แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
จังหวัดน่าน ประจำปีงบประมาณ ๒๕๖๐

จัดทำโดย

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

สำนักงานจังหวัดน่าน

โทร/โทรสาร ๐ ๕๔๗๑ ๖๓๘๗ เว็บไซต์ www.nan.go.th

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสาร จังหวัดน่าน ประจำปีงบประมาณ ๒๕๖๐

จัดทำโดย

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
สำนักงานจังหวัดน่าน
โทร/โทรสาร ๐ ๕๔๗๑ ๖๓๘๗ เว็บไซต์ www.nan.go.th

บทที่ ๑ บทนำ

.....

หลักการและเหตุผล

พระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ.๒๕๓๔ มาตรา ๖๐ และระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ.๒๕๔๕ และพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.๒๕๔๕ รวมทั้งกฎกระทรวงแบ่งส่วนราชการของสำนักงานปลัดกระทรวงมหาดไทย พ.ศ.๒๕๕๓ ข้อ ๑๘ ได้กำหนดให้สำนักงานจังหวัดน่าน มีอำนาจหน้าที่ประกอบด้วย

(๑) แปลงยุทธศาสตร์การพัฒนาระดับชาติไปเป็นยุทธศาสตร์การพัฒนาจังหวัดในพื้นที่

(๒) พัฒนาระบบข้อมูลสารสนเทศเพื่อการบริหาร ระบบสารสนเทศภูมิศาสตร์เพื่อการวางแผน และเครือข่ายสารสนเทศของจังหวัด โดยเป็นศูนย์สารสนเทศของจังหวัด เพื่อการบริหารและวางแผนพัฒนาจังหวัด

(๓) จัดทำแผนพัฒนาจังหวัด ดำเนินการตามแผน กำกับและติดตามผลการดำเนินงานตามยุทธศาสตร์ นโยบายและแผนพัฒนาจังหวัด รวมทั้งประสานการจัดทำแผนพัฒนากลุ่มจังหวัด

(๔) จัดทำแผนปฏิบัติราชการประจำปีของจังหวัดหรือคำของบประมาณของจังหวัด และประสานการจัดทำแผนปฏิบัติราชการประจำปีของกลุ่มจังหวัดหรือคำของบประมาณของกลุ่มจังหวัด

(๕) ดำเนินการด้านการบริหารทรัพยากรบุคคลและการพัฒนาระบบราชการของจังหวัด

(๖) อำนวยการ ประสาน ปฏิบัติงาน และสนับสนุนงานอันเป็นอำนาจหน้าที่ของผู้ว่าราชการจังหวัด

(๗) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือได้รับมอบหมาย

ทั้งนี้ กระทรวงมหาดไทย ได้กำหนดกรอบภารกิจหน้าที่ให้กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัด มีหน้าที่ รับผิดชอบเกี่ยวกับการจัดทำระบบข้อมูลข่าวสาร ข้อมูลเพื่อการบริหารและข้อมูลเพื่อการวางแผน การวิเคราะห์ข้อมูล รวมทั้งการติดตามประเมินผล การดำเนินการตามแผนงานและโครงการของจังหวัด ได้แก่

(๑) พัฒนาระบบข้อมูลสารสนเทศและเป็นศูนย์สารสนเทศเพื่อการพัฒนาจังหวัด

(๒) จัดให้มีและให้บริการเครือข่ายเชื่อมโยงฐานข้อมูลสารสนเทศระหว่างส่วนราชการภายในจังหวัดและอำเภอ ระหว่างจังหวัดและกับส่วนกลาง

(๓) ให้บริการแลกเปลี่ยนข้อมูลสารสนเทศผ่านสื่อสารอิเล็กทรอนิกส์

(๔) รับผิดชอบศูนย์ข้อมูลข่าวสารของราชการจังหวัดน่าน และกำกับดูแลดำเนินงานตาม พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐

ประกอบกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นส่วนหนึ่งของการดำเนินงานตามเกณฑ์คุณภาพการบริหารจัดการภาครัฐระดับพื้นฐาน ฉบับที่ ๒ (PMQA) หมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ โดยเฉพาะรหัส IT๔ จังหวัดต้องมีระบบบริหารความเสี่ยงของฐานข้อมูลและสารสนเทศแสดงผลการปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศโดยส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการ ดังนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกัน หรือลดการเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ การสำรอง และการกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ที่ไม่แน่นอน และภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๓. มีระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูล เช่น ระบบ Anti – Virus ระบบไฟฟ้าสำรอง เป็นต้น

๔. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ Access Rights

การบริหารความเสี่ยงอย่างมีประสิทธิภาพนั้น จังหวัดหรือส่วนราชการต้องมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้

ขั้นตอนที่ ๑ Identify การระบุความเสี่ยงและผลกระทบทั้งทางตรงและทางอ้อม ที่มีผลกระทบต่อเป้าหมายที่กำหนดไว้

ขั้นตอนที่ ๒ Analyze การวิเคราะห์ ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบ

ขั้นตอนที่ ๓ Plan การวางแผน โดยกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุมเพื่อควบคุมผลกระทบของความเสี่ยงให้สามารถบรรลุเป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนด

ขั้นตอนที่ ๔ Track การติดตาม รายงาน และประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

ขั้นตอนที่ ๕ Control การติดตามตรวจสอบ และนำผลที่ได้มาทบทวนบริหารความเสี่ยง โดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของจังหวัด

๒. เพื่อให้มีแนวทางในการปฏิบัติร่วมกันที่เป็นมาตรฐาน ในการรักษาความมั่นคงปลอดภัย กำจัด ป้องกัน หรือลดการเกิดความเสียหายในรูปแบบต่างๆของระบบข้อมูลสารสนเทศ รวมถึงการฟื้นฟูการสำรองและการกู้คืนข้อมูลอย่างเป็นระบบและต่อเนื่อง

๓. เพื่อเป็นเครื่องมือในการกำกับ ติดตาม ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจ เกี่ยวกับการบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศของจังหวัด

๔. เพื่อเป็นเครื่องมือในการสร้างวัฒนธรรมการบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศในทุกระดับ ตั้งแต่ระดับบุคคล หน่วยงาน และระดับจังหวัด

ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๑. **ความเสี่ยง (Risk)** หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาสซึ่งจะมีผลทำให้จังหวัดไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อส่วนราชการและหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อข้อมูลสารสนเทศที่ใช้ในการบริหารงานและปฏิบัติการ เช่น การบริการประชาชน

๒. **การควบคุม (Control)** หมายถึง ขั้นตอนการปฏิบัติ กระบวนการดำเนินงานหรือกลไกการปฏิบัติงานซึ่งจังหวัดกำหนดขึ้นเพื่อให้มั่นใจว่าการบริหารงานจะสามารถบรรลุวัตถุประสงค์ที่ได้กำหนดไว้

๓. **การบริหารความเสี่ยง (Risk Management)** หมายถึง กระบวนการที่ใช้ระบุความเสี่ยงและการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง เพื่อมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าหมายขององค์กร

๔. **การบริหารความเสี่ยงองค์กรโดยรวม (Organization Wide Risk Management)** หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการปฏิบัติงานต่าง ๆ โดยต้องลดมูลเหตุของโอกาสที่จะทำให้ฐานข้อมูลสารสนเทศของจังหวัดเสียหาย

๕. **ระบบฐานข้อมูลสารสนเทศ** หมายถึง ระบบเครื่องคอมพิวเตอร์ ระบบเครื่องมือสื่อสาร ระบบฐานข้อมูล และอุปกรณ์ประกอบระบบต่าง ๆ รวมทั้งอาคารสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด

๖. **ฐานข้อมูลสารสนเทศ** หมายถึง ฐานข้อมูลที่จังหวัดใช้ในการปฏิบัติหน้าที่ซึ่งประกอบด้วย

๖.๑ ฐานข้อมูลเพื่อการบริการประชาชน รวมถึงเว็บไซต์ของจังหวัด

๖.๒ ฐานข้อมูลเพื่อการบริหารงานภายใน

๖.๓ ฐานข้อมูลกลางกระทรวงมหาดไทยและจังหวัด

๖.๔ ฐานข้อมูลระบบติดตามประเมินผแผนงาน โครงการตามแผนปฏิบัติราชการประจำปีของจังหวัดและกลุ่มจังหวัด (PADME)

ความหมายและคำจัดกัดความของทรัพยากรเทคโนโลยีสารสนเทศ

๑. **ข้อมูล (Data)** หมายถึง ข้อมูลในรูปแบบต่าง ๆ ทั้งที่มีโครงสร้างและไม่มีโครงสร้าง ข้อมูลด้านกราฟิกและข้อมูลที่เป็นเสียง

๒. **ระบบงาน (Application System)** ได้แก่ ขั้นตอนและกระบวนการปฏิบัติงาน ทั้งที่ทำด้วยมือและโปรแกรมคอมพิวเตอร์

๓. **เทคโนโลยี (Technology)** ได้แก่ เครื่องคอมพิวเตอร์ (Hardware) โปรแกรมระบบ (Operating System) ระบบบริหารฐานข้อมูล (Database management System) ระบบเครือข่าย (Networking) และระบบมัลติมีเดีย

๔. **องค์ประกอบ (Facilities)** ได้แก่ ทรัพยากรต่างๆที่ใช้เป็นสถานที่ติดตั้งหรือจัดวางตลอดจนสาธารณูปโภคที่จำเป็นเพื่อการปฏิบัติงานของระบบสารสนเทศ

๕. **บุคลากร (People)** ได้แก่ บุคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงานสาหรับการดูแลและจัดทำระบบ

บทที่ ๒ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

.....

ประเภทความเสี่ยง

ความเสี่ยงด้านเทคโนโลยีสารสนเทศนั้น สามารถแบ่งออกได้เป็น ๗ ประเภท คือ

๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

๒. ความเสี่ยงด้านบุคลากร (People Ware)

๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hard Ware)

๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Soft Ware)

๕. ความเสี่ยงด้านระบบข้อมูล

๖. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

๗. ความเสี่ยงด้านการเงิน (Financial Risk)

ลักษณะของความเสี่ยง

สามารถจำแนกได้ ๓ ลักษณะ คือ

๑. ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง

๒. เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงานหรือนโยบาย

๓. ผลกระทบของความเสี่ยง หมายถึง ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

หลักเกณฑ์และขั้นตอนการวิเคราะห์ความเสี่ยง

การจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของจังหวัดน่านนั้น คำนึงถึงหลักเกณฑ์/ขั้นตอนการดำเนินการในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้

ขั้นตอนที่ ๑ Identify การระบุความเสี่ยงและผลกระทบทั้งทางตรงและทางอ้อม ที่มีผลกระทบต่อเป้าหมายที่กำหนดไว้

๑.๑ ระดับความเสี่ยงไว้ ๕ ระดับ ดังนี้

- ระดับ ๕ บ่อย (frequent) พบได้บ่อยครั้งเป็นประจำ
- ระดับ ๔ ประปราย (probable)
- ระดับ ๓ ตามโอกาส (occasional)
- ระดับ ๒ น้อยครั้งมาก (remote)
- ระดับ ๑ แทบไม่เกิดเลย (improbable)

๑.๒ ความรุนแรงของสิ่งที่เกิดขึ้นตามมา (Severity of consequence) แบ่งเป็น ๔ ระดับ

- ระดับ ๔ ความรุนแรงสูงมาก (severe)
- ระดับ ๓ ความรุนแรงสูง (high)
- ระดับ ๒ ความรุนแรงปานกลาง (moderate)
- ระดับ ๑ ความรุนแรงต่ำ (low)

๑.๓ คะแนนระดับความเสี่ยง แบ่งออกได้ ๔ ระดับ ดังนี้

- คะแนนระหว่าง ๑๖ – ๒๐ มีความเสี่ยงสูงมาก
- คะแนนระหว่าง ๑๑ – ๑๕ มีความเสี่ยงสูง
- คะแนนระหว่าง ๖ – ๑๐ มีความเสี่ยงปานกลาง
- คะแนนระหว่าง ๑ – ๕ มีความเสี่ยงต่ำ

ตารางวิเคราะห์ปัจจัยเสี่ยง โอกาส และผลกระทบจากปัจจัยเสี่ยง

ปัจจัยเสี่ยง	รายละเอียดความสูญเสีย	โอกาสจะเกิด (X)	ผลกระทบ (Y)	ระดับความเสี่ยง (X*Y)
๑.ด้านกายภาพและสิ่งแวดล้อม	-อาคารที่ตั้งระบบสารสนเทศถูกทำลายจากภัยธรรมชาติหรืออุบัติภัย	๒	๒	๔
๒.ด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hard Ware)	-มีการพัฒนาอย่างต่อเนื่องส่งผลให้ Hard Ware ขององค์กร/หน่วยงาน ไม่สามารถตอบสนองความต้องการได้อย่างมีประสิทธิภาพ	๔	๓	๑๒
๓.ด้านโปรแกรมคอมพิวเตอร์ (Soft Ware)	-มีการพัฒนารวดเร็วเกินกว่า Soft Ware ของหน่วยงานจะรองรับได้	๔	๓	๑๒
๔.ด้านบุคลากร (People Ware)	-ขาดความรู้ความสามามารถเฉพาะด้าน ไม่ทันต่อ Technology -มีทัศนคติที่ไม่ดีต่อ Technology	๒	๒	๔
๕.ด้านระบบข้อมูล (Data)	-ฐานข้อมูลถูกทำลายหรือเสียหาย	๒	๔	๘
๖.ด้านกลยุทธ์ (Strategic Risk)	-นโยบายรัฐบาล องค์กร หรือผู้บริหารเปลี่ยนแปลงไป ส่งให้ให้การดำเนินงานขาดความต่อเนื่อง หรือหยุดชะงัก	๔	๑	๔
๗.ด้านการเงิน (Financial Risk)	-ไม่ได้รับการสนับสนุนงบประมาณ หรืองบประมาณไม่เพียงพอ	๓	๓	๙

ขั้นตอนที่ ๒ Analyze การวิเคราะห์ ประเมินถึงโอกาสจะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบ

ปัจจัยเสี่ยง	ภัยคุกคาม	จุดอ่อน	มาตรการแก้ไข
๑.ด้านกายภาพและสิ่งแวดล้อม	-อัคคีภัย -อุทกภัย -วาตภัย -กระแสไฟฟ้าขัดข้อง -การก่อการร้าย	- ระบบรักษาความปลอดภัยให้แก่ห้องอุปกรณ์คอมพิวเตอร์แม่ข่ายของหน่วยงานยังไม่เสถียร	(๑) กำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยงสูง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น เครื่องปรับอากาศ, ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย, หน้าต่างระบายความร้อน, ถังดับเพลิง เป็นต้น (๒) ควบคุมการเข้า – ออก Network Operation Center:NOC ห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง เป็นพื้นที่เขตหวงห้ามเฉพาะ โดยกำหนดสิทธิการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง (๓) ป้องกันความเสี่ยงจากระบบไฟฟ้าขัดข้อง โดยมีการติดตั้งเครื่องสำรองไฟสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และการติดตั้งระบบสายดิน (Ground) ที่ได้มาตรฐานอุปกรณ์ป้องกันไฟ (๔) ป้องกันความเสี่ยงจากระบบควบคุมอุณหภูมิและความชื้นให้เหมาะสม โดยการติดตั้งอุณหภูมิเครื่องปรับอากาศ และค่าความชื้นให้มีระดับเหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์
๒.อุปกรณ์เทคโนโลยีสารสนเทศ (Hard Ware)	-ความผิดพลาดของอุปกรณ์จากการเคลื่อนย้าย -อุปกรณ์เกิดความเสียหายจากการติดตั้งในพื้นที่ไม่เหมาะสม	- ไม่มีความชำนาญในการเคลื่อนย้ายและติดตั้ง - สถานที่ไม่เอื้ออำนวยต่อการติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ	(๑) แก้ไขปัญหาเบื้องต้นของเครื่องคอมพิวเตอร์ได้ โดย Administrator และ User และการดูแลอย่างถูกต้องและต่อเนื่อง (๒) ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว (๓) มีการตรวจเช็คไวรัส และกำจัดอย่างสม่ำเสมอ (๔) การติดตั้ง Firewall เพื่อป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่าย Internet สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศได้ (๕) การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ
ปัจจัยเสี่ยง	**ภัยคุกคาม**	**จุดอ่อน**	**มาตรการแก้ไข**
	-ไวรัสคอมพิวเตอร์		(๖) ฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงาน เกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ เช่น การกำหนดรหัสผู้ใช้ การใช้รหัสผ่าน

			(๗) การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ (๘) การสำรองข้อมูล (Backup) สารสนเทศ
๓.ด้านโปรแกรมคอมพิวเตอร์ (Soft Ware)	-การถูกผู้ไม่หวังดีทำลายระบบ (Hacker) -โปรแกรมมีการพัฒนาเร็วเกินกว่าอุปกรณ์คอมพิวเตอร์จะรองรับได้	-	(๑ พัฒนาและปรับปรุงมาตรฐาน Hard ware, Soft ware , People ware, Data และ Network ให้เป็นฐานข้อมูลกลางของงานเทคโนโลยีสารสนเทศ และเป็นไปในทิศทางเดียวกัน (๒) สร้างกลไกการจัดการฐานข้อมูล การจัดระบบสารสนเทศ เพื่อการบริหารจัดการของหน่วยงานให้ครอบคลุม ถูกต้อง และทันสมัย มากยิ่งขึ้น (๓) พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูล ให้มีมาตรฐาน และแบ่งสรรการใช้ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้ (๔) พัฒนาโปรแกรมให้สามารถจัดเก็บ รวบรวม ประมวลผลข้อมูล ศึกษา วิเคราะห์เพื่อการนำเสนอและสนับสนุนการบริหารราชการ และพัฒนา ส่งเสริม บำรุงรักษาระบบ และการเผยแพร่ข้อมูลข่าวสารของจังหวัดได้ในลักษณะของ Web Application เพื่อความสะดวกในการใช้งานและแสดงผล
๔.ด้านบุคลากร (People Ware)	-บุคลากรไม่มีความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ -ไม่มีบุคลากรในการดูแลรักษาความปลอดภัยระบบเทคโนโลยี	- บุคลากรขาดความรู้ความเข้าใจในเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่อง และมีบุคลากรเฉพาะด้านเทคโนโลยีสารสนเทศน้อย	(๑) การกำหนดโครงสร้าง/มอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศที่มีความเหมาะสม (๒) การว่าจ้าง/จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการพัฒนาระบบข้อมูลสารสนเทศ เนื่องจากเป็นผู้มีความชำนาญเป็นพิเศษหรือเป็นผู้มีมือโดยเฉพาะทาง มีเครื่องมือและเทคโนโลยีที่ทันสมัยทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศมากกว่าภาคราชการ ๓) ส่งเจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศ เพื่อพัฒนาประสิทธิภาพ