ภาคผนวก ค
แบบสอบถามการวิจัย ผู้ดูแลระบบสารสนเทศ

มหาวิทยาลัยราชภัฏสกลนคร

มหาวิทยาลัยราชภัฏสกลนคร

แบบสอบถามสำหรับ

การวิจัยเรื่อง “แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร”

คำชี้แจง

แบบสอบถามนี้แบ่งออกเป็น 3 ตอน

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 การจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

ตอนที่ 3 ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ

คำแนะนำในการตอบแบบสอบถาม

กรุณาทำเครื่องหมาย ✓ ลงใน ☐ ที่ตรงกับกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครมากที่สุด

ผู้วิจัยหวังเป็นอย่างยิ่งว่าจะได้รับความอนุเคราะห์จากท่านด้วยดีและโปรดตอบแบบสอบถามทุกตอนให้สมบูรณ์ตรงกับความเป็นจริงมากที่สุด คำตอบของท่านจะนำไปใช้เฉพาะการวิจัยเพื่อเป็นข้อมูลพื้นฐานสำหรับการวิเคราะห์และออกแบบแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศหน่วยงานของรัฐ กรณีศึกษา กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครเท่านั้น จึงขอขอบพระคุณมา ณ โอกาสนี้

นายพงศกร ทองพันธุ์
นักศึกษาปริญญาโท สาขาวิชาวิทยาการสารสนเทศและเทคโนโลยี
มหาวิทยาลัยราชภัฏสกลนคร

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 .....

7.กลุ่มงานของท่าน

☐ งานบริหารทั่วไป ☐ งานธุรการ ☐ งานพัสดุ

☐ งานการเงิน ☐ งานซ่อมบำรุง ☐ งานโรงครัว

☐ งานยานพาหนะ ☐ งานสนาม ☐ งานโภชนาการ

☐ งานเวชกรรมทั่วไป ☐ งานทันตกรรม ☐ งานผู้ป่วยนอก

☐ งานผู้ป่วยใน ☐ งานผู้ป่วยฉุกเฉินและอุบัติเหตุ ☐ งานห้องคลอด

มหาวิทยาลัยราชภัฏสกลนคร

☐ 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
☐ ระบบห้องผ่าตัดและ วิสัญญี
☐ ระบบ Admission Center
☐ ระบบผู้ป่วยใน
☐ ระบบห้องคลอด
☐ ระบบงานโภชนาการ
☐ ระบบส่งเสริมสุขภาพและระบบ One Stop Service
☐ ระบบงานสำรองข้อมูล
☐ ระบบงานรายงาน
☐ ระบบงานผู้ดูแลระบบ
☐ ระบบส่งออกข้อมูล
☐ Data Center
☐ อื่นๆ.....

มหาวิทยาลัยราชภัฏสกลนคร

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						
1.3) มีการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ						
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร						
2.1)ผู้บริหารกำหนดให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศ						
2.2)มีการกำหนดให้มีตัวแทนจากหน่วยงานภายในองค์กรเพื่อประสานงานในการสร้างความมั่นคงปลอดภัยสารสนเทศ						
2.3)มีการกำหนดหน้าที่รับผิดชอบของบุคลากรในการดำเนินการทางด้านความมั่นคงปลอดภัยสารสนเทศไว้ชัดเจน						
2.4)มีการกำหนดกระบวนการในการอนุมัติใช้งานอุปกรณ์ทางระบบสารสนเทศ เช่น คอมพิวเตอร์ เป็นต้น						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
2.5)มีการกำหนดให้บุคลากรลงนามไม่ให้เปิดเผยความลับขององค์กร						
2.6)องค์กรมีรายชื่อและข้อมูลบุคลากร/หน่วยงาน สำหรับติดต่อประสานงานทางด้านความมั่นคงปลอดภัยสารสนเทศในกรณีที่มีความจำเป็น เช่น ผู้ให้บริการอินเตอร์เน็ต ศูนย์ประสานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น						
2.7)มีการกำหนดให้มีการตรวจสอบการจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบอิสระตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร						
2.8)มีการประเมินความเสี่ยงของการเข้าถึงสารสนเทศ หรืออุปกรณ์ในระบบสารสนเทศ						
2.9)มีการกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนการอนุญาตให้เข้าถึงสารสนเทศได้						
2.10)มีการกำหนดข้อกำหนดทางด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นให้ผู้ใช้บริการเข้าถึงสารสนเทศขององค์กร						
2.11)มีการกำหนดข้อกำหนดหรือข้อตกลงกับองค์กรผู้พัฒนาซอฟต์แวร์ในกรณีที่มีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึง						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
สารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กรก่อนที่จะอนุญาตให้สามารถเข้าถึงได้						
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)มีการกำหนดหน้าที่และรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับหน่วยงานหรือผู้ที่องค์กรจ้างงาน						
4.2)ข้อกำหนดหน้าที่และรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศ						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
สำหรับหน่วยงานหรือผู้ที่องค์กรจ้างงานมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร						
4.3)มีการกำหนดระดับการเข้าถึงสารสนเทศสำหรับบุคลากรขององค์กร						
4.4)มีการกำหนดเงื่อนไขการว่าจ้างงาน						
4.5)มีการกำหนดให้บุคลากรที่จะได้รับการว่าจ้างงาน ลงนามเงื่อนไขในการจ้างงาน						
4.6)มีการกำหนดให้บุคลากรขององค์กรหรือจากหน่วยงานภายนอกปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร						
4.7)มีการอบรมให้ความรู้และสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรผู้ปฏิบัติหน้าที่ภายในองค์กร และผู้ที่มาจากหน่วยงานภายนอก						
4.8)มีกระบวนการลงโทษทางวินัยแก่บุคลากรที่ฝ่าฝืน ละเมิดนโยบายหรือระเบียบข้อบังคับด้านความมั่นคงปลอดภัยสารสนเทศ						
4.9)มีการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะงาน						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
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						
5.5)จัดทำแนวทางสำหรับการปฏิบัติงานในพื้นที่ ที่ต้องการรักษาความมั่นคงปลอดภัย						
5.6)จัดให้มีบริเวณสำหรับการเข้าถึงโดยบุคคลภายนอก						
5.7)มีการป้องกันอุปกรณ์ของสำนักงานจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
5.8)จัดวางอุปกรณ์ของสำนักงานในบริเวณที่ไม่เสี่ยงต่อภัยคุกคามต่างๆ						
5.9)มีกลไกการป้องกันการล้มเหลวของระบบไฟฟ้า						
5.10)มีกลไกการป้องกันการล้มเหลวของระบบเครือข่ายคอมพิวเตอร์						
5.11)มีการป้องกันการเข้าถึงสายไฟฟ้าสายสื่อสาร โดยไม่ได้รับอนุญาต						
5.12)มีการกำหนดให้บำรุงรักษาอุปกรณ์ต่างๆ อยู่เสมอ						
5.13)กำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงาน						
5.14)กำหนดให้มีการทำลายข้อมูลและซอฟแวร์ก่อนทิ้งสื่อบันทึกข้อมูล						
5.15)กำหนดให้มีการขออนุญาตก่อนนำสารสนเทศ หรืออุปกรณ์ระบบสารสนเทศ ออกนอกองค์กร						
6.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)						
6.1)จัดทำคู่มือขั้นตอนการปฏิบัติงานด้านเครือข่ายสารสนเทศขององค์กรแจกจ่ายให้กับผู้ที่เกี่ยวข้อง						
6.2)ปรับปรุงคู่มือขั้นตอนการปฏิบัติงานด้านเครือข่ายสารสนเทศขององค์กรตามระยะเวลาอันสมควร						
6.3)มีการกำหนดให้มีการควบคุมเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
6.4)กำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบในงานด้านระบบสารสนเทศขององค์กร						
6.5)มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการระบบสารสนเทศแก่องค์กรออกจากกัน						
6.6)กำหนดให้ผู้ให้บริการภายนอกปฏิบัติตามข้อกำหนด หรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กร และผู้ให้บริการ						
6.7)มีการตรวจสอบการให้บริการระบบสารสนเทศอย่างสม่ำเสมอ						
6.8)มีการกำหนดให้มีการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก						
6.9)มีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต						
6.10)มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม						
6.11)มีการติดตั้งโปรแกรมแอนตี้ไวรัส/มัลแวร์ไว้ในเครื่องคอมพิวเตอร์						
6.12)มีมาตรการในการกู้กลับคืนเมื่อระบบสารสนเทศถูกทำลายโดยไวรัสคอมพิวเตอร์/มัลแวร์						
6.13)มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
6.14)มีการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ						
6.15)มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่อสารสนเทศที่ส่งผ่านทางเครือข่ายขององค์กร						
6.16)กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการเครือข่ายขององค์กร						
6.17)มีข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้ใช้บริการอยู่						
6.18)มีบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้						
6.19)มีขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้						
6.20)มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว						
6.21)ขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งาน เป็นไปอย่างมั่นคงปลอดภัย						
6.22)มีการกำหนดขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศ						
6.23)ขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศได้ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
6.24)ขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศได้ป้องกันการใช้งานผิดวัตถุประสงค์						
6.25)มีมาตรการป้องกันเอกสารของระบบสารสนเทศจากการเข้าถึงโดยไม่ได้รับอนุญาต						
6.26)กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กรโดยผ่านทางช่องทางการสื่อสารทุกชนิด						
6.27)จัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร						
6.28)มีการป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตระหว่างการส่งข้อมูลนั้นไปนอกองค์กร						
6.29)มีมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์						
6.30)มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่สู่สาธารณะ						
6.31)มีการบันทึกกิจกรรมและเหตุการณ์ต่างๆ (Log) ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ						
6.32)มีการกำหนดให้มีขั้นตอนปฏิบัติเพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
6.33)มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ (Log)						
6.34)มีการกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร						
6.35)มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ						
6.36)มีการวิเคราะห์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศและดำเนินการแก้ไขตามสมควร						
6.37)มีการตั้งเวลาของอุปกรณ์ในระบบสารสนเทศให้ตรงกัน						
6.38)มีการตั้งเวลาของอุปกรณ์ในระบบสารสนเทศอ้างอิง จากแหล่งเวลาที่ถูกต้อง						
7 การควบคุมการเข้าถึง (Access control)						
7.1)กำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร						
7.2)ปรับปรุงนโยบายควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศตามระยะเวลาที่กำหนด						
7.3)มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
7.4)มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการยกเลิกสิทธิต่างๆ ในการใช้งานเมื่อพนักงานลาออกหรือเปลี่ยนตำแหน่งงานภายในองค์กร						
7.5)จำกัดสิทธิการใช้งานระบบสารสนเทศตามความจำเป็นในการใช้งานของบุคลากรขององค์กร						
7.6)มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานระบบสารสนเทศอย่างเป็นทางการ						
7.7)กำหนดวิธีปฏิบัติที่ดีในการตั้งรหัสผ่าน						
7.8)กำหนดวิธีปฏิบัติที่ดีในการใช้งานรหัสผ่าน เช่น รักษารหัสผ่านให้เป็นความลับ ไม่บันทึกรหัสผ่านที่สามารถพบเห็นได้ง่าย เป็นต้น						
7.9)มีมาตรการป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงาน						
7.10)มีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่มั่นคงปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น						
7.11)จัดทำนโยบายการใช้งานระบบเครือข่ายขององค์กร						
7.12)มีการระบุชัดเจนว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถเข้าถึงได้						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
7.13)มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กร						
7.14)มีการกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกการเชื่อมต่อจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว						
7.15)มีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย						
7.16)แบ่งแยกเครือข่ายขององค์กรตามกลุ่มของผู้ใช้งาน						
7.17)แบ่งแยกเครือข่ายขององค์กรตามสารสนเทศที่ใช้งาน						
7.18)แบ่งแยกเครือข่ายขององค์กรตามกลุ่มของระบบสารสนเทศ						
7.19)จำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร						
7.20)การเชื่อมต่อระหว่างองค์กรต้องเป็นไปตามนโยบายควบคุมการเข้าถึงขององค์กร						
7.21)กำหนดเส้นทางบนระบบเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง						
7.22)มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
7.23)มีการระบุตัวตนในการเข้าใช้งานระบบสารสนเทศ						
7.24)มีมาตรการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ						
7.25)กำหนดให้ระบบสารสนเทศตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด						
7.26)การเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของซอฟต์แวร์ แยกตามประเภทของผู้ใช้งาน						
7.27)แยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากสำหรับระบบนี้โดยเฉพาะ						
7.28)กำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone, และ tablet เป็นต้น) ในการเข้าสู่ระบบเครือข่าย						
7.29)กำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์อุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone, และ tablet เป็นต้น)						
7.30)กำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
8.การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)						
8.1)ระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว						
8.2)มีกลไกสำหรับตรวจสอบข้อมูลนำเข้าของซอฟแวร์ ว่าข้อมูลนั้นมีความถูกต้องและเหมาะสม						
8.3)มีกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่						
8.4)มีกลไกสำหรับการตรวจสอบข้อมูลนำออกจากซอฟต์แวร์ว่าเป็นไปอย่างถูกต้องเหมาะสม						
8.5)มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูลบังคับใช้ในองค์กร						
8.6)มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล						
8.7)มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบสารสนเทศที่ให้บริการแก่องค์กร						
8.8)ไม่ใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการ สำหรับทำการทดสอบระบบ						
8.9)มีการกำหนดให้มีการป้องกันและควบคุมการใช้งานข้อมูลจริงในการทดสอบระบบ						
8.10)จำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
8.11)กำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ						
8.12)มีการตรวจสอบทางเทคนิคภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าซอฟต์แวร์ทำงานได้ปกติ						
8.13)มีการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ตามความจำเป็นเท่านั้น						
8.14)มีการกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร						
8.15)มีการกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์						
8.16)มีการกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน						
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)						
9.1)มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ผ่านช่องทางการรายงานที่กำหนดไว้						
9.2)บันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่						
9.3)มีการกำหนดหน้าที่ความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
9.4)มีการกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร						
9.5)ขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร รวดเร็ว ได้ผล และเป็นระบบระเบียบที่ดี						
9.6)บันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย ประกอบด้วย ประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย						
9.7)ต้องรวบรวมและจัดเก็บหลักฐานเพื่อใช้ในกระบวนการทางศาลที่เกี่ยวข้อง						
9.8)มีกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงเพื่อใช้ในกระบวนการทางศาล						
10.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)						
10.1)มีการกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร						
10.2)มีการปรับปรุงกระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กรอย่างสม่ำเสมอ						
10.3)กระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กรจะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้าง						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
ความต่อเนื่องให้กับการให้บริการขององค์กร						
10.4)มีการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร						
10.5)มีการประเมินความเสี่ยงระบบสารสนเทศขององค์กร						
10.6)ต้องจัดทำแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้						
10.7)มีการใช้งานแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้						
10.8)มีการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับการให้บริการขององค์กร						
10.9)มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้การให้บริการขององค์กรอย่างสม่ำเสมอ						
11.การปฏิบัติตามข้อกำหนด (Compliance)						
11.1)มีการระบุข้อกำหนดทางด้านกฎหมายทางด้านระเบียบปฏิบัติ และที่ปรากฏใน						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
สัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานขององค์กร และบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร						
11.2)มีการปรับปรุงข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานขององค์กรอย่างสม่ำเสมอ						
11.3)มีการกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา						
11.4)มีการกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจจากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง						
11.5)มีการกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมายระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง						
11.6)ป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ระบบสารสนเทศขององค์กรผิดวัตถุประสงค์						
11.7)ป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต						
11.8)กำหนดให้ใช้มาตรการ การเข้ารหัสข้อมูลโดยสอดคล้องตามกฎหมาย						

มหาวิทยาลัยราชภัฏสกลนคร

มาตรการ	ความคิดเห็น					ความคิดเห็นเพิ่มเติม
	สภาพปัจจุบัน			ความต้องการ		
	มี	ไม่แน่ใจ	ไม่มี	ต้องการ	ไม่ต้องการ	
11.9)ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน						
11.10)มีการตรวจประเมินระบบสารสนเทศอย่างสม่ำเสมอ						
11.11)มีการระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร						
11.12)มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ						

มหาวิทยาลัยราชภัฏสกลนคร

ตอนที่ 3 ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ

กรุณาใส่หมายเลข 1 – 10 หน้าข้อที่ท่านคิดว่าเป็นปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร โดย 1 คือปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยมากที่สุด และ 10 คือปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยน้อยที่สุด

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

มหาวิทยาลัยราชภัฏสกลนคร