**แบบรายละเอียดการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง**
**ด้านเทคโนโลยีสารสนเทศ**
**ระยะเวลาการดำเนินงาน 1 ตุลาคม 2563 - 30 กันยายน 2564**

| ประเด็นความเสี่ยง | แนวทาง/กิจกรรม การจัดการความเสี่ยง | ประเมินผล การควบคุม | การปรับปรุง การควบคุม | ระยะเวลาการดำเนินงาน | ตรวจสอบติดตาม |
|---|---|---|---|---|---|
| GOI105 : เกิดปัญหาด้านข้อมูลสารสนเทศ เช่นไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน | 1. มีการตรวจสอบ กำกับ ติดตาม | • ยังมีการบันทึกข้อมูลที่ผิดพลาด | 1.แนะนำการบันทึกข้อมูลให้ถูกต้อง ครบถ้วน แล้วกำกับติดตาม | 1ครั้ง/สัปดาห์ | งานประกันสุขภาพฯ |
| GPS101 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure) | 1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล<br>2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ | • ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและมีการสำรองฐานข้อมูล<br>• ตรวจสอบการทำงานอุปกรณ์เครือข่าย | 1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล<br>2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ | 1ครั้ง/สัปดาห์<br>1ครั้ง/สัปดาห์ | งานประกันสุขภาพฯ |
| GPS102 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure) | 1. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ<br>2. มีการตรวจสอบ กำกับ ติดตาม | • ยังไม่ตระหนักถึงภัยด้านความมั่นคงปลอดภัยไซเบอร์<br>• ไม่ออกจากระบบเมื่อไม่มีการใช้งานอินเทอร์เน็ต | 1. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม<br>2. มีการตรวจสอบ กำกับ ติดตาม | 1 ครั้ง/ปี<br>1ครั้ง/สัปดาห์ | งานประกันสุขภาพฯ |
| GPS103 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure) | 1. ตรวจสอบการทำงานของระบบเครือข่ายอย่างสม่ำเสมอ | • ตรวจสอบการทำงานอุปกรณ์เครือข่าย | 1. ตรวจสอบการทำงานของระบบเครือข่ายอย่างสม่ำเสมอ | 1ครั้ง/สัปดาห์ | งานประกันสุขภาพฯ |
| GPS104 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) | 1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูลอย่างสม่ำเสมอ | • ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและมีการสำรองฐานข้อมูล | 1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูลอย่างสม่ำเสมอ | 1ครั้ง/สัปดาห์ | งานประกันสุขภาพฯ |

| | | | | | |
|---|---|---|---|---|---|
| ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure | 2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงภัยด้านความมั่นคงปลอดภัยไซเบอร์ | 2. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม | 1 ครั้ง/ปี | |
| GOI102 : เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มีการเข้าถึงโดยผู้ไม่มีสิทธิ์ | 1. ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการอินเทอร์เน็ต<br>2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ<br>3. ดำเนินการตามระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานลาออก โอน ย้าย หรือสิ้นสุดการจ้าง ให้หน่วยงานแจ้งผู้ดูแลระบบทันทีเพื่อปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานให้เป็นปัจจุบัน | • ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการอินเทอร์เน็ต<br>• ตรวจสอบการทำงานอุปกรณ์เครือข่าย<br>• ตรวจสอบสิทธิในการเข้าถึงข้อมูลระบบ | 1. ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการอินเทอร์เน็ต<br>2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ<br>3. ดำเนินการตามระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยฯ | 1ครั้ง/วัน<br>1ครั้ง/วัน<br>ทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งาน | งานประกันสุขภาพฯ |
| GPS105 : เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ | 1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>• ยังไม่ตระหนักถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | 1. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GPS106 : เกิดอุบัติการณ์ความละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอกที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ | 1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>• ยังไม่ตระหนักถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | 1. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |

| | | | | | |
|---|---|---|---|---|---|
| GPS203 : บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก | 1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>2. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>• ยังไม่ตระหนักถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | 1. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GPS204 : เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง | 1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>• ยังไม่ตระหนักถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | 1. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GPS201 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่ | 1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>• ยังไม่ตระหนักถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | 1. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GPS202 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่ | 1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล<br>• ยังไม่ตระหนักถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | 1. เจ้าหน้าที่ศึกษานโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพิ่มเติม | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GOI101 : เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี - เทคนิค | 1. จัดหาคอมพิวเตอร์และอุปกรณ์สำรองที่สามารถใช้ทดแทนได้ทันที สามารถปฏิบัติงาน ได้อย่างต่อเนื่อง | • มีคอมพิวเตอร์และอุปกรณ์สำรอง ที่สามารถใช้ทดแทนได้ทันที | 1. จัดหาคอมพิวเตอร์และอุปกรณ์สำรอง ที่สามารถใช้ทดแทนได้ทันที สามารถปฏิบัติงาน ได้อย่างต่อเนื่อง | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |

| | | | | | |
|---|---|---|---|---|---|
| | 2. ตรวจสอบ บำรุงรักษาคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ | • มีการบำรุงรักษาคอมพิวเตอร์และอุปกรณ์ | 2. ตรวจสอบ บำรุงรักษาคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ | 3เดือน/ครั้ง | |
| GOI103 : เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค | 1. จัดหา Software เตรียมพร้อมไว้สำหรับการใช้งาน | • มี Software เตรียมพร้อมไว้สำหรับการใช้งาน | 1. จัดหาSoftware เตรียมพร้อมไว้สำหรับการใช้งาน | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GOI104 : เกิดปัญหาด้านUser&IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ | 1. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | • ยังไม่ตระหนักถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ | 1. เจ้าหน้าที่ศึกษาคู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ใช้งาน)/คู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ดูแลระบบ) | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GOI201 : เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ,ขาดการตรวจสอบหรือสอบทาน | 1. สร้างเครื่องมือในการกำหนดทะเบียนคุม/เอกสารหลักฐานกำกับ | • มีทะเบียนคุม/เอกสารหลักฐาน | 1. คู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ใช้งาน)/คู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ดูแลระบบ) | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GOI202 : เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุมการแจกจ่าย/การจำหน่าย | 1. สร้างเครื่องมือในการกำหนดทะเบียนคุม/เอกสารหลักฐานกำกับ | • มีทะเบียนคุม/เอกสารหลักฐาน | 1. คู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ใช้งาน)/คู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ดูแลระบบ) | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |
| GOI203 : เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตาม | 1. สร้างเครื่องมือในการกำหนดทะเบียนคุม/เอกสารหลักฐานกำกับ | • มีทะเบียนคุม/เอกสารหลักฐาน | 1. คู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ใช้งาน)/คู่มือการ | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |

| | | | | | |
|---|---|---|---|---|---|
| มาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้ | | | ปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ดูแลระบบ) | | |
| GOI106 : เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร,ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน,ขาดการติดตามประเมินผลการสื่อสาร | 1. จัดทำคู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ใช้งาน) | • เจ้าหน้าที่เข้าใจขั้นตอนการสื่อสารตามคู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ(สำหรับผู้ใช้งาน) | 1. เจ้าหน้าที่ศึกษาคู่มือการปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ (สำหรับผู้ใช้งาน) เพิ่มเติม | 1 ครั้ง/ปี | งานประกันสุขภาพฯ |

ลงชื่อ.....ผู้รายงาน
(นางสาวจุฑารัตน์ โอวาท)
นักวิชาการคอมพิวเตอร์

ลงชื่อ.....ผู้เห็นชอบ
(นางสาวธัณย์จิรา ปัญโญพิพัฒณ์)
นักวิชาการสาธารณสุข ชำนาญการ

ลงชื่อ.....ผู้อนุมัติ
(นายจิระวัตร วิเศษสังข์)
ผู้อำนวยการโรงพยาบาลเมือจันทร์