

การดำเนินการปฏิญญาคุณธรรม (Do & Don't)

หน่วยงานโรงพยาบาลพระแสง

ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

๑. ปฏิญญาคุณธรรม (Do & Don't) หรือข้อตกลงคุณธรรม (ขั้นต้น)

Do (สิ่งที่ควรทำ)	Don't (สิ่งที่ไม่ควรทำ)
๑.ต้อง ป้องกัน ดูแล รักษาบัญชีผู้ใช้ (Username/Password) ของตนเอง เปลี่ยนรหัสผ่านทุก ๙๐ วัน	๑.ห้าม ใช้บัญชีผู้ใช้ (Username, Password) ของผู้อื่น
๒.ต้อง รับผิดชอบต่อความเสียหาย ที่อาจเกิดกับคอมพิวเตอร์ ปริ้นเตอร์ ปลั๊กไฟ หรืออุปกรณ์อิเล็กทรอนิกส์	๒.ห้าม ติดตั้ง แก๊ซ โปรแกรมอื่นใดในโรงพยาบาลโดยไม่ได้รับอนุญาต จากผู้ดูแลระบบ
๓.ต้อง แจ้งเจ้าหน้าที่ IT ก่อนเคลื่อนย้าย คอมพิวเตอร์	๓.ห้าม ใช้อุปกรณ์สำรองข้อมูล (Flash Drive, External Hard disk) กับคอมพิวเตอร์ ที่ใช้ระบบสารสนเทศโรงพยาบาล
	๔.ห้าม เผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคม ออนไลน์ทุกประเภท
	๕.ห้าม นำอุปกรณ์กระจายสัญญาณ มาเชื่อมต่อ กับระบบโรงพยาบาล

๒. วิธีการดำเนินการ

การวางแผน (Plan)

- จัดประชุมระดมสมองภายในหน่วยงาน ๒ ครั้ง เพื่อกำหนดพฤติกรรมที่พึงประสงค์และไม่พึงประสงค์
- ศึกษากฎหมาย ระเบียบ และแนวทางปฏิบัติที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลประกอบการกำหนดข้อตกลงคุณธรรม

การทดลองปฏิบัติ (Do)

- นำข้อตกลงคุณธรรมไปใช้จริงในการทำงานประจำวัน
- จัดประชุมติดตามผลทุกเดือน เพื่อแลกเปลี่ยนปัญหาและแนวทางแก้ไข

การประเมินผลปรับปรุง (Check)

- รอบ ๖ เดือน (๑ ตุลาคม ๒๕๖๘-๓๑ มีนาคม ๒๕๖๙)
ประเมินผลเบื้องต้นว่าพฤติกรรมที่พึงประสงค์เริ่มเกิดขึ้นจริงหรือไม่ และพฤติกรรมที่ไม่พึงประสงค์ลดลงหรือไม่ พร้อมปรับปรุงทันทีหากพบข้อจำกัด
- รอบ ๑๒ เดือน (๑ ตุลาคม ๒๕๖๘-๓๐ กันยายน ๒๕๖๙)
ประเมินผลรวมทั้งปี วิเคราะห์ความต่อเนื่องและผลลัพธ์ที่เกิดขึ้นจริงต่อการแก้ไขปัญหาขององค์กร พร้อมสรุปผลเพื่อยกระดับเป็น “ปฏิญญาคุณธรรม” ของหน่วยงาน

การปฏิบัติ (Act)

- ดำเนินการตามข้อตกลงคุณธรรมที่ผ่านการปรับปรุงแล้วอย่างต่อเนื่องเป็นเวลา ๖ เดือน
- สรุปผลการดำเนินงานและประกาศเป็น “ปฏิญญาคุณธรรม” ของหน่วยงาน

๓. ปฏิญญาคุณธรรม (Do & Don't) ของหน่วยงานที่ผ่านการทดลองปฏิบัติแล้ว

Do (สิ่งที่ควรทำ)	Don't (สิ่งที่ไม่ควรทำ)
-	-
-	-
-	-

แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ โรงพยาบาลพระแสง (Version1.2)

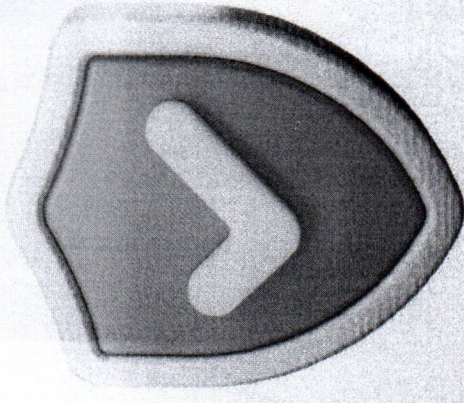
3 DO ต้อง

- 1  **ต้อง** ป้องกัน ดูแล รักษาบัญชีผู้ใช้ (Username/Password) ของตนเอง เปลี่ยนรหัสผ่านทุก 90 วัน
- 2  **ต้อง** รับผิดชอบต่อความเสียหาย ที่อาจเกิดกับคอมพิวเตอร์ ปริ้นเตอร์ ปลั๊กไฟ หรืออุปกรณ์อิเล็กทรอนิกส์
- 3  **ต้อง** แจ้งเจ้าหน้าที่ IT ก่อนเคลื่อนย้าย คอมพิวเตอร์

5 Don't ห้าม

- 1  **ห้าม** ใช้บัญชีผู้ใช้ (Username, Password) ของผู้อื่น
- 2  **ห้าม** ติดตั้ง แก้ไข โปรแกรมอื่นใด ในโรงพยาบาลโดยไม่ได้รับอนุญาต จากผู้ดูแลระบบ
- 3  **ห้าม** ใช้อุปกรณ์สำรองข้อมูล (Flash Drive, External Hard disk) กับคอมพิวเตอร์ ที่ใช้ระบบสารสนเทศโรงพยาบาล
- 4  **ห้าม** เผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคม ออนไลน์ทุกประเภท
- 5  **ห้าม** นำอุปกรณ์กระจายสัญญาณ มาเชื่อมต่อกับระบบโรงพยาบาล

ปรับปรุง: 10 มีนาคม 2568



นโยบายรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ

↑
โรงพยาบาลพระแสงส่งเสริมและสนับสนุนรักษา
ความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ
ให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

↑
โรงพยาบาลพระแสงมีหน้าที่ จำกัด ระบุ
เพิกถอนสิทธิหากมีการละเมิดหรือฝ่าฝืนแนวปฏิบัติ
คณะกรรมการสารสนเทศและคอมพิวเตอร์รายงาน
การฝ่าฝืนให้ต้นสังกัดหรือโรงพยาบาลพิจารณาลงโทษ

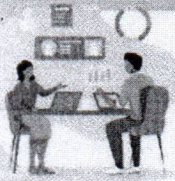
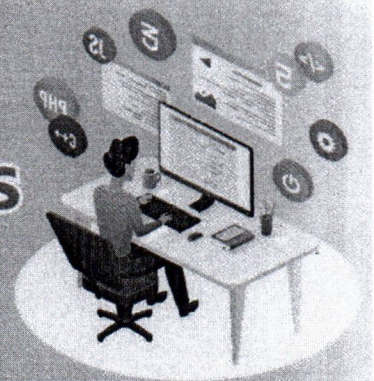
กลุ่มงานดิจิทัลทางการแพทย์

↑
โรงพยาบาลพระแสงสนับสนุนให้เทคโนโลยีสารสนเทศ
มีความถูกต้อง สมบูรณ์และพร้อมใช้งานอยู่เสมอ

↑
โรงพยาบาลพระแสงสนับสนุนการรักษาความปลอดภัย
ของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูล
ความลับของผู้ใช้ และข้อมูลผู้ป่วยอย่างเคร่งครัด

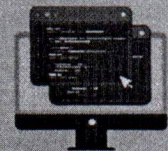
↑
โรงพยาบาลพระแสงสนับสนุนให้ปฏิบัติตามประเพณี
และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กระทรวงสาธารณสุข ตามหนังสือ ที่ สร ๐๒๑๒ / ๖๙๐๔๓

ข้อตกลงระดับการบริการ (Service Level Agreement)



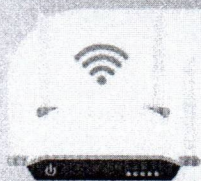
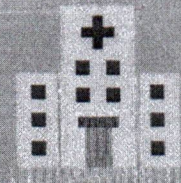
**การให้คำปรึกษา (Help Desk)
ภายใน 5 นาที**

**แก้ไขปัญหาคอมพิวเตอร์ขัดข้อง
ภายใน 15 นาที**



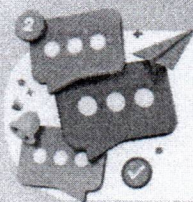
**แก้ไขปัญหาเครื่องพิมพ์ขัดข้อง
ภายใน 20 นาที**

**โปรแกรมโรงพยาบาลขัดข้อง
ภายใน 25 นาที**



**สัญญาณ Internet ขัดข้อง
ภายใน 30 นาที**

**ขอข้อมูลสารสนเทศทางการแพทย์
ภายใน 1 วัน**



**เผยแพร่ข่าวสารลงในเว็บไซต์
เพจโรงพยาบาล ภายใน 1 วัน**

สายด่วน ติดต่อ แจ้งปัญหา เบอร์ภายใน 124