แผนป้องกันและดูแลระบบฐานข้อมูลสารสนเทศ ของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์
สำนักงานคณะกรรมการการอาชีวศึกษา

แผนป้องกันและดูแลระบบฐานข้อมูลสารสนเทศ
ของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

1. หลักการและเหตุผล

ระบบข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ แม้ว่า ด้วยการปฏิบัติการจะมีข้อกำหนดที่จัดทำไว้เพื่อเป็นคู่มือปฏิบัติงานของผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้อง แต่ก็ยังมีข้อจำกัดด้านความรู้และทักษะของผู้ดูแลระบบและเจ้าหน้าที่ อุปกรณ์ เครือข่ายการสื่อสาร และระบบไฟฟ้าที่อาจเกิดความขัดข้อง จนเป็นเหตุให้การทำงานหยุดชะงักและเกิดความเสียหาย วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ตระหนักถึงความสำคัญของระบบฐานข้อมูลสารสนเทศ ซึ่งอาจมีทั้งปัจจัยภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลสารสนเทศ รวมทั้งอุปกรณ์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลสารสนเทศที่ใช้ในการบริหารจัดการ ดังนั้น วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ จึงจัดทำแผนป้องกันและดูแลระบบฐานข้อมูลสารสนเทศของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ เพื่อเป็นกรอบแนวทางในการ ดูแลรักษาระบบ และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลสารสนเทศของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

2. วัตถุประสงค์

2.1 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลสารสนเทศของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

2.2 เพื่อเป็นแนวทางในการดูแลรักษาฐานข้อมูลสารสนเทศของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.3 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดปัญหาเกี่ยวกับระบบสารสนเทศวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์

3. วิเคราะห์ปัจจัยความเสี่ยง

ปัจจัยที่อาจเกิดและทำให้เสียหายกับระบบฐานข้อมูลสารสนเทศ ของวิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ ได้แก่

3.1 ปัจจัยภายนอก

(1) ภัยต่าง ๆ ที่กระทำต่ออาคารสถานที่ตั้งของเครื่องแม่ข่าย (Server) ของระบบฐานข้อมูล ได้แก่ อุทกภัย อัคคีภัยเป็นต้น

(2) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บ และรวบรวมข้อมูล

(3) การชำรุดเสียหายของตัวเครื่องแม่ข่าย (Server)

(4) ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ขัดข้อง

(5) ระบบกระแสไฟฟ้าขัดข้อง

3.2 ปัจจัยภายใน ได้แก่

(1) ระบบฐานข้อมูลหลักเสียหายหรือข้อมูลถูกทำลาย

(2) การถูกไวรัสทำลายฐานข้อมูล โปรแกรมการใช้งาน หรือระบบปฏิบัติการต่าง ๆ

(3) การถูกเจาะหรือลักลอบ(Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก(Hacker) โดยไม่ได้รับอนุญาต

4. แผนป้องกันและดูแลระบบฐานข้อมูลสารสนเทศ

จากการวิเคราะห์ปัจจัยความเสี่ยงในรูปแบบต่าง ๆ ที่อาจเกิดขึ้น เพื่อให้การบริหารที่มีการป้องกันและแก้ไข ตลอดจนการจัดการกับระบบข้อมูลสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีที่เกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น จึงเห็นควรดำเนินการดังนี้

4.1 กำหนดมาตรการหรือแนวทางดำเนินการ ดังนี้

1. การตรวจสอบและสรุปสาเหตุเบื้องต้น การสังเกตอาการหรือเหตุอันผิดปกติ มี 2 องค์ประกอบ คือ

1) ทางกายภาพ สภาพอันผิดปกติเช่น กลิ่น อุณหภูมิ ไฟฟ้าดับเสียง อาการสั่น

2) การทำงานของระบบ เช่น ไม่สามารถเข้าระบบงานได้ ระบบไม่ทำงานผิดพลาด มีข้อความแจ้งเหตุอันผิดปกติ

2. การแจ้งเหตุ

1) แจ้งเหตุกรณีเร่งด่วน ประสานแจ้งผู้ที่เกี่ยวข้องโดยตรง เช่น หัวหน้างาน ผู้ช่วยหัวหน้างาน หรือเจ้าหน้าที่งานศูนย์ข้อมูลสารสนเทศ วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ หรือเจ้าหน้าที่ที่เข้าเวรรักษาการ เป็นต้น

2) แจ้งเหตุกรณีปกติ สรุปสาเหตุและจัดทำรายงานแจ้งไปยัง ผู้ที่เกี่ยวข้อง เจ้าหน้าที่ผู้รับผิดชอบ และรายงานผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

3) การประเมินสถานการณ์ โดยการแจ้งผู้รับผิดชอบหรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ

4) แนวทางการปฏิบัติ

กรณีเครื่องคอมพิวเตอร์แม่ข่าย ไม่สามารถให้บริการได้ เนื่องจากเกิดภัยพิบัติจากสาเหตุต่อไปนี้

1) เครื่องแม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี
2) ตัวเครื่องแม่ข่ายเกิดปัญหาไม่สามารถให้บริการได้ สาเหตุอาจมาจากจานบันทึกข้อมูล (Hard Disk) เสียหาย อุปกรณ์จ่ายไฟเสีย ฯลฯ
3) เกิดไฟไหม้ตัวเครื่องแม่ข่าย หรือภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย
4) เครื่องแม่ข่ายถูกโจรกรรม

5) ข้อมูลสูญหาย

6) การเชื่อมโยงเครือข่ายล้มเหลว

แนวทางหรือกระบวนการแก้ไขปัญหา ควรพิจารณาและดำเนินการ ดังนี้

1. การเตรียมการเบื้องต้น

1.1 การสำรองข้อมูล (Back up) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นให้ทำการสำรองข้อมูลไว้ใน External Harddisk Flash drive DVD CD หรือติดตั้งระบบการ back up อื่น ๆ

1.2 การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟแวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายโดยผู้ใช้งานจำเป็นต้องระมัดระวังการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะการเชื่อมต่ออินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้โดยมีวิธีการ ดังนี้

(1) ติดตั้งโปรแกรมป้องกันไวรัสและมีการ Update อยู่เสมอ

(2) ระวังภัยจากการเปิดไฟล์บันทึกข้อมูลต่าง ๆ เช่น External Harddisk Handy drive USB Flash Drive ควรมีการสแกนก่อนเปิดใช้งานทุกครั้ง ไม่เปิดไฟล์ที่มีนามสกุลแปลก ๆ

(3) ใช้ความระมัดระวังในการเปิด e-mail เช่น อย่าเปิดไฟล์ที่ไม่ทราบแหล่งที่มาหรือถ้าไม่ทราบแหล่งที่มาควรลบทิ้งทันที

(4) ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จาก Internet เช่น ไม่ควรเปิดไฟล์ที่ไม่รู้จักซึ่งแนบมากับโปรแกรมสนทนาต่าง ๆ เช่น MSN ICQ ไม่ DownLoad ไฟล์จาก Website ที่ไม่น่าเชื่อถือ หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

1.3 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

(1) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะเวลาการสำรองไฟได้ประมาณ 20 - 30 นาที

(2) เปิดเครื่องสำรองไฟตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟให้อยู่ในสภาพพร้อมใช้งานได้ตลอดเวลา

(3) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

1.4 การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(1) มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกัน

(2) ความเสียหาย โดยห้ามบุคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหากไม่มีความจำเป็น มีการติดสายยูและกุญแจล็อค

(3) มีการติดตั้งFirewall เพื่อป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่เครือข่ายสารสนเทศ และเครือข่ายคอมพิวเตอร์ของจังหวัดเพชรบูรณ์ โดยให้ Firewall มีการทำงานตลอดเวลา

1.5 การจัดเตรียมอุปกรณ์ที่จำเป็นในการเตรียมความพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเครื่องคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ ดังนี้

(1) แผ่น boot disk

(2) แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานต่าง ๆ

(3) แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

(4) แผ่นโปรแกรม antivirus/ spyware

(5) แผ่น driver อุปกรณ์ต่างๆ

(6) ระบบสำรองไฟฉุกเฉิน

(7) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

2. หลักการปฏิบัติ

2.1 เป้าหมายการปฏิบัติ

1. ส่วนราชการ/หน่วยงานที่เกี่ยวข้องสามารถสนับสนุนและประสานการปฏิบัติด้านข้อมูลสารสนเทศอย่างเป็นระบบและรวดเร็ว

2. สามารถป้องกันละลดความเสียหายที่อาจเกิดขึ้น ทั้งที่เป็นผลที่เกิดจากเหตุการณ์ภัยพิบัติโดยตรงและผลกระทบที่จะตามมาได้อย่างทันท่วงที

2.2 หลักการปฏิบัติ

1) ความรวดเร็วในการแก้ปัญหาการประเมินสถานการณ์ในกรณีที่เกิดเหตุภัยพิบัติในเขตพื้นที่รับผิดชอบ ให้พิจารณาเหตุการณ์ว่าเป็นภัยพิบัติประเภทใดและรายงานให้ฝ่ายบริหารทราบทันที

2) ในกรณีที่ปรากฏว่า ภัยที่เกิดขึ้นเป็นภัยที่เกิดจากระบบเทคโนโลยีให้ถือว่าการรักษาระบบข้อมูลสารสนเทศเพื่อการบริหารเป็นสิ่งสำคัญที่สุดและหากจำเป็นให้ทำการย้ายวัสดุอุปกรณ์และระบบข้อมูลสารสนเทศออกจากบริเวณเกิดภัย

3) ความสม่ำเสมอในการตรวจสอบระบบ โดยใช้โปรแกรม Anti Virus และ Firewall

4) ต้องใช้วัสดุอุปกรณ์ที่ได้มาตรฐานและกำหนดมาตรฐานในการควบคุม ดูแลในกรณีที่มีการเก็บรักษาข้อมูลสารสนเทศที่อาจก่อให้เกิดผลกระทบต่อการดำเนินงานด้านข้อมูลสารสนเทศ

ขั้นตอนการปฏิบัติ (ก่อนเกิดภัย ขณะเกิดภัยและการฟื้นฟูบูรณะ)

1. การเตรียมการก่อนเกิดภัย

1) จัดทำให้มีการฝึกอบรมให้ความรู้แก่เจ้าหน้าที่ให้ทราบถึงพิบัติภัยและวิธีป้องกันในการเก็บรักษาข้อมูลสารสนเทศ หากเกิดภัยพิบัติขึ้นในพื้นที่

2) จัดทำทำเนียบ E-mail หรือเว็บไซต์ของหน่วยงานเพื่อการแจ้งเตือนในกรณีเกิดเหตุภัยพิบัติฉุกเฉินเกิดขึ้นในพื้นที่

3) จัดให้มีการฝึกอบรมเพื่อเตรียมการดูแลรักษาเครื่องมืออุปกรณ์และข้อมูลที่มีการจัดเก็บโดยชี้แจงให้ทราบขั้นตอนและวิธีการปฏิบัติในขณะที่เกิดเหตุภัยพิบัติ

4) จัดให้มีวัสดุ อุปกรณ์ และเครื่องคอมพิวเตอร์ ที่เหมาะสมและเตรียมสถานที่สำรองในการติดตั้ง หากมีปัญหาภัยพิบัติเกิดขึ้น

5) ให้ตรวจสอบวัสดุ/อุปกรณ์ที่ใช้ในการเก็บรักษาข้อมูลสารสนเทศอยู่เป็นประจำ

2. การปฏิบัติเมื่อเกิดภัย

1) ให้เจ้าหน้าที่ที่ได้รับการแต่งตั้งออกปฏิบัติงานตามแผนทันที

2) ให้แจ้ง หัวหน้างาน ผู้ช่วยหัวหน้างาน หรือเจ้าหน้าที่งานศูนย์ข้อมูลสารสนเทศ วิทยาลัยเทคนิคท่าหลวงซิเมนต์ไทยอนุสรณ์ หรือเจ้าหน้าที่ที่เข้าเวรรักษาการเพื่อเข้าแก้ปัญหาเบื้องต้น และแจ้งให้ฝ่ายบริหารรับทราบ

3.การฟื้นฟูบูรณะ

1) ผู้รับผิดชอบพื้นที่ ประเมินค่าความเสียหาย

2) ปรับปรุงแก้ไขให้สถานการณ์คืนสู่สภาพปกติ กู้ข้อมูลคืนในกรณีที่สามารถดำเนินการได้ด้วยวิทยาลัยเอง

3) กรณีที่ไม่สามารถดำเนินการได้โดยวิทยาลัย ให้รายงานความเสียหาย ประมาณการค่าความเสียหายให้กับหน่วยงานบังคับบัญชาเพื่อขอสนับสนุนงบประมาณ

4) กระบวนการควบคุมการปฏิบัติในสถานการณ์ฉุกเฉิน เมื่อเกิดสถานการณ์ภัยพิบัติขึ้นเพื่อให้การแก้ไขปัญหาเป็นไปด้วยความเรียบร้อยหรือดำเนินการไปได้อย่างมีประสิทธิภาพ จึงกำหนดให้มีกระบวนการควบคุมการปฏิบัติในสถานการณ์ฉุกเฉินไว้เป็น 6 ขั้นตอน คือ

1) รายงานปัญหาและรับทราบปัญหา

2) ตรวจสอบข้อเท็จจริง

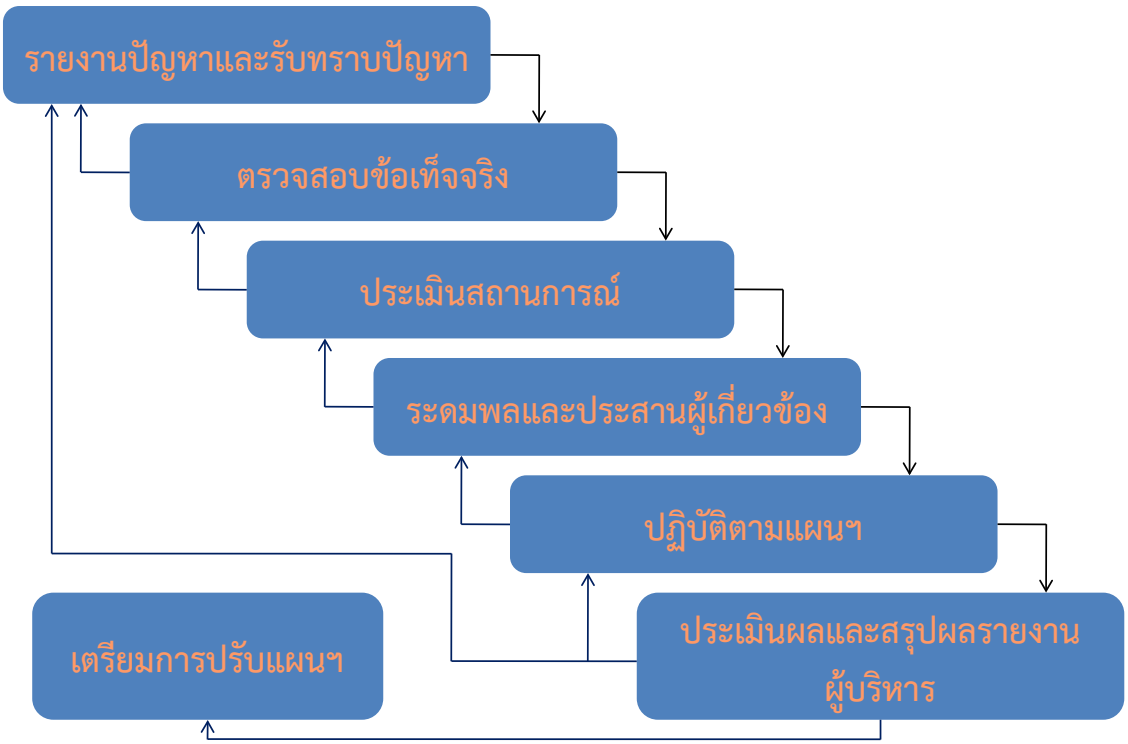
3) ประเมินสถานการณ์

4) ระดมพลและประสานผู้เกี่ยวข้อง

5) ปฏิบัติตามแผนฯ

6) ประเมินผลและสรุปผลรายงานผู้บริหาร ในขั้นตอนนี้หากยังพบปัญหาก็จะย้อนกลับไปสู่แนวทางหรือกระบวนการแก้ไขปัญหา ในขั้นตอนการเตรียมการเบื้องต้น

กระบวนการควบคุมการปฏิบัติในสถานการณ์ฉุกเฉิน
เมื่อเกิดภัยพิบัติด้านเทคโนโลยีสารสนเทศและการสื่อสาร



5. แนวทางปฏิบัติเพื่อป้องกันหรือลดความเสี่ยงด้านระบบข้อมูลสารสนเทศ

1. การบำรุงรักษา

1) มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และมีการดูแลอย่างถูกต้องและต่อเนื่อง

2) ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

3) การใช้แผ่นซีดีหรือ Flash drive ควรตรวจสอบไวรัสก่อนใช้ทุกครั้ง

4) ควรทำความสะอาดเครื่องคอมพิวเตอร์ให้ใหม่อยู่เสมอและมีการตรวจสอบดูแลคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

5) ควรใช้คำสั่งในโปรแกรม Windows ในการบำรุงรักษาเครื่องเป็นประจำ

6) การติดตั้ง Firewall เพื่อเป็นการป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาต เข้า สู่ระบบเครือข่ายได้

7) การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงาน รวมทั้งการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ

2. การรักษาความปลอดภัย

1) กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์ และในกรณีที่พบว่ามีการใช้งานหรือมีการเปลี่ยนแปลงในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

2) ทำการทดสอบระบบซอฟท์แวร์ที่เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพในการใช้งานอย่างสม่ำเสมอ

3) ติดตั้งโปรแกรมระบบรักษาความปลอดภัย เช่น การติดตั้ง Firewall

4) กำหนดเจ้าหน้าที่รับผิดชอบในการดำเนินการไว้อย่างชัดเจน

3. มาตรการในการป้องกันไวรัส

1) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

1.1 ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม

1.2 สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ

1.3 อัพเดตข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดต

1.4 ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ

1.5 ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

2) การป้องกันจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

2.1 ทำการสแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

2.2 ไม่ควนเปิดไฟล์ที่มีนามสกุลแปลก ๆ ที่น่าสงสัย เช่น *.pif เป็นต้น

2.3 หลีกเลี่ยงการใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

4. การจัดการด้านกายภาพและสิ่งแวดล้อม

1) พิจารณาตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและติดตั้งระบบเทคโนโลยี สารสนเทศไว้ที่เครื่องคอมพิวเตอร์แม่ข่าย รวมถึงการกำหนดที่ตั้งของเครื่อง คอมพิวเตอร์ การเดินสายไฟฟ้า สายสัญญาณ โดยหลีกเลี่ยงการติดตั้งระบบไว้ในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันภัยพิบัติในเบื้องต้น เช่น เครื่องปรับอากาศ ตู้Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย ถังดับเพลิงเป็นต้น

2) ควบคุมการเข้าออกห้องปฏิบัติการระบบข้อมูลสารสนเทศ กำหนดเป็นพื้นที่ เขตหวงห้ามเฉพาะและการกำหนดสิทธิการเข้าออกให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

3) จัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะเพื่อความสะดวกในการปฏิบัติงานและยังทำให้การควบคุมและการเข้าถึงอุปกรณ์คอมพิวเตอร์ต่าง ๆ มีประสิทธิภาพมากขึ้น โดย

จัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูลเช่น การสำรองข้อมูลไว้กรณีฉุกเฉินเมื่อข้อมูลเกิดการเสียหาย

4) วางระบบป้องกันภัยที่เหมาะสม โดยจัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลา

5) จัดให้มีระบบป้องกันไฟฟ้ากระชากเพื่อไม่ให้คอมพิวเตอร์ได้รับความเสียหายรวมทั้งติดตั้งระบบสายดินที่ได้มาตรฐานหรือจัดให้มีระบบไฟฟ้าสำรอง

6) มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศ และค่าความชื้นให้มีระดับเหมาะสมระบบคอมพิวเตอร์

5. การสำรองข้อมูลและกู้คืนข้อมูล

แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

1. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ

2. จัดทำบันทึกการสำรองข้อมูล ผู้ดูแลระบบคอมพิวเตอร์ ต้องทำบันทึก รายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้ สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

3. การรายงานข้อผิดพลาด ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

4. ผู้ดูแลระบบคอมพิวเตอร์ มอบ หมายหน้าที่การสำรองข้อมูล แก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

<u>การปฏิบัติเกี่ยวกับการสำรองข้อมูล</u>

1. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

ลำดับ	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
1	Web Servers	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ข้อมูลเผยแพร่บนเว็บไซต์และฐานข้อมูล 1 ครั้งต่อสัปดาห์
2	ระบบ RMS	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ข้อมูลและฐานข้อมูล 1 ครั้งต่อสัปดาห์
3	Server ระบบ RNET ทุกตัว	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ข้อมูลและฐานข้อมูล 1 ครั้งต่อสัปดาห์
4	Server อื่น ๆ	ค่า configure ก่อนและหลังการเปลี่ยนแปลง	ก่อนและหลังการเปลี่ยนแปลง1 ครั้งต่อเดือน

6. การตรวจสอบการเข้าสู่ระบบ

1) กำหนดสิทธิให้แก่ผู้ใช้งาน

1.1. กำหนดสิทธิการเข้าถึงข้อมูลสารสนเทศและระบบคอมพิวเตอร์ เช่น กำหนดสิทธิการเข้าใช้ระบบให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่ และความรับผิดชอบ

1.2. กำหนดให้มีการเปลี่ยนแปลงรหัสผ่านอย่างรอบคอบและมีชั้นความลับ

1.3. ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น จะต้องขออนุญาตจากผู้มีอำนาจหน้าที่ให้การอนุมัติทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นในการเข้าใช้งาน

2) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

2.1. กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากล

2.2. ควรใช้อักขระพิเศษประกอบเช่น @ ; <> เป็นต้น

2.3. สำหรับผู้ใช้งานทั่วไปควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุก 6 เดือน ส่วนผู้ดูแลระบบควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน

2.4. ในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรจะกำหนดรหัสผ่านใหม่ซ้ำชื่อเดิม

2.5. ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่นผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

7. การจัดการด้านบุคลากร

1) กำหนดโครงการสร้างบุคลากรด้านเทคโนโลยีสารสนเทศและการบริหารจัดการในลักษณะกระจายภารกิจและความรับผิดชอบ รวมทั้งการแต่งตั้งเจ้าหน้าที่ที่มีความรู้ความสามารและมีประสบการณ์ด้านคอมพิวเตอร์ ซึ่งสามารถถ่ายทอดความรู้ให้แก่ผู้ใช้งานได้อย่างมีประสิทธิภาพ

2) หากมีการเปลี่ยนแปลงผู้ดูแลระบบหรือเจ้าหน้าที่ผู้รับผิดชอบจะต้องแจ้งให้ผู้บังคับบัญชาทราบเพื่อประโยชน์ในการบริหารงาน

3) การจัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อดำเนินการและควบคุมกำกับ ดูแลหรือเป็นที่ปรึกษาจากบริษัทที่มีความชำนาญเฉพาะทาง มีเครื่องมือ และ เทคโนโลยีทันสมัยซึ่งเอื้อต่อการพัฒนาระบบฐานข้อมูลสารสนเทศ

4) จัดส่งผู้รับผิดชอบในส่วนต่าง ๆ เข้ารับการฝึกอบรมความรู้ทางเทคโนโลยีสารสนเทศตามช่วงระยะเวลาที่เหมาะสม

8. การป้องกันปัญหาที่เกิดจากกระแสไฟฟ้า

1) เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (AVR) ตลอดระยะเวลา

เปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์ส่วนบุคคล

2) เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

9. การปฏิบัติการรักษาความปลอดภัยสถานที่

ให้ถือปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2517

6. ปัญหาและอุปสรรคในการดำเนินกา

- มีข้อจำกัดด้านทรัพยากรเทคโนโลยีสารสนเทศในการดำเนินงาน
- การจัดทำฐานข้อมูลยังไม่มีความครบถ้วน ตามความเหมาะสม ภารกิจที่ต้องดำเนินการมีปริมาณมากกว่าจำนวนบุคลากรผู้รับผิดชอบ
- การสื่อสาร ถ่ายทอดความรู้ ความเข้าใจ ระหว่างบุคลากรผู้จัดทำด้านยุทธศาสตร์ ผลผลิต แผนงานโครงการกับผู้ปฏิบัติงานด้าน ICT ไม่เพียงพอ ทำให้การพัฒนาสารสนเทศและฐานข้อมูล มีความล่าช้าคลาดเคลื่อน ไม่เป็นไปตามความต้องการ ต้องใช้เวลามากในการปรับปรุงและแก้ไข
- หน่วยงานไม่ได้รับงบประมาณในการพัฒนาเทคโนโลยีสารสนเทศตามความจำเป็น โดยเฉพาะเมื่อต้องจัดทำระบบหรือโปรแกรมงานขึ้นใหม่ตามภารกิจที่มี จึงทำให้ระบบงานที่ใช้ประโยชน์ได้ยังไม่ครบถ้วน และเป็นไปตามความต้องการ
- ระบบที่ดำเนินการพัฒนาในปีปัจจุบันอาจต้องมีการปรับปรุงเพื่อให้เป็นไปตามความต้องการใช้งานต่อยอดในการบริหารและจัดการด้านสารสนเทศและการสื่อสาร