

แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลบัญชีผู้ใช้งาน

1. กำหนด 'รหัสผ่าน (password)' จำนวนไม่น้อยกว่า 12 หลักขึ้นไป โดยจะต้องประกอบด้วย
 - 1) ตัวพิมพ์ใหญ่ (A-Z)
 - 2) ตัวพิมพ์เล็ก (a-z)
 - 3) ตัวเลข (0-9)
 - 4) อักขระพิเศษ (@#*_&)
2. หลีกเลี่ยงการตั้งรหัสผ่านที่เป็นรูปแบบ 'แพทเทิร์น (Pattern)' ดังนี้
 - 1) ตัวอักษรพิมพ์ใหญ่ 1 ตัว + ตัวอักษรพิมพ์เล็ก 5 ตัว ตัวเลข 3 หลัก เช่น Docdoc123
 - 2) ตัวอักษรพิมพ์ใหญ่ 1 ตัว + ตัวอักษรพิมพ์เล็ก 6 ตัว ตัวเลข 2 หลัก เช่น Correct12
 - 3) ตัวอักษรพิมพ์ใหญ่ 1 ตัว + ตัวอักษรพิมพ์เล็ก 3 ตัว ตัวเลข 5 หลัก เช่น Ddoc12345
3. ไม่กำหนดรหัสผ่านที่คาดเดาได้ง่าย
 - 1) วัน/เดือน/ปี เกิด
 - 2) เบอร์โทรศัพท์ส่วนตัว
 - 3) ชื่อจริงหรือชื่อเล่น
 - 4) ชื่อหน่วยงาน
4. ห้ามส่งรหัสผ่านทางอีเมล ข้อความโต้ตอบ (Chat) หรือช่องทางการสื่อสารอื่นใดที่ขาดความปลอดภัยในการเข้ารหัสหรือการป้องกันข้อมูล เพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
5. ไม่ควรจดจำรหัสผ่านเว็บเบราว์เซอร์ทุกประเภท เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
6. ควรดำเนินการเปลี่ยน 'รหัสผ่าน (password)' ใหม่ทุก 90 วัน