แผนการแก้ไขปัญหาภัยพิบัติ
ด้านเทคโนโลยีสารสนเทศ ศูนย์ข้อมูลจังหวัดอุทัยธานี

(IT Contingency Plan)

พ.ศ. 2553-2554

กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร

สำนักงานจังหวัดอุทัยธานี ศูนย์ปฏิบัติกาจังหวัด(POC)

โทร/โทรสาร 0-5651-1063

สารบัญ

หน้า

1. หลักการและเหตุผล	1
2. วัตถุประสงค์	1
3. การประเมินสถานการณ์ความเสี่ยง	4
3.1 ภัยที่เกิดจากบุคลากรของหน่วยงาน	4
3.2 ภัยที่เกิดจากไวรัสคอมพิวเตอร์	4
3.3 ภัยที่เกิดจากระบบไฟฟ้า	4
3.4 ภัยที่เกิดจากการโจรกรรม	4
4. แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ	5
4.1 การเตรียมการเบื้องต้น	6
4.2 การกำหนดผู้รับผิดชอบ	8
4.3 สถานที่สำรองข้อมูล	10
4.4 แนวทางการปฏิบัติ	10
5. แผนทำให้ระบบคอมพิวเตอร์กลับสู่สภาพเดิม	14
6. การติดตามและรายงานผล	14
เอกสารแนบท้าย	15

1. หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานด้านต่างๆ ของจังหวัดอุทัยธานี ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานต่างๆ ทำให้การดำเนินงานของจังหวัดมีความสะดวกรวดเร็ว มีประสิทธิภาพ แต่การใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการที่ต้องคำนึงถึง

ภัยที่เกิดกับระบบเทคโนโลยีสารสนเทศ มีอัตราการเกิดเพิ่มขึ้น ตามความก้าวหน้าของเทคโนโลยีสารสนเทศ ภัย “Threat” หมายความว่า อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศโดยฝีมือคน (Human) ได้แก่ บุคลากรของหน่วยงานที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ ทั้งเจตนา และไม่เจตนา ด้วยความรู้เท่าไม่ถึงการณ์ถึงสิ่งต่างๆ หรือ เหตุการณ์ต่างๆ อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผย เปลี่ยนแปลง หรืออาจถูกทำลาย ระบบสารสนเทศหยุดการทำงาน

เพื่อเป็นการลดภัยดังกล่าวที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัด หรือศูนย์ข้อมูลกลางของจังหวัด (POC) จึงเห็นควรให้จัดทำแผนการแก้ไขปัญหาภัยพิบัติด้านระบบเทคโนโลยีสารสนเทศจังหวัดอุทัยธานี เพื่อรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น

2. วัตถุประสงค์

การวางแผนเพื่อรองรับเหตุการณ์เมื่อประสบภัยพิบัติ เป็นแผนสำรองกรณีฉุกเฉินเพื่อรองรับความเสียหายจากเหตุการณ์ที่อาจเกิดขึ้นโดยไม่คาดคิด เช่น ไฟไหม้อาคาร ระเบิด ตึกถล่ม เป็นต้น วัตถุประสงค์ของการจัดทำแผนฉุกเฉินนี้ เพื่อตอบสนองนโยบายในด้านการรักษาความปลอดภัยของข้อมูล รวมถึงการประสานกับหน่วยงานต่าง ๆ เพื่อใช้ในการสำรองข้อมูล ทำให้ทำงานได้รวดเร็วยิ่งขึ้น เพื่อประโยชน์ขององค์กร เกิดผลกระทบน้อยที่สุดหรือสามารถปฏิบัติงานในด้านต่างๆ ต่อไปได้เป็นปกติ โดยเร็วที่สุด หากมีเหตุการณ์ดังกล่าวเกิดขึ้น โดยมีวัตถุประสงค์ ดังนี้

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคง ความปลอดภัยของฐานข้อมูลและสารสนเทศ ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
2. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
5. เพื่อสร้างความเข้าใจร่วมกัน ระหว่างผู้บริหาร และผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัย ของฐานข้อมูลและสารสนเทศของสำนักงานจังหวัดอุทัยธานี

3. การประเมินสถานการณ์ความเสี่ยง

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในด้านเทคโนโลยีสารสนเทศ ของสำนักงานจังหวัดอุทัยธานี พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

3.1 เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจ ในการใช้งานเครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศ เสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศ ได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบ เทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรมสัมมนา ให้มีความรู้ ความเข้าใจ ในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน ความผิดพลาด ที่เกิดจาก บุคลากรให้น้อยที่สุด

3.2 เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

2.1 ติดตั้ง firewall ทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องให้บริการ (server) และ เครื่องลูกข่าย (client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย

2.2 แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่าย Internet รวมทั้งแนะนำวิธีการ ป้องกัน และการกำจัดภัยที่จะเกิดจากไวรัสต่างๆให้เจ้าหน้าที่ได้ศึกษา และสามารถปฏิบัติการป้องกัน และแก้ไขปัญหาในเบื้องต้นได้

3.3 จากระบบไฟฟ้าขัดข้อง หรือความเสียหายจากเพลิงไหม้ โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) ในกรณีเกิดกระแส ไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บ และ สำรองข้อมูลไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงไหม้ มีระบบควบคุม ป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่างๆในอาคารและทำป้ายบอก จุด ติดตั้งเพื่อดับเพลิง

3.4 เกิดจากการโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์ในส่วนของห้องคอมพิวเตอร์แม่ข่ายได้กำหนดห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของฝ่าย เทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ติดตั้งเครื่องอ่านบัตรแบบ แม่เหล็กเพื่อป้องกันไม่ให้บุคคลภายนอกเข้ามาในหน่วยงานโดยไม่ได้รับอนุญาต ในอนาคตคาดว่าจะมี การติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

4. แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ

มีการวิเคราะห์ความเสี่ยงในรูปแบบต่างๆ ที่อาจเกิดขึ้น รวมทั้งมีมาตรการในการบริหารจัดการความเสี่ยง เพื่อให้การบริหารและจัดการกับระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีที่เกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น มีรายละเอียดดังนี้

1. แผนป้องกัน

มีวัตถุประสงค์เพื่อป้องกัน โอกาสอันเป็นเหตุให้เกิดภัยพิบัติ หรือเพื่อลด ขจัดเหตุภัยที่อาจจะเกิดขึ้นระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

2. แผนแก้ไข

มีมาตรการ 4 แนวทาง

2.1 การตรวจสอบและสรุปสาเหตุเบื้องต้น การสังเกตอาการ หรือเหตุอันผิดปกติ มี 2 องค์ประกอบ คือ

1) ทางกายภาพ สภาพอันผิดปกติ เช่น กลิ่น อุณหภูมิ ไฟฟ้าดับ เสียง อาการสั่ง
2) การทำงานของระบบ เช่น ไม่สามารถเข้าระบบงานได้ ,ระบบทำงานผิดพลาด มีข้อความแจ้งเหตุอันผิดปกติ สรุป จดบันทึกข้อความ หรือ Print Screen หน้าจอที่ผิดปกติ

2.2 การแจ้งเหตุ

1) แจ้งเหตุกรณีเร่งด่วน ประสานแจ้งผู้ที่เกี่ยวข้องโดยตรง ได้แก่ หัวหน้ากลุ่มเจ้าหน้าที่ภายในกลุ่มงานสารสนเทศและการสื่อสารจังหวัด หรือเจ้าหน้าที่ที่เข้าเวรยามประจำอาคาร ศาลากลางจังหวัด หรือเจ้าหน้าที่ตำรวจ
2) แจ้งเหตุกรณีปกติ สรุปสาเหตุและจัดทำรายงานแจ้งไปยังผู้ที่เกี่ยวข้อง และเจ้าหน้าที่ผู้รับผิดชอบรายงานผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

2.3 การประเมินสถานการณ์

โดยการแจ้งผู้รับผิดชอบ หรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ

2.4 แนวทางการปฏิบัติ

กรณีเครื่องคอมพิวเตอร์แม่ข่ายของระบบข้อมูล สารสนเทศจังหวัดอุทัยธานีไม่สามารถให้บริการได้ เนื่องจากเกิดภัยพิบัติจากสาเหตุต่อไปนี้

2.1 เครื่องแม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี
2.2 ตัวเครื่องแม่ข่ายเกิดปัญหาไม่สามารถให้บริการได้ สาเหตุอาจมาจากจานบันทึก ข้อมูล (Hard Disk) เสียหาย, อุปกรณ์จ่ายไฟเสีย ฯลฯ
2.3 เกิดไฟไหม้ตัวเครื่องแม่ข่าย หรือภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย
2.4 เครื่องแม่ข่ายถูกโจรกรรม
2.5 ข้อมูลสูญหาย
2.6 การเชื่อมโยงเครือข่ายล้มเหลว

4.1 การเตรียมการเบื้องต้น

4.1 การสำรองข้อมูล (Back up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูล ที่มีปัญหากลับมาใช้งานได้ โดยมีแนวทาง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูลไว้ในเทปบันทึกข้อมูล

4.2 การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟแวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับ เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งาน จำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยมีวิธีการดังนี้

4.2.1 ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัส
- อัพเดตข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

4.2.2 ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆเช่น แผ่นดิสก์ แผ่นซีดี เป็นต้น

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆที่ไม่รู้จักหรือน่าสงสัย เช่น .pif
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

4.2.3 ใช้ความระมัดระวังในการเปิด E-mail

- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

4.2.4 ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น ICQ MSN
- ไม่ควรเข้าไปเปิด website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลด ไฟล์ จาก website ที่ไม่น่าเชื่อถือ

• ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

• หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

4.3 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เป็นการป้องกันและแก้ไข ปัญหา จากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

4.3.1 ติดตั้งเครื่องสำรองไฟฟ้า และปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความ เสียหาย ที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วน ของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลา ใน การสำรองไฟฟ้าได้ประมาณ 20-30 นาที

4.3.2 เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุง รักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

4.3.3 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิด เครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ

4.3.4 มีระบบป้องกันไฟไหม้ เนื่องจากยังขาดงบประมาณในการสนับสนุนการปรับปรุง ห้อง คอมพิวเตอร์แม่ข่าย จึงยังไม่มีระบบป้องกันไฟไหม้ที่เหมาะสม แต่ในเบื้องต้น มีอุปกรณ์ดับเพลิงติดตั้ง ในทุกอาคาร เพื่อการควบคุมเพลิงในเบื้องต้น

4.3.5 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัย ให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

4.3.5.1 มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์ แม่ข่ายและการป้องกัน ความเสียหายโดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หาก จำเป็น ให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป ที่ประตูเข้าออก มี การติดตั้งสายูและกุญแจล็อค ในอนาคตคาดว่าจะได้ติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม

4.3.5.2 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่าย อินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

4.3.5.3 มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ต ของ องค์กรและกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการ

กำหนดค่า Configuration ให้มีความปลอดภัย ต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

4.3.5.4 มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่าย อินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการ เรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

4.3.5.5 การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ ทั้งในส่วนกลาง และส่วน ภูมิภาค ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (user name) และรหัสผ่าน (password) เพื่อตรวจสอบ ก่อนระบบอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ความรับผิดชอบ

4.3.5.6 การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

4.3.6 การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบ เทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นหน่วยงานหลักที่ดูแล ด้านระบบเครือข่าย คอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้อง ใช้งาน ไม่ได้ โดยมีการ เตรียมอุปกรณ์ดังนี้

4.3.6.1 แผ่นติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ

4.3.6.2 เทปสำรองข้อมูลและระบบงานที่สำคัญ

4.3.6.3 แผ่นโปรแกรม antivirus/spyware

4.3.6.4 แผ่น driver อุปกรณ์ต่างๆ

4.3.6.5 ระบบสำรองไฟฉุกเฉิน

4.3.6.6 อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

4.2 การกำหนดผู้รับผิดชอบ

รายชื่อเจ้าหน้าที่ศูนย์ปฏิบัติการจังหวัด POC ในการแก้ไขปัญหาที่เกิดจากภัยพิบัติ

ชื่อ-สกุล	ตำแหน่ง	หน้าที่ในการแก้ไขปัญหา
1.นายจินดา ทวีปัญญายศ	หัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสาร	ควบคุม กำกับ ดูแลเจ้าหน้าที่ศูนย์ปฏิบัติการ POC ในการปฏิบัติตามแผนปฏิบัติงาน
2.นางสาวพรพรรณ บุญศรี	นักวิเคราะห์นโยบายและแผนชำนาญการ	ประสานหน่วยงาน สถานที่ทำงานสำรอง และผู้เกี่ยวข้องในการปฏิบัติงาน สรุปผลการดำเนินงานตามขั้นตอนและ ความเสียหายเสนอผู้บังคับบัญชา ตามลำดับ
3.นายชัยวัฒน์ ขำศรี 4. นางสาวชารินีย์ สาหร่ายทอง	ครูชำนาญการพิเศษ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ดูแลระบบ แก้ไข Server ฐานข้อมูล ณ สถานที่สำรองข้อมูล Back up Database และ Restore กรณีเกิดปัญหา รวมทั้งให้คำแนะนำแก่เจ้าหน้าที่ศูนย์ปฏิบัติการจังหวัด
5.นายศิริวัฒน์ อภิณหพานิชย์ 6.นายจักกฤษณ์ จิตตานันท์	นายช่างไฟฟ้าชำนาญงาน นายช่างโยธาชำนาญงาน	ดำเนินการย้าย หรือติดตั้งระบบไฟฟ้า โทรศัพท์ ระบบการส่งแฟกซ์ เครื่องคอมพิวเตอร์ ซ่อมแก้ไข บำรุงรักษา อุปกรณ์ Software และ Hardware
7.นางดวงรัตน์ พิพัฒนชวลิตกุล 8.นายสุรศักดิ์ วิริยาภรณ์ประภาส 9.นายกมลศักดิ์ วิมลลักษณ์	เจ้าพนักงานธุรการ ชำนาญงาน นักวิชาการสาธารณสุขชำนาญการ เจ้าพนักงานสาธารณสุขชำนาญงาน	จัดเก็บ บันทึก ข้อมูลใหม่ กรณีข้อมูลเสียหายบางส่วน และบริการฐานข้อมูลกับหน่วยงานที่เกี่ยวข้อง

4.3 สถานที่สำรองข้อมูล

เมื่อเกิดภาวะฉุกเฉิน ซึ่งสถานที่ทำงานเดิมไม่สามารถดำเนินการได้เลย จะต้องประกาศภาวะฉุกเฉิน และนำแผนแก้ไขปัญหาภัยพิบัติ คือ แผนปฏิบัติการ POC 2 มาใช้ปฏิบัติ โดยกำหนดสถานที่สำรองข้อมูล (Back up) โรงเรียนอนุบาลเมืองอุทัยธานี และสถานที่ที่ปฏิบัติการสำรองนอกสถานที่ (Back up site) สำนักงานเขตพื้นที่การศึกษาอุทัยธานีเขต 1

4.4 แนวทางการปฏิบัติ

เพื่อให้สามารถแก้ไขปัญหาได้ทันท่วงที จึงกำหนดให้มีแนวทางในการปฏิบัตงานในขณะที่เกิดเหตุภัยพิบัติขึ้น โดยแบ่งเป็นกรณี ดังต่อไปนี้

กรณีที่ 1 : เครื่องคอมพิวเตอร์แม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี

1. การสรุปเหตุเบื้องต้น โดยเครื่องคอมพิวเตอร์จะมีการทำงานที่ผิดปกติไป

1.1 เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ เช่น ไม่สามารถ Log in เข้าระบบได้ (กรณีการเข้าระบบโดยไฟล์สิทธิ์ถูกทำลายด้วยวิธีการลบ แก้ไข หรือปรับเปลี่ยนข้อมูล)

1.2 ไฟล์งานในเครื่องคอมพิวเตอร์หายไป โดยการสังเกตจากข้อความที่แจ้งเตือน

1.3 โปรแกรมไม่สามารถทำงานได้ (Run ไม่ขึ้น)

1.4 อาจมีข้อความ (System message) ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

2.การแจ้งเหตุ โดยทำการ

2.1 จดบันทึก สรุป อาการที่ผิดปกติ

2.2 คัดลอก (Print Screen) หน้าจอที่ผิดปกติ

3. การประเมินสถานการณ์ โดยการแจ้งผู้รับผิดชอบ หรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ

4. แนวทางการปฏิบัติ

กรณีระบบมีปัญหาต้องติดตั้งระบบใหม่ สำหรับศูนย์ปฏิบัติการจังหวัดอุทัยธานี (POC) มีขั้นตอนการติดตั้งระบบดังนี้

1. การติดตั้งโปรแกรมระบบปฏิบัติการ Windows 2003 Server
2. การตั้งค่าระบบการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย
3. การนำเข้าข้อมูลจากระบบสำรองข้อมูลเข้ามาในระบบฐานข้อมูลเดิม

กรณีที่ 2 : ตัวเครื่องแม่ข่ายเกิดปัญหาไม่สามารถให้บริการได้ สาเหตุอาจมาจากจานบันทึกข้อมูล (Hard Disk) เสียหาย

1. การสรุปเหตุเบื้องต้น โดยสังเกตว่า

1.1 เกิดเสียงดังผิดปกติ

1.2 อุปกรณ์มีอาการสั่น

1.3 ไม่ทำงาน

1.4 ให้สังเกตว่าจอคอมพิวเตอร์ (Monitor) มีข้อความเตือน (Message Warning)

2. การแจ้งเหตุ โดยทำการ

2.1 จด / สรุป / อาการ ที่ผิดปกติ

2.2 คัดลอก (Print Screen) หน้าจอที่ผิดปกติ

3. การประเมินสถานการณ์ โดยการแจ้งผู้รับผิดชอบ หรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ

4. แนวทางการปฏิบัติ

ทำการสำรองข้อมูล(Back Up) จัดเก็บไว้ในจานบันทึกข้อมูล แบบภายนอก \ หรือ เขียนใส่แผ่น ซีดีรอม

กรณีที่ 3 : เกิดไฟไหม้ตัวเครื่องแม่ข่าย หรือภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย

1. การสรุปเบื้องต้น โดยสังเกตจาก

1.1 การตรวจเวรดูอุณหภูมิ ควัน กลิ่น ที่ผิดปกติ

1.2 สัญญาณของเครื่องตรวจจับอุณหภูมิ หรือควัน กลิ่น ที่ผิดปกติ

2. การแจ้งเหตุ โดยทำการ

2.1 กดสัญญาณเตือนภัยไว้รับทราบ เพื่อการอพยพเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายที่สำคัญ

2.2 ระบบแจ้งเหตุเตือนภัย ส่งสัญญาณแจ้งเหตุโดยอัตโนมัติ

3. การประเมินสถานการณ์ โดยการแจ้งเจ้าหน้าที่เวรรักษาความปลอดภัย / ตำรวจ เพื่อประสานแจ้งหน่วยดับเพลิง ในกรณีควบคุมเพลิงไม่ได้

4. แนวทางการปฏิบัติ

4.1 ทำการตัดวงจรไฟฟ้าและใช้อุปกรณ์ดับเพลิงเคมีที่ติดตั้งไว้ภายในอาคารศาลากลางจังหวัด ทำการดับเพลิงในกรณีที่สามารถควบคุมเพลิงได้ และประสานแจ้งหน่วยดับเพลิง ในกรณีควบคุมเพลิงไม่ได้

4.2 ทำการกันผู้ที่ไม่เกี่ยวข้องให้ออกจากที่เกิดเหตุโดยด่วน

4.3 นำเครื่องคอมพิวเตอร์แม่ข่ายสำรองมาติดตั้งให้บริการแทนโดยเร็วที่สุด

กรณีที่ 4 : เครื่องคอมพิวเตอร์แม่ข่ายถูกโจรกรรม

1.การสรุปเหตุเบื้องต้น โดยสังเกตจาก

1.1 สังเกตเหตุอันผิดปกติ เช่น มีการงัดแงะและเจาะ หรือร่องรอยการทำลายเพื่อการโจรกรรม

1.2 การสรุปสถานการณ์เพื่อประสานงานผู้เกี่ยวข้องต่อไป

2. การแจ้งเหตุ โดยทำการ

2.1 โทรศัพท์แจ้งเหตุผู้ที่เกี่ยวข้องโดยตรง เช่น ตำรวจ เจ้าหน้าที่เวร รักษาความปลอดภัยประจำอาคารศาลากลางจังหวัดโดยด่วน

3. การประเมินสถานการณ์

3.1 จัดให้มีเวรยาม โดยเจ้าหน้าที่ตำรวจ เจ้าหน้าที่เวรรักษาความปลอดภัย

3.2 กรณีห้องเครื่องคอมพิวเตอร์แม่ข่าย มอบหมายให้มีเจ้าหน้าที่ดูแลรับผิดชอบกุญแจโดยตรง

3.3 จัดให้มีการทำการตรวจตราการปิดประตู กุญแจทุกครั้งก่อนปิดห้อง

3.4 จัดให้มีระบบโทรทัศน์วงจรปิด บันทึกภาพในอาคาร

4. แนวทางการปฏิบัติ

4.1 ให้ติดต่อเจ้าหน้าที่ หรือ เจ้าหน้าที่ที่เกี่ยวข้อง ประสานงานโดยการนำข้อมูลสำรองมาทำการติดตั้ง ให้บริการทดแทน

4.2 ทำการทดสอบระบบ หลังการติดตั้ง โดยเริ่มระบบเพื่อตรวจสอบการทำงาน

4.3 ทำการตรวจสอบข้อมูล ว่าข้อมูลมีความถูกต้อง ครบถ้วน สมบูรณ์ ทันสมัย มีความน่าเชื่อถือ สามารถนำมาใช้ประโยชน์ได้

4.4 ติดตามผลการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย

กรณีที่ 5 : ข้อมูลสูญหาย

1. การสรุปเบื้องต้น

1.1 เกิดความผิดปกติทางกายภาพ เช่น ดิสก์สูญหาย หรือเสียหาย

1.2 เกิดจากการทำงานของระบบ

1.2.1 ไม่สามารถเข้าถึงข้อมูลได้

1.2.2 โปรแกรมระบบฐานข้อมูลไม่ทำงาน

1.2.3 อุปกรณ์คอมพิวเตอร์บางตัว ไม่ทำงาน ติดต่อกับฮาร์ดดิสก์ (Hard Disk) ไม่ได้

1.2.4 มีข้อความแจ้งเหตุที่ผิดปกติ

2. การแจ้งเหตุ โดยทำการจดบันทึก / สรุป และทำการ Print Screen ข้อความที่ผิดปกติ

3. การประเมินสถานการณ์ (Incident Evaluation) แจ้งเหตุให้เจ้าหน้าที่ที่เกี่ยวข้องทราบ
4. แนวทางการปฏิบัติ (Response Operation)

4.1 นำฮาร์ดดิสก์ (Hard Disk) สำรองมาทำการติดตั้ง

4.2 ทดสอบการเชื่อมต่อ

4.3 ทดสอบการทำงานของระบบโดยรวม

4.4 กรณีที่ต้องปรับข้อมูล ต้องทำการปรับข้อมูลตามช่วงวันที่ที่ต้องการ

4.5 นำข้อมูลสำรอง (Back Up) ในช่วงที่ต้องการมากู้คืนข้อมูล

4.6 ทำการตรวจสอบความถูกต้องของข้อมูล ว่าข้อมูลมีความสมบูรณ์ ครบถ้วน มีความน่าเชื่อถือ

4.7 มอบหมายให้มีเจ้าหน้าที่ที่รับผิดชอบทำการสำรองข้อมูล

4.8 การสำรองข้อมูล (Export Data) ลงชื่อผู้ทำการสำรองข้อมูลอย่างสม่ำเสมอ

4.9 ทำการสำรวจผลการสำรองข้อมูล

4.10 ทำการสำรองข้อมูลเต็มรูปแบบ (Full Back UP) ของทุกๆเดือน

4.11 ตรวจสอบการทำงานของฐานข้อมูลหลังจากดำเนินการเสร็จ

กรณีที่ 6 : การเชื่อมโยงเครือข่ายล้มเหลว

1. การสรุปเหตุเบื้องต้น

1.1 เครื่องคอมพิวเตอร์ในศูนย์ปฏิบัติการจังหวัดและผู้บริหารระดับสูง ของจังหวัดไม่สามารถเรียกดูข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายของศูนย์ปฏิบัติการจังหวัดได้

1.2 เครื่องคอมพิวเตอร์จากศูนย์ปฏิบัติการกระทรวงมหาดไทยไม่สามารถเรียกดูข้อมูลจากศูนย์ปฏิบัติการจังหวัดได้

1.3 เครื่องคอมพิวเตอร์ในศูนย์ปฏิบัติการจังหวัดไม่สามารถเรียกดูข้อมูลจากศูนย์ปฏิบัติการเขต/กระทรวง ได้

2. การแจ้งเหตุ

โดยทำการให้เจ้าหน้าที่ของศูนย์ปฏิบัติการจังหวัดตรวจสอบระบบเครือข่ายภายใน (LAN) และเครือข่ายทางด่วนข้อมูลของกระทรวงมหาดไทย (ATM Network) พร้อมสรุปเหตุขัดข้อง

3. การประเมินสถานการณ์

เจ้าหน้าที่ของศูนย์ปฏิบัติการจังหวัด ต้องตรวจสอบและแจ้งสาเหตุที่ขัดข้องให้ชัดเจนว่าอยู่ในกรณีใดตามข้อ 1 และดำเนินการแก้ไขการเชื่อมโยงเครือข่ายต่อไป

4. แนวทางการปฏิบัติ

4.1 เจ้าหน้าที่ช่างประจำศูนย์ปฏิบัติการจังหวัด วิเคราะห์ ตรวจสอบ หาสาเหตุ

ขัดคข้องของอุปกรณ์เชื่อมโยงเครือข่าย

4.1.1 แก้ไขด้วย Software กรณีขัดข้องในเรื่อง configuration

4.1.2 แก้ไขโดยใช้อุปกรณ์ Hardware สับเปลี่ยน กรณีอุปกรณ์เครือข่ายเสีย

4.2 หลังการตรวจสอบ แก้ไขเสร็จเรียบร้อยแล้ว ให้ทำการทดลองระบบ และตรวจสอบผลการใช้งาน

4.3 บันทึกผลการตรวจสอบ แก้ไข

5. แผนทำให้ระบบคอมพิวเตอร์กลับสูสภาพเดิม

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์ระจายสัญญาณ (System Recovery) โดยปกติ ระบบ เครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

5.1 จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

5.2 เปลี่ยนอุปกรณ์ชิ้นส่วนเสียหาย

5.3 ซ่อมบำรุงอุปกรณ์ที่ชำรุด เสียหายให้เสร็จภายใน 2 ชั่วโมง

5.4 ขอยืมอุปกรณ์คอมพิวเตอร์ จากหน่วยงานอื่นมาใช้ชั่วคราว

5.5 นำ BACKUPTAPE/CD-ROM/HARDDISKที่ได้สำรองข้อมูลไว้ไว้นำกลับมาrestoreโดยใช้ผู้ที่มีหน้าที่กู้ระบบ (ผู้ดูแลระบบกับนักวิชาการคอมพิวเตอร์และทีมงานจากบริษัทฯที่พัฒนาระบบสารสนเทศ) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

5.6 ทำการตรวจสอบระบบปฏิบัติการระบบฐานข้อมูลตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆที่เกี่ยวข้อง

7. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กับกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ได้ระบุไว้

เอกสารแนบท้าย

รายชื่อที่อยู่หมายเลขโทรศัพท์ของเจ้าหน้าที่ที่รับผิดชอบในการปฏิบัติตามแผน

ลำดับที่	ชื่อ-สกุล	ตำแหน่ง	เบอร์โทรศัพท์ที่สามารถติดต่อได้
1	นายจินดา ทวีปัญญายศ	หัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสาร	ข่ายมหาดไทย 17929 มือถือ 08 9203 4430
2	นางสาวพรพรรณ บุญศรี	นักวิเคราะห์นโยบายและแผน ชำนาญการ	ข่ายมหาดไทย 17929 มือถือ 08 6734 3317
3	นางสาวชาลินีย์ สาหร่ายทอง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ข่ายมหาดไทย 18028 มือถือ 08 6734 3317
4	นายศิริวัฒน์ อภิณหพานิชย์	นายช่างไฟฟ้าชำนาญงาน	ข่ายมหาดไทย 18028 มือถือ 08 1284 7172
5	นายจักกฤษณ์ จิตตานันท์	นายช่างโยธาชำนาญงาน	ข่ายมหาดไทย 18028 มือถือ 08 7195 4646
5	นางดวงรัตน์ พิพัฒนชวลิตกุล	เจ้าพนักงานธุรการ ชำนาญงาน	ข่ายมหาดไทย 18028 มือถือ 08 6211 7001
5	นายสุรศักดิ์ วิริยาภรณ์ประภาส	นักวิชาการสาธารณสุขชำนาญการ	ข่ายมหาดไทย 18028 มือถือ 08 9857 1888
5	นายกมลศักดิ์ วิมลลักษณ์	เจ้าพนักงานสาธารณสุขชำนาญงาน	ข่ายมหาดไทย 18028 มือถือ 08 1888 0012