แผนการบริหารความเสี่ยง

กระบวนงาน การพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัย

ประจำปี ๒๕๕๖

แผนกการบริหารความเสี่ยงของส่วนราชการ

ส่วนราชการ	**จังหวัดพิจิตร**
ประเด็นยุทธศาสตร์	**พัฒนาองค์การและบริหารกิจการบ้านเมืองที่ดี**
กระบวนงาน	**การพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัย**
ผู้ทบทวน **(นายบุญเวทย์ ศรีพวงใจ)** **หัวหน้าสำนักงานจังหวัดพิจิตร**	**ผู้อนุมัติ**

<u>กระบวนงาน</u> การพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัย

<u>กระบวนการสร้างคุณค่า</u>

ความสำคัญของกระบวนงาน

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 ที่มีโอกาสเกิดขึ้นได้ในอนาคตภายใต้สภาวการณ์ที่ไม่แน่นอน ซึ่งอาจจะทำให้ไม่บรรลุเป้าหมาย ดังนั้น การตัดสินใจกระทำการใด ๆ โดยไม่มีข้อมูล หรือไม่มีการวางแผนใดๆ จึงสามารถกล่าวได้ว่าเป็นการเสี่ยงตัดสินใจในภาวะของความเสี่ยง

การเสี่ยง หมายถึง การตัดสินใจที่จะดำเนินการสิ่งใดสิ่งหนึ่งบนพื้นฐานของการขาดข้อมูลที่ชัดเจน ไม่ครบถ้วน เป็นเพียงการประมาณการ การคาดเดาผลของการตัดสินใจนั้นอาจเป็นไปตามความคาดหมายหรือตรงกันข้ามก็ได้

ความไม่แน่นอน หมายถึง ความเปลี่ยนแปลง ไม่คงที่คงเดิมตลอดเวลาหรือเหตุการณ์ต่าง ๆ ที่มีโอกาสเกิดขึ้นได้ทั้งที่เป็นไปตามความคาดหมายหรือนอกเหนือความคาดหมาย

ปัญหา หมายถึง สิ่งที่เกิดขึ้นและมักส่งผลในทางลบ เป็นอุปสรรคต่อเป้าหมายการดำเนินการ จำเป็นต้องมีการแก้ไข เพราะมิเช่นนั้นปัญหาดังกล่าวอาจก่อให้เกิดความเสียหายตามมา

ความเสี่ยงของระบบเทคโนโลยีสารสนเทศ หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นได้ในอนาคตใต้สภาวการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหายหรือล้มเหลวที่จะบรรลุผลสำเร็จ ต่อการบริหารงานระบบเทคโนโลยีสารสนเทศจังหวัด

การบริหารความเสี่ยง (Risk Management) หมายถึง การปฏิบัติการใด ๆ เพื่อควบคุมความสี่ยง 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 จึงจำเป็นอย่างยิ่งที่จะต้องการเตรียมการและวางแผนรองรับปัญหาเดียวกับความเสี่ยง และภัยพิบัติต่างๆ ที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัด

2. วัตถุประสงค์

1) เพื่อเตรียมความพร้อม และรองรับสถานการณ์ฉุกเฉินที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของจังหวัดพิจิตร

2) เพื่อกำหนดมาตรการในการป้องกันความเสียหายที่จะเกิดกับระบบเทคโนโลยีสารสนเทศของจังหวัดพิจิตร จากภาวะความเสี่ยงต่าง ๆ

3) เพื่อให้ระบบเทคโนโลยีสารสนเทศของจังหวัด สามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ

4) เป็นการเผยแพร่ข้อมูลด้านการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศให้เจ้าหน้าที่ที่เกี่ยวข้องนำไปใช้ประโยชน์

3. องค์ประกอบของระบบเทคโนโลยีสารสนเทศ

1) Hardware หมายถึง อุปกรณ์ต่าง ๆ 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

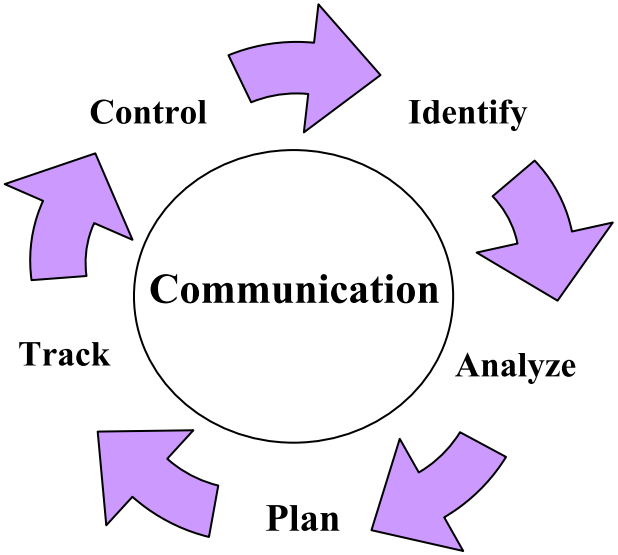
5. การประเมินสถานการณ์ความเสี่ยงที่อาจเกิดขึ้น

จากความหมายของความเสี่ยง ซึ่งมักจะหมายถึงความเป็นไปได้ในอนาคตที่อาจจะทำให้เกิดผลในทางลบขึ้น กับระบบเทคโนโลยีสารสนเทศ จึงตระหนักและให้ความสำคัญของความเสี่ยง และได้มีความบริหารความเสี่ยงที่จะเกิดขึ้น โดยเลือกใช้กลยุทธ์ที่เหมาะสมกับความเป็นไปได้ของสถานการณ์ที่อาจก่อให้เกิดปัญหาและสามารถแก้ไขเหตุการณ์ได้อย่างทันท่วงที โดยป้องกันมิให้เกิดความเสียหายตามมา ก็จะทำให้งานสำเร็จตามเป้าประสงค์

จากโครงสร้างเครือข่ายการทำงานของศูนย์ปฏิบัติการจังหวัดพิจิตร ประกอบด้วยอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์สารสนเทศต่าง ๆ และโครงสร้างการทำงานของระบบ พบว่าความเสี่ยงที่อาจเป็นอันตราย ต่อระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นองค์ประกอบหลักในระบบฐานข้อมูลสารสนเทศของจังหวัดสามารถของจังหวัด สามารถจำแนกความเสี่ยงได้ดังนี้

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

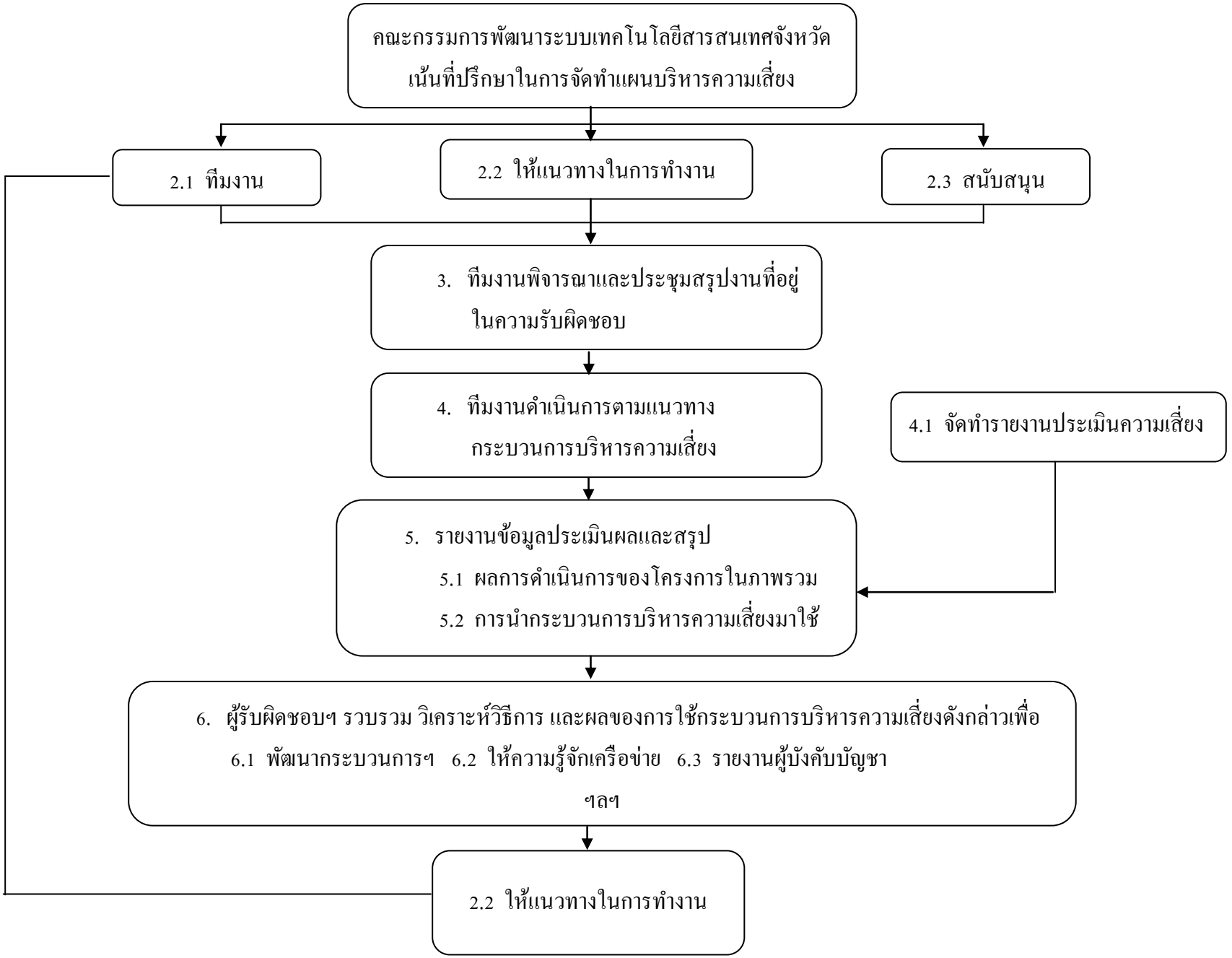
6. กระบวนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ



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

องค์ประกอบที่สำคัญอีกประการหนึ่ง ที่เกี่ยวข้องในการบริหารความเสี่ยงคือการติดต่อสื่อสาร (Communication) เพราะการดำเนินการต่าง ๆ ต้องอาศัยการประสานงาน เชื่อมโยงกับทุกฝ่ายทั้งภายในและภายนอกหน่วยงาน

7. ผังแนวทางในการจัดทำรายงานการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศจังหวัดพิจิตร



ขั้นตอนที่ 1 การระบุความเสี่ยง

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 - ระบบงานเกิดการชะงักเนื่องจากมีการปรับเปลี่ยนตามระบบราชการ (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 - ขาดระบบและขั้นตอนการดำเนินการที่มีประสิทธิภา

ขั้นตอนที่ 1 การระบุความเสี่ยง (ต่อ)

ประเภทความเสี่ยง	กระบวนการ/กิจกรรม	ความเสี่ยงที่อาจเกิดขึ้น
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ - ห้องศูนย์ข้อมูล	ความปลอดภัยในการเข้า - ออก	- ระบบเทคโนโลยีสารสนเทศเกิดความเสียหายใช้การไม่ได้ข้อมูลถูกทำลายโดยที่ตั้งใจ และไม่ตั้งใจ
	การปรับอากาศ เพื่อรักษาอุณหภูมิของห้อง	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้
	อุบัติภัย (ไฟไหม้,น้ำท่วม,ตึกถล่ม)	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้ข้อมูลถูกทำลายเสียหาย
ระบบไฟฟ้า	ไฟฟ้าดิบ,ไฟฟ้ากระชาก,ไฟฟ้าเกิน,ไฟฟ้าผ่า	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้ข้อมูลถูกทำลายเสียหาย
ระบบสื่อสาร - ระบบเครือข่าย	โทรศัพท์,อินทราเน็ต,อินเตอร์เน็ต ใช้งานไม่ได้ตามปกติ,ระบบประชุมทางไกล	- ระบบเทคโนโลยีสารสนเทศใช้งานไม่ได้
อุปกรณ์คอมพิวเตอร์แม่ข่าย	ชำรุดเสียหาย ไม่สามารถใช้งานได้ตามปกติ ไวรัส,สปายแวร์ ทำลายระบบฐานข้อมูล โดนโจมตี,โดนบุกรุก	- ระบบฐานข้อมูลใช้งานไม่ได้,ข้อมูลทำลายเสียหาย
อุปกรณ์คอมพิวเตอร์ลูกข่าย	ชำรุดเสียหาย ไม่สามารถใช้งานได้ตามปกติ ไวรัส,สปายแวร์ ทำลายระบบฐานข้อมูล โดนโจมตี,โดนบุกรุก	- ระบบฐานข้อมูลใช้งานไม่ได้,ข้อมูลทำลายเสียหาย
อุปกรณ์เครือข่าย , อุปกรณ์สื่อสาร	อุปกรณ์ชำรุดเสียหาย,ไม่สามารถใช้งานได้ตามปกติ ตัวนำสัญญาณ,สายสัญญาณต่าง ๆขาดชำรุด	- ระบบฐานข้อมูลใช้งานไม่ได้
ด้านระบบฐานข้อมูล	การเข้าถึงข้อมูลไม่ได้/การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต/ความเชื่อถือไม่ได้ของข้อมูล/ข้อมูลเสียหาย	- ระบบฐานข้อมูลใช้งานไม่ได้ - มีการวิ่งไหลของข้อมูล - ข้อมูลถูกทำลาย

ขั้นตอนที่ 1 การระบุความเสี่ยง (ต่อ)

ประเภทความเสี่ยง	กระบวนการ/กิจกรรม	ความเสี่ยงที่อาจเกิดขึ้น
ด้านการบันทึกสำรองข้อมูล	วิธีการที่ไม่ถูกต้องในการสำรองข้อมูลเลือกสื่อบันทึกข้อมูลไม่เหมาะสม	- ข้อมูลสำรอง เสียหายใช้งานใช้ได้ - ไม่สามารถกู้คืนข้อมูลได้
ความเสี่ยงด้านกระบวนงาน	การจัดการข้อมูล	- แผนการจัดการความรู้ไม่สอดคล้องกับการปฏิบัติงาน
	ผู้ปฏิบัติและการจัดการความรู้	- องค์ความรู้ไม่เพียงพอ ผลกระบวนการเรียนรู้ ไม่เหมาะสมสอดคล้องกับกระบวนงาน
	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 ซึ่งสามารถจำแนกผลกระทบที่อาจเกิดขึ้นจากความเสี่ยง อาจเป็น 5 ระดับ ดังนี้

ระดับ	ผลกระทบ	ความเสียหาย
5	สูงมาก	- องค์กรไม่สามารถดำเนินงานพื้นฐานได้ และประสิทธิภาพลดลงสูงเกิน 60% - องค์กรได้รับความเสียหายต่อทรัพย์สินเกิน 20% - บุคลากรขององค์กรได้รับอันตรายสูงถึงขั้นเสียชีวิตหรือบาดเจ็บอย่างร้ายแรงมาก - องค์กรเสียชื่อเสียงในวงกว้างขวาง เช่น ตกเป็นข่าวในหนังสือพิมพ์
4	สูง	- องค์กรไม่สามารถดำเนินงานพื้นฐานได้ และประสิทธิภาพลดลงสูงเกิน 40% - องค์กรได้รับความเสียหายต่อทรัพย์สินเกิน 10% - บุคลากรได้รับอันตรายถึงขั้นเสียชีวิต หรือบาดเจ็บอย่างรุนแรง - องค์กรเสียชื่อเสียงในวงกว้างขวาง เช่น ตกเป็นข่าวในหนังสือพิมพ์
3	ปานกลาง	- องค์กรสามารถดำเนินงานพื้นฐานได้แต่ประสิทธิภาพลดลง โดยประมาณไม่เกิน 40% - องค์กรได้รับความเสียหายต่อทรัพย์สินไม่เกิน 10% - บุคลากรได้รับอันตรายถึงขั้นต้องเข้ารับการรักษาในโรงพยาบาล แต่ไม่ถึงขั้นเสียชีวิต - องค์กรเสียชื่อเสียงในวงจำกัด
4	น้อย	- องค์กรสามารถดำเนินการพื้นฐานได้ แต่ประสิทธิภาพลดลงบ้างไม่เกิน 20% - องค์กรได้รับความเสียหายต่อทรัพย์สินโดยประมาณไม่เกิน 5% - บุคลากรได้รับอันตรายเล็กน้อยไม่ถึงขนาดเข้ารับการรักษาที่โรงพยาบาล - องค์กรเสียชื่อเสียงในวงจำกัด
5	น้อยมาก	- องค์กรสามารถดำเนินการพื้นฐานได้ แต่ประสิทธิภาพลดลงเล็กน้อยไม่เกิน 10% - องค์กรได้รับความเสียหายต่อทรัพย์สินโดยประมาณไม่เกิน 2.5% - บุคลากรได้รับอันตรายเล็กน้อย - องค์กรแทบไม่เสียชื่อเสียง

ระดับของความเสี่ยง

ระดับของความเสียง พิจารณาจากความสัมพันธ์ระหว่างโอกาสหรือความถี่ที่จะเกิดความเสี่ยงกับผลกระทบที่อาจเกิดความเสี่ยงกับผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงนั้น โดยความสัมพันธ์ดังปรากฏในแผนภาพแสดงระดับความเสี่ยง ดังต่อไปนี้

โอกาสที่จะเกิดความเสี่ยง

ความรุนแรงของความเสียงที่เกิดขึ้น	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 แ ละเสียชื่อเสียงในวงจำกัด

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	
ความเสี่ยงเชิงยุทธศาสตร์	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 - ระบบงานเกิดการชะงักเนื่องจากมีการปรับเปลี่ยนตามระบบราชการ(โยกย้าย)	4	5	20	สูงมาก

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร (ต่อ)

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	
ความเสี่ยงด้านธรรมาภิบาล	ความซื่อสัตย์ สุจริต ปฏิบัติหน้าที่ตรงไปตรงมาตามกฎหมาย กฎระเบียบไม่แสวงหาผลประโยชน์ส่วนตัว	- ใช้อำนาจหน้าที่เพื่อเอื้อประโยชน์ต่อพวกพ้อง - ใช้ช่องโหว่ทางกฎหมายเพื่อแสวงหาประโยชน์ส่วนตัว	3	4	12	ปานกลาง
	การปฏิบัติต่อผู้อื่นด้วยความเป็นธรรมและเท่าเทียมกัน	- การปฏิบัติต่อผู้รับบริการอย่างไม่เป็นธรรมเสมอภาค - เอื้อประโยชน์ให้กลุ่มใดกลุ่มหนึ่งเป็นพิเศษ	3	3	9	ปานกลาง
	ความสามัคคี การช่วยเหลือให้ความเคารพซึ่งกันและกัน ทำงานร่วมกันอย่างมีประสิทธิภาพ	- แบ่งพรรคแบ่งพวกในการทำงาน - ไม่ให้ความร่วมมือในการทำงาน	3	4	12	ปานกลาง
	ความมีประสิทธิภาพ ทำงานอย่างรวดเร็ว และใช้ทรัพยากรที่มีอยู่อย่างจำกัดให้ได้อย่างคุ้มค่า และก่อประโยชน์สูงสุด	- การปฏิบัติงานล่าช้ากว่ากำหนดไม่เป็นไปตามแผนที่กำหนดไว้ - ขาดระบบและขั้นตอนการดำเนินการที่มีประสิทธิภาพ	3	4	12	ปานกลาง

ตารางประเมินความเสี่ยงการพัฒนาเทคโนโลยีและสารสนเทศที่ทันสมัยจังหวัดพิจิตร (ต่อ)

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	**<u>ห้องศูนย์ข้อมูล</u>** - ความปลอดภัยในการเข้า-ออก	- ระบบเทคโนโลยีสารสนเทศเกิดความเสียหายใช้การไม่ได้ ข้อมูลถูกทำลายโดยที่ตั้งใจและไม่ตั้งใจ	4	4	16	สูง
	- การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้	4	4	16	สูง
	- อุบัติภัย (ไฟไหม้,น้ำท่วม ตึกถล่ม)	- อุปกรณ์ชำรุดไม่สามารถใช้งานได้ข้อมูลถูกทำลายเสียหาย	4	5	20	สูงมาก
	<u>ระบบไฟฟ้า</u> - 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/โดนโจมตี/โดนบุรุก	- ระบบฐานข้อมูลใช้งานไม่ได้ - ข้อมูลถูกทำลาย	4	5	20	สูงมาก
	<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u> - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- 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	**<u>การบันทึก - สำรวจข้อมูล</u>** - วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล - เลือกสื่อบันทึกข้อมูลไม่เหมาะสม	- ข้อมูลสำรองเสียหายใช้งานไม่ได้ไม่สามารถกู้คืนข้อมูลได้	3	3	9	กลาง
ความเสี่ยงด้านกระบวนงาน	การจัดการข้อมูล	- มีข้อมูลที่ไม่ถูกต้อง ล่าช้าหรือเชื่อถือไม่ได้	3	5	15	สูง
	ผู้ปฏิบัติและการจัดการความรู้	- แผน จัดการความรู้ไม่สอดคล้องกับการปฏิบัติงาน - องค์ความรู้ไม่เพียงพอ หรือกระบวนการเรียนรู้ ไม่เหมาะสมสอดคล้องกับกระบวนงาน	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

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
1	ด้านบุคลากร	- แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงานเพื่อป้องกันการขาดแคลนเจ้าที่	ถ่ายโอน	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
2	**<u>ระบบไฟฟ้า</u>** - ไฟฟ้าดับ/ไฟกระชาก /ไฟเกิน ฯลฯ	- ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) และระบบไฟฟ้าสำรอง (UPS)	ยอมรับ	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
3	**<u>อุปกรณ์คอมพิวเตอร์แม่ข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
4	**<u>ห้องศูนย์ข้อมูล</u>** - อุบัติภัย (ไฟไหม้,น้ำท่วม ตึกถล่ม)	- ติดตั้งระบบดับเพลิงอัตโนมัติชนิดไพโรเจนในพื้นที่ปิด (Pyrogen) - มีการให้ความรู้เจ้าหน้าที่และซักซ้อมแผนเผชิญเหตุเพลิงไหม้	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
5	**<u>ห้องศูนย์ข้อมูล</u>** - ความปลอดภัยในการเข้า-ออก	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัดเป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
6	**<u>ห้องศูนย์ข้อมูล</u>** - การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัตโนมัติ	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
7	**<u>ระบบสื่อสาร/ระบบเครือข่าย</u>** - โทรศัพท์/Internet/Intranet/ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ	- บำรุงรักษา ตรวจสอบ ตรวจซ่อมระบบให้สามารถใช้งานได้ตอลดเวลา	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
8	**<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์ลูกข่าย และทำการ Update และ Scan เป็นประจำ	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
9	การจัดทรัพยากรสนับสนุน	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
10	ด้านงบประมาณ	- จัดทำแผนงานโครงการเพื่อขอรับการสนับสนุนงบประมาณ	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
11	**<u>ระบบฐานข้อมูล</u>** - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
12	การจัดการข้อมูล	- ตรวจสอบความถูกต้องของข้อมูล และทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของส่วนราชการ	ควบคุม	ตุลาคม 55 – กันยายน 56	ทุกส่วนราชการ
13	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- จัดทำแผนงาน/โครงการ/กิจกรรม ให้ครบถ้วน	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
14	ผู้ปฏิบัติและการจัดการความรู้	- ฝึกอบรม และการจัดการความรู้	ควบคุม	ตุลาคม 55 – กันยายน 56	ทุกส่วนราชการ

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
15	**<u>การบันทึก - สำรวจข้อมูล</u>** - วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล - เลือกสื่อบันทึกข้อมูลไม่เหมาะสม	- มีการ Backup ข้อมูลอย่างสม่ำเสมอ	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
16	การดำเนินตามกฎหมาย กฎระเบียบที่เกี่ยวข้อง	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ - การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
17	ความซื่อสัตย์ สุจริต ปฏิบัติหน้าที่ตรงไปตรงมาตามกฎหมาย กฎระเบียบไม่แสวงหาผลประโยชน์ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	วิธีกำจัดความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
18	ความสามัคคี การช่วยเหลือให้ความเคารพซึ่งกันและกันทำงานร่วมกันอย่างมีประสิทธิภาพ	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
19	ความมีประสิทธิภาพ ทำงานอย่างรวดเร็ว และใช้ทรัพยากรที่มีอยู่อย่างจำกัดให้ได้อย่างคุ้มค่าและก่อประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
20	การปฏิบัติต่อผู้อื่นด้วยความเป็นธรรมและเท่าเทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ควบคุม	ตุลาคม 55 – กันยายน 56	สำนักงานจังหวัด
21	การถ่ายทอดแผนไปสู่การปฏิบัติ	- การปฏิบัติตามแผนงานโครงการที่กำหนดไว้	ควบคุม	ตุลาคม 55 – กันยายน 56	ทุกส่วนราชการ

ขั้นตอนที่ 4 การติดตามข้อมูลเพื่อทราบสภาวะที่อาจจะเกิดขึ้นของความเสี่ยง

ตารางการตอบสนองความเสี่ยงด้านเทคโนโลยีสารสนเทศจังหวัด

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
1	ด้านบุคลากร	- แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงานเพื่อป้องกันการขาดแคลนเจ้าที่	- แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดอบรมเจ้าหน้าที่ให้มีความรู้และทักษะในการใช้ระบบคอมพิวเตอร์ และระบบงานข้อมูลสารสนเทศ สามารถแก้ไขและปรับปรุงข้อมูลได้อย่างถูกต้อง เพื่อดูแลรักษาฐานข้อมูลในเบื้องต้น เพื่อลดความเสี่ยง ด้าน Human error ให้น้อยที่สุด - เจ้าหน้าที่ทำการสำรองข้อมูลให้เป็นปัจจุบันอยู่เสมอ - วางระเบียบกฎเกณฑ์ในการเข้าใช้ระบบฐานข้อมูล	- คณะกรรมการที่ปรึกษาทางเทคนิคประชุมปรึกษาหารือการแก้ไขปัญหาโดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน

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

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
3	**<u>อุปกรณ์คอมพิวเตอร์แม่ข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ	- กำหนดมาตรการหรือระเบียบข้อกำหนดสิทธิการเข้าถึงข้อมูล - ดำเนินการติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ	- ดำเนินการตรวจสอบการทำงานของอุปกรณ์คอมพิวเตอร์แม่ข่ายว่ายังสามารถให้บริการได้หรือไม่ - ตรวจสอบอุปกรณ์รักษาความปลอดภัย (Firewall) ว่ายังทำงานได้ตามปกติหรือไม่ หากไม่ปกติดำเนินการแก้ไขในเบื้องต้น หรือปรึกษาผู้ชำนาญการ บริษัทผู้จัดหาระบบรักษาความปลอดภัย (Appwork Company Limited เบอร์โทรศัพท์ 0-2282-6560-79 ต่อ 51133, 51138 และประสานไปยัง ศสข. 9 นว.

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
4	**<u>ห้องศูนย์ข้อมูล</u>** - อุบัติภัย (ไฟไหม้,น้ำท่วม ตึกถล่ม)	- ติดตั้งระบบดับเพลิงอัติโนมัติชนิดไพโรเจนในพื้นที่ปิด (Pyrogen) - มีการให้ความรู้เจ้าหน้าที่และซักซ่อมแผนเผชิญเหตุเพลิงไหม้	- ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) เพื่อควบคุมการจ่ายไฟของระบบ - มีระบบโทรศัพท์ที่สามารถติดต่อขอความช่วยเหลือหน่วยป้องกันบรรเทาสาธารณภัยได้สะดวก รวดเร็ว - สำรวจอัตรากำลังคน สถานที่ วัสดุอุปกรณ์เครื่องมือเครื่องใช้ของส่วนราชการในพื้นที่ เพื่อขอรับการสนับสนุนในการขนย้ายอุปกรณ์ - จังหวัดมีระบบ Pyrongen เป็นสารดับเพลิงที่เป็นละอองของเหลวที่มีประสิทธิภาพในการดับเพลิงได้ทันที โดยได้ติดตั้งอยู่ ณสถานีสื่อสารจังหวัด	- เจ้าหน้าที่ตรวจสอบสถานที่เกิดเหตุ และดำเนินการระงับเหตุในเบื้องต้น - หากระบบระบบดับเพลิงอัติโนมัติไม่สามารถระงับเหตุได้ ให้แจ้งขอความช่วยเหลือหน่วยดับเพลิง หรือหน่วยบรรเทาสาธารณภัยในเขตรับผิดชอบ เบอร์ 199 หรือ ป้องกันจังหวัด มท. 16708 - ขนย้ายอุปกรณ์ที่เป็นชนวนในการเกิดเพลิงไหม้ออกจากสถานที่เกิดเหตุโดยเร็ว - สำรวจ/รายงานความเสียหายแจ้งให้ผู้บังคับบัญชาทราบในเบื้องต้น

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
5	**<u>ห้องศูนย์ข้อมูล</u>** - ความปลอดภัยในการเข้า-ออก	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัดเป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัดเป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง - กำหนดรายชื่อเจ้าหน้าที่ที่เกี่ยวข้อง และกำหนดสิทธิการเข้าถึงข้อมูล	- ดำเนินการตรวจสอบการทำงานของอุปกรณ์ทุกระบบว่ายังสามารถให้บริการได้ตามปกติหรือไม่ - ตรวจสอบระบบฐานข้อมูลว่าได้รับความเสียหายหรือไม่
6	**<u>ห้องศูนย์ข้อมูล</u>** - การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัติโนมัติ	- ใช้ระบบปรับอากาศที่ได้มาตฐาน - จัดให้มีระบบปรับอากาศสำรอง - ตรวจสอบการทำงานเป็นประจำ สม่ำเสมอ	- หากระบบปรับอากาศอัติโนมัติขัดข้อง ให้ดำเนินการเปิดระบบปรับอากาศสำรอง - แจ้งผู้ชำนาญการด้านครื่องปรับอากาศเข้าดำเนินการตรวจสอบระบบปรับอากาศ

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
7	**<u>ระบบสื่อสาร/ระบบเครือข่าย</u>** - โทรศัพท์/ Internet/Intranet/ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ	- บำรุงรักษา ตรวจสอบ ตรวจซ่อมระบบให้สามารถใช้งานได้ตอลดเวลา	- มีเจ้าหน้าที่ด้านเทคนิคตรวจสอบการทำงานของเครือข่ายให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - มีการตรวจสอบบำรุงรักษาช่องสัญญาณเครือข่ายเป็นประจำ - จังหวัดมีการช่องสัญญาณสำรอง โดยดำเนินการเช่าจากผู้ให้บริการ ISP ที่ได้มาตรฐานมีความมั่นคงปลอดภัยต่อการใช้ระบบงาน (ระบบ ISDN จาก TOT และเครือข่าย GIN)	- ดำเนินการตรวจสอบการทำงานของอุปกรณ์ว่ายังสามารถให้บริการได้ตามปกติหรือไม่ - ติดต่อหน่วยงานผู้ให้บริการเครือข่ายทราบเพื่อขอทราบสถานะและแจ้งหน่วยงานที่เกี่ยวข้องทราบ - ใช้การช่องสัญญาณสำรอง ระบบ ISDN และInternet ความเร็วสูง (GIN) กรณีเครือข่ายมหาดไทยขัดข้อง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
8	**<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์ลูกข่าย และทำการ Update และ Scan เป็นประจำ	- กำหนดมาตรการหรือระเบียบ ข้อกำหนดสิทธิการเข้าถึงข้อมูล - ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ดำเนินการติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์และทำการ Update และ Scan เป็นประจำ	- ดำเนินการตรวจสอบการทำงานของอุปกรณ์คอมพิวเตอร์ว่ายังสามารถให้บริการได้หรือไม่ - ตรวจสอบอุปกรณ์รักษาความปลอดภัย (Firewall) ว่ายังทำงานได้ตามปกติหรือไม่ หากไม่ปกติดำเนินการแก้ไขในเบื้องต้น หรือปรึกษาผู้ชำนาญการ บริษัทผู้จัดหาระบบรักษาความปลอดภัย (Appwork Company Limited เบอร์โทรศัพท์ 0-2282-6560-79 ต่อ 51133, 51138 และประสานไปยัง ศสข. 9 นว.

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
9	การจัดทรัพยากรสนับสนุน	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ	- ดำเนินการชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ - จัดทำแผนผังแสดงถึงขั้นตอนการขอรับบริการ	- ดำเนินการชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ
10	ด้านงบประมาณ	- จัดทำแผนงานโครงการเพื่อขอรับการสนับสนุนงบประมาณ	- จัดทำรายละเอียดแผนงานโครงการเพื่อขอรับการสนับสนุนงบประมาณจากผู้บริหาร	- ชี้แจงทำความเข้าใจกับผู้บริหาร
11	**<u>ระบบฐานข้อมูล</u>** - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	- กำหนดมาตรการหรือระเบียบ ข้อกำหนดสิทธิการเข้าถึงข้อมูล - ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ดำเนินการติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์และทำการ Update และ Scan เป็นประจำ - มีการ Backup ข้อมูลอย่างสม่ำเสมอ - ติดตั้งติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	- ดำเนินการตรวจสอบการทำงานของอุปกรณ์คอมพิวเตอร์ว่ายังสามารถให้บริการได้หรือไม่ - ตรวจสอบอุปกรณ์รักษาความปลอดภัย (Firewall) ว่ายังทำงานได้ตามปกติหรือไม่ หากไม่ปกติดำเนินการแก้ไขในเบื้องต้น หรือปรึกษาผู้ชำนาญการ บริษัทผู้จัดหาระบบรักษาความปลอดภัย (Appwork Company Limited เบอร์โทรศัพท์ 0-2282-6560-79 ต่อ 51133, 51138 และประสานไปยัง ศสข. 9 นว.

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
12	การจัดการข้อมูล	- ตรวจสอบความถูกต้องของข้อมูลและทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของส่วนราชการ	- จัดให้มีเจ้าหน้าที่รับผิดชอบในการตรวจสอบความถูกต้องของข้อมูล - ดำเนินการตรวจสอบความถูกต้องของข้อมูลอย่างสม่ำเสมอ	- ดำเนินการตรวจสอบความถูกต้องของข้อมูลอย่างสม่ำเสมอ -ประสานไปยังส่วนราชการผู้รับผิดชอบข้อมูลเพื่อตรวจสอบความถูกต้อง
13	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- จัดทำแผนงาน/โครงการ/กิจกรรมให้ครบถ้วน	- มีจัดทำแผนงาน/โครงการ/กิจกรรม ให้ครบถ้วน - มีการทบทวนแผนงาน/โครงการ/กิจกรรม	- คณะกรรมการที่ปรึกษาทางเทคนิคประชุมปรึกษาหารือการแก้ไขปัญหาโดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน
14	ผู้ปฏิบัติและการจัดการความรู้	- ฝึกอบรม และการจัดการความรู้	- จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการความรู้	- จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการความรู้

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

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มาตรการบริหารความเสี่ยง	แนวทางปฏิบัติเมื่อเกิดความเสียหาย
17	ความซื่อสัตย์ สุจริต ปฏิบัติหน้าที่ตรงไปตรงมาตามกฎหมาย กฎระเบียบไม่แสวงหาผลประโยชน์ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
18	ความสามัคคี การช่วยเหลือให้ความเคารพซึ่งกันและกัน ทำงานร่วมกันอย่างมีประสิทธิภาพ	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
19	ความมีประสิทธิภาพ ทำงานอย่างรวดเร็ว และใช้ทรัพยากรที่มีอยู่อย่างจำกัดให้ได้อย่างคุ้มค่า และก่อประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
20	การปฏิบัติต่อผู้อื่นด้วยความเป็นธรรมและเท่าเทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล
21	การถ่ายทอดแผนไปสู่การปฏิบัติ	- การปฏิบัติตามแผนงานโครงการที่กำหนดไว้	- จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการความรู้	- จัดทำแผนการจัดการความรู้ - ดำเนินการตามแผนการจัดการความรู้

รายชื่อเจ้าหน้าที่ผู้รับผิดชอบ

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
1	ด้านบุคลากร	- แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิค โดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงานเพื่อป้องกันการขาดแคลนเจ้าที่	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
2	**<u>ระบบไฟฟ้า</u>** - ไฟฟ้าดับ/ไฟกระชาก /ไฟเกิน ฯลฯ	- ติดตั้งระบบป้องกันไฟฟ้ากระชาก ไฟเกิน (AC Line Surge Protection) และระบบไฟฟ้าสำรอง (UPS)	ตุลาคม 55 – กันยายน 56	นายเฉลิมพล ทองโคตร
3	**<u>อุปกรณ์คอมพิวเตอร์แม่ข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ	ตุลาคม 55 – กันยายน 56	นายเฉลิมพล ทองโคตร นายเอกโรจน์ ศัลยพงษ์
4	**<u>ห้องศูนย์ข้อมูล</u>** - อุบัติภัย (ไฟไหม้,น้ำท่วม ตึกถล่ม)	- ติดตั้งระบบดับเพลิงอัตโนมัติชนิดไพโรเจนในพื้นที่ปิด (Pyrogen) - มีการให้ความรู้เจ้าหน้าที่และซักซ้อมแผนเผชิญเหตุเพลิงไหม้	ตุลาคม 55 – กันยายน 56	นางเพ็ญศรี กันเตียง นายเฉลิมพล ทองโคตร

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
5	**<u>ห้องศูนย์ข้อมูล</u>** - ความปลอดภัยในการเข้า-ออก	- กำหนดพื้นที่ห้องเครื่องมือสื่อสาร สำนักงานจังหวัดเป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูล ฯ นางเพ็ญศรี กันเตียง นายเฉลิมพล ทองโคตร นายเอกโรจน์ ศัลยพงษ์
6	**<u>ห้องศูนย์ข้อมูล</u>** - การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัตโนมัติ	ตุลาคม 55 – กันยายน 56	นางเพ็ญศรี กันเตียง นายเฉลิมพล ทองโคตร
7	**<u>ระบบสื่อสาร/ระบบเครือข่าย</u>** - โทรศัพท์/Internet/Intranet/ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ	- บำรุงรักษา ตรวจสอบ ตรวจซ่อมระบบให้สามารถใช้งานได้ตอลดเวลา	ตุลาคม 55 – กันยายน 56	นายเฉลิมพล ทองโคตร
8	**<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์ลูกข่าย และทำการ Update และ Scan เป็นประจำ	ตุลาคม 55 – กันยายน 56	นายเอกโรจน์ ศัลยพงษ์

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
9	การจัดทรัพยากรสนับสนุน	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
10	ด้านงบประมาณ	- จัดทำแผนงานโครงการเพื่อขอรับการสนับสนุนงบประมาณ	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ นายเอกโรจน์ ศัลยพงษ์
11	**ระบบฐานข้อมูล** - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูล ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ตุลาคม 55 – กันยายน 56	นายเฉลิมพล ทองโคตร นายเอกโรจน์ ศัลยพงษ์
12	การจัดการข้อมูล	- ตรวจสอบความถูกต้องของข้อมูล และทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของส่วนราชการ	ตุลาคม 55 – กันยายน 56	ทุกส่วนราชการ
13	การกำหนดกลยุทธ์หรือนโยบายที่ผิดพลาด	- จัดทำแผนงาน/โครงการ/กิจกรรม ให้ครบถ้วน	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ นายเอกโรจน์ ศัลยพงษ์
14	ผู้ปฏิบัติและการจัดการความรู้	- ฝึกอบรม และการจัดการความรู้	ตุลาคม 55 – กันยายน 56	ทุกส่วนราชการ

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
15	**<u>การบันทึก - สำรวจข้อมูล</u>** - วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล - เลือกสื่อบันทึกข้อมูลไม่เหมาะสม	- มีการ Backup ข้อมูลอย่างสม่ำเสมอ	ตุลาคม 55 – กันยายน 56	นายเฉลิมพล ทองโคตร
16	การดำเนินตามกฎหมาย กฎระเบียบที่เกี่ยวข้อง	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการ และข้อมูลการบริการ - การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
17	ความซื่อสัตย์ สุจริต ปฏิบัติหน้าที่ตรงไปตรงมาตามกฎหมาย กฎระเบียบไม่แสวงหาผลประโยชน์ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
18	ความสามัคคี การช่วยเหลือให้ความเคารพซึ่งกันและกันทำงานร่วมกันอย่างมีประสิทธิภาพ	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
19	ความมีประสิทธิภาพ ทำงานอย่างรวดเร็ว และใช้ทรัพยากรที่มีอยู่อย่างจำกัดให้ได้อย่างคุ้มค่าและก่อประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
20	การปฏิบัติต่อผู้อื่นด้วยความเป็นธรรมและเท่าเทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	ตุลาคม 55 – กันยายน 56	หัวหน้ากลุ่มงานข้อมูลฯ และเจ้าหน้าที่กลุ่มงานข้อมูลฯ สำนักงานจังหวัด
21	การถ่ายทอดแผนไปสู่การปฏิบัติ	- การปฏิบัติตามแผนงานโครงการที่กำหนดไว้	ตุลาคม 55 – กันยายน 56	ทุกส่วนราชการ

ขั้นตอนที่ 5 การติดตาม กำกับ ตรวจสอบการปฏิบัติการควบคุมความเสี่ยง และทบทวนแผนบริหารความเสี่ยง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
1	ด้านงบประมาณ	- จัดทำแผนงานโครงการเพื่อขอรับการสนับสนุนงบประมาณ	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

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจาการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
3	ด้านบุคลากร	- แต่งตั้งคณะกรรมการที่ปรึกษาทางเทคนิคโดยผู้มีความรู้ความชำนาญเฉพาะทางทั้งบุคลากรภายในและภายนอกหน่วยงาน - จัดฝึกอบรมเจ้าหน้าที่ให้มีความรู้ความสามารถทักษะและความชำนาญในระบบงาน โดยเน้นในลักษณะของทีมงานเพื่อป้องกันการขาดแคลนเจ้าหน้าที่	- การฝึกอบรมเจ้าหน้าที่จะดำเนินการตามแผนการจัดการความรู้ ยังคงความสำคัญในการพัฒนาบุคลกรไว้เป็นลำดับแรก	20 (4) x (5)	4	5	20
4	**<u>การบันทึก - สำรวจข้อมูล</u>** - วิธีการที่ไม่ถูกต้องในการสำรองข้อมูล - เลือกสื่อบันทึกข้อมูลไม่เหมาะสม	- มีการ Backup ข้อมูลอย่างสม่ำเสมอ	ดำเนินการ Backup ข้อมูลเพื่อป้องกันการสูญหายอยู่ตลอดเวลาซึ่งมีความสำคัญมากเมื่อระบบเกิดขัดข้อง	20 (3) x (3)	4	5	20

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
5	**<u>ห้องศูนย์ข้อมูล</u>** - การปรับอากาศเพื่อรักษาอุณหภูมิของห้อง	- ติดตั้งระบบปรับอากาศอัตโนมัติ	ปัจจุบันเครื่องมือสื่อสารและอุปกรณ์ต่าง ๆ ได้เพิ่มเติมจำนวนมาก ทำให้อุณหภูมิภายในห้องเพิ่มสูงขึ้นมาก ซึ่งจะส่งผลกระทบต่ออุปกรณ์ต่าง ๆ ภายในห้องเครื่องมือสื่อสารเป็นอย่างมาก	16 (4) x (4)	4	5	20
6	**<u>อุปกรณ์คอมพิวเตอร์แม่ข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์แม่ข่าย และทำการ Update และ Scan เป็นประจำ	ยังคงมีความจำเป็นต้องคงมาตรการป้องกัน Antivirus สำหรับเครื่องแม่ข่ายอย่างต่อเนื่อง เนื่องจากมีความเสี่ยงสูงมากขึ้นที่ Server จะถูกโจมตีจากไวรัสทั้งภายนอกและภายใน	20 (4) x (5)	4	5	20

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
7	**<u>ห้องศูนย์ข้อมูล</u>** - อุบัติภัย (ไฟไหม้,น้ำท่วม ตึกถล่ม)	- ติดตั้งระบบดับเพลิงอัตโนมัติชนิดไพโรเจนในพื้นที่ปิด (Pyrogen) - มีการให้ความรู้เจ้าหน้าที่และซักซ้อมแผนเผชิญเหตุเพลิงไหม้	เหตุเพลิงไหม้ไม่เกิดเหตุแต่ยังคงเฝ้าระวังกรณีน้ำท่วมและตึกถล่ม เกิดขึ้นได้ยาก เนื่องจากตัวอาคารศาลากลางจังหวัดมั่นคงแข็งแรง	20 (4) x (5)	4	5	20
8	**<u>อุปกรณ์คอมพิวเตอร์ลูกข่าย</u>** - ชำรุดเสียหายใช้งานไม่ได้ - ไวรัส/สปายแวร์ ทำลายระบบฐานข้อมูล/โดนโจมตี/โดนบุรุก	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งโปรแกรม Antivirus ประจำเครื่องคอมพิวเตอร์ลูกข่าย และทำการ Update และ Scan เป็นประจำ	มีการแพร่กระจายของไวรัสบางแต่ยังไม่ส่งผลกระทบต่อระบบ Server หลัก	16 (4) x (4)	4	4	16

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจาการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
9	**<u>ห้องศูนย์ข้อมูล</u>** - ความปลอดภัยในการเข้า-ออก	- กำหนดพื้นที่ห้องเครื่องมือสื่อสารสำนักงานจังหวัดเป็นเขตพื้นที่หวงห้ามเด็ดขาด เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง	เมื่อมีการกำหนดมาตรการขึ้นมามีเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้นที่เข้าออกพื้นที่	16 (4) x (4)	4	4	16
10	ผู้ปฏิบัติและการจัดการความรู้	- ฝึกอบรม และการจัดการความรู้	ดำเนินการตามแผนการจัดการความรู้ ยังคงพบว่าผู้ปฏิบัติงานงมีการฝึกอบรมด้าน IT น้อย	12 (3) x (4)	4	4	16

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
11	**<u>ระบบฐานข้อมูล</u>** - การเข้าถึงข้อมูลไม่ได้ - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต - ความเชื่อถือได้ของข้อมูล - ข้อมูลเสียหาย	- ติดตั้งอุปกรณ์ รักษาความปลอดภัย Firewall - ติดตั้งระบบการกำหนดสิทธิ์การเข้าถึงข้อมูลตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	หลังจากการติดตั้งระบบรักษาความปลอดภัยและทำความเข้าใจกับผู้ใช้บริการ ซึ่งส่วนใหญ่อยู่ภายในศาลากลางจังหวัดและส่วนราชการ เป็นประจำทำให้มีความเข้าใจและตระหนักมากขึ้น	15 (3) x (5)	3	5	15
12	การจัดการข้อมูล	- ตรวจสอบความถูกต้องของข้อมูล และทันสมัย - ติดตามและประเมินผลการกรอกข้อมูลของส่วนราชการ	มีเจ้าหน้าที่ดำเนินการตรวจสอบความถูกต้องประกอบกับมีการยืนยันจากผู้รับผิดชอบข้อมูลทำให้มีความถูกต้องของข้อมูลมากขึ้น	15 (3) x (5)	3	5	15

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
13	**<u>ระบบสื่อสาร/ระบบเครือข่าย</u>** - โทรศัพท์/ Internet/Intranet/ระบบประชุมทางไกล ใช้งานไม่ได้ตามปกติ	- บำรุงรักษา ตรวจสอบ ตรวจซ่อมระบบให้สามารถใช้งานได้ตอลดเวลา	เนื่องจากระบบต่าง ๆ ได้มีการติดตั้งระบบเครือข่ายสำรองไว้ ถึงว่าระบบหลักไม่สามารถใช้งานได้แต่ระบบเครือข่ายสำรองสามารถใช้งานทดแทนได้	16 (4) x (4)	4	4	16
14	การจัดทรัพยากรสนับสนุน	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการและข้อมูลการบริการ	ได้มีการประชาสัมพันธ์ทำความเข้าใจรวมถึงทำป้ายแสดงถึงขั้นตอนและระเวลาการให้บริการอย่างชัดเจน ทำให้ผู้ใช้บริการมีความเข้าใจมากขึ้น	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	มีการประชุมปรึกษาหารือรวมทั้งมีการทบทวนแผนงานโครงการ	10 (2) x (5)	2	5	10
16	การดำเนินตามกฎหมาย กฎระเบียบที่เกี่ยวข้อง	- ชี้แจงทำความเข้าใจและประชาสัมพันธ์ให้ผู้รับบริการทราบถึงขั้นตอนการรับบริการและข้อมูลการบริการ - การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ได้มีการประชาสัมพันธ์ทำความเข้าใจรวมถึงทำป้ายแสดงถึงขั้นตอนและระเวลาการให้บริการอย่างชัดเจน ทำให้ผู้ใช้บริการมีความเข้าใจมากขึ้น	9 (3) x (3)	3	3	9
17	ความซื่อสัตย์ สุจริต ปฏิบัติหน้าที่ตรงไปตรงมาตามกฎหมาย กฎระเบียบไม่แสวงหาผลประโยชน์ส่วนตัว	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับผู้ปฏิบัติงานให้ทราบถึงผลกระทบต่อองค์กร	9 (3) x (3)	3	3	9

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมควบคุมความเสี่ยง	ผลจากการใช้มาตรการ	ระดับความเสี่ยงเดิม	โอกาสคงเหลือ (1)	ผลกระทบคงเหลือ (2)	ระดับความเสี่ยงคงเหลือ (1) x (2)
18	ความสามัคคี การช่วยเหลือให้ความเคารพซึ่งกันและกันทำงานร่วมกันอย่างมีประสิทธิภาพ	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับผู้ปฏิบัติงานให้ทราบถึงผลกระทบต่อองค์กร	12 (3) x (3)	3	3	9
19	ความมีประสิทธิภาพ ทำงานอย่างรวดเร็ว และใช้ทรัพยากรที่มีอยู่อย่างจำกัดให้ได้อย่างคุ้มค่า และก่อประโยชน์สูงสุด	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับผู้ปฏิบัติงานให้ทราบถึงผลกระทบต่อองค์กร	12 (3) x (4)	2	4	8
20	การปฏิบัติต่อผู้อื่นด้วยความเป็นธรรมและเท่าเทียมกัน	- สนับสนุนให้บุคลากรมีจริยธรรม คุณธรรม ตามหลักธรรมาภิบาล	สร้างความเข้ากับผู้ปฏิบัติงานให้ทราบถึงผลกระทบต่อองค์กร	9 (3) x (3)	2	4	8
21	การถ่ายทอดแผนไปสู่การปฏิบัติ	- การปฏิบัติตามแผนงานโครงการที่กำหนดไว้	มีการปรึกษาหารือกันเป็นประจำระหว่างบังคับบัญชากับปฏิบัติงานอยู่เสมอ	6 (2) x (3)	2	3	6