แผนบริหารความเสี่ยงฐานข้อมูลและสารสนเทศ
กรมการพัฒนาชุมชน พ.ศ. ๒๕๖๑ – ๒๕๖๒

๑. หลักการและเหตุผล

ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน เป็นศูนย์กลางในการจัดเก็บรักษาระบบข้อมูลสารสนเทศที่สำคัญต่าง ๆของหน่วยงานในสังกัดกรมการพัฒนาชุมชนสนับสนุนข้อมูลในการบริหารงานพัฒนาชุมชนที่ใช้ประกอบการตัดสินใจของผู้บริหารการพัฒนาระบบฐานข้อมูลสารสนเทศได้กระทำอย่างต่อเนื่องโดยมีระบบงานหลักดังนี้ ระบบข้อมูลพื้นฐาน (Data System) ระบบโปรแกรมสารสนเทศ (Software System) ระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (Hardware System) ระบบบุคลากร/เจ้าหน้าที่ (Peopleware System) และระบบเครือข่าย (Network System)

ศูนย์สารสนเทศเพื่อการพัฒนาชุมชนมีหน้าที่หลักในการดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมการพัฒนาชุมชนจำเป็นต้องมีแนวทางและแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยให้ความสำคัญอย่างยิ่งต่อการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Management) และการติดตามทบทวนแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการพัฒนาชุมชนเพราะหากมีการวางแผนจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพแล้ว สามารถลดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นตามสภาวการณ์ต่างๆ และอำนวยความสะดวกในการดำเนินการได้ ซึ่งสอดคล้องกับกรอบการปฏิบัติงานราชการ ที่มีแนวทางป้องกันและแก้ไขความเสี่ยงที่อาจจะเกิดขึ้นอันจะช่วยให้การบริหารงานราชการและการให้บริการแก่ประชาชนได้อย่างมีประสิทธิภาพสูงสุด

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ตามพระราชกฤษฎีว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์เป็นการเพิ่มโอกาสและช่วยให้องค์กรส่วนราชการบรรลุเป้าประสงค์และพันธกิจที่ตั้งไว้และเป็นการพัฒนาผลการปฏิบัติงานขององค์กรส่วนราชการที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่า ตลอดจนสามารถพัฒนาคุณภาพบริการที่ให้กับประชาชนทั่วไป

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๒.๑ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศของกรมการพัฒนาชุมชน

๒.๒ เพื่อให้มีแผนควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๓ เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุดและลดโอกาสความเสียหายที่อาจเกิดขึ้น

๒.๔ เพื่อเป็นแนวทางการดำเนินการกำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศของกรมการพัฒนาชุมชน ให้เจ้าหน้าที่ที่เกี่ยวข้องนำไปใช้ประโยชน์

๓. ทรัพยากรด้านเทคโนโลยี(IT Resources)

๓.๑ ข้อมูล(Data)รวมความถึง ข้อมูลในรูปแบบต่างๆทั้งที่มีโครงสร้างและไม่มีโครงสร้าง ข้อมูลด้านกราฟฟิคและข้อมูลที่เกี่ยวข้อง

๓.๒ ระบบงาน(Application System)ไ ด้แก่ ขั้นตอนและกระบวนการปฏิบัติงานทั้งที่ทำด้วยมือและโปรแกรมคอมพิวเตอร์

๓.๓ เทคโนโลยี (Technology) ได้แก่เครื่องคอมพิวเตอร์(hardware) โปรแกรมระบบ (OperatingSystems)ระบบบริหารฐานข้อมูล (Database Management System) ระบบเครือข่าย(Networking) และระบบมัลติมีเดีย

๓.๔ องค์ประกอบ(Facilities) ได้แก่ทรัพยากรต่างๆที่ใช้เป็นสถานที่ติดตั้งหรือจัดวางตลอดจนสาธารณูปโภคที่จำเป็นเพื่อการปฏิบัติงานของระบบสารสนเทศ

๓.๕ บุคลากร (People) ได้แก่ บุคคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงานสำหรับการดูแลและจัดทำระบบ

๔. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานในการบริหารจัดการการจัดเก็บข้อมูลการกำหนดการใช้เครื่องคอมพิวเตอร์ระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆการจัดทำและพัฒนาระบบเทคโนโลยีสารสนเทศในภาพรวมมุ่งหวังให้ระบบสารสนเทศช่วยในการดำเนินงานของหน่วยงานให้มีความสะดวกรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น แต่การนำเทคโนโลยีสารสนเทศมาใช้ย่อมมีความเสี่ยงหลายประการด้วยกันซึ่งการวางแผนและการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ จึงเป็นเรื่องสำคัญและควรมีการเตรียมการที่ดี

โดยหากหน่วยงานไม่มีการบริหารจัดการและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอก็อาจส่งผลกระทบต่อการดำเนินงานและสร้างความเสียหายต่อหน่วยงานได้ ทั้งในด้านการพัฒนาระบบราชการ บุคลากร ความคุ้มค่าทางงบประมาณดังนั้นการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศจะต้องมีทั้งการวางแผน การประเมินทั้งโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น และสามารถประเมินเป็นเชิงปริมาณหรือเชิงคุณภาพได้ กระบวนการที่ใช้ระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของโครงการเทคโนโลยีสารสนเทศขององค์กร

๕. ความเสี่ยงและแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวของกับระบบเทคโนโลยีสารสนเทศ สามารถแบ่งออกเป็น๖ประเภทดังนี้

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม
๒) ความเสี่ยงด้านบุคลากร
๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ
๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์
๕) ความเสี่ยงด้านระบบเครือข่าย
๖) ความเสี่ยงด้านข้อมูล

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

๕.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อมหมายถึงความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติ สิ่งที่มนุษย์กระทำขึ้นลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น

- วาตภัย,อุทกภัย,ฟ้าผ่า,น้ำท่วม
- กระแสไฟฟ้าขัดข้องเพลิงไหม้
- การไม่มีระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย (ServerRoom)

<u>การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม</u>มีประเด็นหลักดังนี้

๕.๑.๑ พิจารณาตำแหน่งของห้องคอมพิวเตอร์แม่ข่าย (ServerRoom)ที่จะเป็นที่จัดเก็บและติดตั้งระบบเทคโนโลยีสารสนเทศไว้ยังเครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และการกำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้าสายวงจรสายสัญญาณของระบบต่างๆ ต้องเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยงสูงรวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้นเช่นเครื่องปรับอากาศ ,ตู้Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย, หน้าต่างระบบความร้อน , ถังดับเพลิงเป็นต้น

๕.๑.๒ การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) ห้องคอมพิวเตอร์แม่ข่ายมีอุปกรณ์คอมพิวเตอร์ที่สำคัญเช่นเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงระบบสัญญาณเครือข่ายที่เชื่อมโยงไว้ในห้องคอมพิวเตอร์แม่ข่าย (ServerRoom) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบปฏิบัติการและอุปกรณ์ จึงต้องกำหนดสิทธิการเข้าออกห้องคอมพิวเตอร์แม่ข่าย โดยให้เฉพาะบุคคลที่ทีหน้าที่เกี่ยวข้องเท่านั้น ได้แก่

(๑) เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (ComputerOperation) งานเทคโนโลยีสารสนเทศเป็นผู้ควบคุมดูแลและรับผิดชอบ

(๒) เจ้าหน้าที่ดูแลระบบและซ่อมบำรุง (System Administrator and Maintain) เป็นผู้ควบคุมดูแลและรับผิดชอบ

(๓) เจ้าหน้าที่พัฒนาระบบระบบสารสนเทศ (Information Development Officer) เป็นผู้ควบคุมดูแลและรับผิดชอบกรณีที่มีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องคอมพิวเตอร์แม่ข่าย จะต้องมีการควบคุมอย่างรัดกุมและรอบคอบ เช่นกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบควบคุมดูแลการทำงานตลอดเวลาแจ้งให้เจ้าหน้าที่งานเทคโนโลยีสารสนเทศทราบก่อนทุกครั้งก่อนเข้าคอมพิวเตอร์แม่ข่าย เป็นต้น

๕.๑.๓ จัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะ โดยแบ่งออกเป็นสัดส่วนดังนี้ ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ส่วนเครื่องคอมพิวเตอร์ลูกข่าย (Clientzone) และส่วนของระบบเครือข่าย (Network Zone) เพื่อความสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์มีประสิทธิภาพมากขึ้น

๕.๑.๔ การจัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูลโดยเจ้าหน้าที่ของศูนย์ข้อมูลเช่น ส่วนที่ใช้เก็บรายงานต่างๆหรือข้อมูลที่งานเทคโนโลยีสารสนเทศได้จัดทำการสำรองข้อมูล (Backup) ไว้กรณีฉุกเฉินเมื่อข้อมูลที่จัดทำไว้เกิดการเสียหายโดยจัดเก็บไว้โดยเจ้าหน้าที่ของศูนย์สารสนเทศฯ

๕.๑.๕ การป้องกันความเสียหายโดยการวางระบบป้องกันไฟที่เหมาะสมจัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลากรณีฉุกเฉินเพื่อใช้ในการดับเพลิงเบื้องต้น

๕.๑.๖ การป้องกันความเสี่ยงจากระบบป้องกันไฟฟ้าขัดข้องทำได้โดยให้มีระบบป้องกันไฟฟ้ากระชากไม่ให้คอมพิวเตอร์แม่ข่ายได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้าอีกทั้งการติดตั้งระบบสายดิน (Ground) ที่ได้มาตรฐานอุปกรณ์ป้องกันไฟจัดให้มีระบบไฟฟ้าสำรองสำหรับคอมพิวเตอร์ทั้งแม่ข่ายและลูกข่ายเพื่อให้การดำเนินงานมีความต่อเนื่องกรณีไฟฟ้าดับหรือเกิดขัดข้องไม่สามารถใช้งานได้

๕.๑.๗ การป้องกันความเสี่ยงจากระบบควบคุมอุณหภูมิและความชื้นทำได้โดยให้มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศและค่าความชื้นให้มีระดับเหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์สิ่งแวดล้อมที่เหมาะสมที่คอมพิวเตอร์จะทำงานได้ดี นั้นอุณหภูมิและความชื้นจะต้องมีความเหมาะสม ดังนั้นห้องทำงานด้านคอมพิวเตอร์จึงควรเป็นห้องปรับอากาศที่มีประสิทธิภาพปราศจากฝุ่นละอองและความชื้นเพราะเครื่องคอมพิวเตอร์และข้อมูลที่อยู่ภายในคอมพิวเตอร์อาจได้รับความเสียหายจากการได้รับความร้อนสูงในส่วนของห้องคอมพิวเตอร์แม่ข่ายที่ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน มีเครื่องปรับอากาศเพื่อรักษาอุณหภูมิตลอด จึงจำเป็นต้องการบำรุงรักษาที่ถูกต้องและสม่ำเสมอทำให้เครื่องปรับอากาศมีอายุใช้งานได้ยาวนาน มีประสิทธิภาพสูงและประหยัดพลังงานไฟฟ้าตลอดเวลาโดยปฏิบัติดังนี้

- ทำความสะอาดแผ่นกรองอากาศทุก ๒ สัปดาห์ เพื่อให้เครื่องสามารถจ่ายความเย็นได้เต็มที่
- ทำความสะอาดแผงท่อทำความเย็นทุก ๓ เดือน เพื่อให้เครื่องทำความเย็นได้อย่างมีประสิทธิภาพ ทำความสะอาดพัดลมส่งลมเย็น เพื่อขจัดฝุ่นละอองที่จับทุกเดือน
- ทำความสะอาดแผงท่อระบายความร้อน ทุก ๑ เดือน เพื่อให้เครื่องสามารถนำความร้อนภายในห้องออกไปทิ้งให้แก่อากาศ ภายนอกได้อย่างมีประสิทธิภาพ
- หากปรากฏว่าเครื่องไม่เย็นเพราะสารทำความเย็นรั่วต้องรีบตรวจหารอยรั่วแล้วทำการแก้ไขโดยแจ้งช่างซ่อมบำรุง
- ตรวจสอบฉนวนหุ้มท่อสารทำความเย็นอย่างสม่ำเสมอ
- วางแผนการใช้ในการใช้งานในเวลากลางวันและกลางคืน

๕.๑.๘ ความเสี่ยงในเรื่องของงบประมาณที่จะดำเนินการอย่างได้ประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง

๕.๑.๙ ความเสี่ยงในเรื่องของการบริหารจัดการสามารถวางแผนบริหารความเสี่ยงและดำเนินการเพื่อลดความเสี่ยงได้ดังนี้

- จัดทำแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศ
- บริหารจัดการติดาม ควบคุม กำกับดูแลและให้คำปรึกษาแก้ไขปัญหาระบบ
- การจัดการ ประเมินผลแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศ
- ติดตามจัดทำควบคุมกำกับดูแลและให้คำแนะนำปรึกษาแก้ไขปัญหาระบบการจัดการและไหลเวียนเอกสารไร้กระดาษ (Paperless)
- ศึกษาวิเคราะห์และจัดทำระบบข้อมูลเพื่อการบริหารราชการในการสนับสนุนการตัดสินใจ ของผู้บริหารระดับสูง (Executive Information System)
- ศึกษาวิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อการวางแผนและคาดการณ์แนวโน้มความต้องการบุคลากรด้านเทคโนโลยีสารสนเทศ
- ให้บริการฝึกอบรมเพื่อพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศของบุคลากร

ความเสี่ยงด้านบุคลากร

๕.๒ ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงการวางแผน การตรวจสอบการทำงานการมอบหมายหน้าที่ และสิทธิของบุคลากรคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วนเพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ตลอดจนบุคคลภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อมล้วนแต่เป็นความเสี่ยง ความเสี่ยงด้านบุคลากรเป็นความเสี่ยงหนึ่งที่สำคัญดังนั้นจึงควรมีแนวทางและการวางแผนที่จะกำกับดูแลการบริหารจัดการและควบคุมความเสี่ยงด้านบุคลากรของกรมการพัฒนาชุมชนอย่างจริงจัง

<u>การบริหารจัดการความเสี่ยงด้านบุคลากร</u> มีประเด็นหลักดังนี้

๕.๒.๑ กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศ การบริหารจัดการด้านบุคลากร การแต่งตั้งเจ้าหน้าที่ฯ ที่มีความเหมาะสม (มีความรู้ความสามารถและประสบการณ์ด้านคอมพิวเตอร์ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีด้านการรักษาความปลอดภัยระบบฯและสามารถถ่ายทอดความรู้นั้น ให้แก่ผู้ใช้งานระบบฯของหน่วยงานได้อย่างมีประสิทธิภาพ) เมื่อมีการปรับและแจ้งรายชื่อผู้รับผิดชอบ (เจ้าหน้าที่รักษาความปลอดภัยระบบฯและผู้ดูแลระบบฯ)ที่มีการเปลี่ยนแปลง เช่นโยกย้ายลาออกฯลฯจะต้องแจ้งให้ทราบเพื่อประโยชน์ในการบริหารบุคลากรการติดต่อประสานแจ้งเตือนภัยฝึกอบรมและ การรักษาความปลอดภัยระบบสารสนเทศอย่างมีประสิทธิภาพหากบุคลากรด้านเทคโนโลยีสารสนเทศไม่มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอก็อาจทำให้เกิดความเสี่ยงด้านโครงสร้างการบริหารงานได้ โดยให้ความสำคัญในเรื่องของการกำหนดโครงสร้างการแบ่งแยก อำนาจหน้าที่การกำหนดนโยบายและขั้นตอนการปฏิบัติงาน และการกำกับดูแลควบคุมการปฏิบัติงานเป็นหลักดังนี้

การกำหนดโครงสร้างการแบ่งแยกอำนาจหน้าที่และความรับผิดชอบงานเทคโนโลยีสารสนเทศไม่ได้มอบหมายให้คนหนึ่งคนใดรับผิดชอบตลอดกระบวนการ แต่จะกระจายความรับผิดชอบและภารกิจที่ดำเนินการเพื่อป้องกันความเสี่ยงด้านบุคลากร ความเข้าใจคลาดเคลื่อน และความซับซ้อนของการทำงาน โดยมีการกำหนดโครงสร้างและ แบ่งแยกอำนาจหน้าที่ความรับผิดชอบดังนี้

๑) ผู้อำนวยการศูนย์สารสนเทศฯ ควบคุมกำกับดูแลการปฏิบัติงานของเจ้าหน้าที่ในสังกัดเกี่ยวกับงานพัฒนาระบบสารสนเทศรวมทั้งบริหารจัดการศูนย์สารสนเทศเพื่อการบริหารและการวางแผนการจัดให้มีและให้บริการเครือข่ายเชื่อมโยงฐานข้อมูลสารสนเทศภายในและให้บริการแลกเปลี่ยนข้อมูลสารสนเทศและงานอื่นๆที่ได้รับมอบหมาย

๒)เจ้าหน้าที่เทคโนโลยีสารสนเทศประกอบด้วย เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (ComputerOperation) ปฏิบัติงานปรับปรุงข้อมูลข่าวสารที่เผยแพร่ในเว็บไซต์ www.cdd.go.th, เจ้าหน้าที่ดูแลระบบและซ่อมบำรุง (System Administrator and Maintain) ปฏิบัติงานในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server Computer) ดูแลการกระจายสัญญาณอินเตอร์เน็ตให้ครอบคลุมทุกหน่วยในหน่วยงานส่วนกลางและส่วนภูมิภาครวมตลอดถึง จัดการดูแลรักษาซ่อมบำรุง คอมพิวเตอร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพและเจ้าหน้าที่พัฒนาระบบสารสนเทศ (Information Development Officer) ปฏิบัติงานพัฒนาระบบข้อมูลสารสนเทศเพื่อการพัฒนางานพัฒนาระบบฐานข้อมูล โดยประสาน รวบรวม วิเคราะห์ข้อมูล ออกแบบและจัดทำฐานข้อมูลเพื่อการวางแผนพัฒนา

๕.๒.๒ การว่าจ้าง/จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการด้านระบบเทคโนโลยีสารสนเทศเพราะเป็นผู้มีความรู้ความชำนาญเฉพาะทางมีเครื่องมือและเทคโนโลยีที่พร้อมใช้และทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศเฉพาะด้านมากกว่าภาคราชการ โดยการว่าจ้างบุคลากรภายนอกจากนี้ก็จะมีความเสี่ยงในเรื่องของความรู้ความเข้าใจในระบบราชการและผลสัมฤทธิ์ที่เกิดจากการทำงานอีกทั้งในแง่ของความคุ้มค่าของการใช้จ่ายงบประมาณ ดังนั้นแนวทางในการวางแผนบริหารความเสี่ยงของการว่าจ้างบุคลากรภายนอกนี้ผู้รับผิดชอบในประเด็นต่างๆ ต้องเป็นผู้เข้ามากำกับดูแลตั้งแต่เริ่มกระบวนการและต่อเนื่องโดยหลักการบริหารจัดการที่ดี อีกทั้งรักษาผลประโยชน์ของทางราชการให้มากที่สุด

๕.๒.๓ บุคลากรของภาคราชการ ขาดความรู้ความเข้าใจในเรื่องของระบบเทคโนโลยีสารสนเทศโดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรมและนวัตกรรมทำให้เกิดช่องว่างในการที่จะประสานงานและ รับผิดชอบงานอย่างมีประสิทธิภาพดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงในประเด็นนี้โดยการส่ง เจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศรวมถึงการรับบุคลากรที่มีความรู้ความเข้าใจด้านระบบ เทคโนโลยีสารสนเทศมาปฏิบัติงานในหน่วยงานราชการมากยิ่งขึ้น

๕.๒.๔ แผนการบริหารความเสี่ยงด้านบุคลากรคือ ต้องมีการฝึกอบรมในด้านที่เกี่ยวข้องกับระบบฐานข้อมูลสารสนเทศสำหรับบุคลากรของกรมใน ๒ ระดับ คือ ระดับผู้ดูแลระบบ (Administrator) และผู้ใช้งานทั่วไป (User) ทำให้บุคลากรของหน่วยงานสามารถใช้งานระบบสารสนเทศดูแลปรับปรุง และพัฒนาระบบได้เป็นการสนับสนุนบุคลากรทางคอมพิวเตอร์ รวมทั้งผู้ใช้งานให้มีความรู้ด้านการรักษา ความปลอดภัยระบบได้อย่างมีประสิทธิภาพ

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ

๕.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเป็นความเสี่ยงที่เกิดจากการทำงานผิดพลาดของอุปกรณ์ ช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆเช่นไวรัสคอมพิวเตอร์เป็นต้น

<u>การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ</u> มีประเด็นหลัก ดังนี้

๕.๓.๑ ความเสี่ยงในเรื่องของจัดหาอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมกับแผนงาน/โครงการ และองค์กร (Planning and Organization) ซึ่งควรให้มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆให้ได้ตาม มาตรฐานของอุปกรณ์คอมพิวเตอร์จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการและเหมาะสมกับงบประมาณ

๕.๓.๒ ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Support) ซึ่งการลดโอกาสที่จะเกิดความเสี่ยงในกรณีได้แก่

(๑) การบำรุงรักษาและลดความเสี่ยง

- มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และการดูแลอย่างถูกต้องและต่อเนื่อง
- ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว
- การใช้แผนซีดีหรือ Handy Drive ควรตรวจสอบไวรัสก่อนใช้ทุกครั้ง
- การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ

- ควรปัดฝุ่นหรือทำความสะอาดเครื่องคอมพิวเตอร์ให้ใหม่อยู่เสมอ เพราะเมื่อมีฝุ่นเข้าสู่เครื่องคอมพิวเตอร์มากๆจะทำให้เครื่องคอมพิวเตอร์ร้อนจัดได้ง่าย เป็นสาเหตุของอาการเครื่องค้างหรือเครื่องรวนได้

- โปรแกรม Windows จะมีคำสั่งในการบำรุงรักษาเครื่อง (Maintenance) ซึ่งผู้ดูแลระบบควรใช้คำสั่งนี้เป็นประจำ

- การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ

- การสำรองข้อมูล (Backup) ข้อมูลระบบสารสนเทศ

- การบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วงได้แก่ระบบปฏิบัติการคอมพิวเตอร์,ระบบเครือข่ายและการใช้งานและประสิทธิผลของเครื่องคอมพิวเตอร์อุปกรณ์เทคโนโลยีสารสนเทศ

(๒) การรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย (Server)

- กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าParameter ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

- ทำการทดสอบ System Softwareเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

- ติดตั้งโปรแกรมระบบรักษาความปลอดภัยเช่น โปรแกรม Personal Firewall

- กำหนดบุคคลรับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆของโปรแกรมคอมพิวเตอร์ที่ติดตั้งในเครื่องคอมพิวเตอร์แม่ข่ายอย่างชัดเจน

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

๕.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่างๆที่ได้จัดทำและพัฒนาขึ้นสาหรับโครงการด้านเทคโนโลยีสารสนเทศ รวมถึงโปรแกรมประยุกต์ อื่นๆ ที่ใช้ประกอบการใช้โปรแกรมและระบบงานตัวอย่างเช่นการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง, ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม,โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่งและการถูกผู้ไม่หวังดีทำลายระบบ (Hacker) เป็นต้น

<u>การบริหารจัดการความเสี่ยงด้านโปรแกรมคอมพิวเตอร์</u> มีประเด็นหลัก ดังนี้

๕.๔.๑ มีการพัฒนามาตรฐานและการบริการโปรแกรมคอมพิวเตอร์

- พัฒนาและปรับปรุงมาตรฐาน Hardware,Software,Peopleware,Data และ Network ให้เป็นฐานข้อมูลกลางของงานเทคโนโลยีสารสนเทศกรมการพัฒนาชุมชนและเป็นไปในทิศทางเดียวกัน

- สร้างกลไกการจัดการฐานข้อมูลการจัดการระบบสารสนเทศเพื่อการบริหารจัดการของหน่วยงานให้ครบถ้วนและครอบคลุมมากยิ่งขึ้น

- พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลของกรม ให้มีมาตรฐานและแบ่งสรรการใช้ทรัพยากรฐานข้อมูลจากโปรแกรมรวมกันได้

- พัฒนาโปรแกรมให้สามารถจัดเก็บรวบรวมประมวลข้อมูลศึกษาวิเคราะห์เพื่อการนำเสนอ และสนับสนุนการบริหารราชการและพัฒนา ส่งเสริมบำรุงรักษาระบบและการเผยแพร่ข้อมูลข่าวสารของจังหวัดได้ ในลักษณะของ Web Application เพื่อความสะดวกในการใช้งานและแสดงผล

ความเสี่ยงด้านระบบเครือข่าย

๕.๕ ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่างๆที่เกิดขึ้นกับระบบเครือข่ายขององค์กร ทั้งระบบอินทราเน็ต (Intranet) และอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล Protocol TCP/IP ด้วยเช่นความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่ายความเสี่ยงจากกการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ

<u>การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย</u> มีประเด็นหลัก ดังนี้

๕.๕.๑ ความเสียหายที่เกิดจากระบบเครือข่ายการเฝ้าระวังและตรวจสอบระบบเครือข่าย และการจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่ายได้มีระบบการติดตามและเฝ้าดูการใช้เครือข่ายภายในและการเข้าออก Internet ทุกวัน รวมทั้งการสร้าง Firewall เพื่อป้องกันการเข้าถึงและการโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูลระบบ Web Server เป็นต้น

๕.๕.๒ พัฒนาระบบงานด้านเครือข่าย โดยการพัฒนาบริหาร ควบคุมกำกับดูแลและบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายสารสนเทศพื้นฐานพัฒนาระบบการให้บริการเครือข่ายการเพิ่มการรักษาและคุ้มครองความปลอดภัยข้อมูล ผ่านระบบเครือข่าย

๕.๕.๓ เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ภายใน ให้มีความเสถียรและมีประสิทธิภาพรองรับกับปริมาณฐานข้อมูล และการเคลื่อนไหวของฐานข้อมูล

๕.๕.๔ หน่วยงานภายในศูนย์สารสนเทศเพื่อการพัฒนาชุมชนต้องร่วมวิเคราะห์ออกแบบวางแผนการจัดการระบบโครงข่ายร่วมกันอย่างบรูณาการและมีการให้คำปรึกษา แนะนำและแก้ไขปัญหาในการพัฒนาเครือข่าย

๕.๕.๕ มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (NetworkSecurity) มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (AccessRisk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูล หรือ การทำงานของระบบเครือข่ายที่จะมีผลถึงระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้องการป้องกันการบุกรุก ผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคลไวรัสมิให้เข้าถึงหรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์โดยมีเนื้อหารายละเอียดเกี่ยวกับแนวในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์เครื่องแม่ข่ายและระบบเครือข่าย

(๑) การบริหารจัดการข้อมูลบนเครือข่าย

- กำหนดชั้นความสำคัญในการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงการเข้าถึงข้อมูลผ่านระบบเครือข่าย
- ในการรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล
- กำหนดมาตรการรักษาความปลอดภัยข้อมูลเช่น กรณีนำเครื่องคอมพิวเตอร์ส่งซ่อมเป็นต้น

(๒) การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

- กำหนดสิทธิการเข้าถึงข้อมูลและระบบคอมพิวเตอร์เช่นสิทธิการใช้โปรแกรมระบบงาน คอมพิวเตอร์ (Application System) ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ
- กำหนดระยะเวลาการใช้งานของ User พร้อม Password และระงับการใช้งานทันทีเมื่อพ้นระยะเวลา

- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบ และมีชั้นความลับ

- ในกรณีที่มีความจำเป็นต้องให้สิทธิใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่างๆ ต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้งโดยบันทึกเหตุผลและความจำเป็น รวมถึงกำหนดระยะเวลาในการใช้งาน

(๓) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account)

(๔) การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงานในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน

๕.๕.๖ การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

(๑) กำหนดแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่นส่วนเครือข่ายภายในส่วนเครือข่ายภายนอก

(๒) ติดตั้งระบบป้องกันการบุกรุกเ ช่น Firewall ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก โดยการติดตั้งผ่านอุปกรณ์คอมพิวเตอร์ติดตั้งระบบป้องกันการบุกรุกในระบบเครือข่ายด้วยซอฟต์แวร์และฮาร์ดแวร์ให้แก่ระบบ Firewallซึ่งเป็นซอฟต์แวร์ทำหน้าที่เสมือนกับกำแพงกันไฟไม่ให้ลุกลามขยายตัวหากมีไฟไหม้เกิดขึ้น Firewall จะอาศัยคอมพิวเตอร์เครื่องหนึ่งเป็นด้านเข้าออกเครือข่ายและเป็นเสมือนกำแพงกันไฟและมีซอฟต์แวร์ที่ผู้ดูแลระบบจะติดตั้งและกำหนดรูปแบบการอนุญาตให้เข้าใช้เครือข่ายอินเทอร์เน็ต

(๓) จัดทำแผนผังเครือข่าย/แผนผังการเชื่อมโยงระบบเครือข่าย (Network Diagram) มีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งภายในและภายนอกและอุปกรณ์ให้เป็นปัจจุบันอยู่เสมอ

(๔) ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัสเป็นต้น

(๕) กำหนดบุคคลผู้รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของอุปกรณ์เครือข่าย

๕.๕.๗ การป้องกันไวรัสสำหรับระบบเครือข่าย

กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่องเช่นการติดตั้งซอฟต์แวร์ป้องกันไวรัสเป็นต้นการปกป้องระบบเครือข่ายสิ่งที่สำคัญอย่างยิ่ง คือ ผู้ใช้งานในระบบจะต้องคอยดูแลและป้องกันไม่ให้ตนเองเป็นช่องทางผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตามและหาวิธีการป้องกันและแก้ไขจุดบกพร่องของซอฟต์แวร์ที่ใช้งานเพราะไม่มีระบบเครือข่ายใดที่ปลอดภัยสมบรูณ์แบบ ดังนั้นจึงต้องมีระบบป้องกันที่ดีโดยมีวิธีการ ดังนี้

ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

- ☐ ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
- ☐ สร้างแผน Emergency Disk เพื่อใช้ในการกู้ระบบ
- ☐ อัพเดตข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดต
- ☐ เปิดใช้งาน Auto Protect
- ☐ ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
- ☐ ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ๑ ครั้ง

การป้องกันจากการเปิดไฟล์จากสื่อบันทึกข้อมูล (Media) ต่างๆ

- ☐ แผ่น CD เทปต่างๆ
- ☐ สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ☐ ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆที่น่าสงสัยเช่น .pifเป็นต้น
- ☐ ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

การป้องกันจากการเปิด E-Mail

- ☐ อย่าเปิดไฟล์E-Mail จากผู้ส่งที่ไม่รู้จักและไม่ทราบที่มา
- ☐ อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ
- ☐ ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที
- ☐ อัพเดตโปรแกรม E-Mail สม่ำเสมอ

การป้องกันจากการดาวน์โหลดจาก Internet

- ☐ ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่นMSN
- ☐ ไม่ควรเข้าWebsite ที่มากับE-Mail
- ☐ ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่น่าเชื่อถือ
- ☐ ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลด้านความปลอดภัยเสมอ
- ☐ หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น
- ☐ หลีกเลี่ยงการแชร์ไฟล์ประเภทPeer to Peer เนื่องจากมีโอกาสติดไวรัสสูง

๕.๕.๘ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

(๑) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

(๒) ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

(๓) หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับ หน่วยงาน ผู้ใช้งาน ต้องแจ้งต่อศูนย์สารสนเทศเพื่อการพัฒนาชุมชนโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

ความเสี่ยงด้านข้อมูล

๕.๖ ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงด้านระบบฐานข้อมูลได้แก่ ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล การโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ซึ่งมีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านระบบฐานข้อมูลและสารสนเทศ

ดังนั้น การรักษาความมั่นคงปลอดภัยของข้อมูลจึงเป็นเรื่องที่สำคัญข้อมูลสารสนเทศเป็นส่วนสำคัญสำหรับผู้บริหารที่จะนำมาเป็นเครื่องมือสำหรับการตัดสนใจในการวางแผน การจัดการข้อมูล (Management of Data and Communication) ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและComputerจ ากภัยต่างๆทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆจึงสำคัญและจำเป็นต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยีการรักษาความปลอดภัยด้านข้อมูลสารสนเทศของศูนย์สารสนเทศฯ มีแนวทางหลักดังนี้

๑. การจัดเก็บข้อมูล

๒. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

๔. การสำรองข้อมูลระบบคอมพิวเตอร์และการดตรียมพร้อมกรณีฉุกเฉิน (Back up and IT Contingency Plan)

๕. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

๖. การรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย (Information andNetwork)

๗. การบำรุงรักษาอุปกรณ์เครือข่ายและระบบคอมพิวเตอร์

<u>การบริหารจัดการความเสี่ยงด้านข้อมูล</u> มีประเด็นหลักดังนี้

๕.๖.๑ การจัดเก็บข้อมูลมีขั้นตอนปฏิบัติ ดังนี้

(๑) จัดแบ่ง ประเภทข้อมูล

- ข้อมูลสารสนเทศด้านบริหาร เช่น ข้อมูลบุคลากร ข้อมูลงบประมาณ เป็นต้น
- ข้อมูลสารสนเทศเพื่อการพัฒนาชุมชน ที่ให้บริการ เช่น ข้อมูลหมู่บ้านเศรษฐกิจพอเพียง ข้อมูลผู้นำชุมชน ข้อมูลสินค้า OTOP ข้อมูล จปฐ. กชช.๒ค เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๕) การกำหนดเวลาที่ได้เข้าถึงดังนี้

- ข้อมูลสารสนเทศด้านบริหารให้เป็นไปตามห้วงเวลาที่หน่วยงานประกาศ
- ข้อมูลสารสนเทศเพื่อการพัฒนาชุมชนสามารถเข้าถึงได้ ๒๔ ชั่วโมง

๕.๖.๒ การไม่กำหนดนโยบายด้านความปลอดภัยของระบบฐานข้อมูล (Database Security) เป็นอีกปัจจัยหนึ่งที่ทำให้เกิดความเสี่ยงการกำหนดนโยบายความปลอดภัยของระบบฐานข้อมูลเป็นการป้องกันผู้ไม่มีสิทธิเข้ามาใช้งานหรือแก้ไขข้อมูล และความสามารถในการป้องกันข้อมูลให้ถูกต้องครบถ้วนสมบูรณ์ โดยมีวัตถุประสงค์ ดังนี้

- เพื่อให้สามารถรักษาข้อมูลเป็นความลับได้ (Secrecy)
- เพื่อให้ข้อมูลในฐานข้อมูลมีความถูกต้องครบถ้วนสมบูรณ์ (Integrity)
- เพื่อให้มีฐานข้อมูลพร้อมใช้งานอยู่เสมอ (Availability)
- เพื่อลดความเสี่ยง (Risk Assessment)

๕.๖.๓ ผู้รับผิดชอบฐานข้อมูลเป็นปัจจัยหนึ่งที่ทำให้เกิดความเสี่ยง จะต้องกำหนดให้มีบุคคลรับผิดชอบฐานข้อมูลทั้งทางด้านเทคนิคในการจัดการเกี่ยวกับการสร้างและการจัดการกับระบบฐานข้อมูล หรือที่เรียกว่า “ผู้ดูแลระบบฐานข้อมูล” (Database Administrator : DBA) อย่างชัดเจน

๕.๖.๔ ระบบสำรองและระบบกู้คืนฐานข้อมูล เป็นอีกปัจจัยหนึ่ง ที่ทำให้เกิดความเสี่ยงจะต้องดำเนินการกำหนดนโยบายการสำรองและการกู้คืนระบบฐานข้อมูลกลับคืนมา หากเกิดความเสียหายต่างๆ ขึ้นกับฐานข้อมูล สามารถที่จะนำข้อมูลส่วนที่เสียหายนั้นกลับคืนมาได้ เพื่อลดการสูญหายของข้อมูลและความเสี่ยงในการที่จะไม่สามารถใช้ฐานข้อมูลได้ ดังนี้

- มีการสำรองข้อมูลด้าน Software
- กำหนดที่เก็บรักษาข้อมูลสำรองโดยเฉพาะ
- สำรองข้อมูลโดยการบันทึกไว้ที่แผ่น CD ROM
- กำหนดทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง
- การกู้ข้อมูล มีการกำหนดบุคลากรผู้ที่ได้รับสิทธิ์กู้ข้อมูลที่ได้สำรองไว้
- จัดทำคู่มือการสำรองข้อมูลและกู้คืนระบบฐานข้อมูล

๕.๖.๕ ระบบมอนิเตอร์ฐานข้อมูล (Monitor) เป็นอีกปัจจัยหนึ่งที่ทำให้เกิดความเสี่ยงการใช้งานระบบตรวจสอบ หรือมอนิเตอร์การใช้งานฐานข้อมูลอย่างสม่ำเสมอ เพื่อตรวจสอบประสิทธิภาพการทำงานของฐานข้อมูลว่ามีประสิทธิภาพในการทำงานเป็นอย่างไร เร็วหรือช้า และตรวจสอบบันทึกการเปลี่ยนแปลงต่างๆ (Audit Log) ที่เกิดขึ้นในฐานข้อมูลเพื่อที่จะสามารถตรวจสอบย้อนหลังได้

๕.๖.๖ การไม่กำหนดสิทธิ์การใช้งานฐานข้อมูลเป็นความเสี่ยงฐานข้อมูล คือการกำหนดสิทธิ์การใช้งานฐานข้อมูล คือ การกำหนดอำนาจหน้าที่ ระดับสิทธิ (Authorization) เข้าถึงฐานข้อมูลให้มีความแตกต่างกันการเข้าใช้งานระบบฐานข้อมูล เพื่อป้องกันไม่ให้บุคคลที่ไม่มีส่วนเกี่ยวข้องเข้ามาดู หรือทำการเปลี่ยนแปลงแก้ไขข้อมูล ซึ่งจะส่งผลให้ระบบฐานข้อมูลเกิดความเสียหายได้ โดยมีการเก็บรายละเอียดเกี่ยวกับผู้ใช้งานแต่ละคนไว้ในพจนานุกรมข้อมูลว่าใครสามารถเข้าใช้งานฐานข้อมูลได้ และต้องมีรหัสผ่าน(Password) ในระดับต่างๆ ที่จะสามารถเข้าไปใช้ข้อมูลได้ เช่น ระดับผู้ดูแลระบบระดับผู้ใช้งานทั่วไป เป็นต้น

๕.๖.๗ ไวรัสคอมพิวเตอร์ เครื่องคอมพิวเตอร์ติดไวรัส หมายถึง ไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำแล้ว เนื่องจากไวรัสเป็นโปรแกรมที่ทำลายระบบซอฟแวร์ การที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้จะต้องมีการถูกเรียกให้ทำงาน เมื่อใดก็ตามที่ไวรัสทำงานผู้ใช้งานไม่สามารถเข้าไปใช้ข้อมูลในเครื่องคอมพิวเตอร์ได้ การใช้โปรแกรมป้องกันไวรัสก็เพื่อป้องกันไม่ให้ไวรัสเข้าไปฝังตัวในหน่วยความจำของเครื่องคอมพิวเตอร์

๖. กระบวนการในการจัดทำแผนบริหารความเสี่ยงของฐานข้อมูลและสารสนเทศ

กระบวนการในการจัดทำแผนบริหารความเสี่ยงของฐานข้อมูลและสารสนเทศ ได้ดำเนินการ ๕ ขั้นตอน ดังนี้

ขั้นตอนที่ ๑ การกำหนดเป้าหมายการบริหารความเสี่ยง (วิเคราะห์ความสำคัญของฐานข้อมูลและสารสนเทศ)

ขั้นตอนที่ ๒ วิเคราะห์ปัจจัยเสี่ยงที่มีผลทางด้านความปลอดภัยของฐานข้อมูลและสารสนเทศ

ขั้นตอนที่ ๓ การประเมินความเสี่ยงและการกำหนดกลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง

ขั้นตอนที่ ๔ การจัดทำแผนภูมิความเสี่ยงฐานข้อมูลและสารสนเทศ

ขั้นตอนที่ ๕ จัดทำแผนบริหารความเสี่ยงฐานข้อมูลและสารสนเทศ

ขั้นตอนที่ ๑

การกำหนดเป้าหมายการบริหารความเสี่ยง
(วิเคราะห์ความสำคัญของฐานข้อมูลและสารสนเทศ)

เป็นการวิเคราะห์ความสำคัญของฐานข้อมูลและสารสนเทศ ซึ่งกำหนดปัจจัยในการพิจารณา ๕ ปัจจัย สำหรับเกณฑ์การให้คะแนนปัจจัยแต่ละปัจจัยถ้าเกี่ยวข้องมากก็ได้คะแนนมาก โดยมีระดับค่าคะแนน ๑-๕ เมื่อได้คะแนนแต่ละปัจจัยแล้วนำผลคูณทั้ง ๕ ปัจจัยมาคูณกัน แล้วนำมาเรียงลำดับความสำคัญตามค่าคะแนนมากน้อย

ปัจจัยการพิจารณา	เกณฑ์การพิจารณา				
	๑	๒	๓	๔	๕
๑. สนับสนุนประเด็นยุทธศาสตร์	ไม่สนับสนุน ประเด็นยุทธศาสตร์	สนับสนุน ๑ ประเด็นยุทธศาสตร์	สนับสนุน ๒ ประเด็นยุทธศาสตร์	สนับสนุน ๓ ประเด็นยุทธศาสตร์	สนับสนุน ๔ ประเด็นยุทธศาสตร์ ขึ้นไป
๒. บุคลากรของกรมฯ ใช้ในการปฏิบัติงานหรือวางแผนการดำเนินงาน (ฐานข้อมูล ๖,๙๐๐ คน)	๑-๒๐ % (๑-๑,๓๔๐ คน)	๒๐.๐๑-๔๐% (๑,๓๔๑-๒,๖๘๐ คน)	๔๐.๐๑-๖๐ % (๒,๖๘๑-๔,๐๒๐ คน)	๖๐.๐๑-๘๐% (๔,๐๒๑-๕,๓๖๐ คน)	๘๐.๐๑% ขึ้นไป (๕,๓๖๑ คน ขึ้นไป)
๓. ผู้รับบริการ (๑๑ กลุ่ม) ๑)ผู้นำ ๒)แกนนำพัฒนา ๓)กลุ่ม/องค์กร ๔)ประชาชน ๕)ผู้บริโภคผลิตภัณฑ์ชุมชน ๖)ชุมชน ๗)หน่วยงานในสังกัด มท. ๘)อปท. ๙)ภาคีเครือข่าย	๑-๒ กลุ่ม	๓-๔ กลุ่ม	๕-๖ กลุ่ม	๗-๘ กลุ่ม	๙ กลุ่มขึ้นไป

ปัจจัยการพิจารณา	เกณฑ์การพิจารณา				
	๑	๒	๓	๔	๕
(พอช./สธ./กษ./ศธ./พณ./อต.) ๑๐)สถาบันการศึกษา ๑๑)สถาบันการเงิน (ออมสิน/ธกส.)	๑-๒ กลุ่ม	๓-๔ กลุ่ม	๕-๖ กลุ่ม	๗-๘ กลุ่ม	๙ กลุ่มขึ้นไป
๔. นโยบายรัฐบาล (๑๑ข้อ)	ไม่สนองต่อนโยบายรัฐบาล	สนองต่อนโยบายรัฐบาล ๑ ข้อ	สนองต่อนโยบายรัฐบาล ๒ ข้อ	สนองต่อนโยบายรัฐบาล ๓ ข้อ	สนองต่อนโยบายรัฐบาล ๔ ข้อขึ้นไป
๕. งบประมาณสนับสนุนฐานข้อมูลและสารสนเทศ	๐ - ๑๐,๐๐๐ บาท	๑๐,๐๐๑ - ๕๐,๐๐๐ บาท	๕๐,๐๐๑ – ๑๐๐,๐๐๐ บาท	๑๐๐,๐๐๑ - ๕๐๐,๐๐๐ บาท	๕๐๐,๐๐๑ บาทขึ้นไป

ขั้นตอนที่ ๒

วิเคราะห์ปัจจัยเสี่ยงที่มีผลทางด้านความปลอดภัยของฐานข้อมูลและสารสนเทศ

ขั้นตอนนี้ประกอบด้วย ๖ ปัจจัย คือ ผู้รับผิดชอบฐานข้อมูล ระบบสำรอง/กู้คืนระบบฐานข้อมูล กำหนดนโยบายด้านความปลอดภัยการใช้งานฐานข้อมูล ระบบมอนิเตอร์ฐานข้อมูล กำหนดสิทธิ์การใช้งานฐานข้อมูลและการป้องกันไวรัสคอมพิวเตอร์ ขั้นตอนนี้นำฐานข้อมูลที่เรียงลำดับไว้แล้ว มาตอบคำถามว่าใน ๖ ปัจจัยดังกล่าว มีการดำเนินการหรือไม่ ถ้ามีการดำเนินการ ให้ตอบ Y หากไม่มีการดำเนินการให้ตอบ N ให้นำส่วนที่ยังไม่ดำเนินการ (ที่ตอบ N ของทุกฐานข้อมูล) ไปดำเนินการในขั้นตอนที่ ๓ ต่อไป

คำนิยามตามขั้นตอนที่ ๒

<u>การป้องกันไวรัสคอมพิวเตอร์</u>

ได้แก่ ติดตั้งและใช้งานโปรแกรมป้องกันไวรัส ESET Endpoint ที่กรมฯ จัดหาให้

<u>ผู้รับผิดชอบฐานข้อมูล</u>

ได้แก่ เอกสารสิทธิ์การเข้าใช้ระบบฐานข้อมูล (Access Right) ของสำนัก กอง ศูนย์

<u>ระบบสำรอง/กู้คืนระบบฐานข้อมูล</u>

ได้แก่ การสำรองข้อมูลเดือนละ ๑ ครั้ง / การสำรองและจัดเก็บข้อมูลจากเครื่องคอมพิวเตอร์ลงบนแผ่น CD, DVD, Hard disk, External Hard disk, Flashdrive, และอุปกรณ์อื่นๆ

<u>กำหนดนโยบายด้านความปลอดภัยการใช้งานฐานข้อมูล</u>

ได้แก่ มีเอกสารการกำหนดแนวทางป้องกันฐานข้อมูลให้มีความปลอดภัย ของสำนัก กอง ศูนย์

<u>ระบบมอนิเตอร์ฐานข้อมูล (Monitor)</u>

ได้แก่ มีการแสดงผลฐานข้อมูลที่สามารถใช้งานได้อย่างต่อเนื่อง เป็นปัจจุบัน

<u>กำหนดสิทธิ์การใช้งานฐานข้อมูล</u>

ได้แก่ จัดทำสิทธิ์การเข้าใช้ระบบฐานข้อมูล (Access Right) ของสำนัก กอง ศูนย์

ขั้นตอนที่ ๓

การประเมินความเสี่ยงและการกำหนดกลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง

ขั้นตอนนี้ประกอบด้วย ๒ ประเด็น คือ โอกาสที่จะเกิด (O) และผลกระทบ (I) สำหรับเกณฑ์การวัดกำหนดให้การให้คะแนน ดังนี้

ประเด็น/องค์ประกอบการพิจารณา	๑= น้อยมาก	๒= น้อย	๓=ปานกลาง	๔= มาก	๕= มากที่สุด
โอกาสที่จะเกิด (O)	**มากกว่า ๑ ปี /ครั้ง**	**๑ปี/ครั้ง**	**๖ เดือน/ครั้ง**	**๓ เดือน/ครั้ง**	**๑เดือน/ครั้ง**
ผลกระทบ (I)					
- ผลกระทบต่อความสำเร็จของประเด็นยุทธศาสตร์ของกรมฯ (I๑)	ไม่มี	๑ ประเด็นยุทธศาสตร์	๒ ประเด็นยุทธศาสตร์	๓ ประเด็นยุทธศาสตร์	๔ ประเด็นยุทธศาสตร์ขึ้นไป
- ผลกระทบต่อการใช้งานบุคลากรของกรมฯ (I๒)	๑-๒๐ % (๑-๑,๓๔๐ คน)	๒๐.๐๑-๔๐% (๑,๓๔๑-๒,๖๘๐ คน)	๔๐.๐๑-๖๐ % (๒,๖๘๑-๔,๐๒๐ คน)	๖๐.๐๑-๘๐% (๔,๐๒๑-๕,๓๖๐ คน)	๘๐.๐๑% ขึ้นไป (๕,๓๖๑ คนขึ้นไป)
-ผลกระทบต่อการใช้งานผู้รับบริการ (I๓) (๑๑ กลุ่ม) ๑.ผู้นำ ๒.แกนนำพัฒนา ๓.กลุ่ม/องค์กร ๔.ประชาชน ๕.ผู้บริโภคผลิตภัณฑ์ชุมชน ๖.ชุมชน ๗.หน่วยงานในสังกัด มท. ๘.อปท. ๙.ภาคีเครือข่าย (พอช./สธ./กษ./ศธ./พณ./อต.) ๑๐.สถาบันการศึกษา ๑๑.สถาบันการเงิน (ออมสิน/ธกส.)	๑-๒ กลุ่ม	๓-๔ กลุ่ม	๕-๖ กลุ่ม	๗-๘ กลุ่ม	๙ กลุ่มขึ้นไป

ประเด็น/องค์ประกอบการพิจารณา	๑= น้อยมาก	๒= น้อย	๓=ปานกลาง	๔= มาก	๕= มากที่สุด
โอกาสที่จะเกิด (O)	**มากกว่า ๑ ปี /ครั้ง**	**๑ปี/ครั้ง**	**๖ เดือน/ครั้ง**	**๓ เดือน/ครั้ง**	**๑เดือน/ครั้ง**
ผลกระทบ (I)					
-นโยบายรัฐบาล (I๔) ๑๑ ข้อ	ไม่สนองต่อนโยบายรัฐบาล	สนองต่อนโยบายรัฐบาล ๑ ข้อ	สนองต่อนโยบายรัฐบาล ๒ ข้อ	สนองต่อนโยบายรัฐบาล ๓ ข้อ	สนองต่อนโยบายรัฐบาล ๔ ข้อขึ้นไป
-งบประมาณสนับสนุนฐานข้อมูลและสารสนเทศ (I๕)	๐ - ๑๐,๐๐๐ บาท	๑๐,๐๐๑ - ๕๐,๐๐๐ บาท	๕๐,๐๐๑ - ๑๐๐,๐๐๐ บาท	๑๐๐,๐๐๑ - ๕๐๐,๐๐๐ บาท	๕๐๐,๐๐๑ บาทขึ้นไป

การกำหนดกลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง มี ๔ กลยุทธ์

๑. การหลีกเลี่ยง (Avoid) : การดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่เกิดความเสี่ยง

๒. การร่วมจัดการ (Share) : การร่วมหรือแบ่งความรับผิดชอบกับผู้อื่นในการจัดการความเสี่ยง

๓. การลด (Reduce) : การดำเนินการเพิ่มเติม เพื่อลดโอกาสที่อาจเกิดขึ้นหรือส่งผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔. การยอมรับ (Accept) : ความเสี่ยงที่เหลือในปัจจุบันอยู่ภายในระดับที่ต้องการและยอมรับได้แล้ว โดยไม่ต้องมีการดำเนินการเพิ่มเติม เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก

กรมการพัฒนาชุมชนได้พิจารณาโอกาส และระดับผลกระทบของแต่ละปัจจัยเสี่ยง โดยได้นำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยงต่อส่วนราชการ ว่าก่อให้เกิดความเสี่ยงในระดับใด (ระดับความเสี่ยง = โอกาสที่จะเกิดเหตุการณ์ (O)x ผลกระทบที่เกิดจากความเสียหาย (I)
ซึ่งจัดแบ่งเป็น ๔ ระดับ ดังนี้

๑. ระดับความเสี่ยงต่ำ คะแนนระดับความเสี่ยง น้อยกว่า หรือเท่ากับ ๓.๐๐ (<=๓.๐๐) คะแนน หมายถึง ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

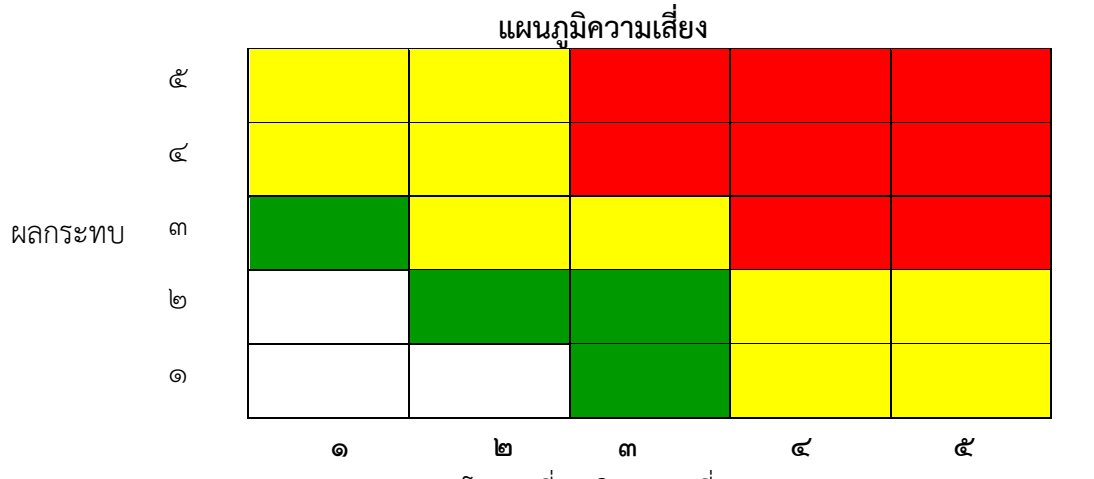
๒. ระดับความเสี่ยงปานกลาง (Medium) คะแนนระดับความเสี่ยง ๓.๐๑-๙.๐๐ คะแนน หมายถึง ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น

๓. ระดับความเสี่ยงสูง (High) คะแนนระดับความเสี่ยง๙.๐๑-๑๕.๐๐ คะแนน หมายถึง ระดับที่ไม่สามารถยอมรับได้ โดยต้องมีการควบคุมเพื่อให้อยู่ในระดับที่ยอมรับได้

๔. ระดับความเสี่ยงสูงมาก (Extreme) คะแนนระดับความเสี่ยง ๑๕.๐๑-๒๕.๐๐ คะแนน หมายถึง ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที

ขั้นตอนที่ ๔

การจัดทำแผนภูมิความเสี่ยงฐานข้อมูลและสารสนเทศ



สีแดง	หมายถึง	ความเสี่ยงสูงมาก
สีเหลือง	หมายถึง	ความเสี่ยงสูง
สีเขียว	หมายถึง	ความเสี่ยงปานกลาง
สีขาว	หมายถึง	ความเสี่ยงต่ำ

ขั้นตอนที่ ๕

จัดทำแผนบริหารความเสี่ยงฐานข้อมูลและสารสนเทศ

ที่	ฐานข้อมูล/สารสนเทศ	ปัจจัยเสี่ยง	กิจกรรมตามแนวทางการจัดการความเสี่ยง	เป้าหมาย/ผลสำเร็จ	ต.ค	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ผู้รับผิดชอบ

การจัดทำแผนบริหารความเสี่ยงฐานข้อมูลและสารสนเทศ กรมการพัฒนาชุมชน พ.ศ. ๒๕๖๑ – ๒๕๖๒

ขั้นตอนที่ ๑

การกำหนดเป้าหมายการบริหารความเสี่ยง

(วิเคราะห์ความสำคัญของฐานข้อมูลและสารสนเทศ)

กรมการพัฒนาชุมชน พ.ศ. ๒๕๖๑ – ๒๕๖๒

ขั้นตอนที่ ๒

วิเคราะห์ปัจจัยเสี่ยงที่มีผลทางด้านความปลอดภัย

ของฐานข้อมูลและสารสนเทศ

กรมการพัฒนาชุมชน พ.ศ. ๒๕๖๑ -๒๕๖๒

ขั้นตอนที่ ๓
การประเมินความเสี่ยงและการกำหนดกลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง
กรมการพัฒนาชุมชน พ.ศ. ๒๕๖๑ – ๒๕๖๒

ขั้นตอนที่ ๔
การจัดทำแผนภูมิความเสี่ยงฐานข้อมูลและสารสนเทศ
กรมการพัฒนาชุมชน พ.ศ. ๒๕๖๑ – ๒๕๖๒

ขั้นตอนที่ ๕

จัดทำแผนบริหารความเสี่ยงฐานข้อมูลและสารสนเทศ

กรมการพัฒนาชุมชน พ.ศ. ๒๕๖๑ – ๒๕๖๒

ภาคผนวก

ภาพการประชุมทบทวนวิเคราะห์แผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ

(Risk Management Plan)

วันศุกร์ที่ ๑๕ มิถุนายน ๒๕๖๑ เวลา ๐๘.๓๐ - ๑๖.๓๐ น.

ณ. ห้องฝึกอบรมคอมพิวเตอร์ ชั้น ๕ กรมการพัฒนาชุมชน