

**แบบประเมินประกอบการพิจารณาการดำเนินงาน**

**ตามแนวนโยบายและแนวปฏิบัติ****ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ**

**ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549**

**ชื่อหน่วยงาน**

**การจัดทำแนวนโยบายและแนวปฏิบัติ** 🞎 ครั้งแรก 🞎 ทบทวน ครั้งที่ ............... ประจำปี พ.ศ. ...............

**เอกสารประกอบการพิจารณา**   **(สามารถแนบเพิ่มเติมได้)**

**คำชี้แจง** : **การประเมินครั้งแรก**

* กรอกข้อมูลในช่อง “หน่วยงานประเมินตนเอง” โดยระบุ “มี” พร้อมอ้างอิงเอกสาร เลขหน้าและรายการที่มีเนื้อหาสอดคล้องกับสาระสำคัญที่กำหนด
* หากรายการใดไม่มีการจัดทำไว้ประกาศ ให้ระบุ “ไม่มี”

**การประเมินรอบทบทวน**

* กรอกข้อมูลในช่อง “หน่วยงานประเมินตนเอง” โดยรายการที่มีการทบทวนและปรับแก้ ให้ระบุ “มี” พร้อมระบุการอ้างอิงหน้า ในข้อที่มีการทบทวนและปรับแก้ และรายละเอียดการปรับแก้
* หากรายการใดไม่มีการทบทวนและปรับแก้ไข ให้ระบุ “ไม่มี”

| **ข้อ** | **แนวนโยบาย / และแนวปฏิบัติ**  **(ประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์)** | **หน่วยงานประเมินตนเอง** | | **ความเห็นจาก สพธอ.**  **เห็นด้วย/ไม่เห็นด้วย** | **ความเห็นจาก สพธอ.  หลังจากหน่วยงานดำเนินการแก้ไข** |
| --- | --- | --- | --- | --- | --- |
| **มี/ไม่มี** | **อ้างอิงหน้า…** |
|  | ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้ |  |  |  |  |
| * 1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด |  |  |  |  |
| * 1. คุณภาพของข้อมูลส่วนบุคคล |  |  |  |  |
| * 1. การระบุวัตถุประสงค์ในการเก็บรวบรวม |  |  |  |  |
| * 1. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้ |  |  |  |  |
| * 1. การรักษาความมั่นคงปลอดภัย |  |  |  |  |
| 1) ป้องกันการสูญหายข้อมูลส่วนบุคคลโดยมิชอบ |  |  |  |  |
| - กระบวนการสำรองข้อมูลส่วนบุคคล ประกอบด้วย ข้อมูลที่สำรอง ความถี่ในการสำรอง สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำไปใช้งาน |  |  |  |  |
| - ความถี่ในการสำรองข้อมูลส่วนบุคคล |  |  |  |  |
| - ความถี่ในการทดสอบข้อมูลที่เก็บสำรองไว้อย่างสม่ำเสมอ |  |  |  |  |
| - การจัดการ Malicious code และ mobile code |  |  |  |  |
| 2) ป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ |  |  |  |  |
| - การแยกระบบที่มีข้อมูลส่วนบุคคลที่สำคัญ |  |  |  |  |
| - การจัดลำดับชั้นความลับของข้อมูลส่วนบุคคลในระบบสารสนเทศ |  |  |  |  |
| - วิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลส่วนบุคคลที่เป็นความลับตามระดับความสำคัญ |  |  |  |  |
| - การเข้าถึงระบบปฏิบัติการ |  |  |  |  |
| - การเข้าถึงระบบเครือข่าย |  |  |  |  |
| 3) ป้องกันการทำลายข้อมูลส่วนบุคคลโดยมิชอบ |  |  |  |  |
| - กระบวนการพิจารณาเพื่อทำลายข้อมูลส่วนบุคคล |  |  |  |  |
| - รอบความถี่ในการทำลายข้อมูลส่วนบุคคล |  |  |  |  |
| - ระบุผู้ที่มีหน้าที่ในการทำลายข้อมูลส่วนบุคคล |  |  |  |  |
| - วิธีการทำลายสื่อบันทึกข้อมูลทั้งชนิดถาวร และการนำกลับมาใช้ใหม่ |  |  |  |  |
| 4) ป้องกันการใช้ข้อมูลส่วนบุคคลโดยมิชอบ |  |  |  |  |
| - การลงทะเบียนพร้อมแจ้งวัตถุประสงค์การขอใช้งาน |  |  |  |  |
| - การยืนยันตัวบุคคลตามรหัสผ่านที่ได้รับอนุญาต |  |  |  |  |
| 5) ป้องการแปลงข้อมูลส่วนบุคคลโดยมิชอบ |  |  |  |  |
| - การแปลงข้อความเข้าระบบอิเล็กทรอนิกส์ |  |  |  |  |
| 6) ป้องกันการแก้ไขข้อมูลส่วนบุคคลโดยมิชอบ |  |  |  |  |
| - ข้อจำกัดในการแก้ไขข้อมูลส่วนบุคคลเท่าที่จำเป็น |  |  |  |  |
| - ระบุผู้ที่ทำหน้าที่ในการแก้ไขข้อมูลส่วนบุคคล |  |  |  |  |
| - บันทึกรายละเอียดการปรับแก้ไขข้อมูลส่วนบุคคล เช่น การอนุมัติจากผู้มีอำนาจ การประมวลผล การบันทึกการแก้ไขเปลี่ยนแปลง และการแจ้งผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงทราบ |  |  |  |  |
| 7) ป้องการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ |  |  |  |  |
| - การแลกเปลี่ยนข้อมูลทั้งภายในและภายนอกหน่วยงาน |  |  |  |  |
| - การกำหนดสัญญารักษาความลับของข้อมูลส่วนบุคคล |  |  |  |  |
| * 1. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบาย ที่เกี่ยวกับข้อมูลส่วนบุคคล |  |  |  |  |
| * 1. การมีส่วนร่วมของเจ้าของข้อมูล |  |  |  |  |
| * 1. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล |  |  |  |  |
| - หน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลในแต่ละระดับชั้นของระบบสารสนเทศ |  |  |  |  |
| - หน้าที่ความรับผิดชอบของผู้ดูแลระบบสารสนเทศในส่วนของข้อมูลส่วนบุคคล |  |  |  |  |
|  | ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ และให้มีรายการอย่างน้อย ดังนี้ |  |  |  |  |
| * 1. ข้อมูลเบื้องต้น ประกอบด้วย |  |  |  |  |
| (ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด |  |  |  |  |
| (ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์ |  |  |  |  |
| (ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอม ก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ |  |  |  |  |
| * 1. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล ให้หน่วยงานของรัฐ รวบรวม จัดเก็บและใช้ข้อมูลส่วนบุคคลจัดทำรายละเอียด ดังต่อไปนี้ |  |  |  |  |
| (ก) การติดต่อระหว่างหน่วยงานของรัฐ |  |  |  |  |
| (ข) การใช้คุกกี้ (Cookies) |  |  |  |  |
| (ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information) |  |  |  |  |
| - การจัดประเภทข้อมูลส่วนบุคคลในระบบสารสนเทศ |  |  |  |  |
| (ง) บันทึกผู้เข้าชมเว็บไซต์ (Log Files) |  |  |  |  |
| 1) กรณีการเข้า-ออกโดยอัตโนมัติ |  |  |  |  |
| - บันทึกและจัดเก็บข้อมูลการขออนุญาตเข้าใช้ระบบ |  |  |  |  |
| - บันทึกและจัดเก็บข้อมูลการเข้า-ออก ของผู้มีสิทธิเข้าใช้ข้อมูลส่วนบุคคล |  |  |  |  |
| - รายละเอียดข้อมูลที่ใช้ในการเก็บ |  |  |  |  |
| 2) กรณีการแลกเปลี่ยนข้อมูล ระหว่างหน่วยงาน |  |  |  |  |
| - บันทึกและจัดเก็บข้อมูลการขออนุญาตเข้าใช้ระบบ |  |  |  |  |
| - บันทึกและจัดเก็บข้อมูลการเข้า-ออก ของผู้มีสิทธิในการแลกเปลี่ยนข้อมูล ระหว่างหน่วยงาน |  |  |  |  |
| - รายละเอียดการดำเนินงานที่เกิดขึ้นในแต่ละครั้ง ที่มีการแลกเปลี่ยนข้อมูล |  |  |  |  |
| - ระบุรายละเอียดข้อมูลที่ใช้ในการจัดเก็บ |  |  |  |  |
| (จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์ |  |  |  |  |
| * 1. การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น |  |  |  |  |
| * 1. การรวมข้อมูลจากที่มาหลาย ๆ แห่ง |  |  |  |  |
| * 1. การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล |  |  |  |  |
| * 1. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ |  |  |  |  |
| * 1. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน |  |  |  |  |
| * 1. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้ |  |  |  |  |
| 1. สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ |  |  |  |  |
| - การอบรม เพิ่มพูนความรู้แก่บุคลากรเก่าและใหม่ อย่างสม่ำเสมอ |  |  |  |  |
| - กระบวนการลงโทษทางวินัย เพื่อลงโทษบุคลากรที่ฝ่าฝืน ละเมิดนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล |  |  |  |  |
| 1. กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด |  |  |  |  |
| - กระบวนการมอบหมายหรือกำหนดสิทธิ์ |  |  |  |  |
| - การกำหนดสิทธิตามหน้าที่ความรับผิดชอบและ ตามความจำเป็น |  |  |  |  |
| - การเพิกถอนสิทธิ เมื่อมีการลาออก เปลี่ยนตำแหน่ง หรือย้าย |  |  |  |  |
| - การให้สิทธิพิเศษสำหรับผู้บริหารระดับสูงของหน่วยงาน และระยะการทบทวนสิทธิของผู้บริหาร |  |  |  |  |
| - การเฝ้าระวังบัญชีที่ได้รับสิทธิพิเศษ |  |  |  |  |
| 1. ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง |  |  |  |  |
| - กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรม |  |  |  |  |
| - ระบุผู้ตรวจสอบภายในหรือหรือผู้ตรวจสอบจากภายนอก |  |  |  |  |
| 1. กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น |  |  |  |  |
| - การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งยวด เช่น หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เป็นต้น |  |  |  |  |
| - การรักษาความมั่นคงปลอดภัยของข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดี ของประชาชน ซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ เช่น  เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น |  |  |  |  |
| - การรักษาความมั่นคงปลอดภัยของข้อมูลที่อาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพ ของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต เป็นต้น |  |  |  |  |
| 1. ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม |  |  |  |  |
| - การรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล ซึ่งอายุไม่เกินสิบแปดปี (ถ้ามี) |  |  |  |  |
| * 1. การติดต่อกับเว็บไซต์   เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐ ควรจะระบุเอาไว้ อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้   1. ชื่อและที่อยู่ 2. หมายเลขโทรศัพท์ 3. หมายเลขโทรสาร 4. ที่อยู่จดหมายอิเล็กทรอนิกส์ |  |  |  |  |

**หมายเหตุ**

1. ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการตามข้อ 1 และข้อ 2 สำหรับหน่วยงานของรัฐที่ได้รับทรัสต์มาร์คจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัสต์มาร์ค (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัสต์มาร์คดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย
2. ให้หน่วยงานของรัฐกำหนดชื่อเรียกนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ซึ่งจะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย

โปรดระบุเพื่อรับทราบ 🞏 กรณีหน่วยงานมีเอกสารที่เป็นความลับ ไม่จำเป็นต้องจัดส่งเอกสาร แต่ให้นำมาชี้แจงประกอบการพิจารณาของคณะกรรมการ

# ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามมาตรา 7 ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ลงชื่อ (ผู้บริหารสูงสุด/ผู้ที่ได้รับมอบอำนาจ)

( )

ตำแหน่ง

ลงวันที่