แผนรองรับภาวะฉุกเฉินและภัยธรรมชาติ
(IT Contingency Plan)

๑. <u>หลักการและเหตุผล</u>

กรมพัฒนาฝีมือแรงงาน ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงาน และให้บริการแก่ประชาชน มีการพัฒนาและการลงทุนที่ต้องใช้ระยะเวลาและการลงทุนสูง องค์ประกอบหลักของระบบเทคโนโลยี ซึ่งประกอบด้วย Hardware และ Software รวมทั้งระบบเครือข่ายที่มีการเชื่อมต่อกับช่องสัญญาณทั้งภายในและภายนอก จึงต้องมีการดูแลรักษาให้สามารถใช้งานได้ตลอดเวลา ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ซึ่งทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของกรม

ศูนย์ข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาฝีมือแรงงาน จึงได้ศึกษาเป้าหมายและแนวทางการดำเนินการ และได้จัดทำแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศขึ้นเพื่อป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้นในอนาคต

๒. <u>วัตถุประสงค์</u>

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๓. <u>การประเมินสถานการณ์ความเสี่ยงและแนวทางปฏิบัติ</u>

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ ของกรมพัฒนาฝีมือแรงงาน พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

๓.๑ เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนา ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด

๓.๒ เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

๑) ติดตั้ง Firewall เพื่อป้องกันไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมพัฒนาฝีมือแรงงานได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๒) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์เพื่อป้องกันไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์แม่ข่ายและมีการติดตั้งซอฟแวร์ป้องกันไวรัสที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๓.๓ เกิดจากระบบไฟฟ้าขัดข้อง หรือความเสียหายจากเพลิงไหม้ โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุมป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่างๆในอาคารและทำป้ายบอกจุดติดตั้งเพื่อดับเพลิง

๓.๔ เกิดจากโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์ ในส่วนของห้องคอมพิวเตอร์แม่ข่ายได้กำหนด ห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของศูนย์ข้อมูลเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ติดตั้งเครื่องอ่านบัตรแบบแม่เหล็กเพื่อป้องกันไม่ให้บุคคลภายนอกเข้ามาในหน่วยงานโดยไม่ได้รับอนุญาต และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๔. <u>การเตรียมการเบื้องต้น</u>

๔.๑ การสำรองข้อมูล (Back up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีแนวทาง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่าย เป็นประจำทุกสัปดาห์ โดยสำรองข้อมูลไว้ในเทปบันทึกข้อมูล

๔.๒ การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ โดยมีวิธีการดังนี้

๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัส
- อัพเดตข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น แผ่นดิสก์ แผ่นซีดี เป็นต้น
- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย เช่น .pif
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๓) ใช้ความระมัดระวังในการเปิด E-mail
- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet
- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น ICQ MSN
- ไม่ควรเข้าไปเปิด website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลด ไฟล์ จาก website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๔.๓ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์ แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ

๔.๔ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

๑) มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป ที่ประตูเข้าออก มีการติดตั้งระบบสแกนลายนิ้วมือที่ประตูห้องแม่ข่าย และติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๔) การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ ในกรมพัฒนาฝีมือแรงงาน ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (user name) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ความรับผิดชอบ

๔.๕ การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑) ควบคุมการใช้คอมพิวเตอร์และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องใช้คอมพิวเตอร์ หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์เป็นผู้รับผิดชอบนำเข้าไป

๒) จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์

๓) สอบถามเหตุผล/หน่วยงาน/ชื่อบุคลากรที่เข้าไปในห้องแม่ข่ายพร้อมกับจดบันทึกไว้เป็นหลักฐาน โดยมีรายละเอียดดังนี้

๑) ชื่อ ที่อยู่ ของผู้ที่ผ่านเข้า-ออก

๒) หน่วยงานต้นสังกัด

๓) วัน เวลา ที่ผ่านเข้าออก

๔) เหตุผลในการผ่านเข้า-ออก พื้นที่

๔) ติดตั้งกล้องโทรทัศน์วงจรปิดในห้องแม่ข่าย ในตำแหน่งและตั้งมุมกล้องที่เห็นรายละเอียดชัดเจน

๔.๖ การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

๑) แผ่นติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
๒) เทปสำรองข้อมูลและระบบงานที่สำคัญ
๓) แผ่นโปรแกรม antivirus/spyware
๔) แผ่น driver อุปกรณ์ต่างๆ
๕) ระบบสำรองไฟฉุกเฉิน (UPS)
๖) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๕. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑. นายปพน โสตถิโภคา นักวิชาการคอมพิวเตอร์ชำนาญการ

๒. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ได้แก่

๒.๑. นายปพน โสตถิโภคา นักวิชาการคอมพิวเตอร์ชำนาญการ

๒.๒. นายธีรัช สุเทวี นักวิชาการคอมพิวเตอร์

๓. รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๓.๑ นางสาวศิริพันธุ์ สุทธิเชาวนะพันธุ์ นักวิชาการคอมพิวเตอร์

๔. รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน ได้แก่

๔.๑ นายธีรัช สุเทวี นักวิชาการคอมพิวเตอร์

๖. <u>มาตรการความปลอดภัยด้วยรหัสผ่าน</u>

มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศ ไม่สามารถเข้าถึง แก้ไข เปลี่ยนแปลงข้อมูล หรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้องโดย

๖.๑ กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้าในระบบได้ตามความรับผิดชอบ (Access) โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละระดับฐานข้อมูล ดังนี้

๑) บุคคลที่สามารถเรียกดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถแก้ไข ปรับปรุงข้อมูลได้

๒) บุคคลที่สามารถเรียกดูข้อมูลและแก้ไข ปรับปรุงข้อมูลในส่วนที่ผู้ใช้รับผิดชอบต่อความถูกต้องของข้อมูลในฐานข้อมูลนั้น

๓) บุคคลที่สามารถเรียกดู แก้ไข ปรับปรุงข้อมูลระดับฐานข้อมูล ในกรณีที่ผู้ใช้มีข้อผิดพลาดในการปรับปรุงข้อมูล ผู้รับผิดชอบของหน่วยงานเจ้าของหน่วยงานเป็นผู้ดูแล แก้ไข ข้อมูลใน

ส่วนนี้ซึ่งการเข้าใช้ฐานข้อมูล ในแต่ละระบบ จะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูล ตามหน้าที่ความรับผิดชอบของผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูล โดยมีการกำหนด Log in และ Password ในการเข้าถึงข้อมูลและผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงและเปลี่ยนแปลงแก้ไขข้อมูลได้ ผู้ใช้ระบบทั่วไปที่ผู้บังคับบัญชาที่เป็นหน่วยงานเจ้าของระบบ เป็นผู้อนุมัติให้ดำเนินการได้ โดยจะแบ่งเป็นการดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถเปลี่ยนแปลงแก้ไขได้ และการที่สามารถปรับปรุงข้อมูลได้ ทั้งนี้ เพื่อเป็นการรักษาความปลอดภัยของฐานข้อมูล

๖.๒ กำหนดระยะเวลาการใช้งานระบบสารสนเทศ ของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้

๖.๓ การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๖ ตัวอักษร และควรใช้ ตัวเลข อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

๗. <u>ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ</u>

๗.๑ กรณีไฟไหม้

๑) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
(ผู้รับผิดชอบ:คุณปพน คุณธีรัช)

๒) หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบปิดเครื่องคอมพิวเตอร์แม่ข่ายหลักและปิดเครื่องสำรองไฟฟ้าทุกเครื่องที่อยู่ในห้องแม่ข่าย
(ผู้รับผิดชอบ:คุณปพน คุณธีรัช)

๓) ผู้ติดต่อประสานงานโทรแจ้งเจ้าหน้าที่ผู้ดูแลอาคารเพื่อสับคัทเอาท์ที่เข้ามาในห้องแม่ข่าย ที่เบอร์๘๐๑ และโทรแจ้งสถานีดับเพลิงสุทธิสาร ที่เบอร์ ๐๒-๒๗๗-๓๖๘๘
(ผู้รับผิดชอบ:คุณศิริพันธุ์)

๔) ให้เจ้าหน้าที่ออกนอกพื้นที่พร้อมนำเทปbackup ของทุกระบบงาน/ฐานข้อมูลไปด้วย (ผู้รับผิดชอบ:คุณปพน คุณธีรัช)

๕) หลังจากไฟไหม้แล้ว เมื่อพบว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไป (ผู้รับผิดชอบ: คุณธีรัช)

๗.๒ กรณีน้ำท่วม

๑) ผู้ดูแลระบบต้องรีบปิดเครื่องคอมพิวเตอร์แม่ข่ายหลักและปิดเครื่องสำรองไฟฟ้าทุกเครื่องที่อยู่ในห้องแม่ข่าย (ผู้รับผิดชอบ:คุณปพน คุณธีรัช)

๒) ผู้ติดต่อประสานงานโทรแจ้งเจ้าหน้าที่ผู้ดูแลอาคารเพื่อสับคัทเอาท์ที่เข้ามาในห้องแม่ข่าย ที่เบอร์ ๘๐๑ (ผู้รับผิดชอบ:คุณศิริพันธุ์)

๓) ให้เจ้าหน้าที่ออกนอกพื้นที่พร้อมนำเทปbackup ของทุกระบบงาน/ฐานข้อมูลไปด้วย (ผู้รับผิดชอบ:คุณปพน คุณศิริพันธุ์ คุณธีรัช)

๔) เมื่อปรากฏพบว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ (ผู้รับผิดชอบ: คุณธีรัช)

๗.๓ กรณีไฟดับหรือไฟฟ้าบกพร่อง

๑) ผู้ดูแลระบบต้องรีบปิดเครื่องคอมพิวเตอร์แม่ข่ายหลักและปิดเครื่องสำรองไฟฟ้าทุกเครื่องที่อยู่ในห้องแม่ข่าย (ผู้รับผิดชอบ:คุณปพน คุณธีรัช)

๒) ให้เจ้าหน้าที่ออกนอกพื้นที่พร้อมนำเทปbackup ของทุกระบบงาน/ฐานข้อมูลไปด้วย (ผู้รับผิดชอบ:คุณปพน คุณศิริพันธุ์ คุณธีรัช)

๓) เมื่อปรากฏพบว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ (ผู้รับผิดชอบ: คุณธีรัช)

๗.๔ กรณีแผ่นดินไหว

๑) ผู้ดูแลระบบต้องรีบปิดเครื่องคอมพิวเตอร์แม่ข่ายหลักและปิดเครื่องสำรองไฟฟ้าทุกเครื่องที่อยู่ในห้องแม่ข่าย (ผู้รับผิดชอบ:คุณปพน คุณธีรัช)

๒) ให้เจ้าหน้าที่ออกนอกพื้นที่พร้อมนำเทปbackup ของทุกระบบงาน/ฐานข้อมูลไปด้วย (ผู้รับผิดชอบ:คุณปพน
คุณศิริพันธุ์ คุณธีรัช)

๓) หลังจากแผ่นดินไหว เมื่อพบว่าอุปกรณ์ต่างๆชำรุดเสียหายให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์มาเพื่อให้การปฏิบัติงานดำเนินต่อไป (ผู้รับผิดชอบ: คุณธีรัช)

๗.๕ กรณีโจรกรรม

๑) เมื่อพบการโจรกรรมในห้องแม่ข่าย ผู้ประสานงาน รายงานให้ผู้บังคับบัญชาทราบโดยด่วนที่สุด เพื่อจะได้ประสานงานกับเจ้าหน้าที่เกี่ยวข้อง หรือเจ้าหน้าที่ตำรวจในการที่จะระงับหรือจับกุมผู้ที่จะกระทำการดังกล่าว (ผู้รับผิดชอบ:คุณศิริพันธุ์)

๒) สำรวจอุปกรณ์ในห้องแม่ข่าย เมื่อพบว่าอุปกรณ์ที่สูญหายหรือชำรุดเสียหายจากการโจรกรรมนั้น ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ มาเพื่อให้การปฏิบัติงานดำเนินต่อไป (ผู้รับผิดชอบ: คุณปพน คุณธีรัช)

๗.๖ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๑) ผู้ดูแลระบบต้องรีบปิดเครื่องคอมพิวเตอร์แม่ข่ายหลักและปิดเครื่องสำรองไฟฟ้าทุกเครื่องที่อยู่ในห้องแม่ข่าย (ผู้รับผิดชอบ:คุณปพน)

๒) ให้ผู้ดูแลระบบทำการสำรองข้อมูลระบบ และนำข้อมูลสำรองเคลื่อนย้ายไปด้วยหากสามารถทำได้ (ผู้รับผิดชอบ:คุณปพน คุณศิริพันธุ์ คุณธีรัช)

๒) หลังจากเหตุการณ์เข้าสู่ภาวะปกติ ให้ผู้ดูแลระบบสำรวจความเสียหายเบื้องต้นเมื่อพบว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์มาเพื่อให้การปฏิบัติงานดำเนินต่อไป (ผู้รับผิดชอบ: คุณธีรัช)

๘. <u>แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม</u>

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕) นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยผู้ดูแลระบบ กู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๖) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง