

แผนการบริหารความเสี่ยง

กระบวนการ การพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัย
ประจำปี ๒๕๕๕

กระบวนการงาน การพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัย

กระบวนการสร้างคุณค่า

ความสำคัญของกระบวนการงาน

กระบวนการทำงานและการตัดสินใจต่าง ๆ ของผู้บริหารจังหวัดจำเป็นต้องอยู่บนพื้นฐานข้อมูล ข่าวสารที่ถูกต้องอยู่บนพื้นฐาน ข่าวสารที่ถูกต้อง รวดเร็ว และเชื่อถือได้ ระบบเทคโนโลยีและสารสนเทศที่เหมาะสมและทันสมัย เป็นส่วนหนึ่งของในกระบวนการช่วยในการตัดสินใจที่ถูกต้องของผู้บริหาร หัวหน้าส่วนราชการ ผู้ที่มีส่วนเกี่ยวข้อง ตลอดจนประชาชนได้รับความสะดวก ลดภาระค่าใช้จ่ายในการเดินทางและเวลา เพิ่มประสิทธิภาพและความรวดเร็วในการทำงานของภาครัฐ และเอกชน

ลักษณะของงาน เป็นกระบวนการที่มุ่งเน้นในการสนับสนุนด้านเทคโนโลยีสารสนเทศ การเข้าถึงข้อมูลข่าวสารที่ถูกต้อง รวดเร็ว และเชื่อถือได้ เป็นช่องทางหนึ่งในการประชาสัมพันธ์งานหรือกิจกรรมของจังหวัด เพื่อให้ประชาชนได้รับข้อมูลข่าวสารที่ถูกต้องจากภาครัฐ ผ่านทางระบบเทคโนโลยีสารสนเทศ เช่น เว็บไซต์จังหวัด (www.phichit.go.th) ศูนย์ข้อมูลกลางกระทรวงมหาดไทย 45 ฐานข้อมูล 32 ตัวชี้วัด (moi.go.th) การให้บริการเครือข่าย internet และการให้บริการการประชุมทางไกล เป็นต้น

การบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศจังหวัดพิจิตร

นิยามที่เกี่ยวข้องกับความเสี่ยง

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่มีโอกาสเกิดขึ้นได้ในอนาคตภายใต้สภาวะการณ์ที่ไม่แน่นอน ซึ่งอาจส่งผลกระทบต่อด้านลบที่ไม่ต้องการ ดังนั้น การตัดสินใจกระทำการใด ๆ โดยไม่มีข้อมูล หรือไม่มีการวางแผนใดๆ จึงสามารถกล่าวได้ว่าเป็นการเสี่ยงตัดสินใจในภาวะของความเสี่ยง

การเสี่ยง หมายถึง การตัดสินใจที่จะดำเนินการสิ่งใดสิ่งหนึ่งบนพื้นฐานของการขาดข้อมูลที่ชัดเจน ไม่ครบถ้วน เป็นเพียงการประมาณการ การคาดเดา ผลของการตัดสินใจนั้นอาจเป็นไปตามความคาดหมายหรือตรงกันข้ามก็ได้

ความไม่แน่นอน หมายถึง ความเปลี่ยนแปลง ไม่คงที่คงเดิมตลอดเวลาหรือเหตุการณ์ต่าง ๆ ที่มีโอกาสเกิดขึ้นได้ทั้งที่เป็นไปตามความคาดหมายหรือนอกเหนือความคาดหมาย

ปัญหา หมายถึง สิ่งที่เกิดขึ้นและมักส่งผลในทางลบ เป็นอุปสรรคต่อเป้าหมายการดำเนินการ จำเป็นต้องมีการแก้ไข เพราะมีเช่นนั้นปัญหาดังกล่าวอาจก่อให้เกิดความเสียหายตามมา

ความเสี่ยงของระบบเทคโนโลยีสารสนเทศ หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นได้ในอนาคตภายใต้สภาวะการณ์ที่ไม่แน่นอน และจะส่งผลกระทบต่อหรือสร้างความเสียหายหรือล้มเหลวที่จะบรรลุผลสำเร็จ ต่อการบริหารงานระบบเทคโนโลยีสารสนเทศจังหวัด

การบริหารความเสี่ยง (Risk Management) หมายถึง การปฏิบัติการใด ๆ เพื่อควบคุมความเสี่ยง ได้แก่ การวางแผนป้องกันความเสี่ยง การประเมินความเสี่ยงด้านต่าง ๆ โอกาส ผลกระทบที่เกิดจากความเสี่ยงนั้น

1. หลักเกณฑ์และเหตุผล

ศูนย์ปฏิบัติการจังหวัดพิจิตร เป็นศูนย์กลางในการจัดการระบบข้อมูลสารสนเทศที่สำคัญต่าง ๆ ของทุกส่วนราชการในจังหวัด ในการเป็นศูนย์กลางสำหรับส่วนราชการบริหารเชิงยุทธศาสตร์ระดับพื้นที่จังหวัด ให้สนับสนุนข้อมูลการบริหารราชการแผ่นดินต่อศูนย์ปฏิบัติการกระทรวงมหาดไทย (MOC) และศูนย์ปฏิบัติการนายกรัฐมนตรี (PMQA) ตลอดจนวิเคราะห์ กลั่นกรองข้อมูลที่จำเป็นเพื่อประกอบการตัดสินใจของผู้บริหารระดับสูงในระดับจังหวัดที่จะนำข้อมูลไปใช้ประโยชน์ในการบริหารจัดการ

ศูนย์ปฏิบัติการจังหวัดพิจิตร มีระบบเครือข่ายในการให้บริการตั้งอยู่ในสถานที่ที่มีความมั่นคงในด้านการรักษาความปลอดภัย และมีการป้องกันระบบที่มีเสถียรภาพ ณ สถานีสื่อสารจังหวัดพิจิตร ศาลากลางจังหวัดพิจิตร อย่างไรก็ตามเพื่อเป็นการป้องกันความเสี่ยง จึงจำเป็นต้องมีการเตรียมการและวางแผนรองรับปัญหาเกี่ยวกับความเสี่ยง และภัยพิบัติต่างๆ ที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัด

2. วัตถุประสงค์

- 1) เพื่อเตรียมความพร้อม และรองรับสถานการณ์ฉุกเฉินที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัดพิจิตร
- 2) เพื่อกำหนดมาตรการในการป้องกันความเสียหายที่จะเกิดกับระบบเทคโนโลยีสารสนเทศของจังหวัดพิจิตร จากภาวะความเสี่ยงต่าง ๆ
- 3) เพื่อให้ระบบเทคโนโลยีสารสนเทศของจังหวัด สามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ
- 4) เป็นการเผยแพร่ข้อมูลด้านการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศให้เจ้าหน้าที่ที่เกี่ยวข้องนำไปใช้ประโยชน์

3. องค์ประกอบของระบบเทคโนโลยีสารสนเทศ

- 1) Hardware หมายถึง อุปกรณ์ต่างๆ ที่ประกอบเป็นเครื่องคอมพิวเตอร์หรือระบบสารสนเทศ
- 2) Software หมายถึง ระบบหรือชุดคำสั่งที่ทำให้เครื่องคอมพิวเตอร์ทำงานหรือประมวลผลข้อมูล
- 3) บุคลากร หมายถึง บุคคลหรือกลุ่มบุคคล ที่เกี่ยวข้องกับการปฏิบัติงานด้านระบบเทคโนโลยีสารสนเทศ
- 4) ข้อมูล หมายถึง วัตถุดิบที่รวบรวมมาทำให้เกิดสารสนเทศ ซึ่งได้จากการรวบรวมด้วยตนเอง หรือจากส่วนราชการอื่น
- 5) สารสนเทศ หมายถึง การจัดเก็บข้อมูลเพื่อใช้ประโยชน์โดยผ่านกระบวนการประมวลผลด้วยระบบคอมพิวเตอร์ด้วยวิธีการที่เหมาะสม ถูกต้อง และเป็นไปตามความต้องการของผู้ใช้ประโยชน์

4. พื้นที่เสี่ยงภัย

- 1) ผู้ให้บริการ ISP
- 2) ศาลากลางจังหวัดพิจิตร
- 3) สถานีสื่อสารจังหวัดพิจิตร
- 4) หน่วยงานผู้รับผิดชอบข้อมูล

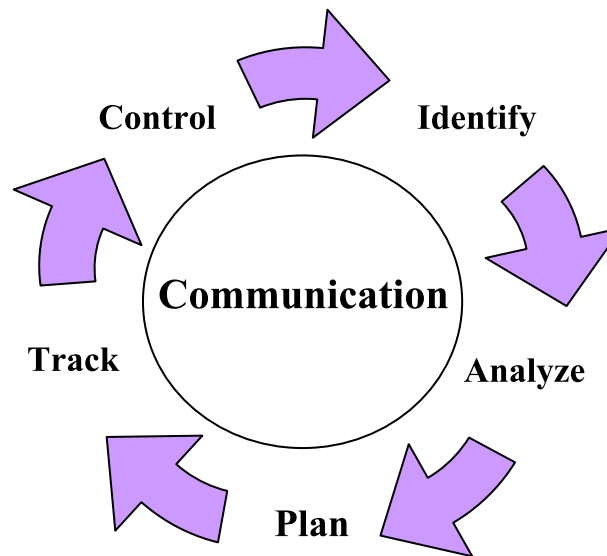
5. การประเมินสถานการณ์ความเสี่ยงที่อาจเกิดขึ้น

จากความหมายของความเสี่ยง ซึ่งมักจะหมายถึงความเป็นไปได้ในอนาคตที่อาจจะทำให้เกิดผลในทางลบขึ้น กับระบบเทคโนโลยีสารสนเทศ จึงตระหนักและให้ความสำคัญของความเสี่ยง และได้มีความบริหารความเสี่ยงที่จะเกิดขึ้น โดยเลือกใช้กลยุทธ์ที่เหมาะสมกับความเป็นไปได้ของสถานการณ์ที่อาจก่อให้เกิดปัญหา และสามารถแก้ไขเหตุการณ์ได้อย่างทันทั่วทั้งที่ โดยป้องกันมิให้เกิดความเสียหายตามมา ก็จะทำงานสำเร็จตามเป้าประสงค์

จากโครงสร้างเครือข่ายการทำงานของศูนย์ปฏิบัติการจังหวัดพิจิตร ประกอบด้วยอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์สารสนเทศต่าง ๆ และโครงสร้างการทำงานของระบบ พบว่าความเสี่ยงที่อาจเป็นอันตราย ต่อระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นองค์ประกอบหลักในระบบฐานข้อมูลสารสนเทศของจังหวัดสามารถของจังหวัด สามารถจำแนกความเสี่ยงได้ดังนี้

- 1) ความเสี่ยงเชิงยุทธศาสตร์
- 2) ความเสี่ยงด้านธรรมาภิบาล
- 3) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- 4) ความเสี่ยงด้านกระบวนการ

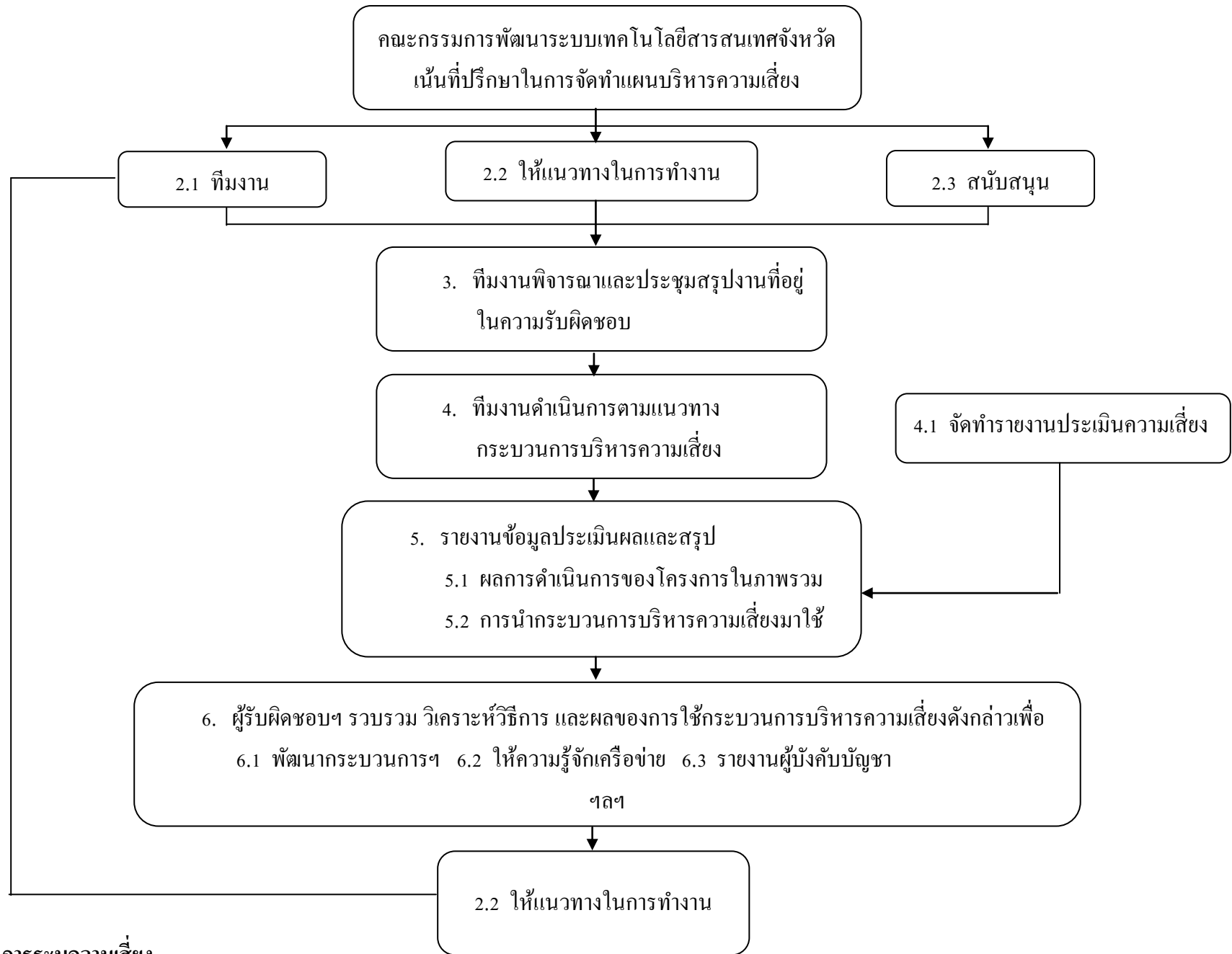
6. กระบวนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ



ขั้นตอนที่ 1	Identify	หมายถึง	การระบุความเสี่ยงและผลกระทบที่มีผลต่อระบบ
ขั้นตอนที่ 2	Analyze	หมายถึง	ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยง และความรุนแรงของผลกระทบ
ขั้นตอนที่ 3	Plan	หมายถึง	วางแผนโดยกำหนดมาตรการ เพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้บรรลุเป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนดไว้
ขั้นตอนที่ 4	Track	หมายถึง	การติดตามข้อมูลเพื่อทราบสถานะที่อาจจะเกิดขึ้นของความเสี่ยง
ขั้นตอนที่ 5	Control	หมายถึง	การติดตาม กำกับ ตรวจสอบการปฏิบัติการควบคุมความเสี่ยง และทบทวนแผนบริหารความเสี่ยง

องค์ประกอบที่สำคัญอีกประการหนึ่ง ที่เกี่ยวข้องในการบริหารความเสี่ยงคือการติดต่อสื่อสาร (Communication) เพราะการดำเนินการต่าง ๆ ต้องอาศัยการประสานงาน เชื่อมโยงกับทุกฝ่ายทั้งภายในและภายนอกหน่วยงาน

7. ฝั่งแนวทางในการจัดทำรายงานการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศจังหวัดพิจิตร



ประเภทความเสี่ยง	กระบวนการ/กิจกรรม	ความเสี่ยงที่อาจเกิดขึ้น
ความเสี่ยงเชิงบูรณาการ	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- การดำเนินงานตามแผนงาน/กิจกรรม/โครงการ ไม่ครบถ้วน - การดำเนินงานตามแผนล่าช้า
	การถ่ายทอดแผนไปสู่การปฏิบัติ	- ผู้ได้รับมอบหมายในการนำแผนไปสู่การปฏิบัติ ได้รับการสื่อสารไม่ครบถ้วนทำให้การนำแผนไปสู่การปฏิบัติเกิดความผิดพลาด
	ด้านงบประมาณ	- การจัดหา วัสดุ อุปกรณ์ ปัจจัยการดำเนินการไม่เป็นไปตามแผนงานที่กำหนดไว้
	ด้านบุคลากร	- ไม่มีผู้เชี่ยวชาญด้านระบบเทคโนโลยีสารสนเทศทำให้การออกแบบระบบมีความเสี่ยงที่จะออกแบบผิดพลาด หรือเกิดปัญหาขึ้นภายหลัง - เจ้าหน้าที่ขาดความรู้ ทักษะ และความเชี่ยวชาญในระบบงาน - ระบบงานเกิดการชะงักเนื่องจากการปรับเปลี่ยนตามระบบราชการ (โยกย้าย)
ความเสี่ยงด้านธรรมาภิบาล	ความซื่อสัตย์ สุจริต ปฏิบัติหน้าที่ตรงไปตรงมาตามกฎหมาย กฎระเบียบ ไม่แสวงหาประโยชน์ส่วนตัว	- ใช้อำนาจหน้าที่เพื่อเอื้อประโยชน์ต่อพวกพ้อง - ใช้ช่องโหว่ทางกฎหมายเพื่อแสวงหาประโยชน์ส่วนตัว
	การปฏิบัติต่อผู้อื่น ด้วยความเป็นธรรมและเท่าเทียมกัน	- การปฏิบัติต่อผู้รับบริการอย่างไม่เป็นธรรมเสมอภาค - เอื้อประโยชน์ให้กลุ่มใด กลุ่มหนึ่งเป็นพิเศษ
	ความสามัคคี การช่วยเหลือให้ความเคารพซึ่งกันและกัน ทำงานร่วมกันอย่างมีประสิทธิภาพ	- แบ่งพรรคแบ่งพวกในการทำงาน - ไม่ให้ความร่วมมือในการทำงาน
	ความมีประสิทธิภาพ ทำงานอย่างรวดเร็ว และใช้ทรัพยากรที่มีอยู่อย่างจำกัดให้ได้ผลคุ้มค่า และก่อประโยชน์สูงสุด	- การปฏิบัติงานล่าช้ากว่ากำหนด ไม่เป็นไปตามแผนที่วางไว้ - ขาดระบบและขั้นตอนการดำเนินการที่มีประสิทธิภาพ

ประเภทความเสี่ยง	กระบวนการ/กิจกรรม	ความเสี่ยงที่อาจเกิดขึ้น
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ - ห้องศูนย์ข้อมูล	ความปลอดภัยในการเข้า - ออก	- ระบบเทคโนโลยีสารสนเทศเกิดความเสียหายใช้การไม่ได้ข้อมูลถูกทำลายโดยที่ตั้งใจ และไม่ตั้งใจ
	การปรับอากาศ เพื่อรักษาอุณหภูมิของห้อง	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้
	อุบัติเหตุ (ไฟไหม้, น้ำท่วม, ติ๊กถล่ม)	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้ข้อมูลถูกทำลายเสียหาย
ระบบไฟฟ้า	ไฟฟ้าดับ, ไฟฟ้ากระชาก, ไฟฟ้าเกิน, ไฟฟ้าผ่า	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้ข้อมูลถูกทำลายเสียหาย
ระบบสื่อสาร - ระบบเครือข่าย	โทรศัพท์, อินเทอร์เน็ต, อินเทอร์เน็ต ใช้งานไม่ได้ตามปกติ, ระบบประชุมทางไกล	- ระบบเทคโนโลยีสารสนเทศใช้งานไม่ได้
อุปกรณ์คอมพิวเตอร์แม่ข่าย	ชำรุดเสียหาย ไม่สามารถใช้งานได้ตามปกติ ไวรัส, สปายแวร์ ทำลายระบบฐานข้อมูล โคน โจมตี, โคนบุกรุก	- ระบบฐานข้อมูลใช้งานไม่ได้, ข้อมูลทำลายเสียหาย
อุปกรณ์คอมพิวเตอร์ลูกข่าย	ชำรุดเสียหาย ไม่สามารถใช้งานได้ตามปกติ ไวรัส, สปายแวร์ ทำลายระบบฐานข้อมูล โคน โจมตี, โคนบุกรุก	- ระบบฐานข้อมูลใช้งานไม่ได้, ข้อมูลทำลายเสียหาย
อุปกรณ์เครือข่าย , อุปกรณ์สื่อสาร	อุปกรณ์ชำรุดเสียหาย, ไม่สามารถใช้งานได้ตามปกติ ตัวนำสัญญาณ, สายสัญญาณต่าง ๆ ขาด ชำรุด	- ระบบฐานข้อมูลใช้งานไม่ได้
ด้านระบบฐานข้อมูล	การเข้าถึงข้อมูลไม่ได้/การเข้าถึงข้อมูลโดยไม่ได้ รับอนุญาต/ความเชื่อถือไม่ได้ของข้อมูล/ข้อมูล เสียหาย	- ระบบฐานข้อมูลใช้งานไม่ได้ - มีการรั่วไหลของข้อมูล - ข้อมูลถูกทำลาย

ประเภทความเสี่ยง	กระบวนการ/กิจกรรม	ความเสี่ยงที่อาจเกิดขึ้น
ด้านการบันทึกสำรองข้อมูล	วิธีการที่ไม่ถูกต้องในการสำรองข้อมูลเลือกสื่อบันทึกข้อมูลไม่เหมาะสม	- ข้อมูลสำรอง เสียหายใช้งานไม่ได้ - ไม่สามารถกู้คืนข้อมูลได้
ความเสี่ยงด้านกระบวนการงาน	การจัดการข้อมูล	- แผนการจัดการความรู้ไม่สอดคล้องกับการปฏิบัติงาน
	ผู้ปฏิบัติและการจัดการความรู้	- องค์กรความรู้ไม่เพียงพอ ผลกระบวนการเรียนรู้ ไม่เหมาะสมสอดคล้องกับกระบวนการงาน
	การจัดการทรัพยากรสนับสนุน	- การปฏิบัติงานไม่สามารถดำเนินการต่อได้หรือล่าช้า
	การจัดการลูกค้า/ผู้รับบริการ	- การประชาสัมพันธ์ที่ไม่สอดคล้องกับกลุ่มลูกค้า/ผู้รับบริการ - ผู้รับบริการไม่มีความเข้าใจในการใช้งาน
	การดำเนินการตามกฎหมาย ระเบียบที่เกี่ยวข้อง	- การละเว้นการปฏิบัติตามกฎหมาย ระเบียบที่กำหนดไว้

ขั้นตอนที่ 2 การประเมินถึงโอกาสที่จะเกิดขึ้นและความรุนแรงของผลกระทบ

โอกาสที่จะเกิด (L:Lilcelihook เป็นระดับของโอกาสหรือความบ่อยครั้งที่จะเกิดความเสี่ยง)

โอกาสที่จะเกิดความเสี่ยง	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ระดับคะแนน
สูงมาก	มากกว่า 1 ครั้งต่อเดือน	5
สูง	ระหว่าง 1 – 6 เดือนต่อครั้ง	4
ปานกลาง	ระหว่าง 6 – 12 เดือนต่อครั้ง	3
น้อย	มากกว่า 1 ปีต่อครั้ง	2
น้อยมาก	มากกว่า 5 ปีต่อครั้ง	1

ผลกระทบ (I : Impack คือ ระดับความรุนแรงของความเสี่ยงที่เกิดขึ้น)

- 1 = โอกาสน้อยมาก / รุนแรงน้อยมาก
- 2 = โอกาสเกิดน้อย / รุนแรงน้อย
- 3 = โอกาสเกิดปานกลาง / รุนแรงปานกลาง
- 4 = โอกาสเกิดสูง / รุนแรงสูง
- 5 = โอกาสเกิดสูงมาก / รุนแรงสูงมาก

ระดับความเสี่ยง L x I

ระดับความรุนแรงของผลกระทบที่เกิดจากเหตุการณ์ความเสี่ยง

กำหนดระดับผลกระทบที่อาจเกิดขึ้นจากความเสี่ยง พิจารณาทั้งในด้านการดำเนินงาน ความสูญเสียต่อทรัพย์สิน การได้รับอันตรายของบุคลากร และชื่อเสียงขององค์กร ซึ่งสามารถจำแนกผลกระทบที่อาจเกิดขึ้นจากความเสียหาย อาจเป็น 5 ระดับ ดังนี้

ระดับ	ผลกระทบ	ความเสียหาย
5	สูงมาก	<ul style="list-style-type: none"> - องค์กรไม่สามารถดำเนินงานพื้นฐานได้ และประสิทธิภาพลดลงสูงเกิน 60% - องค์กรได้รับความเสียหายต่อทรัพย์สินเกิน 20% - บุคลากรขององค์กรได้รับอันตรายสูงถึงขั้นเสียชีวิตหรือบาดเจ็บอย่างร้ายแรงมาก - องค์กรเสียชื่อเสียงในวงกว้างขวาง เช่น ตกเป็นข่าวในหนังสือพิมพ์
4	สูง	<ul style="list-style-type: none"> - องค์กรไม่สามารถดำเนินงานพื้นฐานได้ และประสิทธิภาพลดลงสูงเกิน 40% - องค์กรได้รับความเสียหายต่อทรัพย์สินเกิน 10% - บุคลากรได้รับอันตรายถึงขั้นเสียชีวิต หรือบาดเจ็บอย่างรุนแรง - องค์กรเสียชื่อเสียงในวงกว้างขวาง เช่น ตกเป็นข่าวในหนังสือพิมพ์
3	ปานกลาง	<ul style="list-style-type: none"> - องค์กรสามารถดำเนินงานพื้นฐานได้ แต่ประสิทธิภาพลดลง โดยประมาณไม่เกิน 40% - องค์กรได้รับความเสียหายต่อทรัพย์สินไม่เกิน 10% - บุคลากรได้รับอันตรายถึงขั้นต้องเข้ารับการรักษาในโรงพยาบาล แต่ไม่ถึงขั้นเสียชีวิต - องค์กรเสียชื่อเสียงในวงจำกัด
4	น้อย	<ul style="list-style-type: none"> - องค์กรสามารถดำเนินการพื้นฐานได้ แต่ประสิทธิภาพลดลงบ้างไม่เกิน 20% - องค์กรได้รับความเสียหายต่อทรัพย์สิน โดยประมาณไม่เกิน 5% - บุคลากรได้รับอันตรายเล็กน้อยไม่ถึงขนาดเข้ารับการรักษาที่โรงพยาบาล - องค์กรเสียชื่อเสียงในวงจำกัด
5	น้อยมาก	<ul style="list-style-type: none"> - องค์กรสามารถดำเนินการพื้นฐานได้ แต่ประสิทธิภาพลดลงเล็กน้อยไม่เกิน 10% - องค์กรได้รับความเสียหายต่อทรัพย์สิน โดยประมาณไม่เกิน 2.5% - บุคลากรได้รับอันตรายเล็กน้อย - องค์กรแทบไม่เสียชื่อเสียง

ระดับของความเสียหาย

ระดับของความเสียหาย พิจารณาจากความสัมพันธ์ระหว่างโอกาสหรือความถี่ที่จะเกิดความเสียหายกับผลกระทบที่อาจเกิดความเสียหายกับผลกระทบที่อาจเกิดขึ้น จากความเสี่ยงนั้น โดยความสัมพันธ์ดังปรากฏในแผนภาพแสดงระดับความเสี่ยง ดังต่อไปนี้

โอกาสที่จะเกิดความเสียหาย

ความรุนแรงของความเสียหายที่เกิดขึ้น

	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
สูงมาก (5)	5	10	15	20	25
สูง (4)	4	8	9	16	20
ปานกลาง (3)	3	6	9	12	15
น้อย (2)	2	4	6	8	10
น้อยมาก (1)	1	2	3	4	5

จากตารางแสดงความเสี่ยงข้างต้น จำแนกระดับความเสี่ยงออกเป็น 4 ระดับ ได้แก่ สูงมาก สูง ปานกลาง และต่ำ โดยมีรายละเอียดดังนี้

ระดับความเสี่ยง	ผลลัพธ์ (โอกาสที่จะเกิด × ผลกระทบ)	รายละเอียด
สูงมาก	19-25	- จำเป็นต้องพิจารณากำหนดมาตรการบริหารความเสี่ยงอย่างเร่งด่วน เนื่องจากมีโอกาสที่จะเกิดความเสี่ยงสูงมาก หรือหากเกิดความเสี่ยงขึ้นจะส่งผลกระทบต่อประสิทธิภาพขององค์กรอย่างสูง และชื่อเสียงในวงกว้าง
สูง	13-18	- จำเป็นต้องพิจารณามาตรการบริหารความเสี่ยง เนื่องจากมีโอกาสที่จะเกิดสูง หากเกิดความเสี่ยงขึ้นจะส่งผลกระทบต่อประสิทธิภาพขององค์กรสูง หรือเสียชื่อเสียงในวงกว้าง
ปานกลาง	7-12	- พิจารณากำหนดมาตรการบริหารความเสี่ยงตามความจำเป็นและความเหมาะสม เนื่องจากมีโอกาสที่จะเกิดความเสี่ยง หรือหากเกิดความเสี่ยงขึ้นจะส่งผลกระทบต่อประสิทธิภาพอย่างเห็นได้ชัด และเสียชื่อเสียงในวงจำกัด
ต่ำ	ไม่เกิน 6	- มีโอกาสที่จะเกิดความเสี่ยงต่ำ หรือหากเกิดความเสี่ยงขึ้นจะส่งผลกระทบต่อประสิทธิภาพขององค์กรบ้างเล็กน้อย และเสียชื่อเสียงในวงจำกัด

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร

ประเภท ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผล กระทบ	ระดับ ความเสี่ยง	
ความเสี่ยงเชิง ยุทธศาสตร์	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- การดำเนินงานตามแผนงาน/กิจกรรม/โครงการไม่ครบถ้วน - การดำเนินงานตามแผนล่าช้า	2	5	10	ปานกลาง
	การถ่ายทอดแผนไปสู่การปฏิบัติ	- ผู้ได้รับมอบหมายในการนำแผนไปสู่การปฏิบัติ สื่อสารไม่ครบถ้วน ทำให้การนำแผนไปสู่การปฏิบัติเกิดความผิดพลาด	2	3	6	ต่ำ
	ด้านงบประมาณ	- การจัดหาวัสดุอุปกรณ์ ปัจจัยการดำเนินการไม่เป็นไปตามแผนงานที่กำหนดไว้	3	5	15	สูง
	ด้านบุคลากร	- ไม่มีผู้เชี่ยวชาญด้านระบบเทคโนโลยีสารสนเทศ ทำให้การออกแบบระบบมีความเสี่ยงที่จะผิดพลาดหรือเกิดปัญหาขึ้นภายหลัง - จนท.ขาดความรู้ความสามารถทักษะและความชำนาญในระบบงาน - ระบบงานเกิดการชะงักเนื่องจากการปรับเปลี่ยนตามระบบราชการ(โยกย้าย)	4	5	20	สูงมาก

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร (ต่อ)

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	
ความเสี่ยงด้าน ธรรมาภิบาล	ความซื่อสัตย์ สุจริต ปฏิบัติ หน้าที่ตรงไปตรงมาตาม กฎหมาย กฎระเบียบไม่ แสวงหาผลประโยชน์ส่วนตัว	- ใช้อำนาจหน้าที่เพื่อเอื้อประโยชน์ต่อพวกพ้อง - ใช้ช่องโหว่ทางกฎหมายเพื่อแสวงหาประโยชน์ส่วนตัว	3	4	12	ปานกลาง
	การปฏิบัติต่อผู้อื่นด้วยความ เป็นธรรมและเท่าเทียมกัน	- การปฏิบัติต่อผู้รับบริการอย่างไม่เป็นธรรมเสมอภาค - เอื้อประโยชน์ให้กลุ่มใดกลุ่มหนึ่งเป็นพิเศษ	3	3	9	ปานกลาง
	ความสามัคคี การช่วยเหลือให้ ความเคารพซึ่งกันและกัน ทำงานร่วมกันอย่างมี ประสิทธิภาพ	- แบ่งพรรคแบ่งพวกในการทำงาน - ไม่ให้ความร่วมมือในการทำงาน	3	4	12	ปานกลาง
	ความมีประสิทธิภาพ ทำงาน อย่างรวดเร็ว และใช้ทรัพยากร ที่มีอยู่อย่างจำกัดให้ได้อย่าง คุ้มค่า และก่อประโยชน์สูงสุด	- การปฏิบัติงานล่าช้ากว่ากำหนดไม่เป็นไปตามแผนที่กำหนดไว้ - ขาดระบบและขั้นตอนการดำเนินการที่มีประสิทธิภาพ	3	4	12	ปานกลาง

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร (ต่อ)

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ห้องศูนย์ข้อมูล - ความปลอดภัยในการเข้า-ออก - การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง - อุบัติภัย (ไฟไหม้, น้ำท่วม ดึกถล่ม)	- ระบบเทคโนโลยีสารสนเทศเกิดความเสียหายใช้การไม่ได้ ข้อมูลถูกทำลายโดยที่ตั้งใจและไม่ตั้งใจ	4	4	16	สูง
		- อุปกรณ์ชำรุดไม่สามารถใช้งานได้	4	4	16	สูง
		- อุปกรณ์ชำรุดไม่สามารถใช้งานได้ข้อมูลถูกทำลายเสียหาย	4	5	20	สูงมาก
	ระบบไฟฟ้า - ไฟฟ้าดับ/ไฟกระชาก/ไฟเกิน ฯลฯ	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้ข้อมูลถูกทำลาย	4	5	20	สูงมาก

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร (ต่อ)

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	<u>ระบบสื่อสาร/ระบบเครือข่าย</u> - โทรศัพท์/Internet/Intranet/ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ	- ระบบเทคโนโลยีสารสนเทศใช้งานไม่ได้	4	4	16	สูง
	<u>อุปกรณ์คอมพิวเตอร์แม่ข่าย</u> - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โคนโอมติ/โคนบุรุก	- ระบบฐานข้อมูลใช้งานไม่ได้ - ข้อมูลถูกทำลาย	4	5	20	สูงมาก
	<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u> - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โคนโอมติ/โคนบุรุก	- ระบบฐานข้อมูลใช้งานไม่ได้ - ข้อมูลถูกทำลาย	4	5		สูง
	<u>ระบบฐานข้อมูล</u> - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย	- ระบบฐานข้อมูลใช้งานไม่ได้ - ข้อมูลถูกทำลาย - ข้อมูลถูกทำลาย	3	5	15	สูง

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร (ต่อ)

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	การบันทึก - ตำรวจข้อมูล - วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล - เลือกลูกบันทึกข้อมูลไม่เหมาะสม	- ข้อมูลสำรองเสียหายใช้งานไม่ได้ไม่สามารถกู้คืนข้อมูลได้	3	3	9	กลาง
ความเสี่ยงด้านกระบวนการงาน	การจัดการข้อมูล	- มีข้อมูลที่ไม่ถูกต้อง ล่าช้าหรือเชื่อถือไม่ได้	3	5	15	สูง
	ผู้ปฏิบัติและการจัดการความรู้	- แผน จัดการความรู้ไม่สอดคล้องกับการปฏิบัติงาน - องค์กรความรู้ไม่เพียงพอ หรือกระบวนการเรียนรู้ ไม่เหมาะสม สอดคล้องกับกระบวนการงาน	3	4	12	กลาง
	การจัดทรัพยากรสนับสนุน	- ผู้รับบริการไม่มีความเข้าใจในการใช้งาน - การประชาสัมพันธ์ที่ไม่สอดคล้องกับกลุ่มลูกค้า/ผู้บริการ	4	4	16	สูง
	การดำเนินตามกฎหมาย กฎระเบียบที่เกี่ยวข้อง	- การละเว้นการปฏิบัติตามกฎหมาย กฎระเบียบที่กำหนดไว้	3	3	9	กลาง

ขั้นตอนที่ 3 วางแผนโดยกำหนดมาตรการ เพื่อควบคุมผลกระทบของความเสี่ยง

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความ เสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
1	ด้านบุคลากร	<ul style="list-style-type: none"> - แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงานเพื่อป้องกันการขาดแคลนเจ้าหน้าที่ 	ถ่ายโอน	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
2	<u>ระบบไฟฟ้า</u> - ไฟฟ้าดับ/ไฟกระชาก /ไฟเกิน ฯลฯ	- ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) และระบบไฟฟ้าสำรอง (UPS)	ยอมรับ	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
3	<u>อุปกรณ์คอมพิวเตอร์</u> <u>แม่ข่าย</u> - ซ้ำรูดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุกรุก	<ul style="list-style-type: none"> - ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ 	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
4	<u>ห้องศูนย์ข้อมูล</u> - อุบัติภัย (ไฟไหม้, น้ำท่วม ดึกถล่ม)	<ul style="list-style-type: none"> - ติดตั้งระบบดับเพลิงอัตโนมัติชนิดไพโรเจนในพื้นที่ปิด (Pyrogen) - มีการให้ความรู้เจ้าหน้าที่และซักซ้อมแผนเผชิญเหตุเพลิงไหม้ 	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความ เสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
5	<u>ห้องศูนย์ข้อมูล</u> - ความปลอดภัยในการเข้า-ออก	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัดเป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
6	<u>ห้องศูนย์ข้อมูล</u> - การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัตโนมัติ	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
7	<u>ระบบสื่อสาร/ระบบเครือข่าย</u> - โทรศัพท์/Internet/Intranet/ ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ	- บำรุงรักษา ตรวจสอบ ตรวจสอบระบบให้สามารถใช้งานได้ตลอดเวลา	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
8	<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u> - ซ้ำรูดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โคนโจอมติ/โคนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์ลูกข่าย และทำการ Update และ Scan เป็นประจำ	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความ เสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
9	การจัดทรัพยากรสนับสนุน	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
10	ด้านงบประมาณ	- จัดทำแผนงานโครงการเพื่อขอรับการสนับสนุนงบประมาณ	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
11	ระบบฐานข้อมูล - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
12	การจัดการข้อมูล	- ตรวจสอบความถูกต้องของข้อมูล และทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของส่วนราชการ	ควบคุม	ตุลาคม 54 – กันยายน 55	ทุกส่วน ราชการ
13	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- จัดทำแผนงาน/โครงการ/กิจกรรม ให้ครบถ้วน	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
14	ผู้ปฏิบัติและการจัดการความรู้	- ฝึกอบรม และการจัดการความรู้	ควบคุม	ตุลาคม 54 – กันยายน 55	ทุกส่วน ราชการ

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความ เสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
15	<u>การบันทึก - สำรองข้อมูล</u> - วิธีการที่ไม่ถูกต้องในการ สำรองข้อมูล - เลือกสื่อบันทึกข้อมูลไม่ เหมาะสม	- มีการ Backup ข้อมูลอย่างสม่ำเสมอ	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
16	การดำเนินตามกฎหมาย กฎ ระเบียบที่เกี่ยวข้อง	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึง ขั้นตอนการรับบริการ และข้อมูลการบริการ - การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
17	ความซื่อสัตย์ สุจริต ปฏิบัติ หน้าที่ตรงไปตรงมาตาม กฎหมาย กฎระเบียบไม่แสวงหา ผลประโยชน์ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความ เสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
18	ความสามัคคี การช่วยเหลือให้ ความเคารพซึ่งกันและกันทำงาน ร่วมกันอย่างมีประสิทธิภาพ	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
19	ความมีประสิทธิภาพ ทำงาน อย่างรวดเร็ว และใช้ทรัพยากรที่มี อยู่อย่างจำกัดให้ได้อย่างคุ้มค่า และก่อประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
20	การปฏิบัติต่อผู้อื่นด้วยความเป็น ธรรมและเท่าเทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ควบคุม	ตุลาคม 54 – กันยายน 55	สำนักงาน จังหวัด
21	การถ่ายทอดแผนไปสู่การปฏิบัติ	- การปฏิบัติตามแผนงาน โครงการที่กำหนดไว้	ควบคุม	ตุลาคม 54 – กันยายน 55	ทุกส่วน ราชการ

ขั้นตอนที่ 4 การติดตามข้อมูลเพื่อทราบสถานะที่อาจเกิดขึ้นของความเสียหาย

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
1	ด้านบุคลากร	<ul style="list-style-type: none"> - แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงาน เพื่อป้องกันการขาดแคลนเจ้าหน้าที่ 	<ul style="list-style-type: none"> - แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดอบรมเจ้าหน้าที่ให้มีความรู้และทักษะในการใช้ระบบคอมพิวเตอร์ และระบบงานข้อมูลสารสนเทศ สามารถแก้ไขและปรับปรุงข้อมูลได้อย่างถูกต้อง เพื่อดูแลรักษาฐานข้อมูลในเบื้องต้น เพื่อลดความเสี่ยง ด้าน Human error ให้น้อยที่สุด - เจ้าหน้าที่ทำการสำรองข้อมูลให้เป็นปัจจุบันอยู่เสมอ - วางระเบียบกฎเกณฑ์ในการเข้าใช้ระบบฐานข้อมูล 	<ul style="list-style-type: none"> - คณะกรรมการที่ปรึกษาทางเทคนิค ประชุมปรึกษาหารือการแก้ไขปัญหา โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
2.	<p>ระบบไฟฟ้า</p> <p>- ไฟฟ้าดับ/ไฟกระชาก/ไฟเกิน ฯลฯ</p>	<p>- ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) และระบบไฟฟ้าสำรอง (UPS)</p>	<p>- ดำเนินการตรวจสอบการจ่ายแรงดันไฟฟ้าระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) และระบบไฟฟ้าสำรอง (UPS) อย่างสม่ำเสมอ ทุกสัปดาห์</p>	<p>- ดำเนินการตรวจสอบระบบไฟฟ้าแรงดัน 230 VAc ของห้องเครื่องมือสื่อสารปกติหรือไม่</p> <p>- ตรวจสอบระบบระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) สถานะเครื่องมือปกติหรือไม่ปกติ มีแรงดัน Output 230 VAc หรือไม่ แบตเตอรี่อยู่ในสภาพที่ใช้งานได้หรือเปล่า</p> <p>- ตรวจสอบระบบระบบไฟฟ้าสำรอง (UPS) สถานะเครื่องมือปกติหรือไม่ปกติ มีแรงดัน Output 230 VAc หรือไม่</p> <p>- หากตรวจสอบพบว่าระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) ใช้การไม่ได้ ประสานไปยัง ศสข. 9 นว. เพื่อดำเนินการแก้ไขปัญหา</p> <p>- หากใช้งานไม่ได้ ดำเนินการเปลี่ยนอุปกรณ์ระบบไฟฟ้าสำรอง</p>

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสี่ยง
3	<p>อุปกรณ์คอมพิวเตอร์ แม่ข่าย</p> <ul style="list-style-type: none"> - ซ้ำรูดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/คอนโอมิตี/โคนบรูก 	<ul style="list-style-type: none"> - ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ 	<ul style="list-style-type: none"> - กำหนดมาตรการหรือระเบียบข้อกำหนดสิทธิการเข้าถึงข้อมูล - ดำเนินการติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ 	<ul style="list-style-type: none"> - ดำเนินการตรวจสอบการทำงานของอุปกรณ์คอมพิวเตอร์แม่ข่ายว่ายังสามารถให้บริการได้หรือไม่ - ตรวจสอบอุปกรณ์รักษาความปลอดภัย (Firewall) ว่ายังทำงานได้ตามปกติหรือไม่ หากไม่ปกติ ดำเนินการแก้ไขในเบื้องต้น หรือปรึกษาผู้ชำนาญการ บริษัทผู้จัดหา ระบบรักษาความปลอดภัย (Appwork Company Limited เบอร์โทรศัพท์ 0-2282-6560-79 ต่อ 51133, 51138 และประสานไปยัง ศสข. 9 นว.

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
4	<p>ห้องศูนย์ข้อมูล</p> <p>- อุบัติภัย (ไฟไหม้, น้ำท่วม ดินถล่ม)</p>	<ul style="list-style-type: none"> - ติดตั้งระบบดับเพลิงอัตโนมัติชนิดไพโรเจนในพื้นที่ปิด (Pyrogen) - มีการให้ความรู้เจ้าหน้าที่และซักซ้อมแผนเผชิญเหตุเพลิงไหม้ 	<ul style="list-style-type: none"> - ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) เพื่อควบคุมการจ่ายไฟของระบบ - มีระบบโทรศัพท์ที่สามารถติดต่อขอความช่วยเหลือหน่วยป้องกันบรรเทาสาธารณภัยได้สะดวก รวดเร็ว - สํารวจอัตรากำลังคน สถานที่ วัสดุอุปกรณ์ เครื่องมือเครื่องใช้ของส่วนราชการในพื้นที่ เพื่อขอรับการสนับสนุนในการขนย้ายอุปกรณ์ - จังหวัดมีระบบ Pyrogen เป็นสารดับเพลิงที่เป็นละอองของเหลวที่มีประสิทธิภาพในการดับเพลิงได้ทันที โดยได้ติดตั้งอยู่ ณ สถานที่สื่อสารจังหวัด 	<ul style="list-style-type: none"> - เจ้าหน้าที่ตรวจสอบสถานที่เกิดเหตุ และดำเนินการระงับเหตุในเบื้องต้น - หากระบบระบบดับเพลิงอัตโนมัติไม่สามารถระงับเหตุได้ ให้แจ้งขอความช่วยเหลือหน่วยดับเพลิง หรือหน่วยบรรเทาสาธารณภัยในเขตรับผิดชอบ เบอร์ 199 หรือ ป้องกันจังหวัด มท. 16708 - ขนย้ายอุปกรณ์ที่เป็นชนวนในการเกิดเพลิงไหม้ออกจากสถานที่เกิดเหตุโดยเร็ว - สํารวจ/รายงานความเสียหายแจ้งให้ผู้บังคับบัญชาทราบในเบื้องต้น

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
5	<u>ห้องศูนย์ข้อมูล</u> - ความปลอดภัยในการ เข้า-ออก	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัดเป็นเขตพื้นที่หวง ห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่ เกี่ยวข้อง	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัด เป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่ เกี่ยวข้อง - กำหนดรายชื่อเจ้าหน้าที่ที่เกี่ยวข้อง และกำหนด สิทธิการเข้าถึงข้อมูล	- ดำเนินการตรวจสอบการทำงาน ของอุปกรณ์ทุกระบบว่ายังสามารถ ให้บริการได้ตามปกติหรือไม่ - ตรวจสอบระบบฐานข้อมูลว่า ได้รับความเสียหายหรือไม่
6	<u>ห้องศูนย์ข้อมูล</u> - การปรับอากาศเพื่อ รักษาอุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัตโนมัติ	- ใช้ระบบปรับอากาศที่ได้มาตรฐาน - จัดให้มีระบบปรับอากาศสำรอง - ตรวจสอบการทำงานเป็นประจำ สม่ำเสมอ	- หากระบบปรับอากาศอัตโนมัติ ชัดข้อง ให้ดำเนินการเปิดระบบปรับ อากาศสำรอง - แจ้งผู้ชำนาญการด้านเครื่องปรับ อากาศเข้าดำเนินการตรวจสอบระบบ ปรับอากาศ

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสี่ยง
7	<p><u>ระบบสื่อสาร/ระบบ เครือข่าย</u></p> <p>- โทรศัพท์/ Internet/Intranet/ระบบ ประชุมทางไกล ใช้งาน ไม่ได้ตามปกติ</p>	<p>- บำรุงรักษา ตรวจสอบ ตรวจสอบซ่อม ระบบให้สามารถใช้งานได้ ตลอดเวลา</p>	<p>- มีเจ้าหน้าที่ด้านเทคนิคตรวจสอบการทำงานของ เครือข่ายให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ</p> <p>- มีการตรวจสอบบำรุงรักษาช่องสัญญาณเครือข่ายเป็น ประจำ</p> <p>- จังหวัดมีการช่องสัญญาณสำรอง โดยดำเนินการเช่า จากผู้ให้บริการ ISP ที่ได้มาตรฐานมีความมั่นคง ปลอดภัยต่อการใช้ระบบงาน (ระบบ ISDN จาก TOT และเครือข่าย GIN)</p>	<p>- ดำเนินการตรวจสอบการทำงานของ ของอุปกรณ์ว่ายังสามารถให้บริการ ได้ตามปกติหรือไม่</p> <p>- ติดต่อหน่วยงานผู้ให้บริการ เครือข่ายทราบเพื่อขอทราบสถานะ และแจ้งหน่วยงานที่เกี่ยวข้องทราบ</p> <p>- ใช้การช่องสัญญาณสำรอง ระบบ ISDN และInternet ความเร็วสูง (GIN) กรณีเครือข่ายมหาดไทย ขัดข้อง</p>

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสี่ยง
8	<p>อุปกรณ์คอมพิวเตอร์ถูก ขโมย</p> <p>- ชำรุดเสียหายใช้งาน ไม่ได้</p> <p>- ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/ โคนโอมติ/โคนบุรุก</p>	<p>- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall</p> <p>- ติดตั้งโปรแกรม Antivirus ประจำ เครื่องคอมพิวเตอร์ลูกข่าย และทำการ Update และ Scan เป็น ประจำ</p>	<p>- กำหนดมาตรการหรือระเบียบ ข้อกำหนดคสิทธิการ เข้าถึงข้อมูล</p> <p>- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall</p> <p>- ดำเนินการติดตั้งโปรแกรม Antivirus ประจำเครื่อง คอมพิวเตอร์และทำการ Update และ Scan เป็นประจำ</p>	<p>- ดำเนินการตรวจสอบการทำงาน ของอุปกรณ์คอมพิวเตอร์ว่ายัง สามารถให้บริการได้หรือไม่</p> <p>- ตรวจสอบอุปกรณ์รักษาความ ปลอดภัย (Firewall) ว่ายังทำงานได้ ตามปกติหรือไม่ หากไม่ปกติ ดำเนินการแก้ไขในเบื้องต้น หรือ ปรึกษาผู้ชำนาญการ บริษัทผู้จัดหา ระบบรักษาความปลอดภัย (Appwork Company Limited เบอร์ โทรศัพท์ 0-2282-6560-79 ต่อ 51133, 51138 และประสานไปยัง ศสข. 9 นว.</p>

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
9	การจัดทรัพยากร สนับสนุน	- ชี้แจงทำความเข้าใจและ ประชาสัมพันธ์ให้ผู้รับบริการทราบ ถึงขั้นตอนการรับบริการ และข้อมูล การบริการ	- ดำเนินการชี้แจงทำความเข้าใจและประชาสัมพันธ์ ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และ ข้อมูลการบริการ - จัดทำแผนผังแสดงถึงขั้นตอนการขอรับบริการ	- ดำเนินการชี้แจงทำความเข้าใจและ ประชาสัมพันธ์ให้ผู้รับบริการทราบ ถึงขั้นตอนการรับบริการ และข้อมูล การบริการ
10	ค่านงบประมาณ	- จัดทำแผนงาน โครงการเพื่อขอรับ การสนับสนุนงบประมาณ	- จัดทำรายละเอียดแผนงาน โครงการเพื่อขอรับการ สนับสนุนงบประมาณจากผู้บริหาร	- ชี้แจงทำความเข้าใจกับผู้บริหาร
11	ระบบฐานข้อมูล - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดย ไม่ได้รับอนุญาต - ความเชื่อถือได้ของ ข้อมูล - ข้อมูลเสียหาย	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การ เข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	- กำหนดมาตรการหรือระเบียบ ข้อกำหนดคสิทธิการ เข้าถึงข้อมูล - ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ดำเนินการติดตั้งโปรแกรม Antivirus ประจำเครื่อง คอมพิวเตอร์และทำการ Update และ Scan เป็นประจำ - มีการ Backup ข้อมูลอย่างสม่ำเสมอ - ติดตั้งติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550	- ดำเนินการตรวจสอบการทำงาน ของอุปกรณ์คอมพิวเตอร์ว่ายัง สามารถให้บริการได้หรือไม่ - ตรวจสอบอุปกรณ์รักษาความ ปลอดภัย (Firewall) ว่ายังทำงานได้ ตามปกติหรือไม่ หากไม่ปกติ ดำเนินการแก้ไขในเบื้องต้น หรือ ปรึกษาผู้ชำนาญการ บริษัทผู้จัดหา ระบบรักษาความปลอดภัย (Appwork Company Limited เบอร์ โทรศัพท์ 0-2282-6560-79 ต่อ 51133, 51138 และประสานไปยัง ศสข. 9 นว.

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
12	การจัดการข้อมูล	<ul style="list-style-type: none"> - ตรวจสอบความถูกต้องของข้อมูลและทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของส่วนราชการ 	<ul style="list-style-type: none"> - จัดให้มีเจ้าหน้าที่รับผิดชอบในการตรวจสอบความถูกต้องของข้อมูล - ดำเนินการตรวจสอบความถูกต้องของข้อมูลอย่างสม่ำเสมอ 	<ul style="list-style-type: none"> - ดำเนินการตรวจสอบความถูกต้องของข้อมูลอย่างสม่ำเสมอ - ประสานไปยังส่วนราชการผู้รับผิดชอบข้อมูลเพื่อตรวจสอบความถูกต้อง
13	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	<ul style="list-style-type: none"> - จัดทำแผนงาน/โครงการ/กิจกรรมให้ครบถ้วน 	<ul style="list-style-type: none"> - มีจัดทำแผนงาน/โครงการ/กิจกรรม ให้ครบถ้วน - มีการทบทวนแผนงาน/โครงการ/กิจกรรม 	<ul style="list-style-type: none"> - คณะกรรมการที่ปรึกษาทางเทคนิคประชุมปรึกษาหารือการแก้ไขปัญหาโดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน
14	ผู้ปฏิบัติและการจัดการความรู้	<ul style="list-style-type: none"> - ฝึกอบรม และการจัดการความรู้ 	<ul style="list-style-type: none"> - จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการความรู้ 	<ul style="list-style-type: none"> - จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการความรู้

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
15	<p><u>การบันทึก - สำรองข้อมูล</u></p> <p>- วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล</p> <p>- เลือกสื่อบันทึกข้อมูลไม่เหมาะสม</p>	<p>- มีการ Backup ข้อมูลอย่างสม่ำเสมอ</p>	<p>- ติดตั้งระบบสำรองข้อมูล (Backup)</p> <p>- ดำเนินการสำรองข้อมูลในรูปแบบ Tap Backup และถ่ายโอนข้อมูลไปเก็บไว้ที่กระทรวงมหาดไทย อย่างสม่ำเสมอ</p>	<p>- ดำเนินการกู้คืนระบบข้อมูลที่ทำการ Backup ไว้ทันที หากไม่สามารถดำเนินการแก้ไขในเบื้องต้นได้ ให้ปรึกษาผู้ชำนาญการ บริษัทผู้จัดหาระบบ Backup (Appwork Company Limited เบอร์โทรศัพท์ 0-2282-6560-79 ต่อ 51133, 51138 และประสานไปยัง ศสข. 9 นว.</p>
16	<p>การดำเนินตามกฎหมาย กฎระเบียบที่เกี่ยวข้อง</p>	<p>- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ</p> <p>- การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550</p>	<p>- ดำเนินการชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ</p> <p>- จัดทำแผนผังแสดงถึงขั้นตอนการขอรับบริการ</p> <p>- ชี้แจงให้ผู้รับบริการตระหนักถึงการกระทำความผิด ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550</p>	<p>- ดำเนินการชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ</p> <p>- จัดทำแผนผังแสดงถึงขั้นตอนการขอรับบริการ</p> <p>- ชี้แจงให้ผู้รับบริการตระหนักถึงการกระทำความผิด ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550</p>

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
17	ความซื่อสัตย์ สุจริต ปฏิบัติ หน้าที่ตรงไปตรงมาตาม กฎหมาย กฎระเบียบไม่ แสวงหาผลประโยชน์ ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
18	ความสามัคคี การช่วยเหลือ ให้ความเคารพซึ่งกันและกัน ทำงานร่วมกันอย่างมี ประสิทธิภาพ	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
19	ความมีประสิทธิภาพ ทำงาน อย่างรวดเร็ว และใช้ ทรัพยากรที่มีอยู่อย่างจำกัด ให้ได้อย่างคุ้มค่า และก่อ ประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
20	การปฏิบัติต่อผู้อื่นด้วยความ เป็นธรรมและเท่าเทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
21	การถ่ายทอดแผนไปสู่การ ปฏิบัติ	- การปฏิบัติตามแผนงานโครงการที่กำหนด ไว้	- จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการความรู้	- จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการ ความรู้

รายชื่อเจ้าหน้าที่ผู้รับผิดชอบ

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
1	ด้านบุคลากร	<ul style="list-style-type: none"> - แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงานเพื่อป้องกันการขาดแคลนเจ้าหน้าที่ 	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
2	<u>ระบบไฟฟ้า</u> - ไฟฟ้าดับ/ไฟกระชาก /ไฟเกิน ฯลฯ	- ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) และระบบไฟฟ้าสำรอง (UPS)	ตุลาคม 54 – กันยายน 55	นายเฉลิมพล ทองโคตร
3	<u>อุปกรณ์คอมพิวเตอร์</u> <u>แม่ข่าย</u> - ซ้ำรูดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบ ฐานข้อมูล/โดนโจมตี/โดนบุกรุก	<ul style="list-style-type: none"> - ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ 	ตุลาคม 54 – กันยายน 55	นายเฉลิมพล ทองโคตร นายเอกโรจน์ ศัลยพงษ์
4	<u>ห้องศูนย์ข้อมูล</u> - อุบัติภัย (ไฟไหม้, น้ำท่วม ดึก ถล่ม)	<ul style="list-style-type: none"> - ติดตั้งระบบดับเพลิงอัตโนมัติชนิดไพโรเจนในพื้นที่ปิด (Pyrogen) - มีการให้ความรู้เจ้าหน้าที่และซักซ้อมแผนเผชิญเหตุเพลิงไหม้ 	ตุลาคม 54 – กันยายน 55	นางเพ็ญศรี กันเตียง นายเฉลิมพล ทองโคตร

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
5	<u>ห้องศูนย์ข้อมูล</u> - ความปลอดภัยในการเข้า-ออก	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัดเป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูล ฯ นางเพ็ญศรี กันตียง นายเฉลิมพล ทองโคตร นายเอกโรจน์ ศัลยพงษ์
6	<u>ห้องศูนย์ข้อมูล</u> - การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัตโนมัติ	ตุลาคม 54 – กันยายน 55	นางเพ็ญศรี กันตียง นายเฉลิมพล ทองโคตร
7	<u>ระบบสื่อสาร/ระบบเครือข่าย</u> - โทรศัพท์/Internet/Intranet/ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ	- บำรุงรักษา ตรวจสอบ ตรวจสอบระบบให้สามารถใช้งานได้ตลอดเวลา	ตุลาคม 54 – กันยายน 55	นายเฉลิมพล ทองโคตร
8	<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u> - ซ้ำรูดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โคนโอมติ/โคนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์ลูกข่าย และทำการ Update และ Scan เป็นประจำ	ตุลาคม 54 – กันยายน 55	นายเอกโรจน์ ศัลยพงษ์

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
9	การจัดทรัพยากรสนับสนุน	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
10	ด้านงบประมาณ	- จัดทำแผนงาน/โครงการเพื่อขอรับการสนับสนุนงบประมาณ	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ นายเอกโรจน์ ศัลยพงษ์
11	ระบบฐานข้อมูล - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ตุลาคม 54 – กันยายน 55	นายเฉลิมพล ทองโคตร นายเอกโรจน์ ศัลยพงษ์
12	การจัดการข้อมูล	- ตรวจสอบความถูกต้องของข้อมูล และทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของส่วนราชการ	ตุลาคม 54 – กันยายน 55	ทุกส่วนราชการ
13	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- จัดทำแผนงาน/โครงการ/กิจกรรม ให้ครบถ้วน	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ นายเอกโรจน์ ศัลยพงษ์
14	ผู้ปฏิบัติและการจัดการความรู้	- ฝึกอบรม และการจัดการความรู้	ตุลาคม 54 – กันยายน 55	ทุกส่วนราชการ

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
15	<u>การบันทึก - สำรองข้อมูล</u> - วิธีการที่ไม่ถูกต้องในการ สำรองข้อมูล - เลือกลูกบันทึกข้อมูลไม่ เหมาะสม	- มีการ Backup ข้อมูลอย่างสม่ำเสมอ	ตุลาคม 54 – กันยายน 55	นายเฉลิมพล ทองโคตร
16	การดำเนินตามกฎหมาย กฎ ระเบียบที่เกี่ยวข้อง	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึง ขั้นตอนการรับบริการ และข้อมูลการบริการ - การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
17	ความซื่อสัตย์ สุจริต ปฏิบัติ หน้าที่ตรงไปตรงมาตาม กฎหมาย กฎระเบียบไม่แสวงหา ผลประโยชน์ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
18	ความสามัคคี การช่วยเหลือให้ ความเคารพซึ่งกันและกันทำงาน ร่วมกันอย่างมีประสิทธิภาพ	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
19	ความมีประสิทธิภาพ ทำงาน อย่างรวดเร็ว และใช้ทรัพยากรที่ มีอยู่อย่างจำกัดให้ได้อย่างคุ้มค่า และก่อประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
20	การปฏิบัติต่อผู้อื่นด้วยความเป็น ธรรมและเท่าเทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลัก ธรรมาภิบาล	ตุลาคม 54 – กันยายน 55	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
21	การถ่ายทอดแผนไปสู่การปฏิบัติ	- การปฏิบัติตามแผนงาน โครงการที่กำหนดไว้	ตุลาคม 54 – กันยายน 55	ทุกส่วนราชการ

ขั้นตอนที่ 5 การติดตาม กำกับ ตรวจสอบการปฏิบัติการควบคุมความเสี่ยง และทบทวนแผนบริหารความเสี่ยง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
1	ด้านงบประมาณ	- จัดทำแผนงาน โครงการเพื่อขอรับการสนับสนุนงบประมาณ	ยังคงมีผลกระทบด้านงบประมาณอย่างต่อเนื่องแต่ระบบต่าง ๆ ไม่ได้มีการเปลี่ยนแปลงเพิ่มเติมอุปกรณ์แต่อย่างใด ยังคงใช้อุปกรณ์ที่มีอยู่ให้เกิดประโยชน์สูงสุด	15 (3) x (5)	3	5	15
2	<u>ระบบไฟฟ้า</u> - ไฟฟ้าดับ/ไฟกระชาก/ไฟเกิน ฯลฯ	- ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) และระบบไฟฟ้าสำรอง (UPS)	ระบบไฟฟ้าเมื่อมีการติดตั้งระบบป้องกัน พบว่าระบบงานใช้งานแม้ว่าจะมีไฟฟ้าท้องถิ่นดับบางบางครั้ง แต่ไม่ส่งผลกระทบต่อระบบมากนัก	20 (4) x (5)	4	4	16

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับ ความ เสี่ยงเดิม	โอกาส คงเหลือ (1)	ผลกระทบ คงเหลือ (2)	ระดับความ เสี่ยง คงเหลือ (1) x (2)
3	ด้านบุคลากร	<ul style="list-style-type: none"> - แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงาน เพื่อป้องกันการขาดแคลนเจ้าหน้าที่ 	<ul style="list-style-type: none"> - การฝึกอบรมเจ้าหน้าที่จะดำเนินการตามแผนการจัดการความรู้ ยังคงความสำคัญในการพัฒนาบุคลากรไว้เป็นลำดับแรก 	20 (4) x (5)	4	5	20
4	การบันทึก - สำรองข้อมูล <ul style="list-style-type: none"> - วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล - เลือกสื่อบันทึกข้อมูลไม่เหมาะสม 	<ul style="list-style-type: none"> - มีการ Backup ข้อมูลอย่างสม่ำเสมอ 	<ul style="list-style-type: none"> ดำเนินการ Backup ข้อมูลเพื่อป้องกันการสูญหายอยู่ตลอดเวลา ซึ่งมีความสำคัญมากเมื่อระบบเกิดขัดข้อง 	20 (3) x (3)	4	5	20

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับ ความ เสี่ยงเดิม	โอกาส คงเหลือ (1)	ผลกระทบ คงเหลือ (2)	ระดับความ เสี่ยง คงเหลือ (1) x (2)
5	<u>ห้องศูนย์ข้อมูล</u> - การปรับอากาศเพื่อรักษา อุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัตโนมัติ	ปัจจุบันเครื่องมือ สื่อสารและอุปกรณ์ ต่าง ๆ ได้เพิ่มเติม จำนวนมาก ทำให้ อุณหภูมิภายในห้อง เพิ่มสูงขึ้นมาก ซึ่งจะ ส่งผลกระทบต่อ อุปกรณ์ต่าง ๆ ภายใน ห้องเครื่องมือสื่อสาร เป็นอย่างมาก	16 (4) x (4)	4	5	20
6	<u>อุปกรณ์คอมพิวเตอร์ แม่ข่าย</u> - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลาย ระบบฐานข้อมูล/โดเมนโจมตี/ โดเมนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่อง คอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ	ยังคงมีความ จำเป็นต้องคง มาตรการป้องกัน Antivirus สำหรับ เครื่องแม่ข่ายอย่าง ต่อเนื่อง เนื่องจากมี ความเสี่ยงสูงมากขึ้น ที่ Server จะถูกโจมตี จากไวรัสทั้งภายนอก และภายใน	20 (4) x (5)	4	5	20

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรม ควบคุม ความเสี่ยง	ผลจากการใช้มาตรการ	ระดับ ความ เสี่ยง เดิม	โอกาส คงเหลือ (1)	ผลกระทบ คงเหลือ (2)	ระดับ ความ เสี่ยง คงเหลือ (1) x (2)
7	<u>ห้องศูนย์ ข้อมูล</u> - อุบัติภัย (ไฟไหม้, น้ำ ท่วม ตึก ถล่ม)	- ติดตั้ง ระบบ ดับเพลิง อัตโนมัติ ชนิดไฟโร เจนในพื้นที่ ปิด (Pyrogen) - มีการให้ ความรู้ เจ้าหน้าที่ และ ชัก ซ้อมแผน เผชิญเหตุ เพลิงไหม้	เหตุเพลิงไหม้ไม่เกิดเหตุแต่ยังคงเฝ้าระวัง กรณีน้ำท่วมและตึกถล่ม เกิดขึ้นได้ยาก เนื่องจากตัวอาคารศาลากลางจังหวัดมั่นคงแข็งแรง	20 (4) x (5)	4	5	20
8	<u>อุปกรณ์ คอมพิวเตอร์</u>	- ติดตั้ง อุปกรณ์	มีการแพร่กระจายของไวรัสบางแต่ยังไม่ส่งผลกระทบต่อระบบ Server หลัก	16 (4) x	4	4	16

	<u>ลูกข่าย</u> - ซ้ำรูป เสียหายใช้ งานไม่ได้ - ไวรัส/ สปายแวร์ ทำลายระบบ ฐานข้อมูล/ โดนโจมตี/ โดนบุกรุก	รักษาความ ปลอดภัย Firewall - ติดตั้ง โปรแกรม Antivirus ประจำ เครื่อง คอมพิวเตอร์ ลูกข่าย และทำการ Update และ Scan เป็น ประจำ		(4)			
ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรม ควบคุม ความเสี่ยง	ผลจากการใช้มาตรการ	ระดับ ความ เสี่ยง เดิม	โอกาส คงเหลือ (1)	ผลกระทบ คงเหลือ (2)	ระดับ ความ เสี่ยง คงเหลือ (1) x (2)
9	<u>ห้องศูนย์</u> <u>ข้อมูล</u> - ความ	- กำหนด พื้นที่ห้อง เครื่องมือ	เมื่อมีการกำหนดมาตรการขึ้นมามีเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้นที่เข้าออกพื้นที่	16 (4) x (4)	4	4	16

	ปลอดภัยในการเข้า-ออก	สื่อ สาร สำนักงาน จังหวัดเป็น เขต พื้นที่ หวง ห้าม เต็ม หมด เฉพาะ เจ้าหน้าที่ที่เกี่ยวข้อง					
10	ผู้ปฏิบัติและ การจัดการ ความรู้	- ฝึกอบรม และ การ จัด ก า ร ความรู้	ดำเนินการตามแผนการจัดการความรู้ ยังคงพบว่าผู้ปฏิบัติงานมีการฝึกอบรมด้าน IT น้อย	12 (3) x (4)	4	4	16

ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้ มาตรการ	ระดับ ความ เสี่ยงเดิม	โอกาส คงเหลือ (1)	ผลกระทบ คงเหลือ (2)	ระดับ ความ เสี่ยง คงเหลือ (1) x (2)
11	ระบบฐานข้อมูล - การเข้าถึงข้อมูล ไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับ	หลังจากการติดตั้ง ระบบรักษาความปลอดภัยและทำ	15 (3) x (5)	3	5	15

	<p>รับอนุญาต</p> <ul style="list-style-type: none"> - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย 	คอมพิวเตอร์ พ.ศ. 2550	<p>ความเข้าใจกับ ผู้ให้บริการ ซึ่งส่วน ใหญ่อยู่ภายในศาลา กลางจังหวัดและ ส่วนราชการ เป็น ประจำทำให้มีความ เข้าใจและตระหนัก มากขึ้น</p>				
12	การจัดการข้อมูล	<ul style="list-style-type: none"> - ตรวจสอบความถูกต้องของข้อมูล และ ทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของ ส่วนราชการ 	<p>มีเจ้าหน้าที่ ดำเนินการ ตรวจสอบความ ถูกต้องประกอบกับ มีการยืนยันจาก ผู้รับผิดชอบข้อมูล ทำให้มีความถูกต้อง ของข้อมูลมากขึ้น</p>	15 (3) x (5)	3	5	15
ลำดับ ความ เสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลการใช้ มาตรการ	ระดับ ความ เสี่ยงเดิม	โอกาส คงเหลือ (1)	ผลกระทบ คงเหลือ (2)	ระดับ ความ เสี่ยง คงเหลือ (1) x (2)
13	<p><u>ระบบสื่อสาร/ระบบ เครือข่าย</u></p> <ul style="list-style-type: none"> - โทรศัพท์/ 	<ul style="list-style-type: none"> - บำรุงรักษา ตรวจสอบ ตรวจสอบซ่อมระบบให้ สามารถใช้งานได้ ตลอดเวลา 	<p>เนื่องจากระบบต่าง ๆ ได้มีการติดตั้ง ระบบเครือข่าย</p>	16 (4) x (4)	4	4	16

	Internet/Intranet/ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ		สำรองไว้ ถึงแม้ระบบหลักไม่สามารถใช้งานได้แต่ระบบเครือข่ายสำรองสามารถใช้งานทดแทนได้				
14	การจัดทรัพยากรสนับสนุน	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการและข้อมูลการบริการ	ได้มีการประชาสัมพันธ์ทำความเข้าใจรวมถึงทำป้ายแสดงถึงขั้นตอนและระยะเวลาการให้บริการอย่างชัดเจน ทำให้ผู้ให้บริการมีความเข้าใจมากขึ้น	16 (4) x (4)	3	4	12
ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
15	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- จัดทำแผนงาน/โครงการ/กิจกรรม ให้ครบถ้วน	มีการประชุมปรึกษาหารือรวมทั้งมีการทบทวน	10 (2) x (5)	2	5	10

			แผนงาน โครงการ				
16	การดำเนินการตามกฎหมาย กฎระเบียบที่เกี่ยวข้อง	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการและข้อมูลการบริการ - การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ได้มีการประชาสัมพันธ์ทำความเข้าใจรวมถึงทำป้ายแสดงถึงขั้นตอนและระยะเวลาการให้บริการอย่างชัดเจน ทำให้ผู้ให้บริการมีความเข้าใจมากขึ้น	9 (3) x (3)	3	3	9
17	ความซื่อสัตย์ สุจริต ปฏิบัติหน้าที่ตรงไปตรงมาตามกฎหมาย กฎระเบียบไม่แสวงหาผลประโยชน์ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรมคุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับผู้ปฏิบัติงานให้ทราบถึงผลกระทบต่อองค์กร	9 (3) x (3)	3	3	9
ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
18	ความสามัคคี การช่วยเหลือให้ความเคารพซึ่งกันและกันทำงานร่วมกันอย่างมี	- สนับสนุนให้บุคลากรมีจริยธรรมคุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับผู้ปฏิบัติงานให้ทราบถึงผลกระทบต่อ	12 (3) x (3)	3	3	9

	ประสิทธิภาพ		องค์กร				
19	ความมีประสิทธิภาพ ทำงานอย่างรวดเร็ว และใช้ ทรัพยากรที่มีอยู่อย่างจำกัด ให้ได้อย่างคุ้มค่า และก่อ ประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับ ผู้ปฏิบัติงานให้ทราบ ถึงผลกระทบต่อ องค์กร	12 (3) x (4)	2	4	8
20	การปฏิบัติต่อผู้อื่นด้วย ความเป็นธรรมและเท่า เทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับ ผู้ปฏิบัติงานให้ทราบ ถึงผลกระทบต่อ องค์กร	9 (3) x (3)	2	4	8
21	การถ่ายทอดแผนไปสู่การ ปฏิบัติ	- การปฏิบัติตามแผนงาน โครงการที่กำหนด ไว้	มีการปรึกษาหารือ กันเป็นประจำ ระหว่างบังคับบัญชา กับปฏิบัติงานอยู่ เสมอ	6 (2) x (3)	2	3	6