

การคุ้มครองข้อมูลส่วนบุคคลของธนาคารออมสิน

Personal Data Protection by GSB

ตอนที่ 14 เรื่อง **มาตรฐานการรักษาความมั่นคงปลอดภัย** ของข้อมูลส่วนบุคคล

(ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563)

ผู้ควบคุมข้อมูลส่วนบุคคล



ได้แก่ หน่วยงานตามบัญชีท้ายพระราชกฤษฎีกากำหนด หน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้ บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563

ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล



หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยมีขอบ



หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

1 **แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล** ให้แก่ บุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องทราบ รวมถึงสร้างเสริม ความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

2 **จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล** ครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึง หรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) อย่างน้อยต้องประกอบด้วยการดำเนินการ ดังนี้

01 **ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการ** จัดเก็บและประมวลผลข้อมูลส่วนบุคคล

02 **บริหารจัดการการเข้าถึง** ของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต

03 **กำหนดการอนุญาตหรือการกำหนดสิทธิ** ในการเข้าถึง ข้อมูลส่วนบุคคล

04 **กำหนดหน้าที่ความรับผิดชอบ** ของผู้ใช้งาน

05 **จัดให้มีวิธีการ** เพื่อให้สามารถ**ตรวจสอบย้อนหลัง** เกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล

