ภาคผนวก ข
แบบสอบถามการวิจัย ผู้ใช้ทั่วไป

แบบสอบถามสำหรับ

การวิจัยเรื่อง “แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร”

คำชี้แจง

แบบสอบถามนี้แบ่งออกเป็น 3 ตอน

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 การจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

ตอนที่ 3 ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ

คำแนะนำในการตอบแบบสอบถาม

กรุณาทำเครื่องหมาย ✓ ลงใน ☐ ที่ตรงกับกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรี-สุพรรณ จังหวัดสกลนครมากที่สุด

ผู้วิจัยหวังเป็นอย่างยิ่งว่าจะได้รับความอนุเคราะห์จากท่านด้วยดีและโปรดตอบแบบสอบถามทุกตอนให้สมบูรณ์ตรงกับความเป็นจริงมากที่สุด คำตอบของท่านจะนำไปใช้เฉพาะการวิจัยเพื่อเป็นข้อมูลพื้นฐานสำหรับการวิเคราะห์และออกแบบแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศหน่วยงานของรัฐ กรณีศึกษา กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครเท่านั้น จึงขอขอบพระคุณมา ณ โอกาสนี้

นายพงศกร ทองพันธุ์
นักศึกษาปริญญาโท สาขาวิชาวิทยาการสารสนเทศและเทคโนโลยี
มหาวิทยาลัยราชภัฏสกลนคร

แบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ☐ หน้าข้อความที่ตรงกับความเป็นจริง

ตอนที่ 1.สถานภาพทั่วไปของผู้ตอบแบบสอบถาม

1.สถานที่ทำงาน

☐ โรงพยาบาล ☐ โรงพยาบาลส่งเสริมสุขภาพตำบล

2.ประสบการณ์ทำงาน

☐ ต่ำกว่า 1 ปี ☐ 1-5 ปี ☐ 6-10 ปี

☐ 11 - 15 ปี ☐ 16-20 ☐ 21 ปีขึ้นไป

3.เพศ

☐ ชาย ☐ หญิง

4.อายุ

☐ ต่ำกว่า 20 ปี ☐ 20 - 30 ปี ☐ 31 - 40 ปี

☐ 41 - 50 ปี ☐ 51 ปีขึ้นไป

5.ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ ปริญญาโท

☐ ปริญญาเอก ☐ อื่นๆ โปรดระบุ.....

6.ตำแหน่งของท่าน

☐ แพทย์ ☐ ทันตแพทย์ ☐ เภสัชกร

☐ พยาบาลวิชาชีพ ☐ พยาบาลเทคนิค ☐ นักวิชาการสาธารณสุข

☐ นักจัดการงานทั่วไป ☐ เจ้าพนักงานสาธารณสุข ☐ เจ้าพนักงานทันตสาธารณสุข

☐ เจ้าพนักงานเภสัชกรรม ☐ เจ้าพนักงานวิทยาศาสตร์ ฯ ☐ เจ้าพนักงานธุรการ

☐ เจ้าพนักงานการเงินและบัญชี ☐ เจ้าพนักงานเวชระเบียน ☐ เจ้าพนักงานรังสี

☐ การแพทย์นักกายภาพบำบัด ☐ นักเทคนิคการแพทย์ ☐ แพทย์แผนไทย

☐ อื่นๆ โปรดระบุ.....

7.กลุ่มงานของท่าน

☐ งานบริหารทั่วไป ☐ งานธุรการ ☐ งานพัสดุ

☐ งานการเงิน ☐ งานซ่อมบำรุง ☐ งานโรงครัว

☐ งานยานพาหนะ ☐ งานสนาม ☐ งานโภชนาการ

☐ งานเวชกรรมทั่วไป ☐ งานทันตกรรม ☐ งานผู้ป่วยนอก

☐ งานผู้ป่วยใน ☐ งานผู้ป่วยฉุกเฉินและอุบัติเหตุ ☐ งานห้องคลอด

☐ งานควบคุมและป้องกันการติดเชื้อในโรงพยาบาล ☐ งานหน่วยจ่ายกลางและซักฟอก ☐ งานเภสัชกรรม

☐ งานชันสูตร ☐ งานรังสีเทคนิค ☐ งานกายภาพบำบัด

☐ งานประกันสุขภาพ ☐ งานคอมพิวเตอร์ ☐ งานสถิติ

☐ งานสร้างเสริมสุขภาพ ☐ งานชุมชน ☐ งานสุขาภิบาลและสิ่งแวดล้อม

☐ งานระบาดวิทยา ☐ งานแพทย์แผนไทย

☐ อื่นๆ โปรดระบุ.....

8.ระบบงานที่มีสิทธิใช้งาน เลือกได้มากกว่า 1 ตัวเลือก

☐ ระบบประชาสัมพันธ์ ☐ ระบบเวชระเบียน ☐ ระบบตรวจสอบสิทธิ

☐ ระบบซักประวัติ ☐ ระบบนัดหมาย ☐ ระบบห้องทำงานแพทย์

☐ ระบบงานห้องฉุกเฉิน ☐ ระบบคลินิกพิเศษ ☐ ระบบคัดกรองกลุ่มเสี่ยงเรื้อรัง

☐ ระบบทันตกรรม ☐ ระบบชันสูตร ☐ ระบบรังสีรักษา

☐ ระบบเวชศาสตร์ฟื้นฟู ☐ ระบบแพทย์แผนไทย ☐ ระบบเภสัชกรรม

☐ ระบบการเงิน ☐ ระบบห้องผ่าตัดและวิสัญญี ☐ ระบบ Admission Center

☐ ระบบผู้ป่วยใน ☐ ระบบห้องคลอด ☐ ระบบงานโภชนาการ

☐ ระบบส่งเสริมสุขภาพและระบบ One Stop Service ☐ ระบบงานสำรองข้อมูล ☐ ระบบงานรายงาน

☐ ระบบงานผู้ดูแลระบบ ☐ ระบบส่งออกข้อมูล ☐ Data Center

☐ อื่นๆ.....

ตอนที่ 2 การจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบทาธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550

กรุณาทำเครื่องหมาย ✓ ลงในช่องความคิดเห็น โดยมีรายละเอียด ดังนี้

สภาพปัจจุบัน หมายถึง สภาพการจัดการความมั่นคงปลอดภัยสารสนเทศในปัจจุบัน ที่ตรงกับความเป็นจริง ของกลุ่มเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

ความต้องการ หมายถึง ความคิดเห็นส่วนตัวของท่านต่อการจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

หากท่านมีความคิดเห็นเพิ่มเติมต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ สามารถเขียนแสดงความคิดเห็นในช่อง **ความคิดเห็นเพิ่มเติม**

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
1.นโยบายความมั่นคงปลอดภัยสารสนเทศ (Security policy)						
1.1) มีเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร						
1.2)มีการประกาศใช้นโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ						
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร						
2.1)ผู้บริหารกำหนดให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศ						
2.2)มีการกำหนดให้มีตัวแทนจากหน่วยงานภายในองค์กรเพื่อประสานงานในการสร้างความมั่นคงปลอดภัยสารสนเทศ						
2.3)มีการกำหนดกระบวนการในการอนุมัติใช้งานอุปกรณ์ทางระบบสารสนเทศ เช่น คอมพิวเตอร์ เป็นต้น						
2.4)มีการกำหนดให้บุคลากรลงนามไม่ให้เปิดเผยความลับขององค์กร						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
2.5)มีการกำหนดข้อกำหนดทางด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นให้ผู้ใช้บริการเข้าถึงสารสนเทศขององค์กร						
3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)						
3.1)มีการจัดทำบัญชีทรัพย์สิน (เช่น บัญชีครุภัณฑ์ เป็นต้น) ขององค์กร						
3.2)มีการแก้ไขปรับปรุงบัญชีทรัพย์สินให้มีความถูกต้องอยู่เสมอ						
3.3)มีการจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ						
3.4)มีการจัดทำกฎระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม						
3.5)มีการจัดหมวดหมู่ทรัพย์สินสารสนเทศตามระดับชั้นของความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร						
3.6)มีการจัดทำป้ายชื่อทรัพย์สินทางด้านเทคโนโลยีสารสนเทศขององค์กร						
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)						
4.1)มีการอบรมให้ความรู้และสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรผู้ปฏิบัติหน้าที่ภายในองค์กร และผู้ที่มาจากหน่วยงานภายนอก						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
4.2)มีกระบวนการลงโทษทางวินัยแก่บุคลากรที่ฝ่าฝืน ละเมิดนโยบายหรือระเบียบข้อบังคับด้านความมั่นคงปลอดภัยสารสนเทศ						
4.3)มีการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะงาน						
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)						
5.1)มีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า–ออกที่มีการควบคุม ตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า–ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร						
5.2)ควบคุมพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยอนุญาตให้เข้า–ออกได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น						
5.3)จัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ						
5.4)จัดให้มีการป้องกันทางกายภาพในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัย						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
5.5)จัดทำแนวทางสำหรับการปฏิบัติงานในพื้นที่ ที่ต้องการรักษาความมั่นคงปลอดภัย						
5.6)จัดให้มีบริเวณสำหรับการเข้าถึงโดยบุคคลภายนอก						
5.7)มีการป้องกันอุปกรณ์ของสำนักงานจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ						
5.8)จัดวางอุปกรณ์ของสำนักงานในบริเวณที่ไม่เสี่ยงต่อภัยคุกคามต่างๆ						
5.9)มีกลไกการป้องกันการล้มเหลวของระบบไฟฟ้า						
5.10)มีกลไกการป้องกันการล้มเหลวของระบบเครือข่ายคอมพิวเตอร์						
5.11)มีการป้องกันการเข้าถึงสายไฟฟ้าสายสื่อสาร โดยไม่ได้รับอนุญาต						
5.12)มีการกำหนดให้บำรุงรักษาอุปกรณ์ต่างๆ อยู่เสมอ						
5.13)กำหนดให้มีการป้องกันอุปกรณ์ต่างๆที่ใช้งานอยู่นอกสำนักงาน						
5.14)กำหนดให้มีการขออนุญาตก่อนนำสารสนเทศ หรืออุปกรณ์ระบบสารสนเทศ ออกนอกองค์กร						
6.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)						
6.1)จัดทำคู่มือขั้นตอนการปฏิบัติงานด้านเครือข่ายสารสนเทศขององค์กรแจกจ่ายให้กับผู้ที่เกี่ยวข้อง						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
6.2)ปรับปรุงคู่มือขั้นตอนการปฏิบัติงานด้านเครือข่ายสารสนเทศขององค์กรตามระยะเวลาอันสมควร						
6.3)กำหนดให้ผู้ให้บริการภายนอกปฏิบัติตามข้อกำหนด หรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กร และผู้ให้บริการ						
6.4)มีการติดตั้งโปรแกรมแอนตี้ไวรัส/มัลแวร์ไว้ในเครื่องคอมพิวเตอร์						
6.5)มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่อสารสนเทศที่ส่งผ่านทางเครือข่ายขององค์กร						
6.6)มีขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้						
6.7)ขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งาน เป็นไปอย่างมั่นคงปลอดภัย						
6.8)มีการกำหนดขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศ						
6.9)กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กรโดยผ่านทางช่องทางการสื่อสารทุกชนิด						
6.10)จัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร						
6.11)มีการป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตระหว่างการส่งข้อมูลนั้นไปนอกองค์กร						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
6.12)มีมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์						
6.13)มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่สู่สาธารณะ						
6.14)มีการกำหนดให้มีขั้นตอนปฏิบัติเพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ						
7 การควบคุมการเข้าถึง (Access control)						
7.1)กำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร						
7.2)ปรับปรุงนโยบายควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศตามระยะเวลาที่กำหนด						
7.3)มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น						
7.4)มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการยกเลิกสิทธิต่างๆ ในการใช้งานเมื่อพนักงานลาออกหรือเปลี่ยนตำแหน่งงานภายในองค์กร						
7.5)จำกัดสิทธิการใช้งานระบบสารสนเทศตามความจำเป็นในการใช้งานของบุคลากรขององค์กร						
7.6)มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานระบบสารสนเทศอย่างเป็นทางการ						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
7.7)กำหนดวิธีปฏิบัติที่ดีในการตั้งรหัสผ่าน						
7.8)กำหนดวิธีปฏิบัติที่ดีในการใช้งานรหัสผ่าน เช่น รักษารหัสผ่านให้เป็นความลับ ไม่บันทึกรหัสผ่านที่สามารถพบเห็นได้ง่าย เป็นต้น						
7.9)มีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่มั่นคงปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น						
7.10)จัดทำนโยบายการใช้งานระบบเครือข่ายขององค์กร						
7.11)มีการระบุชัดเจนว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถเข้าถึงได้						
7.12)มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กร						
7.13)มีการระบุตัวตนในการเข้าใช้งานระบบสารสนเทศ						
7.14)มีมาตรการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ						
7.15)กำหนดให้ระบบสารสนเทศตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด						
7.16)การเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอพพลิเคชัน แยกตามประเภทของผู้ใช้งาน						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
8.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)						
8.1)มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ผ่านช่องทางการรายงานที่กำหนดไว้						
8.2)บันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่						
8.3)มีการกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร						
8.4)ขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร รวดเร็ว ได้ผล และเป็นระบบระเบียบที่ดี						
8.5)ต้องรวบรวมและจัดเก็บหลักฐานเพื่อใช้ในกระบวนการทางศาลที่เกี่ยวข้อง						
8.6)มีกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงเพื่อใช้ในกระบวนการทางศาล						
9.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)						
9.1)มีการกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
9.2)มีการปรับปรุงกระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กรอย่างสม่ำเสมอ						
9.3)กระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร						
9.4)มีการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับการให้บริการขององค์กร						
9.5)มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้การให้บริการขององค์กรอย่างสม่ำเสมอ						
10 การปฏิบัติตามข้อกำหนด (Compliance)						
10.1)มีการระบุข้อกำหนดทางด้านกฎหมายทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานขององค์กร และบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร						
10.2)มีการปรับปรุงข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานขององค์กรอย่างสม่ำเสมอ						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
10.3)มีการกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา						
10.4)มีการกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจจากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง						
10.5)มีการกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง						
10.6)ป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ระบบสารสนเทศขององค์กรผิดวัตถุประสงค์						
10.7)ป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต						
10.8)กำหนดให้ใช้มาตรการ การเข้ารหัสข้อมูลโดยสอดคล้องตามกฎหมาย						
10.9)ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน						
10.10)มีการตรวจประเมินระบบสารสนเทศอย่างสม่ำเสมอ						
10.11)มีการระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร						

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
10.12)มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ						

ตอนที่ 3 ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ

กรุณาใส่หมายเลข 1 – 10 หน้าข้อที่ท่านคิดว่าเป็นปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร โดย 1 คือปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยมากที่สุด และ 10 คือปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยน้อยที่สุด

ลำดับปัจจัย	ปัจจัย	เหตุผล
	แผนงานและงบประมาณด้านระบบสารสนเทศขององค์กร	
	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	
	ฮาร์ดแวร์	
	ซอฟแวร์	
	บุคลากร	
	ผู้บริหาร	
	ผู้รับบริการ	
	ข้อมูล	
	กฎหมาย	
	ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ	
	อื่นๆ ระบุ.....	