แผนสำรองฉุกเฉินระบบเทคโนโลยีสารสนเทศ

(Information Technology Contingency Plan)

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

ฉบับ พ.ศ. 2556

คำนำ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่มีความสำคัญยิ่งต่อการให้บริการ การบริหารระบบราชการ และการเรียนการสอนการวิจัย จำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา ดังนั้น เพื่อลดความเสี่ยงต่าง ๆ อันอาจจะเกิดขึ้นกับระบบสารสนเทศจึงได้จัดทำแผนสำรองฉุกเฉินระบบเทคโนโลยีสารสนเทศ (Information Technology Contingency Plan) เพื่อเป็นกรอบแนวทางในการบำรุงรักษาและป้องกันแก้ไขปัญหาอันอาจส่งผลกระทบต่อข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ โปรแกรมระบบฐานข้อมูล ระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

เรื่อง **หน้า**

ภาคผนวก

แผนสำรองฉุกเฉินระบบเทคโนโลยีสารสนเทศ

(IT Contingency Plan)

1. <u>หลักการและเหตุผล</u>

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงาน และเพื่อให้บริการได้รับความสะดวก ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการดำเนินงานของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก เพื่อป้องกันและแก้ไขปัญหาดังกล่าว สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้เล็งเห็นความจำเป็นที่จะต้องมีแผนสำรองฉุกเฉินระบบเทคโนโลยีสารสนเทศ

2. <u>วัตถุประสงค์</u>

2.1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

2.3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

2.4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

3. <u>การประเมินสถานการณ์ความเสี่ยง</u>

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

3.1. เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่

สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนา ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด

3.2. เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) และการบุกรุก สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

1. ติดตั้ง firewall, IDS ทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องให้บริการ (server) และเครื่องลูกข่าย (client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย
2. ติดตั้งอุปกรณ์ป้องกันไวรัสบนเครือข่าย (Network Virus Wall) เพื่อตรวจจับและแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่าย internet รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

3.3. เกิดจากระบบไฟฟ้าขัดข้อง, ฟ้าผ่า หรือความเสียหายจากเพลิงไหม้ โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) และเครื่องกำเหนิดไฟฟ้า (Generator) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ตลอดเวลา ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุม ป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีระบบดับเพลิงอัตโนมัติที่ไม่เป็นอันตรายต่อมนุษย์และอุปกรณ์ สามารถทำงานได้ทั้งอัตโนมัติและแบบบังคับด้วยมือ พร้อมกันนี้ยังมีระบบแจ้งการทำงานและแจ้งเตือนภัยต่างๆ รวมถึงอุทกภัยและการทดสอบการทำงานของระบบทุกสัปดาห์ผ่านเครือข่ายโทรศัพท์มือถือ

3.4. เกิดจากโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์ ในส่วนของห้องคอมพิวเตอร์แม่ข่าย ได้กำหนด ห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ติดตั้งเครื่องอ่านบัตรแบบแม่เหล็กเพื่อป้องกันไม่ให้บุคคลภายนอกเข้ามาในหน่วยงานโดยไม่ได้รับอนุญาต และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

3.5. อุณหภูมิและความชื้นที่ไม่เหมาะสมจะทำให้อุปกรณ์ทำงานผิดปกติหรืออาจจะเกิดความเสียหาย ได้มีการติดตั้งเครื่องปรับอากาศและควบคุมความชื้นที่สามารถทำงานได้ตลอดเวลา สามารถแจ้งความผิดปกติในการทำงานผ่านเครือข่ายโทรศัพท์มือถือ

4. <u>การเตรียมการเบื้องต้น</u>

4.1. การสำรองข้อมูล (Back up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีแนวทาง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย เป็นประจำทุกสัปดาห์ โดยสำรองข้อมูลไว้ในเทปบันทึกข้อมูล ตัวอย่างขั้นตอนการ backup แสดงในภาคผนวก ก.

4.2. การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟแวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ โดยมีวิธีการดังนี้

1. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

ก ติดตั้งโปรแกรมป้องกันไวรัส

ข อัพเดตข้อมูลไวรัส

ค ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ

ง ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

2. ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น แผ่นดิสก์ แผ่นซีดี เป็นต้น

ก สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

ข ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย เช่น .pif

ค ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

3. ใช้ความระมัดระวังในการเปิด E-mail

ก อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

ข ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

4. ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

ก ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น ICQ MSN

ข ไม่ควรเข้าไปเปิด website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา

ค ไม่ ดาวน์โหลด ไฟล์ จาก website ที่ไม่น่าเชื่อถือ

ง ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

จ หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

4.3. การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

1. ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ 20-30 นาที
2. เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
3. เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ
4. มีระบบป้องกันไฟไหม้ ตรวจจับควันและแจ้งผ่านเครือข่ายโทรศัพท์มือถือ

4.4. มีระบบป้องกันไฟไหม้ ตรวจจับควันและแจ้งผ่านเครือข่ายโทรศัพท์มือถือ

4.5. การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

1. มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป ที่ประตูเข้าออก มีการติดตั้งสายูและกุญแจล็อค ในอนาคตคาดว่าจะได้ติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม
2. มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา
3. มีการติดตั้ง Traffic Shaper เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
4. มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

5. การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ จากทุกวิทยาเขต ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (user name) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ความรับผิดชอบ

6. การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัย คุกคามคอมพิวเตอร์ได้เป็นอย่างดี

4.6. การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

1. แผ่นติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
2. เทปสำรองข้อมูลและระบบงานที่สำคัญ
3. แผ่นโปรแกรม antivirus/spyware
4. แผ่น driver อุปกรณ์ต่างๆ
5. ระบบสำรองไฟฉุกเฉิน
6. อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

5. <u>การกำหนดผู้รับผิดชอบ</u>

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

5.1. ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

1. หัวหน้าหน่วยงาน ที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ(CIO)
2. ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

5.2. ระดับปฏิบัติ

1. นายสกุลชาย สารมาศ รองผู้อำนวยการฝ่ายสารสนเทศ

รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวนวางแผน ติดตามการบริหารความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศมทร.ตะวันออก

2. นายสถาพร ทรัพย์วิบูลพงษ์ หัวหน้างานเครือข่าย

รับผิดชอบ

ก ดูแลบำรุงรักษา ระบบเครื่อง ระบบเครือข่าย และระบบความปลอดภัยทั้งหมด เครื่อง โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบคอมพิวเตอร์และระบบเครือข่าย

ข รักษาความปลอดภัยของระบบฐานข้อมูล รวมทั้งการทำสำเนาฐานข้อมูล

6. <u>มาตรการความปลอดภัยด้วยรหัสผ่าน</u>

มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศ ไม่สามารถเข้าถึง แก้ไข เปลี่ยนแปลง ข้อมูล หรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง โดย

6.1. กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้าในระบบได้ตามความรับผิดชอบ (Access) โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละระดับฐานข้อมูล ดังนี้

1. บุคคลที่สามารถเรียกดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถแก้ไข ปรับปรุงข้อมูลได้

2. บุคคลที่สามารถเรียกดูข้อมูลและแก้ไข ปรับปรุงข้อมูลในส่วนที่ผู้ใช้รับผิดชอบต่อความถูกต้องของข้อมูลในฐานข้อมูลนั้น

3. บุคคลที่สามารถเรียกดู แก้ไข ปรับปรุงข้อมูลระดับฐานข้อมูล ในกรณีที่ผู้ใช้มีข้อผิดพลาดในการปรับปรุงข้อมูล ผู้รับผิดชอบของหน่วยงานเจ้าของหน่วยงานเป็นผู้ดูแล แก้ไข ข้อมูลในส่วนนี้ซึ่งการเข้าใช้ฐานข้อมูล ในแต่ละระบบ จะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูล ตามหน้าที่ความรับผิดชอบของผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูล โดยมีการกำหนด Log in และ Password ในการเข้าถึงข้อมูลและผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงและเปลี่ยนแปลงแก้ไขข้อมูลได้ ผู้ใช้ระบบทั่วไปที่ผู้บังคับบัญชาที่เป็นหน่วยงานเจ้าของระบบ เป็นผู้อนุมัติให้ดำเนินการได้ โดยจะแบ่งเป็นการดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถเปลี่ยนแปลงแก้ไขได้ และการที่สามารถปรับปรุงข้อมูลได้ ทั้งนี้ เพื่อเป็นการรักษาความปลอดภัยของฐานข้อมูล

6.2. กำหนดระยะเวลาการใช้งานระบบสารสนเทศ ของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้

6.3. การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า 6 ตัวอักษร และควรใช้ ตัวเลข อักขระพิเศษประกอบ และสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็น

ความลับ ทั้งนี้ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

7. **<u>ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ</u>**

7.1. กรณีเครื่องลูกข่าย

1. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่ศูนย์ทราบ หรือกรณีมีเหตุอันทำให้ฝ่ายเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ฝ่ายเทคโนโลยีสารสนเทศ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ
2. กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย(สาย LAN) ออกจากเครื่องนั้นโดยเร็ว
3. ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

7.2. กรณีเครื่องบริการ (server) และอุปกรณ์เครือข่าย

1. **ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ**
2. **ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า**
3. **ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้กดปุ่มเพื่อใช้งานระบบดับเพลิงเพลิงโดยเร็วและออกจากบริเวณและปิดประตูเพื่อให้การดับไฟมีผลมากที่สุด**
4. **รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย**
5. **ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด**
6. **ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด**
7. **ผู้ดูแลระบบ ต้องรีบรายงานบังคับบัญชาตามลำดับชั้นจนถึงผู้บริหาร ทราบโดยเร็ว**

7.3. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

1. **ติดตั้งโปรแกรม Anti-virus และอัพเดทข้อมูลไวรัสใหม่ๆ**

2. ใช้งานโปรแกรม Anti-virus

7.4. กรณีเมนบอร์ดหรือฮาร์ดดิสก์

1. กรณีเมนบอร์ดเสียหาย

ก ทำการจัดหา เมนบอร์ด Main board หรือ Mather board มาเปลี่ยน(อาจใช้วิธีการพิเศษในการจัดหามาก่อนแล้วจัดซื้อตามที่หลัง)จากนั้นถอด เมนบอร์ดเดิมที่ชำรุดออกแล้วติดตั้งเมนบอร์ดใหม่แทน แล้วทำการบูตระบบใช้งานตามปกติ

2. กรณีฮาร์ดดิสค์เสียหาย

ก จัดหาฮาร์ดดิสค์มาเปลี่ยน

ข ติดตั้งระบบปฏิบัติการ และระบบเครือข่าย

ค นำ BACKUP ที่ได้จัดทำไว้จาก มาทำ RECOVER เพื่อนำข้อมูลเดิมกลับมาใช้เหมือนเดิม

ง ทำการรันเครื่องทำงานตามเดิม

8. <u>แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม</u>

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติ ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

8.1. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

8.2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

8.3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

8.4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

8.5. นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยใช้ทีมกู้ระบบ (ผู้ดูแลระบบ และทีมงานจากบริษัทฯ ที่จัดจ้างบำรุงรักษาระบบสารสนเทศ) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

8.6. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆที่เกี่ยวข้อง