The National Board of Digital Economy and Society Office

มาตรการการรักษาความมั่นคงปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

เรื่อง แนวปฏิบัติในการใช้อุปกรณ์ส่วนตัวในการทำงาน

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) ได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของบุคลากร ซึ่งอาจมีการนำอุปกรณ์ส่วนตัวมาใช้ในการปฏิบัติงาน ดังนั้น เพื่อให้การนำอุปกรณ์ส่วนตัวที่บุคลากรนำมาใช้ในการปฏิบัติงานดังกล่าวเป็นไปอย่างมีความมั่นคงปลอดภัย และเพื่อเป็นการป้องกันมิให้เกิดการรั่วไหลหรือสูญหายของข้อมูลส่วนบุคคล รวมถึงเป็นการป้องกันจากการกระทำใด ๆ ที่อาจเกิดความเสี่ยงที่จะนำไปสู่การละเมิดข้อมูลส่วนบุคคลจากการนำอุปกรณ์ส่วนตัวมาใช้ในการปฏิบัติงาน จึงได้กำหนดแนวปฏิบัติในการใช้อุปกรณ์ส่วนตัวในการทำงาน ดังนี้

1. ขอบเขต

แนวปฏิบัตินี้ไม่ถือเป็นส่วนหนึ่งของสัญญาจ้าง แต่เป็นการกำหนดแนวทางการทำงานที่บุคลากรต้องปฏิบัติ โดยใช้บังคับเป็นการทั่วไปกับบุคลากรทุกระดับ และเป็นส่วนหนึ่งของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. ซึ่งจะครอบคลุมถึงการใช้งานอุปกรณ์ส่วนตัวในการปฏิบัติงานของ ข้าราชการ พนักงานราชการ พนักงานกองทุน จ้างเหมาบริการปฏิบัติงาน และพนักงานของบริษัทที่เป็นคู่สัญญา คู่ค้า ที่ปรึกษา บุคคลภายนอก หรือผู้ใดก็ตามที่ได้รับอนุญาตให้เป็นผู้ใช้งานข้อมูล ระบบเทคโนโลยีสารสนเทศ และทรัพย์สินของ สดช. โดยแนวปฏิบัตินี้จะได้รับการทบทวนและปรับปรุงอยู่เสมอ ซึ่งจะได้แจ้งให้บุคลากรทุกคนทราบทุกครั้ง

2. ข้อปฏิบัติ

สดช. อนุญาตให้มีการนำอุปกรณ์ส่วนตัว อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ก คอมพิวเตอร์แท็บเล็ต หรือโทรศัพท์มือถือ มาใช้เพื่อสนับสนุนการปฏิบัติงานตามภารกิจที่ได้รับมอบหมายจาก สดช. ยกเว้นการใช้สื่อบันทึกข้อมูล จะต้องปฏิบัติตามวิธีการปฏิบัติ (Procedure) ชื่องาน : วิธีการปฏิบัติการจัดการหมวดหมู่สารสนเทศ วิธีการปฏิบัติการจัดการสื่อบันทึกข้อมูล เวอร์ชันควบคุม ๐๑/๒๕๖๗ และผู้ใช้งานจะต้องเป็นผู้ดูแลบำรุงรักษาอุปกรณ์ส่วนตัวให้มีความมั่นคงปลอดภัยในการใช้งานอยู่เสมอ และจะต้องไม่กระทำการใด ๆ ที่เป็นความเสี่ยงที่จะนำไปสู่การละเมิดข้อมูลส่วนบุคคล โดยการนำเครื่องอุปกรณ์ส่วนตัวดังกล่าวไปใช้งาน ให้คำนึงถึงระดับความเสี่ยง ดังนี้

ระดับความเสี่ยง	ตัวอย่าง
ระดับความเสี่ยงต่ำ	ตัวอย่างเช่น - การใช้งานมีข้อมูลที่ใช้ระบุตัวบุคคลได้ เช่น อีเมล หรือแอปพลิเคชันอื่น แต่ไม่ได้อ่อนไหวมากจนจัดอยู่ในระดับที่หากมีการเปิดเผย หรือนำไปใช้ในทางที่ผิดแล้วจะส่งผลเสียต่อเจ้าของข้อมูลหรือหน่วยงาน - การใช้งานมีข้อมูลอันเป็นที่เปิดเผยแก่สาธารณะ หรือสามารถค้นหาได้จากแหล่งข้อมูลอื่นโดยง่าย
ระดับความเสี่ยงสูง	ตัวอย่างเช่น - ข้อมูลของบุคลากรตั้งแต่ 10 คนขึ้นไปที่เกี่ยวกับการประเมินผลการทำงาน การพัฒนาศักยภาพในการทำงาน หรือข้อมูลที่เกี่ยวกับชีวิตส่วนตัว หรือครอบครัวของบุคลากร - บันทึกข้อมูลอ่อนไหวที่ใช้ระบุตัวบุคคลได้ - กลุ่มข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลมากกว่า 10 คนขึ้นไปที่สามารถระบุตัวบุคคลได้ และสามารถนำข้อมูลกลุ่มนี้ไปปลอมแปลงหรือแอบอ้าง ตัวอย่างเช่น ข้อมูลบัญชี หรือบัตรเครดิต หมายเลขประกันสังคม ข้อมูลติดต่อ วันเกิด เงินเดือน เป็นต้น

เมื่อบุคลากรที่ใช้เครื่องอุปกรณ์ส่วนตัวในการทำงานได้ประเมินระดับความเสี่ยงตามตัวอย่างข้างต้นแล้ว ในการปฏิบัติงานด้วยอุปกรณ์ส่วนตัวดังกล่าว ควรมีการดำเนินการเพิ่มเติมดังต่อไปนี้

ระดับความเสี่ยง	แนวทางการปฏิบัติงาน
การปฏิบัติงานที่มีระดับความเสี่ยงต่ำ	- ให้ดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. การตั้งรหัสผ่าน (เช่น PIN หรือ Password) เพื่อใช้อุปกรณ์ และไม่เปิดเผยรหัสดังกล่าวกับผู้อื่น โดยมีแนวทางการตั้งรหัสผ่านที่แข็งแรง (Password Policy Enforcement) ดังนี้ • ตั้งรหัสผ่านที่ซับซ้อน เช่น ความยาวอย่างน้อย ๑๒ ตัวอักษร และต้องมีตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์ • หลีกเลี่ยงการใช้รหัสผ่านซ้ำในหลายบัญชี • ควรเปลี่ยนรหัสผ่านเป็นประจำในทุก ๆ ๑๘๐ วัน - ตั้งค่าให้อุปกรณ์ล็อคอัตโนมัติเมื่อไม่มีการใช้งานเป็นเวลาหลายนาที - เฝ้าระวังอุปกรณ์อย่างเหมาะสม ไม่ทิ้งอุปกรณ์ไว้โดยไม่ดูแล - อัพเดตโปรแกรมอย่างสม่ำเสมอ - ตั้งค่าไม่ให้อุปกรณ์เชื่อมต่อโดยอัตโนมัติกับสัญญาณไร้สายที่มีความเสี่ยง และควรพิจารณาก่อนจะตัดสินใจเชื่อมต่อสัญญาณ - ควรติดตั้งระบบล้างข้อมูลที่สามารถสั่งได้จากระยะไกล ในกรณีที่อุปกรณ์สูญหาย

ระดับความเสี่ยง	แนวทางการปฏิบัติงาน
	- กรณีเป็นอุปกรณ์มือสอง ให้ตั้งค่าให้อุปกรณ์กลับไปเป็นสภาพเครื่องจากโรงงานก่อนเริ่มใช้งาน - ไม่ดาวน์โหลดไฟล์ หรือติดตั้ง Application ใด ๆ ที่ไม่มีความน่าเชื่อถือ หรือเป็นความเสี่ยงต่อความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์ -
การปฏิบัติงานที่มีระดับความเสี่ยงสูง	- ให้ดำเนินการตามแนวทางการปฏิบัติงานที่มีระดับความเสี่ยงต่ำทุกข้อ (หากสามารถดำเนินการได้) - ในกรณีที่บุคคลในครอบครัวใช้อุปกรณ์ส่วนตัวดังกล่าว บุคลากรต้องระมัดระวังมิให้บุคคลในครอบครัวเข้าถึงข้อมูลของหน่วยงานได้ เช่น ควรมีการตั้งรหัสผ่านป้องกันบัญชีผู้ใช้งาน (account) ไว้ด้วย เพื่อป้องการเข้าใช้งานของบุคคลภายนอก ทั้งนี้หน่วยงานขอความร่วมมือไม่ให้แบ่งปันอุปกรณ์ที่ใช้ในการทำงานกับบุคคลภายนอก - ควรดำเนินการจัดการและตรวจสอบข้อมูลภายในเครื่องอยู่เสมอ และทำลายข้อมูลที่ไม่จำเป็น - เมื่อบุคลากรไม่ใช้อุปกรณ์นี้ต่อไปแล้ว (เช่น กรณีที่นำเครื่องอื่นมาใช้แทน) หรือเมื่อลาออกจากการเป็นบุคลากร ให้ทำการลบข้อมูลของหน่วยงานในอุปกรณ์ดังกล่าวออกให้หมด - ควรมีการเข้ารหัสอุปกรณ์ (เพื่อป้องกันการเข้าถึงข้อมูล แม้หน่วยเก็บข้อมูล (Storage Chips) หรือดิสก์จะถูกถอดออกไปใส่ในอุปกรณ์อื่น) - ควรมีการติดตั้งระบบติดตามไว้กับอุปกรณ์ในกรณีที่อุปกรณ์สูญหายหรือถูกขโมย - ควรมีการติดตั้งระบบล้างข้อมูลที่สามารถสั่งได้จากระยะไกลให้ล้างข้อมูลภายใน 36 ชั่วโมง หรือเร็วกว่านั้น - ไม่ควรบันทึกไฟล์ที่มีรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคล บรรจุลงในอุปกรณ์ส่วนตัว เพื่อป้องกันการการรั่วไหลของข้อมูลส่วนบุคคล - ในกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ให้แจ้งต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบทันที - ควรมีการปรับและตั้งค่าอุปกรณ์ให้มีระบบการป้องกันที่มีประสิทธิภาพสูงสุด ใช้เวลาศึกษาและทำความเข้าใจการตั้งค่าต่าง ๆ - ถ้ามีการเข้าถึงข้อมูลของหน่วยงานจากสถานที่อื่น ให้ทำการออกจากระบบและหยุดการเชื่อมต่อสัญญาณทุกครั้งหลังเลิกใช้ - เปิดใช้งานโหมดสูญหาย เช่น ระบบตามหาพิกัด หรือระบบสั่งล้างข้อมูลทางไกล - ควรดาวน์โหลดแอปพลิเคชันจากแหล่งที่มีความน่าเชื่อถือเท่านั้น - ในกรณีของ iPhone หรือ iPad อุปกรณ์จะถูกเข้ารหัส (Encrypt) เอาไว้ โดยให้กำหนดการป้องกันโดยการตั้ง PIN - ในกรณีของแอนดรอยด์ สามารถเลือกให้อุปกรณ์เข้ารหัสในลักษณะ whole-device ได้ที่ “การตั้งค่า” ของอุปกรณ์ (อุปกรณ์ประเภทอื่น ๆ อาจสามารถหรือไม่สามารถตั้งค่าให้ทำการเข้ารหัสได้)

การนำอุปกรณ์ส่วนตัวออกไปใช้นอกสถานที่ ให้ใช้งานด้วยความระมัดระวัง และต้องดำเนินการตามแนวปฏิบัตินี้ และนโยบายอื่น ๆ ของหน่วยงานอย่างเคร่งครัด

****