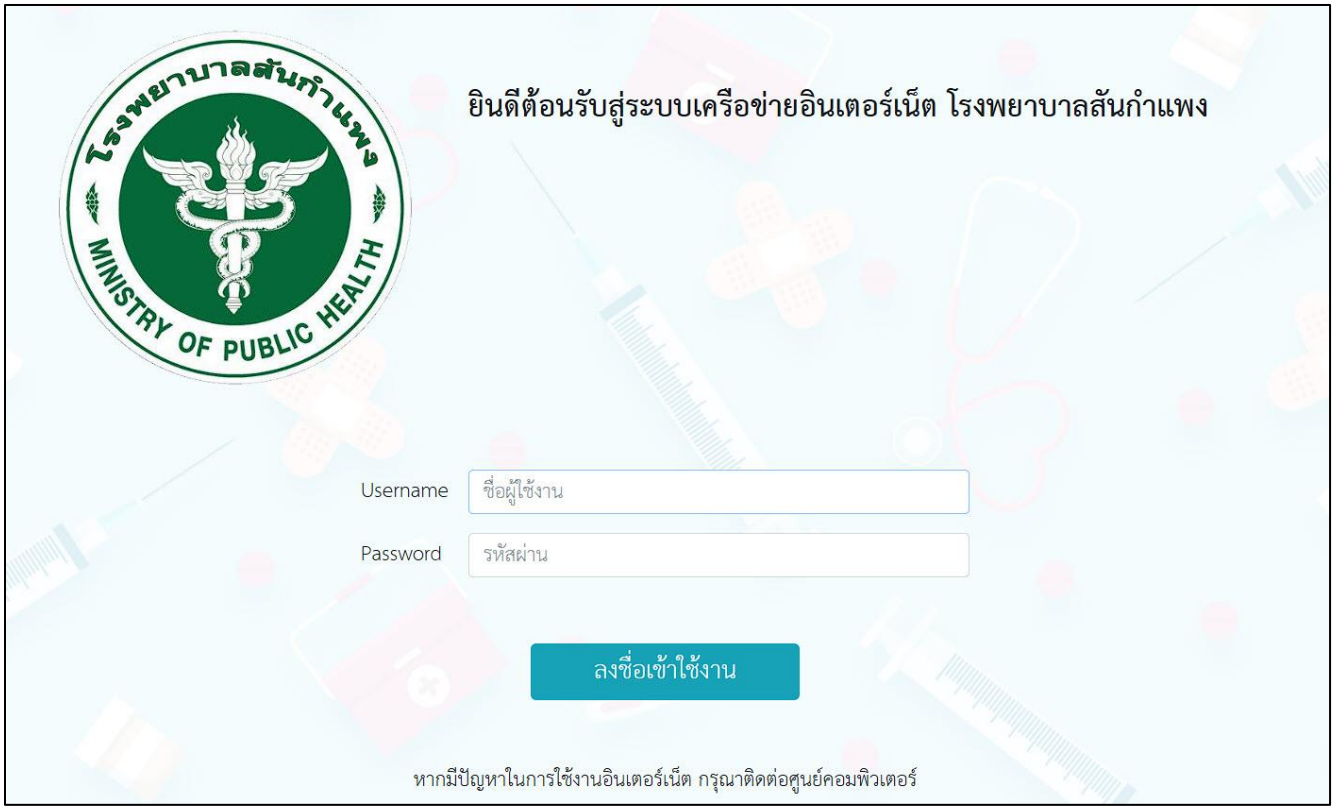
แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

(Specific information security policy)

โรงพยาบาลสันกำแพง

1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)

Privileged Access Management (PAM) : การรักษาความปลอดภัยของข้อมูลติดตาม ตรวจหา และป้องกันการใช้สิทธ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูงมีระบบ Authen login ในการเข้าใช้งานระบบเครือข่าย internet ภายในเพื่อระบุได้ว่าผู้ใช้งานในระบบเป็นบุคคลากรของโรงพยาบาลและมีสิทธิ์การเข้าถึงระบบเครือข่าย internet

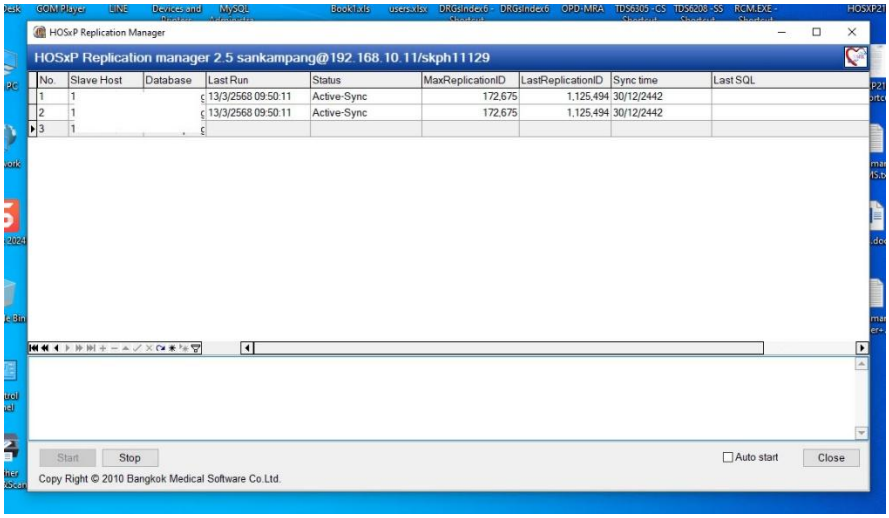


2) การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งานและการจัดทำแผนเตรียมความพร้อมรับมือภัยคุกคาม

Backup : การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้กู้คืนข้อมูลเดิม หลังจากเกิดเหตุการณ์ข้อมูลสูญหาย

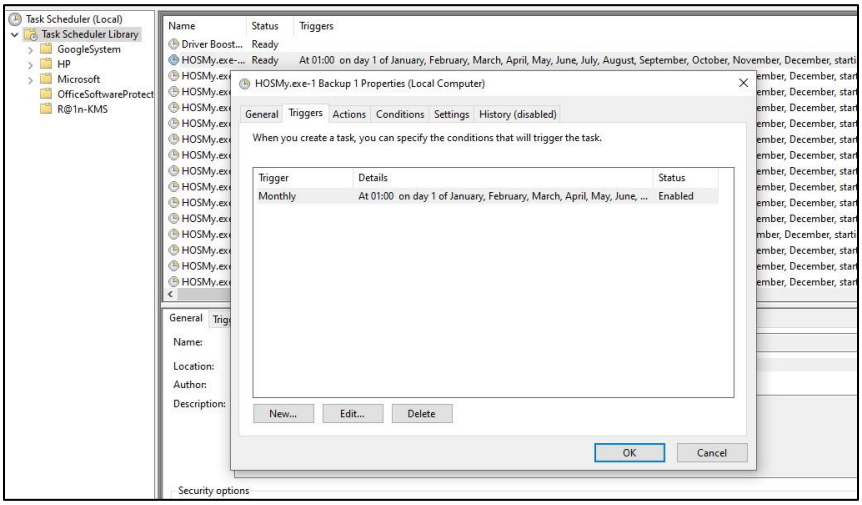
2.1. การใช้ Software Backup (Replication)

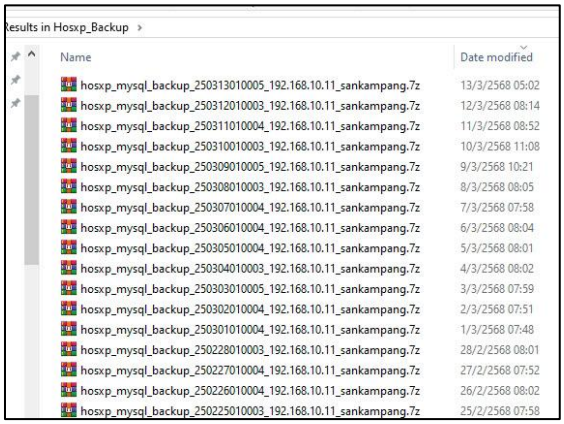
การสำรองข้อมูลแบบ Replication Real Time โดยใช้ HOSxP Replication ตลอด 24 ชั่วโมงเพื่อสำรองข้อมูลที่เป็นปัจจุบันไปที่ Server slave และเมื่อมีเหตุการณ์การข้อมูลสูญหายใน Server master สามารถดึงข้อมูลที่สูญหายไปจากการสำรองเข้ามาใหม่



2.2. การ Backup แบบ Auto Script

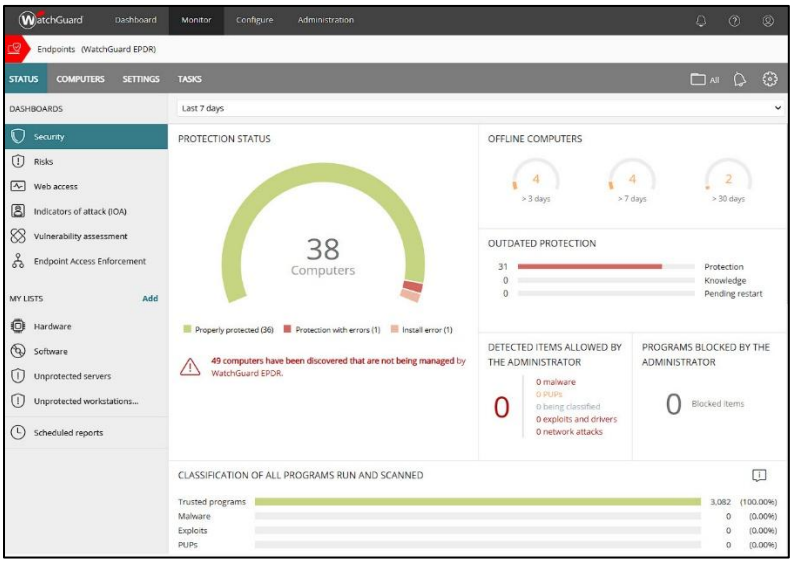
การอัตโนมัติในการสร้างกระบวนการสำรองข้อมูล (backup) โดยใช้สคริปต์คำสั่งที่เขียนในภาษา Bash ทำการบีบอัดเป็นรูปแบบไฟล์ .zip แล้วทำการสำเนาเก็บไว้ ที่ NAS Storage





3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ตรวจสอบและประเมินความเสี่ยงโดยใช้ Antivirus Software : โปรแกรมป้องกันไวรัส คอยตรวจจับป้องกัน และกำจัดความเสี่ยงโปรแกรมคุกคามคอมพิวเตอร์หรือมัลแวร์ โรงพยาบาลสันกำแพงเลือกใช้ซอฟต์แวร์ Watchguard เป็นโซลูชันด้าน ความปลอดภัยสำหรับจุดปลายทาง (endpoint security) ที่รวมฟังก์ชัน Antivirus และ Endpoint Detection and Response (EDR) เข้าด้วยกัน โดยออกแบบมาเพื่อปกป้องระบบจากภัยคุกคาม เช่น มัลแวร์ ขั้นตอนการ โจมตีที่ซับซ้อน (APT) และ ransomware อย่างครอบคลุม



Vulnerability Assessment (VA Scan) : การตรวจสอบช่องโหว่ของระบบเพื่อให้ทราบถึงความเสี่ยง จุดอ่อน และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการถูกโจรกรรมข้อมูลและการโจมตีทางไซเบอร์ มีการ VA Scan ด้วย watchguard ตรวจจับการทำงานของระบบคอมพิวเตอร์และเกิดช่องโหว่เพื่อดำเนินการแก้ไข