# Privileged Access Management (PAM)

**การรักษาความปลอดภัยของข้อมูลติดตาม ตรวจหา และป้องกันการใช้สิทธิการเข้าถึงทรัพยากรที่สำคัญในระดับสูง**

**มีการควบคุมการเข้าถึงระบบโดยใช้งานสิทธิระดับ High privileged ดังนี้**

1. **ดำเนินการ Disable Administrator / Root / Admin บนระบบเพื่อป้องกันการโจมตีในรูปแบบ Brute Force**
2. **มี Policy การเปลี่ยน Password อย่างน้อยทุก 3 เดือน**
3. **มีการกำหนด Role-base access ในการเข้าถึงระบบ**
4. **มีการสร้าง Account ตาม User ที่ใช้งานในระบบ**
5. **มีการตั้ง Password อย่างน้อย 12 ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS**

**ฉบับเผยแพร่บนเว็บไซต์ ตัดภาพหน้าจอระบบภายในออก**