คู่มือการปฏิบัติงาน

การพัฒนาข้อมูลและเทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงสาธารณสุข

สารบัญ

1. วัตถุประสงค์

เพื่อเป็นแนวทางในการปฏิบัติงานด้านการพัฒนาข้อมูลและเทคโนโลยีสารสนเทศ ของสำนักงานปลัดกระทรวงสาธารณสุข ให้มีความมั่นคง ความปลอดภัย มีความถูกต้อง เป็นที่ยอมรับ เป็นที่เชื่อถือได้ โดยใช้หลักบริหารจัดการฐานข้อมูล และ หลักการบริหารความเสี่ยงเป็นเครื่องมือในการดูแลรักษาฐานข้อมูลสารสนเทศและเทคโนโลยีเครือข่ายคอมพิวเตอร์

2. ขอบเขต

การพัฒนาข้อมูลและเทคโนโลยีสารสนเทศ ของสำนักงานปลัดกระทรวงสาธารณสุข จะเกี่ยวข้องโดยตรงกับ 2 หน่วยงานหลัก ได้แก่ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) และสำนักนโยบายและยุทธศาสตร์ (สนย.) ในฐานะของผู้เชี่ยวชาญเฉพาะด้าน ผู้ให้คำปรึกษา และคณะกรรมการพิจารณาดำเนินการ นอกจากนี้ยังเกี่ยวกับทุกหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ที่จะต้องถือปฏิบัติตามคู่มือเล่มนี้ในการดำเนินงานกระบวนการพัฒนาข้อมูลและเทคโนโลยีสารสนเทศ

แบ่งเป็น 2 กระบวนการ

1) การพัฒนาระบบข้อมูลสารสนเทศและความรู้
2) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ครอบคลุมตั้งแต่การศึกษาวิเคราะห์ การออกแบบ จัดทำแผน นำแผนสู่การปฏิบัติ และติดตามผลการดำเนินงาน

3. คำจำกัดความ

3.1 การพัฒนาระบบข้อมูลสารสนเทศและความรู้ หมายถึง การพัฒนาโปรแกรม ระบบงาน ระบบฐานข้อมูล ทั้งที่ดำเนินการเองโดยเจ้าหน้าที่ภายในหน่วยงานสังกัดสำนักงานปลัดกระทรวงสาธารณสุข และดำเนินการโดยการจัดจ้างบริษัท ห้างร้าน ด้วยวิธีการจัดซื้อจัดจ้างตามระเบียบพัสดุ

3.2 ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุขไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อระบบเทคโนโลยีสารสนเทศที่สำนักงานปลัดกระทรวงสาธารณสุขใช้ในการบริหารงานและปฏิบัติการโดยเฉพาะอย่างยิ่งการบริการประชาชน

3.3 การควบคุม (Control) หมายถึง ขั้นตอนการปฏิบัติ กระบวนการดำเนินงานหรือกลไกการปฏิบัติงาน ซึ่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุขกำหนดขึ้นเพื่อให้มั่นใจว่าการบริหารงานจะสามารถบรรลุวัตถุประสงค์ที่ได้กำหนดไว้

3.4 การบริหารความเสี่ยง (Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ ประเมิน จัดการและติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หน่วยงาน หรือกระบวนการดำเนินงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้

3.5 การบริหารความเสี่ยงศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยรวม (Organization Wide Risk Management) หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการปฏิบัติงานต่างๆ โดยต้องลดมูลเหตุของแต่ละโอกาสที่จะทำให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุขเสียหาย

3.6 ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ระบบเครือข่ายคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์ ระบบเครื่องสื่อสาร ระบบฐานข้อมูล และอุปกรณ์ประกอบระบบต่าง ๆ รวมทั้ง อาคารสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด

3.7 ความปลอดภัย หมายถึง สภาพหรือสภาวะที่แสดงถึงการเตรียมการ และการดำเนินการเพื่อป้องกันภัย อันตราย จากการปฏิบัติงานหรือการกระทำต่างๆ รวมถึงการแก้ไขและช่วยเหลือในกรณีฉุกเฉิน

3.8 ประสิทธิภาพ หมายถึง หมายถึง การปฏิบัติงานหรือบริการที่ถูกต้อง รวดเร็ว ใช้เทคนิคที่สะดวกสบายกว่าเดิม คุ้มค่า และใช้ทรัพยากรน้อยที่สุดในขณะที่ต้องการผลงานมากที่สุด (Efficiency is to do thing right)

3.9 เสถียรภาพ หมายถึง เสถียรภาพ (Stability) หมายถึง ระดับความมั่นคงของระบบเครือข่ายการสื่อสารของกระทรวงสาธารณสุขที่ไม่ผันแปรจนเกินระดับที่ยอมรับได้

3.10 ศทส.สป.สธ. หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

4. หน้าที่ความรับผิดชอบ

4.1 ผู้อำนวยการ

- 4.1.1 อนุมัติแผนดำเนินการ/โครงการ
- 4.1.2 แต่งตั้งคณะกรรมการ และคณะทำงาน
- 4.1.3 อนุมัติดำเนินการ

4.2 คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

- 4.2.1 ตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ แก้ไขปัญหาทันที รายงานผู้บริหาร
- 4.2.2 เสนอนโยบาย แนวทางปฏิบัติด้านการป้องกันความเสี่ยง

4.2.3 ควบคุม กำกับ ดูแลให้มีการปฏิบัติตามนโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

4.2.4 จัดทำแผนบริหารความเสี่ยงด้านการปฏิบัติการ (ระบบฐานข้อมูลสารสนเทศ) สำนักงานปลัดกระทรวงสาธารณสุข

4.2.5 ดำเนินการตามแผน/ติดตามกำกับให้หน่วยงานที่เกี่ยวข้องดำเนินการตามแผน

4.2.6 จัดทำรายงานผลการติดตามการปฏิบัติตามแผนการบริหารความเสี่ยงด้านการปฏิบัติการ (ระบบฐานข้อมูลสารสนเทศ)

4.3 คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์

คณะกรรมการดำเนินงานพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุข

4.3.1 พิจารณาความเหมาะสม ความคุ้มค่า ของคุณลักษณะเฉพาะของระบบฐานข้อมูลสารสนเทศที่ต้องการพัฒนา

4.3.2 ให้คำแนะนำ ข้อเสนอแนะ ในการพัฒนาระบบข้อมูลสารสนเทศและความรู้ แก่หน่วยงานเจ้าของเรื่อง

4.3.3 เสนอแนวทางการดำเนินงานตามมาตรฐานการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4.4 คณะกรรมการตามระเบียบพัสดุ

4.4.1 กำหนดคุณลักษณะเฉพาะของโปรแกรมคอมพิวเตอร์ และ/หรือระบบงานสารสนเทศ (TOR)

4.4.2 พิจารณาเกี่ยวกับการเปิดซองราคา สอบราคา หาผู้ที่เสนอผลประโยชน์สูงสุดแก่ราชการ

4.4.3 ตรวจสอบรายละเอียดของโปรแกรมคอมพิวเตอร์ ตามข้อกำหนดการจ้างหรือคุณลักษณะเฉพาะของโปรแกรมคอมพิวเตอร์ และ/หรือระบบงานสารสนเทศ (TOR)

5. **Workflow กระบวนการ**

5.1 กระบวนการพัฒนาระบบข้อมูลสารสนเทศและความรู้ (ตามภาคผนวก 1)

5.2 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ตามภาคผนวก 2)

6. รายละเอียดวิธีปฏิบัติ

6.1 กระบวนการพัฒนาระบบข้อมูลสารสนเทศและความรู้ (ตามภาคผนวก 3)

6.2 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ตามภาคผนวก 4)

7. มาตรฐานการปฏิบัติงาน

7.1 มาตรฐานการพัฒนาระบบข้อมูลสารสนเทศและความรู้

เป็นแนวทางที่ให้ทุกหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ได้นำไปใช้ในการพัฒนาระบบงานฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติงานต่างๆ เพื่อให้ได้ผลลัพธ์ที่มีประสิทธิภาพ ดังนี้

7.1.1 ก่อนการพัฒนาระบบ

1) พิจารณาความต้องการของระบบหรือโปรแกรม ควรให้สอดคล้องกับทิศทางและพันธกิจของหน่วยงาน

2) ควรมีความชัดเจนในเป้าประสงค์ของโปรแกรม และมอบหมายผู้ควบคุมการดำเนินงานให้ชัดเจนเพื่อทำหน้าที่ กำกับดูแลให้การพัฒนาโปรแกรมอยู่ในขอบเขตที่นำไปสู่เป้าประสงค์ และสามารถพัฒนาเสร็จได้ในระยะเวลาที่กำหนด ภายใต้งบประมาณและทรัพยากรที่มีอยู่ในปัจจุบัน

3) พิจารณาถึงผลตอบแทนหรือประโยชน์ที่จะได้รับเมื่อโปรแกรมพัฒนาเสร็จ

4) พิจารณาเทคโนโลยี ภาษาโปรแกรมคอมพิวเตอร์ที่เลือกใช้ ว่ามีความเป็นไปได้ในการพัฒนาตามความต้องการได้จริง และเป็นเทคโนโลยีที่นิยมใช้แพร่หลาย และจะยังคงอยู่ต่อไปในอนาคตอย่างน้อย 3-5 ปีเพื่อลดค่าใช้จ่ายในการบำรุงรักษาโปรแกรมหรือระบบ

5) พิจารณาถึงความต้องการด้านข้อมูลที่จะนำไปใช้กับโปรแกรม ควรต้องมีความสอดคล้องและต่อเนื่อง

6) ทีมพัฒนา ควรได้รับความชัดเจนเรื่องกลุ่มผู้ใช้งาน และเก็บรวบรวมข้อมูลความต้องการของโปรแกรมจากกลุ่มผู้ใช้งานให้ได้มากที่สุด

7) การออกแบบหน้าจอ และขั้นตอนการทำงานของโปรแกรม ต้องให้เหมาะสมกับการปฏิบัติงานจริง ช่วยให้ทำงานได้สะดวก รวดเร็ว และขั้นตอนไม่ซับซ้อน

8) การออกแบบระบบทั้งในส่วนโปรแกรม และโครงสร้างฐานข้อมูลจะต้องรองรับการปรับเปลี่ยน หรือเพิ่มเติมในอนาคตได้ แต่ไม่ควรเผื่อไว้โดยไม่ได้ใช้งานจริง เพราะระบบจะมีขนาดใหญ่เกินจำเป็นและต้องใช้ทรัพยากรเพื่อดูแลรักษาไม่คุ้มค่ากับประโยชน์ที่ได้รับ

7.1.2 การเลือกใช้เครื่องมือในการพัฒนา

1) พิจารณาเลือกใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง หรือเลือกใช้ซอฟต์แวร์ที่เป็น Open Source

2) พิจารณาถึงผลกระทบต่างๆ เช่น การดูแลรักษาระบบที่ยุ่งยาก การพัฒนาบุคลากรในการเรียนรู้เทคโนโลยีใหม่ ข้อจำกัดของเทคโนโลยีที่ส่งผลให้ไม่สามารถเชื่อมโยงการทำงานระหว่างระบบงานเดิมและระบบงานใหม่ได้ เป็นต้น

3) พิจารณาถึงงบประมาณ ระยะเวลาในการพัฒนา ระยะเวลาในการ Implement ระบบ

7.1.3 ขั้นตอนการพัฒนา

พิจารณาดำเนินงานตามวงจรชีวิตของการพัฒนาระบบฐานข้อมูล (Database Life Cycle) หรือที่เรียกอย่างย่อว่า DBLC เป็นขั้นตอนที่กำหนดขึ้น เพื่อใช้เป็นแนวทางในการพัฒนาระบบฐานข้อมูลขึ้นใช้งาน ซึ่งประกอบด้วยขั้นตอนต่างๆ ดังนี้

1) Database Initial Study วิเคราะห์ความต้องการต่าง ๆ ของผู้ใช้ เพื่อกำหนดจุดมุ่งหมาย ปัญหา ขอบเขต และกฎระเบียบต่าง ๆ ของระบบฐานข้อมูลที่จะพัฒนา

2) Database Design นำเอารายละเอียดต่าง ๆ ที่ได้จากการวิเคราะห์มาเป็นแนวทางในการออกแบบ สำหรับแนวทางที่นิยมใช้ในการออกแบบฐานข้อมูล ได้แก่ แนวทางแบบ Data-driven (ให้ความสำคัญกับตัวข้อมูล ต้องออกแบบตัวข้อมูลจนมีความสมบูรณ์ก่อนที่จะทำการออกแบบตัวโปรแกรม) และแนวทางแบบ Joint Data- and Function-driven (สามารถตรวจสอบความสมบูรณ์ของข้อมูลควบคู่ไปกับการตรวจสอบการทำงานของ Function ว่ามีจำนวนครบถ้วนหรือไม่)

3) Implementation and Loading สร้างฐานข้อมูลที่จะใช้เก็บข้อมูลจริง รวมทั้งทำการแปลงข้อมูลของระบบงานเดิมให้สามารถนำมาใช้งานในระบบฐานข้อมูลที่พัฒนาขึ้นใหม่

4) Testing and Evaluation ทดสอบระบบฐานข้อมูลที่พัฒนาขึ้น เพื่อหาข้อผิดพลาดต่าง ๆ รวมทั้งทำการประเมินความสามารถของระบบฐานข้อมูลว่ารองรับความต้องการของผู้ใช้งานด้านต่าง ๆ ได้อย่างถูกต้องและครบถ้วนหรือไม่

5) Operation นำระบบฐานข้อมูลที่พัฒนาเสร็จเรียบร้อยไปใช้งานจริง

6) Maintenance and Evolution ขั้นตอนนี้เกิดขึ้นระหว่างการใช้งานจริง เพื่อบำรุงรักษาให้ระบบฐานข้อมูลทำงานได้อย่างมีประสิทธิภาพ รวมทั้งเป็นขั้นตอนของการแก้ไข ปรับปรุงระบบฐานข้อมูล ตามความต้องการของผู้ใช้งาน

7.1.4 การกำหนดคุณลักษณะของระบบหรือโปรแกรม

แนวทางในการพิจารณาเลือกพัฒนาโปรแกรมใดก่อนหรือหลัง ในช่วงระยะเวลาจำกัดเวลาหนึ่ง ควรพิจารณาดังนี้

1) โครงการเร่งด่วน ตามนโยบาย

2) ความจำเป็นในการใช้งานหรือความต้องการในการใช้งานตามลำดับความสำคัญ

3) ความเป็นไปได้ทางเทคโนโลยี เศรษฐกิจ และการประยุกต์ใช้งาน

4) ระยะเวลาที่เหมาะสมในการพัฒนาโปรแกรมแต่ละระบบ

รายละเอียดในการกำหนดคุณลักษณะเฉพาะของโปรแกรม ควรมีดังนี้

1) สรุประบบงานที่ปฏิบัติอยู่ ปัญหาอุปสรรคที่เกิดขึ้นจากการปฏิบัติ หรือจากการที่ไม่มีระบบโปรแกรมใช้

2) ระยะเวลาที่เพียงพอในแต่ละขั้นตอนของการพัฒนา เช่น การวิเคราะห์ความต้องการ การออกแบบ การพัฒนา การทดสอบ เป็นต้น

3) รายละเอียดฟังก์ชั่นและผลลัพธ์ที่ต้องการ ควรระบุให้ชัดเจน โดยอาจแยกหัวข้อตามระบบงาน เช่น สำหรับผู้ใช้ทั่วไป (End User Tools) สำหรับผู้ดูแลระบบ (Administrator Tools) สำหรับผู้ใช้เฉพาะกลุ่ม (Special User Tools) สำหรับผู้บริหาร (Management Tools) ระบบการทำรายงาน (Reports) ระบบการนำเข้า แก้ไข ปรับปรุงข้อมูล (Editing Data Flow) ซึ่งจำเป็นต้องระบุถึงความสามารถทั่วไปและความสามารถตามภารกิจของหน่วยงาน (Business Flow)

4) คุณสมบัติควรมีความเป็นไปได้ในการตรวจรับงาน ไม่กว้างหรือเจาะจงเกินไป

7.1.5 การทดสอบและตรวจรับระบบหรือโปรแกรม

ควรกำหนดวิธีการตรวจรับร่วมกับผู้พัฒนาระบบ โดยจัดทำเอกสารทดสอบระบบ (Test Checklist) ตามรายละเอียดของฟังก์ชั่นที่ระบุไว้ในเอกสารสรุปความต้องการ ควรให้มีการทดสอบกับข้อมูลจริง โดยหน่วยงานเจ้าของระบบหรือโปรแกรมเป็นผู้จัดเตรียมข้อมูลที่ใช้ทดสอบ และทำการทดสอบก่อนติดตั้งใช้งานจริง เพื่อไม่ให้กระทบกับการปฏิบัติงาน ควรมีการทดสอบ ดังนี้

1) ทดสอบระหว่างการพัฒนา ได้แก่

- การตรวจสอบไวยากรณ์ (Syntax Checking) โดยใช้ Compiler ว่า Code ที่โปรแกรมเมอร์เขียนถูกต้องหรือไม่
- การทดสอบทีละโมดูล (Unit Testing หรือ Module Testing) ตรวจสอบผลลัพธ์ในระดับโมดูล
- การทดสอบแบบรวมโมดูล (Integration Testing) ทดสอบการรับส่งข้อมูลระหว่างโมดูล ทั้งแบบบนลงล่าง (Top-Down Approach) และแบบล่างขึ้นบน (Bottom-Up Approach)
- การทดสอบรวม (System Testing) ทดสอบทั้งระบบงานหรือโปรแกรม

2) ทดสอบภายหลังการพัฒนา ได้แก่ แบบตรวจการณ์ (Inspection) ตรวจสอบตามเอกสารทดสอบระบบ และแบบตามสถานการณ์จริง (Scenario Testing) ตรวจสอบโดยกำหนดขั้นตอนการทำงานเสมือนจริง มีการจัดเตรียมข้อมูลจริง

3) ทดสอบการกู้คือข้อมูล (Recovery Testing)

4) ทดสอบความปลอดภัย (Security Testing) เพื่อป้องกันการลักลอบใช้งานระบบหรือเรียกใช้ข้อมูลโดยไม่ได้รับอนุญาต

5) ทดสอบประสิทธิภาพการทำงาน (Performance Testing) หรือทดสอบความกดดัน (Stress Testing) คือการทดสอบเมื่อมีผู้ใช้งานหลายๆคนพร้อมกัน หรือเมื่อมีการทำงานหนักมากกว่าปกติ เพื่อดูผลลัพธ์ที่จะเกิดขึ้นว่าอะไรบ้างที่อาจเป็นสาเหตุที่ทำให้ระบบล่มได้

7.1.6 การดำเนินงานภายหลังการพัฒนาโปรแกรม

1) การฝึกอบรมการใช้งานโปรแกรม เช่น ฝึกอบรมการใช้งานระบบหลัก เพื่อการตรวจรับโปรแกรม หรือกำหนดฝึกอบรมโดย On the Job Training โดยให้มีการร่วมทีมพัฒนาโปรแกรมด้วย เพื่อสามารถพัฒาต่อเนื่องหรือดูแลระบบได้เองเมื่อหมดระยะเวลารับประกัน นอกจากนี้ควรมีกำหนดจำนวนผู้เรียนในแต่ละหลักสูตร แบ่งกลุ่มตามระดับการใช้งาน และความเกี่ยวข้องในการปฏิบัติงาน เช่น ผู้ดูแลระบบควรจะต้องมีความรู้ในการใช้งานโปรแกรมด้วยเพื่อให้ความช่วยเหลือผู้ใช้งานทั่วไปได้ และควรมีการวัดผลการฝึกอบรมเพื่อให้แน่ใจว่า ผู้รับการฝึกอบรมมีความเข้าใจระบบและสามารถใช้ปฏิบัติงานได้จริง

2) การจัดทำเอกสารประกอบโปรแกรม ได้แก่ เอกสารความต้องการระบบโปรแกรม เอกสารการออกแบบฐานข้อมูล และเอกสารวิธีการใช้งานโปรแกรมประยุกต์ หากหน่วยงานมีรูปแบบมาตรฐานของเอกสารอยู่แล้ว ควรจะแนบรูปแบบมาตรฐาน (Template) ไว้ในข้อกำหนดด้วย

7.1.7 การบำรุงรักษาโปรแกรม

การบำรุงรักษาควรจะต้องมีความสอดคล้องกันทั้ง Hardware Software และโปรแกรม จึงควรมีข้อกำหนดสำหรับการจ้างบำรุงรักษา ดังนี้

1) ดำเนินการแก้ไขข้อบกพร่อง (Bug) ของโปรแกรมให้สามารถใช้งานได้เป็นปกติภายใน 1 วันทำการหลังจากที่ได้รับแจ้ง

2) ติดตั้งโปรแกรมให้สามารถใช้งานได้ดีดังเดิม หลังจากมีการชำรุด บกพร่อง

3) ให้คำปรึกษาในเรื่องใช้งานโปรแกรม และการปรับปรุงแก้ไขโปรแกรมให้มีความสามารถเพิ่มมากขึ้น

4) ทดสอบการทำงานของโปรแกรมร่วมกับซอฟต์แวร์เวอร์ชั่นใหม่ พร้อมส่งรายงานสรุปผลการทดสอบเพื่อให้ทราบถึงผลกระทบของโปรแกรม

5) ดำเนินการปรับปรุงโปรแกรมที่บำรุงรักษาให้สามารถทำงานร่วมกับซอฟต์แวร์เวอร์ชั่นใหม่โดยไม่คิดค่าใช้จ่ายในกรณีที่ไม่มีผลกระทบของโปรแกรม

6) ต้องสามารถมั่นใจได้ว่าระบบหรือโปรแกรม จะใช้งานได้ตลอดเวลา หรือต้องใช้งานได้ทันทีเมื่อมีการร้องขอ

7) ต้องไม่เป็นการเพิ่มภาระงานแก่บุคลากรในการพัฒนาโปรแกรม

8) ควรต้องมีการระบุระยะเวลาดำเนินการแก้ไขปัญหาให้เสร็จ ตามความสำคัญของแต่ละระบบงาน

9) ควรต้องทำการตรวจสอบการรักษาความปลอดภัยของระบบอย่างสม่ำเสมอเพื่อป้องกันปัญหาที่เกิดจากไวรัสคอมพิวเตอร์

10) กรณีที่ระบบงานมีความซับซ้อน และเป็นระบบงานที่สำคัญมาก ควรจัดให้มีเจ้าหน้าที่มาประจำหน่วยงาน (Onsite Support) เพื่อคอยช่วยเหลือและแก้ไขปัญหาได้อย่างรวดเร็ว

11) จัดเตรียมงบประมาณการบำรุงรักษา ซึ่งโดยทั่วไปจะอยู่ในช่วง 15-25% ของราคาค่าพัฒนาโปรแกรม

7.2 มาตรฐานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เป็นแนวทางที่ให้ทุกหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ได้นำไปใช้ในการบริหารจัดการความเสี่ยงด้าน ICT หรือความเสี่ยงด้านระบบฐานข้อมูลและสารสนเทศของหน่วยงาน เพื่อให้สามารถกำจัด หรือควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ ดังนี้

7.2.1 การระบุความเสี่ยง

1) หน่วยงานควรแต่งตั้งคณะทำงานหรือกลุ่มบุคคลเพื่อทำหน้าที่บริหารจัดการความเสี่ยงที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศของหน่วยงาน

2) คณะทำงานประชุมร่วมกันเพื่อพิจารณาระบุความเสี่ยงที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของหน่วยงาน ความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงานว่ามีอะไรบ้าง และระบุว่าอะไรบ้างที่เป็นปัจจัยก่อให้เกิดความเสี่ยงดังกล่าว และความเสี่ยงใดบ้างที่เป็นความเสี่ยงที่ควรหลีกเลี่ยง (Avoid) หรือเป็นความเสี่ยงที่ยอมรับได้ (Accept) หรือเป็นความเสี่ยงที่ต้องมีมาตรการเพื่อลด (Reduce) หรือเป็นความเสี่ยงที่โอน/กระจาย (Share) ไปยัง Out Source ได้

3) จัดทำแผนปฏิบัติการบริหารจัดการความเสี่ยงด้าน ICT ของหน่วยงาน พร้อมทั้งประชาสัมพันธ์ให้บุคลากรทุกคนในหน่วยงานรับทราบถึงความเสี่ยง ปัจจัยเสี่ยงของหน่วยงาน ทำความเข้าใจและร่วมมือปฏิบัติตามแผน

7.2.2 การค้นหาความเสี่ยง

1) พัฒนาแบบฟอร์มเพื่อใช้ในการค้นหาความเสี่ยง ซึ่งความเสี่ยงแต่ละเรื่องอาจต้องใช้แบบฟอร์มที่แตกต่างกัน

2) กำหนดระยะเวลาในการค้นหาความเสี่ยงอย่างสม่ำเสมอ และต่อเนื่อง เช่น ทุกเดือน หรือทุก 3 เดือนเป็นต้น

3) กำหนดผู้รับผิดชอบในการค้นหาความเสี่ยง เพื่อเป็นผู้บันทึกข้อมูลลงในแบบฟอร์มและส่งให้คณะทำงานเก็บรวบรวม

7.2.3 การวิเคราะห์และประเมินความเสี่ยง

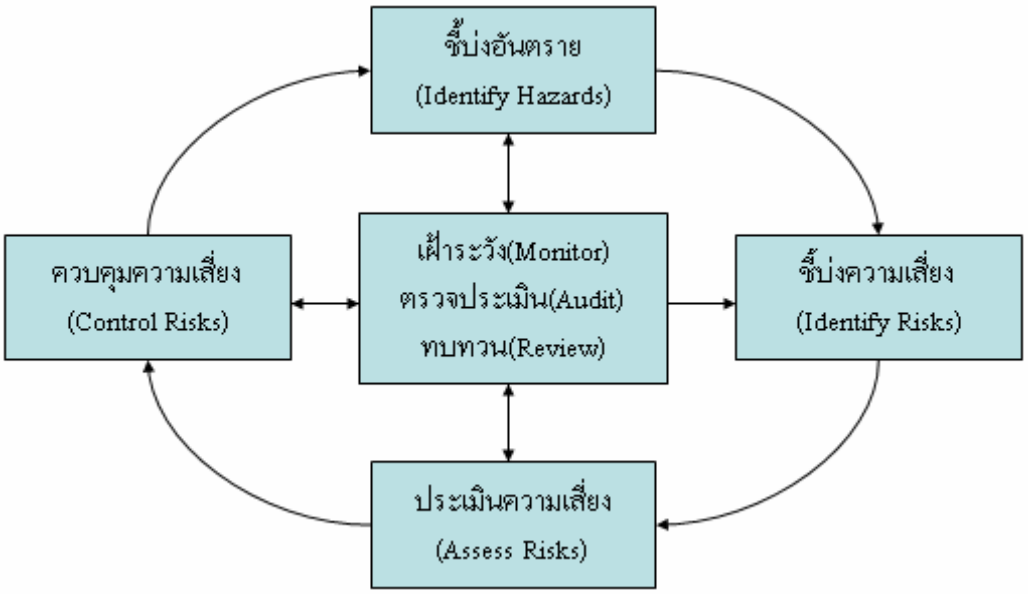
1) คณะทำงานรวบรวมแบบฟอร์มค้นหาความเสี่ยง และนำมาวิเคราะห์ความเสี่ยงที่ตรวจพบ ประเมินความรุนแรงของความเสี่ยง ประเมินผลกระทบที่อาจเกิดขึ้น และโอกาสที่จะเกิดความเสี่ยงแต่ละเรื่องได้อีก

2) วิเคราะห์หาปัจจัยที่ก่อให้เกิดความเสี่ยงแต่ละเรื่อง

3) กำหนดวิธีการจัดการหรือมาตรการ ในการจัดการปัจจัยเสี่ยง รูปแบบการดำเนินการ ระยะเวลาที่ควรดำเนินการ และกลุ่มบุคคลที่เกี่ยวข้องในการดำเนินงาน

7.2.4 การจัดการความเสี่ยง

ตามมาตรฐาน ISO/ IEC 17799 และ ISO/ IEC 27001 ซึ่งถือได้ว่าเป็นมาตรฐานสากล (International Standard) ด้านการบริหารจัดการเรื่องของความปลอดภัยข้อมูล ที่ครอบคลุมเรื่องสำคัญต่างๆ อาทิ เช่น Security Policy และ Security Incident Management ซึ่งมีวัตถุประสงค์ของการบริหารความเสี่ยงระบบสารสนเทศ คือการลดความเสี่ยง (Risk Reduction) ให้อยู่ในจุดที่ยอมรับได้ (Risk Acceptance Level) โดยมีสมมุติฐานเหมือนกันคือ "เราไม่สามารถลดความเสี่ยงให้เท่ากับศูนย์ได้ แต่เราสามารถบริหารจัดการความเสี่ยงให้อยู่ในจุดที่เรายอมรับในความเสียหายที่เกิดขึ้นได้ และสามารถทำให้องค์กรดำเนินงานได้ต่อเนื่องอย่างไม่ติดขัด" ดังนั้น ควรเลือกวิธีการจัดการความเสี่ยงให้เหมาะกับโครงสร้างและทรัพยากรของหน่วยงาน และวิธีการต่างๆ หรือกิจกรรมดังกล่าวต้องมีการในลักษณะวงจร (Cycle) ที่เคลื่อนหมุนอยู่เสมอ กิจกรรมเหล่านี้ต้องถูกเฝ้าระวังหรือตรวจสอบ ตรวจประเมิน ทบทวนอยู่เป็นประจำ



7.2.5 ประเมินผลการดำเนินงาน

1) คณะทำงานประชุมพิจารณาผลการดำเนินงานตามแผนปฏิบัติการบริหารจัดการความเสี่ยงด้าน ICT ถึงผลสำเร็จในขั้นตอนต่างๆ ผลกระทบ ปัญหาอุปสรรคที่พบระหว่างดำเนินงาน

2) สรุปผลการพิจารณา ผลการประเมิน จัดทำเป็นรายงานเสนอผู้บริหารหน่วยงานรับทราบ

7.2.6 เฝ้าระวังความเสี่ยงและบูรณาการแผน

1) คณะทำงานวิเคราะห์และทบทวนผลการดำเนินงานร่วมกับแผนปฏิบัติการที่ผ่านมาเพื่อหาแนวทางปรับปรุง หรือบูรณาการแผนปฏิบัติการให้มีความเหมาะสมกับโครงสร้างหน่วยงาน ทรัพยากรของหน่วยงานและเทคโนโลยีสารสนเทศที่มีการเปลี่ยนแปลง ทันสมัย ในปัจจุบัน

2) คณะทำงานนำผลการวิเคราะห์และทบทวน มาใช้เป็นข้อมูลพื้นฐานเพื่อเข้าสู่กระบวนการระบุความเสี่ยงอีกครั้ง

3) ควบคุม กำกับ และติดตามให้ยังคงดำเนินการตามมาตรฐานการบริหารความเสี่ยงเทคโนโลยีสารสนเทศครบทุกขั้นตอนอย่างต่อเนื่อง

8. ระบบการติดตามและประเมินผลการใช้คู่มือ

ไม่มี

9. เอกสารอ้างอิง

9.1 นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารกระทรวงสาธารณสุข

9.2 นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงสาธารณสุข

9.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

9.4 ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

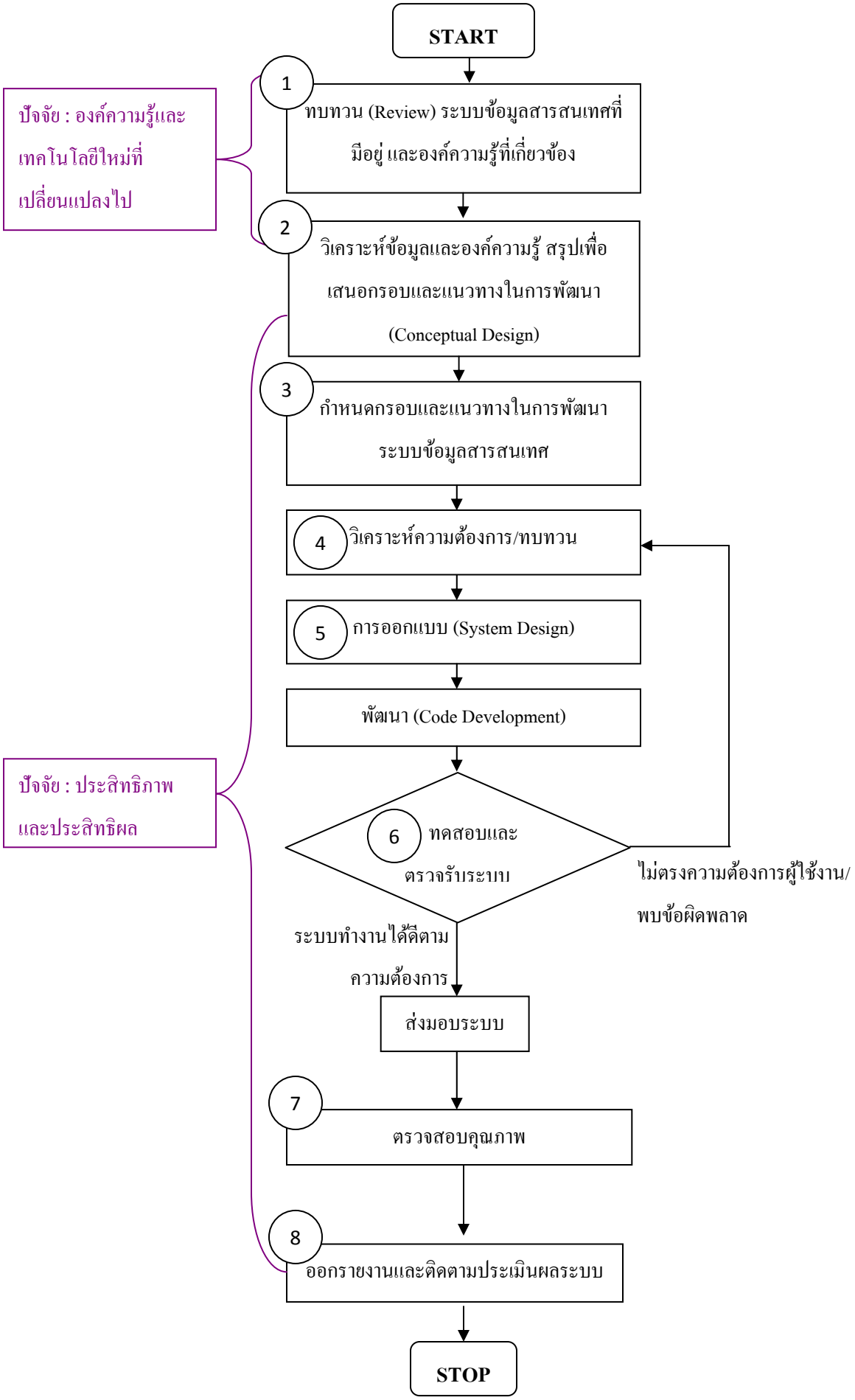
9.5 คู่มือและข้อปฏิบัติสำหรับ USER สป.สธ.

10. แบบฟอร์มที่ใช้

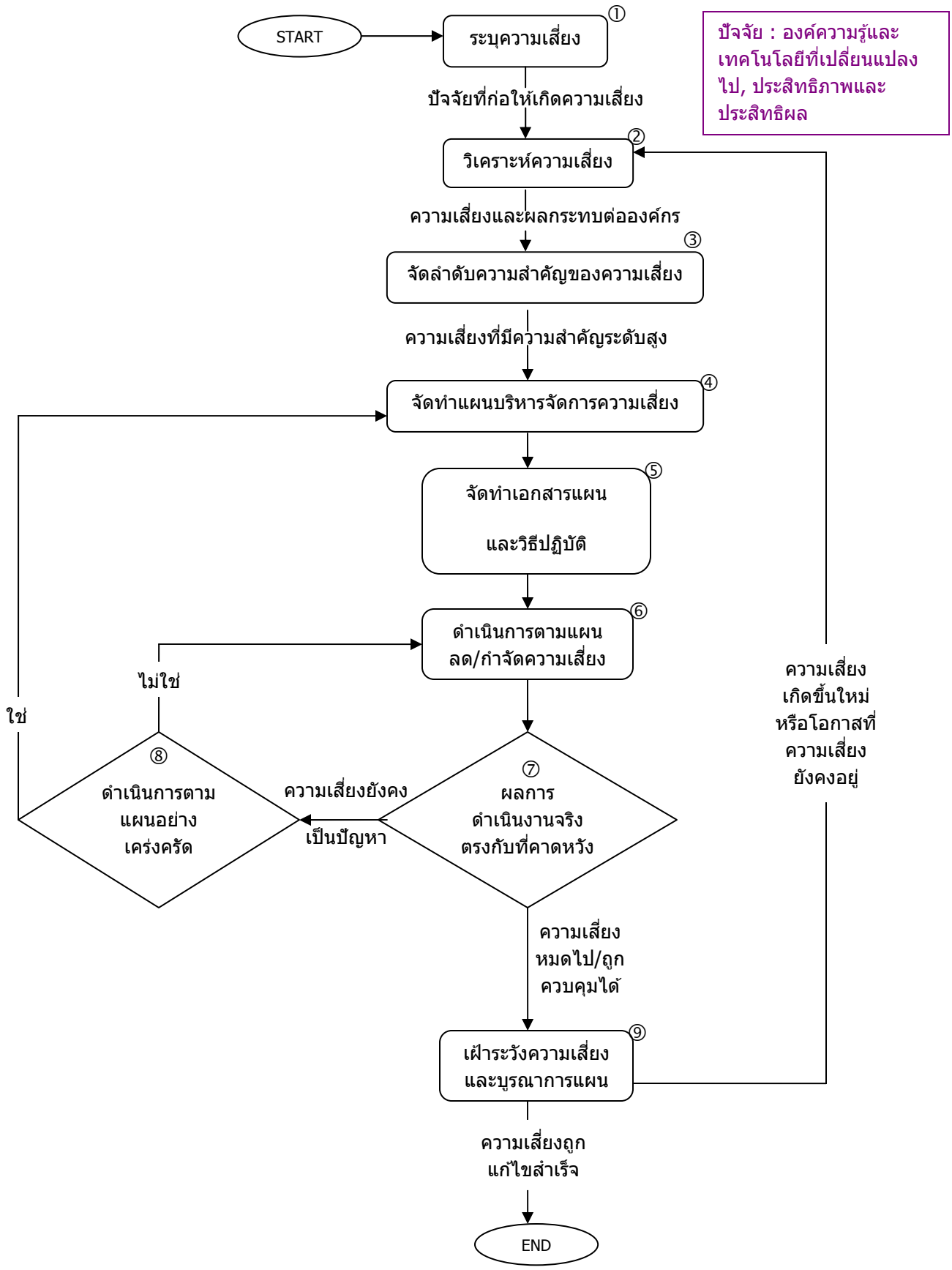
10.1 แบบประเมินความเสี่ยงระบบฐานข้อมูลและสารสนเทศ (Admin Risk Report-01)

10.2 แบบตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ (User Maintenance 01)

10.3 แบบบันทึกการสำรองข้อมูลระบบฐานข้อมูลและสารสนเทศ (Admin Backup Form)

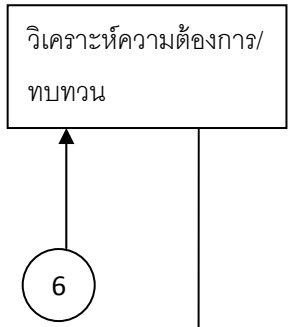
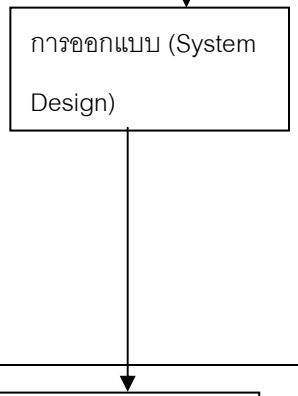
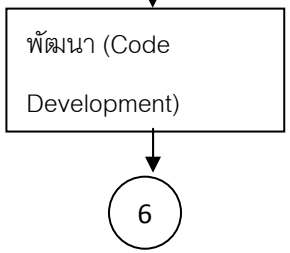

START
1
ทบทวน (Review) ระบบข้อมูลสารสนเทศที่มีอยู่ และองค์ความรู้ที่เกี่ยวข้อง
ปัจจัย : องค์ความรู้และเทคโนโลยีใหม่ที่เปลี่ยนแปลงไป
2
วิเคราะห์ข้อมูลและองค์ความรู้ สรุปเพื่อเสนอกรอบและแนวทางในการพัฒนา (Conceptual Design)
3
กำหนดกรอบและแนวทางในการพัฒนาระบบข้อมูลสารสนเทศ
4
วิเคราะห์ความต้องการ/ทบทวน
5
การออกแบบ (System Design)
พัฒนา (Code Development)
ปัจจัย : ประสิทธิภาพและประสิทธิผล
6
ทดสอบและตรวจรับระบบ
ไม่ตรงความต้องการผู้ใช้งาน/พบข้อผิดพลาด
ระบบทำงานได้ดีตามความต้องการ
ส่งมอบระบบ
7
ตรวจสอบคุณภาพ
8
ออกรายงานและติดตามประเมินผลระบบ
STOP

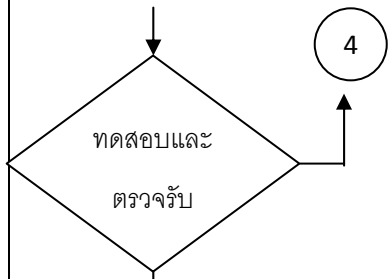
ภาคผนวก 2 : การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ



ภาคผนวก 3 รายละเอียดวิธีปฏิบัติกระบวนการพัฒนาระบบข้อมูลสารสนเทศและความรู้

ลำดับ	ขั้นตอนปฏิบัติ	รายละเอียดวิธีปฏิบัติ	ระยะเวลา
1	ทบทวน (Review) ระบบข้อมูลสารสนเทศที่มีอยู่ และองค์ความร้ที่เกี่ยวข้อง	- ทบทวนระบบข้อมูลและสารสนเทศที่มีอยู่ และองค์ความรู้ที่เกี่ยวข้องกับกระบวนการด้านสุขภาพทั้งในและนอกกระทรวงสาธารณสุข และต่างประเทศ ทั้งทางเว็บไซต์ เอกสาร หรือการสัมภาษณ์ผู้เชี่ยวชาญ (ความถี่ของการทบทวน) ทบทวน master plan ประจำปี,ทบทวนตามความจำเป็น เช่น การพัฒนาระบบใหม่ - ทบทวนสถานภาพของระบบเทคโนโลยีที่ใช้ในกระทรวงสาธารณสุข ทั้งส่วนกลางและจังหวัดเพื่อนำมาวิเคราะห์หากสามารถนำมาใช้ประโยชน์ร่วมกันได้	1 สัปดาห์
2	วิเคราะห์ข้อมูลและองค์ความรู้สรุปเพื่อเสนอกรอบและแนวทางในการพัฒนา (Conceptual Design)	- นำผลการทบทวนที่ได้มาสังเคราะห์เพื่อกำหนดระบบในองค์รวมและวิเคราะห์เพื่อกำหนดรายละเอียดหลัก - จัดทำข้อเสนอแนวทางและกรอบในการพัฒนาระบบข้อมูลและสารสนเทศ	1 สัปดาห์
3	กำหนดกรอบและแนวทางในการพัฒนาระบบข้อมูลสารสนเทศ 4	- ตั้งคณะกรรมการ/คณะทำงานเพื่อพิจารณาข้อเสนอและแนวทางในการพิจารณา - กำหนดกำหนดแนวทางในการพัฒนาระบบข้อมูล โครงสร้างข้อมูล ประกอบด้วย - รายการข้อมูล - ชนิดข้อมูล - ขอบเขตข้อมูล - ระยะเวลา - หน่วยจัดเก็บ - ระดับการจัดเก็บ	2 สัปดาห์

ลำดับ	ขั้นตอนปฏิบัติ	รายละเอียดวิธีปฏิบัติ	ระยะเวลา
4		- จัดทำแผนภาพระบบข้อมูลสารสนเทศ (Data Flow Diagram) ตั้งแต่ input (ผู้ให้ข้อมูลสารสนเทศ) ⟶ กระบวนการ ⟶ output (ผู้ใช้ข้อมูลสารสนเทศ) - จัดทำผังงานระบบ (System Flowchart) เพื่อแสดงวิธีการ ขั้นตอนการทำงานและสิ่งต่าง ๆ ที่เกี่ยวข้องกับระบบ - ควรใช้หลักการพัฒนาแบบวิวัฒนาการ (Evolutionary Development) แบ่งย่อยช่วงเวลาของการพัฒนาเพื่อลดเวลาในการดำเนินการให้ครบวงจรการพัฒนา ทำให้มีโอกาสในการพัฒนาและทบทวน เพื่อเติมเต็มข้อบกพร่องต่างๆ ในการวิเคราะห์ความต้องการและออกแบบได้ดีขึ้น ปรับให้ตรงตามความต้องการเพิ่มเติมจากผู้ใช้งานให้ดีขึ้นในแต่ละวงรอบของการทำงาน และทำซ้ำตามกระบวนการหลายรอบ	2 สัปดาห์ หรือขึ้นอยู่กับความซับซ้อน/ความยากของระบบ
5		- จัดทำรายละเอียดของข้อมูลแต่ละรายการหรือแต่ละตัวชี้วัดเพื่อใช้เป็นคู่มือในการจัดเก็บข้อมูลให้เป็นมาตรฐานเดียวกัน - จัดทำโครงสร้างฐานข้อมูลรวมทั้งรูปแบบของผลลัพธ์ที่ต้องการ (Output) การกำหนดรายละเอียดขั้นตอนการประมวลผล (Process Details), ตารางข้อมูล (Table), - ออกแบบระบบในส่วนของการป้อนข้อมูล (Input), รายละเอียดขั้นตอนการประมวลผล (Process Details) การจัดเก็บข้อมูล (Stored), โครงสร้างการจัดเก็บแฟ้มข้อมูล (File Structure), เครื่องมือที่ใช้ในการจัดเก็บข้อมูล (Storage Device) การสำรองข้อมูล (Backup) การออกแบบตัวเครื่องและอุปกรณ์ประกอบต่าง ๆ (Hardware) เพื่อรองรับกับโปรแกรม (Software) ที่พัฒนาขึ้น	3 สัปดาห์ หรือขึ้นอยู่กับความซับซ้อน/ความยากของระบบ
		นำสิ่งต่าง ๆ ที่วิเคราะห์และออกแบบมาแล้วจากขั้นที่ 4 และ 5 มาสร้างโปรแกรม/ระบบงาน/ระบบข้อมูลสารสนเทศ	ขึ้นอยู่กับความซับซ้อน/ความยากของระบบ

ลำดับ	ขั้นตอนปฏิบัติ	รายละเอียดวิธีปฏิบัติ	ระยะเวลา
6		- ทดสอบการทำงานของระบบก่อนจะนำไปใช้งานจริงและผู้ใช้งานควรใช้ข้อมูลที่ปฏิบัติงานจริงเพื่อดูผลลัพธ์ที่ได้ว่าถูกต้องและตรงตามความต้องการของผู้ใช้หรือไม่ - เมื่อพบว่ามีข้อผิดพลาดเกิดขึ้นจากการทำงานของระบบจะต้องมีการปรับแก้และบำรุงรักษาระบบ กลับไปขั้นที่ 4 วิเคราะห์ความต้องการ	2 สัปดาห์ หรือขึ้นอยู่กับความซับซ้อน/ความยากของระบบ
	การส่งมอบระบบ	- มีการทำเอกสารประกอบ ได้แก่ คู่มือสำหรับโปรแกรมเมอร์ใช้ในการแก้ไขและบำรุงรักษาระบบ - คู่มือประกอบการใช้งานของผู้ใช้ (User Documentation) หรือ - Training ให้ User เพื่อใช้งาน	2 สัปดาห์
7	ตรวจสอบคุณภาพ	- ตรวจสอบคุณภาพ (ความครบถ้วน ถูกต้องของฐานข้อมูล) ที่กำหนด - user friendly (เป็นมิตรกับผู้ใช้)	2 สัปดาห์
8	ออกรายงานและการติดตามประเมินผล	- ทดสอบการสั่งทำรายงานจากระบบข้อมูลสารสนเทศและความรู้ - สอบถามความพึงพอใจจากผู้ใช้งานในระดับต่างๆ	3 – 9 เดือน

ภาคผนวก 4 รายละเอียดวิธีปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ	ขั้นตอนปฏิบัติ	รายละเอียดวิธีปฏิบัติ	ระยะเวลา
1	**ระบุความเสี่ยง**	- แต่งตั้งคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข - แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ - ทบทวนรายชื่อคณะทุกปี - ประชุมคณะทำงาน/คณะกรรมการ เพื่อระบุความเสี่ยงและปัจจัยที่ก่อให้เกิดความเสี่ยง	2 สัปดาห์
2	**วิเคราะห์ความเสี่ยง** ⑨	- นำรายการความเสี่ยงมาวิเคราะห์ถึงผลกระทบและโอกาสเกิด (ความเสี่ยงที่ยังคงเหลืออยู่ และความเสี่ยงที่อาจเกิดขึ้นใหม่ตามสภาพปัจจัยแวดล้อม/เทคโนโลยีที่เปลี่ยนแปลงไป) - พิจารณาวัตถุประสงค์ ภารกิจ ความสำเร็จด้านเทคโนโลยีสารสนเทศและการสื่อสาร และความเสียหายที่ยอมรับได้ ร่วมด้วย	1 สัปดาห์
3	**จัดลำดับความสำคัญของความเสี่ยง**	- ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ เพื่อจัดลำดับความสำคัญ/ความรุนแรงของความเสี่ยงที่อาจเกิดขึ้น - จำแนกความเสี่ยงออกเป็น หลีกเลี่ยงได้ ยอมรับได้ ควบคุมได้ และถ่ายโอนได้	3 วัน
4	**จัดทำแผนบริหารจัดการความเสี่ยง** ⑧ ⑤	- จัดทำ/ทบทวนปรับปรุงแผน ดังนี้ - ระเบียบปฏิบัติ/นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ - แผนบริหารจัดการความเสี่ยงด้าน ICT ของสำนักงานปลัดกระทรวงสาธารณสุข รวมทั้ง แผนปฏิบัติการ และ แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) กรณีที่ดำเนินการตามแผนอย่างเคร่งครัดแล้วแต่ความเสี่ยงยังคงเป็นปัญหาอยู่ ต้องกลับมาทบทวนและปรับปรุงแผนให้เหมาะสม	1 เดือน

ลำดับ	ขั้นตอนปฏิบัติ	รายละเอียดวิธีปฏิบัติ	ระยะเวลา
5	**จัดทำเอกสารแผนและวิธีปฏิบัติ**	- จัดทำเอกสารแผนต่างๆ และวิธีปฏิบัติหรือคู่มือการปฏิบัติเพื่อค้นหา และจัดการความเสี่ยง - ถ่ายทอดแผนและวิธีปฏิบัติ ให้ทุกหน่วยงานรับทราบและถือปฏิบัติอย่างจริงจัง (แจ้งเวียนหนังสือ/ประชุม)	2 สัปดาห์
6	**ดำเนินการตามแผนลด/กำจัดความเสี่ยง** ⑧	- ผู้แทน(ด้าน ICT)ของหน่วยงาน ถ่ายทอดระเบียบ/แผนและวิธีปฏิบัติให้แก่เจ้าหน้าที่ทุกคนในหน่วยงาน รับทราบและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ - ทุกหน่วยงานส่วนกลาง สังกัด สป.สธ. ดำเนินการตามแผน และวิธีปฏิบัติ/คู่มือ - จัดหาอุปกรณ์/เครื่องมือ เพื่อป้องกัน และจัดการความเสี่ยง ICT ที่อาจเกิดขึ้นกับเครือข่ายคอมพิวเตอร์ เช่น Firewall , Anti-virus Server - หากความเสี่ยงยังคงเป็นปัญหา เพราะการดำเนินการไม่เคร่งครัด จะต้องกลับมาดำเนินการตามแผนอย่างเคร่งครัด	6 – 9 เดือน
7	**ผลการดำเนินงานจริงตรงกับที่คาดหวัง** ⑨	- ทุกหน่วยงานส่วนกลาง สังกัด สป.สธ. ดำเนินการตามแผนบริหารความเสี่ยง และค้นหา/ตรวจสอบ ผลการดำเนินงานว่าตรงกับที่คาดหวังไว้หรือไม่ - กรณีความเสี่ยงยังคงเป็นปัญหา ให้ดำเนินการขั้นที่ 8 - กรณีความเสี่ยงหมดไปหรือควบคุมความเสี่ยงให้อยู่ในสถานะยอมรับได้ ให้ดำเนินการขั้นตอนที่ 9	6 – 9 เดือน
8	④ ⑥ **ดำเนินการตามแผนอย่างเคร่งครัด**	- ตรวจสอบว่าได้ดำเนินการตามแผนอย่างเคร่งครัดแล้วหรือไม่ ถ้าดำเนินการอย่างเคร่งครัดแล้ว แต่ความเสี่ยงยังคงเป็นปัญหาอยู่ ให้กลับไปทบทวน/ปรับปรุง แผนบริหารจัดการความเสี่ยงใหม่อีกครั้ง ในขั้นตอนที่ 4 ให้เหมาะสมกับสภาพปัจจัยแวดล้อม องค์ความรู้และเทคโนโลยีใหม่ๆที่เปลี่ยนแปลงไป แต่ถ้ายังดำเนินการไม่เคร่งครัดอย่างจริงจัง ให้กลับเข้าสู่ขั้นตอนที่ 6	6 – 9 เดือน
9	⑦ ② **เฝ้าระวังความเสี่ยงและบูรณาการแผน**	- ทุกหน่วยงานดำเนินการตามแผนเพื่อเฝ้าระวังความเสี่ยงต่อไป - บูรณาการ แผนบริหารจัดการความเสี่ยง โดยนำประสบการณ์ในการจัดการความเสี่ยงที่ผ่านมา และความเสี่ยงที่เกิดขึ้นใหม่ หรือโอกาสที่ความเสี่ยงยังคงอยู่ มาร่วมพิจารณาปรับปรุงแผนและวิธีการให้เหมาะสมกับสภาพปัจจัยของ สป.สธ. และองค์ความรู้/เทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไปในปัจจุบัน (กลับเข้าสู่ขั้นตอนที่ 2) - กรณีความเสี่ยงถูกแก้ไขสำเร็จ ทั้งหมดจึงจบกระบวน แต่เนื่องจากปัจจัยแวดล้อมที่เปลี่ยนแปลงตลอดเวลา จึงต้องเฝ้าระวังอย่างต่อเนื่อง	12 เดือน