คู่มือการดำเนินงาน

กลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร ฝ่ายปฏิบัติการอำนวยการ กลุ่มงานเวชศาสตร์ฉุกเฉิน
โรงพยาบาลอุดรธานี

๑. บทบาทภารกิจ

๑. วางแผนและเสนอแนะนโยบายด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในกลุ่มงานเวชศาสตร์ฉุกเฉินให้สอดคล้องกับนโยบายของโรงพยาบาลอุดรธานี

๒. บริหาร ออกแบบ ดูแล ซ่อมบำรุง ระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบการสื่อสารให้สามารถเชื่อมโยงกับหน่วยงานทั้งภายในและภายนอกกลุ่มงานเวชศาสตร์ฉุกเฉิน ให้มีเสถียรภาพและมีความปลอดภัย

๓. พัฒนาระบบสารสนเทศสำหรับการบริหารจัดการ เพื่อสนับสนุนการปฏิบัติงานและตัดสินใจของฝ่ายบริหาร

๔. พัฒนาองค์ความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารให้แก่บุคลากร

๕. ให้บริการข้อมูลสารสนเทศด้านการแพทย์ฉุกเฉินแก่ชุมชน

๖. ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

โดยสามารถแบ่งงานความรับผิดชอบเป็น ๔ งาน ดังนี้

๑. งานแผนงานสารสนเทศและการสื่อสาร

๑.๑ วิเคราะห์และจัดทำแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๒ วิเคราะห์และจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๓ วิเคราะห์และจัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒. งานบริการข้อมูลสารสนเทศและการสื่อสาร

๑. วิเคราะห์และสังเคราะห์ข้อมูลต่าง ๆ และประมวลผลในเชิงสถิติ เพื่อให้ได้มาซึ่งข้อมูลข่าวสาร

๒. บริการข้อมูลสารสนเทศด้านการแพทย์ฉุกเฉินแก่ชุมชน

๓. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ผู้ป่วยและผู้แจ้งเหตุฯ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

๓. งานพัฒนาระบบสารสนเทศและการสื่อสาร

๑. วางแผน วิเคราะห์ ออกแบบ พัฒนา ระบบฐานข้อมูลและระบบสารสนเทศและการสื่อสาร

๒. บริหาร ดูแล ระบบฐานข้อมูลและระบบงานสารสนเทศและการสื่อสาร

๔. ส่งเสริมและสนับสนุนการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ตามภารกิจอย่างเหมาะสม

๕. ดูแลและจัดหาชุดข้อมูลหรือโปรแกรมประยุกต์ที่จำเป็นสำหรับองค์กร

๖. ประสานกับหน่วยงานภายนอกเพื่อเชื่อมโยงแลกเปลี่ยนข้อมูล

๔. งานระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบโครงข่ายการสื่อสาร

๑. วางแผน วิเคราะห์ ออกแบบ พัฒนา ระบบคอมพิวเตอร์และการสื่อสาร

๒. บริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร

๓. บริหาร ดูแล ซ่อมบำรุงระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบการสื่อสาร

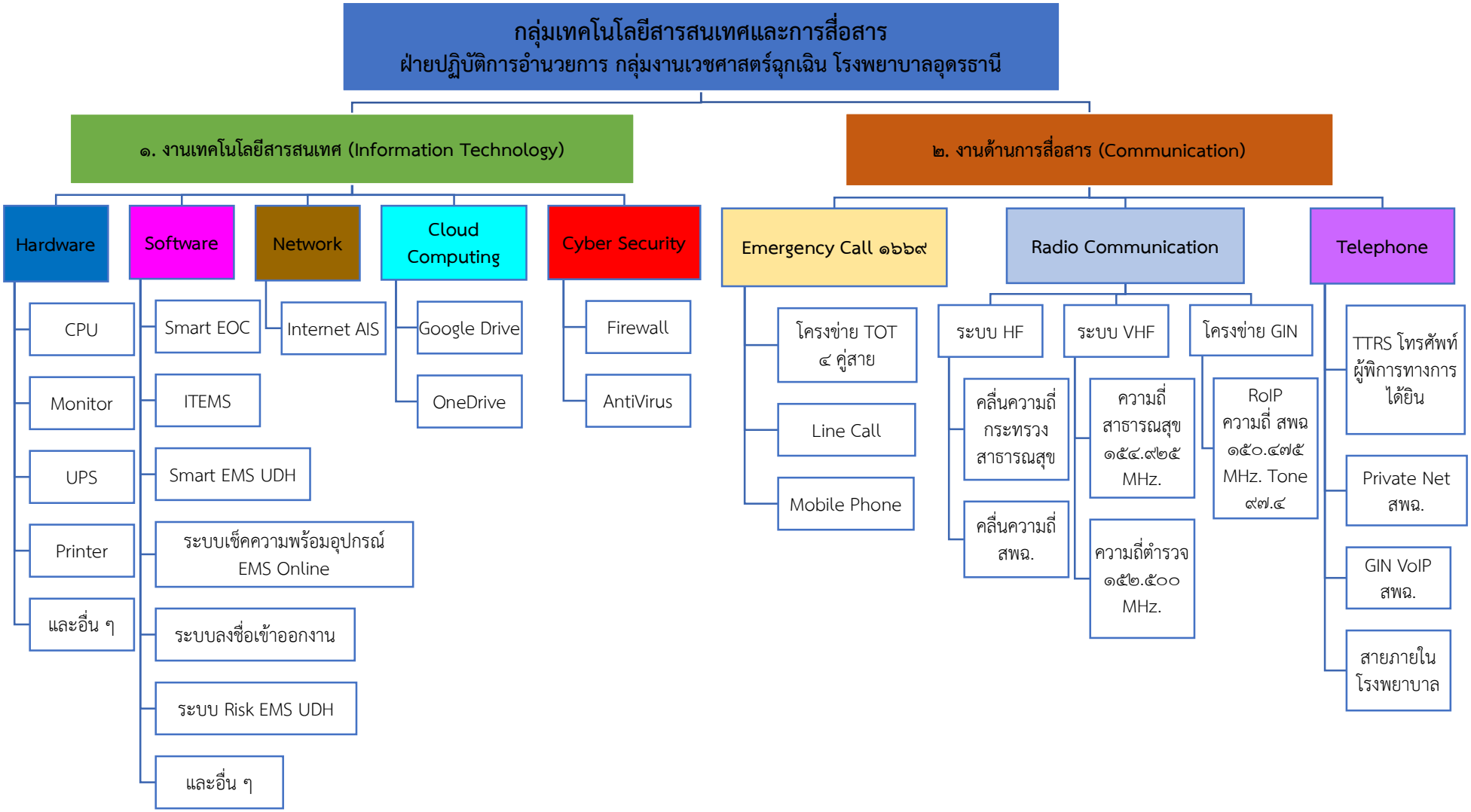
๔. จัดหาให้ได้มาซึ่งระบบเครือข่ายคอมพิวเตอร์ อุปกรณ์ต่อพ่วงและอุปกรณ์การสื่อสาร

๕. ดูแลโครงข่ายการสื่อสารของระบบการแพทย์ฉุกเฉินจังหวัดอุดรธานี

๖. ควบคุมการใช้ระบบเทคโนโลยีสารสนเทศให้เป็นไปตามนโยบายหรือระเบียบของกลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานีและตามกฎหมาย

๗. ติดตามและประเมินผลการพัฒนาเพื่อการจัดหาระบบเครือข่ายคอมพิวเตอร์

๒. ขอบเขตการดำเนินงาน

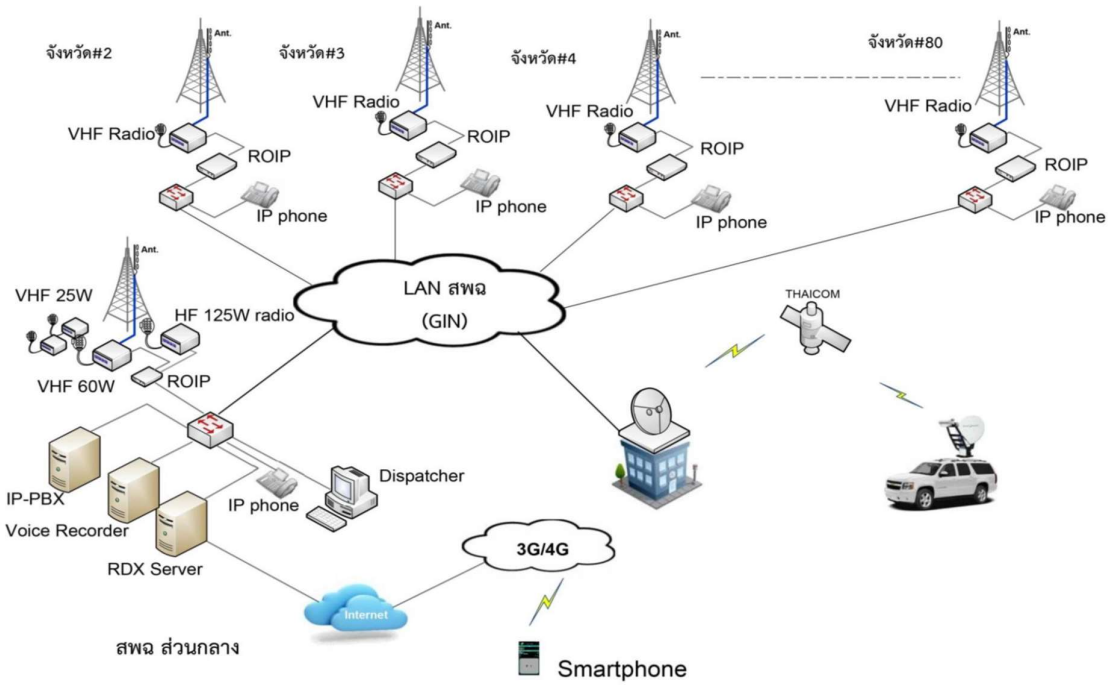


๓. สถานภาพและการบริหารจัดการเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบัน

๓.๑ ระบบเครือข่ายคอมพิวเตอร์และสารสนเทศ

ระบบเครือข่ายคอมพิวเตอร์สารสนเทศและการสื่อสารของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี ประกอบไปด้วย ๒ ส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (Wire Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายที่ใช้สาย (Wire Network) เป็นการใช้บริการจาก ๓ บริษัท ดังนี้

๓.๑.๑ บมจ. กสท. โทรคมนาคม จำกัด (มหาชน) (CAT telecom public company limited) สำหรับใช้ในโครงการ GIN (Government Information Network) คือ ระบบเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ โดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.) ร่วมกับสถาบันการแพทย์ฉุกเฉินแห่งชาติ (สพฉ.) เพื่อบูรณาการเครือข่ายสื่อสารข้อมูลให้เชื่อมโยงถึงกันอย่างเป็นรูปธรรม สะดวก รวดเร็ว และมีความมั่นคงปลอดภัยสูง อีกทั้งเพื่อลดระยะเวลา ลดต้นทุนต่อหน่วยและลดความซ้ำซ้อนในการใช้งบประมาณ และยังมีการตรวจติดตามการให้บริการเครือข่าย (Monitoring) อย่างต่อเนื่อง โดยมีแผนดำเนินงานในระบบ GIN – Voice Over IP ระบบ GIN – ITEMS และระบบ GIN – Radio over IP Gateway (RoIP) คือ ระบบวิทยุสื่อสารและโครงข่ายการสื่อสารโทรคมนาคมสำหรับการแพทย์ฉุกเฉินเพื่อรองรับภาวะวิกฤติของประเทศ



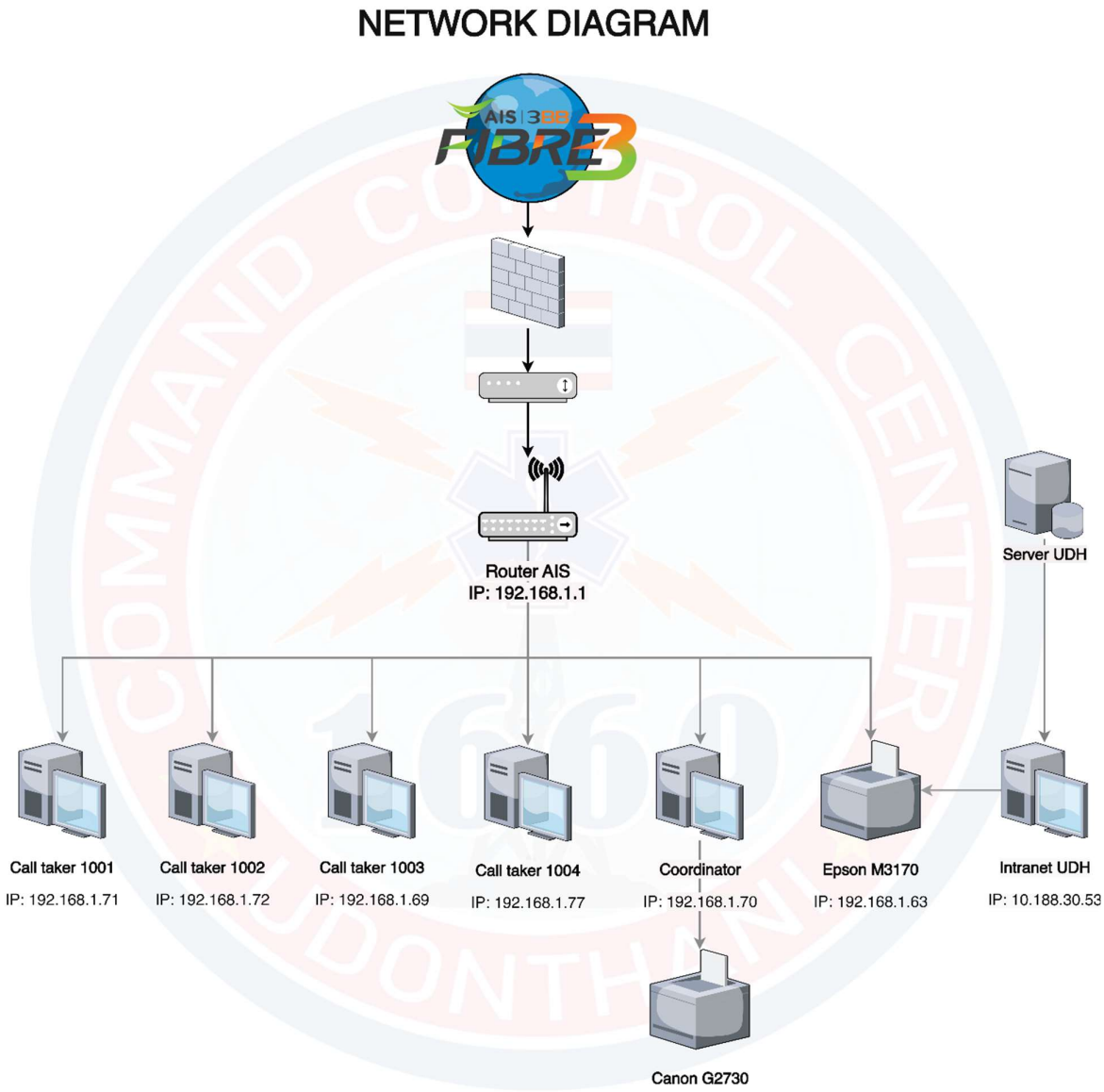
ภาพ ระบบโครงข่าย GIN

๓.๑.๒ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT) เป็นผู้ให้บริการหลักในระบบการสื่อสารของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี ในการรับแจ้งเหตุการเจ็บป่วยฉุกเฉินผ่านโทรศัพท์สายด่วน ๑๖๖๙ โดยมีหมายเลขโทรศัพท์พื้นฐาน ๔ หมายเลข ได้แก่ (๑) ๐๔๒-๒๒๑-๖๙๕, (๒) ๐๔๒-๒๒๓-๗๐๒, (๓) ๐๔๒-๒๒๑-๗๓๕, (๔) ๐๔๒-๒๒๑-๘๒๑

ภาพ ระบบการสื่อสารของโทรศัพท์สายด่วน ๑๖๖๙ อุดรธานี

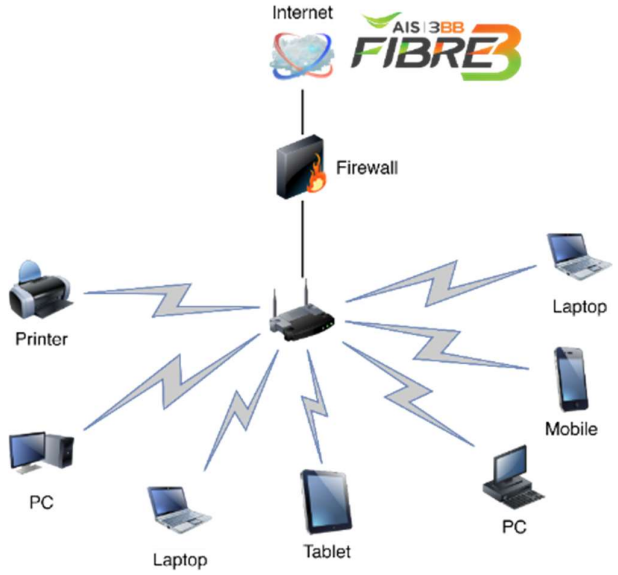
๓.๑.๓ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) เป็นผู้ให้บริการอินเตอร์ (Internet service provider: ISP) ของกลุ่มงานเวชศาสตร์ฉุกเฉิน โดยใช้บริการ ๒ ระบบร่วมกัน ทั้งเครือข่ายที่ใช้สาย (Wire Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดย

๓.๑.๓.๑ เครือข่ายใช้สาย (Wire Network) มีลักษณะคล้ายคลึงกันกับการเชื่อมต่อระบบเครือข่ายจากผู้ให้บริการอินเทอร์เน็ตมายังอุปกรณ์ควบคุม เส้นทางในระบบเครือข่ายของศูนย์ (Router) และเชื่อมต่อไปยังอุปกรณ์ป้องกันการบุกรุก (Firewall) แล้วต่อเข้าอุปกรณ์เครือข่ายหลักของศูนย์ ฯ (Core Switch) ก่อนจะกระจายไปยังส่วนงานต่าง ๆ ภายในกลุ่มงาน



ภาพ ระบบเครือข่ายใช้สาย (Wire Network) ของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี

๓.๑.๓.๒ ระบบเครือข่ายไร้สาย (Wireless Network) โดยผู้ให้บริการอินเทอร์เน็ตเช่นเดียวกับระบบใช้สาย (Wire Network) และมีการควบคุมสิทธิในการใช้งานระบบเครือข่ายไร้สาย



ภาพ ระบบเครือข่ายไร้สาย (Wireless Network) ของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี

๓.๒ ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง เครื่องโทรศัพท์ เครื่องวิทยุคมนาคม และอื่น ๆ

สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ ที่กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานีใช้ในการดำเนินงานปัจจุบัน จะมีการสำรวจสภาพความพร้อมใช้และแผนในการจัดหาทดแทนประจำทุกปี โดยข้อมูลปีงบประมาณ ๒๕๖๗ มีรายละเอียดดังตารางต่อไปนี้

ลำดับ	รายการ	จำนวน (เครื่อง)	หมายเหตุ
๑.	เครื่องคอมพิวเตอร์ PC	๖	
๒.	เครื่องคอมพิวเตอร์โน๊ตบุ๊ก	-	
๓.	เครื่องมินิคอมพิวเตอร์	๑	
๔.	จอแสดงภาพ (Monitor)	๑๑	
๕.	เครื่องพิมพ์ชนิดฉีดหมึก (Inkjet Printer)	๒	
๖.	เครื่องสำรองไฟฟ้า (UPS)	๓	
๗	โทรศัพท์ IP Phone	๔	
๘	โทรศัพท์ IP Phone สำหรับ VoIP (สพฉ.)	๒	
๙	โทรศัพท์มีจอภาพ IP Video Phone (สำหรับผู้พิการทางการได้ยิน)	๑	
๑๐	โทรศัพท์พื้นฐานแบบไร้สาย	๒	
๑๑	โทรศัพท์มือถือ	๒	
๑๒	IPAD	๑	
๑๓	วิทยุคมนาคม ชนิดประจำที่ ระบบ HF (SSB)	๑	
๑๔	วิทยุคมนาคม ชนิดประจำที่ ระบบ VHF สังเคราะห์ความถี่ประเภท ๒	๒	

ลำดับ	รายการ	จำนวน (เครื่อง)	หมายเหตุ
๑๕	วิทยุคมนาคม ชนิดมือถือ ระบบ VHF	๑๐	
๑๖	วิทยุคมนาคม ชนิดประจำที่ ระบบ VHF (RoIP)	๑	
๑๗	เครื่องชุมสายโทรศัพท์ (ตู้สาขา) IP-PABX	๑	
๑๘	อุปกรณ์จัดเก็บข้อมูล NAS (Network Attach Storage)	๑	
๑๙	อุปกรณ์ Network Switches	๑	

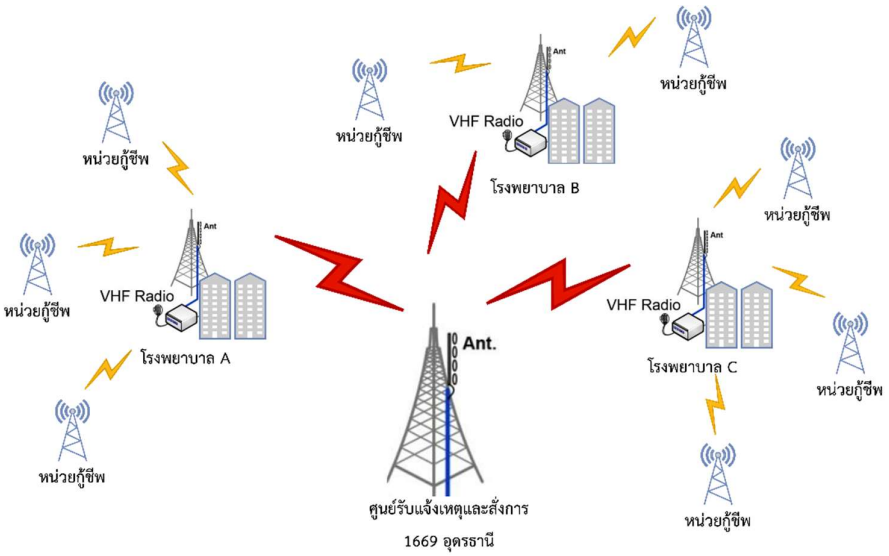
มีระบบเทคโนโลยีสารสนเทศที่จำเป็นต่อการปฏิบัติการฉุกเฉินและเชื่อมต่อการรับ-ส่งคำสั่ง หรือ ข้อมูลกับหน่วยปฏิบัติการ โดยมีโครงสร้างพื้นฐานด้านเทคโนโลยีสานสนเทศสำหรับสนับสนุนการรับแจ้งเหตุเจ็บป่วยฉุกเฉิน ระบบจ่ายงาน ประสานปฏิบัติการฉุกเฉิน โดยมีโปรแกรมพื้นฐานที่จำเป็น ดังนี้

ลำดับ	รายการ	จำนวน (เครื่อง)	หมายเหตุ
๑. ระบบปฏิบัติการ			
๑.	โปรแกรมระบบปฏิบัติการ Microsoft Windows ๑๑	๒	
๒.	โปรแกรมระบบปฏิบัติการ Microsoft Windows ๑๐	-	
๓.	โปรแกรมระบบปฏิบัติการ Microsoft Windows ๗	๔	
๒. ระบบ Document Management			
๑	Microsoft Office	๕	
๒	Acrobat Reader	๓	
๓. Web Browser			
๑	Google Chrome (Version ล่าสุด)	๖	
๒	Microsoft Edge	๖	
๔. Digital EMS ๑๖๖๙ Service			
๑	Operation Information System (OIS)	-	
๒	Communication Information System (CIS)	-	
๓	Medical Information System (MIS)	-	
๔	โปรแกรมบันทึกเสียงการสนทนาผ่านสายด่วน ๑๖๖๙	๑	
๕. Smart EMS UDH			
๑	ระบบการรับแจ้งเหตุออนไลน์ ผ่าน Google From	๑	
๒	ระบบการสั่งการ ฯ ออนไลน์ พร้อมแจ้งเตือนผ่าน Line Notify	๑	
๓	ระบบตรวจสอบความพร้อมอุปกรณ์ในรถกู้ชีพออนไลน์ พร้อมแจ้ง	๑	
	ผ่านเตือนผ่าน Line Nortify		
๔	ระบบลงบันทึกความเสี่ยงออนไลน์ พร้อมแจ้งเตือนผ่าน Line Nortify	๑	
๕	ระบบทดสอบสัญญาณความชัดเจนของวิทยุสื่อสารออนไลน์	๑	
๖	ระบบลงเวลาเข้า-ออกงานออนไลน์ผ่าน QR Code พร้อมแจ้งเตือน	๑	
	ผ่าน Line Nortify และคำนวณเวลาและยอดเงินมาสายให้อัตโนมัติ		

๓.๓ ระบบโครงข่ายการสื่อสารผ่านวิทยุคมนาคมการแพทย์ฉุกเฉิน

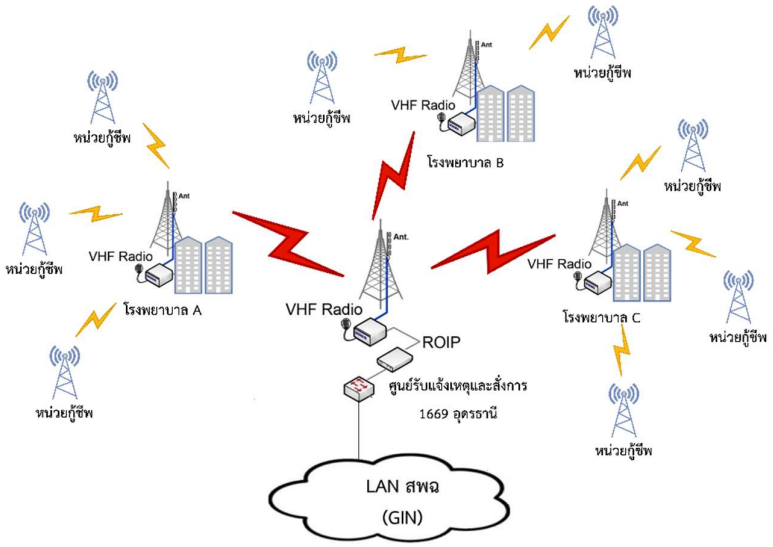
ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี ได้จัดตั้งสถานีวิทยุคมนาคมโครงข่ายสื่อสารการแพทย์ฉุกเฉินขึ้นจำนวน ๓ สถานี ได้แก่

๓.๓.๑ สถานีวิทยุคมนาคมโครงข่ายสื่อสารการแพทย์ฉุกเฉินของกระทรวงสาธารณสุข ระบบ VHF/FM คลื่นความถี่ ๑๕๔.๙๒๕ MHz. ที่ได้รับการจัดสรรจาก กสทช. โดยใช้สายนำสัญญาณ Coaxail รุ่น RG ๕๘ U ใช้สายอากาศชนิดประจำที่แบบแพร่กระจายรอบทิศทาง (Omnidirectional) ย่านความถี่ ๑๕๐-๑๖๐ MHz. แบบไดโพล ๘ ห่วง จำนวน ๒ แผง ในทิศทางตะวันออกเฉียงใต้กับทิศตะวันตกเฉียงเหนือ ติดตั้งบนเสาทาวเวอร์ความสูง ๓๐ เมตร บนชั้นดาดฟ้าตึกอำนวยการโรงพยาบาลอุดรธานี ใช้เครื่องวิทยุคมนาคมชนิดประจำที่ กำลังส่ง ๕๐ วัตต์ ยี่ห้อ Icom รุ่น IC-F๕๑๓๐D ในการติดต่อประสานงานกับเครือข่ายการแพทย์ฉุกเฉินจังหวัดอุดรธานี ตลอด ๒๔ ชั่วโมง



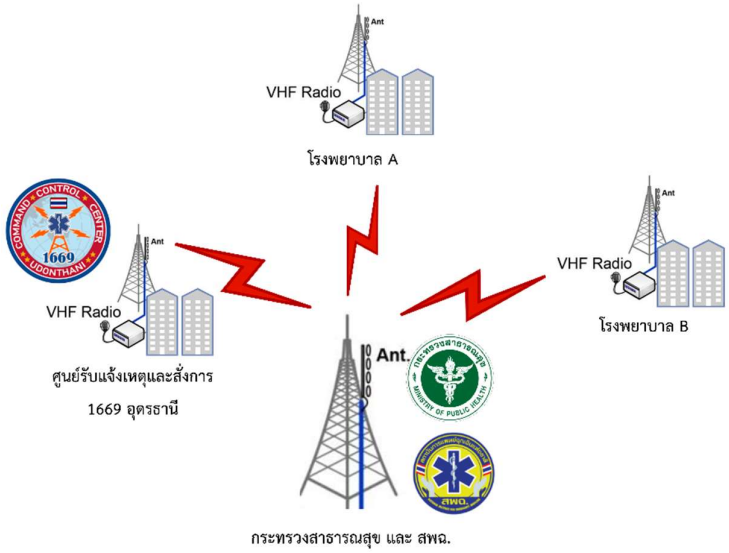
ภาพ โครงข่ายการสื่อสารผ่านวิทยุคมนาคม ระบบ VHF/FM คลื่นความถี่ ๑๕๔.๙๒๕ MHz. ของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี

๓.๓.๒ สถานีวิทยุคมนาคมโครงข่ายสื่อสารการแพทย์ฉุกเฉินของสถาบันการแพทย์ฉุกเฉินแห่งชาติ (สพฉ.) ระบบ VHF/FM ได้กำหนดให้ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี ใช้คลื่นความถี่ ๑๕๐.๔๗๕ MHz. ความถี่ย่อย (Tone) ๙๗.๔ ที่ได้รับการจัดสรรจาก กสทช. เพื่อใช้ในการติดต่อประสานงานเครือข่ายการแพทย์ฉุกเฉินพื้นที่จังหวัดอุดรธานี โดยใช้สายนำสัญญาณ Coaxail รุ่น RG ๕๘ U ใช้สายอากาศชนิดประจำที่แบบแพร่กระจายรอบทิศทาง (Omnidirectional) ย่านความถี่ ๑๕๐-๑๖๐ MHz. แบบไดโพล ๔ ห่วง จำนวน ๑ แผง ในทิศทางตะวันออกเฉียงใต้ ติดตั้งบนเสาทาวเวอร์ความสูง ๓๐ เมตร บนชั้นดาดฟ้าตึกอำนวยการโรงพยาบาลอุดรธานี ใช้เครื่องวิทยุคมนาคม ชนิดทวนสัญญาณแบบดิจิตอล กำลังส่ง ๖๐ วัตต์ ยี่ห้อ Icom รุ่น IC-FR๕๑๐๐H ต่อกับ Radio Over IP Gateway ยี่ห้อ Icom รุ่น VE-PG๓ ทำให้สามารถรับ-ส่งข้อมูลข่าวสารจากผู้บัญชาการเหตุการณ์ในส่วนกลาง (กทม.) สามารถสั่งการถึงผู้ปฏิบัติการในพื้นที่จังหวัดอุดรธานีได้โดยตรงผ่านโครงข่ายสายสัญญาณ GIN (Government Information Network) (RoIP) เพื่อเตรียมพร้อมรับสถานการณ์ฉุกเฉินหรือภัยพิบัติและสามารถติดต่อสื่อสารได้ตลอด ๒๔ ชม.



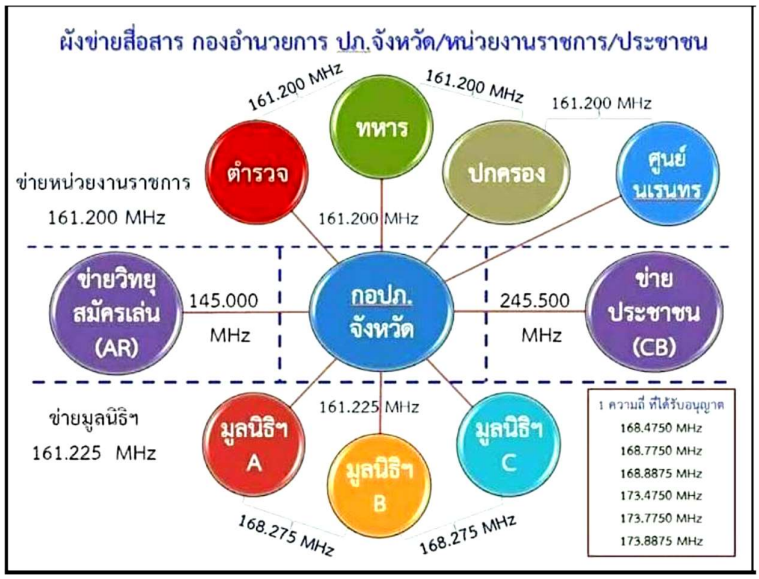
ภาพ โครงข่ายการสื่อสารผ่านวิทยุคมนาคม ระบบ VHF/FM คลื่นความถี่ ๑๕๐.๔๗๕ MHz.
ของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี

๓.๓.๓ สถานีวิทยุคมนาคมโครงข่ายสื่อสารการแพทย์ฉุกเฉินของกระทรวงสาธารณสุข ระบบ HF/AM (Single side-band) คลื่นความถี่ ๗.๖๔๕ MHz. ที่ได้รับการจัดสรรจาก กสทช. โดยใช้สายนำสัญญาณ Coaxail รุ่น RG ๕๘ U ใช้สายอากาศชนิดประจำที่แบบ Half-wave dipole antenna จำนวน ๑ ชุด ในทิศทางตะวันออกกับทิศตะวันตก ติดตั้งบนเสาความสูง ๑๐ เมตร บนชั้นดาดฟ้าตึกอำนวยการโรงพยาบาลอุดรธานี ใช้เครื่องวิทยุคมนาคมชนิดประจำที่ กำลังส่ง ๒๕ วัตต์ ยี่ห้อ KENWOOD (HF SSB RADIO TELEPHONE) รุ่น TRC-๘๐T โดยทำการทดสอบสัญญาณความชัดเจนในวันทำการ เวลา ๐๘.๓๐ น. กับสถานีควบคุมข่ายสื่อสาร “ศูนย์พญาไท” และเวลา ๑๗.๐๐ น. ทดสอบ ฯ กับ “ศูนย์นเรนทร”



ภาพ โครงข่ายการสื่อสารผ่านวิทยุคมนาคม ระบบ HF SSB คลื่นความถี่ ๗.๖๔๕ MHz.
ของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี

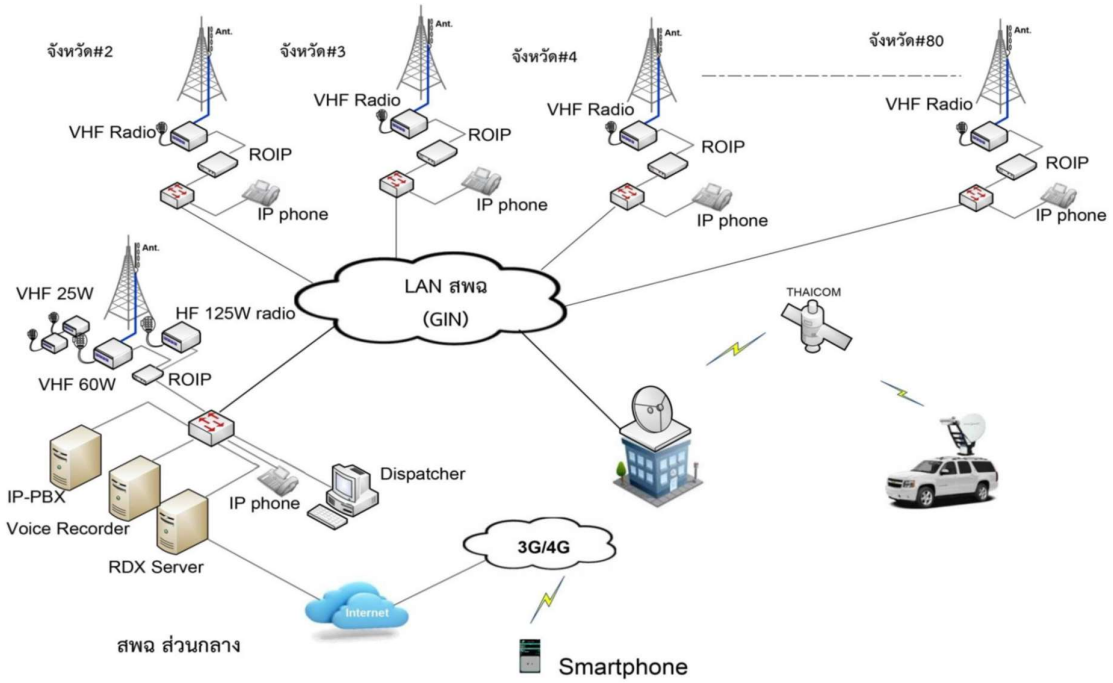
๓.๓.๔ สถานีวิทยุคมนาคมสำหรับเตรียมพร้อม/เฝ้าฟังความถี่ ระบบ VHF/FM คลื่นความถี่ ๑๖๑.๒๐๐ MHz. ที่ กสทช. จัดสรรให้กรมป้องกันและบรรเทาสาธารณภัยเป็นแม่ข่ายหลักใช้เป็นคลื่นความถี่กลาง เป็นช่องเรียกขานและแจ้งเหตุฉุกเฉินและใช้สำหรับติดต่อประสานงานระหว่างหน่วยงานภาครัฐ ทั้งนี้ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี ได้ตั้งสถานีวิทยุคมนาคมดังกล่าวขึ้นเพื่อเป็นการเพิ่มช่องทางรับแจ้งข้อมูลข่าวสารการเจ็บป่วยฉุกเฉินและเหตุการณ์ฉุกเฉินต่าง ๆ ในพื้นที่ และเพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินและภัยพิบัติที่อาจจะเกิดขึ้นในอนาคต โดยใช้อุปกรณ์สายนำสัญญาณ Coaxail รุ่น RG ๑๑ A/U ใช้สายอากาศชนิดประจำที่แบบแพร่กระจายรอบทิศทาง (Omnidirectional) ย่านความถี่ ๑๖๐-๑๗๐ MHz. แบบไดโพล ๔ ห่วง จำนวน ๑ แผง ในทิศทางตะวันตกเฉียงเหนือ ติดตั้งบนเสาทาวน์เวอร์ความสูง ๑๕ เมตร บนชั้นดาดฟ้าตึกอำนวยการโรงพยาบาลอุดรธานี ใช้เครื่องวิทยุคมนาคมชนิดประจำที่ กำลังส่ง ๕๐ วัตต์ ยี่ห้อ Icom รุ่น IC-F๕๑๓๐D ในการให้บริการตลอด ๒๔ ชม.



ภาพ โครงข่ายการสื่อสารผ่านวิทยุคมนาคม ระบบ VHF/FM คลื่นความถี่ ๑๖๑.๒๐๐ MHz. ความถี่กลางใช้เรียกขานและการติดต่อประสานงานระหว่างหน่วยงานภาครัฐ

๓.๔ ระบบโครงข่ายการสื่อสารผ่านโทรศัพท์

๓.๔.๑ ระบบโทรศัพท์ VoIP (Voice over IP) เป็นการสื่อสารผ่านสายแลนเพื่อเชื่อมต่อข้อมูลระหว่างผู้ส่งและผู้รับที่อยู่บนบนเครือข่ายอินเตอร์เน็ต โดยใช้หมายเลข IP Address เป็นตัวอ้างอิงเพื่อกำหนดหมายเลขของเครื่องและใช้โทรศัพท์ IP Phone เป็นเครื่องมือสื่อสารทำให้สัญญาณมีคุณภาพดี เชื่อมโยงผ่านโครงข่ายอินเตอร์เน็ตโครงการ GIN (Government Information Network) คือ ระบบเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ โดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.) ร่วมกับสถาบันการแพทย์ฉุกเฉินแห่งชาติ (สพฉ.) เพื่อบูรณาการเครือข่ายสื่อสารข้อมูลให้เชื่อมโยงถึงกันอย่างเป็นรูปธรรม สะดวก รวดเร็ว และมีความมั่นคงปลอดภัยสูง อีกทั้งเพื่อลดระยะเวลา ลดต้นทุนต่อหน่วยและลดความซ้ำซ้อนในการใช้งบประมาณ และยังมีการตรวจติดตามการให้บริการเครือข่าย (Monitoring) อย่างต่อเนื่อง โดยศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี ได้รับการติดตั้งระบบ GIN – Voice Over IP เครือข่ายของ สพฉ. จำนวน ๒ ระบบ ได้รับหมายเลขในการติดต่อ คือ หมายเลข ๒๓๔๗ และหมายเลข ๖๔๐๕



ภาพ ระบบโทรศัพท์ VoIP โครงข่าย GIN

๓.๔.๒ ระบบ TTRS (Thai Telecommunication Relay Service) คือ ระบบที่ผู้บกพร่องทางการได้ยินเมื่อเกิดเหตุเจ็บป่วยฉุกเฉินสามารถแจ้งขอความช่วยเหลือได้โดยใช้แอพลิเคชั่น หรือ สื่อสารผ่านตู้ TTRS ที่มีมากกว่า ๑๒๐ ตู้ทั่วประเทศ โดยใช้ภาษามือสื่อสารกับเจ้าหน้าที่ TTRS ผ่านวีดีโอคอล ซึ่งให้บริการตลอด ๒๔ ชม. และจะมีการประสานงานต่อมายังศูนย์รับแจ้งเหตุแต่ละจังหวัด เพื่อสอบถามประวัติอาการและตำแหน่งที่เกิดเหตุรวมไปถึงการให้คำแนะนำในการปฐมพยาบาลเบื้องต้นก่อนที่ทีมปฏิบัติการฉุกเฉินจะไปถึง ซึ่งจะเป็นการสนทนาพร้อมกัน ๓ สาย ระหว่างผู้ป่วย ล่าม TTRS และเจ้าหน้าที่ประจำศูนย์รับแจ้งเหตุและสั่งการ ฯ โดยศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี ได้รับการติดตั้งชุดอุปกรณ์ดังกล่าวจำนวน ๑ ชุด หมายเลข ๐๒๐๒๖๐๐๒๑ เพื่อใช้ในภารกิจดังกล่าว

๓.๔.๓ ระบบโทรศัพท์ภายในโรงพยาบาลอุดรธานี โดยศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี ได้รับการจัดสรรหมายเลขโทรศัพท์ภายในของโรงพยาบาลอุดรธานีจำนวน ๑ หมายเลข คือ หมายเลข ๓๑๒๔ เพื่อใช้ในการติดต่อประสานงานทั่วไปภายในโรงพยาบาล ติดต่อประสานงานห้องอุบัติเหตุและฉุกเฉินและศูนย์เปลในการเตรียมพร้อมรับผู้ป่วยวิกฤติ ติดต่อประสานงานแพทย์อำนวยการปฏิบัติการฉุกเฉิน (พอป.) เพื่อรายงานเหตุการณ์ต่าง ๆ เป็นต้น

รายชื่อโรงพยาบาลและหน่วยปฏิบัติการ EMS
ในเขตอำเภอเมืองอุดรธานี

หน่วยงาน	สายตรง	หมายเลขอื่นๆ
๑. รพ.อุดรธานี	๑๖๖๙	๐๔๒-๒๔๕-๕๕๕
๒. รพ.ค่ายประจักษ์	๐๔๒-๙๓๐-๓๐๒ ต่อ ๒๗๓๔๐	๐๔๒-๓๔๒-๘๖๓
๓. รพ.กรุงเทพ-อุดร	๐๔๒-๔๓๔-๔๔๔	๑๗๑๙
๔. รพ.วัฒนา	๐๔๒-๒๑๙-๔๙๐	๐๔๒-๓๒๕-๕๐๙
๕. รพ.เอกอุดร	๐๔๒-๓๔๑-๕๕๕	-
๖. รพ.ศูนย์มะเร็ง	๐๔๒-๒๐๗-๓๘๐	-
๗. รพ.กองบิน ๒๓	๐๔๒-๙๓๐-๑๑๙	๐๔๒-๓๔๕-๑๒๑
๘. รพ.ธัญญารักษ์	๐๔๒-๒๙๕-๗๕๖	-
๙. มูลนิธิเมธาธรรม	๐๔๒-๒๔๕-๔๖๓	-
๑๐. มูลนิธิส่งเสริมธรรม	๐๔๒-๒๒๑-๖๙๕	-
๑๑. ทน.อุดรธานี	๐๘๓-๔๐๓-๕๘๙๕	-
๑๒. ทม.หนองสำโรง	๐๔๒-๒๓๐-๑๓๕	-
๑๓. ทม.โนนสูง-น้ำคำ	๐๔๒-๑๑๓-๒๗๑	-
๑๔. ทต.นาข่า	๐๔๒-๒๑๘-๐๒๓ ต่อ ๗๖	-
๑๕. ทต.นิคมสงเคราะห์	๐๔๒-๒๓๗-๐๙๖	-
๑๖. ทต.บ้านตาด	๐๔๒-๑๒๐-๔๒๙ ต่อ ๒๓	-
๑๗. ทต.หนองไผ่	๐๘๒-๓๐๙-๙๙๗๙	-
๑๘. อบต.บ้านขาว	๐๔๒-๒๑๘-๒๑๓	๐๘๗-๙๔๔-๐๓๖๖
๑๙. อบต.นาดี	๐๔๒-๑๑๐-๑๕๑	-
๒๐. อบต.หนองไฮ	๐๘๑-๗๖๙-๘๗๑๑	-
๒๑. อบต.หนองนาคำ	๐๔๒-๒๙๐-๒๑๕	๐๘๑-๖๗๐-๒๒๑๑
๒๒. อบต.สามพร้าว	๐๔๒-๓๔๙-๑๙๐	-

หมายเลขโทรศัพท์โรงพยาบาลแม่ข่าย EMS ในเขตจังหวัดอุดรธานี

หน่วยงาน	สายตรง ER	โทรศัพท์มือถือ
๑. รพ.กุดจับ	๐๔๒-๒๙๑-๓๒๑-๓ ต่อ ๑๐๔	๐๙๑-๐๕๖-๓๔๕๗
๒. รพ.กุมภวาปี	๐๔๒-๓๓๔-๔๐๖	๐๘๒-๓๐๕-๖๖๑๐
๓. รพ.ห้วยเกิ้ง	๐๔๒-๓๙๘-๔๐๖ ต่อ ๑๑๖	๐๘๘-๓๓๘-๒๖๘๘
๔. รพ.กู่แก้ว	๐๔๒-๒๕๖-๑๘๑ ต่อ ๑๑๑	๐๙๓-๓๒๕-๓๑๔๑
๕. รพ.ไชยวาน	๐๔๒-๒๖๕-๓๓๑ ต่อ ๑๐๖	๐๙๕-๖๖๓-๒๙๒๙
๖. รพ.ทุ่งฝน	๐๔๒-๒๖๘-๐๕๑ ต่อ ๑๑๑	๐๘๗-๘๕๓-๙๒๙๒
๗. รพ.นายูง	๐๔๒-๑๕๐-๐๗๓	๐๙๔-๙๐๒-๔๒๒๒
๘. รพ.น้ำโสม	๐๔๒-๒๘๗-๓๐๖	๐๘๕-๔๖๑-๔๑๘๔
๙. รพ.โนนสะอาด	๐๔๒-๓๙๒-๓๗๗	๐๘๓-๔๔๖-๒๐๙๒
๑๐. รพ.บ้านดุง	๐๔๒-๒๗๓-๗๗๗	๐๘๘-๓๑๔-๙๔๐๙
๑๑. รพ.บ้านผือ	๐๔๒-๒๘๑-๒๙๐	-
๑๒. รพ.ประจักษ์ศิลปาคม	๐๔๒-๓๓๕-๑๒๐ ต่อ ๑๑๑	๐๖๑-๖๙๔-๐๖๖๖
๑๓. รพ.พิบูลย์รักษ์	๐๔๒-๒๕๘-๑๑๑ ต่อ ๑๐๔	๐๘๕-๔๖๕-๐๘๘๐
๑๔. รพ.เพ็ญ	๐๔๒-๒๗๘-๕๗๒	๐๘๔-๗๙๐-๔๑๑๔
๑๕. รพ.วังสามหมอ	๐๔๒-๓๘๗-๖๐๒ ต่อ ๑๐๖	๐๘๙-๙๔๑-๘๗๗๘
๑๖. รพ.ศรีธาตุ	๐๘๘-๕๖๑-๗๒๓๓	๐๘๔-๗๙๗-๕๐๘๔
๑๗. รพ.สร้างคอม	๐๔๒-๒๗๖-๔๕๐	-
๑๘. รพ.หนองวัวซอ	๐๔๒-๒๘๖-๐๓๐	๐๘๗-๖๔๐-๙๗๙๙
๑๙. รพ.หนองแสง	๐๔๒-๓๙๖-๑๘๑	๐๙๑-๐๖๐-๕๓๔๙
๒๐. รพ.หนองหาน	๐๔๒-๒๖๑-๒๔๘	-

หมายเลขโทรศัพท์ภายใน โรงพยาบาลอุดรธานี

หน่วยงาน	โทรศัพท์ ๑	โทรศัพท์ ๒
๑. ห้องฉุกเฉิน (ER)	๓๑๒๕	๓๑๒๖
๒. ห้องสังเกตอาการ	๑๑๔๑	-
๓. จุดคัดกรอง ER	๑๔๒๔	-
๔. ศูนย์ส่งต่อ (Refer)	๓๑๑๕/๑๑๔๓	๐๔๒-๒๔๘-๒๖๑
๕. ศูนย์เปล	๑๑๓๕	-

หมายเลขโทรศัพท์ศูนย์สั่งการ ฯ จังหวัดใกล้เคียง

หน่วยงาน	ความถี่วิทยุ	โทรศัพท์ ๑	IP Phone ๑	IP Phone ๒
๑. ศูนย์สั่งการ ฯ สพฉ.	๑๕๐.๔๗๕	๐๒-๘๗๒-๑๖๖๙	๒๑๐๑	๖๑๐๑
๒. ศูนย์สั่งการ ฯ อุดรธานี	๑๕๔.๙๒๕	๐๔๒-๒๒๓-๗๐๒	๒๔๓๗	๖๔๐๕
๓. ศูนย์สั่งการ ฯ เลย	๑๕๔.๙๒๕	๐๔๒-๘๖๒-๑๓๖	๒๔๐๑	๖๔๐๑
๔. ศูนย์สั่งการ ฯ หนองบัวลำภู	๑๕๒.๒๕๐	๐๔๒-๓๑๓-๒๓๘	๒๔๓๓	๖๔๓๓
๕. ศูนย์สั่งการ ฯ หนองคาย	๑๕๕.๗๒๕	๐๔๒-๔๒๒-๕๘๖	๒๔๓๑	๖๔๓๑
๖. ศูนย์สั่งการ ฯ สกลนคร	๑๕๕.๔๗๕	๐๔๒-๙๗๐-๕๐๖	๒๔๒๗	๖๔๒๗
๗. ศูนย์สั่งการ ฯ บึงกาฬ	๑๕๔.๙๒๕	๐๔๒-๔๙๑-๙๐๐	๒๔๑๓	๖๔๑๓
๘. ศูนย์สั่งการ ฯ นครพนม	๑๕๔.๙๗๕	๐๔๒-๕๑๓-๑๘๐	๒๔๐๙	๖๔๐๙
๙. ศูนย์สั่งการ ฯ ขอนแก่น	๑๕๕.๖๗๕	๐๔๓-๒๓๐-๑๙๒	๒๔๐๕	๖๔๓๗
๑๐. ศูนย์สั่งการ ฯ กาฬสินธุ์	๑๕๕.๗๗๕	๐๔๓-๘๑๖-๕๐๐	๒๔๐๓	๖๔๐๓

หมายเลขสายด่วนอื่นๆ

หน่วยงาน	สายด่วน	โทรศัพท์ใน จ.อุดรธานี
๑. ตำรวจ	๑๙๑	-
๑.๑ สภ.เมืองอุดรธานี	๑๙๑	๐๔๒-๒๒๑-๐๗๗
๑.๒ สภ.นาข่า	๑๙๑	๐๔๒-๒๑๘-๒๔๕
๑.๓ สภ.โนนสูง	๑๙๑	๐๔๒-๒๐๗-๔๖๓
๑.๔ สภ.ห้วยหลวง	๑๙๑	๐๔๒-๑๑๑-๔๖๗
๒. ดับเพลิง	๑๙๙	๐๔๒-๒๔๔-๙๘๙
๓. กรมป้องกันและบรรเทาสาธารณภัย	๑๗๘๔	๐๔๒-๒๔๖-๓๒๙
๔. คุ้มครองคนไร้ที่พึ่ง/คนไร้บ้าน	๑๓๐๐	๐๔๒-๒๒๑-๗๗๓
๕. บัตรทอง	๑๓๓๐	๐๔๒-๓๒๕-๖๘๑
๖. สายด่วนสุขภาพจิต	๑๓๒๓	๑๖๖๗
๗. บำบัดยาเสพติด	๑๑๖๕	-
๘. ท้องไม่พร้อม/เอดส์	๑๖๖๓	-
๙. บริจาคอวัยวะ สภากาชาดไทย	๑๖๖๖	-
๑๐. การไฟฟ้าส่วนภูมิภาค	๑๑๒๙	-
๑๑. การประปาส่วนภูมิภาค	๑๖๖๒	-
๑๒. กรมส่งเสริมการส่งออก	๑๑๖๙	-

๔. ตัวชี้วัดด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ตัวชี้วัดที่ ๑ : ระดับความสำเร็จของการพัฒนาสารสนเทศและการสื่อสาร และการมีข้อมูลเชิงประจักษ์ด้านประสิทธิผล

คะแนนตัวชี้วัด : ๕ คะแนน

คำอธิบาย : ระดับความสำเร็จของการพัฒนาปรับปรุงสารสนเทศและการสื่อสารรวมกับการมีข้อมูลเชิงประจักษ์ด้านประสิทธิภาพ คือ ถูกต้อง ครบถ้วนและทันเวลา โดยประเมินความสำเร็จจากการดำเนินการพัฒนาปรับปรุงระบบข้อมูลและประสิทธิภาพของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อสนับสนุนการบริหารจัดการของผู้บริหาร สนับสนุนการปฏิบัติงานของบุคลากร จำนวน ๑๐ ข้อ ดังนี้

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศและการสื่อสาร	เกณฑ์การตรวจประเมิน
๑. มีฐานข้อมูลที่ครอบคลุมที่ใช้สนับสนุนการปฏิบัติงาน	☐ มีฐานข้อมูลที่ครอบคลุมอย่างน้อยทุกประเด็น ซึ่งสนับสนุนการปฏิบัติงานได้อย่างเหมาะสม ☐ มีฐานข้อมูลเพื่อการดำเนินงานการบริหารงาน
๒. มีการอัพเดทข้อมูลที่จำเป็นอย่างสม่ำเสมอและทันท่วงที	☐ มีการกำหนดผู้รับผิดชอบในการตรวจสอบรอบของการจัดเก็บข้อมูลแต่ละประเภทให้เป็นไปตามแผนที่กำหนด
๓. มีแนวทาง/มาตรการป้องกันความ เสียหายและมีการสำรองข้อมูลสารสนเทศ (Backup)	☐ มีการสำรองข้อมูลสารสนเทศ (back up) ในระบบ Intranet อย่างน้อย ๒ ครั้ง/สัปดาห์ และในระบบ Internet อย่างน้อย ๑-๒ ครั้ง/เดือน หรือตามความเหมาะสม ซึ่งสามารถพิจารณาจากความสำคัญตามปริมาณงาน Transaction
๔. มีการประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร	☐ มีการประกาศนโยบายและแนวทางการปฏิบัติในการรักษาความปลอดภัย หรือ มีคู่มือแนวทางการปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ
๕. มีการประกาศคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)	☐ มีการประกาศคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice) ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือ แนวทางปฏิบัติด้านความปลอดภัยของข้อมูลส่วนบุคคลของผู้ป่วย
๖. มีระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูลและสารสนเทศ	☐ มีระบบการตรวจสอบการบุกรุกและตรวจสอบความปลอดภัยของเครือข่ายครอบคลุมทุกโฮสต์ (Host) รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง เพื่อป้องกันทรัพยากรระบบสารสนเทศและข้อมูลบนเครือข่าย ☐ มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลที่เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศและการสื่อสาร	เกณฑ์การตรวจประเมิน
๗. มีแผนบริหารความเสี่ยงและแผนรองรับสถานการณ์ฉุกเฉินด้านคอมพิวเตอร์ สารสนเทศและการสื่อสาร	☐ มีแผนบริหารความเสี่ยงด้านคอมพิวเตอร์ สารสนเทศและการสื่อสาร มีกระบวนการที่แสดงถึงการตอบสนองต่อการบุกรุกที่เสี่ยงต่อการทำงานของระบบสารสนเทศและการสื่อสารที่ครอบคลุมถึงการสนับสนุนการปฏิบัติงานได้อย่างต่อเนื่องภายใต้ภาวะวิกฤต (เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว เป็นต้น) เพื่อให้สามารถลดความเสียหายได้อย่างรวดเร็ว รวมถึงการป้องกันเหตุการณ์ที่อาจจะเกิดขึ้นและการดำเนินการตามแผน
๘. มีระบบ Access Right ที่ถูกต้องและทันสมัย	☐ มีการกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสม กับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบ ของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมถึงการเปลี่ยนแปลงหรือยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกพ้นจากตำแหน่งหรือยกเลิกการใช้งานและมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
๙. มีหนังสือรับรองการเข้าร่วมข่ายและการจัดสรรคลื่นวิทยุคมนาคมการแพทย์ฉุกเฉิน	☐ มีหนังสือหรือเอกสารการยื่นแสดงความจำนงค์ขอรับรองการเข้าร่วมเครือข่ายและการจัดสรรคลื่นวิทยุคมนาคม จาก สพฉ. ☐ มีหนังสือรับรองการเข้าร่วมข่ายและการจัดสรรคลื่นวิทยุคมนาคมการแพทย์ฉุกเฉิน จาก สพฉ.
๑๐. มีใบอนุญาตให้ตั้งสถานีวิทยุคมนาคม มีใบอนุญาตให้ “มี” และ “ใช้” เครื่องวิทยุคมนาคมจากสำนักงาน กสทช.	☐ มีใบอนุญาตให้ตั้งสถานีวิทยุคมนาคม จาก กสทช. ☐ มีใบอนุญาตให้ “มี” และ “ใช้” เครื่องวิทยุคมนาคมจากสำนักงาน กสทช.

เกณฑ์การให้คะแนน :

ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
๖๐ - ๖๙ คะแนน	**๗๐ - ๗๙ คะแนน**	**๘๐ - ๘๙ คะแนน**	**๙๐ - ๙๙ คะแนน**	**๑๐๐ คะแนน**
มีข้อมูลเชิงประจักษ์ ๖ ข้อ	มีข้อมูลเชิงประจักษ์ ๗ ข้อ	มีข้อมูลเชิงประจักษ์ ๘ ข้อ	มีข้อมูลเชิงประจักษ์ ๙ ข้อ	มีข้อมูลเชิงประจักษ์ ๑๐ ข้อ

เป้าหมายความสำเร็จของงานในแต่ละรอบการประเมิน :

ระดับขั้นความสำเร็จ	รอบการประเมิน/คะแนนการประเมิน		
	รายการประเมิน (ข้อละ ๑๐ คะแนน)	ระดับคะแนน	
		๖ เดือนแรก	๖ เดือนหลัง
ข้อที่ ๑	มีฐานข้อมูลที่ครอบคลุมที่ใช้สนับสนุนการปฏิบัติงาน	๑๐	
ข้อที่ ๒	มีการอัพเดทข้อมูลที่จำเป็นอย่างสม่ำเสมอและทันท่วงที	๑๐	
ข้อที่ ๓	มีแนวทาง/มาตรการป้องกันความ เสียหายและมีการสำรองข้อมูลสารสนเทศ (Backup)	๑๐	
ข้อที่ ๔	มีการประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร	๑๐	
ข้อที่ ๕	มีระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูลและสารสนเทศ	๑๐	
ข้อที่ ๖	มีแผนบริหารความเสี่ยงและแผนรองรับสถานการณ์ฉุกเฉินด้านคอมพิวเตอร์สารสนเทศและการสื่อสาร	๑๐	
ข้อที่ ๗	มีการประกาศคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)	๑๐	
ข้อที่ ๘	มีระบบ Access Right ที่ถูกต้องและ ทันสมัย	๑๐	
ข้อที่ ๙	มีหนังสือรับรองการเข้าร่วมข่ายและการจัดสรรคลื่นวิทยุคมนาคมการแพทย์ฉุกเฉิน	๐	
ข้อที่ ๑๐	มีใบอนุญาตให้ตั้งสถานีวิทยุคมนาคม มีใบอนุญาตให้ “มี” และ “ใช้” เครื่องวิทยุคมนาคมจากสำนักงาน กสทช.	๐	
	คะแนนรวม	๘๐	

หลักฐานอ้างอิง/แหล่งข้อมูล/วิธีการจัดเก็บข้อมูล :

๑. แหล่งข้อมูล : ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี

๒. วิธีการจัดเก็บข้อมูล : รวบรวมข้อมูลจากการดำเนินงานจริง

ผู้กำกับดูแลตัวชี้วัด : นางสาวนันทรีญา ภูหัดสวน หมายเลขติดต่อ : ๐๖๓-๓๖๘-๖๙๖๖

ผู้จัดเก็บข้อมูล : นายยุทธการณ์ ทุมทอง หมายเลขติดต่อ : ๐๘๕-๗๓๘-๔๒๑๓

: นายธนากร ประจิมทิศ หมายเลขติดต่อ : ๐๘๙-๒๗๕-๑๔๓๘

หน่วยงาน : กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี

ตัวชี้วัดที่ ๒ : **ระดับความพร้อมใช้งาน (Service availability) ของระบบสารสนเทศและการสื่อสาร**

คะแนนตัวชี้วัด : ๕ คะแนน

คำอธิบาย : ระดับความพร้อมใช้งานของระบบสารสนเทศและการสื่อสาร โดยประเมินความสำเร็จจากการดำเนินการสามารถใช้งานและประสิทธิภาพของเครื่องมือและอุปกรณ์ระบบสารสนเทศและการสื่อสารได้ตลอดเวลาอย่างต่อเนื่อง เพื่อสนับสนุนการปฏิบัติงาน จำนวน ๑๐ ข้อ ดังนี้

ข้อมูลเชิงประจักษ์ด้านประสิทธิภาพของระบบสารสนเทศและการสื่อสาร	เกณฑ์การตรวจประเมิน
๑. มีแผนการบำรุงรักษาอุปกรณ์สารสนเทศและระบบการสื่อสาร	☐ มีแผนการดูแล บำรุง รักษาอุปกรณ์สารสนเทศคอมพิวเตอร์และระบบเครือข่าย ☐ มีแผนการดูแลบำรุงรักษาอุปกรณ์เครื่องมือสื่อสาร
๒. มีการตรวจสอบความพร้อมใช้งานของอุปกรณ์สารสนเทศและการสื่อสาร	☐ มีเอกสารการบันทึกการตรวจสอบความพร้อมของอุปกรณ์สารสนเทศและการสื่อสาร
๓. ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบโทรศัพท์สายด่วน ๑๖๖๙	☐ ระยะเวลาที่ไม่สามารถให้บริการได้ (Downtime) ของสายด่วน ๑๖๖๙ น้อยกว่า ๒ ครั้ง/เดือน
๔. ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบอินเตอร์เน็ต AIS ๓BB Fiber	☐ ระยะเวลาที่ไม่สามารถให้บริการได้ (Downtime) ของระบบอินเตอร์เน็ต น้อยกว่า ๒ ครั้ง/เดือน
๕. ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบวิทยุสื่อสารการแพทย์ฉุกเฉิน	☐ ระยะเวลาที่ไม่สามารถให้บริการได้ (Downtime) ของระบบวิทยุสื่อสารการแพทย์ ฯ น้อยกว่า ๒ ครั้ง/เดือน
๖. ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบ GIN ทั้ง VoIP และ RoIP	☐ ระยะเวลาที่ไม่สามารถให้บริการได้ (Downtime) ของระบบ GIN น้อยกว่า ๒ ครั้ง/เดือน
๗. การกู้คืนระบบเมื่อเกิดเหตุฉุกเฉินต่อระบบสารสนเทศและการสื่อสาร	☐ สามารถกู้คืนระบบได้ไม่เกิน ๕ นาที/ครั้ง/เดือน
๘. จำนวนครั้งของการถูกบุกรุกและระดับความปลอดภัยที่ยอมรับได้	☐ จำนวนครั้งของการถูกบุกรุกและระดับความปลอดภัยที่ยอมรับได้ไม่เกิน ๓ ครั้ง/เดือน
๙. ลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการ ต่ออายุลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการ	☐ มีเอกสารหลักฐานแสดงถึงการเข้าถึงลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการ
๑๐. การทดสอบสัญญาณความชัดเจนของระบบโทรศัพท์ VoIP, TTRS, ระบบวิทยุ RoIP, E-radio และระบบเครือข่ายท้องถิ่น	☐ มีเอกสารหรือหลักฐานแสดงถึงการเข้าร่วมทดสอบสัญญาณกับส่วนกลาง เช่น กองสาธารณสุขฉุกเฉิน สพฉ. หรือ TTRS หรือเครือข่ายในท้องถิ่น

เกณฑ์การให้คะแนน :

ระดับ ๑	ระดับ ๒	ระดับ ๓	ระดับ ๔	ระดับ ๕
๖๐ - ๖๙ คะแนน	**๗๐ - ๗๙ คะแนน**	**๘๐ - ๘๙ คะแนน**	**๙๐ - ๙๙ คะแนน**	**๑๐๐ คะแนน**
มีข้อมูลเชิงประจักษ์ ๖ ข้อ	มีข้อมูลเชิงประจักษ์ ๗ ข้อ	มีข้อมูลเชิงประจักษ์ ๘ ข้อ	มีข้อมูลเชิงประจักษ์ ๙ ข้อ	มีข้อมูลเชิงประจักษ์ ๑๐ ข้อ

เป้าหมายความสำเร็จของงานในแต่ละรอบการประเมิน :

ระดับขั้นความสำเร็จ	รอบการประเมิน/คะแนนการประเมิน		
	รายการประเมิน (ข้อละ ๑๐ คะแนน)	ระดับคะแนน	
		๖ เดือนแรก	๖ เดือนหลัง
ข้อที่ ๑	มีแผนการบำรุงรักษาอุปกรณ์สารสนเทศและระบบการสื่อสาร	๗	
ข้อที่ ๒	มีการตรวจสอบความพร้อมใช้งานของอุปกรณ์สารสนเทศและการสื่อสาร	๘	
ข้อที่ ๓	ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบโทรศัพท์สายด่วน ๑๖๖๙	๙	
ข้อที่ ๔	ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบอินเตอร์เน็ต AIS ๓BB Fiber	๘	
ข้อที่ ๕	ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบวิทยุสื่อสารการแพทย์ฉุกเฉิน	๙	
ข้อที่ ๖	ระยะเวลาที่ให้บริการไม่ได้ (Downtime) ของระบบ GIN ทั้ง VoIP และ RoIP	๙	
ข้อที่ ๗	การกู้คืนระบบเมื่อเกิดเหตุฉุกเฉินต่อระบบสารสนเทศและการสื่อสาร	๙	
ข้อที่ ๘	จำนวนครั้งของการถูกบุกรุกและระดับความปลอดภัยที่ยอมรับได้	๙	
ข้อที่ ๙	ลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการ ต่ออายุลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการ	๕	
ข้อที่ ๑๐	การทดสอบสัญญาณความชัดเจนของระบบโทรศัพท์ VoIP, TTRS, ระบบวิทยุ RoIP, E-radio และระบบเครือข่ายท้องถิ่น	๕	
	คะแนนรวม	๗๘	

หลักฐานอ้างอิง/แหล่งข้อมูล/วิธีการจัดเก็บข้อมูล :

๑. แหล่งข้อมูล : ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี

๒. วิธีการจัดเก็บข้อมูล : รวบรวมข้อมูลจากการดำเนินงานจริง

ผู้กำกับดูแลตัวชี้วัด : นางสาวนันทรีญา ภูหัดสวน หมายเลขติดต่อ : ๐๖๓-๓๖๘-๖๙๖๖

ผู้จัดเก็บข้อมูล : นายยุทธการณ์ ทุมทอง หมายเลขติดต่อ : ๐๘๕-๗๓๘-๔๒๑๓

: นายธนากร ประจิมทิศ หมายเลขติดต่อ : ๐๘๙-๒๗๕-๑๔๓๘

หน่วยงาน : กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี

แผนบริหารจัดการความเสี่ยง

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

Information Communication Technology

ICT RISK MANAGEMENT

กลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร

ฝ่ายปฏิบัติการอำนวยการ กลุ่มงานเวชศาสตร์ฉุกเฉิน

โรงพยาบาลอุดรธานี

บทที่ ๑
บทนำ
การจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑.๑ หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลและบริหารงานที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรอย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่หน่วยงาน โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงาน ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่ายและวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้การดำเนินงานของทุกหน่วยงานล้วนมีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมาย ดังนั้น กลุ่มเทคโนโลยีสารสนเทศ ฝ่ายปฏิบัติการอำนวยการ กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรานี จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมาย วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้นจัดลำดับความสำคัญของปัจจัยเสี่ยงแล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

๑.๒ วัตถุประสงค์

๑.๒.๑ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๑.๒.๓ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๑.๓ เป้าหมาย

มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เป็นเอกสารและสามารถนำไปปฏิบัติได้จริง

๑.๔ ขอบเขตการดำเนินงาน

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้ความรับผิดชอบของกลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร ฝ่ายปฏิบัติการอำนวยการ กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรานี

๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

๑.๕.๑ มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑.๕.๒ มีแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๑.๖ ระยะเวลาดำเนินการ

ลำดับที่	กิจกรรม	ปีงบประมาณ ๒๕๖๗						หมายเหตุ
		เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑	- ศึกษาข้อมูลในการจัดทำแผนบริหารจัดการความเสี่ยง	→	→					
๒	- วิเคราะห์ความเสี่ยง - จัดทำแผนบริหารจัดการความเสี่ยง			→	→			
๓	- สรุปผลการประเมิน					→	→	

๑.๗ ผู้รับผิดชอบ

๑.๗.๑ นายยุทธการณ์ ทุมทอง เจ้าพนักงานสาธารณสุขชำนาญงาน
๑.๗.๒ นายธนากร ประจิมทิศ พนักงานสื่อสาร

๑.๘ ที่ปรึกษา

๑.๘.๑ นายแพทย์วิสิษฐ์ วิจิตรโกสุม หัวหน้ากลุ่มงานเวชศาสตร์ฉุกเฉิน
๑.๘.๒ นายแพทย์เอกภักดิ์ ระหว่างบ้าน นายแพทย์ชำนาญการพิเศษ
๑.๘.๓ นายแพทย์ณัฐพล ตรีทิพย์สถิตย์ หัวหน้าศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี
๑.๘.๔ นายแพทย์พิทย์ จันทร์สมบูรณ์ รองหัวหน้าศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี

บทที่ ๒
การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๑ สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ฐานข้อมูลการรับแจ้งเหตุและสั่งการ ฯ ในระบบการแพทย์ฉุกเฉิน ฐานข้อมูลการตรวจเช็คอุปกรณ์ในรถปฏิบัติการฉุกเฉิน ฐานข้อมูลระบบสารสนเทศการแพทย์ฉุกเฉิน (ITEMS) เป็นต้น อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเครือข่าย (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) อุปกรณ์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching) และอุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

๒.๒ กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมินและจัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานและการบริหารจัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้

รูปที่ ๑ แสดงกระบวนการบริหารความเสี่ยง

๒.๒.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๒.๒.๑.๑ การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๒.๒.๑.๒ การใช้ Checklist

๒.๒.๑.๓ การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

๒.๒.๑.๔ การวิเคราะห์การปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีต ทั้งที่ประสบผลสำเร็จและปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๒.๒.๒ การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วย การวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๒.๒.๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิญปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒.๒.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

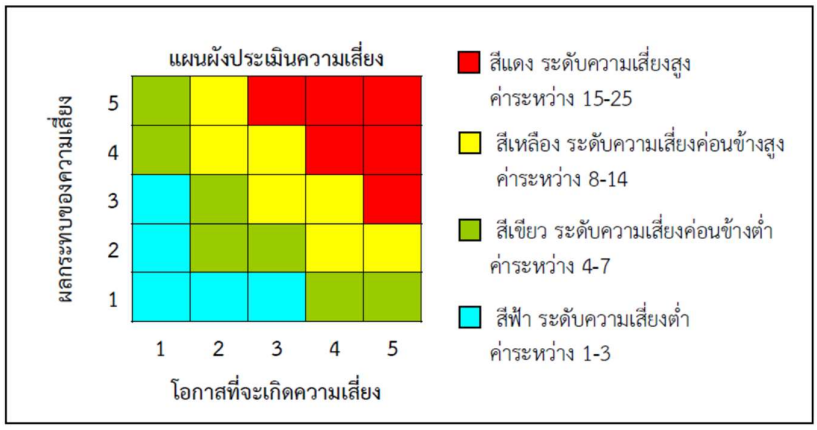
เกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) เป็นดังนี้

ระดับ	การประเมิน
๑	น้อยมาก (แทบไม่มีผลกระทบเลย)
๒	น้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)
๓	ปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
๔	สูง (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)
๕	สูงมาก (ผู้บริหารถูกลงโทษทางวินัย)

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง เป็นดังนี้

ระดับ	การประเมิน
๑	เกิดขึ้นน้อยมาก นานๆครั้ง (แทบไม่เกิดขึ้นเลย)
๒	เกิดขึ้นน้อย ไม่บ่อย (อาจเกิดขึ้นได้ทุก ๕ ปี)
๓	เกิดขึ้นปานกลาง (อาจเกิดขึ้นได้ทุกปี)
๔	เกิดขึ้นสูง หรือ บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
๕	เกิดขึ้นสูงมาก หรือ บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

๒.๒.๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปที่ ๒



รูปที่ ๒ แสดงแผนผังประเมินความเสี่ยง

๒.๒.๒.๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่ผลต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงมากหรือสูง มาจัดทำแผนการบริหารความเสี่ยงก่อน

๒.๒.๓ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ ในการวางแผนจะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้นเพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบและป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๒.๒.๓.๑ ควบคุมเพื่อความป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุมและการเข้าถึงเอกสาร เป็นต้น

๒.๒.๓.๒ การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับและการรายงานข้อบกพร่อง เป็นต้น

๒.๒.๓.๓ การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๒.๒.๓.๔ การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูงมาประเมินมาตรการควบคุมเป็นอันดับแรก โดยใช้ขั้นตอนดังนี้

๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมากหรือสูง มากำหนดวิธีควบคุมที่ควรจะมีเพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

๒) พิจารณาว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๒.๒.๔ การติดตาม การรายงานและการประเมินผลการดำเนินการตามมาตรการที่กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยงหรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง และนำมาวางแผนจัดการความเสี่ยง ซึ่งทางเลือกในการบริหารความเสี่ยงมีหลายวิธีสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์เมื่อทราบความเสี่ยงที่ยังเหลืออยู่แล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือกเพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจากประเด็นต่าง ๆ ดังนี้

๒.๒.๔.๑ พิจารณาว่ายอมรับความเสี่ยงหรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๒.๒.๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๒.๒.๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยง ให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๒.๒.๔.๔ พิจารณาผลการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมา หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมาย ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วย การรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง มีเหลืออยู่ในระดับใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๒.๒.๕ การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลาหรือการติดตามผลในระหว่างการปฏิบัติงาน

๒.๓ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๘ ประเภท ดังนี้

๒.๓.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

๒.๓.๒ ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของเจ้าหน้าที่และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้เจ้าหน้าที่มีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งเจ้าหน้าที่ภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

๒.๓.๓ ความเสี่ยงด้านอุปกรณ์ (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกคุกคามจากภัยต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware, Ransomware เป็นต้น ทั้งที่เป็นการโจมตีจากภายในและมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๒.๓.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัยเพื่อลดช่องโหว่ที่อาจเกิดจากข้อผิดพลาดทางเทคนิค (Bug) ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๒.๓.๕ ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหายเนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูลเพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่หน่วยงาน ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหารและผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

๒.๓.๖ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่าง ๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

๒.๓.๗ ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณที่ไม่เพียงพอและการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

๒.๓.๘ ความเสี่ยงในด้านการบริหารจัดการ (Management Risk) หมายถึง ความเสี่ยงเนื่องมาจากการบริหารที่ไม่รัดกุมและไม่มีแผนงานในการดำเนินการที่ดี

๒.๔ การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) โดยมีหลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๒.๔.๑ การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้นหรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้นโดยมิได้คิดทบทวนถึงผลที่จะได้รับอาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

๒.๔.๒ การยอมรับ (Take) เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

๒.๔.๓ การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ก็ควรขจัดให้หมดไปหรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดแนวทางปฏิบัติไว้ล่วงหน้า วิธีการควบคุมความสูญเสียมี ๒ วิธี คือ

๒.๔.๓.๑ การป้องกันการเกิดความสูญเสียโดยที่พยายามจะลดความถี่ของการเกิดความสูญเสีย การหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น ติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบเข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคลหรือไวรัสคอมพิวเตอร์มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้น

๒.๔.๓.๒ การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อนหรือสัญญาณเตือนภัย เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้อง Server ให้มีความเสียหายน้อยที่สุดหรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย

๒.๔.๔ การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะเวลาในการรับประกันภัยเพียงหนึ่งปีเพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายให้ทันก่อนระยะเวลาในการรับประกันจะสิ้นสุด

๒.๕ ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ มีดังนี้

๒.๕.๑ ปัจจัยภายนอก ได้แก่

๒.๕.๑.๑ ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ไฟไหม้ แผ่นดินไหว น้ำท่วม และภัยพิบัติอื่น ๆ

๒.๕.๑.๒ การขโมยอุปกรณ์เครื่องข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๒.๕.๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) จากการเคลื่อนย้าย หรืออื่น ๆ

๒.๕.๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ขัดข้อง

๒.๕.๑.๕ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๒.๕.๒ ปัจจัยภายใน ได้แก่

๒.๕.๒.๑ ระบบฐานข้อมูลหลักเสียหายหรือข้อมูลถูกทำลาย

๒.๕.๒.๒ การถูกไวรัสคอมพิวเตอร์ (Virus Computer) ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการต่าง ๆ

๒.๕.๒.๓ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลหรือระบบเครือข่ายคอมพิวเตอร์จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๖ การประเมินความเสียหาย

๒.๖.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุดซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒.๖.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้องและกระแสไฟฟ้าขัดข้อง

๒.๗ การติดตามและรายงานผล

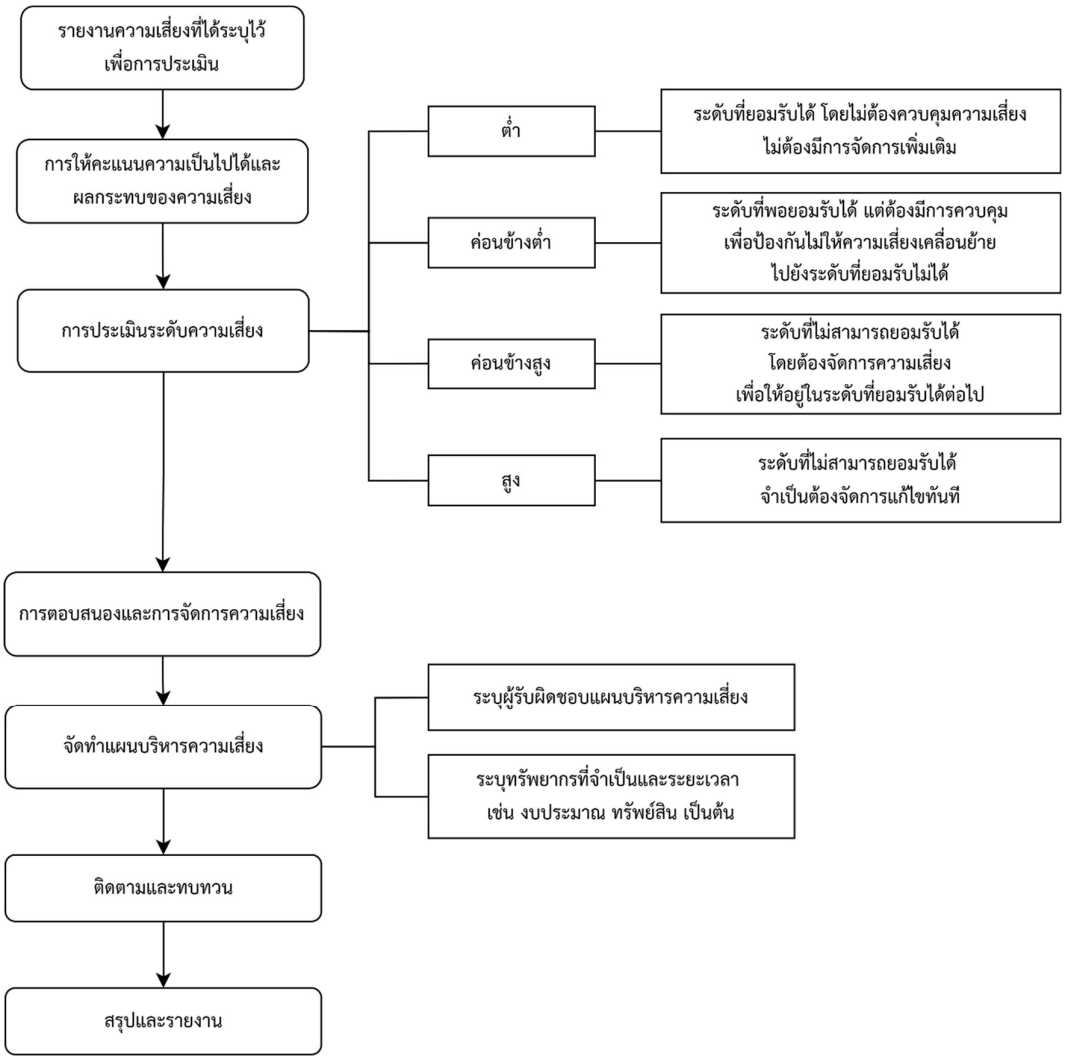
กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือนและให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

บทที่ ๓

การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่อาจประสบกับความเสียหายจากสาเหตุและปัจจัยเสี่ยงต่าง ๆ จึงมอบหมายให้ฝ่ายปฏิบัติการอำนวยการ โดยกลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร ทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารให้สอดคล้องกับประกาศโรงพยาบาลอุดรธานี เรื่อง นโยบายการบริหารความเสี่ยงและความปลอดภัย โดยกำหนดเข็มมุ่งด้านคุณภาพและความปลอดภัยของผู้ป่วยและบุคลากร (ความปลอดภัยทางไซเบอร์) โดยกระบวนการเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยงหรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศและทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้น ๆ ดังตารางการบริหารจัดการความเสี่ยงที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่าง ๆ ดังต่อไปนี้

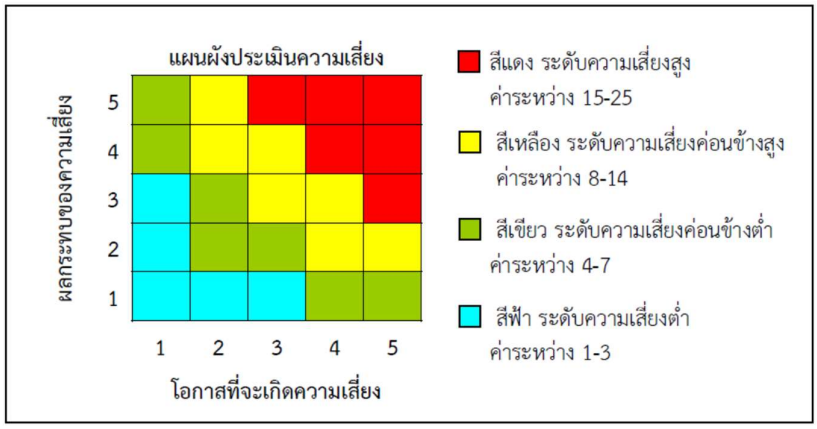
๓.๑ แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๓.๒ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่

ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินระดับความเป็นไปได้และผลกระทบมีดังนี้



รูปที่ ๒ แสดงแผนผังประเมินความเสี่ยง

ลำดับที่	ประเภทความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑	ความเสี่ยงจากอัคคีภัย	๕	๕	๒๕
๒	ระบบกระแสไฟฟ้าขัดข้อง	๕	๓	๑๕
๓	ระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย	๕	๓	๑๕
๔	การไม่สำรองข้อมูล/การสำรองข้อมูลขาดการอัพเดท	๕	๓	๑๕
๕	การเชื่อมต่อระบบอินเทอร์เน็ตขัดข้อง	๓	๕	๑๕
๖	การบุกรุกโจมตีจากภายนอก	๓	๔	๑๒
๗	ลิขสิทธิ์ซอฟต์แวร์	๒	๕	๑๐
๘	ไวรัสคอมพิวเตอร์/Malware	๒	๔	๘
๙	ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๒	๓	๖
๑๐	ความเสี่ยงจากการถูก Black List จาก Search	๓	๒	๖
	Engine/Spamhaus			
๑๑	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผน	๒	๓	๖
	บริหารความต่อเนื่อง			
๑๒	ความเสี่ยงจากอุทกภัย	๒	๓	๖
๑๓	ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	๒	๓	๖
๑๔	ความเสี่ยงจากแมลง/สัตว์กัดแทะ	๑	๕	๕
๑๕	การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์	๑	๕	๕

ลำดับที่	ประเภทความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑๖	การโจมตีเซิร์ฟเวอร์ของหน่วยงานไม่ให้สามารถ	๑	๕	๕
	ให้บริการ ได้ (Denial of Service-DoS)			
๑๗	ความเสี่ยงจากการใช้ Wireless เข้าเครือข่าย อินทราเน็ต	๑	๕	๕
๑๘	เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	๒	๒	๔
๑๙	ความเสี่ยงจากไฟกระชากจากปลั๊กพ่วง	๒	๒	๔
๒๐	วินาศภัย/การก่อการร้าย	๑	๓	๓
๒๑	ความเสี่ยงจากความชื้น อุณหภูมิ	๒	๑	๒
๒๒	ความเสี่ยงจากแผ่นดินไหว	๑	๑	๑
๒๓	การโจรกรรมฐานข้อมูล	๑	๑	๑

๓.๓ ผลประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๑. ความเสี่ยงสูงมาก						
๑. ความเสี่ยงจากการเกิดอัคคีภัย	๑. คอมพิวเตอร์และเครือข่ายถูกทำลาย ๒. ข้อมูลถูกทำลาย ๓. การบาดเจ็บหรือเสียชีวิตของจ้าหน้าที่	๑. เสียงบประมาณในการจัดหาระบบทดแทน ๒. ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน	สูงมาก ๕ x ๕ = ๒๕	๑. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง ๒. ติดตั้งระบบตรวจจับควัน เพื่อแจ้งเตือนไฟไหม้ระบบดับเพลิง ๓. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	๑	
๒. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	๑. ไม่สามารถใช้งานเครื่องแม่ข่ายและเครือข่ายได้ ๒. ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูก Shutdown อย่างเหมาะสม	๑. ข้อมูลเสียหาย ๒. ระบบปฏิบัติการ โปรแกรม หรือฐานข้อมูลเสียหายต้องมีการติดตั้งใหม่	สูงมาก ๕ x ๓ = ๑๕	๑. ตรวจสอบระบบสำรองไฟฟ้า (UPS) ๒. วางแผนการจัดหาและติดตั้งเครื่องกำเนิดไฟฟ้า (Electrical Generator)	๑	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๑. ความเสี่ยงสูงมาก (ต่อ)						
๓. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๑. ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ ๒. เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	๑. การใช้งานระบบงานไม่สามารถใช้ได้ตามปกติ	สูงมาก ๓ x ๕ = ๑๕	- ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒. จัดตั้งศูนย์สำรองข้อมูล (Backup Site)	๕	
๔. ความเสี่ยงจากการไม่ได้สำรองข้อมูลหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	๑. เสี่ยงต่อการสูญหายของข้อมูลในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานได้ตามปกติ ๒. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	๑. เสียค่าใช้จ่ายในการกู้คืนข้อมูลหรือการจัดทำขึ้นมาใหม่ ๒. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้ เนื่องจากขาดความมั่นใจในข้อมูล	สูงมาก ๕ x ๓ = ๑๕	๑. มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	๕	
๕. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	๑. ไม่สามารถใช้งานระบบงานของหน่วยงานฯ ผ่านเครือข่ายอินทราเน็ตได้ ๒. ไม่สามารถเชื่อมต่อภายนอกหน่วยงานฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	๑. ขัดขวางการทำงานของเจ้าหน้าที่และผู้บริหารงานหน่วยงานฯ ๒. บุคคลภายนอกไม่สามารถเข้าใช้ Web Server หรือค้นหาข้อมูลที่ต้องการได้	สูงมาก ๕ x ๓ = ๑๕	๑. ตรวจสอบสัญญาณเครือข่ายสื่อสารกับผู้ให้บริการอินเตอร์เน็ต ๒. ตรวจสอบสายสัญญาณ	๓	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๒. ความเสี่ยงสูง						
๑. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	๑. เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	๑. ทำให้ระบบเครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่น ๆ ทั้งหมดในเครือข่าย ๒. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือ รูปภาพบน Web Site ของหน่วยงาน ฯ ๓. ถูกโจรกรรมข้อมูลที่เป็นความลับ	สูง ๓ x ๔ = ๑๒	๑. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย ๒. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ ๓. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	๓	
๒. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑. การสูญหายของข้อมูล ๒. การถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือของสำนักงานฯ	๑. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์ ๒. อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ ๓. ความไม่สะดวกหากไปใช้งานด้วยซอฟต์แวร์ที่ไม่จำเป็นต้องมีลิขสิทธิ์ (Open Source)	สูง ๒ x ๕ = ๑๐	๑. จัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๒. ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย	๔	
๓. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	๑. โปรแกรมหรือข้อมูลถูกทำลาย ๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ ๓. การถูกขโมยข้อมูล	๑. ใช้คอมพิวเตอร์ไม่ได้ ๒. ใช้ระบบงานไม่ได้ ๓. ข้อมูลที่สำคัญสูญหาย	สูง ๒ x ๔ = ๘	๑. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย ๒. อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ	๓	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๓. ความเสี่ยงปานกลาง						
๑. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. การถูกขโมยข้อมูล ๒. โปรแกรมเสียหาย ๓. การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง	๑. ลดความน่าเชื่อถือต่อหน่วยงานหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ ๒. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อหน่วยงานเป็นอย่างยิ่ง	ปานกลาง ๒ x ๓ = ๖	๑. ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP - Top ๑๐ Web Application Security Risks เพื่อลดความเสี่ยง ๒. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ	๔	
๒. ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	๑. เสี่ยงต่อการถูกขโมยข้อมูล ๒. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม ๓. ไม่สามารถแก้ไขข้อบกพร่องได้เอง ๔. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูลทำให้ไม่สามารถใช้งานได้ในระยะยาว ๕. เสียค่าใช้จ่ายสูง	๑. ลดความน่าเชื่อถือต่อหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ ๒. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อหน่วยงาน ฯ เป็นอย่างยิ่ง๓ ๓. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลพร้อมกับการทำการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัพเดทอยู่เสมอ	ปานกลาง ๒ x ๓ = ๖	๑. การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level ๒ ๒. การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล – ER Diagram ๓. ให้มีการส่งมอบ Source Code ในรูปแบบ DVD ในฟอร์แมตที่ไม่เข้ารหัสใด ๆ และสามารถปรับปรุงแก้ไขได้	๔	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๓. ความเสี่ยงปานกลาง (ต่อ)						
๒. ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง (ต่อ)				๔. หากมีการพัฒนา Library ด้วยตนเอง ต้องส่ง Source Code Library ที่สามารถแก้ไขได้ ๕. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ ๖. มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม ๗. มีแผนการบำรุงรักษาระบบงานที่ดีรวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม(Bug) การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น		

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๓. ความเสี่ยงปานกลาง (ต่อ)						
๓. ความเสี่ยงจากการเกิดอุทกภัย	๑. ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	๑. เสียงบประมาณในการซ่อมแซมหรือจัดหาใหม่ทดแทน	ปานกลาง ๒ x ๓ = ๖	๑. ติดตั้งเครื่องตรวจจับระดับน้ำรั่วไหลพื้นที่ที่มีความไวต่อน้ำ ๒. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	๑	
๔. ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	๑. ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือม้วนเทป (Cartridge Tape) แผ่น DVD/ CD	๑. ข้อมูลที่อยู่ในชั้นความลับรั่วไหลทำให้เสียหายต่อความเชื่อถือ ๒. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	ปานกลาง ๒ x ๓ = ๖	๑. มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/ CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้วหากทำได้	๕	
๕. ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์สายไฟฟ้า/สายสัญญาณ	๑. เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	๑. เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน	ปานกลาง ๑ x ๕ = ๕	๑. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack ๒. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	๑	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๓. ความเสี่ยงปานกลาง (ต่อ)						
๖. ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง ๖.๑ เครื่องแม่ข่าย	๑. เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	๑. เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง ๒. เสียเวลาในการกู้ระบบ ๓. เสียภาพลักษณ์ของหน่วยงานฯ	ปานกลาง ๑ x ๕ = ๕	๑. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย ๒. ตู้ Rack ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์จัดเก็บข้อมูล (Disk Array)และอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา ๓. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน	๑	
๖.๒ เครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	๑. เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	๑. เสียงบประมาณในการจัดหาอุปกรณ์ทดแทน ๒. เสียภาพลักษณ์ของหน่วยงาน	ปานกลาง ๑ x ๕ = ๕	๑. ควบคุมการเข้าออกอาคาร ๒. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออกอาคารตลอดเวลา ๓. ติดตั้งกล้องวงจรปิดให้ครอบ-คลุมทุกที่ ๆ มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	๑	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๓. ความเสี่ยงปานกลาง (ต่อ)						
๗. ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	๑. เสี่ยงต่อผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลเข้าใช้เครือข่าย อินทราเน็ตผ่านทาง WiFi	๑. ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ อันจะนำมาซึ่งการขาดความเชื่อถือของหน่วยงาน	ปานกลาง ๑ x ๕ = ๕	๑. ควบคุมการเข้าใช้เครือข่าย ๒. เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)	๓	
๘. ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	๑. เสี่ยงต่อการใช้งานในทางที่ผิด ๒. การใช้Resourceทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	๑. สูญเสีย Bandwidth ในเครือข่ายทำให้ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี ๒. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	ปานกลาง ๒ x ๒ = ๔	๑. บริหารจัดการด้วยข้อแนะนำ Ten Ways to Protect Your Network From Insider Threats เพื่อลดความเสี่ยง ๒. กำหนด Policy ของFirewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น ๓. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่างๆ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา	๒	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๓. ความเสี่ยงปานกลาง (ต่อ)						
๙. ความเสี่ยงจากไฟกระชากจากสายพ่วง (Extension Cord)	๑. เสี่ยงต่อไฟไหม้ ไฟดูดไฟย้อนกลับ ทำให้อุปกรณ์เครื่องคอมพิวเตอร์เสียหายทั้งหมดได้	๑. ไม่สามารถใช้งานเครื่องคอมพิวเตอร์ได้ตามปกติ ๒. ไฟอาจลัดวงจรทำให้เครื่องเสียหาย	ปานกลาง ๒ x ๒ = ๔	๑. งดใช้สายพ่วง หรืองดใช้สายพ่วงที่ไม่ได้มาตรฐาน ม.อ.ก. และไม่มีสายดิน ๒. ไม่ใช้อุปกรณ์ที่ไม่มีสายดิน (ปลั๊ก ๒ ขา หรือ ๓ ขาแต่หักสายดินออก) ต่อเข้ากับสายพ่วงหรือเต้าไฟฟ้า (Receptacle) ๓. ต่อสายพ่วงเข้ากับอุปกรณ์ที่มีระบบStabilizer	๒	
๔. ความเสี่ยงต่ำ						
๑. ความเสี่ยงจากวินาศภัย/การก่อการร้าย	๑. การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	๑. ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ต่ำ ๑x๓=๓	๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน ๒. จัดทำแผนสำรองฉุกเฉิน ๓. จัดทำศูนย์สำรอง (Backup Site)	๑	
๒. ความเสี่ยงจากความชื้นอุณหภูมิ	๑. เครื่องมีประสิทธิภาพและความเชื่อถือได้ลดลง และเครื่องอาจหยุดทำงานได้	๑. อายุของเครื่องและอุปกรณ์สั้นลง	ต่ำ ๒ x ๑ = ๒	๑. จัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	๓	

๓.๓ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	ประเภทความเสี่ยง	หมายเหตุ
๔. ความเสี่ยงต่ำ (ต่อ)						
๓. ความเสี่ยงจากแผ่นดินไหว	๑. ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	๑. ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ต่ำ ๑ x ๑ = ๑	๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน ๒. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไร และจะใช้เครื่องทดแทนจากที่ใดเพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง ๓. จัดทำศูนย์สำรอง (Backup Site)	๑	
๔. ความเสี่ยงจากการโจรกรรมฐานข้อมูล	๑. ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	๑. เสียชื่อเสียงและความน่าเชื่อถือ ๒. การสูญหายหรือถูกทำลายของข้อมูล	ต่ำ ๑ x ๑ = ๑	๑. มีการบริหารจัดการด้านการป้องกันข้อมูล ๒. มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) ๓. มีการบริหารสื่อจัดเก็บข้อมูล เช่น Hard ๔. Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์ หรือสื่อเก็บข้อมูลนั้นๆ ทิ้งแล้ว	๕	

๓.๕ แผนปฏิบัติการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารบรรลุเป้าประสงค์ของการบริหารจัดการความเสี่ยง

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติการ	ระยะเวลาเริ่มต้น/สิ้นสุด	พ.ศ. ๒๕๖๖						พ.ศ. ๒๕๖๗						ผลลัพธ์/ความก้าวหน้า
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑. ความเสี่ยงจากการเกิดอัคคีภัย	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	- วันที่ ๓๐ ก.ย. ของทุกปี												●	
๒. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	- ตรวจสอบระบบสำรองไฟฟ้า (UPS)	- วันที่ ๓๐ ก.ย. ของทุกปี												●	
๓. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	- ตรวจสอบระบบคอมพิวเตอร์แม่ข่าย	- ทุก ๓ เดือน	●			●			●			●			
๔. ความเสี่ยงจากการไม่สำรองข้อมูลหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ ทดสอบการกู้คืน	- ทุกวัน - ทุก ๓ เดือน	←———											———→	
			●			●			●			●			
๕. ความเสี่ยงจากการเชื่อมต่อระบบครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก	- ทุก ๓ เดือน	●			●			●			●			
๖. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	- ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	- ทุกวันที่ ๑ ทุกวันที่ ๑๖ ของเดือน	←———											———→	

แผนผังและขั้นตอน

รองรับสถานการณ์ฉุกเฉิน

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

Information Communication Technology

ICT Contingency Plan

กลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร

ฝ่ายปฏิบัติการอำนวยการ กลุ่มงานเวชศาสตร์ฉุกเฉิน

โรงพยาบาลอุดรธานี

บทที่ ๑
บทนำ
สถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๑ หลักการและเหตุผล

ปัจจุบันหน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในหน่วยงานและสนับสนุนการปฏิบัติงานเพิ่มมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการสร้างข้อมูลสารสนเทศอันมีประโยชน์ต่อการวางแผนพัฒนาและบริหารจัดการองค์กร รวมถึงการปฏิบัติงานของเจ้าหน้าที่ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์กรต่าง ๆ จึงจำเป็นต้องมีการจัดการฐานข้อมูลการเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศดังกล่าวเพื่อให้เกิดความมั่นคงปลอดภัยและมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี ได้นำเทคโนโลยีมาใช้เพื่อเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงานและการให้บริการแก่เจ้าหน้าที่และประชาชนให้สะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศและการสื่อสารอาจได้รับความเสียหายจากการถูกโจมตีโดยไวรัสคอมพิวเตอร์ ปัญหาระบบไฟฟ้า อัคคีภัย หรือปัจจัยทั้งภายในและภายนอกต่าง ๆ และส่งผลกระทบต่อการดำเนินงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น

๑.๒ วัตถุประสงค์

๑. เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูล เทคโนโลยีสารสนเทศและระบบการสื่อสารให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบสารสนเทศและระบบการสื่อสาร

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบการสื่อสารสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและระบบการสื่อสาร

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงานในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลสารสนเทศและการสื่อสาร

บทที่ ๒
การวิเคราะห์ความเสี่ยงเพื่อรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑ การวิเคราะห์ความเสี่ยง

ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี มีการนำเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยง เพื่อหาวิธีการป้องกันและลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยง อันจะส่งผลกระทบต่อระบบเทคโนโลยีสานสนเทศและการสื่อสาร เพื่อให้ระบบเทคโนโลยีและการสื่อสารเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีมาใช้ในการปฏิบัติงานให้เกิดประโยชนสูงสุด

การวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศและการสื่อสารของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี พบว่าประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ขัดข้อง เช่น การถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ทั้งที่เกิดจากความตั้งใจหรือไม่ตั้งใจ ไฟฟ้าขัดข้อง เป็นต้น

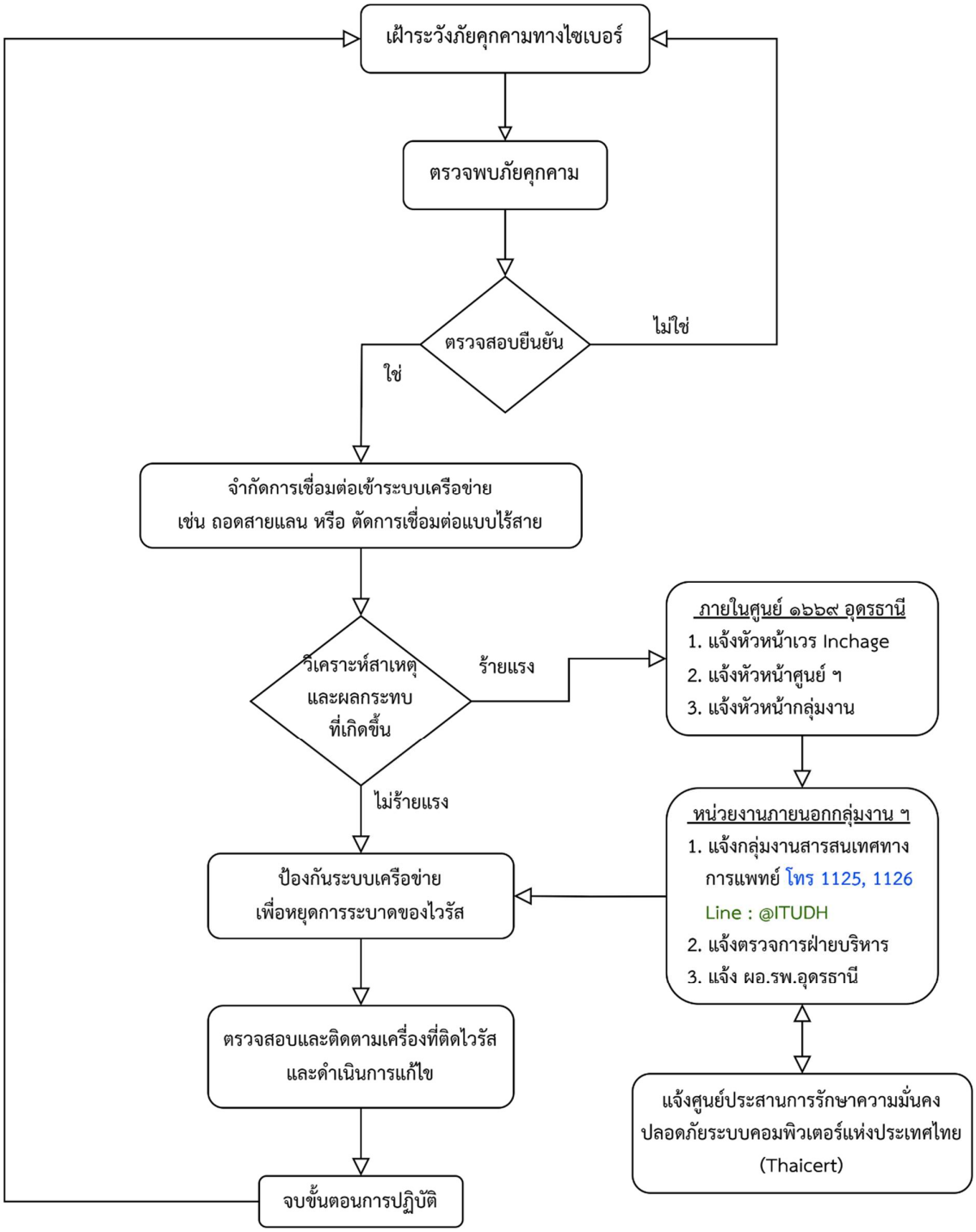
๒. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยธรรมชาติ หรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศและการสื่อสาร เช่น ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่เกิดจากการดำเนินการ การจัดลำดับความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศและการสื่อสาร

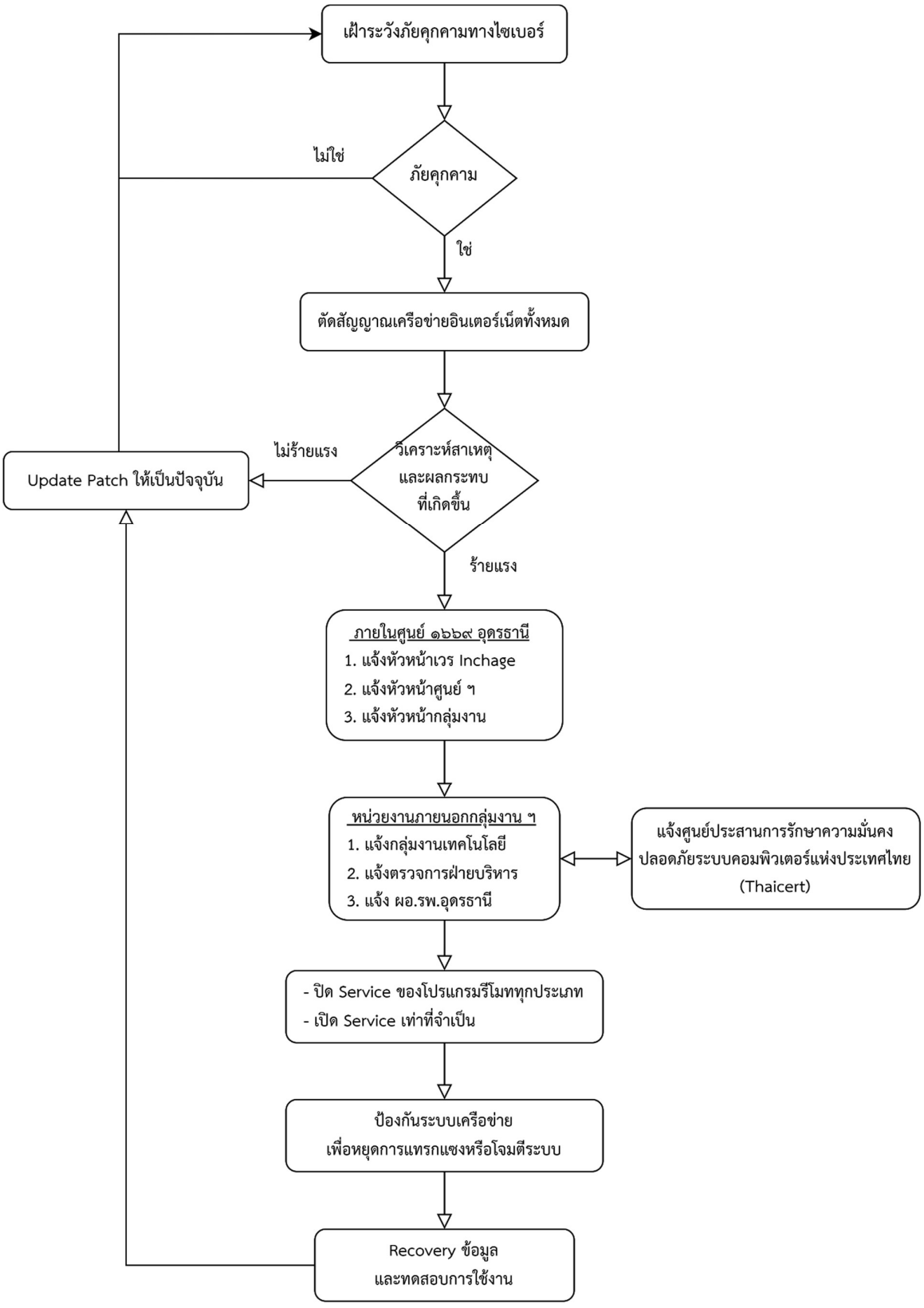
จากการวิเคราะห์และตรวจสอบดังที่กล่าวมาแล้วพบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศและระบบการสื่อสาร ดังนั้นเพื่อให้ระบบสารสนเทศและการสื่อสารของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศและการสื่อสารมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสานสนเทศและการสื่อสาร และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสานสนเทศและการสื่อสาร

บทที่ ๓
แผนผังและขั้นตอนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศและการสื่อสาร

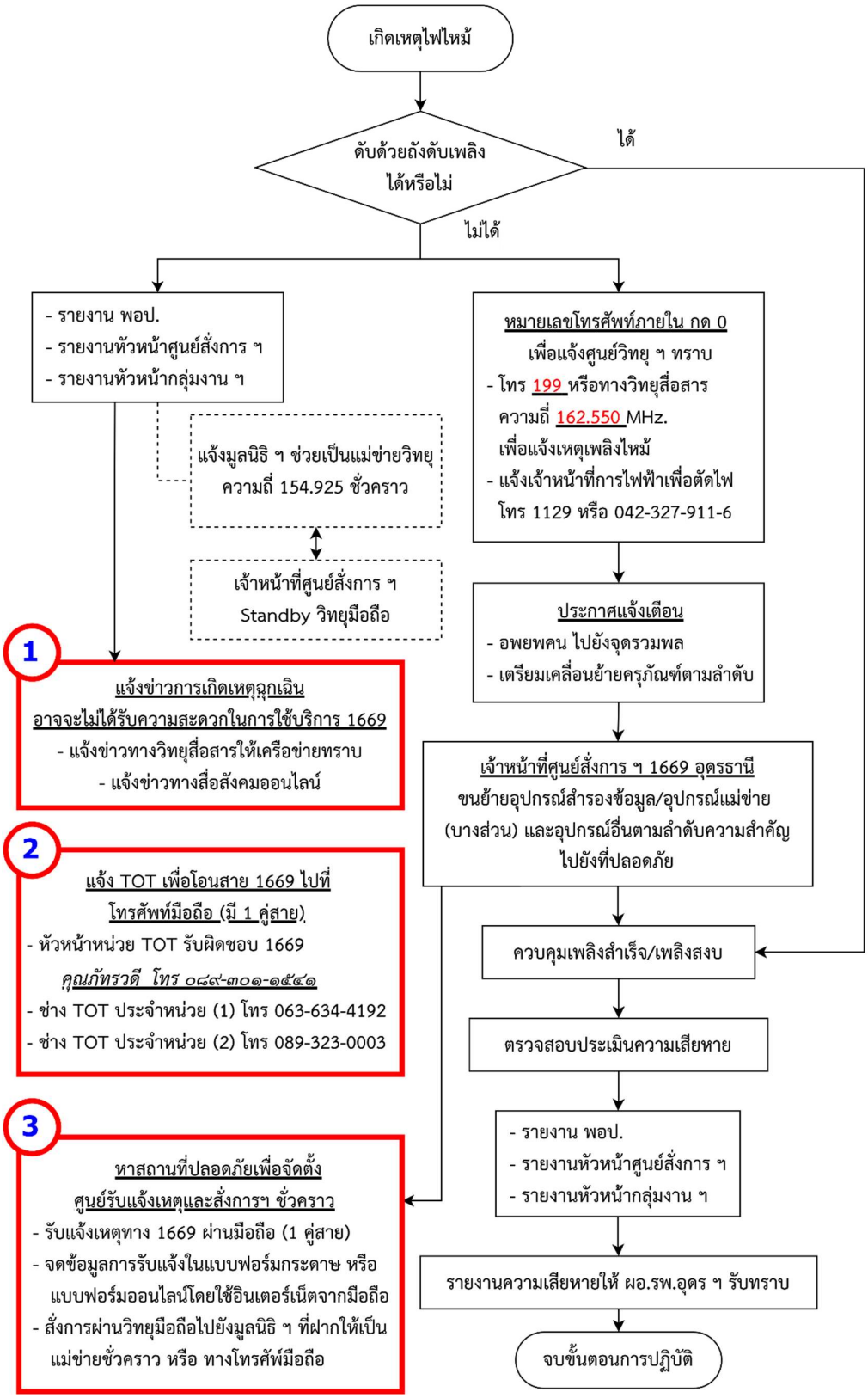
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๑ การป้องกันไวรัสล้มเหลว



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๒ การถูกแทรกแซงระบบ

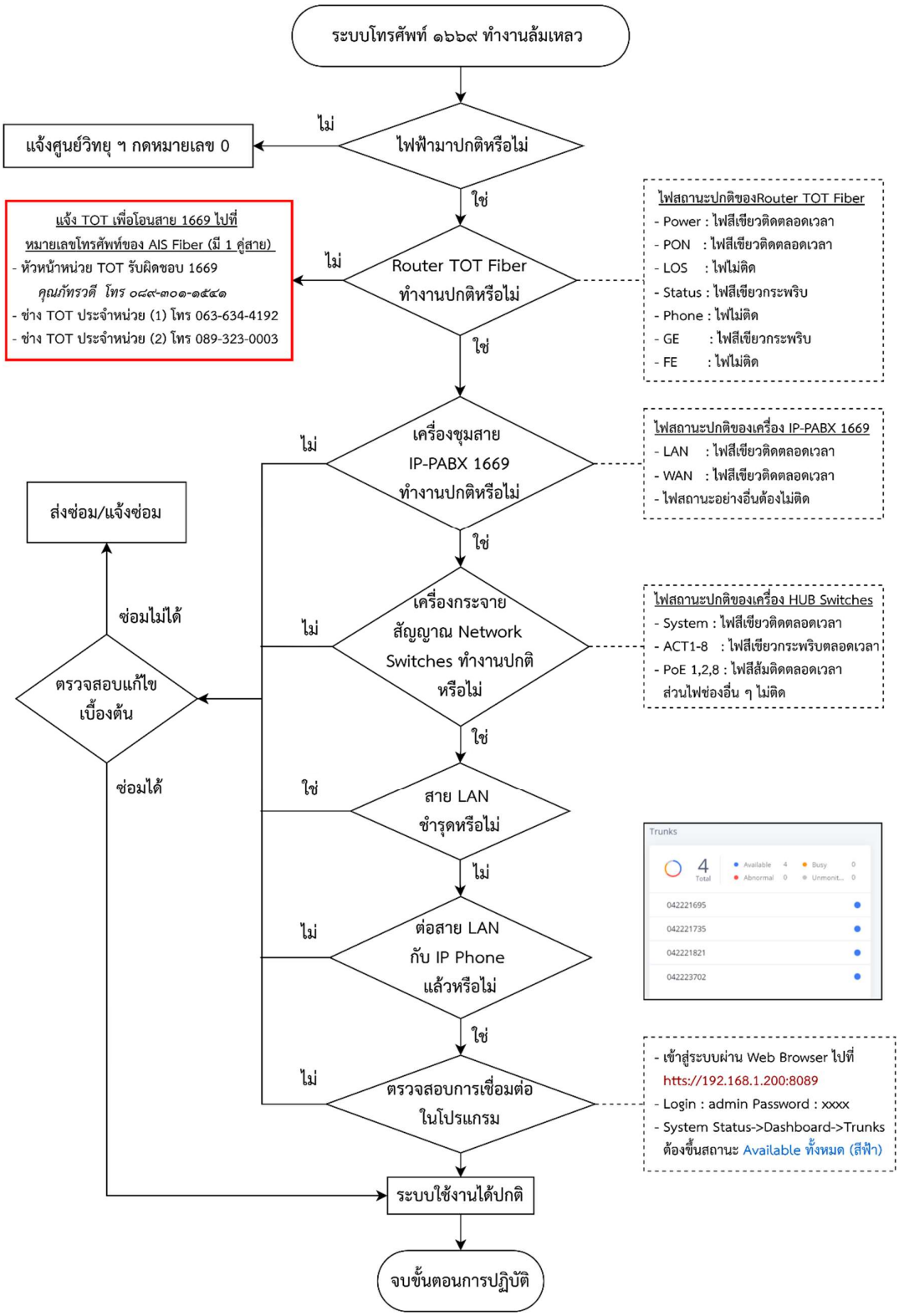


แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๓ ไฟไหม้



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๔ ไฟฟ้าขัดข้อง

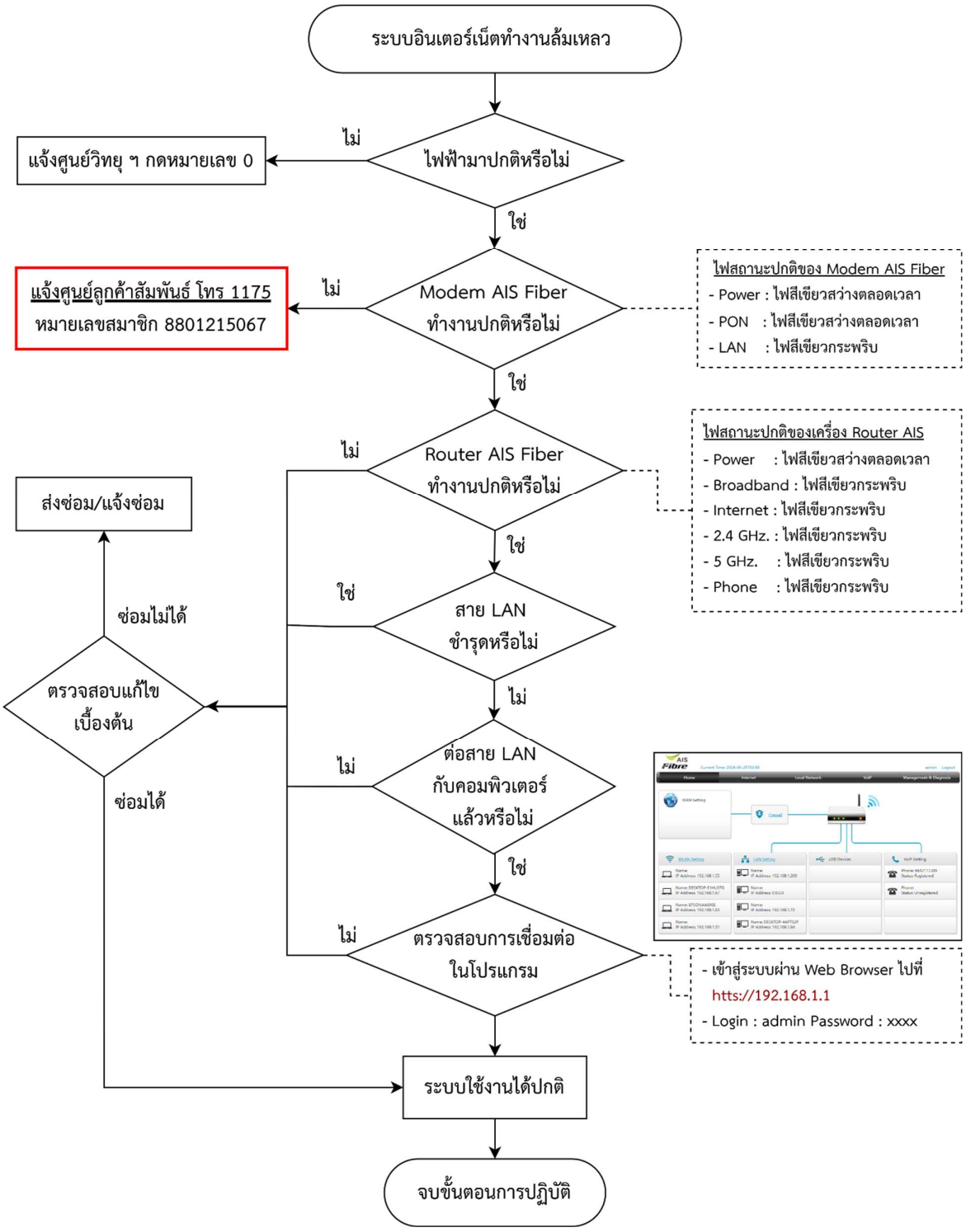
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๕ ระบบโทรศัพท์ ๑๖๖๙ ทำงานล้มเหลว



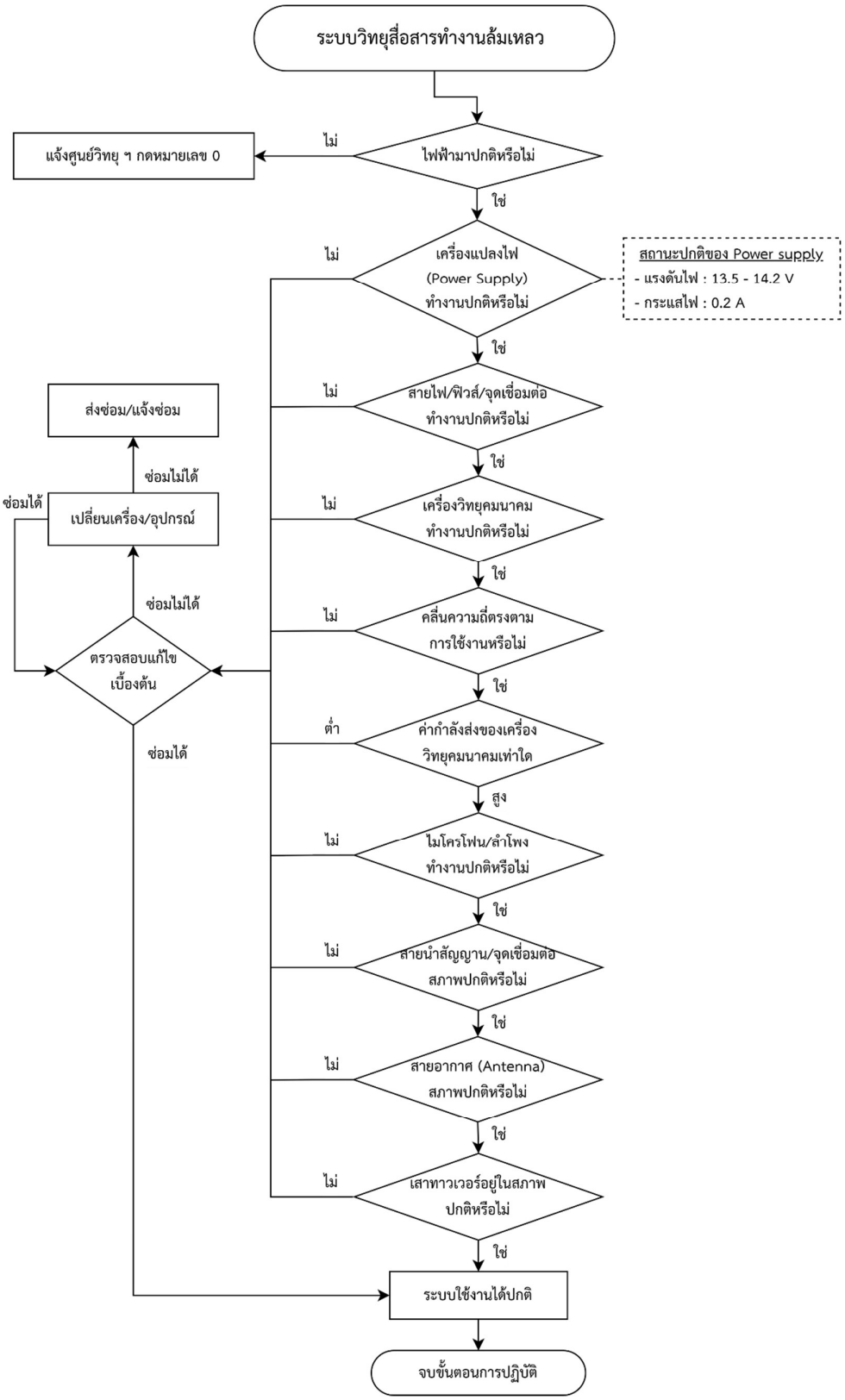
ป้ายประชาสัมพันธ์ กรณีระบบโทรศัพท์ ๑๖๖๙ ขัดข้อง

ที่เก็บภาพ : Google Drive (udems๑๖๖๙@gmail.com)

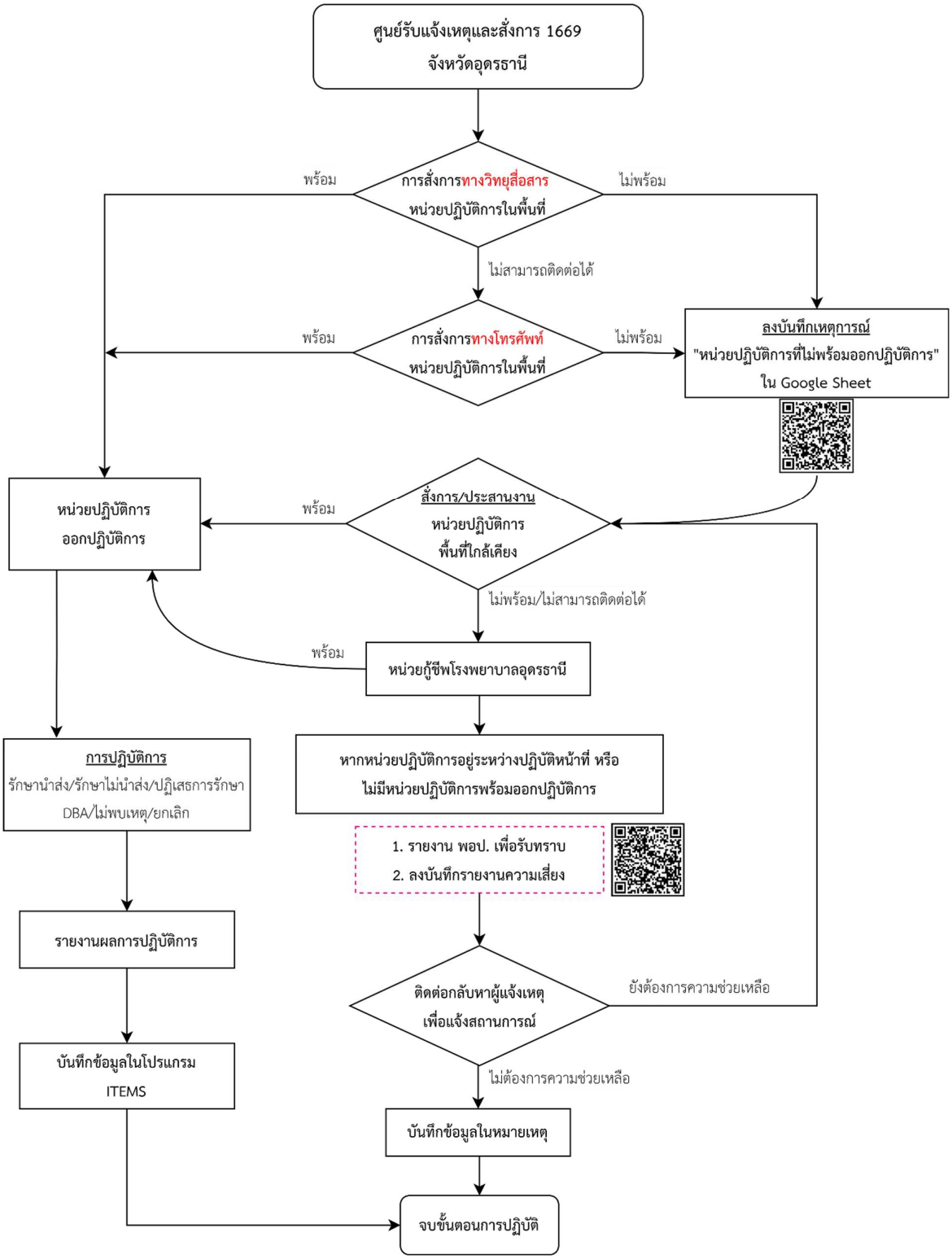
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๖ ระบบเครือข่ายอินเตอร์เน็ตล้มเหลว



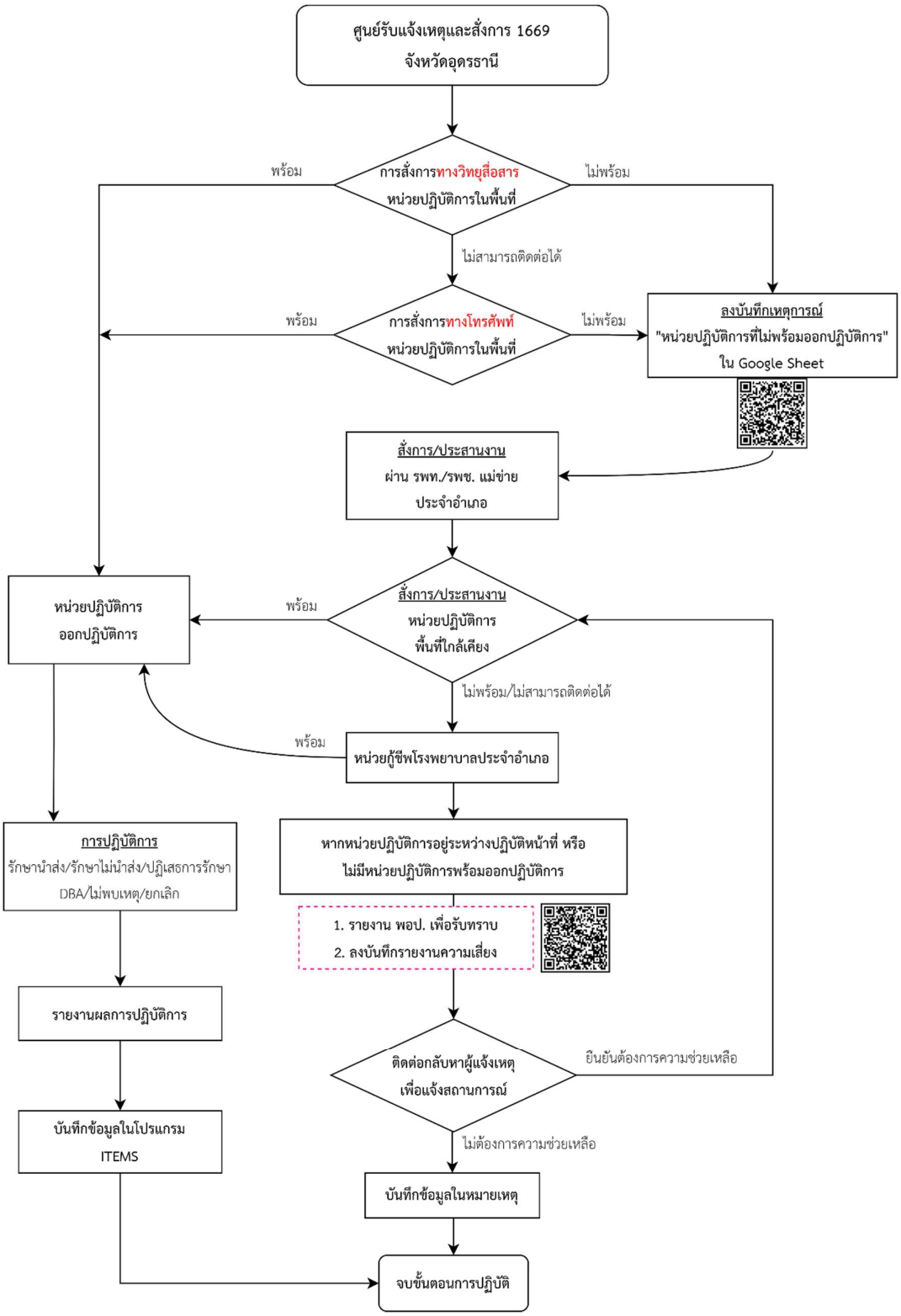
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๗ ระบบวิทยุคมนาคมทำงานล้มเหลว



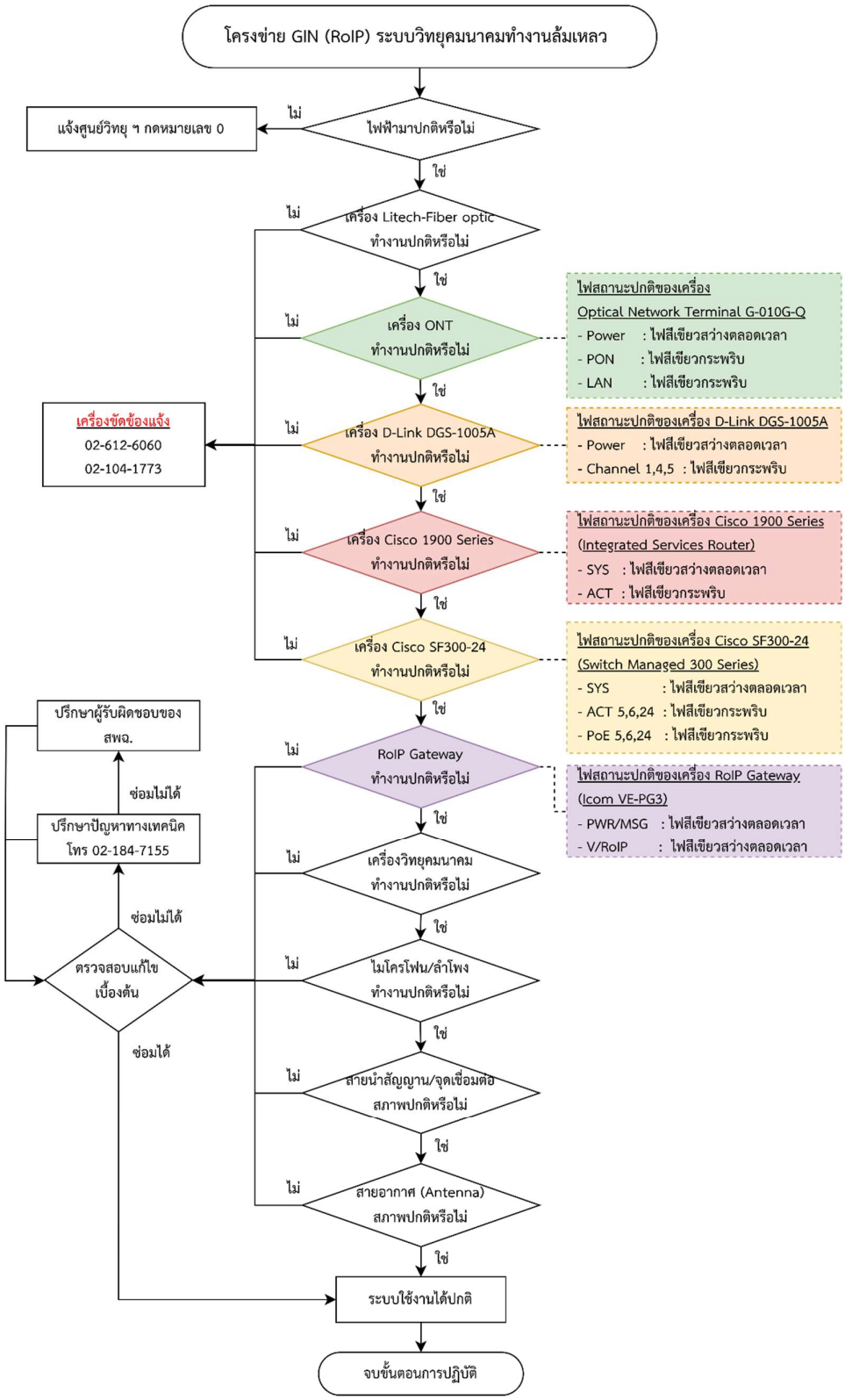
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๘ การสั่งการ/การประสานงานหน่วยปฏิบัติการแล้วไม่พร้อมออกปฏิบัติการหรือไม่สามารถติดต่อได้
(เขตอำเภอเมืองอุดรธานี)



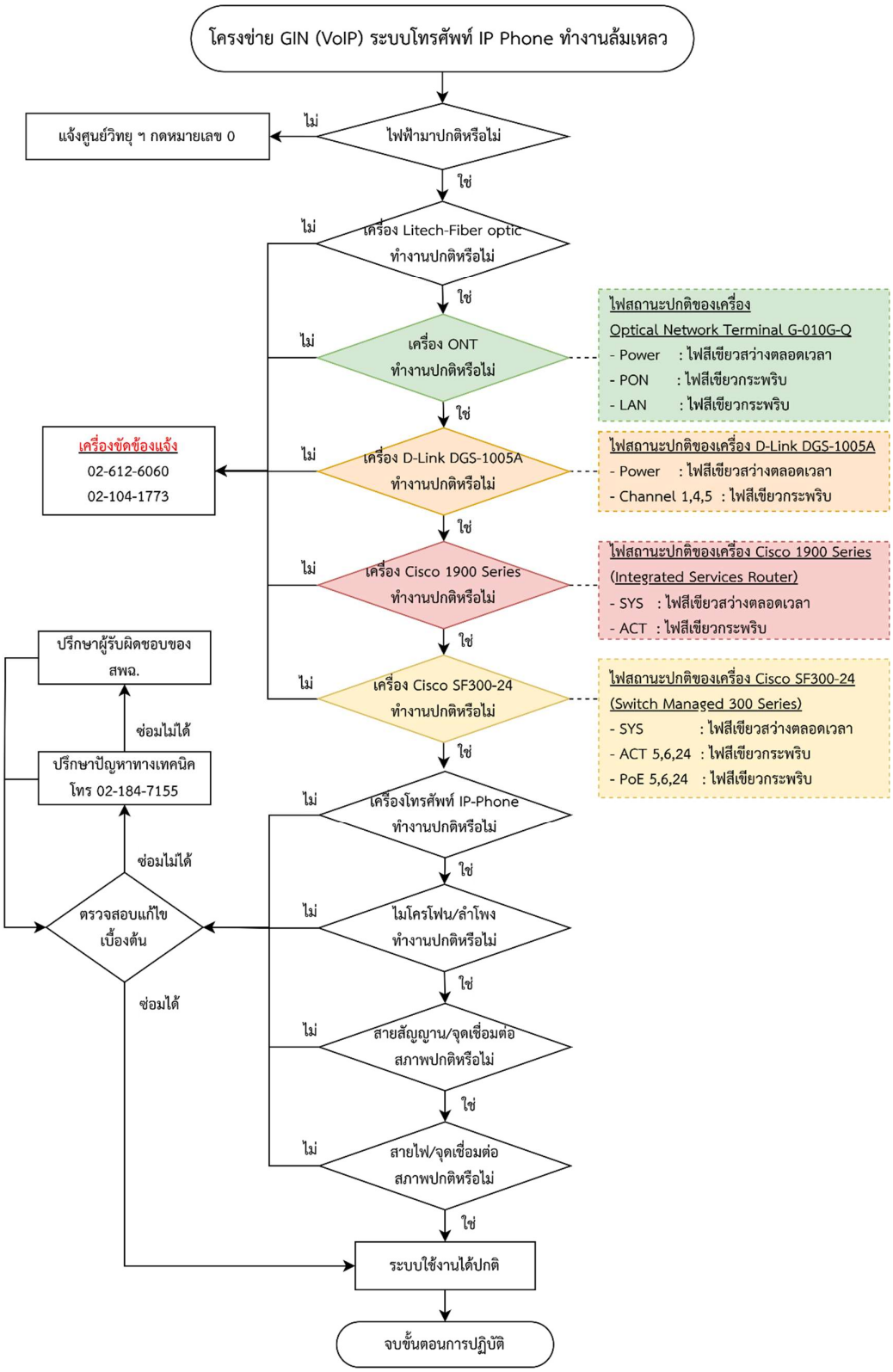
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๙ การสั่งการ/การประสานงานหน่วยปฏิบัติการแล้วไม่พร้อมออกปฏิบัติการหรือไม่สามารถติดต่อได้
(เขตอำเภออื่น ๆ ในจังหวัดอุดรธานี)



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๑๐ โครงข่าย GIN (RoIP) ระบบวิทยุคมนาคมทำงานล้มเหลว



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีที่ ๑๑ โครงข่าย GIN (VoIP) ระบบโทรศัพท์ IP-Phone ทำงานล้มเหลว



แผนการบำรุงรักษาเชิงป้องกัน

ระบบคอมพิวเตอร์ ระบบสารสนเทศ

และระบบการสื่อสาร

Preventive Maintenance Plan

กลุ่มเทคโนโลยีสารสนเทศและการสื่อสาร

ฝ่ายปฏิบัติการอำนวยการ กลุ่มงานเวชศาสตร์ฉุกเฉิน

โรงพยาบาลอุดรธานี

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี ได้นำระบบเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานและการบริการให้ได้รับความสะดวกรวดเร็วขึ้น แต่ขณะเดียวกันระบบเทคโนโลยีสารสนเทศดังกล่าวอาจได้รับความเสียหาย เช่น การถูกโจมตีจากไวรัส ระบบคอมพิวเตอร์ บุคคล ไฟฟ้าขัดข้อง อัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ซึ่งอาจทำให้ระบบเทคโนโลยีเกิดความเสียหายและส่งผลกระทบต่อระบบฐานข้อมูล ฮาร์ดแวร์และการปฏิบัติงานของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี

ดังนั้นเพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี จึงได้จัดทำแผนการดูแลบำรุงรักษาระบบคอมพิวเตอร์ ระบบสารสนเทศและระบบการสื่อสารของหน่วยงาน เพื่อใช้เป็นแนวทางในการปฏิบัติงาน

๑.๒ วัตถุประสงค์

๑.๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูล ระบบสารสนเทศและการสื่อสารให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๑.๒.๒ เพื่อลดความเสี่ยงและความเสียหายที่จะอาจเกิดกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารสามารถดำรงอยู่และดำเนินการได้อย่างต่อเนื่องอย่างมีประสิทธิภาพและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๑.๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๒.๕ เพื่อสร้างความเข้าใจอันดีร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ

๑.๒.๖ ลดการเสื่อมสภาพและค่าใช้จ่ายในการซ่อมบำรุง

๑.๓ ขอบเขต

การจัดทำคู่มือแผนการบำรุงรักษาเชิงป้องกันในครั้งนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี สามารถใช้งานอย่างเป็นระบบและมีประสิทธิภาพ อีกทั้งยังสามารถใช้งานได้แม้เกิดสถานการณ์ฉุกเฉิน เช่น ไฟดับ เครือข่ายอินเตอร์เน็ตหรือระบบการสื่อสารขัดข้อง เป็นต้น โดนครอบคลุมขั้นตอนการสำรวจ การจัดทำแผนบำรุงรักษาอุปกรณ์ การตรวจสภาพและบำรุงรักษา การประเมินสภาพการใช้งานและการสรุปและรายงานผลการบำรุงรักษาเชิงป้องกัน

๑.๔ การประเมินสถานการณ์ความเสี่ยง

การตรวจสอบความเสี่ยงต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ พบว่าสาเหตุของความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ อาจเกิดขึ้นได้จากปัจจัยเสี่ยง ดังนี้

๑.๔.๑ เจ้าหน้าที่หรือบุคลากร (Human error) ขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการหยุดชะงักหรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

๑.๔.๒ ไวรัสคอมพิวเตอร์ (Computer virus) อาจสร้างความเสียหายให้แก่เครื่อง คอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ถึงขั้นใช้งานไม่ได้

๑.๔.๓ ระบบไฟฟ้าขัดข้อง หรือความเสียหายจากความร้อนหรือเพลิงไหม

๑.๔.๔ ปัจจัยภายนอก เช่น ระบบ Internet ไม่สามารถใช้งานได้ หรืออาจเกิดจากการบุกรุกโจมตีจากภายนอก เป็นต้น

๑.๕ การเตรียมความพร้อมรับสถานการณ์เบื้องต้น

๕.๑ จัดฝึกอบรม สัมมนา หรือแนะนำแนวทางใช้งาน เสริมสร้างความรู้ ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศ ทั้งด้าน Hardware และ Software เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด

๕.๒ การสำรองข้อมูล (Backup) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทาลายโดยไวรัสคอมพิวเตอร์ และ/หรือผู้บุกรุกทาลายหรือเปลี่ยนแปลงข้อมูลให้สามารถนำข้อมูลดังกล่าวกลับมาใช้งานได้ โดยมีแนวทางดำเนินการ ดังนี้

๕.๒.๑ การตั้งค่าเครื่องคอมพิวเตอร์แม่ข่ายให้สำรองข้อมูลเป็นประจำอย่างน้อย ๑ ครั้งต่อเดือน

๕.๒.๒ การสำรองข้อมูลไว้ในอุปกรณ์บันทึกหรือคอมพิวเตอร์เครื่องอื่น ๆ เช่น USB Flash drive, External Hard disk, แผ่น DVD หรือ CD รายเดือน

๕.๓ การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยมีวิธีการดังนี้

๕.๓.๑ ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง (Update) ข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัส
- Update ข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่าง ๆ
- ใช้โปรแกรมเพื่อทาการตรวจสอบหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๕.๓.๒ ระวังภัยจากการเปิดไฟล์จากสื่อต่าง ๆ เช่น แผ่น CD-DVD และ Flash drive เป็นต้น

- แสกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลที่ไม่รู้จักหรือน่าสงสัย เช่น .pif, .inf เป็นต้น
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๕.๓.๓ ใช้ความระมัดระวังในการเปิด e-Mail

- อย่าเปิดไฟล์ e-Mail ถ้าไม่ทราบแหล่งที่มา
- ลบ e-Mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๕.๓.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จักที่แนบมากับโปรแกรมสนทนาต่าง
- ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง e-Mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่าง ๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๕.๔ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ที่ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ

๕.๔.๑ ติดตั้งเครื่องสำรองไฟฟ้า (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าได้นานประมาณ ๒๐ - ๓๐ นาที

๕.๔.๒ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๕.๔.๓ เมื่อเกิดกระแสไฟฟ้าดับ หากมีเครื่องสำรองไฟฟ้าใช้งานอยู่ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ด้วย

๕.๕ ติดตั้งระบบป้องกันไฟไหม้ โดยติดตั้งอุปกรณ์ดับเพลิงเพื่อการควบคุมเพลิงในเบื้องต้น

๕.๖ การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ โดยมีแนวทางดังนี้

๕.๖.๑ มาตรการควบคุมการใช้งานคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าใช้คอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ผู้ดูแลระบบเป็นผู้ดูแล

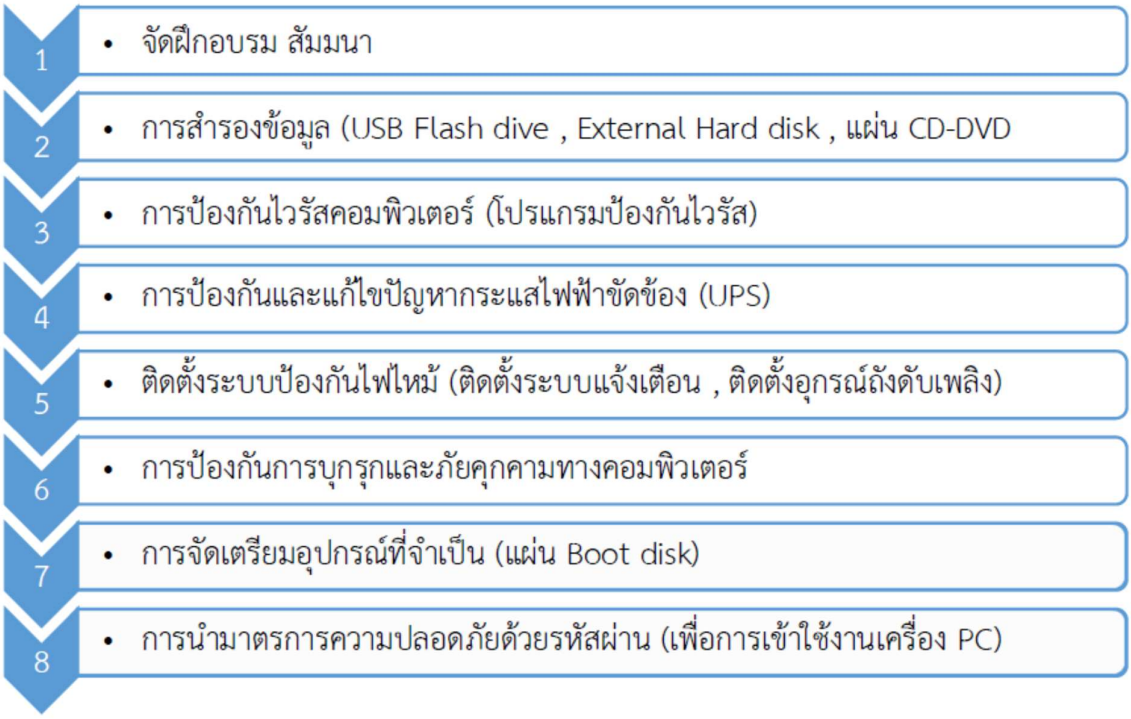
๕.๖.๒ มีเจ้าหน้าที่ดูแลระบบเครือข่าย ดูแลตรวจสอบระบบ อย่างสม่ำเสมอ

๕.๗ การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติและความเสี่ยงที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดเหตุขัดข้อง ไม่สามารถใช้งานได้ โดยการเตรียมอุปกรณ์ ดังนี้

- แผ่น Boot disk
- แผ่น Disk สำหรับติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานที่สำคัญ
- แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม Antivirus/Spyware
- แผ่น Driver อุปกรณ์ต่าง ๆ
- อุปกรณ์สาหรับระบบสารองไฟฉุกเฉิน
- อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๕.๘ การนำมาตรการความปลอดภัยด้วยรหัสผ่าน เพื่อการเข้าใช้งานเครื่อง Server รหัสผ่านการเข้าโปรแกรม และรหัสผ่านการใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ภายในบริเวณอาคาร เป็นต้น

ระบบการเตรียมความพร้อมรับสถานการณ์เบื้องต้น



บทที่ ๒
หลักเกณฑ์วิธีการปฏิบัติงานบำรุงรักษาอุปกรณ์เชิงป้องกัน

๒.๑ หลักเกณฑ์การปฏิบัติงาน

ในการปฏิบัติงานตามคู่มือ เรื่องการบำรุงรักษาอุปกรณ์เชิงป้องกัน ต้องเป็นผู้รอบรู้ในงานที่พึงปฏิบัติ ทั้งในวิธีปฏิบัติงาน กฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง โดยมีหน้าที่ต้องศึกษา ปฏิบัติ ให้คำปรึกษาแนะนำ ตรวจสอบ และรายงานผลการปฏิบัติงานตามกฎหมาย ระเบียบ ข้อบังคับ และหลักเกณฑ์แนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับการบำรุงรักษาเชิงป้องกันอุปกรณ์ ดังนี้

๒.๑.๑ แนวคิดการบำรุงรักษา (Maintenance) หมายถึง กิจกรรมหรืองานที่กระทำต่อเครื่องจักร เครื่องมือ อุปกรณ์ต่าง ๆ เพื่อรักษาหรือป้องกันไม่ให้เกิดการชำรุดเสียหาย โดยให้อยู่ในสภาพพร้อมที่จะใช้งานได้ตลอดเวลาช่วยลดการเสื่อมสภาพและยืดอายุการใช้งานให้นานขึ้นและลดค่าใช้จ่ายในการบำรุงรักษาให้น้อยที่สุด

ประวัติความเป็นมาของการบำรุงรักษา

ยุคที่ ๑ (ก่อนปี พ.ศ. ๒๔๙๓) เป็นยุคที่นิยมทำการบำรุงรักษาและซ่อมแซมอุปกรณ์หลังจากเกิดเหตุขัดข้องแล้ว ไม่มีการวางแผนการป้องกันการชำรุดเสียหายของอุปกรณ์ไว้ก่อน เมื่อเกิดขัดข้องชำรุดเสียหายส่งผลกระทบต่อการทำงานหรือกระบวนการผลิตไม่สามารถใช้งานได้แล้วจึงทำการซ่อมแซม

ยุคที่ ๒ (ปี พ.ศ. ๒๔๙๓ - ๒๕๐๓) เป็นยุคที่ได้นำแนวคิดเกี่ยวกับการบำรุงรักษาโดยมุ่งเน้นการป้องกัน (preventive maintenance) มาใช้เพื่อวางแผนป้องกันอุปกรณ์เกิดการชำรุด การทำงานหรือกระบวนการผลิตสามารถทำงานได้อย่างต่อเนื่อง

ยุคที่ ๓ (ปี พ.ศ. ๒๕๐๓ - ๒๕๑๓) เป็นยุคที่ได้นำแนวคิดเกี่ยวกับการบำรุงรักษาทวีผลให้ความสำคัญในขั้นตอนของการออกแบบเครื่องมือ เครื่องจักร อุปกรณ์ มีความน่าเชื่อถือมากยิ่งขึ้น โดยคำนึงถึงความยากง่ายของการบำรุงรักษาและนำหลักการด้านเศรษฐศาสตร์มาใช้ร่วมด้วย

ยุคที่ ๔ (พ.ศ. ๒๕๑๓ - ปัจจุบัน) เป็นยุคที่ได้นำเอาแนวคิดของทุกยุคเข้ามาประกอบด้วยกัน โดยให้ทุกฝ่ายได้มีส่วนร่วมในงานบำรุงรักษา ไม่ได้เป็นงานเฉพาะฝ่ายบำรุงรักษาเท่านั้น เป็นลักษณะของการบำรุงรักษาโดยมุ่งเน้นการป้องกัน (preventive maintenance) การเกิดปัญหาเป็นหลักเพื่อเพิ่มประสิทธิภาพของเครื่องจักร เครื่องมืออุปกรณ์ให้มากยิ่งขึ้น

ประเภทของการบำรุงรักษา

๑. Breakdown maintenance (การซ่อมบำรุงโดยการซ่อมแซมส่วนที่เสีย) การบำรุงรักษาวิธีนี้ ถือได้ว่าเป็นแนวคิดในงานการบำรุงรักษาที่เก่าแก่ที่สุด ในตำราบางเล่มให้นิยามวิธีการบำรุงรักษาแบบนี้ว่า “ดำเนินการโดยไร้การบำรุงรักษา” เพราะในความเป็นจริงฝ่ายซ่อมบำรุงจะไม่ต้องปฏิบัติงานใด ๆ เลย จนกว่าจะมีรายงานว่าเครื่องจักรชำรุดใช้งานต่อไปไม่ได้ อย่างไรก็ตามการบำรุงรักษาประเภทนี้ก็ยังคงมีใช้ในบางสถานการณ์ เช่น ในอาคารที่ไม่สลับซับซ้อน หรือ มีอุปกรณ์อะไหล่ทดแทนพร้อมอยู่เสมอ หรือ สามารถสั่งซื้อได้อย่างทันทีทันใด โดยที่ค่าใช้จ่ายที่เกิดขึ้นจากการบำรุงรักษาประเภทนี้ควรน้อยกว่าการประยุกต์ใช้วิธีการบำรุงรักษาแบบอื่น เช่น การ บำรุงรักษาหลอดไฟฟ้าที่ปล่อยทิ้งไว้จนหลอดขาด หรือก๊อกน้ำประปาชำรุด

๒. Planned/Preventive maintenance (การบำรุงรักษาตามแผน) เพื่อเป็นการลบล้างข้อบกพร่องในการบำรุงรักษาเมื่อชำรุด จึงได้มีการพัฒนางานทางด้านการบำรุงรักษาตามแผนขึ้นมา กล่าวโดยย่อก็คือ การบำรุงรักษาอาคารและอุปกรณ์ตามระยะเวลาที่กำหนดขึ้นโดยอาจจะได้มาจากประสบการณ์หรือจากคู่มือการใช้งานของระบบและอุปกรณ์นั้น ๆ อย่างไรก็ตามการชำรุดของอาคารและอุปกรณ์โดยไม่คาดฝันก็ไม่สามารถขจัดออกไปได้ เพราะว่าในทางสถิติแล้วการชำรุดของอาคารและอุปกรณ์ไม่ได้เป็นการกระจายตัวแบบสม่ำเสมอ หรือ มีรูปแบบที่แน่นอน ดังนั้นจึงเป็นการยากที่จะเลือกช่วงการบำรุงรักษาตามแผนที่เหมาะสม และในบางกรณีถึงแม้ว่าได้ปฏิบัติการบำรุงรักษาตามแผนแล้วก็ตามยังคงมีโอกาสที่จะเกิดการชำรุดของเครื่องจักรและอุปกรณ์โดยไม่คาดคิดอย่างหลีกเลี่ยงไม่ได้ สรุปได้ว่าการบำรุงรักษาแบบนี้จะทำให้เป็นการเพิ่มค่าใช้จ่ายในการผลิตทั้งทางตรงและทางอ้อม ตัวอย่างการบำรุงรักษาแบบนี้ได้แก่ การ ตรวจเช็คระดับน้ำมันลิฟท์โดยสารที่บริเวณช่องตรวจระดับน้ำมัน การเปลี่ยนถ่ายน้ำมันเครื่องตามระยะเวลา การถอดเปลี่ยนชิ้นส่วนที่สำคัญบางชิ้นตามระยะเวลา ปัญหาหนึ่งที่พบเสมอในการทำการบำรุงรักษาตามระยะเวลา คือ ทำการเปลี่ยนชิ้นส่วนบางชิ้นโดยไม่จำเป็นและในบางกรณีอาจจะเป็นการรบกวนชิ้นส่วนในระบบอื่นโดยไม่จำเป็นรวมถึงอาจจะมีการประกอบกลับชิ้นส่วนไม่ถูกต้อง ซึ่งนับว่าเป็นผลเสียมากกว่าผลดีเสียอีก ในช่วงศตวรรษที่ผ่านมาจึงมีวิธีการบำรุงรักษาแบบใหม่ที่เรียกว่า “การบำรุงรักษาเน้นความเชื่อถือได้” หรือ Reliability centered maintenance (RCM) ซึ่งจะประกอบไปด้วยคำถามหลัก ๗ ข้อ ดังต่อไปนี้

๑. หน้าที่และมาตรฐานสมรรถนะของสินทรัพย์การใช้งานปัจจุบันมีอะไรบ้าง
๒. การที่ไม่สามารถทำตามหน้าที่นั้นจะเป็นไปอย่างไรได้บ้าง
๓. อะไรคือสาเหตุที่จะทำให้เกิดการล้มเหลวของหน้าที่
๔. จะมีเกิดอะไรขึ้นบ้างเมื่อความเสียหายได้ปรากฏขึ้นมา
๕. ความเสียหายที่เกิดขึ้นมานั้นมีความสำคัญอย่างไรบ้าง
๖. จะทำอะไรได้บ้างเพื่อที่จะพยากรณ์หรือป้องกันความเสียหายไม่ให้เกิดขึ้น
๗. ควรทำอะไรหากการพยากรณ์หรือการป้องกันความเสียหายไม่เหมาะสม

๓. Predictive maintenance (การบำรุงรักษาโดยการคาดคะเน) เครื่องจักรสมัยใหม่มีกลไกที่ละเอียดและซับซ้อนกว่าเครื่องจักรในสมัยก่อน ๆ รวมทั้งเป็นการยากที่จะทำการถอดเปลี่ยนหรือทำการตรวจเช็คตามจุดที่สำคัญของงานบำรุงรักษาตามแผน (PM) วิธีการในการบำรุงรักษาโดยการคาดคะเนนับได้ว่าเป็นปรัชญาใหม่ในศาสตร์ของการบำรุงรักษาเครื่องจักร แนวความคิดโดยสรุปก็คือ การใช้วิธีการหรือเทคนิคใหม่ของเครื่องมือวัดชนิดต่าง ๆ เช่น อุปกรณ์ในการวัดแรงสั่นสะเทือน กล้องอินฟาเรด เทอร์โมกราฟฟี่ เป็นต้น โดยพื้นฐานแล้วพอที่จะจัดแบ่งการบำรุงรักษาแบบนี้ออกเป็นวิธีย่อย ๆ คือ Vibration analysis, Oil/wear particle analysis, Performance monitoring, Temperature monitoring

การศึกษาติดตามสภาพเครื่องจักร (Condition monitoring) หรือเรียกอีกชื่อหนึ่งว่าการติดตามสุขภาพเครื่องจักร (Machine health monitoring) ก็จัดได้ว่าเป็นส่วนหนึ่งของการบำรุงรักษา แบบคาดคะเน ความจริงแล้วการทำ CM (Condition monitoring) หรือ MHM (Machine health monitoring) ไม่ใช่ของใหม่เพราะโดยทั่วไปแล้วผู้ควบคุมเครื่องก็ใช้สามัญสำนึกในการบำรุงรักษาเครื่องจักรอยู่แล้ว เช่น การใช้สายตาตรวจดูลักษณะทั่วไป การใช้จมูกดมกลิ่นไหม้ การใช้หูฟังเสียงที่ผิดปกติและการใช้นิ้วสัมผัส (ความร้อน) เป็นต้น อย่างไรก็ตามวิธีการตรวจสอบดังกล่าวจะเป็นลักษณะการประเมินสภาพเครื่องจักรที่ไม่มีข้อยุติที่แน่นอน

ทั้งนี้เนื่องจากความไม่เที่ยงตรงของประสาทสัมผัสของคนแต่ละคนไม่เหมือนกัน ดังนั้นการใช้เครื่องมือวัดเชิงปริมาณสำหรับการบำรุงรักษาแบบคาดคะเนจึงเป็นสิ่งสำคัญ ทั้งนี้เพราะทำให้ได้ข้อสรุปที่ไม่มีการบิดพริ้วได้ในการประเมินสภาพของเครื่องจักร ดังนั้นความหมายของ Predictive maintenance ก็พอที่จะสรุปได้ว่า เมื่อสามารถทราบถึงลักษณะของต้นทุนของการชำรุดจึงพอที่จะสามารถจัดเตรียมการล่วงหน้าสำหรับแรงงานชิ้นส่วนอะไหล่และกำหนดช่วงเวลาการทำงานที่ไม่ขัดกับแผนการทำงานหลักได้

๔. Proactive maintenance (การบำรุงรักษาแบบป้องกันล่วงหน้า) นับเป็นวิธีบำรุงรักษาอาคารและเครื่องจักรโดยที่มุ่งพิจารณารากของปัญหา (Root cause of failure)

๒.๒ มาตรฐานและระเบียบที่เกี่ยวข้อง

การปฏิบัติงานบำรุงรักษาอุปกรณ์เครือข่ายเชิงป้องกันในระบบเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี มีมาตรฐานและระเบียบที่เกี่ยวข้องดังนี้

๑. มาตรฐาน ISO/IEC ๒๗๐๐๒:๒๐๑๓ ซึ่งเป็นมาตรฐานที่ว่าด้วยข้อควรปฏิบัติในการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Code of Practice for Information Security) เพื่อลดความเสี่ยงที่อาจส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ได้กล่าวไว้ในข้อย่อยที่ ๗.๒.๔ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) อุปกรณ์เครือข่ายต่าง ๆ ต้องได้รับการบำรุงรักษาอย่างต่อเนื่องเพื่อให้มีความพร้อมใช้งานตลอดเวลาและใช้งานได้อย่างถูกต้อง

๒. ระเบียบกระทรวงสาธารณสุข ว่าด้วยการควบคุมการใช้วิทยุคมนาคมแบบสังเคราะห์ความถี่ พ.ศ. ๒๕๕๕ หมวดที่ ๒ ศูนย์ควบคุมข่ายและสถานีวิทยุ ข้อ ๑๒ (๓) (ฉ) แนะนำการใช้หรือการบำรุงรักษาเบื้องต้นให้แก่สถานีวิทยุ

๓. ระเบียบสถาบันการแพทย์ฉุกเฉินแห่งชาติ ว่าด้วยการควบคุมการใช้เครื่องวิทยุคมนาคมแบบสังเคราะห์ความถี่ (Synthesizer) ของสถานบันการแพทย์ฉุกเฉินแห่งชาติ พ.ศ. ๒๕๖๒ ข้อ ๗ (๓) จัดทำรายงานการใช้งานเครื่องวิทยุคมนาคม บัญชีคุมสถานะการมี การใช้และที่ตั้งของสถานีวิทยุคมนาคม การเบิกจ่ายเครื่องวิทยุคมนาคมในสังกัด ตามแบบที่สถานีวิทยุคมนาคมแม่ข่ายกลางกำหนดให้เป็นปัจจุบันอยู่เสมอเป็นประจำทุกปี

๒.๓ ปัจจัยที่ส่งผลกระทบต่อการทำงานของอุปกรณ์

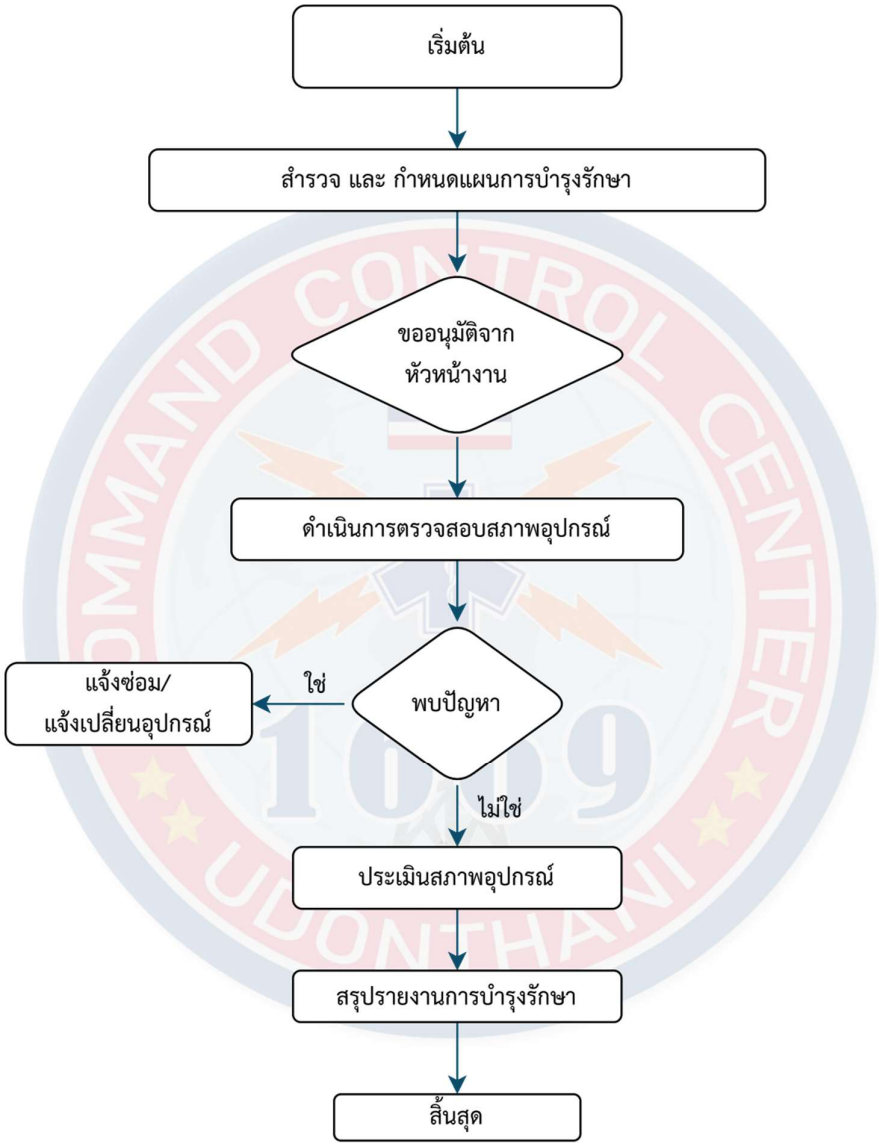
๒.๓.๑ สภาวะแวดล้อมทั้งหมดโดยรอบ เช่น ฝุ่นละออง อุณหภูมิทั้งความร้อนและความชื้นโดยรอบหรือแม้กระทั้งกระแสไฟฟ้าที่ผิดปกติสามารถส่งผลต่อความเสียหายของอุปกรณ์และเพิ่มโอกาสให้อุปกรณ์เครือข่ายเสื่อมสภาพก่อนกำหนดได้

๒.๓.๒ ช่องโหว่ของระบบปฏิบัติการ สำหรับอุปกรณ์ที่มีความสามารถบริหารจัดการได้หรือติดตั้งซอฟต์แวร์ระบบปฏิบัติการหรือซอฟต์แวร์ให้บริการต่าง ๆ มีความเสี่ยงต่อการถูกโจมตีจากผู้ประสงค์ร้าย ส่งผลกระทบต่อผู้ใช้งานระบบสารสนเทศ ผู้ปฏิบัติงานควรปรับปรุงหรืออัพเดตเวอร์ชั่นของซอฟต์แวร์อย่างสม่ำเสมอ

๒.๓.๓ ผู้ใช้งาน หลายครั้งที่เกิดปัญหาจะพบว่าผู้ใช้งานใช้งานระบบผิดประเภทจนเกิดปัญหา เช่น การนำอุปกรณ์ต่อพ่วงเข้าติดตั้งหรือนำโปรแกรมบางชนิดที่ไม่ได้รับมาตรฐานเข้าเชื่อมต่อสู่ระบบคอมพิวเตอร์

๒.๔ ขั้นตอนการปฏิบัติงาน

การปฏิบัติงานบำรุงรักษาอุปกรณ์มีขั้นตอน ดังนี้



ขั้นตอนการปฏิบัติงานบำรุงรักษาอุปกรณ์เครือข่ายแบ่งออกได้ดังนี้

๒.๔.๑ ขั้นตอนการสำรวจอุปกรณ์และกำหนดแผนการบำรุงรักษาอุปกรณ์เครือข่าย

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติงาน ต้องมีการสำรวจอุปกรณ์เครือข่ายและอุปกรณ์ต่อพ่วงที่ติดตั้งให้บริการภายในศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี และที่ติดตั้งภายในห้องศูนย์กลางควบคุมระบบเครือข่าย (Server Room) ผู้ปฏิบัติต้องมีการศึกษารายละเอียดของอุปกรณ์และวิธีการบำรุงรักษาอุปกรณ์ทั้งหมด พร้อมทั้งดำเนินงานวางแผนงานและกำหนดการปฏิบัติงานบำรุงรักษาอุปกรณ์เครือข่าย แล้วนำเสนอต่อหัวหน้าศูนย์ ฯ เพื่อพิจารณาอนุมัติแผนการบำรุงรักษาก่อนการดำเนินงาน

๒.๔.๒ ขั้นตอนการดำเนินการตรวจสอบสภาพอุปกรณ์

เป็นขั้นตอนการดำเนินงานตรวจสภาพอุปกรณ์เครือข่ายและการบำรุงรักษาอุปกรณ์เครือข่าย กรณีพบปัญหาและไม่สามารถแก้ไขได้ให้ดำเนินการแก้ไขและต้องเปลี่ยนอุปกรณ์ให้ดำเนินการแจ้งบริษัทผู้รับผิดชอบให้ดำเนินการเปลี่ยนอุปกรณ์ทันทีตามข้อกำหนดคุณสมบัติการบำรุงรักษาอุปกรณ์เครือข่าย โดยต้องดำเนินการให้แล้วเสร็จตามเวลาที่กาหนด

การตรวจสภาพและบำรุงรักษาอุปกรณ์เครือข่าย สามารถดำเนินการได้ทั้งในรูปแบบ Hardware และ Software การตรวจสภาพและการบำรุงรักษา Hardware เช่น สังเกตสัญลักษณ์ไฟแจ้งเตือนการทำงาน ตรวจการเชื่อมต่อระบบสายสัญญาณต่าง ๆ ทำความสะอาดอุปกรณ์ เป็นต้น การตรวจสภาพและบำรุงรักษา Software เช่น ตรวจการทำงานของระบบปฏิบัติการ ตรวจสอบ Status ของอุปกรณ์ ตรวจสอบ Log Message ของอุปกรณ์ การอัพเดทเฟิร์มแวร์ของอุปกรณ์ เป็นต้น

การจัดเตรียมวัสดุอุปกรณ์ในการดำเนินงานตรวจสภาพและบำรุงรักษาอุปกรณ์เครือข่าย มีดังนี้

๑) เครื่องคอมพิวเตอร์และสายเชื่อมต่อเพื่อใช้ในการตรวจสอบอุปกรณ์ในรูปแบบ Local manage เพื่อตรวจสอบ config และ log file

๒) ผ้าสำหรับเช็ดฝุ่นละอองที่เกาะกับอุปกรณ์เครือข่ายหรือตู้เก็บอุปกรณ์

๓) น้ำยาทำความสะอาด ใช้เช็ดคราบบนอุปกรณ์ที่ทำความสะอาดได้ยาก

๔) เครื่องเป่า/ดูดฝุ่น ภายในตู้เก็บอุปกรณ์หรือภายในอุปกรณ์เครือข่าย

๒.๔.๓ สรุปรายงานการบำรุงรักษาอุปกรณ์

เป็นขั้นตอนสุดท้ายของการปฏิบัติงาน ผู้ปฏิบัติงานจะต้องจัดทำรายงานผลการดำเนินงานบำรุงรักษาและนำเสนอต่อหัวหน้างานให้ทราบ เพื่อใช้เป็นแนวทางในการวางแผนพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ อุดรธานี ต่อไป

๒.๕ ข้อควรระวังในการปฏิบัติงาน

ในการปฏิบัติงานบำรุงรักษาระบบอุปกรณ์ครือข่ายมีข้อควรระวัง ดังนี้

๑. การตรวจสภาพและบำรุงรักษาอุปกรณ์เครือข่ายที่กำลังทำงาน หรือ ให้บริการแก่ผู้ใช้งานอยู่ ควรมีการแจ้งให้ผู้ใช้งานทราบและปฏิบัติงานอย่างระมัดระวังไม่ให้อุปกรณ์หยุดทำงาน อาจมีผลกระทบต่อการผู้ใช้งานระบบสารสนเทศได้

๒. ควรหลีกเลี่ยงการใช้ของเหลวในการทำความสะอาดอุปกรณ์อาจทำให้อุปกรณ์ชำรุดเสียหาย

๓. ก่อนปฏิบัติควรศึกษาคู่มือการบำรุงรักษาอุปกรณ์แต่ละประเภท

๒.๖ ข้อปฏิบัติในการแก้ไขปัญหาสถานการณ์ฉุกเฉิน

๒.๖.๑ กรณีเครื่องลูกข่ายคอมพิวเตอร์ไม่สามารถดำเนินการใช้งานระบบเทคโนโลยีสารสนเทศได้ ให้ดำเนินการ ดังนี้

๒.๖.๑.๑ กรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารได้ตามปกติ ให้เจ้าหน้าที่ผู้พบเหตุขัดข้องแจ้งผู้บำรุงรักษาดูแลระบบทราบโดยเร็วที่สุด

๒.๖.๑.๒ กรณีเกิดเหตุขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ ให้เจ้าหน้าที่ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องคอมพิวเตอร์โดยเร็วเพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายและแจ้งผู้ดูแลระบบทราบ

๒.๖.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่ายขัดข้องให้ดำเนินการดังนี้

๒.๖.๒.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็วแล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒.๖.๒.๒ กรณีไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองไฟฟ้า

๒.๖.๒.๓ ตัดระบบจ่ายไฟ กรณีเกิดเหตุไฟไหม้เครื่องคอมพิวเตอร์และเครือข่าย ให้ตัดระบบจ่ายไฟและใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๒.๖.๒.๔ รีบขนย้ายเครื่องคอมพิวเตอร์และเครือข่ายไปไว้ในที่ปลอดภัย

๒.๖.๒.๕ กรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรองและซ่อมให้สามารถใช้งานได้ให้เร็วที่สุด

๒.๖.๓ กรณีเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ให้ดำเนินการ ดังนี้

๒.๖.๓.๑ กรณีที่เครื่องคอมพิวเตอร์มีโปรแกรมป้องกันไวรัสอยู่แล้วให้ดำเนินการสแกนไวรัส

๒.๖.๓.๒ กรณีที่เครื่องคอมพิวเตอร์ไม่มีโปรแกรมป้องกันไวรัสให้ดำเนินการติดตั้งและใช้งานโปรแกรม Antivirus หรือดำเนินการให้เครื่องสามารถใช้งานได้ตามปกติ

๒.๖.๔ กรณีอุปกรณ์และฮาร์ดแวร์เสียหายให้จัดหาอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด หรือถ้าเกินขีดความสามารถในการดูแล ติดต่อร้านซ่อมหรือผู้เชี่ยวชาญมาดูแลให้เป็นปกติ

๒.๗. แผนกู้ระบบคอมพิวเตอร์กลับสู่สภาพปกติตามเดิม

การกู้ระบบเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์กระจายสัญญาณ (System recovery) โดยปกติระบบเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์กระจายสัญญาณจะต้องอยู่ในสภาพพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องดำเนินการกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ โดยแผนการกู้ระบบคอมพิวเตอร์นี้เป็นวิธีการที่จะทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และฐานข้อมูลสารสนเทศกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยให้ดำเนินการ ดังนี้

๒.๗.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒.๗.๒ เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๒.๗.๓ กรณีเครื่อง Server เสียหาย ใช้คอมพิวเตอร์เครื่องอื่นทดแทนชั่วคราว

๒.๗.๔ นำ Backup ที่ได้สำรองข้อมูลไว้กลับมา Restore โดยผู้ดูแลระบบและทีมดูแลให้ระบบสามารถกลับมาใช้งานตามปกติ ภายใน ๔๘ ชั่วโมง

๒.๗.๕ ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูลสารสนเทศ และความถูกต้องของข้อมูล รวมทั้งระบบเครือข่ายคอมพิวเตอร์อื่น ๆ ที่เกี่ยวข้อง

ระบบการดูแลรักษาเครื่องคอมพิวเตอร์และอุปกรณ์

คอมพิวเตอร์เมื่อใช้ไประยะหนึ่งจะมีการเสื่อมชำรุดไปตามสภาพระยะเวลาที่ใช้งาน ผู้ใช้คอมพิวเตอร์จึงควรเอาใจใส่ดูแลและบำรุงรักษาอย่างเหมาะสมสม่ำเสมอเพื่อเพิ่มอายุการใช้งานของเครื่องคอมพิวเตอร์ซึ่งจะช่วย

ให้สามารถประหยัดงบประมาณในการซ่อมบำรุงหรือการเปลี่ยนอุปกรณ์ จัดระบบสิ่งแวดล้อมที่เหมาะสมกับคอมพิวเตอร์อยู่ในห้องที่มีเครื่องปรับอากาศหรืออากาศถ่ายเทสะดวกไม่ร้อนเกินไป ไม่มีความชื้นมากเกินไป ปราศจากฝุ่น การทำความสะอาดระบบคอมพิวเตอร์ ทำได้ดังนี้

๑. ไม่ควรทำความสะอาดเครื่องคอมพิวเตอร์ในขณะที่เครื่องยังเปิดอยู่ ถ้าจะทำความสะอาดเครื่องควรปิดเครื่องทิ้งไว้ ๕ นาที ก่อนลงมือทำความสะอาด

๒. อย่าใช้ผ้าเปียกหรือผ้าชุ่มน้ำเช็ดคอมพิวเตอร์อย่างเด็ดขาด ใช้ควรผ้าแห้งเท่านั้น

๓. อย่าใช้สบู่ น้ำยาทำความสะอาดกับคอมพิวเตอร์ เพราะจะทำให้ระบบของเครื่องเสียหาย

๔. ไม่ควรฉีดสเปรย์ใด ๆ ไปที่คอมพิวเตอร์ แป้นพิมพ์และอุปกรณ์ต่าง ๆ

๕. ไม่ควรใช้เครื่องดูดฝุ่นกับคอมพิวเตอร์และอุปกรณ์ประกอบอื่น ๆ

๖. ถ้าจำเป็นต้องทำความสะอาดคอมพิวเตอร์ โปรดใช้อุปกรณ์ที่คู่มือแนะนำเท่านั้น

๗. ไม่ควรดื่มน้ำชา กาแฟ เครื่องดื่มต่าง ๆ ในขณะที่ใช้คอมพิวเตอร์

๘. ไม่ควรกินของคบเคี้ยวหรืออาหารใด ๆ ขณะทำงานด้วยเครื่องคอมพิวเตอร์

วิธีแก้ปัญหาในการใช้คอมพิวเตอร์เบื้องต้น

๑. ความร้อน

ความร้อนที่เป็นสาเหตุทำให้คอมพิวเตอร์มีปัญหา ส่วนใหญ่เกิดจากความร้อนของอุปกรณ์อิเล็กทรอนิกส์บนเมนบอร์ดของคอมพิวเตอร์เองวิธีแก้ปัญหา คือ จะต้องรีบระบายความร้อนที่เกิดจากอุปกรณ์ต่าง ๆ ออกไปให้เร็วที่สุด

วิธีแก้ไข

• พัดลมระบายความร้อนทุกตัวในระบบต้องอยู่ในสภาพดี ๑๐๐ % อุณหภูมิที่เหมาะสมที่สุดควรจะอยู่ระหว่าง ๖๐-๗๐ องศาฟาเรนไฮต์

• ใช้เพาเวอร์ซัพพลายขนาดที่ถูกต้อง

• ใช้งานเครื่องในอุณหภูมิที่ปลอดภัย ไม่ตั้งอยู่บริเวณที่มีแสงแดดส่องถึงเป็นเวลานาน ๆ

๒. ฝุ่นผง

ในอากาศมีฝุ่นผงกระจัดกระจายอยู่ในทุกๆ ที่ ฝุ่นผงที่เกาะติดอยู่บนแผงวงจรของคอมพิวเตอร์ทำหน้าที่เสมือนฉนวนป้องกันความร้อน ทำให้ความร้อนที่เกิดขึ้นในระบบไม่สามารถระบายออกสู่สภาพแวดล้อมภายนอก นอกจากนี้อาจไปอุดตันช่องระบายอากาศของเพาเวอร์ซัพพลายหรือฮาร์ดดิสค์ หรืออาจเข้าไปอยู่ระหว่างแผ่นดิสก์กับหัวอ่าน ทำให้แผ่นดิสก์หรือหัวอ่านเกิดความเสียหายได้

วิธีแก้ไข

• ทำความสะอาดภายในเครื่องทุก ๖ เดือน หรือทุกครั้งที่ถอดฝาครอบตัวถังหรือชิ้นส่วนภายนอกให้ใช้สเปรย์ทำความสะอาด

• วงจรภายในให้ใช้ลมเป่าและใช้แปรงขนอ่อน ๆ ปัดฝุ่นออก

• ห้ามสูบบุหรี่ใกล้เครื่องคอมพิวเตอร์

๓. สนามแม่เหล็ก

แม่เหล็กสามารถทำให้ข้อมูลในแผ่นดิสก์หรือฮาร์ดดิสก์สูญหายได้อย่างถาวร แหล่งที่ให้กำเนิดสนามแม่เหล็กในสำนักงานมีอยู่มากมาหลายประเภท อาทิเช่น

- แม่เหล็กติดกระดาษบันทึกบนตู้เก็บแฟ้ม
- คลิปแขวนกระดาษแบบแม่เหล็ก
- ไขควงหัวแม่เหล็ก
- ลำโพง
- มอเตอร์ในพรินเตอร์
- UPS

วิธีแก้ไข

- โยกย้ายอุปกรณ์ที่มีกำลังแม่เหล็กมาก ๆ ให้ห่างจากระบบคอมพิวเตอร์

๔. ไฟฟ้าสถิตย์

ไฟฟ้าสถิตย์สามารถเกิดขึ้นได้ทุกฤดูกาล แต่ในสภาวะที่อากาศแห้ง จะส่งผลให้ความเป็นฉนวนไฟฟ้าสูง ประจุของไฟฟ้าสถิตจะสะสมอยู่เป็นจำนวนมากและหาทางวิ่งผ่านตัวนำไปยังบริเวณที่มีศักย์ไฟฟ้าต่ำกว่า ดังนั้นเมื่อจับอุปกรณ์อิเล็กทรอนิกส์ ประจุของไฟฟ้าสถิตย์จากตัวท่านจะวิ่งไปยังอุปกรณ์อิเล็กทรอนิกส์เหล่านั้น ทำให้อุปกรณ์เกิดความเสียหายได้ แต่ในสภาวะที่มีความชื้นสูง ไฟฟ้าสถิตย์ที่เกิดขึ้นจะรั่วไหลหายไปในระยะเวลาอันสั้น

วิธีแก้ไข

- ควรทำการคายประจุไฟฟ้าสถิตย์ ด้วยการจับต้องโลหะอื่นที่ไม่ใช้ตัวถังเครื่องคอมพิวเตอร์ ก่อนจะสัมผัสอุปกรณ์ต่างๆ ในระบบคอมพิวเตอร์

๕. น้ำและสนิม

น้ำและสนิมเป็นศัตรูตัวร้ายของอุปกรณ์อิเล็กทรอนิกส์ทุกชนิด สนิมที่พบในเมนบอร์ดของคอมพิวเตอร์ มักจะเกิดจากการรั่วซึมของแบตเตอรี่บนเมนบอร์ด ซึ่งถ้าเกิดปัญหานี้ขึ้นจะทำให้เสียงบประมาณในการซ่อมแซมคอมพิวเตอร์

วิธีแก้ไข

- หลีกเลี่ยงการนำของเหลวทุกชนิดมาวางบนโต๊ะคอมพิวเตอร์
- กรณีการรั่วซึมของแบตเตอรี่ แก้ไขได้โดยการเปลี่ยนแบตเตอรี่ใหม่ทุกปี

การบำรุงรักษาตัวเครื่องทั่วไป

- เครื่องจ่ายไฟสำรอง (UPS) ควรติดตั้งร่วมกับตัวเครื่องคอมพิวเตอร์ด้วยเพราะ UPS จะช่วยป้องกันและแก้ปัญหาทางไฟฟ้าไม่ว่าจะเป็นไฟตก ไฟเกินหรือไฟกระชาก อันเป็นสาเหตุที่จะทาให้เกิดความเสียหายของข้อมูลและชิ้นส่วนอื่น ๆ

- การติดตั้งตัวเครื่องคอมพิวเตอร์ ควรติดตั้งในห้องที่มีเครื่องปรับอากาศหรือถ้าไม่มีเครื่องปรับอากาศควรเลือกห้องที่ปลอดฝุ่นมากที่สุดและการติดตั้งตัวเครื่องควรห่างจากผนังพอสมควรเพื่อการระบายความร้อนที่ดี

- การต่อสาย Cable ระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์ต่าง ๆ เช่น Printer Modem Fax หรือส่วนอื่น ๆ จะต้องทำเมื่อ power off เท่านั้น

- อย่าปิด-เปิดเครื่องบ่อย ๆ เกินความจำเป็นเพราะจะทำให้เกิดความเสียหายแก่โปรแกรมที่กำลังทำงาน

• ไม่เคลื่อนย้ายเครื่องคอมพิวเตอร์ขณะที่เครื่องทำงานอยู่เพราะจะทำให้อุปกรณ์เกิดความเสียหายได้
• อย่าเปิดฝาเครื่องขณะใช้งานอยู่ ถ้าต้องการเปิดต้อง power off และถอดปลั๊กไฟก่อน
• ควรศึกษาคู่มือหรือรับการอบรม Software ก่อนการใช้งาน

การบำรุงรักษา Hard Disk

• การติดตั้งเครื่องคอมพิวเตอร์ควรติดตั้งโดยให้ด้านหลังของตัวเครื่องห่างจากฝาผนังไม่น้อยกว่า ๓ นิ้ว เพื่อระบายความร้อนได้ดียิ่งขึ้น

• ควรเลือกใช้โต๊ะทำงานที่แข็งแรงเพื่อป้องกันการโยกไปมาเพราะอาจจะทำให้หัวอ่านของฮาร์ดดิสก์ถูกกระทบกระเทือนได้

• ควรมีการตรวจสอบสถานภาพของ Hard Disk ด้วยโปรแกรม Utility ต่าง ๆ ว่ายังสามารถใช้งานได้ครบ ๑๐๐ % หรือมีส่วนใดของ Hard Disk ที่ใช้งานไม่ได้

การบำรุงรักษา Disk Drive

ช่องอ่านดิสก์เมื่อทำงานไปนาน ๆ หัวอ่านแผ่นดิสก์อาจจะเสื่อมสภาพไปได้ หัวอ่านดิสก์เกิดความสกปรกเนื่องจากมีฝุ่นละอองเข้าไปเกาะที่หัวอ่าน หรือเกิดจากความสกปรกของแผ่นดิสก์ที่มีฝุ่นหรือคราบไขมันจากมือ ผลที่เกิดขึ้นทำให้การบันทึกหรืออ่านข้อมูลจากแผ่นดิสก์ไม่สามารถดำเนินการได้ การดูแลรักษา Disk Drive ควรปฏิบัติดังนี้

• เลือกใช้แผ่นดิสก์ที่สะอาดคือไม่มีคราบฝุ่น ไขมัน หรือรอยขูดขีดใด ๆ
• ใช้น้ำยาล้างหัวอ่านดิสก์ทุก ๆ เดือน
• หลีกเลี่ยงการใช้แผ่นดิสก์เก่าที่เก็บไว้นาน ๆ เพราะจะทำให้หัวอ่าน Disk Drive สกปรกได้ง่าย
• ก่อนนำแผ่นดิสก์ออกจากช่องอ่าน Disk Drive ควรให้ไฟสัญญาณดับก่อน ป้องกันหัวอ่านชำรุด
• ควรเก็บแผ่นดิสก์ไว้ในอุณหภูมิที่เหมาะสม อย่าทิ้งไว้หน้ารถให้ตากแดดนาน ๆ

การบำรุงรักษาหน้าจอ Monitor

ในส่วนของจอภาพนั้นอาจเสียหายได้ เช่น ภาพอาการเลื่อนไหล ภาพล้ม ภาพเต้นหรือไม่มีภาพเลย ซึ่งความเสียหายดังกล่าวจะต้องให้ช่างผู้เชี่ยวชาญเป็นผู้แก้ไข โดยปฏิบัติดังนี้

• อย่าให้วัตถุหรือน้ำไปกระทบหน้าจอคอมพิวเตอร์
• ควรเปิดไฟที่จอก่อนที่สวิตช์ไฟที่ CPU เพื่อ boot เครื่อง
• ไม่ควรปิด ๆ เปิด ๆ เครื่องติดกัน เมื่อปิดเครื่องแล้วทิ้งระยะไว้เล็กน้อยก่อนเปิดใหม่
• ควรปรับความสว่างของจอภาพให้เหมาะสมกับสภาพของห้องทำงาน ถ้าสว่างมากทำให้จอภาพอายุสั้น
• อย่าเปิดฝาหลัง Monitor ซ่อมเอง เพราะจะเป็นอันตรายจากกระแสไฟฟ้าแรงสูง
• เมื่อมีการเปิดจอภาพทิ้งไว้นาน ๆ ควรจะมีการเรียกโปรแกรมถนอมจอภาพ (Screen Sever)

บทที่ ๓
แผนการปฏิบัติงานบำรุงรักษาอุปกรณ์เชิงป้องกัน

๓.๑ กิจกรรมและแผน

๓.๑.๑ กิจกรรมและแผนการบำรุงรักษาเครือข่าย

กิจกรรม	รายละเอียด	มาตรฐานการปฏิบัติงาน	ระยะเวลาดำเนินงาน
๑. สำรวจและจัดทำหมายเลขประจำอุปกรณ์เครือข่าย	- สำรวจจำนวนอุปกรณ์เครือข่ายทั้งหมดและอุปกรณ์ที่เกี่ยวข้องพร้อมทั้งจัดทำทะเบียน	๑ สัปดาห์	๑ ครั้ง/ปี
๒. จัดทำแผนการบำรุงรักษาอุปกรณ์	- วางแผน กำหนดการบำรุงรักษาอุปกรณ์และนำเสนอต่อหัวหน้างาน	๓ วัน	๓ ครั้ง/ปี
๓. ดำเนินการตรวจสภาพซ่อมแซมและบำรุงรักษา	- ดำเนินการตามแผนที่กำหนด	๓ เดือน	ตามสภาพอุปกรณ์
๔. ทดสอบและประเมินผลการใช้งาน	- ทดสอบประสิทธิภาพและประเมินสภาพหลังจากที่ผ่านการบำรุงรักษาและซ่อมแซมเรียบร้อยแล้ว	๓ วัน	๑๒ ครั้ง/ปี
๕. สรุปผลและจัดทำรายงาน	- สรุปและรายงานผลการบำรุงรักษาอุปกรณ์ต่อหัวหน้างาน	๑ วัน	๑๒ ครั้ง/ปี

๓.๑.๒ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์กระจายสัญญาณและอุปกรณ์คอมพิวเตอร์แม่ข่าย

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
- ไฟสถานการณ์ทำงาน	✓			D
- สถานะการทำงานที่แสดงในจอ LCD	✓			D
- สถานะการทำงานด้วยเสียง	✓			D
๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			D
๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			D
๒. การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q

๓.๑.๓ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบโทรศัพท์สายด่วน ๑๖๖๙

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. ชุมสายโทรศัพท์ (ตู้สาขา) IP-PABX				
๑.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	W
- ไฟสถานะการทำงาน				
๑) LAN ไฟสีเขียวสว่างตลอด	✓			E
๒) WAN ไฟสีเขียวสว่างตลอด	✓			E
- สถานะการทำงานที่แสดงในจอ LCD				
“UCM๖๒๐๔ V๑.๗A”,	✓			E
“IP๑: ๑๙๒.๑๖๘.๑.๒๐๐”	✓			E
๑.๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			E
๑.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๑.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๑.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๑.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๑.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๑.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๒. อุปกรณ์ Network Switches				
๒.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๒.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	W
- ไฟสถานะการทำงาน				
๑) System ไฟสีเขียวสว่างตลอด	✓			E
๒) Link/ACT๑-๘ ไฟสีเขียวกระพริบ	✓			E
๓) Link/PoE๑,๒,๘ ไฟสีส้มสว่างตลอด	✓			E
๒.๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			E
๒.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๓. อุปกรณ์จัดเก็บข้อมูล NAS (Network Attach Storage)				
๓.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๓.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	W
- ไฟสถานะการทำงาน				
๑) Power ไฟสีน้ำเงินสว่างตลอด	✓			E

๓.๑.๓ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบโทรศัพท์สายด่วน ๑๖๖๙ (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๓. อุปกรณ์จัดเก็บข้อมูล NAS (Network Attach Storage) (ต่อ)				
๒) STATUS ไฟสีเขียวสว่างตลอด	✓			E
๓) LAN ไฟสีเขียวกระพริบ	✓			E
๔) DISK๑ ไฟสีเขียวสว่างตลอด	✓			E
๓.๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			E
๓.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๓.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๓.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๓.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๓.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๓.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๔. โทรศัพท์ IP Phone				
๔.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๔.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	E
- สถานะการทำงานที่แสดงในจอ LCD	✓			E
- การทำงานของระบบเสียงผ่านลำโพง	✓			E
- การทำงานของระบบเสียงผ่านหูฟัง	✓			E
- การทำงานของระบบเสียงผ่านชุด Headset	✓			E
๔.๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			E
๔.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๔.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๔.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๓.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๔.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๔.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q

๓.๑.๔ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบวิทยุคมนาคม

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. เครื่องวิทยุคมนาคม ชนิดประจำที่ กำลังส่ง ๕๐ วัตต์ ยี่ห้อ Icom รุ่น IC-F๕๑๓๐D				
๑.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	E
- สถานะการทำงานที่แสดงในจอ LCD				
๑) แสดงคลื่นความถี่ที่ใช้งานในปัจจุบัน	✓			E
๒) ระดับความแรงของสัญญาณ	✓			E
- ระบบเสียง และ ไมโครโฟน	✓			E
- ปุ่มกดต่าง ๆ	✓			E
๑.๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			E
๑.๑.๓ ตรวจสอบสายไฟและจุดเชื่อมต่อ	✓			E
๑.๑.๔ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๑.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๑.๒.๑ วัดค่ากำลังส่งที่ออกจากตัวเครื่องวิทยุคมนาคม		✓		Y
๑.๒.๒ การทดสอบสัญญาณความชัดเจน (เช็ค ว ๑๖)		✓		D
๑.๒.๓ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Y
๒. ระบบสายอากาศ (Antenna) และสายนำสัญญาณ				
๒.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๒.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก	✓			Y
- สภาพเสาทาวเวอร์	✓			Y
๒.๑.๒ ตรวจสภาพแวดล้อมจุดติดตั้งสายอากาศ	✓			Y
๒.๑.๓ ตรวจสอบรอยต่อ/จุดเชื่อมต่อของสายสัญญาณ	✓			Y
๒.๑.๔ ตรวจสภาพสายอากาศ/ย่านความถี่ใช้งาน	✓			Y
๒.๑.๕ ตรวจสภาพสายนำสัญญาณ/ย่านความถี่ใช้งาน	✓			Y
๒.๑.๖ ตรวจสอบสายล่อฟ้า/สายดิน	✓			Y
๒.๑.๗ ตรวจสอบสายยึดโยง	✓			Y
๒.๑.๘ ไฟแดงยอดเสา และกลางเสาทาวเวอร์	✓			Y
๒.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๒.๑ วัดค่ากำลังส่งที่ออกจากปลายสายนำสัญญาณ		✓		Y
๒.๒.๒ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Y

๓.๑.๔ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบวิทยุคมนาคม (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๓. เครื่องแปลงไฟฟ้า (Power supply)				
๓.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๓.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	E
- สถานะการทำงานที่แสดงในจอ LCD				
๑) แรงดันไฟ อยู่ระหว่าง ๑๓.๕ – ๑๔.๒ V	✓			E
๒) กระแสไฟ ๐.๒ A	✓			E
- ปุ่มกดต่าง ๆ	✓			E
๓.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๓.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๓.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๓.๒.๑ วัดค่าแรงดันและค่ากระแสไฟ		✓		Y

๓.๑.๕ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบโทรศัพท์ TTRS (ผู้พิการทางการได้ยิน)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	E
- ไฟสถานะการทำงาน	✓			E
- สถานะการทำงานที่แสดงในจอ LCD	✓			E
- สถานะการเชื่อมต่ออินเตอร์เน็ต	✓			E
๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			E
๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๒. การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q

๓.๑.๖ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์โครงข่าย GIN ระบบวิทยุสื่อสาร Radio over IP และระบบโทรศัพท์ Voice over IP

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. ระบบโครงข่าย GIN [เครื่อง Litech-Fiber Optic (Model : CAT Telecom)]				
๑.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
๑.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๑.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๑.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๑.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๑.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๑.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๑.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๒. ระบบโครงข่าย GIN [เครื่อง Nokia Optical Network Terminal (ONT) G-๐๑๐G-Q]				
๒.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๒.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
- ไฟสถานะการทำงาน				
๑) ไฟ Power ไฟสีเขียวสว่างตลอด	✓			E
๒) ไฟ PON ไฟสีเขียวสว่างตลอด	✓			E
๓) ไฟ LAN ไฟสีเขียวสว่างตลอด	✓			E
- ปุ่มกดเปิด-ปิด	✓			E
๒.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๒.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๒.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๒.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๒.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๒.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๓. ระบบโครงข่าย GIN [เครื่อง D-Link DGS-๑๐๐๕A Gigabit Desktop Switch]				
๓.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๓.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M

๓.๑.๖ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์โครงข่าย GIN ระบบวิทยุสื่อสาร Radio over IP และระบบโทรศัพท์ Voice over IP (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
- ไฟสถานะการทำงาน				
๑) ไฟ POWER ไฟสีเขียวสว่างตลอด	✓			E
๒) ไฟช่อง ๑, ๔, ๕ ไฟสีเขียวกระพริบ	✓			E
๓.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๓.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๓.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๓.๒.๑ วัดค่าแรงดันและค่ากระแสไฟ		✓		Q
๓.๒.๒ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๔. ระบบโครงข่าย GIN [เครื่อง Cisco ๑๙๐๐ Series Integrated Services Router]				
๔.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๔.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
- ไฟสถานะการทำงาน				
๑) ไฟ SYS ไฟสีเขียวสว่างตลอด	✓			E
๒) ไฟ ACT ไฟสีเขียวกระพริบ	✓			E
- ปุ่มกดเปิด-ปิด (หลังเครื่อง)	✓			E
๔.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๔.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๔.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๔.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๔.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๔.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๔.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๕. ระบบโครงข่าย GIN [เครื่อง Cisco SF๓๐๐-๒๔ (Switch Managed ๓๐๐ Series)]				
๕.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๕.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
- ไฟสถานะการทำงาน				
๑) ไฟ System ไฟสีเขียวสว่างตลอด	✓			E
๒) LINK/ACT ช่อง ๕, ๖, ๒๔ ไฟสีเขียวกระพริบ	✓			E
๓) PoE ๑๐๐M ช่อง ๕, ๖, ๒๔ ไฟสีเขียวกระพริบ	✓			E
- ปุ่มกดเปิด-ปิด	✓			E

๓.๑.๖ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์โครงข่าย GIN ระบบวิทยุสื่อสาร Radio over IP และระบบโทรศัพท์ Voice over IP (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๕.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๕.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๕.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๕.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๕.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๕.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๕.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๖. ระบบวิทยุสื่อสาร RoIP [เครื่อง Radio Over IP Gateway ยี่ห้อ Icom รุ่น VE-PG๓]				
๖.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๖.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
- ไฟสถานะการทำงาน				
๑) ไฟ PWR/MSG ไฟสีเขียวสว่างตลอด	✓			E
๒) ไฟ V/RoIP ไฟสีเขียวสว่างตลอด	✓			E
๖.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๖.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๖.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๖.๒.๑ วัดค่าแรงดันและค่ากระแสไฟ		✓		Q
๖.๒.๒ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๗. ระบบวิทยุสื่อสาร RoIP [เครื่องวิทยุคมนาคม VHF/FM ยี่ห้อ Icom รุ่น IC-FR๕๑๐๐H]				
๗.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๗.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
- ไฟสถานะการทำงาน				
๑) A PWR ไฟสีเขียวสว่างตลอด	✓			E
- สถานะการทำงานที่แสดงในจอ LCD				
๑) แสดงคลื่นความถี่ F๑-๑๕๐.๔๗๕	✓			E
- ระบบเสียง และ ไมโครโฟน	✓			E
- ปุ่มกดต่าง ๆ	✓			E
๗.๑.๒ ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓			E
๗.๑.๓ ตรวจสอบสายไฟและจุดเชื่อมต่อ	✓			E
๗.๑.๔ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E

๓.๑.๖ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์โครงข่าย GIN ระบบวิทยุสื่อสาร Radio over IP และระบบโทรศัพท์ Voice over IP (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๗.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๗.๒.๑ วัดค่ากำลังส่งที่ออกจากตัวเครื่องวิทยุคมนาคม		✓		Y
๗.๒.๒ การทดสอบสัญญาณความชัดเจน (เช็ค ว ๑๖)		✓		D
๗.๒.๓ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Y
๘. ระบบวิทยุสื่อสาร RoIP [ระบบสายอากาศ (Antenna) และสายนำสัญญาณ]				
๘.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๘.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพทั่วไป/ฝุ่นละออง/ความสกปรก	✓			Y
๘.๑.๒ ตรวจสภาพแวดล้อมจุดติดตั้งสายอากาศ	✓			Y
๘.๑.๓ ตรวจสอบรอยต่อ/จุดเชื่อมต่อของสายสัญญาณ	✓			Y
๘.๑.๔ ตรวจสภาพสายอากาศ/ย่านความถี่ใช้งาน	✓			Y
๘.๑.๕ ตรวจสภาพสายนำสัญญาณ/ย่านความถี่ใช้งาน	✓			Y
๘.๑.๖ ตรวจสอบสายล่อฟ้า/สายดิน	✓			Y
๘.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๘.๒.๑ วัดค่ากำลังส่งที่ออกจากปลายสายนำสัญญาณ		✓		Y
๘.๒.๒ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Y
๙. ระบบวิทยุสื่อสาร RoIP [เครื่องแปลงไฟฟ้า (Power supply)]				
๙.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๙.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	M
- ไฟสถานะการทำงาน				
๑) ไฟ ON ไฟสีแดงสว่างตลอด	✓			E
๒) ไฟ POWER ไฟสีแดงสว่างตลอด	✓			E
- ปุ่มกดเปิด-ปิด	✓			E
๙.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๙.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๙.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๙.๒.๑ วัดค่าแรงดันและค่ากระแสไฟ		✓		Y
๑๐. ระบบโทรศัพท์ [IP Phone]				
๔.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๔.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	E

๓.๑.๖ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์โครงข่าย GIN ระบบวิทยุสื่อสาร Radio over IP และระบบโทรศัพท์ Voice over IP (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
- ไฟสถานะการทำงาน	✓			E
- สถานะการทำงานที่แสดงในจอ LCD	✓			E
- สถานะการเชื่อมต่ออินเตอร์เน็ต	✓			E
๔.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๔.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๔.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๔.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๔.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๔.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๔.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q

๓.๑.๗ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบอินเตอร์เน็ต

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. Modem HUAWEI AIS FIBER				
๑.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	Q
- ไฟสถานะการทำงาน				
๑) POWER ไฟสีเขียวสว่างตลอด	✓			E
๒) PON ไฟสีเขียวสว่างตลอด	✓			E
๓) LAN ไฟสีเขียวกระพริบ	✓			E
- ปุ่มกดเปิด-ปิด	✓			E
๑.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๑.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๑.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๑.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๑.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๑.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๑.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q

๓.๑.๗ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบอินเตอร์เน็ต (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๒. Router Internet AIS Fiber				
๒.๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๒.๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	Q
- ไฟสถานะการทำงาน				
๑) Power ไฟสีเขียวสว่างตลอด	✓			E
๒) Broadband ไฟสีเขียวกระพริบ	✓			E
๓) Internet ไฟสีเขียวกระพริบ	✓			E
๔) ๒.๔ GHz. ไฟสีเขียวกระพริบ	✓			E
๕) ๕ GHz. ไฟสีเขียวกระพริบ	✓			E
๖) Phone ไฟสีเขียวกระพริบ	✓			E
- ปุ่มกดเปิด-ปิด	✓			E
๒.๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๒.๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๒.๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๒.๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๒.๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๒.๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q

๓.๑.๘ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบโทรศัพท์ภายในโรงพยาบาลอุดรธานี

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	E
- ไฟสถานะการทำงาน	✓			E
- สถานะการทำงานที่แสดงในจอ LCD	✓			E
๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E

๓.๑.๘ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบโทรศัพท์ภายในโรงพยาบาลอุดรธานี (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๑ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๒.๒ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๒.๓ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q

๓.๑.๙ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์สำรองไฟ

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑ การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑ ตรวจสภาพอุปกรณ์โดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	E
- ไฟสถานะการทำงาน	✓			E
- สถานะการทำงานที่แสดงในจอ LCD	✓			E
- สถานะการทำงานด้วยเสียง	✓			E
๑.๒ ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓			E
๑.๓ ตรวจสอบอุณหภูมิของอุปกรณ์	✓			E
๒ การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๑ ทดสอบประสิทธิภาพของแบตเตอรี่		✓		Q
๒.๒ วัดค่าแรงดันและค่ากระแสไฟ		✓		Q

๓.๑.๑๐ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบคอมพิวเตอร์

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. การตรวจสภาพและบำรุงรักษาเชิงกายภาพ				
๑.๑ ตรวจสภาพโดยทั่วไป				
- สภาพฝุ่นละออง/ความสกปรก			✓	Q
- ไฟสถานะการทำงาน	✓			E
- สถานะการทำงานที่แสดงในจอ LCD	✓			E
- สถานะการทำงานด้วยเสียง	✓			E
- การเชื่อมต่อสายสัญญาณ	✓			E
- อุณหภูมิของอุปกรณ์	✓			E

๓.๑.๑๐ รายการตรวจสภาพและบำรุงรักษาอุปกรณ์ระบบคอมพิวเตอร์ (ต่อ)

รายการตรวจสภาพซ่อมแซมและบำรุงรักษา	วิธีปฏิบัติ			ความถี่
	ตรวจจากการสังเกต	ตรวจจากการทดสอบ	ทำความสะอาด	
๑. การตรวจสภาพและบำรุงรักษาเชิงกายภาพ (ต่อ)				
๑.๒ เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง				
- Monitor	✓			E
- Keyboard	✓			E
- Mouse	✓			E
- Mainboard		✓		M
- Memory		✓		M
- Hard disk		✓		M
- VGA Card		✓		M
- CPU		✓		M
- Printer		✓		M
- Scanner		✓		M
๒. การตรวจสภาพและบำรุงรักษาเชิงระบบ				
๒.๑ การตั้งค่าและการสำรองไฟล์ Config		✓		Q
๒.๒ ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ		✓		Q
๒.๓ ตรวจประวัติการใช้งานผ่าน Log Message		✓		Q
๒.๔ ทดสอบการทำงานของเครื่องด้วยโปรแกรม		✓		Q
๒.๕ ตรวจสอบโปรแกรมสแกนไวรัส		✓		M
๒.๖ Web Cleanup		✓		M
๒.๗ Disk Cleanup		✓		M
๒.๘ Clean up Temporary files		✓		M
๒.๙ Clean up system files		✓		M
๒.๑๐ Defragment and optimize drives		✓		M

หมายเหตุ : ความถี่ของการปฏิบัติงาน	
✓ = การปฏิบัติ	M = ปฏิบัติทุกเดือน
E = ปฏิบัติทุกเวร	Q = ปฏิบัติทุก ๓ เดือน
D = ปฏิบัติทุกวัน	H = ปฏิบัติทุก ๖ เดือน
W = ปฏิบัติทุกสัปดาห์	Y = ปฏิบัติทุกปี

บทที่ ๕

สรุปผลการดำเนินงาน

๑. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำเวร</u>

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
อุปกรณ์ระบบโทรศัพท์สายด่วน ๑๖๖๙				
๑	**ชุมสายโทรศัพท์ (ตู้สาขา) IP-PABX**	✓		
	- ไฟสถานะการทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๒	**อุปกรณ์ Network Switches**			
	- ไฟสถานะการทำงาน	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๓	**อุปกรณ์จัดเก็บข้อมูล NAS (Network Attach Storage)**			
	- ไฟสถานะการทำงาน	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๔	**โทรศัพท์ IP Phone**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- การทำงานของระบบเสียงผ่านลำโพง	✓		
	- การทำงานของระบบเสียงผ่านหูฟัง	✓		
	- การทำงานของระบบเสียงผ่านชุด Headset	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
อุปกรณ์ระบบวิทยุคมนาคม				
๑	**เครื่องวิทยุคมนาคม ยี่ห้อ Icom รุ่น IC-F๕๑๓๐D**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- ระบบเสียง และ ไมโครโฟน	✓		
	- ปุ่มกดต่าง ๆ	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบสายไฟและจุดเชื่อมต่อ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		

๑. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำเวร</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
๒	**เครื่องแปลงไฟฟ้า (Power supply)**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
อุปกรณ์ระบบโทรศัพท์ TTRS (ผู้พิการทางการได้ยิน)				
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- ไฟสถานะการทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- สถานะการเชื่อมต่ออินเตอร์เน็ต	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
อุปกรณ์โครงข่าย GIN				
๑	**เครื่อง Litech-Fiber Optic**			
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๒	**เครื่อง Nokia Optical Network Terminal**			
	- ไฟสถานะการทำงาน	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๓	**เครื่อง D-Link DGS-๑๐๐๕A**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- ไฟสถานะการทำงาน	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๔	**เครื่อง Cisco ๑๙๐๐ Integrated Services Router**			
	- ไฟสถานะการทำงาน	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๕	**เครื่อง Cisco SF๓๐๐-๒๔ (Switch Managed)**			
	- ไฟสถานะการทำงาน	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ปุ่มกดเปิด-ปิด	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		

๑. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำเวร</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
อุปกรณ์โครงข่าย GIN ระบบวิทยุคมนาคม RoIP				
๑	**Radio Over IP Gateway ยี่ห้อ Icom รุ่น VE-PG๓**			
	- ไฟสถานะการทำงาน	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๒	**เครื่องวิทยุคมนาคม Icom รุ่น IC-FR๕๑๐๐H**			
	- ไฟสถานะการทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- ระบบเสียง และ ไมโครโฟน	✓		
	- ปุ่มกดต่าง ๆ	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบสายไฟและจุดเชื่อมต่อ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๓	**เครื่องแปลงไฟฟ้า (Power supply)**			
	- ไฟสถานะการทำงาน	✓		
	- ปุ่มกดต่าง ๆ	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
อุปกรณ์โครงข่าย GIN ระบบโทรศัพท์ VoIP				
๑	**โทรศัพท์ IP Phone**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- ไฟสถานะการทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- สถานะการเชื่อมต่ออินเตอร์เน็ต	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
อุปกรณ์ระบบอินเตอร์เน็ต				
๑	**Modem HUAWEI AIS FIBER**			
	- ไฟสถานะการทำงาน	✓		
	- ปุ่มกดต่าง ๆ	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
๒	**Router Internet AIS Fiber**			
	- ไฟสถานะการทำงาน	✓		

๑. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำเวร</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
	- ปุ่มกดต่าง ๆ	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
ระบบโทรศัพท์ภายในโรงพยาบาลอุดรธานี				
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- ไฟสถานะการทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
อุปกรณ์สำรองไฟ				
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- ไฟสถานะการทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- ตรวจสอบสายไฟ ฟิวส์และจุดเชื่อมต่อต่าง ๆ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		
อุปกรณ์ระบบคอมพิวเตอร์				
	- ไฟสถานะการทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- สถานะการทำงานด้วยเสียง	✓		
	- การเชื่อมต่อสายสัญญาณ	✓		
	- อุณหภูมิของอุปกรณ์	✓		
	- Monitor	✓		
	- Keyboard	✓		
	- Mouse	✓		

๒. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำวัน</u>

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
๑. อุปกรณ์กระจายสัญญาณและอุปกรณ์คอมพิวเตอร์แม่ข่าย				
	- ไฟสถานการณ์ทำงาน	✓		
	- สถานะการทำงานที่แสดงในจอ LCD	✓		
	- สถานะการทำงานด้วยเสียง	✓		
	- ตรวจสอบระบบการเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสอบอุณหภูมิของอุปกรณ์	✓		

๒. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำวัน</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
๒. เครื่องวิทยุคมนาคม ยี่ห้อ Icom รุ่น IC-F๕๑๓๐D				
	- การทดสอบสัญญาณความชัดเจน (เช็ค ว ๑๖)	✓		
๓. เครื่องวิทยุคมนาคม Icom รุ่น IC-FR๕๑๐๐H				
	- การทดสอบสัญญาณความชัดเจน (เช็ค ว ๑๖)	✓		

๓. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำสัปดาห์</u>

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
อุปกรณ์ระบบโทรศัพท์สายด่วน ๑๖๖๙				
๑	**ชุมสายโทรศัพท์ (ตู้สาขา) IP-PABX**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
๒	**อุปกรณ์ Network Switches**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
๓	**อุปกรณ์จัดเก็บข้อมูล NAS (Network Attach Storage)**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		

๔. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำเดือน</u>

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
อุปกรณ์โครงข่าย GIN				
๑	**เครื่อง Litech-Fiber Optic**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
๒	**เครื่อง Nokia Optical Network Terminal**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
๓	**เครื่อง D-Link DGS-๑๐๐๕A**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
๔	**เครื่อง Cisco ๑๙๐๐ Integrated Services Router**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
๕	**เครื่อง Cisco SF๓๐๐-๒๔ (Switch Managed)**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
อุปกรณ์โครงข่าย GIN ระบบวิทยุคมนาคม RoIP				
๑	**Radio Over IP Gateway ยี่ห้อ Icom รุ่น VE-PG๓**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		

๔. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำเดือน</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
๒	**เครื่องวิทยุคมนาคม Icom รุ่น IC-FR๕๑๐๐H**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
๓	**เครื่องแปลงไฟฟ้า (Power supply)**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
อุปกรณ์ระบบคอมพิวเตอร์				
	- Mainboard	✓		
	- Memory	✓		
	- Hard disk	✓		
	- VGA Card	✓		
	- CPU	✓		
	- Printer	✓		
	- Scanner	✓		
	- ตรวจสอบโปรแกรมสแกนไวรัส	✓		
	- Web Cleanup	✓		
	- Disk Cleanup	✓		
	- Clean up Temporary files	✓		
	- Clean up system files	✓		
	- Defragment and optimize drives	✓		

๕. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำทุก ๓ เดือน</u>

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
๑. อุปกรณ์กระจายสัญญาณและอุปกรณ์คอมพิวเตอร์แม่ข่าย				
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
อุปกรณ์ระบบโทรศัพท์สายด่วน ๑๖๖๙				
๑	**ชุมสายโทรศัพท์ (ตู้สาขา) IP-PABX**	✓		
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		

๕. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำทุก ๓ เดือน</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
๓	**อุปกรณ์จัดเก็บข้อมูล NAS (Network Attach Storage)**			
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๔	**โทรศัพท์ IP Phone**			
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
อุปกรณ์ระบบโทรศัพท์ TTRS (ผู้พิการทางการได้ยิน)				
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
อุปกรณ์โครงข่าย GIN				
๑	**เครื่อง Litech-Fiber Optic**			
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๒	**เครื่อง Nokia Optical Network Terminal**			
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๓	**เครื่อง D-Link DGS-๑๐๐๕A**			
	- วัดค่าแรงดันและค่ากระแสไฟ	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๔	**เครื่อง Cisco ๑๙๐๐ Integrated Services Router**			
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		

๕. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำทุก ๓ เดือน</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
๕	**เครื่อง Cisco SF๓๐๐-๒๔ (Switch Managed)**			
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
อุปกรณ์โครงข่าย GIN ระบบวิทยุคมนาคม RoIP				
๑	**Radio Over IP Gateway ยี่ห้อ Icom รุ่น VE-PG๓**			
	- วัดค่าแรงดันและค่ากระแสไฟ	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
อุปกรณ์โครงข่าย GIN ระบบโทรศัพท์ VoIP				
๑	**โทรศัพท์ IP Phone**			
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
อุปกรณ์ระบบอินเตอร์เน็ต				
๑	**Modem HUAWEI AIS FIBER**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๒	**Router Internet AIS Fiber**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
ระบบโทรศัพท์ภายในโรงพยาบาลอุดรธานี				
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		

๕. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำทุก ๓ เดือน</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
อุปกรณ์สำรองไฟ				
	- ทดสอบประสิทธิภาพของแบตเตอรี่	✓		
	- วัดค่าแรงดันและค่ากระแสไฟ	✓		
อุปกรณ์ระบบคอมพิวเตอร์				
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- การตั้งค่าและการสำรองไฟล์ Config	✓		
	- ตรวจสอบเวอร์ชั่นซอฟต์แวร์ของระบบปฏิบัติการ	✓		
	- ตรวจประวัติการใช้งานผ่าน Log Message	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		

๖. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำทุกปี</u>

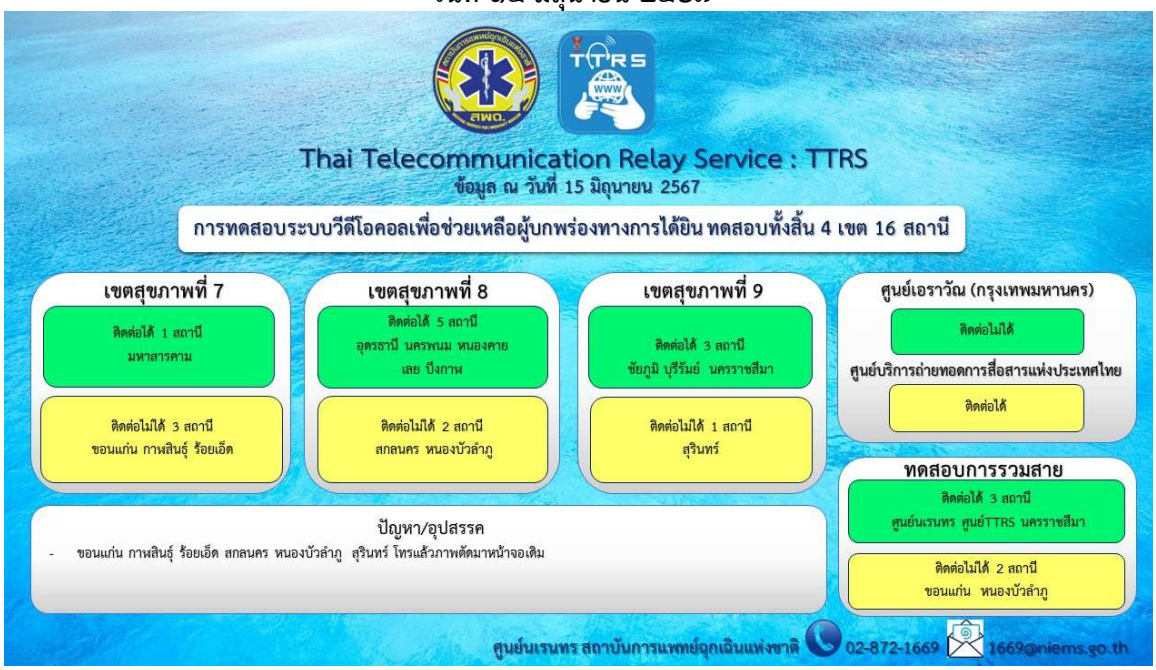
NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
อุปกรณ์ระบบวิทยุคมนาคม				
๑	**เครื่องวิทยุคมนาคม ยี่ห้อ Icom รุ่น IC-F๕๑๓๐D**			
	- วัดค่ากำลังส่งที่ออกจากตัวเครื่องวิทยุคมนาคม	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๒	**ระบบสายอากาศ (Antenna) และสายนำสัญญาณ**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- สภาพเสาทาวเวอร์	✓		
	- ตรวจสภาพแวดล้อมจุดติดตั้งสายอากาศ	✓		
	- ตรวจสอบรอยต่อ/จุดเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสภาพสายอากาศ/ย่านความถี่ใช้งาน	✓		
	- ตรวจสภาพสายนำสัญญาณ/ย่านความถี่ใช้งาน	✓		
	- ตรวจสอบสายล่อฟ้า/สายดิน	✓		
	- ตรวจสอบสายยึดโยง	✓		
	- ไฟแดงยอดเสา และกลางเสาทาวเวอร์	✓		
	- วัดค่ากำลังส่งที่ออกจากปลายสายนำสัญญาณ	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๓	**เครื่องแปลงไฟฟ้า (Power supply)**			
	วัดค่าแรงดันและค่ากระแสไฟ	✓		

๖. สรุปกิจกรรมและแผนการบำรุงรักษา <u>ประจำทุกปี</u> (ต่อ)

NO.	Description	Result of Checking		Detail of Not OK
		OK	Not OK	
อุปกรณ์โครงข่าย GIN ระบบวิทยุคมนาคม RoIP				
๑	**เครื่องวิทยุคมนาคม Icom รุ่น IC-FR๕๑๐๐H**			
	- วัดค่ากำลังส่งที่ออกจากตัวเครื่องวิทยุคมนาคม	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๒	**ระบบสายอากาศ (Antenna) และสายนำสัญญาณ**			
	- สภาพฝุ่นละออง/ความสกปรก	✓		
	- สภาพเสาทาวเวอร์	✓		
	- ตรวจสภาพแวดล้อมจุดติดตั้งสายอากาศ	✓		
	- ตรวจสอบรอยต่อ/จุดเชื่อมต่อของสายสัญญาณ	✓		
	- ตรวจสภาพสายอากาศ/ย่านความถี่ใช้งาน	✓		
	- ตรวจสภาพสายนำสัญญาณ/ย่านความถี่ใช้งาน	✓		
	- ตรวจสอบสายล่อฟ้า/สายดิน	✓		
	- ตรวจสอบสายยึดโยง	✓		
	- ไฟแดงยอดเสา และกลางเสาทาวเวอร์	✓		
	- วัดค่ากำลังส่งที่ออกจากปลายสายนำสัญญาณ	✓		
	- ทดสอบการทำงานของเครื่องด้วยโปรแกรม	✓		
๓	**เครื่องแปลงไฟฟ้า (Power supply)**			
	วัดค่าแรงดันและค่ากระแสไฟ	✓		

ผลการทดสอบระบบวีดีโอคอลเพื่อช่วยเหลือผู้บกพร่องทางการได้ยิน
Thai Telecommunication Relay Service: TTRS

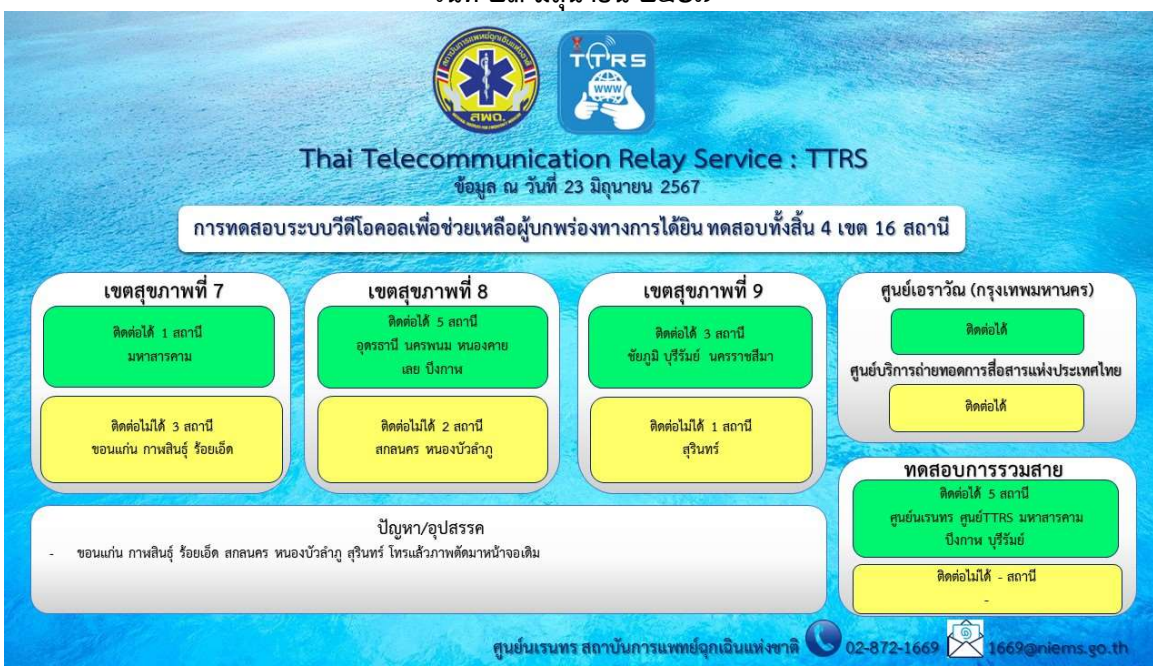
วันที่ ๑๕ มิถุนายน ๒๕๖๗



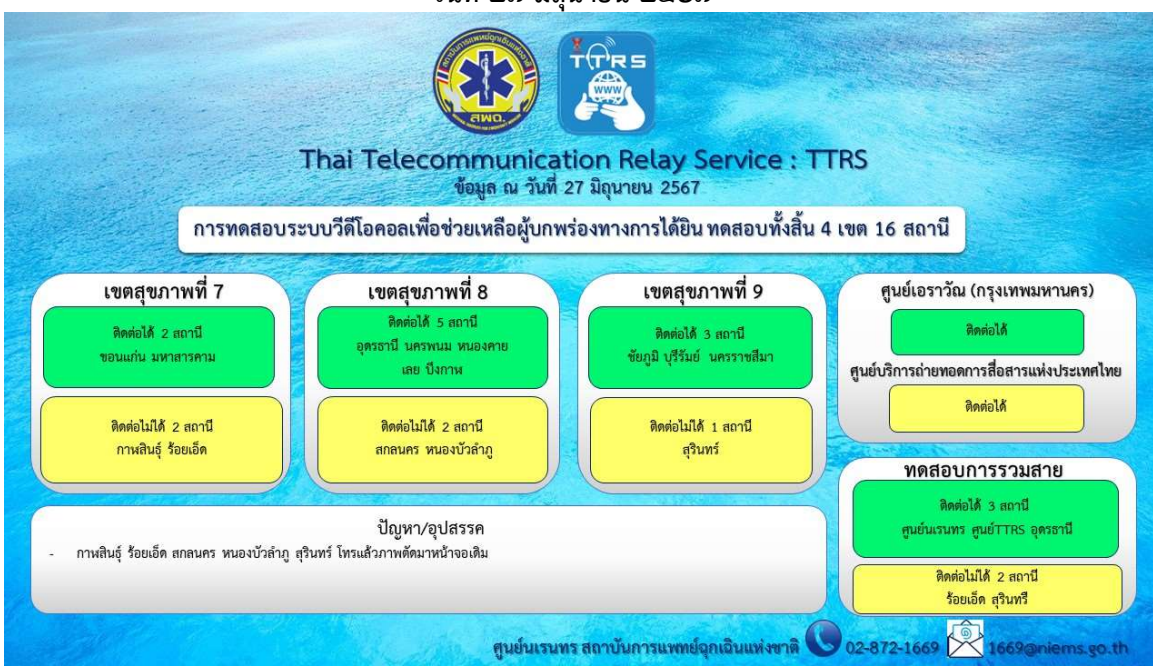
วันที่ ๑๙ มิถุนายน ๒๕๖๗

ผลการทดสอบระบบวีดีโอคอลเพื่อช่วยเหลือผู้บกพร่องทางการได้ยิน (ต่อ)
Thai Telecommunication Relay Service: TTRS

วันที่ ๒๓ มิถุนายน ๒๕๖๗

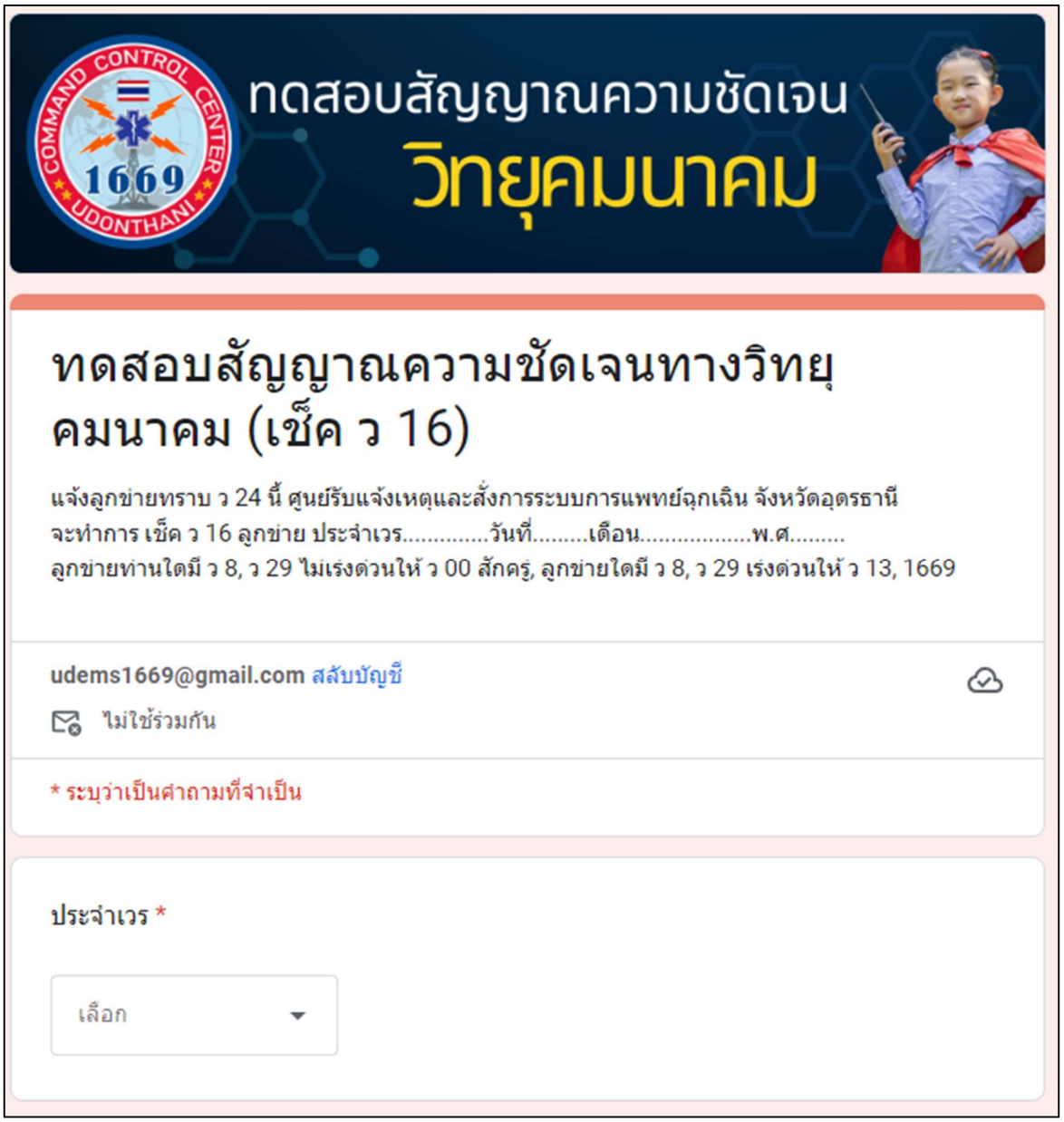


วันที่ ๒๗ มิถุนายน ๒๕๖๗



ผลการวิเคราะห์คุณภาพของสายอากาศ (Antenna) และสายนำสัญญาน
ระบบวิทยุคมนาคม VHF/FM คลื่นความถี่ ๑๕๔.๙๒๕ MHz.

การทดสอบสัญญาณความชัดเจนทางวิทยุคมนาคม (เช็ค ว ๑๖)



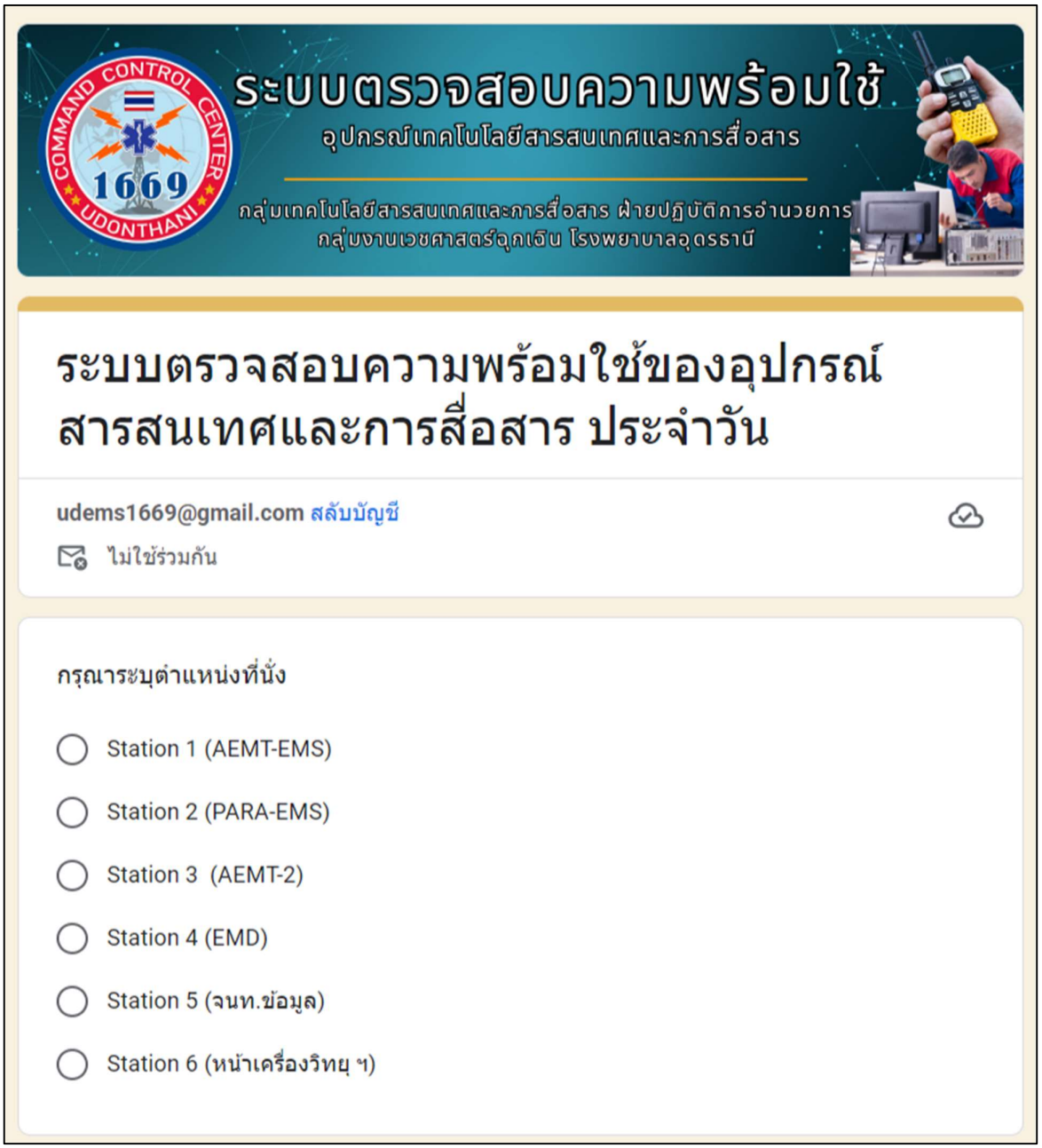
Google Form

ทดสอบ ว ๑๖

Google Sheet

รายงานผล

การตรวจความพร้อมใช้ของระบบคอมพิวเตอร์สารสนเทศและการสื่อสาร



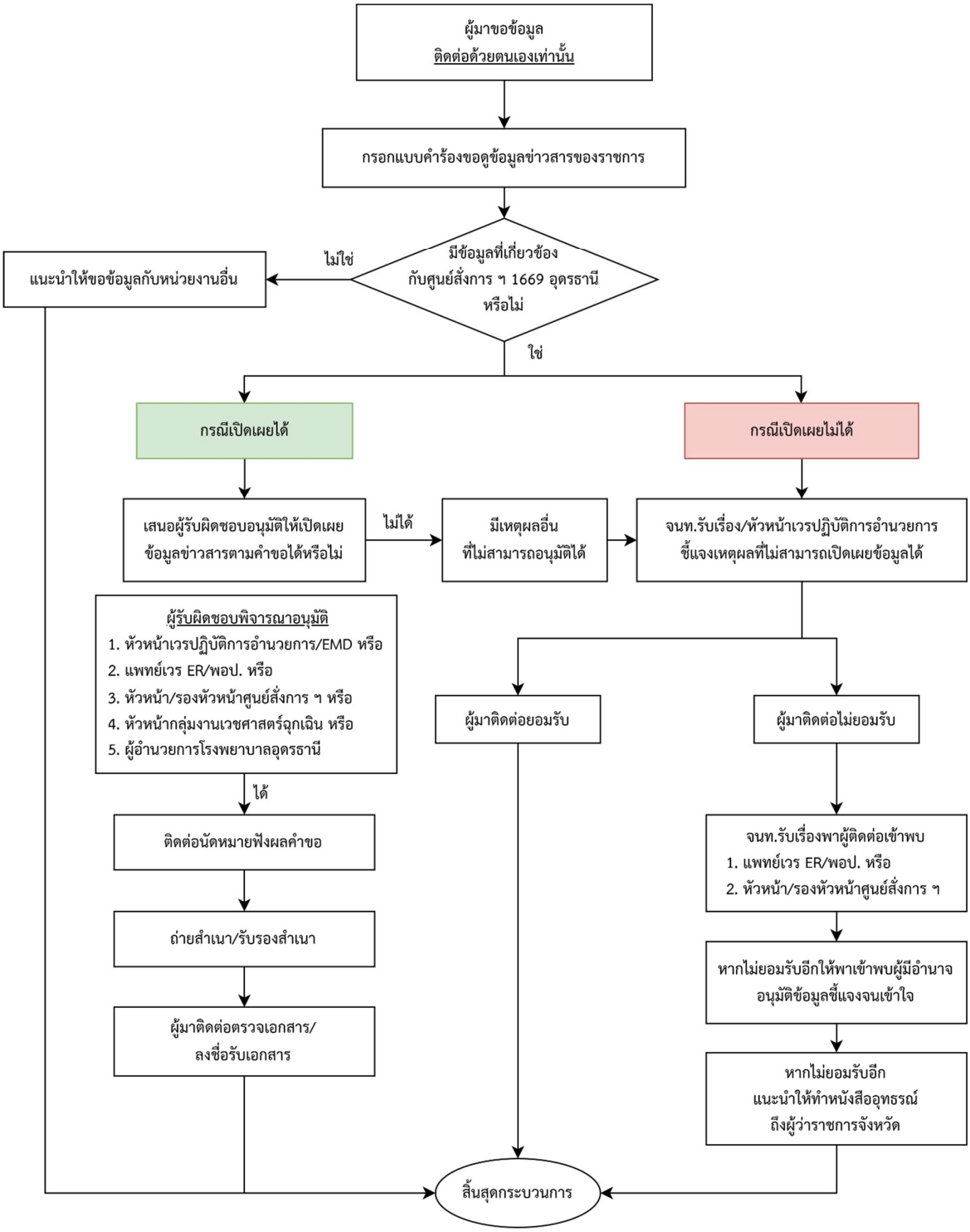
Google FORMS

ตรวจเช็คอุปกรณ์ IT

Google Sheets

รายงานผล
ตรวจเช็คอุปกรณ์ IT

ขั้นตอนการให้บริการข้อมูลข่าวสาร ณ ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี



<u>หมายเหตุ</u> กรอบเวลาให้บริการให้เป็นไปตาม พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ (เนื่องจาก พ.ร.บ. ดังกล่าวมิได้กำหนดระยะเวลาในการให้ข้อมูลข่าวสารแก่ผู้ขอไว้ ดังนั้นเจ้าหน้าที่ของรัฐเมื่อได้รับคำขอข้อมูลข่าวสารจากประชาชนแล้วมีหน้าที่จัดให้แก่ประชาชนหรือมีคำสั่งไม่เปิดเผยข้อมูลข่าวสารตามที่ขอโดยเร็ว

ขั้นตอนการให้บริการข้อมูลข่าวสาร ณ ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี (ต่อ)

ข้อมูลข่าวสารที่เปิดเผยได้	ข้อมูลข่าวสารที่เปิดเผยไม่ได้
๑. วันและเวลาที่เกิดเหตุ	๑. ลำดับผู้ป่วย (CN)
๒. เลขที่สั่งการจังหวัด	๒. ชื่อ/รหัสผู้แจ้งเหตุ
๓. เลขที่ปฏิบัติการ (ON)	๓. หมายเลขโทรศัพท์ผู้แจ้งเหตุ
๔. ช่องทางการรับแจ้งเหตุ	๔. สถานที่เกิดเหตุ (กรณีเกิดเหตุที่บ้านเรือน)
๕. สถานที่เกิดเหตุ (กรณีเกิดเหตุที่ไม่ใช่บ้านเรือน)	๕. ข้อมูลผู้ออกปฏิบัติการ
๖. อาการนำสำคัญ (CBD)	๖. ชื่อ-สกุล ผู้ป่วย
๗. อาการ/เหตุการณ์/รายละเอียดอื่น ๆ	๗. HN
๘. การให้รหัสความรุนแรง (IDC)	๘. หมายเลขบัตรประจำตัวประชาชน
๙. ชื่อหน่วยปฏิบัติการ/ชื่อชุดปฏิบัติการ	๙. เลขที่หนังสือเดินทาง (กรณีต่างชาติ)
๑๐. ข้อมูลเวลาตั้งแต่รับแจ้งเหตุจนกลับถึงฐาน	๑๐. สิทธิการรักษา/ประกันภัย
๑๑. ข้อมูลเลขไมล์ตั้งแต่ออกปฏิบัติการจนถึงฐาน	๑๑. ข้อมูลทะเบียนรถที่เกิดอุบัติเหตุ
๑๒. การให้รหัสความรุนแรง ณ จุดเกิดเหตุ	๑๒. ข้อมูลประวัติการให้บริการผู้ป่วย
๑๓. การออกปฏิบัติการ (มีการรักษา/ไม่มีการรักษา)	๑๓. การวินิจฉัยโรค
๑๔. เพศ/อายุของผู้ป่วย	
๑๔. ชื่อสถานพยาบาลที่นำส่ง	
๑๕. ข้อมูลระดับการคัดแยกผู้ป่วย ณ ห้องฉุกเฉิน	
๑๖. ข้อมูลการ Admitted	

<u>แบบคำร้องขอดูข้อมูลข่าวสารของราชการ</u>

ศูนย์รับแจ้งเหตุและสั่งการ ๑๖๖๙ จังหวัดอุดรธานี กลุ่มงานเวชศาสตร์ฉุกเฉิน โรงพยาบาลอุดรธานี

เขียนที่.....

วันที่.....เดือน.....พ.ศ.....

เรื่อง ขอข้อมูลข่าวสารของราชการ

เรียน .....

ข้าพเจ้า.....อาชีพ.....

อยู่บ้านเลขที่.....หมู่ที่.....ถนน.....ตำบล.....

อำเภอ.....จังหวัดอุดรธานี.....โทรศัพท์.....

มีความประสงค์ขอดูข้อมูลข่าวสาร ดังต่อไปนี้

๑.....

.....

๒.....

.....

๓.....

.....

จึงเรียนมาเพื่อโปรดดำเนินการให้ตามความประสงค์ของข้าพเจ้าต่อไป

ขอแสดงความนับถือ

ลงชื่อ.....

(.....)

☐ อนุมัติให้เปิดเผยข้อมูลข่าวสารตามคำขอได้

☐ ไม่อนุมัติให้เปิดเผยข้อมูลข่าสารตามคำขอ

เนื่องจาก.....

.....

ลงชื่อ.....

(.....)

วันที่.....เดือน..... พ.ศ.....