กรมอนามัย
DEPARTMENT OF HEALTH

ศูนย์พัฒนาอนามัยพื้นที่สูง ลำปาง
Highland Health Development Center

แผนสำรองฉุกเฉินระบบเทคโนโลยีสารสนเทศ

งานเทคโนโลยีสารสนเทศ ฝ่ายบริหารยุทธศาสตร์
ศูนย์พัฒนาอนามัยพื้นที่สูง

คำนำ

งานเทคโนโลยีสารสนเทศ ตระหนักถึงความสำคัญของข้อมูลสารสนเทศสำหรับให้บริการ จำเป็นต้องได้ตรวจสอบและบำรุงรักษาให้มีความมั่นคงปลอดภัย สามารถใช้งานได้อย่างมีประสิทธิภาพและตลอดเวลา ดังนั้นเพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศจึงได้จัดทำแผนสำรองฉุกเฉินระบบเทคโนโลยีสารสนเทศเพื่อเป็นกรอบแนวทางในการาบำรุงรักษาและป้องกัน แก้ไขปัญหาที่จะส่งผลกระทบต่อข้อมูล ระบบสารสนเทศของศูนย์ฯ เครื่องคอมพิวเตอร์ และอุปกรณ์

งานเทคโนโลยีสารสนเทศ ฝ่ายบริหารยุทธศาสตร์
ศูนย์พัฒนาอนามัยพื้นที่สูง

แผนสำรองฉุกเฉินระบบเทคโนโลยีสารสนเทศ

1. หลักการและเหตุผล

ศูนย์พัฒนาอนามัยพื้นที่สูงได้นำเทคโนโลยีสารสนเทศมาช่วยเพิ่มประสิทธิในการให้บริการด้านข้อมูลสารสนเทศ และอินเทอร์เน็ต แก่ผู้รับบริการทั้งบุคลากรศูนย์ฯ และบุคลภายนอก ในขณะเดียวกันการให้บริการดังกล่าวอาจได้รับความเสียหาย จากไวรัสคอมพิวเตอร์ บุคลากร ไฟฟ้า อัคคีภัย หรือจากปัจจัยอื่นทั้งภายในและภายนอก งานเทคโนโลยีสารสนเทศ ศูนย์พัฒนาอนามัยพื้นที่สูง จึงได้จัดทำแผนสำรองฉุกเฉินระบบเทคโนโลยีสารเทศ ของศูนย์ฯ เพื่อเป็นแนวทางการป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้นในอนาคต

2. **วัตถุประสงค์**

2.1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและระบบสารสนเทศของศูนย์ฯ ให้มีเสถียรภาพ มีความพร้อมสำหรับการใช้งาน

2.2. เพื่อให้ระบบสารสนเทศของศูนย์ฯ สามารถใช้งานได้อย่างสม่ำเสมอ มีประสิทธิภาพ และสามารถแก้ไขปัญหาได้อย่างทันท่วงที

2.3. เพื่อลดความเสียหายที่อาจจะเกิดขึ้นกับข้อมูล หรือระบบสารเทศของศูนย์ฯ

2.4. เพื่อเตรียมความพร้อมกับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับข้อมูล หรือระบบสารสนเทศของศูนย์ฯ

3. การประเมินสถานการณ์ความเสี่ยง

จากการวิเคราะห์และตรวจสอบความเสี่ยงในระบบเทคโนโลยีสารสนเทศของศูนย์พัฒนาอนามัยพื้นที่สูง พบว่า ความเสี่ยงที่อาจเป็นอันตราย มีดังนี้

3.1. เจ้าหน้าที่หรือบุคลากรของหน่วยงาน ขาดความรู้ความเข้าใจในเครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่น ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการใช้งาน ทำให้ไม่สามารถใช้งานได้เต็มประสิทธิภาพ

3.2. ไวรัสคอมพิวเตอร์ หรือการบุกรุก สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

3.3. ระบบไฟฟ้าขัดข้อง, ฟ้าผ่า หรือความเสียหายจากเพลิงไหม้

3.4. การขโมยอุปกรณ์คอมพิวเตอร์

3.5. อุณหภูมิที่ไม่เหมาะสมจะทำให้อุปกรณ์ทำงานผิดปกติ

4. การเตรียมการเบื้องต้น

4.1. จัดการอบรม สัมมนา ให้ความรู้ความเข้าใจเกี่ยวกับ Hardware และ Software เบื้องต้น แก่เจ้าหน้าที่และบุคลากรของศูนย์ฯ เพื่อลดความเสี่ยงที่เกิดจากเจ้าหน้าที่หรือบุคลากรให้น้อยที่สุด

4.2. ติดตั้ง firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่าย internet สามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์

4.3. การสำรองข้อมูล เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย สูญหาย หรือเปลี่ยนแปลงข้อมูล สามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ มีแนวทางคือให้เจ้าหน้าที่งานเทคโนโลยีสารสนเทศเป็นผู้สำรองข้อมูลเป็นประจำทุกเดือน โดยสำรองข้อมูลไว้ในเทปบันทึกข้อมูล

4.4. การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย และผู้ใช้จะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับ internet เพื่อป้องกันไม่ให้เป็นช่องทางให้ผู้ไม่ประสงค์ดีเข้ามาบุกรุก หรือทำลายระบบ โดยมีวิธีดังนี้

4.4.1.โปรแกรมป้องกันไวรัสคอมพิวเตอร์

4.4.1.1. ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์

4.4.1.2. อัพเดทข้อมูลไวรัสคอมพิวเตอร์

4.4.1.3. ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

4.4.2.ระวังภัยจากการเปิดไฟล์จากสื่อบันทึก ข้อมูลต่างๆ เช่น เฟลชไดร์ แผ่นดิสก์ แผ่นซีดี เป็นต้น

4.4.2.1. สแกนไวรัสจากสื่อบันทึกข้อมูลก่อนใช้ทุกครั้ง

4.4.2.2. ไม่ควรเปิดไฟล์ที่มีนามสกุลที่ไม่รู้จัก หรือน่าสงสัย

4.4.2.3. ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

4.4.3.ใช้ความระมัดระวังในการเปิด e-mail โดยไม่เปิดไฟล์ e-mail ถ้าไม่ทราบแหลงที่มา และลบไฟล์ e-mail ที่ไม่ทราบแหล่งที่มาทิ้ง

4.4.4.ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก internet

4.4.4.1. ไม่เปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น line เป็นต้น

4.4.4.2. ไม่เข้าเว็บไซต์ที่แนะนำทาง e-mail ที่ไม่ทราบแหล่งที่มา

4.4.4.3. ไม่ดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ

4.4.4.4. หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

4.5. การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง โดยมีการติดตั้งอุปกรณ์สำรองไฟฟ้า เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับเครื่องคอมพิวเตอร์ ทั้งเครื่องแม่ข่าย และเครื่องลูกข่าย รวมถึงอุปกรณ์ระบบเครือข่ายที่ให้บริการ internet intranet ของศูนย์ฯ ในกรณีเกิดกระแสไฟฟ้าขัดข้อง

4.6. การป้องกันการสูญหายของเครื่องคอมพิวเตอร์และอุปกรณ์ บริเวณห้องคอมพิวเตอร์แม่ข่าย ได้ติดตั้งกุญแจและห้ามบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าก่อนได้รับอนุญาต หากมีความจำเป็นเข้าห้องจะต้องมีเจ้าหน้าที่งานเทคโนโลยีสารสนเทศนำเข้าไปทุกครั้ง

4.7. ติดตั้งเครื่องปรับอากาศบริเวณห้องคอมพิวเตอร์แม่ข่าย

4.8. การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

4.9. จัดอุปกรณ์ที่จำเป็น ในการเตรียมความพร้อมรับภัยพิบัติที่จะเกิดขึ้น ดังนี้

4.9.1.ติดตั้งอุปกรณ์ดับเพลิงสำหรับระงับเหตุเพลิงไหม้บริเวณห้องคอมพิวเตอร์แม่ข่าย

4.9.2.แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

4.9.3.เทปสำรองข้อมูลและระบบงานที่สำคัญ

4.9.4.แผ่นโปรแกรม Anti-Virus/Spyware

4.9.5.แผ่นไดรเวอร์อุปกรณ์ต่างๆ

4.9.6.อุปกรณ์อื่นๆ

5. <u>การกำหนดผู้รับผิดชอบ</u>

หน้าที่รับความรับผิดชอบของผู้เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

5.1. ระดับนโยบาย

5.1.1.ผู้อำนวยการศูนย์พัฒนาอนามัยพื้นที่สูง

5.1.2.หัวหน้างานเทคโนโลยีสารสนเทศ

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ติดตาม กำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

5.2. ระดับปฏิบัติการ

5.2.1.นายชัยวัฒน์ สุวรรณวิภาต

5.2.2.นายวิเชียร พรหมไชย

5.2.3.นายสุรสีห์ ฉันทกุล

รับผิดชอบ บำรุงรักษาระบบเครื่อง ระบบเครือข่าย ระบบความปลอดภัยทั้งหมด รวมทั้งแก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่ายคอมพิวเตอร์และระบบเครือข่าย และรักษาความปลอดภัยของระบบฐานข้อมูล ตลอดจนการทำสำเนาฐานข้อมูล

6. <u>ข้อปฏิบัติในการแก้ไขปัญหาภัยพิบัติ</u>

6.1. กรณีเครื่องลูกข่าย

6.1.1.กรณีมีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ที่ใช้เครื่องๆ นั้น แจ้งให้เจ้าหน้าที่ไอทีทราบ หรือถ้ามีเหตุที่ไม่สามารถให้บริการระบบสารสนเทศได้ เจ้าหน้าที่งานไอทีต้องแจ้งให้เจ้าหน้าที่ศูนย์ฯ ทุกฝ่ายทราบ

6.1.2.กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันการแพร่กระจ่ายไปยังเครื่องอื่นหรือระบบเครือข่าย ให้ตัดการเชื่อมโยงระบบเครือข่ายออกจากเครื่องนั้นโดยเร็ว

6.1.3.ในกรณีที่มีเหตุขัดข้องและเกรงว่าจะเหตุนั้นให้เกิดอันตรายต่อเครื่องคอมพิวเตอร์ต่อกลุ่มงาน/หน่วยงาน ให้ดึงสายเชื่อมโยงระบบออกจากจุดชุมสายให้หมด

6.1.4.กรณีเครื่องติดไวรัสคอมพิวเตอร์ ให้ดำเนินการติดตั้งโปรแกรม Anti-virus และอัพเดทข้อมูลไวรัส จากนั้นเปิดใช้งานโปแกรม Anti-virus ที่ติดตั้งเพื่อค้นหาและทำลายไวรัสคอมพิวเตอร์ภายในเครื่อง

6.1.5.อุปกรณ์ Hardware เสียหาย

6.1.5.1. กรณีเมนบอร์ดเสียหาย ให้จัดหาเมนบอร์ด มาเปลี่ยน ติดตั้งระบบปฏิบัติการ

6.1.5.2. กรณี Hard disk เสียหาย ให้จัดหา Hard disk มาเปลี่ยน จากนั้นติดตั้งระบบปฏิบัติการและระบบเครือข่าย หากมีการสำรองข้อมูลจาก Hard disk เดิมให้นำข้อมูลใส่ให้ Hard disk ใหม่ด้วย

6.1.5.3. อุปกรณ์อื่นๆ ให้จัดหาอุปกรณ์นั้นๆ มาเปลี่ยน

6.2. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

6.2.1.ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

6.2.2.ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

6.2.3.ในกรณีมีไฟไหม้ ให้ตัดระบบจ่ายไฟฟ้า และรีบระงับเหตุไฟไหม้ดังกล่าว หากไม่สามารถระงับเพลิงได้ให้ รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

6.2.4.ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบเครื่องแม่ข่ายโดยเร็วที่สุด

6.2.5.กรณีที่อุปกรณ์ด้าน Hardware เสียให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

6.2.6.ผู้ดูแลระบบ ต้องรีบรายงานผู้บังคับบัญชาตามลำดับ ให้ทราบโดยเร็ว

7. <u>แผนกู้ระบบคอมพิวเตอร์กลับสู่สภาพปกติ</u>

โดยปกติ ระบบเครือข่าย อุปกรณ์กระจายสัญญาณ เครื่องคอมพิวเตอร์แม่ข่าย ต้องอยู่ในสภาพที่พร้อมให้บริการ ได้ตลอด 24 ชั่วโมง หากไม่สามารถให้บริการได้ จำเป็นต้องกู้ระบบคืนให้ได้โดยเร็วที่สุด หรือเท่าที่จะทำได้ โดยดำเนินการดังนี้

7.1. จัดหาอุปกรณ์ใหม่

7.2. เปลี่ยนอุปกรณ์ที่เสียหาย

7.3. ซ่อมบำรุงอุปกรณ์ที่เสียหายภายใน 24 ชั่วโมง / หาทดแทน

7.4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

7.5. นำข้อมูลที่ได้สำรองไว้ มาทำการ restore เพื่อให้ระบบสามารถใช้งานได้โดยเร็ว ภายใน 24 ชั่วโมง*

7.6. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

* หมายเหตุ ข้อมูลที่ได้สำรองไว้ หมายถึง ข้อมูลที่ได้จากการสำรองข้อมูล ตามแนวทางของคู่มือการสำรองข้อมูลและการกู้คืนข้อมูล ศูนย์พัฒนาอนามัยพื้นที่สูง กรมอนามัย กระทรวงสาธารณสุข