แผนบริหารความเสี่ยง

ของระบบฐานข้อมูลและสารสนเทศ

และแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ

(Contingency Plan)

สำนักงานสาธารณสุขจังหวัดสุรินทร์

ประจำปีงบประมาณ 2552

ศูนย์เทคโนโลยีสารสนเทศ

สำนักงานสาธารณสุขจังหวัดสุรินทร์

ถนนกรุงศรีนอก อำเภอเมือง จังหวัดสุรินทร์ 32000

สารบัญ

การทบทวนแผนบริหารความเสี่ยงและแผนการแก้ไขปัญหาจากภัยพิบัติที่อาจเกิดกับ

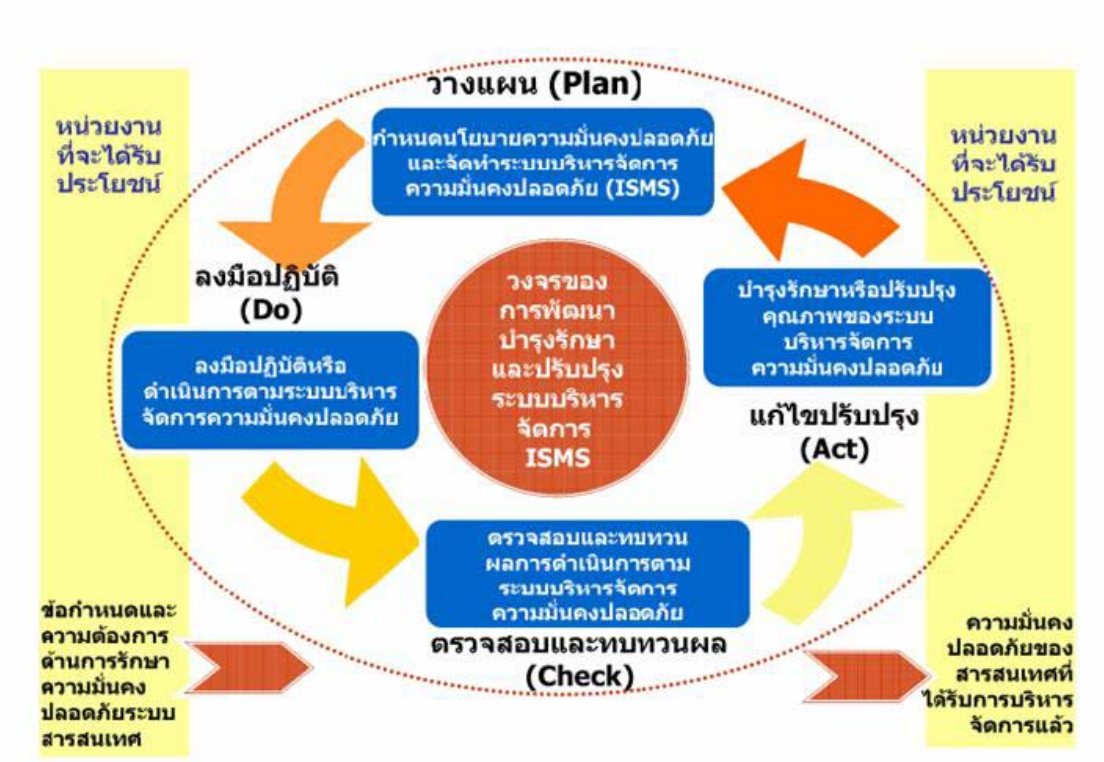
ระบบฐานข้อมูลและสารสนเทศ(Contingency Plan)

สำนักงานสาธารณสุขจังหวัดสุรินทร์ ปี 2552

1. หลักการและเหตุผล

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงของหน่วยงาน ที่อาจเกิดขึ้นในระบบบริหารงาน

จึงได้จัดทบทวนแผน ปี 2552 โดยอ้างอิงมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิคส์ (เวอร์ชั่น 2.5) ประจำปี 2550 แนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan-Do-Check-Act หรือ P-D-C-A มาประยุกต์ใช้ ตามแสดงในรูป



แผนภาพแสดงวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน P-D-C-A

2. สถานภาพของระบบสารสนเทศของสำนักงานสาธารณสุข (PLAN)

2.1 การดำเนินงานจัดทำระบบสารสนเทศของสำนักงานสาธารณสุขจังหวัดสุรินทร์

สำนักงานสาธารณสุขจังหวัดสุรินทร์ โดยศูนย์เทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำระบบสารสนเทศของจังหวัด โดยทำโครงการพัฒนาระบบข้อมูลสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข ขอให้สำนักงานสาธารณสุขจังหวัดดำเนินการจัดตั้งระบบเครือข่ายภายในจังหวัดและเชื่อมโยงผ่านระบบเครือข่ายการสื่อสาร (ATM) กระทรวงมหาดไทย ความละเอียดแจ้งอยู่แล้วตามหนังสือที่อ้างถึง และแนบท้ายนี้

1. หนังสือสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ 0235/4/182 ลงวันที่ 26 พฤษภาคม 2543
2. หนังสือสำนักเทคโนโลยีสารสนเทศ ที่ สธ 0235/4/ว 7 ลงวันที่ 31 สิงหาคม 2543

เมื่อวันที่ 2 ธันวาคม 2545 รัฐมนตรีว่าการกระทรวงสาธารณสุขได้กำหนดนโยบายเร่งด่วนในการดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสารประจำปี 2546 พร้อมกำหนดให้หน่วยงานดำเนินการดังต่อไปนี้

1. การเชื่อมโยงแบบ Broadband จากสำนักงานสาธารณสุขจังหวัดทุกแห่งมายังหน่วยงานสื่อสารของกระทรวงมหาดไทยระดับจังหวัด ให้แล้วเสร็จภายในเดือนมกราคม 2546
2. การเชื่อมโยงแบบ Broadband จากโรงพยาบาลศูนย์ /ทั่วไปทุกแห่งมายังหน่วยสื่อสารของกระทรวงมหาดไทยระดับจังหวัด ให้แล้วเสร็จภายในเดือนมีนาคม 2546
3. สำนักงานสาธารณสุขจังหวัด โรงพยาบาลศูนย์/ทั่วไปทุกแห่ง ดำเนินการ
   3.1 ติดตั้ง Linux Server อย่างน้อย 1 เครื่อง เพื่อทำหน้าที่เป็น Digital Nervous Center ระดับจังหวัดและเป็นที่ติดตั้งฐานข้อมูล Minimum Dataset
   3.2 ตั้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นการภายในโดยมีบุคลากรรับผิดชอบเป็นการประจำอย่างน้อยศูนย์ฯ ละ 3 คน เพื่อการติดตั้งเชื่อมโยงระบบเครือข่าย และติดตั้งและดูแลฐานข้อมูล Minimum Dataset ทั้งนี้ สำนักงานปลัดกระทรวงจะเร่งดำเนินการเรื่องการกำหนดสายงานใหม่ เพื่อรองรับความก้าวหน้าของเจ้าหน้าที่ดังกล่าว
4. สำนักนโยบายยุทธศาสตร์ ดำเนินการจัดทำ Minimum Dataset โดยประสานงานกับสำนักตรวจราชการ กรมกองวิชาการและตัวแ ทนจากจังหวัด เพื่อปฏิรูประบบรายงานเดิมให้อยู่ในรูปอิเล็กทรอนิกส์ทั้งหมด ให้แล้วเสร็จภายในเดือนกุมภาพันธ์ 2546

สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้จัดตั้งศูนย์เทคโนโลยีสารสนเทศ โดยมีการจัดหาและติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายข้อมูลพร้อมอุปกรณ์ และโปรแกรมคอม พิวเตอร์ ติดตั้ง ณ ศูนย์เทคโนโลยีสารสนเทศ อาคารกันเกรา ชั้น2 สำนักงานสาธารณสุขจังหวัดสุรินทร์

2.1.1 ระบบฐานข้อมูล สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้ดำเนินการพัฒนาระบบเว็บเพจเพื่อนำเสนอข้อมูลและฐานข้อมูล ในระบบ Internet สามารถเรียกดูได้ที่ URL http://www.spho.moph.go.th และ http://www.surinpho.net และ http://www.surinpho.com สามารถใช้ฐานข้อมูลเพื่อสนับสนุนการบริหารงาน ฐานข้อมูลในส่วนของกระทรวงสาธารณสุขและสำนักงานสาธารณสุขจังหวัดสุรินทร์ ทั้งยังสามารถใช้งานระบบฐานข้อมูลของจังหวัดสุรินทร์แบบบูรณาการ (CEO) ตามยุทธศาสตร์ส่วนต่อขยายฐานข้อมูลและสารสนเทศ ใช้งานระบบของศูนย์ปฏิบัติการของจังหวัดสุรินทร์ ได้ ที่ http://www.surin.go.th การใช้งานเพื่อ Link POC Surin (ศูนย์ปฏิบัติการของจังหวัดสุรินทร์) หรือที่ http://www.surinpoc.com

2.1.1.1 **การเชื่อโยงข้อมูล** จำแนกข้อมูลเป็น 2 ส่วนได้แก่

- ข้อมูล 45 กลุ่มเรื่อง กับข้อมูล 33 ตัวชี้วัด ที่มีรายละเอียดข้อมูลเดียวกันหรือซ้ำกัน มีการเชื่อมโยงข้อมูลเพื่อนำมาใช้จากแหล่งเดียวกัน ผู้ที่เกี่ยวข้องสามารถเข้าถึงข้อมูล บันทึกข้อมูลเข้าฐานข้อมูลจังหวัดได้โดยตรงผ่าน Web Browser โดยจัดเก็บใน Database Server (Microsoft SQL Server) และสามารถนำมาวิเคราะห์ได้ทั้งในระบบ MIS และ GIS รวมทั้งมีการส่งผ่านข้อมูลระหว่าง สำนักงานสาธารณสุขจังหวัดสุรินทร์ ไปยังศูนย์ปฏิบัติการจังหวัด (POC) ด้วยรูปแบบเอกสารและไฟล์ข้อมูล
- ข้อมูลที่สำนักงานสาธารณสุขจังหวัดสุรินทร์ ต้องส่งเข้าฐานข้อมูลกลางเพื่อประมวลผล เช่น ข้อมูล0110 รง.5 / ข้อมูลฐานข้อมูลสถานีอนามัย18 แฟ้ม (HCIS) /ข้อมูลการเงินและการคลังอีเล็กทรอนิกส์ (GGIMIS) ฯลฯ ใช้การส่งและเชื่อมโยงข้อมูลผ่านทาง Internet เส้นทางของสำนักงานบริหารเทคโนโลยีสารสนเทศ Gi-Net

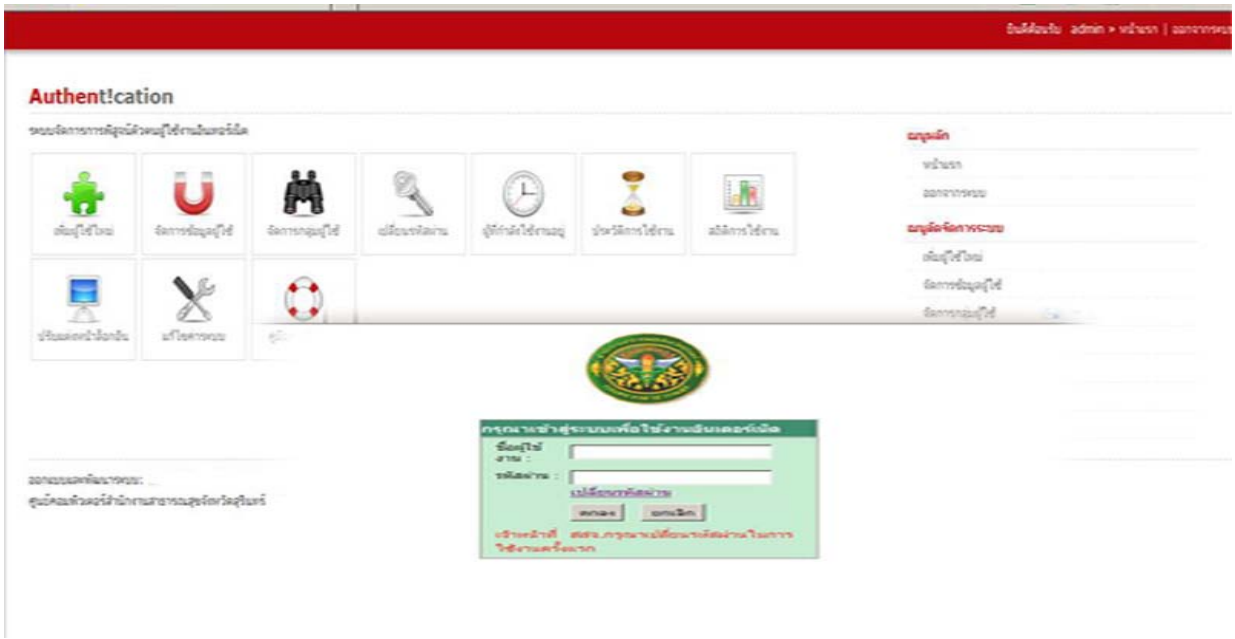
2.1.1.2 **การตรวจสอบข้อมูล** ดำเนินการตรวจสอบความเชื่อถือและความเที่ยงตรงของข้อมูล โดยมีการแสดงแหล่งที่มาของข้อมูล และสูตรที่ใช้ในการคำนวณ พร้อมทั้งการแสดงผลทั้งในเชิงตัวเลข ตาราง กราฟ และแผนภูมิ สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้มอบหมายหน้าที่ความรับผิดชอบแก่เจ้าหน้าที่ผู้รับผิดชอบโดยตรงและมีการรับรองความถูกต้องจาก นายแพทย์สาธารณสุขจังหวัดสุรินทร์ ก่อนและหลังนำเข้าข้อมูล รวมทั้งมีการตรวจสอบข้อมูลที่มีการนำเข้าโดยเจ้าหน้าที่ของศูนย์ปฏิบัติการจังหวัด (POC) อีกครั้งหนึ่งด้วย

2.1.1.3 **ระบบการปรับปรุงข้อมูล** ดำเนินการแต่งตั้งเจ้าหน้าที่และหน่วยงานรับผิดชอบข้อมูลในแต่ละเรื่อง โดยกำหนดความถี่ในการปรับปรุงข้อมูลตามความเหมาะสมในแต่ละเรื่อง และสามารถปรับปรุงข้อมูลผ่านระบบเครือข่ายและระบบอินทราเน็ตได้ ซึ่งเจ้าหน้า ที่ดูแลระบบสามารถตรวจสอบวันที่ปรับปรุงข้อมูลล่าสุดของทุกฐานข้อมูลได้

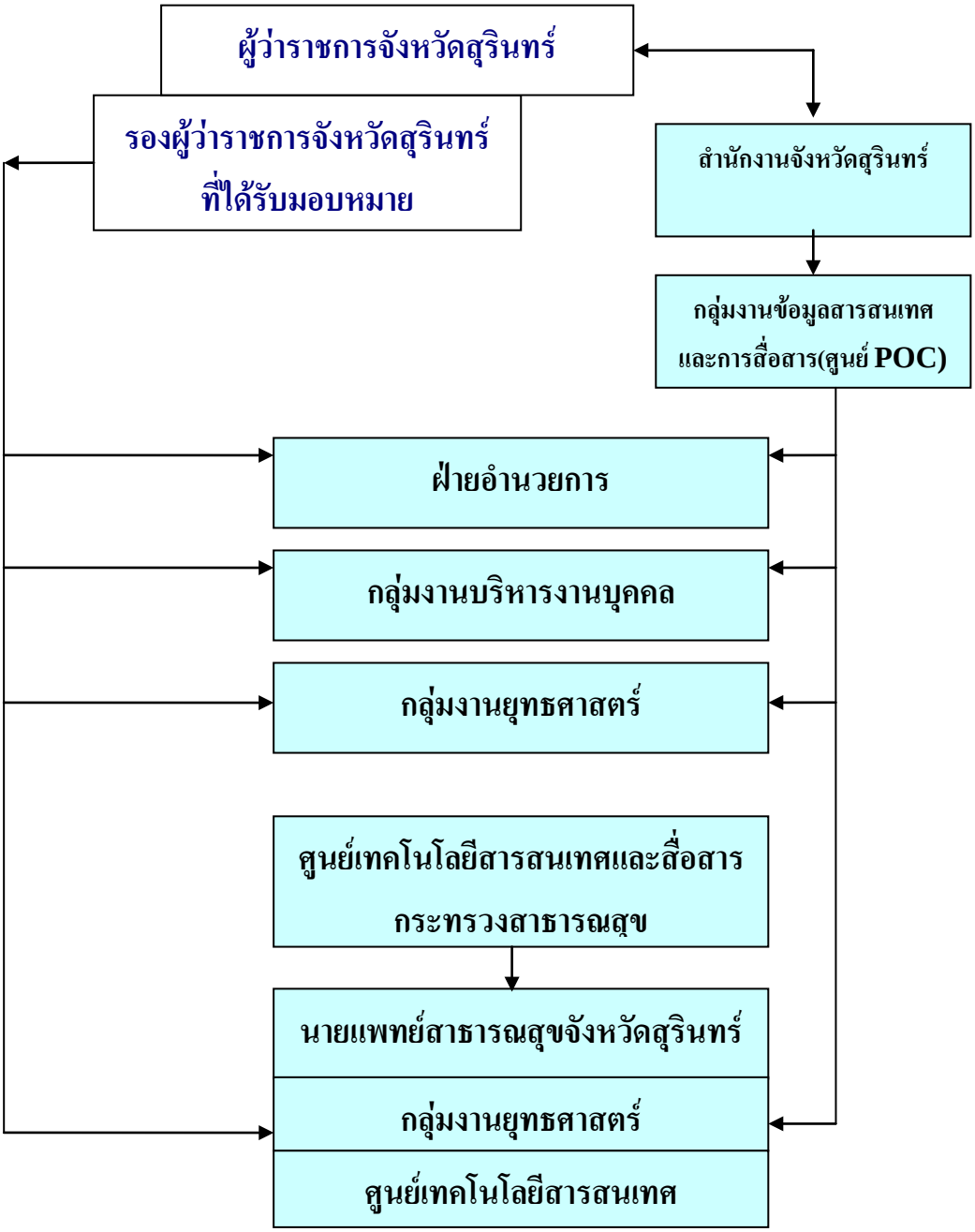
2.2 การพัฒนาบุคลากรเจ้าหน้าที่ที่ปฏิบัติงาน ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการฝึกอบรมให้ความรู้ในเรื่องการจัดการระบบฐานข้อมูลสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของจังหวัด แก่บุคลากร และเจ้าหน้าที่ที่ปฏิบัติงาน ด้านสารสนเทศของสำนักงานสาธารณสุขจังหวัดสุรินทร์

2.3 กำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ ที่ปฏิบัติหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ ออกคำสั่งสำนักงานสาธารณสุขจังหวัดสุรินทร์ เพื่อกำหนดหน้าที่ความรับผิดชอบดูแล ระบบข้อมูลศูนย์เทคโนโลยีสารสนเทศสำนักงานสาธารณสุขจังหวัดสุรินทร์

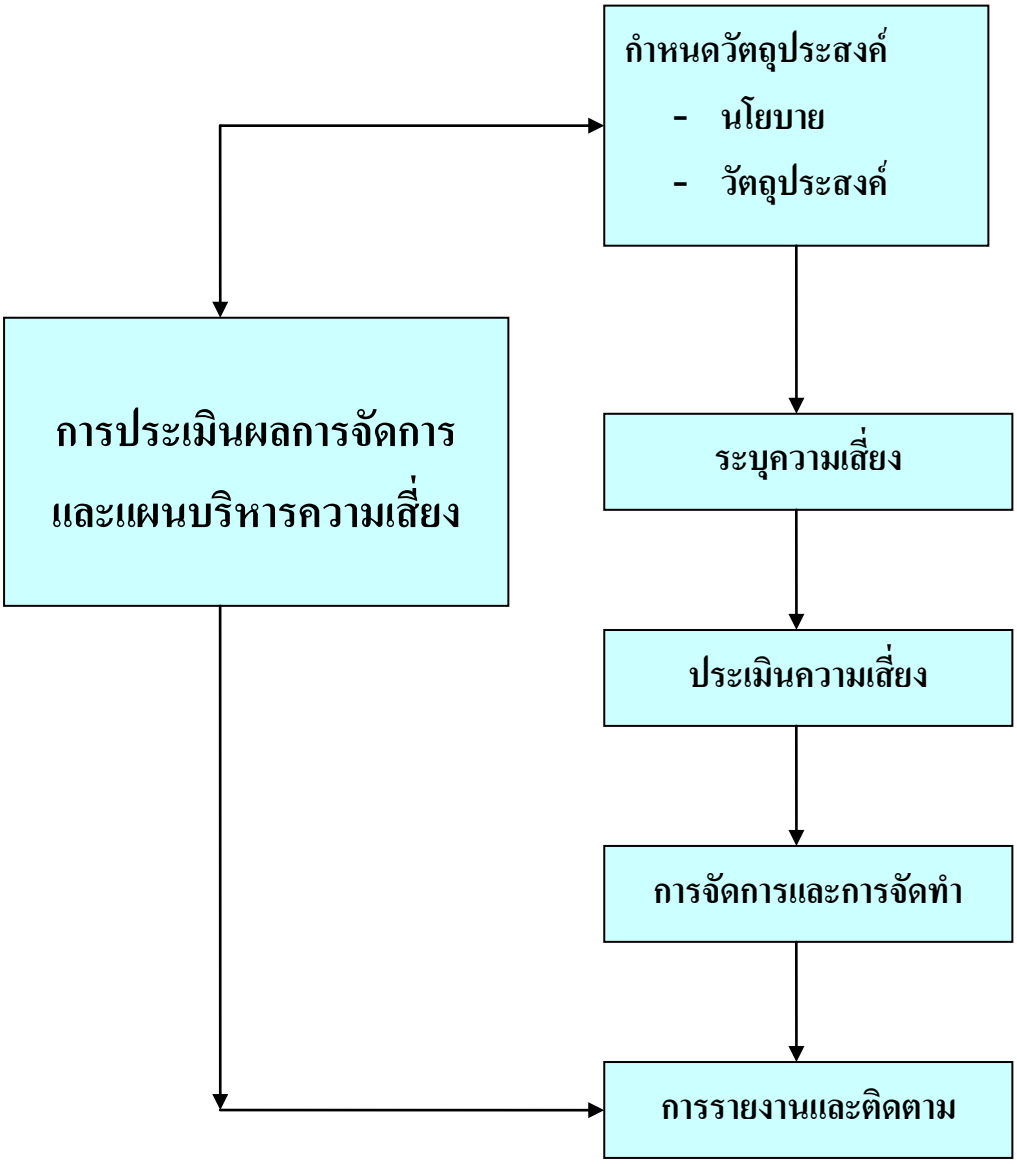
2.4 การจัดทำระบบตรวจสอบสิทธิเพื่อจัดเก็บ Log File ตาม พรบ.ความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550
สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้ดำเนินการติดตั้งอุปกรณ์คอมพิวเตอร์ Authentication Server เป็นข้อมูลล็อกการพิสูจนตัวตนของเซิรฟเวอร์หรืออุปกรณ์ พิสูจน์ตัวตนและกำหนดสิทธิบนการใช้งานบนระบบเครือขาย เซิรฟเวอรRADIUS วิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะทำการตรวจสอบจาก username และ password จุดประสงค์หลักของการ Authentication คือพิสูจน์ตัวบุคคลว่าคน ๆ นั้นที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต คือใคร พร้อมทั้งทำการตรวจสอบสิทธิ์ว่า ผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตของท่านนั้นมีสิทธิ์ใช้ได้นานเท่าไหร่และสามารถ upload หรือ download ได้ด้วยความเร็วเท่าไหร่ ซึ่งระบบนั้นจะทำการตัดผู้ใช้ออกไปจากการให้บริการทันทีที่เวลาหมด อีกทั้งยังสามารถกำหนดเวลาและความเร็วได้ตามความเหมาะสมด้วย ต่อจากนั้นจะทำการบันทึกข้อมูลการใช้งานระบบเครือข่าย



2.5 โครงสร้างการบริหารงานความเสี่ยงและแผนการแก้ไขปัญหาจากภัยพิบัติ ที่อาจเกิดกับระบบฐานข้อมูลและสารสนเทศ(Contingency Plan) สำนักงานสาธารณสุขจังหวัดสุรินทร์ ปี 2552



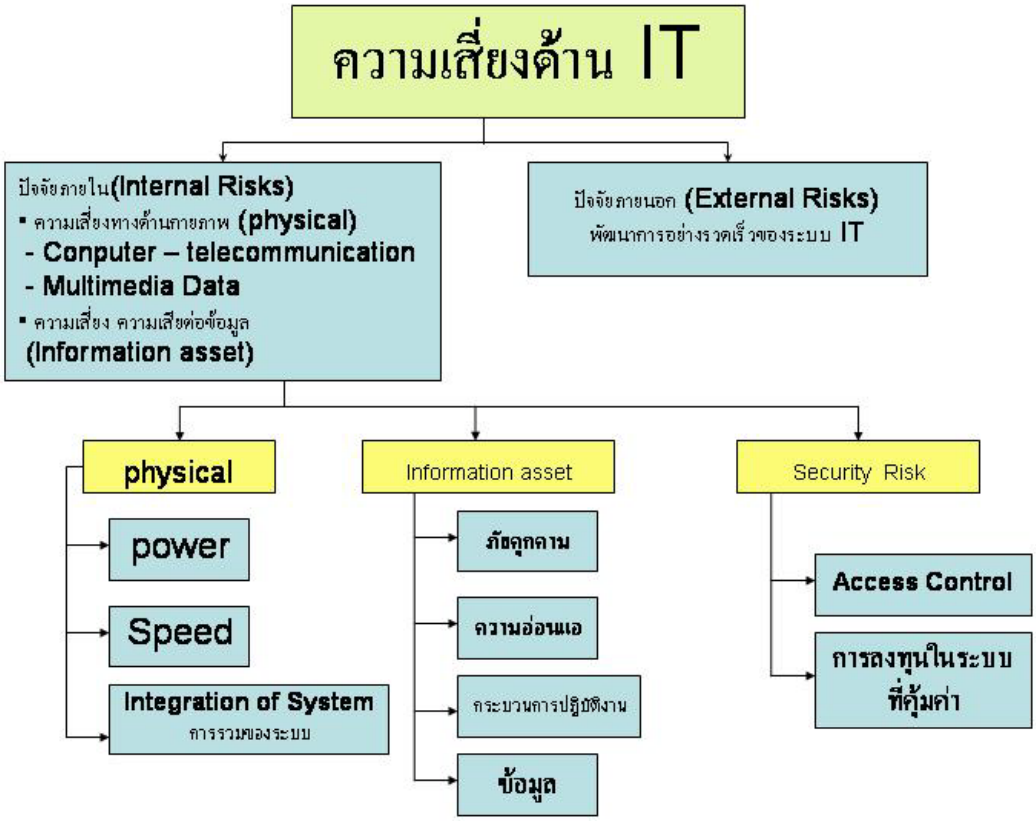
2.6 กระบวนการบริหารความเสี่ยง



2.7 การกำหนดวัตถุประสงค์ความเสี่ยง

- เพื่อกำหนดความเสี่ยงที่มีโอกาสเกิดขึ้นต่อระบบฐานข้อมูลสานสนเทศของศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์
- กำหนดกิจกรรมป้องกันรองรับความเสี่ยงที่มีโอกาสเกิดขึ้น เพื่อป้องกันความเสียหาย และลดความเสียหายที่เกิดขึ้นให้อยู่ในระดับที่น้อยที่สุด

2.8 การระบุความเสี่ยงของระบบสารสนเทศของศูนย์เทคโนโลยีสารสนเทศ สสจ. สุรินทร์



ความเสี่ยง คือ สิ่งที่เป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กร อุปสรรคหรืออันตรายที่คาดหรือมิได้คาดคิดมาก่อนทำให้ระบบสารสนเทศเสียหายได้ สิ่งที่เป็นอันตรายและทำให้ระบบสารสนเทศเกิดความเสี่ยง นอกจากทางด้าน IT แล้วยังมีความเสี่ยงจากภัยธรรมชาติ ได้แก่ น้ำท่วม แผ่นดินไหว ฟ้าผ่า ล้วนแล้วแต่มีผลกระทบต่อระบบคอมพิวเตอร์เป็นอย่างยิ่ง ไม่ว่าจะโดยทางตรงหรือทางอ้อม เช่นทำให้เกิดปัญหากับระบบไฟฟ้า ซึ่งเป็นที่ทราบดีอยู่แล้วว่าไฟฟ้าเป็นแหล่งพลังงานของระบบคอมพิวเตอร์ จึงต้องมีการจัดตั้งแผนป้องกัน

2.9 การประเมินความเสียหายจากความเสี่ยง

- ความเสี่ยงที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติหรือวินาศภัย ตัวเครื่องคอมพิวเตอร์ ประมวลผลหลักหรือคอมพิวเตอร์แม่ข่ายเสียหาย และระบบฐานข้อมูลหลักเสียหาย รวมทั้งการลักลอบเข้าสู่อาคารศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์
- ความเสี่ยงที่เกิดผลเสียหายและจะต้องหยุดระบบลงชั่วขณะ ได้แก่ ระบบกระแสไฟฟ้าขัดข้อง ระบบสื่อสารข้อมูลหลักเสียหาย หรือการเจาะระบบ (Hack)

2.10 การจัดการความเสี่ยง

- **การจัดการให้มีการจัดเก็บข้อมูลคอมพิวเตอร์ แยกกัน 2 แหล่ง** ได้แก่

  1. ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์

  2. ศูนย์ปฏิบัติการกระทรวงสาธารณสุข(MOC) ตั้งอยู่ที่ ศูนย์เทคโนโลยีสารสนเทศและสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข จังหวัดนนทบุรี

เพื่อให้การประมวลผลข้อมูล ระบบฐานข้อมูลสารสนเทศของศูนย์ปฏิบัติการจังหวัดสุรินทร์ สามารถประมวลผลได้อย่างต่อเนื่อง เพราะมีระบบการจัดเก็บข้อมูลคอมพิวเตอร์แยกกัน เพื่อป้องกันปัญหาความเสี่ยงที่ต้องหยุดประมวลผลเพราะประสบวินาศภัย ภัยพิบัติทางธรรมชาติ หรือความเสียหายอย่างรุนแรงที่เกิดขึ้นกับระบบเครื่องแม่ข่ายประมวลผล หรือระบบฐานข้อมูลหลัก

- **การจัดการให้มีระบบสำรองฐานข้อมูล** โดยศูนย์เทคโนโลยีสารสนเทศ จะมีการจัดทำระบบสำรองข้อมูลไว้ตามวงรอบที่กำหนดไว้ โดยมีการจัดทำในระบบ Manual โดยมีการกำหนดให้มีการสำรองข้อมูล (Backup) ฐานข้อมูล ตามระยะเวลาที่กำหนด ได้แก่
  - การสำรองข้อมูลประจำสัปดาห์
  - การสำรองข้อมูลประจำเดือน
  - การสำรองข้อมูลประจำปี

  รวมทั้งการจัดให้มีระบบการบำรุงรักษา (Restructure/Reformat) ระบบฐานข้อมูล

- **การจัดการให้มีระบบสำรองไฟฟ้า (UPS)** เพื่อจ่ายพลังงานไฟฟ้าสำรองให้แก่เครื่องคอมพิวเตอร์แม่ข่าย โดยมีเครื่องสำรองไฟฟ้าหลัก จำนวน 2 ชุด ติดตั้ง ณ ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ จัดเจ้าหน้าหน้าที่ดูแล มีการบำรุงรักษา มีระบบการบันทึกข้อมูล

- **การจัดให้มีอุปกรณ์คอมพิวเตอร์เพิ่มเติม** เพื่อรักษาความปลอดภัยโครงข่ายและระบบเครือข่ายการประมวลผลข้อมูล เพื่อการบริการประชาชนและสนับสนุนข้อมูลให้ผู้บริหารใช้ประกอบการตัดสินใจ

- **<u>การให้มีระบบสื่อสารสำรองสำหรับศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์</u>**

<u>1. ระบบสื่อสารเครือข่ายหลัก</u> เพื่อป้องกันความเสียหายที่เกิดขึ้นจากการติดขัดของระบบรับส่งข้อมูล ของศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ ที่ต้องทำงานร่วมกับหน่วยงานต่างๆ ดังรายละเอียดต่อไปนี้เครือข่ายอินเตอร์เน็ต มีการเชื่อมต่อระบบ Leased Line กับสำนักงานบริการเทคโนโลยีสารสนเทศภาครัฐ(Gi-Net) ผ่านเครือข่าย G-Nodeของบริษัท ทีโอที จำกัด(มหาชน) ความเร็ว 512 Kbps แต่เนื่องจากมีการส่งข้อมูลจำนวนมาก ผ่านเส้นทางดังกล่าวเช่น ระบบส่งข้อมูลการเงินการคลังอีเลคทรอนิคส์ และส่งข้อมูลฐานข้อมูลสถานีอนามัยที่ส่งตลอด 24 ชั่วโมง ทำให้ช่องสัญญาณ (Bandwitd)ไม่เพียงพอ สำนักงานสาธารณสุขจังหวัดสุรินทร์ จึงได้จัดหาเส้นทางเครือข่ายหลักเพิ่มเติม โดยประสานงานติดตั้งระบบเชื่อมต่อระบบ Leased Line จากบริษัท กสท โทรคมนาคม จำกัด(มหาชน) ความเร็ว 2 Mbps โดยติดตั้งและเริ่มใช้งานระบบตั้งแต่เดือนกรกฎาคม 2552 ที่ผ่านมา รวมมีเส้นทางหลักในการใช้งาน 2 วงจร

<u>2. ระบบระบบสื่อสารเครือข่ายสำรอง</u> ได้จัดทำระบบเส้นทางเครือข่ายสำรองระบบ ADSL จากบริษัท กสท โทรคมนาคม จำกัด(มหาชน) ความเร็ว 4 Mbps จำนวน 2 วงจร ทำโหลดบาลานซ์ เพื่อให้บริการการใช้งานแก่เจ้าหน้าที่ในสำนักงานสาธารณสุขจังหวัดสุรินทร์ และบริษัท ทีโอที จำกัด(มหาชน) ความเร็ว 2 Mbps เพื่อใช้งานรองรับระบบโทรศัพท์และโทรสาร ระบบ Voip เส้นทาง และยังได้จัดหาเส้นทางเครือข่ายระบบ ADSL เพื่อใช้งานเฉพาะส่งข้อมูลเพื่อประกันความเชื่อถือของเครือข่ายที่กลุ่มงานคุ้มครองผู้บริโภค และกลุ่มงานประกันสุขภาพ สำนักงานสาธารณสุขจังหวัดสุรินทร์ โดยใช้บริการระบบ ADSL ของบริษัท ทีทีแอนด์ที จำกัด (มหาชน) ความเร็ว 2 Mbps รวม 2 วงจร

ลำดับ	ผู้ให้บริการ/เครือข่าย	ความเร็ว	ระบบ	หมายเหตุ
1	สำนักงานบริการเทคโนโลยีสารสนเทศภาครัฐ(Gi-Net)	512 Kbps	Leased Line	เครือข่ายหลัก 1
2	บริษัท กสท โทรคมนาคม จำกัด(มหาชน)	2 Mbps	Leased Line	เครือข่ายหลัก 2
3	บริษัท กสท โทรคมนาคม จำกัด(มหาชน)	4 Mbps	ADSL	เครือข่ายสำรอง1/2
4	บริษัท ทีโอทีจำกัด (มหาชน)	2 Mbps	ADSL	VOIp และFax
5	บริษัท ทีทีแอนด์ที จำกัด (มหาชน)	2 Mbps	ADSL	งานประกันสุขภาพ
6	บริษัท ทีทีแอนด์ที จำกัด (มหาชน)	2 Mbps	ADSL	งานคุ้มครองฯ

2.11 เจ้าหน้าที่ผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยง

เพื่อให้การดำเนินงานตามแผนฯ เป็นไปอย่างรวดเร็วทันต่อการดำเนินการ จึงกำหนดให้เจ้าหน้าที่ต่อไปนี้เป็นผู้รับผิดชอบดำเนินการจัดการความเสี่ยงที่เกิดขึ้น โดยสำนักงานสาธารณสุขจังหวัดสุรินทร์ กำหนดบทบาทหน้าที่ให้ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ เป็นผู้รับผิดชอบดำเนินการให้นายแพทย์สาธารณสุขจังหวัดสุรินทร์ กำกับดูแลควบคุมการดำเนินการ

2.12 การรายงานผล

กำหนดให้ผู้รับผิดชอบดำเนินการรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีที่ระบุไว้การจัดการความเสี่ย

3. แนวทางการดำเนินการ (DO)

สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้กำหนดแนวทางในการสร้างความปลอดภัยให้กับระบบเครือข่ายสารสนเทศของจังหวัด เพื่อเป็นแนวทางในการบริหารจัดการ เพื่อให้ครอบคลุมถึงระดับขั้นของความสำเร็จในขั้นตอนที่ 3 โดยมีงานที่เกี่ยวข้องกับการสร้างความปลอดภัยให้กับระบบเครือข่าย ดังนี้

3.1 การบริหารความเสี่ยงของระบบสารสนเทศ (Risk Mannagement) มีการบริหารความเสี่ยงเพื่อกำจัด/ป้องกันหรือลดการเกิดความเสียหาย ในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองข้อมูลและระบบกู้คืนข้อมูล จากความเสียหาย (Back up & Recovery) ประกอบด้วย

1) ศึกษาระบบเครือข่ายปัจจุบัน
2) วิเคราะห์ความเสี่ยงที่มีโอกาสเกิดขึ้นได้จาการใช้งานระบบเครือข่าย
3) ออกแบบวิธีการเพื่อลดความเสี่ยงที่พบ ซึ่งจะประกอบไปด้วย

- การสร้างความปลอดภัยทางกายภาพ ได้แก่ การควบคุมการเข้าออกห้องปฏิบัติการเซิร์ฟเวอร์ ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์
- การสร้างความปลอดภัยให้กับระบบปฏิบัติการ ได้แก่การติดตั้งระบบปฏิบัติการ ทั้งเครื่องคอมพิวเตอร์ลูกข่าย และเครื่องเซิร์ฟเวอร์ ให้ทำงานอย่างปลอดภัย และมีประสิทธิภาพ
- การสร้างความปลอดภัยให้กับเซิร์ฟเวอร์ ทำการติดตั้ง Web Server , FTP Server) โดยมีการกำหนดการเข้าถึงข้อมูลโดยการใช้บัญชีรายชื่อผู้ใช้ และรหัสผู้ใช้(UserName Password)
- การป้องกันการบุกรุกระบบ
- การพัฒนานโยบายการใช้งานระบบเครือข่าย
- การสร้างความตระหนักให้กับผู้ใช้
- การสำรองและเรียกคืนข้อมูล มีระบบสำรองข้อมูล (Data Backup) โดยอัตโนมัติ
- การบริหารและจัดการเมื่อมีเหตุการณ์ที่ไม่ปลอดภัยเกิดขึ้น

3.2 การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (Contingency Plan) เช่น การเกิดภัยธรรมชาติ อัคคีภัย การก่อการร้าย

3.3 มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบสารสนเทศ

3.4 กำหนดสิทธิให้ผู้ใช้แต่ละระดับ (Access rights)

3.5 ทบทวนแผนเพื่อสร้างความปลอดภัย

4. วิธีดำเนินการ (CHECK),(ACT)

4.1 การเฝ้าระวังและทบทวนระบบ

การดำเนินการตามแนวทางที่ได้กำหนดไว้ ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้พิจารณากรณีความเสี่ยงและภัยที่อาจจะเกิดกับระบบ ลงมือปฏิบัติตามขั้นตอนเพื่อให้สามารถบริหารจัดการในกรณีที่เกิดเหตุการณ์ ดังนี้คือ

4.1.1 การบริหารความเสี่ยงของระบบสารสนเทศ มีการบริหารความเสี่ยงเพื่อกำจัด/ป้องกันหรือลดการเกิดความเสียหาย ในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Back up & Recovery) ประกอบด้วย

1) ทำการศึกษาระบบเครือข่ายปัจจุบัน
2) วิเคราะห์ความเสี่ยงที่มีโอกาสเกิดขึ้นได้จากการใช้งานระบบเครือข่าย
3) ออกแบบวิธีการเพื่อลดความเสี่ยงที่พบ ซึ่งประกอบไปด้วย

- การสร้างความปลอดภัยทางกายภาย ได้แก่ การควบคุมการเข้าออกห้องปฏิบัติการเซิร์ฟเวอร์ ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์
- การสร้างความปลอดภัยให้กับระบบปฏิบัติการ ได้แก่การติดตั้งระบบปฏิบัติการ ทั้งเครื่องคอมพิวเตอร์ลูกข่าย และเครื่องเซิร์ฟเวอร์ ให้ทำงานอย่างปลอดภัย และมีประสิทธิภาพ
- การสร้างความปลอดภัยให้กับเซิร์ฟเวอร์ ทำการติดตั้งเว็ปต์เซิร์ฟเวอร์(Web Sever) ไฟล์เซิร์ฟเวอร์ (File Server) ระบบดาต้าเบสเซิร์ฟเวอร์ (Data Base Server) ระบบเอฟทีพีเซิร์ฟเวอร์ (FTP Server) โดยมีการกำหนดการเข้าขึ้นถึงข้อมูลโดยการใช้บัญชีรายชื่อผู้ใช้ และรหัสผู้ใช้ (UserName & Password)
- การสร้าง เป็นไปตาม พรบ.ความรับผิดทางคอมพิวเตอร์ ปี 2550 มีระบบ Login เข้าระบบพิสูจน์ตัวตน ก่อนเข้าใช้งานระบบอินเทอร์เน็ต มีระบบการจัดเก็บLogไฟล์ และการจราจรทางคอมพิวเตอร์ ทางสำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้ดำเนินเรียบร้อยแล้ว
- การป้องกันการบุกรุกระบบ ประกอบไปด้วย
  - จัดทำระบบไฟล์วอลล์ สำหรับศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ โดยสามารถทำการเชื่อมต่อพร้อมกันได้สูงสุด (Concurrent Connections) รองรับการใช้งานของผู้ใช้แบบไม่จำกัดจำนวนผู้ใช้

- การจัดทำระบบป้องกันการบุกรุกในกรณีที่ไฟล์วอลล์อนุญาตให้เข้ามาใช้งานได้ โดยที่อาจจะใช้ช่องโหว่ในตัวซอฟต์แวร์ของเว็บเซิร์ฟเวอร์ที่ยังไม่ได้อุด เป็นช่องทางในการบุกรุก งานจัดทำระบบป้องกันการบุกรุกนี้ มีจุดประสงค์หลักคือเพื่อลดความเสี่ยงจากช่องโหว่ในตัวซอฟต์แวร์
- การจัดทำระบบค้นหาจุดอ่อนโดยให้มีความสามารถหาช่องโหว่ในตัวซอฟต์แวร์
- อุดช่องโหว่ในตัวซอฟต์แวร์ที่ใช้งานในระบบเครือข่าย เช่นซอฟต์แวร์ระบบปฏิบัติการซอฟต์แวร์เซิร์ฟต่าง ๆ ที่มีช่องโหว่
- การตรวจสอบความสมบรูณ์ของไฟล์ในระบบ ในการป้องกันการบุกรุกระบบไม่ว่าจะด้วยไฟล์วอลล์ ระบบป้องกันการบุกรุก หรือระบบค้นหาจุดอ่อน ก็ตามก็ยังอาจมีโอกาสที่ผู้บุกรุกจะสามารถจู่โจมเข้ามาได้ ซึ่งอย่างไรก็ตามเมื่อการบุกรุกครั้งหนึ่งๆ เกิดขึ้น ผู้บุกรุกมักทิ้งร่องรอยไว้ในระบบที่บุกรุกเข้าไป เช่นการเปลี่ยแปลงแก้ไขไฟล์การติดตั้งซอฟต์แวร์(ไฟล์) เข้าไปในระบบที่บุกรุกเข้าไป งานนี้จะเป็นทางหนึ่งที่จะช่วยให้ผู้ดูแลระบบทราบถึงการกระทำที่เกิดขึ้นกับไฟล์ในระบบและหาทางดำเนินการแก้ไขต่อไป
- ป้องกันไวรัส การบุกรุกของไวรัสภายในเครือข่ายอาจจะมาจาการดาวน์ โหลดไฟล์ของผู้ใช้ผ่านอินเตอร์เน็ตหรือจากทางอีเมล์ที่ได้รับ โดยทั่วไปไฟล์วอลล์จะอนุญาตการดาวน์โหลดของผู้ใช้ผ่านอินเตอร์เน็ต รวมทั้งจะอนุญาตการส่งมอบอีเมล์จาก เมล์เซิร์ฟเวอร์ที่อยู่ภายนอกเข้ามาสู่เมล์เซิร์ฟเวอร์ภายใน โดยที่ในทั้งสองกรณีไฟล์วอลล์ จะไม่รับรู้ว่ามีว่ามีไวรัสติดมาด้วยหรือไม่ ดังนั้นงานป้องกันไวรัส จึงเป็นทางเสริมอีกทางหนึ่ง ที่สำคัญเพื่อป้องกันการบุกรุกจากภายนอกเข้ามาสู่เครือข่ายภายใน
- ตรวจสอบปริมาณข้อมูลบนเครือข่าย ปริมาณข้อมูลบนเครือข่ายที่สูงมากผิดปกติอาจมีสาเหตุมาจากมีไวรัสกำลังแพร่กระจายอยู่ หรือมีการส่งหรือรับข้อมูลในเครือข่ายเป็นปริมาณสูง มีผลกำไรการใช้งานเครือข่ายเกิดการล่าช้า ติดขัด หรืออาจถึงขั้นไม่สามารถใช้งานไม่ได้เลย จึงให้ผู้ดูแลระบบตรวจสอบปริมาณข้อมูลอย่างสม่ำเสมอเพื่อจะได้ทราบว่ามีความผิดปกติเกิดขึ้นหรือไม่และจะได้ดำเนินการแก้ไขได้ทัน
- เฝ้าดูการทำงานของเซิร์ฟเวอร์ กิจกรรมการเข้าใช้งานของ ผู้ใช้ที่เซิร์ฟเวอร์บันทึกไว้ เช่นวันเวลาที่เข้าใช้ กิจกรรมที่ทำ เป็นต้น ผู้ดูแลระบบมีการนำมาตรวจสอบอย่างสม่ำเสมอ เพื่อตรวจสอบหาสิ่งผิดปกติ เช่น มีผู้ไม่ประสงค์ดี พยายาม login เข้ามาในระบบเข้ามางาน หรือเจาะระบบเซิร์ฟเวอร์โดยที่ไม่มีสิทธิ ผู้ดูแลระบบจะได้หาทางแก้ไขต่อไป

- การพัฒนานโยบายการใช้งานระบบเครือข่าย โดยติดตั้งโปรแกรมแอนตี้ไวรัสและเซอร์วิสแพ็ค ของโปรแกรมให้เป็นปัจจุบันอยู่เสมอ
    - ทำการบล็อกไอพี สำหรับเครื่องที่ติดไวรัสที่ไม่ทำการแก้ไข พร้อมทั้งแจ้งหัวหน้าหน่วยงานนั้น ๆ เพื่อให้ได้รับทราบถึงปัญหา และให้กำชับเจ้าหน้าที่ในหน่วยปฏิบัติตามกฎเกณฑ์อย่างเคร่งครัด
    - ผู้บริหารต้องนิเทศกำกับและติดตามการปฏิบัติงานอย่างสม่ำเสมอ เพื่อควบคุมพฤติกรรมการใช้งานระบบเครือข่าย ทั้งผู้ดูแลระบบและผู้ใช้งานทั่วไป เพื่อไม่ให้ละเลยหรือปฏิบัติออกนอกลู่นอกทางที่ควรกระทำ
- การสร้างความตระหนักให้กับผู้ใช้
    - จัดให้มีการประชุมสัมมนาเจ้าหน้าที่ผู้ปฏิบัติงานด้านคอมพิวเตอร์ของหน่ายงานต่างๆ ในสำนักงานสาธารณสุขจังหวัดสุรินทร์ เพื่อนำเสนอปัญหาในกรณีที่ไม่ปฏิบัติตามกฎเกณฑ์ที่ไว้ เช่น การดาวน์โหลดไฟล์โดยไม่มีการตรวจสอบไวรัส การแชร์ไฟล์โดยไม่มีรหัสผ่านทางอีเมล์ หรือพฤติกรรมที่มีความเสี่ยงอื่น
    - ประชาสัมพันธ์และแจ้งเตือนการระบาดของไวรัสในแต่ละช่วงโดยชี้ให้เห็นถึง ภัยของไวรัสแต่ละตัวและความเสียหายที่เกิดขึ้น
- การสำรองและเรียกคืนข้อมูล มีระบบสำรองฐานข้อมูล จัดทำคู่มือสำรองฐานและปฏิบัติตามขั้นตอนเพื่อให้สามารถจัดการกับปัญหาได้อย่างรวดเร็วและมีประสิทธิภาพ
- การบริหารและจัดการเมื่อมีเหตุการณ์ที่ไม่ปลอดภัยเกิดขึ้น
    - มีการจัดการเมื่อมีเหตุการณ์บุกรุกเกิดขึ้น เช่น มีไวรัสบนระบบเครือข่าย เครือข่ายถูกบุกรุกหรือพบความพยายามในการบุกรุก
    - จัดทำรายงานให้ผู้บังคับบัญชาได้รับทราบ

4.1.2 มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (Contingency Plan) เช่น การเกิดภัยธรรมชาติ อัคคีภัย การก่อการร้าย เป็นต้น

4.1.3 มีระบบรักษาความมั่นคงและปลอดภัย(Security) ของระบบสารสนเทศ

- กำหนดอำนาจหน้าความรับผิดชอบของผู้ที่เกี่ยวข้อง เช่น เจ้าหน้าที่ดูแลระบบเครื่อง เจ้าหน้าที่พัฒนาระบบงาน การอนุญาตเข้าสู่ห้องที่ติดตั้งระบบ Hardware ของศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์
- มีการติดตั้งระบบ Firewall ป้องกันก่อนที่จะผ่านเข้าสู่ Sever จากทุกหน่วยงาน

4.1.4 กำหนดสิทธิให้ผู้ใช้แต่ละระดับ (Access rights) มีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง/ผู้รับผิดชอบ และผู้ใช้ทั่วไปสามารถเข้าสู่ระบบ (Accessability) ได้ตามระดับหรือขอบเขตความรับผิดชอบ โดยแบ่งออกเป็น 3 กลุ่ม คือ

- Guests คือกลุ่มผู้ใช้ทั่วไปสามารถอ่านข้อมูลได้อย่างเดียว
- Users คือกลุ่มที่สามารถอ่านและแก้ไขข้อมูลได้ โดยสามารถแก้ไขได้เฉพาะข้อมูลที่รับผิดชอบเท่านั้น
- Admin คือกลุ่มผู้ดูแลระบบสามารถปรับปรุงแก้ไขได้ทั้งหมด

4.1.5 ทบทวนแผนเพื่อสร้างความปลอดภัย

- จัดทำรายงานประเมินผลความเสี่ยงของระบบสารสนเทศและการใช้ประโยชน์ระบบสารสนเทศเพื่อเป็นข้อมูลประกอบการประเมินผล
- ทบทวนแผนภายหลังจากที่ได้มีการนำวิธีการเพื่อลดความเสี่ยงมาใช้ เช่น ในช่วงระยะเวลาที่ผ่านมามีการนำเทคโนโลยีใหม่มาใช้งาน การอัพเกรดซอฟต์แวร์ เป็นต้นจะทำให้องค์กรรับความเสี่ยงใหม่เข้ามาจึงต้องทำการวิเคราะห์ความเสี่ยงและหาวิธีแก้ไขเพิ่มเติม

4.2 การบำรุงรักษาและปรับปรุง (ACT)

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ ได้พิจารณากรณีความเสี่ยงและภัยที่จะเกิดกับระบบ และใช้มาตรการแก้ไขและป้องกันในกรณีที่เกิดเหตุการณ์ตลอดจนการบำรุงรักษาและปรับปรุงระบบ ดังนี้คือ

1. กรณีความร้อนจังหวัดดำเนินการการติดตั้งเครื่องปรับอากาศและกำหนดให้ทำการเปิดเครื่องปรับอากาศตลอด 24 ชั่วโมง จัดให้มีระบบตั้งเวลา ได้มีการติดตั้งเครื่องปรับอากาศเป็น 2 เครื่องเพื่อสำรองไว้และเปิดสลับกัน มีการมอบหมายให้เจ้าหน้าที่ศูนย์ฯดูแลอย่างเข้มงวด
2. จัดหาเครื่องดับเพลิง เพื่อเตรียมการไว้ถ้าหากเกิดอัคคีภัย

2. กรณีการเชื่อมโยงเครือข่ายล้มเหลว จังหวัดฯ ได้จัดทำเส้นทางการเชื่อมโยงเครื่อข่ายสำรองโดยผ่านเครือข่ายของบริษัท ทศท.คอร์เปอเรชั่น จำกัด (มหาชน) และบริษัท กสท. โทรคมนาคม จำกัด(มหาชน) ใช้ระบบ ADSL ในการเชื่อมต่อระบบอินเตอร์เน็ต

3. จัดหาอุปกรณ์สำรองข้อมูลทดแทนอุปกรณ์ที่ชำรุด โดยจำหาหน่วยจัดเก็บข้อเก็บข้อมูลแบบ SCSI RAID เพื่อนำมาใช้ทดแทน จำนวน 1 ชุด และสำรองไว้จำนวน 1 ชุด

5. กรณีข้อมูลสูญหาย มอบหมายให้เจ้าหน้าที่ประจำศูนย์ทำการ Backup ข้อมูลประจำทุกรายสัปดาห์ โดยใช้ดีวีดีรอมอีกหนึ่งชุดเพื่อแยกเก็บ

6. การทดสอบระบบที่ทำการ Backup โดยการ Recovery ที่เครื่อง Server สำรอง เพื่อตรวจสอบข้อมูลที่ได้ทำการ Backup ไว้ว่าสามารถใช้ได้จริง

7. กรณีมีการโจมตีของไวรัสและหนอนอินเตอร์เน็ตมอบหมายให้เจ้าหน้าที่ประจำศูนย์ทำการตรวจสอบและติดตามการแพร่ระบาดของไวรัสเป็นรายวัน พร้อมทั้งติดตั้งเพิ่ม Service Pack และหมั่น Update Virus Data

8. ปรับปรุงระบบเพื่อให้สามารถรองรับ พรบ .คอมพิวเตอร์ ปี 2550 โดยการจัดทำระบบตรวจสอบสิทธิเพื่อการใช้งานระบบอินเตอร์เน็ตในระดับ User โดยใช้ Radius Server ตรวจสอบสิทธิสำหรับบุคคลภายในและภายนอกที่เข้ามาใช้บริการระบบเครือข่ายภายในสำนักงานสาธารณสุข

5. ระยะเวลาดำเนินการ (ปีงบประมาณ 2552)

วันที่ 1 ตุลาคม 2551 ถึงวันที่ 30 กันยายน 2552

6. งบประมาณ

ใช้งบปกติของหน่วยงาน

7. ผลที่คาดว่าจะได้รับ

ระบบฐานข้อมูลสารสนเทศของ ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์ มีความปลอดภัยและสามารถใช้งานได้อย่างมีประสิทธิภาพสูงสุด

8. หน่วยงานรับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดสุรินทร์

9. การประเมินโครงการ

สรุปผลการดำเนินโครงการเมื่อสิ้นสุดโครงการ โดยผู้รับผิดชอบโครงการ