แผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
จังหวัดสระแก้ว

ส่วนที่ 1
บทนำ

1.1 หลักการและเหตุผล

สารสนเทศเป็นทรัพยากรที่สำคัญยิ่งขององค์การเดิม เป็นข้อมูลที่มีความหมาย และมีประโยชน์ต่อการตัดสินใจองค์การต่างๆ จึงจัดให้มีระบบสารสนเทศเพื่อช่วยให้การดำเนินงานมีประสิทธิภาพยิ่งขึ้น มีการตัดสินใจที่รวดเร็วและถูกต้อง ตลอดจนเสริมสร้างภาพลักษณ์ที่ดีขององค์การ ดังนั้น ระบบสารสนเทศที่มีประสิทธิภาพจึงเป็นหัวใจสำคัญของหน่วยงาน การรักษาความปลอดภัยให้กับระบบสารสนเทศ เพื่อป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อระบบเป็นเรื่องที่ต้องตระหนักเป็นลำดับแรก

1.2 วิสัยทัศน์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของจังหวัด

เป็นศูนย์กลางการบริหารจัดการ การพัฒนาบุคลากรของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค และส่วนท้องถิ่นในจังหวัด โดยใช้เทคโนโลยีสารสนเทศที่เหมาะสม มีความทันสมัยและมีประสิทธิภาพ

1.3 พันธกิจ

พัฒนาศักยภาพการจัดการ ระบบเทคโนโลยีสารสนเทศเพื่อประโยชน์ในการบริหารจัดการ การพัฒนาคุณภาพ การรายงานผลที่มีประสิทธิภาพ เพื่อการบริหารจัดการพัฒนาจังหวัดแบบบูรณาการ ให้เกิดการพัฒนาอย่างมีประสิทธิภาพ ประสิทธิผลก่อให้เกิดการพัฒนาอย่างยั่งยืน

1.4 ยุทธศาสตร์ในการพัฒนา

(1) ศึกษาวิเคราะห์ วางแผน ออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศ ของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่ายให้มีความเหมาะสม ตอบสนองต่อการพัฒนาจังหวัดแบบบูรณาการได้อย่างมีประสิทธิภาพ ประสิทธิผลก่อให้เกิดการพัฒนาอย่างยั่งยืน

(2) การเชื่อมโยงระบบข้อมูลสารสนเทศ การดูแลรักษาระบบเทคโนโลยีสารสนเทศ ของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่าย ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

(3) เป็นศูนย์กลางการประสานงานด้านข้อมูลสารสนเทศของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่าย เพื่อให้มีการจัดระบบข้อมูลสารสนเทศ การบริการข้อมูลสารสนเทศ และการเผยแพร่ข้อมูลสารสนเทศให้เกิดประโยชน์ในการบริหารจัดการพัฒนาจังหวัดแบบบูรณาการ

(4) พัฒนาศักยภาพบุคลกรของหน่วยงานราชการส่วนกลาง ส่วนภูมิภาค ส่วนท้องถิ่น และเครือข่าย ให้มีความรู้ความสามารถในด้านการใช้เทคโนโลยีสารสนเทศในการจัดระบบข้อมูลสารสนเทศได้อย่างมีประสิทธิภาพ ส่งผลให้เกิดการพัฒนาจังหวัดอย่างยั่งยืน

1.5 วัตถุประสงค์

เพื่อควบคุมความเสี่ยงและสร้างความปลอดภัยให้กับระบบสารสนเทศของจังหวัด

ส่วนที่ 2
ความเสี่ยงและการระบุความเสี่ยง

2.1 นิยามความเสี่ยง

- Australian and New Zealand Public Sector Guidelines for Managing Risk ได้ให้คำจำกัดความเสี่ยงว่า หมายถึง โอกาสของบางสิ่งบางอย่างซึ่งเมื่อเกิดขึ้นแล้วจะมีผลกระทบต่อการบรรลุวัตถุประสงค์ โดยสามารถวัดความเสี่ยงได้จากผลที่ติดตามมา (Consequences) เป็นโอกาสที่น่าจะเกิดขึ้น (likelihood)

- The Canadian Institute of Chartered Accounts ให้คำจำกัดความว่าความเสี่ยง คือความเป็นไปได้ที่บุคคลใดบุคคลคนหนึ่งหรือกลุ่มหนึ่ง หรือองค์การจะประสบความยากลำบากซึ่งเป็นผลจากเหตุการณ์หรือกรณีบางอย่าง

- Treasury Board of Canada ได้ให้ความหมายของความเสี่ยงว่าเป็นความไม่แน่นอนที่อยู่ห้อมล้อมเหตุการณ์ในอนาคตและผลลัพธ์ ซึ่งสามารถแสดงออกในลักษณะของโอกาสที่น่าจะเกิดขึ้นและผลกระทบของเหตุการณ์ที่มีแนวโน้มว่าจะส่งผลกระทบต่อความสำเร็จของวัตถุประสงค์ขององค์การ โดยสรุป ความเสี่ยง (Risk) เป็นสิ่งที่มนุษย์ทุกคนไม่อาจหลีกเลี่ยงได้และเกิดขึ้นในชีวิตประจำวันทั่วไป

2.2 การระบุความเสี่ยง

ความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศ ประกอบด้วยดังนี้

(1) ความมีประสิทธิผลของระบบสารสนเทศ Effectiveness ความเสี่ยงที่อาจเกิดขึ้นมาจากการที่ระบบสารสนเทศอาจไม่สามารถตอบสนองความต้องการทางธุรกิจได้อย่างทันท่วงที จากการที่ไม่สามารถนำระบบสารสนเทศไปใช้ในทางไปปฏิบัติได้ ไม่สามารถเพิ่มมูลค่าให้กับองค์การ และไม่สามารถนำเสนอบริการใหม่ ๆ ให้กับผู้ใช้บริการ เช่น ความเสี่ยงในการวางแผน การจัดโครงสร้างงานสารสนเทศที่ไม่เหมาะสม ขาดความร่วมมือจากผู้ใช้งาน และความเสี่ยงในกระบวนการพัฒนาระบบงาน เป็นต้น

(2) ความมีประสิทธิผลของระบบสารสนเทศ Effectiveness ความเสี่ยงในการให้บริการด้านสารสนเทศอาจไม่มีประสิทธิภาพ โดยเฉพาะอย่างยิ่งด้านการบริหารและการใช้ทรัพยากรด้านสารสนเทศ เช่น ความเสี่ยงด้านการขาดแคลนบุคลากร การใช้เทคโนโลยีที่ล้าสมัย เป็นต้น

(3) การรักษาความลับ Confidentiality ความเสี่ยงเกี่ยวกับการรักษาความลับและความปลอดภัยของข้อมูล และระบบสารสนเทศ หรือความเสี่ยงที่ข้อมูลอาจถูกเปิดเผยหรือใช้โดยที่ไม่ได้รับอนุญาต เช่น ความเสี่ยงจากการเจาะระบบ โครงสร้างการรักษาความปลอดภัย บุคลากรขาดความเอาใจใส่

(4) ความถูกต้องและความครบถ้วนของข้อมูล Integrity ความเสี่ยงที่ข้อมูลอาจไม่ถูกต้องและครบถ้วน ซึ่งอาจสืบเนื่องมาจากการนำข้อมูลที่ผิดพลาดเข้าสู่ระบบหรือการประมวลผลที่ไม่ถูกต้อง ซึ่งอาจมีผลกระทบต่อการดำเนินธุรกิจเนื่องจากใช้ข้อมูลที่ไม่ถูกต้อง เช่น ความเสี่ยงด้านการนำข้อมูลเข้าสู่ระบบ ความเสี่ยงจากการประมวลผลผิดพลาด ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงข้อมูล เป็นต้น

(5) การมีระบบใช้อย่างต่อเนื่อง Availability ความเสี่ยงที่สารสนเทศอาจหยุดชะงัก และไม่สามารถให้บริการกับธุรกิจได้อย่างต่อเนื่อง เช่น ความเสี่ยงเกี่ยวกับอุบัติภัย อุบัติเหตุ เทคโนโลยีที่ล้าสมัย การไม่มีแผนฉุกเฉิน และระบบเครือข่าย เป็นต้น

(6) การปฏิบัติตามกฎเกณฑ์ Compliance ความเสี่ยงที่ระบบสารสนเทศไม่สามารถช่วยให้องค์การปฏิบัติตาม กฎเกณฑ์ หรือกฎหมายที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

(7) ความน่าเชื่อถือของระบบสารสนเทศ Reliability ความเสี่ยงที่ระบบสารสนเทศขาดความน่าเชื่อถือ ซึ่งมีผลกระทบต่อความเชื่อมั่นต่อข้อมูลหรือรายงานต่าง ๆ จากระบบสารสนเทศ ทั้งรายงานเพื่อการบริหารงานภายในและรายงานต่อบุคคลภายนอก เช่น ความผิดพลาดของโปรแกรมและข้อมูลที่เกิดขึ้นบ่อย ๆ เป็นต้น

ส่วนที่ 3
การบริหารจัดการความเสี่ยง

3.1 องค์ประกอบสำคัญของความเสี่ยง

ความเสี่ยงอาจก่อให้เกิดการสูญเสียหรือเกิดสิ่งที่ไม่พึงประสงค์ การบริหารจัดการความเสี่ยงจึงมีวัตถุประสงค์เพื่อรับรู้ จำกัด และควบคุมความเสี่ยง จากปัจจัยเสี่ยงดังกล่าวแล้วสามารถกำหนดเป็นองค์ประกอบหลักที่จะต้องบริหารจัดการได้ 3 องค์ประกอบ คือ

3.1.1 บุคลากร หากบุคลากรไม่เข้าใจหรือไม่มีประสิทธิภาพ โอกาสที่ต้องการให้ระบบมีความปลอดภัยในระดับที่ต้องการคงเกิดขึ้นได้ยาก

3.1.2 เทคโนโลยี ความผิดพลาดในการประมวลผลอาจมีผลต่อการให้บริการข้อมูล ซึ่งจะทำให้กระทบต่อการตัดสินใจและการวางแผน

3.1.3 การบริหารจัดการหากขาดคุณภาพอาจส่งผลให้เกิดปัญหาในหลายประการ เช่น ไม่มีนโยบายด้านการรักษาความปลอดภัยสารสนเทศ ทำให้ผู้ใช้ ผู้ดูแลระบบเครือข่ายไม่มีมาตรฐาน/แนวทางในการปฏิบัติงานอย่างถูกต้อง

3.2 แนวทางการลดความเสี่ยง

3.2.1 บุคลากร

1) สร้างความตระหนักให้กับบุคลากรในการรักษาความปลอดภัยให้กับเทคโนโลยีสารสนเทศ โดยมุ่งเน้นพฤติกรรมการใช้งานระบบเครือข่าย ได้แก่ การตรวจสอบไวรัสก่อนการดาวน์โหลดไฟล์ การแชร์ รหัสผ่าน

2) ฝึกอบรมเพื่อเพิ่มทักษะความชำนาญตลอดจนความเข้าใจที่ถูกต้องกับปัญหาเรื่องความปลอดภัยข้อมูลคอมพิวเตอร์

3.2.2 เทคโนโลยี

1) ติดตั้งระบบปฏิบัติการให้ทำงานอย่างปลอดภัย

2) จัดให้มีระบบการบำรุงรักษาที่ต่อเนื่องเหมาะสมและควบคุมครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ทุกประเภท

3) จัดทำระบบป้องกันการบุกรุก

4) ติดตั้งระบบเตือนภัย

5) ติดตั้งระบบสำรองไฟ

3.2.3 การบริหารจัดการ

1) วางกฎระเบียบควบคุมการปฏิบัติงาน

2) การสอบทานกระบวนการหรือวิธีการจัดเก็บเอกสารหรือ Media ที่ใช้ประกอบการออกแบบระบบงานรวมทั้งวิธีการเก็บหรือดูแลรักษา Source Program อย่างสม่ำเสมอ

3) กำหนดให้มีการจัดทำทะเบียนคุมการติดตั้งหรือการนำ Software จากภายนอกเข้ามาใช้กับเครื่องคอมพิวเตอร์ในหน่วยงาน

4)กำหนดผู้ที่มีหน้าที่รับผิดชอบศึกษาทบทวนระบบรักษาความปลอดภัยและกำหนดสิทธิในการเข้าถึงระบบงานและฐานข้อมูลที่สำคัญ

5) การปรับปรุงพัฒนาระบบและสิทธิหรือ User ID ในการเข้าถึงระบบงานและระบบข้อมูลเป็นระยะ

6) จัดให้มีการตรวจสอบข้อมูลหรือเอกสารที่จะนำเข้าระบบ รวมทั้งจัดให้มีการรายงานจากโปรแกรมระบบงานสำหรับใช้ในการตรวจสอบหรือสอบทานความถูกต้องของข้อมูลก่อนการส่งต่อ

7) กำหนดระบบการจัดเก็บและสำรองแฟ้มข้อมูล ฐานข้อมูล และรายงานต่าง ๆให้เหมาะสมกับการใช้งาน

8) กำหนดให้มีวิธีการ Backup หรือทำสำเนา Source Program ระบบงานและทำเอกสารประกอบที่สำคัญอย่างน้อย 2 ชุด และแยกสถานที่จัดเก็บรวมทั้งจัดทำทะเบียนไว้เป็นหลักฐาน

9) จัดให้มีการสำรองข้อมูลให้ครบถ้วนตามความเหมาะสมของแต่ละระบบงานและตามเวลาที่กำหนด เช่น จัดเก็บทุกสิ้นวัน ทุกสัปดาห์ หรือทุกเดือนตามความจำเป็นและเหมาะสม

10) จัดให้มีการทดสอบความถูกต้องของข้อมูลที่สำรองไว้เป็นครั้งคราวและทำรายงานผลการทดสอบ

ส่วนที่ 4
การควบคุมการปฏิบัติงาน

เพื่อรักษาความปลอดภัยให้กับระบบสารสนเทศและควบคุมความเสี่ยงที่อาจเกิดขึ้นได้ตลอดเวลาจำเป็นต้องมีการควบคุมการปฏิบัติงานเพื่อเป็นมาตรการป้องกันผลกระทบที่จะเกิดตามมา โดยกำหนดขั้นตอน กิจกรรม และผู้รับผิดชอบให้ชัดเจน ดังนี้

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
1. บุคลากร วัตถุประสงค์ 1.1 เพื่อให้บุคลากรมีความตระหนักในการรักษาความปลอดภัยให้กับเทคโนโลยีสารสนเทศ 1.2 เพื่อให้บุคลากรมีทักษะความชำนาญและความเข้าใจที่ถูกต้องกับปัญหาเรื่องความปลอดภัยข้อมูลคอมพิวเตอร์	พฤติกรรมการใช้งานระบบเครือข่ายขาดความระมัดระวังในการป้องกัน	มีโอกาสเกิดขึ้นซึ่งมีผลทำให้ฐานข้อมูลอาจได้รับความเสียหายจากไวรัสหรือการถูกบุกรุก	ปานกลาง	1. จาก กฎ ระเบียบควบคุมการใช้งาน กำหนดรหัสการใช้งาน 2. การจัดฝึกอบรมให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศ	ทุกส่วนราชการ
2. เทคโนโลยีสารสนเทศ วัตถุประสงค์ เพื่อให้ระบบปฏิบัติการสามารถใช้งานได้อย่างมีประสิทธิภาพไม่สร้างปัญหาให้กับฐานข้อมูล	1. เครื่องคอมพิวเตอร์ทั้งแฟ้มข้อมูลเสียหายเนื่องจากถูกไวรัสการถูกคุกคามทางอินเตอร์เน็ต	1. ระบบคอมพิวเตอร์เสียหายไม่สามารถใช้งานได้	ปานกลาง	1. ติดตั้งระบบปฏิบัติการให้ทำงานอย่างปลอดภัย 2. จัดให้มีระบบการบำรุง รักษาที่ต่อเนื่องและเหมาะสม 3. ติดตั้งระบบป้องกันการบุกรุก 4. ติดตั้งระบบเตือนภัย	ทุกส่วนราชการ

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
	2. ระบบการควบคุมความปลอดภัยจากเหตุการณ์ไฟฟ้าดับไฟฟ้าลัดวงจร ซึ่งส่งผลให้อุปกรณ์ต่าง ๆ เกิดการเสียหาย	2. ข้อมูลอาจเกิดความเสียหาย	ปานกลาง	ติดตั้งระบบสำรองไฟ	ทุกส่วนราชการ
3. การบริหารจัดการวัตถุประสงค์เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มีระบบที่เอื้ออำนวยต่อการให้บริการและลดโอกาสที่จะเกิดความเสียหาย	1. ไม่สามารถตอบสนองความต้องการด้านสารสนเทศได้อย่างทันท่วงที 2. การให้บริการด้านสารสนเทศไม่มีประสิทธิภาพ 3. ข้อมูลอาจถูกเปิดเผยหรือใช้โดยไม่ได้รับอนุญาต	ความเสี่ยงมีโอกาสเกิดขึ้นซึ่งมีผลทำให้ไม่สามารถนำระบบสารสนเทศไปใช้ในทางปฏิบัติได้ ไม่สามารถเพิ่มมูลค่าให้กับองค์กรและไม่สามารถเสนอบริการใหม่ ๆ ให้กับผู้ใช้รวมทั้งทำให้ผู้บริหารขาดข้อมูลในการตัดสินใจและวางแผน	ปานกลาง	1) วางกฎระเบียบควบคุมการปฏิบัติงาน 2) การสอบทานกระบวนการหรือวิธีการจัดเก็บเอกสารหรือ Media ที่ใช้ประกอบการออกแบบระบบงาน รวมทั้งวิธีการเก็บหรือดูแลรักษา Source Program อย่างสม่ำเสมอ 3)กำหนดให้มีการจัดทำทะเบียนคุมการติดตั้งหรือการนำ Software จากภายนอกเข้ามาใช้กับเครื่องคอมพิวเตอร์ในหน่วยงาน 4) กำหนดผู้มีหน้าที่รับผิดชอบศึกษาทบทวนระบบรักษาความปลอดภัยและกำหนดสิทธิในการเข้าถึงระบบงานและฐานข้อมูลที่สำคัญ 5) การปรับปรุงพัฒนา ระบบและสิทธิหรือ User ID	ทุกส่วนราชการ

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
				ในการเข้าถึงระบบงานและระบบข้อมูลเป็นระยะ 6) จัดให้มีการตรวจสอบข้อมูลหรือเอกสารที่จะนำเข้าระบบรวมทั้งจัดให้มีการรายงานจากโปรแกรมระบบงานสำหรับใช้ในการตรวจสอบหรือสอบทานความถูกต้องของข้อมูลก่อนการส่งต่อ 7) กำหนดระบบการจัดเก็บและสำรองแฟ้มข้อมูลฐานข้อมูลและรายงานต่าง ๆให้เหมาะสมกับการใช้งาน 8) กำหนดให้มีวิธีการ Backup หรือทำสำเนา Source Program ระบบงานและเอกสารประกอบที่สำคัญอย่างน้อย 2 ชุด และแยกสถานที่จัดเก็บรวมทั้งจัดทำทะเบียนคุมไว้เป็นหลักฐาน 9) จัดให้มีการสำรองข้อมูลให้ครบถ้วนตามความเหมาะสมของแต่ละระบบงานและตามเวลาที่กำหนด เช่น จัดเก็บทุกสิ้นวัน ทุก	

องค์ประกอบ	ความเสี่ยง	การวิเคราะห์ความเสี่ยง		การควบคุม	หน่วยรับผิดชอบ
		โอกาสที่จะเกิดความเสี่ยง	ระดับความเสี่ยง		
				สัปดาห์ หรือทุกเดือนตามความจำเป็นและความเหมาะสม 10) จัดให้มีการทดสอบความถูกต้องของข้อมูลที่สำรองไว้เป็นครั้งคราว และทำรายงานผลการทดสอบ	