เกณฑ์การเยี่ยมประเมินมาตรฐานระบบบริการสุขภาพ และเกณฑ์การให้คะแนน
ด้านที่ ๙ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ จำนวน ๕ ข้อ

๑.๑ มีการจัดทีมดูแลระบบสารสนเทศของสถานพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

คำอธิบายเกณฑ์

สถานพยาบาลมีการจัดทำเอกสารคำสั่งแต่งตั้งคณะกรรมการหรือคณะทำงานที่มีบทบาทหน้าที่ดูแลและรับผิดชอบระบบสารสนเทศของสถานพยาบาล ซึ่งประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** คำสั่งแต่งตั้งทีมดูแลระบบสารสนเทศของสถานพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ
๐.๕	มีทีมดูแลระบบสารสนเทศของสถานพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ แต่ขาดเอกสาร**s**คำสั่งแต่งตั้งเป็นลายลักษณ์อักษร **หรือ** เอกสารแนบไม่ตรงกับวัตถุประสงค์
๑	มีทีมดูแลระบบสารสนเทศของสถานพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ **และ** แสดงเอกสารคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร

เอกสารอ้างอิง คำสั่งแต่งตั้งทีมดูแลระบบสารสนเทศของสถานพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ, คำสั่งแต่งตั้งคณะกรรมการด้านพัฒนาคุณภาพ เป็นต้น

เอกสารตัวอย่าง ข้อ 1.1

สำเนาคู่ฉบับ

คำสั่งกรมสนับสนุนบริการสุขภาพ
ที่ ๑๒๓๑ /๒๕๖๓
เรื่อง แต่งตั้งคณะกรรมการอำนวยการและคณะทำงาน
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ รวมทั้งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ มีผลบังคับใช้ ส่งผลให้กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข เป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่มีผลกระทบต่อประชาชนโดยตรงจากการเชื่อมโยงข้อมูลด้านสารสนเทศ

ด้วยกรมสนับสนุนบริการสุขภาพ ได้ปรับปรุงการแบ่งส่วนราชการใหม่ ดังประกาศในราชกิจจานุเบกษา เล่มที่ ๑๓๗ ตอนที่ ๔๑ ก ลงวันที่ ๙ มิถุนายน ๒๕๖๓ มีผลบังคับใช้ในการแบ่งส่วนราชการและภารกิจของหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ ดังนั้นอาศัยอำนาจตามมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม กรมสนับสนุนบริการสุขภาพ จึงออกคำสั่งดังต่อไปนี้

ข้อ ๑ ยกเลิกคำสั่งกรมสนับสนุนบริการสุขภาพ ที่ ๒๕๗/๒๕๖๓ ลงวันที่ ๗ กุมภาพันธ์ พ.ศ. ๒๕๖๓ เรื่อง แต่งตั้งคณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ข้อ ๒ แต่งตั้งคณะกรรมการอำนวยการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ประกอบด้วยบุคคล ดังต่อไปนี้

๒.๑ อธิบดีกรมสนับสนุนบริการสุขภาพ	ที่ปรึกษา
๒.๒ รองอธิบดีกรมสนับสนุนบริการสุขภาพ ที่ได้รับมอบหมาย ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (Department Chief Information Officer : DCIO)	ประธานกรรมการ
๒.๓ เลขานุการกรม	กรรมการ
๒.๔ ผู้อำนวยการกองกฎหมาย	กรรมการ
๒.๕ ผู้อำนวยการกองแบบแผน	กรรมการ
๒.๖ ผู้อำนวยการกองวิศวกรรมการแพทย์	กรรมการ
๒.๗ ผู้อำนวยการกองสถานประกอบการเพื่อสุขภาพ	กรรมการ
๒.๘ ผู้อำนวยการกองสถานพยาบาลและการประกอบโรคศิลปะ	กรรมการ
๒.๙ ผู้อำนวยการกองสนับสนุนสุขภาพภาคประชาชน	กรรมการ
๒.๑๐ ผู้อำนวยการกองสุขศึกษา	กรรมการ
๒.๑๑ ผู้อำนวยการกลุ่มตรวจสอบภายใน	กรรมการ

๒.๑๒ ผู้อำนวยการ...

๒.๑๒ ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร	กรรมการ
๒.๑๓ ผู้อำนวยการกลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม	กรรมการ
๒.๑๔ ผู้อำนวยการกลุ่มแผนงาน สำนักงานเลขานุการกรม	กรรมการ
๒.๑๕ หัวหน้ากลุ่มงานคุ้มครองจริยธรรม	กรรมการ
๒.๑๖ ผู้อำนวยการกองสุขภาพระหว่างประเทศ	กรรมการ
๒.๑๗ ผู้อำนวยการศูนย์คุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ	กรรมการ
๒.๑๘ ผู้อำนวยการสำนักผู้เชี่ยวชาญ	กรรมการ
๒.๑๙ ผู้อำนวยการศูนย์บริการแบบเบ็ดเสร็จ	กรรมการ
๒.๒๐ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๑	กรรมการ
๒.๒๑ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๒	กรรมการ
๒.๒๒ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๓	กรรมการ
๒.๒๓ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๔	กรรมการ
๒.๒๔ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๕	กรรมการ
๒.๒๕ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๖	กรรมการ
๒.๒๖ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๗	กรรมการ
๒.๒๗ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๘	กรรมการ
๒.๒๘ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๙	กรรมการ
๒.๒๙ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๐	กรรมการ
๒.๓๐ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๑	กรรมการ
๒.๓๑ ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๒	กรรมการ
๒.๓๒ ผู้อำนวยการศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคเหนือ จังหวัดนครสวรรค์	กรรมการ
๒.๓๓ ผู้อำนวยการศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น	กรรมการ
๒.๓๔ ผู้อำนวยการศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคกลาง จังหวัดชลบุรี	กรรมการ
๒.๓๕ ผู้อำนวยการศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคใต้ จังหวัดนครศรีธรรมราช	กรรมการ
๒.๓๖ ผู้อำนวยการศูนย์พัฒนาการสาธารณสุขมูลฐาน ชายแดนใต้ จังหวัดยะลา	กรรมการ
๒.๓๗ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม	กรรมการและเลขานุการ

๒.๓๘ นางสาวธนิมา สังข์สุวรรณ์ กรรมการและ
กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม ผู้ช่วยเลขานุการ

ให้คณะกรรมการมีอำนาจหน้าที่ดังต่อไปนี้

๑. กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๒. บริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพภายใต้มาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศและเกี่ยวข้อง

๓. กำกับ ดูแลการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๔. กำกับ ดูแลการพัฒนาและการบริหารจัดการข้อมูลของกรมสนับสนุนบริการสุขภาพให้มีคุณภาพและมีความมั่นคงปลอดภัย

๕. กำกับ ติดตามการทำงานของคณะทำงานรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๖. แต่งตั้งคณะอนุกรรมการหรือคณะทำงานตามความเหมาะสม

ข้อ ๓ แต่งตั้งคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ประกอบด้วย บุคคลดังต่อไปนี้

๓.๑ รองอธิบดีกรมสนับสนุนบริการสุขภาพ ที่ได้รับมอบหมาย ประธานคณะทำงาน
ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (Department Chief Information Officer : DCIO)

๓.๒ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ รองประธานคณะทำงาน
สำนักงานเลขานุการกรม

๓.๓ ผู้แทนสำนักงานเลขานุการกรม คณะทำงาน

๓.๔ ผู้แทนกองกฎหมาย คณะทำงาน

๓.๕ ผู้แทนกองแบบแผน คณะทำงาน

๓.๖ ผู้แทนกองวิศวกรรมการแพทย์ คณะทำงาน

๓.๗ ผู้แทนกองสถานประกอบการเพื่อสุขภาพ คณะทำงาน

๓.๘ ผู้แทนกองสถานพยาบาลและการประกอบโรคศิลปะ คณะทำงาน

๓.๙ ผู้แทนกองสนับสนุนสุขภาพภาคประชาชน คณะทำงาน

๓.๑๐ ผู้แทนกองสุขศึกษา คณะทำงาน

๓.๑๑ ผู้แทนกลุ่มตรวจสอบภายใน คณะทำงาน

๓.๑๒ ผู้แทนกลุ่มพัฒนาระบบบริหาร คณะทำงาน

๓.๑๓ ผู้แทนกลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม คณะทำงาน

๓.๑๔ ผู้แทนกลุ่มแผนงาน สำนักงานเลขานุการกรม คณะทำงาน

๓.๑๕ ผู้แทนกลุ่มงานคุ้มครองจริยธรรม คณะทำงาน

๓.๑๖ ผู้แทนกองสุขภาพระหว่างประเทศ คณะทำงาน

๓.๑๗ ผู้แทนศูนย์คุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ คณะทำงาน

๓.๑๘ ผู้แทนสำนักผู้เชี่ยวชาญ คณะทำงาน

๓.๑๙ ผู้แทนศูนย์บริการแบบเบ็ดเสร็จ	คณะทำงาน
๓.๒๐ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๑	คณะทำงาน
๓.๒๑ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๒	คณะทำงาน
๓.๒๒ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๓	คณะทำงาน
๓.๒๓ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๔	คณะทำงาน
๓.๒๔ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๕	คณะทำงาน
๓.๒๕ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๖	คณะทำงาน
๓.๒๖ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๗	คณะทำงาน
๓.๒๗ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๘	คณะทำงาน
๓.๒๘ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๙	คณะทำงาน
๓.๒๙ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๐	คณะทำงาน
๓.๓๐ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๑	คณะทำงาน
๓.๓๑ ผู้แทนศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๒	คณะทำงาน
๓.๓๒ ผู้แทนศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคเหนือ จังหวัดนครสวรรค์	คณะทำงาน
๓.๓๓ ผู้แทนศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น	คณะทำงาน
๓.๓๔ ผู้แทนศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคกลาง จังหวัดชลบุรี	คณะทำงาน
๓.๓๕ ผู้แทนศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคใต้ จังหวัดนครศรีธรรมราช	คณะทำงาน
๓.๓๖ ผู้แทนศูนย์พัฒนาการสาธารณสุขมูลฐาน ชายแดนใต้ จังหวัดยะลา	คณะทำงาน
๓.๓๗ นางสาวธนิมา สังข์สุวรรณ์ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม	คณะทำงานและเลขานุการ

ให้คณะทำงานมีอำนาจและหน้าที่ดังนี้

๑. ทบทวนมาตรการ วางแผนการพัฒนา กำหนดแนวทางปฏิบัติ แบบฟอร์มและเอกสารที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลของส่วนราชการ รวมทั้งข้อมูลส่วนบุคคลและข้อมูลที่เกี่ยวข้องให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ

๒. วิเคราะห์ รวบรวม สถานการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ

๓. เผยแพร่ ประชาสัมพันธ์ นโยบาย มาตรการ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศให้แก่บุคลากรในหน่วยงานที่รับผิดชอบ

๔. ควบคุม ตรวจสอบ ติดตาม และประเมินผลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศภายในหน่วยงานที่รับผิดชอบให้เป็นไปตามมาตรฐานหรือแนวทางที่กรมสนับสนุนบริการสุขภาพกำหนด

๕. สรุปผลการดำเนินงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ เสนอคณะกรรมการอำนวยการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ทุก ๓ เดือน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๖ มิถุนายน พ.ศ. ๒๕๖๓

(นายธเรศ กรัษนัยรวิวงค์)
อธิบดีกรมสนับสนุนบริการสุขภาพ

ร่าง
พิมพ์
ตรวจ

๑.๒ มีการจัดทำแผนแม่บทหรือแผนพัฒนาของสถานพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

คำอธิบายเกณฑ์

สถานพยาบาลจัดทำมีการจัดให้มีแผนแม่บทหรือแผนพัฒนา (Master Plan) ของสถานพยาบาล โดยมีองค์ประกอบที่สำคัญ คือ วิสัยทัศน์ เป้าหมาย และยุทธศาสตร์ โดยในส่วนของยุทธศาสตร์ นอกจากจะกำหนดเป้าหมายเชิงยุทธศาสตร์แล้ว จะต้องกำหนดแนวทางการพัฒนาและวิธีการนำเทคโนโลยีสารสนเทศมาใช้งาน เพื่อวัดผลการดำเนินงานที่ชัดเจนและเป็นรูปธรรมเพื่อให้สามารถปฏิบัติและวัดผลได้จริงแล้ว

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** แผนแม่บทหรือแผนพัฒนาของสถานพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน
๐.๕	มีแผนแม่บทหรือแผนพัฒนาของสถานพยาบาลโดยมีการกำหนดเป้าหมาย **หรือ** แนวทางการพัฒนา **หรือ** การใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน (แผนดังกล่าวครอบคลุมปีที่ทำการประเมิน)
๑	มีแผนแม่บทหรือแผนพัฒนาของสถานพยาบาลโดยมีการกำหนดเป้าหมาย **และ** แนวทางการพัฒนา **และ** การใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน (แผนดังกล่าวครอบคลุมปีที่ทำการประเมิน)

เอกสารอ้างอิง แผนแม่บทของสถานพยาบาล, โครงการหรือแนวทางการพัฒนางานและการใช้เทคโนโลยีสารสนเทศ, แผนพัฒนาดิจิตัล เป็นต้น

ประเด็นยุทธศาสตร์ (Strategic Issue)

๑. การพัฒนาโครงสร้างพื้นฐาน และบุคลากรด้านเทคโนโลยีสารสนเทศ
๒. การพัฒนาคุณภาพสารสนเทศโรงพยาบาลตามกรอบ HITQIF v.๑.๒
๓. การพัฒนาระบบคลังข้อมูลสารสนเทศและระบบเครือข่ายเพื่อเชื่อมโยงและบูรณาการข้อมูลสุขภาพ
๔. พัฒนาช่องทางการเข้าถึงระบบบริการสุขภาพ และเตรียมความพร้อมแก่บุคลากรเพื่อให้สามารถให้บริการได้อย่างมีคุณภาพ

เป้าประสงค์ (Goal)

๑. โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศทันสมัยเพื่อเชื่อมโยงระบบเครือข่ายให้พร้อมต่อการให้บริการประชาชน เหมาะสมต่อการปฏิบัติงานโดยใช้ทรัพยากรอย่างมีประสิทธิภาพ
๒. ประชาชนเข้าถึงบริการที่มีคุณภาพผ่านช่องทางเทคโนโลยีสารสนเทศที่สะดวก รวดเร็ว และปลอดภัย
๓. มีคลังข้อมูลที่เชื่อมโยงระบบงานเพื่อให้มีการบูรณาการ และการใช้ประโยชน์จากข้อมูลในเครือข่ายบริการสุขภาพร่วมกัน
๔. บุคลากรขององค์กรเข้าถึงและใช้ประโยชน์จากเทคโนโลยีสารสนเทศในการปฏิบัติงานได้อย่างมีประสิทธิภาพ
๕. โรงพยาบาลเป็นองค์กรที่มีคุณภาพด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัยได้มาตรฐาน

กลยุทธ์ (Strategic operation)

๑. พัฒนาและลงทุนในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่คุ้มค่าและเหมาะสมต่อความต้องการขององค์กร
๒. การพัฒนาเทคโนโลยีสารสนเทศเพื่อเชื่อมโยงการปฏิบัติงาน การบริหารจัดการที่รวดเร็วและมีประสิทธิภาพ
๓. การใช้ประโยชน์จากโครงสร้างพื้นฐาน/บริการกลางร่วมกันเพื่อให้เกิดการใช้ทรัพยากรอย่างคุ้มค่า
๔. พัฒนาช่องทางให้ประชาชนเข้าถึงบริการสุขภาพของโรงพยาบาลผ่านระบบเทคโนโลยีสารสนเทศในรูปแบบต่างๆ
๕. พัฒนาระบบคลังข้อมูลสารสนเทศที่มีคุณภาพ ทันสมัย
๖. เชื่อมโยงเครือข่ายสุขภาพผ่านเทคโนโลยีสารสนเทศที่รวดเร็ว ปลอดภัย

๗. ส่งเสริมและสนับสนุนการเรียนรู้ด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องแก่บุคลากรทุกระดับเพื่อเพิ่มประสิทธิภาพในการทำงาน

๘. เสริมสร้างศักยภาพของบุคลากรด้านเทคโนโลยีสารสนเทศ โดยเพิ่มพูนองค์ความรู้ มาตรฐานทางวิชาชีพ และทักษะด้านการบริหารจัดการเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ

๙. พัฒนาโรงพยาบาลให้เป็นองค์กรคุณภาพด้านเทคโนโลยีสารสนเทศผ่านการรับรองมาตรฐานคุณภาพ (HITQIF)

โดยเป้าประสงค์มีตัวชี้วัดและค่าเป้าหมายของเป้าประสงค์ดังนี้

ตัวชี้วัด	ผลงานที่ผ่านมา	ค่าเป้าหมาย (พ.ศ. ๒๕๖๑ - ๒๕๖๕)				
		๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
<u>เป้าประสงค์ที่ ๑</u> โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศทันสมัยเพื่อเชื่อมโยงเครือข่ายให้พร้อมต่อการให้บริการประชาชน เหมาะสมต่อการปฏิบัติงานโดยใช้ทรัพยากรอย่างมีประสิทธิภาพ						
ระดับความสำเร็จของการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ Hardware, Software และ Network Infrastructure	๑G BaseT Ethernet network, Wifi network, ระบบพิสูจน์ตัวตน, ระบบจัดเก็บข้อมูลจราจรเครือข่าย, ระบบป้องกันการโจมตีผ่านเครือข่าย, เว็บไซท์	Software Defined Datacenter	-	Fibre Optics Network	Software Defined Network,	Local Disastered Recovery Site
<u>เป้าประสงค์ที่ ๒</u> ประชาชนเข้าถึงบริการที่มีคุณภาพผ่านช่องทางเทคโนโลยีสารสนเทศที่สะดวก รวดเร็ว และ ปลอดภัย						
ระดับความสำเร็จของการพัฒนาช่องทางการเข้าถึงบริการของโรงพยาบาลผ่านเทคโนโลยีสารสนเทศ	ระบบ HIS : HosXp	H4U	Q4U	Health IoT	HIS Gateway	HIS Gateway
<u>เป้าประสงค์ที่ ๓</u> มีคลังข้อมูลที่เชื่อมโยงระบบงานเพื่อให้มีการบูรณาการ และการใช้ประโยชน์จากข้อมูลในเครือข่ายบริการสุขภาพร่วมกัน						

ตัวชี้วัด	ผลงานที่ผ่านมา	ค่าเป้าหมาย (พ.ศ. ๒๕๖๑ - ๒๕๖๕)				
		๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
จำนวนฐานข้อมูลด้านต่างๆ ระบบบริหารจัดการคลังข้อมูล และเครื่องมือที่เชื่อมโยงเครือข่ายบริการสุขภาพ	คลังข้อมูลสุขภาพ อ. ธัญบุรี	Virtual Private Network, H4U	Q4U	ระบบบริหารจัดการสารสนเทศ : Glpi,	HIS Gateway	Data warehouse
<u>เป้าประสงค์ที่ ๔</u> บุคลากรขององค์กรเข้าถึงและใช้ประโยชน์จากเทคโนโลยีสารสนเทศในการปฏิบัติงานได้อย่างมีประสิทธิภาพ						
ร้อยละของบุคลากรที่ขอมีบัญชีรายชื่อเพื่อใช้งานในระบบที่ให้บริการและได้รับอนุมัติบัญชีใช้งาน	- HosXp - Thairefer - Internet - VPN - LDAP - Mifare Card - Website	๑๐๐%	๑๐๐%	๑๐๐%	๑๐๐%	๑๐๐%
ร้อยละของบุคลากรที่ได้รับการอบรมการใช้งานระบบงานที่ให้บริการ	ยังไม่ได้ดำเนินการ					
<u>เป้าประสงค์ที่ ๕</u> โรงพยาบาลเป็นองค์กรที่มีคุณภาพด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัยได้มาตรฐาน						
ระดับความสำเร็จในการพัฒนาคุณภาพเทคโนโลยีสารสนเทศในโรงพยาบาล		←	—	HITQIF	—	→

โรงพยาบาลได้ทำการวิเคราะห์ศักยภาพ และการวิเคราะห์สภาพแวดล้อมมากำหนดทิศทางการพัฒนาและกลยุทธดังนี้

กลยุทธ์ที่ ๑ พัฒนาและลงทุนในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่คุ้มค่าและเหมาะสมต่อความต้องการขององค์กร

มาตรการและแนวปฏิบัติของกลยุทธ์

- ศึกษาวิเคราะห์ทิศทางและเป้าหมายของการพัฒนา/การลงทุนด้านโครงสร้างพื้นฐาน เทคโนโลยีสารสนเทศตามทิศทางของแผนแม่บทเทคโนโลยีสารสนเทศ ดังนี้
    - กำหนดทิศทางและเป้าหมายของการพัฒนาการลงทุนด้านโครงสร้างพื้นฐานเทคโนโลยี

สารสนเทศ ในแผนยุทธศาสตร์การพัฒนาของโรงพยาบาล และแผนแม่บทเทคโนโลยีสารสนเทศโรงพยาบาล

- การสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศเป็นกระบวนการตรวจสอบและทำบัญชีทรัพยากรด้านเทคโนโลยีสารสนเทศทั้งหมดของโรงพยาบาล เพื่อให้ทราบสถานะปัจจุบันก่อนที่จะเพิ่มเติมในส่วนที่ขาด หรือปรับปรุงแก้ไขในส่วนที่ล้าสมัย เพื่อให้ทรัพยากรทั้งหมดตอบสนองต่อการดำเนินการตามแผนยุทธศาสตร์ที่กำหนดไว้อย่างมีประสิทธิภาพ
- วิเคราะห์ช่องว่าง (Gap Analysis) เพื่อประเมินความแตกต่างระหว่าง สถานะปัจจุบันกับเป้าหมายหรือมาตรฐานที่ควรจะเป็น
- การวางแผนศักยภาพเทคโนโลยีสารสนเทศเป็นการสำรวจและวิเคราะห์ศักยภาพของทรัพยากรด้าน Hardware และ Network เพื่อวางแผนจัดการให้ทรัพยากรเหล่านี้ไม่ขาดแคลน ป้องกันปัญหาที่จะเกิดขึ้น และให้มั่นใจว่าใช้ทรัพยากรอย่างมีประสิทธิภาพ

- พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (ปรับปรุงข้อด้อย)
  - พัฒนาและลงทุนด้านทรัพยากรเทคโนโลยีสารสนเทศในองค์กรให้ครอบคลุมทุกด้าน
  - เพื่อเพิ่มเติมในส่วนที่ขาด หรือปรับปรุงแก้ไขในส่วนที่ล้าสมัย ได้แก่ Hardware, Software, Network, People และ Data and Information ให้เพียงพอและทันสมัย
  - ดำเนินการจัดสรรทรัพยากร งบประมาณเพื่อการลงทุน/พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศตามแนวทางที่กำหนด

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

กลยุทธ์ที่ ๒ การพัฒนาเทคโนโลยีสารสนเทศเพื่อเชื่อมโยงการปฏิบัติงาน การบริหารจัดการที่รวดเร็วและมีประสิทธิภาพ

มาตรการและแนวปฏิบัติของกลยุทธ์

- พัฒนาระบบสารสนเทศที่สนับสนุนการปฏิบัติงานที่เอื้อต่อการปฏิบัติงานในทุกที่ ทุกเวลา
  - กำหนดแนวทาง มาตรฐาน และกลไกในการจัดเก็บ แลกเปลี่ยน และเชื่อมโยงข้อมูลระหว่างหน่วยงานภายในองค์กร และหน่วยงานภายนอกองค์กร
  - วางระบบการจัดเก็บโดยกำหนดข้อมูลสำคัญที่ต้องจัดเก็บใน ให้มีข้อมูลเพียงพอต่อการให้ปฏิบัติงาน จัดระบบควบคุมเพื่อให้แน่ใจว่าข้อมูลและสารสนเทศในระบบถูกต้อง แม่นยำ

เชื่อถือได้และทันเวลา

- พัฒนาระบบสารสนเทศที่เป็นระบบกลางของโรงพยาบาล ที่ทุกหน่วยงานภายในองค์กรสามารถใช้ร่วมกันได้
    - การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อการเชื่อมโยงฐานข้อมูลการบริการ ประกอบด้วย ระบบห้องปฏิบัติการ ระบบรังสีวิทยา และฐานข้อมูลของระบบสนับสนุน ประกอบด้วย ระบบการเงินและบัญชี ระบบพัสดุ ระบบซ่อมและบำรุงรักษา ระบบประกันสุขภาพ ระบบบริหารทั่วไป ระบบสารบรรณ ระบบยานพาหนะ ระบบห้องประชุม
    - พัฒนาระบบสารสนเทศเพื่อลดความซ้ำซ้อนของการปฏิบัติงานระหว่างภายในองค์กร และเพิ่มประสิทธิภาพการปฏิบัติงานให้มีความสะดวก คล่องตัว รวดเร็ว เช่น ระบบลาออนไลน์ ระบบจองห้องประชุม ระบบขอใช้ยานพาหนะ ระบบขอใช้บริการต่างๆ ให้เป็นสำนักงานดิจิตัล (Office digital)
- การสนับสนุนให้มีการพัฒนาระบบสารสนเทศที่สามารถเข้าถึงผ่านทางอุปกรณ์เข้าถึงอินเทอร์เน็ตแบบเคลื่อนที่ (Mobile device) เพิ่มมากขึ้น
    - ศึกษาสำรวจความต้องการใช้ Applications และกำหนดแนวทางการพัฒนา/ใช้ประโยชน์จากเทคโนโลยีสมัยใหม่ เพื่อให้สามารถเข้าถึงระบบสารสนเทศผ่านทาง อุปกรณ์อินเทอร์เน็ตแบบเคลื่อนที่ (Mobile device) เข้าถึงทุกที่ ทุกเวลา

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนพัฒนาระบบบริหารจัดการด้วย เทคโนโลยีสารสนเทศ

กลยุทธ์ที่ ๓ การใช้ประโยชน์จากโครงสร้างพื้นฐาน/บริการกลางร่วมกันเพื่อให้เกิดการใช้ทรัพยากรอย่างคุ้มค่า

มาตรการและแนวปฏิบัติของกลยุทธ์

- พัฒนาโครงสร้างพื้นฐานที่เป็นระบบกลางเพื่อให้ทุกหน่วยงานสามารถใช้ประโยชน์ร่วมกันได้
    - ศึกษาความเป็นไปได้และความเหมาะสมในการนำเทคโนโลยีคอมพิวเตอร์ที่มีการประมวลผลบนเครื่องแม่ข่าย (Server) เครื่องเดียว และสามารถใช้งานร่วมกันได้บนเครื่องลูกข่าย (Client) หลายๆเครื่อง เช่น ระบบ Zero Client หรือ Thin Client
    - ศึกษาความเป็นไปได้และความเหมาะสมในการนำเทคโนโลยีและอุปกรณ์ที่มีการเชื่อมต่อแบบไร้สาย (Wireless) หรือใช้งานผ่านระบบเครือข่ายแบบ Ethernet

- ใช้ประโยชน์จากทรัพยากรให้มีประสิทธิภาพ และประหยัดค่าใช้จ่ายในการบำรุงรักษาภายใต้การใช้จ่ายงบประมาณที่มีอยู่อย่างจำกัด
    - ศึกษาความเป็นไปได้และความเหมาะสมในการใช้ประโยชน์จาก Cloud Services เพื่อให้สามารถใช้ประโยชน์ร่วมกันได้ และช่วยลดการซื้ออุปกรณ์โดยเฉพาะฮาร์ดแวร์ที่สิ้นเปลืองได้ และเพื่อลดความเสี่ยงต่อความเสียหายของข้อมูลบนเครื่องแม่ข่ายได้ เช่น การใช้ระบบ Cloud ภาครัฐ หรือ G-Cloud และ ระบบ GIN
    - ศึกษาความเป็นไปได้และความเหมาะสมของการใช้งาน Cloud Computing ร่วมกัน พร้อมทั้งจัดทำแนวทางการเปลี่ยนผ่านไปสู่ระบบ Cloud ขององค์กร
    - ศึกษาความเป็นไปได้และความเหมาะสมในการใช้บริการ Outsource Service ใน การเช่าอุปกรณ์ วางระบบและบำรุงรักษา เช่น การเช่าอุปกรณ์เครือข่ายทั้งระบบบสาย และไร้สาย เป็นต้น

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนเสริมสร้างการใช้ทรัพยากรเทคโนโลยีสารสนเทศอย่างประหยัดและคุ้มค่า

กลยุทธ์ที่ ๔ พัฒนาช่องทางให้ประชาชนเข้าถึงบริการสุขภาพของโรงพยาบาลผ่านระบบเทคโนโลยีสารสนเทศในรูปแบบต่างๆ

มาตรการและแนวปฏิบัติของกลยุทธ์

- การสำรวจความต้องการใช้บริการของประชาชนหรือผู้มารับบริการ
    - ศึกษาความต้องการของประชาชนหรือผู้รับบริการ ที่มีต่อบริการสุขภาพของ โรงพยาบาล
    - กำหนดแนวทางการพัฒนาระบบการให้บริการสุขภาพของโรงพยาบาลให้สามารถ เข้าถึงได้หลากหลายช่องทาง ตรงตามความต้องการของประชาชนและผู้มารับบริการ
- สำรวจช่องทางการนำเทคโนโลยีสารสนเทศมาใช้พัฒนาระบบบริการในรูปแบบต่างๆ
    - ศึกษาความเป็นไปได้และความเหมาะสมในการให้บริการในรูปแบบ Self Service เพื่อความสะดวก รวดเร็ว ทันต่อเวลา และลดระยะเวลารอคอยบริการ
    - ศึกษาเทคโนโลยีสารสนเทศสมัยใหม่เข้ามาช่วยในการให้บริการที่สามารถเข้าถึงได้ทุกที่ ทุกเวลา อุปกรณ์ที่สามารถเข้าถึงระบบบริการผ่านอินเตอร์เน็ต การประชาสัมพันธ์บริการต่างๆ ของโรงพยาบาล อินเตอร์เน็ต

- การพัฒนาช่องการเข้าถึงบริการทางผ่านระบบเทคโนโลยีสารสนเทศ
  - ช่องทางการเข้าถึงระบบบริการผ่านอินเตอร์ เช่น ระบบเครือข่ายสังคมออนไลน์ (Social network Online) เช่น Facebook, Line, Youtube หรือ Website เป็นต้น
  - พัฒนารูปแบบการเข้าถึงบริการผ่านอุปกรณ์เคลื่อนที่ เช่น Mobile Application ทั้งในระบบ Android, IOS และ Windows phone หรือ Website ที่สามารถแสดง ผลได้เหมาะสมทุกอุปกรณ์ทั้ง Computer, Notebook, Smart Phone หรือ Tablet
  - ช่องทางการให้บริการของโรงพยาบาลผ่านระบบการแพทย์ทางไกล (Telemedicine) หรือระบบนัดหมายแพทย์ออนไลน์ ระบบให้บริการความรู้ออนไลน์
  - ช่องทางการให้บริการเครือข่ายบริการสุขภาพ เช่น ระบบให้บริการรับ-ส่งต่อผู้ป่วยออนไลน์

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนพัฒนาช่องทางการให้บริการผ่านระบบเทคโนโลยีสารสนเทศ

กลยุทธ์ที่ ๕ พัฒนาระบบคลังข้อมูลสารสนเทศที่มีคุณภาพ ทันสมัย

มาตรการและแนวปฏิบัติของกลยุทธ์

๑) ปรับปรุงระบบฐานข้อมูล และระบบอินเตอร์เน็ต ตามแนวทาง ดังนี้

- จัดทำระบบข้อมูลภายในให้เป็นระบบที่เอื้อต่อการถ่ายทอดผ่านระบบอินเตอร์เน็ต
- ปรับปรุงระบบอินเตอร์เน็ตที่ทันสมัยเป็นการบริการออนไลน์ ที่มีข้อมูลที่สมบูรณ์

๒) สร้างคลังข้อมูลเพื่อการเชื่อมโยงและบูรณาการตามแนวทาง ดังนี้

- ศึกษาความเป็นไปได้ในการจัดหาเครื่องมือเพื่อนำมาใช้ในการบริหารจัดการระบบฐานข้อมูลทั้งหมด
- ทำการสร้างคลังข้อมูลจากฐานข้อมูลภายในหน่วยงาน ตลอดจนสร้างช่องทางในการเชื่อมโยง/แลกเปลี่ยนข้อมูล

๓) พัฒนาเทคโนโลยีด้านสารสนเทศให้ทันกับการเปลี่ยนแปลงของเทคโนโลยีในปัจจุบัน

- ปรับปรุงระบบบริหารจัดการฐานข้อมูลให้ทันสมัยตลอดเวลา
- สร้างช่องทางการเข้าถึงสารสนเทศสุขภาพผ่านระบบเทคโนโลยีสารสนเทศที่ทันสมัย

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนพัฒนาระบบคลังข้อมูล

กลยุทธ์ที่ ๖ เชื่อมโยงเครือข่ายสุขภาพผ่านเทคโนโลยีสารสนเทศที่รวดเร็ว ปลอดภัย

มาตรการและแนวปฏิบัติของกลยุทธ์

- พัฒนาโครงสร้างพื้นฐานระบบเครือข่ายอินเตอร์เน็ตให้มีความเสถียร เพื่อการเชื่อมโยงที่มีคุณภาพและประสิทธิภาพ
    - ใช้ระบบเครือข่ายอินเตอร์เน็ตที่มีความเร็วสูงและมีเสถียรภาพ คุณภาพ ผ่านระบบ บริการอินเทอร์เน็ตสำหรับองค์กร (MPLS) หรือระบบอินเทอร์เน็ตแบบโครงข่ายใยแก้วนำแสง (FTTX)
    - ใช้การติดต่อสื่อสารโดยใช้โทรศัพท์ผ่านระบบอินเตอร์เน็ต หรือ (Voice over IP)
    - เชื่อมโยงเครือข่ายฯ ทั้งภาครัฐต่อภาครัฐ และภาครัฐต่อประชาชน ให้เป็นระบบที่ สามารถเข้าถึงได้ง่ายสะดวก ผ่านระบบเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงาน ภาครัฐ ซึ่งมีความมั่นคงปลอดภัยและเชื่อถือได้ รวมทั้งสามารถรองรับการใช้งาน บริการแบบ Multi-Media โดยการบูรณาการให้เกิดบริการต่าง ๆ ใน ซึ่งทุกคน สามารถเข้าถึงบริการของภาครัฐผ่านทางบริการอินเทอร์เน็ตด้วยความสะดวก รวดเร็ว ตลอดเวลาไม่มีวันหยุด เช่น ระบบ GIN (Government Information Network)

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนพัฒนาโครงสร้างพื้นฐานระบบเครือข่าย

กลยุทธ์ที่ ๗ ส่งเสริมและสนับสนุนการเรียนรู้ด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องแก่บุคลากรทุกระดับเพื่อเพิ่มประสิทธิภาพในการทำงาน

มาตรการและแนวปฏิบัติของกลยุทธ์

- พัฒนาองค์กรให้มีบรรยากาศเอื้อต่อการพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศ
    - ปรับระบบการทำงานในองค์กรโดยนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการปฏิบัติงานในทุก

ระดับทั้งระดับการบริหารจัดการ การวางแผน การปฏิบัติงาน การติดตามและประเมินผลงาน เพื่อสร้างการเรียนรู้ให้บุคลากรได้สัมผัสการใช้งานระบบเทคโนโลยีมากขึ้น

- ใช้ระบบเทคโนโลยีสารสนเทศที่ทันสมัยเข้ามาอำนวยความสะดวกในการปฏิบัติงาน แสดงให้เห็นประโยชน์ของการใช้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบแสดงสถานะงานบริการต่างๆ ระบบเรียกคิวออนไลน์ ระบบแบบสอบถามออนไลน์ เป็นต้น

- จัดสถานที่ให้บุคลากรได้เรียนรู้การใช้งานเทคโนโลยี
  - จัดให้มีพื้นที่สำหรับเรียนรู้/ใช้งานเทคโนโลยีสารสนเทศแบบ Self Learning
  - ส่งเสริมให้บุคลากรที่มีความสนใจด้านระบบเทคโนโลยีสารสนเทศได้เข้าร่วมการอบรมพัฒนาความรู้และทักษะด้านเทคโนโลยีสารสนเทศทั้งหลักสูตรที่จัดภายในองค์และภายนอกองค์กร
  - สร้างหลักสูตรด้านเทคโนโลยีสารสนเทศเพื่อพัฒนาความรู้และทักษะด้านเทคโนโลยีสารสนเทศแก่บุคลากรทุกระดับ ให้มีศักยภาพในการนำระบบเทคโนโลยีสารสนเทศ มาใช้ในการปฏิบัติงานให้มีประสิทธิภาพ เช่น หลักสูตรการใช้โปรแกรม LibreOffice หรือ Internet Security Awareness เป็นต้น
- สร้างระบบประเมินความรู้และทักษะด้านเทคโนโลยีสารสนเทศที่ได้มาตรฐานเพื่อประเมินสมรรถนะด้านเทคโนโลยีสารสนเทศ
  - มีระบบการประเมินสมรรถนะด้านเทคโนโลยีสารสนเทศของบุคลากรทุกปีเพื่อเป็นการวัดผลความรู้และทักษะด้านเทคโนโลยีสารสนเทศของบุคลากรทุกคน

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนงานสร้างเสริมการเรียนรู้ด้านเทคโนโลยีสารสนเทศ

กลยุทธ์ที่ ๘ เสริมสร้างศักยภาพของบุคลากรด้านเทคโนโลยีสารสนเทศ โดยเพิ่มพูนองค์ความรู้ มาตรฐานทางวิชาชีพ และทักษะด้านการบริหารจัดการเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ

มาตรการและแนวปฏิบัติของกลยุทธ์

- พัฒนาความรู้ ทักษะ และศักยภาพ ทักษะหลักที่เกี่ยวข้องกับงานโดยตรงของบุคลากรด้านเทคโนโลยีสารสนเทศ
  - กำหนดสมรรถนะเชิงเทคนิค (IT Competency Framework) ของบุคลากรที่สำคัญในระบบเทคโนโลยีสารสนเทศ (CIO, หัวหน้าหน่วยเทคโนโลยีสารสนเทศ, ช่างเทคนิค)

- ส่งเสริมให้บุคลากรเข้ารับการฝึกอบรมด้านเทคโนโลยีสารสนเทศในหลักสูตรที่จ าเป็นต่อการปฏิบัติงานดังที่ระบุใน IT Competency Framework

- พัฒนาทักษะด้านการบริหารจัดการเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ
  - จัดให้มีการฝึกอบรมในหลักสูตรทีเกี่ยวกับ soft skills ให้กับบุคลากรสายเทคนิคเพื่อส่งเสริมการทำงานกับบุคลากรในสายงานด้านอื่นๆ ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น เช่น การสื่อสาร การมีแนวคิดเกี่ยวกับนวัตกรรมเชิงบริการ และการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ
- พัฒนาความเข้มแข็งของกลุ่มผู้บริหารเทคโนโลยีสารสนเทศขององค์กร (CIO และผู้บริหารศูนย์เทคโนโลยีสารสนเทศขององค์กร)
  - ส่งเสริมให้กลุ่มผู้บริหารเทคโนโลยีสารสนเทศ ขององค์กร มีหลักสูตรการฝึกอบรมด้านเทคโนโลยีสารสนเทศ อย่าง น้อยปีละ ๒ ครั้งเพื่อเรียนรู้เกี่ยวกับความก้าวหน้าและการเปลี่ยนแปลงของเทคโนโลยีใหม่ๆ ที่ส่งผลต่อองค์กรรวมถึงแนวคิดในการบริหารจัดการสารสนเทศยุคใหม่ เช่น แนวคิดเชิงนวัตกรรมบริการภาครัฐโดยการประยุกต์ใช้เทคโนโลยีสารสนเทศ การออกแบบระบบเทคโนโลยีสารสนเทศ ในแนวทางของสถาปัตยกรรมขององค์กร (Enterprise Architecture: EA)

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ

กลยุทธ์ที่ ๙ พัฒนาโรงพยาบาลให้เป็นองค์กรคุณภาพด้านเทคโนโลยีสารสนเทศผ่านการรับรองมาตรฐานคุณภาพ (HITQIF)

มาตรการและแนวปฏิบัติของกลยุทธ์

- การพัฒนามาตรฐานด้านการพัฒนาคุณภาพด้านเทคโนโลยีสารสนเทศในโรงพยาบาล
  - การสร้างพื้นฐานความรู้ทางการพัฒนาคุณภาพด้านเทคโนโลยีสารสนเทศ แก่บุคลากร พร้อมเสริมการศึกษา เรียนรู้จากแนวปฏิบัติที่ดีในประเทศเพื่อการนำมาประยุกต์ในโรงพยาบาล

- การสร้างระบบกระบวนการปฏิบัติงานตามเกณฑ์มาตรฐาน HITQIF และบูรณาการสู่งานประจำและแผนแม่บทด้าน เทคโนโลยีสารสนเทศ
- ดำเนินการจัดทำแผนการพัฒนาคุณภาพเทคโนโลยีสารสนเทศในโรงพยาบาลตามหลัก PDCA ในทุกประเด็น

- การพัฒนาคุณภาพเทคโนโลยีสารสนเทศในโรงพยาบาล ตามมาตรฐาน HITQIF มีแนวทาง ดังนี้
  - การวางแผนเทคโนโลยีสารสนเทศเพื่อกำหนดแนวทางการนำเทคโนโลยีสารสนเทศมาประยุกต์ให้โรงพยาบาลดำเนินงานอย่างมีประสิทธิภาพและประสิทธิผล
  - การวางระบบข้อมูลเพื่อกำหนดข้อมูลสำที่ต้องจัดการให้มีข้อมูลเพียงพอต่อการให้บริการ มีการเผยแพร่และส่งต่อข้อมูลที่เหมาะสม จัดระบบควบคุมเพื่อให้แน่ใจว่าข้อมูลและสารสนเทศในระบบถูกต้อง แม่นยำ เชื่อถือได้และทันเวลา
  - การสำวจทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อตรวจสอบแลทำบัญชีทรัพยากรด้านเทคโนโลยีสารสนเทศทั้งหมดของโรงพยาบาล เพื่อให้ทราบสถานะปัจจุบัน ก่อนที่จะเพิ่มเติมในส่วนที่ขาด หรือปรับปรุงแก้ไขในส่วนที่ล้าสมัย
  - วิเคราะห์ช่องว่าง (Gap Analysis) เพื่อประเมินความแตกต่างระหว่างสถานะปัจจุบัน กับเป้าหมายหรือมาตรฐานที่ควรจะเป็น
  - การวางแผนศักยภาพเทคโนโลยีสารสนเทศ เพื่อการสำรวจและวิเคราะห์ศักยภาพของทรัพยากรด้าน Hardware และ Network เพื่อวางแผนจัดการให้ทรัพยากรเหล่านี้ไม่ขาดแคลน ป้องกันปัญหาที่จะเกิดขึ้น และให้มั่นใจว่าใช้ทรัพยากรอย่างมีประสิทธิภาพ
  - การจัดตั้งจุดบริการและการจัดการให้ระบบดำเนินอย่างต่อเนื่อง เป็นหน่วยงานที่คอยรับการแจ้งปัญหาที่ผู้ใช้ระบบเทคโนโลยีสารสนเทศแจ้งเข้ามาแล้วให้บริการแก้ไข ปัญหาเบื้องต้น รวบรวมปัญหาที่ต้องแก้ไขระยะกลางและระยะยาว
  - การจัดการระดับบริการของหน่วยบริการเทคโนโลยีสารสนเทศ ด้วยการทำข้อตกลง ระดับบริการ (Service Level Agreement) ซึ่งเป็นเอกสารที่กำหนดระดับการให้บริการเทคโนโลยีสารสนเทศกับหน่วยงานอื่นๆของโรงพยาบาล
  - การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดการรักษาความลับ (Confidentiality) ข้อมูลเที่ยงตรงแม่นยำ (Integrity) และมีความพร้อมให้ใช้งาน

(Availability) โดยการจัดการให้ผู้มีสิทธิระดับที่สมควรเท่านั้นที่สามารถเข้าถึงข้อมูลลับได้

- การจัดการอุบัติการณ์ (Incident Management) เพื่อให้ระบบกลับมาดำเนินการตามปกติอย่างรวดเร็วที่สุดเท่าที่เป็นไปได้โดยเกิดความเสียหายน้อยที่สุด
- การจัดการปัญหา (Problem Management) ต้องการกำจัดสาเหตุที่ทำให้เกิดอุบัติการณ์ให้หมดไปอย่างถาวร
- การจัดการโครงการ (IT Project Management) เพื่อให้ได้ระบบใหม่ที่มีคุณภาพ ตรงตามความต้องการ สำเร็จใช้งานได้ทันเวลา ภายในงบประมาณที่กำหนด
- ระบบจัดการการเปลี่ยนแปลง (IT Project Management) เพื่อให้ได้การเปลี่ยนแปลงที่ดีขึ้น ตรงตามความต้องการ สำเร็จใช้งานได้ทันเวลา ภายในงบประมาณ ที่กำหนดและไม่ส่งผลกระทบอันไม่พึงปรารถนา
- การจัดการปรับเปลี่ยนและติดตั้งเทคโนโลยีที่ออกมาใหม่ (Release and Deploy Management) เพื่อจัดการปรับเปลี่ยนและติดตั้งให้ผู้ใช้งานได้ใช้งานเทคโนโลยีที่ใหม่
- การจัดการทรัพย์สินและข้อมูลทรัพยากรการให้บริการ (Service Asset and Configuration Management) เพื่อเป็นการจัดทำฐานข้อมูลทรัพย์สินที่เกี่ยวข้องกับการให้บริการเทคโนโลยีสารสนเทศ
- การจัดการรายการบริการเพื่อให้มั่นใจได้ว่า มีการจัดทำรายการบริการ (Service Catalog) และมีการดำเนินการปรับปรุงแก้ไขให้รายการบริการทันสมัยตรงตามการบริการเทคโนโลยีสารสนเทศที่โรงพยาบาลมีอยู่
- การจัดการความรู้และปรับปรุงคุณภาพอย่างต่อเนื่อง เพื่อจัดทำรายงานและบทสรุปจากการทำโครงการหรือกิจกรรมมาสังเคราะห์สารสนเทศและสร้างให้เกิดความรู้

หน่วยงานที่รับผิดชอบในการขับเคลื่อนกลยุทธ์

๑. ศูนย์เทคโนโลยีสารสนเทศ

แผนงาน/โครงการสำคัญ

๑. แผนพัฒนาคุณภาพเทคโนโลยีสารสนเทศ

๑.๓ มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของสถานพยาบาล

คำอธิบายเกณฑ์

สถานพยาบาลมีการจัดทำนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศ (Action Plan) ซึ่งเป็นแผนระยะสั้นที่กำหนดขึ้นเป็นปีต่อปีเพื่อช่วยขับเคลื่อนให้แผนระยะยาว (แผนแม่บทหรือแผนพัฒนา)

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** นโยบายหรือแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศ (Action Plan) ของสถานพยาบาล
๐.๕	มีนโยบาย **หรือ** แผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของสถานพยาบาล (Action Plan)
๑	มีนโยบาย **และ** แผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของสถานพยาบาล (Action Plan) (แผนการปฏิบัติของปีปัจจุบัน)

เอกสารอ้างอิง นโยบายต่างๆ ของสถานพยาบาล, แผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของสถานพยาบาล, แผนพัฒนาดิจิตัล เป็นต้น

บทที่ ๔ แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์

การแปลงยุทธศาสตร์สู่การพัฒนาเทคโนโลยีสารสนเทศ โรงพยาบาลธัญบุรี พ.ศ. ๒๕๖๑ – ๒๕๖๕ ไปสู่การปฏิบัติประกอบด้วย ๙ แผนงาน ดังต่อไปนี้

แผนงานที่ ๑ แผนพัฒนาโครงสร้างพื้นฐานด้านทคโนโลยีสารสนเทศ

แผนงานที่ ๒ แผนพัฒนาระบบบริหารจัดการด้วยเทคโนโลยีสารสนเทศ

แผนงานที่ ๓ แผนส่งเสริมการใช้ทรัพยากรเทคโนโลยีสารสนเทศอย่างคุ้มค่า

แผนงานที่ ๔ แผนพัฒนาช่องทางการให้บริการผ่านระบบเทคโนโลยีสารสนเทศ

แผนงานที่ ๕ แผนคลังความข้อมูลสารสนเทศ

แผนงานที่ ๖ แผนถ่ายทอดความรู้ผ่านระบบเทคโนโลยีสารสนเทศ

แผนงานที่ ๗ แผนสร้างเสริมการเรียนรู้ด้านเทคโนโลยีสารสนเทศ

แผนงานที่ ๘ แผนพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ

แผนงานที่ ๙ แผนพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศ

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	ผลผลิต	ผู้รับผิดชอบ	งบประมาณ ๕ ปี	งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)				
				๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
แผนงานที่ ๑ แผนพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ								
กิจกรรมที่ ๑ พัฒนาระบบ เทคโนโลยีสารสนเทศ Infrastructure ด้าน Hardware, Software, Network, Data and Information, และ People								
โครงการจัดหาและปรับปรุงประสิทธิภาพระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	- มีอุปกรณ์คอมพิวเตอร์ และอุปกรณ์ต่อพ่วงใช้งานเพียงพอ มีประสิทธิภาพเหมาะสมกับงาน	ศูนย์เทคโนโลยีสารสนเทศ	๑,๑๐๐,๐๐๐	๒๒๐,๐๐๐	๒๒๐,๐๐๐	๒๒๐,๐๐๐	๒๒๐,๐๐๐	๒๒๐,๐๐๐
โครงการจัดหาและติดตั้งระบบ Fibre Optic เพื่อเชื่อมต่อระบบเครือข่ายระหว่างอาคารผู้ป่วย ๔ ชั้น กับอาคารผู้ป่วย ๑๐ ชั้น และระหว่างชั้นภายในอาคารผู้ป่วย ๑๐ ชั้น	- มีระบบเครือข่ายที่รองรับการขยายตัวของข้อมูลในระบบเครือข่ายทั้งในเชิงปริมาณและความเร็ว โดยรองรับการขยายตัวได้ในระดับ ๑๐ - ๑๐๐ Gb/s	ศูนย์เทคโนโลยีสารสนเทศ	๔๔๐,๐๐๐			๔๔๐,๐๐๐		
โครงการจัดหาและปรับปรุงประสิทธิภาพระบบเครือข่ายคอมพิวเตอร์แบบ ๑๐G BaseT, ๑G BaseT Ethernet และระบบไร้สาย	- มีอุปกรณ์กระจายสัญญานเครือข่ายที่รองรับการเชื่อมต่อที่ความเร็ว ๑๐Gb/s ณ จุดกระจายสัญญาณหลัก - มีระบบไร้สายที่มีสัญญาณ	ศูนย์เทคโนโลยีสารสนเทศ	๓,๐๐๐,๐๐๐			๑,๐๐๐,๐๐๐	๑,๐๐๐,๐๐๐	๑,๐๐๐,๐๐๐

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	ผลผลิต	ผู้รับผิดชอบ	งบประมาณ ๕ ปี	งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)				
				๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
	ครอบคลุมการใช้งานในจุดที่จำเป็น - มีระบบเครือข่ายแบบ ๑G BaseT Ethernet ที่ครอบคลุมพื้นที่ใช้งานทั้งหมด							
โครงการจัดตั้งศูนย์ข้อมูลสำรองภายในหน่วยงาน (Local Disaster Recovery Site : Local DR Site)	- มีอุปกรณ์จำเป็นสำหรับการสำรองข้อมูลในระบบ Virtualization ได้แก่ ● เครื่องแม่ข่าย Hypervisor จำนวน ๒ เครื่อง ● SAN Storage จำนวน ๒ เครื่อง ● L๓ Switch ๑๖ SFP+ ports จำนวน ๒ เครื่อง ● Virtualization Disaster Recovery Software ● อุปกรณ์สำรองไฟฟ้าขนาด	ศูนย์เทคโนโลยีสารสนเทศ	๕,๐๐๐,๐๐๐	๑,๐๐๐,๐๐๐	๑,๐๐๐,๐๐๐	๑,๐๐๐,๐๐๐	๑,๐๐๐,๐๐๐	๑,๐๐๐,๐๐๐

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	ผลผลิต	ผู้รับผิดชอบ	งบประมาณ ๕ ปี	งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)				
				๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
	๑๐ KVA จำนวน ๒ ชุด - มีพื้นที่สำหรับจัดตั้งเป็นศูนย์สำรองข้อมูลภายในหน่วยงาน โดยต้องอยู่ต่างพื้นที่กับศูนย์ข้อมูล							
โครงการปรับปรุงพื้นที่ศูนย์ข้อมูล (Data Center)	- ศูนย์ข้อมูลได้รับการปรับปรุงให้เป็นไปตามมาตรฐาน HITQIF v ๑.๒	ศูนย์เทคโนโลยีสารสนเทศ	๑,๐๐๐,๐๐๐	๒๐๐,๐๐๐	๒๐๐,๐๐๐	๒๐๐,๐๐๐	๒๐๐,๐๐๐	๒๐๐,๐๐๐
โครงการจัดหา Software ลิขสิทธิ์ / Freeware / Opensource Software	- อุปกรณ์คอมพิวเตอร์ทุกเครื่องในโรงพยาบาลมีการติดตั้งเฉพาะ Software ที่มีลิขสิทธิ์/สิทธิในการใช้งานถูกต้องตามกฎหมาย	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการจัดหาและปรับปรุงประสิทธิภาพระบบ Virtualization	- มีอุปกรณ์ที่จำเป็นสำหรับการขยายระบบ Virtualization เพื่อรองรับการขยายตัวขององค์กรและภารกิจ ได้แก่ ● E5 ๒๖๔๐ CPU Chip สำหรับ Lenovo system x	ศูนย์เทคโนโลยีสารสนเทศ	๕๗๕,๐๐๐	๑๑๕,๐๐๐	๑๑๕,๐๐๐	๑๑๕,๐๐๐	๑๑๕,๐๐๐	๑๑๕,๐๐๐

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	ผลผลิต	ผู้รับผิดชอบ	งบประมาณ ๕ ปี	งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)				
				๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
	๓๕๕๐ M๕ จำนวน 3 ชุด ● Registered DDR-๔ ๒๓๓๓ MHz RAM R-Dim ๑๖ GB จำนวน ๓๖ ชุด ● SAS Hard disk ๑๐k rpm ๑.๒ TB จำนวน ๒๔ ชุด							
<u>กิจกรรมที่ ๒</u> พัฒนาระบบ Maintenance Software และ infrastructure ด้านต่างๆ								
โครงการบำรุงรักษาระบบป้องกันการโจมตีผ่านเครือข่าย (Firewall)	- จ้างเหมาการบำรุงรักษาอุปกรณ์ Fortigate 240D และ Fortigate 100D	ศูนย์เทคโนโลยีสารสนเทศ	๗๓๐,๐๐๐	๑๔๖,๐๐๐	๑๔๖,๐๐๐	๑๔๖,๐๐๐	๑๔๖,๐๐๐	๑๔๖,๐๐๐
โครงการบำรุงรักษาระบบจัดเก็บข้อมูลจราจรเครือข่าย (Network Traffic Log Server)	- จ้างเหมาการบำรุงรักษาอุปกรณ์ Fortianalyzer 200D	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการต่ออายุ HosXp Activation	- ซื้อสิทธิ์ในการเข้าถึง/ดาวน์โหลดโปรแกรม HosXp รุ่นใหม่ เพื่อปรับปรุงระบบ Hospital Information System (HIS) ให้	ศูนย์เทคโนโลยีสารสนเทศ	๑๓๕,๐๐๐	๒๗,๐๐๐	๒๗,๐๐๐	๒๗,๐๐๐	๒๗,๐๐๐	๒๗,๐๐๐

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	**ผลผลิต**	**ผู้รับผิดชอบ**	**งบประมาณ ๕ ปี**	**งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)**				
				๒๕๖๑	**๒๕๖๒**	**๒๕๖๓**	**๒๕๖๔**	**๒๕๖๕**
	มีความทันสมัย							
โครงการต่ออายุ VMware Subscription	- ซื้อสิทธิ์ในการเข้าถึง/ดาวน์โหลดระบบ VMware vSphere เพื่อปรับปรุงระบบ Virtualization ของโรงพยาบาลให้มีประสิทธิภาพ และทันกับความเปลี่ยนแปลงของระบบเทคโนโลยีปัจจุบัน	ศูนย์เทคโนโลยีสารสนเทศ	๒๐๐,๐๐๐	๔๐,๐๐๐	๔๐,๐๐๐	๔๐,๐๐๐	๔๐,๐๐๐	๔๐,๐๐๐
โครงการบำรุงรักษาอุปกรณ์บันทึกข้อมูลแบบภายนอก (External Storage)	- จ้างเหมาการบำรุงรักษาอุปกรณ์ IBM Storwize V3700 และ Lenovo Storwize V3700 V2	ศูนย์เทคโนโลยีสารสนเทศ	๔๗๐,๐๐๐	๙๔,๐๐๐	๙๔,๐๐๐	๙๔,๐๐๐	๙๔,๐๐๐	๙๔,๐๐๐
แผนงานที่ ๒ แผนพัฒนาระบบบริหารจัดการด้วยเทคโนโลยีสารสนเทศ								
<u>กิจกรรมที่ ๑</u> พัฒนาระบบสารสนเทศเพื่อการตัดสินใจ								
โครงการพัฒนาระบบคลังข้อมูล (Data warehouse)	- มีระบบคลังข้อมูลกลางเพื่อรองรับการประมวลผลข้อมูลขนาดใหญ่ (Big Data)	ศูนย์เทคโนโลยีสารสนเทศ						

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	**ผลผลิต**	**ผู้รับผิดชอบ**	**งบประมาณ ๕ ปี**	**งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)**				
				๒๕๖๑	**๒๕๖๒**	**๒๕๖๓**	**๒๕๖๔**	**๒๕๖๕**
กิจกรรมที่ ๒ พัฒนาระบบสารสนเทศเพื่อการบริหารจัดการ		ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบ E-Learning	- มีระบบ E-Learning สำหรับใช้ในการพัฒนาความรู้ ทักษะด้านเทคโนโลยีสารสนเทศแก่บุคลากร	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบบริหารจัดการงานสารสนเทศ	- ติดตั้งระบบบริหารจัดการสารสนเทศ GLPI	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบขอใช้บริการต่างๆ	- ติดตั้งระบบบริหารจัดการสารสนเทศ GLPI	ศูนย์เทคโนโลยีสารสนเทศ						
กิจกรรมที่ ๓ พัฒนาระบบสารสนเทศเพื่อการประชาสัมพันธ์องค์กร								
โครงการพัฒนาเว็บไซต์บนพื้นฐานของระบบ Cloud	- มีเว็บไซท์ขององค์กรที่เข้าถึงได้ทุกที่ ทุกเวลา	ศูนย์เทคโนโลยีสารสนเทศ	๑๙๐,๐๐๐	๓๘,๐๐๐	๓๘,๐๐๐	๓๘,๐๐๐	๓๘,๐๐๐	๓๘,๐๐๐
แผนงานที่ ๓ แผนส่งเสริมการใช้ทรัพยากรเทคโนโลยีสารสนเทศ อย่างคุ้มค่า								
กิจกรรมที่ ๑ พัฒนาระบบบริหารจัดการทรัพยากร เทคโนโลยีสารสนเทศ แบบรวมศูนย์								

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	ผลผลิต	ผู้รับผิดชอบ	งบประมาณ ๕ ปี	งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)				
				๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
โครงการพัฒนาติดตั้งจุดบริการ Printer แบบรวมศูนย์ผ่านระบบเครือข่าย (Network Printer)	- มีการใช้งานเครื่องพิมพ์ร่วมกันในจุดให้บริการที่อยู่ในบริเวณใกล้เคียง	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการจัดการฐานข้อมูลแบบรวมศูนย์ (Centralized Database Management)	- มีระบบคลังข้อมูลกลางเพื่อรองรับการประมวลผลข้อมูลขนาดใหญ่ (Big Data)	ศูนย์เทคโนโลยีสารสนเทศ						
กิจกรรมที่ ๒ ส่งเสริมความประหยัด เทคโนโลยีสารสนเทศ สีเขียว ช่วยประหยัดพลังงานและค่าใช้จ่าย								
โครงการส่งเสริมการจัดเก็บและประมวลผลข้อมูลแบบ Cloud	- ส่งเสริมให้บุคลากรมีการจัดเก็บข้อมูลงานส่วนบุคคลที่ไม่เกี่ยวข้องในระดับชั้นความลับหรือกระทบต่อสิทธิ์ของบุคคล ในระบบ Public Cloud	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการส่งเสริมการใช้อุปกรณ์ที่เชื่อมต่ออินเตอร์เน็ตแบบไร้สาย BYOD	- มีการกำหนดแนวทาง เงื่อนไขและระเบียบในการนำอุปกรณ์สารสนเทศส่วนบุคคลมาเชื่อมต่อเพื่อใช้งานภายในองค์กร	ศูนย์เทคโนโลยีสารสนเทศ						

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	**ผลผลิต**	**ผู้รับผิดชอบ**	**งบประมาณ ๕ ปี**	**งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)**				
				๒๕๖๑	**๒๕๖๒**	**๒๕๖๓**	**๒๕๖๔**	**๒๕๖๕**
แผนงานที่ ๔ แผนพัฒนาช่องทางการให้บริการผ่านระบบเทคโนโลยีสารสนเทศ								
กิจกรรมที่ ๑ พัฒนาระบบบริการสุขภาพโดยประยุกต์ใช้ระบบ เทคโนโลยีสารสนเทศ (E-Service)								
โครงการติดตั้งระบบสมุดสุขภาพประชาชน (H๔U)	- ระบบสมุดสุขภาพประชาชน (H๔U)	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการติดตั้งระบบคิวออนไลน์ (Q๔U)	- ระบบคิวออนไลน์ (Q๔U)	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบ Virtual Private Network (VPN)	- ระบบ Virtual Private Network (VPN)	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการติดตั้งระบบ His-Gateway	- ระบบ His-Gateway	ศูนย์เทคโนโลยีสารสนเทศ						
กิจกรรมที่ ๒ พัฒนาช่องทางการเข้าถึงบริการของ รพ.ผ่านระบบ เทคโนโลยีสารสนเทศ								
โครงการพัฒนาเว็บไซต์ ๒ ภาษา	- เว็บไซท์ทางการของโรงพยาบาลสนับสนุนการเข้าถึงทั้งภาษาไทย	ศูนย์เทคโนโลยีสารสนเทศ						

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	**ผลผลิต**	**ผู้รับผิดชอบ**	**งบประมาณ ๕ ปี**	**งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)**				
				๒๕๖๑	**๒๕๖๒**	**๒๕๖๓**	**๒๕๖๔**	**๒๕๖๕**
	และภาษาอังกฤษ							
โครงการติดตั้งและปรับระบบรับ-ส่งต่อ (ThaiRefer)	- มีการติดตั้ง และปรับปรุงระบบรับ-ส่งต่อผู้ป่วยให้ทันสมัย	ศูนย์เทคโนโลยีสารสนเทศ						
แผนงานที่ ๕ โครงการคลังข้อมูลสารสนเทศ								
กิจกรรมที่ ๑ ผลิตสื่อความรู้ในรูปแบบ Digital Content								
โครงการผลิตสื่อความรู้ในรูปแบบ E-document		ศูนย์เทคโนโลยีสารสนเทศ						
โครงการผลิตสื่อความรู้ในรูปแบบ Clip Video		ศูนย์เทคโนโลยีสารสนเทศ						
โครงการผลิตสื่อความรู้ในรูปแบบ Infographic		ศูนย์เทคโนโลยีสารสนเทศ						
โครงการผลิตสื่อความรู้ในรูปแบบ Banner		ศูนย์เทคโนโลยีสารสนเทศ						
แผนงานที่ ๖ แผนถ่ายทอดความรู้ผ่านระบบเทคโนโลยีสารสนเทศ								
กิจกรรมที่ ๑ ถ่ายทอดความรู้ผ่านระบบ								

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	**ผลผลิต**	**ผู้รับผิดชอบ**	**งบประมาณ ๕ ปี**	**งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)**				
				๒๕๖๑	**๒๕๖๒**	**๒๕๖๓**	**๒๕๖๔**	**๒๕๖๕**
เทคโนโลยีสารสนเทศ								
โครงการพัฒนาระบบถ่ายทอดความรู้ผ่านระบบอินเตอร์เน็ตช่องทางเว็บไซต์		ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบถ่ายทอดความรู้ผ่านระบบ e-learning		ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบถ่ายทอดความรู้ผ่านคลังข้อมูลออนไลน์ (Data Warehouse)		ศูนย์เทคโนโลยีสารสนเทศ						
แผนงานที่ ๗ แผนสร้างเสริมการเรียนรู้ด้านเทคโนโลยีสารสนเทศ								
กิจกรรมที่ ๑ ปรับปรุงสภาพแวดล้อมและบรรยากาศในการทำงานที่เอื้อต่อการเรียนรู้								
โครงการพัฒนาห้องเรียนรู้ เทคโนโลยีสารสนเทศ Self Learning		ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาห้องบริการอินเตอร์เน็ตสืบค้น		ศูนย์เทคโนโลยีสารสนเทศ						
กิจกรรมที่ ๒ ปรับปรุงระบบงานโดยนำระบบเทคโนโลยีสารสนเทศ มาใช้เพิ่มประสิทธิภาพการทำงาน								

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	ผลผลิต	ผู้รับผิดชอบ	งบประมาณ ๕ ปี	งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)				
				๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
โครงการพัฒนาระบบเรียกคิวผ่านระบบเสียงอัตโนมัติ	- มีระบบเรียกคิวผ่านระบบเสียงอัติโนมัติ	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบสแกนลายนิ้วมือสำหรับการยืนยันตัวตน	- มีระบบสแกนลายนิ้วมือและเก็บเป็นฐานข้อมูลสำหรับใช้ในการยืนยันตัวตนของบุคลากร	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบแบบสอบถามออนไลน์	- มีระบบจัดทำ เก็บรวบรวม และประมวลผลแบบสอบถามออนไลน์	ศูนย์เทคโนโลยีสารสนเทศ						
กิจกรรมที่ ๓ ปรับปรุงระบบงานโดยนำระบบเทคโนโลยีสารสนเทศมาใช้เพิ่มประสิทธิภาพการทำงาน								
โครงการพัฒนาความรู้ และทักษะด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรทุกระดับ	- มีชุดหลักสูตรมาตรฐานสำหรับพัฒนาทักษะด้านสารสนเทศที่จำเป็นต่อการปฏิบัติงานแก่บุคลากรทุกระดับ	ศูนย์เทคโนโลยีสารสนเทศ						
โครงการพัฒนาระบบประเมินความรู้ และทักษะด้านเทคโนโลยีสารสนเทศ	- มีระบบทดสอบ จัดเก็บผล และประมวลผลการประเมินความรู้	ศูนย์เทคโนโลยีสารสนเทศ						

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	ผลผลิต	ผู้รับผิดชอบ	งบประมาณ ๕ ปี	งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)				
				๒๕๖๑	๒๕๖๒	๒๕๖๓	๒๕๖๔	๒๕๖๕
	และทักษะด้านเทคโนโลยีสารสนเทศของบุคลากร							
แผนงานที่ ๘ แผนพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ								
กิจกรรมที่ ๑ พัฒนาความรู้ ทักษะ และศักยภาพเกี่ยวข้องกับงานโดยตรงเฉพาะด้าน								
โครงการอบรมเชิงปฏิบัติการที่จัดขึ้นทั้งภายในและภายนอกองค์กรอย่างน้อยปีละ 1 ครั้ง	- การส่งเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศเข้ารับการอบรมในเนื้อหาที่เกี่ยวข้องกับการปฏิบัติงาน และจากผลการประเมินศักยภาพของบุคลากรในด้านที่จำเป็นต้องเพิ่มเติม	ศูนย์เทคโนโลยีสารสนเทศ	๑๕๐,๐๐๐			๕๐,๐๐๐	๕๐,๐๐๐	๕๐,๐๐๐
โครงการสนับสนุนให้บุคลากรด้านเทคโนโลยีสารสนเทศได้มีการสอบใบอนุญาติวิชาชีพด้านสารสนเทศ	- บุคลากรด้านเทคโนโลยีสารสนเทศมีใบอนุญาติวิชาชีพด้านสารสนเทศในสาขาที่เกี่ยวข้องกับการปฏิบัติงาน	ศูนย์เทคโนโลยีสารสนเทศ						
กิจกรรมที่ ๒ จัดสรรกรอบอัตรากำลังบุคลากรด้านเทคโนโลยีสารสนเทศให้เหมาะสมกับภาระ								

เอกสารตัวอย่าง ข้อ 1.3

แผนปฏิบัติการเพื่อการขับเคลื่อนยุทธศาสตร์การพัฒนา								
โครงการ/กิจกรรม	**ผลผลิต**	**ผู้รับผิดชอบ**	**งบประมาณ ๕ ปี**	**งบประมาณประจำปี พ.ศ. (ที่มาของงบประมาณ)**				
				๒๕๖๑	**๒๕๖๒**	**๒๕๖๓**	**๒๕๖๔**	**๒๕๖๕**
งาน								
โครงการขออนุมัติจัดสรรกรอบอัตรากำลังบุคลากรด้านเทคโนโลยีสารสนเทศเพิ่มเติม	- ได้รับการจัดสรรกรอบอัตรากำลังบุคลากรด้านเทคโนโลยีสารสนเทศเพิ่มเติม ได้แก่ นักวิชาการคอมพิวเตอร์, ช่างคอมพิวเตอร์	ศูนย์เทคโนโลยีสารสนเทศ		-	-	-	-	-
แผนงานที่ ๙ แผนพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศ								
กิจกรรมที่ ๑ การพัฒนาคุณภาพระบบสารสนเทศตามกรอบ HITQIF v๑.๒								

๑.๔ มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม

คำอธิบายเกณฑ์

สถานพยาบาลมีการจัดทำแผนผังที่แสดงถึงกลุ่มตำแหน่งงาน ซึ่งรวมกลุ่มเป็นสายการบังคับบัญชา โดยมีการแบ่งกลุ่มแบ่งระดับและแสดงให้เห็นถึงอัตรากำลังของหน่วยงานสารสนเทศ

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การแสดงโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม
๐.๕	มีการแสดงโครงสร้างหรือการจัดอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม **แต่ไม่แสดงให้เห็นถึงอัตรากำลังของหน่วยงาน**
๑	มีการแสดง **โครงสร้าง และ อัตรากำลัง** ของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม

เอกสารอ้างอิง แผนผังโครงสร้างหน่วยงานสารสนเทศของสถานพยาบาล เป็นต้น

เอกสารตัวอย่าง ข้อ 1.4

โครงสร้างบุคลากร

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม

นายอภินันท์ นิลฉาย
ตำแหน่ง นักเทคโนโลยีสารสนเทศชำนาญการพิเศษ
(ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ)

ข้าราชการ	11 อัตรา
พนักงานราชการ	2 อัตรา
จ้างเหมาบริการ	3 อัตรา

1. งานบริหารงานทั่วไปและแผนงาน
ขรก. 5 / จม. 1

หัวหน้างาน : นางสาวยุภาพันธ์ บินมิตตอร์
ตำแหน่งนักวิเคราะห์นโยบายและแผนชำนาญการ

1. นางกัญธิยารัตน์ รอดแสวง
ตำแหน่ง นักวิเคราะห์นโยบายและแผนชำนาญการ
2. นายชินโชติ พลนาคู
ตำแหน่ง นักวิเคราะห์นโยบายและแผนชำนาญการ
3. นางสาวนภาส์ณัฐ ชูเสิศธนาพันธ์
ตำแหน่ง เจ้าพนักงานธุรการชำนาญงาน
4. นางสาวณัทธรันทน์ บุญรักษา
ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน
5. นายรณชัย พานะกุล
ตำแหน่ง ปฏิบัติงานด้านบริหารงานทั่วไป

2. งานพัฒนาระบบเทคโนโลยีสารสนเทศ
ขรก. 5 / พรก. 1

หัวหน้างาน : นายอภินันท์ นิลฉาย
ตำแหน่ง ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ

1. นายสรายุทธ ภูตาสีบ
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
2. นางสาวนรารัตน์ มุลจันดา
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ
3. นายนันทชัย นุ่มน้อย
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ
4. นางสาววิภาพร วะเกิดแป้ม
ตำแหน่ง เจ้าพนักงานสถิติปฏิบัติการ
5. นายสมภพ ลายา
ตำแหน่ง นักวิชาการคอมพิวเตอร์

3. งานพัฒนานวัตกรรมดิจิทัล
ขรก. 2 / พรก. 1 / จม. 2

หัวหน้างาน : นายสรายุทธ ภูตาสีบ
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ

1. นางสาวฐิตาภรณ์ สุวรรณหงษ์
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ
2. นายภูวเดช เกิดอรุณเดช
ตำแหน่ง นักวิชาการคอมพิวเตอร์
3. นางสาวอุบลรัตน์ เทศนาบูรณ์
ตำแหน่ง ปฏิบัติงานด้านพัฒนาระบบสารสนเทศ
4. นางสาวหทัยภัทร พงศ์มานุรักษ์
ตำแหน่ง ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

๑.๕ มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม

คำอธิบายเกณฑ์

สถานพยาบาลมีการกำหนดระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล และแสดงเอกสารหลักฐานของมาตรฐานต่างๆ อย่างครบถ้วน ดังนี้

มาตรฐานข้อมูล คือ เป็นการจัดทำข้อมูลให้อยู่ในลักษณะรูปแบบกลาง (Neutral format) โดยเนื้อหาของมาตรฐานข้อมูลหลักๆ เช่น โครงสร้างมาตรฐานข้อมูลด้านสุขภาพ กระทรวงสาธารณสุขจะต้องมีการกำหนดคำศัพท์ (Data dictionaries) และข้อมูลจะต้องมีคุณภาพของข้อมูล (data quality) และในด้านคำอธิบายข้อมูล (Metadata) ซึ่งเป็นรายละเอียดบอกถึงเนื้อหาคุณลักษณะของข้อมูล

มาตรฐานรหัสข้อมูล คือ กฎเกณฑ์และแนวทางในการกำหนดรูปแบบและการนิยามข้อมูลที่ใช้ร่วมกัน เพื่ออำนวยความสะดวกในการแลกเปลี่ยนข้อมูลผ่านทางระบบคอมพิวเตอร์ กฎเกณฑ์จัดทำขึ้นจากการเห็นพ้องต้องกัน และได้รับความเห็นชอบจากองค์กรอันเป็นที่ยอมรับ เช่น มาตรฐานรหัสและข้อมูลสุขภาพแห่งชาติ (THCC) กระทรวงสาธารณสุข

มาตรฐานการปฏิบัติงาน คือ ข้อตกลงร่วมกันระหว่างผู้บังคับบัญชากับผู้ใต้บังคับบัญชาในงานที่ต้องปฏิบัติ โดยจะมีกรอบในการพิจารณากำหนดมาตรฐานหลายๆ ด้าน ด้วยกัน อาทิ ด้านปริมาณ คุณภาพ ระยะเวลา ค่าใช้จ่าย หรือพฤติกรรมของผู้ปฏิบัติงาน

มาตรฐานความปลอดภัยและความลับของผู้ป่วย คือ นโยบายหรือกฎเกณฑ์ และแนวทางปฏิบัติในการป้องกันไม่ให้เกิดความเสี่ยงต่อความปลอดภัยและความลับผู้ป่วย ซึ่งกำหนดให้ทุกคนตระหนักและเคารพสิทธิในการเก็บรักษาความลับข้อมูลของผู้รับบริการตามข้อกำหนดของมาตรฐานวิชาชีพ

มาตรฐานระบบเครือข่ายคอมพิวเตอร์ คือ แผนผังที่อธิบายอุปกรณ์ต่างๆ ที่ใช้ในเครือข่ายเป็นโครงสร้างในแง่ของการต่ออุปกรณ์ที่ใช้ในเครือข่าย เช่น Router , Switch โดยแสดงถึงเส้นทางการสื่อสารกัน

มาตรฐานทางกายภาพและสภาพแวดล้อม คือ นโยบายการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม และมาตรการเกี่ยวกับการเข้าถึงทางกายภาพและสภาพแวดล้อมสำหรับพื้นที่สำนักงาน พื้นที่จัดส่งและรับของ

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การแสดงหลักฐาน ระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล เช่น มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม
๐.๕	มีการแสดงมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล เช่น มาตรฐานข้อมูล หรือ มาตรฐานรหัสข้อมูล หรือ มาตรฐานการปฏิบัติงาน หรือ มาตรฐานความปลอดภัยและความลับของผู้ป่วย **ไม่น้อยกว่ากึ่งหนึ่ง**
๑	มีการแสดงหลักฐาน ระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม โดยมีการแสดงเอกสารหลักฐานระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ของ **อย่างครบถ้วน**

เอกสารอ้างอิง ผังระบบซอฟแวร์และเชื่อมโยงระบบฐานข้อมูลที่มีการใช้งานในสถานพยาบาล (มาตรฐานข้อมูล), การออกแบบฐานข้อมูลของระบบงาน (มาตรฐานรหัสข้อมูล), ระบบงานหน้าห้องตรวจของสถานพยาบาล (มาตรฐานการปฏิบัติงาน), นโยบายการใช้งานสื่อสังคมออนไลน์ของบุคลากร (มาตรฐานความปลอดภัยและความลับของผู้ป่วย), เอกสารผังเครือข่าย (มาตรฐานระบบเครือข่ายคอมพิวเตอร์), รูปภาพของสภาพแวดล้อมภายในสถานพยาบาล (มาตรฐานทางกายภาพและสภาพแวดล้อม) เป็นต้น

Name	Data Type	Length	Required?	Validation เอกสารตัวอย่าง ข้อ 1.5.1	Description	Sample
$txtID	text	7	Yes	Must exist	Student college ID	BLA0001
$txtPwd	text	20	Yes	Letters and numbers only	Password	2FatCats
$txtFood	text	15	Yes		Description of food item	Ham & Salad
$curPrice	currency	4	Yes		Cost of food items	$9.90
$intQty	integer	auto	No	<=5	Quantity of food item ordered	3

แบบฟอร์มแจ้งรายละเอียดผลิตภัณฑ์ยาที่ต้องการให้กำหนดรหัสยามาตรฐาน 24 หลัก

เลขทะเบียนยา หรือรหัสยาองค์การเภสัชกรรม	ชื่อการค้า	รูปแบบของยา	ตัวยาสำคัญ	ความแรง	บริษัทผู้จำหน่าย	บริษัทผู้ผลิต/นำเข้า (ถ้ามี)	รหัสยามาตรฐาน 24 หลัก
1C 1/64(NBC)	COVID-19 Vaccine AstraZeneca	SOLUTION FOR INJECTION	COVID-19 Vaccine	10 doses/vial (0.5 ml/dose)		**บริษัท แอสตร้าเซนเนก้า (ประเทศไทย) จำกัด**	**110070224038664210181597**
1C 3/64(NBC)	CoronaVac	SUSPENSION FOR INJECTION	COVID-19 Vaccine	1 dose/vial (0.5 ml/dose)		**องค์การเภสัชกรรม**	**110070224038664110181506**

เอกสารตัวอย่าง ข้อ 1.5.2

เอกสารตัวอย่าง ข้อ 1.5.3

มาตรฐานการพยาบาลและการผดุงครรภ์

พระราชบัญญัติวิชาชีพการพยาบาลและการผดุงครรภ์ (ฉบับที่ 2) พ.ศ.2540 กำหนดวัตถุประสงค์ให้สภาการพยาบาลส่งเสริมการศึกษา การบริการ การวิจัย และความก้าวหน้าในวิชาชีพการพยาบาลและการผดุงครรภ์ ประกอบกับข้อบังคับสภาการพยาบาลว่าด้วยข้อจำกัดและเงื่อนไขในการประกอบวิชาชีพ และการรักษาจริยธรรมแห่งวิชาชีพ กำหนดให้ผู้ประกอบวิชาชีพต้องรักษามาตรฐานของการประกอบวิชาชีพการพยาบาลและการผดุงครรภ์ในระดับที่ดีที่สุดในการปฏิบัติต่อผู้ป่วยหรือผู้รับบริการ ดังนั้นสภาการพยาบาลจึงได้กำหนดมาตรฐานหลักของบริการพยาบาลและการผดุงครรภ์ ทั้งที่เป็นบริการในชุมชนและในสถานบริการด้านการสาธารณสุข เพื่อให้หน่วยงานนำไปใช้ในการสร้างมาตรฐานที่เฉพาะเจาะจง สำหรับแต่ละหน่วยงานซึ่งจะนำไปสู่การบริการพยาบาลที่มีคุณภาพต่อไป ดังต่อไปนี้

ข้อ 1 มาตรฐานการพยาบาลและการผดุงครรภ์ (Nursing and Midwifery Standard) ประกอบด้วย มาตรฐานการบริหารองค์กรบริการพยาบาลและการผดุงครรภ์ (Standard of Nursing and Midwifery Service Organization) มาตรฐานการปฏิบัติการพยาบาลและการผดุงครรภ์ (Nursing and Midwifery Practice Standard) มาตรฐานผลลัพธ์การพยาบาลและการผดุงครรภ์ (Nursing and Midwifery Outcome Standard)

ข้อ 2 มาตรฐานการบริหารองค์กรบริการพยาบาลและการผดุงครรภ์ (Standard of Nursing and Midwifery Service Organization) มีรายละเอียดดังนี้

มาตรฐานที่ 1 การจัดองค์กรและการบริหารองค์กรบริการพยาบาลและการผดุงครรภ์

1.1 การบริหารจัดการการพยาบาลดำเนินการโดยองค์กรการพยาบาลและการผดุงครรภ์

1.2 ผู้บริหารสูงสุดขององค์กรเป็นพยาบาลวิชาชีพ

1.3 องค์กรการพยาบาลและการผดุงครรภ์มีอำนาจ หน้าที่และความรับผิดชอบในการกำหนดปรัชญา นโยบายทางการพยาบาลเพื่อเป็นทิศทางการปฏิบัติของทุกหน่วยงานบริการพยาบาลและการผดุงครรภ์

1.4 องค์กรการพยาบาลและการผดุงครรภ์มีโครงสร้างและขอบเขตงานในความรับผิดชอบชัดเจน

1.5 มีระบบและกลไกการบริหารที่เน้นการมีส่วนร่วมของบุคลากร และการประสานความร่วมมือระหว่างหน่วยงาน

1.6 มีนโยบาย เป้าหมายและแผนงานที่ส่งเสริมคุณภาพบริการพยาบาล และการส่งเสริมเอกสิทธิ์ในการปฏิบัติการพยาบาล

เอกสารตัวอย่าง ข้อ 1.5.3

มาตรฐานที่ 2 การบริหารจัดการทรัพยากรบุคคล

2.1 มีระบบและกลไกการคัดสรรบุคลากรให้เหมาะสมกับงาน

2.2 พยาบาลทุกระดับมีคุณสมบัติเหมาะสมและประสบการณ์ที่เพียงพอ ดังนี้

2.2.1 พยาบาลทุกคนต้องมีใบอนุญาตเป็นผู้ประกอบวิชาชีพ ตามกฎหมายวิชาชีพการพยาบาลและการผดุงครรภ์

2.2.2 พยาบาลวิชาชีพระดับหัวหน้าหน่วย / หอผู้ป่วย

(1) ได้รับการศึกษาต่อ และ/หรือฝึกอบรมในสาขาที่ให้บริการนั้น ๆ

(2) มีประสบการณ์ด้านการบริหาร และ/หรือผ่านการฝึกอบรมด้านบริหาร

2.2.3 พยาบาลวิชาชีพระดับผู้บริหารสูงสุดขององค์กรการพยาบาล

(1) สำเร็จการศึกษาในระดับปริญญาตรีหรือเทียบเท่า และได้รับการอบรมด้านการบริหาร หรือสำเร็จการศึกษาระดับปริญญาโท หรือเทียบเท่า หรือปริญญาเอก

(2) มีประสบการณ์ด้านการบริหารในระดับหอผู้ป่วยหรือหน่วยงาน

2.3 มีการกำหนดบทบาทหน้าที่ (Jobdescriptions) และคุณสมบัติเฉพาะตำแหน่ง (Jobspecification) ของผู้ให้บริการการพยาบาลทุกระดับชัดเจนตามลักษณะงานที่รับผิดชอบ

2.4 การจัดอัตรากำลังเหมาะสมกับความต้องการบริการพยาบาล (Nursing needs)

2.5 มีการจัดการเตรียมการการควบคุมกำกับและการประเมินผลการปฏิบัติงานที่สามารถสร้างความเชื่อมั่นให้กับผู้รับบริการว่าจะได้รับการบริการที่มีคุณภาพ

2.6 มีระบบการพัฒนาความรู้ ความสามารถบุคลากรเพื่อเสริมสร้างและพัฒนาความรู้ความสามารถในการปฏิบัติการพยาบาลที่ทันสมัย

มาตรฐานที่ 3 การจัดระบบงาน และกระบวนการให้บริการการพยาบาล และการผดุงครรภ์

3.1 การบริการพยาบาลและการผดุงครรภ์ต้องคำนึงถึงคุณภาพและความปลอดภัยของผู้รับบริการมีการกำหนดนโยบายและวิธีปฏิบัติ (NursingPolicy&Procedures) แนวทางการพยาบาลผู้ป่วย (NursingStandardofPatientCare) ภายใต้กฎหมายว่าด้วยการประกอบวิชาชีพการพยาบาลและการผดุงครรภ์รวมทั้งกฎหมายอื่นที่เกี่ยวข้องและขอบเขตการปฏิบัติการพยาบาลและการผดุงครรภ์

3.2 มีพยาบาลวิชาชีพเป็นหัวหน้าทีมการพยาบาลในการให้บริการการพยาบาลและการผดุงครรภ์ตลอดระยะเวลาที่ให้บริการ

3.3 การมอบหมายงานให้แก่บุคลากรที่มีความรู้และทักษะต่ำกว่าระดับวิชาชีพการพยาบาลและการผดุงครรภ์ ต้องไม่ใช่งานในระดับวิชาชีพการพยาบาลและการผดุงครรภ์ และมีพยาบาลผดุงครรภ์ ระดับวิชาชีพเป็นผู้กำกับดูแล

3.4 กำหนดนโยบาย และสนับสนุนการใช้กระบวนการพยาบาลในการปฏิบัติการพยาบาลและการผดุงครรภ์

3.5 มีกลไกส่งเสริมให้พยาบาลและผดุงครรภ์ประกอบวิชาชีพที่ได้มาตรฐาน และธำรงไว้ซึ่งจริยธรรม และจรรยาบรรณแห่งวิชาชีพ

3.6 มีการจัดระบบสารสนเทศ และใช้ข้อมูลสารสนเทศทางการพยาบาล ในการบริหารจัดการการดูแลช่วยเหลือผู้รับบริการและการพัฒนาคุณภาพการพยาบาลและการผดุงครรภ์

มาตรฐานที่ 4 ระบบการพัฒนาคุณภาพการพยาบาลและการผดุงครรภ์

4.1 มีนโยบายและแผนงานการจัดการคุณภาพการพยาบาล และการผดุงครรภ์

4.2 มีระบบการบริหารความเสี่ยง (Risk Management)

4.3 มีระบบประกันคุณภาพการพยาบาลและการผดุงครรภ์

4.4 มีการพัฒนาคุณภาพอย่างต่อเนื่อง (Continuous Quality Improvement)

ข้อ 3 มาตรฐานการปฏิบัติการพยาบาล และการผดุงครรภ์ (Nursing and Midwifery Practice Standard) เป็นการปฏิบัติที่มีเป้าหมายหลักเพื่อให้ผู้รับบริการ มีภาวะสุขภาพที่ดีที่สุดตามศักยภาพของแต่ละบุคคล ปัญหาสุขภาพและปัญหาที่เกี่ยวข้องได้รับการแก้ไขโดยพยาบาลและผดุงครรภ์ต้องปฏิบัติตามมาตรฐานการปฏิบัติการพยาบาลและการผดุงครรภ์ 5 มาตรฐาน ดังนี้

มาตรฐานที่ 1 การใช้กระบวนการพยาบาลในการปฏิบัติการพยาบาลและการผดุงครรภ์ต้องใช้กระบวนการพยาบาลแก่ผู้รับบริการอย่างเป็นองค์รวมทั้งในระดับบุคคล กลุ่มบุคคล ครอบครัว และชุมชน ตามศาสตร์และศิลปะการพยาบาลในด้านการส่งเสริมสุขภาพ การป้องกันโรค การรักษาพยาบาล และการฟื้นฟูสภาพ โดยผู้รับบริการมีส่วนร่วมอย่างเหมาะสม และมีการประสานความร่วมมือในทีมการพยาบาลและทีมสหสาขาวิชา

มาตรฐานที่ 2 การรักษาสิทธิผู้ป่วย จริยธรรม และจรรยาบรรณวิชาชีพยึดหลักคุณธรรม จริยธรรม และจรรยาบรรณวิชาชีพในการปฏิบัติการพยาบาลและการผดุงครรภ์ รวมทั้งการปฏิบัติเพื่อปกป้องและรักษาไว้ซึ่งสิทธิ ที่เกี่ยวข้องกับสุขภาพและการรักษาพยาบาลของ ผู้รับบริการ

มาตรฐานที่ 3 การพัฒนาคุณภาพการปฏิบัติการพยาบาลและการผดุงครรภ์ปฏิบัติการพยาบาลและการผดุงครรภ์ บนพื้นฐานของศาสตร์ทางการพยาบาลและศาสตร์ที่เกี่ยวข้อง ที่ทันสมัย โดยยึดผู้รับบริการเป็นศูนย์กลาง มีการทบทวน ประเมินกระบวนการการดูแล ผู้รับบริการอย่างเป็นระบบ มีการนำความรู้จากการวิจัยมาประยุกต์ใช้ในการปฏิบัติ เพื่อพัฒนาคุณภาพการปฏิบัติการพยาบาลและการผดุงครรภ์อย่างต่อเนื่อง

มาตรฐานที่ 4 การจัดการ การดูแลต่อเนื่อง ให้ผู้รับบริการได้รับการดูแลที่สอดคล้องกับภาวะสุขภาพอย่างต่อเนื่อง โดยมีการวางแผนร่วมกับทีมสุขภาพ ผู้รับบริการและ/หรือผู้เกี่ยวข้อง เพื่อพัฒนาศักยภาพของผู้รับบริการในการดูแลตนเอง และสามารถใช้แหล่งประโยชน์ในการดูแลตนเองอย่างเหมาะสม

เอกสารตัวอย่าง ข้อ 1.5.3

มาตรฐานที่ 5 การบันทึกและรายงานบันทึกและรายงานการพยาบาลและการผดุงครรภ์ให้ครอบคลุมการดูแลผู้รับบริการตามกระบวนการพยาบาล โดยครบถ้วน ถูกต้องตามความเป็นจริง ชัดเจน กะทัดรัด มีความต่อเนื่องและสามารถใช้เพื่อประเมินคุณภาพบริการการพยาบาลและการผดุงครรภ์ได้

ข้อ 4 มาตรฐานผลลัพธ์การพยาบาลและการผดุงครรภ์ (Nursing and Midwifery Outcome Standard) เป็นองค์ประกอบสำคัญในการประเมินคุณภาพของบริการพยาบาลและผดุงครรภ์ สามารถประเมินได้จากผลลัพธ์การปฏิบัติการพยาบาลและการผดุงครรภ์ โดยใช้กระบวนการพยาบาลว่าบรรลุ เป้าหมายที่กำหนดหรือไม่ และผลลัพธ์โดยรวมของบริการพยาบาลและผดุงครรภ์ทั้งหน่วยงาน ซึ่งอาจประเมินได้จากองค์ประกอบ ดังต่อไปนี้

4.1 ความปลอดภัยจากความเสี่ยง และภาวะแทรกซ้อนที่ป้องกันได้ ทั้งด้าน กาย จิตใจ สังคม และจิตวิญญาณ

4.2 ผู้รับบริการได้รับการบรรเทาจากความทุกข์ทรมาน ทั้งด้านกาย จิตใจ สังคม และจิตวิญญาณ

4.3 ความรู้ของผู้รับบริการเกี่ยวกับภาวะสุขภาพ

4.4 ความสามารถในการดูแลตนเองของผู้รับบริการ

4.5 ความพึงพอใจของผู้รับบริการและสิทธิที่พึงได้รับ

ทั้งนี้ หน่วยงานต้องพิจารณากำหนดตัวชี้วัดในแต่ละองค์ประกอบ ให้เหมาะสมกับลักษณะงานในหน่วยงานของตน และกำหนดเกณฑ์ที่ยอมรับได้ (threshold) ในแต่ละดัชนี

เอกสารตัวอย่าง ข้อ 1.5.4

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีและสารสนเทศ โรงพยาบาลกำแพงเพชร โทร ๑๒๑๙

ที่ กพ ๐๐๓๒.๒๐๒.๗/๐๐๒ **วันที่** ๑ ธันวาคม ๒๕๖๔

เรื่อง ประกาศใช้นโยบายและแนวทางปฏิบัติในการรักษามาตรฐานความปลอดภัยของผู้ป่วย สำหรับหน่วยงานในโรงพยาบาลกำแพงเพชร

เรียน หัวหน้ากลุ่มภารกิจ/หัวหน้ากลุ่มงาน/หัวหน้างาน และบุคลากรโรงพยาบาลกำแพงเพชรทุกท่าน

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง

ในการนี้โรงพยาบาลกำแพงเพชรจึงได้ดำเนินการจัดทำ "นโยบายและแนวทางปฏิบัติในการรักษามาตรฐานความปลอดภัยของผู้ป่วยโรงพยาบาลกำแพงเพชร" เพื่อให้การใช้งานระบบสารสนเทศของโรงพยาบาลกำแพงเพชรมีความปลอดภัย และสอดคล้องตามหลักกฎหมาย จึงประกาศใช้นโยบายและแนวทางปฏิบัติในการรักษามาตรฐานความปลอดภัยของผู้ป่วย ควบคุมการดำเนินการใดๆ ที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลกำแพงเพชร รายละเอียดตามประกาศที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อทราบ และถือปฏิบัติตามประกาศแนวทางดังกล่าวโดยเคร่งครัดต่อไป

(นายเจษฎา พวงสายใจ)
หัวหน้ากลุ่มภารกิจด้านพัฒนาระบบบริการ
และสนับสนุนบริการสุขภาพ

(นายสุรชัย แก้วหิรัญ)
ผู้อำนวยการโรงพยาบาลกำแพงเพชร

ร่าง.....
พิมพ์.....
ทาน.....
ตรวจ.....

เอกสารตัวอย่าง ข้อ 1.5.4

ประกาศโรงพยาบาลกำแพงเพชร

เรื่อง แนวทางปฏิบัติมาตรฐานความปลอดภัยของผู้ป่วยโรงพยาบาลกำแพงเพชร

เพื่อให้การดำเนินการใดๆ ต่อระบบสารสนเทศโรงพยาบาลกำแพงเพชร เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีการรักษาความมั่นคงปลอดภัย และตอกย้ำความสำคัญของความลับของผู้ป่วย ให้ผู้ปฏิบัติระมัดระวังในการให้ข้อมูลหรือเปิดเผยข้อมูลต่างๆ ของผู้ป่วยหรือผู้รับบริการด้านสารสนเทศ

โดยมีแนวทางการปฏิบัติ ดังต่อไปนี้

1. การแก้ไขข้อมูลผู้ป่วย ให้ดำเนินการได้ตามระเบียบปฏิบัติว่าด้วยการแก้ไขข้อมูลโดยเคร่งครัด เช่น หากเขียนผิดห้ามใช้ปากการะบายสีทึบทับข้อความจนมองไม่เห็นข้อความเดิม ห้ามใช้น้ำยาลบคำผิดในเวชระเบียนผู้ป่วย การแก้ไขทำได้โดยการลากเส้นทับข้อความเดิมเพียงเส้นเดียว แล้วเขียนข้อความที่แก้ไขไว้ใกล้กับข้อความเดิม พร้อมลงนามกำกับ และวันเวลาที่แก้ไข สำหรับการเขียนข้อความที่แก้ไขในระบบคอมพิวเตอร์ ห้ามลบข้อมูลเดิมทิ้ง แต่ให้ทำเครื่องหมายว่ามีการแก้ไข แล้วเชื่อมโยงข้อมูลที่เพิ่มเติมแก้ไขให้รู้ว่าข้อความใหม่ใช้แทนข้อความเดิมอย่างไร
2. การส่งข้อมูลผู้ป่วยให้กับบุคลากรภายในสถานพยาบาลเดียวกัน ให้ดำเนินการตามระเบียบการส่งข้อมูลอย่างเคร่งครัด เช่น ไม่ใช้ให้ผู้ป่วยถือเวชระเบียนจากจุดบริการหนึ่งไปยังจุดอื่นๆ
3. ตั้งรหัสผ่านในการเข้าใช้งานระบบคอมพิวเตอร์ของตนเองให้คาดเดาได้ยาก ตรงตามระเบียบของสถานพยาบาล ปกปิดรหัสผ่านเป็นความลับส่วนตัวอย่างเคร่งครัด ไม่อนุญาติให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ
4. ห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วย ในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ
5. ห้ามส่งข้อมูลผู้ป่วยที่ระบบตัวตนโดยใช้ช่องทางที่ไม่เหมาะสม เช่น ส่งทาง Line หรือ Social media
6. ห้ามใช้คอมพิวเตอร์ของสถานพยาบาลเปิดไฟล์จากภายนอกทุกกรณี สำหรับการเปิดไฟล์งานจากหน่วยงานภายในให้ตรวจหาไวรัสภายในไฟล์ทุกครั้งก่อนเปิดไฟล์
7. ห้ามนำคอมพิวเตอร์ อุปกรณ์อื่นๆ รวมถึงอุปกรณ์จัดเก็บข้อมูล เช่น CD-ROM, USB Drive, External Hard disk อุปกรณ์เครือข่าย เช่น Hub, Switch, Wi-fi Router ฯลฯ มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของโรงพยาบาลที่ใช้ฐานข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้อำนวยการ

8. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเตอร์เน็ตทุกกรณี ยกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเตอร์เน็ตพร้อมกันกับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วย ซึ่งได้รับอนุญาตจากผู้อำนวยการ

ประกาศนี้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่.....พ.ศ.2564

(นายสุรชัย แก้วหิรัญ)

ผู้อำนวยการโรงพยาบาลกำแพงเพชร

ประกาศคณะกรรมการสุขภาพแห่งชาติ

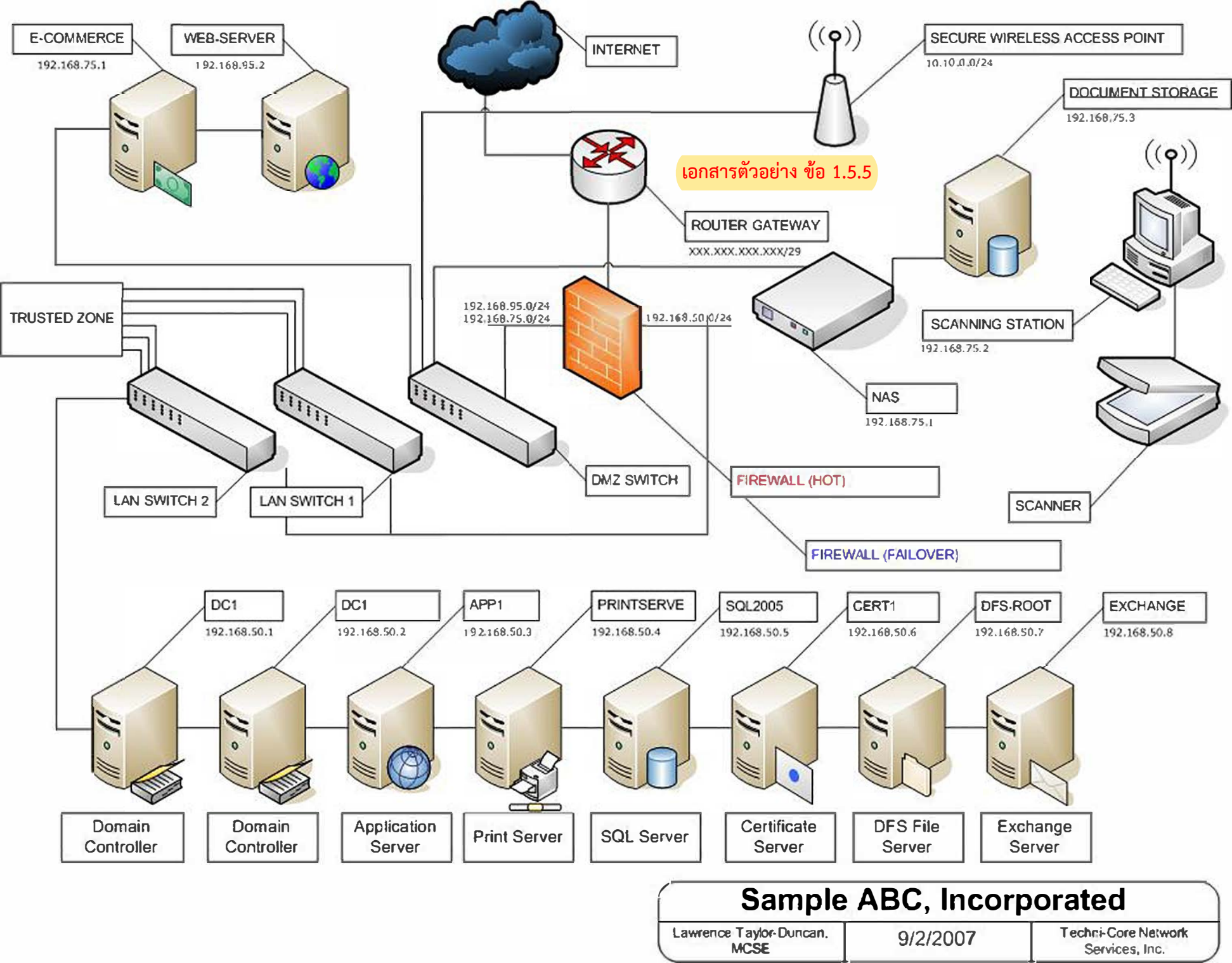
เรื่อง แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพ พ.ศ. ๒๕๕๙

ตามที่มาตรา ๗ แห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ บัญญัติให้ข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรงหรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย คณะกรรมการสุขภาพแห่งชาติได้เล็งเห็นความสำคัญในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพ เนื่องจากปัจจุบันมีการนำสื่อสังคมออนไลน์ (Social media) มาใช้อย่างแพร่หลายทั้งในเรื่องการทำงานและเรื่องการดำเนินชีวิต หากมีการใช้ไม่เหมาะสมอาจทำให้เกิดปัญหาในเรื่องการคุ้มครองข้อมูลด้านสุขภาพของผู้รับบริการสาธารณสุข จึงได้กำหนดแนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพขึ้น เพื่อนำไปประยุกต์ใช้เป็นแนวทางปฏิบัติของหน่วยงานด้านสุขภาพ หรือหน่วยงานที่เกี่ยวข้องได้กว้างขวางมากขึ้น

อาศัยอำนาจตามความในมาตรา ๒๕ (๑๐) แห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ ประกอบกับมติที่ประชุมคณะกรรมการสุขภาพแห่งชาติ ในการประชุมครั้งที่ ๕/๒๕๕๙ เมื่อวันที่ ๒๓ กันยายน ๒๕๕๙ คณะกรรมการสุขภาพแห่งชาติจึงประกาศแนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพ พ.ศ. ๒๕๕๙ ตามท้ายประกาศนี้เพื่อให้มีผลบังคับใช้ต่อไป

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ ธันวาคม พ.ศ. ๒๕๕๙
พลเรือเอก ณรงค์ พิพัฒนาศัย
รองนายกรัฐมนตรี
ประธานกรรมการสุขภาพแห่งชาติ



Sample ABC, Incorporated

Lawrence Taylor-Duncan, MCSE	9/2/2007	Techni-Core Network Services, Inc.

สมรรถนะในการปฏิบัติงาน การอบรมเพิ่มเติมต่อเนื่อง รวมถึงประวัติอุบัติเหตุจากการปฏิบัติงาน ประวัติการได้รับวัคซีนและสถานะภูมิคุ้มกันโรค

3.4 มีการประเมินผลการพัฒนาบุคลากรหลังการพัฒนาทุกครั้ง โดยพิจารณาในด้านทักษะ การเปลี่ยนพฤติกรรม ความสามารถ หรือผลกระทบต่อการดูแลและการบริการแก่ผู้ป่วยทั้งภายในหน่วยงานหรือภายนอกทุกครั้ง

3.5 ควรสนับสนุนให้บุคลากรที่ผ่านการพัฒนามีการถ่ายทอดความรู้ โดยนำเสนอความรู้ที่ได้รับจากการประชุม/อบรม/สัมมนาต่อที่ประชุมประจำเดือนของหน่วยงาน เพื่อถ่ายทอดความรู้ให้แก่ผู้ร่วมงานทุกคน พร้อมทั้งติดตามประเมินการนำความรู้ที่ได้รับสู่การปฏิบัติ เพื่อเป็นการพัฒนางานที่รับผิดชอบและปรับปรุงการให้บริการให้เกิดประโยชน์สูงสุดแก่ผู้ป่วยและหน่วยงาน

มาตรฐานที่ 4 สิ่งแวดล้อมและอาคารสถานที่

การจัดสิ่งแวดล้อม พื้นที่ใช้สอย หรือสิ่งอำนวยความสะดวกที่จำเป็นให้พร้อมและเพียงพอสำหรับปฏิบัติงานให้บรรลุตามพันธกิจ และต้องมีการบำรุงรักษาโดยคำนึงถึงความปลอดภัย เพื่อให้การบริการ ตอบสนองความต้องการของผู้รับบริการและผู้ให้บริการดำเนินงานเป็นไปอย่างมีประสิทธิภาพและมีประสิทธิผล

4.1 จัดโครงสร้างทางกายภาพและสิ่งอำนวยความสะดวกให้มีความเหมาะสมและปลอดภัย โครงสร้าง อาคาร สถานที่ และสิ่งแวดล้อมต้องมีเพียงพอ ตลอดจนเอื้ออำนวยให้ผู้ปฏิบัติงานสามารถดำเนินการผลิตและให้บริการอาหารผู้ป่วยได้อย่างสะดวก ปลอดภัย และมีประสิทธิภาพ

4.1.1 สถานที่ตั้งหน่วยงานมีความเหมาะสม สะดวกต่อการให้บริการ และสะดวกต่อการขนส่งอาหารไปยังหน่วยงานที่เกี่ยวข้อง

4.1.2 มีพื้นที่ใช้สอยที่จำเป็นต่อการปฏิบัติงาน มีพื้นที่เพียงพอต่อการปฏิบัติงาน และเอื้ออำนวยต่อการดำเนินกิจกรรมต่างๆได้อย่างมีประสิทธิภาพ สภาพทั่วไปภายในหน่วยงานมีความปลอดภัย มิดชิด มีการระบายอากาศดี แสงสว่างเพียงพอ ไม่มีสิ่งรบกวน มีความสะอาดเป็นระเบียบ มีการแบ่งโซนการปฏิบัติงานที่ถูกต้องตามหลักสุขาภิบาลอาหาร

4.1.3 หน่วยผลิตอาหารทางสายให้อาหารต้องแยกพื้นที่ปฏิบัติงานเป็นสัดส่วนชัดเจน เป็นระบบปิด มีการป้องกันการปนเปื้อนจากภายนอก และสามารถป้องกันสัตว์พาหะนำโรคได้ ต้องมีระบบระบายอากาศที่ดี ห้องเตรียมต้องมีการแยกบริเวณล้างวัตถุดิบ/ภาชนะ เตรียมวัตถุดิบและผลิตอาหารชัดเจนเพื่อป้องกันการปนเปื้อน

4.2 สิ่งแวดล้อมภายในและภายนอกอาคาร เป็นไปตามมาตรฐานสุขาภิบาลอาหารโรงพยาบาลหรือสถาบันมาตรฐานที่เป็นสากล

4.3 จัดให้มีแหล่งน้ำอุปโภคและน้ำบริโภคที่สะอาดต้องจัดให้มีแหล่งน้ำอุปโภคและน้ำบริโภคที่สะอาดเพียงพอต่อการผลิตอาหารควรมีทั้งระบบน้ำร้อนน้ำเย็น มีการสำรองน้ำเมื่อมีปัญหา มาตรฐานของน้ำในกระบวนการผลิตที่สัมผัสกับอาหารต้องมีคุณภาพเป็นไปตามมาตรฐานผลิตภัณฑ์อุตสาหกรรม

4.4 ระบบระบายน้ำ ต้องมีระบบระบายน้ำที่ดี รางระบายน้ำมีพื้นเรียบ มีความลาดเอียงที่เหมาะสม มีขนาดใหญ่เพียงพอในการระบายน้ำได้ในระยะเวลารวดเร็ว ไม่มีน้ำขัง มีฝาปิดมิดชิด ง่ายในการทำความสะอาดและมีการป้องกันสัตว์พาหะนำโรคจากท่อน้ำทิ้งเข้ามาบริเวณผลิตอาหาร

4.5 ระบบดักไขมัน ต้องมีระบบดักไขมันที่มีประสิทธิภาพและมีการกำจัดไขมันเป็นระยะๆ

4.6 วิธีการกำจัดขยะ มีวิธีการกำจัดขยะที่ถูกสุขลักษณะเป็นไปตามมาตรฐานสุขาภิบาลอาหารโรงพยาบาลหรือสถาบันมาตรฐานที่เป็นสากล

4.7 จัดระบบการควบคุมสารเคมีและวัตถุไวไฟ องค์กรต้องจัดให้มีการควบคุมดูแลสารเคมี วัตถุไวไฟ หรือวัสดุที่เป็นอันตราย ต้องมีสถานที่เก็บถังแก๊สหุงต้มแยกอยู่นอกอาคาร โดยต้องมีระบบป้องกันการล้มของถังแก๊สและการเข้าสู่บริเวณเก็บถังแก๊สโดยไม่ได้รับอนุญาต ต้องแยกเก็บสารเคมีให้เป็นสัดส่วน ไม่ปะปนกับวัตถุดิบและอาหาร ต้องมีการป้องกันการปนเปื้อนสารเคมีในอาหารและป้องกันการผิดพลาดในการหยิบใช้ มีการชี้บ่งบนฉลากและบริเวณที่เก็บอย่างชัดเจน ต้องมีการมอบหมายมีผู้ดูแลรับผิดชอบโดยเฉพาะและต้องมีการจัดทำคู่มือการควบคุมสารเคมีและวัตถุไวไฟเพื่อใช้เป็นแนวทางปฏิบัติ

4.8 สิ่งแวดล้อมและอาคารสถานที่มีการป้องกันอัคคีภัยที่เหมาะสมและติดตั้งถังดับเพลิงชนิด Wet Chemical

มาตรฐานที่ 5 เครื่องมือ อุปกรณ์และสิ่งอำนวยความสะดวก

องค์กรต้องจัดหาเครื่องมือ เครื่องทุ่นแรง วัสดุ ภาชนะ และอุปกรณ์ที่ช่วยผ่อนแรง และอำนวยความสะดวกให้เพียงพอ เพื่อให้ผู้ปฏิบัติงานสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพและปลอดภัยขณะปฏิบัติงาน

5.1 จัดหาเครื่องมือ เครื่องทุ่นแรง วัสดุ ภาชนะ และอุปกรณ์ที่อำนวยความสะดวกให้เพียงพอกับภาระงาน อุปกรณ์ผลิตด้วยวัสดุที่ไม่เป็นอันตรายและมีรูปแบบที่ทำความสะอาดง่าย ภาชนะบรรจุอาหารผู้ป่วยต้องคงทนต่อความร้อนและสารเคมีที่ใช้ทำความสะอาดหรือฆ่าเชื้อโรค

5.1.1 มีการสำรวจ ประเมินชนิดและปริมาณเครื่องมือ วัสดุ ภาชนะ และอุปกรณ์ที่จำเป็นสำหรับการผลิตและบริการอาหารผู้ป่วย มีระบบการสำรวจ วัสดุ อุปกรณ์ ครุภัณฑ์

๒. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ จำนวน ๕ ข้อ

๒.๑ มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

คำอธิบายเกณฑ์

สถานพยาบาลมีการวิเคราะห์และจัดลำดับความสำคัญของความเสี่ยง โดยพิจารณาจากการประเมินจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง (Impact) ต่อการบรรลุวัตถุประสงค์ของการดำเนินงาน **ด้านระบบเทคโนโลยีสารสนเทศของหน่วยงาน** คือ

๑. การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นการกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับของความเสี่ยง โดยคณะกรรมการบริหารความเสี่ยงของแต่ละหน่วยงานจะต้องกำหนดเกณฑ์ของหน่วยงาน เป็นเกณฑ์ในเชิงปริมาณและเชิงคุณภาพ

๒. การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้ มาประเมินโอกาส (Likelihood) ที่จะเกิดเหตุการณ์ความเสี่ยงต่าง ๆ และประเมินระดับความรุนแรงหรือมูลค่าความเสียหาย (Impact) จากความเสี่ยง เพื่อให้เห็นถึงระดับคะแนนของเสี่ยงที่แตกต่างกัน ทำให้สามารถกำหนดการควบคุมความเสี่ยงได้อย่างเหมาะสม

๓. การวิเคราะห์ความเสี่ยง เมื่อหน่วยงานพิจารณาโอกาส / ความถี่ที่จะเกิดเหตุการณ์ และความรุนแรงของผลกระทบในแต่ละปัจจัยเสี่ยง และนำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อหน่วยงานว่า ก่อให้เกิดความเสี่ยงในระดับคะแนนใด ตามตารางระดับความเสี่ยง ซึ่งจะทำให้หน่วยงานทราบว่า มีความเสี่ยงใดเป็นความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน

๔. การจัดลำดับความเสี่ยง เมื่อได้ค่าคะแนนระดับความเสี่ยงแล้ว จะนำมาจัดลำดับความรุนแรงของความเสี่ยง โดยพิจารณาจากระดับของความเสี่ยงที่เกิดจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยง ที่ประเมินได้ตามตารางการวิเคราะห์ความเสี่ยง ซึ่งจัดเรียงตามลำดับจากระดับคะแนนสูงมาก สูง ปานกลาง น้อย

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การประเมินความเสี่ยง และการให้คะแนนความเสี่ยง และการจัดลำดับความสำคัญ
๐.๕	มีการประเมินความเสี่ยง **แต่ขาด** การให้คะแนนความเสี่ยง **หรือ** การจัดลำดับความสำคัญ
๑	มีการประเมินความเสี่ยง **และ** การให้คะแนนความเสี่ยง **และ** การจัดลำดับความสำคัญ

เอกสารอ้างอิง แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ , การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศสถานพยาบาล เป็นต้น

เอกสารตัวอย่าง ข้อ 2.1

ขั้นที่ ๔ ระบุและจัดลำดับความเสี่ยง

ตารางที่ ๔ การประเมินความเสี่ยง

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
ปัจจัยเสี่ยง	**รายละเอียดความสูญเสีย**	**โอกาส**	**ผลกระทบ**	**ระดับความเสี่ยง**
๑. การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่)	- ทำให้ประชาชนไม่มั่นใจในคุณภาพข้อมูลของกรมสนับสนุนบริการสุขภาพ/ขาดความเชื่อมั่นใน ความปลอดภัยของข้อมูล - ทำให้ตกเป็นข่าวในประเทศ และต่างประเทศ	๓	๕	๑๕
๒. ความเสี่ยงจาก กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๓	๕	๑๕
๓. เครื่องแม่ข่ายถูกโจมตี	- ทำให้ระบบสารสนเทศ/ระบบสำคัญทำงานได้ช้ำ หรือทำงานไม่ได้	๓	๔	๑๒
๔. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	- เจ้าหน้าที่ในกรมสนับสนุนบริการสุขภาพ ไม่สามารถใช้งานระบบสารสนเทศภายในได้ - เจ้าหน้าที่ลงรับหนังสือไม่สามารถให้บริการผู้ที่มาติดต่อได้ ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๓	๔	๑๒
๕. ระบบให้บริการอินเทอร์เน็ต	- ทำให้กรมสนับสนุนบริการสุขภาพ ไม่สามารถให้บริการผ่านทางอินเทอร์เน็ต	๓	๔	๑๒
๖. เครื่องลูกข่ายถูกโจมตี	- ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	๓	๓	๙

ผลการประเมิน พบว่าความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพทุกระบบไม่ว่าจะเป็นการนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่) / ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย,ระบบให้บริการ Internet ล่มเครื่อง Server และเครื่อง Client ติดไวรัส กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ ภัยหรือสถานการณ์ฉุกเฉิน สถานการณ์ความไม่สงบเรียบร้อย ในบ้านเมือง มีระดับความเสี่ยงสูง คะแนนระดับความเสี่ยง (๑๐ – ๑๕) ไม่สามารถที่จะยอมรับความเสี่ยงนั้นได้ จำเป็นต้องมีแผนควบคุมความเสี่ยง

๒.๒ มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน

คำอธิบายเกณฑ์

สถานพยาบาลมีแผนจัดการความเสี่ยง เพื่อเป็นเครื่องมือในการสนับสนุน และกำหนดแนวทางดำเนินงานด้านบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สามารถนำไปปฏิบัติและใช้งานได้จริงภายในหน่วยงาน โดยจัดทำแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** แผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบอย่างชัดเจน
๐.๕	มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร **แต่ไม่มี** การกำหนดกลยุทธ์โครงการ **หรือ** ระยะเวลาดำเนินการ **หรือ** ผู้รับผิดชอบ
๑	มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน

เอกสารอ้างอิง แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ , การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศสถานพยาบาล เป็นต้น

เอกสารตัวอย่าง ข้อ 2.2

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบ ๒๕๖๑				ปีงบ ๒๕๖๒				ปีงบ ๒๕๖๓				งบประมาณ	ผู้รับผิดชอบ
			Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔		
๔.ความเสี่ยงจากการการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	- ตรวจสอบการตั้งค่าของ Firewall, PS อย่างสม่ำเสมอ	- ตลอดปี	←											→	NA	กลุ่มสารสนเทศ
	- บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ	- ตลอดปี	←											→		กลุ่มสารสนเทศ
	- ติดตั้งโปรแกรมป้องกันไวรัสและ Patch ของระบบ	- ทุก ๖ ปี				●										
	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ	เดือน มิ.ย. ๒๕๖๑		●												
	- จัดทำแผนจัดซื้อ Firewall ทดแทน															
	- อัปเดท Firmware content ของระบบ Firewall															

๒.๓ มีการดำเนินการตามแผนจัดการความเสี่ยง

คำอธิบายเกณฑ์

สถานพยาบาลมีการติดตามการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อเก็บรวบรวมข้อมูลที่ได้มาเป็นเครื่องมือ ควบคุม กำกับ ติดตามดูว่าการปฏิบัติงานมีความก้าวหน้าไปในทิศทางที่สอดคล้องกับแผนปฏิบัติงานตลอดจนงบประมาณที่กำหนดไว้หรือไม่

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การดำเนินการตามแผนจัดการความเสี่ยงตาม ข้อ ๒.๒
๐.๕	มีการดำเนินการตามแผนจัดการความเสี่ยง ตามข้อ ๒.๒ **แต่ไม่เป็นไปตามระยะเวลาที่กำหนดในแผนจัดการความเสี่ยง**
๑	มีการดำเนินการตามแผนจัดการความเสี่ยง ตามข้อ ๒.๒ **และ** ตามระยะเวลาที่กำหนดในแผนจัดการความเสี่ยง

เอกสารอ้างอิง แผนปฏิบัติงานการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ , รายงานการดำเนินงานตามแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เอกสารตัวอย่าง ข้อ 2.3

ขั้นที่ ๖ รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง

ตารางที่ ๘ การติดตามกิจกรรมการจัดการความเสี่ยง

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

รายงานความเสี่ยง **๑.ระบบงานและข้อมูล (System & information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย**

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรค และแนวทางการแก้ไข
๑. จัดประชุม คณะทำงานในการรักษาความมั่นคงปลอดภัย					
๒.จัดจ้างหน่วยงานภายนอกเฝ้าระวัง					
๓.จัดซื้อจัดจ้างระบบป้องกันความปลอดภัยของข้อมูล					
๔.จัดอบรมให้ความรู้ด้านความปลอดภัย					

๒.๔ มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

คำอธิบายเกณฑ์

สถานพยาบาลมีกระบวนการติดตาม วิเคราะห์ ประเมินผล และจัดทำรายงานผลการดำเนินการตามแผนจัดการความเสี่ยง

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน
๐.๕	มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และ วิเคราะห์ผลการประเมิน แต่ **ไม่มี** การจัดทำเป็นรายงาน
๑	มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และ วิเคราะห์ผลการประเมิน **มี** การจัดทำเป็นรายงาน

เอกสารอ้างอิง แผนปฏิบัติงานการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ , รายงานการดำเนินงานตามแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เอกสารตัวอย่าง ข้อ 2.4

ตารางที่ ๙ การประเมินผลการจัดการความเสี่ยง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๑.	การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่	- ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาข้อมูลของ กรมสนับสนุนบริการสุขภาพ ทำให้ตกเป็นข่าวใน หนังสือพิมพ์ในประเทศ และต่างประเทศ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับ ป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ			
๒.	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่	- ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้าหรือทำงาน ไม่ได้ ระบบงาน/ข้อมูลเสียหรือ สูญหาย	- บำรุงรักษาเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติ และ เครื่องปั่นไฟให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ			

๒.๕ มีการนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

คำอธิบายเกณฑ์

สถานพยาบาลนำผลการประเมินการดำเนินตามแผนจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน และนำผลวิเคราะห์มาปรับปรุงนแผนจัดการความเสี่ยงต่อไป

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** ผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น
๐.๕	มีผลการประเมินการดำเนินการจัดการความเสี่ยง แต่ **ไม่นำมาปรับ** แผนการจัดการความเสี่ยงให้ดีขึ้น
๑	มีผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

เอกสารอ้างอิง แผนปฏิบัติงานการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ , รายงานการดำเนินงานตามแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เอกสารตัวอย่าง ข้อ 2.5

แบบติดตาม-ปค.๕

ชื่อหน่วยงาน สำนักงานสาธารณสุขอำเภอทุ่งหัวช้าง

รายงานการประเมินผลการควบคุมภายใน

สำหรับสำหรับระยะเวลาดำเนินการสิ้นสุด ๓๐ เดือน กันยายน พ.ศ. ๒๕๖๑

กระบวนการปฏิบัติงาน/โครงการ/กิจกรรมด้านของงานที่ประเมินและวัตถุประสงค์ของการควบคุม (๑)	ความเสี่ยงที่ยังมีอยู่ (๒)	งวด/เวลาที่พบจุดอ่อน (๓)	การปรับปรุงการควบคุม (๔)	กำหนดเสร็จ/ผู้รับผิดชอบ (๕)	สถานะดำเนินการ (๖)	วิธีการติดตามและสรุปผลการประเมิน/ข้อคิดเห็น (๗)
งานติดต่อสื่อสาร -เพื่อให้การติดต่อสื่อสารมีประสิทธิภาพสูงขึ้น -เพื่อให้สามารถจัดส่งรายงานต่างๆได้ทันเวลา	ระบบข้อมูลสารสนเทศ ระบบรายงานยังไม่มีความชัดเจนทั้งระบบ และช่องทางการเผยแพร่ข้อมูลไม่เพียงพอ การสื่อสารยังไม่ครอบคลุมถึงหน่วยงานและภาคีที่เกี่ยวข้อง	๓๐ กันยายน ๒๕๖๑	-สนับสนุนให้ รพ.สต. ใช้โทรศัพท์เคลื่อนที่และตัวรับสัญญาณอินเทอร์เน็ตเพิ่มเติม ด้วยระบบโปรแกรมคอมพิวเตอร์ (Software) โดยมีการเชื่อมต่อระหว่างกันด้วยระบบ E - Office และ E – Mail โทรศัพท์ ทั้งระบบสายหลักและระบบมือถือ เช่น Line Facebook Page ให้ทุกหน่วยงาน	๓๐กันยายน ๒๕๖๒ นายณรงค์ฤทธิ์ สายมณี สสอ.ทุ่งหัวช้าง	☆	รพ.สต. ได้ใช้โทรศัพท์เคลื่อนที่และตัวรับสัญญาณอินเทอร์เน็ตเพิ่มเติมมีการพัฒนาระบบโปรแกรมคอมพิวเตอร์ (Software) โดยมีการเชื่อมต่อระหว่างกันด้วยระบบ E - Office และ E – Mail โทรศัพท์ ได้

สถานะดำเนินงาน

☆ดำเนินการแล้วเสร็จตามกำหนด

✓ดำเนินการแล้วเสร็จล่าช้ากว่ากำหนด

✖ ยังไม่ได้ดำเนินการ

Oอยู่ระหว่างดำเนินการ

ลายมือชื่อ.....

(นายธวัชชัย รัตนไพบูลย์วิทย์)

ตำแหน่ง สาธารณสุขอำเภอทุ่งหัวช้าง

วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๑

๓. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ จำนวน ๖ ข้อ

๓.๑ มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

คำอธิบายเกณฑ์

สถานพยาบาลจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** นโยบายด้านความมั่นคงปลอดภัยและระเบียบปฏิบัติสำหรับผู้ใช้
๐.๕	มีนโยบายด้านความมั่นคงปลอดภัย **หรือ** ระเบียบปฏิบัติสำหรับผู้ใช้ระบบ (มีเพียงอย่างใดอย่างหนึ่ง)
๑	มีนโยบายด้านความมั่นคงปลอดภัย **และ** ระเบียบปฏิบัติสำหรับผู้ใช้ระบบ

เอกสารอ้างอิง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ , นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย เป็นต้น

เอกสารตัวอย่าง ข้อ 3.1

ประกาศกระทรวงสาธารณสุข
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงสาธารณสุข เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ กระทรวงสาธารณสุขจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

อาศัยอำนาจตามความในมาตรา ๗ วรรคหนึ่ง แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ปลัดกระทรวงสาธารณสุขโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข มีวัตถุประสงค์ ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของกระทรวงสาธารณสุข ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดกระทรวงสาธารณสุข และผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกระทรวงสาธารณสุข ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของกระทรวงสาธารณสุขในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ ๕. นโยบาย...

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่กระทรวงสาธารณสุขจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๕.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๕.๓ ต้องตรวจสอบ...

๕.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๖. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๗. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕ ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๓ มีนาคม พ.ศ. ๒๕๖๕

(นายเกียรติภูมิ วงศ์รจิต)
ปลัดกระทรวงสาธารณสุข

เอกสารตัวอย่าง ข้อ 3.1

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕

เอกสารตัวอย่าง ข้อ 3.1

สารบัญ

๓.๒ มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

คำอธิบายเกณฑ์

สถานพยาบาลจัดทำแนวนโยบายและแนวปฏิบัติที่กำหนดให้เจ้าหน้าที่ผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยเท่านั้น ที่สามารถเข้าถึงข้อมูลที่เกี่ยวกับภารกิจเฉพาะหน้าที่ของตนเท่านั้น โดยทุกคนจะต้องกำหนดสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมกับหน้าที่ตำแหน่งหน้าที่

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** นโยบาย และ ระเบียบปฏิบัติที่กำหนดห้ามเจ้าหน้าที่ผู้รับผิดชอบและผู้ที่เกี่ยวข้องเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบปัจจุบัน
๐.๕	มีนโยบายและระเบียบปฏิบัติที่กำหนดห้ามเจ้าหน้าที่ผู้รับผิดชอบและผู้ที่เกี่ยวข้องเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบปัจจุบัน แต่ **ไม่มี** การลงนามเป็นลายลักษณ์อักษร
๑	มีนโยบายและระเบียบปฏิบัติที่กำหนดห้ามเจ้าหน้าที่ผู้รับผิดชอบและผู้ที่เกี่ยวข้องเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบปัจจุบัน ที่มีการลงนามเป็นลายลักษณ์อักษร

เอกสารอ้างอิง นโยบายและแนวปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

เอกสารตัวอย่าง ข้อ 3.2

	คู่มือคุณภาพ				ฉบับที่	A(1)	หน้า 3 จาก 5
	เรื่อง	การรักษาความลับและความปลอดภัยของข้อมูลผู้ป่วย			เลขที่	QM-ISI-MR-001-00	
	ผู้จัดทำ	เวชระเบียน	วันที่เริ่มใช้	1 ก.ค. 2559	ผู้อนุมัติ	สมยศ พนธารา	

1.วัตถุประสงค์

1.1เพื่อรักษาความลับและความปลอดภัยของข้อมูลผู้ป่วย

1.2เพื่อป้องกันการละเมิดสิทธิผู้ป่วย

1.3เพื่อป้องกันความเสี่ยงต่อการฟ้องร้อง

1.4เพื่อเป็นมาตรฐานสำหรับผู้ปฏิบัติงาน

2.ขอบข่าย

เป็นการรักษาความลับและความปลอดภัยของข้อมูลผู้ป่วย

3.แนวทางปฏิบัติ

1.การกำหนดผู้มีสิทธิเข้าถึงข้อมูล

มีการกำหนดผู้มีสิทธิการเข้าถึงข้อมูลที่เป็นความลับ ได้แก่ แพทย์ ทันตแพทย์ เภสัชกร พยาบาล นักกายภาพบำบัด นักวิทยาศาสตร์การแพทย์ เจ้าหน้าที่ห้องบัตร เจ้าหน้าที่การเงิน เจ้าหน้าที่ที่ลงข้อมูลผู้ป่วย โดยทุกคนจะมี USERNAME และ PASSWORD เฉพาะตน เจ้าหน้าที่อื่น เช่น คนงาน ลูกจ้าง หมอนวด พนักงานขับรถ เจ้าหน้าที่แผนกซักฟอก เจ้าหน้าที่ผลิตสมุนไพร ที่ไม่ต้องลงข้อมูลผู้ป่วย จะไม่สามารถเข้าถึงข้อมูลได้

2.ข้อมูลที่ผู้เกี่ยวข้องแต่ละระดับสามารถเข้าถึงได้

กำหนดให้เจ้าหน้าที่ที่มีสิทธิเข้าถึงข้อมูล สามารถเข้าถึงข้อมูลได้เฉพาะที่เกี่ยวกับการใช้งานของตนเท่านั้น เช่น เจ้าหน้าที่ห้องบัตรดูข้อมูลหน้าประวัติผู้ป่วยและส่งต่อผู้ป่วยไปแผนกอื่น พยาบาลผู้ป่วยนอกเป็นต้น

3.มาตรการในการรักษาความลับของข้อมูลผู้ป่วยที่เก็บไว้ด้วยคอมพิวเตอร์

กำหนดให้เจ้าหน้าที่ทุกคน ปฏิบัติดังนี้

1.การดูข้อมูลผู้ป่วยในโปรแกรมHOSxP ให้เจ้าหน้าที่ใช้ USERNAME และ PASSWORD เฉพาะตนเท่านั้น

2.ไม่อนุญาตให้เจ้าหน้าที่คนอื่นใช้ USERNAME และ PASSWORD ของตน ในการเข้าดูข้อมูล

3.ข้อมูลเชิงลึกของผู้ป่วยดูได้เฉพาะบางวิชชาชีพเท่านั้น

4.การอนุญาตให้เปิดเผยข้อมูลผู้ป่วย

กำหนดให้แพทย์ผู้รักษา หรือเจ้าหน้าที่ที่แพทย์มอบหมายให้เปิดเผยข้อมูลผู้ป่วย เป็นผู้เปิดเผยข้อมูลของผู้ป่วยได้(ในกรณีข้อมูลการติดเชื้อของผู้ติดเชื้อ/ผู้ป่วยHIV ต้องได้รับความยินยอมจากผู้ติดเชื้อ ด้วย) รวมทั้งแนวทางการขอประวัติการรักษา โดยปฏิบัติตาม WI-MRL-01.006การขอถ่ายสำเนาเวชระเบียน และ WI-MRL-01.014การขอประวัติจากรพศ.

5.หน้าที่ในการรักษาความลับของผู้ที่เข้าถึงข้อมูล

ทางโรงพยาบาลเขาคิชฌกูฏ ให้เจ้าหน้าที่ทุกคน ตะหนักเรื่อง การเก็บรักษาความลับผู้ป่วย ให้รักษาความลับของคนอื่นเสมือนความลับของตนและญาติ ถึงแม้จะทราบโดยบังเอิญ หรือจากแหล่งใดก็ตาม ไม่นำไปพูดต่อ เพราะจะมีผลต่อผู้ป่วยหรือญาติผู้ป่วย

6.วิธีปฏิบัติเมื่อมีการละเมิด

ถ้าพบว่าเจ้าหน้าที่นำความลับของผู้ป่วยไปเปิดเผย จะมีการดำเนินการตามลำดับดังนี้(อ้างอิงตามพราะราชบัญญัติระเบียบข้าราชการพลเรือน พ.ศ. 2551)

6.1 กระทำผิดครั้งที่1 ภาคทัณฑ์ ว่ากล่าวตักเตือน โดยผู้บังคับบัญชาขั้นต้น

6.2 กระทำผิดครั้งที่2 ตัดเงินเดือน 5% เป็นเวลา 2 เดือน นำเข้าเงินบำรุงของโรงพยาบาลและว่ากล่าวตักเตือนเป็นลายลักษณ์อักษร โดยผู้บังคับบัญชาระดับสูงขึ้น เมื่อพ้นระยะ 2 เดือนแล้ว ก็ให้ได้รับเงินเดือนตามปกติ

6.3 กระทำผิดครั้งที่3 ลดเงินเดือนตลอดไป โดยให้ลดลง 2% ของอัตราปกติที่ได้รับอยู่(กรณีที่เงินเดือนส่งมาจากส่วนกลาง ให้ฝ่ายการเงินเป็นผู้หักเงินจากเงินเดือนของผู้กระทำผิดขึ้นมา 2% ทุกเดือน นำเข้าเงินบำรุงของโรงพยาบาล กรณีโรงพยาบาลเป็นผู้จ่ายเงินเดือน ให้จ่ายในอัตราที่หัก2%แล้ว)

6.4 กรณีผู้ป่วยหรือญาติฟ้องร้อง ให้มีการชดใช้ค่าเสียหายทางโรงพยาบาล(เจ้าหน้าที่ที่ได้รับมอบหมายให้เป็นผู้ไกล่เกลี่ย) จะช่วยไกล่เกลี่ยให้จ่ายน้อยที่สุด โดยเจ้าหน้าที่ที่เป็นผู้เปิดเผยข้อมูลผู้ป่วยและเป็นผู้ถูกร้องเรียน จะต้องเป็นผู้จ่าย หรือร่วมกันจ่ายค่าเสียหายนั้น

6.5 เมื่อมีเจ้าหน้าที่ใหม่มาปฏิบัติงานในแผนก/งานใด ให้หัวหน้าแผนก/งาน นั้น แจ้งนโยบายให้เจ้าหน้าที่ใหม่ทราบและยึดถือปฏิบัติด้วย หากเจ้าหน้าที่ใหม่ไม่ทราบและกระทำโดยรู้เท่าไม่ถึงการณ์ ให้ถือเป็นความผิดของหัวหน้าแผนก/งาน นั้น

7.ลักษณะข้อมูลบางอย่างที่ควรมีมาตรการพิเศษ เช่น เวชระเบียนของผู้ป่วยที่ถูกข่มขืนหรือทำแท้ง,ผลการตรวจHIVที่เป็นผลบวก

เวชระเบียนของผู้ป่วยที่ถูกข่มขืนหรือทำแท้งจะจัดเก็บในศูนย์พึงได้ มีเฉพาะพยาบาลศูนย์พึงได้

เท่านั้นที่เข้าถึงเวชระเบียน โดยปฏิบัติตามแนวทางปฏิบัติเพื่อการช่วยเหลือเด็กและสตรีที่เข้ารับบริการ ศูนย์พึ่งได้

8.ข้อมูลผู้ป่วยทั้งหมดในเวชระเบียน ถือเป็นความลับของผู้ป่วย ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540 เจ้าหน้าที่โรงพยาบาลเขาคิชฌกูฏไม่มีสิทธิเปิดเผยข้อมูลของผู้ป่วย ที่รับรู้มาระหว่างปฏิบัติหน้าที่ เว้นแต่จะได้รับมอบหมาย

1. 9. ข้อมูลผู้ป่วยทั้งหมดในเวชระเบียน เป็นความลับของผู้ป่วย เจ้าหน้าที่โรงพยาบาลเขาคิชฌกูฏทุกคนต้องไม่นำข้อมูลผู้ป่วยมาเปิดเผยในที่สาธารณะ

10.ข้อมูลผู้ป่วยทั้งหมดในเวชระเบียน ควรมุ่งในเรื่องของการดูแลรักษาผู้ป่วย หรือเพื่อการศึกษาเท่านั้น

11.การขอเปิดเผยข้อมูลของผู้ป่วย ผู้ขอ ต้องแสดงความจำนงเป็นลายลักษณ์อักษร ที่ผ่านความเห็นชอบโดย ผู้อำนวยการโรงพยาบาลเขาคิชฌกูฏ หรือผู้ที่ได้รับมอบหมาย

12.เวชระเบียนผู้ป่วย เป็นเอกสารราชการตามกฎหมายและเป็นสมบัติของโรงพยาบาลเขาคิชฌกูฏ ผู้ที่ไม่มีหน้าที่รับผิดชอบโดยตรง ไม่มีสิทธินำออกจากโรงพยาบาลเขาคิชฌกูฏ

13.การขอถ่ายสำเนาเวชระเบียนผู้ป่วยบางส่วนหรือทั้งฉบับ ผู้ขอ ต้องแสดงความจำนงเป็นลายลักษณ์อักษร ที่ผ่านความเห็นชอบ โดยผู้อำนวยการโรงพยาบาลเขาคิชฌกูฏ หรือผู้ที่ได้รับมอบหมาย

๓.๓ มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

คำอธิบายเกณฑ์

สถานพยาบาลจัดทำระเบียบหรือนโยบายเกี่ยวกับข้อมูลส่วนบุคคลด้านสุขภาพของผู้ป่วย โดยมีเนื้อหาสอดคล้องกับพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ มาตรา ๗ และจริยธรรมของผู้ประกอบวิชาชีพ เพื่อเน้นย้ำถึงความสำคัญของการป้องกันความลับของผู้ป่วยมิให้รั่วไหลในทุกช่องทาง รวมถึงช่องทาง Social Media ทุกด้านด้วย

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** นโยบายและระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วยมิให้รั่วไหล
๐.๕	มีนโยบายและระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วยมิให้รั่วไหล แต่ **ไม่มี** เป็นลายลักษณ์อักษร
๑	มีนโยบายและระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วยมิให้รั่วไหลและมีเป็นลายลักษณ์อักษร

เอกสารอ้างอิง นโยบายและแนวปฏิบัติในการรักษาความลับและความปลอดภัยของข้อมูลผู้ป่วย

เอกสารตัวอย่าง ข้อ 3.3

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีและสารสนเทศ โรงพยาบาลกำแพงเพชร โทร ๑๒๑๙

ที่ กพ ๐๐๓๒.๒๐๒.๗/๐๐๒ **วันที่** ๑ ธันวาคม ๒๕๖๔

เรื่อง ประกาศใช้นโยบายและแนวทางปฏิบัติในการรักษามาตรฐานความปลอดภัยของผู้ป่วย สำหรับหน่วยงานในโรงพยาบาลกำแพงเพชร

เรียน หัวหน้ากลุ่มภารกิจ/หัวหน้ากลุ่มงาน/หัวหน้างาน และบุคลากรโรงพยาบาลกำแพงเพชรทุกท่าน

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง

ในการนี้โรงพยาบาลกำแพงเพชรจึงได้ดำเนินการจัดทำ "นโยบายและแนวทางปฏิบัติในการรักษามาตรฐานความปลอดภัยของผู้ป่วยโรงพยาบาลกำแพงเพชร" เพื่อให้การใช้งานระบบสารสนเทศของโรงพยาบาลกำแพงเพชรมีความปลอดภัย และสอดคล้องตามหลักกฎหมาย จึงประกาศใช้นโยบายและแนวทางปฏิบัติในการรักษามาตรฐานความปลอดภัยของผู้ป่วย ควบคุมการดำเนินการใดๆ ที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลกำแพงเพชร รายละเอียดตามประกาศที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อทราบ และถือปฏิบัติตามประกาศแนวทางดังกล่าวโดยเคร่งครัดต่อไป

(นายเจษฎา พวงสายใจ)
หัวหน้ากลุ่มภารกิจด้านพัฒนาระบบบริการ
และสนับสนุนบริการสุขภาพ

(นายสุรชัย แก้วหิรัญ)
ผู้อำนวยการโรงพยาบาลกำแพงเพชร

ร่าง.....
พิมพ์.....
ทาน.....
ตรวจ.....

เอกสารตัวอย่าง ข้อ 3.3

ประกาศโรงพยาบาลกำแพงเพชร

เรื่อง แนวทางปฏิบัติมาตรฐานความปลอดภัยของผู้ป่วยโรงพยาบาลกำแพงเพชร

เพื่อให้การดำเนินการใดๆ ต่อระบบสารสนเทศโรงพยาบาลกำแพงเพชร เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีการรักษาความมั่นคงปลอดภัย และตอกย้ำความสำคัญของความลับของผู้ป่วย ให้ผู้ปฏิบัติระมัดระวังในการให้ข้อมูลหรือเปิดเผยข้อมูลต่างๆ ของผู้ป่วยหรือผู้รับบริการด้านสารสนเทศ

โดยมีแนวทางการปฏิบัติ ดังต่อไปนี้

1. การแก้ไขข้อมูลผู้ป่วย ให้ดำเนินการได้ตามระเบียบปฏิบัติว่าด้วยการแก้ไขข้อมูลโดยเคร่งครัด เช่น หากเขียนผิดห้ามใช้ปากการะบายสีทึบทับข้อความจนมองไม่เห็นข้อความเดิม ห้ามใช้น้ำยาลบคำผิดในเวชระเบียนผู้ป่วย การแก้ไขทำได้โดยการลากเส้นทับข้อความเดิมเพียงเส้นเดียว แล้วเขียนข้อความที่แก้ไขไว้ใกล้กับข้อความเดิม พร้อมลงนามกำกับ และวันเวลาที่แก้ไข สำหรับการเขียนข้อความที่แก้ไขในระบบคอมพิวเตอร์ ห้ามลบข้อมูลเดิมทิ้ง แต่ให้ทำเครื่องหมายว่ามีการแก้ไข แล้วเชื่อมโยงข้อมูลที่เพิ่มเติมแก้ไขให้รู้ว่าข้อความใหม่ใช้แทนข้อความเดิมอย่างไร
2. การส่งข้อมูลผู้ป่วยให้กับบุคลากรภายในสถานพยาบาลเดียวกัน ให้ดำเนินการตามระเบียบการส่งข้อมูลอย่างเคร่งครัด เช่น ไม่ใช้ให้ผู้ป่วยถือเวชระเบียนจากจุดบริการหนึ่งไปยังจุดอื่นๆ
3. ตั้งรหัสผ่านในการเข้าใช้งานระบบคอมพิวเตอร์ของตนเองให้คาดเดาได้ยาก ตรงตามระเบียบของสถานพยาบาล ปกปิดรหัสผ่านเป็นความลับส่วนตัวอย่างเคร่งครัด ไม่อนุญาติให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ
4. ห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วย ในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ
5. ห้ามส่งข้อมูลผู้ป่วยที่ระบบตัวตนโดยใช้ช่องทางที่ไม่เหมาะสม เช่น ส่งทาง Line หรือ Social media
6. ห้ามใช้คอมพิวเตอร์ของสถานพยาบาลเปิดไฟล์จากภายนอกทุกกรณี สำหรับการเปิดไฟล์งานจากหน่วยงานภายในให้ตรวจหาไวรัสภายในไฟล์ทุกครั้งก่อนเปิดไฟล์
7. ห้ามนำคอมพิวเตอร์ อุปกรณ์อื่นๆ รวมถึงอุปกรณ์จัดเก็บข้อมูล เช่น CD-ROM, USB Drive, External Hard disk อุปกรณ์เครือข่าย เช่น Hub, Switch, Wi-fi Router ฯลฯ มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของโรงพยาบาลที่ใช้ฐานข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้อำนวยการ

8. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเตอร์เน็ตทุกกรณี ยกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเตอร์เน็ตพร้อมกันกับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วย ซึ่งได้รับอนุญาตจากผู้อำนวยการ

ประกาศนี้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่.....พ.ศ.2564

(นายสุรชัย แก้วหิรัญ)

ผู้อำนวยการโรงพยาบาลกำแพงเพชร

เอกสารตัวอย่าง ข้อ 3.3

โรงพยาบาลมะเร็งลำปาง
กรมการแพทย์

นโยบายการใช้สื่อสังคมออนไลน์ในโรงพยาบาล
(Social Media Policy)
โรงพยาบาลมะเร็งลำปาง กรมการแพทย์ กระทรวงสาธารณสุข

๑. วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแล การเผยแพร่ข้อมูล และการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของโรงพยาบาลมะเร็งลำปาง หรือต่อไปนี้เรียกว่า “องค์กร” รวมถึงบริการอิเล็กทรอนิกส์ ตลอดจนการแสดงความคิดเห็นของบุคลากรในองค์กร ผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม มีความเป็นระเบียบเรียบร้อยและเกิดประโยชน์สูงสุด ดังนั้น เพื่อให้ผู้ปฏิบัติงานในองค์กรทุกท่าน สามารถใช้สื่อสังคมออนไลน์ได้อย่างมีประสิทธิภาพ จึงเห็นสมควรกำหนดนโยบาย และแนวปฏิบัติการใช้สื่อสังคมออนไลน์ โดยมีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้มีการกำหนดขอบเขตของการใช้สื่อสังคมออนไลน์ทั้งในระดับตัวบุคคล และระดับองค์กร

๑.๒ เพื่อสร้างภาพลักษณ์ของบุคลากรและการดำเนินงานขององค์กร

๑.๓ เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาอันอาจจะเกิดขึ้นจากการใช้สื่อสังคมออนไลน์

๑.๔ เพื่อป้องกันการเปิดเผยข้อมูลความลับในทุกระดับทั้งองค์กร

๑.๕ เพื่อให้บุคลากรที่ปฏิบัติงานใช้งานสื่อสังคมออนไลน์อย่างเหมาะสม

๑.๖ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้บุคลากรในองค์กรตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้ประโยชน์จากสื่อสังคมออนไลน์ และปฏิบัติตามอย่างเคร่งครัด

๒. ขอบเขตของนโยบาย

ภายใต้นโยบายนี้ การเข้าถึงสื่อเครือข่ายสังคมออนไลน์ และการเผยแพร่ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง ข้อมูลใดๆ หรือแสดงความคิดเห็นส่วนตัวผ่านสื่อสังคมออนไลน์ มีผลบังคับเหมือนกับการเผยแพร่ข้อมูล หรือแสดงความคิดเห็นผ่านทางช่องทางอื่นๆ โดยการใช้งานสื่อสังคมออนไลน์ทุกประเภทจะต้องปฏิบัติ และสอดคล้องตามแนวนโยบายขององค์กรอย่างเคร่งครัด

นโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์

๑. หลักการและแนวปฏิบัติทั่วไป

๑.๑ องค์กรอนุญาตให้ใช้ระบบเครือข่าย สำหรับเข้าถึงสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบรรณองค์กร

๑.๒ เคารพกฎหมาย จริยธรรมแห่งวิชาชีพกฎระเบียบองค์กรในการใช้สื่อออนไลน์

๑.๓ หน่วยงานภายในองค์กร บุคลากร สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ ประชาสัมพันธ์เกี่ยวข้องกับองค์กรติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ชัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” ข้อความใดเป็น “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่นๆ และความคิดเห็นดังกล่าวควรคำนึงถึงประโยชน์สาธารณะด้วย

๑.๔ พึงระมัดระวังการใช้ถ้อยคำ ภาษาที่อาจเป็นการดูหมิ่น หรือหมิ่นประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์

๑.๕ พึงงดเว้นการโต้ตอบด้วยความรุนแรง กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง การละเว้นไม่โต้ตอบจะทำให้ความขัดแย้ง ไม่บานปลายจนหาที่สิ้นสุดไม่ได้

๑.๖ พึงงดเว้นการใช้สื่อสังคมวิพากษ์ วิจารณ์ ตลอดจนแสดงความเห็นในเรื่องที่เป็นข้อมูลภายในองค์กร หรืออาจส่งผลกระทบต่อองค์กรได้

๑.๗ พึงระมัดระวังข้อความที่ส่งผลกระทบต่อผู้ป่วย หรือละเมิดสิทธิมนุษยชน

๑.๘ รักษาความเป็นวิชาชีพ มีพฤติกรรมออนไลน์เหมาะสม แยกเรื่องส่วนตัวกับวิชาชีพ กำหนดขอบเขตความเป็นวิชาชีพกับผู้ป่วยและผู้อื่นอย่างเหมาะสม

๒. หลักการส่งต่อข้อมูล

๒.๑ ควรส่งข้อมูลข่าวสารเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานะชัดเจนเท่านั้น

๒.๒ ละเว้นการส่งข้อมูลที่เป็นข่าวลือ ข่าวไม่ปรากฏที่มา หรือเป็นเพียงการคาดเดา

๒.๓ งดเว้นการส่งต่อข้อความเกี่ยวข้องกับองค์กรทุกกรณี ยกเว้น ข้อความนั้นๆ เป็นที่เผยแพร่ต่อสาธารณะแล้ว

๒.๔ พึงระลึกเสมอว่า การส่งต่อข้อความที่เป็นเท็จ หรือข้อความที่เจ้าของประสงค์กระจายข่าวสร้างความสบสนวุ่นวายในบ้านเมือง เท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น

๒.๕ การส่งต่อข้อความเชิญชวนไปร่วมชุมนุมหรือกระทำกิจกรรมทางสังคมใดๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

๒.๖ ไม่ควรปรึกษาการดูแลผู้ป่วยทางไลน์ ได้แก่ ถ่ายภาพ x-ray ด้วยกล้องที่มีความละเอียดต่ำซึ่งอาจนำมาสู่การวินิจฉัยที่ผิดพลาด

๒.๗ ใช้ไลน์ในลักษณะบุคคลต่อบุคคล หลีกเลี่ยงการใช้ไลน์กลุ่ม โดยกำหนดให้ผู้ส่งข้อมูลคือผู้ตรวจการเวรพยาบาลเป็นผู้ส่งข้อมูลให้กับแพทย์ผู้อยู่เวร เพื่อป้องกันการรั่วไหลของข้อมูล

๒.๘ หลีกเลี่ยงการขอคำปรึกษาผู้ป่วยพร้อมกันมากกว่า ๑ รายในการปรึกษาหนึ่งครั้ง เพราะอาจมีการสลับของข้อมูลของบุคคลได้

๒.๙ ผู้ที่ให้คำปรึกษาต้องรักษาความลับของผู้ป่วย และทำลายข้อมูลที่ได้รับ เมื่อกระบวนการให้คำปรึกษาเสร็จสิ้น เพื่อป้องกันการรั่วไหลของข้อมูล

๓. หลักความรับผิดชอบ

๓.๑ ควรแสดงความรับผิดชอบ ด้วยการขอโทษแสดงความเสียใจทันที เมื่อรู้ว่ามีการเผยแพร่ข้อมูลที่ผิดพลาดหรือกระทบต่อบุคคลอื่น

๓.๒ หากพบข้อมูลใดๆ ที่ไม่เหมาะสมควรดำเนินการอย่างรวดเร็ว โดยลบข้อความดังกล่าวออกทันทีเพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อองค์กร

๔. การไม่เปิดเผยข้อมูลที่เป็นความลับ

๔.๑ ต้องไม่เปิดเผยหรือส่งต่อข้อมูล ชื่อ-นามสกุล เลขประจำตัวผู้ป่วย ข้อมูลการเจ็บป่วย รูปภาพการตรวจต่างๆ รวมถึงคลิปวีดีโอการดูแลรักษาของผู้ป่วยทางสื่อสังคมออนไลน์ เช่น โปรแกรมไลน์ เฟสบุ๊ค เป็นต้น

๔.๒ ระมัดระวังในการให้คำปรึกษาออนไลน์ บันทึกการสื่อสารออนไลน์ที่เกี่ยวข้อง

๕. ความน่าเชื่อถือของข้อมูล

ไม่โพสต์ข้อความที่เป็นเท็จหรือก่อให้เกิดความเข้าใจผิด และระบุที่มาของข้อมูลนั้นอย่างชัดเจน การโพสต์ข้อความใดๆ ควรพิจารณาเนื้อหาอย่างรอบคอบและระมัดระวัง โดยเฉพาะการเปิดเผยข้อมูลส่วนบุคคล

๖. การคำนึงถึงผลกระทบต่อการปฏิบัติงาน

การใช้สื่อเครือข่ายสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงาน หรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

๗. คำนึงถึงผู้เข้าชมและผู้เกี่ยวข้อง

บุคลากรขององค์กรไม่ควรโพสต์ข้อมูลใดๆ ที่ขัดแย้งกับข้อกำหนดขององค์กร รวมถึงละเว้นการแสดงออกถึงความคิดเห็นที่ก้าวร้าว หมิ่นประมาท ดูถูกเป็นการส่วนตัว ลามกอนาจาร และอื่นๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม เช่น การเมือง ศาสนา ชาติ เป็นต้น

ประกาศนโยบาย ณ วันที่ ๙ มกราคม ๒๕๖๓

ลงชื่อ.....

(นายวีรวัต อุครานันท์)

ผู้อำนวยการโรงพยาบาลมะเร็งลำปาง

๓.๔ มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ

คำอธิบายเกณฑ์

สถานพยาบาลจัดให้มีการสร้างความตระหนักรู้ (awareness education) เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแก่เจ้าหน้าที่และผู้ปฏิบัติงาน โดยเนื้อหาต้องสอดคล้องกับนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย (ข้อ ๓.๑) และ นโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้ (ข้อ ๓.๒) และ นโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media (ข้อ ๓.๓) รวมถึงหน้าที่ความรับผิดชอบของบุคลากรภายในหน่วยงานได้รับทราบอย่างครบถ้วนและสม่ำเสมอ

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** หลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ
๐.๕	มีหลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ แต่**ไม่ครบถ้วน** (ข้อ ๓.๑ - ข้อ ๓.๓)
๑	มีหลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ (ข้อ ๓.๑ - ข้อ ๓.๓) อย่างครบถ้วน

เอกสารอ้างอิง เอกสาร/หลักฐาน การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย, นโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้, นโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน ให้บุคคลการ

เอกสารตัวอย่าง ข้อ 3.4

ประกาศกรมสนับสนุนบริการสุขภาพ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพและการเป็นหน่วยงานหลักในการควบคุมกำกับ มาตรฐานสถานพยาบาล ด้านที่ ๙ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัลระดับกรมอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่องสามารถป้องกันภัยคุกคามไซเบอร์ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมสนับสนุนบริการสุขภาพและหน่วยงานในสังกัด จึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ดังต่อไปนี้

ข้อ ๑ ยกเลิกประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๔

ข้อ ๒ ประกาศนี้ เรียกว่า "ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๕"

ข้อ ๓ ในประกาศนี้

(๑) "กรม สบส." หมายความว่า กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

(๒) "ผู้บริหารระดับสูงสุด" (Chief Executive Officer : CEO) หมายความว่า อธิบดีกรม สบส.

(๓) "ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม" (Department Chief Information Officer: DCO) หมายความว่า รองอธิบดีหรือผู้ซึ่งได้รับมอบหมายให้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ กรม สบส.

(๔) "คณะกรรมการ" หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรม สบส.

(๕) "นโยบาย" หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๕.๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๕.๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๕.๓)พระราชบัญญัติว่า...

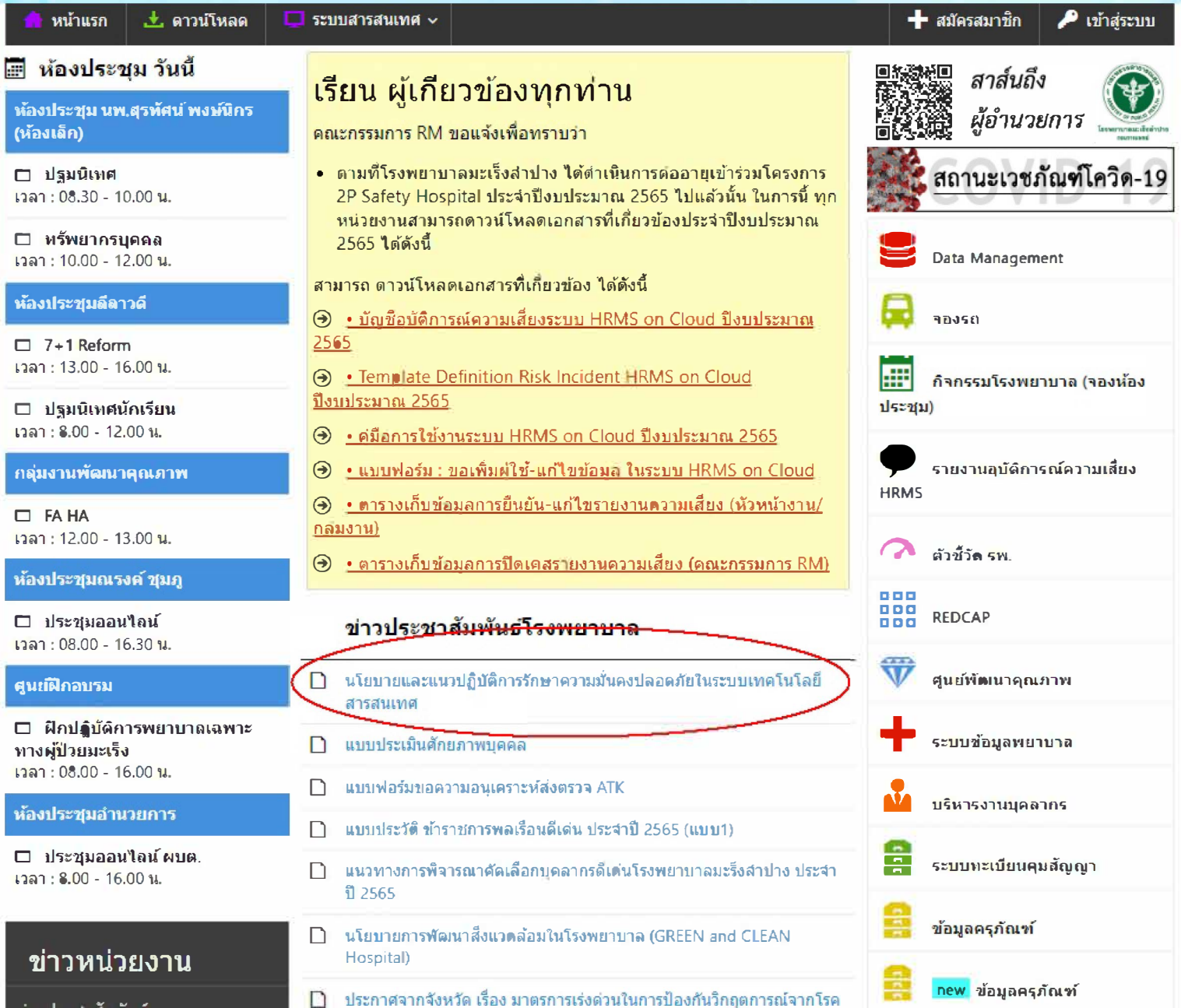
ข้อ ๙ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของกรม สบส. เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ต้องรายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับกรมสั่งการตรวจสอบผู้ละเลยที่ก่อให้เกิดความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกรม สบส. เพื่อรายงานต่อผู้บริหารระดับสูงสุด

ข้อ ๑๐ กรม สบส. กำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบในการบริหารความเสี่ยงควบคุมความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม สบส.

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ สิงหาคม พ.ศ. ๒๕๖๕

ลงนามโดยผู้บริหาร



หน้าแรก | ดาวน์โหลด | ระบบสารสนเทศ | สมัครสมาชิก | เข้าสู่ระบบ

ห้องประชุม วันนี้

ห้องประชุม นพ.สุรพัศน์ พงษ์นิกร (ห้องเล็ก)

ปฐมนิเทศ
เวลา : 08.30 - 10.00 น.

ทรัพยากรบุคคล
เวลา : 10.00 - 12.00 น.

ห้องประชุมลีลาวดี

7+1 Reform
เวลา : 13.00 - 16.00 น.

ปฐมนิเทศนักเรียน
เวลา : 8.00 - 12.00 น.

กลุ่มงานพัฒนาคุณภาพ

FA HA
เวลา : 12.00 - 13.00 น.

ห้องประชุมณรงค์ ชุมภู

ประชุมออนไลน์
เวลา : 08.00 - 16.30 น.

ศูนย์ฝึกอบรม

ฝึกปฏิบัติการพยาบาลเฉพาะทางผู้ป่วยมะเร็ง
เวลา : 08.00 - 16.00 น.

ห้องประชุมอำนวยการ

ประชุมออนไลน์ ผบต.
เวลา : 8.00 - 16.00 น.

ข่าวหน่วยงาน

เรียน ผู้เกี่ยวข้องทุกท่าน

คณะกรรมการ RM ขอแจ้งเพื่อทราบว่า

- ตามที่โรงพยาบาลมะเร็งลำปาง ได้ดำเนินการต่ออายุเข้าร่วมโครงการ 2P Safety Hospital ประจำปีงบประมาณ 2565 ไปแล้วนั้น ในการนี้ ทุกหน่วยงานสามารถดาวน์โหลดเอกสารที่เกี่ยวข้องประจำปีงบประมาณ 2565 ได้ดังนี้

สามารถ ดาวน์โหลดเอกสารที่เกี่ยวข้อง ได้ดังนี้

- บัญชีอบัติการณ์ความเสี่ยงระบบ HRMS on Cloud ปีงบประมาณ 2565
- Template Definition Risk Incident HRMS on Cloud ปีงบประมาณ 2565
- คู่มือการใช้งานระบบ HRMS on Cloud ปีงบประมาณ 2565
- แบบฟอร์ม : ขอเพิ่มผู้ใช้-แก้ไขข้อมูล ในระบบ HRMS on Cloud
- ตารางเก็บข้อมูลการยืนยัน-แก้ไขรายงานความเสี่ยง (หัวหน้างาน/กลุ่มงาน)
- ตารางเก็บข้อมูลการปิดเคสรายงานความเสี่ยง (คณะกรรมการ RM)

ข่าวประชาสัมพันธ์โรงพยาบาล

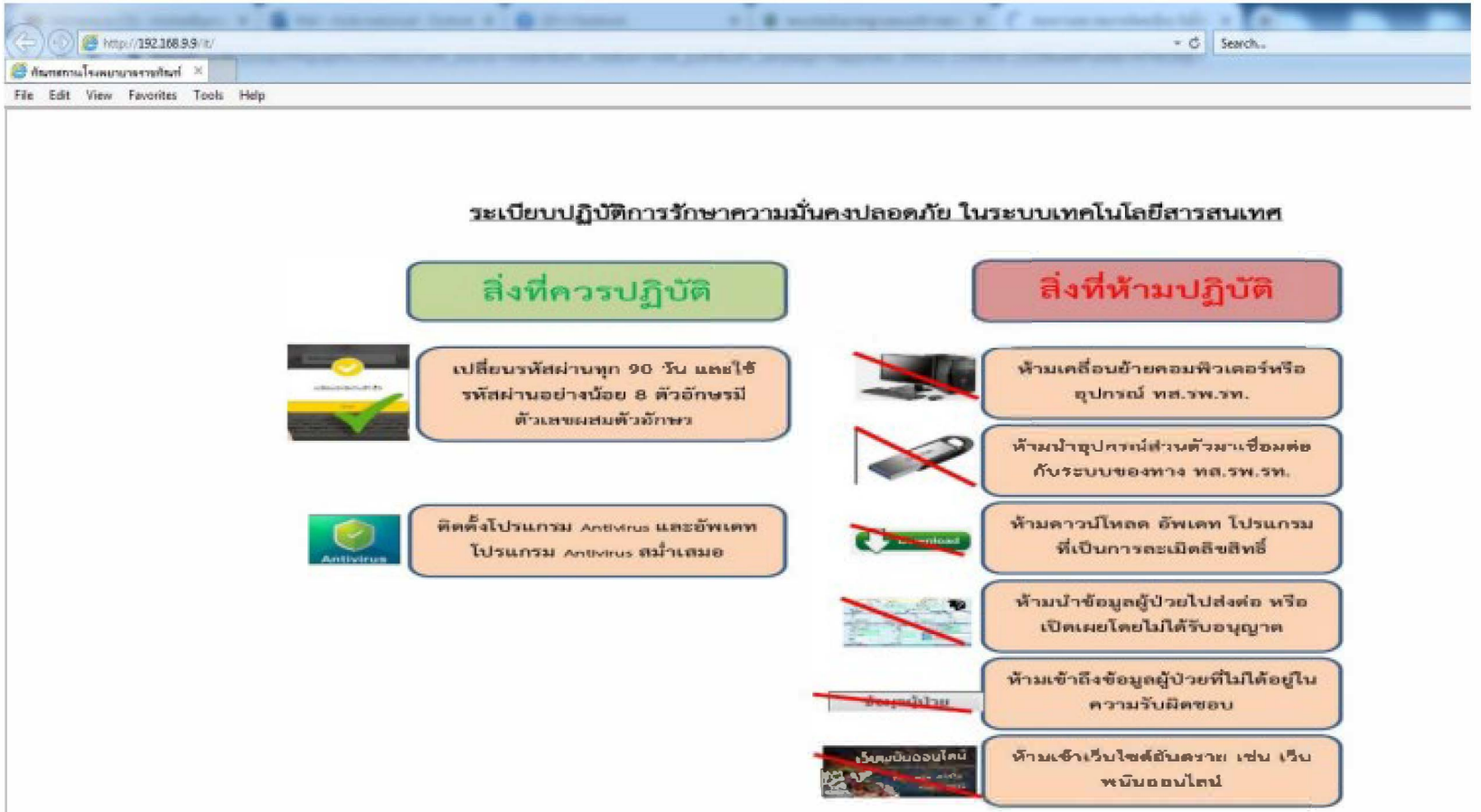
- นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ
- แบบประเมินศักยภาพบุคคล
- แบบฟอร์มขอความอนุเคราะห์ส่งตรวจ ATK
- แบบประวัติ ข้าราชการพลเรือนดีเด่น ประจำปี 2565 (แบบ1)
- แนวทางการพิจารณาคัดเลือกบุคลากรดีเด่นโรงพยาบาลมะเร็งลำปาง ประจำปี 2565
- นโยบายการพัฒนาสิ่งแวดล้อมในโรงพยาบาล (GREEN and CLEAN Hospital)
- ประกาศจากจังหวัด เรื่อง มาตรการเร่งด่วนในการป้องกันวิกฤตการณ์จากโรค

สาส์นถึงผู้อำนวยการ

สถานะเวชภัณฑ์โควิด-19

- Data Management
- จองรถ
- กิจกรรมโรงพยาบาล (จองห้องประชุม)
- รายงานอุบัติการณ์ความเสี่ยง HRMS
- ตัวชี้วัด รพ.
- REDCAP
- ศูนย์พัฒนาคุณภาพ
- ระบบข้อมูลพยาบาล
- บริหารงานบุคลากร
- ระบบทะเบียนคุมสัญญา
- ข้อมูลครุภัณฑ์
- new ข้อมูลครุภัณฑ์

ประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคคลทุกคนรับทราบ



ข้อตกลงการให้บริการ Service Level Agreement (SLA)

งานเทคโนโลยีสารสนเทศ ทันตแพทยาลัยโรงพยาบาลราชทันตฯ สายด่วนประกันสวัสดิการ โทร. ๐๙๗๖๖,๐๙๗๖๗,๐๙๗๖๘

- ตอบปัญหาทางโทรศัพท์ ๓๐ นาที
- ติดตั้งคอมพิวเตอร์ ๔ ชม.
- เปลี่ยนหมึกพิมพ์ ๓๐ นาที
- การปรับปรุงแก้ไขข้อมูลผิดพลาดโปรแกรม และข้อมูลในฐานข้อมูล ๖๐ นาที

๓.๕ มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด

คำอธิบายเกณฑ์

สถานพยาบาลมีกระบวนการสำรวจในเรื่องการรับทราบ เข้าใจ ยอมรับ และปฏิบัติตามนโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของเจ้าหน้าที่ ซึ่งประกอบด้วยนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย และ นโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้ และ นโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้านเพื่อตรวจสอบความรู้ ความเข้าใจ และปฏิบัติงานตามนโยบาย/ระเบียบปฏิบัติของหน่วยงานอย่างเคร่งครัด

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** ผลการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับและปฏิบัติตามระเบียบด้านความมั่นคงปลอดภัย
๐.๕	มีผลการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ **ไม่ครบถ้วน** ตามระเบียบปฏิบัติ และ **ไม่มี** การสรุปผลรายงานด้านความมั่นคงปลอดภัย
๑	มีผลการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับและปฏิบัติตามระเบียบด้านความมั่นคงปลอดภัย **ครบถ้วน** ตามระเบียบปฏิบัติ และมีการสรุปผลรายงาน

เอกสารอ้างอิง รายงานการประเมินการรับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของบุคลากรของหน่วยงาน

สรุปผลการประเมินแบบสอบถาม
เรื่องระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กลุ่มงานสารสนเทศทางการแพทย์ โรงพยาบาลเชียงรายประชานุเคราะห์

ตัวอย่างแบบสอบถามการรับรู้รับทราบระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีข้อคำถังนี้

ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย		รับรู้	ไม่รับรู้	เข้าใจ	ไม่เข้าใจ
สิ่งที่ควรทำ					
1	การเปลี่ยนรหัสผ่านทุก 90 วัน และควรมีความยาวอย่างน้อย 8 ตัวอักษร และมีตัวเลขผสม				
สิ่งที่ไม่ควรทำ					
2	ห้ามโยกย้ายเครื่องคอมพิวเตอร์				
3	ห้ามดาวน์โหลดหรือติดตั้งโปรแกรมอื่นใดเพิ่มเติม				
4	ห้ามให้ผู้อื่นใช้รหัสผ่านของตนเอง				
5	ห้ามติดรหัสผู้ใช้งานและรหัสผ่านในที่เปิดเผยเช่น หน้าจอคอมพิวเตอร์				
6	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบโดยไม่ได้ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง				
7	ห้ามนำข้อมูลผู้ป่วยไปส่งต่อหรือเปิดเผยต่อสาธารณะชนผ่านทางสื่อ Social ต่างๆ เช่น Line, Facebook เป็นต้น โดยไม่ได้ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง				
การรับรู้รับทราบด้านประกันเวลา (SLA)					
1	การให้บริการข้อมูล (1 วัน)				
2	การกู้คืนระบบเครือข่ายคอมพิวเตอร์ (1 ชั่วโมง)				
3	การแก้ไขปัญหา, เปลี่ยนหรือทดแทนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (30 นาที)				

รายงานการประเมินการรับรู้รับทราบระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลเชียงรายประชานุเคราะห์ ปีงบประมาณ 2562

1. จำนวนผู้ตอบแบบสอบถาม 386 คน
2. รูปแบบการประเมินใช้การสุ่มประเมินแต่ละหน่วยงานโดยการลงสำรวจหน้างาน
3. ผลการประเมิน

ผลการสำรวจการรับรู้		ผลการสำรวจการรับทราบ	
หัวข้อ	ผลการสำรวจ	หัวข้อ	ผลการสำรวจ
เปลี่ยนรหัสผ่าน	43.80	เปลี่ยนรหัสผ่าน	65.50
ห้ามโยกย้าย	75.90	ห้ามโยกย้าย	80.10
ห้ามดาวน์โหลด	79.80	ห้ามดาวน์โหลด	82.60
ห้ามให้รหัสผู้อื่น	95.90	ห้ามให้รหัสผู้อื่น	96.10
ห้ามติดรหัสผ่าน	93.50	ห้ามติดรหัสผ่าน	94.60
ห้ามเข้าถึง	95.60	ห้ามเข้าถึง	96.40
ห้ามส่งต่อ	98.70	ห้ามส่งต่อ	98.40

4. สรุปผลการประเมินการรับรู้ หัวข้อที่มีการรับรู้มากที่สุดคือ หัวข้อที่ 7. ห้ามนำข้อมูลผู้ป่วยไปส่งต่อหรือเปิดเผยต่อสาธารณะชนผ่านทางสื่อ Social ต่างๆ เช่น Line, Facebook เป็นต้น โดยไม่ได้ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรงคิดเป็นร้อยละ 98.70 รองลงมาคือหัวข้อที่ 4. ห้ามให้ผู้อื่นใช้รหัสผ่านของตนเองร้อยละ 95.90 และหัวข้อที่ 1. การเปลี่ยนรหัสผ่านทุก 90 วัน และควรมีความยาวอย่างน้อย 8 ตัวอักษร และมีตัวเลขผสม เป็นสิ่งที่บุคลากรมีความรับรู้น้อยที่สุดร้อยละ 43.80
5. สรุปผลการประเมินการรับทราบ หัวข้อที่มีการรับรู้มากที่สุดคือ หัวข้อที่ 7. ห้ามนำข้อมูลผู้ป่วยไปส่งต่อหรือเปิดเผยต่อสาธารณะชนผ่านทางสื่อ Social ต่างๆ เช่น Line, Facebook เป็นต้น โดยไม่ได้ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรงคิดเป็นร้อยละ 98.40 รองลงมาคือหัวข้อที่ 6. ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ได้ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรงร้อยละ 96.40 และหัวข้อที่มีการรับทราบน้อยที่สุดคือหัวข้อที่ 1. การเปลี่ยนรหัสผ่านทุก 90 วัน และควรมีความยาวอย่างน้อย 8 ตัวอักษร และมีตัวเลขผสม ร้อยละ 65.50
6. เสนอแนะแนวทางการแก้ไข

- ควรมีการสำรวจจำนวนของเจ้าหน้าที่ทั้งหมดแทนการสุ่มสำรวจเพื่อให้ได้รับข้อมูลที่เป็นจริงมาก

๓.๖ มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

คำอธิบายเกณฑ์

สถานพยาบาลมีกระบวนการประเมินผลการปฏิบัติตาม นโยบาย/ระเบียบปฏิบัติ ด้านความมั่นคงปลอดภัย เพื่อวัดผลสำเร็จของการบังคับใช้ นโยบาย/ระเบียบปฏิบัติ ภายในหน่วยงาน โดยนำผลการประเมินที่ได้ไปใช้ในการพัฒนาช่องทางการรับรู้ ปรับเปลี่ยนวิธีการสร้างความรู้ความเข้าใจ และปรับปรุงกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป
๐.๕	มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติ **แต่ไม่ได้** นำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป
๑	มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติ **และ** นำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป

เอกสารอ้างอิง รายงานสรุปผลการประเมินผลการปฏิบัติตาม นโยบาย/ระเบียบปฏิบัติ ด้านความมั่นคงปลอดภัย

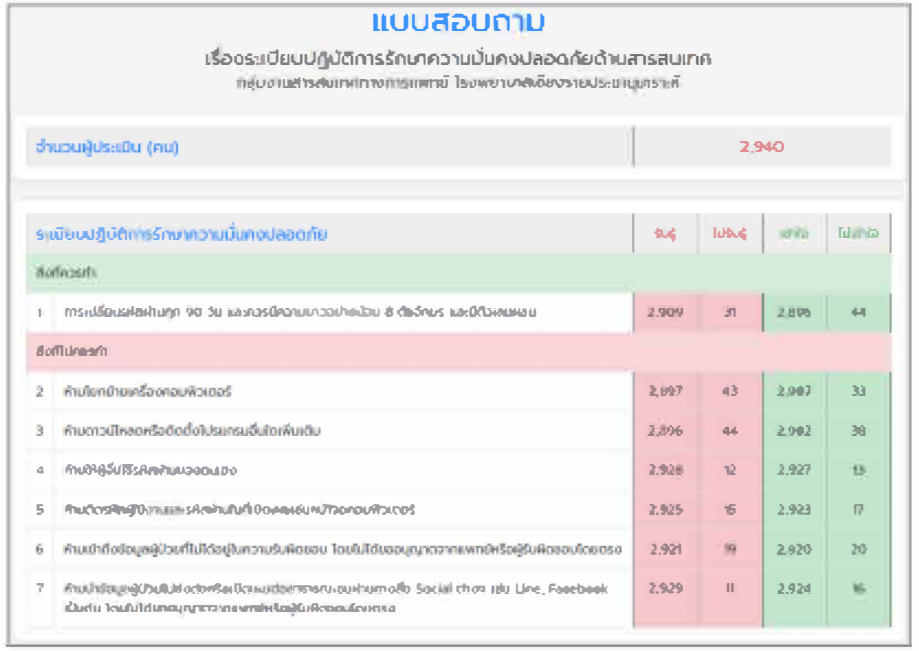
เอกสารตัวอย่าง ข้อ 3.6

รายงานการประเมินการรับรู้รับทราบระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลเชียงรายประชานุเคราะห์ ปีงบประมาณ 2564

1. จำนวนผู้ตอบแบบสอบถาม

ผู้ตอบแบบสอบถาม	2,940 คน
จำนวนเจ้าหน้าที่ทั้งหมด	2,953 คน
คิดเป็นร้อยละ	99.56

2. รูปแบบการประเมินใช้การประเมินผ่านระบบออนไลน์ ก่อนการเข้าประเมินระบบประเมิน Competencies
3. ผลการประเมิน



แบบสอบถาม

เรื่องระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

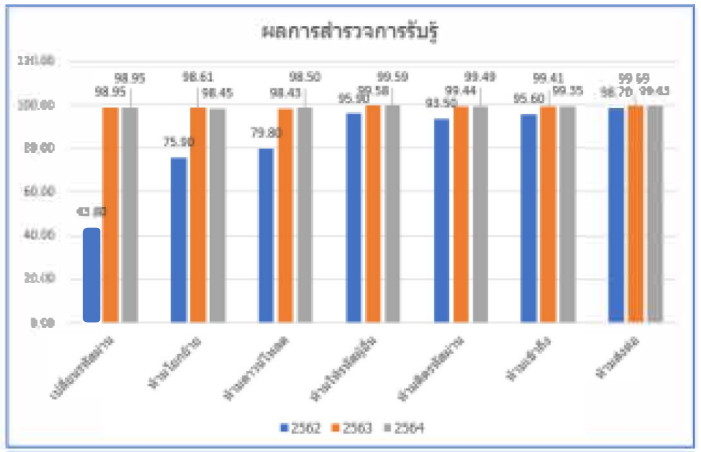
กลุ่มงานสารสนเทศทางการแพทย์ โรงพยาบาลเชียงรายประชานุเคราะห์

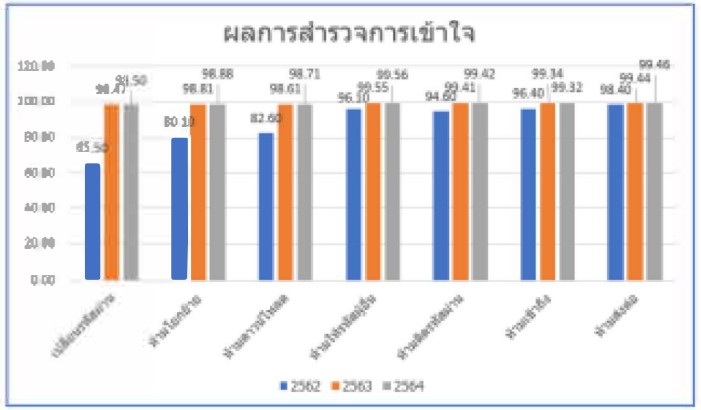
จำนวนผู้ประเมิน (คน)	2,940

ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย	ข้อ	ไม่ข้อ	เห็น	ไม่เห็น
สิ่งที่ควรทำ				
1 การเปลี่ยนรหัสผ่านทุก 90 วัน และควรมีความยาวอย่างน้อย 8 ตัวอักษร และมีตัวเลขผสม	2,909	31	2,896	44
สิ่งที่ไม่ควรทำ				
2 ห้ามโยกย้ายเครื่องคอมพิวเตอร์	2,897	43	2,907	33
3 ห้ามดาวน์โหลดหรือติดตั้งโปรแกรมอื่นเพิ่มเติม	2,896	44	2,902	38
4 ห้ามให้รหัสผ่านแก่ผู้อื่น	2,928	12	2,927	13
5 ห้ามติดรหัสผ่านและคัดลอกรหัสผ่านไว้ข้างคอมพิวเตอร์	2,925	15	2,923	17
6 ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ได้รับอนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง	2,921	19	2,920	20
7 ห้ามนำข้อมูลผู้ป่วยลงในช่องทางต่างๆ บนอินเทอร์เน็ต เช่น Social chat เช่น Line, Facebook เป็นต้น โดยไม่ได้รับอนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง	2,929	11	2,924	16

ผลการสำรวจการรับรู้		ผลการสำรวจการรับทราบ	
หัวข้อ	ผลการสำรวจ	หัวข้อ	ผลการสำรวจ
เปลี่ยนรหัสผ่าน	98.95	เปลี่ยนรหัสผ่าน	98.50
ห้ามโยกย้าย	98.45	ห้ามโยกย้าย	98.88
ห้ามดาวน์โหลด	98.50	ห้ามดาวน์โหลด	98.71
ห้ามให้รหัสผู้อื่น	99.59	ห้ามให้รหัสผู้อื่น	99.56
ห้ามติดรหัสผ่าน	99.49	ห้ามติดรหัสผ่าน	99.42

4. สรุปผลการประเมินการรับรู้ หัวข้อที่มีการรับรู้มากที่สุดคือ หัวข้อที่ 7. ห้ามนำข้อมูลผู้ป่วยไปส่งต่อหรือเปิดเผยต่อสาธารณะชนผ่านทางสื่อ Social ต่างๆ เช่น Line, Facebook เป็นต้น โดยไม่ได้ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรงคิดเป็นร้อยละ 99.63 รองลงมาคือหัวข้อที่ 4. ห้ามให้ผู้อื่นใช้รหัสผ่านของตนเองร้อยละ 99.59 และหัวข้อที่ 2. ห้ามดาวน์โหลดหรือติดตั้งโปรแกรมอื่นใดเพิ่มเติม เป็นสิ่งที่บุคลากรมีความรับรู้น้อยที่สุดร้อยละ 98.45
5. สรุปผลการประเมินการรับทราบ หัวข้อที่มีการรับรู้มากที่สุดคือ หัวข้อที่ 4. ห้ามให้ผู้อื่นใช้รหัสผ่านของตนเอง คิดเป็นร้อยละ 99.56 รองลงมาคือหัวข้อที่ 7. ห้ามนำข้อมูลผู้ป่วยไปส่งต่อหรือเปิดเผยต่อสาธารณะชนผ่านทางสื่อ Social ต่างๆ เช่น Line, Facebook เป็นต้น โดยไม่ได้ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรงคิดเป็นร้อยละ 99.46 และหัวข้อที่มีการรับทราบน้อยที่สุดคือหัวข้อที่ 1. การเปลี่ยนรหัสผ่านทุก 90 วัน และควรมีความยาวอย่างน้อย 8 ตัวอักษร และมีตัวเลขผสม ร้อยละ 98.50

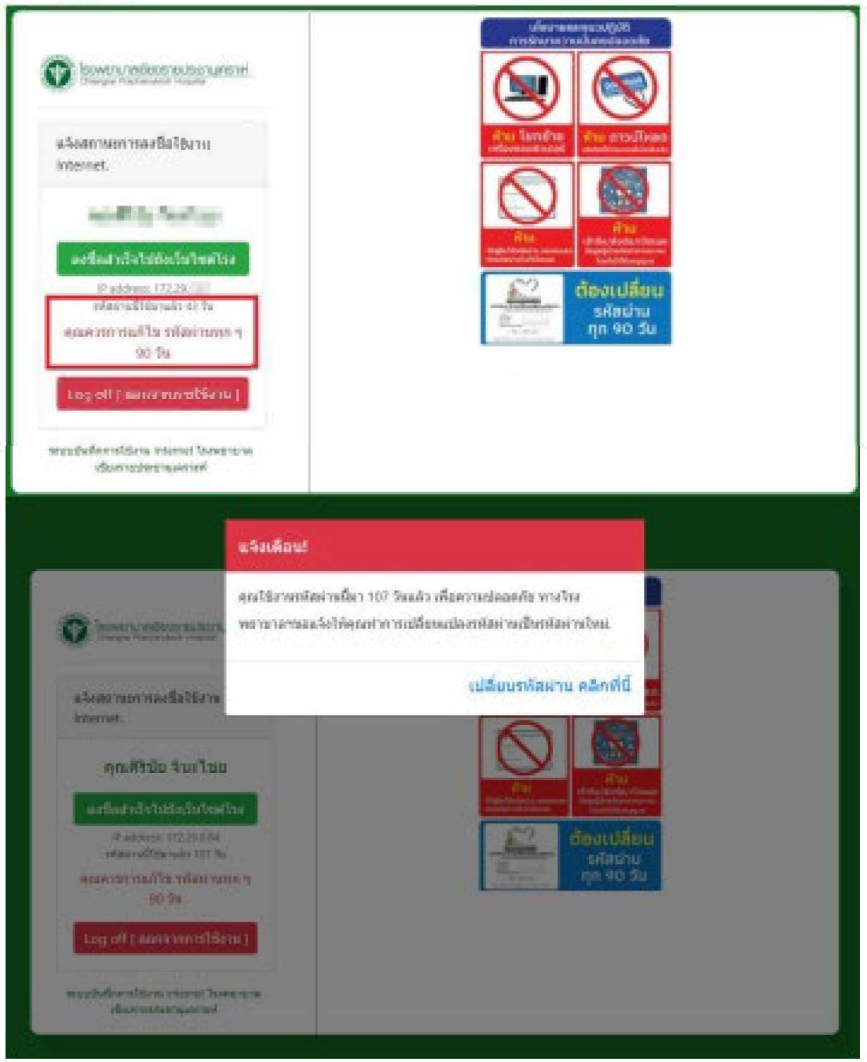


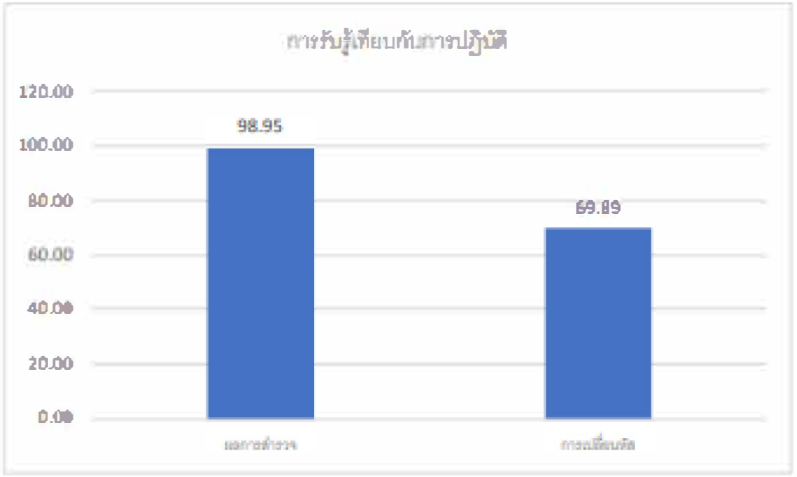


6. สรุปการบริหารจัดการเพื่อเพิ่มผู้ตอบแบบสอบถามปีงบประมาณ 2563

6.1. ดำเนินการทำระบบเก็บ log เพื่อให้ได้ข้อมูลจำนวนวันใช้งาน
ดำเนินการเพิ่มการจัดเก็บวันเริ่ม login และวันที่ login ล่าสุดในฐานข้อมูล

6.2. จัดทำระบบแจ้งเตือนเมื่อจำนวนการใช้งานครบ 90 วันแนะนำให้เจ้าหน้าที่ดำเนินการเปลี่ยนรหัสผ่าน





7. เสนอแนะแนวทางการแก้ไข
   - เพื่อให้เป็นไปตามมาตรฐานควรมีการเพิ่มข้อกำหนดที่เข้มงวดขึ้น เพื่อให้ได้อัตราการเป็นรหัสผ่านเป็นไปในร้อยละที่สูงขึ้นกว่านี้

8. การพัฒนากระบวนการครั้งถัดไป

การบริหารจัดการเพื่อเพิ่มผู้ตอบแบบสอบถามปีงบประมาณ 2564	
ปัญหา	ระดับความรู้ความเข้าใจ การเปลี่ยนรหัสผ่านทุก 90 วัน และควรมีความยาวอย่างน้อย 8 ตัวอักษร ที่ร้อยละ 98.95 แต่เจ้าหน้าที่ได้ดำเนินการดำเนินการจริงร้อยละ 69.89
แผน	1. ปรับโปรแกรมแจ้งเตือนเป็นต้องดำเนินการเปลี่ยนรหัสเมื่อครบ 90 วัน 2. จัดทำรายงานแยกวิชาชีพเพื่อรายงานคณะกรรม CIO
ดำเนินการ	3. มอบหมายเจ้าหน้าที่ดำเนินการแก้ไขระบบ login เมื่อจำนวนวันครับให้ต้องเปลี่ยนรหัสผ่าน 4. มอบหมายเจ้าหน้าที่ดำเนินการจัดทำรายงานแยกวิชาชีพเพื่อรายงานคณะกรรม CIO
การติดตาม	1. อัตราการเปลี่ยนรหัสผ่านทุก 90 วัน ไม่น้อยกว่าร้อยละ 70 2. มีรายงานแยกวิชาชีพเพื่อรายงานคณะกรรม CIO

๔. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ จำนวน ๕ ข้อ

๔.๑ มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร

คำอธิบายเกณฑ์

สถานพยาบาลมีการวิเคราะห์ปัจจัยภายใน เพื่อการตรวจสอบความสามารถและความพร้อมในด้านระบบเทคโนโลยีสารสนเทศ โดยมุ่งเน้นในส่วนที่เป็นจุดแข็ง (Strengths) และจุดอ่อน (Weaknesses) ของหน่วยงาน และการวิเคราะห์ช่องว่าง (Gap Analysis) ซึ่งเป็นการประเมินเบื้องต้นเพื่อหาความแตกต่างระหว่างระบบที่มีอยู่ในปัจจุบันของหน่วยงานกับมาตรฐานที่ต้องการจะเป็นในอนาคต ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร ครบทุกด้าน

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** ผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร
๐.๕	มีผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร **แต่ไม่ครบทุกด้าน**
๑	มีผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร **ครบทุกด้าน**

เอกสารอ้างอิง การวิเคราะห์ปัจจัยภายใน ด้าน Hardware, Software, Network, บุคลากร,
การวิเคราะห์ช่องว่าง (Gap Analysis) ด้าน Hardware, Software, Network, บุคลากร

ทรัพยากรเทคโนโลยีสารสนเทศปีงบประมาณ 2564 โรงพยาบาลมะเร็งลำปาง

ลำดับ	รายการ	สถานการณ์ปัจจุบัน	เป้าหมายที่ต้องการ	การดำเนินการ
1	Datacenter หลัก	Memory 1024 GB (ใช้ไป 46%) Storage 17 TB (Flash + SAS) (ใช้ไป 54%)	Storage 20 TB (All Flash)	เปลี่ยนระบบใหม่ในปี 2566 เนื่องจากของเดิมช่องใส่ HDD เต็มแล้วและจะย้าย Hardware เดิมไปใช้ที่ Datacenter สำรอง
2	Datacenter สำรอง	Memory 128 GB (ใช้ไป 40%) Storage 12 TB (ใช้ไป 70%)	Storage 20 TB	เปลี่ยน Hardware ของ Datacenter หลักในปี 2566 และเอาของเก่ามาใช้ที่ Datacenter สำรอง
3	Network Bandwidth	1 Gb/s (Up-link 10 Gb/s) (ใช้ไม่เกิน 35%)		
4	Internet Lease Line (หลัก)	90 Mb/s (ใช้เฉลี่ย 34%)		
5	Internet สำรอง	1000 Mb/s (ใช้เฉลี่ย 40%)		
6	นักวิชาการคอมพิวเตอร์	4 ตำแหน่ง		
7	นักเทคโนโลยีสารสนเทศ	1 ตำแหน่ง		
8	เจ้าพนักงานเครื่องคอมพิวเตอร์	1 ตำแหน่ง	2 ตำแหน่ง	ได้รับจัดสรรแล้วในปีงบประมาณ 2565
9	เครื่องคอมพิวเตอร์ All In One สำหรับงานประมวลผล	จำนวน 66 ต้องการทดแทนของเก่า 1	จำนวน 91	ขอเพิ่มและขอทดแทนในปีงบประมาณ 2565
10	เครื่องคอมพิวเตอร์โน๊ตบุ๊กสำหรับงานประมวลผล	จำนวน 15 ต้องการทดแทนของเก่า 1	จำนวน 22	ขอเพิ่มและขอทดแทนในปีงบประมาณ 2565
11	เครื่องพิมพ์ Multifunction แบบฉีดหมึกพร้อมติดตั้งถังหมึกพิมพ์	จำนวน 6	จำนวน 14	ขอเพิ่มและขอทดแทนในปีงบประมาณ 2565
12	เครื่องพิมพ์เลเซอร์ หรือแบบ LED ชนิดขาวดำ	จำนวน 115 ต้องการทดแทนของเก่า 1	จำนวน 124	ขอเพิ่มและขอทดแทนในปีงบประมาณ 2565
13	ศูนย์บริการ แบบที่ 1	จำนวน 25	จำนวน 32	ขอเพิ่มใหม่ในปีงบประมาณ 2565
14	เครื่องสำรองไฟฟ้า ขนาด 800 VA	จำนวน 83	จำนวน 118	ขอเพิ่มใหม่ในปีงบประมาณ 2565
	ชุดโปรแกรมจัดการสำนักงานที่มีลิขสิทธิ์ถูกต้อง			

๒. การวิเคราะห์ช่องว่าง (Gap Analysis)

รายการที่วิเคราะห์	สถานการณ์ปัจจุบัน	เป้าหมายที่ต้องการ	การดำเนินการ
๒.๑ ผลการวิเคราะห์ช่องว่าง **ด้านระบบ Hardware**			
เครื่องคอมพิวเตอร์	- เครื่องคอมพิวเตอร์เช่า 160 เครื่อง สถานะหมดสัญญาเช่า ก.พ. 64 มีหน่วยความจำหลัก RAM 4 GB มีหน่วยจัดเก็บข้อมูล ชนิด SATA 500 GB - เครื่องคอมพิวเตอร์เช่า 500 เครื่อง สถานะหมดสัญญาเช่า มี.ค. 65 มีหน่วยความจำหลัก RAM 4 GB มีหน่วยจัดเก็บข้อมูล ชนิด SATA 500 GB - เครื่องคอมพิวเตอร์เช่า 35 เครื่อง สถานะสัญญาเช่า ก.ค 67 มีหน่วยความจำหลัก RAM 4 GB มีหน่วยจัดเก็บข้อมูล ชนิด Solid State Drive 250 GB - เครื่องคอมพิวเตอร์เช่า 130 เครื่อง สถานะสัญญาเช่า มี.ค. 65 มีหน่วยความจำหลัก RAM 8 GB มีหน่วยจัดเก็บข้อมูล ชนิด Solid State Drive 480 GB - เครื่องคอมพิวเตอร์เช่า 420 เครื่อง สถานะสัญญาเช่า มี.ค. 65 ถึง มี.ค. 68 มีหน่วยความจำหลัก RAM 4 GB มีหน่วยจัดเก็บข้อมูล ชนิด Solid State Drive 250 GB	ต้องการเปลี่ยนคอมพิวเตอร์ทั้งโรงพยาบาลเป็นระบบเช่าโดยมีการจำแนกสเปคเป็น 3 กลุ่ม ดังนี้คือ **กลุ่มที่ 1** เครื่องคอมพิวเตอร์ สำหรับงานประมวลผล แบบที่ 2 * (จอแสดงภาพขนาดไม่น้อยกว่า 19 นิ้ว) **คุณลักษณะพื้นฐาน** มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 6 แกนหลัก (6 core) โดยมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 3.0 GHz และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง จำนวน 1 หน่วย มีหน่วยความจำหลัก (RAM) ชนิด DDR4 หรือดีกว่า มีขนาดไม่น้อยกว่า 8 GB หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันขนาดไม่น้อยกว่า 12 MB มีหน่วยประมวลผลเพื่อแสดงภาพ โดยมีคุณลักษณะอย่างใดอย่างหนึ่ง หรือดีกว่า ดังนี้ 1) เป็นแผงวงจรเพื่อแสดงภาพแยกจากแผงวงจรหลักที่มีหน่วยความจำขนาดไม่น้อยกว่า 2 GB หรือ 2) มีหน่วยประมวลผลเพื่อแสดงภาพติดตั้งอยู่ภายในหน่วยประมวลผลกลาง แบบ Graphics Processing Unit ที่สามารถใช้	- ปี 2565 ขอเช่าทดแทนคอมพิวเตอร์ที่หมดสัญญา จำนวน 160 เครื่อง จำนวน 500 เครื่อง กลุ่มครุภัณฑ์ รพ. จำนวน 40 เครื่อง **รวมจำนวน 700 เครื่อง**

๒.๒. ผลการวิเคราะห์ช่องว่างด้านระบบ Software			
ระบบ Anti-Virus	ซอฟต์แวร์ลิขสิทธิ์ ESET N●D๓๒ ต้องต่อสัญญาเป็นรายปี ครอบคลุม ๑๐๐๐ เครื่อง	ต่อสัญญา Anti-Virus เป็นรายปี ครอบคลุมทุกเครื่อง	ขอต่อสัญญาและขยาย ครอบคลุม ๑๐๐ %
โปรแกรมใช้งาน	■ มีการใช้งานโดยพัฒนาตามคำขอพัฒนาโปรแกรมซึ่งพิจารณาโดยคณะทำงานพัฒนาระบบสารสนเทศของโรงพยาบาล ■ ระบบ HIS และระบบ Back Office ต้องต่อสัญญาบำรุงรักษารายปี ■ การพัฒนาโปรแกรมคอมพิวเตอร์ ยังขาด ดังนี้ ๑. ปรับปรุงระบบ DSS ๒. ปรับปรุงระบบงานสารบัญ ๓. ระบบลงทะเบียนประชุมสำหรับภายนอกรพ. ๔. ระบบประเมินสมรรถนะบุคคลากร IDP ๕. Docstation : Request LAB ๖. Docstation : ยาตามแพทย์ ๗. ระบบ IPD Viewer ๘. ปรับปรุงระบบแสดงคิวห้องจ่ายยา ๙. OP● Viewer (เอกสารทางการพยาบาล) ๑๐. ระบบงานสำหรับตู้ Locker จ่ายยา ๑๑. ปรับปรุงระบบประชุมอบรมสัมมนา ๑๒. ปรับปรุงระบบบันทึกข้อมูลงานโรคเอดส์ ๑๓. ปรับปรุงระบบบันทึกข้อมูลงาน TB ๑๔. ปรับปรุงตู้ Kiosk : แสดงคิวห้องตรวจ ๑๕. พัฒนาระบบฐานข้อมูลงานประกันสุขภาพ ๑๖. ปรับปรุงระบบการออกรายงาน ๔๓ แฟ้ม ๑๗. การปรับปรุงระบบอินเตอร์เน็ต	■ พัฒนาตามรายการที่ผ่านการอนุมัติโดยคณะทำงานพัฒนาระบบสารสนเทศของโรงพยาบาล ■ ต่อสัญญาบำรุงรักษา ระบบ HIS และระบบ Back Office ดำเนินการพัฒนา ๑. ปรับปรุงระบบ DSS ๒. ปรับปรุงระบบงานสารบัญ ๓. ระบบลงทะเบียนประชุมสำหรับภายนอกรพ. ๔. ระบบประเมินสมรรถนะบุคคลากร IDP ๕. Docstation : Request LAB ๖. Docstation : ยาตามแพทย์ ๗. ระบบ IPD Viewer ๘. ปรับปรุงระบบแสดงคิวห้องจ่ายยา ๙. OPD Viewer (เอกสารทางการพยาบาล) ๑๐. ระบบงานสำหรับตู้ Locker จ่ายยา ๑๑. ปรับปรุงระบบประชุมอบรมสัมมนา ๑๒. ปรับปรุงระบบบันทึกข้อมูลงานโรคเอดส์ ๑๓. ปรับปรุงระบบบันทึกข้อมูลงาน TB ๑๔. ปรับปรุงตู้ Kiosk : แสดงคิวห้องตรวจ ๑๕. พัฒนาระบบฐานข้อมูลงานประกันสุขภาพ ๑๖. ปรับปรุงระบบการออกรายงาน ๔๓ แฟ้ม ๑๗. การปรับปรุงระบบอินเตอร์เน็ต	■ พัฒนาเพิ่มเติม ■ ต่อสัญญา MA ■ พัฒนาระบบเพิ่มเติม

๒.๓. ผลการวิเคราะห์ช่องว่างด้านระบบ Network			
Firewall	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) **คุณลักษณะพื้นฐาน** -เป็นอุปกรณ์ทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service โดยเฉพาะสามารถติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด ๑๙ นิ้ว ได้ -มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๓ ช่อง -มีความเร็วในการส่งผ่านข้อมูล (Throughput) ไม่น้อยกว่า ๕๐๐ Mbps หรือ รองรับการส่งผ่านข้อมูลได้ไม่น้อยกว่า ๕,๐๐๐ Transactions ต่อวินาที -สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ CLI ได้เป็นอย่างน้อย -สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ได้ -อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge) หรือ Transparent และ Span-mode (Monitor) สำหรับตรวจสอบพฤติกรรมได้เป็นอย่างน้อย -มีความสามารถในการทำงานและปกป้อง Web Application ต่างๆ ได้ โดยรองรับ HTTPS ได้เป็นอย่างน้อย -สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) **คุณลักษณะพื้นฐาน** -เป็นอุปกรณ์ทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service โดยเฉพาะสามารถติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด ๑๙ นิ้ว ได้ -มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๓ ช่อง -มีความเร็วในการส่งผ่านข้อมูล (Throughput) ไม่น้อยกว่า ๕๐๐ Mbps หรือ รองรับการส่งผ่านข้อมูลได้ไม่น้อยกว่า ๕,๐๐๐ Transactions ต่อวินาที -สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ CLI ได้เป็นอย่างน้อย -สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ได้ -อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge) หรือ Transparent และ Span-mode (Monitor) สำหรับตรวจสอบพฤติกรรมได้เป็นอย่างน้อย -มีความสามารถในการทำงานและปกป้อง Web Application ต่างๆ ได้ โดยรองรับ HTTPS ได้เป็นอย่างน้อย -สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน	ขอต่อสัญญา MA

การจัดการทรัพยากรและศักยภาพของระบบเทคโนโลยีสารสนเทศ (ด้าน Hardware, Software, Network, People ware)

การจัดการทรัพยากรและศักยภาพของระบบเทคโนโลยีสารสนเทศ
(ด้าน Hardware, Software, Network, People ware)

งานเทคโนโลยีสารสนเทศ ได้จัดทำการบริหารจัดการการทรัพยากรและวางแผนขีดความสามารถของระบบเทคโนโลยีสารสนเทศ

การกำหนดวัตถุประสงค์ (Objective)

- เพื่อเฝ้าระวังและวัดประสิทธิภาพการทำงานของระบบเทคโนโลยีสารสนเทศ ให้มีทรัพยากรเพียงพอในการรองรับการทำงานและการให้บริการได้อย่างต่อเนื่อง
- ปรับปรุงขีดความสามารถของระบบเทคโนโลยีสารสนเทศ ให้เหมาะสมและเพียงพอต่อการใช้งาน

การกำหนดขอบเขต (Scope)

- กำหนดค่าระดับของประสิทธิภาพให้กับระบบเทคโนโลยีสารสนเทศ และอุปกรณ์ต่างๆที่เกี่ยวข้อง เพื่อใช้เป็นมาตรฐานสำหรับทำการตรวจสอบ
- เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ ต้องจัดทำทะเบียนประวัติ รวมทั้งทำการตรวจสอบอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ทั้งหมดภายในระบบ ว่าสามารถใช้งานได้อย่างปกติหรือไม่
- กำหนดให้มีการบันทึกข้อมูลการใช้งานทรัพยากรของระบบเทคโนโลยีสารสนเทศ ทุกวันเพื่อติดตามการทำงานและกำหนดการ แจ้งเตือนให้ผู้ที่เกี่ยวข้องทราบ หากมีความผิดปกติเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
- การนำข้อมูลสถิติมาใช้ในการประเมิน เพื่อวางแผนปรับปรุงขีดความสามารถของระบบเทคโนโลยีสารสนเทศ
- จัดทำแผน เพื่อขยายขีดความสามารถให้รองรับความต้องการภายในองค์กรเป็นประจำ ทุกปีเพื่อให้มั่นใจว่ามีทรัพยากรเพียงพอสำหรับการให้บริการ

การกำหนดตัวชี้วัดการทำงาน (Key Performance Indicator)

- ลดการ Downtime ของระบบเทคโนโลยีสารสนเทศ ไม่เกิน ๖ ชั่วโมงต่อปี อันเนื่องมาจากทรัพยากรไม่เพียงพอ (CPU ,Hard disk ,Memory)

การกำหนดผู้รับผิดชอบกระบวนการ (Process Ownership)

- หัวหน้างานเทคโนโลยีสารสนเทศ
- เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ

๔.๒ มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากร ด้าน Hardware, Software, Network

คำอธิบายเกณฑ์

สถานพยาบาลมีการจัดทำแผนพัฒนาศักยภาพทรัพยากรในระบบเทคโนโลยีสารสนเทศ (Hardware, Software, Network) ให้สอดคล้องกับการวิเคราะห์ความพร้อมในด้านระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับส่วนขาดและความจำเป็นในการใช้งาน

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network
๐.๕	มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network **แต่ขาดด้านใดด้านหนึ่ง**
๑	มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network **ครบทุกด้าน**

เอกสารอ้างอิง แผนเพิ่มศักยภาพด้านเทคโนโลยีสารสนเทศ, แผนการยื่นของบประมาณด้านเทคโนโลยีสารสนเทศ ประจำปี, แผนจัดซื้อ-จัดจ้าง ด้านเทคโนโลยีสารสนเทศ ประจำปี

๓. การจัดทำแผนเพิ่มศักยภาพด้านเทคโนโลยีสารสนเทศ (Capacity Planning)

ได้จัดทำแผนเพิ่มศักยภาพระบบเทคโนโลยีสารสนเทศ ที่ได้จากการวิเคราะห์หาส่วนต่าง โดยพิจารณาตามความจำเป็นและเหมาะสมตามบริบทของการทำงานในแต่ละหน่วยงาน หลังจากนั้นได้มีการนำผลไปใช้ในการจัดทำแผนยุทธศาสตร์สารสนเทศประจำปี พ.ศ. ๒๕๖๔ ซึ่งมีรายการดังต่อไปนี้

การพัฒนาด้าน Hardware

๑. จ้างเหมาบำรุงรักษาระบบ Front Office
๒. จ้างเหมาบำรุงรักษาระบบ Back Office
๓. จ้างเหมาบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์
๔. จ้างเหมาบำรุงรักษาระบบ Vmware vcenter และ vSphere ๖ Foundation
๕. จ้างเหมาบำรุงรักษาระบบแอนตี้ไวรัส
๖. จ้างเหมาบำรุงรักษาระบบความปลอดภัยห้องแม่ข่าย
๗. จ้างเหมาบำรุงรักษา VMWare vcenter และ vSphere ๖ standard
๘. จ้างเหมาบำรุงรักษา VMware vSphere ๗ Essentials Plus Kit
๙. จ้างเหมาบำรุงรักษาโปรแกรม DellEMC RecoverPoint for VMs
๑๐. จ้างเหมาบำรุงรักษาอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ (Fewall)
๑๓. จ้างเหมาบำรุงรักษาอุปกรณ์จัดเก็บข้อมูล EMC VNXE๓๒๐๐ SN:CKM๐๐๑๗๐๔๕๐๒๒๐๔ (HIS)
๑๒. จ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย Dell R๗๓๐ ๕ เครื่อง Serial No:
๑XTY๔๙๒ ,๓XTW๔๙๒,๕DXM๘F๒,๕DXJ๘F๒,๕DWH๘F๒
๑๓. จ้างเหมาติดตั้งสาย LAN สำหรับชั้นได้ดิน ๒๔ จุด
๑๔. ระบบสัญญาณ Wi-Fi บริเวณพื้นที่รักษา
๑๕. จ้างเหมาติดตั้งสาย Fiber Optic สำหรับห้องประชุมเสม พริ้งพวงแก้ว
๑๖. ค่าเช่าเครื่องคอมพิวเตอร์ ๓๓๐ ชุด
๑๗. ค่าเช่าเครื่องคอมพิวเตอร์ ๔๒๐ ชุด
๑๘. ค่าเช่าเครื่องคอมพิวเตอร์ ๖๖๐ ชุด
๑๙. ค่าเช่าสัญญาณอินเตอร์เน็ต AIS
๒๐. ค่าเช่าสัญญาณอินเตอร์เน็ต CAT
๒๓. ค่าเช่าเครื่องพิมพ์ ๓๗ เครื่อง
๒๒. ค่าเช่าเครื่องพิมพ์ ๖๐ เครื่อง
๒๓. ค่าเช่าเครื่องคอมพิวเตอร์ ๖๐ ชุด
๒๔. ค่าเช่าเครื่องพิมพ์ ๔๐ เครื่อง

การพัฒนาระบบ Software

๑. จัดสร้างการสั่งตรวจ Lab ด้วย Homc-API
๒. จัดสร้างฟอร์ม Lab API ในส่วน UI
๓. พัฒนาระบบ Verify ใบสั่งยาผู้ป่วยนอก
๔. ระบบบันทึกข้อมูลการเบิกจ่ายชุดตรวจ ATK

๔.๓ มีการกำหนดสมรรถนะตามบทบาทหน้าที่ที่จำเป็น (Functional Competency) ของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่ และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

คำอธิบายเกณฑ์

สถานพยาบาลมีการกำหนดสมรรถนะที่จำเป็นสำหรับบุคลากรด้านเทคโนโลยีสารสนเทศทุกคนที่เหมาะสมกับหน้าที่ความรับผิดชอบ โดยมีกระบวนการในการประเมินความรู้ ทักษะ ความสามารถ พฤติกรรมการทำงานของบุคคล รวมทั้งคุณลักษณะที่แสดงออกและเปรียบเทียบกับระดับสมรรถนะที่คาดหวังในตำแหน่งงานนั้นๆ เพื่อวางแผนและจัดทำแผนเพิ่มสมรรถนะได้เป็นรายบุคคล

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคน ผลการประเมินสมรรถนะตามบทบาทหน้าที่ และแผนการเพิ่มสมรรถนะรายบุคคล
๐.๕	มีการกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคน **หรือ** ผลการประเมินสมรรถนะตามบทบาทหน้าที่ **หรือ** แผนการเพิ่มสมรรถนะรายบุคคล
๑	มี การกำหนดสมรรถนะตามบทบาทหน้าที่ของของบุคลากรด้าน IT ทุกคน **และ** ผลการประเมินสมรรถนะตามบทบาทหน้าที่ **และ** มีแผนการเพิ่มสมรรถนะรายบุคคล

เอกสารอ้างอิง ผลการประเมินสมรรถนะของบุคลากร, แผนพัฒนาบุคคลด้านเทคโนโลยีสารสนเทศของหน่วยงานเป็นรายบุคคล

๓.๒ การกำหนดระดับคะแนนสูงสุดในแต่ละสมรรถนะที่ประเมิน

ทั้งในการประเมินผลสมรรถนะของบุคลากรในแต่ละระดับ จำเป็นต้องกำหนดคะแนนมาตรฐาน (คะแนนสูงสุด) สำหรับบุคลากรแต่ละประเภท เนื่องจากบุคลากรแต่ละกลุ่มมีระดับความชำนาญที่แตกต่างกันออกไป ทำให้ได้ระดับคะแนนสูงสุดดังต่อไปนี้

ตารางที่ ๓.๒ ระดับคะแนนสูงสุดของบุคลากรจำแนกตามสมรรถนะที่จะทำการประเมิน

ประเด็นการประเมิน		ประเภทของบุคลากร				
		บุคลากรแรกบรรจุ (ทำงานน้อยกว่า ๑ ปี)	บุคลากรที่มีประสบการณ์ (ทำงานมากกว่า ๑ ปี)	บุคลากรที่มีบทบาทหัวหน้างาน	หัวหน้ากลุ่มงาน/หน่วยงาน	บุคลากรประเมินเชี่ยวชาญ
Core Competency	๑.การมุ่งผลสัมฤทธิ์	๕	๕	๕	๕	๕
	๒.บริการที่ดี	๕	๕	๕	๕	๕
	๓.การสั่งสมความเชี่ยวชาญในสาขาอาชีพ	๕	๕	๕	๕	๕
	๔.จริยธรรม	๕	๕	๕	๕	๕
	๕.ความร่วมแรงร่วมใจ	๕	๕	๕	๕	๕
onal etency on	๑.การจัดการภาวะฉุกเฉิน (CPRและอื่นๆ)	-	๓	๓	-	-
	๒.Infection control (DMHTT)	-	๓	๓	-	-
	๓.การใช้โปรแกรมสำเร็จรูปของโรงพยาบาล	-	๒	๓	-	-
	๔.การสื่อสารโน้มน้าวที่มีประสิทธิภาพ	-	๒	๓	-	-

ผลการประเมินสมรรถนะของบุคลากร

หลังจากประเมินสมรรถนะของบุคลากรโดยตัวของบุคลากรเองและหัวหน้างาน ทำให้ได้ค่าเฉลี่ยคะแนนสมรรถนะในแต่ละข้อ จากนั้นนำมาหาค่าร้อยละของสมรรถนะในแต่ละด้านของบุคลากรแต่ละราย ทำให้ได้ผลการประเมินสมรรถนะบุคลากร จำแนกได้ตามกลุ่มตำแหน่งดังต่อไปนี้

๔.๒.๑ ผลประเมินสมรรถนะบุคลากรตำแหน่งงานด้านการพัฒนาโปรแกรม

ตารางที่ ๔.๑ ร้อยละของคะแนนผลการประเมินสมรรถนะตามตำแหน่งด้านพัฒนาโปรแกรม

หัวข้อ		ประเด็นการประเมิน	ช่องว่าง (GAP) คะแนนประเมินที่ได้							
			๑. ปิยะลิตา วัชระกาจร	๒. เทพนิมิตร มหาวรรณ์	๓. ศิริชัย จินะใชย	๔. รัสสรวี สาลิกา	๕. ยุทธนา ห้าวคำแข่ง	๖.ภิรวัฒน์ ขยันขาย	๗. ดำรงพล ใช้เสา	๘. วิศรุต คำโต
Core Competency		๑.การมุ่งผลสัมฤทธิ์	๒	๓	๐	๐	๓	๓	๓	๓
		๒.บริการที่ดี	๒	๓	๐	๐	๓	๒.๕	๓	๓
		๓.การสั่งสมความเชี่ยวชาญในสาขาอาชีพ	๒	๓	๐	๓	๓	๓	๓	๓
		๔.จริยธรรม	๒	๓	๐	๐	๓	๒.๕	๒	๓
		๕.ความร่วมแรงร่วมใจ	๓	๓	๐	๐	๓	๒.๕	๓	๓
Functional Competency	Common	๑.การจัดการภาวะฉุกเฉิน (CPRและอื่นๆ)	๓.๕	๐.๕	๐.๕	๐.๕	๓	๓	๓.๕	๓.๕
		๒.Infection control (DMHT)	๐	๐	๐	๐	๐.๕	๐	๐	๐
		๓.การใช้โปรแกรมสำเร็จรูปของโรงพยาบาล	๐	๐	๐	๐	๐.๕	๐	๐	๐
		๔.การสื่อสารโน้มน้าวที่มีประสิทธิภาพ	๐	๐	๐	๐	๐.๕	๓	๐	๐
		๕.การพัฒนางานประจำ (risk management/CQI/RoRo/Research)	๐	๐	๐	๐	๐.๕	๐	๐	๐
		๖.มาตรฐานวิชาชีพ	๐	๐	๐	๐	๐.๕	๐	๐	๐
	Specific	ทักษะการปฏิบัติงานตามมาตรฐานวิชาชีพ:การพัฒนาโปรแกรม	๐	๐	๐	๐	๐.๕	๐	๓	๐.๕

๔.๒.๒ ผลประเมินสมรรถนะบุคลากรตำแหน่งงานด้านการซ่อมบำรุงคอมพิวเตอร์

ตารางที่ ๔.๒ ร้อยละของคะแนนผลการประเมินสมรรถนะตามตำแหน่งด้านซ่อมบำรุงคอมพิวเตอร์

หัวข้อ		ประเด็นการประเมิน	ช่องว่าง (GAP) คะแนนประเมินที่ได้			
			๑. ณรงค์ศักดิ์ พรมลี	๒. จิรวุฒิ แสนวรรณ	๓. ชาญกฤษณ์ แก้วคำแดง	๔. อภิชาต สิงห์สุข
Core Competency		๑.การมุ่งผลสัมฤทธิ์	๐	๐	๐	๓
		๒.บริการที่ดี	๐	๐	๐	๓
		๓.การสั่งสมความเชี่ยวชาญในสาขาอาชีพ	๐	๐	๐	๓
		๔.จริยธรรม	๐	๐	๐	๓
		๕.ความร่วมแรงร่วมใจ	๐	๐	๐	๓
Functional Competency	Common	๑.การจัดการภาวะฉุกเฉิน (CPRและอื่นๆ)	๓.๕	๓.๕	๓.๕	๓
		๒.Infection control (DMHT)	๓	๐	๓	๓
		๓.การใช้โปรแกรมสำเร็จรูปของโรงพยาบาล	๐	๐	๐	๐
		๔.การสื่อสารโน้มน้าวที่มีประสิทธิภาพ	๐.๕	๐	๐	๐

๔.๒.๓ ผลประเมินสมรรถนะบุคลากรตำแหน่งงานด้านบริการข้อมูลสถิติ

ตารางที่ ๔.๒ ร้อยละของคะแนนผลการประเมินสมรรถนะตามตำแหน่งด้านบริการข้อมูลสถิติ

หัวข้อ	ประเด็นการประเมิน	ช่องว่าง (GAP) คะแนนประเมินที่ได้		
		๑. นลคราญ ปะมุล	๒. กัญญา สมประสงค์	๓. พรชพรรณ บุตรพรหม
Core Competency	๑.การมุ่งผลสัมฤทธิ์	๐	๒	๓
	๒.บริการที่ดี	๓	๓	๐
	๓.การสั่งสมความเชี่ยวชาญในสาขาอาชีพ	๓	๓	๓
	๔.จริยธรรม	๐	๒	๐

แนวทางการพัฒนาแผนพัฒนารายบุคคลและการจัดทำแผนการพัฒนา
รายบุคคลในปีงบประมาณ ๒๕๖๕

จากผลการประเมินสมรรถนะของบุคลากร คณะทำงาน ผู้บริหารส่วนงานและบุคลากรได้ร่วมกันพูดคุย หารือ แลกเปลี่ยนกับบุคลากรให้ทราบถึงจุดอ่อน จุดแข็งและความต้องการในการพัฒนาของบุคลากรเพื่อกำหนดเครื่องมือในการพัฒนาบุคลากร เพื่อให้ได้แนวทางในการพัฒนาความสามารถที่ตรงกับความต้องการและมีความเหมาะสมกับบุคลากรแต่ละคนให้มากที่สุด โดยมีรายละเอียดดังต่อไปนี้

๕.๑ สมรรถนะที่จำเป็นต้องได้รับการพัฒนา

ผลการประเมินสมรรถนะทำให้ทราบว่าบุคลากรแต่ละรายมีจุดอ่อนอย่างไรบ้าง ในการกำหนดแผนการพัฒนา คณะทำงานได้คัดเลือกสมรรถนะในด้านที่เป็นจุดอ่อนและจำเป็นต้องได้รับการพัฒนามากที่สุดในบุคลากรแต่ละราย (มี GAP สูงและมีความจำเป็นต่อการปฏิบัติงานมากที่สุด) พร้อมกับพูดคุยเพื่อทราบความต้องการในการพัฒนา ทำให้เหลือประเด็นจุดอ่อนที่บุคลากรต้องการพัฒนา โดยปรากฏดังตารางต่อไปนี้

ตารางที่ ๕.๑ สมรรถนะที่จำเป็นต้องได้รับการพัฒนา

กลุ่มตำแหน่งงาน	สมรรถนะที่จำเป็นต้องได้รับการพัฒนา (มี GAP สูง และจำเป็นต้องการปฏิบัติงาน)
ด้านพัฒนาโปรแกรม	
๑. น.ส.ปิยะธิดา วัชระภาสร	เทคนิคใหม่ๆ ในการพัฒนาโปรแกรม การใช้เทคโนโลยีเพื่อนำเสนอข้อมูล
๒. นายเทพนิมิตร มหาวรรณ์	เทคนิคใหม่ๆ ในการพัฒนาโปรแกรม
๓. นายศิริชัย จินะไชย	เทคนิคใหม่ๆ ในการพัฒนาโปรแกรม ความปลอดภัยทางไซเบอร์ (Cyber Security)
๔. นายรังสรรค์ สาริกา	เทคนิคใหม่ๆ ในการพัฒนาโปรแกรม
๕. นายยุทธนา ท้าวคำหล่อ	เทคนิคใหม่ๆ ในการพัฒนาโปรแกรม การใช้เทคโนโลยีเพื่อนำเสนอข้อมูล
๖. นายถิรวัฒน์ ขยันขาย	เทคนิคใหม่ๆ ในการพัฒนาโปรแกรม
๗. นายดำรงพล โจ่ยสา	เทคนิคใหม่ๆ ในการพัฒนาโปรแกรม ความปลอดภัยทางไซเบอร์ (Cyber Security)

ประเมินสมรรถนะบุคลากร IT

งานเทคโนโลยีสารสนเทศ ทัณฑสถานโรงพยาบาลราชทัณฑ์ ได้จัดทำ Competency Dictionary เพื่อเป็นมาตรฐานในการประเมินบุคลากรตามตำแหน่งดังนี้

Competency Dictionary ปีงบประมาณ ๒๕๖๔ -๒๕๖๘

ตำแหน่ง ผู้บริหารงานเทคโนโลยีสารสนเทศระดับสูง (CIO) นายวัฒน์ชัย มิ่งบรรเจิดสุข ผู้อำนวยการทัณฑสถานโรงพยาบาลราชทัณฑ์	
Competency Description	
A๑.	ด้านนโยบายและองค์กร
	ภารกิจ หน้าที่ นโยบาย วิธีการและโครงสร้างขององค์กร
	กำหนด กฎ ระเบียบ วิธีการควบคุม และถ่ายทอดชี้นำองค์กร
	การตัดสินใจขององค์กรและกระบวนการกำหนดนโยบายด้านงบประมาณ
	การบริหารแผนงาน/โครงการด้านเทคโนโลยีสารสนเทศ
	สามารถปรับแผนด้านเทคโนโลยีสารสนเทศ ให้สนับสนุนวิสัยทัศน์ พันธกิจ เข็มมุ่งและแผนกลยุทธ์ของ ทัณฑสถานฯได้
A๒.	ความเป็นผู้นำและการบริหารจัดการ
	เทคนิคในการบริหารจัดความสามารถของบุคคล
	การอนุรักษ์บุคลากรผู้มีความสามารถด้านเทคโนโลยีสารสนเทศ
	ความสัมพันธ์ที่เป็นหุ้นส่วน / เทคนิคในการสร้างทีม
	สามารถควบคุมกำกับ ประเมินผลให้การดำเนินงานด้านเทคโนโลยีสารสนเทศระหว่างหน่วยงานทุกหน่วยในทัณฑสถานฯเป็นไปอย่างเหมาะสมและราบรื่น
A๓.	การบริหารกระบวนการ / การเปลี่ยนแปลง
	วิธีการ รูปแบบและเครื่องมือต่างๆ ในการจำลองสถานการณ์
	รูปแบบและวิธีการต่างๆ ในการปรับปรุงคุณภาพ
	เทคนิค / รูปแบบต่าง ๆในการพัฒนาและเปลี่ยนแปลงองค์กร
	เทคนิคและรูปแบบต่างๆของการบริหารและควบคุมกระบวนการ
	รูปแบบและวิธีการต่างๆในการออกแบบการรื้อปรับ
	สามารถเรียนรู้เทคโนโลยีใหม่และนำเทคโนโลยีใหม่มาประเมิน พิจารณาว่าจะนำมาประยุกต์ใช้ในทัณฑสถานฯได้
A๔.	ยุทธศาสตร์และการวางแผนด้านทรัพยากรสารสนเทศ
	การวิเคราะห์เพื่อกำหนดพื้นฐานทางด้านเทคโนโลยีสารสนเทศ
	การวิเคราะห์ด้านเทคโนโลยีสารสนเทศบนความเกี่ยวข้องในงาน
	ขั้นตอนการวางแผนเพื่อรองรับสถานการณ์เฉพาะหน้า
	วิธีการและเทคนิคต่างๆ ในการเฝ้าตรวจและประเมินผล

ตำแหน่ง หัวหน้างานเทคโนโลยีสารสนเทศ นายโชติ มาลัยนวล พยาบาลวิชาชีพชำนาญการ	
Competency Description	
B๑.	ด้านนโยบายและองค์กร
	การออกแบบระบบ ICT ให้เข้ากับพันธกิจองค์กร
	การบริหารเทคโนโลยีสารสนเทศ
	การบริหารโครงการ (Project management)
	การบริหารความสัมพันธ์ การนำเสนอ การสื่อสาร
	การบริหารข้อมูลและฐานข้อมูล
	การพัฒนาระบบเทคโนโลยีสารสนเทศ
B๒.	ความเป็นผู้นำและการบริหารจัดการ
	การคิดวิเคราะห์และมองภาพองค์รวม (Analytical and Conceptual Thinking)
	การตัดสินใจและแก้ปัญหาอย่างเป็นระบบ (Decision Making and Problem Solving)
	การให้คำปรึกษา (Consultation Skills)
	เทคนิคในการบริหารจัดความสามารถของบุคคล
	การอนุรักษ์บุคลากรผู้มีความสามารถด้านเทคโนโลยีสารสนเทศ
	สามารถควบคุมกำกับประเมินผลให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ
B๓.	การบริหารกระบวนการ / การเปลี่ยนแปลง
	เทคนิค / รูปแบบต่าง ๆ ในการพัฒนาและเปลี่ยนแปลงองค์กร
	เทคนิคและรูปแบบต่างๆ ของการบริหารและควบคุมกระบวนการ
	รูปแบบและวิธีการต่างๆในการออกแบบการรื้อปรับ
	สามารถจัดการป้องกัน ดูแลและแก้ปัญหาต่างๆที่เกิดขึ้นในการดำเนินงานและแก้ไข
B๔.	การวางแผนด้านทรัพยากรสารสนเทศ
	สามารถกำหนดสารสนเทศที่ต้องการ (What) โดยพิจารณาจากลักษณะงานหรือหน้าที่ของหน่วยงาน
	สามารถพิจารณาเวลา (When) ที่ต้องใช้สารสนเทศนั้น เพื่อที่จะกำหนดเวลาในการรวบรวมประมวล และจัดทำรายงานให้สอดคล้องกับเวลาที่ต้องการ
	ทราบว่าจะหาสารสนเทศได้ที่ไหน (Where) จะเป็นแหล่งข้อมูลจากภายในหน่วยงานหรือ ภายนอก
	ทราบว่าผู้ใช้ (For whom) สารสนเทศคือใคร เพื่อจะได้จัดทำรูปแบบในการนำเสนอให้เหมาะสม
	สามารถวิเคราะห์ได้ว่าจะใช้เครื่องมืออะไร (How) ในการเก็บรวบรวม ประมวล รักษาสารสนเทศ
	สามารถเข้าใจความหมายของสารสนเทศที่ได้มาได้
	สามารถดำเนินการหรือปฏิบัติงานได้อย่างเหมาะสม โดยอาศัยการพิจารณาจากสารสนเทศที่มีอยู่หรือที่ได้มา
	สามารถใช้สารสนเทศอย่างถูกต้องตามกฎหมายและอย่างมีจริยธรรม
	สามารถประเมินและพัฒนาศักยภาพของบุคลากรในหน่วยงานให้มีสมรรถนะที่จำเป็นในการดำเนินการตามแผนในแต่ละปี

ตำแหน่ง งานเทคโนโลยีสารสนเทศ ทัณฑสถานโรงพยาบาลราชทัณฑ์	
C๑ : สมรรถนะด้านการออกแบบและวิเคราะห์ระบบ	
ความหมาย	การค้นหาความต้องการของระบบสารสนเทศว่าคืออะไร หรือต้องการอะไรเพิ่มเข้ามาในระบบแล้วนำความต้องการของระบบมาเป็นแบบแผนในการสร้างระบบสารสนเทศให้ใช้งานได้จริง
ระดับ	Competency Description
๑	การค้นหาปัญหาของระบบงานเดิมที่ใช้อยู่ การวางแผนเพื่อศึกษาปัญหา
๒	แสดงสมรรถนะระดับที่ ๑ และการวิเคราะห์ความต้องการ รวบรวมความต้องการของระบบ
๓	แสดงสมรรถนะระดับที่ ๒ และการออกแบบระบบ
๔	แสดงสมรรถนะระดับที่ ๓ การวิเคราะห์ระบบด้วยวิธีเชิงวัตถุ (Object – Oriented Analysis :OOA)
๕	แสดงสมรรถนะระดับที่ ๔ การออกแบบด้วยวิธีเชิงวัตถุ (Object – Oriented Analysis :OOA)
C๒ : สมรรถนะด้านการดูแลระบบเครือข่าย (Network)	
ความหมาย	กลุ่มของคอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่าง ๆ ที่นำมาเชื่อมต่อกัน เพื่อให้ผู้ใช้ในเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนข้อมูลและใช้อุปกรณ์ต่างๆ ร่วมกันในเครือข่ายได้
ระดับ	Competency Description
๑	มีความรู้พื้นฐานเกี่ยวกับอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์
๒	แสดงสมรรถนะระดับที่ ๑ และติดตั้งระบบเครือข่ายเชื่อมต่ออินเตอร์เน็ต เพิ่มความเร็วอินเตอร์เน็ต
๓	แสดงสมรรถนะระดับที่ ๒ Mail Server
๔	แสดงสมรรถนะระดับที่ ๓ การจัดการความปลอดภัย
๕	แสดงสมรรถนะระดับที่ ๔ การทำ virtual Private Network
C๓ : สมรรถนะด้านการดูแลระบบแม่ข่าย Windows Server (ผู้ดูแลระบบ)	
ความหมาย	ระบบปฏิบัติการที่ออกแบบและพัฒนาขึ้นเพื่อรองรับการให้บริการ (Service ต่างๆ) กับผู้ใช้มากมายไม่ว่าจะเป็นบริการผ่านทางอินเทอร์เน็ต (Internet)หรืออินทราเน็ต (Intranet)
ระดับ	Competency Description
๑	ความรู้พื้นฐานเกี่ยวกับระบบปฏิบัติการ Windows Server เริ่มต้นใช้งาน Windows Server
๒	แสดงสมรรถนะระดับที่ ๑ และ การติดตั้ง Active Directory บน Windows Server ๒๐๐๘ บริหารจัดการงานพื้นฐานของ Active Directory
๓	แสดงสมรรถนะระดับที่ ๒ และการรองและกู้คืนข้อมูล
๔	แสดงสมรรถนะระดับที่ ๓ และการใช้นโยบายความปลอดภัยบน Windows Server
๕	แสดงสมรรถนะระดับที่ ๔ และการบริหารเครื่องคอมพิวเตอร์ในรูปแบบ Virtualization
C๔ : สมรรถนะการกำหนดค่า (Config)	
ความหมาย	การกำหนดค่าคุณสมบัติของคอมพิวเตอร์ อุปกรณ์หรือโปรแกรมใดๆ ที่จะนำมาใช้กับคอมพิวเตอร์ เพื่อให้ทำงานมีประสิทธิภาพเหมาะสมกับงานที่ทำ
ระดับ	Competency Description
๑	มีความรู้พื้นฐานในการ Config ค่าต่างๆได้ ตั้งค่า IP Address

C๕ : สมรรถนะด้านการดูแลโปรแกรม (Software)	
ความหมาย	องค์ประกอบของคอมพิวเตอร์ที่เราไม่สามารถสัมผัสจับต้องได้โดยตรง เป็นชุดคำสั่งหรือโปรแกรม(Program) เพื่อให้คอมพิวเตอร์ทำงาน ซอฟแวร์จึงเป็นเสมือนตัวเชื่อมระหว่างผู้ใช้งานกับคอมพิวเตอร์ให้สามารถเข้าใจกัน
ระดับ	Competency Description
๑	มีความรู้พื้นฐานเกี่ยวกับซอฟแวร์ระบบและซอฟแวร์ประยุกต์
๒	แสดงสมรรถนะระดับที่ ๑ และ ซอฟแวร์ระบบปฏิบัติการ
๓	แสดงสมรรถนะระดับที่ ๒ และซอฟแวร์ประยุกต์
๔	แสดงสมรรถนะระดับที่ ๓ และDevice Driver หรือ Driver
๕	แสดงสมรรถนะระดับที่ ๔ และรู้จักการใช้งานซอฟแวร์ประยุกต์ให้มีประสิทธิภาพ
C๖ : สมรรถนะด้านการซ่อมบำรุง (Hardware)	
ความหมาย	แก้ไขปรับปรุงอุปกรณ์ที่เป็นชิ้นส่วนในการนำมาประกอบเป็นเครื่องคอมพิวเตอร์และรวมถึงอุปกรณ์ที่นำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ด้วย
ระดับ	Competency Description
๑	มีความรู้พื้นฐานเกี่ยวกับอุปกรณ์คอมพิวเตอร์
๒	แสดงสมรรถนะระดับที่ ๑ มีความรู้พื้นฐานเกี่ยวกับอาการเสียของคอมพิวเตอร์
๓	แสดงสมรรถนะระดับที่ ๒ แก้ปัญหา Driver มีปัญหา (กรณีลงอัพเดต Driver)
๔	แสดงสมรรถนะระดับที่ ๓ แก้ปัญหาคอมพิวเตอร์เบื้องต้นเกี่ยวกับ Windows ได้
๕	แสดงสมรรถนะระดับที่ ๔ แก้ปัญหาคอมพิวเตอร์เบื้องต้น ฮาร์ดแวร์และอุปกรณ์ต่างๆ
C๗ : สมรรถนะด้านการดูแลระบบเครื่องแม่ข่าย (Server)	
ความหมาย	ระบบปฏิบัติการที่ออกแบบและพัฒนาขึ้นเพื่อรองรับการให้บริการ (Services) ต่างๆ กับผู้ใช้มากมาย ไม่ว่าจะเป็นบริการผ่านอินเตอร์เน็ต (Internet) หรืออินทราเน็ต (Intranet)
ระดับ	Competency Description
๑	มีความรู้พื้นฐานในการติดตั้งแม่ข่าย (Server Build)
๒	แสดงสมรรถนะระดับที่ ๑ บำรุงรักษาแม่ข่าย (Server Maintenance and Support)
๓	แสดงสมรรถนะระดับที่ ๒ การสำรองข้อมูล (Server Backup Management)
๔	แสดงสมรรถนะระดับที่ ๓ การกู้ข้อมูล (Server Recovery Management)
๕	แสดงสมรรถนะระดับที่ ๔ การตรวจสอบ วิเคราะห์(Server Performance Management)
C๘ : สมรรถนะด้านการดูแลระบบเครือข่าย (Network)	
ความหมาย	กลุ่มของคอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่าง ๆ ที่นำมาเชื่อมต่อกัน เพื่อให้ผู้ใช้ในเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนข้อมูลและใช้อุปกรณ์ต่างๆ ร่วมกันในเครือข่ายได้
ระดับ	Competency Description
๑	มีความรู้พื้นฐานเกี่ยวกับอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์
๒	แสดงสมรรถนะระดับที่ ๑ และติดตั้งระบบเครือข่ายเชื่อมต่ออินเตอร์เน็ต เพิ่มความเร็วอินเตอร์เน็ต
๓	แสดงสมรรถนะระดับที่ ๒ Mail Server
๔	แสดงสมรรถนะระดับที่ ๓ การจัดการความปลอดภัย

๔.๔ มีการดำเนินการตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ มีการประเมิน วิเคราะห์ผลการดำเนินตามแผน

คำอธิบายเกณฑ์

สถานพยาบาลมีการตรวจสอบ การควบคุม และการวัดผลการปฏิบัติตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) ในข้อ ๔.๒ เพื่อให้ทราบถึงความก้าวหน้าหรือข้อบกพร่องหรือข้อจำกัดของแผนนั้นๆ พร้อมทั้งหาแนวทางแก้ไขปัญหาเพื่อให้สามารถดำเนินการได้ตามแผนที่กำหนดไว้

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ **ไม่มี** การประเมิน วิเคราะห์ผลการดำเนินตามแผน
๐.๕	มีการดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) **หรือ** การประเมินหรือวิเคราะห์ผลการดำเนินตามแผน
๑	มีการดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) **และ** มีการประเมิน วิเคราะห์ผลการดำเนินตามแผน

เอกสารอ้างอิง รายงานผลดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network)

โครงการ/กิจกรรม	เป้าหมาย	ผลการดำเนินงาน	ตัวชี้วัด/แผน (น้ำหนักร้อยละ)	ผล (น้ำหนักร้อยละ)
12. พัฒนาแบบสำรวจความผูกพันและความพึงพอใจของบุคลากร	มีแบบสำรวจความผูกพันและความพึงพอใจของบุคลากร ที่ได้รับการพัฒนาอย่างเหมาะสม	ดำเนินการจัดทำแบบสำรวจความผูกพันและความพึงพอใจของบุคลากร	5	5
13. ความปลอดภัย/สุขอนามัยและสภาพแวดล้อมในการทำงาน (Safety/Health/Environment : SHE)	มีการดำเนินงานตามแผนงานด้านความปลอดภัยฯ ประจำปีที่กำหนดอย่างครบถ้วน	มีการดำเนินงานตามแผนงานความปลอดภัย/สุขอนามัยและสภาพแวดล้อมในการทำงาน (SHE) ได้อย่างครบถ้วน	5	5
14. การจัดระบบสารสนเทศที่สนับสนุนงานด้านทรัพยากรบุคคล (HR Information System: HRIS)	มีฐานข้อมูลที่สำคัญด้านทรัพยากรบุคคลที่ครบถ้วน	มีฐานข้อมูลที่สำคัญด้านทรัพยากรบุคคลที่ครบถ้วน ประกอบด้วย 1.ข้อมูลส่วนบุคคล 2.ข้อมูลการทำงาน 3.ข้อมูลการพัฒนาของบุคลากร 4.ข้อมูลเรื่องผลตอบแทนและสิทธิประโยชน์ 5.ข้อมูลอัตรากำลัง	5	5
รวม			**100**	**100**

๔.๕ มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

คำอธิบายเกณฑ์

สถานพยาบาลมีนำผลการวิเคราะห์การดำเนินตามแผนในข้ ๔.๔ นำมาปรับปรุงแผนเพิ่มหรือจัดการศักยภาพของทรัพยากร ในข้อ ๔.๒ ให้สามารถนำไปปฏิบัติได้บรรลุตามเป้าหมายและวัตถุประสงค์ที่กำหนดไว้

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น
๐.๕	มีการนำผลการวิเคราะห์มาปรับปรุงแผน แต่ **ไม่มี** การปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น **หรือ** ขาดอย่างใดอย่างหนึ่ง
๑	มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

เอกสารอ้างอิง สรุปผลดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network)

เอกสารตัวอย่าง ข้อ 4.5

ส่วนที่ 5

ปัจจัยสำเร็จ ปัญหา/อุปสรรค และข้อเสนอแนะ

1. ปัจจัยสำเร็จ

ผู้บริหารระดับสูงของ สสว. มีความมุ่งมั่นในการพัฒนาการทำงานของ สสว. ให้เป็นระบบที่มีประสิทธิภาพ มีพลังในการขับเคลื่อนวิสาหกิจขนาดกลางและขนาดย่อมตามบทบาทและภารกิจที่ได้รับมอบหมาย โดยที่ผ่านมา สสว. ได้มีการเริ่มพัฒนาระบบบริหารและพัฒนาทรัพยากรบุคคลในด้านต่าง ๆ โดยจัดทำแนวทางหรือเครื่องมือต่างๆ เพื่อรองรับความเปลี่ยนแปลง และเสริมสร้างพัฒนาบุคลากรของ สสว.ให้มีสมรรถนะสูง ดังต่อไปนี้

ปี 2560-2561

(1) จัดทำสมรรถนะประเภทต่างๆ (Core /Managerial /Functional Competency)

(2) จัดทำแผนพัฒนาสมรรถนะรายบุคคล (IDP)

(3) จัดทำการประเมินระดับสมรรถนะ และผลการประเมินสมรรถนะหลักและบริหาร

(4) จัดทำรายงานตัวชี้วัดระดับองค์กร (Corporate KPIs) และตัวชี้วัดระดับฝ่าย (Department KPIs)

(5) จัดทำแผนการฝึกอบรมระยะยาว (Training Roadmap)

ปี 2562

(1) จัดทำแผนงานการพัฒนากลุ่มบุคลากรที่มีศักยภาพ (Talent Management) และแผนงาน การพัฒนากลุ่มบุคลากรผู้สืบทอดตำแหน่ง (Successor Plan)

(2) จัดทำแผนงานด้านความปลอดภัย สุขอนามัย และสภาพแวดล้อมในการทำงาน (Safety / Health / Environment : SHE)

(3) จัดทำแผนงานการสร้างความผูกพันและความพึงพอใจของบุคลากร (Employee Engagement & Satisfaction)

(4) จัดทำคู่มือแนวทาง/หลักเกณฑ์ในการสรรหาพนักงาน

(5) วิเคราะห์กระบวนการทำงานที่สำคัญ (Workflow Analysis) และการวิเคราะห์การทดแทนอัตรากำลัง (Workforce Management) ของฝ่ายทรัพยากรบุคคล

(6) จัดทำเส้นทางความก้าวหน้าในสายอาชีพ (Career Path)

(7) จัดทำรายงานการประเมินค่างาน (Job Evaluation) ของตำแหน่งงานตามโครงสร้างการบริหาร

(8) จัดทำคู่มือการประเมินผลการปฏิบัติงานบุคลากร (KPI ระดับบุคคล)

(9) ทบทวนและจัดทำคู่มือมาตรฐานกำหนดตำแหน่งและแบบลักษณะงาน (Job Description: JD) สำหรับแต่ละตำแหน่งงาน

(10) จัดทำคู่มือการประเมินระดับสมรรถนะ และผลการประเมินสมรรถนะตามหน้าที่งาน (Functional Competency) ของกลุ่มตัวอย่างพนักงาน (Pilot Group)

(11) จัดทำการประเมินสมรรถนะหลัก (Core Competency) ของพนักงานทุกระดับ

ปี 2563

(1) จัดทำแผนพัฒนาสมรรถนะรายบุคคล หรือ IDP (Individual Development Plan)

(2) ทบทวนสมรรถนะหลัก (Core Competency) สมรรถนะด้านบริหาร (Managerial Competency) และสมรรถนะด้านตามหน้าที่งาน (Functional Competency)

(3) ดำเนินการประเมินสมรรถนะหลัก (Core Competency) สมรรถนะด้านบริหาร (Managerial Competency) และสมรรถนะด้านตามหน้าที่งาน (Functional Competency)

(4) พัฒนาระบบการบริหารผลการปฏิบัติงาน (Performance Management System)

(5) จัดทำแผนยุทธศาสตร์ด้านการบริหารและพัฒนาทรัพยากรบุคคลปี 2561-2565 (ฉบับทบทวนปี 2564-2565) และแผนปฏิบัติการด้านการบริหารและพัฒนาทรัพยากรบุคคลปี 2564

(6) วิเคราะห์จัดทำกรอบอัตรากำลัง (Workforce Management)

(7) พัฒนาแบบสำรวจความผูกพันและความพึงพอใจของบุคลากร (Employee Engagement & Satisfaction)

(8) ทบทวนและพัฒนาระบบสาสนเทศด้านทรัพยากรบุคคล (Human Resource Information System : HRIS)

2. ปัญหา/อุปสรรค

(1) การขออนุมัติดำเนินกิจกรรมต้องใช้ระยะเวลาและมีขั้นตอนหลายขั้นตอน อาจทำให้เกิดการล่าช้า

(2) เกิดการแพร่กระจายของเชื้อโรคโควิด-19 ทำให้บางโครงการ/กิจกรรม เกิดความล่าช้ากว่ากำหนด หรือยกเลิกกิจกรรม

(3) การบริหารงานในบางครั้งไม่เป็นไปตามระบบที่กำหนดไว้ อาจทำให้งานไม่สำเร็จตามที่ได้ตั้งเป้าหมายไว้

3. ข้อเสนอแนะ

(1) ควรจัดวางระบบ PDCA ซึ่งเป็นเครื่องมือสำหรับการวางแผนพัฒนาคุณภาพงาน และจัดทำ Workflow ในการกำหนดกิจกรรมในการดำเนินการตั้งแต่ต้นจนแล้วเสร็จ เพื่อใช้สำหรับการพัฒนาและปรับปรุงระบบการทำงานในองค์กรได้อย่างมีประสิทธิภาพ

(2) ในสถานการณ์การระบอดของเชื้อโควิด-19 ควรวางระบบการทำงาน ประชุม และการอบรมออนไลน์เข้ามาช่วยในแต่ละกิจกรรม

(3) ควรมีการติดตามงานอย่างต่อเนื่องและสม่ำเสมอ และงานที่ไม่บรรลุเป้าหมายต้องหาวิธีการปรับปรุงแก้ไข และงานที่บรรลุเป้าหมายพัฒนาให้งานดีขึ้น

๕. การจัดการห้อง Data Center จำนวน ๕ ข้อ

๕.๑ มีการจัดการ Data Center ของสถานพยาบาลให้มีความมั่นคงปลอดภัย

คำอธิบายเกณฑ์

สถานพยาบาลมีการจัดดทำนโยบายหรือแผนการบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย ระบบรักษาความปลอดภัย และระบบอื่นๆ ที่เกี่ยวข้องของหน่วยงาน ภานในห้อง Data Center เพื่อดูแลบำรุงรักษา ซ่อมแซม ให้ทำงานได้อย่างมีประสิทธิภาพ สามารถทำงานร่วมกับระบบสารสนเทศที่มีอยู่ได้อย่างต่อเนื่องและมีความมั่นคงปลอดภัย

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** แนวทางการจัดการห้อง Data Center ของสถานพยาบาลให้มีความมั่นคงปลอดภัย
๐.๕	**ไม่มี** การจัดทำแผนในการจัดการห้อง Data Center **แต่มี** การแนวทางในการบำรุงรักษาหรือแนวปฏิบัติ **หรือ** ระเบียบปฏิบัติในการจัดการห้อง Data center **หรือ** หลักฐานประกอบในการจัดการห้อง Data Center ของสถานพยาบาลแต่ไม่มีเป็นลายลักษณ์อักษร
๑	มีการจัดทำแผนในการจัดการห้อง Data Center **และ** มีการจัดการห้อง Data Center ของสถานพยาบาลให้มีความมั่นคงปลอดภัย **และ** มีการลงนามเป็นลายลักษณ์อักษร

เอกสารอ้างอิง เอกสาร/หลักฐาน หรือ ภาพถ่าย หรือ นโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ,การจัดการระบบความมั่นคงปลอดภัยของ Data Center

หมวดที่ ๙
การรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวทางปฏิบัติ

๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ต้องมีลักษณะ ดังนี้

๒.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

๒.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๒.๔ จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

๒.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

๒.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

๒.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area)พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN CoverageArea) เป็นต้น

๔. การควบคุมการเข้าออก อาคารสถานที่

๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๔.๒ การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๔.๓ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔.๔ ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๔.๕ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๔.๖ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๔.๗ ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๔.๘ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๔.๙ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๐ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๔.๑๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๔.๑๒ มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๔.๑๓ จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๔ จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

๕.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS)

๕.๑.๒ เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

๕.๑.๓ ระบบระบายอากาศ

๕.๑.๔ ระบบปรับอากาศ และควบคุมความชื้น

๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๖.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๖.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๖.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๖.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๖.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๖.๗ พิจารณาใช้งานสายไฟเบอร์ออปติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

๖.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๗.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๗.๖ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๘.๑ ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๘.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๘.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๘.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

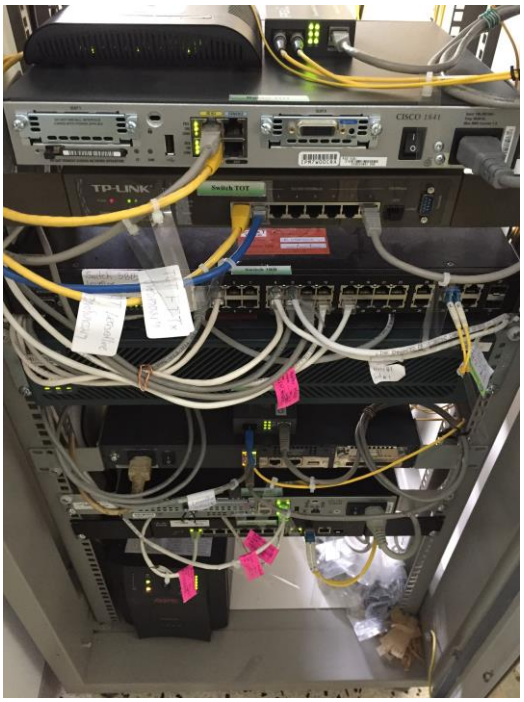
๙.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง ดังนี้

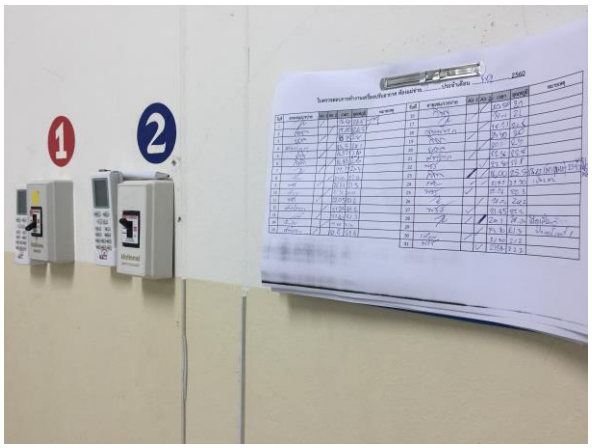
๑๐.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

เอกสารตัวอย่าง ข้อ 5.1



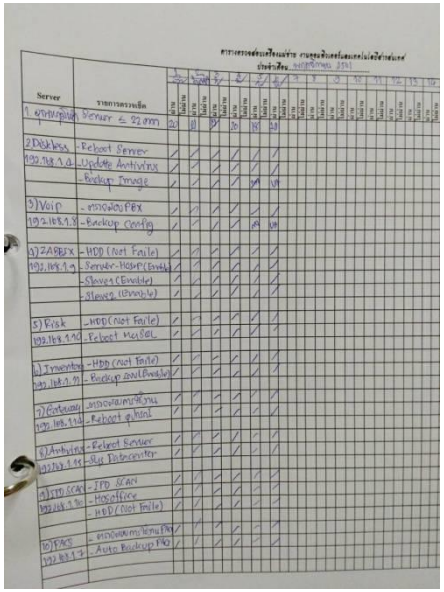
2. **ด้านอุณหภูมิ** ติดตั้งเครื่องปรับอากาศ ควบคุมอุณหภูมิที่ 23องศาจำนวน2 เครื่อง มีการเข้ามาตรวจเช็คและสลับแอร์ทำงาน ทุกวันในช่วงเวรบ่าย และตรวจสอบความปลอดภัยทางภาพภาพพร้อมกัน



เอกสารตัวอย่าง ข้อ 5.1

- ระบบการบำรุงรักษาเครื่อง Server

ตรวจสอบ Serverประจำวัน



ตรวจสอบพื้นที่การใช้งานของ Server

ตรวจสอบอุณหภูมิห้อง Server ให้คงที่(22 C)

ปรับเปลี่ยนแบตเตอรี่เครื่องสำรองไฟตามรอบ

๕.๒ ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

คำอธิบายเกณฑ์

สถานพยาบาลต้องมีการรักษาความมั่นคงปลอดภัยให้กับห้อง Data Center โดยจัดให้มีระบบควบคุมการเข้าออกอย่างรัดกุม เช่น ระบบ face/finger scan หรือ ระบบกล้องวงจรปิด และกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง และทบทวนสิทธิอย่างสม่ำเสมอ โดยคำนึงถึงความมั่นคงปลอดภัยจากภัยคุกคามจากมนุษย์ เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้ามและพื้นที่ที่ตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ อาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การแสดงหลักฐานห้อง สถานที่ และสิ่งแวดล้อม ต้องจัดให้มีความปลอดภัย จากบุคคลภายนอก โดยอย่างน้อยมีแผนผังห้อง รูปถ่ายหรือรูปภาพประกอบ (ไม่มีหลักฐาน หรือ ไม่สอดคล้อง)
๐.๕	**มี** การแสดงหลักฐานห้อง สถานที่ และสิ่งแวดล้อม **แต่ไม่มี** ความปลอดภัยจากบุคคลภายนอก
๑	มีการแสดงหลักฐานห้อง สถานที่ และสิ่งแวดล้อม ต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

เอกสารอ้างอิง เอกสาร/หลักฐาน หรือ ภาพถ่าย ภายในและภายนอก ห้อง สถานที่ และสิ่งแวดล้อม ที่แสดงถึงความมั่นคงปลอดภัยจากบุคคลภายนอก

เอกสารตัวอย่าง ข้อ 5.2

ข้อกำหนดการเข้าใช้งานห้องควบคุมระบบเครือข่าย

ห้องควบคุมระบบเครือข่าย งานเทคโนโลยีสารสนเทศ คณะเวชศาสตร์เขตร้อน เป็นสถานที่จัดเก็บและติดตั้งระบบเทคโนโลยีสารสนเทศ อุปกรณ์เครือข่ายสื่อสารคอมพิวเตอร์หลักของคณะฯ และเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งระบบสารสนเทศต่างๆ ของคณะฯ ดังนั้น เพื่อให้การเข้าออกห้องควบคุมระบบเครือข่ายเป็นไปด้วยความสะดวก เรียบร้อย มีความปลอดภัย จึงได้ทำการติดตั้งระบบผ่านเข้าออกห้องควบคุมระบบเครือข่าย และกำหนดแนวทางการปฏิบัติในการเข้าใช้งาน ดังนี้

1. บุคคลผู้มีสิทธิเข้าใช้งานห้องควบคุมระบบเครือข่าย
   - บุคลากรของงานเทคโนโลยีสารสนเทศที่มีหน้าที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่าย และอุปกรณ์อื่นที่ติดตั้งภายในห้องควบคุมระบบเครือข่าย
   - บุคลากรของหน่วยงานภายในคณะเวชศาสตร์เขตร้อน ที่มีหน้าที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานนั้นๆ หรืออุปกรณ์อื่นที่ติดตั้งภายในห้องควบคุมระบบเครือข่าย
   - บุคลากรของกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ที่มีหน้าที่รับผิดชอบดูแลอุปกรณ์เครือข่าย และอุปกรณ์อื่นที่ติดตั้งภายในห้องควบคุมระบบเครือข่าย
   - บุคลากรของบริษัท/หน่วยงานภายนอกที่มีความจำเป็นในการเข้าถึงห้องควบคุมระบบเครือข่าย เพื่อการบริหารจัดการระบบเครือข่ายสื่อสารคอมพิวเตอร์ ระบบสารสนเทศ หรือการจัดการทางกายภาพที่เกี่ยวข้อง
2. การเข้าใช้งานห้องควบคุมระบบเครือข่าย
   - บุคลากรของงานเทคโนโลยีสารสนเทศที่มีหน้าที่รับผิดชอบดูแล สามารถใช้ Key Card เพื่อใช้ดูแลและบำรุงรักษาระบบ
   - บุคคลภายนอกที่จะขอเข้าใช้ห้องควบคุมระบบเครือข่าย เช่น ติดตั้งและซ่อมบำรุงรักษาอุปกรณ์ต่างๆ ภายในห้อง จะต้องแจ้งให้ผู้ดูแลห้องควบคุมระบบเครือข่ายก่อน
3. ระยะเวลาการใช้งานห้องควบคุมระบบเครือข่าย
   - วันและเวลาราชการที่มีการทำงานตามปกติ 8.30 น. – 16.30 น. ยกเว้นวันหยุดราชการ
   - กรณีที่มีเหตุฉุกเฉิน ที่มีความจำเป็นจะเข้าห้องควบคุมระบบเครือข่าย ให้แจ้งผู้ดูแลห้องควบคุมระบบเครือข่าย ทราบถึงเหตุผลและความจำเป็นในการเข้าไปใช้งาน
4. ห้ามนำอาหาร น้ำดื่ม เข้ามาในห้องควบคุมระบบเครือข่าย
5. ห้ามถ่ายรูปภายในห้อง/อุปกรณ์ ก่อนได้รับอนุญาตจากผู้ดูแล
6. กรณีที่มีการปรับปรุง/แก้ไข server ต้องแจ้งให้ผู้เกี่ยวข้องในแต่ละระบบทราบล่วงหน้าด้วย
7. ผู้ที่เข้าไปปฏิบัติหน้าที่ภายในห้องควบคุมระบบเครือข่าย จะต้องบันทึกลงชื่อและเวลาการเข้าออกห้องควบคุมระบบเครือข่ายทุกครั้ง และกรณีที่นำบุคคลอื่นเข้าไปด้วยจะต้องบันทึกรายละเอียดผู้ที่เข้าไปด้วย

การควบคุม เข้า-ออก

- มีระบบการสแกนลายนิ้วมือ เข้า- ออก
- ห้อง Server เข้าได้เฉพาะผู้ดูแลระบบเท่านั้น
- ห้ามบุคคลอื่นที่ไม่ได้รับอนุญาตเข้าโดยเด็ดขาด

เอกสารตัวอย่าง ข้อ 5.2

ระบบสแกน
ลายนิ้วมือ

CCTV
บริเวณหน้าห้อง

สมุดลงชื่อ

๕.๓ มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ

คำอธิบายเกณฑ์

สถานพยาบาลต้องมีการรักษาความมั่นคงปลอดภัยให้กับห้อง Data Center โดยติดตั้งระบบตรวจจับควัน ระบบเตือนภัย และระบบดับเพลิง ภายในห้อง Data Center ให้ครบถ้วน พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ เพื่อลดความเสี่ยงของการหยุดทำงานของเครื่อง Server จากเหตุไม่พึงประสงค์ โดยมีอุปกรณ์รักษาความปลอดภัยที่มีมาตรฐาน

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การแสดงหลักฐานด้านระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย และระบบดับเพลิง
๐.๕	**มี** การแสดงหลักฐานด้านระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน **หรือ** ระบบเตือนภัย **หรือ** ระบบดับเพลิง เพียงอย่างใดอย่างหนึ่ง **(ขาดอย่างใดอย่างหนึ่ง)**
๑	มีการแสดงหลักฐานด้านระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย และระบบดับเพลิง **อย่างครบถ้วน**

เอกสารอ้างอิง เอกสาร/หลักฐาน หรือ ภาพถ่าย ภายในห้อง Data Center ที่แสดงถึงการมีอยู่ของระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิง

เอกสารตัวอย่าง ข้อ 5.3

มีระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิง และระบบดับเพลิงอัตโนมัติ

5.3 มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิง และระบบดับเพลิงอัตโนมัติ

มีตัวตรวจจับควันไฟ และมีระบบดับเพลิงอัตโนมัติ

ระบบตรวจจับควัน

ถังสารเคมีดับเพลิง

ระบบดับเพลิงอัตโนมัติ

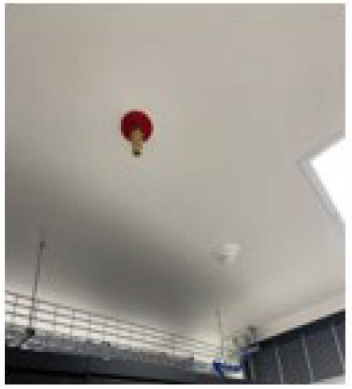
ระบบห้องคอมพิวเตอร์เครือข่ายใหม่

PLC ควบคุมแอร์

แจ้งเตือนเสียง

แอร์

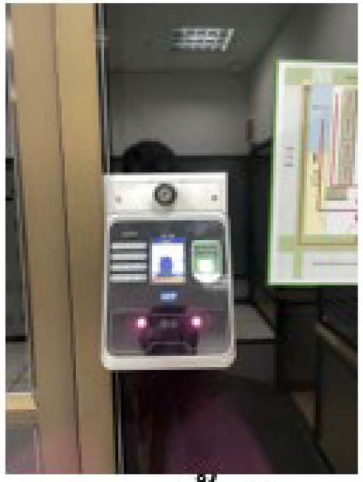
สำรองไฟฟ้า



ระบบดับเพลิงชนิด Novac

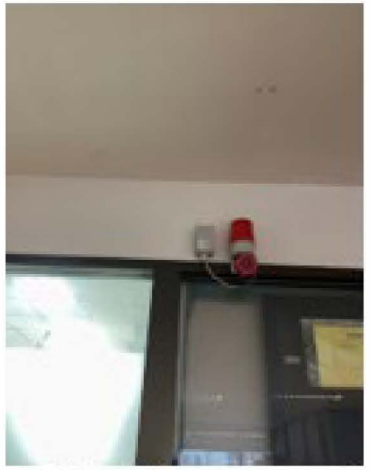
ระบบห้องDATA CENTER (DC)

สำรองไฟ



Scan นิ้วมือ

PLC ควบคุมแอร์



แจ้งเตือนเสียง

แอร์

Server

PLC ควบคุมแอร์

ถังดับเพลง

การรักษาความมั่นคงปลอดภัย (Security Management) ห้อง Data center

อุปกรณ์ตรวจจับควันและอุณหภูมิ

ระบบเข้า-ออก ห้อง

ระบบสำรองไฟ

ระบบระบายอากาศ

แนวทางการสำรองข้อมูลให้ปลอดภัยมากขึ้น

Database

↓

มีการสำรองข้อมูลหลายประเภท

↓

มีการแยกเก็บข้อมูลคนละที่

ห้อง Data center ห้อง DR site

เจ้าหน้าที่ผู้รับผิดชอบข้อมูลในหน่วยบริการ

๕.๔ มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server

คำอธิบายเกณฑ์

สถานพยาบาลมีการป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server อย่างครบถ้วน เพื่อป้องกันการสูญหายของข้อมูลและสามารถใช้งานระบบได้อย่างต่อเนื่อง

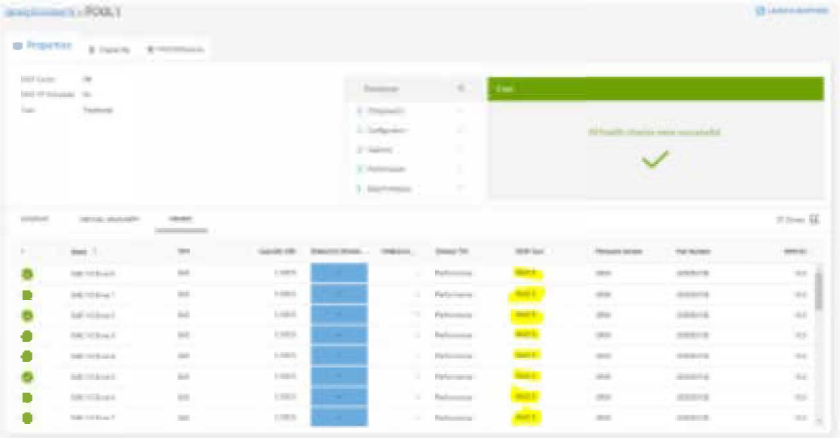
วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การแสดงหลักฐานด้านการป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server
๐.๕	**มี** การแสดงหลักฐานด้านการป้องกันความเสียหายของข้อมูลและระบบ **หรือ** ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server **(ขาดอย่างใดอย่างหนึ่ง)**
๑	มีการแสดงหลักฐานด้านการป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึงระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server **อย่างครบถ้วน**

เอกสารอ้างอิง ภาพถ่าย/รูปถ่าย ภายในห้อง Data Center ที่แสดงถึงการมีอยู่ของการป้องกันความเสียหายของข้อมูลและระบบ ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server

5.4 มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) , ระบบ RAID , Redundant Power supply , Redundant Server

- ส่วนของห้อง Server มี UPS 30k รองรับทั้งห้องได้ประมาณ 3 ชั่วโมง และมีไฟฟ้าสำรองของโรงพยาบาลเป็นแบบ Generator
- ส่วนของ Server และ Storage มีการทำ RAID5 และมี Power Supply 2 อัน



๕.๕ มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center

คำอธิบายเกณฑ์

สถานพยาบาลมีการวิเคราะห์ความเหมาะสม มาตรฐาน และปัจจัยเสี่ยงในการเลือกใช้อุปกรณ์ของห้อง Data Center โดยนำผลการวิเคราะห์มาประเมินความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ของห้อง Data Center เพื่อให้หน่วยงานสามารถเลือกใช้อุปกรณ์ได้อย่างเหมาะสมกับความต้องการ คุ้มค่าในการใช้งานได้ในระยะยาว และทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

วิธีการให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๐	**ไม่มี** การวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center
๐.๕	**มี** การวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยง **แต่** ไม่ได้นำผลการวิเคราะห์มาวัดความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center และไม่มีการลงนามเป็นลายลักษณ์อักษร
๑	มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยง **และ**นำผลการวิเคราะห์มาวัดความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center **และ**มีการลงนามเป็นลายลักษณ์อักษร

เอกสารอ้างอิง คู่มือปฏิบัติงานจัดหาอุปกรณ์ฮาร์ดแวร์ ซอฟแวร์ ของห้อง Data Center, Flow chart ขั้นตอนดำเนินการจัดหา ฮาร์ดแวร์ ซอฟแวร์ ของห้อง Data Center, TOR การจัดซื้ออุปกรณ์ ฮาร์ดแวร์ ซอฟแวร์ ของห้อง Data Center

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	หน้า : ๑ /๑๓ แบบ: ICT-MGNT๐๑-F๐๑

ก. ข้อมูลทั่วไป

๑. ชื่อโครงการ

โครงการพัฒนาความปลอดภัย Data Center

๒. ส่วนราชการ / รัฐวิสาหกิจ

๒.๑ ชื่อหน่วยงาน	กรมป่าไม้	
๒.๒ หัวหน้าส่วนราชการ	ชื่อ: นายอรรถพล เจริญชันษา	โทร: ๐ ๒๕๖๑ ๔๒๙๒ ต่อ ๕๑๗๓
	ตำแหน่ง:อธิบดีกรมป่าไม้	e-mail: athapol.rfd๑@forest.go.th
๒.๓ CIO	ชื่อ: นางอำนวยพร ชลดำรงค์กุล	โทร: ๐๒-๕๖๑๔๒๙๒-๓ ต่อ ๕๕๘๒
	ตำแหน่ง:รองอธิบดีกรมป่าไม้	e-mail: am.chol@forest.go.th
๒.๔ ผู้รับผิดชอบโครงการ	ชื่อ: นางวราวรรณ ธนะกิจรุ่งเรือง	โทร: ๐ ๒๕๖๑ ๔๒๙๒ ต่อ ๕๗๕๔
	ตำแหน่ง: ผู้อำนวยการสำนักแผนงานและสารสนเทศ	e-mail: warawan.tana@forest.go.th

๓. วงเงินงบประมาณ ปี พ.ศ..๒๕๖๓...

๓.๑ งบประมาณรวม	(ตัวเลข) ๗,๐๐๐,๐๐๐ บาท (ตัวอักษร) เจ็ดล้านบาทถ้วน
๓.๒ อำนาจการอนุมัติโครงการ	☑ คณะกรรมการบริหารฯ (กระทรวง) ☐ กระทรวง DE (วงเงินมากกว่า ๑๐๐ ล้านบาท)
๓.๓ แหล่งเงิน	☑ งบประมาณประจำปี ☐ เปลี่ยนแปลงรายการ/เงินเหลือจ่าย ☐ เงินรายได้ ☐ เงินช่วยเหลือ / เงินนอกงบประมาณ ☐ อื่นๆ (ระบุ) .....

๔. วิธีการจัดหา

☐ จัดซื้อ ☑ การจ้าง ☐ การจ้างที่ปรึกษา
☐ การจ้างออกแบบและควบคุมงาน ☐ การแลกเปลี่ยน ☐ การเช่า

๕. ลักษณะโครงการ

๕.๑ ☐ พัฒนาระบบ	☐ มีเอกสารแบบบัญชีราคากลาง ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ ☐ มีเหตุผลประกอบในข้อ ข. ๔. (กรณีมีใบเสนอราคาไม่ครบ ๓ ผู้ประกอบการ)
๕.๒ ☐ ระบบกล้องโทรทัศน์วงจรปิด (CCTV)	☐ มีเอกสารแบบฟอร์มการพิจารณาคุณสมบัติกล้องโทรทัศน์วงจรปิด (CCTV) ☐ ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ☐ ไม่ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ☐ มีใบเสนอราคาจำนวน_____ผลิตภัณฑ์ (รายการที่.....) ☐ มีใบเสนอราคาจำนวน_____ผลิตภัณฑ์ (รายการที่.....) ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ (รายการที่.....) ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ (รายการที่.....) ☐ มีเหตุผลประกอบในข้อ ข. ข้อ ๔.๓ (กรณีมีใบเสนอราคาไม่ครบ ๓ ผลิตภัณฑ์ / ๓ ผู้ประกอบการ)

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	หน้า : ๒ /๑๓ แบบ: ICT-MGNT๐๑-Fo๑

๕.๓ ☑ จัดซื้อครุภัณฑ์ / โปรแกรม	☐ ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ☑ ไม่ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ☐ มีใบเสนอราคาจำนวน_____ผลิตภัณฑ์ (รายการที่.....) ☑ มีใบเสนอราคาจำนวน__๓__ผลิตภัณฑ์ (รายการที่....๔.....) ☑ มีใบเสนอราคาจำนวน__๓__ผู้ประกอบการ (รายการที่...๑-๓,๕-๘.....) ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ (รายการที่.....) ☐ มีเหตุผลประกอบในข้อ ข. ข้อ ๔.๓ (กรณีมีใบเสนอราคาไม่ครบ ๓ ผลิตภัณฑ์ / ๓ ผู้ประกอบการ)

๖. การจัดหา

๖.๑ ☑ ขยายระบบเดิม / ต่อเนื่อง ☐ จัดหาใหม่

๖.๒ ☑ โครงการตามแผนยุทธศาสตร์/บูรณาการ ☐ โครงการตามภารกิจพื้นฐาน ☐ โครงการตามแนวพระราชดำริ
☐ โครงการตามแผนพัฒนาจังหวัด/กลุ่มจังหวัด ☐ โครงการตามข้อสั่งการ รมว.ทส./ปกท.ทส.
☑ อื่นๆ (ระบุ)..แผนปฏิบัติการดิจิทัลของกรมป่าไม้ (พ.ศ.๒๕๖๑-๒๕๖๔)

.....

๗. ลักษณะการจัดหาตามเงื่อนไขที่กระทรวง DE กำหนด

ข้อ ๑) การจัดหาที่หน่วยงานสามารถดำเนินการได้เอง (มูลค่าไม่เกิน ๑๐๐ ล้านบาท)

☐ ๑.๑) เป็นการจัดหาครุภัณฑ์คอมพิวเตอร์และโปรแกรมสำนักงานพื้นฐาน ตามคุณสมบัติและราคามาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด ภายใต้เงื่อนไขในการใช้งานคอมพิวเตอร์ไม่เกิน ๑ เครื่อง / คน โดยเฉลี่ย ตามความเหมาะสมกับภารกิจของหน่วยงาน

☐ ๑.๒) เป็นการจัดหาระบบคอมพิวเตอร์เพื่อทดแทนระบบที่ใช้มาแล้วไม่น้อยกว่า ๕ ปี (จัดหาได้ในวงเงินไม่มากกว่าเดิม และให้วงเงินที่ขอครอบคลุมถึงการถ่ายโอนข้อมูลด้วย)

☑ ๑.๓) เป็นการจัดหาระบบคอมพิวเตอร์เพื่อเพิ่มศักยภาพของระบบ ตามงาน / แผนงาน / โครงการเดิม โดยระบบงานดังกล่าวไม่มีความซ้ำซ้อน / เชื่อมโยง / สัมพันธ์กับงานในภารกิจของหน่วยงานอื่น

☐ ๑.๔) รัฐวิสาหกิจสามารถจัดหาระบบคอมพิวเตอร์ได้โดยไม่ต้องขอความเห็นชอบจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ข้อ ๒) การจัดหาต้องขอความเห็นชอบต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (มูลค่าเกิน ๑๐๐ ล้านบาท)

☐ ๒.๑) เป็นการจัดหาระบบคอมพิวเตอร์งาน / แผนงาน / โครงการที่นอกเหนือจากข้อ ๑.

☐ ๒.๒) เป็นการปรับปรุงเปลี่ยนแปลงโครงการตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ให้ความเห็นชอบแล้ว (ต้องขอความเห็นชอบใหม่)

☐ เป็นหน่วยงานที่ได้รับการยกเว้นการปฏิบัติตามหลักเกณฑ์ฯ เนื่องจากยุทธศาสตร์ของกระทรวงได้รับความเห็นชอบจากคณะรัฐมนตรีและได้ลงนามในคำรับรองการปฏิบัติราชการแล้ว โดยให้กระทรวงฯ ดำเนินการพิจารณาอนุมัติการจัดหาระบบฯ ของหน่วยงานในสังกัดได้เอง (มติคณะรัฐมนตรี ๒๓ มีนาคม ๒๕๔๗)

หมายเหตุ โปรดดูรายละเอียด / เงื่อนไขการดำเนินงาน และการรายงานที่เกี่ยวเนื่อง ได้เพิ่มเติมใน หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุดที่ ๐๕๐๔/๔๙๕๖ ลงวันที่ ๓๑ มีนาคม ๒๕๔๗ เรื่อง หลักเกณฑ์และแนวทางปฏิบัติการจัดหาระบบคอมพิวเตอร์ของรัฐ

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	หน้า : ๓ /๑๓
		แบบ: ICT-MGNT๐๑-Fo๑

ข. ข้อมูลโครงการ

๑. หลักการและเหตุผลความเป็นมาของโครงการ

ด้วยศูนย์สารสนเทศ กรมป่าไม้ มีหน้าที่ให้บริการคอมพิวเตอร์ บริการสารสนเทศ บริการเครือข่าย บริการอินทราเน็ต ภายในหน่วยงาน และให้บริการอินเตอร์เน็ตสู่ภายนอก หน่วยงานโดยทำการควบคุม ดูแล พัฒนาระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้ตลอดเวลาและมีประสิทธิภาพ รวมถึงการเชื่อมเชื่อมโยงข้อมูลสารสนเทศเพื่อให้บริการและการสนับสนุนการปฏิบัติราชการแก่หน่วยงาน ณ อาคารเทียมคมกฤษ ชั้น ๓ ห้องสารสนเทศ โดยห้องศูนย์ปฏิบัติการคอมพิวเตอร์ (Data Center) เป็นศูนย์รวมการควบคุมระบบเทคโนโลยีสารสนเทศต่างๆ จำเป็นต้องมีการพัฒนาปรับปรุงระบบสนับสนุนศูนย์คอมพิวเตอร์ให้เหมาะสมกับสภาพใช้งานในปัจจุบันให้มีความเป็นมาตฐาน ทันสมัย มีเสถียรภาพน่าเชื่อถือ และมีความปลอดภัยสูง ทั้งนี้ คำนึกถึงความจำเป็นและความเหมาะสมกับเทคโนโลยีปัจจุบัน เพื่อลดความเสี่ยงจากการหยุดทำงานของระบบสารสนเทศ (Down Time) ด้วยเหตุขัดข้องต่างๆ ที่ไม่พึงประสงค์

๒. วัตถุประสงค์ของโครงการ

๑. เพื่อปรับปรุงโครงสร้างพื้นฐานห้อง Data Center กรมป่าไม้ให้มีความปลอดภัย
๒. เพื่อลดความเสี่ยงของการหยุดทำงานของระบบสารสนเทศ (Down Time) จากเหตุขัดข้องต่างๆ ที่ไม่พึ่งประสงค์ เช่น ไฟไหม้ ไฟฟ้าดับ
๓. เพื่อให้ห้อง Data Center มีความปลอดภัย ได้มาตฐานตามข้อกำหนดการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี

๓. เป้าหมายของโครงการ

ดำเนินการพัฒนาความปลอดภัย Data Center เพื่อสนับสนุนการปฏิบัติราชการแก่หน่วยงาน แล้วเสร็จ ภายในปี ๒๕๖๓

๔. สภาพพื้นฐานก่อนเริ่มโครงการ (Project Baseline Data)

๔.๑ สถานภาพพื้นฐานโดยทั่วไป

ห้องศูนย์ปฏิบัติการคอมพิวเตอร์ (Data Center) กรมป่าไม้ยังไม่มีระบบการป้องกันการเกิดอัคคีภัย การตรวจจับควันที่เหมาะสมกับสภาพใช้งานในปัจจุบันและยังไม่เป็นเป็นมาตฐานที่ทันสมัย มีเสถียรภาพน่าเชื่อถือ และมีความปลอดภัย

๔.๒ สภาพปัญหาของผู้รับบริการ ผู้เกี่ยวข้องที่มีส่วนได้ส่วนเสีย ตลอดจนผู้ประกอบการเอกชนหรือประชาชนโดยรวม (ถ้ามี)

ห้องศูนย์ปฏิบัติการคอมพิวเตอร์ (Data Center) กรมป่าไม้มีความเสี่ยงต่อการเกิดเหตุเพลิงไหม้ซึ่งอาจทำให้ข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่ายเกิดความสูญเสียและไม่สามารถให้บริการได้

๔.๓ ปัญหาอุปสรรคในการปฏิบัติงาน/เหตุผลความจำเป็นที่ต้องจัดหาครั้งนี้

ไม่สามารถปิดระบบคอมพิวเตอร์และระบบเครือข่ายเพื่อปรับปรุงได้เป็นระยะเวลานาน เพื่อให้ห้องศูนย์ปฏิบัติการคอมพิวเตอร์ (Data Center) มีระบบรักษาความปลอดภัยด้านกายภาพที่พร้อมต่อการใช้งาน

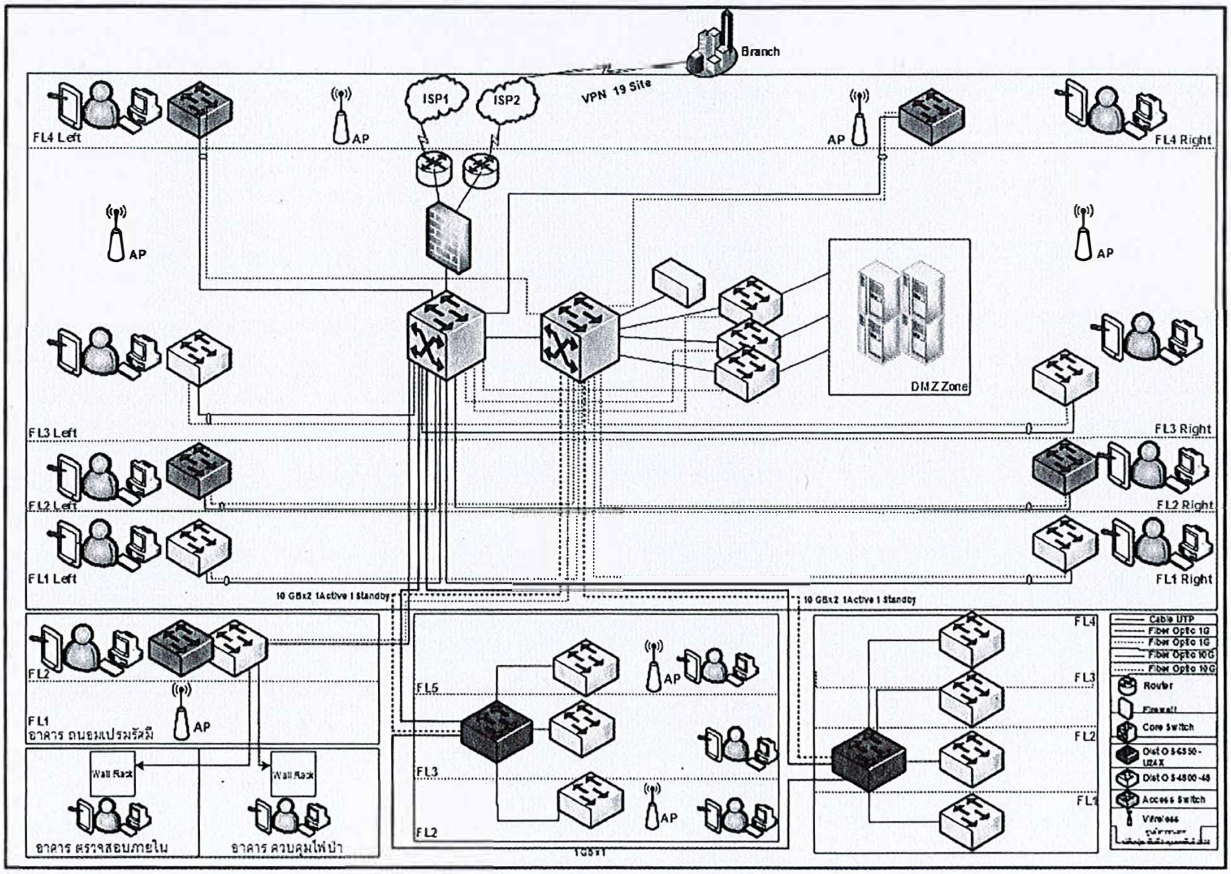
	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	หน้า : ๔ /๑๓
		แบบ: ICT-MGNT๐๑-F๐๑

๔. สภาพพื้นฐานก่อนเริ่มโครงการ (Project Baseline Data)

๔.๔ ระบบหรืออุปกรณ์ทั้งหมดที่มีอยู่ในปัจจุบันของหน่วยงาน

รายการ	สถานที่ติดตั้ง/ชื่อระบบงาน	ติดตั้งเมื่อปี พ.ศ.
๑. เครื่องปรับอากาศดูดความชื้น	ห้อง Data Center	๒๕๕๕
๒. เครื่องสำรองไฟฟ้า	ห้อง Data Center	๒๕๕๕
๓. เครื่องดับเพลิงอัตโนมัติ	ห้อง Data Center	๒๕๕๕
๔. เครื่องตรวจจับหมอกควัน	ห้อง Data Center	๒๕๕๕

๔.๔ ผังโครงสร้างเครือข่ายคอมพิวเตอร์ของหน่วยงานและ/หรือแผนผังโครงการตามข้อ ๑. (ถ้ามี)



๕. ขอบเขตและข้อกำหนดความต้องการของระบบฯ ภายในโครงการ

๕.๑ ขอบเขตโครงการ (Project / System Scope)

ระยะเวลา ๑๒ เดือน ตั้งแต่ มกราคม ๒๕๖๓ – ธันวาคม ๒๕๖๓

๕.๒ ข้อกำหนดความต้องการของระบบ (System Requirements)

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	หน้า : ๕ /๑๓ แบบ: ICT-MGNT๐๑-F๐๑

๖. แนวทางการดำเนินงาน รายการจัดหา ระยะเวลาดำเนินการ และกำหนดการ

๖.๑ แนวทางการดำเนินงาน

ดำเนินการจัดซื้อตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ. ๒๕๖๐ และตามประกาศสำนักนายกรัฐมนตรีเรื่อง แนวทางปฏิบัติในการจัดหาพัสดุด้วยวิธีตลาดอิเล็กทรอนิกส์ (Electronic Market : e market) และด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (Electronic : e - Bidding)

๖.๒ รายการที่จะจัดหา

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
๑. **งานปรับปรุงภายในห้อง** - งานโต๊ะเก้าอี้กทำงานห้อง Data center - ปรับปรุงพื้นที่ และทำการออกแบบ จัดหาวัสดุ อุปกรณ์และติดตั้งตลอดจนดับแปลง ปรับปรุง ย้าย แก้ไข ระบบต่างๆ ที่มีอยู่เดิมให้เหมาะสม - ดำเนินการทาสีบริเวณพื้นที่ศูนย์ข้อมูล (Data Center) - ดำเนินการรื้อถอนและติดตั้งฝ้าเพดานใหม่ โดยให้มีความสูงตามที่ระบุในแบบ - คำนวณการับน้ำหนักจากอุปกรณ์และน้ำหนักอื่นๆ ต่อโครงสร้างอาคารให้ไม่เกินกว่าน้ำหนักที่ผู้ออกแบบอาคารได้ออกแบบกำหนดไว้ เพื่อความมั่นคงแข็งแรงของโครงสร้าง และความปลอดภัยของผู้ใช้อาคารโดยมีวิศกรผู้คำนวณและรับรองความมั่นคงแข็งแรงของโครงสร้างอาคารที่ดำเนินการปรับปรุงระดับไม่น้อยกว่าสามัญวิศวกรโยธา		✓	๑ งาน	๒,๐๐๐,๐๐๐	**๒,๐๐๐,๐๐๐**
๒. **งานปรับปรุงระบบพื้นยกสำเร็จรูป** - ปรับปรุงระบบพื้นยก (Raised Floor System) ในห้องปฏิบัติการคอมพิวเตอร์ (Data Center) เดิม - แผ่นพื้นยกที่ใช้มีผิวหน้าเป็น High Pressure Laminated (HPL-antistatic) - แผ่นพื้นยกสำเร็จรูปจะต้องวางอยู่บนขาตั้ง (Pedestal) ทำจากเหล็กชุบสังกะสีหรือสารป้องกันการเกิดสนิม และมีระบบคานรับพื้น เพื่อเสริมการรับน้ำหนักได้ดียิ่งขึ้น		✓	๑ งาน	๕๐๐,๐๐๐	**๕๐๐,๐๐๐**
๓. **งานปรับปรุงระบบไฟฟ้า ภายในห้อง** - ผู้รับจ้างต้องเสนอแบบไดอะแกรมระบบไฟฟ้า (Single Line Diagram) ให้ทางกรมป่าไม้พิจารณาอนุมัติก่อนการดำเนินงาน - ระบบไฟฟ้าที่ออกแบบและติดตั้งต้องสามารถจ่ายกระแสไฟฟ้าได้เพียงพอกับอุปกรณ์ภายในห้องศูนย์คอมพิวเตอร์		✓	๑ งาน	๓๐๐,๐๐๐	**๓๐๐,๐๐๐**

๖. แนวทางการดำเนินงาน รายการจัดหา ระยะเวลาดำเนินการ และกำหนดการ

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
- ผู้รับจ้างต้องออกแบบ และติดตั้งระบบไฟส่องสว่างภายในห้องศูนย์คอมพิวเตอร์ติดตั้งรางเดินสายไฟฟ้าไว้ใต้พื้นยกสำเร็จรูป (Raised Floor) พร้อมติดตั้ง Power Plug แบบ ๒P+E IP๔๔ ขนาดไม่น้อยกว่า ๑๖A ๒๒๐V					
๔. **เครื่องสำรองไฟฟ้า ขนาด ๔๐ kVA (ระบบไฟฟ้า ๓ เฟส) จำนวน ๒ เครื่อง** - เครื่องสำรองไฟฟ้ามีคุณสมบัติแบบ Rack - มีกำลังไฟฟ้าด้านนอกไม่น้อยกว่า ๔๐ kVA - มีช่วงแรงดันไฟฟ้า Input (VAC) แบบ ๓ เฟส ไม่น้อยกว่า ๓๘๐ +/-๒๐% หรือดีกว่า - มีช่วงแรงดันไฟฟ้า Output (VAC) อย่างน้อย ๒๒๐ +/-๑% หรือดีกว่า - สามารถสำรองไฟฟ้าที่ Full Load ได้ไม่น้อยกว่า ๓๐ นาทีหรือดีกว่า		✓	๑ งาน	๘๐๐,๐๐๐	๘๐๐,๐๐๐
๕. **งานระบบเครื่องปรับอากาศแบบควบคุมความชื้น** - จัดหาและติดตั้งระบบปรับอากาศแบบควบคุมอุณหภูมิและความชื้น ชนิดทำระบายความร้อนด้วยอากาศ แบบส่งลมเย็นลงด้านล่าง (Down Flow) จำนวน ๒ เครื่อง โดยติดตั้งภายในห้องศูนย์ข้อมูล (Data Center) - จัดหาและติดตั้งเครื่องปรับอากาศแบบควบคุมอุณหภูมิและความชื้น ชนิดทำระบายความร้อนด้วยอากาศ แบบส่งลมเย็นลงด้านล่าง (Down Flow) มีค่า Net Sensible Cooling Capacity ไม่น้อยกว่า ๑๘.๙kW จำนวน ๒ ชุด ทำงานแบบ (N+๑) ที่อุณหภูมิลมกลับ ๒๔oC ความชื้นสัมพัทธ์ ๕๐%RH (Relative Humidity) ความดันลมส่ง External Static Pressure ๒๐Pa และอุณหภูมิภายนอก ๔๐oC โดยค่า Sensible Heat Ratio (SHR) ไม่น้อยกว่า ๙๖.๙% - ผู้ผลิตเครื่องปรับอากาศควบคุมอุณหภูมิและความชื้นที่เสนอต้องมีโรงงานที่ได้รับมาตรฐาน ISO ๙๐๐๑ และ ISO ๑๔๐๐๐		✓	๑ งาน	๘๐๐,๐๐๐	๘๐๐,๐๐๐

ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์

๖. แนวทางการดำเนินงาน รายการจัดหา ระยะเวลาดำเนินการ และกำหนดการ

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
๖. งานระบบปรับปรุงสายสัญญาณสื่อสารคอมพิวเตอร์ (Cablin System) มีคุณสมบัติอย่างน้อยดังนี้ - ติดตั้งสายสัญญาณคู่บิดตีเกลียวหรือสาย LAN ชนิด Category ๖ หรือดีกว่า เชื่อมโยงระหว่างตู้ Network Rack หลัก ไปยังตู้ Rack อื่นๆ ที่ติดตั้งภายในห้องศูนย์คอมพิวเตอร์ (Server Room) จำนวน ๗ ตู้ ไม่น้อยกว่าตู้ละ ๒๔ Port โดยติดตั้งพร้อมแผงกระจายสัญญาณ (UTP Patch Panel) - เดินสายภายในศูนย์คอมพิวเตอร์ (Server Room) ต้องติดตั้งโดยเดินสายร้อยในรางตะแกรงเหล็ก (Cable basket) หรือ ท่อเหล็ก (EMT Conduit) หรือท่ออ่อน (Flexible Conduit) หรือดีกว่า เมื่อติดตั้งระบบสายสัญญาณคอมพิวเตอร์ (UTP) แล้วเสร็จ ต้องทดสอบ และจัดทำรายงานผลการทดสอบสายสัญญาณ		✓	๑ งาน	๓๐๐,๐๐๐	๓๐๐,๐๐๐
๗. งานระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environmental Monitoring System) มีคุณสมบัติอย่างน้อยดังนี้ - สามารถรองรับการเชื่อมต่อซอฟต์แวร์ผ่าน network protocol มาตรฐาน เช่น HTTP,TCP/IP และ SNMP ได้เป็นอย่างน้อย เพื่อความสะดวกต่อการบริหารจัดการ - มีระบบความปลอดภัยในการเข้าถึง (Password Security) และมีฟังก์ชั่นบริหารจัดการผู้ใช้งานได้ - สามารรองรับการแจ้งเตือนเป็น e-mail ได้ - ผู้รับจ้างจะต้องทำการเชื่อมระบบต่างๆ ภายในห้อง Server มาที่อุปกรณ์เฝ้าระวังและแจ้งเตือนอัตโนมัติอย่างน้อยดังนี้ เครื่องปรับอากาศแบบควบคุมอุณหภูมิและความชื้น,เครื่องสำรองไฟฟ้า,ระบบดับเพลิงอัตโนมัติด้วยสารสะอาด,ระบบตรวจจับน้ำรั่วซึม		✓	๑ งาน	๘๐๐,๐๐๐	๘๐๐,๐๐๐

ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์

๖. แนวทางการดำเนินงาน รายการจัดหา ระยะเวลาดำเนินการ และกำหนดการ

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
๘. งานระบบรักษาความปลอดภัยในห้อง ๘.๑ ระบบดับเพลิงอัตโนมัติ (Automatic Fire Suppression System) มีคุณสมบัติอย่างน้อยดังนี้ - เป็นสารสะอาดดับเพลิง (clean agent) เมื่อฉีดออกมาจะกลายเป็นไอและไม่เหลือสิ่งตกค้างหลังการใช้งาน มีพิษต่อคนน้อย และไม่ทำอันตรายต่อทรัพย์สินหรืออุปกรณ์อิเล็กทรอนิกส์ - ดับเพลิงที่ใช้ต้องไม่ทำลายสภาพแวดล้อม โดยค่า Ozone Depletion Potential มีค่าไม่เกินกว่า ๐ และ Global Warming Potential มีค่าไม่เกินกว่า ๑ - ถังบรรจุสารดับเพลิง ต้องเป็นผลิตภัณฑ์ที่ได้มาตรฐาน UL หรือ FM หรือ NFPA หรือเทียบเท่า - หัวจ่ายก๊าซ (Discharge Nozzle) เป็นชนิดทองเหลือง หรือ สแตนเลส หรือดีกว่า - ตู้ควบคุมการทำงานของระบบ (Releasing Control Panel) ควบคุมการทำงานของระบบแบบยืนยันการแจ้งเตือน (Cross-Zone) ได้รับมาตรฐาน หรือ FM - มีแผงควบคุมการทำงานของระบบ (Fire Control Panel) มีสัญญาณแสดงการทำงานของระบบและสภาวะขัดข้องของระบบพร้อมมีแบตเตอรี่เพื่อสำรองในกรณีไฟฟ้าดับ - มีอุปกรณ์ตรวจจับควัน (Smoke Detector) มี LED แสดงสภาวะการทำงานปกติและเมื่อมีการตรวจจับควันได้ - มีระบบควบคุมการฉีดด้วยมือ (Manual Pull Station) อุปกรณ์ควบคุมนี้จะใช้เมื่อต้องการให้ระบบฉีดสารดับเพลิงทันทีโดยไม่ต้องรอการนับเวลาฉีดอัตโนมัติตามที่ตั้งไว้ - มีกระดิ่งสัญญาณ (Alarm Bell) และมีความดังไม่น้อยกว่า ๗๕ เดซิเบล - มีไฟแฟลชกระพริบและสัญญาณเสียง Horn ความดังไม่น้อยกว่า ๗๕ เดซิเบล		✓	๑ งาน	๑,๕๐๐,๐๐๐	๑,๕๐๐,๐๐๐

ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์

๖. แนวทางการดำเนินงาน รายการจัดหา ระยะเวลาดำเนินการ และกำหนดการ

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
๘.๒ ระบบตรวจจับควันไฟความไวสูง (High Sensitivity Smoke Detector System) มีคุณสมบัติอย่างน้อยดังนี้ - มีชุดตรวจจับควันไฟความไวสูงที่มีความละเอียดในการตรวจจับอนุภาควันขนาดเล็ก - มีระดับการแจ้งเตือนไม่น้อยกว่า ๓ ระดับ - ติดตั้งพร้อมชุดท่อสุ่มตัวอย่าง และสามารถรองรับการตรวจจับครอบคลุมพื้นที่ทั้งหมดภายในห้องปฏิบัติการ คอมพิวเตอร์		✓			
๘.๓ ระบบควบคุมการเข้าออก (Access Control System) มีคุณสมบัติอย่างน้อยดังนี้ - เครื่องสแกนลายนิ้วมือมีหน้าจอแสดงผลขนาดไม่น้อยกว่า ๒ นิ้วพร้อมมีปุ่มกดเพื่อป้อนรหัส Pin ในการยืนยันตัวบุคคล - มีสัญญาณเตือนในกรณีมีการเปิดประตูโดยผิดปกติหรือประตูปิดไม่สนิท หรือเปิดประตูค้างนานเกินกำหนด - กลอนประตูไฟฟ้าเป็นชนิด Magnetic หรือ Drop Bolt ใช้งานร่วมกับชุดควบคุมการผ่านเข้าออกประตู โดยมีชุดจ่ายไฟฟ้าและแบตเตอรี่สำรองไฟฟ้าได้ไม่น้อยกว่า ๖ ชั่วโมง - มีระบบ Emergency สำหรับเปิดประตูกรณีเหตุผิดปกติ - เชื่อมต่อระบบควบคุมการเข้าออกผ่านการสแกนลายนิ้วมือไปยังเครื่องคอมพิวเตอร์ที่เตรียมไว้สำหรับบันทึกข้อมูลในการเข้าออกผ่านประตูห้อง เพื่อให้สามารถทำการตรวจสอบการเข้าออกย้อนหลังได้		✓			
๘.๔ ระบบตรวจจับการรั่วของน้ำ (WaterLeak Detection System) มีคุณสมบัติอย่างน้อยดังนี้ - อุปกรณ์ตรวจจับสามารถทำงานได้ ที่อุณหภูมิ ๑๐-๔๐ องศาเซลเซียส และความชื้นสัมพัทธ์ ๑๐-๙๐ %RH โดยไม่เกิดการกลั่นตัวของไอน้ำในอากาศ - มีอุปกรณ์ตรวจจับการรั่วซึมของน้ำที่ได้รับรองตามมาตฐาน UL ๙๑๖ หรือ CE หรือ FCC compliance เป็นอย่างน้อย - สามารถตรวจจับการรั่วซึมของน้ำและแจ้งเตือนได้โดยแสดงสัญญาณไฟแบบ LED หรือดีกว่าที่อุปกรณ์ตรวจจับ		✓			

ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์

๖. แนวทางการดำเนินงาน รายการจัดหา ระยะเวลาดำเนินการ และกำหนดการ

- สามารถแจ้งเตือนเมื่อระบบสายตรวจจับมีปัญหา (Cable fault) ระบบวงจรมีปัญหา (circuit failure) หรือ ระบบจ่ายไฟมีปัญหา (Loss of Power)					

* หมายเหตุ : ในรายการที่จัดหาให้ใช้เครื่องหมาย / ระบุใน SPEC ที่กำหนด
(DE:กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม/ DEPT:หน่วยงานกำหนดเอง)

๖.๓ หน่วยงานที่จะทำการติดตั้งระบบ / อุปกรณ์

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	จำนวน	ชื่อหน่วยงานที่ติดตั้ง
๑. งานปรับปรุงภายในห้อง	๑ งาน	กรมป่าไม้ส่วนกลาง
๒. งานปรับปรุงระบบพื้นยกสำเร็จรูป	๑ งาน	กรมป่าไม้ส่วนกลาง
๓. งานปรับปรุงระบบไฟฟ้า ภายในห้อง	๑ งาน	กรมป่าไม้ส่วนกลาง
๔. งานระบบสำรองไฟฟ้าอย่างต่อเนื่อง (UPS)	๑ งาน	กรมป่าไม้ส่วนกลาง
๕. งานระบบเครื่องปรับอากาศแบบควบคุมความชื้น	๑ งาน	กรมป่าไม้ส่วนกลาง
๖. งานระบบปรับปรุงสายสัญญาณสื่อสารคอมพิวเตอร์ (Cablin System)	๑ งาน	กรมป่าไม้ส่วนกลาง
๗. งานระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environmental Monitoring System)	๑ งาน	กรมป่าไม้ส่วนกลาง
๘. งานระบบรักษาความปลอดภัยในห้อง	๑ งาน	กรมป่าไม้ส่วนกลาง

๖.๔ ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการ ๑๒ เดือน
เริ่มตั้งแต่ มกราคม ๒๕๖๓ ถึง ธันวาคม ๒๕๖๓

๖.๕ กำหนดการ (Schedule)

กิจกรรม	กำหนดการ (เดือนที่)												หมายเหตุ
	๑	๒	๓	๔	๕	๖	๗	๘	๙	๑๐	๑๑	๑๒	
๑. โครงการเพิ่มประสิทธิภาพความปลอดภัยระบบเครือข่ายคอมพิวเตอร์เพื่อสนับสนุนภารกิจของกรมป่าไม้	←	—	→										
๒. นำเสนอโครงการเพื่อขอความเห็นชอบ				←	—	→							
๓. แต่งตั้งคณะกรรมการจัดทำ TOR							↔						
๔. จัดทำ TOR								↔					
๕. ประกาศจัดหาผู้จ้างและดำเนินการจัดจ้าง									←	—	→		
๖. ตรวจรับพัสดุ											↔		
๗. ดำเนินการติดตั้งพัสดุ												↔	

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	หน้า : ๑๑ /๑๓
		แบบ: ICT-MGNT๐๑-F๐๑

๗. ผลผลิตของโครงการ (Output / Deliverables)

ห้อง Data Center มีความปลอดภัย และมีบริหารจัดการได้สะดวก รวดเร็ว

๘. ตัวชี้วัดสัมฤทธิ์ผล หรือปัจจัยสำเร็จของโครงการ

ตัวชี้วัดเป้าหมายโครงการ (Outputs)

ดำเนินการพัฒนาความปลอดภัย Data Center เพื่อสนับสนุนการปฏิบัติราชการแก่หน่วยงาน แล้วเสร็จ ภายในปี ๒๕๖๓

ตัวชี้วัดผลลัพธ์ (Outcomes)

ห้อง Data Center มีความปลอดภัย และมีบริหารจัดการได้สะดวก รวดเร็ว

๙. ความสอดคล้องเชิงยุทธศาสตร์ของโครงการ

๙.๑ ความสอดคล้องกับแผนยุทธศาสตร์ของรัฐบาล กระทรวง หรือหน่วยงาน / แผนปฏิบัติราชการ ๔ ปี ฯลฯ

แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่๑๒ (พ.ศ. ๒๕๖๒-๒๕๖๔)

ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่งคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน

๙.๒ ความสอดคล้องกับแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม / แผนพัฒนารัฐบาลดิจิทัล / แผนปฏิบัติการดิจิทัลของกระทรวง

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

ยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

๙.๓ ความสอดคล้องกับแผนปฏิบัติการดิจิทัลของหน่วยงาน แผน

แผนปฏิบัติการดิจิทัลของกรมป่าไม้ (พ.ศ. ๒๕๖๑ – ๒๕๖๔)

ยุทธศาสตร์ที่ ๔ : บริหารจัดการทรัพยากรป่าไม้ด้วยเทคโนโลยีดิจิทัลที่ปลอดภัย

๑๐. ความพร้อมของโครงการ

๑๐.๑ บุคลากรของหน่วยงานที่เกี่ยวข้องกับโครงการ (ตามข้อ ๑.)

ด้าน / สาขา	จำนวน
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ	๑
นักวิชาการป่าไม้ชำนาญการ	๑
นักวิชาการคอมพิวเตอร์ชำนาญการ	๒
นักวิเคราะห์นโยบายและแผนชำนาญการ	๑
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๕
นักวิเคราะห์นโยบายและแผนปฏิบัติการ	๖
เจ้าหน้าที่ระบบงานคอมพิวเตอร์	๒
นักวิเคราะห์นโยบายและแผน	๕
รวม	๒๓

๑๐. ความพร้อมของโครงการ

๑๐.๒ ประเด็นความพร้อมด้านอื่นๆ (ถ้ามี)

-

๑๐.๓ ประเด็นความเสี่ยงของโครงการและแนวทางการบรรเทา (Project Risks and Risk Mitigations)

-

๑๑. ประโยชน์ที่จะได้รับ

๑. โครงสร้างพื้นฐานห้อง Data Center มีความมั่นคงปลอดภัย

๒. ระบบภายในห้อง Data Center มีความเรียบร้อยและง่ายต่อการบริหารจัดการ

๓. เพื่อลดความเสี่ยงของการหยุดทำงานของระบบสารสนเทศ (Down Time) จากเหตุขัดข้องต่างๆ ที่ไม่พึงประสงค์ เช่น ไฟไหม้ ไฟฟ้าดับ

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	หน้า : ๑๓ /๑๓ แบบ: ICT-MGNT๐๑-F๐๑

ค. การลงนามรับรองโครงการ

๑. ผู้จัดทำ / ขออนุมัติโครงการ

ลงชื่อ .....

(นายทนงศักดิ์ มนตรี)

ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

หน่วยงาน ศูนย์สารสนเทศ

๒. ผู้ตรวจสอบโครงการ

ลงชื่อ .....

(นายสุกันต์ พึ่งกุล)

ตำแหน่ง ผู้อำนวยการศูนย์สารสนเทศ

หน่วยงาน ศูนย์สารสนเทศ

๓. ผู้รับผิดชอบโครงการระดับกรม / รัฐวิสาหกิจ

ลงชื่อ .....

(นางอำนวยพร ชลดำรงค์กุล)

ตำแหน่ง รองอธิบดีกรมป่าไม้

ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสาร (CIO)

หน่วยงาน กรมป่าไม้

๔. ผู้รับรองผลการพิจารณาอนุมัติโครงการจากคณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสารประจำกระทรวง

โครงการฯ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมเมื่อวันที่ ๐๓ เม.ย. 2562

ลงชื่อ .....

(นายสุพจน์ โตวิจักษณ์ชัยกุล)

ตำแหน่ง **รองปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม**

ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสาร (CIO) ประจำกระทรวง

กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

เอกสารตัวอย่าง ข้อ 5.5

บริษัท เฟิร์ส โซลูชั่น โพรไวเดอร์ จำกัด

FIRST SOLUTIONS PROVIDER CO.,LTD.

90/739 ม.5 ซ.ท่าอิฐ ถ.รัตนาธิเบศร์ ต.ท่าอิฐ อ.ปากเกร็ด จ.นนทบุรี 11120

โทรศัพท์ : (02) 149-0368 โทรสาร : (02) 149-0368

Website : www.firstsolutionsprovider.com E-mail : Sales@fs-provider.com

เลขประจำตัวผู้เสียภาษีอากร 0125554001440

Quotation / ใบเสนอราคา

Customer :

Name :	K.Tanong Montri	Quotation No :	PNW6205-006
Company :	Royal Forest Department	Quotation Date :	2 พฤษภาคม 2562
Address :	61 Phaholyothin Road, Chatuchak, Bangkok 10900	Mobile :	
		Tel :	
E-mail :	tanong@forest.go.th	Fax :	

Subject : โครงการพัฒนาความปลอดภัย Data Center

No.	Description รายการ	Qty จำนวน	Unit Price หน่วยละ	Amount จำนวนเงิน
1	งานปรับปรุงภายในห้อง	1	1,800,000.00	1,800,000.00
2	งานปรับปรุงระบบไฟฟ้า ภายในห้อง	1	300,000.00	300,000.00
3	เครื่องสำรองไฟฟ้า ขนาด 40 kVA (ระบบไฟฟ้า 3 เฟส) / APC UPS 40KVA 400V	2	500,000.00	1,000,000.00
4	งานปรับปรุงระบบพื้นยกสำเร็จรูป	1	500,000.00	500,000.00
5	งานระบบปรับปรุงสายสัญญาณสื่อสารคอมพิวเตอร์ (Cablin System)	1	300,000.00	300,000.00
6	งานระบบเครื่องปรับอากาศแบบควบคุมความชื้น	1	800,000.00	800,000.00
7	งานระบบรักษาความปลอดภัยในห้อง	1	1,500,000.00	1,500,000.00
	7.1 ระบบดั บเพลิงอัตโนมัติ(Automatic Fire Suppression System)			-
	7.2 ระบบตรวจจับควันไฟความไวสูง (High Sensitivity Smoke Detector System)			-
	7.3 ระบบควบคุมการเข้าออก (Access Control System)			-
	7.4 ระบบตรวจจั บการรั่วของน้ำ(WaterLeak Detection System)			-
8	งานระบบเฝ้าดูและแจ้งเตือนอั ตโนมัติ(Environmental Monitoring System)	1	800,000.00	800,000.00
			GRAND TOTAL	**7,000,000.00**
			DISCOUNT	**-**
			TOTAL	**7,000,000.00**

Terms and Conditions

Price Validity	Delivery Date	Payment Term	Warranty	Type
30 Days	*30 Days*	*10 Days*	*1 Year*	*HW*

Purchase approved in accordance with this quotation

(อนุมัติสั่งซื้อตามใบเสนอราคานี้)

ประทับตราบริษัท

( )

Purchaser Authorized Signature & Sale

ลงนามผู้มีอำนาจในการสั่งซื้อ

Best Regards,

(Miss Aumpornpen Lukkanawimol)

Marketing Executive

Aumpornpen.l@fsp.in.th

(Mobile : 02-717-1114)

เอกสารตัวอย่าง ข้อ 5.5

F-SM-03-Rev.00

i-Tree Innovative Services Company Limited
21/104 Moo 6 Soi Chinnakhet2, Ngamwongwan Road, Tungsonghong, Laksi, Bangkok 10210 Tel : 097-159-9250 Fax. 02-954-9717

Quotation

Name: Tanong Montri
Title: โครงการพัฒนาความปลอดภัย Data Center
Company: กรมป่าไม้
Address: 61 ถนน พหลโยธิน แขวง ลาดยาว เขต จตุจักร กรุงเทพมหานคร 10900
Tel/Fax :

Quotation No.: 0519-1S
Date: 2-May-19
Revise:

วันที่ส่งของ Delivery Date	กำหนดยืนราคา Quote Validity	กำหนดการชำระเงิน Term Payment	พนักงานขาย Account Manager
90 Days	30 Days	30 Days	Sangarun S.

ลำดับที่ Item	รหัสสินค้า Part Number	รายการสินค้า Description	ปริมาณ Qty.	ราคาต่อหน่วย Unit List Price	ราคา Amount
1		งานระบบรักษาความปลอดภัยในห้อง - ระบบดับเพลิงอัตโนมัติ (Automatic Fire Suppression System) - ระบบควบคุมการเข้า-ออก (Access Control System) - ระบบตรวจจับการรั่วของน้ำ (WaterLeak Detection System) - ระบบตรวจจับควันไฟความไวสูง (High Sensitivity Smoke Detector System)	1	1,500,000.00	1,500,000.00
2		งานปรับปรุงระบบพื้นยกสำเร็จรูป	1	500,000.00	500,000.00
3		เครื่องสำรองไฟฟ้า ขนาด 40 kVA (ระบบไฟฟ้า 3 เฟส) / Cyber power 40KVA	2	400,000.00	800,000.00
4		งานระบบปรับปรุงสายสัญญาณสื่อสารคอมพิวเตอร์(Cablin System)	1	300,000.00	300,000.00
5		งานปรับปรุงภายในห้อง	1	2,000,000.00	2,000,000.00
6		งานระบบเครื่องปรับอากาศแบบควบคุมความชื้น	1	800,000.00	800,000.00
7		งานระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environmental Monitoring System)	1	800,000.00	800,000.00
8		งานปรับปรุงระบบไฟฟ้า ภายในห้อง	1	300,000.00	300,000.00
		TOTAL PRICE Include VAT 7%			**7,000,000.00**
		GRAND TOTAL PURCHASE ORDER			**7,000,000.00**

Remark:

( )
Authorized signature of purchaser
Name..... Date: .....

Proposed by : .....
(Sangarun Sripradab)
Account Manager

Approved by : .....
(Rungchai Triyaprasertporn)
Sales Director

บริษัท ไอ-ทรี อินโนเวทีฟ เซอร์วิสเซส จำกัด
i-Tree Innovative Services Co., Ltd.

เอกสารตัวอย่าง ข้อ 5.5

บริษัท เคมิท กรุ๊ป จำกัด
KMIT-GROUP CO., LTD.

333/94 Moo 4, Lak Si Plaza Building Tower 1 Floor 8,
Kamphaeng Phet 6 Rd., Tarad Bang Khen, Lak Si, Bangkok 10210
Tel. 02-576-1304-5 Fax. 02-576-1306
Website : www.kmit-group.com E-mail : sales@kmit-group.com
เลขประจำตัวผู้เสียภาษีอากร (TAX ID.) : 0125550003758

KMIT GROUP

QUOTATION / ใบเสนอราคา

Name :	Khun Tanong Montri	Quotation No.	QONBART1905_001
Company :	Royal Forest Department	Date :	2/May/2019
Address :	61 Phaholyothin Road, Chatuchak, Bangkok 10900	Tel :	
		Fax :	
E-mail :		Revised No.	

Subject : โครงการพัฒนาความปลอดภัย Data Center

No.	Part Number	Description	Qty	Unit	Unit Price	Amount
		โครงการพัฒนาความปลอดภัย Data Center				
1		งานปรับปรุงภายในห้อง	1	งาน	2,000,000.00	2,000,000.00
2		งานปรับปรุงระบบพื้นยกสำเร็จรูป	1	งาน	500,000.00	500,000.00
3		งานปรับปรุงระบบไฟฟ้า ภายในห้อง	1	งาน	300,000.00	300,000.00
4		เครื่องสำรองไฟฟ้า ขนาด 40 kVA (Emerson UPS 40KVA 400V)	2	เครื่อง	450,000.00	900,000.00
5		งานระบบเครื่องปรับอากาศแบบควบคุมความชื้น	1	งาน	800,000.00	800,000.00
6		งานระบบปรับปรุงสายสัญญาณสื่อสารคอมพิวเตอร์ (Cablin System)	1	งาน	300,000.00	300,000.00
7		งานระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environmental Monitoring System)	1	งาน	800,000.00	800,000.00
8		งานระบบรักษาความปลอดภัยในห้อง - ระบบดับเพลิงอัตโนมัติ (Automatic Fire Suppression System) - ระบบตรวจจับควันไฟความไวสูง (High Sensitivity Smoke Detector System) - ระบบควบคุมการเข้าออก (Access Control System) - ระบบตรวจจับการั่วของน้ำ (WaterLeak Detection System)	1	งาน	1,500,000.00	1,500,000.00
		REMARK : ราคารวม Vat 7%			TOTAL	7,100,000.00

จำนวนเงิน (BAHT) : เจ็ดล้านหนึ่งแสนบาทถ้วน

Terms and Conditions

Price Validity	Payment Term	Delivery Date	Type
30 Days	*Credit 30 Days*	*30 Days*	*HW & Service*

Purchase approved in accordance with this quotation
(อนุมัติสั่งซื้อตามใบเสนอราคานี้)

( )

Purchaser Authorized Signature & Sale
ลงนามผู้มีอำนาจในการสั่งซื้อ

Best Regards,

อมรรัตน์ ทิพยาช

(Miss. Amonrat Tipparat)
Sales Manager
ti_amonrat@kmit-group.com
(Mobile : 099-2870839)