหรือแลกเปลี่ยนข้อมูล

๒) การให้องค์กรอื่นเข้าถึงระบบฐานข้อมูลทางอิเล็กทรอนิกส์ขององค์กรเพื่อวัตถุประสงค์ด้านการวิจัย

๓) การนำข้อมูลมาใช้ร่วมกันในรูปแบบ pooling data และใช้ข้อมูลดังกล่าวร่วมกันหรือแบ่งปันไปยังองค์กรภายนอกด้วย

๔) มีการแบ่งปันข้อมูลเป็นประจำอย่างเป็นระบบเพื่อวัตถุประสงค์ที่กำหนด

๕) การโอนครั้งเดียวหรือเฉพาะกิจ

๖) การโอนครั้งเดียวในกรณีฉุกเฉิน

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล Data Sharing Agreement ควรมีรายละเอียดดังนี้

๑) ชื่อคู่สัญญา/คู่ความร่วมมือ

๒) วัตถุประสงค์ของการแบ่งปันข้อมูล คืออย่างไร ซึ่งควรระบุถึงที่มา ความจำเป็น และประโยชน์ที่จะ ได้รับจากการแบ่งปันข้อมูลส่วนบุคคล

๓) หน่วยงานอื่นนอกจากคู่สัญญาตามข้อ ๑ ที่เข้ามามีบทบาทในการแบ่งปันข้อมูล (ถ้ามี)

๔) รายละเอียดของข้อมูลส่วนบุคคลที่มีการแบ่งปัน/แลกเปลี่ยน (data specification)

๕) ฐานการประมวลผล (ดูตัวอย่างจากกรณีศึกษาข้างต้น)

๖) ข้อตกลงในส่วนที่เกี่ยวกับการใช้ข้อมูลส่วนบุคคลอ่อนไหว

๗) ข้อตกลงในส่วนที่เกี่ยวข้องกับการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

๘) ข้อตกลงในส่วนของการบริหารจัดการข้อมูล อาทิ เงื่อนไขการแบ่งปันข้อมูลระหว่างกัน การบริหารความถูกต้องครบถ้วนของข้อมูล รูปแบบการบันทึกข้อมูล แนวทางปฏิบัติร่วมกันเรื่องระยะเวลาและการลบทำลาย มาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม การอบรมและสร้างความตระหนักรู้แก่ผู้เกี่ยวข้อง และการการดำเนินการเมื่อยกเลิกสัญญาหรือสิ้นสุดข้อตกลง เป็นต้น

๙) เอกสารประกอบที่อาจมี อาทิ แบบฟอร์มการขอใช้ข้อมูล เป็นต้น

ส่วนที่ ๖.ระยะเวลาในการจัดเก็บข้อมูล

หน่วยงานต้องกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคล ที่ชัดเจนและสอดคล้องกับวัตถุประสงค์การใช้ข้อมูล โดยปฏิบัติตามนโยบายระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลและการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดเวลา

ส่วนที่ ๗. การรักษาความมั่นคงปลอดภัย

กรมการปกครองจะใช้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกัน ด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุม การใช้งานข้อมูลส่วนบุคคล (Access Control) เพื่อป้องกันการเข้าถึงและเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และสอดคล้องกับการดำเนินงานของกรมการปกครองและมาตรฐานที่รับรองโดยทั่วไป ตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของกรมการปกครอง พ.ศ. ๒๕๖๗ แนบท้ายประกาศกรมการปกครอง เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๗

การจัดจ้างผู้ให้บริการภายนอก กรมการปกครองจะมีการสอบทานและปรับปรุงมาตรการต่าง ๆ เพื่อให้แน่ใจว่า ผู้ให้บริการภายนอกที่ กรมการปกครองทำการว่าจ้างจะมีการใช้มาตรการในการ เก็บรวบรวม ประมวลผล โอนย้าย จัดการ และรักษาความมั่นคงปลอดภัย ของข้อมูลอย่างเพียงพอในการให้บริการภายใต้วัตถุประสงค์ของกรมการปกครองเป็นไปตามมาตรฐานต่าง ๆ ของประเทศ และกฎระเบียบที่เกี่ยวข้อง

หน่วยงานจัดทำนโยบาย แนวปฏิบัติและขั้นตอนวิธีการต่าง ๆ เพื่อการจัดการข้อมูลอย่างปลอดภัยและป้องกันการ เข้าถึงโดยไม่ได้รับอนุญาตโดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

กำหนดนโยบายและขั้นตอนวิธีการต่าง ๆ เพื่อจัดการข้อมูลอย่างปลอดภัย และอาจกำหนดเพิ่มเติมในสัญญาระหว่างกรมการปกครองกับคู่สัญญาแต่ละราย มีการบริหารจัดการสิทธิของพนักงานและลูกจ้างในการเข้าถึงข้อมูลส่วนบุคคล อย่างเหมาะสม ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น การเข้ารหัสข้อมูล การตรวจสอบตัวตนและเทคโนโลยีการตรวจจับไวรัส ตามความจำเป็น รวมถึงจัดให้มีช่องทางการสื่อสารแบบปลอดภัยสำหรับข้อมูลดังกล่าวด้วยการเข้ารหัสลับข้อมูลดังกล่าว เช่น จัดให้มีการใช้ Secure Socket Layer (SSL) protocol เป็นต้น บริหารจัดการให้ ผู้ให้บริการภายนอกที่หน่วยงานทำการว่าจ้าง ต้องปฏิบัติตามหลักเกณฑ์ ตามกฎหมาย และระเบียบต่าง ๆ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล มีติดตามตรวจสอบเว็บไซต์และระบบออนไลน์ ของกรมการปกครองผ่านหน่วยงาน ที่มีความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย จัดให้มีการฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรของกรมการปกครองประเมินผลแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การจัดการข้อมูล และการรักษาความมั่นคงปลอดภัยของข้อมูลของกรมการปกครองเป็นประจำ

ส่วนที่ ๘. การลบหรือทำลายข้อมูลส่วนบุคคล

หน่วยงานต้องกำหนดวิธีการและขั้นตอน และบันทึกรายงานการลบและทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาจัดเก็บข้อมูลส่วนบุคคคล หรือปฏิบัติตามนโยบายและระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลและการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดเวลา หน่วยงานต้องจัดให้มีผู้ทำหน้าที่ตรวจสอบและรวบรวมรายการข้อมูลส่วนบุคคลที่ต้องดำเนินการลบหรือทำลาย เมื่อพ้นกำหนดระยะยะเวลาการเก็บรักษาทั้งในระบบอิเล็กทรอนิกส์ และในรูปแบบเอกสารต่างๆ โดยจัดทำรายการข้อมูลที่ต้องดำเนินการลบแจ้งต่อผู้บังคับบัญชาเพื่อขออนุมัติดำเนินการลบทำลายข้อมูล กรณีข้อมูลส่วนบุคคลที่มีการใช้เพื่อดำเนินคดีตามกฎหมาย และ/หรือมีการบังคับคดี หน่วยงานให้ทำการเก็บข้อมูลเอกสาร และฐานข้อมูลดังกล่าวไว้เพื่อใช้ในการดำเนินคดีจนกว่าคดีจะถึงที่สุด จึงจะทำลายเอกสารที่เป็นข้อมูลส่วนบุคคลนั้นได้

ส่วนที่ ๙. การมีส่วนร่วมของเจ้าของข้อมูล

หน่วยงานจะเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรงเท่านั้น และต้อง “ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือระหว่างเก็บรวบรวมข้อมูลส่วนบุคคล ”เว้นแต่การเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด หากกรมการปกครองจำเป็นต้อง “เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ”ที่ไม่ใช่เก็บจากเจ้าของข้อมูลส่วนบุคคลโดยตรง กรมการปกครองจะแจ้งเหตุผลความจำเป็นนั้นให้เจ้าของข้อมูลส่วนบุคคลทราบ และขอความยินยอมในเวลาตามที่กำหนด เว้นแต่การเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด

ส่วนที่ ๑๐. สิทธิของเจ้าของข้อมูล วิธีการใช้สิทธิของเจ้าของข้อมูล และการดำเนินการที่ต้องปฏิบัติตามหรือไม่ปฏิบัติตามการใช้สิทธิของเจ้าของข้อมูล

๑๐.๑ หลักเกณฑ์วิธีการใช้สิทธิและการแจ้งสิทธิของเจ้าของข้อมูล

เจ้าของข้อมูลมีสิทธิในการคัดค้าน การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเมื่อใดก็ได้และมีสิทธิขอให้ผู้ควบคุมข้อมูล ดำเนินการลบ ทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ หรือขอระงับการใช้ข้อมูลส่วนบุคคลได้

สิทธิของเจ้าของข้อมูลตามพระราชบัญญัตินี้ ได้แก่

๑) สิทธิในการได้รับแจ้งข้อมูล

๒) สิทธิในการเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล

๓) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

๔) สิทธิในการโอนถ่ายข้อมูลส่วนบุคคล

๕) สิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้นได้

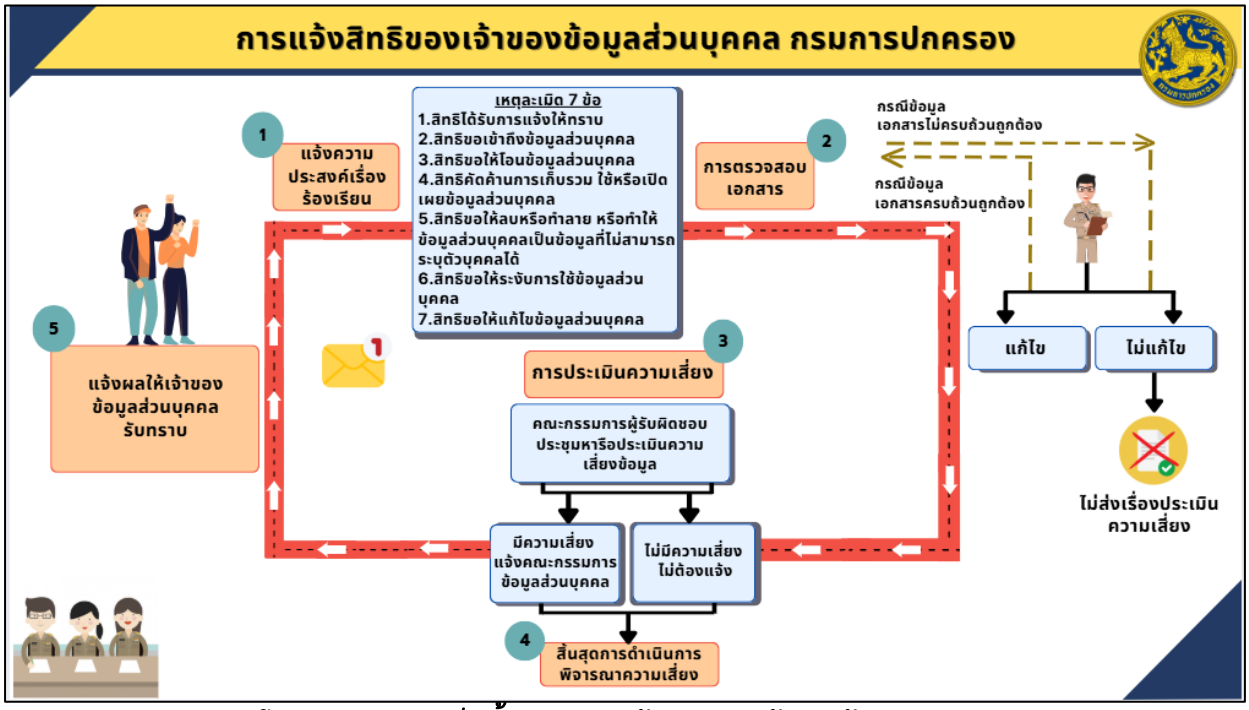
๖) สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล

๗) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล

๘) สิทธิในการเพิกถอนความยินยอม

คำอธิบายขั้นตอนแนวปฏิบัติต่อความประสงค์ในการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล

ลำดับ	ขั้นตอน	คำอธิบาย	ผู้ที่เกี่ยวข้อง
๑	แจ้งความประสงค์เรื่องร้องเรียน	เจ้าของข้อมูลส่วนบุคคล/ผู้ร้องขอ แจ้งความประสงค์เรื่องร้องเรียน เจ้าหน้าที่ทำการพิจารณาเหตุละเมิด ๗ ข้อ	เจ้าของข้อมูลส่วนบุคคล
๒	การตรวจสอบเอกสาร	กรณีข้อมูลเอกสารครบถ้วนถูกต้อง จะแจ้งไปยังเจ้าของข้อมูลส่วนบุคคล และทำเรื่องส่งประเมินความเสี่ยง ในขั้นตอนที่ ๓ หากกรณีข้อมูลเอกสารไม่ครบ จะไม่ส่งเรื่องประเมินความเสี่ยง	เจ้าหน้าที่ผู้รับเรื่อง
๓	การประเมินความเสี่ยง	คณะกรรมการผู้รับผิดชอบประชุมหารือประเมินความเสี่ยงข้อมูล ถ้ามีความเสี่ยงให้แจ้งคณะกรรมการข้อมูลส่วนบุคคล และหากพบว่าไม่มีความเสี่ยงไม่ต้องทำการแจ้ง ถือว่าดำเนินการเสร็จสิ้น	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
๔	สิ้นสุดการดำเนินการพิจารณาประเมินความเสี่ยง	ในกรณีที่ไม่มีความเสี่ยงของข้อมูล หากมีความเสี่ยงให้แจ้งเจ้าของข้อมูลส่วนบุคคล เป็นขั้นตอนที่ ๕ เป็นลำดับถัดไป	เจ้าหน้าที่ผู้รับเรื่อง
๕	แจ้งผลให้เจ้าของข้อมูลส่วนบุคคลรับทราบ	แจ้งผลกรณีมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล	เจ้าหน้าที่ผู้รับเรื่อง



โดยสามารถสรุปเป็นขั้นตอนการแจ้งสิทธิของเจ้าของข้อมูล ดังภาพ

๑๐.๒ แนวปฏิบัติตามคำร้องขอของเจ้าของข้อมูล

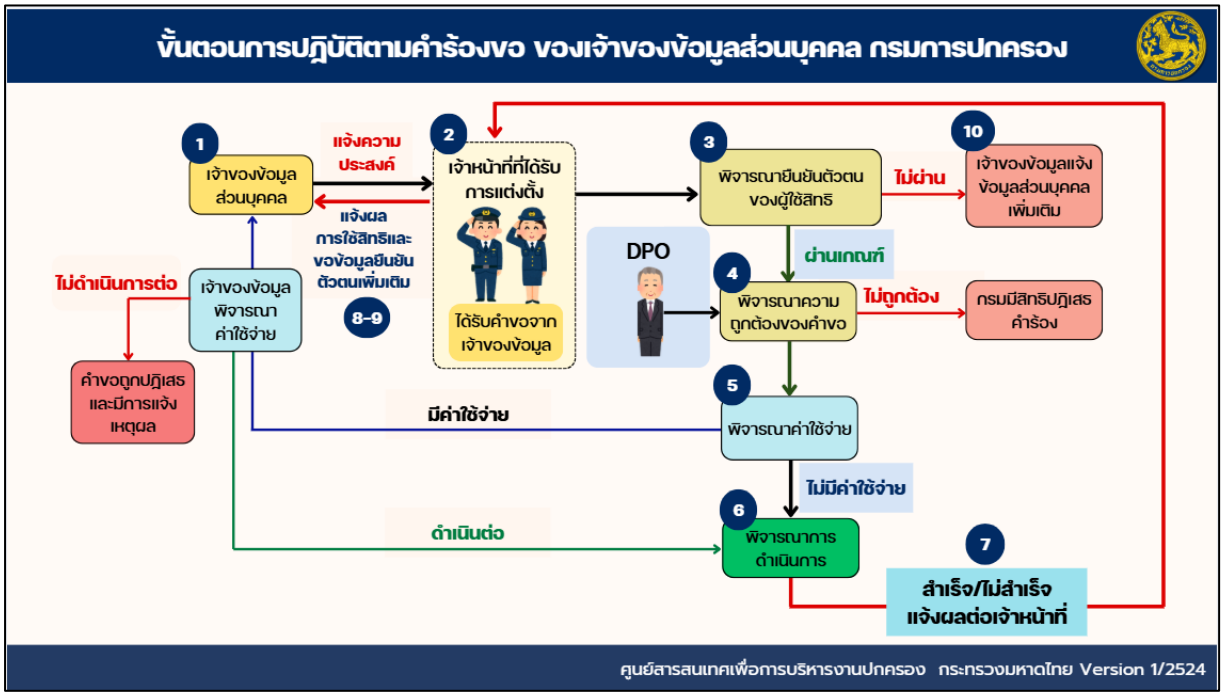
กรณีที่เจ้าของข้อมูลมีความประสงค์จะใช้สิทธิ์ตามข้อ ๑๐.๑ ข้างต้น ด้วยตนเอง หรือมอบอำนาจให้ตัวแทนมาทำการแทน ให้ใช้แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูล พร้อมเอกสารประกอบคำร้องเพื่อยืนยันตัวตนตามที่กำหนดไว้ เช่น สำเนาบัตรประจำตัวประชาชนหรือสำเนาหนังสือเดินทางของเจ้าของข้อมูล และหรือตัวแทนผู้รับมอบอำนาจ หนังสือมอบอำนาจ ให้แก่หน่วยงาน

คำอธิบายขั้นตอนแนวปฏิบัติต่อคำขอของเจ้าของข้อมูลส่วนบุคคล

ลำดับ	ขั้นตอน	คำอธิบาย	ผู้ที่เกี่ยวข้อง
๑	แจ้งความประสงค์ขอใช้สิทธิ	เจ้าของข้อมูลส่วนบุคคล/ผู้ร้องขอ แจ้งความประสงค์ขอใช้สิทธิ ผ่านแบบฟอร์มการแจ้งสิทธิของกรม	เจ้าของข้อมูลส่วนบุคคล
๒	ได้รับคำขอจากเจ้าของข้อมูลส่วนบุคคล	เจ้าหน้าที่ผู้รับเรื่องได้รับคำขอจากเจ้าของข้อมูลส่วนบุคคล	เจ้าหน้าที่ผู้รับเรื่อง
๓	พิจารณายืนยันตัวตนของผู้ใช้สิทธิ	เจ้าหน้าที่ผู้รับเรื่องยืนยันตัวตนของผู้ขอใช้สิทธิว่าเป็นเจ้าของข้อมูลส่วนบุคคลตามเกณฑ์ที่กรมกำหนดหรือไม่ - กรณีผ่านเกณฑ์เจ้าหน้าที่ผู้รับเรื่องบันทึกรายละเอียดการขอใช้สิทธิและส่งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล(DPO) และดำเนินการตามขั้นตอนที่ ๔ - กรณีไม่ผ่านเกณฑ์ ให้ดำเนินการตามขั้นตอนที่ ๑๐	เจ้าหน้าที่ผู้รับเรื่อง
๔	พิจารณาความถูกต้องของคำขอ	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) พิจารณาคำร้องขอของเจ้าของข้อมูลส่วนบุคคลว่าถูกต้อง สมบูรณ์หรือไม่ หรือมีข้อยกเว้นในการปฏิเสธ เช่น คำร้องขอนั้นไม่สมเหตุสมผล หรือฟุ่มเฟือยเกินความจำเป็นอย่างชัดแจ้ง หรือเหตุอื่น ๆ ตามตารางเปรียบเทียบเหตุแห่งการปฏิเสธการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคล - ในกรณีที่คำร้องขอถูกต้อง ครบถ้วน จะดำเนินการต่อตามขั้นตอนที่ ๕ - ในกรณีที่คำร้องขอไม่ถูกต้อง กรมมีสิทธิที่จะปฏิเสธการดำเนินการตามคำร้องขอได้ คำขอดังกล่าวจะถูกปฏิเสธและแจ้งเหตุผลการปฏิเสธให้เจ้าของข้อมูลส่วนบุคคลรับทราบ พร้อมทั้งบันทึกเหตุการปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคล	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
๕	มีค่าใช้จ่ายสำหรับคำขอหรือไม่	พิจารณาว่ามีการเรียกเก็บค่าใช้จ่ายหรือไม่ - หากมีการเรียกเก็บเงิน เจ้าของข้อมูลส่วนบุคคลจะได้รับแจ้งการเรียกเก็บเงินและมีโอกาสตัดสินใจว่าจะดำเนินการต่อหรือไม่ - หากเจ้าของข้อมูลส่วนบุคคลตัดสินใจที่จะดำเนินการต่อให้ดำเนินการตามขั้นตอนที่ ๖ - หากเจ้าของข้อมูลส่วนบุคคลตัดสินใจที่จะไม่ดำเนินการต่อคำขอจะถูกปฏิเสธและมีการแจ้งเหตุผล พร้อมทั้งบันทึกเหตุการปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคล	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ลำดับ	ขั้นตอน	คำอธิบาย	ผู้ที่เกี่ยวข้อง
๖	พิจารณาการดำเนินการ	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) พิจารณาผลการดำเนินการตอบสนองการขอใช้สิทธิจากผู้ควบคุมข้อมูลส่วนบุคคลว่าดำเนินการตอบสนองได้สำเร็จหรือไม่ - กรณีดำเนินการสำเร็จหรือไม่สำเร็จ ให้ดำเนินการตามขั้นตอนที่ ๘	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
๗	แจ้งผลการใช้สิทธิให้เจ้าหน้าที่ผู้รับเรื่องรับทราบ	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) แจ้งผลการใช้สิทธิให้เจ้าหน้าที่ผู้รับเรื่องรับทราบ	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
๘	แจ้งผลการใช้สิทธิให้เจ้าของข้อมูลส่วนบุคคลรับทราบ	เจ้าหน้าที่ผู้รับเรื่องแจ้งผลการใช้สิทธิให้เจ้าของข้อมูลส่วนบุคคลรับทราบผ่านทางช่องทางที่เหมาะสม	เจ้าหน้าที่ผู้รับเรื่อง
๙	แจ้งเจ้าของข้อมูลส่วนบุคคลเพื่อขอข้อมูลส่วนบุคคลยืนยันตัวตนเพิ่มเติม	เจ้าหน้าที่ผู้รับเรื่องแจ้งเจ้าของข้อมูลส่วนบุคคลเพื่อขอข้อมูลส่วนบุคคลยืนยันตัวตนเพิ่มเติม	เจ้าหน้าที่ผู้รับเรื่อง
๑๐	แจ้งข้อมูลส่วนบุคคลเพิ่มเติม	เจ้าของข้อมูลส่วนบุคคลแจ้งข้อมูลส่วนบุคคลเพิ่มเติมเพื่อสนับสนุนการใช้สิทธิ	เจ้าของข้อมูลส่วนบุคคล

โดยสามารถสรุปเป็นขั้นตอนแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูล ดังภาพ



๑๐.๓ กรณีหน่วยงานตรวจพบความไม่ถูกต้องหรือความไม่สมบูรณ์ของข้อมูล

กรณีที่หน่วยงานพบว่า ข้อมูลที่เก็บรวบรวมมีความไม่ถูกต้อง อันเนื่องจากความผิดพลาดในการพิจารณาและสอบทาน หรือข้อมูลไม่สมบูรณ์และจำเป็นต้องปรับปรุงหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลเพื่อประโยชน์ของผู้รับบริการในภายหลัง หน่วยงานจะต้องแจ้งให้เจ้าของข้อมูลทราบ และให้เจ้าของข้อมูลจัดทำคำร้องขอใช้สิทธิให้แก่หน่วยงานเพื่อที่จะได้แก้ไขข้อมูลให้ถูกต้อง

การแก้ไขปรับปรุง เปลี่ยนแปลงข้อมูล จะต้องได้รับการอนุมัติจากผู้บริหาร หรือผู้ที่รับการแต่งตั้งก่อนการดำเนินการ

๑๐.๔ แนวทางการปฏิบัติเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคล

กรมการปกครอง กำหนดกรอบการทำงานเป็นขั้นตอนของผู้ควบคุมข้อมูล (Data Controller) ในส่วนของการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ แนวปฏิบัติการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ของกรมการปกครองอ้างอิงตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

เมื่อมีเหตุละเมิดข้อมูลส่วนบุคคลเกิดขึ้นภายในหน่วยงาน ผู้ที่ทราบเหตุจะต้องแจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเร็วที่สุด เพื่อที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะทำการตรวจสอบถึงสาเหตุที่มาและระบุจุดต้นเหตุของการละเมิดข้อมูลส่วนบุคคล พร้อมทั้งแจ้งแก่เจ้าของข้อมูลส่วนบุคคลและ/หรือ สำนักงานคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดโดยไม่ชักช้า รวมทั้งออกมาตรการเยียวยาเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่จดบันทึกเหตุการณ์การการละเมิดข้อมูลส่วนบุคคลและประเมินความเสี่ยง เมื่อเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น ในการประเมินความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคลนั้น อาจพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล ถ้าหากพิจารณาแล้วว่า ไม่ได้มีผลกระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถทำการจดบันทึกไว้และอาจไม่จำเป็นต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลหรือแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลถึงเหตุการณ์การละเมิดที่เกิดขึ้น แต่หากผลการประเมินแสดงให้เห็นว่าการละเมิดข้อมูลอาจจะทำให้เกิดความเสี่ยงสูง ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีการดำเนินการแจ้งแก่เจ้าของข้อมูลส่วนบุคคลรวมทั้งแนวทางในการเยียวยา อีกทั้งแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในระยะเวลา ๗๒ ชั่วโมง นับจากทราบเหตุการณ์การละเมิดข้อมูลส่วนบุคคล

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไม่ว่าโดยทางวาจาเป็นหนังสือ หรือวิธีการอื่นทางอิเล็กทรอนิกส์ หรือผู้ควบคุมข้อมูลส่วนบุคคลทราบเอง ว่ามีหรือน่าจะมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ดังต่อไปนี้

๑) ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูล

ส่วนบุคคลหรือไม่ โดยผู้ควบคุมข้อมูลส่วนบุคคลพึงดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว ทั้งในส่วนที่เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถยืนยันได้ว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

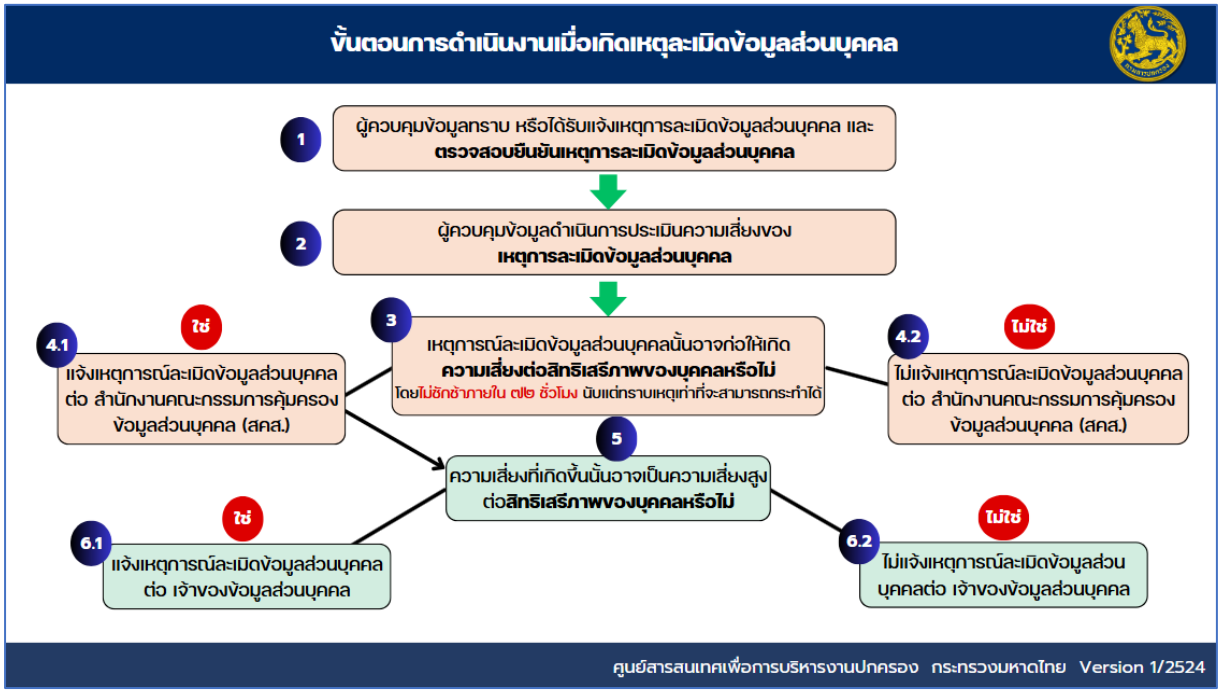
๒) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลตาม (๑) พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและหมาะสม

๓) เมื่อพิจารณาจากข้อเท็จจริงตาม (๑) แล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการณ์ละเมิดแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๔) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

๕) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

โดยสามารถสรุปเป็นขั้นตอนการแจ้งเหตุละเมิด ดังภาพ



ส่วนที่ ๑๑. การจ้างการประมวลผลหรือมอบหมายให้ประมวลผล

แนวปฏิบัติในการทำสัญญาจ้างการประมวลผลข้อมูลส่วนบุคคล หรือมอบหมายให้ผู้อื่นประมวลผลข้อมูลส่วนบุคคล ให้หน่วยงานปฏิบัติดังนี้

๑. ก่อนทำการจ้างหรือมอบหมายผู้ประมวลผลข้อมูล ต้องประเมินระบบ สอบทานและปรับปรุงมาตรการต่าง ๆ ในการคุ้มครองข้อมูลส่วนบุคคลของผู้รับจ้างหรือผู้ถูกมอบหมาย เพื่อให้แน่ใจว่าระบบการรักษาความมั่นคงปลอดภัยข้อมูลมีความเหมาะสม เพียงพอ รวมถึงต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ในส่วนของผู้รับจ้างหรือผู้รับมอบหมาย

๒. ในสัญญาจ้างหรือข้อตกลงการประมวลผล ต้องระบุวัตถุประสงค์ วิธีการเก็บข้อมูลการแจ้งเจ้าของข้อมูลส่วนบุคคล การใช้ การส่งและโอนข้อมูล และการทำลายข้อมูล

๓. คู่สัญญาต้องลงนามในสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลตามแบบฟอร์มที่กรมการปกครองกำหนด โดยมีแนวทาง ดังนี้

๓.๑ กรณีที่ ๑ ยังไม่ได้ดำเนินการจัดซื้อจัดจ้าง ในการจัดทำข้อกำหนดและขอบเขตการจ้าง (TOR) เพิ่มข้อตกลงการประมวลข้อมูลส่วนบุคคลเป็นข้อตกลงของสัญญา

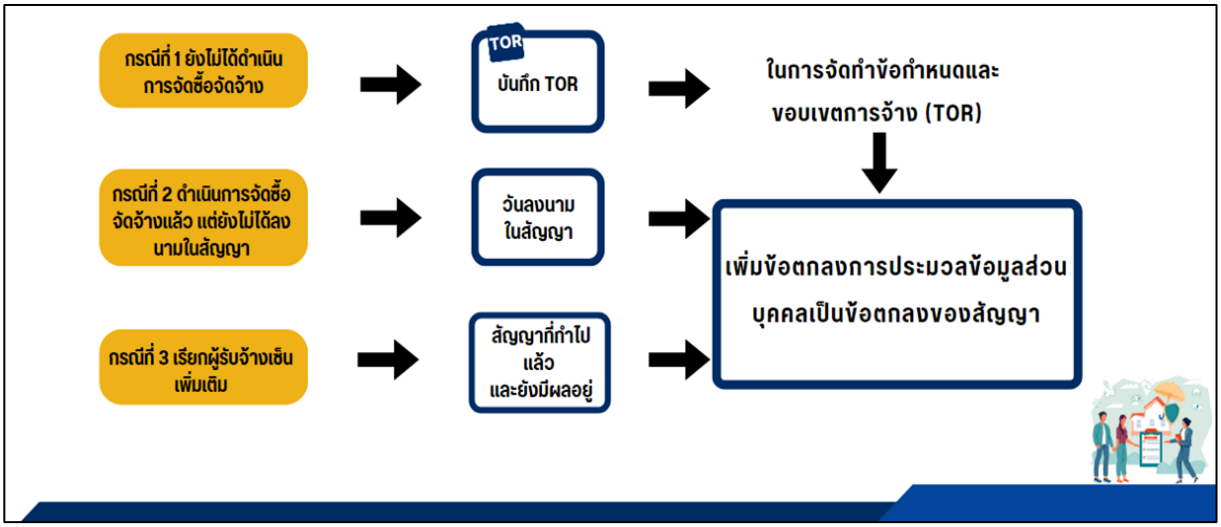
๓.๒ กรณีที่ ๒ ดำเนินการจัดซื้อจัดจ้างแล้ว แต่ยังไม่ได้ลงนามในสัญญา วันลงนามในสัญญาเพิ่มข้อตกลงการประมวลข้อมูลส่วนบุคคลเป็นข้อตกลงของสัญญา

๓.๓ กรณีที่ ๓ สัญญาที่ทำไปแล้วและยังมีผลอยู่ เรียกผู้รับจ้างเซ็นเพิ่มข้อตกลงการประมวลข้อมูลส่วนบุคคลเป็นข้อตกลงของสัญญา

๔. เมื่อมีการจ้างหรือมอบหมายให้มีการประมวลผลข้อมูล ต้องทำการควบคุมการประมวลผลและควบคุมการปฏิบัติให้เป็นไปตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลที่กรมการปกครองกำหนด

๕. เมื่อครบกำหนดการเก็บรักษาข้อมูล ต้องควบคุมให้ผู้รับประมวลผลทำลายข้อมูลตามกำหนด

โดยสามารถสรุปเป็นขั้นตอนการทำสัญญาจ้างการประมวลผลข้อมูลส่วนบุคคล ดังภาพ



ส่วนที่ ๑๒. การดำเนินการกับข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่กฎหมายมีผลบังคับใช้

กรมการปกครองกำหนดให้ทุกหน่วยงานภายใต้สังกัดดำเนินการตรวจสอบ แยกแยะ ข้อมูลส่วนบุคคล ที่ถูกเก็บรวมรวมไว้ก่อนวันที่กฎหมายมีผลบังคับใช้ ว่ายังเป็นข้อมูลส่วนบุคคลที่ยังมีความจำเป็นต้องเก็บไว้หรือไม่ หากหมดความจำเป็นที่จะต้องเก็บรักษาไว้ ก็ให้ดำเนินการลบทำลาย

ส่วนข้อมูลที่ยังมีความจำเป็นต้องเก็บรักษาไว้เพื่อใช้งานต่อไป ให้พิจารณาว่า เป็นข้อมูลที่ต้องขอความยินยอมก่อนการรวบรวมหรือไม่ (รายละเอียดในการพิจารณาขอให้ศึกษาในคู่มือปฏิบัติของข้อมูลส่วนบุคคลแต่ละประเภท) หากต้องขอความยินยอมให้ประสานงานกับเจ้าของข้อมูลและถ้าเจ้าของข้อมูลส่วนบุคคลไม่ประสงค์ ให้กรมการปกครองเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ดังกล่าว ก็ให้ดำเนินการยกเลิกความยินยอมได้ตามประสงค์

ส่วนที่ ๑๓. การขอความยินยอมและการถอนความยินยอม

การใช้ฐานความยินยอมในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นฐาน ในการประมวลผลที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะจัดการกับข้อมูลส่วนบุคคลของตนเองได้อย่างเต็มที่ซึ่งกรมการปกครองจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการประมวลผล ยกเว้น กรณีการประมวลผลข้อมูลส่วนบุคคล ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด

ภารกิจโดยส่วนใหญ่เกือบทั้งหมดของกรมการปกครองเป็นการดำเนินการ โดยใช้ฐานอำนาจตามกฎหมาย เนื่องจากมีความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่กรมการปกครองหรือเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข หรือประโยชน์สาธารณะ ที่สำคัญอื่น ๆ เป็นต้น และไม่ต้องขอความยินยอม

๑๓.๑ การเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องขอความยินยอมให้หน่วยงานที่ต้องการดำเนินการดังกล่าวประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ก่อนเริ่มดำเนินการเพื่อพิจารณาให้ความเห็นชอบแนวทางปฏิบัติทั้งการขอความยินยอมและการถอนความยินยอม เว้นแต่เป็นการดำเนินการตามที่คู่มือปฏิบัติได้กำหนดไว้

๑๓.๒ หน่วยงานควรเลือกใช้ฐานในการประมวลผลให้เหมาะสมกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลเนื่องจากฐานความยินยอมไม่สามารถใช้ได้ทุกกรณี เว้นแต่กรณีที่ต้องขอความยินยอมตามข้อกำหนดของกฎหมายอื่น ฐานความยินยอมจะเหมาะสมเมื่อการประมวลผลข้อมูลไม่ได้มีความจำเป็น

ตามเงื่อนไขสัญญา นอกจากนั้นการให้ความยินยอมจะต้องเป็นสิ่งที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเลือกได้ว่าจะให้หรือปฏิเสธก็ได้ และการปฏิเสธจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญาการขอความยินยอมจะต้องอาศัยหลักการกระทำโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness, and Transparency) โดยหน่วยงานจะต้องไม่ใช้ข้อความที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์และจะต้องคำนึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลใน การตัดสินใจให้ความยินยอม โดยการให้ความยินยอมจะต้องเป็นการสมัครใจ ดังนั้นการขอความยินยอมจะต้องระบุวัตถุประสงค์ในการประมวลผลข้อมูลอย่างชัดเจนว่าจะขอความยินยอมในเรื่องใด

๑๓.๓ เงื่อนไขในการใช้ฐานความยินยอมมีดังต่อไปนี้

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผย ข้อมูลนั้นๆได้ เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเมื่อใดก็ได้ การใช้ฐานความยินยอมนั้นจะต้องให้สิทธิเจ้าของข้อมูลส่วนบุคคลสามารถปฏิเสธไม่ให้ความยินยอมได้การขอความยินยอมจะต้องกระทำอย่างชัดเจนไม่คลุมเครือ ดังนั้นหน่วยงานจึงควรออกแบบแบบฟอร์มการขอความยินยอม ที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเห็นได้อย่างชัดเจนว่า หน่วยงานขอความยินยอมในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใดบ้าง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงอิสระของเจ้าของข้อมูลส่วนบุคคล ในการให้ความยินยอมทั้งนี้การขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms& Conditions) หรือข้อความในสัญญาการขอความยินยอมจะทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

๑๓.๔ หน่วยงานต้องไม่นำฐานความยินยอมและฐานสัญญามาปะปนกันต้องแยกให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาก็ควรระบุอยู่ในสัญญา ซึ่งการขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) เนื่องจากการกระทำดังกล่าวอาจทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการหรือมีผลต่อการใช้ผลิตภัณฑ์หรือบริการของหน่วยงาน

๑๓.๕ การใช้ฐานความยินยอมอาจเหมาะสมในสถานการณ์ที่จะประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เฉพาะเจาะจงมากกว่า และหน่วยงานไม่สามารถประมวลผลข้อมูลตามวัตถุประสงค์ที่เพิ่มเติมขึ้นมาใหม่เองได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หน่วยงานจะต้องขอความยินยอมใหม่หากต้องการประมวลผลข้อมูลเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่เคยได้รับความยินยอมไปแล้ว เว้นแต่หากพิจารณาแล้วว่าการประมวลผลเพื่อวัตถุประสงค์นั้นสามารถทำได้ภายใต้ฐานกฎหมายฐานอื่น

๑๓.๖ การขอความยินยอมสามารถทำได้หลายวิธีเช่น การยินยอมจากการเลือก ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจนเป็นลายลักษณ์อักษร หน่วยงานควรออกแบบให้เจ้าของข้อมูลส่วนบุคคลต้องมีการกระทำให้ความยินยอมอย่างชัดเจน (Clear Affirmative Action) เช่น การทำเป็นช่องเช็คถูก (Checkbox) โดยให้เจ้าของข้อมูลส่วนบุคคล กด/เขียน/เช็คเองได้ (Signatures or Ticks Indicating Consent) การขอความยินยอมในรูปแบบวาจา (Verbal Consent) สำหรับรูปแบบการขอความยินยอมนี้ ใช้ในกรณีที่มีการบันทึกความยินยอมในรูปแบบเสียง (Voice Record) ด้วยระบบดิจิทัล เช่น บันทึกผ่านการติดต่อกับเจ้าของข้อมูลส่วนบุคคลทาง Contact Center หรือผ่านทางระบบ Interactive Voice Response (IVR) โดยขอให้เจ้าของข้อมูลส่วนบุคคลกดปุ่มยืนยันการให้ความยินยอม ซึ่งหน่วยงานจะต้องมีกระบวนการพิสูจน์และยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคลก่อนทำการขอความยินยอมเพื่อให้มั่นใจว่าคู่สนทนาเป็นเจ้าของข้อมูลส่วนบุคคลจริง นอกจากนั้นหน่วยงานควรให้ข้อมูลแก่เจ้าของข้อมูลส่วนบุคคล อย่างเพียงพอต่อการตัดสินใจมีทางเลือกและเนื้อหาชัดเจน

ไม่ก่อให้เกิดความเข้าใจผิด และให้เจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมหรือไม่ให้ความยินยอมก็ได้ โดยสมัครใจไม่เป็นการบังคับ

๑๓.๗ การถอนความยินยอม (Withdraw of Consent)ทในกรณีที่ท่านได้ให้ความยินยอมไว้ ท่านมีสิทธิที่จะขอเพิกถอนความยินยอม ที่ให้ไว้กับหน่วยงานในการเก็บรวบรวม ใช้ หรือ เปิดเผย ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเมื่อใดก็ได้ และหน่วยงานจะต้องดำเนินการหยุดการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเคยได้ให้ความยินยอมไว้หากหน่วยงานไม่มีฐานโดยชอบด้วยกฎหมายอื่นที่จะทำการเก็บรวบรวมใช้หรือเปิดเผยต่อไปให้หน่วยงานดำเนินการลบข้อมูลออกการใช้สิทธิถอนความยินยอมผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม

ส่วนที่ ๑๔. การตรวจสอบและปรับปรุงระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

กรมการปกครอง อาจพิจารณาปรับปรุง แก้ไขหรือเปลี่ยนแปลงนโยบายนี้ตามที่เห็นสมควร และจะทำการแจ้งให้ท่านทราบผ่านช่องทางเว็บไซต์ www.dopa.go.th/pdpa โดยมีวันที่มีผลบังคับใช้ของแต่ละฉบับแก้ไขกำกับอยู่ อย่างไรก็ดี กรมการปกครอง ขอแนะนำให้ท่านโปรดตรวจสอบเพื่อรับทราบนโยบายฉบับใหม่อย่างสม่ำเสมอ ผ่านเว็บไซต์ หรือช่องทางเฉพาะกิจกรรมที่ กรมการปกครอง ดำเนินการ โดยเฉพาะก่อนที่ท่านจะทำการเปิดเผยข้อมูลส่วนบุคคลแก่กรมการปกครอง การรับบริการของ กรมการปกครอง ภายหลังการบังคับใช้นโยบายใหม่ ถือเป็นการรับทราบตามข้อตกลง ในนโยบายใหม่แล้ว ทั้งนี้ โปรดหยุดการเข้าใช้งานหากท่านไม่เห็นด้วยกับรายละเอียดในนโยบายฉบับนี้และ โปรดติดต่อมายัง กรมการปกครองเพื่อชี้แจงข้อเท็จจริงต่อไป

ส่วนที่ ๑๕. การควบคุมเอกสาร

กรมการปกครองมีการควบคุมเอกสาร แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล เอกสารที่เกี่ยวข้อง เพื่อให้ทุกหน่วยงานในสังกัดถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและมีประสิทธิภาพ ให้หน่วยงานปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ของกรมการปกครอง พ.ศ. ๒๕๖๗ แนบท้ายประกาศกรมการปกครอง เรื่องนโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๗

ส่วนที่ ๑๖. การกำกับดูแลการเก็บรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล

การเปิดเผยข้อมูลส่วนบุคคล กรมการปกครอง จะดำเนินการตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล โดยกรมการปกครอง อาจเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นอย่างจำกัดให้แก่หน่วยงานหรือบุคคลภายนอก ทั้งนี้กรมการปกครองห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้น โดย ไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือ มาตรา ๒๖ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

การนำข้อมูลส่วนบุคคลไปใช้ประโยชน์หรือเปิดเผย กรมการปกครอง อาจใช้ประโยชน์หรือเปิดเผยข้อมูลส่วนบุคคลให้แก่ผู้ปฏิบัติงานของ กรมการปกครอง หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลของกรมการปกครอง ได้ เพื่อการใช้ประโยชน์หรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่นนอกเหนือจากกรณีดังกล่าวจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน เว้นแต่เป็นกรณีที่ กรมการปกครองจะต้องปฏิบัติให้เป็นไปตามกฎหมายหรือมีกฎหมายบัญญัติให้กระทำได้ดำเนินการให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้ ซึ่งอาจรวมถึงการเปิดเผยข้อมูลส่วนบุคคลให้กับหน่วยงานต่อไปนี้

๑. หน่วยงานของรัฐซึ่งมีอำนาจหน้าที่ตาม

๒. หน่วยงานกำกับดูแลเรื่องข้อมูลส่วนบุคคล เช่น สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๓. บุคคลหรือหน่วยงานที่ กรมการปกครอง จ้างให้เก็บข้อมูลหรือประมวลผลข้อมูลส่วนบุคคล

๔. หน่วยงานที่มีอำนาจตามกฎหมายอื่น ๆ เพื่อดำเนินวัตถุประสงค์ ด้านการตรวจสอบการดำเนินงานของกรมการปกครอง

๕. กรมการปกครอง จะดูแลไม่ให้ผู้ปฏิบัติงานของ กรมการปกครอง หรือผู้ประมวลผลข้อมูลส่วนบุคคลนำข้อมูลส่วนบุคคลไปใช้ประโยชน์หรือเปิดเผยแก่บุคคลอื่นนอกเหนือไปจากวัตถุประสงค์ในการดำเนินงานตามภารกิจของ กรมการปกครอง เว้นแต่ จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน หรือเป็นกรณีที่ กรมการปกครอง จะต้องปฏิบัติให้เป็นไปตามกฎหมายหรือมีกฎหมายบัญญัติให้กระทำได้

๖. ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลเป็นบุคคลภายนอก กรมการปกครอง จะจัดให้มีข้อตกลงระหว่างกรมการปกครอง กับผู้ประมวลผลข้อมูล เพื่อกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัย การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามที่กรมการปกครองกำหนดเท่านั้น ทั้งนี้ กรมการปกครอง จะจัดให้มีการควบคุมและตรวจสอบการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายและข้อตกลงดังกล่าวอย่างเคร่งครัดด้วย

๗. กรมการปกครองจะกำกับดูแลมิให้ผู้ที่ไม่มีหน้าที่หรือไม่ได้รับมอบหมายเก็บรวบรวมข้อมูลส่วนบุคคล นำไปใช้ประโยชน์ เปิดเผย แสดง หรือทำให้ปรากฏในลักษณะอื่นใดแก่บุคคลอื่น นอกเหนือวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ เว้นแต่กรณีที่กฎหมายอนุญาตให้เปลี่ยนแปลงวัตถุประสงค์การใช้ข้อมูลได้

๘. กรมการปกครองอาจใช้เทคโนโลยีคุกกี้ (Cookies) เพื่อเก็บรวบรวมข้อมูลพฤติกรรมของเจ้าของข้อมูลส่วนบุคคล เกี่ยวกับการเข้าถึง การใช้งาน หรือการรับบริการผ่านเว็บไซต์และแอปพลิเคชันของกรมการปกครองเพื่อประโยชน์ในการอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการเข้าถึง การใช้งาน หรือการรับบริการผ่านเว็บไซต์และแอปพลิเคชัน ของกรมการปกครอง

๙. กรมการปกครองอาจทำการเก็บข้อมูลส่วนบุคคลไว้ในระบบประมวลผลแบบคลาวด์ โดยใช้บริการจากบุคคลที่สามไม่ว่าตั้งอยู่ในประเทศไทยหรือต่างประเทศหรือ ผู้ให้บริการเซิร์ฟเวอร์ สำหรับเว็บไซต์ การวิเคราะห์ข้อมูล การประมวลผลการจ่ายและรับชำระเงิน การทำคำสั่งซื้อ การให้บริการโครงสร้างพื้นฐานเกี่ยวกับเทคโนโลยีสารสนเทศ เป็นต้น

ในกรณีที่กรมการปกครองจำเป็นต้องส่งข้อมูลส่วนบุคคลให้แก่บุคคลภายนอก กรมการปกครองจะดำเนินการตามขั้นตอนที่เหมาะสม เพื่อให้มั่นใจว่า บุคคลภายนอกจะดูแลข้อมูลส่วนบุคคลของเจ้าของข้อมูลไม่ให้เกิด การสูญหาย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การใช้ การดัดแปลง การเปิดเผย หรือการใช้งานที่ไม่ถูกต้อง

๑๐. ข้อมูลส่วนบุคคลที่ กรมการปกครอง เก็บรวบรวมจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล โดยที่แหล่งข้อมูลดังกล่าวมีอำนาจหน้าที่ มีเหตุผลที่ชอบด้วยกฎหมายหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้วในการเปิดเผยข้อมูลแก่กรมการปกครอง เช่น การเชื่อมโยงบริการดิจิทัลของหน่วยงานของรัฐในการให้บริการเพื่อประโยชน์สาธารณะแบบเบ็ดเสร็จแก่เจ้าของข้อมูลส่วนบุคคลเอง การรับข้อมูลส่วนบุคคลจากหน่วยงานของรัฐแห่งอื่นในฐานะที่ กรมการปกครอง มีหน้าที่ตามพันธกิจในการดำเนินการจัดให้มีศูนย์แลกเปลี่ยนข้อมูลกลางเพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล รวมถึงจากความจำเป็นเพื่อให้บริการตามสัญญาที่อาจมีการแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานคู่สัญญาได้

ส่วนที่ ๑๗. การติดต่อสอบถามหรือใช้สิทธิ

หากท่านมีข้อสงสัย ข้อเสนอแนะหรือข้อกังวลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของ กรมการปกครอง หรือเกี่ยวกับนโยบายนี้ หรือท่านต้องการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านสามารถติดต่อสอบถามได้ที่

๑. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

รองอธิบดีกรมการปกครอง ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ
๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : dpo@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๘๒-๑๐๔๗

๒. ผู้ควบคุมข้อมูลส่วนบุคคล กรมการปกครอง

๖๖๖ อาคารธนาลงกรณ์ทาวเวอร์ ชั้น ๑๑ ถนนบรมราชชนนี
แขวงบางบำหรุ เขตบางพลัด กรุงเทพฯ ๑๐๗๐๐
ช่องทางการติดต่อ : webmaster@dopa.go.th
หมายเลขโทรศัพท์ : ๐๒-๒๒๔๑-๐๑๕๑-๘

Logo คู่สัญญา

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล

(Personal Data Sharing Agreement)

ระหว่าง

กรมการปกครอง กับ .....(ชื่อคู่สัญญาอีกฝ่าย) .....

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ทำขึ้น เมื่อวันที่ .... ๒๕๖๘ ณ กรมการปกครอง

โดยที่ กรมการปกครอง ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “ปค.” ฝ่ายหนึ่ง ได้ตกลงใน.... *(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก) .... ฉบับลงวันที่ ..... *(ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก) ..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “สัญญาหลัก” กับ ..... (ระบุชื่อคู่สัญญาอีกฝ่าย) ..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “..... (ระบุชื่อเรียกคู่สัญญาอีกฝ่าย .....” อีกฝ่ายหนึ่ง รวมเรียกว่า “คู่สัญญา”

เพื่อให้บรรลุวัตถุประสงค์ภายใต้ความตกลงของสัญญาหลัก คู่สัญญามีความจำเป็นต้องแบ่งปัน โอน แลกเปลี่ยน หรือเปิดเผย (รวมเรียกว่า “แบ่งปัน”) ข้อมูลส่วนบุคคลที่ตนเก็บรักษาแก่อีกฝ่าย ซึ่งข้อมูลส่วนบุคคลที่แต่ละฝ่าย เก็บรวมรวม ใช้หรือเปิดเผย (รวมเรียกว่า “ประมวลผล”) นั้น แต่ละฝ่ายต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล กล่าวคือแต่ละฝ่ายต่างเป็นผู้มีอำนาจตัดสินใจกำหนดรูปแบบ และกำหนดวัตถุประสงค์ ในการประมวลผลข้อมูลส่วนบุคคลในข้อมูลที่ตนต้องแบ่งปัน ภายใต้ข้อตกลงนี้

ด้วยเหตุนี้ คู่สัญญาจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาหลัก เพื่อเป็นหลักฐานการแบ่งปันข้อมูลส่วนบุคคลระหว่างคู่สัญญาและเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่ออกตามความใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้ และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๑. คู่สัญญารับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยคู่สัญญาแต่ละฝ่าย จะดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

๒. ข้อมูลส่วนบุคคลที่คู่สัญญาแบ่งปันกัน คู่สัญญาแต่ละฝ่ายตกลงแบ่งปันข้อมูลส่วนบุคคลดังรายการต่อไปนี้แก่คู่สัญญาอีกฝ่าย

ข้อมูลส่วนบุคคลที่แบ่งปันโดย ปค.	**วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล**
๑. (ระบุรายการข้อมูลส่วนบุคคลที่ ปค. แบ่งปันให้คู่สัญญาอีกฝ่าย เช่น ชื่อ นามสกุลของเจ้าหน้าที่ หมายเลขโทรศัพท์ ข้อมูลผู้ใช้งานแอปพลิเคชันทางรัฐ)	๑. เพื่อความจำเป็นในการ ... (ระบุเหตุผลความจำเป็นในการแบ่งปันข้อมูลส่วนบุคคล ระหว่างคู่สัญญา เช่น เพื่อการเชื่อมโยงแสดงผลข้อมูลในแอปพลิเคชัน)
๑. ...	๒. ...
๒. ...	๓. ...
ข้อมูลส่วนบุคคลที่แบ่งปันโดย (ระบุชื่อคู่สัญญาอีกฝ่าย)	**วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล**
๑. (ระบุรายการข้อมูลส่วนบุคคลที่คู่สัญญาอีกฝ่ายแบ่งปันแก่ สพร. เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ ข้อมูล Location)	๑. เพื่อความจำเป็นในการ ... (ระบุเหตุผลความจำเป็นในการแบ่งปันข้อมูลส่วนบุคคล ระหว่างคู่สัญญา เช่น เพื่อการเชื่อมโยงแสดงผลข้อมูลในแอปพลิเคชัน)
๒. ...	๒. ...
๓. ...	๓. ...

๓. ฐานกฎหมายในการแบ่งปันข้อมูลส่วนบุคคล ภายใต้วัตถุประสงค์ที่ระบุในข้อ ๒ คู่สัญญาแต่ละฝ่ายมีฐานกฎหมายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้ ในการแบ่งปันข้อมูลส่วนบุคคลแก่คู่สัญญาอีกฝ่าย (แต่ละฝ่ายอาจใช้ฐานกฎหมายที่ต่างกันในการแบ่งปันข้อมูลส่วนบุคคล)

ฐานกฎหมายของ ปค.
1. (ระบุฐานกฎหมายในการแบ่งปันข้อมูลส่วนบุคคลของ ปค. เช่น เพื่อการให้บริการตามสัญญากับเจ้าของข้อมูลส่วนบุคคล) 2. เพื่อการดำเนินภารกิจสาธารณะหรือใช้อำนาจรัฐที่ ปค. ได้รับตาม... 3. ได้รับความยินยอมในการเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคล
ฐานกฎหมายของ (ระบุชื่อคู่สัญญาอีกฝ่าย)
1. (ระบุฐานกฎหมายในการแบ่งปันข้อมูลส่วนบุคคลของคู่สัญญาอีกฝ่าย เช่น เพื่อการให้บริการตามสัญญากับเจ้าของข้อมูลส่วนบุคคล) 2. ได้รับความยินยอมในการเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคล

๔. คู่สัญญารับทราบและตกลงว่า แต่ละฝ่ายต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของข้อมูลส่วนบุคคลที่ตนประมวลผล และต่างอยู่ภายใต้บังคับในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบทบัญญัติที่เกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคลต่างหากจากกัน

๕. คู่สัญญารับรองและยืนยันว่า ก่อนการแบ่งปันข้อมูลส่วนบุคคลแก่อีกฝ่าย ตนได้ดำเนินการแจ้งข้อมูลที่จำเป็นเกี่ยวกับการแบ่งปันข้อมูลและขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และ/หรือ มีฐานกฎหมายหรืออำนาจหน้าที่โดยชอบด้วยกฎหมายให้สามารถเปิดเผยข้อมูลส่วนบุคคลให้อีกฝ่าย และให้อีกฝ่ายสามารถทำการประมวลผลข้อมูลส่วนบุคคลที่ได้รับนั้นตามวัตถุประสงค์ที่ได้ตกลงกันอย่างถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว

๖. คู่สัญญารับรองว่า คู่สัญญาฝ่ายที่แบ่งปันข้อมูลส่วนบุคคล จะไม่ถูกจำกัดสิทธิ ยับยั้งหรือมีข้อห้ามใด ๆ ในการ

๖.๑ ประมวลผลข้อมูลส่วนบุคคลที่ตนเป็นฝ่ายแบ่งปัน ภายใต้วัตถุประสงค์ที่กำหนดในข้อตกลงฉบับนี้

๖.๒ แบ่งปันส่วนบุคคลไปยังคู่สัญญาอีกฝ่ายเพื่อการปฏิบัติหน้าที่ตามข้อตกลงฉบับนี้

๗. คู่สัญญาจะทำการประมวลผลข้อมูลส่วนบุคคลที่รับมาจากอีกฝ่ายเพียงเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ที่ได้กำหนดในข้อ ๒ ของข้อตกลงฉบับนี้ และแต่ละฝ่ายจะไม่ประมวลผลข้อมูลเพื่อวัตถุประสงค์อื่นเว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือเป็นความจำเป็นเพื่อปฏิบัติตามกฎหมายเท่านั้น

๘. คู่สัญญารับรองว่าจะควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลที่ได้รับจากอีกฝ่ายภายใต้ข้อตกลงฉบับนี้ รักษาความลับและปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ตามข้อตกลงฉบับนี้เท่านั้น โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วน เป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของสัญญาหลัก หรือกฎหมายที่เกี่ยวข้องจะระบุหรือบัญญัติไว้เป็นประการอื่น

๙. คู่สัญญารับรองว่าจะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น

๑๐. คู่สัญญาฝ่ายที่รับข้อมูลจะไม่เปิดเผยข้อมูลส่วนบุคคลที่ได้รับจากฝ่ายที่โอนข้อมูลแก่บุคคลของคู่สัญญาฝ่ายที่รับข้อมูลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องในการประมวลผล หรือบุคคลภายนอกใด ๆ เว้นแต่ที่มีความจำเป็นต้องกระทำตามหน้าที่ในสัญญาหลัก ข้อตกลงฉบับนี้หรือเพื่อปฏิบัติตามกฎหมายที่ใช้บังคับ หรือ ที่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากคู่สัญญาฝ่ายที่โอนข้อมูลก่อน

๑๑. คู่สัญญาจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศกำหนดและ/หรือตามมาตรฐานสากล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูล เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ ลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

๑๒. กรณีที่คู่สัญญาฝ่ายหนึ่งฝ่ายใด พบพฤติการณ์ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่แบ่งปันกันภายใต้ข้อตกลงฉบับนี้ ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ ลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย คู่สัญญาฝ่ายที่พบเหตุดังกล่าวจะดำเนินการแจ้งให้คู่สัญญาอีกฝ่ายทราบโดยทันทีภายในเวลาไม่เกิน.... (ระบุเวลาเป็นหน่วยชั่วโมงที่คู่สัญญาต้องแจ้งเหตุแก่คู่สัญญาอีกฝ่าย เช่น ภายใน 24 ชั่วโมงหรือ 48 ชั่วโมง ทั้งนี้ไม่ควรเกิน 48 ชั่วโมง เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุดังกล่าวแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง) .... ชั่วโมง

๑๓. การแจ้งถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นภายใต้ข้อตกลงนี้ คู่สัญญาแต่ละฝ่ายจะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่อีกฝ่ายภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนด ดังต่อไปนี้

๑๓.๑ รายละเอียดของลักษณะและผลกระทบที่อาจเกิดขึ้นของการละเมิด

๑๓.๒ มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด

๑๓.๓ ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด หากมีปรากฏ

๑๓.๔ ข้อมูลอื่น ๆ เกี่ยวข้องกับการละเมิด

๑๔. คู่สัญญาตกลงจะให้ความช่วยเหลืออย่างสมเหตุสมผลแก่อีกฝ่าย เพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลที่ใช้บังคับ ในการตอบสนองต่อข้อเรียกร้องใด ๆ ที่สมเหตุสมผลจากการใช้สิทธิต่าง ๆ ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคล โดยพิจารณาถึงลักษณะการประมวลผล ภาระหน้าที่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับ และข้อมูลส่วนบุคคลที่แต่ละฝ่ายประมวลผล

ทั้งนี้ กรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อคู่สัญญาฝ่ายหนึ่งฝ่ายใด เพื่อใช้สิทธิในข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบหรือได้รับมาจากอีกฝ่าย คู่สัญญาฝ่ายที่ได้รับคำร้องจะต้องดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่คู่สัญญาซึ่งเป็นฝ่ายโอนข้อมูลโดยทันที โดยคู่สัญญาฝ่ายที่รับคำร้องนั้นจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการจัดการตามคำขอหรือข้อร้องเรียนของเจ้าของข้อมูลส่วนบุคคลนั้นด้วย

๑๕. หากคู่สัญญาฝ่ายหนึ่งฝ่ายใดมีความจำเป็นจะต้องเปิดเผยข้อมูลส่วนบุคคลที่ได้รับจากอีกฝ่ายไปยังต่างประเทศ การส่งออกซึ่งข้อมูลส่วนบุคคลดังกล่าวจะต้องได้รับปกป้องตามมาตรฐานการส่งข้อมูลระหว่างประเทศตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศที่ส่งข้อมูลไปนั้นกำหนด ทั้งนี้ คู่สัญญาทั้งสองฝ่ายตกลงที่จะเข้าทำสัญญาใด ๆ ที่จำเป็นต่อการปฏิบัติตามกฎหมายที่ใช้บังคับกับการโอนข้อมูล

๑๖. คู่สัญญาแต่ละฝ่ายอาจใช้ผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อทำการประมวลผลข้อมูลส่วนบุคคลที่โอนและรับโอน โดยคู่สัญญาฝ่ายนั้นจะต้องทำสัญญากับผู้ประมวลผลข้อมูลเป็นลายลักษณ์อักษร ซึ่งสัญญาดังกล่าวจะต้องมีเงื่อนไขในการคุ้มครองข้อมูลส่วนบุคคลที่โอนและรับโอนไม่น้อยไปกว่าเงื่อนไขที่ได้ระบุไว้ในข้อตกลงฉบับนี้ และเงื่อนไขทั้งหมดต้องเป็นไปตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อหลีกเลี่ยงข้อสงสัย หากคู่สัญญาฝ่ายหนึ่งฝ่ายใดได้ว่าจ้างหรือมอบหมายผู้ประมวลผลข้อมูลส่วนบุคคล คู่สัญญาฝ่ายนั้นยังคงต้องมีความรับผิดต่ออีกฝ่ายสำหรับการกระทำการหรือละเว้นกระทำการใด ๆ ของผู้ประมวลผลข้อมูลส่วนบุคคลนั้น

๑๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น คู่สัญญาจะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ตนได้รับจากอีกฝ่ายภายใต้ข้อตกลงฉบับนี้ภายใน.... (ระบุจำนวนวันที่จะทำการลบทำลายข้อมูล) .... วัน นับแต่วันที่ดำเนินการประมวลผลตามวัตถุประสงค์ภายใต้ข้อตกลงฉบับนี้เสร็จสิ้น หรือวันที่คู่สัญญาได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกสัญญาหลักแล้วแต่กรณีใดจะเกิดขึ้นก่อน

ทั้งนี้ ในกรณีที่ปรากฏว่าคู่สัญญาฝ่ายหนึ่งฝ่ายใดหมดความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลที่ตนได้รับจากอีกฝ่ายตามข้อตกลงฉบับนี้ก่อนสิ้นระยะเวลาตามวรรคหนึ่ง คู่สัญญาฝ่ายนั้นจะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ตนได้รับตามข้อตกลงฉบับนี้ทันที

๑๘. คู่สัญญาแต่ละฝ่ายจะต้องชดใช้ความเสียหายให้แก่อีกฝ่ายในค่าปรับ ความสูญหายหรือเสียหายใด ๆ ที่เกิดขึ้นกับฝ่ายที่ไม่ได้ผิดเงื่อนไข อันเนื่องมาจากการฝ่าฝืนข้อตกลงฉบับนี้ แม้ว่าจะมีข้อจำกัดความรับผิดภายใต้สัญญาหลักก็ตามw

๑๙. หน้าที่และความรับผิดของคู่สัญญาในการปฏิบัติตามข้อตกลงฉบับนี้จะสิ้นสุดลงนับแต่วันที่การดำเนินการตามสัญญาหลักเสร็จสิ้นลง หรือ วันที่คู่สัญญาได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกสัญญาหลัก แล้วแต่กรณีใดจะเกิดขึ้นก่อน อย่างไรก็ดี การสิ้นผลลงของข้อตกลงฉบับนี้ ไม่กระทบต่อหน้าที่ของคู่สัญญาแต่ละฝ่ายในการลบหรือทำลายข้อมูลส่วนบุคคลตามที่ได้กำหนดในข้อ ๑๗ ของข้อตกลงฉบับนี้

ในกรณีที่ข้อตกลง คำรับรอง การเจรจา หรือข้อผูกพันใดที่คู่สัญญามีต่อกันไม่ว่าด้วยวาจาหรือเป็นลายลักษณ์อักษรใดขัดหรือแย้งกับข้อตกลงที่ระบุในข้อตกลงฉบับนี้ ให้ใช้ข้อความตามข้อตกลงฉบับนี้บังคับ

ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว เพื่อเป็นหลักฐานแห่งการนี้ ทั้งสองฝ่ายจึงได้ลงนามไว้เป็นหลักฐานต่อหน้าพยาน ณ วัน เดือน ปี ที่ระบุข้างต้น

ลงชื่อ	ลงชื่อ .....
(.....)	(.....)
.....	.....
ลงชื่อ ..... พยาน	ลงชื่อ ..... พยาน
(.....)	(.....)
.....	.....

ร่าง

รายการประเมินคู่ค้า/คู่สัญญา (Vendor/Contractor Assessment)

ให้หน่วยงานที่รับผิดชอบจัดทำแบบการประเมินนี้ประกอบกับการจัดซื้อจัดจ้างผู้ประมวลผลข้อมูลส่วนบุคคลทุกกรณี
- รายการใดที่ไม่เกี่ยวข้องกับกิจกรรมการประมวลผลตามสัญญา ให้ระบุว่า “N/A”
- การประเมินให้อ้างอิงไปยังกิจกรรมที่ระบุไว้ตาม ROP ของหน่วยงานเป็นหลัก
– กรณีที่ผลการประเมินระดับความเสี่ยงสูง ให้หน่วยงานหลีกเลี่ยงไม่ใช้บริการดังกล่าว ในกรณีที่จำเป็นจะต้องให้เหตุผลชี้แจงประกอบการพิจารณาอนุมัติ
- กรณีที่ผลการประเมินระดับความเสี่ยงปานกลาง ให้หน่วยงานคัดเลือกผู้ใช้บริการด้วยความระมัดระวังและอาจกำหนดเงื่อนไขการทำงานร่วมกันเพิ่มเติมตามที่เหมาะสมประกอบการพิจารณาอนุมัติ
- ให้หน่วยงานที่รับผิดชอบทำความเห็นประกอบไว้ว่าเหมาะสมที่จะใช้บริการหรือไม่ อย่างไร
- ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำความเห็นประกอบ
- ให้ทบทวนการประเมินดังกล่าวเป็นอย่างน้อยปีละหนึ่งครั้ง หรือตามที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๑.ข้อมูลทั่วไป

ชื่อคู่ค้า / คู่สัญญา	
รายละเอียดของคู่ค้า / คู่สัญญา * ประเภทของบริการและรายละเอียดที่เกี่ยวข้อง	
สถานะการให้บริการ / การดำเนินการ * ดำเนินการอยู่ / ไม่มีการดำเนินการ	
ที่อยู่ที่ติดต่อ	
หน่วยงานที่รับผิดชอบ * ส่วนงานหรือฝ่ายงานที่ใช้บริการ	
กิจกรรมการประมวลผลที่ใช้บริการ * อ้างอิงไปที่กิจกรรมใน ROP ID	

ระบบงานที่เกี่ยวข้องกับการบริการ * อ้างอิงไปที่ Assets/Databases	
สัญญาการใช้บริการ * อ้างอิงไปที่สัญญาและกองกฎหมายที่ตรวจสอบ	
การจ้างช่วง (Sub-Processor) * มีการจ้างช่วงหรือไม่	
สถานที่ที่จัดเก็บข้อมูล (Hosting Location) * ระบุสถานที่และประเทศที่ตั้ง	
ผู้ให้บริการจัดเก็บข้อมูล (Hosting Provider) * ระบุผู้ให้บริการ	
เอกสารมาตรฐานที่ได้รับรอง * ISO๒๗๐๐๑ / NIST / GDPR Approved Code of Conduct etc.	
มีข้อมูลส่วนบุคคลที่ส่งให้ดำเนินการ หรือไม่ * มี / ไม่มี	
ประเภทเจ้าของข้อมูลที่เกี่ยวข้อง * อ้างอิงตาม ROP	
ข้อมูลส่วนบุคคลที่ส่งให้ดำเนินการ * ระบุ field ข้อมูล	

๒. การคุ้มครองข้อมูลส่วนบุคคล

มาตรการความเป็นส่วนตัว	
ข้อมูลส่วนบุคคลที่ส่งให้เป็นข้อมูลที่เปิดเผยสาธารณะอยู่ก่อนแล้วหรือไม่ * ใช่ / ไม่ใช่	
มีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลหรือไม่ * มี / ไม่มี	
ลักษณะของการแจ้งรายละเอียดการประมวลผล * อ่านง่ายเข้าใจง่าย * เข้าถึงง่าย * ไม่มีค่าใช้จ่าย	
ระดับความเสี่ยงของการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานที่รับผิดชอบประเมิน * สูง / กลาง / ต่ำ * หน่วยงานประเมินจากข้อมูลข้างต้นประกอบกับกิจกรรมตาม ROP ที่ระบุ	

มาตรการความมั่นคงปลอดภัย	
มาตรการเชิงเทคนิคเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล ระบุรายละเอียด เช่น * SOPs * Access control lists * Secure email * Virtual privacy networks * File-based encryption * Secure, dedicated line transfer	
มาตรการเชิงองค์กรเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล ระบุรายละเอียด เช่น * Security card access – building * Security card access – room or work area * Locked file cabinets * Clean Desk Policy / Procedure * Data Breach Notification	
มาตรการทางกายภาพเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล ระบุรายละเอียด เช่น * Secure zones be defined and protected by appropriate entry controls * Intruder detection systems * Automatic fire suppression system	
ระดับความเสี่ยงของความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่หน่วยงานที่รับผิดชอบประเมิน * สูง / กลาง / ต่ำ * หน่วยงานประเมินจากข้อมูลข้างต้นประกอบกับกิจกรรมตาม ROP ที่ระบุ	
มาตรการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ	
มีการส่งข้อมูลส่วนบุคคลไปนอกองค์กรหรือไม่ * มี / ไม่มี	
มีการส่งข้อมูลส่วนบุคคลไปต่างประเทศหรือไม่ * มี / ไม่มี	
ประเทศที่รับข้อมูลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decision) หรือไม่ * มี / ไม่มี	
มาตรการความปลอดภัยที่เหมาะสม (Appropriate Safeguards) อื่นๆ * ISO๒๗๐๐๑ / NIST / GDPR Approved Code of Conduct etc.	
ความเห็นของส่วนงาน	

* เช่น กรณีจำเป็นต้องใช้บริการที่มีระดับความเสี่ยงของความมั่นคงปลอดภัยสูง หรือมีการส่งข้อมูลส่วนบุคคลตามคำถาม ข้างต้น แต่ไม่มีมาตรการรองรับที่เหมาะสม เป็นต้น
ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

Logo คู่สัญญา

ข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม

(Joint Controller Agreement)

ระหว่าง

กรมการปกครอง กับ ...(ชื่อคู่สัญญา)...

ข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (“**ข้อตกลง**”) ฉบับนี้ ทำขึ้นเมื่อวันที่ ... (ระบุวันที่ลงนาม)... ณ กรมการปกครอง

โดยที่ กรมการปกครอง ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**ปค.**” ฝ่ายหนึ่ง ได้ตกลงใน ...(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญา)... ฉบับลงวันที่ ... (ระบุวันที่ลงนาม)... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**สัญญาหลัก**” กับ ...(ชื่อคู่สัญญา)... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “...(ชื่อเรียกคู่สัญญา)...” อีกฝ่ายหนึ่ง รวมทั้งสองฝ่ายว่า “**คู่สัญญา**”

เพื่อให้บรรลุตามวัตถุประสงค์ที่คู่สัญญาได้ตกลงกันภายใต้สัญญาหลัก คู่สัญญามีความจำเป็นต้องร่วมกันเก็บรวบรวม ใช้หรือเปิดเผย (รวมเรียกว่า “**ประมวลผล**”) ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยที่คู่สัญญามีอำนาจตัดสินใจ กำหนดรูปแบบ รวมถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นร่วมกัน ในลักษณะของผู้ควบคุมข้อมูลส่วนบุคคลร่วม

คู่สัญญาจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาหลัก เพื่อกำหนดขอบเขตอำนาจหน้าที่และความรับผิดชอบของคู่สัญญาในการร่วมกันประมวลผลข้อมูลส่วนบุคคล โดยข้อตกลงนี้ใช้บังคับกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลทั้งสิ้นที่ดำเนินการโดยคู่สัญญา รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งถูกหรืออาจถูกมอบหมายให้ประมวลผลข้อมูลส่วนบุคคลโดยคู่สัญญา ทั้งนี้ เพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายอื่น ๆ ที่ออกตามความของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**กฎหมายคุ้มครองข้อมูลส่วนบุคคล**” ทั้งที่มีผลใช้บังคับอยู่ ณ วันที่ทำข้อตกลงฉบับนี้ และที่อาจมีเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังต่อไปนี้

๑. ภายใต้ข้อตกลงของการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมนี้

๑.๑. คู่สัญญาร่วมกันกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลดังรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (“**กิจกรรมการประมวลผลข้อมูลส่วนบุคคลหลัก**”) ดังต่อไปนี้

ในส่วนนี้ให้ระบุชื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่คู่สัญญาทำร่วมกัน เช่น ร่วมกันดำเนินการเพื่อให้บรรลุภารกิจหรือวัตถุประสงค์ที่กำหนดขึ้นร่วมกัน เช่น พัฒนาและให้บริการแอปพลิเคชันสำหรับรับบริการจดทะเบียนก่อตั้งธุรกิจ ก่อสร้างอาคาร และนำเข้าสินค้า (ซึ่งภายใต้กิจกรรมหลักประกอบด้วยกิจกรรมย่อย ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลแต่ละรายรับผิดชอบ)

ทั้งนี้ หากมีกิจกรรมหลักมากกว่า ๑ กิจกรรม ให้ระบุเป็นข้อ ๆ

นอกจากนี้ จากรายการกิจกรรมการประมวลผลหลักที่คู่สัญญาร่วมกันกำหนดวัตถุประสงค์ข้างต้น คู่สัญญาแต่ละฝ่ายมีการประมวลผลข้อมูลส่วนบุคคล (“**กิจกรรมการประมวลผลข้อมูลส่วนบุคคลย่อย**”) ดังรายละเอียดต่อไปนี้

๑.๒. กิจกรรมการประมวลผลข้อมูลส่วนบุคคลย่อยซึ่งดำเนินการโดย ปค.

รายการกิจกรรมการประมวลผล	**ฐานกฎหมายที่ใช้ในการประมวลผล**	**รายการข้อมูลส่วนบุคคลที่ใช้ประมวลผล**
(ระบุรายการ “กิจกรรม” การประมวลผลข้อมูลส่วนบุคคลที่ ปค. ดำเนินการภายใต้ขอบเขตของสัญญาหลัก เช่น การเก็บข้อมูลจากเอกสารลงทะเบียน, การเชื่อมโยงข้อมูล, การยืนยันตัวตน เป็นต้น)	(ระบุ “ฐานกฎหมาย” การประมวลผลข้อมูลส่วนบุคคลที่ ปค. ดำเนินการตามรายการกิจกรรม)	(ระบุรายการข้อมูลส่วนบุคคลที่ ปค. ใช้เพื่อประมวลผลตามกิจกรรมที่ระบุ เช่น ชื่อนามสกุล วันเกิด เบอร์โทรศัพท์ เป็นต้น) ... ...

๑.๓. กิจกรรมการประมวลผลข้อมูลส่วนบุคคลย่อยซึ่งดำเนินการโดย...(ชื่อเรียกคู่สัญญา)...

รายการกิจกรรมการประมวลผล	**ฐานกฎหมายที่ใช้ในการประมวลผล**	**รายการข้อมูลส่วนบุคคลที่ใช้ประมวลผล**
(ระบุรายการ “กิจกรรม” การประมวลผลข้อมูลส่วนบุคคลที่คู่สัญญาอีกฝ่าย ดำเนินการภายใต้ขอบเขตของสัญญาหลัก เช่น การเก็บข้อมูลจากเอกสารลงทะเบียน, การเชื่อมโยงข้อมูล, การยืนยันตัวตน เป็นต้น)	(ระบุ “ฐานกฎหมาย” การประมวลผลข้อมูลส่วนบุคคลที่ คู่สัญญาอีกฝ่ายดำเนินการตามรายการกิจกรรม)	(ระบุรายการข้อมูลส่วนบุคคลที่คู่สัญญาอีกฝ่ายใช้เพื่อประมวลผลตามกิจกรรมที่ระบุ เช่น ชื่อ นามสกุล วันเกิด เบอร์โทรศัพท์ เป็นต้น) ... ...

ทั้งนี้ คู่สัญญาแต่ละฝ่ายรับรองว่าจะดำเนินการประมวลผลข้อมูลส่วนบุคคลดังรายละเอียดข้างต้นให้เป็นไปตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยเฉพาะอย่างยิ่งในเรื่องความชอบด้วยกฎหมายของการประมวลผลข้อมูลภายใต้ความเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม โดยคู่สัญญาแต่ละฝ่ายจะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศกำหนดและ/หรือตามมาตรฐานสากล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูล เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย เป็นต้น

๒. คู่สัญญารับรองว่าจะควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ รักษาความลับและปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ตามข้อตกลงฉบับนี้เท่านั้น โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของสัญญาหลัก หรือกฎหมายที่เกี่ยวข้องจะระบุหรือบัญญัติไว้เป็นประการอื่น

๓. คู่สัญญารับรองว่าจะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น

๔. คู่สัญญาจะไม่เปิดเผยข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้แก่บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการประมวลผล หรือบุคคลภายนอก เว้นแต่ที่มีความจำเป็นต้องกระทำตามหน้าที่ในสัญญาหลัก ข้อตกลงฉบับนี้หรือเพื่อปฏิบัติตามกฎหมายที่ใช้บังคับ หรือ ที่ได้รับความยินยอมจากคู่สัญญาอีกฝ่ายก่อน

๕. คู่สัญญาแต่ละฝ่ายมีหน้าที่ต้องแจ้งรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลซึ่งถูกประมวลผลข้อมูลก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล ทั้งนี้ รายการรายละเอียดที่ต้องแจ้งให้เป็นไปตามที่กำหนดในมาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๖.กรณีที่คู่สัญญาฝ่ายหนึ่งฝ่ายใด พบพฤติการณ์ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ประมวลผลภายใต้ข้อตกลงฉบับนี้ ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย คู่สัญญาฝ่ายที่พบเหตุดังกล่าวจะดำเนินการแจ้งให้คู่สัญญาอีกฝ่ายทราบ พร้อมรายละเอียดของเหตุการณ์โดยทันที ทั้งนี้ คู่สัญญาแต่ละฝ่ายต่างมีหน้าที่ต้องแจ้งเหตุดังกล่าวแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลตามแต่กรณี

๗. คู่สัญญาตกลงจะให้ความช่วยเหลืออย่างสมเหตุสมผลแก่อีกฝ่ายในการตอบสนองต่อข้อเรียกร้องใด ๆ ที่สมเหตุสมผลจากการใช้สิทธิต่าง ๆ ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคล โดยพิจารณาถึงลักษณะการประมวลผล ภาระหน้าที่ภายใต้กฎหมายคุ้มครองข้อมูลที่ใช้บังคับ และข้อมูลส่วนบุคคลที่ประมวลผล ทั้งนี้ คู่สัญญาทราบว่าเจ้าของข้อมูลส่วนบุคคลอาจยื่นคำร้องขอใช้สิทธิดังกล่าวต่อคู่สัญญาฝ่ายหนึ่งฝ่ายใดก็ได้ ซึ่งคู่สัญญาฝ่ายที่ได้รับคำร้องจะต้องดำเนินการแจ้งถึงคำร้องดังกล่าวแก่คู่สัญญาอีกฝ่ายโดยทันที โดยคู่สัญญาฝ่ายที่รับคำร้องนั้นจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงการจัดการตามคำขอหรือข้อร้องเรียนของเจ้าของข้อมูลนั้นด้วย

๘. ในกรณีที่มีการใช้ผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อทำการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ ให้ดำเนินการแจ้งต่อคู่สัญญาอีกฝ่ายก่อน ทั้งนี้คู่สัญญาฝ่ายที่ใช้ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องทำสัญญากับผู้ประมวลผลข้อมูลเป็นลายลักษณ์อักษรตามเงื่อนไขที่กฎหมายคุ้มครองข้อมูลกำหนด เพื่อหลีกเลี่ยงข้อสงสัย หากคู่สัญญาฝ่ายหนึ่งฝ่ายใดได้ว่าจ้างหรือมอบหมายผู้ประมวลผลข้อมูลส่วนบุคคล คู่สัญญาฝ่ายนั้นยังคงต้องมีความรับผิดต่ออีกฝ่ายสำหรับการกระทำการหรือละเว้นกระทำการใด ๆ ของผู้ประมวลผลข้อมูลส่วนบุคคลนั้น

๙. คู่สัญญาแต่ละฝ่ายจะต้องชดใช้ความเสียหายให้แก่อีกฝ่ายในค่าปรับ ความสูญหายหรือเสียหายใด ๆ ที่เกิดขึ้นกับฝ่ายที่ไม่ได้ผิดเงื่อนไข อันเนื่องมาจากการฝ่าฝืนข้อตกลงฉบับนี้ แม้ว่าจะมีข้อจำกัดความรับผิดภายใต้สัญญาหลักก็ตาม

๑๐. ...(สามารถตกลงกันนำข้อนี้ออกได้)... ในกรณีที่คู่สัญญาต้องรับผิดร่วมกันในค่าปรับหรือการชดใช้ความเสียหายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยไม่สามารถพิจารณาเป็นที่ประจักษ์ได้ว่าฝ่ายหนึ่งฝ่ายใดการทำการเป็นเหตุให้เกิดความเสียหายแต่เพียงผู้เดียว หรือจากการถูกศาลหรือหน่วยงานผู้มีอำนาจมีคำพิพากษาหรือคำสั่งถึงที่สุดให้คู่สัญญาร่วมกันรับผิดดังกล่าว คู่สัญญาตกลงกันแบ่งความรับผิดเป็นสัดส่วนดังต่อไปนี้

๑๐.๑ กรมการปกครอง ร้อยละ ...(ระบุอัตราส่วนความรับผิด)...

๑๐.๒ ...(ชื่อคู่สัญญา)... ร้อยละ ...(ระบุอัตราส่วนความรับผิด)...

ทั้งนี้ การตกลงกันของคู่สัญญานี้ ไม่มีอำนาจเหนือไปกว่าคำพิพากษาหรือคำสั่งถึงที่สุดของศาลหรือหน่วยงานผู้มีอำนาจที่กำหนดให้คู่สัญญาหรือคู่สัญญาฝ่ายหนึ่งฝ่ายใดต้องถูกปรับหรือชดใช้ค่าเสียหาย

๑๑. หน้าที่และความรับผิดของคู่สัญญาในการปฏิบัติตามข้อตกลงฉบับนี้จะสิ้นสุดลงนับแต่วันที่การดำเนินการตามสัญญาหลักเสร็จสิ้นลง หรือ วันที่คู่สัญญาได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกสัญญาหลัก แล้วแต่กรณีใดจะเกิดขึ้นก่อน

๑๒. คู่สัญญาตกลงแต่งตั้งผู้แทนของแต่ละฝ่าย ดังรายการต่อไปนี้

๑๒.๑ กรมการปกครอง

ผู้แทน : ...(ระบุชื่อ-นามสกุลผู้แทน)... ติดต่อได้ที่ : ...(ระบุช่องทางติดต่อผู้แทน)...

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล : ...(ระบุชื่อ-นามสกุลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)... ติดต่อได้ที่ : ...(ระบุช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)...

๑๒.๒ ...(ชื่อคู่สัญญา)...

ผู้แทน : ...(ระบุชื่อ-นามสกุลผู้แทน)... ติดต่อได้ที่ : ...(ระบุช่องทางติดต่อผู้แทน)...

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (หากมี) : ...(ระบุชื่อ-นามสกุลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)... ติดต่อได้ที่ : ...(ระบุช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)...

ในกรณีที่ข้อตกลง คำรับรอง การเจรจาหรือข้อผูกพันใดที่คู่สัญญามีต่อกันไม่ว่าด้วยวาจาหรือเป็นลายลักษณ์อักษรใดขัดหรือแย้งกับข้อตกลงที่ระบุในข้อตกลงฉบับนี้ ให้ใช้ข้อความตามข้อตกลงฉบับนี้บังคับ

ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว เพื่อเป็นหลักฐานแห่งการนี้ ทั้งสองฝ่ายจึงได้ลงนามไว้เป็นหลักฐานต่อหน้าพยาน ณ วัน เดือน ปี ที่ระบุข้างต้น

ลงชื่อ	ลงชื่อ .....
(.....)	(.....)
.....	.....
ลงชื่อ ..... พยาน	ลงชื่อ ..... พยาน
(.....)	(.....)
.....	.....