3.1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)

3.2 ภัยที่เกิด Software

3.3 ภัยที่เกิดจากไฟไหม้ หรือ ระบบไฟฟ้า

3.1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)

ศูนย์ปฏิบัติการจังหวัดสระแก้ว ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

1. ชี้แจงเจ้าหน้าที่ของหน่วยงานในจังหวัด ให้มีความรู้ความเข้าใจ ในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน human error ให้น้อยที่สุด เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก human error ลดน้อยลง

2. วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์

3.2 ภัยที่เกิด Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) , หนอนอินเตอร์เน็ต (Internet Worm) , ม้าโทรจัน (Trojan Horse) , และข่าวไวรัสหลอลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของจังหวัดสระแก้วใช้งานไม่ได้

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software

1. จังหวัดสระแก้วได้ตระหนักถึงปัญหาเหล่านี้ จึงได้ทำการติดตั้ง firewall ซึ่งเป็นฮาร์ดแวร์ติดตั้งอยู่ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟแวร์ป้องกันไวรัสที่เครื่องให้บริการ (server) และเครื่องลูกข่าย (client) ซึ่งทำหน้าที่เป็นซอฟต์แวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของจังหวัดสระแก้ว

2. แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านทางระบบอินทราเน็ตที่ http://10.2.14.31 อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจาก Software ดังกล่าว ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

3.3 ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งจังหวัดสระแก้วได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

แนวทางการปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้อง

ศูนย์ปฏิบัติการจังหวัดสระแก้วได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการดังนี้

1. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) จำนวน 3 เครื่อง เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) 5 ตัว ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งระบบสำรองไฟฟ้าที่ใช้ควบคุมระบบเครือข่ายของศูนย์ปฏิบัติการจังหวัดสระแก้ว สามารถสำรองไฟฟ้าเพื่อใช้งานได้นานประมาณ 30 นาที แต่ทั้งนี้จังหวัดได้มีระบบจ่ายไฟฟ้าสำรองติดตั้งไว้ด้วยแล้ว ในกรณีที่เกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

2. ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

3. ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

4. การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ของจังหวัดสระแก้ว ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

4.1 แผ่น book disk

4.2 แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

4.3 แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

4.4 แผ่นโปรแกรม antivirus/spyware

4.5 แผ่น driver อุปกรณ์ต่าง ๆ

4.6 ระบบสำรองไฟฉุกเฉิน

4.7 Hard disk สำรอง

ข้อควรปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติหรือการใช้งานระบบเครือข่ายขัดข้อง (Contingency Plan)

กรณีเครื่องลูกข่าย

1. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่ศูนย์ปฏิบัติการจังหวัดสระแก้วทราบ หรือกรณีมีเหตุอันทำให้ศูนย์ปฏิบัติการจังหวัดสระแก้วไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดจังหวัดสระแก้วทราบ

2. เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย Lan) ออกจากเครื่องนั้นโดยเร็ว

3. ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย Lan ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

4. ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด และ/หรือ

5. ขนย้ายเครื่องไปไว้ในที่ปลอดภัย

6. ให้เจ้าหน้าที่ศูนย์ปฏิบัติการจังหวัดสระแก้ว แจ้งเหตุขัดข้องนั้นให้ Chief Information Officer (CIO) ทราบโดยเร็วที่สุด

กรณีเครื่องบริการ (server) และอุปกรณ์เครือข่าย

1. ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

2. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

3. ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้ น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

4. รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

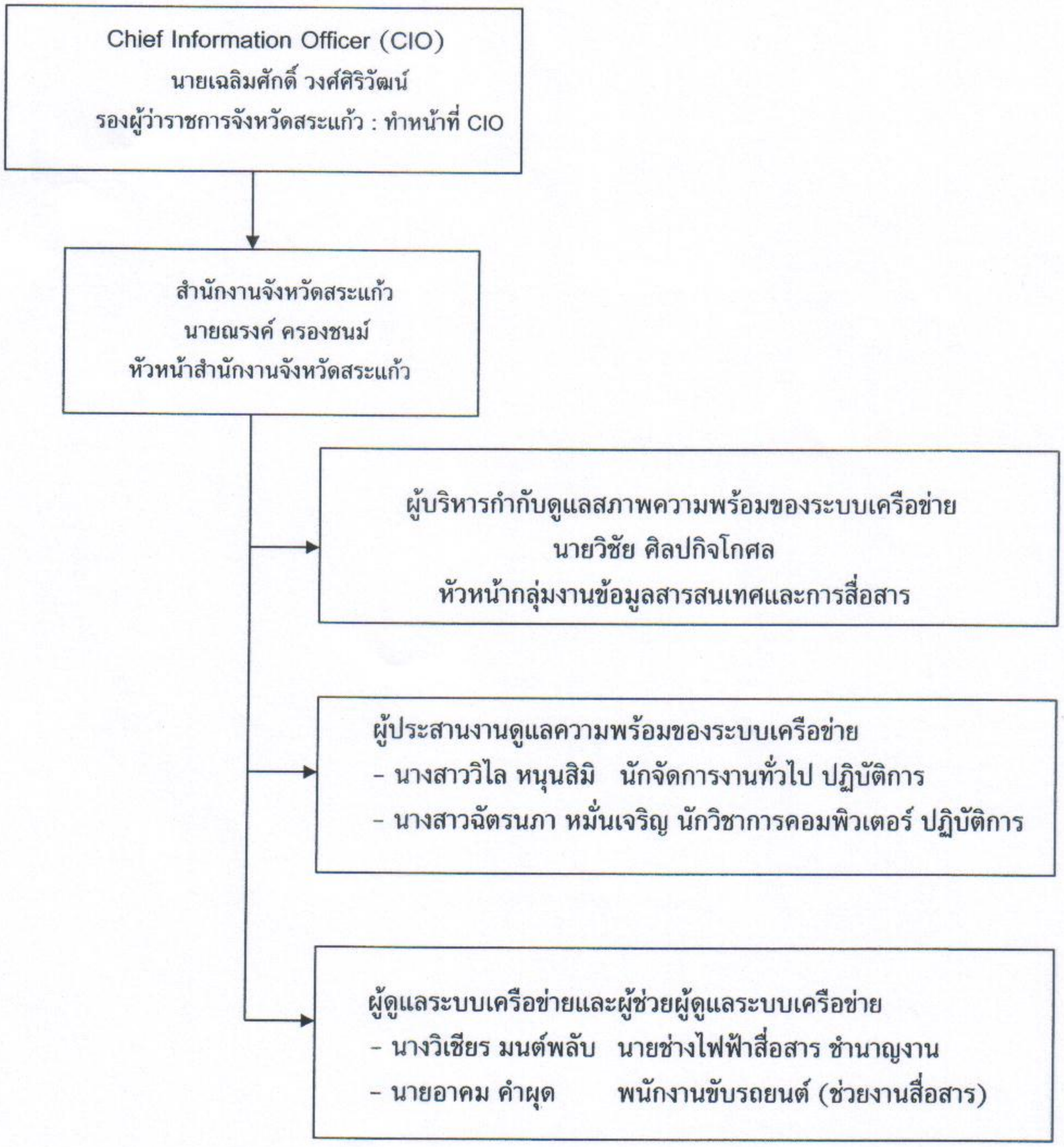
5. ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

6. ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

7. ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์สารสนเทศทราบโดยเร็ว

ข. แผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

เพื่อแก้ไขระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้วที่เกิดจากภัยพิบัติให้ใช้งานได้อย่างรวดเร็วและต่อเนื่องอย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ จังหวัดสระแก้วได้ดำเนินการจัดแบ่งหน้าที่และบุคลากรผู้รับผิดชอบดำเนินงาน ดังนี้



การจัดองค์กรปฏิบัติการฉุกเฉินในระบบสารสนเทศจังหวัดสระแก้วเมื่อเกิดเหตุฉุกเฉิน

การจัดองค์กรปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา (Lines of authority) เมื่อเกิดเหตุฉุกเฉิน

2.1 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

2.1.1 กำหนดนโยบายให้ศูนย์ปฏิบัติการจังหวัดสระแก้ว

2.1.2 ให้คำปรึกษาแก่ผู้อำนวยการศูนย์สารสนเทศในฐานะประธานศูนย์ฯ

2.2 หัวหน้าสำนักงานจังหวัด

2.2.1 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

2.2.2 มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

2.2.3 มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

2.2.4 ประชุมหารือกับคณะกรรมการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง

2.2.5 ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

2.2.6 รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริการเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

2.3 ผู้บริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย

2.3.1 วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการศูนย์สารสนเทศ

2.3.2 มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

2.3.3 สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

2.3.4 ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย

2.4 ผู้ประสานงานดูแลสภาพความพร้อมของระบบเครือข่าย

2.4.1 ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

2.4.2 รายงานให้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

2.4.3 กำหนดอัตรากำลังพล วัสดอปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

2.4.4 ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

2.5 ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administer and Staffs)

2.5.1 กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

2.5.2 พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่น ๆมาช่วย

2.5.3 ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

2.5.4 ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

2.5.5 หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุอุปกรณ์ ที่ชำรุดเสียหาย แล้วรายงานให้ประธานศูนย์ประสานงานรักษาความปลอดภัยสารสนเทศทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ Firewall
- ทำการตรวจสอบ Virus, worm, spy ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานฐานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

2.5.6 เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

2.5.7 ประสานงานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ข้อมูล

2.5.8 ทำการสำรองข้อมูลทุกวัน วันจันทร์-พฤหัส ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันศุกร์ การสำรองข้อมูลทั้งระบบ

2.5.9 ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup} รายชื่อโปรแกรม เอกสารที่เกี่ยวข้องกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรอง สำเนาคู่มือ

2.5.10 นำระบบสำรองข้อมูลออกมาใช้งานเพื่อให้ระบบสามารถดำเนินการต่อไปได้

ค. แผนทำให้ระบบคอมพิวเตอร์กลับสู่สภาวะเดิม (Disaster Recovery Plan)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery)

ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ โดยปกติจะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆได้ ตลอด 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้โดยเร็วที่สุดเท่าที่จะทำได้ เนื่องจากเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณต้องทำงานด้านบริการ(Service) แก่เครื่องลูกข่ายให้สามารถใช้งานได้ปกติ การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณจำเป็นต้องทำอย่างรวดเร็ว เพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด

แผนการนี้เป็นวิธีที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และแฟ้มข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน

1. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
5. นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมาrestoreใช้
6. ทีมกู้ระบบ (ผู้ดูแลระบบ นักวิชาการคอมพิวเตอร์ และทีมที่ปรึกษา) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง
7. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆที่เกี่ยวข้อง

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
(Contingency Plan)
ของศูนย์ปฏิบัติการจังหวัดสระแก้ว

- - - - - - - - - - - -

ศูนย์ปฏิบัติการจังหวัดสระแก้ว ได้มีการจัดทำแผนแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ซึ่งสามารถใช้เป็นแนวทางปฏิบัติการสำหรับระบบการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว เป็น 3 แผน มีรายละเอียด ดังนี้

ก. แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (Contingency Plan)

1. หลักการและเหตุผล

ปัจจุบันภัยที่เกิดแก่ระบบเทคโนโลยีสารสนเทศมีอัตราการเกิดเพิ่มขึ้น ตามความก้าวหน้าของเทคโนโลยีสารสนเทศ ภัยอันตรายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศอาจเกิดขึ้นได้โดยคน ซึ่งได้แก่ เจ้าหน้าที่บุคลากรของหน่วยงานที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ สถานการณ์ หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผย หรือเปลี่ยนแปลงทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่น ๆตามความต้องการของภัย ดังนั้นเพื่อเป็นการลดภัยดังกล่าวที่จะเกิดขึ้นในระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว จึงเห็นว่ามีความจำเป็นอย่างยิ่ง จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ จังหวัดสระแก้ว เพื่อรองรับสถานการณ์ดังกล่าวที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศจังหวัดสระแก้ว แผนนี้จัดแบ่งออกเป็น 3 ด้าน ได้แก่ แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan) , แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation plan) . และแผนฟื้นตัวจากภัยพิบัติ (Disaster Recovery Plan)

2. วัตถุประสงค์

2.1 เพื่อลดความเสียหายที่จะเกิดแก่ระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว

2.2 เพื่อให้ระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว สามารถดำเนินการได้อย่างต่อเนื่อง

2.3 เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว

3. การประเมินสถานการณ์ความเสี่ยง ที่อาจเกิดขึ้น

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆในระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว พบว่าความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว สามารถแยกเป็นภัยต่าง ๆได้ 3 ประเภท ดังนี้