คู่มือรองรับภาวะฉุกเฉิน กรณีระบบสารสนเทศล่ม

กลุ่มสารนิเทศ

สำนักงานคณะกรรมการการอุดมศึกษา

หน่วยงาน	สำนักงานคณะกรรมการการอุดมศึกษา
หน่วยงานที่เกี่ยวข้อง	สำนัก/หน่วยงาน ที่สังกัดสำนักงานคณะกรรมการการอุดมศึกษา และมีที่ตั้งอยู่ในอาคารสำนักงานคณะกรรมการการอุดมศึกษา
ผู้จัดทำ	กลุ่มสารนิเทศ สำนักอำนวยการ

คำนำ

ในปัจจุบัน การปฏิบัติงานโดยอาศัยเทคโนโลยีสารสนเทศและการสื่อสารเป็นสิ่งที่มีความจำเป็นเพิ่มมากขึ้นอย่างต่อเนื่องจนกลายเป็นส่วนหนึ่งของการปฏิบัติงานทั่วไปของทุกองค์กร ทั้งในองค์กรที่เป็นหน่วยงานราชการและองค์กรเอกชนพร้อมๆ กับการใช้เทคโนโลยีสารสนเทศและการสื่อสารที่เพิ่มมากขึ้น การพัฒนาเทคโนโลยีสารสนเทศก็มีความรุดหน้าเป็นเงาตามตัว การพัฒนาดังกล่าวก่อให้เกิดความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศอันมีค่ายิ่งต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากรในหน่วยงานนั้นๆ ข้อมูลสารสนเทศที่มีจำนวนเพิ่มมากขึ้นอันเป็นผลจากเทคโนโลยีสารสนเทศก็ได้พัฒนาทั้งในด้านปริมาณและคุณภาพ ทำให้การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศได้รับความยอมรับในความสำคัญเพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

สำนักงานคณะกรรมการการอุดมศึกษา ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่าง ๆ จึงได้จัดทำคู่มือรองรับภาวะฉุกเฉิน กรณีระบบสารสนเทศล่มเพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร

กลุ่มสารนิเทศ
สำนักอำนวยการ

สารบัญ

คู่มือรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร

หลักการและเหตุผล

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อองค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ กลุ่มสารนิเทศ ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยเสี่ยงต่างๆ ทั้งจากภายนอกและภายในมากระทบทำให้ระบบฐานข้อมูล และสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้โดยเฉพาะอย่างยิ่งฐานข้อมูลและสารสนเทศที่ใช้ในการบริหารจัดการ กลุ่มสารนิเทศจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ และการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและสารสนเทศขององค์กร

วัตถุประสงค์

1. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศขององค์กร
2. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ เพื่อให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
4. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ที่อาจเกิดขึ้นได้อย่างทันท่วงที
5. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของ สำนักงานคณะกรรมการการอุดมศึกษา สามารถจำแนกได้เป็นสองกลุ่มหลัก ๆ ได้แก่

<u>ภัยพิบัติจากภายนอก</u>

ภัยพิบัติจากภายนอกที่อาจเกิดขึ้น ได้แก่

(ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องแม่ข่าย และระบบเครือข่าย เช่น แผ่นดินไหว อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แมลงกัดแทะ ฯลฯ

(ข) การโจรกรรมอุปกรณ์ระบบเครือข่าย หรือคอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

(ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

(ง) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

(จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

(ฉ) โปรแกรมที่ไม่พึงประสงค์ต่างๆ เช่น ไวรัสคอมพิวเตอร์ Spam Malware เป็นต้น

<u>ภัยพิบัติจากภายใน</u>

ภัยพิบัติจากภายในที่อาจเกิดขึ้น ได้แก่

(ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

(ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

(ค) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

(ง) อุปกรณ์ต่างๆ มีการชำรุดหรือเสื่อมไปตามสภาพการใช้งานตามปกติ หรือเร็วกว่าปกติ

แนวทางการจัดการภัยพิบัติ

<u>ภัยพิบัติจากภายนอก</u>

(ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้ง ของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แมลงกัดแทะ ฯลฯ

<u>การป้องกันอัคคีภัย</u>

<u>การดำเนินการ</u>

1. กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ
2. อบรมขั้นต้นสำหรับพนักงานทุกคนในแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิงการหนีไฟ
3. ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเลคทรอนิคส์สำหรับห้องคอมพิวเตอร์แม่ข่าย
4. จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์แม่ข่าย เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

<u>การป้องกันอุทกภัย และการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม</u>

เนื่องจากที่ทำการอยู่บนอาคารสูงปัญหาจากอุทกภัยจึงไม่มี แต่เนื่องจากเครื่องปรับอากาศมีความชื้นสูง จึงมีความเสี่ยงต่อการอายุการใช้งานของอุปกรณ์คอมพิวเตอร์แม่ข่าย

<u>การดำเนินการ</u>

1. การเปิดเครื่องปรับอากาศ ตลอด 24 ชั่วโมง
2. ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

(ข) การโจรกรรมอุปกรณ์ระบบเครือข่าย หรือคอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

<u>การดำเนินการ</u>

1. ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของกลุ่มสารนิเทศ เป็นผู้รับผิดชอบนำพาเข้าไป
2. จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย โดยมีระบบยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ
3. ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

(ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง สำนักงานคณะกรรมการการอุดมศึกษามีเส้นทางออกสู่อินเตอร์เน็ตผ่านสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)

การดำเนินการ

1. การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ทุกวัน

(ง) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

การดำเนินการ

1. แยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายเมนหลัก

2. ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ 20-30 นาที

3. เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอตรวจสอบระบบสำรองไฟฟ้า(UPS) ทุกวันศุกร์

4. เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ

(จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

การดำเนินการ

1. สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยการใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

2. ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

3. ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กร และกลั่นกรองข้อมูลที่มาทาง Website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

4. จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

5. ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่ใช้บริการทั้งหมด

6. กำหนดรหัสผ่านไม่น้อยกว่า 8 ตัวอักษร ไม่ใช่คำที่ก่อให้เกิดการคาดเดาได้ง่าย ไม่ใช่รหัสผ่านเดียวกันทุกระบบ และมีการเปลี่ยนรหัสผ่านทุก 3 เดือน

7. ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ D-DOS

(ฉ) ไวรัสคอมพิวเตอร์

การดำเนินการ

1. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
   - ติดตั้งโปรแกรมป้องกันไวรัส
   - อัพเดตข้อมูลไวรัส
   - ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่างๆ
   - ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง
2. ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น แผ่นดิสก์ แผ่นซีดี เป็นต้น
   - สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
   - ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย เช่น .pif เป็นต้น
   - ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา
3. ใช้ความระมัดระวังในการเปิด E-mail
   - อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
   - ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา
4. ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet
   - ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น ICQ MSN เป็นต้น
   - ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา
   - ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่น่าเชื่อถือ
   - ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
   - หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

ภัยพิบัติจากภายใน

(ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

การดำเนินการ

1. ทำการสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้ในจานแม่เหล็ก 1 ชุดในเวลาเที่ยงคืนของทุกวันศุกร์

2. การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรองข้อมูลตามระยะเวลาที่กำหนดเป็นประจำเดือน โดยจะทำการสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในแผ่นซีดีรอมทุกวันศุกร์แรกของทุกเดือน

3. ทำการทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้ทำการสำรองไว้ในแผ่นซีดีรอม

4. ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

5. ข้อมูลที่ต้องทำการ Recovery ทันที ได้แก่ โปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์องค์กร (Web Application Programming) และข้อมูลระบบงานสารบรรณอิเล็กทรอนิกส์

6. จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลจานแม่เหล็กของเครื่องแม่ข่าย เพื่อลดความเสียหายของข้อมูล

(ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

การดำเนินการ

1. ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้
2. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ
3. ไตร่ตรองให้รอบคอบก่อนที่จะขอข้อมูลของผู้อื่นโดยผ่านอุปกรณ์ Thumb Drive
4. หลีกเลี่ยงการใช้แชร์ไฟล์โดยไม่จำเป็น

(ค) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

การดำเนินการ

1. ให้ความรู้แก่บุคลากรและหน่วยงาน

2. ใส่กุญแจตู้ชุมสาย (Hub) และตู้สวิทช์ (Switches) เพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่หรือบุคลการที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

1. การสำรองข้อมูล (Back Up)

(1) การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้ในจานแม่เหล็ก ๑ ชุดในเวลาเที่ยงคืนของทุกวันศุกร์

(2) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรองข้อมูลตามระยะเวลาที่กำหนดเป็นประจำทุกเดือน โดยจะทำการสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในแผ่นซีดีรอม

2. การกู้ข้อมูล (Recovery)

(1) มีหนังสือแจ้งเตือนการกระทำอันควรจะกระทำให้ระบบเครือข่ายภายในล่มไปยังสำนัก/ หน่วยงาน ภายในองค์กรเพื่อกำกับการดำเนินการดังกล่าว

- ทำการทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้ทำการสำรองไว้ในแผ่นซีดีรอม ทุกวันศุกร์ของสัปดาห์

- ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

(2) ข้อมูลที่ต้องทำการ Recovery ทันทีได้แก่ โปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์องค์กร (Web Application Programming) และข้อมูลระบบงานสารบรรณอิเล็กทรอนิกส์

3. การป้องกันไวรัส

(1) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

(2) มีการตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูล นอกจากนี้ควรมีการตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

(3) ใช้ความระมัดระวังในการเปิด e-mail ที่ไม่ทราบแหล่งที่มา

(4) ระมัดระวังในการดาวน์โหลดไฟล์ต่างๆ จากอินเตอร์เน็ต

(5) หลีกเลี่ยงการใช้แชร์ไฟล์โดยไม่จำเป็น

4. ระบบไฟฟ้า

(1) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล

(2) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(3) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ ที่กำลังใช้งานอยู่

5. อุปกรณ์อื่นๆ ที่เกี่ยวข้อง

(1) อุปกรณ์บันทึกข้อมูล และอุปกรณ์ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและห้องสำรองข้อมูล

(2) เครื่อง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

(3) อุปกรณ์ดับเพลิงด้วยสารเคมี สำหรับอุปกรณ์ IT ติดตั้งอยู่ที่กลุ่มสารนิเทศ ชั้น 2 สำนักงานคณะกรรมการการอุดมศึกษา สำหรับกรณีเกิดไฟไหม้ในอาคาร

(4) คอมพิวเตอร์ที่ใช้บันทึกข้อมูลผู้ใช้งานอินเตอร์เน็ต

(5) โปรแกรมตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูล ความถี่ และการเรียกใช้บนเครือข่าย เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

(6) มีอุปกรณ์คอมพิวเตอร์ที่แสดงความเคลื่อนไหวของระบบงานต่างๆ หากเกิดปัญหาจะสามารถแก้ไขได้ทันที

มาตรการความปลอดภัยด้วยรหัสผ่าน

การสร้างความปลอดภัยให้กับระบบสารสนเทศ มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศ ไม่สามารถเข้าถึง แก้ไข เปลี่ยนแปลง ข้อมูล หรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิได้อำนาจหน้าที่เกี่ยวข้อง โดย

1. กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้าในระบบได้ตามความรับผิดชอบ โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละดับ ดังนี้

(1) ผู้ดูแลระบบเครือข่าย หรือผู้ดูแลเครื่องแม่ข่ายจะต้องเป็นผู้ควบคุมรหัสผู้ใช้งานทั้งหมดโดยกำหนดรหัสผู้ใช้งานให้แก่บุคคลที่รับผิดชอบโดยตรงในแต่ละงานให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบเครือข่าย

(2) การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ FTP Server จะต้องระบุถึง IP Address ของผู้ใช้งาน และแฟ้มข้อมูลที่ต้องการเข้าถึง

(3) การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ Database Server จะต้องกำหนดแยกเป็นรายฐานข้อมูลที่ต้องการใช้งานและเข้าถึง

2. กำหนดระยะเวลาการใช้งานระบบสารสนเทศของผู้ใช้ระบบ โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้

3. การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และควรใช้ตัวเลข อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

1. กรณีเครื่องลูกข่าย

(1) ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศรับทราบ หรือกรณีมีเหตุอันทำให้ศูนย์เทคโนโลยีสารสนเทศ ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

(2) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องนั้นโดยเร็ว

(3) ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ดึงสายแลนออกจากจุดชุมสายในชั้นนั้นออกให้หมด

(4) ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ แจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้อำนวยการรับทราบโดยเร็วที่สุด

2 กรณีเครื่องแม่ขายและอุปกรณ์เครือข่าย

(1) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

(2) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

(3) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

(4) รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

(5) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

(6) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

(7) ผู้ดูแลระบบ ต้องรีบแจ้งให้หัวหน้าหรือผู้อำนวยการรับทราบโดยเร็ว

3. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

(1) เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์ เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

(2) ทำการสแกนและฆ่าไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัสที่มีอยู่ในเครื่อง

(3) แจ้งเจ้าหน้าที่กลุ่มสารนิเทศ เพื่อตรวจสอบละเอียด

4 หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัย

เพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติของบุคลากรในกลุ่มสารนิเทศ ดังนี้

(1) ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

(2) ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

(3) ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบดูทางออกฉุกเฉินไม่ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉินทั้งสองทางเพื่อให้ไปถึงทางหนีฉุกเฉินได้ถึงแม้ว่าจะดับหรือปกคลุมไปด้วยควัน

(4) เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นหนีจากอาคารแล้วโทรศัพท์แจ้งหน่วยดับเพลิง โทร 199 ทันที หรือแจ้ง 1669

(5) เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

(6) ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันที รีบแจ้งฝ่ายอาคารและสถานที่เพื่อโทรศัพท์แจ้งหน่วยดับเพลิงต่อไป

(7) ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อยๆ ปิดประตู แล้วหนีไปยังทางหนีไฟฉุกเฉินที่อยู่ใกล้ที่สุด

(8) ถ้าเพลิงไหม้อยู่บริเวณใกล้ๆ ประตูจะมีความร้อน ห้ามเปิดประตูเด็ดขาด ให้รีบโทรศัพท์เรียกหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งถูกเพลิงไหม้ หาผ้าเช็ดตัวเปียกๆ ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

(9) เมื่อต้องเผชิญกับควันไฟที่ปกคลุม ให้ใช้วิธีคลานหนีไปทางฉุกเฉิน เพราะอากาศบริสุทธิ์จะอยู่ด้านล่าง (เหนือพื้นห้อง) นำกุญแจห้องทำงานไปด้วยหากหมดหนทางหนีจะได้สามารถกลับเข้าห้องได้

(10) ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

5. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ จะมีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับสูงมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากที่จะหลีกเลี่ยงได้ก็คือผลกระทบต่างๆ ที่เกิดขึ้นจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหาของข้อมูลที่สำคัญ รวมถึงการสูญเสียเวลา จากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ซึ่งประกอบด้วย

(1) ไฟฟ้าตก (Sag หรือ Brown out)

ไฟฟ้าตก คือ สภาวะที่แรงดันไฟฟ้าลดต่ำลงจากปกติในช่วงเวลาสั้นๆ ซึ่งเป็นปัญหาทางไฟฟ้าที่พบบ่อยที่สุด

สาเหตุ เกิดจากการเปิดสวิตซ์อุปกรณ์บางชนิดที่ต้องการใช้กระแสไฟฟ้ามาก เช่น เครื่องปรับอากาศ ลิฟต์ และเครื่องมือเครื่องจักร เป็นต้น อุปกรณ์เหล่านี้ต้องการกระแสไฟฟ้ามากในการติดเครื่อง เมื่อเทียบกับการทำงานในภาวะปกติ ส่งผลให้แรงดันไฟฟ้าในสายส่งการไฟฟ้าฯ ลดต่ำลง

(2) ไฟฟ้าดับ (Black out)

ไฟฟ้าดับ คือ สภาวะที่กระแสไฟฟ้าหยุดไหล

สาเหตุ เกิดจากความต้องการกระแสไฟฟ้าจากสายส่งการไฟฟ้าฯ ที่มากเกินไป เกิดไฟฟ้าลัดวงจรในสายส่ง พายุฟ้าคะนอง แผ่นดินไหว และปัญหาที่เกิดกับสายส่งไฟฟ้าฯ เช่น เสาไฟฟ้าล้ม หรือหม้อแปลงระเบิด ฯลฯ ซึ่งส่งผลให้ไม่สามารถจ่ายไฟจากการไฟฟ้าได้ผลกระทบ การทำงานของ RAM หยุดชะงักทันที ทำให้ข้อมูลปัจจุบันสูญหายได้ รวมถึง การบันทึกข้อมูลของตารางการจัดการแฟ้ม (FAT) สูญหายได้ มีผลให้ข้อมูลที่เก็บไว้ทั้งหมดสูญหายได้

(3) ไฟฟ้ากระชาก (Spike)

ไฟฟ้ากระชาก คือ สภาวะที่แรงดันไฟฟ้าเพิ่มสูงขึ้นอย่างกะทันหัน โดยสามารถเข้าไปยังอุปกรณ์ไฟฟ้าได้ทั้งจากสายส่งการไฟฟ้าฯ เครือข่ายสื่อสาร และสายโทรศัพท์

สาเหตุ เกิดจากฟ้าผ่าในบริเวณใกล้เคียง หรืออาจเกิดจากสายส่งการไฟฟ้าฯ ที่หยุดการทำงานไปและกลับมาทำงานใหม่อย่างกะทันหัน

ผลกระทบ สร้างความเสียหายหรือทำลายชิ้นส่วนอุปกรณ์อิเล็กทรอนิกส์ของอุปกรณ์ไฟฟ้าได้รวมถึงข้อมูลเกิดการสูญหาย

(4) ไฟฟ้าเกิน (Surge)

ไฟฟ้าเกิน คือ สภาวะที่มีแรงดันไฟฟ้าไหลมามากเกินในช่วงเวลาสั้นๆ (1/120 วินาที)

สาเหตุ เกิดจากการใช้อุปกรณ์ไฟฟ้าที่มีมอเตอร์กินไฟมาก เช่น เครื่องปรับอากาศ หรืออุปกรณ์ไฟฟ้าอื่นๆ ที่ลักษณะใกล้เคียงกัน ฯลฯ เนื่องจากอุปกรณ์เหล่านี้เมื่อหยุดทำงานแรงดันไฟฟ้าส่วนหนึ่งที่เหลืออยู่ในมอเตอร์ จะไหลกลับเข้าไปในสายส่งการไฟฟ้าฯ ทำให้เกิดแรงดันไฟฟ้าสูงเกิน

ผลกระทบ ทำให้ชิ้นส่วนอุปกรณ์ภายในเสื่อมสภาพเร็วกว่าปกติหรือเสียหายได้ รวมถึงหน่วยความจำของคอมพิวเตอร์สูญหายและคลาดเคลื่อน Power Supply เสียหาย และการทำงานของระบบสื่อสารผิดพลาด

(5) สัญญาณรบกวน (Noise)

สัญญาณรบกวน คือ สัญญาณรบกวนที่เกิดจากสนามแม่เหล็กไฟฟ้า (EMI) และสัญญาณคลื่นความถี่วิทยุ (RFI) ซึ่ง 2 สัญญาณเหล่านี้จะไปรบกวนสัญญาณคลื่นไซน์ (Sine Wave) ของสายส่งการไฟฟ้าฯ

สาเหตุ เกิดขึ้นได้จากปรากฏการณ์ทางธรรมชาติ (เช่น ฟ้าผ่า) การเปิด-ปิดสวิตช์อุปกรณ์ไฟฟ้า เครื่องส่งวิทยุ เป็นต้น โดยสัญญาณรบกวนอาจเกิดขึ้นเป็นระยะ ๆ หรืออาจเกิดอย่างสม่ำเสมอได้

ผลกระทบ ทำให้การประมวลผลของโปรแกรมและแฟ้มข้อมูลผิดพลาด และเกิดข้อบกพร่องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้มีการป้องกันปัญหาจากกระแสไฟฟ้าดังกล่าวโดยการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptable Power Supply : UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล