นโยบายการบริหารจัดการรหัสผ่าน

(Password Management Policy)

๑. วัตถุประสงค์

นโยบายนี้กำหนดขึ้นเพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่านเพื่อการระบุตัวตน และสร้างความปลอดภัยจากบุคคลที่ไม่ได้รับอนุญาตเข้ามาล่วงรู้รหัสผ่าน อันส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศของ สป.ทส.

๒. การบริหารจัดการรหัสผ่าน

รหัสผ่านเป็นวิธีพื้นฐานในการระบุตัวตน ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิเข้าสู่ระบบเทคโนโลยีสารสนเทศของ สป.ทส. และมีแนวทางปฏิบัติดังนี้

๒.๑ ผู้ใช้งานระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน

๒.๒ สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านเริ่มแรกในการผ่านเข้าระบบเทคโนโลยีสารสนเทศและเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที **ยกเว้น**ในกรณีที่ระบบที่ผู้ใช้งานสามารถกำหนดรหัสผ่านได้เอง และการกำหนดรหัสผ่านนั้นต้องเปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสม เช่น อย่างน้อยเดือนละ ๑ ครั้ง

๒.๓ รหัสผ่านชั่วคราวจะมีการนำมาใช้สำหรับผู้ใช้งานที่ลืมรหัสผ่านและมีหลักฐานพิสูจน์ตนได้ว่าเป็นผู้ใช้งานที่มีสิทธิใช้งานระบบจริง เช่น ตรวจสอบบัตรประชาชน เป็นต้น รหัสผ่านดังกล่าว ต้องใช้อย่างระมัดระวังและจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๒.๔ ไม่ควรส่งรหัสผ่านผ่านระบบเครือข่าย โดยไม่ดำเนินการเข้ารหัสเพื่อรักษาความลับก่อน

๒.๕ ต้องกำหนดให้ผู้ใช้งานป้อนรหัสผู้ใช้งานและรหัสผ่านในการใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

๒.๖ กำหนดให้ผู้ใช้งานสามารถกำหนดรหัสผ่านของตนเองได้และมีกระบวนการตรวจสอบอีกครั้งก่อนยืนยันการเปลี่ยนรหัสผ่านเพื่อป้องกันความผิดพลาด

๒.๗ ระบบเทคโนโลยีสารสนเทศต้องมีการแนะนำผู้ใช้งานในการกำหนดรหัสผ่านที่มีคุณภาพ เช่น รหัสผ่านที่ผู้ใช้งานกำหนดนั้นอยู่ในระดับอ่อน ปานกลาง หรือแข็งแกร่ง เป็นต้น

๒.๘ บันทึกประวัติการเปลี่ยนรหัสผ่านเพื่อป้องกันการใช้ซ้ำ

๒.๙ ต้องไม่แสดงรหัสผ่านที่พิมพ์ลงไป หรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

๓. การใช้งานรหัสผ่าน

๓.๑ **“ผู้ใช้งาน”** ต้องเก็บรหัสผ่านไว้เป็นความลับ

๓.๒ **“ผู้ใช้งาน”** ต้องไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้ หรือไม่ควรเก็บรักษารหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย เช่น บนเครื่องคอมพิวเตอร์ บนโต๊ะทำงาน เป็นต้น และต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

๓.๓ **“ผู้ใช้งาน”** ต้องไม่พิมพ์รหัสผ่านในขณะที่มีผู้อื่นเห็นการพิมพ์ดังกล่าว

๓.๔ **“ผู้ใช้งาน”** ต้องไม่ทำการใดๆ เพื่อให้ตนเองทราบถึงบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น

๓.๕ **“ผู้ใช้งาน”** ต้องเปลี่ยนรหัสผ่านส่วนของตนเองในครั้งแรกของการใช้งาน ไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตาม และไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม

๓.๖ หากมีเหตุที่น่าเชื่อถือได้ว่ามีการเปิดเผยรหัสผ่าน **“ผู้ใช้งาน”** ต้องรายงานเหตุการณ์ไปยังผู้ดูแลระบบ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

๓.๗ ถ้าพบว่ารหัสผ่านของตนถูกล็อคโดยไม่ทราบสาเหตุ **“ผู้ใช้งาน”** ต้องแจ้งให้ผู้ดูแลระบบทราบ

๓.๘ ในกรณีที่ได้รับความช่วยเหลือในการแก้ไขปัญหาและต้องการให้ใส่รหัสผ่าน **“ผู้ใช้งาน”** ไม่ควรให้รหัสผ่านแก่ผู้ช่วยเหลือ แต่ต้องใส่รหัสผ่านด้วยตนเอง

๔. การกำหนดรหัสผ่าน

๔.๑ การกำหนดรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรม ชื่อหนัง ชื่อสถานที่ หรือชื่อสิ่งลึกลับ และต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับ สป.ทส. หรือเป็นข้อมูลส่วนตัวของผู้ใช้งานซึ่งอาจง่ายแก่การคาดเดา เช่น รหัสประจำตัวเจ้าหน้าที่ ที่อยู่ ชื่อบุคคลในครอบครัว เป็นต้น

๔.๒ ต้องไม่กำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรหรือตัวเลขที่เรียงซ้ำกันเกินกว่า ๓ ตัว หรือเรียงกันตามลำดับ เช่น aaaabbbb, 11111111, abcdefg

๔.๓ รหัสผ่านที่ดีต้องมีลักษณะดังนี้

๔.๓.๑. ต้องมีความยาวอย่างน้อย ๘ ตัวอักษร

๔.๓.๒. ต้องมีส่วนประกอบของอักษร ตัวเลข และอักขระพิเศษ ประสมกันตามลักษณะดังนี้

๔.๓.๒.๑. ตัวอักษรใหญ่ เช่น A, B, C, ...

๔.๓.๒.๒. ตัวอักษรเล็ก เช่น a, b, c, ...

๔.๓.๒.๓. ตัวเลข เช่น 0, 1, 2, ...

๔.๓.๒.๔. อักขระพิเศษ เช่น !, @, # , $, ...

๕. การเปลี่ยนรหัสผ่าน

๕.๑ รหัสผ่านของ **“ผู้ดูแลระบบ”** ต้องเปลี่ยนอย่างน้อยทุก ๓ เดือน

๕.๒ รหัสผ่านของ **“ผู้ใช้งาน”** ต้องเปลี่ยนอย่างน้อยทุก ๖ เดือน

๕.๓ รหัสผ่านของระบบที่ให้บริการประชาชนจะต้องเป็นส่วนหนึ่งของการจัดการฐานข้อมูลรหัสผ่านส่วนกลาง

๖. การยกเลิกรหัสผ่าน

รหัสผ่านของผู้ใช้งานที่ลาออก สิ้นสุดการจ้างงาน หรือย้ายงาน ต้องทำการยกเลิกสิทธิของผู้ใช้งานในระบบทันทีภายใน ๓๐ วัน