บทที่ 4

ผลการวิเคราะห์ข้อมูล

การวิจัยเรื่อง แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีความมุ่งหมายในการวิจัย คือ 1) เพื่อศึกษาบริบทการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร 2) เพื่อศึกษาการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กับกรอบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ 3) เพื่อศึกษาปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร 4) เพื่อพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประชากรที่ใช้ในการวิจัย บุคลากรกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กลุ่มตัวอย่างได้จากการสุ่มแบบชั้นภูมิ จำนวน 93 คน เครื่องมือในการวิจัย คือ แบบสัมภาษณ์กึ่งมีโครงสร้างใช้สัมภาษณ์ผู้ดูแลระบบสารสนเทศ จำนวน 8 คน และแบบสอบถามใช้เก็บข้อมูลกับบุคลากรกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร จำนวน 93 คน ซึ่งได้ผลจากการวิเคราะห์ข้อมูล ดังนี้

บริบทการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

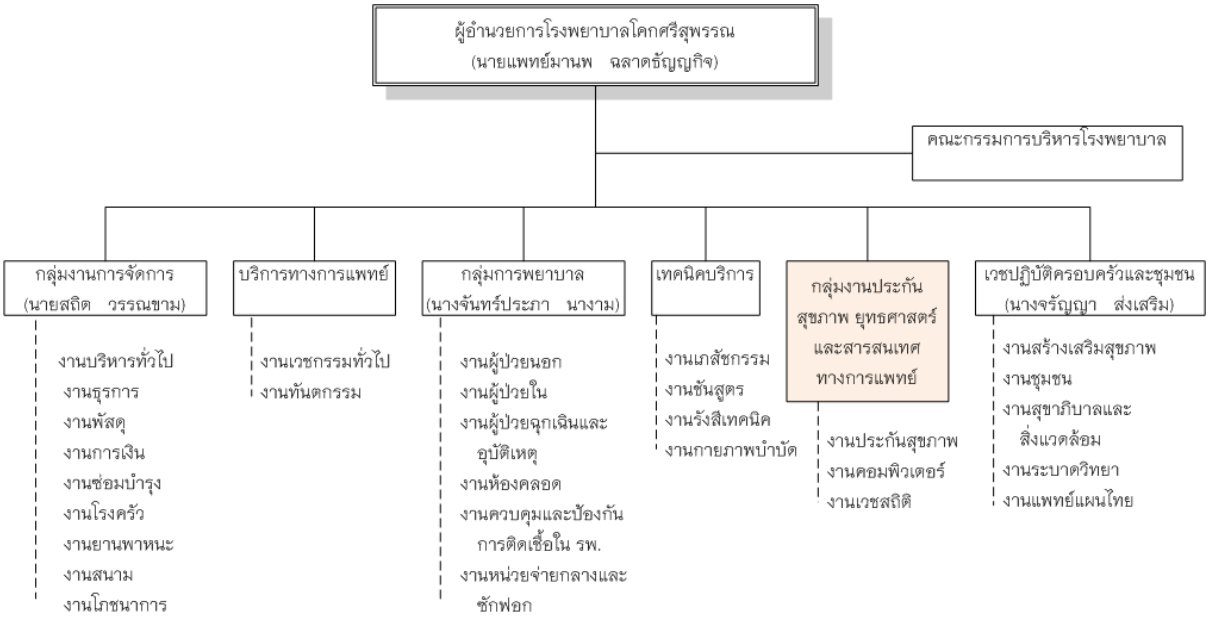
กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประกอบด้วย โรงพยาบาลโคกศรีสุพรรณ โรงพยาบาลส่งเสริมสุขภาพตำบล โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี โรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนา

1. โรงพยาบาลโคกศรีสุพรรณ

1.1 ที่มาประวัติของหน่วยงาน

โรงพยาบาลโคกศรีสุพรรณเป็นหน่วยงานสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ตั้งอยู่ที่บ้านตองโขบน้อย ถนนสกล–นาแก หมู่ที่ 8 ตำบลตองโขบ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เปิดบริการให้กับประชาชน เมื่อวันที่ 13 พฤษภาคม 2528 จนถึงปัจจุบัน (ผิน ฮ่มป่า, สัมภาษณ์, 17 ธันวาคม 2558)

โรงพยาบาลแบ่งโครงสร้างหน่วยงานภายในเป็น 6 หน่วยงาน ดังภาพประกอบ 3 ซึ่งหน่วยงาน ที่ทำหน้าที่และรับผิดชอบดูแลระบบสารสนเทศของโรงพยาบาลโคกศรีสุพรรณ งานซ่อมคอมพิวเตอร์ของ โรงพยาบาลส่งเสริมสุขภาพตำบล ในกลุ่มเครือข่าย ให้คำปรึกษาและช่วยเหลือผู้ดูแลระบบสารสนเทศของ โรงพยาบาลส่งเสริมสุขภาพตำบล รวมถึงการจัดการความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล สังกัดอยู่ในกลุ่มงานประกันยุทธศาสตร์ และสารสนเทศทางการแพทย์



ข้อมูล ณ วันที่ 11 ธันวาคม 2561

ภาพประกอบ 3 ผังการบริหารโรงพยาบาลโคกศรีสุพรรณ

1.2 การจัดการงานด้านเทคโนโลยีสารสนเทศ

ฝ่ายสารสนเทศ และงานประกันสุขภาพสังกัดกลุ่มงานประกัน ยุทธศาสตร์และสารสนเทศทางการแพทย์ มีนักวิชาการคอมพิวเตอร์จำนวน 3 คน ทำหน้าที่ดูแลระบบสารสนเทศของโรงพยาบาลโคกศรีสุพรรณทั้งหมด รวมถึงการเข้าร่วมการประชุมผู้ดูแลระบบสารสนเทศในระดับจังหวัดเพื่อรับนโยบายทางด้านเทคโนโลยีสารสนเทศ แนวทางปฏิบัติการติดตามงานต่างๆ

1.3 ระบบสารสนเทศของโรงพยาบาล

โรงพยาบาลโคกศรีสุพรรณ ได้นำระบบเทคโนโลยีสารสนเทศ เข้ามาใช้ในการจัดการงานและการสื่อสารภายในโรงพยาบาลระหว่างโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร โดยเริ่มใช้ตั้งแต่ปี พ.ศ.2548 ซึ่งมีรายละเอียดของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.3.1 ฮาร์ดแวร์ (Hardware)

อุปกรณ์สารสนเทศที่ใช้ในโรงพยาบาล ประกอบด้วย เครื่องแม่ข่าย เครื่องลูกข่ายดังแสดงในตาราง 9

ตาราง 9 ประเภทคอมพิวเตอร์และระบบปฏิบัติการที่ใช้ในโรงพยาบาล

ประเภทคอมพิวเตอร์	ระบบปฏิบัติการ	จำนวน (เครื่อง)	ประเภทการใช้
เครื่องลูกข่าย (Client)	Windows XP	32	เครื่องลูกข่ายสำหรับใช้ระบบ HOSxP
	Windows 7	20	เครื่องลูกข่ายสำหรับใช้ระบบ HOSxP
	Windows 8	20	เครื่องลูกข่ายสำหรับใช้ระบบ HOSxP
	Windows 8.1	2	เครื่องลูกข่ายสำหรับใช้ระบบ HOSxP
	รวม	74	

ตาราง 9 (ต่อ)

ประเภทคอมพิวเตอร์	ระบบปฏิบัติการ	จำนวน (เครื่อง)	ประเภทการใช้
เครื่องแม่ข่าย (Server)	CentOS	2	เครื่องแม่ข่ายหลัก HOSxP และเครื่องแม่ข่ายสำรอง
	Windows 8	1	เครื่องแม่ข่ายสำหรับรับข้อมูลระบบ Data center
	Windows XP	1	เครื่องแม่ข่ายระบบ Diskless
	pfSense	1	Firewall
	รวม	5	

จากตาราง 9 พบว่า เครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายส่วนใหญ่เป็นอุปกรณ์ที่เปิดใช้งานตลอดเวลาเกือบ 24 ชั่วโมงทำงาน รวมถึงเป็นอุปกรณ์ที่ซื้อมาด้วยเงินงบประมาณนานกว่า 3 ปี ทำให้เครื่องคอมพิวเตอร์ชำรุดหรือเสียบ่อย แต่การซื้อเครื่องใหม่ทดแทนเครื่องเดิมยังไม่สามารถทำได้ทุกจุด เพราะติดปัญหาด้านงบประมาณจัดซื้อ

1.3.2 ซอฟต์แวร์ (software)

โรงพยาบาลโคกศรีสุพรรณมีซอฟต์แวร์ที่ใช้สำหรับการจัดการข้อมูลของโรงพยาบาล ดังนี้

1.3.2.1 โปรแกรม HOSxP

เป็นโปรแกรมสำหรับจัดการกับข้อมูลเวชระเบียนของผู้ป่วย เช่น การส่งตรวจผู้ป่วย การจ่ายยา ระบบการชำระเงินค่ารักษา เป็นต้น จัดทำรายงานส่งสำนักงานสาธารณสุขจังหวัด พร้อมทั้งมีรวบรวมข้อมูลเวชระเบียนของผู้ป่วยจากโรงพยาบาลส่งเสริมสุขภาพตำบลในกลุ่มเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณเข้าด้วยกันหรือเรียกว่า ระบบ Data Center โดยชำระค่าบริการเป็นรายปี

1.3.2.2 ซอฟต์แวร์อื่นๆ

ซอฟต์แวร์อื่นๆ ที่พัฒนาเองโดยกลุ่มงานยุทธศาสตร์และสารสนเทศทางการแพทย์ของโรงพยาบาล ซึ่งใช้งานภายในหน่วยงานของโรงพยาบาล เช่น ระบบจองใช้รถ ระบบแจ้งซ่อม โปรแกรมความเสี่ยง เป็นต้น ซึ่งซอฟต์แวร์ที่พัฒนาจะพัฒนาด้วยเทคโนโลยีเว็บแอปพลิเคชัน (Web Application) รายละเอียดซอฟต์แวร์แสดงดังตาราง 10

ตาราง 10 ซอฟต์แวร์ที่ใช้ในโรงพยาบาลโคกศรีสุพรรณ

ชื่อซอฟต์แวร์	ผู้พัฒนา	ค่าใช้จ่ายในการดูแลระบบ	ผู้ดูแล
HOSxP	บริษัท บางกอกเมดิ–คอลซอฟต์แวร์ จำกัด	19,000 บาท	ผู้ดูแลระบบสารสนเทศของโรงพยาบาล
BMS Datacenter	บริษัท บางกอกเมดิ–คอลซอฟต์แวร์ จำกัด	โรงพยาบาลชุมชน 140,000 บาท โรงพยาบาลส่งเสริมสุขภาพตำบลแห่งละ 30,000 บาทรวม 150,000 บาท *เสียเฉพาะแรกเข้า	ผู้ดูแลระบบสารสนเทศของโรงพยาบาล
ระบบงานสารบรรณ	สำนักงานสาธารณสุขจังหวัด	–	สำนักงานสาธารณสุขจังหวัด
ระบบแจ้งซ่อมออนไลน์	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)	–	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)
ระบบบริหารความเสี่ยงออนไลน์ (Risk Management)	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)	–	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)
ระบบจองห้องประชุมออนไลน์	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)	–	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)
ระบบจองรถยนต์ออนไลน์	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)	–	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)

ตาราง 10 (ต่อ)

ชื่อซอฟต์แวร์	ผู้พัฒนา	ค่าใช้จ่ายในการดูแลระบบ	ผู้ดูแล
ระบบแจ้งขอรายงาน	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)	–	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)
ระบบคอมพิวเตอร์เซอร์วิสออนไลน์	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)	–	โรงพยาบาลโคกศรีสุพรรณ (จิรวัฒน์ ยาทองไชย)
SSO Media 2.0	สปสช.	–	สปสช.
LIS (Lab Information System)	บริษัท ไฟน์ดิ้ง จำกัด	–	บริษัท ไฟน์ดิ้ง จำกัด
MPI	–	–	สำนักงานสาธารณสุขจังหวัดสกลนคร

1.3.3 ข้อมูล (data)

ข้อมูลที่ถูกรวบรวมและจัดเก็บในโรงพยาบาลแบ่งตามลักษณะการใช้งานได้ 2 ประเภท คือ 1) ข้อมูลการรักษาผู้ป่วย จะแสดงรายละเอียดการรักษาของผู้ป่วยที่มารับบริการในโรงพยาบาลและโรงพยาบาลส่งเสริมสุขภาพตำบลในกลุ่มเครือข่าย เช่น ประวัติการวินิจฉัยโรค ประวัติการจ่ายยา ผลตรวจทางห้องแลป เป็นต้น 2) ฐานข้อมูลพื้นฐานสำหรับใช้ในโรงพยาบาล เช่น ฐานข้อมูลแจ้งซ่อม ฐานข้อมูลการจองใช้รถ ฐานข้อมูลฝ่ายบุคคล เป็นต้น

1.3.4 บุคลากร (people)

บุคลากรโรงพยาบาลโคกศรีสุพรรณแบ่งหน้าที่ความรับผิดชอบตามโครงสร้างของงาน และมีงานสารสนเทศ และงานประกันสุขภาพทำหน้าที่ดูแลและให้บริการเทคโนโลยีสารสนเทศกับบุคลากรในโรงพยาบาลรวมถึงการให้สิทธิในการเข้าถึงฐานข้อมูล เช่น บุคลากรที่ปฏิบัติหน้าที่เกี่ยวข้องกับการรักษาผู้ป่วย จะได้รับสิทธิในการเข้าถึงและใช้งานโปรแกรม HOSxP แสดงดังตาราง 11

บุคลากรในงานเทคโนโลยีสารสนเทศของโรงพยาบาลสำเร็จการศึกษาทางด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้องกับคอมพิวเตอร์ มีประสบการณ์ในการเขียนโปรแกรม เช่น โปรแกรมที่พัฒนาด้วยภาษา Delphi เป็นต้น ผู้ดูแลระบบสารสนเทศทำหน้าที่ในการดูแลระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร นอกเหนือจากงานประจำยังทำหน้าที่อื่นๆ เช่น เข้าร่วมการประชุมที่เกี่ยวกับระบบสารสนเทศของโรงพยาบาล และหน่วยงานในสังกัดกระทรวงสาธารสุข จัดอบรมในบุคลากรในหน่วยงานเครือข่าย

ตาราง 11 ความสัมพันธ์ของการเข้าถึงระบบงานและกลุ่มผู้ใช้

ระบบงาน	ผู้อำนวยการโรงพยาบาล	กลุ่มแพทย์	พยาบาล	กลุ่มห้องยา	งานห้อง X-RAY	กลุ่มงานชันสูตร	การเงิน	ลูกจ้าง (ผู้ช่วยแพทย์ไม่ใช้)	เภสัชกรและผู้ช่วย	หน่วยงานอื่น
1. ระบบประชาสัมพันธ์	✓	✓	✓	✓	✓	✓	✓	✓	✓	
2. ระบบเวชระเบียน	✓	✓	✓	✓	✓	✓	✓	✓	✓	
3. ระบบตรวจสอบสิทธิ								✓	✓	✓
4. ระบบซักประวัติ			✓					✓	✓	
5. ระบบนัดหมาย		✓	✓			✓			✓	
6. ระบบห้องทำงานแพทย์		✓	✓						✓	
7. ระบบงานห้องฉุกเฉิน		✓	✓						✓	
8. ระบบคลินิกพิเศษ		✓	✓	✓					✓	
9. ระบบคัดกรองกลุ่มเสี่ยงเรื้อรัง		✓	✓						✓	
10. ระบบทันตกรรม		✓	✓						✓	
11. ระบบชันสูตร		✓	✓			✓				
12. ระบบรังสีรักษา		✓	✓		✓	✓			✓	

ตาราง 11 (ต่อ)

ระบบงาน	ผู้ดูแลระบบ	แพทย์	พยาบาล	ห้องปฏิบัติการ	งานห้อง X-RAY	เภสัชกรรม	การเงิน	ผู้ช่วย (ผู้ที่ไม่มีสิทธิ์)	เจ้าหน้าที่	ประชาสัมพันธ์
13. ระบบเวชศาสตร์ฟื้นฟู		✓	✓						✓	
14. ระบบแพทย์แผนไทย									✓	
15. ระบบเภสัชกรรม				✓					✓	
16. ระบบการเงิน							✓			
17. ระบบห้องผ่าตัด และวิสัญญี		✓	✓						✓	
18. ระบบ Admission Center		✓	✓							
19.ระบบผู้ป่วยใน		✓	✓							
20. ระบบห้องคลอด		✓	✓							
21. ระบบงานโภชนาการ		✓	✓							
22. ระบบส่งเสริมสุขภาพ และระบบ One Stop Service		✓	✓							
23. ระบบงานสำรองข้อมูล									✓	
24. ระบบงานรายงาน	✓	✓	✓	✓	✓	✓	✓	✓	✓	
25. ระบบงานผู้ดูแลระบบ									✓	
26. ระบบส่งออกข้อมูล									✓	
27. Data Center	✓	✓	✓	✓			✓		✓	

1.3.5 ขั้นตอนการปฏิบัติงาน (procedure)

งานคอมพิวเตอร์ไม่มีข้อปฏิบัติ หรือประกาศที่เป็นลายลักษณ์อักษร แต่มีการปฏิบัติงานของงานคอมพิวเตอร์ เพื่ออำนวยความสะดวกแก่หน่วยงานต่างๆ ภายในโรงพยาบาล ให้สามารถใช้บริการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลได้อย่างราบรื่น และมั่นคงปลอดภัย โดยมีการปฏิบัติงานของงานคอมพิวเตอร์ ดังนี้

1.3.5.1 การสร้างบัญชีผู้ใช้ (Account)

การสร้างบัญชีผู้ใช้ (Account) สำหรับเจ้าหน้าที่จะพิจารณาสร้างให้เฉพาะเจ้าหน้าที่ผู้ที่เกี่ยวข้องกับการรักษาผู้ป่วย โดยห้ามใช้บัญชีผู้ใช้ร่วมกัน และจำกัดสิทธิให้เข้าถึงได้เฉพาะส่วนงานที่รับผิดชอบเท่านั้น การพิจารณาสิทธิของการใช้งานกลุ่มงานยุทธศาสตร์และสารสนเทศทางการแพทย์จะเป็นผู้พิจารณาเท่านั้น

1.3.5.2 งานซ่อมบำรุงและดูแลรักษาระบบเทคโนโลยีสารสนเทศ

หากมีการแจ้งจากผู้ใช้ไม่ว่าจะเป็นช่องทางการแจ้งทางโทรศัพท์ หรือการแจ้งผ่านระบบแจ้งซ่อมคอมพิวเตอร์ ออนไลน์ งานคอมพิวเตอร์จะส่งเจ้าหน้าที่ดำเนินการแก้ไขปัญหาให้ผู้ใช้ทันที

งานคอมพิวเตอร์มีหน้าที่รับผิดชอบในการดูแล บำรุงรักษาให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลโคกศรีสุพรรณ มีความพร้อมใช้ตลอด 24 ชั่วโมง

1.3.5.3 งานสร้างรายงานจากระบบ HOSxP

หน่วยงานที่ต้องการรายงานจากข้อมูลของระบบ HOSxP สามารถแจ้งขอรายงานได้ในช่องทางทางโทรศัพท์ ช่องทางระบบแจ้งขอรายงานออนไลน์ และช่องทางการติดต่อที่หน่วยงานคอมพิวเตอร์

1.3.6 เครือข่าย (Network)

ระบบเครือข่ายของโรงพยาบาลโคกศรีสุพรรณแบ่งเป็น 2 ประเภท มีรายละเอียดดังนี้

1.3.6.1 เครือข่ายภายใน (Intranet)

หมายถึงเครือข่ายภายในโรงพยาบาลให้บริการผ่านระบบแลนและไวเลสแลน ซึ่งการเดินสายการติดตั้งเครือข่ายทำโดยผู้ดูแลระบบของโรงพยาบาลเองทั้งหมด

ผู้ใช้งานอินเทอร์เน็ตต้องมีชื่อผู้ใช้และรหัสผ่าน สำหรับการเข้าใช้ ห้ามใช้งานชื่อผู้ใช้ร่วมกัน โดยชื่อผู้ใช้ 1 รายชื่อ จะเข้าใช้อินเทอร์เน็ตได้เพียง 1 อุปกรณ์เท่านั้น ซึ่งผู้ใช้สามารถขอเพิ่มรายชื่อเพื่อใช้กับอุปกรณ์อื่นเพิ่มเติมได้ การขอใช้อินเทอร์เน็ตทำได้โดย ผู้ใช้ต้องมาลงทะเบียนเพื่อขอเข้าใช้อินเทอร์เน็ตที่กลุ่มงานคอมพิวเตอร์ โดยทางกลุ่มงานคอมพิวเตอร์จะเก็บเอกสารผู้ใช้เพื่อเป็นหลักฐานในการใช้อินเทอร์เน็ต

การกำหนดการตั้งค่าที่ไฟล์วอลเพื่ออนุญาตให้ใช้แอปพลิเคชันใดได้บ้าง ต้องมีการประชุมคณะกรรมการบริหารของโรงพยาบาลเพื่อกำหนดนโยบายในการใช้แอปพลิเคชันต่างๆ ของโรงพยาบาล

1.3.6.2 เครือข่ายภายนอก (Internet)

ระบบเครือข่ายของโรงพยาบาลโคกศรีสุพรรณใช้บริการอินเทอร์เน็ต จากผู้ให้บริการอินเทอร์เน็ต (Internet service provider : ISP) เช่น บริษัท กสท. โทรคมนาคม จำกัด ดาวน์โหลด 30 Mb อัพโหลด 3 Mb บริษัท ทริปเปิลที บรอด-แบนด์ จำกัด (มหาชน) ดาวน์โหลด 5 Mb อัพโหลด 1 Mb พร้อมหมายเลขไอพี 110.164.210.137 เป็นต้น

ระบบอินเทอร์เน็ตของโรงพยาบาลใช้ระบบโหลดบาลานซ์ (Load balance) ในการให้บริการอินเทอร์เน็ต ซึ่งเป็นการใช้อินเทอร์เน็ตของผู้ให้บริการสองที่ทำงานร่วมกัน โดยใช้บริการผู้ให้บริการอินเทอร์เน็ตคือ บริษัท กสท. โทรคมนาคม จำกัด และบริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) เพื่อให้เกิดความต่อเนื่องของการให้บริการ

1.4. ปัญหาของระบบสารสนเทศ

จากการสัมภาษณ์นายผิน ฮ่มป่า หัวหน้างานสารสนเทศ และงานประกันสุขภาพ (ผิน ฮ่มป่า, สัมภาษณ์, 22 มิถุนายน 2558) พบปัญหาของระบบสารสนเทศของโรงพยาบาล ดังนี้

1.4.1 คอมพิวเตอร์ที่มีอายุการใช้งานนานเกิดปัญหาเป็นประจำ ไม่สามารถให้บริการได้อย่างต่อเนื่อง แต่ไม่สามารถจัดซื้อตามความต้องการของผู้ดูแลระบบสารสนเทศได้ เนื่องจากติดปัญหาข้อจำกัดในระเบียบการจัดซื้อของโรงพยาบาล

1.4.2 ผู้ใช้ในกลุ่มเครือข่ายบริการสุขภาพฯ ใช้ความสามารถระบบ Data Center น้อย ถ้าเทียบกับความสามารถของ Data center ที่มีอยู่ ไม่คุ้มค่ากับการลงทุนด้าน Data Center อีกทั้งผู้ใช้ยังไม่ทราบช่องทางการเข้าถึงและการนำข้อมูลไปใช้

ประโยชน์ โดยผู้ดูแลระบบสารสนเทศเสนอว่า ต้องจัดให้มีการอบรม ทั้งผู้ใช้และผู้ดูแลระบบสารสนเทศ เพื่อเรียนรู้ในการใช้ข้อมูลใน Data center โดยที่ผ่านมามีการอบรมผู้ดูแลระบบสารสนเทศแต่ละสถานบริการ

1.5 ความต้องการระบบสารสนเทศ

จากการสัมภาษณ์นายผิน ฮ่มป่า หัวหน้างานสารสนเทศ และงานประกันสุขภาพ (ผิน ฮ่มป่า, สัมภาษณ์, 22 มิถุนายน 2558) มีความต้องการในการพัฒนาระบบสารสนเทศของโรงพยาบาล ดังนี้

ระบบ HOSxP ที่ใช้เริ่มมีข้อจำกัด ซึ่งต่อไปต้องเปลี่ยนเป็นโปรแกรม HOSxP เวอร์ชันใหม่ ซึ่งโปรแกรมในเวอร์ชันใหม่นี้รองรับเทคโนโลยีมากขึ้น เช่น การสแกนม่านตา การสแกนรอยนิ้วมือ เป็นต้น โดยขณะนี้อยู่ระหว่างการศึกษาโปรแกรม HOSxP เวอร์ชันใหม่

2. โรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนา

2.1 ประวัติหน่วยงาน

โรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนา หรือสถานีอนามัยโพนทองวัฒนาก่อตั้งขึ้นในปี พ.ศ.2552 ได้ยกระดับจากสถานีอนามัยเป็นโรงพยาบาลส่งเสริมสุขภาพเพื่อให้บริการด้านสาธารณสุขแก่ประชาชนในเขตตำบลโพนทองวัฒนา

การบริหารงานของโรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนาขึ้นตรงกับสาธารณสุขอำเภอโคกศรีสุพรรณ ที่ว่าการอำเภอโคกศรีสุพรรณ (นายอำเภอ) และสำนักงานสาธารณสุขจังหวัดตามลำดับ

ภาพประกอบ 4 โรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนา

2.2 การจัดการด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนา ไม่มีโครงสร้างงานเกี่ยวกับเทคโนโลยีสารสนเทศโดยมอบหมายให้บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบล ทำหน้าที่ดูแลระบบสารสนเทศ 1 คน ปฏิบัติหน้าที่ผู้ดูแลระบบสารสนเทศเพิ่มนอกเหนือจากงานประจำ คือ การปฏิบัติหน้าที่ทางด้านสาธารณสุข ซึ่งบุคลากรดังกล่าวไม่จบหลักสูตรเกี่ยวกับเทคโนโลยีสารสนเทศ ใช้วิธีการเรียนรู้ด้วยตนเองจากสื่อต่างๆ เช่น หนังสือ เว็บไซต์ เป็นต้น และปรึกษานักวิชาการคอมพิวเตอร์ของโรงพยาบาลโคกศรีสุพรรณ

2.3 ระบบสารสนเทศ

2.3.1 ฮาร์ดแวร์ (hardware)

คอมพิวเตอร์ที่ใช้ภายใน โรงพยาบาลส่งเสริมสุขภาพตำบล ได้มาจากการตั้งงบประมาณ ผ่านทางกลุ่มเครือข่ายบริการสุขภาพ คุณลักษณะคอมพิวเตอร์ส่วนใหญ่ติดตั้งระบบปฏิบัติการ Windows และเครื่องแม่ข่ายของโปรแกรม HOSxP PCU ติดตั้งระบบปฏิบัติการ CentOS โดยดำเนินการติดตั้งเครื่องแม่ข่ายไว้ที่ห้องยาของโรงพยาบาลส่งเสริมสุขภาพตำบล

2.3.2 ซอฟต์แวร์ (software)

ซอฟต์แวร์ที่ใช้ในโรงพยาบาลส่งเสริมสุขภาพตำบล ได้แก่ HOSxP PCU สำหรับบริหารจัดการข้อมูลการให้บริการแก่ประชาชนผู้รับบริการ รวมถึงการส่งออกข้อมูลเพื่อรายงานแก่หน่วยงานต้นสังกัดที่เกี่ยวข้อง โดยเป็นซอฟต์แวร์ที่สามารถใช้ได้โดยไม่เสียค่าใช้จ่าย

2.3.3 ข้อมูล (Data)

ข้อมูลที่มีการเก็บในโรงพยาบาลส่งเสริมสุขภาพตำบล คือ ข้อมูลการรักษาคนไข้ และผู้มารับบริการ โดยเก็บอยู่ใน 2 ลักษณะ คือ แฟ้มเวชระเบียน และข้อมูลที่เก็บอยู่ในฐานข้อมูลของโปรแกรม HOSxP PCU

ข้อมูลการรักษาผู้ป่วยในลักษณะของแฟ้มข้อมูลเวชระเบียนจะถูกจัดเก็บอยู่ในตู้เอกสารภายในโรงพยาบาลส่งเสริมสุขภาพตำบลพร้อมทั้งล็อคกุญแจไว้เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องกับการรักษาเท่านั้น ต้องเก็บย้อนหลังเป็นเวลา 5 ปี

ข้อมูลซึ่งเก็บไว้ในระบบ HOSxP PCU ของโรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนาได้รับการตั้งค่าให้ดำเนินการสำรองข้อมูลในทุกวัน โดย

ฐานข้อมูล HOSxP PCU ที่ดำเนินการสำรองเสร็จ จะแยกสำรองไว้ในฮาร์ดดิสภายนอก (External Hardisk)ทุกวัน

2.3.4 บุคลากร (people)

บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบล จะถูกกำหนดและได้รับสิทธิในการเข้าใช้งานระบบ HOSxP PCU ตามหน้าที่รับผิดชอบ และสิทธิการเข้าถึงข้อมูลการรักษาคนไข้ ข้อมูลการให้บริการ ได้ตามหน้าที่รับผิดชอบเช่นกัน

บุคลากรผู้ทำหน้าที่ดูแลระบบสารสนเทศของโรงพยาบาลได้รับการแต่งตั้งจากบุคลากรเดิมของ รพสต. ซึ่งรับผิดชอบงานในตำแหน่งนักวิชาการสาธารณสุข ผู้ดูแลระบบสารสนเทศมีหน้าที่รับผิดชอบระบบสารสนเทศของ รพสต. ดูแลตรวจสอบความถูกต้องของข้อมูลการรักษาของคนไข้ ข้อมูลการให้บริการ เข้าร่วมการประชุมผู้ดูแลระบบสารสนเทศทั้งในระดับอำเภอ และระดับจังหวัด

ตาราง 12 การเข้าถึงระบบงานและกลุ่มผู้ใช้

ระบบงาน	ผู้ใช้งานทั่วไป	เภสัชกร	ทันตแพทย์	แพทย์แผนไทย	ผู้ใช้เฉพาะหน่วยงาน
การวินิจฉัย	✓	✓	✓	✓	
Medication	✓	✓	✓	✓	
หัตถการ	✓	✓	✓	✓	
สรุปค่าใช้จ่าย	✓	✓	✓	✓	
ข้อมูลการส่งต่อ	✓	✓	✓	✓	
การนัดหมาย	✓	✓	✓	✓	
ทันตกรรม	✓	✓	✓	✓	
ตัวเลือกการพิมพ์	✓	✓	✓	✓	
ลงผล Lab	✓	✓	✓	✓	

ตาราง 12 (ต่อ)

ระบบงาน	นักวิชาการสาธารณสุข	แพทย์แผนไทย	ทันตแพทย์	พยาบาลวิชาชีพ	ผู้ช่วยเหลือคนไข้
Vaccine	✓	✓	✓	✓	
การคัดกรอง	✓	✓	✓	✓	
กายภาพ	✓	✓	✓	✓	
ตรวจยืนยันโรคเรื้อรัง	✓	✓	✓	✓	
การประเมินสุขภาพ	✓	✓	✓	✓	
ข้อมูลเวชระเบียน	✓	✓	✓	✓	✓

2.3.5 ขั้นตอนการปฏิบัติงาน (procedure)

นโยบายทางด้านเทคโนโลยีสารสนเทศของ โรงพยาบาลส่งเสริมสุขภาพตำบล ยังไม่มีประกาศเป็นลายลักษณ์อักษร แต่มีการบอกต่อกฎระเบียบการใช้ระบบสารสนเทศว่า ห้ามใช้นอกเหนือจากภาระงานที่รับผิดชอบ

2.3.6 เครือข่าย (Network)

ระบบเครือข่ายภายในโรงพยาบาลส่งเสริมสุขภาพตำบลมีระบบเครือข่ายในลักษณะแลน (Lan) และมีการใช้เครือข่ายไร้สาย (wireless lan) สำหรับให้บริการแก่บุคลากร โดยการบริหารจัดการ การเดินสายติดตั้ง และการบำรุงรักษาเป็นหน้าที่ของผู้ดูแลระบบสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลโพนทองวัฒนาใช้บริการอินเตอร์เน็ตของบริษัท กสท โทรคมนาคม จำกัด (มหาชน) โดยกระทรวงสาธารณสุขเป็นผู้รับผิดชอบค่าใช้จ่ายในส่วนนี้

2.4 ปัญหาของระบบสารสนเทศ

คอมพิวเตอร์หากมีการชำรุด หรือไม่สามารถให้บริการได้ จนต้องนำไปซ่อมนั้น ระหว่างที่มีการซ่อมคอมพิวเตอร์นั้น โรงพยาบาลส่งเสริมสุขภาพตำบล ไม่มี

เครื่องคอมพิวเตอร์สำรอง ทำให้จุดที่มีคอมพิวเตอร์เสียนั้นไม่มีคอมพิวเตอร์สำหรับให้บริการ

ผู้ดูแลระบบสารสนเทศไม่เพียงพอต่อการปฏิบัติงาน เนื่องจากมีผู้ดูแลระบบสารสนเทศเพียงคนเดียว หากติดราชการที่อื่นอาจจะส่งผลต่อการแก้ปัญหาระบบสารสนเทศที่เกิดขึ้นได้ และงานหลักที่รับผิดชอบคืองานทางด้านสาธารณสุข

2.5 ความต้องการระบบสารสนเทศ

ผู้ดูแลระบบสารสนเทศของโรงพยาบาลส่งเสริมสุขภาพตำบลโพนทอง วัฒนาควรรับผู้ที่สำเร็จการศึกษาทางด้านเทคโนโลยีสารสนเทศ หรือทางด้านคอมพิวเตอร์ หรืออาจกำหนดตำแหน่งผู้ดูแลระบบสารสนเทศซึ่งรับผิดชอบดูแลระบบสารสนเทศของ รพสต. ทั้ง 5 แห่ง ของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

3. โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ

3.1 ประวัติหน่วยงาน

โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ เดิมคือ สถานีอนามัยห้วยหีบ ใน พ.ศ.2552 ได้ยกระดับเป็นโรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ โดยให้บริการด้านสาธารณสุขแก่ประชาชนในเขตตำบลห้วยหีบ อำเภอโคกศรีสุพรรณ

การบริหารงานของโรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ ขึ้นตรงกับสาธารณสุขอำเภอ ที่ว่าการอำเภอโคกศรีสุพรรณ (นายอำเภอ) และสำนักงานสาธารณสุขจังหวัดตามลำดับ

ภาพประกอบ 5 โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบ

3.2 การจัดการด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณมีเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศของ รพสต. 1 คน ซึ่งนโยบายของกลุ่มเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณมีนโยบายให้มีผู้ดูแลระบบสารสสนเทศของโรงพยาบาลส่งเสริมสุขภาพตำบล แห่งละ 1 คน ดูแลระบบสารสนเทศทั้งหมดของโรงพยาบาลส่งเสริมสุขภาพตำบลประสานงาน ให้ความช่วยเหลือ กับผู้ดูแลระบบสารสนเทศคนอื่นของโรงพยาบาลส่งเสริมสุขภาพตำบล

3.3 ระบบสารสนเทศ

3.3.1 ฮาร์ดแวร์ (hardware)

คอมพิวเตอร์ที่ใช้ใน โรงพยาบาลส่งเสริมสุขภาพตำบล ประกอบด้วย เครื่องลูกข่าย เป็นคอมพิวเตอร์แบบเดสทอป (computer desktop) คอมพิวเตอร์แบบโน้ตบุ๊ค (computer notebook) ติดตั้งระบบปฏิบัติการ Windows และเครื่องแม่ข่าย 1 เครื่อง ติดตั้งระบบปฏิบัติการ CentOS ซึ่งเป็นเครื่องแม่ข่ายของโปรแกรม HOSxP PCU

3.3.2 ซอฟต์แวร์ (software)

ซอฟต์แวร์ที่ใช้ในการให้บริการแก่ประชาชนของโรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ คือ ระบบ HOSxP PCU ของบริษัท บางกอกเมดิคอลซอฟต์แวร์ จำกัด โรงพยาบาลส่งเสริมสุขภาพตำบลทุกแห่ง สามารถใช้ระบบ HOSxP PCU ได้ โดยไม่มีค่าใช้จ่าย

3.3.3 ข้อมูล (Data)

ข้อมูลที่มีการเก็บใน โรงพยาบาลส่งเสริมสุขภาพตำบล คือ ข้อมูลการรักษาผู้ป่วย โดยเก็บอยู่ใน 2 ลักษณะ คือ แฟ้มเวชระเบียน และข้อมูลที่เก็บอยู่ในฐานข้อมูลของโปรแกรม HOSxP PCU

แฟ้มเวชระเบียนจะถูกจัดเก็บไว้ในตู้ภายในอาคารของ โรงพยาบาลส่งเสริมสุขภาพตำบล มีการจัดเป็นหมวดหมู่ โดยจะแยกแฟ้มเวชระเบียนที่เป็นโรคเรื้อรังและแฟ้มเวชระเบียนที่เป็นโรคที่ต้องปกปิดเป็นความลับออกจากแฟ้มเวชระเบียนทั่วไป แฟ้มเวชระเบียนที่เป็นความลับจะถูกเก็บไว้ในที่เก็บเอกสารซึ่งเจ้าหน้าที่ผู้รับผิดชอบเท่านั้นที่จะสามารถเข้าถึงข้อมูลนี้ได้

ฐานข้อมูลของโปรแกรม HOSxP PCU จำกัดสิทธิการเข้าถึงข้อมูลของคนไข้ ข้อมูลการให้บริการ ตามหน้าที่รับผิดชอบของเจ้าหน้าที่แต่ละตำแหน่ง โดยฐานข้อมูลของโปรแกรม HOSxP PCU มีการสำรองข้อมูลในทุกวัน และคัดลอกฐานข้อมูลที่สำรองไว้นี้

เก็บไว้ที่ฮาร์ดดิสแบบพกพา (external harddisk) รับผิดชอบโดยผู้ดูแลระบบสารสนเทศของ รพสต.

3.3.4 บุคลากร (people)

โรงพยาบาลส่งเสริมสุขภาพห้วยหีบรุ่งอรุณมีเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศ 1 คน โดยแต่งตั้งจากบุคลากรเดิมของ โรงพยาบาลส่งเสริมสุขภาพตำบล ซึ่งทำหน้าที่ในตำแหน่งนักวิชาการสาธารณสุข ทำหน้าที่ดูแลระบบสารสนเทศทั้งหมดของ รพสต. และดูแลความถูกต้องของข้อมูลการรักษาของคนไข้ และข้อมูลการการให้บริการ

บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ ได้รับการกำหนดสิทธิในการใช้ระบบ HOSxP PCU และข้อมูลการรักษาคนไข้ ข้อมูลการให้บริการ ตามหน้าที่รับผิดชอบในแต่ละตำแหน่ง

3.3.5 ขั้นตอนการปฏิบัติงาน (procedure)

โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณด้านการบริหารรับนโยบายจาก สำนักงานสาธารณสุขอำเภอ ที่ว่าการอำเภอโคกศรีสุพรรณ (นายอำเภอ) และสำนักงานสาธารณสุขจังหวัดตามลำดับ ซึ่งนโยบายที่รับมาส่วนมากจะเป็นนโยบายด้านข้อมูล ที่ โรงพยาบาลส่งเสริมสุขภาพตำบล ต้องส่งให้หน่วยงานต้นสังกัด

โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณไม่มีนโยบายด้านเทคโนโลยีสารสนเทศที่ประกาศเป็นลายลักษณ์อักษร

3.3.6 เครือข่าย (Network)

โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณใช้เครือข่ายแลน (LAN) และเครือข่ายไร้สาย ในการให้บริการเครือข่ายแก่บุคลากร การเดินสายแลน และการขยายจุดเชื่อมต่อเครือข่ายไร้สายดำเนินการโดยผู้ดูแลระบบสารสนเทศเอง หรือมีการจ้างบุคคลภายนอกในการเดินสายในบางจุด

อินเทอร์เน็ตโรงพยาบาลส่งเสริมสุขภาพตำบล ห้วยหีบรุ่งอรุณ ใช้บริการของบริษัท กสท. โทรคมนาคม จำกัด (CAT) ซึ่งเป็นนโยบายกระทรวงสาธารณสุขให้ รพสต. สามารถใช้งานได้โดยไม่มีค่าใช้จ่าย

3.4 ปัญหาของระบบสารสนเทศ

ปัญหาของระบบสารสนเทศมีดังต่อไปนี้

3.4.1 ผู้ใช้โปรแกรม HOSxP PCU คีย์ข้อมูลเข้าโปรแกรมไม่ถูกต้อง ทำให้รายงานที่ส่งไปยังต้นสังกัดไม่ถูกต้อง แก้ปัญหาโดยผู้ดูแลระบบสารสนเทศสอนการคีย์ข้อมูลที่ถูกต้องแก่ผู้ใช้ และศึกษาเพิ่มเติมการคีย์ข้อมูลจากคู่มือ

3.4.2 ตารางในฐานข้อมูลของ โรงพยาบาลส่งเสริมสุขภาพตำบลห้วยหีบรุ่งอรุณ มีความเฉพาะตัว ทำให้เมื่อถึงเวลาอัพเกรด ต้องทำการอัพเกรดเองโดยผู้ดูแลระบบสารสนเทศของโรงพยาบาลส่งเสริมสุขภาพตำบล ไม่สามารถอัพเกรด โดยใช้การอัพเกรดจากบริษัทผู้พัฒนาโดยตรงทั้งหมดได้

3.4.3 ระบบ HOSxP PCU มีส่วนติดต่อผู้ใช้และเมนูแตกต่างระบบ HOSxP ที่ใช้ในโรงพยาบาลโคกศรีสุพรรณ ทำให้เจ้าหน้าที่ของโรงพยาบาลโคกศรีสุพรรณที่มาออกตรวจที่ โรงพยาบาลส่งเสริมสุขภาพตำบล ไม่สามารถใช้ระบบ HOSxP PCU ได้โดยสะดวก ส่งผลให้เกิดความล่าช้าในการปฏิบัติหน้าที่

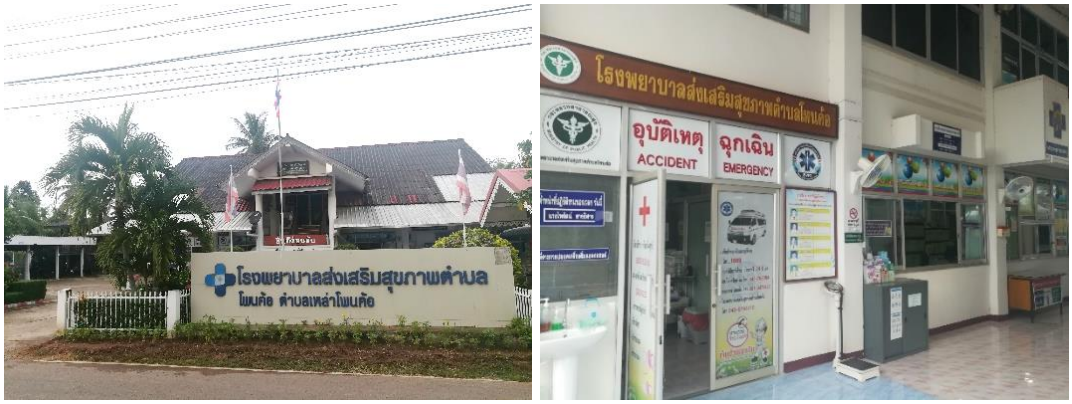
3.5 ความต้องการระบบสารสนเทศ

บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบล ในทุกระดับต้องให้ความสำคัญ ให้ความร่วมมือกับผู้ดูแลระบบสารสนเทศในการใช้ระบบ HOSxP PCU และการคีย์ข้อมูลเข้าไปในระบบ HOSxP PCU

4. โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ

4.1 ที่มาประวัติหน่วยงาน

โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ ตั้งอยู่ที่ ตำบลห้วยหีบ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร แต่เดิมชื่อว่า สถานีอนามัยเหล่าโพนค้อ ในปี พ.ศ.2552 ยกระดับเปลี่ยนเป็นโรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ และได้ดำเนินการให้บริการแก่ประชาชนในเขตตำบลเหล่าโพนค้อเป็นต้นมาจนถึงปัจจุบัน



ภาพประกอบ 6 โรงพยาบาลส่งเสริมสุขภาพตำบลโพนค้อ

4.2 การจัดการงานด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ มีบุคลากรทำหน้าที่ดูแลระบบสารสนเทศของโรงพยาบาลเป็นหลัก 1 คน โดยเป็นบุคลากรของ รพสต.เหล่าโพนค้อ อยู่เดิม และบุคลากรของ รพสต. คนอื่น ที่รับผิดชอบในแต่ละงาน จะทำหน้าที่เป็นผู้ดูแลระบบสารสนเทศของในงานนั้นๆ เป็นการแบ่งเบาภาระงานของผู้ดูแลระบบสารสนเทศหลักของ รพสต.

4.3 ระบบสารสนเทศ

4.3.1 ฮาร์ดแวร์ (Hardware)

คอมพิวเตอร์ที่ใช้ใน รพสต. มีจำนวนเพียงพอต่อบุคลากร โดยประกอบไปด้วยเครื่องแม่ข่าย และเครื่องลูกข่าย ดังแสดงในตาราง 13

ตาราง 13 จำนวนคอมพิวเตอร์ของโรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ

ประเภทของคอมพิวเตอร์	**ระบบปฏิบัติการ**	**จำนวน (เครื่อง)**	**ประเภทการใช้**
เครื่องลูกข่าย	Windows XP	6	เครื่องลูกข่ายระบบ HOSxP
เครื่องลูกข่าย	8	2	เครื่องลูกข่ายระบบ HOSxP
	xp	2	เครื่องลูกข่ายระบบ HOSxP
	รวม	10	

ตาราง 13 (ต่อ)

ประเภทของคอมพิวเตอร์	ระบบปฏิบัติการ	จำนวน (เครื่อง)	ประเภทการใช้
เครื่องแม่ข่าย	Centos	1	เครื่องแม่ข่ายหลักระบบ HOSxP
	รวม	1	

คอมพิวเตอร์ของโรงพยาบาลส่งเสริมตำบลเหล่าโพนค้อโดยส่วนมากมีอายุการใช้งานมากกว่า 5 ปี และทำงานได้ช้า ซึ่งทาง รพสต. มีความต้องการคอมพิวเตอร์ใหม่เพื่อรองรับการให้บริการแก่ประชาชน และรองรับการทำงานของโรงพยาบาลส่งเสริมสุขภาพตำบลแต่ยังไม่สามารถจัดซื้อเครื่องใหม่ได้ เนื่องจากติดปัญหาในด้านงบประมาณและการจัดซื้อ

4.3.2 ซอฟต์แวร์ (Software)

โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ มีซอฟต์แวร์ที่ใช้งาน คือ

4.3.2.1 โปรแกรม HOSxPPCU ทำหน้าที่ในการบริหารจัดการการให้บริการแก่ประชาชน ผู้มารับบริการของ รพสต. บันทึกข้อมูลการรักษาของผู้มารับบริการ จัดทำรายงานส่งสาธารณสุขจังหวัดและหน่วยงานที่เกี่ยวข้อง รวมถึงส่งข้อมูลของผู้รับบริการไปยังระบบ Data Center ของกลุ่มเครือข่ายบริการสุขภาพ

4.3.2.2 โปรแกรมพัสดุครุภัณฑ์ซึ่งได้รับมาจากโรงพยาบาลโคกศรีสุพรรณ

4.3.2.3 ซอฟต์แวร์ที่สำหรับการส่งรายงาน เช่น ระบบ Cockpit ซึ่งเป็นระบบสำหรับส่งรายงานไปยังสาธารณสุขจังหวัด โปรแกรมเฝ้าระวังทางระบาดวิทยา (R506) เป็นต้น

4.3.3 ข้อมูล (Data)

4.3.3.1 ข้อมูลที่มีการจัดเก็บที่โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ คือ ข้อมูลของผู้มารับบริการในแต่ละวัน และส่งข้อมูลของผู้มารับบริการนี้ไปยังระบบ Data center โดยข้อมูลของผู้รับบริการ ถูกเก็บไว้สองลักษณะ คือ ข้อมูลที่เก็บในระบบ HOSxP PCU และข้อมูลของผู้รับบริการ ที่เก็บไว้ในเวชระเบียน

4.3.3.2 ข้อมูลในฐานของข้อมูลของโปรมแกรมพัสดุครุภัณฑ์

4.3.4 บุคลากร (People)

บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อที่ปฏิบัติหน้าที่เกี่ยวข้องกับการให้บริการแก่ผู้มารับบริการชอง รพสต. จะได้รับสิทธิในการเข้าใช้งาน HOSxP PCU โดยจะได้รับการจำกัดสิทธิการเข้าถึงข้อมูลเฉพาะข้อมูลที่เกี่ยวกับงานที่รับผิดชอบเท่านั้น

ผู้ดูแลระบบสารสนเทศของโรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อได้รับการแต่งตั้งจากบุคลากรเดิมของ รพสต.ซึ่งรับผิดชอบงานในตำแหน่งนักวิชาการสาธารณสุข แต่ได้รับมอบหมายให้ทำหน้าที่เป็นผู้ดูแลระบบสารสนเทศของ รพสต. เพิ่มเติมจากภาระงานเดิม

4.3.5 ขั้นตอนการปฏิบัติงาน (Procedure)

นโยบาย ระเบียบการใช้ระบบสารสนเทศของ รพสต. ไม่มีประกาศที่เป็นลายลักษณ์อักษร แต่กำหนดนโยบายให้ผู้ดูแลระบบสารสนเทศดูแลระบบสารสนเทศทั้งหมดของ รพสต. กำหนดสิทธิในการเข้าถึงระบบสารสนเทศของโรงพยาบาลตามคำสั่งชี้แจงหน้าที่รับผิด

4.3.6 เครือข่าย (Network)

ระบบเครือข่ายภายในของ รพสต. ประกอบไปด้วยระบบเครือข่ายไร้สาย (Wi-Fi) และระบบเครือข่ายแลน (LAN) ซึ่งเป็นระบบเครือข่ายขนาดเล็ก รพสต. ใช้บริการอินเทอร์เน็ตของ บริษัท กสท. โทรคมนาคม จำกัด

4.4 ปัญหาของระบบสารสนเทศ

ปัญหาของระบบสารสนเทศของโรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อ มีดังนี้

4.4.1 คอมพิวเตอร์มีอายุการใช้งานมาก มักเกิดปัญหาหากมีการใช้งานหนัก

4.4.2 ขาดการติดตามการใช้ซอฟต์แวร์ที่ได้รับนโยบายมาให้ใช้ในการทำงานของ รพสต. ว่าหลังจากที่ใช้งานแล้วมีข้อดี ข้อเสียอย่างไร และบุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบลมีความพร้อมในการใช้ซอฟต์แวร์หรือไม่อย่างไร

4.5 ความต้องการระบบสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลเหล่าโพนค้อมีความต้องการคอมพิวเตอร์ใหม่ที่มีประสิทธิภาพเพียงพอต่อการทำงานของ รพสต. และการให้บริการแก่ผู้รับบริการได้อย่างรวดเร็ว ใช้งานได้อย่างสม่ำเสมอ

5. โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย

5.1 ที่มาประวัติหน่วยงาน

โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย ตั้งอยู่ที่ ตำบลม่วงไข่ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เดิมเป็นสถานีอนามัยม่วงไข่น้อย จนเมื่อปี พ.ศ.2552 ได้ยกระดับเป็นโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย

โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อยรับนโยบาย ตามลำดับ คือ สำนักงานสาธารณสุขจังหวัดสกลนคร สำนักงานสาธารณสุขอำเภอโคกศรีสุพรรณ และสำนักงานที่ว่าการอำเภอโคกศรีสุพรรณ

ภาพประกอบ 7 โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย

5.2 การจัดการงานด้านเทคโนโลยีสาสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย มีบุคลากรทำหน้าที่ดูแลระบบสารสนเทศของโรงพยาบาล 1 คน โดยเป็นบุคลากรของ รพสต.ม่วงไข่น้อย ทำงานในตำแหน่งนักวิชาการสาธารณสุขชำนาญการ

5.3 ระบบสารสนเทศ

5.3.1 ฮาร์ดแวร์ (Hardware)

คอมพิวเตอร์ของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย ประกอบไปด้วยเครื่องแม่ข่ายและเครื่องลูกข่าย ดังแสดงในตาราง 14

ตาราง 14 จำนวนคอมพิวเตอร์ของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย

ประเภทของคอมพิวเตอร์	ระบบปฏิบัติการ	จำนวน (เครื่อง)	ประเภทการใช้
เครื่องแม่ข่าย	CentOS	1	เครื่องแม่ข่ายระบบ HOSxP PCU
คอมพิวเตอร์ส่วนบุคคล แบบ all in one	Windows 8	4	เครื่องลูกข่าย
คอมพิวเตอร์แบบเดสทอป	Windows 7, Windows XP	4	เครื่องลูกข่าย
คอมพิวเตอร์โน้ตบุ๊ค	Windows 7, Windows 10	5	เครื่องลูกข่าย

5.3.2 ซอฟต์แวร์ (Software)

5.3.2.1 โปรแกรม HOSxP PCU

HOSxP PCU เป็นซอฟต์แวร์หลักของแต่ละโรงพยาบาลส่งเสริมสุขภาพตำบล ทำหน้าที่ในการบริหารจัดการ การให้บริการแก่ประชาชน ผู้มารับบริการของ รพสต. บันทึกข้อมูลการรักษาของผู้มารับบริการ จัดทำรายงานส่งสาธารณสุขจังหวัดและหน่วยงานที่เกี่ยวข้อง รวมถึงส่งข้อมูลของผู้รับบริการไปยังระบบ Data Center ของกลุ่มเครือข่ายบริการสุขภาพ

5.3.2.2 ซอฟต์แวร์สำหรับเตรียมข้อมูลส่งรายงาน

ซอฟต์แวร์สำหรับเตรียมข้อมูลส่งรายงาน เช่น R506, 506 Dashboard, cascap, ovsk เป็นต้น โดยซอฟต์แวร์เหล่านี้เจ้าหน้าที่ผู้รับผิดชอบต้องดำเนินการกรอกข้อมูลเข้าในแต่ละซอฟต์แวร์ หรือนำข้อมูลที่ทำการส่งออกจากระบบ HOSxP PCU นำเข้าในซอฟต์แวร์เหล่านั้น เพื่อเตรียมรูปแบบของข้อมูลตามรูปแบบของรายงานที่ต้องส่ง

5.3.3 ข้อมูล (Data)

ข้อมูลที่มีการจัดเก็บของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อยประกอบด้วย

5.3.3.1 ข้อมูลของผู้รับบริการ ซึ่งจัดเก็บในระบบ HOSxP PCU ซึ่งผู้ที่มีสิทธิเข้าถึงเท่านั้นที่สามารถมีบัญชีผู้ใช้ สำหรับการเข้าใช้ระบบ รวมถึงเข้าดูข้อมูลการให้บริการแก่ประชาชน

5.3.3.2 ข้อมูลของผู้รับบริการ ซึ่งจัดเก็บในแฟ้มเวชระเบียน โดยการจัดเรียงแฟ้มเวชระเบียนตามเลขที่บ้าน เพื่อความสะดวกในการค้นหา โดยแฟ้มเวชระเบียนจัดเก็บไว้ในตู้เก็บเอกสาร

ข้อมูลของบริการให้บริการแก่ประชาชน มีการสำรองข้อมูลสม่ำเสมอ โดยการตั้งค่าให้มีการสำรองข้อมูลอัตโนมัติในช่วงเวลา 8.30 และในตอนเย็นหลังเลิกงาน เวลา 18.00 จากนั้นจึงนำข้อมูลที่ได้รับการสำรองข้อมูลไว้แล้ว คัดลอก เก็บไว้ยังฮาร์ดดิสแบบพกพา (external hard disk) เพื่อเป็นการสำรองข้อมูลแยกออกจากระบบสารสนเทศของ รพสต. เพื่อป้องกันกรณีร้ายแรงที่ไม่สามารถเข้าใช้ระบบสารสนเทศของโรงพยาบาลผู้ดูแลระบบสารสนเทศจะใช้ข้อมูลที่สำรองไว้นี้ในการให้บริการประชาชนผู้มารับบริการ

ข้อมูลผู้รับบริการของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย มีความถูกต้อง น่าเชื่อถือสูง หน่วยงานท้องถิ่นที่ต้องการข้อมูลประชากรที่ถูกต้องจะมาทำเรื่องขอข้อมูลกับโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย

5.3.4 บุคลากร (People)

โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย มีเจ้าหน้าที่ทำหน้าที่ดูแลระบบสารสนเทศ 1 คน โดยแต่งตั้งให้ทำหน้าที่ดูแลระบบสารสนเทศเพิ่มเติม จากภาระงานเดิมด้านนักวิชาการสาธารณสุข

บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย ผู้มีหน้าที่รับผิดชอบด้านการให้บริการแก่ประชาชน จะได้รับบัญชีผู้ใช้ สำหรับเข้าใช้ระบบ HOSxP PCU โดยกำหนดการเข้าถึงข้อมูลการให้บริการแยกกันแต่ละหน้าที่รับผิดชอบ

5.3.5 ขั้นตอนการปฏิบัติงาน (Procedure)

โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย มีไกด์ไลน์ (guideline) เรื่องการส่งข้อมูล และการดูแลรักษาซ่อมบำรุงระบบคอมพิวเตอร์ ซึ่งเป็นข้อกำหนดที่ รพสต. ติดดาวต้องมี

นโยบายด้านเทคโนโลยีสารสนเทศ นโยบายใหม่ การส่งรายงานเพิ่มเติม โปรแกรมใหม่สำหรับการให้บริการประชาชนที่ต้องรับนโยบาย การติดตามการส่งรายงานข้อมูล ทางโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อยจะได้รับนโยบายโดยการเข้าประชุมผู้ดูแลระบบสารสนเทศของโรงพยาบาล และโรงพยาบาลส่งเสริมสุขภาพตำบล โดยจะมีการนัดประชุมเดือนละ 1 ครั้ง ที่สำนักงานสาธารณสุขจังหวัดสกลนคร และจะมีการนัดประชุมผู้ดูแลระบบสารสนเทศในส่วนของระดับอำเภออีกอย่างน้อยเดือนละ

1 ครั้ง เพื่อเป็นติดตามนโยบาย และติดตามการส่งรายงานข้อมูล รวมถึงปัญหาการดูแลระบบสารสนเทศของโรงพยาบาลในแต่ละหน่วยงาน

การกำหนดสิทธิการเข้าถึงข้อมูลของผู้รับบริการ ผู้ดูแลระบบสารสนเทศ จะกำหนดสิทธิโดยพิจารณาจากคำสั่งการแบ่งงานตามหน้าที่รับผิดชอบ ซึ่งลงนามโดยสาธารณสุขอำเภอ

5.3.6 เครือข่าย (Network)

ระบบเครือข่ายของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย แบ่งออกเป็น 2 ส่วน ได้แก่ 1) เครือข่ายที่ให้บริการแก่ประชาชนทั่วไป ซึ่งเป็นการให้บริการด้วยระบบเครือข่ายไร้สาย ซึ่งผู้ใช้เครือข่ายนี้จะไม่สามารถ เชื่อมต่อเข้าเครือข่ายภายในของโรงพยาบาลส่งเสริมสุขภาพตำบลได้ 2) เครือข่ายภายในของโรงพยาบาลส่งเสริมสุขภาพตำบล ซึ่งให้บริการเฉพาะเจ้าหน้าที่ บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบลเท่านั้น

โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อยใช้อินเทอร์เน็ตของผู้ให้บริการ 2 แห่ง คือ บริษัท กสท. โทรคมนาคม จำกัด ซึ่งเป็นอินเทอร์เน็ตที่กระทรวงสาธารณสุขมีนโยบายให้โรงพยาบาลส่งเสริมสุขภาพตำบลใช้ได้โดยไม่มีค่าใช้จ่าย และบริษัท ทีโอที จำกัด ทำงานร่วมกันในลักษณะโหลดบาลานซ์ (Load balance)

5.4 ปัญหาของระบบสารสนเทศ

ปัญหาของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย มีดังนี้

5.4.1 การส่งข้อมูลรายงาน ที่มีการกรอกข้อมูลเข้าระบบรายงานโดยมีการกรอกข้อมูลรายงานเดิมซ้ำกันในหลายระบบทำให้ภาระงานของบุคลากรของโรงพยาบาลมีมากขึ้นส่งผลกระทบต่อหน้าที่การปฏิบัติงานหลักคืองานด้านสาธารณสุข

5.4.2 ไฟฟ้าของโรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อยเกิดไฟตก และไฟดับบ่อย ส่งผลต่อความต่อเนื่องในการทำงานตามภารกิจของ รพสต.

5.5 ความต้องการระบบสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลม่วงไข่น้อย มีความต้องการดังนี้

5.5.1 ระบบโซลาเซลล์

รพสต. ม่วงไข่น้อยต้องการระบบโซลาเซลล์เพื่อแก้ปัญหาไฟฟ้าตกหรือดับในช่วงเวลาการให้บริการของ รพสต. เนื่องจาก รพสต. เปิดให้บริการประชาชนในเวลากลางวัน ซึ่งเวลาดังกล่าวมักมีปัญหาเรื่องไฟฟ้าตก และไฟฟ้าดับเป็นประจำ ทำให้

การให้บริการไม่ต่อเนื่อง การนำระบบโซลาเซลล์มาใช้สำหรับจ่ายไฟฟ้าให้ รพสต. ในช่วงกลางวันจะทำให้การให้บริการแก่ประชาชนทำได้อย่างต่อเนื่อง และลดค่าไฟฟ้าลงได้

5.5.2 นักวิชาการคอมพิวเตอร์

รพสต. ม่วงไข่น้อยต้องการนักวิชาการคอมพิวเตอร์ ในระดับอำเภอเพื่อดูแลรับผิดชอบในภาพรวมของระบบสารสนเทศ ของทั้ง 5 รพสต. โดยเป็นผู้จบการศึกษาด้านคอมพิวเตอร์ แบ่งเบาภาระงานของผู้ดูแลระบบสารสนเทศของแต่ละโรงพยาบาลส่งเสริมสุขภาพตำบลลง ทำให้ผู้ดูแลระบบสารสนเทศของแต่ละ รพสต. สามารถปฏิบัติหน้าที่หลักทางด้านสาธารณสุขได้มากขึ้น ส่งผลให้การให้บริการของ รพสต. มีความคล่องตัวมากยิ่งขึ้น

5.5.3 ค่าตอบแทน

ในกรณีที่บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบลทำงานในตำแหน่งผู้ดูแลระบบสารสนเทศเสริมจากตำแหน่งงานหลัก ควรได้รับค่าตอบแทนเพิ่มเติม เนื่องจากการปฏิบัติหน้าที่ในตำแหน่งผู้ดูแลระบบของโรงพยาบาลส่งเสริมสุขภาพตำบลมีภาระงานมาก รวมทั้งต้องปฏิบัติงานในหน้าที่หลักให้สมบูรณ์อีกด้วย

6. โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี

6.1 ที่มาประวัติหน่วยงาน

โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี เดิมเป็นอนามัยโคกนาดี เมื่อปี พ.ศ.2552 ได้ยกระดับเป็นโรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี

โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี รับนโยบายจาก สำนักงานสาธารณสุขอำเภอโคกศรีสุพรรณ ที่ว่าการอำเภอโคกศรีสุพรรณ และสำนักงานสาธารณสุขจังหวัดสกลนครตามลำดับการบังคับ บัญชา การบริหารงานภายใน รพสต. บุคลากรทุกคนจะทำงานภายใต้การบริหารงานของผู้อำนวยการโดยตรง ไม่มีหัวหน้างาน หรือหัวหน้าแผนก

ภาพประกอบ 8 โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี

6.2 การจัดการงานด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี ให้บริการแก่ประชาชนในเขตตำบลโคกนาดี อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร โดยมีระบบ HOSxP PCU เป็นระบบสารสนเทศหลักที่ใช้บริหารจัดการข้อมูลการให้บริการแก่ประชาชน รพสต. ไม่มีหน่วยงานที่ดูแลด้านระบบสารสนเทศ แต่มีการกำหนดมอบหมายให้ทำหน้าที่ผู้ดูแลระบบสารสนเทศของ รพสต. โดยมอบหมายให้บุคลากรเดิมรับผิดชอบเสริมจากหน้าที่หลักด้านสาธารณสุข ซึ่งผู้ดูแลระบบสารสนเทศของ รพสต. เป็นผู้ดูแลระบบสารสนเทศทั้งหมดของ รพสต. พร้อมทั้งทำหน้าที่ตรวจสอบความถูกต้องของข้อมูลที่บุคลากรใน รพสต. กรอกเข้าสู่ระบบ รวมถึงการเข้าประชุม รับนโยบายและประสานงานกับหน่วยงานอื่นๆ ที่เกี่ยวข้อง

6.3 ระบบสารสนเทศ

6.3.1 ฮาร์ดแวร์ (Hardware)

คอมพิวเตอร์และครุภัณฑ์คอมพิวเตอร์ของโรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดีได้มาโดยการตั้งงบของ รพสต. แล้วเสนอไปยังสำนักงานสาธารณสุขอำเภอ จากนั้นจึงดำเนินการจัดซื้อตามระเบียบของงานพัสดุ คอมพิวเตอร์ของโรงพยาบาลส่งเสริมสุขภาพตำบลดังแสดงในตาราง 15

ตาราง 15 จำนวนคอมพิวเตอร์ของโรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี

ประเภทของคอมพิวเตอร์	ระบบปฏิบัติการ	จำนวน (เครื่อง)	ประเภทการใช้
เครื่องแม่ข่าย	CentOS	1	เครื่องแม่ข่ายระบบ HOSxP PCU
คอมพิวเตอร์แบบเดสทอป	Windows 7, Windows XP	6	เครื่องลูกข่าย
คอมพิวเตอร์โน้ตบุ๊ค	Windows 7, Windows 8	3	เครื่องลูกข่าย

6.3.2 ซอฟต์แวร์ (Software)

โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี มีซอฟต์แวร์ที่ใช้ในการให้บริการของ รพสต. ดังนี้

6.3.2.1 ระบบ HOSxP PCU เป็นซอฟต์แวร์หลักที่ใช้ในการบริหารจัดการข้อมูลของผู้มารับบริการของโรงพยาบาลส่งเสริมสุขภาพตำบล รวมถึงการทำรายงานไปยังหน่วยงานที่เกี่ยวข้อง

6.3.2.2 ซอฟต์แวร์สำหรับการเตรียมข้อมูลส่งรายงาน ได้แก่ โปรแกรม R506, 506 Dashboard ระบบ Cockpit โปรแกรม R506 จะรับข้อมูลนำเข้าซึ่งได้มาจากการส่งออกข้อมูล (export) จากระบบ HOSxP PCU เพื่อเป็นเตรียมข้อมูลสำหรับส่งรายงาน และโปรแกรม 506 Dashboard เป็นระบบที่ทำงานในลักษณะเว็บแอปพลิเคชัน ซึ่งผู้ดูแลระบบสารสนเทศเป็นผู้ส่งข้อมูลเข้าระบบ รวมถึงระบบ Cockpit ก็เป็นเว็บแอปพลิเคชันที่พัฒนาโดยสำนักงานสาธารณสุขจังหวัดสกลนคร เป็นระบบสำหรับรับรายงานที่ส่งโดยโรงพยาบาลส่งเสริมสุขภาพตำบล

6.3.3 ข้อมูล (Data)

ข้อมูลที่เก็บรักษาที่โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี คือ ข้อมูลการรักษาคนไข้ ข้อมูลของผู้รับบริการ โดยแบ่งเป็น 2 ประเภท คือ

6.3.3.1 ข้อมูลที่เก็บบนระบบ HOSxP PCU เป็นข้อมูลการรักษาคนไข้ ข้อมูลของผู้รับบริการของโรงพยาบาลส่งเสริมสุขภาพตำบล โดยจำกัดการเข้าถึงได้เฉพาะผู้ที่เกี่ยวข้อง

6.3.3.2 ข้อมูลที่เก็บในรูปแบบเอกสาร เป็นข้อมูลการรักษาคนไข้ ข้อมูลของผู้รับบริการ ซึ่งเก็บเป็นแฟ้ม แยกตามทะเบียนบ้าน

ข้อมูลของผู้รับบริการของโรงพยาบาลโคกนาดีมีความถูกต้องสูง หน่วยงานท้องถิ่นที่ต้องการข้อมูลประชากรจะทำหนังสือขอข้อมูลมายังโรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดีเสมอ โดยในทุกวันผู้ดูแลระบบสารสนเทศจะเป็นผู้ตรวจสอบความถูกต้องครบถ้วนของข้อมูลที่กรอกเข้าสู่ระบบ HOSxP PCU พร้อมทั้งแจ้งผู้รับผิดชอบแก้ไขหากมีการกรอกข้อมูลผิด หรือไม่ครบถ้วน

ข้อมูลการรักษาของคนไข้ที่ต้องการปกปิดเป็นความลับ รพสต. โคกนาดีจะเก็บแฟ้มข้อมูลการรักษาแยกออกจากสถานที่เก็บหลัก โดยเก็บรักษาไว้ในตู้เก็บเอกสารที่มีการล็อกกุญแจ ให้สามารถเข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น พร้อมทั้งไม่บันทึกข้อมูลเข้าสู่ระบบ HOSxP PCU

6.3.4 บุคลากร (people)

โรงพยาบาลส่งเสริมสุขภาพตำบล มีผู้ดูแลระบบสารสนเทศ 1 คน โดยแต่งตั้งให้ทำหน้าที่เพิ่มเติมจากตำแหน่งเดิม บุคลากรผู้รับผิดชอบในการให้บริการคนไข้และผู้รับบริการ จะได้รับบัญชีผู้ใช้ สำหรับเข้าใช้งาน เพื่อบันทึกข้อมูลการรักษาและข้อมูลผู้รับบริการ

6.3.5 ขั้นตอนการปฏิบัติงาน (Procedure)

โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี รับนโยบายด้านเทคโนโลยีสารสนเทศโดยการเข้าประชุมผู้ดูแลระบบสารสนเทศในระดับอำเภอ และประชุมผู้ดูแลระบบสารสนเทศในระดับจังหวัด เมื่อได้รับนโยบายมาแล้วจึงถ่ายทอดไปยังเจ้าหน้าที่ผู้รับผิดชอบงานเหล่านั้น ซึ่งผู้ดูแลระบบสารสนเทศในระดับอำเภอจะมีการประชุมกันอย่างต่อเนื่องเพื่อติดตามผล รับข้อเสนอแนะ แก้ไขปัญหาร่วมกัน และให้คำแนะนำสำหรับ รพสต. ที่พบปัญหา โดยนโยบายที่รับมาจะประกอบด้วยเกณฑ์ตัวชี้วัดในการบันทึกข้อมูลรอบเวลาของการส่งออกข้อมูลรายงาน เช่น ส่งออกข้อมูลรายงานทุกวัน ส่งออกรายงานทุกเดือน

การกำหนดสิทธิการใช้งานของบุคลากรโรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี จะกำหนดตามหน้าที่รับผิดชอบ โดยชี้แจงโดยผู้อำนวยการโรงพยาบาลส่งเสริมสุขภาพตำบล ดำเนินการกำหนดสิทธิโดยผู้ดูแลระบบสารสนเทศของ รพสต.

6.3.6 เครือข่าย (Network)

โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดีใช้อินเทอร์เน็ตของผู้ให้บริการ 2 แห่ง คือ บริษัท กสท. โทรคมนาคม จำกัด ซึ่งเป็นอินเทอร์เน็ตที่กระทรวง

สาธารณสุขมีนโยบายให้โรงพยาบาลส่งเสริมสุขภาพตำบลใช้ได้โดยไม่มีค่าใช้จ่าย และบริษัท ทีโอที จำกัด ทำงานร่วมกันในลักษณะโหลดบาลานซ์ (Load balance)

6.4 ปัญหาของระบบสารสนเทศ

ระบบไฟฟ้าของโรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดีไม่เสถียร ระบบไฟฟ้าดับ และตกบ่อย ทำให้การให้บริการแก่ประชาชนได้ไม่ต่อเนื่อง

ข้อมูลที่กรอกเข้าระบบ HOSxP PCU ผู้ดูแลระบบสารสนเทศต้องตรวจสอบความถูกต้อง ความครบถ้วนเป็นประจำในทุกวัน ทำให้มีภาระงานที่มาก

6.5 ความต้องการระบบสารสนเทศ

โรงพยาบาลส่งเสริมสุขภาพตำบลโคกนาดี ต้องการตำแหน่งผู้ดูแลระบบสารสนเทศที่เรียนจบ มีวุฒิการศึกษาทางด้านคอมพิวเตอร์ เพื่อประสิทธิภาพในการทำงานและเจ้าหน้าที่สามารถให้บริการประชาชนทางด้านสาธารณสุขได้อย่างเต็มที่

จากการสัมภาษณ์ผู้ดูแลระบบสารสนเทศของโรงพยาบาลโคกศรีสุพรรณ และผู้ดูแลระบบสารสนเทศของโรงพยาบาลส่งเสริมสุขภาพตำบล 5 แห่ง พบว่า โรงพยาบาลโคกศรีสุพรรณใช้ระบบ HOSxP จัดการข้อมูลผู้รับบริการ และโรงพยาบาลส่งเสริมสุขภาพตำบลทั้ง 5 แห่ง ใช้ระบบ HOSxP PCU จัดการข้อมูลผู้รับบริการในพื้นที่ ส่วนข้อมูลการให้บริการของแต่ละโรงพยาบาลเชื่อมต่อกันด้วยระบบ Data center โดยการเชื่อมข้อมูลการให้บริการเข้าด้วยกันนี้ทำให้ข้อมูลการให้บริการของกลุ่มเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณ มีความสอดคล้องกันทุกโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณ สามารถเข้าถึงข้อมูลประวัติการรับบริการของผู้รับบริการได้เหมือนกันทุกโรงพยาบาล

กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครมีนโยบายกำหนดสิทธิการใช้ระบบ HOSxP และการเข้าถึงข้อมูลสำหรับบุคลากรผู้ที่เกี่ยวข้องเท่านั้น

กลุ่มเครือข่ายบริการสุขภาพอำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีการส่งข้อมูลผ่านระบบเครือข่ายของผู้ให้บริการ (ISP) เก็บไว้ยังเครื่องแม่ข่ายของโรงพยาบาลโคกศรีสุพรรณ โดยภายในแต่ละโรงพยาบาลเชื่อมโยงเครื่องแม่ข่าย และเครื่องลูกข่ายผ่านระบบเครือข่ายแบบมีสาย และเครือข่ายแบบไร้สาย

โรงพยาบาลโคกศรีสุพรรณมีโครงสร้างการบริหารที่มีหน่วยงานที่รองรับการดูแลระบบสารสนเทศ คือ งานสารสนเทศ และงานประกันสุขภาพ ซึ่งมีบุคลากรนักวิชาการคอมพิวเตอร์ 3 คน แต่โรงพยาบาลส่งเสริมสุขภาพตำบลทั้ง 5 แห่ง ไม่มีหน่วยงานดูแลระบบสารสนเทศ ผู้อำนวยการ ฯ จึงมอบหมายให้บุคลากรของโรงพยาบาลส่งเสริมสุขภาพตำบลเป็นผู้ดูแลระบบสารสนเทศแห่งละ 1 คน

การจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กับกรอบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

1. ข้อมูลผู้ตอบแบบสอบถาม

ผู้วิจัยแจกแบบสอบถามให้กับบุคลากรของโรงพยาบาล และบุคลากรของโรงพยาบาลส่งเสริมสุขภาพดำบล จำนวน 93 คน ได้รับแบบสอบถามกลับคืนทั้งหมด ผลการวิเคราะห์ข้อมูลเกี่ยวกับผู้ตอบแบบสอบถาม มีดังนี้

1.1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ผลวิเคราะห์ข้อมูลเกี่ยวกับข้อมูลทั่วไปของผู้ตอบแบบสอบถาม แสดงในตาราง 16 ดังนี้

ตาราง 16 ข้อมูลทั่วไปผู้ตอบแบบสอบถาม

ข้อมูล	ความถี่	ร้อยละ
เพศ		
ชาย	17	18.28
หญิง	76	81.72
รวม	93	100

ตาราง 16 (ต่อ)

ข้อมูล	ความถี่	ร้อยละ
อายุ		
20 – 30 ปี	33	35.48
31 – 40 ปี	23	24.73
41 – 50 ปี	24	25.81
มากกว่า 50 ปี	13	13.98
รวม	93	100
ระดับการศึกษา		
ต่ำกว่าระดับปริญญาตรี	11	11.83
ปริญญาตรี	75	80.65
ปริญญาโท	6	6.45
ปริญญาเอก	1	1.08
รวม	93	100
สถานที่ทำงาน		
โรงพยาบาล	65	69.89
โรงพยาบาลส่งเสริมสุขภาพตำบล	28	30.11
รวม	93	100
ประสบการณ์ทำงาน		
ต่ำกว่า 1 ปี	1	1.08
1–5 ปี	24	25.81
6–10 ปี	21	22.58
11–15 ปี	9	9.68
15–20 ปี	9	9.68

ตาราง 16 (ต่อ)

ข้อมูล	ความถี่	ร้อยละ
21 ปีขึ้นไป	29	31.18
รวม	93	100

จากตาราง 16 ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง (ร้อยละ 81.72) ส่วนใหญ่อายุ 20 – 30 ปี (ร้อยละ 35.48) รองลงมาอายุ 41 – 50 ปี (ร้อยละ 25.81) ส่วนใหญ่จบการศึกษาระดับปริญญาตรี (ร้อยละ 80.65) รองลงมาคือจบการศึกษาต่ำกว่าปริญญาตรี (ร้อยละ 11.83) บุคลากรส่วนใหญ่ปฏิบัติงานในโรงพยาบาลโคกศรีสุพรรณ (ร้อยละ 69.89) และส่วนใหญ่มีประสบการณ์ทำงานมากกว่า 21 ปีขึ้นไป (ร้อยละ 31.18) รองลงมาคือประสบการณ์ทำงาน 1 – 5 ปี (ร้อยละ 25.81)

ผลวิเคราะห์ข้อมูลเกี่ยวกับตำแหน่งงานของผู้ตอบแบบสอบถาม แสดงในตาราง 17 ดังนี้

ตาราง 17 ตำแหน่งงานของผู้ตอบแบบสอบถาม

ตำแหน่งงาน	จำนวน	ร้อยละ
แพทย์	2	2.15
ทันตแพทย์	2	2.15
เภสัชกร	4	4.30
พยาบาลวิชาชีพ	36	38.71
นักวิชาการสาธารณสุข	12	12.90
นักจัดการงานทั่วไป	1	1.08
เจ้าพนักงานสาธารณสุข	5	5.38
เจ้าพนักงานทันตสาธารณสุข	3	3.23

ตาราง 17 (ต่อ)

ตำแหน่งงาน	จำนวน	ร้อยละ
เจ้าพนักงานเภสัชกรรม	2	2.15
เจ้าพนักงานธุรการ	2	2.15
เจ้าพนักงานการเงินและบัญชี	2	2.15
เจ้าพนักงานเวชระเบียน	1	1.08
นักกายภาพบำบัด	3	3.23
นักเทคนิคการแพทย์	3	3.23
แพทย์แผนไทย	6	6.45
ผู้ช่วยเหลือคนไข้	6	6.45
นักวิชาการคอมพิวเตอร์	3	3.23
รวม	93	100

จากตาราง 17 บุคลากรที่ตอบแบบสอบถามส่วนใหญ่ดำรงตำแหน่งงาน คือ พยาบาล (ร้อยละ 38.71) รองลงมา คือ นักวิชาการสาธารณสุข (ร้อยละ 12.90) แพทย์แผนไทยและผู้ช่วยเหลือคนไข้ (ร้อยละ 6.45)

ผลวิเคราะห์ข้อมูลเกี่ยวกับกลุ่มงานของผู้ตอบแบบสอบถาม แสดงในตาราง 18 ดังนี้

ตาราง 18 กลุ่มงานของกลุ่มตัวอย่าง

ตำแหน่งงาน	จำนวน	ร้อยละ
งานบริหารทั่วไป	8	8.60
งานเวชกรรมทั่วไป	1	1.08
งานทันตกรรม	5	5.38
งานผู้ป่วยนอก	8	8.60
งานผู้ป่วยใน	10	10.75

ตาราง 18 (ต่อ)

ตำแหน่งงาน	จำนวน	ร้อยละ
งานผู้ป่วยฉุกเฉิน และอุบัติเหตุ	8	8.60
งานห้องคลอด	3	3.23
งานควบคุมและป้องกัน การติดเชื้อในโรงพยาบาล	1	1.08
งานเภสัชกรรม	6	6.45
งานชันสูตร	4	4.30
งานกายภาพบำบัด	3	3.23
งานสถิติ	1	1.08
งานสร้างเสริมสุขภาพ	7	7.53
งานชุมชน	3	3.23
งานระบาดวิทยา	2	2.15
งานแพทย์แผนไทย	9	9.68
งานเวชระเบียน	4	4.30
กลุ่มการพยาบาล	3	3.23
หน่วยงานปฐมภูมิและองค์รวม	4	4.30
งานสารสนเทศ และประกันสุขภาพ	3	3.23
รวม	93	100

จากตาราง 18 บุคลากรส่วนใหญ่สังกัดหน่วยงานคือ งานผู้ป่วยใน (ร้อยละ 10.75) รองลงมาคือ งานแพทย์แผนไทย (ร้อยละ 9.68) และงานผู้ป่วยนอก (ร้อยละ 8.60)

2. การจัดการความมั่นคงปลอดภัยสารสนเทศ

จากการสัมภาษณ์ผู้ดูแลระบบสารสนเทศของโรงพยาบาลโคกศรีสุพรรณ (ผิน ฮ่มป่า, สัมภาษณ์, 22 มิถุนายน 2558) พบว่ากลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ไม่มีนโยบายความมั่นคงปลอดภัยระบบสารสนเทศที่เป็นลายลักษณ์อักษร แต่ได้ดำเนินการด้านความมั่นคงปลอดภัยระบบสารสนเทศ โดยการใช้งานระบบ HOSxP บุคลากรของโรงพยาบาลเข้าใช้งานระบบ HOSxP ด้วยบัญชีผู้ใช้

(account) ของตนเองเท่านั้น การเข้าถึงข้อมูลของผู้ป่วย จำกัดสิทธิ์ให้เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น โดยการกำหนดสิทธิ์การเข้าถึงข้อมูล ต้องกระทำโดยผู้ดูแลระบบสารสนเทศที่ได้รับการแต่งตั้งจากโรงพยาบาลเท่านั้น ห้ามเปิดเผยข้อมูลการรักษาผู้ป่วยแก่สาธารณะ การใช้งานอินเตอร์เน็ตเจ้าหน้าที่ของโรงพยาบาลเข้าใช้งานอินเตอร์เน็ตด้วย Account ของตนเองเท่านั้น การใช้งานคอมพิวเตอร์ การติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์ ต้องได้รับการติดตั้งโดยผู้ดูแลระบบสารสนเทศของโรงพยาบาล

แนวทางการปกปิดข้อมูลการรักษา (ณปภัช แก้วกิ่ง, สัมภาษณ์, 13 ตุลาคม 2560) ของผู้รับบริการที่ต้องรักษาความลับเป็นกรณีพิเศษ โดยเมื่อผู้ป่วยเข้ามารับบริการที่โรงพยาบาลต้องผ่านจุดคัดกรองซึ่งจะส่งตัวผู้ป่วยเข้ารับบริการโดยตรงที่ห้องให้คำปรึกษา เจ้าหน้าที่ผู้รับผิดชอบในห้องให้คำปรึกษาจะเป็นผู้ประสานงานผู้มีส่วนเกี่ยวข้องในการรักษาให้ผู้ป่วยรับบริการในจุดเดียว ซึ่งประวัติ ข้อมูลการรักษาผู้ป่วย ข้อมูลผู้รับบริการของโรงพยาบาลมีอยู่ 2 ลักษณะ คือ 1)ข้อมูลในรูปแบบเอกสาร โดยรวบรวมอยู่ในแฟ้มเวชระเบียน แยกเป็นรายบุคคล และ2)ข้อมูลในระบบฐานข้อมูลในระบบ HOSxP

ข้อมูลการรักษาผู้ป่วย ข้อมูลผู้รับบริการ ในรูปแบบเวชระเบียน มีแนวทางในการปกปิดข้อมูลการรักษาผู้ป่วยที่ถูกทารุณกรรม ล่วงละเมิดทางเพศ ยาเสพติด ผู้ติดเชื้อเอชไอวี โดยเก็บแฟ้มเวชระเบียนแยกเป็นสองชุด คือ 1) แฟ้มเวชระเบียนฉบับจริง ซึ่งมีข้อมูลการรักษาผู้ป่วยครบถ้วนสมบูรณ์ แยกเก็บรักษาไว้จากสถานที่เก็บแฟ้มเวชระเบียนหลักของโรงพยาบาล 2) แฟ้มเวชระเบียนฉบับสำรอง ซึ่งมีข้อมูลทั่วไปของผู้ป่วย เช่น ชื่อ สกุล ที่อยู่ วัน เดือน ปี เกิด เป็นต้น โดยไม่มีข้อมูลที่เกี่ยวข้องกับการทารุณกรรม ล่วงละเมิดทางเพศ ยาเสพติด ข้อมูลผลตรวจเลือดของผู้ติดเชื้อเอชไอวี และข้อมูลที่เกี่ยวข้องกับการติดเชื้อเอชไอวี ในกรณีแฟ้มเวชระเบียนสำรองของผู้ติดเชื้อเอชไอวีจะมีการติดสติกเกอร์เพื่อเป็นสัญลักษณ์สื่อสารกับเจ้าหน้าที่ผู้รับผิดชอบ

ข้อมูลการรักษาผู้ป่วยซึ่งบันทึกในระบบ HOSxP มีแนวทางการปกปิดข้อมูลการรักษาผู้ป่วย และปกปิดประวัติการเข้ารับบริการ ดังนี้ ผู้ป่วยยาเสพติด ข้อมูลการรักษาผู้ป่วยยาเสพติดตั้งค่าการปกปิดให้ผู้ที่เกี่ยวข้องเท่านั้นที่สามารถเข้าดูข้อมูลการรักษาที่ตั้งปกปิดได้ และในระบบ HOSxP จะไม่สามารถค้นหาข้อมูลการรักษาผู้ป่วยที่ได้รับการตั้งค่าการปกปิดได้ ส่วนผู้ป่วยกรณีถูกทารุณกรรม ล่วงละเมิดทางเพศ การตั้งครรภ์โดยไม่พร้อมในระบบ HOSxP จะมีการลงช้อมูลเพียงว่า “ให้คำปรึกษา” และผู้ติดเชื้อเอชไอวี ในระบบ HOSxP จะลงแค่ข้อมูลการมารับยา และไม่ลงผลการตรวจจากห้องแลป

ข้อมูลประวัติการรักษาผู้ป่วยที่ต้องมีการปกปิด มีระบบสารสนเทศสำหรับบริหารจัดการแยกในแต่ละงาน ได้แก่ ระบบการบำบัด รักษา และฟื้นฟูสมรรถภาพ ผู้เสพผู้ติดยาเสพติด สำหรับบริหารจัดการข้อมูลการรักษาผู้ป่วยยาเสพติด โดยสามารถเข้าใช้ระบบได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น การเข้าใช้ระบบต้องใช้ pin code ในบัตรประชาชนสมาร์ทการ์ด ซึ่งผู้ที่ต้องเข้าใช้ระบบ ต้องทำเรื่องขอเข้าใช้ระบบได้ที่เทศบาล หรือที่ว่าการอำเภอ ระบบ OSCC ศูนย์ช่วยเหลือสังคม เป็นระบบสารสนเทศสำหรับบริหารจัดการผู้ป่วยกรณีถูกทารุณกรรม ล่วงละเมิดทางเพศ การตั้งครรภ์โดยไม่พร้อม และระบบสารสนเทศการให้บริการผู้ติดเชื้อเอชไอวี ผู้ป่วยเอดส์ แห่งชาติ (Nap plus) สำหรับบริหารจัดการผู้ติดเชื้อเอชไอวี และผู้ป่วยเอดส์ โดยระบบทั้งหมดนี้ผู้ที่มีหน้าที่รับผิดชอบเท่านั้นจึงจะมีบัญชีผู้ใช้ และในการเข้าใช้ระบบจะมีการบันทึกการเข้าใช้งานระบบทั้งหมด

การบันทึกข้อมูลการรักษาผู้ป่วย ข้อมูลผู้รับบริการกรณีถูกทารุณกรรม ล่วงละเมิดทางเพศ การตั้งครรภ์โดยไม่พร้อม ยาเสพติด ผู้ติดเชื้อเอชไอวี มีระบบสารสนเทศรองรับสำหรับให้บริการซึ่งพัฒนาเฉพาะกับผู้ป่วยแต่ละแบบ แต่ผู้ป่วยยาเสพติด ระบบสารสนเทศเฉพาะยังรองรับไม่ครบถ้วน เจ้าหน้าที่ผู้รับผิดชอบจึงต้องบันทึกข้อมูลการรักษา ข้อมูลการรับบริการในระบบ การบำบัด รักษา และฟื้นฟูสมรรถภาพ ผู้เสพ ผู้ติดยาเสพติด และข้อมูลที่ไม่สามารถบันทึกในระบบหลักได้ จะถูกบันทึกในระบบ HOSxP ของโรงพยาบาล พร้อมกับตั้งค่าเป็นปกปิด เพื่อปกปิดข้อมูลการรักษาผู้ป่วย และข้อมูลการรับบริการให้สามารถเข้าถึงได้เฉพาะผู้มีส่วนเกี่ยวข้องเท่านั้น รวมถึงระบบรายงานของระบบ HOSxP ก็จะไม่สามารถเข้าถึงข้อมูลในส่วนนี้ได้เช่นกัน

ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

จากการเก็บข้อมูลด้วยแบบสอบถามกับกลุ่มตัวอย่างของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร โดยให้กลุ่มตัวอย่างเรียงลำดับความสำคัญของปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ ตั้งแต่ลำดับที่ 1 ถึงลำดับที่ 10 โดยลำดับที่ 1 หมายถึงปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยมากที่สุด และลำดับที่ 10 หมายถึงปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยน้อยที่สุด

ซึ่งกลุ่มตัวอย่างมีความคิดเห็นต่อปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังแสดงในตาราง 19 ดังนี้

ตาราง 19 ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ

ลำดับปัจจัย	แผนงานและระบบระเบียบในการจัดการสารสนเทศขององค์กร	โครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	ฮาร์ดแวร์	ซอฟต์แวร์	บุคลากร	ผู้บริหาร	ผู้รับบริการ	ข้อมูล	กฎหมาย	ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ
1	14 (15.05)	24 (25.81)	6 (6.45)	2 (2.15)	7 (7.53)	17 (18.28)	4 (4.30)	4 (4.30)	9 (9.68)	5 (5.38)
2	19 (20.43)	21 (22.58)	5 (5.38)	7 (7.53)	13 (13.98)	8 (8.60)	2 (2.15)	5 (5.38)	2 (2.15)	4 (4.30)
3	17 (18.28)	12 (12.90)	6 (6.45)	5 (5.38)	6 (6.45)	17 (18.28)	6 (6.45)	6 (6.45)	4 (4.30)	4 (4.30)
4	11 (11.83)	7 (7.53)	9 (9.68)	12 (12.90)	14 (15.05)	4 (4.30)	4 (4.30)	9 (9.68)	10 (10.75)	2 (2.15)
5	2 (2.15)	4 (4.30)	20 (21.51)	12 (12.90)	5 (5.38)	9 (9.68)	-	11 (11.83)	7 (7.53)	12 (12.90)
6	6 (6.45)	2 (2.15)	9 (9.68)	21 (22.58)	9 (9.68)	5 (5.38)	7 (7.53)	12 (12.90)	7 (7.53)	5 (5.38)
7	6 (6.45)	3 (3.23)	16 (17.20)	8 (8.60)	9 (9.68)	4 (4.30)	11 (11.83)	15 (16.13)	7 (7.53)	4 (4.30)
8	4 (4.30)	6 (6.45)	3 (3.23)	9 (9.68)	6 (6.45)	9 (9.68)	13 (13.98)	11 (11.83)	17 (18.28)	5 (5.38)
9	4 (4.30)	4 (4.30)	6 (6.45)	4 (4.30)	12 (12.90)	2 (2.15)	7 (7.53)	8 (8.60)	18 (19.35)	19 (20.43)
10	2 (2.15)	2 (2.15)	5 (5.38)	5 (5.38)	4 (4.30)	10 (10.75)	31 (33.33)	4 (4.30)	4 (4.30)	25 (26.88)
รวม	85	85	85	85	85	85	85	85	85	85

จากตาราง 19 ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ แสดงให้เห็นว่า กลุ่มตัวอย่างส่วนใหญ่มีความคิดเห็นต่อลำดับความสำคัญของปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ลำดับที่ 1 คือ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร จำนวน 24 คน คิดเป็นร้อยละ 25.81 รองลงมาคือ ผู้บริหาร จำนวน 17 คน คิดเป็นร้อยละ 18.28 และแผนงานและงบประมาณด้านระบบสารสนเทศขององค์กร จำนวน 14 คน คิดเป็นร้อยละ 15.05

ลำดับที่ 2 คือ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร จำนวน 21 คน คิดเป็นร้อยละ 22.58 แผนงานและงบประมาณด้านระบบสารสนเทศขององค์กร จำนวน 19 คน คิดเป็นร้อยละ 20.43 รองลงมาคือ และบุคลากร จำนวน 13 คน คิดเป็นร้อยละ 14.0

ลำดับที่ 3 คือ ผู้บริหาร แผนงานและงบประมาณด้านระบบสารสนเทศขององค์กร จำนวน 17 คน คิดเป็นร้อยละ 18.28 รองลงมาคือ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร จำนวน 12 คน คิดเป็นร้อยละ 12.90 และฮาร์ดแวร์ บุคลากร ผู้รับบริการ ข้อมูล จำนวน 6 คน คิดเป็นร้อยละ 6.45

ลำดับที่ 4 คือ บุคลากร จำนวน 14 คน คิดเป็นร้อยละ 15.05 รองลงมา คือ ซอฟต์แวร์ จำนวน 12 คน คิดเป็นร้อยละ 12.90 และแผนงานและงบประมาณด้านระบบสารสนเทศของ จำนวน 11 คน คิดเป็นร้อยละ 11.83

ลำดับที่ 5 คือ ฮาร์ดแวร์ จำนวน 20 คน คิดเป็นร้อยละ 21.51 รองลงมาคือ ซอฟต์แวร์ ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศเท่ากัน จำนวน 12 คน คิดเป็นร้อยละ 12.90 และข้อมูล จำนวน 11 คน คิดเป็นร้อยละ 11.83

การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

จากการประเมินความคิดเห็นของกลุ่มตัวอย่าง เกี่ยวกับกรอบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล กับการจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ซึ่งใช้กับบุคลากรผู้ใช้ระบบสารสนเทศ เช่น แพทย์ พยาบาล เภสัชกร นักกายภาพบำบัด

แพทย์แผนไทย เป็นต้น และผู้ดูแลระบบสารสนเทศ ผลการประเมินการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร แสดงดังตาราง 20

ตาราง 20 ผลการประเมินการจัดการความมั่นคงปลอดภัยสารสนเทศ

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Security policy)						
1.1) มีเอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร			42/45 64		✓	✓
1.2) มีการประกาศใช้นโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ			48 65		✓	✓
1.3) มีการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ	5 5				-	✓
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)						
2.1) ผู้บริหารกำหนดให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศ	66 62				✓	✓
2.2) มีการกำหนดให้มีตัวแทนจากหน่วยงาน ภายในองค์กรเพื่อประสานงานในการสร้างความมั่นคงปลอดภัยสารสนเทศ	54 61				✓	✓
2.3) มีการกำหนดหน้าที่รับผิดชอบของบุคลากรในการดำเนินการทางด้านความมั่นคงปลอดภัยสารสนเทศไว้ชัดเจน	74 61				-	✓
2.4) มีการกำหนดกระบวนการในการอนุมัติใช้งานอุปกรณ์ทางระบบสารสนเทศ เช่น คอมพิวเตอร์ เป็นต้น	51 56				✓	✓
2.5) มีการกำหนดให้บุคลากรลงนามไม่ให้เปิดเผยความลับขององค์กร	54 59				✓	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
2.6) องค์กรมีรายชื่อและข้อมูลบุคลากร/หน่วยงาน สำหรับติดต่อประสานงานทางด้านความมั่นคงปลอดภัยสารสนเทศในกรณีที่มีความจำเป็น เช่น ผู้ให้บริการอินเตอร์เน็ต ศูนย์ประสานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น	6 5				–	✓
2.7) มีการกำหนดให้มีการตรวจสอบการจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบอิสระตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร			4 5		–	✓
2.8) มีการประเมินความเสี่ยงของการเข้าถึงสารสนเทศ หรืออุปกรณ์ในระบบสารสนเทศ		5 4			–	✓
2.9) มีการกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนการอนุญาตให้เข้าถึงสารสนเทศได้			4 5		–	✓
2.10) มีการกำหนดข้อกำหนดทางด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นให้ผู้ใช้บริการเข้าถึงสารสนเทศขององค์กร		5 4			–	✓
2.11) มีการกำหนดข้อกำหนดหรือข้อตกลงกับองค์กรผู้พัฒนาซอฟต์แวร์ในกรณีที่มีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กรก่อนที่จะอนุญาตให้สามารถเข้าถึงได้	5 5				–	✓
3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)						
3.1) มีการจัดทำบัญชีทรัพย์สิน (เช่น บัญชีครุภัณฑ์ เป็นต้น) ขององค์กร	74 61				✓	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
3.2) มีการแก้ไขปรับปรุงบัญชีทรัพย์สินให้มีความถูกต้องอยู่เสมอ	64 60				✓	✓
3.3) มีการจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ	69 63				✓	✓
3.4) มีการจัดทำกฎระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม	59 61				✓	✓
3.5) มีการจัดหมวดหมู่ทรัพย์สินสารสนเทศตามระดับชั้นของความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร	61 60				✓	✓
3.6) มีการจัดทำป้ายชื่อทรัพย์สินทางด้านเทคโนโลยีสารสนเทศขององค์กร	68 59				✓	✓
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)						
4.1) มีการกำหนดหน้าที่และรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับหน่วยงานหรือผู้ที่องค์กรจ้างงาน		6 4			-	✓
4.2) ข้อกำหนดหน้าที่และรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศสำหรับหน่วยงานหรือผู้ที่องค์กรจ้างงานมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร			4 5		-	✓
4.3) มีการกำหนดระดับการเข้าถึงสารสนเทศสำหรับบุคลากรขององค์กร	8 5				-	✓
4.4) มีการกำหนดเงื่อนไขการว่าจ้างงาน		7 4			-	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
4.5) มีการกำหนดให้บุคลากรที่จะได้รับการว่าจ้างงาน ลงนามเงื่อนไขในการจ้างงาน	8 5				–	✓
4.6) มีการกำหนดให้บุคลากรขององค์กรหรือจากหน่วยงานภายนอกปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร	5 5				✓	✓
4.7) มีการอบรมให้ความรู้และสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรผู้ปฏิบัติหน้าที่ภายในองค์กร และผู้ที่มาจากหน่วยงานภายนอก	50 61				✓	✓
4.8) มีกระบวนการลงโทษทางวินัยแก่บุคลากรที่ฝ่าฝืน ละเมิดนโยบายหรือระเบียบข้อบังคับด้านความมั่นคงปลอดภัยสารสนเทศ			51 61		✓	✓
4.9) มีการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะงาน			51 61		✓	✓
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)						
5.1) มีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า–ออกที่มีการควบคุม ตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า–ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร	49 56				✓	✓
5.2) ควบคุมพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยอนุญาตให้เข้า–ออกได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น	57 52				✓	✓
5.3) จัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ	53 63				✓	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบ ระดับสูง
5.4) จัดให้มีการป้องกันทางกายภาพในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัย	60 62				✓	✓
5.5) จัดทำแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย	56 63				✓	✓
5.6) จัดให้มีบริเวณสำหรับการเข้าถึงโดยบุคคลภายนอก	50 60				✓	✓
5.7) มีการป้องกันอุปกรณ์ของสำนักงานจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ	52 60				✓	✓
5.8) จัดวางอุปกรณ์ของสำนักงานในบริเวณที่ไม่เสี่ยงต่อภัยคุกคามต่างๆ	59 61				✓	✓
5.9) มีกลไกการป้องกันการล้มเหลวของระบบไฟฟ้า	69 61				✓	✓
5.10)มีกลไกการป้องกันการล้มเหลวของระบบเครือข่ายคอมพิวเตอร์	61 64				✓	✓
5.11) มีการป้องกันการเข้าถึงสายไฟฟ้า สายสื่อสาร โดยไม่ได้รับอนุญาต	55 62				✓	✓
5.12) มีการกำหนดให้บำรุงรักษาอุปกรณ์ต่างๆ อยู่เสมอ	77 57				✓	✓
5.13) กำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงาน	52 60				✓	✓
5.14) กำหนดให้มีการทำลายข้อมูลและซอฟต์แวร์ก่อนทิ้งสื่อบันทึกข้อมูล	5 5				-	✓
5.15) กำหนดให้มีการขออนุญาตก่อนนำสารสนเทศ หรืออุปกรณ์ระบบสารสนเทศ ออกนอกองค์กร	62 61				✓	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)						
6.1) จัดทำคู่มือขั้นตอนการปฏิบัติงานด้านเครือข่ายสารสนเทศขององค์กรแจกจ่ายให้กับผู้ที่เกี่ยวข้อง			58 64		✓	✓
6.2) ปรับปรุงคู่มือขั้นตอนการปฏิบัติงานด้านเครือข่ายสารสนเทศขององค์กรตามระยะเวลาอันสมควร			60 63		✓	✓
6.3) มีการกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ	6 5				-	✓
6.4) กำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบในงานด้านระบบสารสนเทศขององค์กร	6 5				-	✓
6.5) มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการระบบสารสนเทศแก่องค์กรออกจากกัน				5 4	-	✓
6.6)กำหนดให้ผู้ให้บริการภายนอกปฏิบัติตามข้อกำหนด หรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กร และผู้ให้บริการ			51 60		✓	✓
6.7) มีการตรวจสอบการให้บริการระบบสารสนเทศอย่างสม่ำเสมอ	6 5				-	✓
6.8) มีการกำหนดให้มีการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก				5 4	-	✓
6.9) มีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต	7 5				-	✓
6.10) มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม	5 5				-	✓
6.11) มีการติดตั้งโปรแกรมแอนตี้ไวรัส/มัลแวร์ไว้ในเครื่องคอมพิวเตอร์	70 58				✓	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
6.12) มีมาตรการในการกู้กลับคืนเมื่อระบบสารสนเทศถูกทำลายโดยไวรัสคอมพิวเตอร์/มัลแวร์			4 5		-	✓
6.13) มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ	8 5				-	✓
6.14) มีการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ	6 5				-	✓
6.15) มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่อสารสนเทศที่ส่งผ่านทางเครือข่ายขององค์กร	47 61				✓	✓
6.16) กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการเครือข่ายขององค์กร				5 4	-	✓
6.17) มีข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่			4 5		-	✓
6.18) มีการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้				4 4	-	✓
6.19) มีขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้			48 58		✓	✓
6.20) มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว			54 64		-	✓
6.21) ขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งาน เป็นไปอย่างมั่นคงปลอดภัย			5 5		-	✓
6.22) มีการกำหนดขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศ		6 4			-	✓
6.23) ขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศได้ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต		6 4			-	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
6.24) ขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศได้ป้องกันการใช้งานผิดวัตถุประสงค์				4 4	-	✓
6.25) มีมาตรการป้องกันเอกสารของระบบสารสนเทศจากการเข้าถึงโดยไม่ได้รับอนุญาต		5 4			-	✓
6.26) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กรโดยผ่านทางช่องทางการสื่อสารทุกชนิด			52 57		✓	✓
6.27) จัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร			60 60		✓	✓
6.28) มีการป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตระหว่างการส่งข้อมูลนั้นไปนอกองค์กร			53 60		✓	✓
6.29) มีมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์			48 60		✓	✓
6.30) มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่สู่สาธารณะ			54 63		✓	✓
6.31) มีการบันทึกกิจกรรมและเหตุการณ์ต่างๆ (Log) ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ		7 4			-	✓
6.32) มีการกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ			49 61		✓	✓
6.33) มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ (Log)		6 4			-	✓
6.34) มีการกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบสารสนเทศหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร		6 4			-	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
6.35) มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ				5 4	-	✓
6.36) มีการวิเคราะห์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศและดำเนินการแก้ไขตามสมควร				4 4	-	✓
6.37) มีการตั้งเวลาของอุปกรณ์ในระบบสารสนเทศให้ตรงกัน	6 5				-	✓
6.38) มีการตั้งเวลาของอุปกรณ์ในระบบสารสนเทศอ้างอิงจากแหล่งเวลาที่ถูกต้อง	6 5				-	✓
7. การควบคุมการเข้าถึง (Access control)						
7.1) กำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร			50 60		✓	✓
7.2) ปรับปรุงนโยบายควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศตามระยะเวลาที่กำหนด			56 61		✓	✓
7.3) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น	57 58				✓	✓
7.4) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการยกเลิกสิทธิต่างๆ ในการใช้งานเมื่อพนักงานลาออกหรือเปลี่ยนตำแหน่งงานภายในองค์กร			54 62		✓	✓
7.5) จำกัดสิทธิการใช้งานระบบสารสนเทศตามความจำเป็นในการใช้งานของบุคลากรขององค์กร	56 53				✓	✓
7.6) มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานระบบสารสนเทศอย่างเป็นทางการ	68 57				✓	✓
7.7) กำหนดวิธีปฏิบัติที่ดีในการตั้งรหัสผ่าน	61 53				✓	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
7.8) กำหนดวิธีปฏิบัติที่ดีในการใช้งานรหัสผ่าน เช่น รักษารหัสผ่านให้เป็นความลับ ไม่บันทึกรหัสผ่านที่สามารถพบเห็นได้ง่าย เป็นต้น	71 57				✓	✓
7.9) มีมาตรการป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงาน			4 5		–	✓
7.10) มีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่มั่นคงปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น	55 62				✓	✓
7.11) จัดทำนโยบายการใช้งานระบบเครือข่ายขององค์กร	50 63				–	✓
7.12) มีการระบุชัดเจนว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถเข้าถึงได้	54 51				–	✓
7.13) มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กร	58 58				✓	✓
7.14) มีการกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกการเชื่อมต่อจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว	7 5				–	✓
7.15) มีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย			5 5		–	✓
7.16) แบ่งแยกเครือข่ายขององค์กรตามกลุ่มของผู้ใช้งาน			4 5		–	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
7.17) แบ่งแยกเครือข่ายขององค์กรตามสารสนเทศที่ใช้งาน			5 5		-	✓
7.18) แบ่งแยกเครือข่ายขององค์กรตามกลุ่มของระบบสารสนเทศ			4 5		-	✓
7.19) จำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร	5 5				-	✓
7.20) การเชื่อมต่อระหว่างองค์กรต้องเป็นไปตามนโยบายควบคุมการเข้าถึงขององค์กร			4 5		-	✓
7.21) กำหนดเส้นทางบนระบบเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง			4 5		-	✓
7.22) มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ			4 5		-	✓
7.23) มีการระบุตัวตนในการเข้าใช้งานระบบสารสนเทศ	7 5				✓	✓
7.24) มีมาตรการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ				4 4	✓	✓
7.25) กำหนดให้ระบบสารสนเทศตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด	60 57				✓	✓
7.26) การเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของซอฟต์แวร์แยกตามประเภทของผู้ใช้งาน	53 58				✓	✓
7.27) แยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากสำหรับระบบนี้โดยเฉพาะ				4 4	-	✓
7.28) กำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone, และ tablet เป็นต้น) ในการเข้าสู่ระบบเครือข่าย				4 4	-	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
7.29) กำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์อุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone, และ tablet เป็นต้น)				4 4	–	✓
7.30) กำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน				4 4	–	✓
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)						
8.1) ระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว				4 4	–	✓
8.2) มีกลไกสำหรับตรวจสอบข้อมูลนำเข้าของซอฟต์แวร์ ว่าข้อมูลนั้นมีความถูกต้องและเหมาะสม				4 4	–	✓
8.3) มีกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่				4 4	–	✓
8.4) มีกลไกสำหรับการตรวจสอบข้อมูลนำออกจากซอฟต์แวร์ว่าเป็นไปอย่างถูกต้องเหมาะสม			4 5		–	✓
8.5) มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูลบังคับใช้ในองค์กร	5 5				–	✓
8.6) มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล		6 4			–	✓
8.7) มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบสารสนเทศที่ให้บริการแก่องค์กร				5 4	–	✓
8.8) ไม่ใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการ สำหรับทำการทดสอบระบบ			5 5		–	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่ต้องการ	ผู้ใช้ทั่วไป	ผู้ดูแลระบบ
8.9) มีการกำหนดให้มีการป้องกันและควบคุมการใช้งานข้อมูลจริงในการทดสอบระบบ	5 5				-	✓
8.10) จำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ		5 4			-	✓
8.11) กำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ	5 5				-	✓
8.12) มีการตรวจสอบทางเทคนิค ภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าซอฟต์แวร์ทำงานได้ปกติ			4 5		-	✓
8.13) มีการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ตามความจำเป็นเท่านั้น	5 5				-	✓
8.14) มีการกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร			4 5		-	✓
8.15) มีการกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์			4 5		-	✓
8.16) มีการกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน			4 5		-	✓
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)						
9.1) มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ผ่านช่องทางการรายงานที่กำหนดไว้			48 59		✓	✓
9.2) บันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่			57 61		✓	✓
9.3) มีการกำหนดหน้าที่ความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร				4 4	-	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
9.4) มีการกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร			55 61		✓	✓
9.5) ขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร รวดเร็ว ได้ผล และเป็นระบบระเบียบที่ดี			53 61		✓	✓
9.6) บันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย ประกอบด้วย ประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย		6 4			-	✓
9.7) ต้องรวบรวมและจัดเก็บหลักฐานเพื่อใช้ในกระบวนการทางศาลที่เกี่ยวข้อง			54 63		✓	✓
9.8) มีกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงเพื่อใช้ในกระบวนการทางศาล			59 64		✓	✓
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)						
10.1) มีการกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร	47 61				✓	✓
10.2) มีการปรับปรุงกระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กรอย่างสม่ำเสมอ			48 62		✓	✓
10.3) กระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร		61 49			✓	✓
10.4) มีการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร		6 5			-	✓
10.5) มีการประเมินความเสี่ยงระบบสารสนเทศขององค์กร		7 5			-	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบ สารสนเทศ
10.6) ต้องจัดทำแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้				4 4	-	✓
10.7) มีการใช้งานแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้				5 4	-	✓
10.8) มีการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับการให้บริการขององค์กร			49 61		✓	✓
10.9) มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้การให้บริการขององค์กรอย่างสม่ำเสมอ			53 62		✓	✓
11. การปฏิบัติตามข้อกำหนด (Compliance)						
11.1) มีการระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานขององค์กร และบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร			58 60		✓	✓
11.2) มีการปรับปรุงข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานขององค์กรอย่างสม่ำเสมอ			56 60		✓	✓
11.3) มีการกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา			56 60		✓	✓

ตาราง 20 (ต่อ)

กรอบมาตรฐานการจัดการความมั่นคงปลอดภัย	ความคิดเห็นของกลุ่มตัวอย่าง (คน)				ประเภท	
	มี และต้องการ	มี และไม่ต้องการ	ไม่มี และต้องการ	ไม่มี และไม่	ผู้ใช้ทั่วไป	ผู้ดูแลระบบสารสนเทศ
11.4) มีการกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจจากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง			56 63		✓	✓
11.5) มีการกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง			53 63		✓	✓
11.6) ป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ระบบสารสนเทศขององค์กรผิดวัตถุประสงค์			55 63		✓	✓
11.7) ป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต			55 65		✓	✓
11.8) กำหนดให้ใช้มาตรการ การเข้ารหัสข้อมูลโดยสอดคล้องตามกฎหมาย			49 62		✓	✓
11.9)ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน			49 59		✓	✓
11.10)มีการตรวจประเมินระบบสารสนเทศอย่างสม่ำเสมอ	48 60				✓	✓
11.11)มีการระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร			49 61		✓	✓
11.12)มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ			50 58		✓	✓

* ค่าที่แสดงในตาราง คือ ค่าความถี่ของ ผู้ใช้ระบบสารสนเทศ / ผู้ดูแลระบบสารสนเทศ

จากตาราง 20 การจัดการความมั่นคงปลอดภัยสารสนเทศในกลุ่มผู้ใช้ทั่วไป กลุ่มเครือข่ายบริการสุขภาพ ฯ มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และต้องการให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศในหมวด 1) นโยบายความมั่นคงปลอดภัยสารสนเทศ จำนวน 1 ข้อย่อย หมวด 2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร จำนวน 4 ข้อย่อย หมวด 3) การบริหารจัดการทรัพย์สินขององค์กร จำนวน 6 ข้อย่อย หมวด 4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร จำนวน 2 ข้อย่อย หมวด 5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม จำนวน 14 ข้อย่อย หมวด 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร จำนวน 2 ข้อย่อย หมวด 7) การควบคุมการเข้าถึง จำนวน 10 ข้อย่อย หมวด 8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ หมวดนี้เป็นการจัดการความมั่นคงปลอดภัยสารสนเทศของผู้ดูแลระบบสารสนเทศเท่านั้น หมวด 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ไม่มีการจัดการความมั่นคงปลอดภัยสารสนเทศ หมวด 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร จำนวน 1 ข้อย่อย หมวด 11) การปฏิบัติตามข้อกำหนด จำนวน 1 ข้อย่อย

ผู้ใช้ทั่วไปของกลุ่มเครือข่ายบริการสุขภาพ ฯ มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และไม่ต้องการการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ หมวด 10)การบริหารความต่อเนื่องในการดำเนินงานขององค์กร จำนวน 1 ข้อย่อย

ผู้ใช้ทั่วไปของกลุ่มเครือข่ายบริการสุขภาพ ฯ ไม่มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และต้องการการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ หมวด 1) นโยบายความมั่นคงปลอดภัยสารสนเทศ จำนวน 2 ข้อย่อย หมวด 4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร จำนวน 2 ข้อย่อย หมวด 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร จำนวน 10 ข้อย่อย หมวด 7) การควบคุมการเข้าถึง จำนวน 3 ข้อย่อย หมวด 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร จำนวน 6 ข้อย่อย หมวด 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร จำนวน 3 ข้อย่อย หมวด 11) การปฏิบัติตามข้อกำหนด จำนวน 11 ข้อย่อย

ผู้ใช้ทั่วไปของกลุ่มเครือข่ายบริการสุขภาพ ฯ ไม่มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และไม่ต้องการการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ หมวด 7) การควบคุมการเข้าถึง จำนวน 1 ข้อย่อย

ผู้ดูแลระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ ฯ ไม่มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และไม่ต้องการการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ และไม่ต้องการการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ หมวด 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร จำนวน 7 ข้อย่อย หมวด 7) การควบคุมการเข้าถึง จำนวน 5 ข้อย่อย หมวด 8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ จำนวน 4 ข้อย่อย หมวด 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร จำนวน 1 ข้อย่อย หมวด 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร จำนวน 2 ข้อย่อย

ส่วนผู้ดูแลระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ ฯ มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และต้องการให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ หมวด 1) นโยบายความมั่นคงปลอดภัยสารสนเทศ จำนวน 1 ข้อย่อย หมวด 2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร จำนวน 7 ข้อย่อย หมวด 3) การบริหารจัดการทรัพย์สินขององค์กร จำนวน 6 ข้อย่อย หมวด 4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร จำนวน 4 ข้อย่อย หมวด 5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม จำนวน 15 ข้อย่อย หมวด 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร จำนวน 14 ข้อย่อย หมวด 7) การควบคุมการเข้าถึง จำนวน 14 ข้อย่อย หมวด 8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ จำนวน 4 ข้อย่อย หมวด 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร จำนวน 1 ข้อย่อย หมวด 11) การปฏิบัติตามข้อกำหนด จำนวน 1 ข้อย่อย

ผู้ดูแลระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ ฯ มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และไม่ต้องการให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ หมวด 2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร จำนวน 2 ข้อย่อย หมวด 4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร จำนวน 2 ข้อย่อย หมวด 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ

ขององค์กร จำนวน 6 ข้อย่อย หมวด 8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ จำนวน 2 ข้อย่อย หมวด 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร จำนวน 1 ข้อย่อย หมวด 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร จำนวน 3 ข้อย่อย

ผู้ดูแลระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ ฯ ไม่มีการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ และต้องการการปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ หมวด 1) นโยบายความมั่นคงปลอดภัยสารสนเทศ จำนวน 2 ข้อย่อย หมวด 2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร จำนวน 2 ข้อย่อย หมวด 4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร จำนวน 3 ข้อย่อย หมวด 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร จำนวน 14 ข้อย่อย หมวด 7) การควบคุมการเข้าถึง จำนวน 11 ข้อย่อย หมวด 8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ จำนวน 6 ข้อย่อย หมวด 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร จำนวน 6 ข้อย่อย หมวด 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร จำนวน 3 ข้อย่อย หมวด 11) การปฏิบัติตามข้อกำหนด จำนวน 11 ข้อย่อย

แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

จากการประเมินตามกรอบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดังตาราง 20 และจัดทำร่างแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เพื่อใช้ในการสนทนากลุ่มย่อยกับผู้ทรงคุณวุฒิและตัวแทนผู้ใช้ระบบสารสนเทศของโรงพยาบาล และโรงพยาบาลส่งเสริมสุขภาพตำบล ในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร จำนวน 13 คน มีข้อเสนอแนะต่อร่างแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดังตาราง 21

ตาราง 21 ข้อเสนอแนะร่างแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ

ที่	ร่างแนวทางการจัดการ ความมั่นคงปลอดภัย	สถานะ	เหตุผล
1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Security policy)			
	เห็นด้วยในทุกข้อ		
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร(Organization of information security)			
2.7	มีการตรวจสอบการจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร โดยผู้ตรวจสอบอิสระตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร	ตัดร่างแนวทาง ฯ	มีนโยบายการตรวจสอบโดยหน่วยงานภายในโรงพยาบาล และโรงพยาบาลส่งเสริมสุขภาพตำบลซึ่งเพียงพอต่อการดำเนินงานขององค์กร และการใช้ผู้ตรวจสอบอิสระทำให้มีค่าใช้จ่ายเพิ่มขึ้น โรงพยาบาลไม่มีงบเพียงพอสำหรับการทำงานในส่วนนี้
2.8	ควรจัดทำการประเมินความเสี่ยงของการเข้าถึงสารสนเทศ และอุปกรณ์สารสนเทศ เพื่อคำนึงถึงผลกระทบและความสำคัญของข้อมูลแต่ละประเภท	เพิ่มร่างแนวทาง ฯ	การประเมินความเสี่ยงของการเข้าถึงเข้าถึงสารสนเทศและอุปกรณ์สารสนเทศ ทำให้สามารถป้องกันภัยคุกคามที่จะเกิดขึ้นแต่เนิ่นๆ ได้
2.10	มีการกำหนดข้อกำหนดทางด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นให้ผู้ใช้บริการเข้าถึงสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ	เพิ่มร่างแนวทาง ฯ	เป็นนโยบายความมั่นคงปลอดภัยในกรณีที่ผู้ใช้บริการเข้าถึงสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ
3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)			
	เห็นด้วยในทุกข้อ		

ตาราง 21 (ต่อ)

ที่	ร่างแนวทางการจัดการความมั่นคงปลอดภัย	สถานะ	เหตุผล
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)			
4.1	กำหนดหน้าที่และความรับผิดชอบทางด้านความ อย่างเป็นลายลักษณ์อักษร	เพิ่มร่างแนวทาง ฯ	กำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศแนบท้ายโดยเป็นลายลักษณ์อักษร
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)			
	เห็นด้วยในทุกข้อ		
6. การบริหารจัดการด้านการสื่อสารและการดาเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)			
6.5	มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการระบบสารสนเทศแก่องค์กรออกจากกัน	เพิ่มร่างแนวทาง ฯ	เป็นนโยบายเพื่อเป็นแนวทางในการพัฒนาระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ ฯ
6.8	มีการกำหนดให้มีการปรับปรุงรายละเอียดข้อตกลง เงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก	เพิ่มร่างแนวทาง ฯ	ถ้ามีการเปลี่ยนแปลงใดๆ กับระบบสารสนเทศ (HOSxP) ต้องแจ้งผู้ใช้งาน
6.16	กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการเครือข่ายคอมพิวเตอร์ และอินเทอร์เน็ตขององค์กร	เพิ่มร่างแนวทาง ฯ	จำเป็นต้องมีนโยบายในข้อนี้ไว้เพื่อเป็นแนวทางในการให้บริการเครือข่าย
6.18	มีการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (รวมถึงสื่อบันทึกข้อมูลที่เป็นเอกสาร ซึ่งรวมถึงแฟ้มข้อมูลผู้รับบริการของโรงพยาบาล)	เพิ่มร่างแนวทาง ฯ	เป็นนโยบายที่มีการปฏิบัติอยู่แล้ว ต้องทำบันทึกขออนุญาต แจ้งไปยังผู้อำนวยการโรงพยาบาล

ตาราง 21 (ต่อ)

ที่	ร่างแนวทางการจัดการความมั่นคงปลอดภัย	สถานะ	เหตุผล
6.22	มีการกำหนดขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศ	เพิ่มร่างแนวทาง ฯ	มีการปฏิบัติ แต่ยังไม่มีนโยบายเป็นลายลักษณ์อักษร
6.23	ขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศได้ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	เพิ่มร่างแนวทาง ฯ	มีการปฏิบัติ แต่ยังไม่มีนโยบายเป็นลายลักษณ์อักษร
6.24	ขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศได้ป้องกันการใช้งานผิดวัตถุประสงค์	เพิ่มร่างแนวทาง ฯ	มีการปฏิบัติ แต่ยังไม่มีนโยบายเป็นลายลักษณ์อักษร
6.25	มีมาตรการป้องกันเอกสารของระบบสารสนเทศจากการเข้าถึงโดยไม่ได้รับอนุญาต	เพิ่มร่างแนวทาง ฯ	มีการปฏิบัติ แต่ยังไม่มีนโยบายเป็นลายลักษณ์อักษร
6.31	มีการบันทึกกิจกรรมและเหตุการณ์ต่างๆ (Log) ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ	เพิ่มร่างแนวทาง ฯ	มีการเก็บ log แต่ยังไม่มีการประกาศเป็นลายลักษณ์อักษร
6.33	มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ (Log)	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
6.34	มีการกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบสารสนเทศหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
6.35	มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล

ตาราง 21 (ต่อ)

ที่	ร่างแนวทางการจัดการ ความมั่นคงปลอดภัย	สถานะ	เหตุผล
6.36	มีการวิเคราะห์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศและดำเนินการแก้ไขตามสมควร	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
7. การควบคุมการเข้าถึง (Access control)			
7.27	แยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากสำหรับระบบนี้โดยเฉพาะ	ตัดร่างแนวทาง ฯ	โรงพยาบาลขาดงบประมาณในการแยกเครือข่ายของระบบสารสนเทศที่มีความสำคัญไว้ในพื้นที่ต่างหาก และการบริหารจัดการเป็นไปได้ยาก โดยข้อมูลของผู้รับบริหารที่ต้องปกปิดเป็นความลับจะมีระบบสารสนเทศเฉพาะที่แยกจากระบบ HOSxP ของโรงพยาบาล
7.28	กำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone, และ tablet เป็นต้น) ในการเข้าสู่ระบบเครือข่าย	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
7.29	กำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์อุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone, และ tablet เป็นต้น)	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
7.30	กำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล โดยการบริหารจัดการระบบสารสนเทศของโรงพยาบาล อาจมีการ

ตาราง 21 (ต่อ)

ที่	ร่างแนวทางการจัดการความมั่นคงปลอดภัย	สถานะ	เหตุผล
			remote desktop เพื่อแก้ไขปัญหา การกำหนดเป็นนโยบายนี้จะส่งผลดีให้มีการปฏิบัติงานในมาตรฐานเดียวกัน
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)			
8.1	ระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
8.2	มีกลไกสำหรับตรวจสอบข้อมูลนำเข้าของซอฟต์แวร์ ว่าข้อมูลนั้นมีความถูกต้องและเหมาะสม	เพิ่มร่างแนวทาง ฯ	มีการปฏิบัติ แต่ยังไม่มีนโยบายเป็นลายลักษณ์อักษร
8.3	มีกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่	เพิ่มร่างแนวทาง ฯ	มีการปฏิบัติ แต่ยังไม่มีนโยบายเป็นลายลักษณ์อักษร
8.6	มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล	ตัดร่างแนวทาง ฯ	โรงพยาบาลขาดบุคลากร เครื่องมือ งบประมาณ ในการบริหารจัดการเกี่ยวกับการเข้ารหัสข้อมูล
8.7	มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบสารสนเทศที่ให้บริการแก่องค์กร	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
8.8	ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ โปรแกรมเมอร์ไม่ใช้ข้อมูลจริงที่ใช้งานสำหรับการทดสอบระบบสารสนเทศ	ตัดร่างแนวทาง ฯ	ในการจัดทำ หรือแก้ไขรายงานเพื่อส่งให้หน่วยงานต้นสังกัด จำเป็นต้องใช้ข้อมูลจริงเพื่อตรวจสอบ

ตาราง 21 (ต่อ)

ที่	ร่างแนวทางการจัดการความมั่นคงปลอดภัย	สถานะ	เหตุผล
			ความถูกต้อง และความสมบูรณ์ของรายงาน
8.10	จำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ตัดร่างแนวทาง ฯ	ผู้ดูแลระบบสารสนเทศมีความจำเป็นต้องเข้าถึงซอร์สโค้ดของระบบสารสนเทศเพื่อให้การบริหารจัดการมีประสิทธิภาพ
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)			
9.3	มีการกำหนดหน้าที่ความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
9.6	บันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย ประกอบด้วย ประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย	เพิ่มร่างแนวทาง ฯ	มีการปฏิบัติ แต่ยังไม่มีนโยบายเป็นลายลักษณ์อักษร
10. การบริหารความต่อเนื่องในการดาเนินงานขององค์กร (Business continuity management)			
10.4	มีการประเมินความเสี่ยงในแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล เพื่อให้แผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กรมีความสมบูรณ์มากยิ่งขึ้น
10.5	มีการประเมินความเสี่ยงระบบสารสนเทศขององค์กร	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล

ตาราง 21 (ต่อ)

ที่	ร่างแนวทางการจัดการความมั่นคงปลอดภัย	สถานะ	เหตุผล
10.6	ต้องจัดทำแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
10.7	มีการใช้งานแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้	เพิ่มร่างแนวทาง ฯ	กำหนดเป็นนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศของโรงพยาบาล
11. การปฏิบัติตามข้อกำหนด (Compliance)			
	เห็นด้วยในทุกข้อ		


ภาพประกอบ 9 การสนทนากลุ่มย่อย

จากการปรับปรุงร่างแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ตามผู้ทรงคุณวุฒิตัวแทนผู้ใช้ระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครได้ข้อสรุปแนวทางแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศสำหรับกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดังตาราง 22

ตาราง 22 แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ สำหรับผู้ใช้ทั่วไป

แนวทางการจัดการความมั่นคงปลอดภัย
1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Security policy)
1.1 กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดำเนินการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศให้เป็นลายลักษณ์อักษร
1.2 ประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ภายในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร(Organization of information security)
2.1 กำหนดให้ฝ่ายสารสนเทศ และงานประกันสุขภาพมีบทบาทหน้าที่ในการจัดการความมั่นคงปลอดภัยสารสนเทศ หรือจัดตั้งหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศในระดับกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
2.2 ดำเนินการแต่งตั้งบุคลากรในโรงพยาบาล และโรงพยาบาลส่งเสริมสุขภาพตำบล ในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครทำงานร่วมกันเพื่อประสานงานด้านความมั่นคงปลอดภัยสารสนเทศ
2.3 โรงพยาบาลในกลุ่มครือข่ายบริการสุขภาพ อำเภอ ฯ มีข้อกำหนดกระบวนในการอนุมัติใช้งานอุปกรณ์ระบบสารสนเทศ เช่น การใช้คอมพิวเตอร์ การใช้เครื่องแม่ข่าย การใช้ปริ้นเตอร์ การใช้งานเครือข่ายคอมพิวเตอร์ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เป็นต้น
2.4 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประกาศและกำหนดให้บุคลากรที่เกี่ยวข้องกับฐานข้อมูลทุกคนลงนามไม่เปิดเผยข้อมูลความลับของกลุ่มเครือข่ายบริการสุขภาพ
3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)
3.1 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดำเนินการจัดทำบัญชีครุภัณฑ์ของโรงพยาบาล
3.2 ดำเนินการปรับปรุงบัญชีครุภัณฑ์ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ให้ถูกต้องอยู่เสมอ
3.3 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ระบุผู้รับผิดชอบครุภัณฑ์แต่ละรายการที่เกี่ยวข้องกับระบบสารสนเทศ
3.4 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดกฎระเบียบการใช้ระบบเทคโนโลยีสารสนเทศและครุภัณฑ์ที่เกี่ยวข้องของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

ตาราง 22 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
3.5 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดำเนินการจัดหมวดหมู่ของครุภัณฑ์ ข้อมูลในรูปแบบต่างๆ เช่น ข้อมูลในฐานข้อมูลของระบบสารสนเทศ ข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ข้อมูลในรูปแบบเอกสาร เป็นต้น ตามระดับชั้นความลับ และความสำคัญที่มีต่อโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
3.6 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร จัดทำป้ายกำกับทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กร เช่น ป้ายเลขครุภัณฑ์ติดเครื่องคอมพิวเตอร์ ป้ายชื่อติดสายไฟเบอร์ เป็นต้น
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)
4.1 บุคลากรภายในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร บุคคลภายนอกต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
4.2 กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดำเนินการอบรมหรือจัดทำสื่อให้ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรภายใน และภายนอกกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
4.3 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดการลงโทษแก่ผู้ละเมิด นโยบาย กฎ ข้อบังคับ ด้านความมั่นคงปลอดภัยของกลุ่มเครือข่ายบริการสุขภาพอำเภอ ฯ
4.4 ถอดถอน ยกเลิกสิทธิในการเข้าถึง การเข้าใช้ระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เมื่อสิ้นสุดสภาพการเป็นบุคลากร หรือมีการปรับเปลี่ยนตำแหน่งหน้าที่
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)
5.1 พื้นที่ ควบคุมการเข้าออกสำนักงานหรือฝ่ายสารสนเทศ และงานประกันสุขภาพของโรงพยาบาล เพื่อป้องกันการเข้าถึงข้อมูล และระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์เทคโนโลยีสารสนเทศ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
5.2 ควบคุมพื้นที่โรงพยาบาลที่ต้องการรักษาความมั่นคงปลอดภัย ให้เข้าและออกได้ เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
5.3 มีมาตรการป้องกันต่อภัยคุกคามต่างๆ ที่สามารถส่งผลกระทบแก่โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ทั้งที่เกิดจากมนุษย์และธรรมชาติ

ตาราง 22 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
5.4 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดการป้องกันทางกายภาพในบริเวณของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ที่ต้องการรักษาความมั่นคงปลอดภัย
5.5 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดแนวทางและประกาศให้ทราบโดยทั่วสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย
5.6 ติดตั้งอุปกรณ์ในบริเวณที่ไม่มีความเสียงและมีการป้องกันความเสี่ยงที่จะเกิดกับอุปกรณ์จากภัยคุกคามต่างๆ
5.7 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีการป้องกันความล้มเหลวของระบบไฟฟ้าเพื่อให้บริการได้ 24 ชั่วโมง
5.8 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีกลไกเป้องกันความล้มเหลวของระบบเครือข่ายคอมพิวเตอร์ให้บริการได้ 24 ชั่วโมง
5.9 มีการป้องกันการเข้าถึง สายไฟฟ้า สายสื่อสารต่างๆ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร โดยไม่ได้รับอนุญาต
5.10 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดให้มีการบำรุงรักษาอุปกรณ์ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพให้พร้อมใช้งานเสมอ
5.11 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดให้มีการป้องกันอุปกรณ์ของโรงพยาบาล ที่มีการใช้งานภายนอกสำนักงาน ไม่ให้ได้รับความเสียหาย
5.12 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดให้มีการขออนุญาตก่อนนำ อุปกรณ์คอมพิวเตอร์ คอมพิวเตอร์และอุปกรณ์ต่อพ่วง ข้อมูล สารสนเทศ
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)
6.1 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร จัดทำคู่มือการปฏิบัติงานด้านเครือข่ายสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
6.2 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดรอบระยะเวลาในการปรับปรุงคู่มือการปฏิบัติงานด้านเครือข่ายสารสนเทศ
6.3 ผู้ให้บริการภายนอกต้องปฏิบัติตามข้อกำหนด หรือข้อตกลงที่จัดทำขึ้นระหว่างโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
6.4 ติดตั้งโปรแกรมป้องกันไวรัส/มัลแวร์บนคอมพิวเตอร์ที่ใช้ในโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

ตาราง 22 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
6.5 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่อสารสนเทศที่ส่งผ่านทางระบบเครือข่ายของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
6.6 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เช่น แฟรชไดรฟ์ ฮาร์ดดิส เอกสาร ซีดี ดีวีดี เป็นต้น
6.7 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการ เพื่อป้องกันปัญหาของการแลกเปลี่ยนข้อมูลการรักษาผู้ป่วย ข้อมูลการให้บริการ ข้อมูลและสารสนเทศอื่นๆ ระหว่างองค์กรทั้งภายในและภายนอก
6.8 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ และผู้ที่เกี่ยวข้องจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลการรักษาผู้ป่วย ข้อมูลการให้บริการ ข้อมูลและสารสนเทศอื่นๆ ระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร
6.9 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ผู้ที่เกี่ยวข้อง มีการป้องกันการเข้าถึงสื่อบันทึกข้อมูล (ฮาร์ดดิส แฟรชไดรฟ์ ซีดี ดีวีดี เอกสาร) จากการเข้าถึงโดยไม่ได้รับอนุญาต ระหว่างการส่งข้อมูลไปยังหน่วยงานภายนอก
6.10 กำหนดมาตรการป้องกัน ข้อมูล สารสนเทศ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ที่ส่งผ่านทางอีเมล์ หรือสื่อสังคมออนไลน์
6.11 กำหนดการป้องกันความถูกต้องและความสมบูรณ์ของข้อมูล สารสนเทศ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ที่เผยแพร่สู่สาธารณะ
6.12 กำหนดขั้นตอนปฏิบัติในการตรวจสอบการใช้เครื่องมือ คอมพิวเตอร์ อุปกรณ์ต่อพ่วง ข้อมูล สารสนเทศ ทรัพย์สิน ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครอย่างสม่ำเสมอ
7. การควบคุมการเข้าถึง (Access control)
7.1 กำหนดนโยบายการควบคุมการเข้าถึงระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร อย่างเป็นลายลักษณ์อักษร
7.2 กำหนดระยะเวลาในการปรับปรุงนโยบายการควบคุมการเข้าถึงระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.3 กำหนดขั้นตอนปฏิบัติสำหรับการลงทะเบียนบุคลากรใหม่เพื่อให้มีสิทธิในการใช้ระบบสารสนเทศตามความจำเป็น

ตาราง 22 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
7.4 กำหนดขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิต่างๆ ในการใช้ระบบสารสนเทศเมื่อพนักงานลาออกหรือเปลี่ยนตำแหน่งงานภายในโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.5 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร จำกัดสิทธิการใช้งานระบบสารสนเทศของบุคลากรตามความจำเป็นในการใช้งาน
7.6 กำหนดข้อกำหนด นโยบายในการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.7 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดขั้นตอนปฏิบัติที่ดีในการตั้งรหัสผ่าน
7.8 กำหนดขั้นตอนปฏิบัติในการใช้รหัสผ่านที่ดี เช่น การรักษารหัสผ่านเป็นความลับ การเปลี่ยนรหัสผ่านทุก 3 เดือน ไม่บันทึกรหัสผ่านในลักษณะที่พบเห็นได้ง่าย เป็นต้น
7.9 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดนโยบายควบคุมไม่ให้ข้อมูลการรักษาผู้ป่วย ข้อมูลของผู้รับบริการ ข้อมูล สารสนเทศ สื่อบันทึกข้อมูล อยู่ในสถานที่ ที่ไม่มั่นคงปลอดภัย เช่น สามารถเข้าถึง หรือพบเห็นได้ง่ายในสถานที่สาธารณะ หรือผู้รับบริการบุคคลภายนอก ผู้ไม่ได้รับอนุญาต สามารถเข้าถึงได้ง่าย เป็นต้น
7.10 กำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.11 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดให้มีการระบุตัวตนในการเข้าใช้ระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.12 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดมาตรการการกำหนดรหัสผ่านที่มีคุณภาพ เช่น กำหนดรหัสผ่านตั้งแต่ 8 ตัวอักษรขึ้นไป รหัสผ่านต้องประกอบด้วยอักษรและตัวเลข รหัสผ่านต้องไม่ซ้ำกับชื่อผู้ใช้ เป็นต้น
7.13 กำหนดให้มีการตัดการใช้งานของผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครตามระยะเวลาที่กำหนด
7.14 กำหนดการเข้าถึงระบบสารสนเทศ ข้อมูล สารสนเทศ ข้อมูลการรักษาผู้ป่วย ข้อมูลการให้บริการแยกตามประเภท หรือกลุ่มของบุคลากรโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
8. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

ตาราง 22 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
8.1 บุคลากรในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ผ่านช่องทางการรายงานที่กำหนดไว้
8.2 บุคลากรในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร บันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่
8.3 กำหนดขั้นตอนปฏิบัติในการรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ให้มีความรวดเร็วทันต่อสถานการณ์ ได้ผลลัพธ์ที่ดี เป็นระเบียบแบบแผน
8.4 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดกฎหรือหลักเกณฑ์ในการรวบรวม จัดเก็บหลักฐานต่างๆ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เพื่อใช้ในกระบวนการทางศาล
9. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)
9.1 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดกระบวนการในการสร้างความต่อเนื่องของการให้บริการของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
9.2 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดให้มีการปรับปรุงกระบวนการในการสร้างความต่อเนื่องของการให้บริการอย่างสม่ำเสมอ
9.3 กระบวนการในการสร้างความต่อเนื่องให้กับการให้บริการขององค์กร จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับการให้บริการของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
9.4 กำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับการให้บริการของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
9.5 ทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้การให้บริการของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร อย่างสม่ำเสมอ
10. การปฏิบัติตามข้อกำหนด (Compliance)
10.1 ระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างโรงพยาบาล และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร และบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร

ตาราง 22 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
10.2 ปรับปรุงข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างโรงพยาบาล และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร อย่างสม่ำเสมอ
10.3 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร กำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา
10.4 กำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง
10.5 กำหนดให้มีการป้องกันข้อมูลส่วนบุคคลที่มีอยู่ในโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง
10.6 ป้องกันไม่ให้ผู้ใช้ ใช้อุปกรณ์ระบบสารสนเทศ (คอมพิวเตอร์ อุปกรณ์ต่อพ่วงต่างๆ) ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ผิดวัตถุประสงค์ และใช้อุปกรณ์ระบบสารสนเทศโดยไม่ได้รับอนุญาต
10.7 ผู้บริหารของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร คอยกำกับ ดูแล และควบคุมการปฏิบัติงานของบุคลากรให้ให้ปฏิบัติตามนโยบาย กฎ ขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบ
10.8 กำหนดการตรวจประเมินระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร อย่างสม่ำเสมอ
10.9 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร และจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ

ผู้ดูแลระบบสารสนเทศปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ใช้ทั่วไป และต้องปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ดูแลระบบสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดังตาราง 23

ตาราง 23 แนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศ ผู้ดูแลระบบสารสนเทศ

แนวทางการจัดการความมั่นคงปลอดภัย
1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Security policy)
1.1 ทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ตามระยะเวลาที่กำหนด
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร(Organization of information security)
2.1 กำหนดหน้าที่รับผิดชอบของบุคลากรโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ในการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน
2.2 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีข้อมูลการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ผู้ให้บริการอินเทอร์เน็ต กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ศูนย์ประสานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น
2.3 ดำเนินการจัดทำการประเมินความเสี่ยงของการเข้าถึงอุปกรณ์ เพื่อคำนึงถึงผลกระทบและความสำคัญของข้อมูลแต่ละประเภท
2.4 ดำเนินการกำหนดมาตรการรองรับที่เหมาะสมก่อนการอนุญาตให้เข้าถึงสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
2.5 กำหนดข้อกำหนดทางด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นให้ผู้ใช้บริการเข้าถึงสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ
2.6 กำหนดข้อกำหนด หรือข้อตกลงระหว่างผู้พัฒนาซอฟต์แวร์กับโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ก่อนการอนุญาตการเข้าถึงข้อมูลการรักษาผู้ป่วย ข้อมูลการให้บริการ และสารสนเทศขององค์กร
3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)
ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ปฏิบัติตามแนวทางในการจัดการความมั่นคงปลอดภัยสารสนเทศแบบเดียวกับผู้ใช้ทั่วไปของโรงพยาบาล
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)
4.1 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครแเป็นลายลักษณ์อักษร
4.2 กำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศสำหรับองค์กร หรือผู้ถูกจ้างงาน โดยต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

ตาราง 23 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
4.3 กำหนดระดับการเข้าถึงข้อมูลการรักษาผู้ป่วย ข้อมูลการให้บริการ ข้อมูลอื่นๆ สารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร แยกตามสิทธิของบุคลากร
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)
5.1 ดำเนินการทำลายข้อมูลภายในสื่อบันทึกข้อมูลของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครก่อนการทิ้งสื่อบันทึกข้อมูลทุกครั้ง
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)
6.1 กำหนดให้มีการควบคุมการเปลี่ยนแปลง หรือการแก้ไขใดๆ ที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
6.2 แบ่งหน้าที่รับผิดชอบงานด้านระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร แก่บุคลากรฝ่ายสารสนเทศ และงานประกันสุขภาพ
6.3 ดำเนินการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการระบบสารสนเทศแก่องค์กรออกจากกัน
6.4 ตรวจสอบการให้บริการระบบสารสนเทศ (HOSxP) ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ให้สามารถให้บริการได้อย่างสม่ำเสมอ
6.5 แก้ไข ปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น ระบบอินเทอร์เน็ต อีเมล์ เป็นต้น
6.6 หน่วยงานต่างๆ ภายในโรงพยาบาลของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร วางแผนกำหนดความต้องการทรัพยากรระบบเทคโนโลยีสารสนเทศเพิ่มเติมในอนาคต
6.7 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดเกณฑ์ตรวจรับระบบสารสนเทศใหม่
6.8 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดมาตรการ การกู้กลับคืน เมื่อระบบสารสนเทศได้รับความเสียหาย หรือถูกทำลายโดยไวรัสคอมพิวเตอร์/มัลแวร์
6.9 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ สำรองข้อมูลระบบสารสนเทศ และข้อมูลสำคัญอย่างสม่ำเสมอ
6.10 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ทดสอบข้อมูลที่สำรองไว้ว่าสามารถใช้งานได้อย่างสม่ำเสมอ

ตาราง 23 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
6.11 กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการเครือข่ายคอมพิวเตอร์ และอินเทอร์เน็ตขององค์กร
6.12 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดข้อกำหนดสำหรับการบริหารจัดการ สำหรับการบริการเครือข่ายที่องค์กรใช้บริการ
6.13 ดำเนินการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (รวมถึงสื่อบันทึกข้อมูลที่เป็นเอกสาร ซึ่งรวมถึงแฟ้มข้อมูลผู้รับบริการของโรงพยาบาล)
6.14 กำหนดข้อปฏิบัติในการทำลายสื่อบันทึกข้อมูล เอกสาร ที่ไม่ต้องใช้งาน ให้มีความมั่นคงปลอดภัย และขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูลที่ไม่ได้ใช้งานมีความมั่นคงปลอดภัยในทุกขั้นตอน
6.15 กำหนดขั้นตอนปฏิบัติในการจัดเก็บข้อมูลการรักษาผู้ป่วย ข้อมูลผู้มารับบริการ และข้อมูล หรือสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
6.16 มาตรการ ขั้นตอนปฏิบัติสำหรับการจัดเก็บสารสนเทศ โดยสารสนเทศได้ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และป้องกันการใช้งานผิดวัตถุประสงค์
6.17 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดำเนินการบันทึกล็อก (Log) กิจกรรมต่างๆ ของระบบสารสนเทศ ตามข้อกำหนดของกฎหมายที่เกี่ยวข้อง โดยล็อกที่บันทึกนี้ไม่สามารถดำเนินการแก้ไขได้
6.18 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบสารสนเทศหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร
6.19 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ และวิเคราะห์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศและดำเนินการแก้ไขตามสมควร
6.20 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดำเนินการตั้งเวลาของ อุปกรณ์ระบบสารสนเทศให้ตรงกัน หรือตั้งเวลาให้ตรงกันโดยใช้เครื่องแม่ข่ายเอ็นทีพี (ntp server)
6.21 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ดำเนินการตั้งเวลาของ อุปกรณ์ระบบสารสนเทศโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เชื่อถือได้ เช่น time.navy.mi.th, clock.nectec.or.th เป็นต้น
7. การควบคุมการเข้าถึง (Access control)
7.1 กำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร โดยอนุญาตให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิเท่านั้น

ตาราง 23 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
7.2 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ดำเนินการจัดทำนโยบายการใช้ระบบเครือข่ายของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.3 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ระบุบริการที่อนุญาตให้ผู้ใช้ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ที่สามารถใช้งานได้อย่างชัดเจน
7.4 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดให้อุปกรณ์ในระบบเครือข่ายระบุและพิสูจน์ตัวตน เพื่อบ่งบอกการเชื่อมต่อจากอุปกรณ์ และสถานที่ที่อนุญาตเท่านั้น
7.5 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดมาตรการป้องกันการเข้าถึงพอร์ตสำหรับการบริหารจัดการระบบสารสนเทศ โดยป้องกันทั้งทางกายภาพ และการเข้าถึงผ่านระบบเครือข่าย
7.6 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ จำกัดผู้ใช้ในการเชื่อมต่อเครือข่ายระหว่างองค์กร ทั้งภายในและภายนอกกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร เฉพาะผู้ใช้ที่อนุญาตเท่านั้น
7.7 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ดำเนินการให้การเชื่อมต่อระบบเครือข่ายระหว่างองค์กร และการกำหนดเส้นทางระบบเครือข่าย เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.8 กำหนดขั้นตอนปฏิบัติสำหรับการเข้าถึง หรือใช้งานระบบปฏิบัติการอย่างมั่นคงปลอดภัย
7.9 กำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone และ tablet เป็นต้น) ในการเข้าสู่ระบบเครือข่ายของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
7.10 กำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์อุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, smartphone, และ tablet เป็นต้น)
7.11 กำหนดนโยบายเพื่อใช้เป็นแนวทางบริหารจัดการระบบสารสนเทศ ในกรณีที่มีการเข้าถึงคอมพิวเตอร์จากระยะไกล (remote desktop) เพื่อแก้ไขปัญหา ซึ่งการกำหนดเป็นนโยบายนี้จะส่งผลดีให้มีการปฏิบัติงานในมาตรฐานเดียวกัน
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)
8.1 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

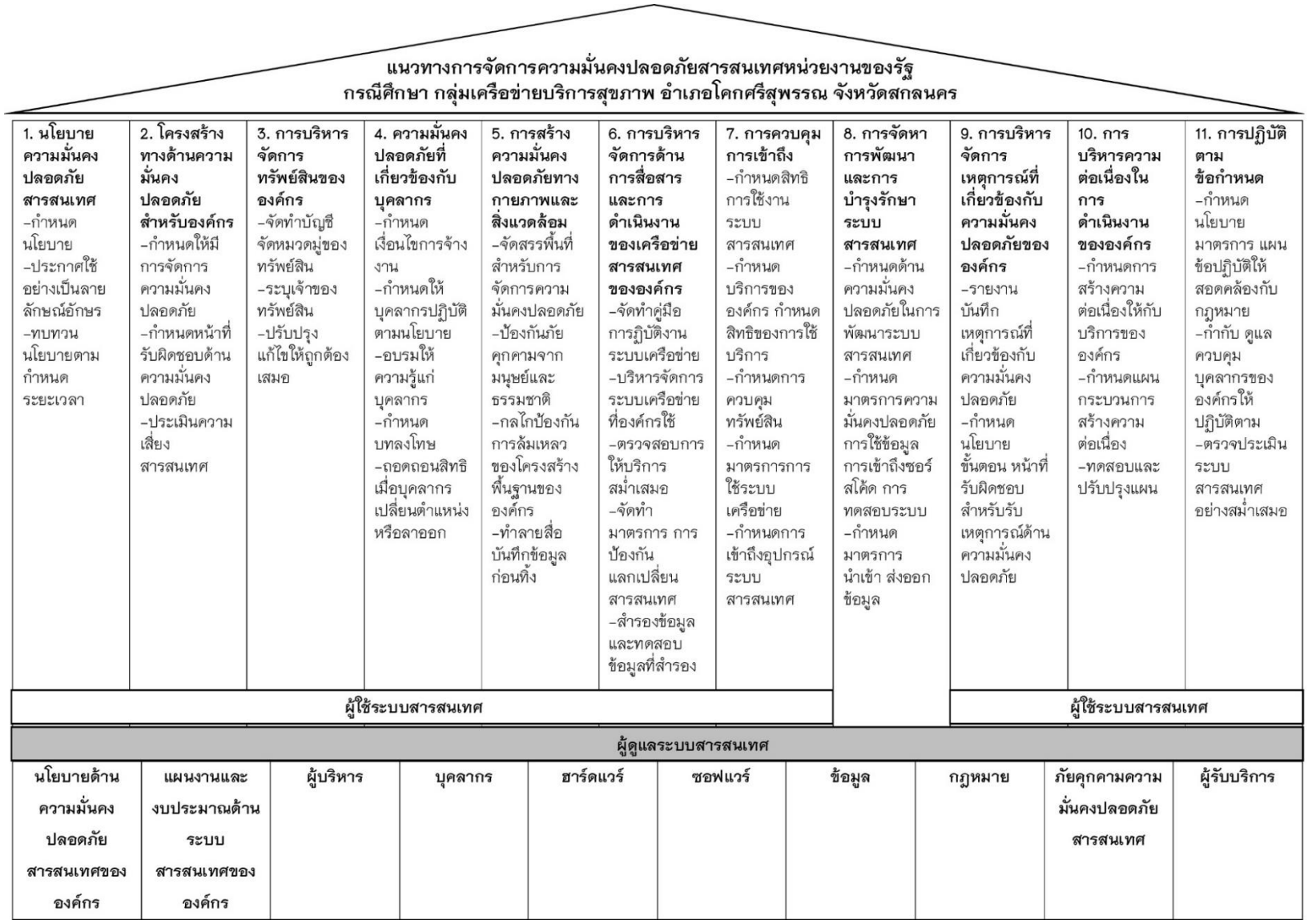
ตาราง 23 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
8.2 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีข้อปฏิบัติสำหรับการตรวจสอบข้อมูลนำเข้าของซอฟต์แวร์ ว่าข้อมูลนั้นมีความถูกต้องและเหมาะสม
8.3 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร มีข้อปฏิบัติสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่
8.4 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ มีกลไก การตรวจสอบข้อมูลนำออกจากซอฟต์แวร์เป็นไปอย่างถูกต้อง น่าเชื่อถือ
8.5 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบสารสนเทศที่ให้บริการแก่องค์กร
8.6 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดให้มีการป้องกันและควบคุมการใช้งานข้อมูลการให้บริการจริงในการทดสอบระบบ
8.7 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดขั้นตอนปฏิบัติเพื่อควบคุมการเปลี่ยนแปลง และการแก้ไขระบบสารสนเทศ
8.8 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ดำเนินการทดสอบซอฟต์แวร์หลังจากมีการเปลี่ยนแปลงระบบปฏิบัติการและส่วนที่เกี่ยวข้อง
8.9 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ดำเนินการแก้ไขซอฟต์แวร์เท่าที่จำเป็นเท่านั้น
8.10 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดมาตรการป้องกันการรั่วไหลข้อมูลการรักษาผู้ป่วย ข้อมูลการให้บริการ ข้อมูลหรือสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
8.11 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ กำหนดมาตรการ ควบคุม และตรวจสอบการพัฒนาซอฟต์แวร์ ของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
8.12 ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศ ติดตามข้อมูล ข่าว ที่เกี่ยวข้องกับช่องโหว่ในระบบสารสนเทศที่ให้บริการในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)
9.1 กำหนดหน้าที่ความรับผิดชอบของบุคลากรกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนครเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

ตาราง 23 (ต่อ)

แนวทางการจัดการความมั่นคงปลอดภัย
9.2 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร บันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย ประกอบด้วย ประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)
10.1 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร จัดทำแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้
10.2 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประเมินความเสี่ยงในแผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร
10.3 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประเมินความเสี่ยงระบบสารสนเทศขององค์กร
10.4 โรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประกาศใช้แผนสร้างความต่อเนื่องให้กับการให้บริการขององค์กร ให้สามารถดำเนินการให้บริการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ไม่สามารถให้บริการขององค์กรได้
11. การปฏิบัติตามข้อกำหนด (Compliance)
ฝ่ายสารสนเทศ และงานประกันสุขภาพ ผู้ดูแลระบบสารสนเทศของโรงพยาบาลในกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ปฏิบัติตามแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศเดียวกับ แนวทางแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศผู้ดูแลระบบสารสนเทศ

แนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร สามารถสรุปได้ดังภาพประกอบ 10



ภาพประกอบ 10 แนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร