แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
(Contingency Plan)
ของจังหวัดสระแก้ว

จังหวัดสระแก้ว ได้มีการจัดทำแผนแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ซึ่งสามารถใช้เป็นแนวทางปฏิบัติการสำหรับระบบการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว เป็น ๓ แผน มีรายละเอียด ดังนี้

ก. แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (Contingency Plan)

๑. หลักการและเหตุผล

ปัจจุบันภัยที่เกิดแก่ระบบเทคโนโลยีสารสนเทศมีอัตราการเกิดเพิ่มขึ้น ตามความก้าวหน้าของเทคโนโลยีสารสนเทศ ภัยอันตรายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศอาจเกิดขึ้นได้โดยคน ซึ่งได้แก่ เจ้าหน้าที่บุคลากรของหน่วยงานที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ สถานการณ์หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผย หรือเปลี่ยนแปลงทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่น ๆ ตามความต้องการของภัย ดังนั้นเพื่อเป็นการลดภัยดังกล่าวที่จะเกิดขึ้นในระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว จึงเห็นว่ามีความจำเป็นอย่างยิ่งจะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศจังหวัดสระแก้ว เพื่อรองรับสถานการณ์ดังกล่าวที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ แผนนี้จัดแบ่งออกเป็น ๓ ด้าน ได้แก่ แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบคอมพิวเตอร์ (Contingency Plan), แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continnuity of Operation plan) และแผนฟื้นตัวจากภัยพิบัติ (Disaster Recovery Plan)

๒. วัตถุประสงค์

๒.๑ เพื่อลดความเสียหายที่จะเกิดแก่ระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว

๒.๒ เพื่อให้ระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว สามารถดำเนินการได้อย่างต่อเนื่อง

๒.๓ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว

๓. การประเมินสถานการณ์ความเสี่ยง ที่อาจเกิดขึ้น

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ ในระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว พบว่าความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว สามารถแยกเป็นภัยต่างๆ ได้ ๓ ประเภท ดังนี้

๓.๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)

๓.๒ ภัยที่เกิด Software

๓.๓ ภัยที่เกิดจากไฟไหม้ หรือ ระบบไฟฟ้า

๓.๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ใช้ระบบเทคโนโลยีสารสนเทศได้อย่างไม่เต็มประสิทธิภาพ

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)

จังหวัดสระแก้ว ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ดังนี้

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

๒. วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์

๓.๒ ภัยที่เกิด Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), สปายแวร์ (Spyware) และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software

๑. จังหวัดสระแก้วได้ตระหนักถึงปัญหาเหล่านี้ จึงได้ทำการติดตั้ง firewall ซึ่งเป็นฮาร์ดแวร์ติดตั้งอยู่ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟแวร์ป้องกันไวรัสที่เครื่องให้บริการ (server) และเครื่องลูกข่าย (client) ซึ่งทำหน้าที่เป็นซอฟแวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของจังหวัดสระแก้ว

๒. แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านระบบอินทราเน็ตที่ http://๑๐.๒.๑๔.๓๑ อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่เกิดจาก Software ดังกล่าวให้เจ้าหน้าที่ได้ศึกษาและสามารถป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๓.๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งจังหวัดสระแก้วได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

แนวทางการปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้อง

จังหวัดสระแก้วได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการ ดังนี้

๑. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) จำนวน ๓ เครื่อง เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ๕ ตัว ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งระบบสำรองไฟฟ้าที่ใช้ควบคุมระบบเครือข่ายของจังหวัดสระแก้ว สามารถสำรองไฟฟ้าเพื่อใช้งานได้นานประมาณ ๓๐ นาที แต่ทั้งนี้จังหวัดได้มีระบบจ่ายไฟฟ้าสำรองติดตั้งไว้ด้วยแล้ว ในกรณีที่เกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

๒. ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์ อย่างสม่ำเสอม

๓. ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

๔. การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้ว กลุ่มงานอำนวยการ และกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด ซึ่งเป็นหน่วยงานที่ดูแลระบบเครือข่ายคอมพิวเตอร์ของจังหวัดสระแก้ว ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ไว้ ดังนี้

๔.๑ แผ่น book disk

๔.๒ แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

๔.๓ แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

๔.๔ แผ่นโปรแกรม antivirus/spyware

๔.๕ แผ่น driver อุปกรณ์ต่างๆ

๔.๖ ระบบสำรองไฟฉุกเฉิน

๔.๗ Hard disk สำรอง

ข้อควรปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติหรือการใช้งานระบบเครือข่ายขัดข้อง (Contingency Plan)

กรณีเครื่องลูกข่าย

๑. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่สำนักงานจังหวัดสระแก้วทราบ หรือกรณีมีเหตุอันทำให้ห้องควบคุมระบบเครือข่ายจังหวัดสระแก้วไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดสระแก้วทราบ

๒. เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย Lan) ออกจากเครื่องนั้นโดยเร็ว

๓. ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย Lan ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๔. ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด และ/หรือ

๕. ขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๖. ให้เจ้าหน้าที่สำนักงานจังหวัดสระแก้ว แจ้งเหตุขัดข้องนั้นให้ Chief Information Office (CIO) ทราบโดยเร็วที่สุด

กรณีเครื่องบริการ (server) และอุปกรณ์เครือข่าย

๑. ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓. ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้ น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔. รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

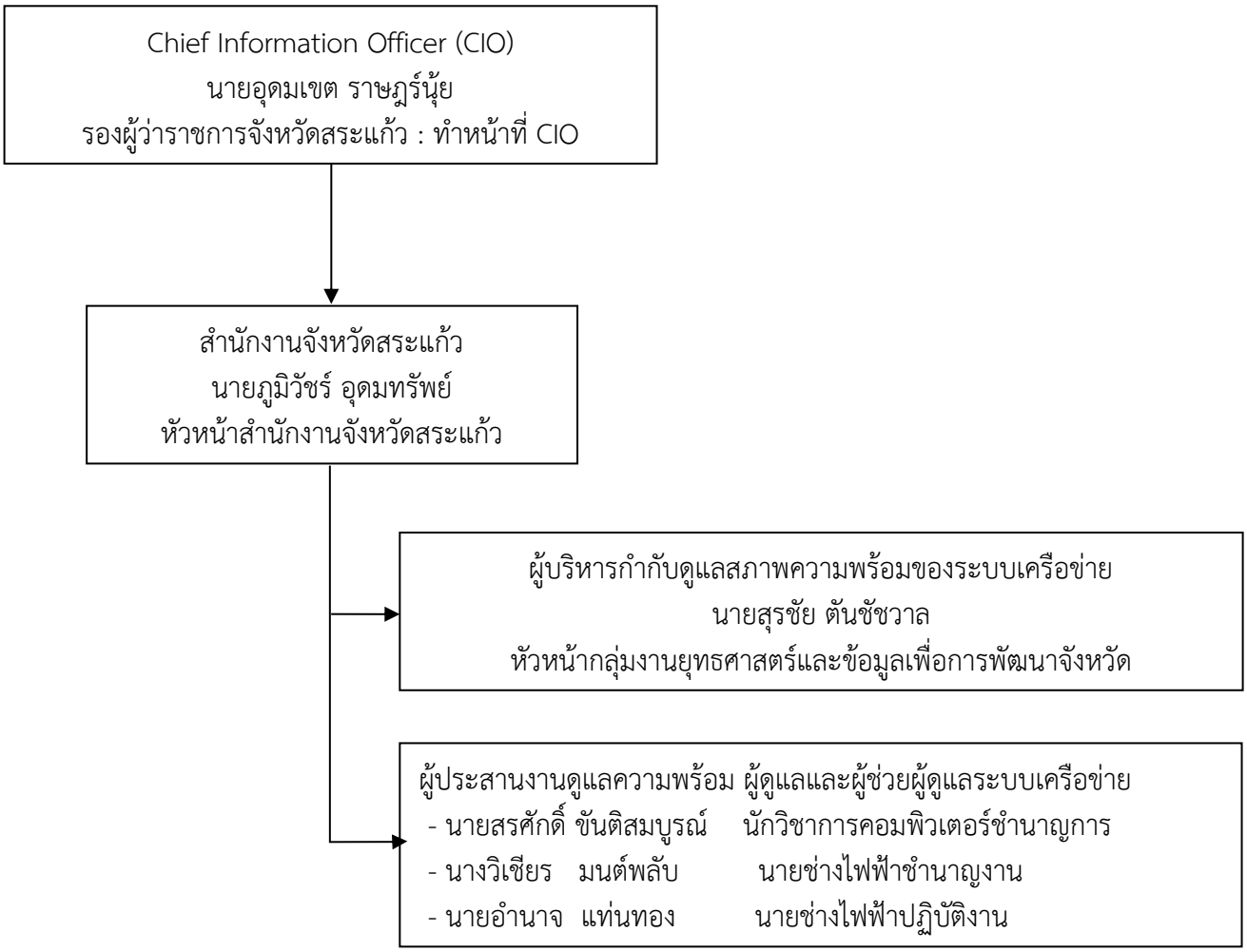
๕. ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖. ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗. ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์สารสนเทศทราบโดยเร็ว

ข. แผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

เพื่อแก้ไขระบบเทคโนโลยีสารสนเทศของจังหวัดสระแก้วที่เกิดจากภัยพิบัติให้ใช้งานได้อย่างรวดเร็ว ต่อเนื่อง และมีประสิทธิภาพ จังหวัดสระแก้วได้ดำเนินการจัดแบ่งหน้าที่และบุคลากรผู้รับผิดชอบดำเนินงาน ดังนี้



การจัดองค์กรปฏิบัติการฉุกเฉินในระบบสารสนเทศจังหวัดสระแก้วเมื่อเกิดเหตุฉุกเฉิน

การจัดองค์กรปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา (Lines of authority) เมื่อเกิดเหตุฉุกเฉิน

๒.๑ ผู้บริหารเทคโนโลยีสารเทศระดับสูง (Chief Information Officer : CIO)

๒.๑.๑ กำหนดนโยบายให้ศูนย์ปฏิบัติการจังหวัดสระแก้ว

๒.๑.๒ ให้คำปรึกษาแก่ผู้อำนวยการศูนย์สารสนเทศในฐานะประธานศูนย์ฯ

๒.๒ หัวหน้าสำนักงานจังหวัด

๒.๒.๑ เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๒.๒.๒ มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๒.๒.๓ มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

๒.๒.๔ มีประชุมหารือกับคณะกรรมการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์และคณะกรรมการอื่นที่เกี่ยวข้อง

๒.๒.๕ ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

๒.๒.๖ รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

๒.๓ ผู้บริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย

๒.๓.๑ วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการศูนย์สารสนเทศ

๒.๓.๒ มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

๒.๓.๓ สั่งการให้ผู้เกี่ยวข้องมาปฏิบัติตามแผนฯ

๒.๓.๔ ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตาที่ได้รับมอบหมาย

๒.๔ ผู้ประสานงานดูแลสภาพความพร้อมของระบบเครือข่าย

๒.๔.๑ ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง

๒.๔.๒ รายงานให้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

๒.๔.๓ กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

๒.๔.๔ ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๒.๕ ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administer and Staffs)

๒.๕.๑ กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

๒.๕.๒ พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ มาช่วย

๒.๕.๓ ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

๒.๕.๔ ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

๒.๕.๕ หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุอุปกรณ์ ที่ชำรุดเสียหาย แล้วรายงานให้ประธานศูนย์ประสานงานรักษาความปลอดภัยสารสนเทศทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ Firewall
- ทำการตรวจสอบ Virus, worm, spy ware
- ทำการตรวจสอบ UPS

- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานฐานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๒.๕.๖ เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

๒.๕.๗ ประสานงานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ข้อมูล

๒.๕.๘ ทำการสำรองข้อมูลทุกวัน วันจันทร์ – พฤหัสบดี ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันศุกร์ การสำรองข้อมูลทั้งระบบ

๒.๕.๙ ต้องเก็บสิ่งสำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup รายชื่อโปรแกรมเอกสารที่เกี่ยวข้องกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรอง สำเนาคู่มือ

๒.๕.๑๐ นำระบบสำรองข้อมูลออกมาใช้งานเพื่อให้ระบบสามารถดำเนินการต่อไปได้

ค. แผนทำให้ระบบคอมพิวเตอร์กลับสู่สภาวะเดิม (Disaster Recovery Plan)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery)

ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ โดยปกติจะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืน ให้ได้โดยเร็วที่สุดเท่าที่จะทำได้ เนื่องจากเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณต้องทำงานด้านบริการ (Service) แก่เครื่องลูกข่ายให้สามารถใช้งานได้ปกติ การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์ กระจายสัญญาณจำเป็นต้องทำอย่างรวดเร็ว เพื่อให้ได้อย่างรวดเร็วที่สุด

แผนการนี้เป็นวิธีที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และแฟ้มข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน

๑. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕. นำ Backup Tape / CD-ROM / Harddisk ที่ได้สำรองข้อมูลไว้นำกลับมา Restore ใช้

๖. ทีมกู้ระบบ (ผู้ดูแลระบบ นักวิชาการคอมพิวเตอร์ และทีมปรึกษา) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๗. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง