โรงพยาบาลนครพนม	
ระดับเอกสาร : แนวทางปฏิบัติ (Work Instruction) **เลขที่ :** COM-NI-๐๐๗-๐๐	**ฉบับที่ :**
เรื่อง : การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security)	**วันที่ :**
หน่วยงาน : ศูนย์คอมพิวเตอร์ – สารสนเทศ	

ผู้จัดทำ : ..... (นางพิณทิพย์ ซ้ายกลาง) หัวหน้าศูนย์คอมพิวเตอร์ – สารสนเทศ **ผู้ทบทวน :** ..... (นายจรุงธรรม ขันตี) รอง ฯ ด้านพัฒนาระบบบริการสุขภาพรอง ผู้อำนวยการด้านพัฒนาระบบบริการสุขภาพ	**ผู้อนุมัติ :** ..... (นายยุทธชัย ตริสกุล) ผู้อำนวยการโรงพยาบาลนครพนม

๑. วัตถุประสงค์ : -เพื่อให้ระบบข้อมูลสารสนเทศ ครบถ้วน ถูกต้อง เชื่อถือได้ นำมาใช้ได้ทันเหตุการณ์

๒. ขอบข่าย : ใช้สำหรับให้เจ้าหน้าที่ศูนย์คอมพิวเตอร์ – สารสรเทศ เฝ้าระวังทุกระบบเครือข่ายภายในโรงพยาบาลนครพนม

๓. อุปกรณ์/เครื่องมือ : -

๔. ความรับผิดชอบ : เจ้าหน้าที่ศูนย์คอมพิวเตอร์ – สารสนเทศ

๕. คำจำกัดความ : -

๖. เอกสารอ้างอิง : -

๗. รายระเอียด : เพื่อให้การจัดการระบบข้อมูลสารสนเทศ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้เทคโนโลยีระบบคอมพิวเตอร์ที่มีระบบการรักษาความปลอดภัยในขั้นพื้นฐานที่เป็นมาตรฐานสากลอยู่แล้ว และเสริมด้วยการทำงานด้านอุปกรณ์ความปลอดภัยเฉพาะอีกชั้น และโดยหลักการทั่วไปในการควบคุมและรักษาความปลอดภัยให้กับระบบข้อมูลข่าวสาร ได้แก่การควบคุมส่วนต่างๆ ของระบบอย่างรัดกุม วิธีการที่ใช้ในการควบคุมมีดังนี้

๑. การควบคุมรักษาความปลอดภัยโดยตัวซอฟต์แวร์ (Software Control) โดยมีระดับวิธีการ ๓ วิธีคือ

๑.๑ การควบคุมจากระบบภายในของซอฟต์แวร์ (Internal Program Control) คือ การที่ โปรแกรมนั้นได้มีการควบคุมสิทธ์การเข้าถึง และสิทธิในการใช้งานข้อมูลภายในระบบ ซึ่งถูกจัดเก็บไว้ในระบบฐานข้อมูลภายในระบบเอง

๑.๒ การควบคุมวาวปลอดภัยโดยระบบปฏิบัติการ (Operating System Control) คือการควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่างๆ ภายในระบบคอมพิวเตอร์ของผู้ใช้งานคนหนึ่ง และจำแนกแตกต่างจากผู้ใช้คนอื่นๆ

๑.๓ การควบคุมและการออกแบบโปรแกรม (Development Control) คือการควบคุมตั้งแต่การออกแบบ การทอสอบก่อนการใช้งานจริง

๒. การควบคุมความปลอดภัยของระบบโดยฮาร์ดแวร์ (Hardware Control) โดยเลือกใช้เทคโนโลยีทางด้านฮาร์ดแวร์ ที่สามารถควบคุมการเข้าถึง และป้องกันการทำงานผิดพลาด ด้วยอุปกรณ์ภายในตัวเอง

๓. การใช้นโยบายในการควบคุม (Policies) โดยมีการประกาศใช้นโยบาย และการปรับปรุงนโยบายให้มีการทำงานสอดคล้องกับการดำเนินธุรกิจ และสภาพแวดล้อมที่เปลี่ยนแปลง โดยมีผลบังคับใช้ทั้งองค์กร

๔. การป้องกันทางกายภาพ (Physical Control) การมีมาตรการเข้าถึงศูนย์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์ที่สำคัญได้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น รวมทั้งมีระบบสำรองข้อมูลอย่างสม่ำเสมอ