# แผนบริหารความเสี่ยง
# ด้านเทคโนโลยีสารสนเทศ
# จังหวัดตราด

==========

กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดตราด
โทร. 0 – 3951 – 1282 โทรสาร 0 –3951-1282

# ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

**บทนำ**

ศูนย์ปฏิบัติการจังหวัดถือได้ว่าเป็นศูนย์สารสนเทศที่มีนัยสำคัญในการเป็นศูนย์กลางด้านข้อมูลเพื่อสนับสนุนการบริหารงานเชิงยุทธศาสตร์ของจังหวัด ไม่ว่าจะเป็นข้อมูลด้านโครงสร้างพื้นฐาน เศรษฐกิจ อุตสาหกรรม พลังงาน การเกษตร สิ่งแวดล้อม ท่องเที่ยวตลอดจนแผนงานโครงการยุทธศาสตร์ เป็นมิติสัมพัทธ์เชิงข้อมูลภายในจังหวัด ระดับกลุ่มจังหวัดและรวมไปถึงระดับประเทศด้วย

เนื่องจากภารกิจของศูนย์ปฏิบัติการจังหวัดมีความหลากหลายและรองรับการใช้งานจากหน่วยงานต่างๆ มาก ดังนั้นจึงต้องมีการสำรวจระบบเดิมทีมีอยู่ เพื่อพิจารณาถึงปัจจัยแวดล้อมอย่างครบถ้วน ไม่ว่าจะเป็น เสถียรภาพของระบบฮาร์ดแวร์และเครือข่าย ระบบฐานข้อมูล โปรแกรมประยุกต์และบริการต่าง ๆ ระบบรักษาความปลอดภัยของข้อมูล การพัฒนาบุคลากรเพื่อรองรับภารกิจของศูนย์ฯ รวมถึงการประชาสัมพันธ์สร้างความเข้าใจให้กับหน่วยงานราชการ ภาคธุรกิจเอกชนและภาคประชาชน ดังนั้นจึงจำเป็นต้องมีระบบบริหารความเสี่ยงของระบบสารสนเทศศูนย์ปฏิบัติการจังหวัด เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบสารสนเทศของศูนย์ปฏิบัติการจังหวัดและเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการการบริหารงานจังหวัดแบบบูรณาการเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น

ระบบการบริหารความเสี่ยงของระบบสารสนเทศศูนย์ปฏิบัติการจังหวัดมีวัตถุประสงค์ในการจัดทำเพื่อให้ความรู้แก่บุคลากรหรือเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศ และเป็นแผนที่ใช้สำหรับคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริง และนำแผนบริหารความเสี่ยงฉบับนี้ไปใช้ในการแก้ไขปัญหา แผนบริหารความเสี่ยงประกอบไปด้วยเนื้อหาดังนี้ การบำรุงรักษาระบบสารสนเทศ, การป้องกันสภาวะความเสี่ยงที่คาดว่าจะเกิดขึ้น, การแก้ไขปัญหากรณีสภาวะความเสี่ยง

**คำนิยาม**

**ความเสี่ยง** หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตาม วัตถุประสงค์และเป้าหมายที่กำหนด

**การประเมินความเสี่ยง** หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

**การวิเคราะห์ความเสี่ยง** หลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นต่อไปคือ การวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเพราะการวัดความเสี่ยงเป็น

ตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิดหรือ โอกาสที่จะเกิดความเสี่ยง

**การบริหารความเสี่ยง** เมื่อทราบความเสี่ยงที่มีนัยสำคัญและ โอกาสที่จะเกิดความเสี่ยงแล้วควรวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยง และพิจารณาว่าจะยอมรับความเสี่ยงนั้นหรือจะกำหนดกิจกรรมการควบคุมต่าง ๆ เพื่อป้องกัน หรือลดความเสี่ยงให้อยู่ในระดับที่สามารถยอมรับได้

**ความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

จากการศึกษาค้นคว้า ประกอบกับการตรวจสอบหน่วยงานต่างๆที่เกี่ยวข้องกับการบริหารจัดการและการควบคุมความเสี่ยงด้านสารสนเทศของจังหวัด พิจารณาแล้วเห็นว่าความเสี่ยงด้านสารสนเทศที่เกี่ยวข้องกับศูนย์ปฏิบัติการจังหวัดสามารถ แบ่งออกเป็น 4 ประเภทหลัก ดังนี้

1. **Access Risk** : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานที่รับผิดชอบไม่ได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปใช้ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมไม่ได้มีการกำหนดรหัสผ่าน(password)ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การไม่ได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

2. **Integrity Risk** : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานที่รับผิดชอบไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบ

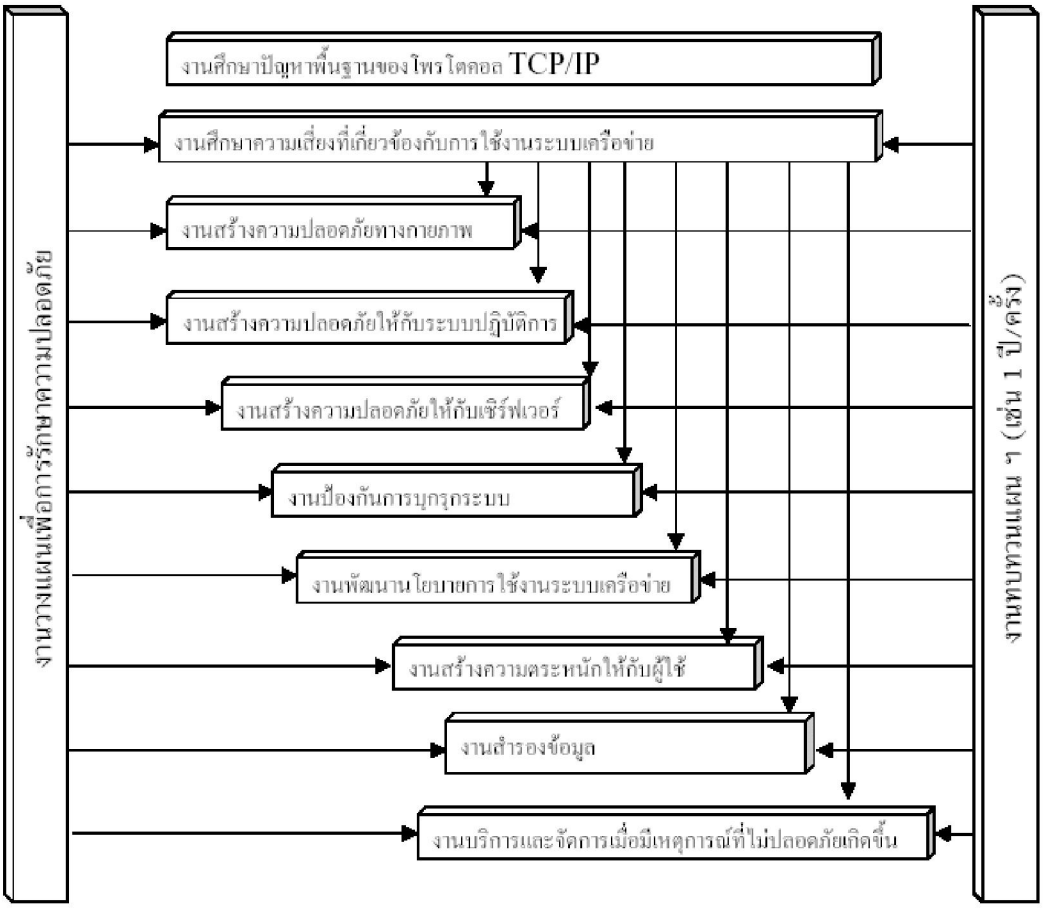
คอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

3. **Availability Risk** : เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการซึ่งอาจทำให้การปฏิบัติงานหรือการให้บริการด้านต่างๆอาจหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการที่ไม่ได้มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้ทำการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ ถ้าหากไม่ได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

4. **Infrastructure Risk** : เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานที่รับผิดชอบไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดีรวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการปฏิบัติงาน โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการที่ไม่ได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการทีไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินธุรกิจ และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบนอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น

ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงหนึ่งที่ทำให้เกิดผลกระทบต่อระบบฐานข้อมูลศูนย์ปฏิบัติการจังหวัด เนื่องด้วยความเสี่ยงดังกล่าวอาจทำให้ระบบขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อภาพรวมของระบบศูนย์ปฏิบัติการจังหวัดได้ จึงจำเป็นต้องมีการจัดทำระบบบริหารจัดการความเสี่ยงและแผนแก้ไขปัญหาที่อาจเกิดขึ้นและแนวทางป้องกันต่อไป

ขบวนการสร้างความปลอดภัยให้กับระบบเครือข่ายสารสนเทศขององค์กร (Information and Network Security Process) จะมีงานที่เกี่ยวข้องกับการสร้างความปลอดภัยให้กับระบบเครือข่ายโดยพื้นฐานสามารถแสดงได้ดังรูปที่ 2.1




รูปที่ 2.1 กระบวนการสร้างความปลอดภัยให้กับระบบเครือข่าย

ลูกศรในรูปหมายถึงผลของงานซึ่งอยู่ที่<u>ปลายลูกศรมีผลต่องานที่อยู่ที่หัวลูกศร</u> เช่น งานวางแผน (ที่อยู่ในแนวตั้งทางซ้ายมือ) มีผลต่องานทุกๆงานที่อยู่ตรงกลาง (ยกเว้นงานศึกษาปัญหาพื้นฐานของโปรโตรคอล TCP/IP) งานศึกษาความเสี่ยงและงานทบทวนแผนสร้างความปลอดภัยก็มีผลต่องานทุกงานเช่นเดียวกัน ซึ่งสามารถมองถึงความสัมพันธ์ของงานทั้งหมดได้ดังนี้

1. งานศึกษาปัญหาพื้นฐานของโพรโตคอล TCP/IP ปัญหาความไม่ปลอดภัยเป็นจำนวนมากที่เกิดขึ้นบนระบบเครือข่ายรวมทั้งอินเทอร์เน็ตด้วย มีสาเหตุสำคัญมาจากตัวโพรโตคอลที่ใช้ในการสื่อสารบนเครือข่ายหรือที่เรียกกันว่า TCP/IP (Transmission Control Protocol and Internet Protocol) ดังนั้นผู้วางระบบเครือข่ายควรจะได้เรียนรู้และทำความเข้าใจพื้นฐานนี้เป็นสิ่งแรก
2. งานศึกษาความเสี่ยงที่เกี่ยวข้องกับการใช้งานระบบเครือข่าย งานศึกษานี้จะเป็นการศึกษาถึงความเสี่ยงหรือภัยต่างๆ ที่สำคัญๆ และพบอยู่บ่อยๆ ทั้งบนระบบเครือข่ายขององค์กรและอินเทอร์เน็ต ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล TCP/IP ด้วย
3. งานวางแผนเพื่อสร้างความปลอดภัย งานวางแผนนี้โดยทั่วไปประกอบด้วย
   - งานศึกษาระบบเครือข่ายปัจจุบัน
   - งานวิเคราะห์ความเสียงที่มีโอกาสเกิดขึ้นได้จากการใช้งานระบบเครือข่าย
   - งานออกแบบวิธีการเพื่อลดความเสี่ยงที่พบ
4. งานทบทวนแผนเพื่อสร้างความปลอดภัย ภายหลังจากที่ได้มีการนำวิธีการเพื่อลดความเสี่ยงมาใช้งานเป็นระยะเวลาหนึ่งเช่น 1 ปี องค์กรควรจะได้ทบทวนแผนนี้ใหม่ ทั้งนี้เนื่องจากในช่วงระยะเวลาที่ผ่านมา การนำเทคโนโลยีใหม่มาใช้งานการอัพเกรดซอฟต์แวร์ เป็นต้น จะทำให้องค์กรรับความเสี่ยงใหม่เข้ามาจึงต้องทำการวิเคราะห์ความเสี่ยงและหาวิธีการแก้ไขเพิ่มเติม จึงเป็นการเข้าสู่กระบวนการขั้นที่ 1, 2 และ 3 ของงานวางแผนเพื่อสร้างความปลอดภัยอีกครั้งหนึ่ง

**งานออกแบบวิธีการเพื่อลดความเสี่ยงในขั้นที่ 3 นั้นโดยทั่วไปประกอบไปด้วย**

1. งานสร้างความปลอดภัยทางกายภาพ ได้แก่ งานควบคุมการเข้าออกอาคารสำนักงาน ห้องคอมพิวเตอร์ ห้องเซิร์ฟเวอร์ หรือห้องที่มีความสำคัญอื่นๆ งานควบคุมและจำกัดการใช้อุปกรณ์คอมพิวเตอร์ต่าง ๆ
2. งานสร้างความปลอดภัยให้กับระบบปฏิบัติการ งานติดตั้งระบบปฏิบัติการให้ทำงานอย่างปลอดภัยถือเป็นพื้นฐานสำคัญประการหนึ่งที่ไม่ควรละเลยไม่ว่าเครื่องคอมพิวเตอร์นั้นจะเป็นเครื่องของผู้ใช้ทั่วไปหรือเครื่องเซิร์ฟเวอร์ก็ตาม งานติดตั้งนี้ควรถือเป็นภาคบังคับก่อนที่จะก้าวไปสู่งานสร้างความปลอดภัยให้กับเซิร์ฟเวอร์
3. งานสร้างความปลอดภัยให้กับเซิร์ฟเวอร์ เมื่อได้ทำการติดตั้งระบบปฏิบัติการอย่างปลอดภัยแล้ว ขั้นต่อไปคืองานติดตั้งและใช้งานเซิร์ฟเวอร์ เช่น เว็บเซิร์ฟเวอร์(Web Server) เอฟทีพีเซิร์ฟเวอร์ (FTP Server) ซีเคียลเชลล์เซิร์ฟเวอร์ (Secure Shell Server) ดีเอ็นเอสเซิร์ฟเวอร์ (DNS Server) ให้สามารถทำงานอย่างปลอดภัย งานสร้างความปลอดภัยนี้จะเกี่ยวข้องกับงานศึกษาเพื่อสร้างความปลอดภัยในกับเซิร์ฟเวอร์ทุกเครื่องขององค์กร

4. งานป้องกันการบุกรุกระบบ งานนี้เป็นงานเสริมสร้างระบบเครือข่ายให้มีความแข็งแกร่งมากยิ่งขึ้น เพื่อให้เซิร์ฟเวอร์หรือเครื่องผู้ใช้ทั่วไปปลอดภัยจากการบุกรุกที่อาจมาจากทางอินเตอร์เน็ต งานป้องกันนี้ประกอบด้วย

4.1 งานจัดทำไฟร์วอลล์ (Fire wall)

งานนี้เป็นงานควบคุมหรือจำกัดการเข้าออกเครือข่ายขององค์กร ซึ่งหมายรวมถึงการป้องกันเพื่อไม่ให้ผู้ที่ไม่มีสิทธิเข้ามาใช้งานเครือข่ายและเซิร์ฟเวอร์ขององค์กร

4.2 งานจัดทำระบบป้องกันการบุกรุก

ในกรณีที่ไฟร์วอลล์อนุญาตให้เข้ามาใช้งานได้ เช่น เข้ามาใช้งานเว็บเซิร์ฟเวอร์ขององค์กร สิ่งนี้ไม่ได้หมายความว่าองค์กรจะปลอดภัย 100 เปอร์เซ็นต์ ช่องโหว่ในซอฟต์แวร์ของเว็บเซิร์ฟเวอร์ที่ยังไม่ได้รับการอุดช่องโหว่อาจยังมีอยู่และสามารถใช้เป็นช่องทางในการบุกรุก งานจัดทำระบบป้องกันการบุกรุกนี้มีจุดประสงค์หลักหนึ่งคือเพื่อลดความเสี่ยงของช่องโหว่ในตัวซอฟต์แวร์

4.3 งานจัดทำระบบค้นหาจุดอ่อน

ระบบป้องกันการบุกรุกโดยทั่วไปจะสามารถทำการแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบความพยายามในการบุกรุก โดยทั่วไประบบนี้จะทำงานอยู่ตลอด 24 ชั่วโมง โดยจะทำการตรวจสอบข้อมูลที่ผ่านเข้าออกเครือข่ายองค์กรเพื่อดูว่ามีความพยายามที่จะบุกรุกหรือไม่ สำหรับระบบค้นหาจุดอ่อนความสามารถส่วนหนึ่งที่สำคัญของระบบนี้คือสามารถค้นห่าช่องโหว่ในตัวซอฟต์แวร์ซึ่งนับเป็นจุดอ่อนหนึ่ง (เช่นเดียวกับระบบป้องกันการบุกรุก) แต่ระบบนี้โดยปกติจะไม่ได้ทำงานอยู่ตลอด 24 ชั่วโมง และจะมีการนำมาใช้ตามช่วงระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ เดือน รวมทั้งระบบจะไม่ได้ตรวจสอบข้อมูลที่ผ่านเข้าออกเครือข่าย

4.4 งานตรวจสอบความสมบูรณ์ของไฟล์ในระบบ

ความพยายามอย่างยิ่งในการป้องกันการบุกรุกระบบไม่ว่าจะด้วยไฟร์วอลล์ ระบบป้องกันการบุกรุก หรือระบบค้นหาจุดอ่อน ก็ตาม ก็ยังอาจมีโอกาสที่ผู้บุกรุกจะสามารถจู่โจมเข้ามาได้อยู่ดี (เรื่องของความปลอดภัยเป็นเรื่องของการลดความเสี่ยงแต่ไม่สามารถทำให้ความเสี่ยงเป็นศูนย์) อย่างไรก็ตามเมื่อการบุกรุกครั้งหนึ่ง ๆ เกิดขึ้น ผู้บุกรุกมักทิ้งร่องรอยไว้ในระบบที่บุกรุกเข้าไป เช่น การเปลี่ยนแปลงแก้ไขไฟล์ การติดตั้งซอฟต์แวร์ เข้าไปในระบบ งานตรวจสอบความสมบูรณ์นี้จะเป็นทางหนึ่งที่จะช่วยให้ผู้ดูแลระบบสามรรถทราบถึงการกระทำที่เกิดขึ้นกับไฟล์ในระบบ เช่น ในเครื่องเซิร์ฟเวอร์หนึ่ง ๆ เพื่อจะได้หาทางดำเนินการแก้ไขต่อไป

4.5 งานป้องกันไวรัส

การบุกรุกของไวรัสภายในองค์กรอาจจะมาจากการดาวน์โหลดไฟล์ของผู้ใช้ผ่านทางอินเตอร์เน็ตหรือจากทางอีเมล์ที่ได้รับ โดยทั่วไปไฟร์วอลล์จะอนุญาตการดาวน์โหลดของผู้ใช้ผ่านทางอินเตอร์เน็ต รวมทั้งจะอนุญาตการส่งมองอีเมล์จากเมล์เซิร์ฟเวอร์ที่อยู่ภายนอกเข้ามาสู่เมล์เซิร์ฟเวอร์ขององค์กร โดยที่ในทั้งสองกรณีไฟร์วอลล์จะไม่รับรู้ว่ามีไวรัสติดมาด้วยหรือไม่ ดังนั้นงานป้องกันไวรัสจึงเป็นทางเสริมอีกทางหนึ่งที่สำคัญเพื่อป้องกันการบุกรุกจากภายนอกเข้ามาสู่เครือข่ายภายในองค์กร

4.6 งานตรวจสอบปริมาณข้อมูลบนเครือข่าย

ปริมาณข้อมูลบนเครือข่ายขององค์กรที่สูงมากผิดปกติอาจมีสาเหตุมาจากมีไวรัสกำลังแพร่กระจายอยู่หรือมีการส่งหรือรับข้อมูลในเครือข่ายขององค์กรเป็นปริมาณสูง ปริมาณข้อมูลในเครือข่ายที่สูงเกินไปนี้จะมีผลทำให้การใช้งานเครือข่ายของพนักงานเป็นไปอย่างล่าช้า ติดขัด หรืออาจถึงขั้นไม่สามารถใช้งานได้เลย ดังนั้นงานตรวจสอบปริมาณข้อมูลนี้ควรจะดำเนินการอย่างสม่ำเสมอเพื่อจะได้รู้ทราบว่ามีความผิดปกติเกิดขึ้นหรือไม่และจะได้ดำเนินการแก้ไขได้อย่างทันท่วงที

4.7 งานเฝ้าดูการทำงานของเซิร์ฟเวอร์

เซิร์ฟเวอร์ให้บริการส่วนใหญ่ขององค์การจะให้บริการต่าง ๆ เช่น เว็บ (Web) เอฟทีพี (FTP) ซีเคียลเชลล์ (Secure Shell) MySQL เป็นต้น ซึ่งเซิร์ฟเวอร์ให้บริการนี้จะสามารถบันทึกกิจกรรมการเข้าใช้งานของผู้ใช้เพื่อเก็บเอาไว้เป็นหลักฐานยืนยันในภายหลังได้ เช่น วันและเวลาที่เข้าใช้งาน กิจกรรมที่ทำ เป็นต้น ข้อมูลที่บันทึกไว้นี้โดยปกติควรจะได้รับการตรวจสอบอย่างสม่ำเสมอจากผู้ดูแลระบบ (ซึ่งเป็นการเฝ้าดูว่ามีความพยายามที่จะบุกรุกเซิร์ฟเวอร์ขององค์กรหรือไม่) หากพบความผิดปกติ เช่น ความพยายามในการเข้าใช้งานเซิร์ฟเวอร์โดยที่ไม่มีสิทธิ ผู้ดูแลระบบจะได้หาทางแก้ไขต่อไป

4.8 งานอุดช่องโหว่ในตัวซอฟต์แวร์

ซอฟต์แวร์ที่ใช้งานในระบบเครือข่าย เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์เซิร์ฟเวอร์ต่าง ๆ อาจจะมีช่องโหว่ที่ผู้บุกรุกสามารถใช้ให้เป็นประโยชน์ในการเจาะระบบ ดังนั้นจึงมีความจำเป็นที่จะต้องหาทางอุดช่องโหว่เหล่านี้ ระบบค้นหาจุดอ่อนเป็นวิธีหนึ่งที่สามารถช่วยค้นหา ช่องโหว่ในตัวซอฟต์แวร์ได้ นอกจากนั้นแล้วในปัจจุบันมีซอฟต์แวร์อยู่หลายชนิดที่สามารถช่วยในการอุดช่องโหว่ให้โดยอัตโนมัติ

5. งานพัฒนานโยบายการใช้ระบบเครือข่าย งานทางเทคนิคหลายงานที่ได้กล่าวถึงข้างต้น ได้แก่ งานสร้างความปลอดภัยให้กับระบบปฏิบัติการและเซิร์ฟเวอร์ งานป้องกันการบุกรุก อาจจะไม่เป็นผลเท่าที่ควร หากผู้ดูแลระบบละเลยการติดตั้งระบบปฏิบัติการหรือเซิร์ฟเวอร์ให้ทำงานอย่างปลอดภัย

พนักงานละเลยไม่ติดตั้งซอฟต์แวร์ป้องกันไวรัส พนักงานไม่ทำการสำรองข้อมูลเก็บไว้ ผู้ดูแลระบบไม่เคยตรวจสอบข้อมูลกิจกรรมการเข้าใช้งานเซิร์ฟเวอร์ที่บันทึกไว้ พนักงานขาดการตระหนักถึงภัยของไวรัสที่มีต่อระบบเครือข่ายขององค์กร สิ่งต่าง ๆ เหล่านี้จึงทำให้มีความจำเป็นที่จะต้องจัดทำนโยบายการใช้งานออกมา (เป็นคล้าย ๆ กฎเหล็กที่ต้องปฏิบัติตาม) เพื่อควบคุมพฤติกรรมการใช้งานระบบเครือข่ายของทั้งผู้ดูแลระบบและผู้ใช้งานทั่วไป เพื่อไม่ให้ละเลยหรือปฏิบัติออกนอกลู่นอกทางที่ตนควรกระทำ

6. งานสร้างความตระหนักให้กับผู้ใช้พฤติกรรมการใช้งานระบบเครือข่าย เช่น การดาวน์โหลดไฟล์โดยไม่มีการตรวจสอบไวรัส การแชร์รหัสผ่าน การแชร์ไฟล์โดยไม่มีรหัสผ่าน การส่งรหัสผ่านทางอีเมล์ หรือพฤติกรรมที่มีความเสี่ยงอื่น ๆ ทั้งหมดนี้สามารถทำให้ระบบเครือข่ายขององค์การมีความเสี่ยงที่อาจจะถูกผู้บุกรุกหรือได้รับความเสียหายได้ จึงทำให้มีความจำเป็นที่จะต้องจัดกิจกรรมต่าง ๆ เพื่อสร้างความตระหนักให้กับผู้ใช้ เช่น การจัดอบรมเพื่อให้ความรู้ การติดประกาศในที่ ๆ สามารถมองเห็นได้ง่าย เป็นต้น ทั้งนี้เพื่อให้ผู้ใช้มีความระมัดระวังมากยิ่งขึ้นในการใช้งานระบบเครือข่าย
7. งานสำรองข้อมูลความเสี่ยงมักเกิดขึ้นได้หลากหลาย เช่น ความเสี่ยงที่เกิดจากฮาร์ดดิสก์เสียหาย ความเสี่ยงที่เกิดจากไวรัสทำลายข้อมูล ความเสี่ยงที่ผู้บุกรุกลบข้อมูลสำคัญทิ้งไป ความเสี่ยงเหล่านี้ล้วนทำให้มีความจำเป็นที่จะต้องสำรองข้อมูลเอาไว้ หากข้อมูลที่ใช้งานเกิดการเสียหาย จะได้นำข้อมูลสำรองมาใช้งานได้
8. งานบริหารและการจัดการเมื่อมีเหตุการณ์ที่ไม่ปลอดภัยเกิดขึ้นเมื่อมีเหตุการณ์บุกรุกเกิดขึ้น เช่น มีไวรัสบนระบบเครือข่าย เครือข่ายถูกบุกรุก ข้อมูลหน้าหลักบนเว็บไซต์ขององค์กรถูกเปลี่ยนแปลง ความพยายามในการบุกรุก ผู้ที่พบเห็นเหตุการณ์ควรจะได้ทราบขั้นตอนปฏิบัติที่จำเป็นเพื่อจะได้รายงานให้ผู้ที่มีอำนาจได้รับทราบเพื่อจะได้หาทางดำเนินการแก้ไขต่อไป งานบริหารและจัดการนี้มีจุดประสงค์สำคัญคือจัดทำขั้นตอนปฏิบัติเพื่อให้ผู้ใช้สามารถรายงานเหตุการณ์ที่พบได้อย่างทันท่วงที

จากที่กล่าวมาข้างต้นจะเห็นได้ว่าขบวนการสร้างความปลอดภัยให้กับระบบเครือข่ายสารสนเทศขององค์กรจะมีองค์ประกอบหลายส่วนซึ่งการกำหนดกำกับดูแลระบบรักษาความปลอดภัยและการกำหนดแผนงานเพื่อให้ระบบมีความน่าเชื่อถือ มีประสิทธิภาพ หน่วยงานควรจะมีระบบบริหารความเสี่ยงและแนวทางในการปฏิบัติพร้อมทั้งกำหนดเจ้าภาพผู้รับผิดชอบในเรื่องต่างๆ ดังนี้

**มาตรการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

**ด้านโครงสร้างพื้นฐาน (Infrastructure)**

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 1 | **ห้องศูนย์ข้อมูล** | | | | |
| | ความปลอดภัยในการผ่านเข้าออก | ระดับกลาง/<br>ระดับสูง | ติดระบบรักษาความปลอดภัย<br>กำหนดบุคคลที่สามารถผ่านเข้าออกได้ | จัดสร้างเป็นข้อกำหนดหรือระเบียบ<br>เพื่อใช้ในการปฏิบัติ | หน่วยงานผู้เป็น<br>เจ้าของศูนย์ข้อมูล |
| | การปรับอากาศ เพื่อรักษาอุณหภูมิของห้อง | ระดับกลาง/<br>ระดับกลาง | ใช้ระบบปรับอากาศที่ได้มาตรฐาน<br>จัดให้มีระบบปรับอากาศสำรอง | กำหนดระยะเวลาในการตรวจสอบ<br>บำรุงรักษา และทดสอบการทำงาน<br>ของระบบให้สม่ำเสมอ | หน่วยงานผู้เป็น<br>เจ้าของศูนย์ข้อมูล |
| | อุบัติภัย (ไฟไหม้, น้ำท่วม, ตึกถล่ม) | ระดับต่ำ/<br>ระดับสูง | จัดให้มีอุปกรณ์ดับเพลิง<br>ออกแบบห้องให้อยู่ในระดับที่น้ำไม่สามารถท่วมถึงได้<br>อุปกรณ์สื่อสารต่าง ๆ ให้จัดเก็บไว้ในตู้ที่ทนทางต่อการกระทบกระแทก | จัดสร้างเป็นข้อกำหนดหรือระเบียบ<br>เพื่อใช้ในการปฏิบัติ เพื่อป้องกัน<br>และแก้ไขเมื่อมีเหตุการณ์ดังกล่าว<br>เกิดขึ้น | หน่วยงานผู้เป็น<br>เจ้าของศูนย์ข้อมูล |

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 2 | **ระบบไฟฟ้า** | | | | |
| | ไฟฟ้าดับ, ไฟฟ้ากระชาก, ไฟฟ้าเกิน ,ฟ้าผ่า | ระดับสูง/ ระดับสูง | จัดให้มีอุปกรณ์สำรองไฟฟ้า<br>ติดตั้งระบบป้องกันฟ้าผ่า<br>ติดตั้งระบบป้องกันไฟฟ้ากระชาก<br>ติดตั้งระบบสายดิน | กำหนดระยะเวลาในการตรวจสอบ บำรุงรักษา และทดสอบการทำงานของระบบให้สม่ำเสมอ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 3 | **ระบบสื่อสาร – ระบบเครือข่าย** | | | | |
| | โทรศัพท์ ใช้งานไม่ได้ตามปกติ | ระดับต่ำ/ระดับต่ำ | ใช้ระบบตู้สาขาเพื่อจะได้บริหารจัดการได้อย่างมีประสิทธิภาพจัดให้มีสายสำรองในกรณีที่ระบบหลักใช้งานไม่ได้ | ตรวจสอบให้อยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| | อินทราเน็ต ใช้งานไม่ได้ตามปกติ | ระดับกลาง/ ระดับกลาง | จัดให้มีระบบอินเตอร์เน็ตสำรองไว้ใช้แทนเมื่อระบบอินทราเน็ตใช้งานไม่ได้ | ตรวจสอบให้ระบบอินเตอร์เน็ตมีสภาพพร้อมใช้งานได้ทันทีเมื่อระบบหลักไม่สามารถใช้งานได้ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| | อินเตอร์เน็ต | ระดับกลาง/ ระดับกลาง | จัดให้มีระบบอินเตอร์เน็ตสำรองไว้ใช้แทนเมื่ออินทราเน็ตและอินเตอร์เน็ตหลักใช้การไม่ได้ | หมั่นตรวจสอบอยู่เสมอเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |

**ด้านอุปกรณ์คอมพิวเตอร์ – อุปกรณ์เครือข่าย (Computer Hardware)**

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 4 | **อุปกรณ์คอมพิวเตอร์ลูกข่าย** | | | | |
| | เสียหาย, ไม่สามารถใช้งานได้ตามปกติ | ระดับกลาง/ระดับกลาง | จัดให้มีเครื่องสำรองไว้ใช้งาน | ตรวจเช็คสภาพ และบำรุงรักษาอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |
| | ไวรัส, สปายแวร์ ฯลฯ | ระดับสูง/ระดับสูง | เครื่องลูกข่ายทุกเครื่องต้องติดตั้งโปรแกรมป้องกัน | ตรวจสอบติดตั้งให้โปรแกรมทันสมัยอยู่ตลอดเวลาสแกนไวรัสให้แก่เครื่องลูกข่ายอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |
| 5 | **อุปกรณ์คอมพิวเตอร์แม่ข่าย** | | | | |
| | หยุดให้บริการ, เสียหาย, ไม่สามารถใช้งานได้ตามปกติ | ระดับสูง/ระดับสูง | ดูแลเครื่องแม่ข่ายให้พร้อมใช้งานอยู่เสมอ | ตรวจเช็คสภาพ และบำรุงรักษาอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |
| | ไวรัส, สปายแวร์ ฯลฯ | ระดับสูงระดับสูง | ติดตั้งระบบตรวจสอบ, ตรวจจับ, ป้องกันไวรัส, สปายแวร์ ฯลฯ | ตรวจสอบติดตั้งให้โปรแกรมทันสมัยอยู่ตลอดเวลาติดตามข่าสารและวิธีป้องกันเครื่องแม่ข่ายเป็นประจำ | หน่วยงานเจ้าของเครื่อง |
| | โดนโจมตี, โดนบุกรุก ฯลฯ | ระดับสูง/ระดับสูง | ติดตั้งระบบตรวจสอบ, ตรวจจับ, ป้องกันการโจมตี – บุกรุก | ตรวจสอบติดตั้งให้โปรแกรมทันสมัยอยู่ตลอดเวลาติดตามข่าวสารและวิธีป้องกันเครื่องแม่ข่ายเป็นประจำ | หน่วยงานเจ้าของเครื่อง |

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| **6** | **อุปกรณ์เครือข่าย, อุปกรณ์สื่อสาร ฯลฯ** | | | | |
| | เสียหาย, ไม่สามารถใช้งานได้ตามปกติ | ระดับต่ำ/ระดับสูง | จัดให้มีอุปกรณ์สำรองไว้ใช้งาน | ตรวจเช็คสภาพ และบำรุงรักษาอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |
| | ตัวนำสัญญาณ, สายสื่อสารต่าง ๆ ขาด, ชำรุด | ระดับต่ำ/ระดับกลาง | ในขั้นตอนการติดตั้งสายสัญญาณควรจัดให้มีการร้อยท่อเพื่อป้องกัน เปลี่ยนมาใช้ระบบไร้สายแทนระบบใช้สาย | ตรวจเช็คสภาพสายสัญญาณ พร้อมทั้งซ่อมแซมให้อยู่ในสภาพพร้อมใช้งานอยู่ตลอดเวลา | หน่วยงานเจ้าของเครื่อง |

**ด้านข้อมูล – อุปกรณ์สำรองข้อมูล (Data and Backup Media)**

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 7 | **ด้านข้อมูล** | | | | |
| | การเข้าถึงข้อมูลไม่ได้ | ระดับกลาง/ ระดับกลาง | ดูแลระบบเครือข่าย, ระบบแม่ข่าย และระบบฐานข้อมูล ให้พร้อมใช้งาน | ทดสอบเรียกใช้งานข้อมูล เพื่อดูว่าใช้งานได้ตามปกติหรือไม่ | หน่วยงานผู้เป็นเจ้าของ ศูนย์ข้อมูล |
| | การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต | ระดับต่ำ/ ระดับสูง | จัดให้มีระบบตรวจสอบสิทธิในการเข้าถึงข้อมูลในแต่ละระดับ | ตรวจสอบรายการการเข้าใช้ข้อมูล เพื่อดูการเข้าถึงข้อมูลที่ผิดปกติ | หน่วยงานผู้เป็นเจ้าของ ศูนย์ข้อมูล |
| | ความเชื่อถือไม่ได้ของข้อมูล | ระดับกลาง/ ระดับกลาง | กำหนดผู้รับผิดชอบ, หน่วยงาน และระยะเวลาในการปรับปรุงข้อมูลแต่ละเรื่องให้ชัดเจน | ตรวจสอบรายงานการปรับปรุงข้อมูลว่าเป็นปัจจุบัน หรือไม่ | หน่วยงานผู้เป็นเจ้าของ ศูนย์ข้อมูล |
| | ข้อมูลเสียหาย | ระดับต่ำ/ ระดับสูง | จัดให้มีระบบในการสำรองข้อมูล (Backup) | ทดสอบเรียกใช้งานข้อมูล เพื่อดูว่าใช้งานได้ตามปกติหรือไม่ | หน่วยงานผู้เป็นเจ้าของ ศูนย์ข้อมูล |

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 8 | **ด้านอุปกรณ์บันทึก – สำรองข้อมูล** | | | | |
| | วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล | ระดับกลาง/ ระดับกลาง | ศึกษาวิธีการใช้งานให้ถูก | จัดทำเป็นระเบียบ หรือมาตรการในการสำรองข้อมูลที่เป็นแบบแผนชัดเจน | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| | เลือกสื่อบันทึกข้อมูลไม่เหมาะสมกับข้อมูล | ระดับกลาง/ ระดับสูง | ศึกษาและเลือกใช้อุปกรณ์ในการบันทึกข้อมูลให้เหมาะสมกับข้อมูลของหน่วยงาน | จัดทำเป็นระเบียบ หรือมาตรการที่ชัดเจน | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |

**ด้านบุคคลากรและผู้ใช้งาน (Staff And User)**

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 9 | **ด้านบุคคลากร** | | | | |
| | ขาดเจ้าหน้าที่ผู้มีความเชี่ยวชาญผู้ทำหน้าที่ในการบริหารจัดการระบบ | ระดับสูง/ ระดับสูง | จัดหาบุคคลากรผู้มีความเชี่ยวชาญด้านไอทีมาดูแลระบบ | จัดให้มีมาตรการในการติดตามและประเมินผลความรู้ความสามารถของเจ้าหน้าที่ผู้ปฏิบัติงาน | หน่วยงานที่บุคคลากรสังกัด |
| | เจ้าหน้าที่ผู้รับผิดชอบอยู่ในปัจจุบัน ไม่มีความรู้ทางด้านไอทีโดยตรง | ระดับสูง/ ระดับกลาง | จัดอบรมให้ความรู้พัฒนาศักยภาพแก่บุคคลากรทางด้านไอที | จัดให้มีมาตรการในการติดตามและประเมินผลความรู้ ความสามารถของเจ้าหน้าที่ ผู้ปฏิบัติงาน | หน่วยงานที่บุคคลากรสังกัด |
| | ความไม่ชัดเจนทางด้านโครงสร้างของการบริหารงานด้านไอที | ระดับกลาง/ ระดับกลาง | ผู้บริหารควรจัดโครงสร้างสายการปฏิบัติงาน และมอบหมายหน้าที่รับผิดชอบให้แก่ผู้ปฏิบัติงานให้ชัดเจน | จัดให้มีมาตรการในการติดตามและประเมินผลการปฏิบัติงานของเจ้าหน้าที่ผู้ปฏิบัติงาน | หน่วยงานที่บุคคลากรสังกัด |
| | | | | | |

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| **10** | **ด้านผู้ใช้งาน** | | | | |
| | ผู้ใช้ขาดความรู้ทางด้านไอที | ระดับกลาง/ ระดับกลาง | ให้ความรู้แก่ผู้ใช้งานทางด้านไอที | จัดให้มีการวัดผลความรู้ทางด้านไอที และตรวจสอบติดตามความสำเร็จในการใช้งานระบบของผู้ใช้งาน | หน่วยงานที่ผู้ใช้งานสังกัด |
| | ผู้ใช้งานขาดความรู้ความเข้าใจในการใช้งานระบบ | ระดับกลาง/ ระดับกลาง | จัดทำคู่มือการใช้งานในระบบ | จัดให้มีการวัดผลความรู้ทางด้านไอที และตรวจสอบติดตามความสำเร็จในการใช้งานระบบของผู้ใช้งาน | หน่วยงานที่ผู้ใช้งานสังกัด |
| | ผู้ใช้งานเป็นผู้ประสงค์ร้ายมีเจตนาเข้าถึงระบบในส่วนที่ไม่ได้รับสิทธิ | ระดับต่ำ/ ระดับสูง | ติดตั้งระบบตรวจสอบ, ตรวจจับ, ป้องกันการโจมตี – บุกรุก | ติดตามรายงานจากโปรแกรมตรวจจับการบุกรุกอย่างสม่ำเสมอเพื่อดูการใช้งานที่ผิดปกติ | หน่วยงานที่ผู้ใช้งานสังกัด |

# โครงสร้างอำนาจหน้าที่ศูนย์ปฏิบัติการจังหวัด

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นความเสี่ยงหนึ่งที่หน่วยงานให้ความสำคัญเนื่องด้วยความเสี่ยงดังกล่าวอาจทำให้หน่วยงานที่รับผิดชอบขาดความหน้าเชื่อถือซึ่งส่งผลต่อหน่วยงานและบุคลากร ดังนั้นจึงได้มีการกำหนดโยบายและแผนการแก้ปัญหาเพื่อเป็นข้อกำหนดให้หน่วยงานที่รับผิดชอบปฏิบัติตามแนวทางที่ได้กำหนดไว้ เพื่อใช้เป็นแนวทางในการบริหารจัดการระบบความเสี่ยงระบบสารสนเทศต่อไป โดยจะกำหนดเป็นเรื่องต่างๆดังนี้

**โครงสร้างหน่วยงานและการบริหารจัดการ**

หากหน่วยงานเทคโนโลยีสารสนเทศมิได้มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอ ก็อาจก่อให้เกิดความเสี่ยงด้าน infrastructure risk ได้ ซึ่งหน่วยงานที่รับผิดชอบให้ความสำคัญในเรื่องของการแบ่งแยกอำนาจหน้าที่ การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน และการกำกับดูแลและควบคุมการปฏิบัติงานเป็นหลัก ดังนี้

**การแบ่งแยกอำนาจหน้าที่**

การแบ่งแยกอำนาจหน้าที่และความรับผิดชอบภายในหน่วยงานนั้นควรเป็นไปตามหลักการควบคุมภายในที่ดี โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ซึ่งการมอบหมายให้บุคลากรคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กันในบางกรณี ยังอาจเป็นช่องทางให้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขหรือเปลี่ยนแปลงได้โดยง่าย (integrity risk) ควรที่จะกระจายความรับผิดชอบตามความเหมาะสมตามโครงสร้างขององค์กร เพื่อกำหนดเป็นแนวทางในการกำกับดูแลระบบเทคโนโลยีสารสนเทศจังหวัดต่อไป

1. งานพัฒนาระบบสารสนเทศ
2. งานพัฒนาระบบข้อมูลเพื่อการพัฒนาจังหวัด
3. งานพัฒนาและบำรุงรักษาระบบเทคโนโลยีสารสนเทศจังหวัด

**งานพัฒนาระบบสารสนเทศจังหวัด**

รับผิดชอบโดย หัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสารหน้าที่ กำกับดูแลการปฏิบัติงานของเจ้าหน้าที่ในกลุ่มงาน โดยรับผิดชอบงานพัฒนาระบบสารสนเทศ จัดให้มีและให้บริการเชื่อมโยงฐานข้อมูลสารสนเทศระหว่างส่วนราชการภายในจังหวัด อำเภอ และท้องถิ่น ระดับจังหวัดกับส่วนกลาง รวมทั้งการให้บริการแลกเปลี่ยนข้อมูลข่าวสารสารสนเทศผ่านสื่ออิเล็กทรอนิกส์ และงานอื่นๆที่ผู้บังคับบัญชามอบหมาย และกำหนดหน้าที่ความรับผิดชอบให้เจ้าหน้าที่

**งานพัฒนาระบบฐานข้อมูลเพื่อการพัฒนาจังหวัด**

รับผิดชอบโดย สำนักงานจังหวัดตราด

หน้าที่รับผิดชอบ

- งานศูนย์ปฏิบัติการจังหวัด
- งานพัฒนาระบบฐานข้อมูล โดยจัดตั้งคณะทำงาน ประสานงาน รวบรวม วิเคราะห์ข้อมูล ออกแบบ และจัดทำฐานข้อมูลเพื่อการวางแผนและพัฒนาจังหวัด
    - ข้อมูลความต้องการของจังหวัด
    - ข้อมูลความต้องการของส่วนราชการ
    - ข้อมูลเชิงบริหารและนโยบายของจังหวัด
    - ข้อมูลเชิงยุทธศาสตร์เพื่อการวางแผนพัฒนาจังหวัด
- ประสานงานและติดตามข้อมูลจากส่วนราชการและหน่วยงานที่เกี่ยวข้อง
- การนำเสนอข้อมูล
- การให้บริการข้อมูล
- การประชาสัมพันธ์ระบบฐานข้อมูล

รับผิดชอบโดย คณะทำงานด้านข้อมูลศูนย์ปฏิบัติการจังหวัด(POC)

1 หัวหน้าสำนักงานจังหวัด

2 หัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสาร

3 นายช่างไฟฟ้าสื่อสารชำนาญงาน

4 นักวิชาการคอมพิวเตอร์ปฏิบัติการ

หน้าที่รับผิดชอบ

- พัฒนาระบบฐานข้อมูลจังหวัด โดย ประสานงาน รวบรวม วิเคราะห์ข้อมูล ออกแบบ และจัดทำฐานข้อมูลเพื่อการวางแผนและพัฒนา
    - ข้อมูล 45 กลุ่มเรื่องตามข้อกำหนดของกระทรวงมหาดไทย
    - ข้อมูล 33 ตัวชี้วัดตามข้อกำหนดของ สศช.
    - นำเสนอข้อมูล
    - ให้คำปรึกและคำแนะนำแก่ส่วนราชการต่างๆ
    - รวบรวม วิเคราะห์ และแก้ปัญหาระบบฐานข้อมูล

**งานพัฒนาและบำรุงรักษาระบบเทคโนโลยีสารสนเทศจังหวัด**

| | |
|---|---|
| 1 นางสาววาสนา แย้มกมล | นายช่างไฟฟ้าสื่อสาร ชำนาญงาน |
| 2 นายอนุชิต อารีเอื้อ | นักวิชาการคอมพิวเตอร์ ปฏิบัติการ |
| 3 นายธวัทชัย ตรีรัตน์ฤดี | นายช่างไฟฟ้า |

หน้าที่รับผิดชอบ

(1) งานพัฒนาเครือข่ายอินทราเน็ต (Intranet) และอินเตอร์เน็ต (Internet)

- ออกแบบวิธีการเชื่อมต่อที่ได้รับการร้องขอจากส่วนราชการต่างๆ
- ติดตั้ง ตรวจซ่อม บำรุงรักษา ระบบ LAN และ WAN ที่เชื่อมต่อมายังเครื่องคอมพิวเตอร์แม่ข่าย(SERVER)ของจังหวัด
- ตรวจเช็คดูแลระบบรักษาความปลอดภัย
- ให้คำปรึกษาและคำแนะนำแก่ส่วนราชการต่างๆ

(2) ระบบโทรศัพท์

- ติดตั้ง
- ตรวจซ่อม
- บำรุงรักษา

(3) งานพัฒนาและปรับปรุง web site ทั้ง อินทราเน็ต(Intranet)และ อินเตอร์เน็ต(Internet)

(4) งานระบบไฟฟ้า

- ติดตั้งระบบไฟฟ้าสำรอง
- ตรวจเช็คและบำรุงรักษาอุปกรณ์ไฟฟ้าสำรอง

(5) งานดูแลระบบและการจัดการเครือข่าย

- ตรวจเช็คและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย(server)
- ปฏิบัติตามแผนการสำรองข้อมูลและการกู้คืนข้อมูล(back up and Recovery)
- ตรวจสอบระบบรักษาความปลอดภัย นำผลจากอุปกรณ์รักษาความปลดภัยมาวิเคราะห์เพื่อกำหนดนโยบาย(Policy)ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

# แผนงานมาตรการป้องกันความเสี่ยง
# ด้านเทคโนโลยีสารสนเทศ

---

มาตรการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์ปฏิบัติการจังหวัดสามารถแบ่งได้เป็น 4 ส่วนหลัก ดังนี้

1. ด้านโครงสร้างพื้นฐาน (Infrastructure) ประกอบด้วย
    1) ห้องศูนย์ข้อมูล
    2) ระบบไฟฟ้า
    3) ระบบสื่อสาร-ระบบเครือข่าย
2. ด้านอุปกรณ์คอมพิวเตอร์-อุปกรณ์เครือข่าย (Computer Network) ประกอบด้วย
    1) อุปกรณ์คอมพิวเตอร์ลูกข่าย (Client)
    2) อุปกรณ์คอมพิวเตอร์ลูกแม่ข่าย (Server)
    3) อุปกรณ์เครือข่าย,อุปกรณ์สื่อสาร ฯลฯ
3. ด้านข้อมูล-อุปกรณ์สำรองข้อมูล (Data and Backup media) ประกอบด้วย
    1) ด้านข้อมูล
    2) ด้านอุปกรณ์บันทึก-สำรองข้อมูล
4. ด้านบุคลากรและผู้ใช้งาน (Staff and User)
    1) ด้านบุคลากร
    2) ด้านผู้ใช้งาน

**ด้านโครงสร้างพื้นฐาน (Infrastructure)**

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 1 | **ห้องศูนย์ข้อมูล** | | | | |
| 1.1 | ความปลอดภัยในการผ่านเข้าออก | ระดับกลาง/ ระดับสูง | ติดระบบรักษาความปลอดภัยกำหนดบุคคลที่สามารถผ่านเข้าออกได้ | จัดสร้างเป็นข้อกำหนดหรือระเบียบเพื่อใช้ในการปฏิบัติ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 1.2 | การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง | ระดับกลาง/ ระดับกลาง | ใช้ระบบปรับอากาศที่ได้มาตรฐานจัดให้มีระบบปรับอากาศสำรอง | กำหนดระยะเวลาในการตรวจสอบ บำรุงรักษา และทดสอบการทำงานของระบบให้สม่ำเสมอ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 1.3 | อุบัติภัย (ไฟไหม้, น้ำท่วม, ตึกถล่ม) | ระดับต่ำ/ ระดับสูง | จัดให้มีอุปกรณ์ดับเพลิง<br>ออกแบบห้องให้อยู่ในระดับที่น้ำไม่สามารถท่วมถึงได้<br>อุปกรณ์สื่อสารต่าง ๆ ให้จัดเก็บไว้ในตู้ที่ทนทางต่อการกระทบกระแทก | จัดสร้างเป็นข้อกำหนดหรือระเบียบเพื่อใช้ในการปฏิบัติ เพื่อป้องกัน และแก้ไขเมื่อมีเหตุการณ์ดังกล่าวเกิดขึ้น | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |

**ความปลอดภัยในการผ่านเข้าออก** ผู้ที่รับผิดชอบห้ามบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ที่ได้รับสิทธิเข้าออกเป็นผู้รับผิดชอบนำพาเข้าไป

**การปรับอากาศ เพื่อรักษาอุณหภูมิของห้อง** ผู้ที่รับผิดชอบต้องตรวจสอบสภาพการใช้งานอย่างสม่ำเสมอ

**อุบัติภัย (ไฟไหม้, น้ำท่วม, ตึกถล่ม)** ผู้ที่รับผิดชอบต้องดำเนินการตามขั้นตอนที่กำหนดไว้

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 2 | **ระบบไฟฟ้า** | | | | |
| | ไฟฟ้าดับ, ไฟฟ้ากระชาก, ไฟฟ้าเกิน ,ฟ้าผ่า | ระดับสูง/ระดับสูง | จัดให้มีอุปกรณ์สำรองไฟฟ้า<br>ติดตั้งระบบป้องกันฟ้าผ่า<br>ติดตั้งระบบป้องกันไฟฟ้ากระชาก<br>ติดตั้งระบบสายดิน | กำหนดระยะเวลาในการตรวจสอบบำรุงรักษา และทดสอบการทำงานของระบบให้สม่ำเสมอ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |

**ไฟฟ้าดับ, ไฟฟ้ากระชาก, ไฟฟ้าเกิน,ฟ้าผ่า** ผู้ดูแลระบบ ทำการสำรวจและตรวจสอบอุปกรณ์ป้องกันที่มีอยู่ให้สามารถใช้งานได้ตลอดเวลา

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 3 | **ระบบสื่อสาร – ระบบเครือข่าย** | | | | |
| 3.1 | โทรศัพท์ ใช้งานไม่ได้ตามปกติ | ระดับต่ำ/ระดับต่ำ | ใช้ระบบตู้สาขาเพื่อจะได้บริหารจัดการได้อย่างมีประสิทธิภาพจัดให้มีสายสำรอง ในกรณีที่ระบบหลักใช้งานไม่ได้ | ตรวจสอบให้อยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 3.2 | อินทราเน็ต ใช้งานไม่ได้ตามปกติ | ระดับกลาง/ระดับกลาง | จัดให้มีระบบอินเตอร์เน็ตสำรองไว้ใช้แทนเมื่อระบบอินทราเน็ตใช้งานไม่ได้ | ตรวจสอบให้ระบบอินเตอร์เน็ตมีสภาพพร้อมใช้งานได้ทันทีเมื่อระบบหลักไม่สามารถใช้งานได้ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 3.3 | อินเตอร์เน็ต | ระดับกลาง/ระดับกลาง | จัดให้มีระบบอินเตอร์เน็ตสำรองไว้ใช้แทนเมื่ออินทราเน็ตและอินเตอร์เน็ตหลักใช้การไม่ได้ | หมั่นตรวจสอบอุปกรณ์อยู่เสมอเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |

**โทรศัพท์ ใช้งานไม่ได้ตามปกติ** ผู้ที่รับผิดชอบ จะดำเนินการตรวจสอบและแก้ไข

**อินเตอร์เน็ตและอินทราเน็ตใช้งานไม่ได้** ผู้ที่ดูแลระบบเมื่อตรวจพบหรือได้รับแจ้งต้องรีบดำเนินการแก้ไขอย่างรวดเร็วที่สุด

**ด้านอุปกรณ์คอมพิวเตอร์ – อุปกรณ์เครือข่าย (Computer Network)**

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| **4** | **อุปกรณ์คอมพิวเตอร์ลูกข่าย** | | | | |
| 4.1 | เสียหาย, ไม่สามารถใช้งานได้ตามปกติ | ระดับกลาง/ระดับกลาง | จัดให้มีเครื่องสำรองไว้ใช้งาน | ตรวจเช็คสภาพและบำรุงรักษาอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |
| 4.2 | ไวรัส, สปายแวร์ ฯลฯ | ระดับสูง/ระดับสูง | เครื่องลูกข่ายทุกเครื่องต้องติดตั้งโปรแกรมป้องกัน | ตรวจสอบติดตั้งให้โปรแกรมทันสมัยอยู่ตลอดเวลา สแกนไวรัสให้แก่เครื่องลูกข่ายอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |

**อุปกรณ์คอมพิวเตอร์เสียหาย** ผู้ที่รับผิดชอบต้องรีบดำเนินการตรวจซ่อมหรือนำเครื่องสำรองไปทดแทน

**เครื่องติดไวรัส สปายแวร์** ผู้ดูแลระบบต้องตรวจเช็คระบบเครือข่ายและให้คำแนะนำในการติดตั้งและใช้งานโปรแกรมป้องกันไวรัสแก่ผู้ใช้งาน

| ที่ | รายการความเสี่ยง | โอกาส/ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| **5** | **อุปกรณ์คอมพิวเตอร์แม่ข่าย** | | | | |
| 5.1 | หยุดให้บริการ, เสียหาย, ไม่สามารถใช้งานได้ตามปกติ | ระดับสูง/ระดับสูง | จัดให้มีเครื่องแม่ข่ายสำรองไว้ใช้งาน | ตรวจเช็คสภาพ และบำรุงรักษาอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |
| 5.2 | ไวรัส, สปายแวร์ ฯลฯ | ระดับสูง ระดับสูง | ติดตั้งระบบตรวจสอบ, ตรวจจับ, ป้องกันไวรัส, สปายแวร์ ฯลฯ | ตรวจสอบติดตั้งให้โปรแกรมทันสมัยอยู่ตลอดเวลาติดตามข่าสารและวิธีป้องกันเครื่องแม่ข่ายเป็นประจำ | หน่วยงานเจ้าของเครื่อง |
| 5.3 | โดนโจมตี, โดนบุกรุก ฯลฯ | ระดับสูง/ระดับสูง | ติดตั้งระบบตรวจสอบ, ตรวจจับ, ป้องกันการโจมตี – บุกรุก | ตรวจสอบติดตั้งให้โปรแกรมทันสมัยอยู่ตลอดเวลาติดตามข่าวสารและวิธีป้องกันเครื่องแม่ข่ายเป็นประจำ | หน่วยงานเจ้าของเครื่อง |

**เครื่องคอมพิวเตอร์แม่ข่าย หยุดให้บริการ เสียหาย** ผู้ที่รับผิดชอบต้องตรวจเช็คระบบอย่างสม่ำเสมอ หรือต้องแก้ไปอย่างเร่งด่วนเมื่อได้รับแจ้งจากผู้ใช้ว่าใช้งานไม่ได้

**ไวรัส สปายแวร์** ผู้ที่รับผิดชอบ ต้องดำเนินการติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย

**โดนโจมตี โดนบุกรุก** ผู้ดูแลระบบต้องจัดทำระบบรักษาความปลอดภัยโดยจัดหาอุปกรณ์ Firewall ติดตั้งและกำหนดนโยบายสำหรับการเข้าถึง

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับ ดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 6 | **อุปกรณ์เครือข่าย, อุปกรณ์สื่อสาร ฯลฯ** | | | | |
| 6.1 | เสียหาย, ไม่สามารถใช้งานได้ตามปกติ | ระดับต่ำ/ ระดับสูง | จัดให้มีอุปกรณ์สำรองไว้ใช้งาน | ตรวจเช็คสภาพและบำรุงรักษาอย่างสม่ำเสมอ | หน่วยงานเจ้าของเครื่อง |
| 6.2 | ตัวนำสัญญาณ, สายสื่อสารต่าง ๆ ขาด, ชำรุด | ระดับต่ำ/ ระดับกลาง | ในขั้นตอนการติดตั้งสายสัญญาณควรจัดให้มีการร้อยท่อเพื่อป้องกัน<br>เปลี่ยนมาใช้ระบบไร้สายแทนระบบใช้สาย | ตรวจเช็คสภาพสายสัญญาณพร้อมทั้งซ่อมแซมให้อยู่ในสภาพพร้อมใช้งานอยู่ตลอดเวลา | หน่วยงานเจ้าของเครื่อง |

**อุปกรณ์เครือข่ายและอุปกรณ์สื่อสาร** ผู้ที่รับผิดชอบ จัดให้มีอุปกรณ์สำรองไว้ใช้งานและตรวจสอบการใช้งานอย่าสม่ำเสมอ เพื่อระบบสามารถใช้งานได้ตลอดเวลา

**ด้านข้อมูล – อุปกรณ์สำรองข้อมูล (Data and Backup Media)**

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| **7** | **ด้านข้อมูล** | | | | |
| 7.1 | การเข้าถึงข้อมูลไม่ได้ | ระดับกลาง/ ระดับกลาง | ดูแลระบบเครือข่าย, ระบบแม่ข่าย และระบบฐานข้อมูล ให้พร้อมใช้งาน | ทดสอบเรียกใช้งานข้อมูล เพื่อดูว่าใช้งานได้ตามปกติหรือไม่ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 7.2 | การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต | ระดับต่ำ/ ระดับสูง | จัดให้มีระบบตรวจสอบสิทธิในการเข้าถึงข้อมูลในแต่ละระดับ | ตรวจสอบรายการการเข้าใช้ข้อมูลเพื่อดูการเข้าถึงข้อมูลที่ผิดปกติ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 7.3 | ความเชื่อถือไม่ได้ของข้อมูล | ระดับกลาง/ ระดับกลาง | กำหนดผู้รับผิดชอบ, หน่วยงาน และระยะเวลาในการปรับปรุงข้อมูลแต่ละเรื่องให้ชัดเจน | ตรวจสอบรายงานการปรับปรุงข้อมูลว่าเป็นปัจจุบันหรือไม่ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 7.4 | ข้อมูลเสียหาย | ระดับต่ำ/ ระดับสูง | จัดให้มีระบบในการสำรองข้อมูล (Backup) | ทดสอบเรียกใช้งานข้อมูล เพื่อดูว่าใช้งานได้ตามปกติหรือไม่ | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |

**การเข้าถึงข้อมูลไม่ได้** ผู้ดูแลระบบเครือข่ายทำการตรวจสอบและแก้ไขทันทีเมื่อตรวจพบหรือได้รับแจ้งจากหน่วยงานอื่นที่ใช้ไม่ได้

**การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต** ผู้ที่รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายและระบบฐานข้อมูลเป็นผู้กำหนดสิทธิผู้ที่จะเข้าไปใช้ระบบได้ระดับไหนบ้าง

**ความเชื่อถือไม่ได้ของข้อมูล** คณะทำงานระบบฐานข้อมูล จัดประชุมกำหนดผู้บันทึกข้อมูลและผู้รับรองข้อมูลของแต่ละส่วนราชการ

**ข้อมูลเสียหาย** ผู้ที่รับผิดชอบจะทำการสำรองข้อมูล(Backup)และกู้คืน(Recovery) ในกรณีที่เกิดปัญหา

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| **8** | **ด้านอุปกรณ์บันทึก – สำรองข้อมูล** | | | | |
| 8.1 | วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล | ระดับกลาง/ ระดับกลาง | ศึกษาวิธีการใช้งานให้ถูก | จัดทำเป็นระเบียบหรือมาตรการในการสำรองข้อมูลที่เป็นแบบแผนชัดเจน | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |
| 8.2 | เลือกสื่อบันทึกข้อมูลไม่เหมาะสมกับข้อมูล | ระดับกลาง/ ระดับสูง | ศึกษาและเลือกใช้อุปกรณ์ในการบันทึกข้อมูลให้เหมาะสมกับข้อมูลของหน่วยงาน | จัดทำเป็นระเบียบหรือมาตรการที่ชัดเจน | หน่วยงานผู้เป็นเจ้าของศูนย์ข้อมูล |

**วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล** ผู้ที่รับผิดชอบ จัดทำแผนทดสอบการสำรองข้อมูลและการกู้คืนข้อมูลอย่างสม่ำเสมอ

**เลือกสื่อบันทึกข้อมูลไม่เหมาะสมกับข้อมูล** ผู้ที่รับผิดชอบ ศึกษาวีธีการที่เหมาะสมสำหรับการบันทึกข้อมูล

**ด้านบุคคลากรและผู้ใช้งาน (Staff And User)**

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| 9 | **ด้านบุคคลากร** | | | | |
| 9.1 | ขาดเจ้าหน้าที่ผู้มีความเชี่ยวชาญ ผู้ทำหน้าที่ในการบริหารจัดการระบบ | ระดับสูง/ ระดับสูง | จัดหาบุคคลากรผู้มีความเชี่ยวชาญด้านไอทีมาดูแลระบบ | จัดให้มีมาตรการในการติดตาม และประเมินผลความรู้ความ สามารถของเจ้าหน้าที่ ผู้ปฏิบัติงาน | หน่วยงานที่บุคคลากรสังกัด |
| 9.2 | เจ้าหน้าที่ผู้รับผิดชอบอยู่ในปัจจุบัน ไม่มีความรู้ทางด้านไอทีโดยตรง | ระดับสูง/ ระดับกลาง | จัดอบรมให้ความรู้พัฒนาศักยภาพแก่บุคคลากรทางด้านไอที | จัดให้มีมาตรการในการติดตาม และประเมินผลความรู้ความสามารถของเจ้าหน้าที่ ผู้ปฏิบัติงาน | หน่วยงานที่บุคคลากรสังกัด |
| 9.3 | ความไม่ชัดเจนทางด้านโครงสร้างของการบริหารงานด้านไอที | ระดับกลาง/ ระดับกลาง | ผู้บริหารควรจัดโครงสร้างสายการปฏิบัติงาน และมอบหมายหน้าที่รับผิดชอบให้แก่ผู้ปฏิบัติงานให้ชัดเจน | จัดให้มีมาตรการในการติดตามและประเมินผลการปฏิบัติงานของเจ้าหน้าที่ ผู้ปฏิบัติงาน | หน่วยงานที่บุคคลากรสังกัด |

**ขาดเจ้าหน้าที่ผู้มีความเชี่ยวชาญ ผู้ทำหน้าที่ในการบริหารจัดการระบบ** ผู้ที่รับผิดชอบด้านนโยบายและแผนกำหนดผู้รับผิดชอบด้านต่างๆ

**เจ้าหน้าที่ผู้รับผิดชอบอยู่ในปัจจุบัน ไม่มีความรู้ทางด้านไอทีโดยตรง** ผู้ที่รับผิดชอบนโยบายและแผนกำหนดการอบรมเพื่อพัฒนาศักยภาพแก่บุคลากรทางด้านไอที

**ความไม่ชัดเจนทางด้านโครงสร้างของการบริหารงานด้านไอที** ผู้บริหารจัดตั้งคณะทำงานรับผิดชอบด้านต่างๆ

| ที่ | รายการความเสี่ยง | โอกาส/ ผลกระทบ | มาตรการป้องกัน | แนวทางการกำกับดูแล | เจ้าภาพ |
|---|---|---|---|---|---|
| **10** | **ด้านผู้ใช้งาน** | | | | |
| 10.1 | ผู้ใช้ขาดความรู้ทางด้านไอที | ระดับกลาง/ ระดับกลาง | ให้ความรู้แก่ผู้ใช้งานทางด้านไอที | จัดให้มีการวัดผลความรู้ทางด้านไอที และตรวจสอบติดตามความ สำเร็จในการใช้งานระบบของผู้ใช้งาน | หน่วยงานที่ผู้ใช้งานสังกัด |
| 10.2 | ผู้ใช้งานขาดความรู้ความเข้าใจในการใช้งานระบบ | ระดับกลาง/ ระดับกลาง | จัดทำคู่มือการใช้งานในระบบ | จัดให้มีการวัดผลความรู้ทางด้านไอที และตรวจสอบติดตามความ สำเร็จในการใช้งานระบบของผู้ใช้งาน | หน่วยงานที่ผู้ใช้งานสังกัด |
| 10.3 | ผู้ใช้งานเป็นผู้ประสงค์ร้ายมีเจตนาเข้าถึงระบบในส่วนที่ไม่ได้รับสิทธิ | ระดับต่ำ/ ระดับสูง | ติดตั้งระบบตรวจสอบ, ตรวจจับ, ป้องกันการโจมตี - บุกรุก | ติดตามรายงานจากโปรแกรมตรวจจับการบุกรุกอย่างสม่ำเสมอเพื่อดูการใช้งานที่ผิดปกติ | หน่วยงานที่ผู้ใช้งานสังกัด |

**ผู้ใช้ขาดความรู้ทางด้านไอที** คณะทำงานจัดให้มีการให้ความรู้การใช้งานระบบไอทีแก่ส่วนราชการต่างๆ

**ผู้ใช้งานขาดความรู้ความเข้าใจในการใช้งานระบบ** คณะทำงานจัดทำคู่มือการใช้งานระบบแก่ส่วนราชการต่างๆ

**ผู้ใช้งานเป็นผู้ประสงค์ร้ายมีเจตนาเข้าถึงระบบในส่วนที่ไม่ได้รับสิทธิ** ติดตั้งระบบตรวจสอบ ตรวจจับ ป้องกันการโจมตีด้วยอุปกรณ์Firewall

# แผนดำเนินการมาตรการป้องกันความเสี่ยง

**ด้านโครงสร้างพื้นฐาน**

**1. ห้องศูนย์ข้อมูล**

1.1 ความปลอดภัยในการผ่านเข้าออก ห้องเครื่องคอมพิวเตอร์แม่ข่าย

<u>แนวทางการปฏิบัติ</u>

1) กำหนดสิทธิและเจ้าหน้าที่ผู้รับผิดในการเก็บรักษา Key card
2) บุคคลภายนอกเข้าออกเจ้าหน้าที่รับผิดชอบต้องรับทราบและอนุญาตทุกครั้ง

1.2 การปรับอากาศ เพื่อรักษาอุณหภูมิห้อง

<u>แนวทางการปฏิบัติ</u>

1) กำหนดระยะเวลาการใช้งานแต่ละเครื่อง(กรณีที่มีเครื่องมากกว่า 1 เครื่อง)
2) ทำความสะอาดแผ่นกรองอากาศอย่างสม่ำเสมอ
3) ล้างเครื่องปรับอากาศทุก 6 เดือน(ตามระยะเวลาการซ่อมบำรุง)
4) ทำการบันทึกในสมุดการบำรุงรักษาประจำเครื่องทุกครั้ง
5) กรณีที่เครื่องชำรุด ติดต่อประสานงานผู้ชำนาญการโดยเร่งด่วน

1.3 อุบัติภัย

<u>แนวทางการปฏิบัติ</u>

**ไฟไหม้**

1) ติดตั้งระบบป้องกันอัคคีภัย
2) ตรวจเช็คสภาพอุปกรณ์ตามระยะเวลาที่กำหนด
3) กรณีที่เกิดอัคคีภัย ให้ทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย(server) เป็นอันดับแรก

**น้ำท่วม**

1) วางอุปกรณ์สื่อสารและเครื่องคอมพิวเตอร์แม่ข่ายในห้องที่น้ำท่วมไม่ถึง
2) ทำการสำรองข้อมูลอย่างสม่ำเสมอ และแยกเก็บไว้คนละที่กับห้องเครื่องคอมพิวเตอร์แม่ข่าย(server room) กรณีที่น้ำท่วมเครื่องเสียหายจะได้มีข้อมูลสำรอง

**ตึกถล่ม**

1) วางอุปกรณ์สื่อสารและเครื่องคอมพิวเตอร์แม่ข่ายในตู้ที่ทนทานต่อแรงกระแทก
2) ทำการสำรองข้อมูลอย่างสม่ำเสมอ และแยกเก็บไว้คนละที่กับห้องเครื่องคอมพิวเตอร์แม่ข่าย(server room) กรณีที่ตึกถล่มเครื่องเสียหายจะได้มีข้อมูลสำรอง

## 2. ระบบไฟฟ้า

2.1 ไฟฟ้าดับ ไฟฟ้ากระชาก ไฟฟ้าเกิน ฟ้าผ่า

<u>แนวทางการปฏิบัติ</u>

1) ติดตั้งระบบป้องกันฟ้าผ่า
2) ติดตั้งระบบป้องกันไฟกระชาก
3) ติดตั้งระบบสายดิน
4) จัดหาอุปกรณ์ ไฟฟ้าสำรอง(UPS) สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสาร
5) ตรวจเช็คระบบให้สามารถใช้ได้อย่างสม่ำเสมอ

## 3. ระบบสื่อสาร- ระบบเครือข่าย

3.1 โทรศัพท์ใช้งานไม่ได้

<u>แนวทางการปฏิบัติ</u>

1) จัดหาเครื่องสำรอง
2) ตรวจเช็คระบบโทรศัพท์และสายสัญญาณอย่างสม่ำเสมอ

3.2 อินทราเน็ต(Intranet)ใช้งานไม่ได้

<u>แนวทางการปฏิบัติ</u>

1) ตรวจเช็คระบบอย่างสม่ำเสมอ
2) จัดหาอุปกรณ์สำรอง เช่น switch/hub, LAN Card
3) จัดหาช่องทางอื่นสำรอง เช่นระบบ Internet

3.3 อินเตอร์เน็ต(Internet)ใช้งานไม่ได้

<u>แนวทางการปฏิบัติ</u>

1) ตรวจเช็คระบบอย่างสม่ำเสมอ
2) จัดหาอุปกรณ์สำรอง เช่น switch/hub, LAN Card
3) จัดหาช่องทางอื่นสำรอง เช่น ช่องทาง Internet อื่น หรือ ระบบ Intranet

**ด้านอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่าย**

**4. อุปกรณ์คอมพิวเตอร์ลูกข่าย**

4.1 เครื่องคอมพิวเตอร์เสียหายใช้งานไม่ได้

<u>แนวทางการปฏิบัติ</u>

1) จัดหาเครื่องสำรอง
2) จัดหาอุปกรณ์สำรอง เช่น เมาส์ คีย์บอร์ด จอภาพ ฮาร์ดดิสก์ ซีดีรอมไดรฟ์
3) ตรวจเช็คและบำรุงรักษาเครื่องอย่างสม่ำเสมอ
4) ให้คำแนะนำวิธีการทดสอบเบื้องต้นแก่ผู้ใช้

4.2 ไวรัส สปายแวร์

<u>แนวทางการปฏิบัติ</u>

1) กำหนดให้เครื่องลูกข่ายทุกเครื่องต้องติดตั้งโปรแกรมป้องกันไวรัส
2) ให้คำแนะนำ การใช้งานเครือข่ายอย่างปลอดภัยแก่ผู้ใช้
3) จัดหาอุปกรณ์ที่ทำหน้าที่รักษาความปลอดภัย(Firewall)

**5. อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย**

5.1 หยุดการใช้บริการ,เสียหาย,ไม่สามารถใช้งานได้ตามปกติ

<u>แนวทางการปฏิบัติ</u>

1) ตรวจสอบทางด้านฮาร์ดแวร์ว่าทำงานปกติหรือไม่
    - ตรวจสอบว่าเครื่องสามารถเปิดได้หรือไม่
        - **เปิดไม่ได้** ให้ตรวจสอบ ฮาร์ดแวร์และระบบไฟฟ้า
        - **เปิดได้** ดำเนินการต่อ ข้อ 2
2) ตรวจสอบระบบปฏิบัติการ(Operation System)ว่ายังทำงานปกติหรือไม่
    - **ระบบปฏิบัติการไม่สามารถทำงานได้**
        - ให้ทำการติดตั้งระบบปฏิบัติการใหม่
        - ติดตั้งโปรแกรมประยุกต์ทั้งหมด
        - ติดตั้งข้อมูลที่สำรองไว้กลับสู่ระบบ
    - **ระบบปฏิบัติการทำงานเป็นปกติ** ดำเนินการต่อ ข้อ 3
3) ตรวจสอบเซอร์วิสต่างๆ เช่น Network , Database, Web base service ว่ายังทำงานปกติหรือไม่
    - **ปกติ** ทดสอบการใช้งานทั้งระบบ
    - **ไม่ปกติ** แก้ไขตามสาเหตุที่เกิดขึ้น

5.2 ไวรัส สปายแวร์

<u>แนวทางการปฏิบัติ</u>

1) ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย
2) ปรับปรุงให้เป็นเวอร์ชั่นที่ล่าสุด
3) ตรวจเช็คเครื่องอย่างสม่ำเสมอ

5.3 โดนโจมตี โดนบุกรุก

<u>แนวทางการปฏิบัติ</u>

1) ผู้ดูแลระบบต้องติดตามข่าวสารและหาวิธีการป้องกันใหม่ๆ
2) ปรับปรุงซอฟต์แวร์ที่ทันสมัยอยู่เสมอ
3) จัดหาอุปกรณ์ป้องกันความปลอดภัย(Firewall)

## 6. อุปกรณ์เครือข่ายและอุปกรณ์สื่อสาร

6.1 เสียหาย ไม่สามารถใช้งานได้ตามปกติ

<u>แนวทางการปฏิบัติ</u>

1) จัดหาอุปกรณ์สำรอง เช่น Switch/Hub , เครื่องโทรศัพท์,สายนำสัญญาณต่างๆ
2) ตรวจเช็คระบบเครือข่ายอย่างสม่ำเสมอ
3) เมื่อพบอาการขัดข้องต้องรีบดำเนินการแก้ไขโดยรีบด่วน

6.2 ตัวนำสัญญาณ สายสื่อสัญญาณต่างๆขาดชำรุด

<u>แนวทางการปฏิบัติ</u>

1) จัดหาอุปกรณ์สำรอง เช่น สายโทรศัพท์ , สาย LAN ,ท่อเดินสายต่างๆ
2) ตรวจเช็คสายนำสัญญาณอย่างสม่ำเสมอ
3) เมื่อเดินสายสัญญาณใหม่ต้องร้อยท่อป้องกันสาย
4) เปลี่ยนมาใช้ระบบไร้สาย

**ด้านข้อมูล-อุปกรณ์สำรองข้อมูล**

**7. ด้านข้อมูล**

7.1 การเข้าถึงข้อมูลไม่ได้

<u>แนวทางการปฏิบัติ</u>

1) ตรวจสอบระบบเครือข่าย
2) ตรวจสอบระบบเครื่องคอมพิวเตอร์แม่ข่าย
3) ตรวจสอบระบบฐานข้อมูล
4) ตรวจสอบเซอร์วิสต่างๆของเครื่องคอมพิวเตอร์แม่ข่าย
5) ทดสอบระบบว่าใช้งานได้เป็นปกติหรือไม่
6) ถ้ายังไม่ได้ให้ตรวจสอบขั้นตอนที่ยังมีปัญหา

7.2 การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

<u>แนวทางการปฏิบัติ</u>

1) ติดตั้งระบบที่สามารถกำหนดสิทธิการเข้าถึงแต่ระดับได้
2) กำหนดสิทธิการเข้าถึงให้สอดคล้องตามนโยบาย
3) ตรวจเช็คระบบการกำหนดสิทธิว่าเป็นสิทธิเดิมหรือไม่

7.3 ความเชื่อถือไม่ได้ของข้อมูล

<u>แนวทางการปฏิบัติ</u>

1) กำหนดผู้รับผิดชอบแต่ละมิติข้อมูลของหน่วยงาน
2) กำหนดความถี่ในการปรับปรุงและรับรองข้อมูล

7.4 ข้อมูลเสียหาย

<u>แนวทางการปฏิบัติ</u>

1) จัดให้มีระบบสำรองข้อมูล เช่น สำรองเครื่องคอมพิวเตอร์แม่ข่าย , Tape Drive
2) CD Writer
3) กำหนดให้สำรองข้อมูล(Backup)ทุกสัปดาห์
4) เมื่อเกิดเหตุขัดข้องที่เครื่องคอมพิวเตอร์แม่ข่ายหรือข้อมูลศูนย์หายให้นำข้อมูลสำรองล่าสุดมาใช้(Recovery)

**8. ด้านอุปกรณ์บันทึก-สำรองข้อมูล**

8.1 วิธีการไม่ถูกต้องในการสำรองข้อมูล

<u>แนวทางการปฏิบัติ</u>

1) ศึกษาวิธีการที่เหมาะสมกับระบบที่มีใช้งานอยู่
2) ดำเนินการตามวิธีที่เหมาะสม
3) กำหนดเวลาสำรองข้อมูลทุกสัปดาห์

8.2 เลือกสื่อบันทึกข้อมูลไม่เหมาะสมกับข้อมูล

<u>แนวทางการปฏิบัติ</u>

1) ศึกษาองค์ประกอบต่างๆเกี่ยวกับอุปกรณ์บันทึกข้อมูลว่าสามารถรองรับระบบที่มีหรือไม่
2) จัดหาอุปกรณ์บันทึกข้อมูลที่เหมาะสม

8.3 เสียหาย ไม่สามารถใช้งานได้

<u>แนวทางการปฏิบัติ</u>

1) จัดให้มีอุปกรณ์สำรอง
2) ตรวจเช็คบำรุงอย่างสม่ำเสมอ

**ด้านบุคลากรและผู้ใช้งาน**

**9. ด้านบุคลากร**

9.1 ขาดเจ้าหน้าที่ผู้เชี่ยวชาญ ผู้ทำหน้าที่ในการบริหารจัดการ

<u>แนวทางการปฏิบัติ</u>

1) จัดตั้งคณะทำงานผู้รับผิดชอบด้านต่างๆ
2) กำหนดเจ้าหน้าที่รับผิดชอบเฉพาะด้าน
3) ฝึกอบรมเจ้าหน้าที่เฉพาะด้านเพื่อให้เกิดความเชี่ยวชาญ

9.2 เจ้าหน้าที่ผู้รับผิดชอบอยู่ในปัจจุบันไม่มีความรู้ทางด้านไอทีโดยตรง

<u>แนวทางการปฏิบัติ</u>

1) กำหนดผู้รับผิดชอบร่วมในเรื่องยังขาดความชำนาญ

9.3 ความไม่ชัดเจนทางด้านโครงสร้างของการบริหารงานด้านไอที

<u>แนวทางการปฏิบัติ</u>

1) ผู้บริหารควรจัดโครงสร้างสายการปฏิบัติงานและมอบหมายงานให้ชัดเจน
2) จัดให้มีการติดตามและประเมินผล

**10. ด้านผู้ใช้**

10.1 ผู้ใช้ขาดความรู้ทางด้านไอที

<u>แนวทางการปฏิบัติ</u>

1) จำแนกกลุ่มผู้ใช้
2) จัดทำเอกสารคู่มือวิธีการใช้

10.2 ผู้ใช้ขาดความรู้ความเข้าใจในการใช้งานระบบ

<u>แนวทางการปฏิบัติ</u>

1) จัดทำคู่มือการใช้งานระบบ
2) แนะนำประชาสัมพันธ์ความสามารถของระบบ

10.3 ผู้ใช้เป็นผู้ประสงค์ร้ายมีเจตนาเข้าถึงระบบในส่วนที่ไม่ได้รับสิทธิ

<u>แนวทางการปฏิบัติ</u>

1) ติดตั้งระบบตรวจสอบ ตรวจจับ ป้องกัน โดยอุปกรณ์รักษาความปลอดภัย (Firewall)
2) กำหนดนโยบายรักษาความปลอดภัย (Policy) ที่เหมาะสม
3) ศึกษารูปแบบการโจมตีแบบต่างๆเพื่อนำมาใช้ในการป้องกัน

# แผนการแก้ไขกรณีความเสี่ยง

เนื่องจากความเสี่ยงของระบบสารสนเทศนั้นไม่สามารถป้องกันได้ทั้งหมด การที่ความเสี่ยงจะเกิดขึ้นกับระบบสารสนเทศทั้งหมดนั้นสามารถเกิดได้ทุกขณะ นอกจากการวางแผนการป้องกันความเสี่ยงที่จะเกิดขึ้นกับระบบให้รัดกุมที่สุดแล้ว การเตรียมแผนการแก้ไขกรณีที่คาดว่าความเสี่ยงเกิดขึ้นก็เป็นขั้นตอนหนึ่งที่ต้องมีการจัดเตรียมไว้ปฏิบัติ เพื่อแก้ไขปัญหาต่อการให้บริการด้านข้อมูลของศูนย์ปฏิบัติการจังหวัด และความเสถียรภาพของระบบสารสนเทศและศูนย์ปฏิบัติการจังหวัด

ทางจังหวัดได้ทำการออกแบบแผนการแก้ไขกรณีที่ความเสี่ยงของระบบสารสนเทศในแต่ละกรณีได้เกิดขึ้นจริง โดยแผนการแก้ไขกรณีความเสี่ยงที่ได้ออกแบบมานี้ ได้ทำการรวบรวมปัญหาที่ได้เกิดขึ้นจริงกับระบบสารสนเทศและศูนย์ปฏิบัติการจังหวัด และนำมาออกแบบเป็นแผนการปฏิบัติ โดยมีกรณีความเสี่ยงอยู่ทั้งหมด ดังนี้

- เครื่องปรับอากาศขัดข้อง
- คอมพิวเตอร์แม่ข่ายเสียหายฉับพลัน
- ระบบเครือข่ายขัดข้อง
- ระบบปฏิบัติการทำงานผิดพลาด
- ข้อมูลสูญหาย
- อัคคีภัย
- อุทกภัย
- แผ่นดินไหว

กรณีความเสี่ยงที่ได้ทำการจัดเตรียมแผนการแก้ไขปัญหาข้างต้น เป็นความเสี่ยงของระบบสารสนเทศที่มักจะเกิดขึ้นกับระบบสารสนเทศและศูนย์ปฏิบัติการจังหวัด และทางจังหวัดยังคาดว่ากรณีความเสี่ยงที่ได้คาดการไว้นั้น ยังจะเกิดขึ้นกับระบบสารสนเทศและศูนย์ปฏิบัติการจังหวัดอยู่บ้าง

**เครื่องปรับอากาศขัดข้อง**

ระบบสารสนเทศและศูนย์ปฏิบัติการจังหวัดนั้น ล้วนเป็นอุปกรณ์อิเล็กทรอนิกส์ซึ่งเมื่อมีการทำงานแล้วจะสร้างความร้อนออกมาเป็นจำนวนมาก การแก้ไขปัญหาดังกล่าว ซึ่งเป็นที่นิยมก็คือสร้างห้องสื่อสารที่มิดชิด และติดเครื่องปรับอากาศเพื่อลดอุณภูมิให้กับอุปกรณ์อิเล็กทรอนิกส์ดังกล่าว แต่เนื่องจากเครื่องปรับอากาศซึ่งประกอบไปด้วยอุปกรณ์อิเล็กทรอนิกส์ด้วยเช่นกัน อาจจะทำให้เครื่องปรับอากาศเกิดการขัดข้องได้ และเมื่อเครื่องปรับอากาศเกิดการขัดข้องแล้ว ทำให้อุณหภูมิในห้องสื่อสารสูงขึ้นในเวลาอันรวดเร็วและอาจจะทำให้อุปกรณ์ระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย เกิดการชำรุดเสียหายได้

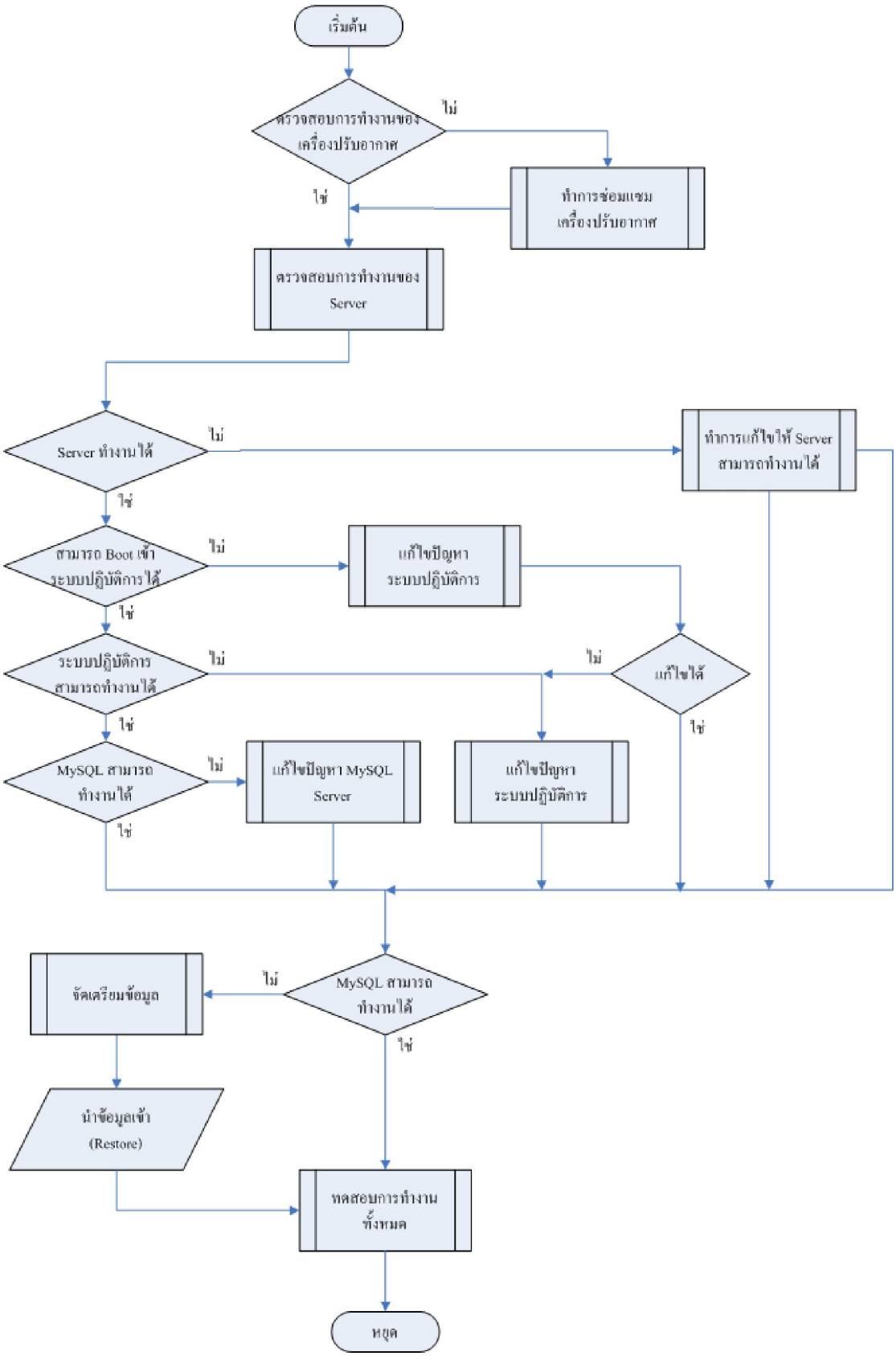
ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

หลังจากที่ผู้ดูแลระบบสารสนเทศประจำจังหวัดรับทราบปัญหาที่เกิดขึ้นเกี่ยวกับการทำงานของเครื่องปรับอากาศซึ่งมีผลกระทบกับศูนย์ปฏิบัติการจังหวัด ผู้ดูแลระบบสารสนเทศจะต้องปฏิบัติตามขั้นตอนเพื่อแก้ไขปัญหาดังต่อไปนี้

1. ผู้ดูแลระบบสารสนเทศต้องทำการตรวจสอบการทำงานของเครื่องปรับอากาศที่เป็นตัวควบคุม
2. ในกรณีที่เครื่องปรับอากาศประจำห้องสื่อสารไม่สามารถทำงานได้ตามปกติ ผู้ดูแลระบบสารสนเทศจำเป็นจะต้องทำการแก้ไข ซ่อมแซม เครื่องปรับอากาศให้สามารถทำงานได้เต็มประสิทธิภาพ
3. เนื่องจากการที่เครื่องปรับอากาศในห้องสื่อสารมีการงานที่ขัดข้อง อาจจะทำให้เครื่องคอมพิวเตอร์แม่ข่ายเสียหายได้ ผู้ดูแลระบบต้องทำการตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดที่ติดตั้งอยู่ในห้องสื่อสาร
4. ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายสามารถไม่สามารทำงานได้ตามปกติ ผู้ดูแลระบบสารสนเทศต้องทำการแก้ไขให้เครื่องคอมพิวเตอร์แม่ข่ายสามารถทำงานได้ตามปกติโดยเร็วที่สุด และในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหายจนไม่สามารถทำงานได้ ผู้ดูแลระบบจะต้องทำการจัดหาเครื่องคอมพิวเตอร์แม่ข่าย เพื่อมาติดตั้งระบบใหม่ทั้งหมด โดยเร็วที่สุด
5. ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายสามารถทำงานได้ตามปกติ ผู้ดูแลระบบจะต้องทำการตรวจสอบการทำงานทั้งหมดของระบบ ให้มั่นใจว่า ระบบทั้งหมดสามารถทำงานได้ตามปกติ และจะไม่เกิดปัญหาตามมาในภายหลัง
6. ขั้นตอนต่อไปของการแก้ไขปัญหาคือการตรวจสอบการทำงานของระบบปฏิบัติการ (Operating System) สามารถเรียกค่าการทำงานเริ่มต้นได้หรือไม่ ถ้าหากไม่สามารถ

ทำงานตามการทำงานปกติได้ ผู้ดูแลระบบสารสนเทศจะต้องทำการติดตั้งระบบใหม่ทั้งหมดให้กับเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด

7. การตรวจสอบการทำงานของระบบปฏิบัติการ ต้องพิจารณาจากการทำงานของศูนย์ปฏิบัติการจังหวัดเป็นหลัก นั่นคือการทำงานอยู่บนระบบปฏิบัติการที่มีความพร้อมในการให้บริการ หากว่าการทำงานไม่เป็นไปตามปกติ ผู้ดูแลระบบสารสนเทศจะต้องทำการติดตั้งระบบใหม่ทั้งหมดให้กับเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด
8. หลังจากที่ทำการตรวจสอบและแก้ปัญหาของระบบปฏิบัติการแล้ว ผู้ดูแลระบบจะต้องทำการตรวจสอบการทำงานของโปรแกรม MySQL Server ซึ่งเป็นหัวใจหลักของการบันทึกข้อมูลของศูนย์ปฏิบัติการจังหวัด และในกรณีที่โปรแกรม MySQL Server ไม่สามารถทำงานได้ จะต้องทำการแก้ไขปัญหา ด้วยการติดตั้งโปรแกรม MySQL Server ใหม่พร้อมกับทดสอบการทำงานอีกครั้ง
9. จัดเตรียมข้อมูลที่ได้จาการสำรองข้อมูลตามตารางการสำรองข้อมูล และทำการนำเข้าข้อมูล เข้าสู่ศูนย์ปฏิบัติการจังหวัด
10. ทำการทดสอบระบบศูนย์ปฏิบัติการ โดยทดสอบการทำงานทั้งหมด ตามที่ศูนย์ปฏิบัติการสามารถทำงานได้ อีกครั้งหนึ่งเพื่อให้แน่ใจว่าการทำงานของศูนย์ปฏิบัติการจังหวัดสามารถทำงานได้ โดยจำจะไม่เกิดปัญหาขึ้นภายหลัง



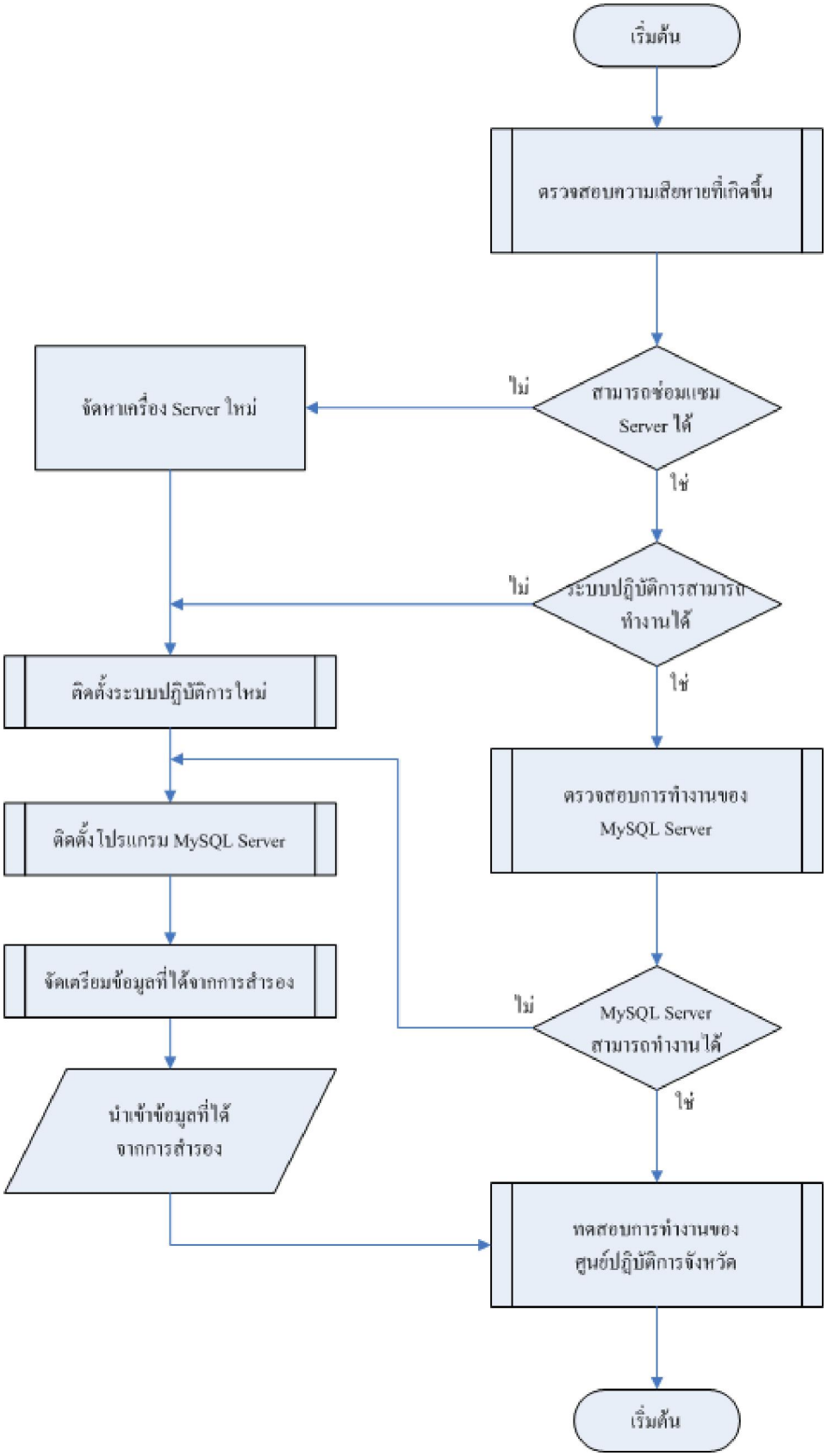

แสดงแผนการแก้ไขปัญหากรณีเครื่องปรับอากาศเสียหาย

**คอมพิวเตอร์แม่ข่ายเสียหายฉับพลัน**

เครื่องคอมพิวเตอร์แม่ข่ายมีส่วนประกอยไปด้วยอุปกรณ์อิเล็กทรอนิกส์ที่ละเอียดอ่อน การที่เครื่องคอมพิวเตอร์จะเกิดความเสียหายได้ก็มีความเป็นไปได้สูง ยกตัวอย่างเช่นการถูกละอองความชื้นจับตัวอยู่บนวงจรอิเล็กทรอนิกส์เหล่านั้น ทำให้เกิดการลัดวงจรของอุปกรณ์เหล่านั้น หรือถูกสัตว์ฟันแทะเข้ามาทำลายอุปกรณ์ดังกล่าว ซึ่งส่งผลทำให้เครื่องคอมพิวเตอร์แม่ข่ายเกิดการทำงานที่ผิดพลาด หรืออาจจะถึงขึ้นใช้งานไม่ได้เลยก็เป็นได้

ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

1. ผู้ดูแลระบบสารสนเทศทำการตรวจสอบความเสียหายที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย หลังจากเกิดความเสียหายกับคอมพิวเตอร์แม่ข่ายอย่างฉับพลัน
2. ถ้าหากว่าผู้ดูแลระบบสารสนเทศทำการแก้ไข ซ่อมแซมเครื่องคอมพิวเตอร์แม่ข่ายได้ ให้ทำการแก้ไข ซ่อมแซมเครื่องคอมพิวเตอร์แม่ข่ายให้สามารถทำงานได้ตามปกติ และทำการตรวจสอบระบบปฏิบัติการว่าสามารถทำงานได้ตามปกติหรือไม่ ถ้าไม่สามารถทำงานได้ จะต้องทำการติดตั้งระบบปฏิบัติการใหม่พร้อมทั้งติดตั้งโปรแกรม MySQL Server
3. ถ้าหากว่าไม่สามารถแก้ไข ซ่อมแซมเครื่องคอมพิวเตอร์แม่ข่ายได้ ผู้ดูแลระบบจะต้องทำการจัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายเครื่องใหม่ เพื่อมาใช้งานแทนเครื่องคอมพิวเตอร์แม่ข่ายเครื่องเดิม
4. ทำการติดตั้งระบบปฏิบัติการใหม่ และปรับแต่งระบบปฏิบัติการให้สามารถรองรับการทำงานของศูนย์ปฏิบัติการจังหวัด ให้ครบทุกคุณสมบัติ
5. จัดเตรียมข้อมูลที่ได้จากการสำรอง เข้าสู่ระบบฐานข้อมูลของศูนย์ปฏิบัติการจังหวัด
6. ทดสอบการทำงานของศูนย์ปฏิบัติการจังหวัด ให้ครบทุกคุณสมบัติของการทำงานอีกครั้ง เพื่อเตรียมให้บริการออกสู่ระบบเครือข่ายต่อไป




แสดงแผนการแก้ไขปัญหากรณีเครื่องคอมพิวเตอร์แม่ข่ายเสียหายฉับพลัน

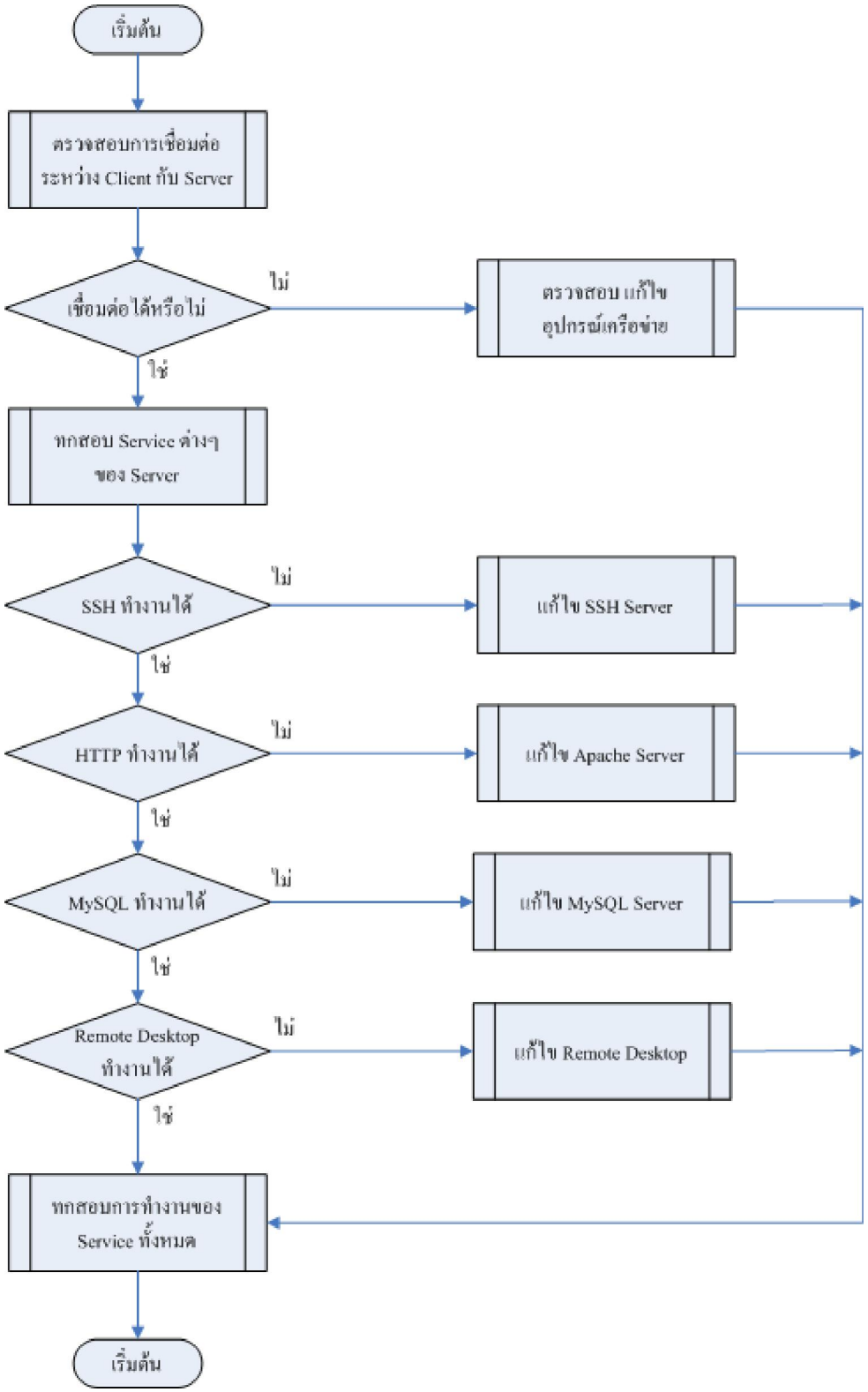
**ระบบเครือข่ายขัดข้อง**

ศูนย์ปฏิบัติการจังหวัดเป็นระบบที่ทำงานที่เรียกว่า Web Base Service และมีให้บริการข้อมูลอยู่บนระบบเครือข่ายทั้งระบบเครือข่ายอินเตอร์เน็ท และระบบเครือข่ายอินทราเน็ท ซึ่งศูนย์ปฏิบัติการจะต้องมีการเชื่อมอยู่บนระบบเครือข่ายตลอดเวลา การที่กรณีความเสี่ยงระบบสารสนเทศเกิดขึ้นกับระบบเครือข่ายแล้วจะทำให้ศูนย์ปฏิบัติการจังหวัดไม่สามารถให้บริการแก่สาธารณชนได้ ซึ่งโดยปกติแล้วจะถือว่าได้เป็นระบบที่ไม่มีความเสถียรภาพ และไม่มีความน่าเชื่อถือเลย

การวิเคราะห์แก้ไขปัญหาเกี่ยวกับระบบเครือข่ายนั้นมักจะเกิดขึ้นอยู่เป็นประจำ เนื่องจากการเชื่อมต่อศูนย์ปฏิบัติการจังหวัดของจังหวัดนั้น ได้มีการเชื่อมต่ออยู่กับระบบเครือข่ายอินเตอร์เน็ทที่มีการเช่าวงจรของ ISP และในปัจจุบันยังพบว่าการเชื่อมยังมีปัญหาอยู่เป็ประจำ

ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

1. ทำการตรวจสอบการทำงานของระบบเครือข่ายโดยตรวจสอบจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้วิธีการ ping
2. ในกรณีที่ไม่สามารถเชื่อมต่อได้ ผู้ดูแลระบบจะต้องทำการตรวจสอบพร้อมทั้งแก้ไขการเชื่อมต่อของเครื่องคอมพิวเตอร์แม่ข่าย เข้ากับระบบเครือข่าย
3. ทำการตรวจสอบ Service ต่างๆ ของระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายศูนย์ปฏิบัติการจังหวัด ว่าสามารถทำงานได้ถูกต้องหรือไม่ โดยต้องตรวจสอบการทำงานของ Service ดังนี้ SSH Server, HTTP Server, MySQL Server, Remote Desktop
4. ทำการตรวจสอบการทำงานของ SSH Server ผ่านระบบเครือข่าย ถ้าหากว่าไม่สามารถทำการติดต่อได้ ผู้ดูแลระบบจะต้องทำการแก้ไขระบบเครือข่ายให้สามารถทำงานได้
5. ทำการตรวจสอบการทำงานของ HTTP Server ผ่านระบบเครือข่าย ถ้าหากว่าไม่สามารถทำการติดต่อได้ ผู้ดูแลระบบจะต้องทำการแก้ไขระบบเครือข่ายให้สามารถทำงานได้
6. ทำการตรวจสอบการทำงานของ MySQL Server ผ่านระบบเครือข่าย ถ้าหากว่าไม่สามารถทำการติดต่อได้ ผู้ดูแลระบบจะต้องทำการแก้ไขระบบเครือข่ายให้สามารถทำงานได้
7. ทำการตรวจสอบการทำงานของ Remote Desktop ผ่านระบบเครือข่าย ถ้าหากว่าไม่สามารถทำการติดต่อได้ ผู้ดูแลระบบจะต้องทำการแก้ไขระบบเครือข่ายให้สามารถทำงานได้
8. ทดสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบเครือข่าย ให้ครบทุกคุณสมบัติทั้งหมด เพื่อเตรียมความพร้อมให้ศูนย์ปฏิบัติการจังหวัดสามารถบริการข้อมูลได้ถูกต้อง



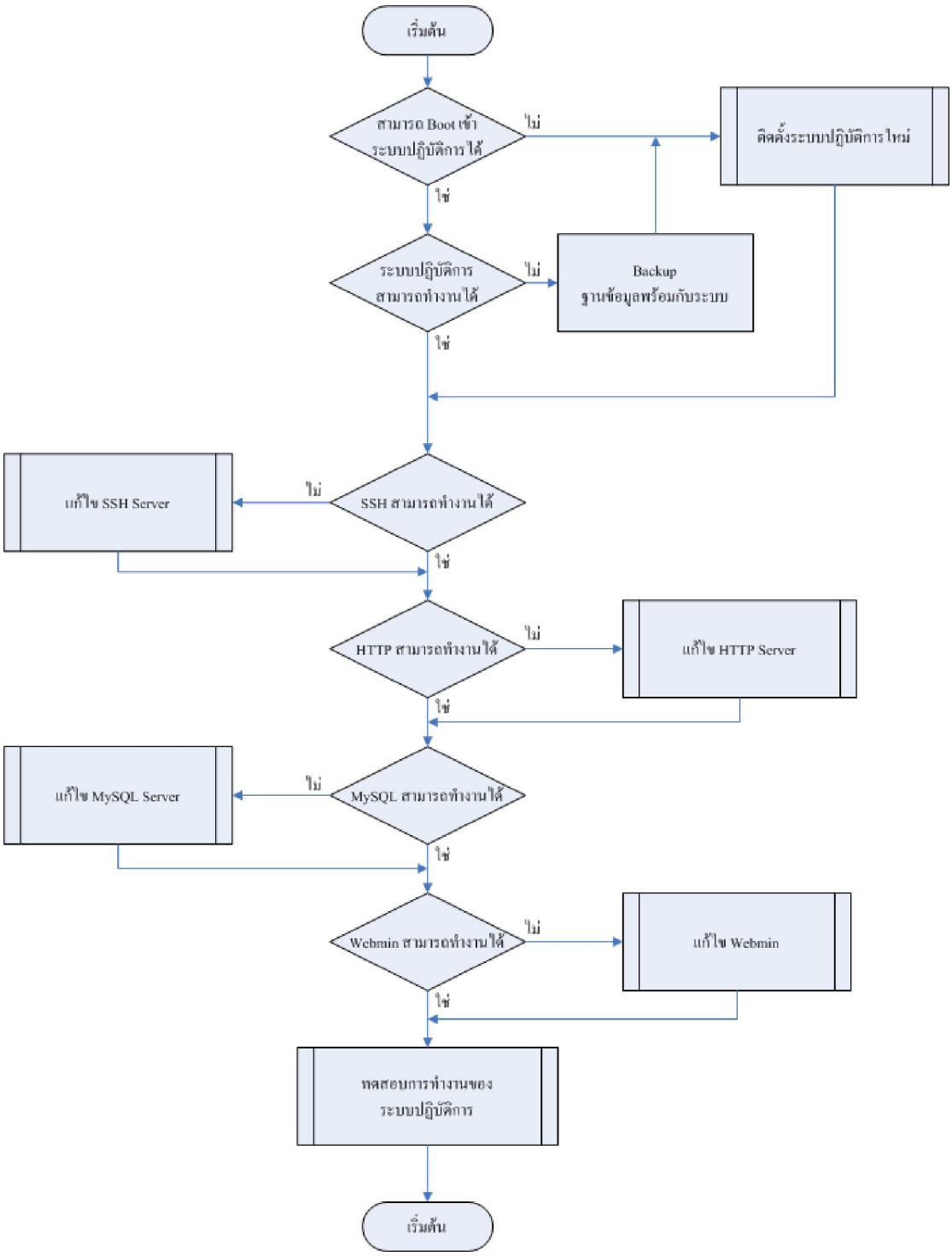

แสดงแผนการแก้ไขปัญหากรณีระบบเครือข่ายขัดข้อง

**ระบบปฏิบัติทำงานผิดพลาด**

ศูนย์ปฏิบัติการจังหวัดถูกพัฒนาให้มีการทำงานบนระบบปฏิบัติการ Linux เพื่อความเสถียรภาพของระบบ และในการทำงานจริง อาจจะเป็นไปได้ว่ากรณีที่เครื่องคอมพิวเตอร์แม่ข่ายมีผลกระทบจากกรณีความเสี่ยงอื่นๆ เช่นคอมพิวเตอร์แม่ข่ายหยุดการทำงานฉับพลัน อาจจะทำให้ระบบปฏิบัติการทำงานผิดพลาด ซึ่งจะส่งผลกระทบโดยตรงกับการทำงานของศูนย์ปฏิบัติการจังหวัด

ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

1. ทำการตรวจสอบการทำงานของระบบปฏิบัติการ โดยตรวจสอบการทำงานในการเริ่มต้นของระบบปฏิบัติการ ถ้าไม่สามารถเริ่มต้นการทำงานได้ แสดงว่าระบบปฏิบัติการเสียหายและจะไม่สามารถใช้งานได้ ผู้ดูแลระบบต้องทำการติดตั้งระบบปฏิบัติการใหม่ทั้งหมด
2. ในกรณีที่ระบบปฏิบัติการสามารถเริ่มต้นระบบได้ ให้ผู้ดูแลระบบทำการตรวจสอบการทำงานของระบบปฏิบัติการ โดยตรวจสอบการทำงานให้ครบทุกคุณสมบัติของระบบปฏิบัติการ
3. ในกรณีที่ระบบปฏิบัติการไม่สามารถทำงานได้ครบทุกคุณสมบัติการทำงาน ให้ผู้ดูแลระบบทำการสำรองฐานข้อมูลพร้อมทั้งศูนย์ปฏิบัติการจังหวัด ไว้บนสื่อบันทึกข้อมูล และทำการติดตั้งระบบปฏิบัติการใหม่ทั้งหมด
4. ทำการตรวจสอบการทำงานของ SSH Server ของระบบปฏิบัติการ และในกรณีที่ไม่สามารถทำงานได้ ผู้ดูแลระบบต้องทำการปรับแต่งให้สามารถทำงานได้
5. ทำการตรวจสอบการทำงานของ HTTP Server ของระบบปฏิบัติการ และในกรณีที่ไม่สามารถทำงานได้ ผู้ดูแลระบบต้องทำการปรับแต่งให้สามารถทำงานได้
6. ทำการตรวจสอบการทำงานของ MySQL Server ของระบบปฏิบัติการ และในกรณีที่ไม่สามารถทำงานได้ ผู้ดูแลระบบต้องทำการปรับแต่งให้สามารถทำงานได้
7. ทำการตรวจสอบการทำงานของ Webmin ของระบบปฏิบัติการ และในกรณีที่ไม่สามารถทำงานได้ ผู้ดูแลระบบต้องทำการปรับแต่งให้สามารถทำงานได้




แสดงแผนการแก้ไขปัญหากรณีระบบปฏิบัติการทำงานผิดพลาด

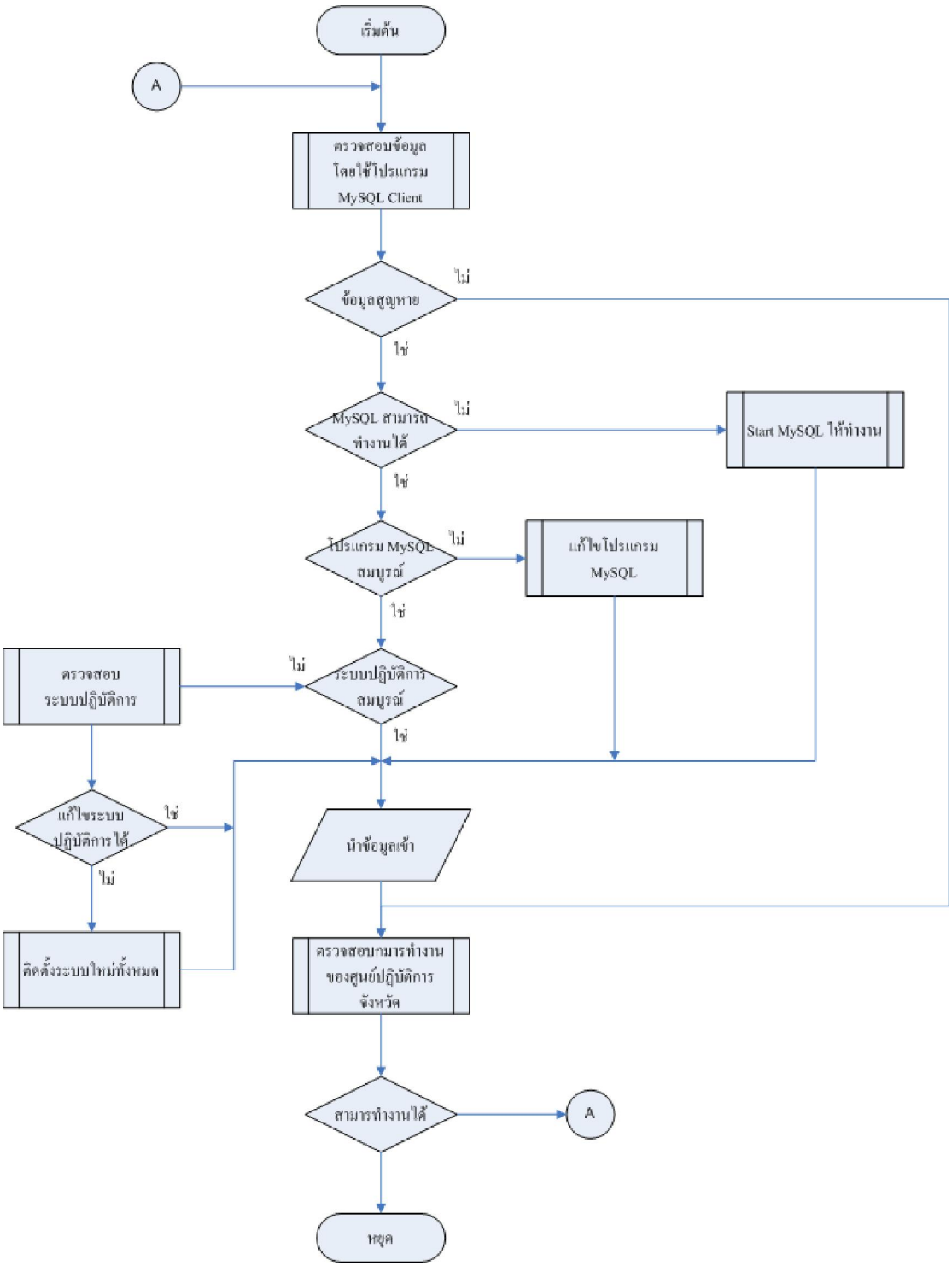
**ข้อมูลสูญหาย**

ศูนย์ปฏิบัติการจังหวัดการจังหวัดได้ถูกออกแบบให้มีการบันทึกข้อมูลบนโปรแกรมบริหารจัดการฐานข้อมูลยี่ห้อ MySQL เวอร์ชัน 4.0.25 หรือสูงกว่า และเนื่องจากกรณีความเสี่ยงที่ทางจังหวัดเคยประสบก็คือการที่เครื่องคอมพิวเตอร์แม่ข่ายหยุดการทำงานฉับพลัน และทำให้ระบบปฏิบัติการมีการทำงานที่ผิดพลาด และสั่งงานให้โปรแกรมบริหารจัดการฐานข้อมูล MySQL ทำงานผิดขั้นตอน และข้อมูลสูญหายในที่สุด

จะเห็นได้ว่ากรณีความเสี่ยงอาจจะส่งผลให้การทำงานของระบบสารสนเทศและศูนย์ปฏิบัติการจังหวัดมีการทำงานที่ผิดพลาด โดยมีความสัมพันธ์ต่อเนื่องกันไป จากกรณีข้อมูลสูญหาย ทางจังหวัดได้ออกแบบให้มีแผนการแก้ไขปัญหาตามขั้นตอนดังนี้

ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

1. ทำการตรวจสอบข้อมูลที่ถูกบันทึกลงในโปรแกรมระบบจัดการฐานข้อมูล โดยใช้โปรแกรม MySQL Client ยกตัวอย่างเช่น MySQL Front, Premiumsoft Navicat ฯลฯ
2. ในกรณีที่ข้อมูลเกิดการสูญหาย ผู้ดูแลระบบต้องทำการตรวจสอบการทำงานของโปรแกรม MySQL Server ให้ครบทุกคุณสมบัติ และถ้าไม่สามารถทำงานได้ตามคุณสมบัติแล้ว ผู้ดูแลระบบต้องทำการสำรองฐานข้อมูลเก่า และทำการติดตั้งโปรแกรม MySQL Server ใหม่ เพื่อให้โปรแกรม MySQL Server สามารถทำงานได้ทุกคุณสมบัติ
3. ถ้าหากว่าโปรแกรม MySQL Server สามารถทำงานได้ตามคุณสมบัติ แต่ข้อมูลยังเกิดการสูญหาย ผู้ดูแลระบบต้องทำการตรวจสอบการทำงานของระบบปฏิบัติการที่ติดถึงอยู่บนศูนย์ปฏิบัติการจังหวัด
4. ถ้าหากว่าระบบปฏิบัติการมีการทำงานที่ขัดข้องแล้ว ผู้ดูแลระบบจะต้องทำการแก้ไขปัญหาการทำงานของระบบปฏิบัติการ ให้ทำงานได้ตามปกติ
5. ในกรณีที่ระบบปฏิบัติการไม่สามารถทำการแก้ไขปัญหาที่เกิดขึ้นได้ ผู้ดูแลระบบต้องทำการติดตั้งระบบปฏิบัติการใหม่ ให้กับเครื่องคอมพิวเตอร์แม่ข่ายสำหรับศูนย์ปฏิบัติการจังหวัดใหม่ทั้งหมด พร้อมทั้งติดตั้งโปรแกรมและ Service ต่างๆ ให้ครบทุกคุณสมบัติการทำงาน
6. นำข้อมูลที่ได้จากการสำรอง เข้าสู่โปรแกรมจัดการฐานข้อมูล MySQL Server และติดตั้งศูนย์ปฏิบัติการจังหวัด
7. ทดสอบการทำงานของศูนย์ปฏิบัติการจังหวัดให้ครบทุกคุณสมบัติการทำงาน ถ้าหากสามารถทำงานได้ ให้เตรียมความพร้อมในการให้บริการศูนย์ปฏิบัติการจังหวัด แต่ถ้าไม่สามารถทำงานได้ ให้เริ่มวิเคราะห์เพื่อแก้ไขปัญหาใหม่ทั้งหมด




แสดงแผนการแก้ไขปัญหากรณีข้อมูลสูญหาย

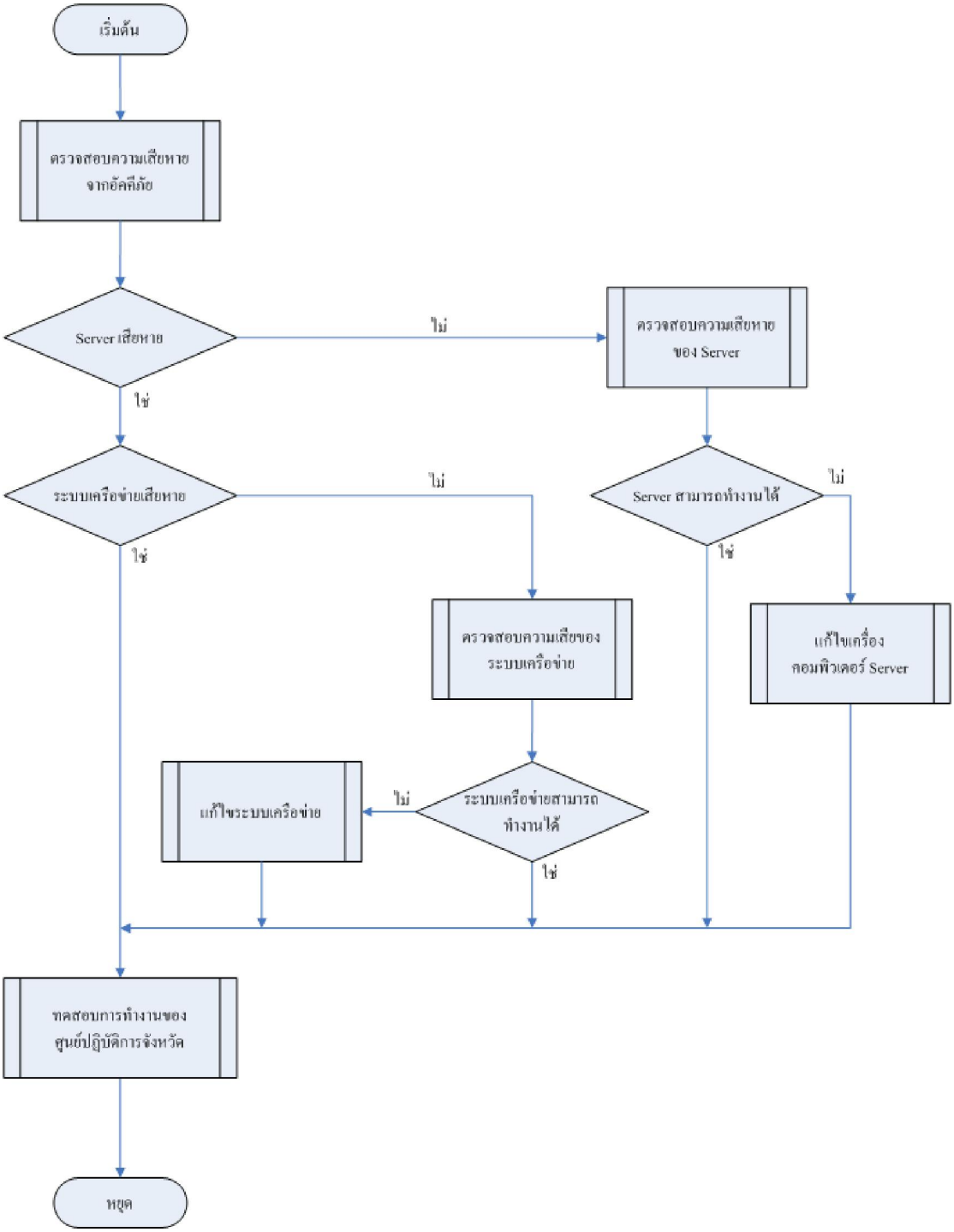
**อัคคีภัย**

กรณีที่ห้องสื่อสารจังหวัดเกิดกรณีความเสี่ยงที่เกิดมาจากอัคคีภัย ทางจังหวัดได้ให้ความสำคัญเป็นอันดับต้นๆ ของกรณีความเสี่ยง เนื่องจากว่าหากเกิดไฟไหม้ห้องสื่อสารแล้ว ความเสียหายที่คาดว่าจะเกิดขึ้นนั้น จะสูงกว่ากรณีความเสี่ยงอื่นๆ

การแก้ไขกรณีความเสี่ยงที่เกิดจากไฟไหม้นั้น กรณีที่ได้ยกตัวอย่างขึ้นมาคือการสร้างระบบใหม่มาทั้งหมด ตั้งแต่การคัดเลือกเครื่องคอมพิวเตอร์แม่ข่าย และการติดตั้งระบบปฏิบัติการใหม่ทั้งหมด ส่วนตัวระบบของศูนย์ปฏิบัติการจังหวัดและฐานข้อมูลนั้นจะได้จากการที่เจ้าหน้าที่ผู้ดูแลระบบระบบสารสนเทศได้ทำการสำรองไว้

ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

1. ผู้ดูแลระบบทำการตรวจสอบความเสียหายที่เกิดจากอัคคีภัย ซึ่งรวมไปถึงเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย
2. ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเกิดการเสียหายขึ้น ผู้ดูแลระบบต้องทำการแก้ไขซ่อมแซมเครื่องคอมพิวเตอร์แม่ข่าย และในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเสียหายจนไม่สามารถทำการแก้ไขซ่อมแซมได้ ผู้ดูแลระบบต้องทำการจัดหาเครื่องคอมพิวเตอร์แม่ข่ายเครื่องใหม่ มาติดตั้งระบบแทน
3. ในกรณีที่ระบบเครือข่ายเกิดความเสียหาย ผู้ดูแลระบบต้องทำการแก้ไข ซ่อมแซมระบบเครือข่าย และในกรณีที่อุปกรณ์ระบบเครือข่ายเสียหายจนไม่สามารถแก้ไข ซ่อมแซมได้ ผู้ดูแลระบบต้องทำการจัดหาอุปกรณ์เครือข่าย มาติดตั้งแทนอุปกรณ์ระบบเครือข่ายเดิม
4. ผู้ดูแลระบบทำการตรวจสอบการทำงานของศูนย์ปฏิบัติการจังหวัด โดยทำการทดสอบให้ครบทุกคุณสมบัติของศูนย์ปฏิบัติการจังหวัด และทำการทดสอบการทำงานผ่านระบบเครือข่ายทั้งหมด




แสดงแผนการแก้ไขปัญหากรณีอัคคีภัย

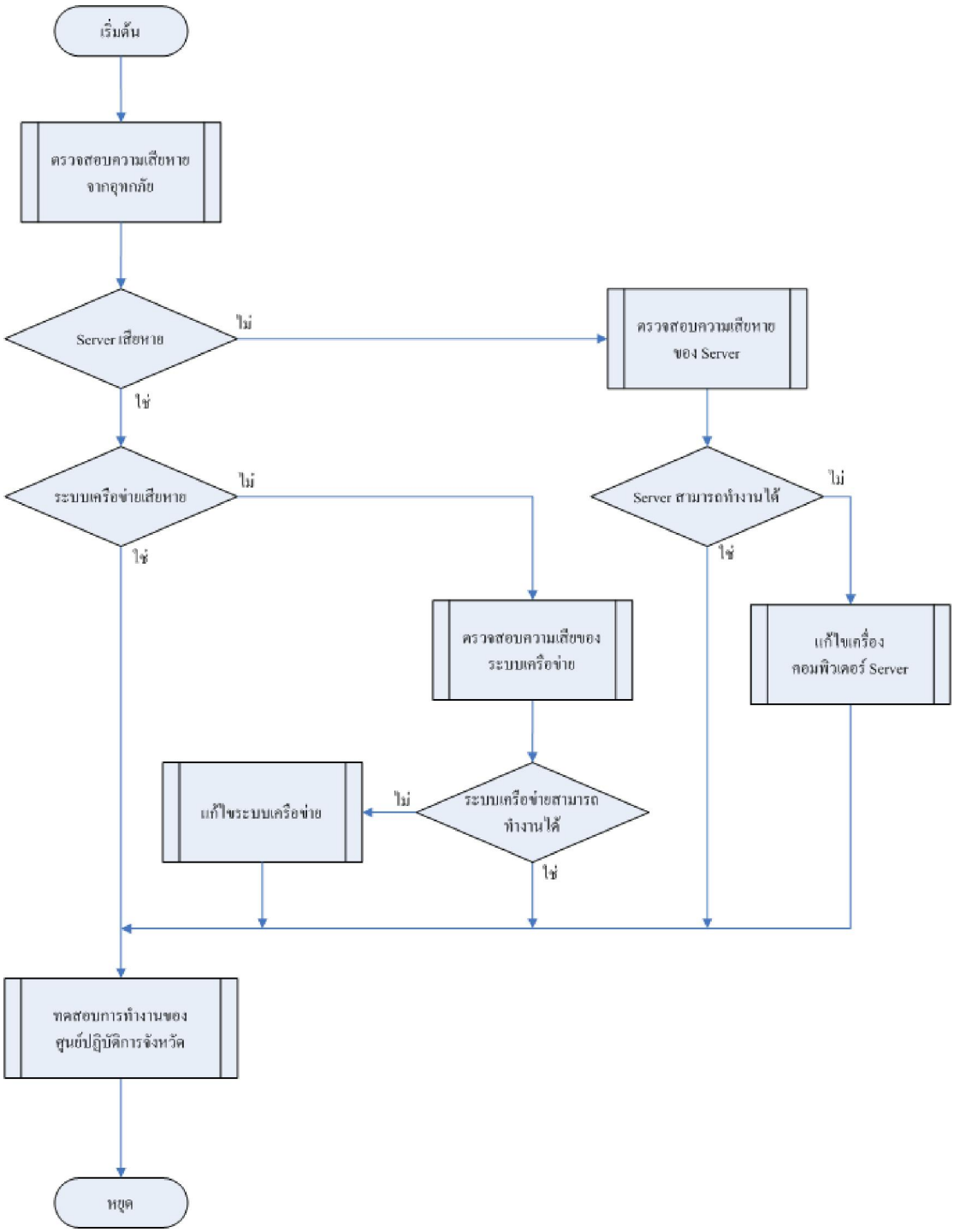
**อุทกภัย**

อุทกภัยหมายถึงภัยพิบัติที่เกิดจากน้ำ ยกตัวอย่างเช่น น้ำท่วม น้ำซึม น้ำสาด ฯ โดยระบบสารสนเทศศูนย์ปฏิบัติการจังหวัดเป็นระบบที่ประกอบไปด้วยอุปกรณ์อิเล็กทรอนิกส์

กรณีความเสี่ยงที่เกิดจากอุทกภัย สำหรับจังหวัดแล้วได้ออกแบบให้มีความสำคัญน้อย เนื่องจากห้องสื่อสารได้ติดตั้งอยู่บนพื้นที่ที่มีลักษณะของภูมิประเทศที่น้ำไม่สามารถท่วมถึงได้ แต่อย่างไรก็ตามทางจังหวัดได้ทำการออกแบบแผนการแก้ไขไว้ในกรณีที่ระบบสารสนเทศและศูนย์ปฏิบัติการจังหวัดเกิดความเสียหายจากละอองน้ำและละอองฝนที่อาจจะเข้ามาทางหน้าต่าง, น้ำที่มาจากการรั่วซึมของหลังคา, การรั่วไหลของน้ำจากห้องน้ำ เป็นต้น

ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

1. ผู้ดูแลระบบทำการตรวจสอบความเสียหายที่เกิดจากอุทกภัย ซึ่งรวมไปถึงเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย
2. ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเกิดการเสียหายขึ้น ผู้ดูแลระบบต้องทำการแก้ไขซ่อมแซมเครื่องคอมพิวเตอร์แม่ข่าย และในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเสียหายจนไม่สามารถทำการแก้ไขซ่อมแซมได้ ผู้ดูแลระบบต้องทำการจัดหาเครื่องคอมพิวเตอร์แม่ข่ายเครื่องใหม่ มาติดตั้งระบบแทน
3. ในกรณีที่ระบบเครือข่ายเกิดความเสียหาย ผู้ดูแลระบบต้องทำการแก้ไข ซ่อมแซมระบบเครือข่าย และในกรณีที่อุปกรณ์ระบบเครือข่ายเสียหายจนไม่สามารถแก้ไข ซ่อมแซมได้ ผู้ดูแลระบบต้องทำการจัดหาอุปกรณ์เครือข่าย มาติดตั้งแทนอุปกรณ์ระบบเครือข่ายเดิม
4. ผู้ดูแลระบบทำการตรวจสอบการทำงานของศูนย์ปฏิบัติการจังหวัด โดยทำการทดสอบให้ครบทุกคุณสมบัติของศูนย์ปฏิบัติการจังหวัด และทำการทดสอบการทำงานผ่านระบบเครือข่ายทั้งหมด




แสดงแผนการแก้ไขปัญหากรณีอุทกภัย

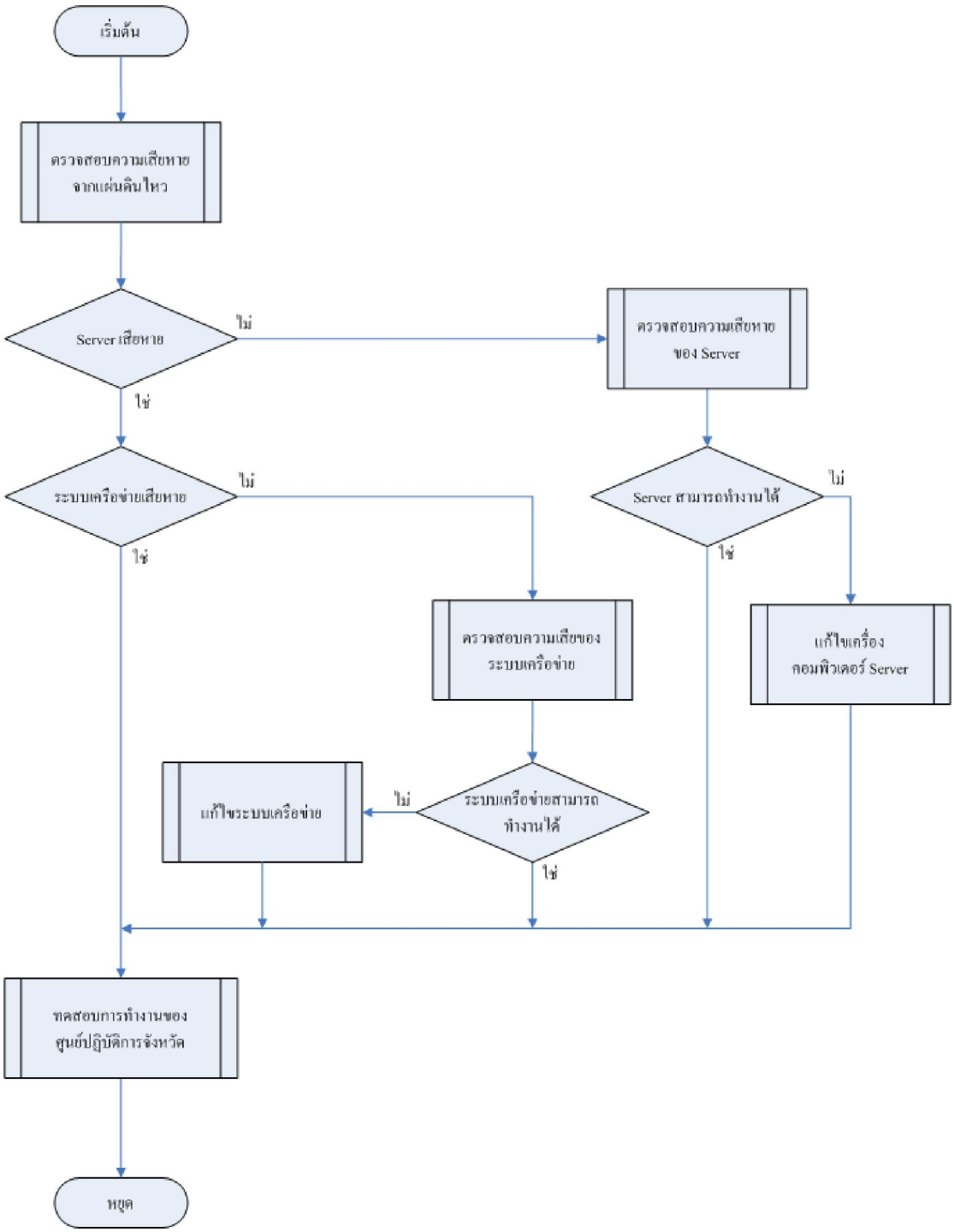
**แผ่นดินไหวและตึกถล่ม**

จังหวัดเป็นจังหวัดที่มีลักษณะเป็นเกาะ ดังนั้นการที่จะเกิดแผ่นดินไหวนั้นจึงเป็นไปได้สูง ซึ่งมีผลกระทบกับการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายโดยตรง ซึ่งอุปกรณ์ที่มีผลกระทบมากที่สุดก็คืออุปกรณ์ที่มีชื่อว่า ฮาร์ดดิสก์ไดร์ฟ (อุปกรณ์สำหรับบันทึกข้อมูล) ซึ่ง ฮาร์ดดิสก์ไดร์ฟ จะมีการทำงานอยู่ตลอดเวลาถึงแม้ว่าจะไม่มีการเรียกดูข้อมูลอยู่ก็ตาม โดยลักษณะของการทำงานคือ แผ่นจานแม่เหล็กสำหรับบันทึกข้อมูลนั้นจะหมุนเป็นรูปวงกลม และมีหัวเข็มที่ใช้สำหรับอ่านข้อมูลถูกติดตั้งห่างจากแผ่นจานแม่เหล็กเพียงไม่กี่ไมโครเมตรเท่านั้น ซึ่งหากเกิดแรงสั่นสะเทือนถึงขั้นที่หัวเข็มกระแทกกับแผ่นจานแม่เหล็ก จะทำให้ศูนย์ปฏิบัติการจังหวัดล้มเหลวในการทำงานทันทีและจะไม่สามารถเรียกใช้งานข้อมูล, ฐานข้อมูล ที่มีอยู่ได้อีกเลย

การออกแบบแผนการแก้ไขกรณีความเสี่ยงที่เกิดจากแรงกระแทก ได้ออกแบบให้มีการตรวจสอบความรุนแรงของแรงกระแทกจนเป็นเหตุให้เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้เลยหรือไม่ หากเครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถทำงานได้แล้ว เจ้าหน้าที่ผู้ดูแลระบบสารสนเทศจะต้องทำการติดตั้งระบบใหม่ทั้งหมด

ลำดับขั้นของการแก้ไขกรณีความเสี่ยง

1. ผู้ดูแลระบบทำการตรวจสอบความเสียหายที่เกิดจากแผ่นดินไหวและตึกถล่ม ซึ่งรวมไปถึงเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย
2. ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเกิดการเสียหายขึ้น ผู้ดูแลระบบต้องทำการแก้ไขซ่อมแซมเครื่องคอมพิวเตอร์แม่ข่าย และในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายเสียหายจนไม่สามารถทำการแก้ไขซ่อมแซมได้ ผู้ดูแลระบบต้องทำการจัดหาเครื่องคอมพิวเตอร์แม่ข่ายเครื่องใหม่ มาติดตั้งระบบแทน
3. ในกรณีที่ระบบเครือข่ายเกิดความเสียหาย ผู้ดูแลระบบต้องทำการแก้ไข ซ่อมแซมระบบเครือข่าย และในกรณีที่อุปกรณ์ระบบเครือข่ายเสียหายจนไม่สามารถแก้ไข ซ่อมแซมได้ ผู้ดูแลระบบต้องทำการจัดหาอุปกรณ์เครือข่าย มาติดตั้งแทนอุปกรณ์ระบบเครือข่ายเดิม
4. ผู้ดูแลระบบทำการตรวจสอบการทำงานของศูนย์ปฏิบัติการจังหวัด โดยทำการทดสอบให้ครบทุกคุณสมบัติของศูนย์ปฏิบัติการจังหวัด และทำการทดสอบการทำงานผ่านระบบเครือข่ายทั้งหมด




แสดงแผนการแก้ไขปัญหากรณีแผ่นดินไหวและตึกถล่ม