แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(IT Contingency Plan) โรงพยาบาลหนองหงส์ ปีงบประมาณ พ.ศ. ๒๕๖๔-๒๕๖๕

หลักการและเหตุผล

ปัจจุบันหน่วยงานราชการได้นำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้นข้อมูลสารสนเทศถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการจำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัยสามารถนำไปใช้ประโยชน์ในการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานชองบุคลากรในหน่วยงานชิ่งข้อมูลสารสนเทศต่างๆ มีจำนวนเพิ่มมากขึ้นตลอดเวลา ดังนั้นองค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเต่าระวัง การจัดเก็บและการ ดูแลรักษาข้อมูลสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลาโรงพยาบาลหนองหงส์ได้ตระหนักถึงความสำคัญ ของระบบเทคโนโลยีสารสนเทศขององค์กรชิ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศรวมทั้งระบบอุปกรณ์ต่างๆ เสียหายได้โรงพยาบาลจึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)ปีงบประมาณ พ.ศ. ๒๕๖๔-๒๕๖๕ เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศรวมถึง ระบบอุปกรณ์ต่างๆ

วัตถุประสงค์

๑. เพื่อสร้างความเข้าใจร่วมดันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของ ระบบเทคโนโลยีสารสนเทศขององค์กร
๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ
๓. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ องค์กร ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
๔. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถ แก้ไขสถานการณ์ได้อย่างทันท่วงที
๕. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร

ภัยพิบัติ

ภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลหนองหงส์สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่
๑. ภัยพิบัติจากภายนอก
๑.๑ ภัยธรรมชาติ ที่กระทำต่ออาคาร สถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น
๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
๑.๓ ระบบการเชื่อมโยงเครือข่ายเกิดความขัดข้อง
๑.๔ ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ
๑.๔ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
๑.๖ ไวรัสคอมพิวเตอร์
๑.๗ ระบบเสียหายจากสถานการณ์ความไม่สงบเรียบร้อย เหตุจลาจล การชุมนุมประท้วงฯ

๒. ภัยพิบัติจากภายใน

๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๓ เจ้าหน้าที่ หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ

๑. ภัยพิบัติจากภายนอก

๑.๑ ภัยธรรมชาติที่กระทำต่ออาคาร สถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยและการฟ้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

๑.๑.๑ การป้องกันและการดำเนินการเมื่อเกิดอัคคีภัย

(๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ

(๒) อบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิง การหนีไฟ ขั้นต้นให้แก่เจ้าหน้าที่ทุกราย

(๓) ระบบควบคุมความชื้นและแจ้งเตือนอุณหภูมิ ห้องคอมพิวเตอร์แม่ข่าย

(๔) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์ สำหรับห้อง คอมพิวเตอร์แม่ข่าย

(๕) จัดทำเครื่องหมายระบุความสำคัญตามลำดับ ของอุปกรณ์คอมพิวเตอร์ และอุปกรณ์จัดเก็บข้อมูล เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิด เหตุฉุกเฉิน

(๖) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออก ภายนอกตัวอาคาร ให้ผู้ที่สามารถใช้งานเครื่องดับเพลิงได้ ใช้เครื่อง ดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

(๗) แจ้งเหตุงานรักษาความปลอดภัย โรงพยาบาลหนองหงส์

(๘) หากไม่สามารถควบคุมไฟได้ จะต้องเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ และอุปกรณ์จัดเก็บข้อมูลสำคัญตามลำดับ ออกภายนอกตัวอาคาร

(๙) หากเกิดไฟไหมในขณะที่ไม่มีผู้ปฏิบัติงานแล้วปรากฏว่าอุปกรณ์ต่างๆ ชำรุดเสียหายให้รีบดำเนินการจัดซ่อมหรือ จัดหาอุปกรณ์ต่างๆ มาเพื่อให้ การปฏิบัติงานดำเนินต่อไปได้

(๑๐)หากระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งงานประชาสัมพันธ์ กด ๑๐๓ เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลหนองหงส์ทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไขเพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง

(๑๑)รายงานผู้บังคับบัญชาตามสำดับขั้นได้แก่หัวหน้าสำนักงานสารสนเทศและคอมพิวเตอร์ประธานคณะกรรมการพัฒนาระบบสารสนเทศและคอมพิวเตอร์และผู้อำนวยการโรงพยาบาลหนองหงส์ ตามสำคับ

๑.๑.๒ การป้องกันอุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม

(๑) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น สำหรับเครื่องแม่ข่ายตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงาน ให้ใช้งานได้อย่างสม่ำเสมอ

(๒) ตรวจสอบการรั่วซึมของอาคารเพื่อป้องกันการรั่วซึมของน้ำที่ค้างสะสม

(๓) ห้องคอมพิวเตอร์แม่ข่ายต้องไม่ตั้งอยู่ในบริเวณที่น้ำท่วมถึง

(๔) หากเกิดน้ำท่วมถึงห้องคอมพิวเตอร์แม่ข่ายหลัก ชั้น อาคารOPD ให้ผู้ปฏิบัติงานปิดระบบและทำการเคลื่อนย้ายอุปกรณ์สำคัญต่างๆที่ยังสามารถใช้งานได้ไปติดตั้งที่ห้องแม่ข่ายสำรอง อาคารตึกสงฆ์ โรงพยาบาลหนองหงส์

(๕) นำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

(๖) ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือ จัดหาทดแทน เพื่อให้สามารถดำเนินการได้ (๗) หากระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งงานประชาสัมพันธ์ กด ๑๐๓ เพื่อประกาศให้ทุกหน่วยงานใน สังกัดของโรงพยาบาลหนองหงส์ทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้กำลังดำเนินการแก่ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง

(๘) รายงานผู้บังคับบัญชาตามสำคับขั้นได้แก่หัวหน้าสำนักงานสารสนเทศและคอมพิวเตอร์ประธานคณะกรรมการ พัฒนาระบบสารสนเทศและ คอมพิวเตอร์ และผู้อำนวยการโรงพยาบาลหนองหงส์ ตามสำคับ

๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๒.๑ ควบคุมการเข้าออก ห้องคอมพิวเตอร์แม่ข่าย และป้องกันความเสียหายโดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าโปในห้องคอมพิวเตอร์แม่ข่ายหากจำเป็นให้มีเจ้าหน้าที่ของสำนักงานสารสนเทศและคอมพิวเตอร์เป็นผู้รับผิดชอบ นำเข้าไป

๑.๒.๒ จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตนด้วยลายนิ้วมือ (Finger Scan) และมีการตรวจสอบการ ทำงานของระบบให้ใช้งานได้อยู่เสมอ

๑.๒.๓ ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพของผู้ดูแลรับผิดขอบ

๑.๒.๔ หากเก็ดการโจรกรรม ให้แจ้งผู้บังคับบัญชาตามสำดับขั้นให้ทราบโดยด่วน

๑.๒.๕ แจ้งงานรักษาความปลอดภัย โรงพยาบาลหนองหงส์

๑.๒.๖ สำรวจตรวจสอบรายการทรัพย์สินที่สูญหายรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เติมและนำข้อมูลที่ได้สำรองไว้ผู้คืนให้ผู้ปฏิบัติงาน สามารถใช้งานระบบงานต่างๆ ได้โดยเร็ว

๑.๒.๗ หากระบบคอมพิวเตอร์มีสามารถใช้งานได้ตามปกติให้แจ้งงานประขาสัมพันธ์ กด ๑๐๓ เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลหนองหงส์ทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้กำลังดำเนินการแก้ไขเพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการตามแผน ของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง

๑.๒.๘ รายงานผู้บังคับบัญชาตามลำดับขั้น ได้แก่ หัวหน้าสำนักงานสารสนเทศและคอมพิวเตอร์ ประธานคณะกรรมการพัฒนาระบบสารสนเทศและคอมพิวเตอร์ และผู้อำนวยการโรงพยาบาลหนองหงส์ตามลำดับ

๑.๓ การเชื่อมโยงระบบเครือข่ายเกิดความขัดข้อง

๑.๓.๑ การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ ตลอดเวลา และมีระบบเครือข่ายสำรอง

๑.๓.๒ ต้องจัดให้มีเครื่องแม่ข่ายสำรอง สำหรับใช้ในกรณีที่เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้

๑.๓.๓ ดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหาหากสายเคเบิลขาด เพื่อดำเนินการ ซ่อมแซมสายเคเบิลให้เสร็จเรียบร้อยโดยเร็ว

๑.๓.๔ หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคารให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ Core Switch ทีติดตั้งอยู่ ณ อาคารนั้นๆ

๑.๓.๕ หากระบบคอมพิวเตอร์ไม่สามานรถใช้งานได้ตามปกติให้แจ้งงานประชาสัมพันธ์ กด ๑๐๓ เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลหนองหงส์ทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วย ให้บริการตามแผน ของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง

๑.๓.๖ ดำเนินการตรวจสอบจุดที่มีปัญหาพร้อมทำการแก้ไข โดยใช้เวลาน้อยที่สุด

๑.๓.๗ รายงานผู้บังคับบัญชาตามลำดับขั้น ได้แก่ หัวหน้าสำนักงานสารสนเทศและคอมพิวเตอร์ ประธานคณะกรรมการ พัฒนาระบบสารสนเทศและคอมพิวเตอร์ และผู้อำนวยการโรงพยาบาลหนองหงส์ ตามสำคับ

๑.๔ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าคับ

๑.๔.๑ แยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายไฟหลักที่ผ่านสะพานไฟเข้าสู่ หน่วยงาน และมีระบบไฟฟ้าสำรอง (Generator)

๑.๔.๒ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงคันอัตโนมัติ (UPS) เพื่อป่องคันความ เสียหายที่อาจเกิดขึ้นกับอุปกรณ์เครื่อง คอมพิวเตอร์แม่ข่าย (Server) ซึ่งต้องมี ระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที และเครื่องคอมพิวเตอร์ ส่วนบุคคล (PC) ต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๑๔ นาที

๑.๔.๓ เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้ อยู่ในสภาพพร้อมใช้งานเสมอ

๑.๔.๔ ดำเนินการปิดระบบคอมพิวเตอร์แม่ข่าย (Server) เพื่อฟ้องกันความเสียหายใน กรณีที่เครื่องสำรองไฟฟ้าและปรับแรงคันอัตโนมัติ (UPS) เครื่องแม่ข่ายและ ระบบไฟฟ้าสำรองไฟฟ้า (Generator) มีปัญหา

๑.๔.๔ เมื่อเกิดกระแสไฟฟ้าคับ ให้ผู้ใช้งานเครื่องคอมพิวเตอร์บันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่างๆ

๑.๔.๖ หากระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งงานประขาสัมพันธ์ กด ๑๐๓ เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการตามแผนของแต่ละหน่วยงาน สำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง

๑.๔.๗ รายงานผู้บังคับบัญชาตามลำดับขั้น ได้แก่ หัวหน้าสำนักงานสารสนเทศและคอมพิวเตอร์ ประธานคณะกรรมการพัฒนาระบบสารสนเทศและคอมพิวเตอร์ และผู้อำนวยการโรงพยาบาลหนองหงส์ ตามลำดับ

๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๑.๔.๑ สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อนโดยใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว

๑.๔.๒ ติดตั้ง Firewall เพื่อป่องคันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้อง เป็ดใช้งาน Firewall ตลอดเวลา

๑.๔๓.จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขององค์กรเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบเทคโนโลยีสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะใต้สรุปหาสาเหตุ และปองกันต่อไปติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัยและอัพเดทอย่างสม่ำเสมอและปิดพอร์ตที่ไม่มีการใช้งาน

กำหนดรหัสฝานเพื่อป้องกันการเข้าอิงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติดังนี้

(๑) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๒) ไม่เป็ดเผยรหัสผ่านของตนเองแก่ผู้อื่น

(๓) จัดเก็บรหัสผ่านไว้ ในสถานที่ที่มีความปลอดภัย

(๔) เปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเป็ดเผย หรือล่วงรู้โดยผู้อื่น

(๕) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย ๘ อักขระ

(๖) ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้ กำหนดไว้
(๗) ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม
(๘) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓, abed เป็น ต้น หรือเป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑๑๑, aaa, bbb เป็นต้น
(๙) เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกๆ ๖ เดือน ส่วนในกรณีของผู้ดูแลระบบ ให้เปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่ มากกว่ายูใช้งานทั่วไป เช่น ทุกๆ ๓ เดือน
(๑๐) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว
(๑๑)เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ ระบบงาน
(๑๒) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้บนหน้าจอล็อกอิน (ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอิน ในภายหลังจะได้ ไม่ต้องใส่รหัสผ่านอีกครั้ง)
(๑๓) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
(๑๔) หลีกเลียงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน ป้องกันการปลอมแปลง IP address โดยการกรอง Packet ที่มาจากภายนอก โดยการนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ

๑.๕.๘ หากเกิดการบุกรุกหรือโจมตีจากภายนอกแล้วระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งงานปะชาสำพันธ์ กด ๑๐๓ เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้กำลัง เพื่อให้หน่วยงานที่ต้องให้บริการกับ ผู้ป่วยให้บริการตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ ขัดข้อง
๑.๕.๙ รายงานผู้บังคับบัญชาตามลำดับขั้น ได้แก่ หัวหนาสำนักงานสารสนเทศและคอมพิวเตอร์ ประธานคณะกรรมการพัฒนาระบบสารสนเทศและคอมพิวเตอร์ และผู้อำนวยการโรงพยาบาลหนองหงส์ตามสำคับ
๑.๕.๑๐ แจงบริษัทภายนอกที่เกี่ยวข้องเพื่อดำกานในการตรวจสอบแก้ไขเช่นระบบ PACS ,LAB และ his ฯลฯ

๑.๖ ไวรัสคอมพิวเตอร์

๑.๖.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้ โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง
๑.๖.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ
(๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
(๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย
(๓) ไมใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา
๑.๖.๓ ใช้ความระมัดระวัง,ในการเปิด E-mail
(๑) ไม่เปิดไฟล์ E-mailที่ไม่ทราบแหล่งที่มา
(๒) ลบ E-mail ทิ้งทันทีไม่ทราบแหล่งที่มา
๑.๖.๔ ระมัดระวังการดาวโหลดไฟล์ต่างๆ จากอินเทอร์เน็ต
(๑) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมาคับโปรแกรมสนทนาต่างๆ
(๒) ไม่ควรเปิด Website ที่แนะนำมาทาง E-mail
(๓) ไม่ดาวโหลดไฟล์จาก Website ที่ไม่น่าเชื่อถือ
(๔) ติดตามข้อมูลการแจงเตือนการโจมตีของไวรัสต่างๆอย่างสม่ำเสมอ
(๕) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๑.๖.๕ กรณีถูกไวรัสบุกรุกเพื่อจำกัดความเลียหายที่อาจแพร่กระจายไปยังเครื่องอื่นใน ระบบเครือข่าย ให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

๑.๖.๖ ดำเนินการป้องคันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัสตรวจสอบและติดตามเครื่องที่ติดไวรัสและ ดำเนินการแก้ไข กรณีที่ทำให้ระบบ คอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ ให้แจ้งงานประชาสัมพันธ์ กด ๑๐๓ เพื่อประกาศให้ทุกหน่วยงานในสังกัดทราบว่าระบบ คอมพิวเตอร์ไม่สามารถใช้การได้กำลังดำเนินการแล้

๑.๖.๗ รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ หัวหน้าลำนักงานสารสนเทศและคอมพิวเตอร์ ประธานคณะกรรมการพัฒนาระบบสารสนเทศและคอมพิวเตอร์ และผู้อำนวยการโรงพยาบาลหนองหงส์ ตามลำดับ

๑.๖.๘ แจ้งบริษัทภายนอกที่เกี่ยวข้องเพื่อดำเนินการตรวจสอบ เช่น ระบบ PACS ,LAB และHIS ฯลฯ

๑.๗ ระบบเสียหายจากสถานการณ์ความไม,สงบเรียบร้อย เช่น เหตุจลาจล การชุมนุมประท้วง เนื่องจากเป็นภัยจากป้จจัยภายนอกที่ไม่สามารถยับยั้งได้ ในการป้องกัน หากไม'สามารถย้าย สถานที่หรือป้องกันสถานที่ได้ ควรมีการ Back Up ข้อมูลไว้มากกว่า Back Up และแยก สถานที่จัดเก็บ และถ้าเกิดความเสียหายขึ้นคับข้อมูล ก็สามารถน่าข้อมูลที่มีการ Back Up ไว้ และอุปกรณ์คอมพิวเตอร์ ลำรองมาใช้แทนได้ทันทีหากเกิดสถานการณ์ความไม่สงบเรียบร้อยให้ปฏิบัติดังนี้

๑.๗.๑ กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ให้ผู้รับผิดชอบ Remote เข้ามาเพื่อ ตรวจสอบการทำงานของระบบหากพบว่าระบบไม่สามารถดำเนินการได้ ตามปกติ จะดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

๑.๗.๒ รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ หัวหน้าสำนักงานตามลำดับ

๑.๗.๓ หลังเหตุการณ์ความไม่สงบ ตรวจสอบรายการทรัพย์สิน ตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ดำเนินการบำรุงรักษาและซ่อมแซมเพื่อให้กลับสู่สภาวะปกติโดยเร็วที่สุดภัยพิบัติจาภายใน

๒.ภัยพิบัติจากภายใน

๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๑.๑ การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรอง ข้อมูลไว้ในเครื่องคอมพิวเตอร์แม่ข่ายซึ่งทำหน้าที่สำรองข้อมูลกลางทุกวัน และจะส่งข้อมูลไปไว้ที่เครื่องคอมพิวเตอร์ห้องแม่ข่ายสำรอง

๒.๑.๒ การลำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ สำรองข้อมูล ตามระยะเวลาที่กำหนดทุกสัปดาห์ โดยจะสำรองข้อมูล โครงสร้างข้อมูล Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๒.๑.๓ ทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการที่ได้สำรองไว้ใน เครื่องคอมพิวเตอร์ห้องแม่ข่ายอย่างสม่ำเสมอทุกระบบ อย่างน้อยปีละ ๒ ค?ง

๒.๑.๔ ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการของเครื่องแม่ข่าย ลำรองที่ได้ลำรองไว้อย่างน้อยปีละ ๒ ครั้ง เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

๒.ภัยพิบัติจากภายใน

๒.๑ ระบบแม่ข่ายหลักระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๑.๑ การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในเครื่องคอมพิวเตอร์แม่ข่ายซึ่งทำหน้าที่สำรองข้อมูลกลางทุกวัน และจะส่งข้อมูลไปไว้ที่เครื่องคอมพิวเตอร์ห้องแม่ข่ายลำรอง อาคารตึกสงฆ์

๒.๑.๒ การลำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ สำรองข้อมูล ตามระยะเวลาที่กำหนด ทุกสัปดาห์ โดยจะสำรองข้อมูล โครงสร้างข้อมูล Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๒.๑.๓ ทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการที่ได้สำรองไว้ในเครื่องคอมพิวเตอร์ห้องแม่ข่ายอย่างสม่ำเสมอทุกระบบ อย่างน้อยปีละ ๒

ขั้นตอนการปฏิบัติในมาตรการที่สำคัญ

๑. การสำรองข้อมูล (Back Up)

๑.๑ การสำรองข้อมูลอัตโนมัติ โดยสำรองข้อมูลไจ้ที่เครื่องคอมพิวเตอร์แม่ข่ายซึ่งทำหน้าที่สำรองข้อมูลกลางทุกวัน

๑.๒ การสำรองข้อมูลอัตโนมัติ โดยสำรองข้อมูลไว้ที่เครื่องคอมพิวเตอร์ห้องแม่ข่ายสำรอง อาคารตึกสงฆ์

๒. การกู้ข้อมูล (Recovery)

๒.๑ ทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการที่ได้สำรองไว้ในเครื่องคอมพิวเตอร์ห้องแม่ข่าย อย่างสม่ำเสมอทุกระบบอย่างน้อยปีละ ๒ ครั้ง

๒.๒ ทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการที่ได้สำรองไว้ในเครื่องคอมพิวเตอร์ ห้องแม่ข่ายสำรอง อาคารตึกสงฆ์ อย่างสม่ำเสมอทุกระบบอย่างน้อยปีละ ๒ ครั้ง

ข้อปฏิบัติในการแก้ปัญหาจากสถานการณ์ฉุกเฉิน

๑. กรณีเครื่องลูกข่าย

๑.๑ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศ ได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบเพื่อดำเนินการแก้ไข

๑.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ติงสายเชื่อมโยงระบบเครือข่าย (LAN) ออก จากเครื่องโดยเร็ว

๑.๓ ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง

๑.๔ ให้เจ้าหน้าที่ที่เกี่ยวข้องแจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

๒. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๒.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็วแล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญ ของการให้บริการ

๒.๒ ล้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณา ตามความสำคัญของการ ให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรอง ไฟฟ้า

๒.๓ ปดระบบจ่ายไฟในกรณีไฟไหม้ ให้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๒.๔ รีบขนย้ายเครื่องไปไวในที่ปลอดภัย ตามสำดับความสำคัญ

๒.๕ประสานขอความช่วยเหลือภัยผู้เชี่ยวชาญที่รับผิดขอบดูแลระบบคอมพิวเตอร์แม่ข่าย (Server)และระบบเครือข่าย (Network) โดยเร็วที่สุด

๒.๖ ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็ว ที่สุด

๒.๗ ผู้ดูแลระบบต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

๓. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

๓.๑ เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๓.๒ สแกนและกำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

๓.๓ แจ้งเจ้าหน้าที่ที่เกี่ยวข้องเพื่อตรวจสอบ

๔. หลักปฏิบัติของบุคลากรในการฟ้องคันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคารและบุคลากรสามารถปฏิบัติตนได้ ถูกต้องเมื่อเกิดอัคคีภัยจึงกำหนดหลักปฏิบัติ ดังนี้

๔.๑ ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๔.๒ ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์ เกี่ยวกับความปลอดภัยจากเพลิงไหม้ และการหนีไฟอย่างละเอียด

๔.๓ ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉิน มิให้ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัยให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเองไปยังทางออกฉุกเฉินเพื่อให้ไปถึงทางได้แม้ว่าไฟดับ หรือ ปกคลุมไปด้วยควัน

๔.๔ เมื่อเกิดเพลิงไหมิให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้จากนั้น ออกจากอาคารแล้วแจ้ง หน่วยดับเพลิงทันที

๔.๕ เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ให้รีบหาทางหนีออกจากอาคารทันที

๔.๖ หากเพลิงไหม้ในห้องทำงานให้ออกจากห้อง เปิดประตู แล้วแจ้งฝ่ายอาคารและสถานที่เพื่อ แจ้งหน่วยดับเพลิงทันที

๔.๗ หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงานก่อนออกจากอาคารให้วางมือบนประตูหากประตูมีความเย็นอยู่ค่อยๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

๔.๘ หากเพลิงไหม้อยู่บริเวณใกล้ประตูจะมีความร้อนห้ามเปิดประตูโดยเด็ดขาดให้รบแจ้งหน่วยดับเพลิงและแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้หาผ้าเปียกปิดทางเข้าของควันปิดพัดลมและเครื่องปรับอากาศ

๔.๙ เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

๕. ระบบป้องกันและแก่ไขปัญหาที่เกิดจากกระแสไฟฟ้าเนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย คอมพิวเตอร์ส่วนใหญ่มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับมากดังนั้นสิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือผลกระทบต่างๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญรวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้าประกอบด้วย

๔.๑ เป็ดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาเปิดใช้งานทั้งเครื่องคอมพิวเตอร์ แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๔.๒ เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติ

การคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ เครือข่ายต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆได้ตลอดเวลา ๒๔ ชั่วโมงหากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุดเพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการ ดังนี้

๑. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน

๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๔. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้เป็นการชั่วคราว

๕. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง

๖. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบ

หน้าที่ความรับผิดขอบของเจ้าหน้าที่สำนักงานสารสนเทศและคอมพิวเตอร์โรงพยาบาลหนองหงส์ดังต่อไปนี้

๑. รับผิดขอบในการกำหนดนโยบาย ให้ข้อเสนอแนะคำปรึกษาตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑ แพทย์วิมลพรรณ อาจสม ผู้อำนวยการ โรงพยาบาลหนองหงส์

๒. รับผิดชอบงานฐานข้อมูล แม่ข่าย และ Software ได้แก่

๒.๑ นายณัฐวัฒณ์ เหมือยไธสง นักวิชาการสาธารณสุขชำนาญการ

๒.๒ นางสมิตรา สงวนเชื้อ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๒.๓ นายอาณัติ สีหะวงษ์ นักวิชาการคอมพิวเตอร์

๓. รับผิดชอบงานช่างเทคนิคคอมพิวเตอร์ และNetwork

๓.๑ นายณัฐวัฒณ์ เหมือยไธสง นักวิชาการสาธารณสุขชำนาญการ

๓.๒ นางสมิตรา สงวนเชื้อ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๓.๓ นายอาณัติ สีหะวงษ์ นักวิชาการคอมพิวเตอร์

๔. รับผิดชอบงานด้าน Website

๔.๑ นายณัฐวัฒณ์ เหมือยไธสง นักวิชาการสาธารณสุขชำนาญการ

๔.๒ นางสมิตรา สงวนเชื้อ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๔.๓ นายอาณัติ สีหะวงษ์ นักวิชาการคอมพิวเตอร์

๕. รับผิดชอบงานด้านบริการข้อมูล รายงานสารสนเทศ

๕.๑ นายณัฐวัฒณ์ เหมือยไธสง นักวิชาการสาธารณสุขชำนาญการ

๕.๒ นางสมิตรา สงวนเชื้อ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๕.๓ นายอาณัติ สีหะวงษ์ นักวิชาการคอมพิวเตอร์

การทบทวนและปรับปรุงแผน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องได้รับการปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคลองกับการใช้งานตามภารกิจตามที่ระบุอย่างน้อยปีละ ๑ ครั้ง

การติดตามและรายงานผล

กำหนดให้ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้หัวหน้าสำนักงานสารสนเทศและคอมพิวเตอร์ทราบเป็นประจำทุกเดือน เพื่อรายงานสรุปให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) ทราบและหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดชองหน่วยงาน ทราบทันที

ลงชื่อ ..... ผู้เสนอแผน
(นายอาณัติ สีหะวงษ์)
นักวิชาการคอมพิวเตอร์

ลงชื่อ ..... ผู้ตรวจสอบ
(นายณัฐวัฒณ์ เหมือยไธสง)
หัวหน้ากลุ่มงานประกันสุขภาพและเทคโนโลยีสารสนเทศทางการแพทย์

ลงชื่อ ..... ผู้อนุมัติแผน
(แพทย์หญิงวิมลพรรณ อาจสม)
ผู้อำนวยการโรงพยาบาลหนองหงส์