

การวิเคราะห์ช่องว่างของระบบที่เป็นอยู่ปัจจุบันกับมาตรฐาน/เป้าหมายที่กำหนด

กรมอนามัย กระทรวงสาธารณสุข มีภารกิจในการส่งเสริมให้ประชาชนมีสุขภาพดี โดยมีการศึกษา วิเคราะห์ วิจัย พัฒนาและถ่ายทอดองค์ความรู้และเทคโนโลยีด้านการส่งเสริมสุขภาพ การจัดการปัจจัยเสี่ยงต่อสุขภาพ และการจัดการอนามัยสิ่งแวดล้อมที่เอื้อต่อการมีสุขภาพดี รวมทั้งการประเมินผลกระทบต่อสุขภาพ เพื่อยืนยันให้ประชาชนมีความรู้และทักษะในการดูแลตนเอง ครอบครัวและชุมชน รวมตลอดจนถึงการสนับสนุนให้หน่วยงาน ส่วนภูมิภาค องค์การปกครองส่วนท้องถิ่น และภาคีเครือข่ายทั้งภาครัฐและภาคเอกชน มีส่วนร่วมในการสร้างเสริมสุขภาพและจัดการอนามัยสิ่งแวดล้อมเพื่อส่งเสริมให้คนไทยมีสุขภาพดีโดยถ้วนหน้า

โดยทางกรมอนามัยได้มีการติดตั้งโครงสร้างพื้นฐานทางด้านระบบเครือข่ายและการสื่อสาร รวมทั้งระบบ คอมพิวเตอร์ ในการให้บริการทางด้านเทคโนโลยีสารสนเทศและการสื่อสารตามแผนยุทธศาสตร์การพัฒนา เทคโนโลยีสารสนเทศและการสื่อสาร ตามที่กระทรวงสาธารณสุขได้กำหนดขึ้น ให้เป็นเครื่องมือในการสนับสนุน เพื่อเพิ่มประสิทธิภาพของระบบบริการและบริหารจัดการในการสถานการณ์ปัญหาสถานะสุขภาพของประชาชน และเป็นกลไกสำคัญในการขับเคลื่อนระบบบริการสุขภาพที่มีประสิทธิภาพ ซึ่งได้มีการปรับปรุงระบบเครือข่ายและการสื่อสาร และระบบคอมพิวเตอร์อย่างเนื่องจนถึงปัจจุบัน โดยอยู่ในขอบเขตการปรับปรุงตามพันธกิจขององค์กร ได้แก่

๑. จัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างคุ้มค่า ทันสมัย พอเพียง และมีประสิทธิภาพ เพื่อสนับสนุนต่อการขับเคลื่อนยุทธศาสตร์ขององค์กร
๒. บูรณาการระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งจากภายในและภายนอกองค์กรให้สอดคล้อง เป็นไปในทิศทางเดียวกันอย่างไร้รอยต่อ
๓. พัฒนามาตรฐานข้อมูลและการเชื่อมโยงระบบสารสนเทศทั้งภายในและภายนอกองค์กร
๔. นำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เพิ่มขีดความสามารถให้บริการข้อมูลข่าวสารด้านการส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อมแก่ประชาชนได้ทั่วถึง เท่าเทียมทุกที่ ทุกเวลา
๕. ส่งเสริมการพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสารและบุคลากรทั่วไปของกรม อนามัยให้มีทักษะด้านเทคโนโลยีสารสนเทศและการสื่อสารเพียงพอต่อการปฏิบัติงาน

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

- เพื่อเป็นแนวทางในการบริหารเทคโนโลยีสารสนเทศของกรมอนามัยให้มีความมั่นคงปลอดภัยมากขึ้น
- เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพและประสิทธิผลมากขึ้น
- เพื่อให้เกิดการพัฒนาบุคลากรให้มีทักษะด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ
- เพื่อป้องกันความเสียหายที่เกิดจากการเหตุการณ์ที่ไม่พึงประสงค์ต่อทรัพยากรด้านสารสนเทศและมีผลต่อการดำเนินงานของกรมอนามัย

๒. การระบุความเสี่ยง (Risk Identification)

การประเมินความเสี่ยงนี้ได้ใช้กรอบโครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of information security) ของ ISO/IEC ๒๗๐๐๑: ๒๐๑๓ มาเป็นเกณฑ์เพื่อระบุถึงความเสี่ยงพื้นฐานที่สำคัญและที่จำเป็นต้องจัดการ จากการศึกษาสถานภาพปัจจุบันของการบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศของกรมอนามัยเมื่อเทียบกับกรอบโครงสร้างความมั่นคงปลอดภัยสารสนเทศ ดังกล่าว พบความเสี่ยงด้านต่างๆ ดังตารางที่ ๑ ส่วนรายละเอียดที่เป็นสาเหตุหรือปัจจัยของความเสี่ยง และผลกระทบของความเสี่ยงอธิบายไว้ในตารางที่ ๒

ตารางที่ ๑ การระบุความเสี่ยงเทียบเคียงกับกรอบโครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of information security) ของ ISO/IEC ๒๗๐๐๑: ๒๐๑๓

รหัสความเสี่ยง	ความเสี่ยง	กรอบโครงสร้างความมั่นคงปลอดภัยสารสนเทศของ ISO/IEC ๒๗๐๐๑ :๒๐๑๓
Ro๑	ความพร้อมใช้งานอย่างต่อเนื่อง (availability) ของระบบสารสนเทศภายในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ของกรมอนามัย	ด้านความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environment Security)
Ro๒	การเข้าถึงระบบเครือข่ายไร้สาย (wireless network) ของกรมอนามัย	ด้านการควบคุมการเข้าถึง (Access Control)
Ro๓	ระบบการบริหารจัดการรหัสผ่าน (password management system)	ด้านการควบคุมการเข้าถึง (Access Control) และ ด้านการเข้ารหัสข้อมูล (Cryptography)
Ro๔	การติดตั้งซอฟต์แวร์ภายในกรมอนามัย	ด้านการควบคุมการเข้าถึง (Access Control) และ ด้านความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
Ro๕	การป้องกันซอฟต์แวร์ไม่พึงประสงค์ (malicious software)	ด้านความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

รหัส ความเสี่ยง	ความเสี่ยง	กรอบโครงสร้างความมั่นคงปลอดภัยสารสนเทศ ของ ISO/IEC ๒๗๐๐๑ :๒๐๑๓
Ro๖	การสำรองข้อมูลและซอฟต์แวร์ประยุกต์ที่จัดเก็บ อยู่ที่ห้องควบคุมระบบคอมพิวเตอร์และ เครือข่าย ของกรมอนามัยและที่ส่วนอื่นๆ	ด้านความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
Ro๗	การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์	ด้านความสอดคล้อง (Compliance)
Ro๘	การดำเนินงานด้านเทคโนโลยีสารสนเทศให้ เป็นไปตามข้อกำหนดที่เกี่ยวข้อง	ด้านความสอดคล้อง (Compliance)
Ro๙	การควบคุมและกำกับการพัฒนาระบบ สารสนเทศในกรมฯให้เป็นไปตามเกณฑ์มาตรฐาน ของกรมอนามัย	ด้านการจัดหา การพัฒนา และการบำรุงรักษา ระบบ (System acquisition, development and maintenance)
Ro๑๐	การมีทักษะที่ทันยุคทันสมัยทางด้านเทคโนโลยี สารสนเทศ	ด้านโครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

ตารางที่ ๒ รายละเอียดของความเสี่ยง (ปัจจัยและผลกระทบ)

รหัสความ เสี่ยง	สาเหตุของความเสี่ยง/ ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
Ro๑	ระบบสารสนเทศของกรมอนามัย ส่วนใหญ่ติดตั้งไว้ ที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ของ กรมอนามัย ศูนย์ข้อมูลกลางนี้มีระบบไฟฟ้าสำรอง (UPS) เพื่อใช้ในกรณีไฟฟ้าล้มเหลว อย่างไรก็ตาม ถ้าระบบไฟฟ้าล้มเหลวเป็นเวลานาน ไฟฟ้าสำรอง ดังกล่าวจะไม่สามารถเลี้ยงอุปกรณ์ต่างๆ ได้อย่าง เพียงพอ เมื่อไฟฟ้าสำรองหมดลง การทำงานของ ระบบสารสนเทศทั้งหมดก็จะล้มเหลวและมี ผลกระทบต่อการดำเนินงานของกรมอนามัย	๑. การทำงานตามภารกิจของกรมอนามัย ในส่วนที่ต้องพึ่งพาระบบสารสนเทศต้อง หยุดชะงักและมีผลกระทบต่อการบริการ ประชาชน ๒. ประชาชนไม่สามารถใช้บริการของกรม อนามัยผ่านระบบเครือข่ายอินเทอร์เน็ตได้ ๓. การสื่อสารของกรมอนามัยที่ต้องใช้ระบบ เครือข่ายไม่สามารถทำได้

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
Ro๒	กรมอนามัยมีการติดตั้งระบบเครือข่ายไร้สาย (wireless network) เพื่อให้ผู้ปฏิบัติงานสามารถเข้าถึงการใช้บริการด้านสารสนเทศได้อย่างมีประสิทธิภาพและประสิทธิผลมากขึ้น อย่างไรก็ตามในกระบวนการของการยืนยันตัวบุคคล (authentication) เพื่อเข้าใช้บริการยังมีช่องโหว่ ซึ่งจะทำให้ผู้ไม่ประสงค์ดีสามารถปลอมแปลงตัวตนเพื่อเข้ามาใช้บริการได้ - ผู้ใช้ระดับปฏิบัติการ ใช้วิธีการ login ด้วยชื่อผู้ใช้ (username) และ รหัสผ่าน (password) ซึ่งกระบวนการนี้ไม่มีการเข้ารหัสลับ (encryption) นอกจากนี้ การเข้าใช้ไม่จำเป็นต้องลงทะเบียนอุปกรณ์ - ผู้ใช้ระดับผู้บริหาร ใช้วิธีการลงทะเบียนอุปกรณ์ และไม่ต้องทำการ login ใดๆ	๑. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจใช้งานอินเทอร์เน็ตของกรมอนามัย ในการทำสิ่งที่ไม่ผิดกฎหมาย เช่น โพสต์ข้อความหมิ่นประมาทผู้อื่น หรือ บุกรุกระบบเครือข่ายขององค์กรอื่นๆ อีก ซึ่งอาจจะมีผลทำให้กรมอนามัยต้องรับผิดชอบทางกฎหมาย และสูญเสียภาพลักษณ์ขององค์กรได้ ๒. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจขโมยข้อมูล ดัดแปลงข้อมูลหรือทำลายข้อมูลที่สามารถเข้าถึงได้ ซึ่งอาจจะทำให้ข้อมูลที่ใช้ในการปฏิบัติงานเสียหายได้ ๓. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจลักลอบเข้าไปในระบบบริหารจัดการเครือข่าย เพื่อให้ได้สิทธิ์ในการควบคุมเครือข่ายไร้สายดังกล่าวได้
Ro๓	กรมอนามัย ได้มีการกำหนดการใช้ชื่อผู้ใช้และรหัสผ่านเป็นการทำการยืนยันตัวบุคคลเพื่อเข้าใช้ทรัพยากรด้านสารสนเทศ อย่างไรก็ตาม การบริหารจัดการรหัสผ่าน (password management) ยังไม่เป็นระบบที่เป็นมาตรฐานและสามารถเป็นช่องโหว่ ให้ผู้บุกรุกสามารถคาดเดารหัสผ่าน รวมทั้ง การโจรกรรมรหัสผ่านได้ เช่น ข้อกำหนดในการตั้งรหัสผ่านที่สามารถป้องกันการตั้งรหัสผ่านที่อ่อนแอ (weak password) ได้ หรือ ข้อกำหนดในการจัดเก็บรหัสผ่านด้วยการเข้ารหัสลับ (encrypted passwords) ก่อนจัดเก็บในหน่วยความจำสำรอง (secondary storage) หรือ ข้อกำหนดในการสื่อสารข้อมูลที่เป็นรหัสผ่านที่ส่งระหว่างอุปกรณ์เพื่อป้องกันการแอบดักขโมย หรือ ข้อกำหนดในการปรับเปลี่ยนและตรวจสอบการใช้รหัสผ่านที่มากับอุปกรณ์ (default passwords)	๑. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาครอบครองและควบคุมทรัพยากรด้านสารสนเทศ ในการทำสิ่งต่างๆ ที่ไม่พึงประสงค์ ๒. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจขโมยข้อมูลที่เป็นความลับ ดัดแปลงข้อมูลหรือทำลายข้อมูลที่สามารถเข้าถึงได้ ซึ่งอาจจะทำให้ข้อมูลที่ใช้ในการปฏิบัติงานเสียหายและไม่สามารถใช้งานได้ (confidentiality, integrity and availability) ๓. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจลักลอบเข้าไปในระบบบริหารจัดการเครือข่ายเพื่อให้ได้สิทธิ์ในการควบคุมระบบเครือข่ายและอุปกรณ์ต่างๆ ได้

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
Ro๔	ผู้ใช้งาน (end-users) สามารถที่จะติดตั้งซอฟต์แวร์ต่างๆ ได้เองโดยไม่มีกระบวนการในการควบคุม (control of operational software) ซอฟต์แวร์ที่สามารถติดตั้งได้เองนี้เป็นทั้งซอฟต์แวร์ระบบ (system software) ซอฟต์แวร์ประยุกต์ (application software) รวมถึงซอฟต์แวร์อรรถประโยชน์ใดๆ (utility software)	๑. การติดตั้งซอฟต์แวร์บางอย่างอาจทำให้ไม่สามารถควบคุมการรักษาลับข้อมูลของกรมอนามัยได้ ๒. การติดตั้งอาจมีการเปลี่ยนแปลงการกำหนดค่ารูปแบบการทำงาน (configuration) ของอุปกรณ์และอาจจะมีผลทำให้เกิดปัญหากับการทำงานของซอฟต์แวร์ตัวอื่นๆ ๓. การติดตั้งซอฟต์แวร์โดยไม่คำนึงถึงเรื่องลิขสิทธิ์ ซึ่งอาจจะทำให้กรมอนามัยถูกฟ้องร้องและเกิดความเสียหายได้ ๔. ซอฟต์แวร์ที่ถูกนำมาติดตั้งอาจติดไวรัสหรือซอฟต์แวร์ที่ไม่พึงประสงค์ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลและซอฟต์แวร์อื่นๆ
Ro๕	ผู้ใช้งาน (end users) ค่อนข้างมีอิสระสูงในการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศของกรมอนามัย ดังนั้นถ้าหากผู้ใช้งานขาดความระมัดระวังมันจะมีผลทำให้ซอฟต์แวร์ที่ไม่พึงประสงค์ (malicious software หรือ malware) สามารถเข้าสู่ระบบคอมพิวเตอร์และแพร่กระจายผ่านระบบเครือข่ายได้ ปัจจุบัน ซอฟต์แวร์ที่ไม่พึงประสงค์ดังกล่าวอาจจะมากับ e-mail, social media, thumb-drive หรือ ซอฟต์แวร์ที่นำมาติดตั้ง	๑. การใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศอาจจะมีประสิทธิภาพ เช่น เครื่องคอมพิวเตอร์หรือระบบเครือข่ายทำงานช้าลง และส่งผลต่อประสิทธิภาพ ๒. ข้อมูลอาจจะถูกขโมยออกไปหรืออาจจะถูกทำลายหรืออาจจะถูกปิดกั้นไม่ให้สามารถเข้าถึงได้ ๓. ซอฟต์แวร์ที่ใช้งานจริงที่ติดตั้งบนเครื่องคอมพิวเตอร์อาจจะถูกทำให้ใช้งานไม่ได้
Ro๖	ข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่ายที่ตั้งอยู่ที่ศูนย์ข้อมูลกลางได้ถูกสำเนาเก็บไว้ตามช่วงเวลาที่กำหนด อย่างไรก็ตาม ตัวสำเนาดังกล่าวกลับถูกเก็บไว้ที่ศูนย์ข้อมูลกลางเช่นเดียวกัน ดังนั้นถ้าหากเกิดไฟไหม้หรือน้ำท่วมที่ศูนย์ข้อมูลกลางตัวข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่ายรวมทั้งสำเนาของมันก็จะเกิดความเสียหายไปด้วยกัน นอกจากนี้ เครื่องแม่ข่ายของบางหน่วยงานก็ไม่ได้ถูกเก็บไว้ที่ศูนย์ข้อมูลกลาง	๑. กรณีที่หน่วยเก็บข้อมูลสำรอง (secondary storage) ของเครื่องแม่ข่ายเกิดความเสียหายและไม่มีสำเนาเก็บไว้ จะมีผลทำให้ข้อมูลสูญหายและซอฟต์แวร์ประยุกต์ไม่สามารถใช้งานได้ อีก ถ้าเป็นระบบที่สำคัญต่อการทำธุรกรรมของหน่วยงาน ก็จะมีผลต่อการดำเนินงานทันที

รหัสความ เสี่ยง	สาเหตุของความเสี่ยง/ ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
	ข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่ายดังกล่าวจึงอาจจะไม่ได้ถูกสำเนาเก็บไว้	๒. กรณีที่เกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อศูนย์ข้อมูลกลาง เช่น ไฟไหม้ จะมีผลทำให้ข้อมูลสูญหายและซอฟต์แวร์ประยุกต์ไม่สามารถใช้งานได้อีก ถ้าเป็นระบบที่สำคัญต่อการทำธุรกรรมของหน่วยงานต่างๆ ก็จะมีผลต่อการดำเนินงานของหน่วยงานเหล่านั้นทันที
Ro๗	การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ยังมียกโอกาสเกิดขึ้นได้ในกรมอนามัย ทั้งนี้เนื่องจากการขาดการสร้าง ความตระหนักในผลลัพธ์ที่จะเกิดขึ้น รวมทั้งการขาดกลไกในการควบคุมและติดตาม จากการตรวจสอบ พบว่ายังคงมีการใช้ระบบปฏิบัติการ (operating systems) ที่ไม่มีใบอนุญาต (license)	๑. การใช้ระบบปฏิบัติการที่ไม่มีใบอนุญาตมีผลทำให้ขาดการบำรุงรักษาจากผู้ผลิตและอาจจะมีผลทำให้เกิดช่องโหว่ในระบบคอมพิวเตอร์ที่ผู้ไม่ประสงค์ดีอาจจะบุกรุกเข้ามาได้และสร้างความเสียหายให้กับระบบ รวมทั้งการโจรกรรมข้อมูลต่างๆ ๒. การใช้ระบบปฏิบัติการที่ไม่มีใบอนุญาตเป็นสิ่งที่ผิดกฎหมายและอาจจะถูกฟ้องร้องเรียกค่าเสียหายได้ ซึ่งจะทำให้กรมฯ ต้องสูญเสียค่าใช้จ่ายสูงและสูญเสียภาพลักษณ์ขององค์กร ๓. ซอฟต์แวร์ที่ผิดกฎหมายอาจจะมาพร้อมกับ malware เช่น virus หรือ spyware ซึ่งสามารถสร้างความเสียหายให้กับข้อมูลและทรัพยากรด้านสารสนเทศได้
Ro๘	การดำเนินงานด้านเทคโนโลยีสารสนเทศต้องเป็นไปตามข้อกำหนดทางกฎหมาย เช่น การสร้าง log file บนเครื่องแม่ข่าย เนื่องจากการมอณามัย มี <u>หน่วยงานที่อยู่ต่างจังหวัดด้วย</u> จึงทำให้ยังไม่สามารถควบคุมและติดตามการดำเนินงานทั้งหมดให้เป็นไปตามข้อกำหนดทางกฎหมายได้	การไม่เก็บ log file เป็นการกระทำผิดตาม พรบ. คอมพิวเตอร์ ซึ่งมีโทษปรับค่อนข้างสูงและทำให้เสียภาพลักษณ์ขององค์กร

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R๐๙	การพัฒนาระบบสารสนเทศในกรมอนามัย เป็นลักษณะที่ผู้ใช้งาน (end-users) สามารถจัดหาหรือจัดจ้างได้เอง รวมทั้งสามารถพัฒนาระบบขึ้นมาเองด้วย ถึงแม้ว่ามีเอกสารที่กำหนดรูปแบบของการพัฒนาระบบ แต่ยังขาดการควบคุมและกำกับดูแลจากกลุ่มเทคโนโลยีสารสนเทศ กองแผนงาน และบางครั้งบริษัทภายนอกก็สามารถเข้ามาจัดการกับระบบของตนเอง โดยผ่านระบบเครือข่ายของกรมอนามัย	๑. บริษัทผู้รับจ้างจากภายนอก สามารถเข้ามากำหนดรูปแบบการทำงานของระบบผ่าน VPN ซึ่งไม่มีกระบวนการในการควบคุมการดำเนินงานดังกล่าวและอาจเกิดช่องโหว่ด้านความมั่นคงของระบบเครือข่ายได้ ๒. การเชื่อมโยงระบบเพื่อใช้ประโยชน์จากข้อมูลทำได้ยาก ๓. การเกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบต่างๆ ภายในกรมอนามัย
R๑๐	เทคโนโลยีสารสนเทศมีความก้าวหน้าและเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งเครื่องมือและเทคนิคใหม่ๆ ที่มีการพัฒนาอยู่ตลอดเวลา ซึ่งสิ่งที่เกิดขึ้นดังกล่าวทำให้บุคลากรที่ดูแลด้านเทคโนโลยีสารสนเทศไม่สามารถติดตามและรู้ทันผู้ที่ไม่ประสงค์ดีในการบุกรุกเข้าสู่ระบบเครือข่ายได้ รวมทั้งไม่รู้จักระบบและเทคนิคใหม่ๆ ที่มีประสิทธิภาพและประสิทธิผลทันยุคทันเหตุการณ์ในการรับมือการโจมตีได้	๑. การโจมตีเพื่อให้ระบบเครือข่ายล้มเหลวและมีผลต่อการปฏิบัติงานและการให้บริการประชาชน ๒. การบุกรุกเข้ามาใช้ประโยชน์จากทรัพยากรด้านสารสนเทศ โดยเฉพาะอย่างยิ่งเครื่องแม่ข่ายที่อ่อนแอ เพื่อไว้ใช้ในการโจมตีเครื่องอื่นๆ เช่น การทำ Cryptojacking ซึ่งนอกจากจะทำให้ประสิทธิภาพของทรัพยากรลดลงแล้ว ยังอาจจะทำให้เสียภาพลักษณ์ขององค์กรอีกด้วย

๓. การวิเคราะห์และประเมินความเสี่ยง (Risk Analysis and Assessment)

การวิเคราะห์และประเมินความเสี่ยงซึ่งเป็นการวิเคราะห์โอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดจากเหตุการณ์ที่ความเสี่ยงนั้นเกิดขึ้นจริง รวมไปถึงการประเมินระดับคะแนนของความเสี่ยงแต่ละความเสี่ยงและการจัดลำดับความสำคัญ การประเมินโอกาสและผลกระทบนั้นมาจากการประชุมระดมความคิดเห็นของผู้เกี่ยวข้อง (stakeholders) เป็นหลัก

ตารางที่ ๓ รายละเอียดของผลการวิเคราะห์และประเมินความเสี่ยง

รหัสความเสี่ยง	ระดับของโอกาสที่จะเกิด (P)	ระดับของผลกระทบที่เกิดขึ้น (I)	ระดับคะแนนความเสี่ยง (P*I)
Ro๑	๓	๓	๙
Ro๒	๒	๓	๖
Ro๓	๒	๓	๖
Ro๔	๓	๓	๙
Ro๕	๑	๒	๒
Ro๖	๑	๓	๓
Ro๗	๓	๒	๖
Ro๘	๒	๑	๒
Ro๙	๓	๓	๙
R๑๐	๒	๒	๔

หมายเหตุ

ความหมายของ “ระดับของโอกาสที่จะเกิด (P)” กำหนดได้ดังนี้

๑. สูง (๓) หมายถึง การมีโอกาที่จะเกิดขึ้นมากกว่า ๓ ครั้งต่อปี
๒. ปานกลาง (๒) หมายถึง การมีโอกาที่จะเกิดขึ้นเกิน ๑ ครั้งแต่ไม่เกิน ๓ ครั้งต่อปี
๓. ต่ำ (๑) หมายถึง การมีโอกาที่จะเกิดขึ้นไม่เกิน ๑ ครั้งต่อปี

ความหมายของ “ระดับของผลกระทบที่เกิดขึ้น (I)” กำหนดได้ดังนี้

๑. มาก (๓) หมายถึง ระบบต่างๆ ที่ใช้ในการปฏิบัติงานประจำวัน (transaction processing systems) ล้มเหลวตั้งแต่ ๓ วันขึ้นไป และ/หรือ ข้อมูลที่จำเป็นต้องการปฏิบัติงานประจำถูกทำให้เกิดความเสียหาย (ถูกโจรกรรม ถูกปิดกั้นการเข้าถึง หรือ ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต)
๒. ปานกลาง (๒) หมายถึง ระบบต่างๆ ที่ใช้ในการปฏิบัติงานประจำวัน (transaction processing systems) ล้มเหลวเกิน ๑ ชั่วโมงแต่ไม่เกิน ๒ วันขึ้นไป
๓. น้อย (๑) หมายถึง ระบบต่างๆ ที่ใช้ในการปฏิบัติงานประจำวัน (transaction processing systems) ล้มเหลวไม่เกิน ๑ ชั่วโมง

ตารางที่ ๔ รายละเอียดของผลการจัดลำดับความสำคัญในรูปแบบเมทริกซ์ของความทนต่อความเสี่ยง
(Risk Tolerance Matrix)

		ระดับของผลกระทบ		
ระดับของโอกาสที่จะเกิด		๑ (ต่ำ)	๒ (ปานกลาง)	๓ (สูง)
	๓ (สูง)	ไม่มี	Ro๗	Ro๑, Ro๔, Ro๙
	๒ (ปานกลาง)	Ro๘	Ro๑๐	Ro๒, Ro๓
	๑ (ต่ำ)	ไม่มี	Ro๕	Ro๖

แสดงให้เห็นถึงการจัดกลุ่มของความเสี่ยงตามช่วงคะแนน ซึ่งสามารถแบ่งได้เป็น ๓ กลุ่มดังนี้

๑. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง ๖ – ๙ คะแนน ซึ่งถือว่าเป็นระดับความเสี่ยง “สูง” (สีแดง) ได้แก่ความเสี่ยงที่มีรหัส Ro๑, Ro๒, Ro๓, Ro๔, Ro๗ และ Ro๙
๒. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง ๓ – ๕ คะแนน ซึ่งถือว่าเป็นระดับความเสี่ยง “ปานกลาง” (สีส้ม) ได้แก่ความเสี่ยงที่มีรหัส Ro๖ และ Ro๑๐
๓. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง ๑ – ๒ คะแนน ซึ่งถือว่าเป็นระดับความเสี่ยง “ต่ำ” (สีเขียว) ได้แก่ความเสี่ยงที่มีรหัส Ro๕ และ Ro๘

๔. การวางกลยุทธ์ในการจัดการความเสี่ยง (Risk Strategies)

จากคะแนนความเสี่ยงที่ได้รับจากการประเมิน โดยกำหนดให้มีการจัดการความเสี่ยง ดังต่อไปนี้

หากระดับความเสี่ยง ไม่สามารถยอมรับได้ ต้องมีการเฝ้าระวัง “ปานกลาง” และ “สูง” ควบคุม แก้ไข และจัดการเพิ่มเติม เพื่อควบคุมความเสี่ยงไม่ให้ขยายออกไป โดยให้ดำเนินการ “ควบคุมความเสี่ยง)Controlling)”

หากระดับความเสี่ยง ความเสี่ยงนั้นอยู่ในเกณฑ์ที่ยอมรับได้ “ต่ำ” โดยให้ดำเนินการ “ยอมรับความเสี่ยง)Accepting)”

ตารางที่ ๕ กลยุทธ์ในการจัดการความเสี่ยง (Risk Strategies)

ความ เสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC ๒๗๐๐๑:๒๐๑๓	แนวทางแผนการดำเนินงาน/
Ro๑	ควบคุมความเสี่ยง (Controlling)	Availability of information processing facilities	- กำหนดให้มีแผนการบำรุงรักษาอุปกรณ์เครื่อง สำรองไฟ (UPS) ให้สามารถใช้งานได้อย่างมี ประสิทธิภาพอยู่ตลอดเวลา - กำหนดให้ดำเนินการจัดหาเครื่องกำเนิดไฟฟ้า ฉุกเฉิน (Generator) เข้ามาใช้งาน และมีแผนการ บำรุงรักษาอย่างต่อเนื่อง - กำหนดรอบระยะเวลาในการทดสอบความพร้อมใช้ ของอุปกรณ์สำรอง
Ro๒	ควบคุมความเสี่ยง (Controlling)	Access to networks and network services	- กำหนดให้มีขั้นตอนการลงทะเบียนอุปกรณ์ที่จะเข้า ใช้ระบบ wireless network ของหน่วยงาน - กำหนดให้มีการ login ด้วยชื่อผู้ใช้ (user name) และ รหัสผ่าน (password) พร้อมกับการเข้ารหัสลับ ก่อนส่งไปยัง access point เพื่อเข้าใช้ระบบ - เฝ้าระวังการเชื่อมต่ออุปกรณ์เข้าระบบเครือข่าย ของกรมฯ และการใช้งานอุปกรณ์ดังกล่าว
Ro๓	ควบคุมความเสี่ยง (Controlling)	Password management system	- กำหนดมาตรฐานและควบคุมการตั้งรหัสผ่านที่มี ความมั่นคงปลอดภัยให้มีความเข้มแข็ง (strong password) ตามหลักสากล - กำหนดให้มีการเข้ารหัสลับของรหัสผ่านในรูปแบบ ของการทำ hash ก่อนจัดเก็บในระบบ และ ระหว่างการสื่อสาร - กำหนดให้มีการเข้ารหัสลับของชื่อผู้ใช้ (user name) และ รหัสผ่าน (password) ก่อนส่ง ระหว่างอุปกรณ์ทุกครั้ง - ตั้งค่าการบริหารจัดการรหัสผ่านในระบบ สารสนเทศของกรมฯ ให้บังคับให้ผู้ใช้ทบทวน รหัสผ่านเปลี่ยนรหัสผ่านตามระยะเวลาที่/ เหมาะสมหรือตามที่ผู้ใช้งานต้องการ

ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC ๒๗๐๐๑:๒๐๑๓	แนวทางแผนการดำเนินงาน/
Ro๔	ควบคุมความเสี่ยง (Controlling)	Installation of software on operational systems	๑. กำหนดระเบียบปฏิบัติในการติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์ของกรมอนามัยให้ชัดเจน ๒. ใช้เครื่องมือทางด้าน IT ในการป้องกันไม่ให้มีการติดตั้งซอฟต์แวร์โดยพลการ เช่น การกำหนด Policy ผ่านระบบ AD ๓. การกำหนดสิทธิ์ของผู้ใช้งานไม่ให้อำนาจติดตั้งซอฟต์แวร์ได้เอง ๔. การกำหนดวิธีการรับมือเมื่อมีเหตุการณ์ผู้ใช้งานละเมิดระเบียบ เช่น การกักกัน หรือการถอดถอน ๕. การให้ความรู้เกี่ยวกับความตระหนักแก่ผู้ใช้งาน
Ro๕	ยอมรับความเสี่ยง (Accepting)	Controls against malware	ไม่มี
Ro๖	ควบคุมความเสี่ยง (Controlling)	Information backup	๑. กำหนดและสื่อสารขั้นตอนปฏิบัติในการสำรองข้อมูลระบบสารสนเทศของกรมฯ ให้ทั่วกัน ๒. จัดหาเทคโนโลยีที่เหมาะสมในการสำรองข้อมูลให้ตรงตามความต้องการของกรมฯ ๓. กำหนดพื้นที่หรือสถานที่ (off-site) ในการเก็บข้อมูลสำรองนอก data center โดยจะต้องมีระยะห่างจาก data center ในระยะที่มั่นใจได้ว่าหากเกิดภัยพิบัติที่ data center แล้วข้อมูลสำรองจะได้รับความเสียหาย ๔. กำหนดรอบในการทดสอบข้อมูลสำรองอย่างเหมาะสมและเพียงพอ ๕. กำหนดให้มีการเข้ารหัสและจัดลำดับชั้นความลับของข้อมูลสำรอง

ความ เสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC ๒๗๐๐๑:๒๐๑๓	แนวทางแผนการดำเนินงาน/
Ro๗	ควบคุมความเสี่ยง (Controlling)	Intellectual property rights	๑. กำหนดและสื่อสารนโยบายการบริหารจัดการ ลิขสิทธิ์ของกรมอนามัย ให้ทั่วถึง ๒. จัดทำ Record สำหรับบันทึกการซอฟต์แวร์ ลิขสิทธิ์ ๓. สุ่มตรวจสอบซอฟต์แวร์ลิขสิทธิ์บนเครื่อง คอมพิวเตอร์ที่เกี่ยวข้อง
Ro๘	ยอมรับความเสี่ยง (Accepting)	Identification of applicable legislation and contractual requirements	ไม่มี
Ro๙	ควบคุมความเสี่ยง (Controlling)	Information security requirements analysis and specification	๑. สื่อสารระเบียบปฏิบัติเกี่ยวกับรูปแบบการพัฒนา ระบบของกรมฯ ให้ทราบโดยทั่วกัน ๒. สุ่มตรวจสอบคุณลักษณะเฉพาะ (TOR) หรือเกณฑ์ การพัฒนาระบบของแต่ละหน่วยงาน
R๑๐	ควบคุมความเสี่ยง (Controlling)	Contact with special interest groups	๑. กำหนดช่องทางต่างๆสำหรับติดต่อกับกลุ่มบุคคล องค์กร หรือหน่วยงานทางด้านการรักษาความ มั่นคงปลอดภัยสารสนเทศ

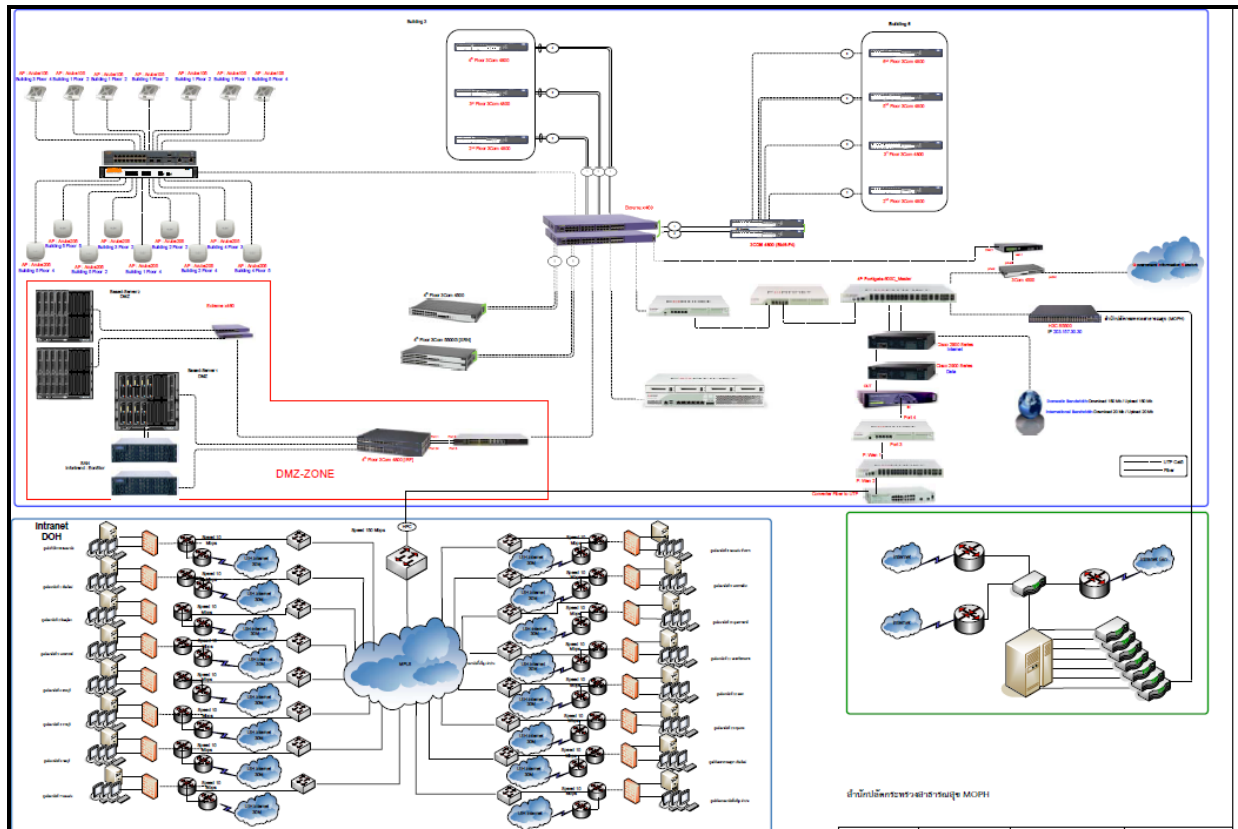
การวิเคราะห์ช่องว่างของระบบ

๑. การศึกษาสถานภาพปัจจุบันด้านเทคโนโลยีสารสนเทศและการสื่อสาร

โดยในการศึกษาสถานภาพปัจจุบันด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมอนามัย ได้ทำการศึกษาส่วนงานต่างๆ ของกรมอนามัย ด้วยวิธีการเก็บรวบรวมข้อมูล ได้แก่ แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย พ.ศ. ๒๕๕๘ – ๒๕๖๑ การสำรวจข้อมูลจากการจัดเก็บข้อมูลจรรยาบรรณทางคอมพิวเตอร์ของกรมอนามัย และการศึกษาจากเอกสารและข้อมูลต่าง ๆ จากนั้นนำข้อมูลทั้งหมดที่ได้รับมาทำการประมวลผล และสรุปบทวนสถานภาพการใช้งานระบบเครือข่ายของกรมอนามัยในปัจจุบัน ดังมีรายละเอียดดังนี้

๑.๑ สถานภาพทางด้าน ระบบเครือข่ายคอมพิวเตอร์ภาพรวมของกรมอนามัย

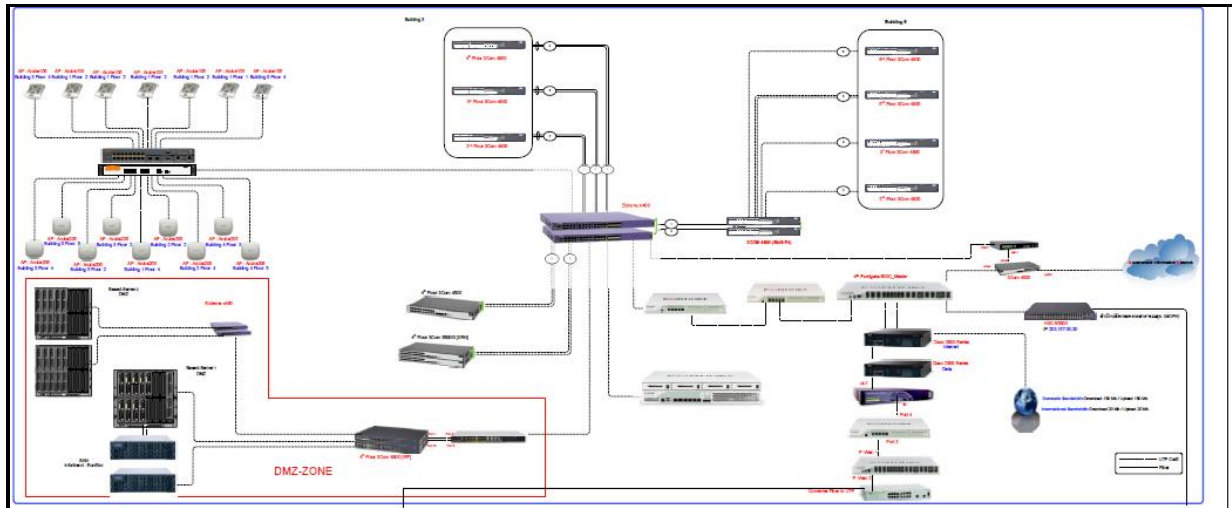
ระบบเครือข่าย (Network) ของกรมอนามัย แสดงได้ดังรูปที่ ๑ โดยมีการติดตั้งอุปกรณ์ Switch ในเครือข่ายภายในกรมอนามัยส่วนกลาง และมีการเชื่อมต่อกันด้วยความเร็ว ๔ Gbps ซึ่งใช้เทคโนโลยี link aggregation ระหว่างตึกภายในกรมอนามัยที่ส่วนกลาง และได้ทำการแบ่งเครือข่ายออกเป็นเครือข่ายย่อยที่ใช้เทคโนโลยี Virtual Lan โดยแยกออกเป็นตามชั้นของอาคาร โดยปัจจุบันได้ทำการแบ่ง Virtual Lan เป็น อาคาร E(๕), อาคาร C(๓), อาคาร A(๑), อาคาร B(๒), อาคาร D(๔), อาคาร F(๖) และอาคาร G(๗) โดยกำหนดให้ หมายเลข IP มีรูปแบบดังนี้ XX.อาคาร.ชั้น.XX ในการจัด Virtual Lan จำนวน ๔๐ VLAN อีกทั้งได้มีการเชื่อมต่อหน่วยงานสังกัดกรมอนามัยที่ตั้งอยู่ในภูมิภาคโดยผ่านบริการ Leased Line ของผู้ให้บริการภายนอก จำนวนทั้งหมด ๑๕ หน่วยงาน สำหรับการเชื่อมต่อกับเครือข่าย Internet ได้ผ่านผู้ให้บริการ (ISP) ภายนอก ที่ความเร็ว ๔๐ Mbps สำหรับการให้บริการอินเทอร์เน็ตในส่วนออกต่างประเทศ (International) และ ที่ความเร็ว ๒๕๕ Mbps สำหรับการให้บริการอินเทอร์เน็ตในส่วนในประเทศ (Domestic) และผ่านทางเครือข่ายกระทรวงสาธารณสุข นอกจากนี้ยังได้มีการให้บริการการเชื่อมต่อเครือข่ายในรูปแบบ Wireless หรือ Wi-Fi แก่เจ้าหน้าที่ภายในกรมอนามัยด้วยมาตรฐาน IEEE ๘๐๒.๑๑n ที่คลื่นความถี่ ๒.๔ GHz และ ๕.๐ GHz



รูปที่ ๑ ระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย

๑.๒ สถานภาพทางด้านระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย ส่วนกลาง

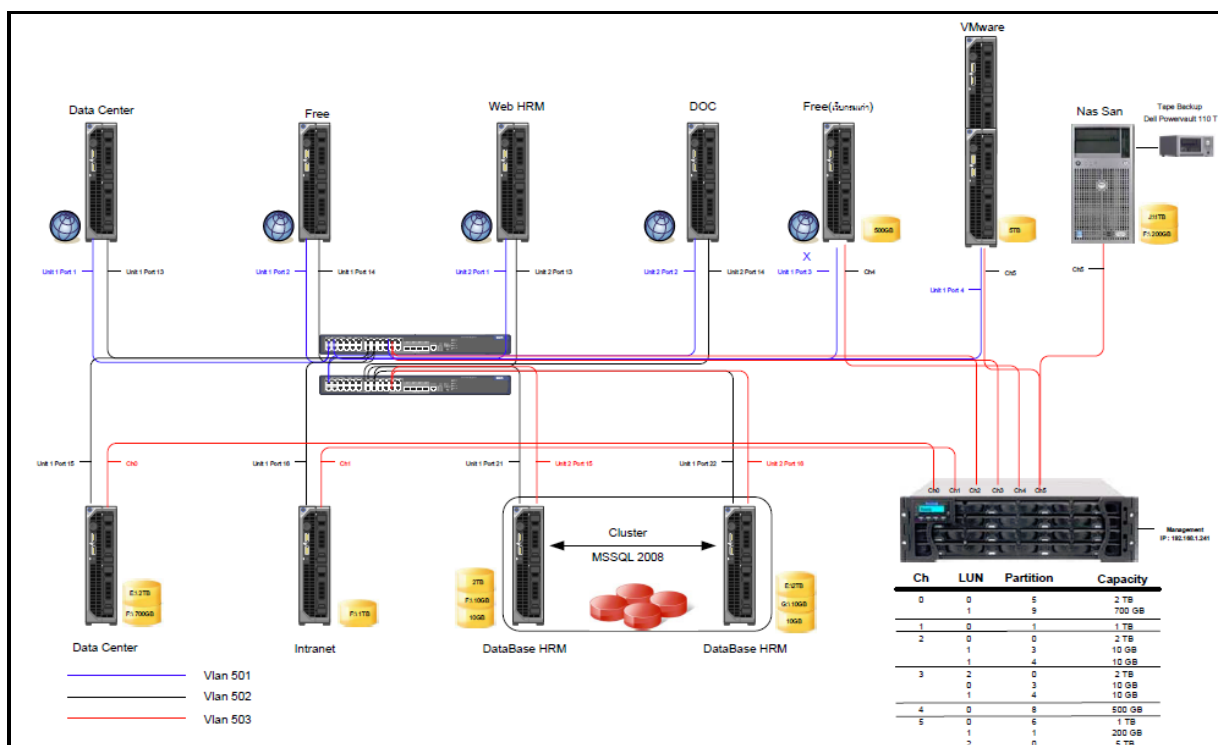
ระบบเครือข่าย (Network) ของกรมอนามัยในส่วนกลาง โดยมีการติดตั้งระบบรักษาความปลอดภัย (Firewall) ไว้ป้องกันภัยคุกคามจากผู้ที่ไม่ประสงค์ดีต่อกรมอนามัย และยังมีระบบในตรวจสอบผู้บุกรุกที่เรียกว่า Intrusion Prevention System (IPS) ติดตั้งไว้ในจุดต่าง ๆ จำนวน ๒ จุด เพื่อที่จะตรวจสอบและป้องกันผู้ที่บุกรุกระบบเครือข่ายของกรม อีกทั้งกรมยังมีระบบในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่รองรับพรบ. คอมพิวเตอร์ ปี ๒๕๕๐ และ ๒๕๖๐



รูปที่ ๒ ระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย ส่วนกลาง

๑.๓ สถานภาพทางด้านระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย ส่วนเครื่องแม่ข่าย (Demilitarized Zone: DMZ)

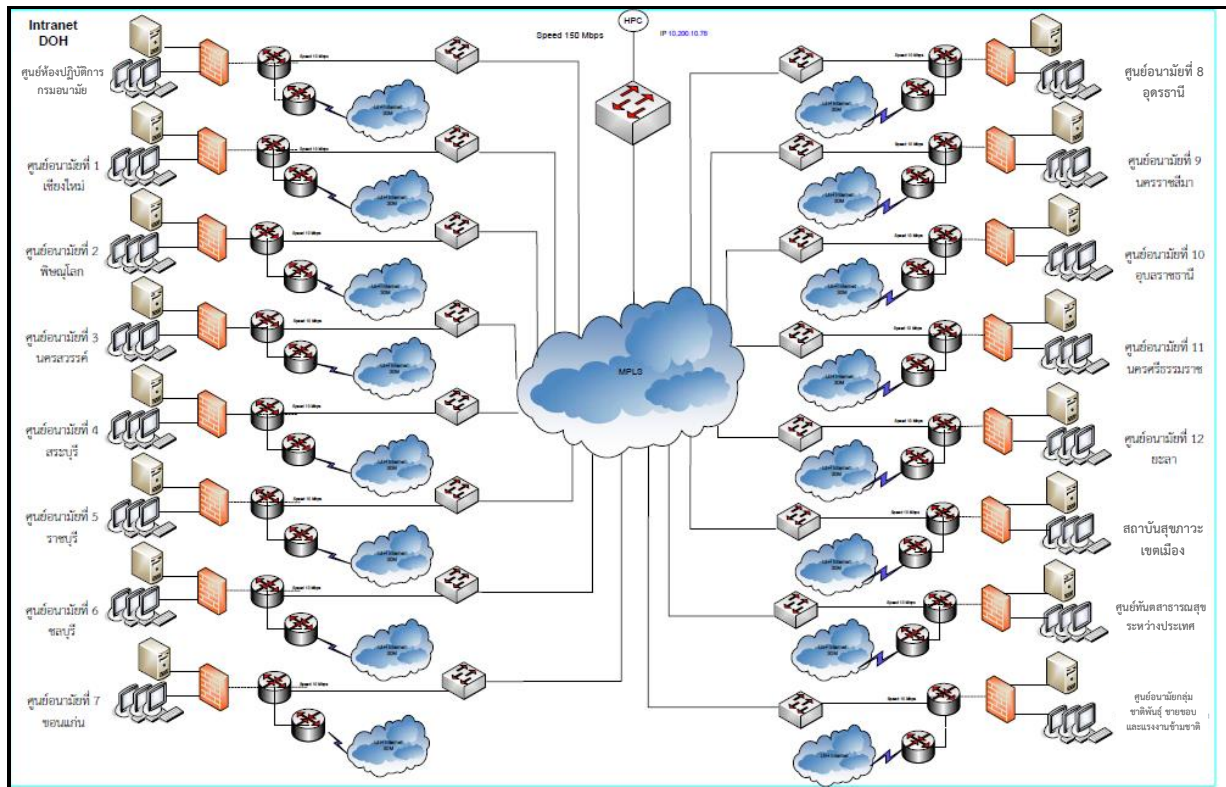
ระบบเครือข่าย (Network) ของกรมอนามัยใน ส่วนของเครื่องแม่ข่าย DMZ ได้มีการติดตั้งเครื่องแม่ข่ายที่ให้บริการต่าง ๆ ในรูปแบบของเครื่องแม่ข่ายเสมือน (Virtual Machine Server) ได้แก่ Web Server, Data Center Server และเครื่องแม่ข่ายที่ให้บริการของระบบสารสนเทศในกรมต่าง ๆ เป็นต้น โดยมีการแบ่งการเชื่อมต่อออกเป็นจากภายนอก และภายใน รวมทั้งแบ่งแยกช่องทางการจัดเก็บข้อมูล โดยมีระบบ Firewall ในการป้องกันการโจมตีจากผู้บุกรุกได้อย่างมีประสิทธิภาพ



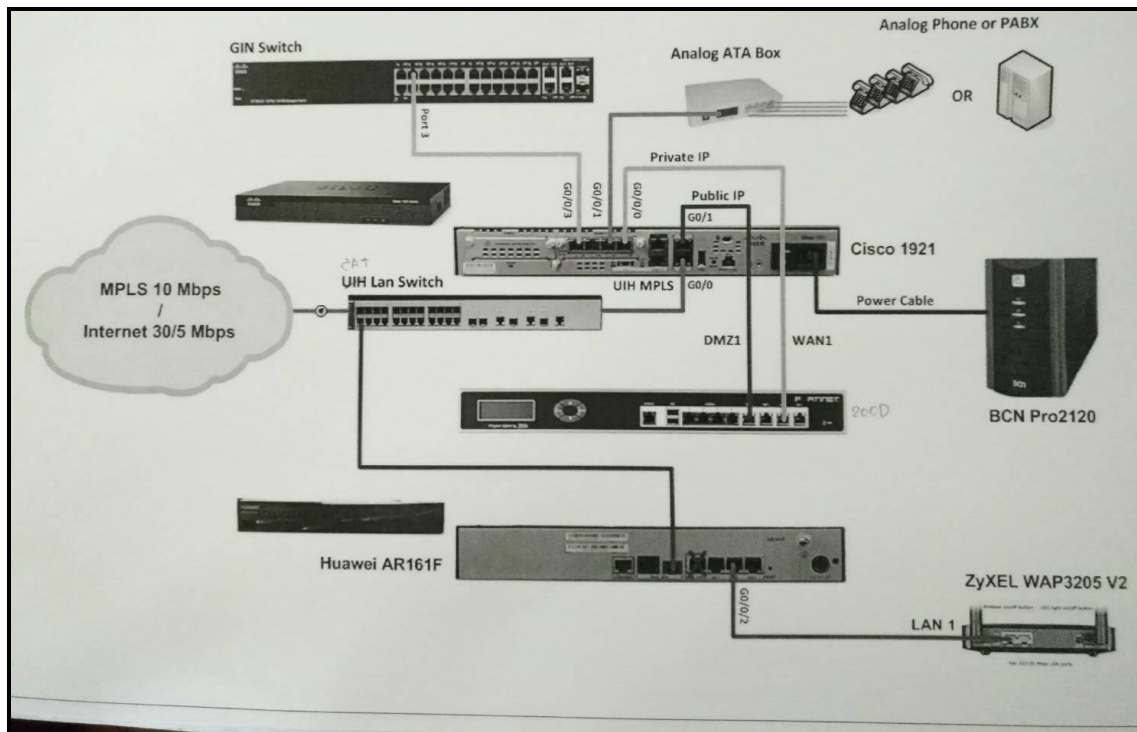
รูปที่ ๓ ระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย ส่วน DMZ

๑.๔ สถานภาพทางด้านระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย ส่วนภูมิภาค

ระบบเครือข่ายของส่วนภูมิภาค ได้มีการเชื่อมกับทางส่วนกลางผ่านระบบ Leased Line ซึ่งระบบเครือข่ายภายในของแต่ละศูนย์ทั้ง ๑๕ ศูนย์มีการเชื่อมต่อภายในที่ไม่เหมือนกันซึ่งขึ้นอยู่กับแต่ละศูนย์ ซึ่งโดยแต่ละศูนย์จะมีจุดที่เหมือนกันคือระบบรักษาความปลอดภัยที่จะใช้ในการเชื่อมต่อเข้ากับส่วนกลาง



รูปที่ ๔ ระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย ส่วนภูมิภาค



รูปที่ ๕ ตัวอย่างระบบเครือข่ายคอมพิวเตอร์ของกรมอนามัย ส่วนภูมิภาค (ศูนย์อนามัยที่ ๖ ชลบุรี)

๑.๕ สถานภาพทางด้านการควบคุมการเชื่อมต่อทางเครือข่าย

กรมอนามัยควบคุมการเชื่อมต่อทางเครือข่ายและกำหนดสิทธิในการเข้าถึงเครือข่ายให้เป็นไปตามนโยบายที่กำหนดเพื่อที่จะกรองข้อมูลจราจรให้มีความปลอดภัยในการใช้งานบนระบบเครือข่าย โดยมีการใช้อุปกรณ์หรือเครื่องมือในการควบคุมได้แก่ Firewall และ IPS โดยมีรายละเอียดดังนี้

๑.๑การป้องกัน การโอนย้าย File Download และ Upload File ทางเครือข่าย ที่อาจจะทำให้เกิดความเสียหายต่อระบบเครือข่ายตามมาตรฐาน ISO ๒๗๐๐๑ ดังนี้

ตารางที่ ๖ แสดงประเภทของ File ที่จะเกิดความเสียหายในการป้องกันการ Download และ Upload

- *.exe	- *.lnk	- *.sct	- *.chm	- *.cmd
- *.com	- *.mde	- *.shs	- *.cpl	- *.inf
- *.scr	- *.mscmstp	- *.wsf	- *.bas	- *.jes
- *.adp	- *.ade	- *.vbs	- *.crt	- *.vb
- *.wsh	- *.pif	- *.mst	- *.reg	- *.url
- *.hlp	- *.pcd	- *.vbe	- *.bat	- *.wsc

๑.๒การจัดการปริมาณการ Download และ Upload File โดยมีรายละเอียดดังนี้

ตารางที่ ๗ แสดงการจำกัดปริมาณการ Download และ Upload File ในส่วนกลาง

ส่วนกลาง							
Profile Name	ประเภทการใช้งาน	Service					
		HTTP	FTP	IMAP	POP3	SMTP	IM
Inbound	เครื่องคอมพิวเตอร์แม่ข่ายเข้า	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่เปิด
Outbound	เครื่องคอมพิวเตอร์แม่ข่ายออก	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่เปิด
User	บุคลากรกรมอนามัย	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่จำกัด
Executives	ผู้บริหารระดับสูง	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่จำกัด

ตารางที่ ๘ แสดงการจำกัดปริมาณการ Download และ Upload File ในส่วนภูมิภาค

ส่วนภูมิภาค							
Profile Name	ประเภทการใช้งาน	Service					
		HTTP	FTP	IMAP	POP3	SMTP	IM
Inbound	เครื่องคอมพิวเตอร์แม่ข่ายเข้า	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่เปิด
Outbound	เครื่องคอมพิวเตอร์แม่ข่ายออก	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่เปิด
User	บุคลากรกรมอนามัย	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่จำกัด
Executives	ผู้บริหารระดับสูง	ไม่จำกัด	ไม่จำกัด	ไม่เปิด	ไม่เปิด	ไม่จำกัด	ไม่จำกัด

๑.๓การกำหนดนโยบาย (Policy Firewall) การเข้าถึงเครือข่ายโดยใช้อุปกรณ์ Firewall ของกรมอนามัย ได้มีการกำหนดข้อมูลให้เข้าและออกโดยมีการควบคุมข้อมูลที่เข้าไปยังเครื่องแม่ข่ายที่ให้บริการต่าง ๆ ของกรมอนามัยตามช่องทางที่ให้บริการแต่ละเครื่องแม่ข่ายเท่านั้น โดยมีตัวอย่างการควบคุมดังนี้

- การทำงานของอุปกรณ์ : ควบคุมระบบเครือข่ายของกรมอนามัยส่วนกลาง
- จำนวนพอร์ตที่ใช้งาน:

ตารางที่ ๙ แสดงจำนวนพอร์ตที่ใช้งานของอุปกรณ์ Firewall ของกรมอนามัย

Port	เครือข่าย
1	Lead line กรมอนามัยส่วนภูมิภาค
2	Internet
3	Wireless Aruba (Vlan 801,802,803)
4	เครือข่ายสารสนเทศภาครัฐ (PV GIN)
5	เครือข่ายสารสนเทศภาครัฐ (PB GIN)
6	เครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายของกรมอนามัยส่วนกลาง
7	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข (MOPH)

ตารางที่ ๑๐ แสดงการกำหนดนโยบาย (Policy Firewall) การเข้าถึงเครือข่าย จากบุคคลภายนอก

VLAN 801 > Port 1

ลำดับ	ลักษณะการทำงาน	ต้นทาง	ปลายทาง	Port Number	Port Protocol			Protection Profile
					TCP	UDP	ICMP	
1	บุคคลภายนอก	ทุกหมายเลข	ทุกหมายเลข	80	✓	✓	✓	
				445	✓			

VLAN 801 > Port 6

ลำดับ	ลักษณะการทำงาน	ต้นทาง	ปลายทาง	Port Number	Port Protocol			Protection Profile
					TCP	UDP	ICMP	
1	บุคคลภายนอก	ทุกหมายเลข	ทุกหมายเลข	80	✓	✓	✓	
				53	✓	✓		
				161	✓	✓		
				9100	✓			
				515	✓			
				35	✓			
				170	✓			
				631	✓			
				3396	✓			
				137		✓		
				13000-15000	✓	✓		

ตารางที่ ๑๑ แสดงการกำหนดนโยบาย (Policy Firewall) การเข้าถึงเครือข่ายจากเครือข่ายภายใน

Port 1 > Port 2								
ลำดับ	ลักษณะการทำงาน	ต้นทาง	ปลายทาง	Port Number	Port Protocol			Protection Profile
					TCP	UDP	ICMP	
1	ระบบเครือข่ายภูมิภาคใช้งานอินเทอร์เน็ต (UIH)	ทุกหมายเลข	ทุกหมายเลข	All	✓	✓	✓	

Port 2 > Port 6								
ลำดับ	ลักษณะการทำงาน	ต้นทาง	ปลายทาง	Port Number	Port Protocol			Protection Profile
					TCP	UDP	ICMP	
1	เครือข่ายภูมิภาคเชื่อมต่อภายใน	ทุกหมายเลข	ทุกหมายเลข	25	✓			Inbound
				110	✓			
				443	✓			
				445	✓			
				465	✓			
				993	✓			
2	VPN	ทุกหมายเลข	ทุกหมายเลข	All	✓			
3	Proxy	ทุกหมายเลข	203.157.71.5	All	✓	✓	✓	

๒. สถานภาพทางด้านการป้องกันอุปกรณ์สื่อสารประเภทพกพา

กรมอนามัยมีอุปกรณ์ที่ให้บริการอุปกรณ์สื่อสารประเภทพกพาแบบไร้สาย Access point ยี่ห้อ Aruba AP ๑๐๕,๒๐๕ ซึ่งได้มีการป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ที่เชื่อมต่อเข้ากับระบบของกรมอนามัยดังนี้

๒.๑ แบ่งแยกระบบเครือข่าย โดยใช้เทคโนโลยี VLAN แบ่งระบบเครือข่ายไร้สายออกจากระบบเครือข่ายปกติ

๒.๒ ควบคุมการเข้าถึงอุปกรณ์ โดยการตั้งค่า SSID ให้มีความแตกต่างกันและการจำกัดจำนวนอุปกรณ์สื่อสารที่จะเชื่อมต่อ

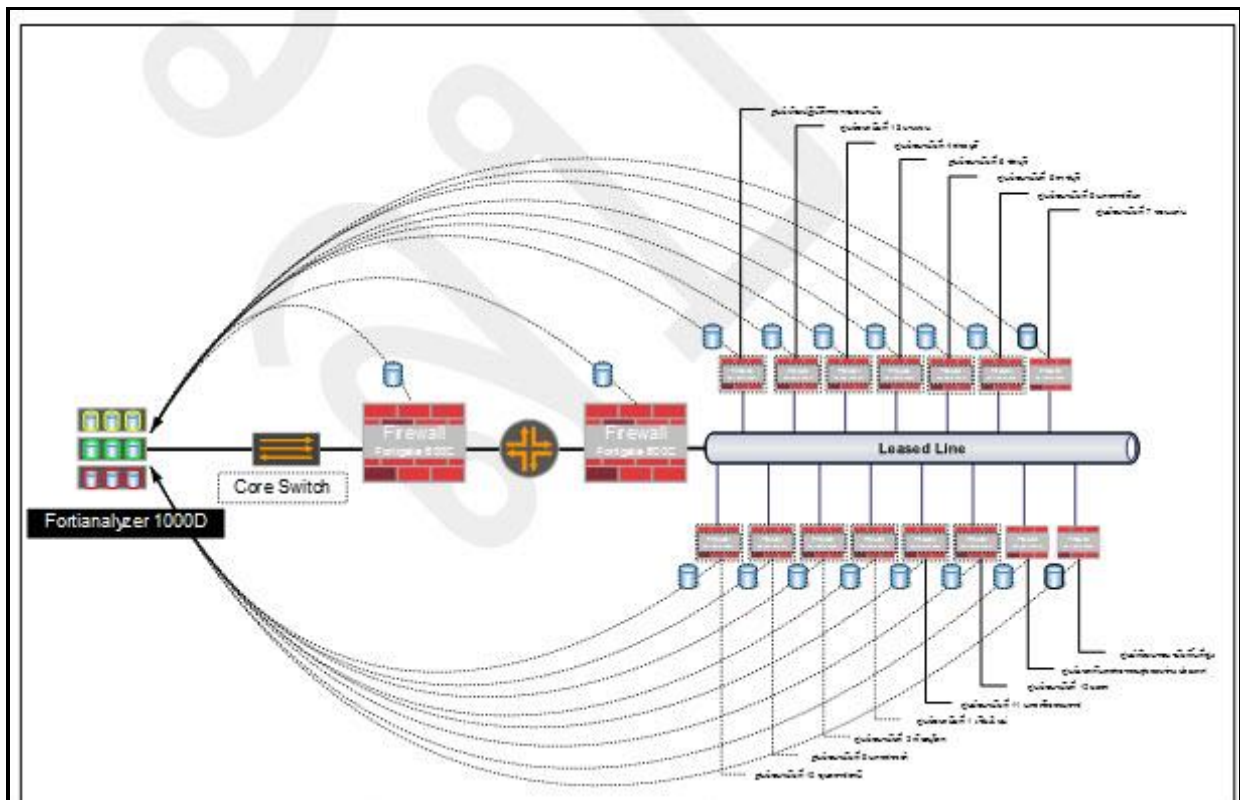
๒.๓ มีการควบคุมการอนุญาตในการเข้าใช้งานระบบ Wireless หรือ Wifi แบบ Open System Authentication mode โดยใช้ MAC-address Authentication

๒.๔ ป้องกันการรบกวนของสัญญาณโดยการปรับ Channel การรับ-ส่งสัญญาณให้ต่างกัน

๓. สถานภาพทางด้านการปริมาณการใช้งานระบบเครือข่ายที่ผ่านมา

กรมอนามัย มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยอุปกรณ์ Fortianalyzer รุ่น ๑๐๐๐D โดยอุปกรณ์ Fortianalyzer จะเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นแบบ Centralized Log แสดงได้ดังรูปที่ ๑.๑๓ กล่าวคือ เป็นระบบบริหารจัดการเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยมีการจัดเก็บที่ส่วนกลางแบบรวม ศูนย์ รองรับข้อมูลจราจรทางคอมพิวเตอร์ สำหรับผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) จากอุปกรณ์เครือข่ายคอมพิวเตอร์ เช่น Firewall, Router, Switch โดยมีระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า ๙๐ วันแต่ไม่เกิน ๑ ปี ข้อมูลจราจรทางคอมพิวเตอร์ที่มีการจัดเก็บ มีดังนี้

- ผู้ใช้งานอินเทอร์เน็ต
- ต้นทางที่ส่งข้อมูล
- เส้นทางที่ข้อมูลส่งผ่าน
- เวลาที่ส่งข้อมูล
- ปริมาณของข้อมูล
- ระยะเวลาที่เชื่อมต่อ
- ปลายทางที่ข้อมูลส่งไปถึง
- ชนิดของบริการ



รูปที่ ๖ การส่งข้อมูลจราจรทางคอมพิวเตอร์จากศูนย์ภูมิภาคไปยังส่วนกลาง และในส่วนกลาง

๒. วิเคราะห์ข้อจำกัดของกรมอนามัยเพื่อพัฒนาโครงสร้างพื้นฐานและระบบสารสนเทศ

จากการที่กรมอนามัยจะก้าวต่อไปยัง กรมอนามัย ๔.๐ เพื่อคนไทย ๔.๐ จึงต้องมีการวิเคราะห์ข้อจำกัดของกรมอนามัยเพื่อที่จะได้มีการพัฒนาโครงสร้างพื้นฐานและระบบสารสนเทศของกรมอนามัยทั้งส่วนกลางและส่วนภูมิภาคในศูนย์ต่าง ๆ ทางด้านเป้าหมายเชิงเทคนิคและข้อจำกัด ซึ่งจะเป็หัวข้อในการวิเคราะห์ความต้องการดังนี้

๑. **การรองรับการขยายตัวในอนาคต (Scalability)** หมายถึงการขยายตัวของระบบเครือข่ายในอนาคต ๓ – ๕ ปีในเรื่องโครงสร้างพื้นฐานของระบบเครือข่ายในการเชื่อมต่อกับระบบเครือข่ายทั้งมีสายและแบบไร้สาย เพื่อที่จะรองรับการทำงานของกรมอนามัย
๒. **การทำงานอย่างต่อเนื่องไม่หยุดชะงัก (Availability)** หมายถึงการใช้งานระบบสารสนเทศของเจ้าหน้าที่ในกรมอนามัย ได้อย่างต่อเนื่องไม่ว่าจะมีการใช้งานในช่วงเวลาใด ใช้งานจากทุกไหน หรืออยู่ที่ไหนก็สามารถที่จะทำงานในระบบสารสนเทศของกรมอนามัย
๓. **การส่งข้อมูลอย่างรวดเร็ว (Performance)** หมายถึงการใช้งานระบบสารสนเทศที่มีปริมาณข้อมูลมาก ๆ เพื่อรองรับข้อมูลทางด้านสุขภาพในอนาคต ๓ – ๕ ปี ที่สามารถรับส่งข้อมูลได้อย่างรวดเร็วต่อการตอบสนองการใ้ในยุคประเทศไทย ๔.๐ หรือ กรมอนามัย ๔.๐
๔. **ความปลอดภัยของข้อมูล (Security)** หมายถึงการรักษาความปลอดภัยของ ข้อมูลและระบบสารสนเทศของกรมอนามัย ทั้งที่เป็น Software และ Hardware ในการใช้งานภายในกรมอนามัย อาทิ ระบบเครือข่ายภายในกรมอนามัย การรักษาความลับของข้อมูลการสุขภาพที่สำคัญของกรมอนามัย ความถูกต้องของข้อมูลในกรมอนามัยที่มีการรับส่งระหว่างระบบสารสนเทศและการสื่อสาร การตรวจสอบระดับในการเข้าถึงข้อมูลต่างๆ ของกรมอนามัย การรองรับลายเซ็นแบบดิจิทัล เป็นต้น
๕. **การบริหารจัดการ (Manageability)** หมายถึงการบริหารจัดการระบบสารสนเทศและการสื่อสารของกรมอนามัยในการที่จะเข้าไปควบคุมระบบ/อุปกรณ์ต่าง ๆ การแก้ไขเปลี่ยนแปลงค่าของระบบ/อุปกรณ์ต่าง ๆ ภายในกรมอนามัย
๖. **การใช้งานง่ายและสะดวก (Usability)** หมายถึงการใช้งานระบบสารสนเทศที่สามารถใช้งานได้ง่าย และสะดวกสบายในการใช้งาน และไม่เกิดความซับซ้อน ยุ่งยากในการใช้งาน รวมทั้งสามารถทำงานได้รวดเร็ว ทำงานได้ทุกที่ ทุกเวลา (Anywhere Anytime)
๗. **การรองรับการเปลี่ยนแปลงในอนาคต (Adaptability)** หมายถึงการที่ระบบสารสนเทศและการสื่อสารพร้อมที่จะรองรับการเปลี่ยนแปลงในอนาคต ๓ – ๕ ปี
๘. **ต้นทุนค่าใช้จ่ายที่เหมาะสม (Affordability)** หมายถึงการลดการลงทุน โดยลงทุนในระบบสารสนเทศที่เหมาะสมกับค่าใช้จ่ายในการลงทุน ในอนาคต ๓ – ๕ ปี

จากหัวข้อข้างต้นที่ได้กล่าวมา จะนำมาใช้ในการวิเคราะห์ความต้องการและข้อเสนอแนะ โดยแบ่งออกเป็นส่วนกลาง และส่วนภูมิภาค/ศูนย์อนามัย ซึ่งจะอาศัยข้อมูลสภาพการใช้งานปัจจุบัน และการกรอกแบบสอบถามที่ได้สอบถามไปยังแต่ละหน่วยงานภายในกรมอนามัยทั้งส่วนกลางและส่วนภูมิภาค/ศูนย์

๓. การรวบรวมและวิเคราะห์ข้อมูลความต้องการและความคาดหวังของ customer และ stakeholder ทั้งในปัจจุบันและพึงมีในอนาคต

การวิเคราะห์ความต้องการ โดยระบบที่มีการขับเคลื่อนและสนับสนุนเทคโนโลยีสารสนเทศ

๓.๑ ระบบศูนย์กลางข้อมูลกรมนามัย (Cloud Storage Service)

การวิเคราะห์ความต้องการ

ทางด้าน การรองรับการเปลี่ยนแปลงในอนาคต (Adaptability)

สภาพปัจจุบัน

จากสถานภาพในปัจจุบันทางกรมนามัยได้มีการออกแบบระบบสารสนเทศและการสื่อสารที่รองรับการเปลี่ยนแปลงในอนาคต ไม่ว่าจะเป็นในส่วนของอุปกรณ์ (Hardware) หรือ โปรแกรมระบบสารสนเทศภายในกรม (Software) รวมทั้งการรองรับการเปลี่ยนทางด้านเครือข่ายในเรื่องของการใช้งาน IPv6 เป็นต้น

ข้อเสนอแนะความต้องการ

การรองรับการเปลี่ยนแปลงที่จะก้าวไปสู่ขั้นที่ “กรมนามัย ๔.๐” นั้นจะต้องมีการรองรับการเพิ่มขึ้นของปริมาณข้อมูลที่มีใช้งานในระบบสารสนเทศและการสื่อสารจึงควรมีโครงการจัดทำโครงการบูรณาการข้อมูลรองรับกรมนามัย ๔.๐ บนระบบการประมวลผลแบบกลุ่มเมฆ (Cloud computing system)

เป้าหมาย (ความคาดหวัง)

- จัดหาระบบศูนย์กลางข้อมูลกรมนามัย (Cloud Storage Service)
- ขยายพื้นที่จัดเก็บข้อมูลให้ครอบคลุมภารกิจ หน้าที่ความรับผิดชอบ กรมนามัย จากเดิม ๑๗ TB เป็น ๓๓ TB อีกทั้งสามารถขยายฐานเพิ่มได้ตามความต้องการและปริมาณของข้อมูล โดยจัดหาเฉพาะหน่วยจัดเก็บข้อมูล
- ขยายพื้นที่ระบบฐานข้อมูลรองรับการให้บริการข้อมูลประชาชน
- ลดความซ้ำซ้อนของข้อมูล จากเดิมเก็บไว้ตามหน่วยงาน เป็นเก็บไว้กับระบบศูนย์กลางข้อมูลกรมนามัย
- เพิ่มการเข้าถึงข้อมูลของผู้บริหาร จากเดิมขอข้อมูลตามหน่วยงาน เป็นสามารถเข้าถึงได้ตามสิทธิ์
- เพิ่มการเข้าถึงข้อมูลของผู้ปฏิบัติงาน จากเดิมขอข้อมูลตามหน่วยงาน เป็นสามารถเข้าถึงได้ตามสิทธิ์หน้าที่ความรับผิดชอบ และการได้รับอนุญาตเข้าถึงข้อมูล
- เพิ่มประสิทธิภาพการสำรองและกู้คืนข้อมูล จากเดิมสำรองเป็นชุดไฟล์ข้อมูล เป็นสำรองเป็น Image files.
- ป้องกันปัญหาระบบล่มอย่างมีประสิทธิภาพ

๓.๒ การปรับปรุงระบบเครือข่ายคอมพิวเตอร์

การวิเคราะห์ความต้องการ

ทางด้าน การส่งข้อมูลอย่างรวดเร็ว (Performance)

สภาพปัจจุบัน

จากสถานการณ์ในปัจจุบันในการรับส่งข้อมูลบางจุดการเชื่อมต่อมีการส่งข้อมูลที่ไม่ราบรื่นทำให้ไม่สามารถใช้งานบนโปรแกรม (Application) ที่มีการเชื่อมต่อไปยังเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ ซึ่งส่งผลให้เกิดการส่งข้อมูลไปได้บ้างช่วงเวลา ทั้งภายในและภายนอก

ข้อเสนอแนะความต้องการ

การรับส่งข้อมูลในระบบเครือข่ายที่ไม่ราบรื่นในการรับส่งข้อมูลภายในเครือข่ายกรมอนามัย กล่าวคือเมื่อมีการใช้งานระบบสาย LAN ที่มีหัวในการเชื่อมต่อจะอุปกรณ์ patch panel ที่เชื่อมต่อสายแลนเกิดความเสื่อมสภาพ ในการใช้งาน โดยปกติ patch panel ในการเชื่อมต่อจะมีอายุการใช้งานประมาณ ๑๔ ปี ในสภาวะการใช้งานทั่วไป จึงต้องมีการซ่อมบำรุงโดยการเข้าโดยการทำความสะอาดและเข้าสายแลนใหม่ เพื่อให้พร้อมในการใช้งาน

เป้าหมาย (ความคาดหวัง)

- กรมอนามัยมีระบบเครือข่ายที่มีเสถียรภาพ และรองรับเทคโนโลยีความเร็วอินเทอร์เน็ต
- กรมอนามัยมีโครงสร้างที่รองรับระบบสุขภาพ Health Data Center (HDC)
- ระบบเครือข่ายของกรมอนามัยครอบคลุมพื้นที่การปฏิบัติงานของเจ้าหน้าที่

๓.๓ การรวบรวมและวิเคราะห์ข้อมูลความต้องการและความคาดหวังของ customer และ stakeholder ของระบบเครือข่ายที่เหมาะสมกับพันธกิจ

๓.๓.๑ customer และ stakeholder ของกรมอนามัยในส่วนกลาง

ตารางที่ ๑๒ แสดงการวิเคราะห์ความต้องการของกรมอนามัยในส่วนกลาง

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
๑	การรองรับการขยายตัวในอนาคต (Scalability)	- จากสถานะปัจจุบันพบว่า ระบบเครือข่ายของกรมอนามัยยังสามารถที่จะรองรับการขยายตัวของเครื่องลูกข่ายภายในกรมอนามัย เนื่องจากจำนวนเครื่องลูกข่ายที่มีการเชื่อมต่อผ่านทางระบบสายแลน มีจำนวนที่ไม่มีการเปลี่ยนแปลงจากปัจจุบันไปยังอนาคตไม่มากนัก แต่มีการเพิ่มปริมาณการใช้งานของเครื่องลูกข่ายทางการเชื่อมต่อผ่านทางระบบไร้สายมากขึ้นในบางพื้นที่ในการให้บริการ ทำให้การเชื่อมต่อไม่เพียงพอต่อการใช้งาน หรือกล่าวได้ว่าการเชื่อมต่อเต็มในการใช้งาน - ในส่วนของการขยายตัวสำหรับอุปกรณ์ในการใช้งานของระบบเครือข่ายในส่วนกลางทั้งเครือข่ายแบบสายหรือไร้สายที่เป็นระบบ IPv๖ ก็มีการรองรับการใช้งานในระบบ IPv๖ address ที่จะเริ่มมีการใช้งานไปยังอนาคต	ข้อเสนอแนะในเรื่องระบบเครือข่ายไร้สายให้ทำการเพิ่มปริมาณของ Access point แล้วทำการปรับแต่งสัญญาณในการให้บริการให้ครอบคลุมการใช้งานของเจ้าหน้าที่ภายในกรมอนามัย โดยจะต้องมีการกำหนดขอบเขตของสัญญาณในปลายขอบสัญญาณว่าจะให้มีปริมาณการรับส่งข้อมูลได้เท่าไร อาทิ ขั้นต่ำ ๕.๕Mbps หรือ ๑๒Mbps เป็นต้น โดยควรจะมีการจัดทำโครงการพัฒนาระบบเครือข่ายไร้สายของกรมอนามัย
๒	การทำงานอย่างต่อเนื่องไม่หยุดชะงัก (Availability)	จากสถานะปัจจุบันพบว่าทางกรมอนามัยได้มีการป้องกันระบบเครือข่ายที่ไม่สามารถให้บริการได้ ที่เกิดมากจากระบบไฟฟ้าขัดข้อง โดยได้นำเอาระบบสำรองไฟฟ้า (UPS) มาช่วยในการสำรองไฟฟ้าให้แก่อุปกรณ์ในระบบเครือข่าย ทำให้ระบบเครือข่ายสามารถที่จะทำงานได้ในสภาวะที่ระบบไฟฟ้ากรมอนามัยขัดข้อง แต่ทางด้านระบบเครื่องแม่ข่ายที่เป็นในส่วนของ การให้บริการทั้งระบบโปรแกรมและระบบข้อมูลต่าง ๆ ภายในกรมอนามัย เมื่อเกิดปัญหาที่ไม่สามารถเชื่อมต่อได้หรือปัญหาทางภัยพิบัติ ทางกรมอนามัยยังไม่มีระบบ	ข้อเสนอแนะควรเตรียมการในการจัดทำ โครงการศูนย์ข้อมูลและระบบงานสำรอง (DR Site) เพื่อที่รองรับการทำงานของระบบงานและข้อมูลได้ตลอด ๒๔ ชม. โดยในการจัดทำโครงการดังกล่าว ควรที่จะจัดเตรียมในระดับ Warm Site หมายถึง จะมี Hardware และ Software ตั้งอยู่ที่ Backup Site เหมือนกับที่ Main Site ระบบสำรองจะทำงานในลักษณะ Standby ไม่ได้ใช้งานจริง ข้อมูลที่ถูก update ในระบบหลัก จะถูก update ในระบบสำรองตามช่วงเวลาที่กำหนด เมื่อเกิดปัญหากับระบบหลัก ระบบสำรองก็จะถูกนำมาใช้

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
		สำรองเครื่องแม่ข่าย หรือ ศูนย์ข้อมูลสำรองเวลาเกิดปัญหาทางด้านภัยพิบัติ ซึ่งอาจจะส่งผลให้เครื่องลูกข่ายไม่สามารถใช้งานได้จากที่ใดที่หนึ่งในการทำงานของกรมอนามัย ซึ่งในอนาคตกรมอนามัยได้มีการวางแผนงานของอนามัยในการก้าวไปสู่ กรมอนามัย ๔.๐ ที่ต้องอาศัยระบบโครงสร้างพื้นฐานรวมถึงศูนย์กลางข้อมูลสำรองเพื่อที่จะระบบงานต่าง ๆ และข้อมูลต่าง ๆ สามารถใช้งานได้ตลอด ๒๔ ชม. ในการให้บริการแก่เจ้าหน้าที่ของกรม และบุคคลภายนอก กรมอนามัยเข้ามาใช้งานได้อย่างมีประสิทธิภาพ	งาน โดยจะต้องทำการ update ข้อมูลส่วนที่ขาดหายไปให้ครบถ้วนเสียก่อน ปกติก็ประมาณ ๑ วัน จึงจะสามารถใช้งานได้ ซึ่งปัจจัยในการจะเลือกกว่าจะใช้ DR Site ระดับใด ขึ้นอยู่กับองค์ประกอบดังนี้ ๑. องค์กรสามารถปล่อยให้ระบบคอมพิวเตอร์ของตัวเองล่มได้นานสุดเท่าไร โดยไม่กระทบต่อธุรกิจ (RTO: Real Time Objective) ๒. เมื่อ Recovery DR Site แล้ว จะสามารถใช้งานได้เมื่อมีข้อมูลอย่างน้อยที่สุดอัปเดตแค่ไหน (RPO: Real Point Objective)
๓	การส่งข้อมูลอย่างรวดเร็ว (Performance)	จากสถานภาพในปัจจุบันในการรับส่งข้อมูลบางจุดการเชื่อมต่อมีการส่งข้อมูลที่ไม่ราบรื่นทำให้ไม่สามารถใช้งานบนโปรแกรม (Application) ที่มีการเชื่อมต่อไปยังเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ ซึ่งส่งผลให้เกิดการส่งข้อมูลไปได้บ้างช่วงเวลา ทั้งภายในและภายนอก	○ ข้อเสนอแนะในเรื่องการรับส่งข้อมูลในระบบเครือข่ายที่ไม่ราบรื่นในการรับส่งข้อมูลภายในเครือข่ายกรมอนามัย กล่าวคือเมื่อมีการใช้งานระบบสาย LAN ที่มีหัวในการเชื่อมต่อจะอุปกรณ์ patch panel ที่เชื่อมสายแลนเกิดความเสื่อมสภาพ ในการใช้งาน โดยปกติ patch panel ในการเชื่อมต่อจะมีอายุการใช้งานประมาณ ๑๔ ปี ในสภาวะการใช้งานทั่วไป จึงต้องมีการซ่อมบำรุงโดยการเข้าโดยการทำความสะอาดและเข้าสายแลนใหม่ เพื่อให้พร้อมในการใช้งาน ○ ข้อเสนอแนะในเรื่องการรับส่งข้อมูลในระบบเครือข่ายที่ไม่ราบรื่นในการรับส่งข้อมูลภายนอกเครือข่ายกรมอนามัย ควรที่จะทำการเพิ่ม Bandwidth ของการใช้งานจากเดิม โดยวิธีการคิดปริมาณ Bandwidth จะทำการคิดประมาณการใช้งานในปัจจุบัน แต่ต้องไม่เกิน ๕๐ – ๗๐ เปอร์เซ็นต์ของปริมาณ Bandwidth อินเทอร์เน็ตที่มีทั้งหมด

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
			○ ข้อเสนอแนะควรที่จะมีการจำกัดปริมาณ Bandwidth ที่มีการใช้งาน ซึ่งโดยปกติในการใช้งานทั่วไป ปริมาณ Bandwidth ที่มีการใช้งานกันอย่างราบรื่นในการรับส่งข้อมูลควรอยู่ที่ ๔ – ๕ Mbps โดยในปริมาณ Bandwidth ดังกล่าวจะสามารถใช้งาน Application แบบ video streaming ได้ที่ ๗๒๐p เป็นต้น
๔	ความปลอดภัยของข้อมูล (Security)	● จากสถานภาพในปัจจุบันทางกรมอนามัยได้มีการนำเอาระบบสารสนเทศและการสื่อสาร เข้ามาใช้ในการปฏิบัติงานของกรมอนามัย ไม่ว่าจะเป็นระบบต่าง ๆ ของกรมอนามัย ที่จะต้องมีการจัดเก็บข้อมูล ซึ่งทางกรมอนามัยก็ได้มีการออกแบบระบบรักษาความปลอดภัยทั้งทางด้านระบบเครือข่าย และการใช้งานของเจ้าหน้าที่ในกรมอนามัย โดยทางด้านระบบเครือข่ายกรมอนามัยได้มีการติดตั้งระบบรักษาความปลอดภัย (Firewall) และระบบตรวจจับผู้บุกรุก (IPS: Intrusion Prevention System) เพื่อที่จะทำการป้องกันและตรวจจับผู้บุกรุกที่โจมตีเข้ามาทางระบบเครือข่าย ในส่วนของเข้าใช้งานในระบบสารสนเทศของกรมอนามัย ทางกรมอนามัยได้มีการจัดระดับการเข้าไปใช้งานในระบบสารสนเทศออกเป็นระดับต่าง ๆ ตามชั้นความปลอดภัยที่ได้กำหนดเป็นนโยบายของกรมอนามัย	○ ข้อเสนอแนะ จากการตรวจสอบทางด้านระบบความปลอดภัยของกรมอนามัยในการป้องกันการโจมตีจากผู้ไม่ประสงค์ดี พบว่า ข้อมูลขั้นพื้นฐานในการที่จะโจมตีต่อระบบเครื่องแม่ข่ายของกรมอนามัยยังไม่มีมีการปกปิดทำให้มีโอกาสสูงที่จะทำให้ผู้บุกรุกสามารถโจมตีสำเร็จและเข้ายึดเครื่องแม่ข่ายในกรมอนามัยได้อย่างสมบูรณ์ ทางแก้ไขควรที่จะจัดทำโครงการตรวจสอบระบบความปลอดภัยของระบบสารสนเทศและการสื่อสารของกรมอนามัย (penetration test) ในส่วนของระบบงานการให้บริการหรือระบบงานที่ต้องการทำการเผยแพร่ข้อมูลของกรมอนามัย และโครงการเสริมสร้างความแข็งแกร่งของระบบสารสนเทศและการสื่อสาร (Hardening System) เพื่อช่วยการป้องกันการโจมตีจากผู้ไม่ประสงค์ดีได้อย่างมีประสิทธิภาพ ○ ข้อเสนอแนะในการให้ความรู้ทางด้านความมั่นคงปลอดภัย ควรจะมีการอบรมด้านระบบความปลอดภัยขั้นพื้นฐานในการใช้งานระบบเครือข่ายอินเทอร์เน็ต เพื่อให้เจ้าหน้าที่มีความตระหนักถึงการป้องกันตัวเองและองค์กรต่อการโจมตีของผู้บุกรุกในรูปแบบต่าง ๆ บนระบบเครือข่ายอินเทอร์เน็ตเป็นประจำทุกปี

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
๕	การบริหารจัดการ (Manageability)	จากสถานภาพในปัจจุบันทางกรมอนามัยได้มีการนำระบบการจัดการทั้งทางด้านระบบเครือข่ายและระบบงานสารสนเทศที่กรมอนามัยเข้ามาใช้งานได้อย่างมีประสิทธิภาพ และง่ายในการใช้งานสำหรับผู้ดูแลระบบ รวมทั้งได้มีการจัดหาที่ปรึกษาทางด้านระบบสารสนเทศและการสื่อสารเข้ามาช่วยในการบริหารจัดการระบบสารสนเทศและการสื่อสารของกรมอนามัย	ข้อเสนอแนะ ควรจะมีระบบในการจัดเก็บปัญหาและแนวทางในการแก้ไขที่เกิดขึ้นกับระบบสารสนเทศและการสื่อสารของกรมอนามัย เพื่อที่จะได้แก้ไขปัญหาดัง ๆ ที่เกิดขึ้นได้อย่างรวดเร็วและสามารถที่จะพัฒนาไปยังการแก้ไขปัญหาอื่น ๆ ได้ในอนาคต
๖	การใช้งานง่ายและสะดวก (Usability)	จากสถานภาพในปัจจุบันทางกรมอนามัยได้ทำการปรับปรุงระบบสารสนเทศและการสื่อสารของกรมอนามัยให้มีการใช้งานที่ง่ายและสะดวกต่อการใช้งานของผู้ใช้ในงานในกรมอนามัย และได้มีการอบรมในการใช้งานของระบบสารสนเทศและการสื่อสารของกรมอนามัยอย่างต่อเนื่อง ซึ่งเมื่อทางกรมอนามัยได้มีการเปลี่ยนแปลงก็จะมีการอัปเดตข้อมูลไปยังเจ้าหน้าที่ในกรมอย่างต่อเนื่อง แต่ก็มีในบางครั้งที่เจ้าหน้าที่ไม่ได้รับข่าวสารในการปรับเปลี่ยนการใช้งานทำให้เกิดการใช้งานที่ไม่สามารถใช้งานได้	ข้อเสนอแนะ ควรจะมีการแจ้งข่าวสารผ่านทางระบบ อีเมลล์ หรือ ช่องที่เป็นประชาสัมพันธ์ของกรมอนามัยเพื่อที่จะทำให้เจ้าหน้าที่ผู้ใช้งานในระบบสารสนเทศและการสื่อสารได้รับข่าวสารอย่างทั่วถึง
๗	การรองรับการเปลี่ยนแปลงในอนาคต (Adaptability)	จากสถานภาพในปัจจุบันทางกรมอนามัยได้มีการออกแบบระบบสารสนเทศและการสื่อสารที่รองรับการเปลี่ยนแปลงในอนาคต ไม่ว่าจะเป็นในส่วนของอุปกรณ์ (Hardware) หรือ โปรแกรมระบบสารสนเทศภายในกรม (Software) รวมทั้งการรองรับการเปลี่ยนทางด้านเครือข่ายในเรื่องของการใช้งาน IPv6 เป็นต้น	ข้อเสนอแนะ ในการรองรับการเปลี่ยนแปลงที่จะก้าวไปสู่ นิยามที่ว่า “กรมอนามัย ๔.๐” นั้นจะต้องมีการรองรับการเพิ่มขึ้นของปริมาณข้อมูลที่มีใช้งานในระบบสารสนเทศและการสื่อสารจึงควรที่จะมี โครงการจัดทำฐานข้อมูลรองรับกรมอนามัย ๔.๐ บนระบบการประมวลผลแบบกลุ่มเมฆ (Cloud computing system)

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
๘	ต้นทุนค่าใช้จ่ายที่เหมาะสม (Affordability)	- การออกแบบระบบเครือข่ายแลน (LAN) ในแต่ละหน่วยงานรองรับการทำงานในของเจ้าหน้าที่ในตำแหน่งที่ต่าง ๆ โดยจะอยู่ในกระบวนการในการสร้างตึก/การตกแต่งปรับปรุงสถานที่ใหม่ของสำนักงาน แต่เมื่อเวลาผ่านไปจะเกิดปัญหาการใช้งานที่ไม่ราบรื่น ๆ ไม่ว่าจะเป็นการเคลื่อนย้ายตำแหน่งหรือที่นั่งต่าง ๆ กันใหม่ ซึ่งต้องมีการมีจัดซื้อจัดจ้างในการเดินสายใหม่ รวมไปถึงการรับส่งข้อมูลที่ไม่ราบรื่นในการใช้งานบนระบบเครือข่ายทำให้เกิดปัญหาขึ้นในการใช้งาน - จากสถานภาพในปัจจุบันทางกรมอนามัยได้มีการนำเอาระบบเครื่องแม่ข่ายเสมือน (Virtual server) เข้ามาใช้งาน ในศูนย์ข้อมูลของกรมอนามัยทำให้สามารถที่จะประหยัดค่าใช้จ่ายในการลงทุน เพื่อให้ให้บริการได้อย่างมีประสิทธิภาพและประสิทธิผลอย่างสูงสุดในการใช้งานทรัพยากรของกรมอนามัย	ข้อเสนอแนะในเรื่องระบบเครือข่าย (LAN) ในส่วนที่การเคลื่อนตำแหน่งที่นั่งไปยังที่ต่าง ภายในหน่วยงานของกรมอนามัย ควรที่จะต้องมี เจ้าหน้าที่ดูแลรับผิดชอบในการเดินสายแลน ภายในเพื่อที่จะได้ทำการปรับปรุงอัปเดตโครงสร้างของระบบเครือข่ายให้ทันสมัย ซึ่งเมื่อเกิดปัญหาจะได้ทำการแก้ไขได้อย่างมีประสิทธิภาพ

๓.๓.๒ customer และ stakeholder ของกรมอนามัยในส่วนภูมิภาค/ศูนย์

ตารางที่ ๑๓ แสดงการวิเคราะห์ความต้องการของกรมอนามัยในส่วนภูมิภาค/ศูนย์

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
๑	การรองรับการขยายตัวในอนาคต (Scalability)	- จากสถานะปัจจุบันพบว่าทางศูนย์ต่าง ๆ ของกรมอนามัยได้มีการออกแบบและใช้งานระบบเครือข่ายภายในของแต่ละศูนย์ที่แตกต่างกัน ทำให้เวลาที่มีการขยายตัวของระบบเครือข่ายในการเชื่อมต่อของผู้ใช้งานทั้งภายในและภายนอกเกิดความยุ่งยากในการพัฒนาระบบเครือข่าย และเกิดความซับซ้อนในการขยายระบบเครือข่าย ไม่ว่าจะเป็นเครือข่ายระบบแลนและเครือข่ายไร้สาย - ในส่วนของการขยายตัวสำหรับอุปกรณ์ในการใช้งานของระบบเครือข่ายในส่วนของศูนย์ทั้งเครือข่ายแบบสาย หรือไร้สายที่เป็นระบบ IPv6 อาจจะยังไม่มี การรองรับการใช้งานในระบบ IPv6 address ที่จะเริ่มมีการใช้งานไปยังอนาคต	○ ข้อเสนอแนะ ควรที่จะมีการกำหนดรูปแบบการเชื่อมต่อเครือข่ายภายในของศูนย์ต่าง ๆ ให้เป็นไปในรูปแบบเดียวกัน โดยมีส่วนกลางเป็นผู้ช่วยในการดูแลและพัฒนา ระบบเครือข่ายของศูนย์ต่าง ๆ เพื่อที่จะทำให้เกิดการรองรับการขยายตัวของระบบเครือข่ายไปในแนวทางเดียวกันของทุกศูนย์
๒	การทำงานอย่างต่อเนื่องไม่หยุดชะงัก (Availability)	จากสถานะปัจจุบันพบว่าทางศูนย์ของกรมอนามัย <u>บางส่วน</u> ได้มีการป้องกันระบบเครือข่ายที่ไม่สามารถให้บริการได้ ที่เกิดมากจากระบบไฟฟ้าขัดข้อง โดยได้นำเอาระบบสำรองไฟฟ้า (UPS) มาช่วยในการสำรองไฟฟ้าให้แก่อุปกรณ์ในระบบเครือข่าย ทำให้ระบบเครือข่ายสามารถที่จะทำงานได้ในสภาวะที่ระบบไฟฟ้าของศูนย์ต่าง ๆ ขัดข้อง แต่ทางด้านระบบเครื่องแม่ข่ายที่เป็นในส่วนของการให้บริการทั้งระบบโปรแกรมและระบบข้อมูลต่าง ๆ ภายในศูนย์กรมอนามัย เมื่อเกิดปัญหาที่ไม่สามารถเชื่อมต่อได้หรือปัญหาทางภัยพิบัติทางศูนย์ของกรมอนามัยต่าง ๆ ยังไม่มีระบบสำรองเครื่องแม่ข่าย หรือ ศูนย์ข้อมูลสำรองเวลาเกิดปัญหาทางด้านภัยพิบัติ ซึ่งอาจจะส่งผลให้เครื่องลูกข่ายไม่	○ ข้อเสนอแนะทางศูนย์ต่าง ๆ ของกรมอนามัยส่วนที่ยังขาดระบบสำรองไฟฟ้าให้กับเครื่องแม่ข่ายและอุปกรณ์เครือข่าย จะต้องทำการติดตั้ง เพื่อจะได้ไม่เกิดปัญหาในการใช้งานที่หยุดชะงักในการทำงานของระบบสารสนเทศและการสื่อสาร ○ ข้อเสนอแนะทางศูนย์ต่าง ๆ ของกรมอนามัยควรที่จะต้องทำการสำรองระบบสารสนเทศของแต่ละศูนย์ฯ ไว้ที่กรมอนามัย ซึ่งจะทำหน้าที่เป็น ศูนย์ข้อมูลและระบบงานสำรอง (DR Site) เพื่อที่รองรับการทำงานของระบบงานและข้อมูลของศูนย์ต่าง ๆ ได้ตลอด ๒๔ ชม. โดยควรที่จะวางแผนงานในการจัดตั้งศูนย์สำรองระบบงานและข้อมูล กับกรมอนามัยในส่วนกลางในรูปแบบระดับ Warm Site

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
		สามารถใช้งานได้จากที่ใดที่หนึ่งในการทำงานของศูนย์ต่าง ๆ ของกรมอนามัย ซึ่งในอนาคตทางกรมอนามัยได้มีการวางแผนงานของอนามัยในการก้าวไปสู่ กรมอนามัย ๔.๐ ที่ต้องอาศัยระบบโครงสร้างพื้นฐานรวมไปถึงศูนย์กลางข้อมูลสำรองเพื่อที่ระบบงานต่าง ๆ และข้อมูลต่าง ๆ สามารถใช้งานได้ตลอด ๒๔ ชม. ในการให้บริการแก่เจ้าหน้าที่ของศูนย์ของกรม และบุคคลภายนอกของศูนย์ต่าง ๆ ของกรมอนามัยเข้ามาใช้งานได้อย่างมีประสิทธิภาพ	
๓	การส่งข้อมูลอย่างรวดเร็ว (Performance)	จากสถานภาพในปัจจุบันพบว่าทางศูนย์ต่าง ๆ ของกรมอนามัย ในการรับส่งข้อมูลบ้างจุดการเชื่อมต่อมีการส่งข้อมูลที่ไม่ราบรื่นทำให้ไม่สามารถใช้งานบนโปรแกรม (Application) ที่มีการเชื่อมต่อไปยังเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ ซึ่งส่งผลให้เกิดการส่งข้อมูลไปได้บ้างช่วงเวลา ทั้งภายในและภายนอก	○ ข้อเสนอแนะในเรื่องการรับส่งข้อมูลในระบบเครือข่ายที่ไม่ราบรื่นในการรับส่งข้อมูลภายในเครือข่ายกรมอนามัย กล่าวคือเมื่อมีการใช้งานระบบสาย LAN ที่มีหัวในการเชื่อมต่อจะอุปกรณ์ patch panel ที่เชื่อมสายแลนเกิดความเสื่อมสภาพ ในการใช้งาน โดยปกติ patch panel ในการเชื่อมต่อจะมีอายุการใช้งานประมาณ ๑๔ ปี ในสภาวะการใช้งานทั่วไป จึงต้องมีการซ่อมบำรุงโดยการเข้าโดยการทำความสะอาดและเข้าสายแลนใหม่ เพื่อให้พร้อมในการใช้งาน ○ ข้อเสนอแนะในเรื่องการรับส่งข้อมูลในระบบเครือข่ายที่ไม่ราบรื่นในการรับส่งข้อมูลภายนอกเครือข่ายกรมอนามัย ควรที่จะทำการเพิ่ม Bandwidth ของการใช้งานจากเดิม โดยวิธีการคิดปริมาณ Bandwidth จะทำการคิดประมาณการใช้งานในปัจจุบัน แต่ต้องไม่เกิน ๕๐ – ๗๐ เปอร์เซ็นต์ ของปริมาณ Bandwidth อินเทอร์เน็ตที่มีทั้งหมด

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
			○ ข้อเสนอแนะในการควรที่จะมีการจำกัดปริมาณ Bandwidth ที่มีการใช้งาน ซึ่งโดยปกติในการใช้งานทั่วไป ปริมาณ Bandwidth ที่มีการใช้งานกันอย่างราบรื่นในการรับส่งข้อมูลควรอยู่ที่ ๔ – ๕ Mbps โดยในปริมาณ Bandwidth ดังกล่าวจะสามารถใช้งาน Application แบบ video streaming ได้ที่ ๗๒๐p เป็นต้น
๔	ความปลอดภัยของข้อมูล (Security)	● จากสถานภาพในปัจจุบันพบว่าทางศูนย์ต่าง ๆ ของกรมอนามัย ได้มีการนำเอาระบบสารสนเทศและการสื่อสาร เข้ามาใช้ในการปฏิบัติงานของกรมอนามัย ไม่ว่าจะเป็นระบบต่าง ๆ ของกรมอนามัย ที่จะต้องมีการจัดเก็บข้อมูล ซึ่งทางศูนย์ต่าง ๆ ของกรมอนามัยก็ได้มีการออกแบบระบบรักษาความปลอดภัยทั้งทางด้านระบบเครือข่าย และการใช้งานของเจ้าหน้าที่ในกรมอนามัย โดยทางด้านระบบเครือข่ายกรมอนามัยได้มีการติดตั้งระบบรักษาความปลอดภัย (Firewall) และระบบตรวจจับผู้บุกรุก (IPS: Intrusion Prevention System) เพื่อที่จะทำการป้องกันและตรวจจับผู้บุกรุกที่โจมตีเข้ามาทางระบบเครือข่าย ในส่วนของเข้าใช้งานในระบบสารสนเทศของกรมอนามัย ทางกรมอนามัยได้มีการจัดระดับการเข้าไปใช้งานในระบบสารสนเทศออกเป็นระดับต่าง ๆ ตามชั้นความปลอดภัยที่ได้กำหนดเป็นนโยบายของกรมอนามัย	○ ข้อเสนอแนะ จากการตรวจสอบทางด้านระบบความปลอดภัยของศูนย์ต่าง ๆ ของกรมอนามัยในการป้องกันการโจมตีจากผู้ที่ไม่ประสงค์ดี พบว่า ข้อมูลชั้นพื้นฐานในการที่จะโจมตีต่อระบบเครื่องแม่ข่ายของศูนย์ ๆ ของกรมอนามัยที่ให้บริการแก่บุคคลภายนอก ยังไม่มีการปกปิดทำให้มีโอกาสสูงที่จะทำให้ผู้บุกรุกสามารถโจมตีสำเร็จและเข้ายึดเครื่องแม่ข่ายในกรมอนามัยได้อย่างสมบูรณ์ ทางแก้ไขควรที่จะจัดทำโครงการตรวจสอบระบบความปลอดภัยของระบบสารสนเทศและการสื่อสารของกรมอนามัย (penetration test) ในส่วนของระบบงานการให้บริการหรือระบบงานที่ต้องการทำการเผยแพร่ข้อมูลของศูนย์ต่าง ๆ ของกรมอนามัย และโครงการเสริมสร้างความแข็งแกร่งของระบบสารสนเทศและการสื่อสาร (Hardening System) เพื่อช่วยการป้องกันการโจมตีจากผู้ที่ไม่ประสงค์ดีได้อย่างมีประสิทธิภาพ ○ ข้อเสนอแนะในการให้ความรู้ทางด้านความมั่นคงปลอดภัย ควรจะมีการอบรมด้านระบบความปลอดภัยขั้นพื้นฐานในการใช้งานระบบเครือข่ายอินเทอร์เน็ต เพื่อให้เจ้าหน้าที่ที่มีความตระหนักถึงการป้องกันตัวเองและองค์กรต่อการโจมตีของผู้บุกรุกในรูปแบบต่าง ๆ บนระบบเครือข่ายอินเทอร์เน็ตเป็นประจำทุกปี

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
๕	การบริหารจัดการ (Manageability)	จากสถานภาพในปัจจุบันพบว่าทางศูนย์ต่าง ๆ ของกรมอนามัย มีบางส่วนยังขาดระบบการจัดการทางด้านระบบเครือข่ายที่ประสิทธิภาพไม่ว่าจะเป็นระบบเครือข่ายที่มีสายแลนหรือระบบเครือข่ายที่ไร้สายทำให้เมื่อเกิดปัญหาในการใช้งานมีความล่าช้าในการแก้ไขปัญหาและการบริหารจัดการระบบเครือข่าย	ข้อเสนอแนะ ควรมีการจัดอบรมในเรื่องระบบเครือข่ายขั้นพื้นฐานในการดูแลระบบเครือข่ายไม่ว่าจะเป็นระบบแลนหรือระบบเครือข่ายไร้สายให้แก่เจ้าหน้าที่ของศูนย์ ๆ ของกรมอนามัยเพื่อที่จะสามารถและดูแลระบบเครือข่ายเบื้องต้นได้อย่างมีประสิทธิภาพ
๖	การใช้งานง่ายและสะดวก (Usability)	จากสถานภาพในปัจจุบันพบว่าทางศูนย์ต่าง ๆ ของกรมอนามัยได้มีการใช้งานระบบสารสนเทศส่วนใหญ่จะเป็นระบบที่ส่วนกลางของกรมอนามัยเป็นผู้จัดทำและให้บริการแก่ศูนย์ต่าง ๆ ของกรมอนามัย และทางส่วนกลางได้มีการจัดทำคู่มือและอบรมการใช้งานระบบสารสนเทศที่พัฒนาขึ้นมาใช้งานของกรมอนามัยอย่างต่อเนื่อง ทำให้สามารถใช้งานได้ง่ายและสะดวกในการใช้งาน	ไม่มี
๗	การรองรับการเปลี่ยนแปลงในอนาคต (Adaptability)	จากสถานภาพในปัจจุบันพบว่าทางศูนย์ต่าง ๆ ของกรมอนามัย บางส่วนยังขาดการออกแบบและการรองรับการเปลี่ยนแปลงของระบบเครือข่ายที่จะต้องเกิดขึ้นในอนาคต ไม่ว่าจะเป็นในส่วนของอุปกรณ์ (Hardware) หรือ โปรแกรมระบบสารสนเทศภายในกรม (Software) รวมทั้งการรองรับการเปลี่ยนทางด้านเครือข่ายในเรื่องของการใช้งาน IPv6 เป็นต้น	ข้อเสนอแนะทางส่วนกลางของกรมอนามัยควรจะต้องเข้ามาร่วมในการออกแบบและปรับเปลี่ยนโครงสร้างระบบเครือข่ายเพื่อที่จะได้รองรับการเปลี่ยนแปลงในอนาคตของกรมอนามัย

ลำดับที่	หัวข้อการวิเคราะห์ความต้องการ	สภาพปัจจุบัน	ข้อเสนอแนะความต้องการของระบบเครือข่าย
๘	ต้นทุนค่าใช้จ่ายที่เหมาะสม (Affordability)	จากสถานภาพในปัจจุบันพบว่าทางศูนย์ต่าง ๆ ของกรมอนามัย ได้มีการลงทุนในการที่จะเชื่อมต่อระบบเครือข่ายภายในของแต่ละศูนย์ต่าง ๆ ของกรมอนามัย กับระบบอินเทอร์เน็ตเป็นของแต่ละศูนย์ และได้มีการเชื่อมต่อมาจากส่วนกลาง ซึ่งจะทำให้การใช้งบประมาณของการลงทุนที่ซับซ้อนกับทางส่วนกลางของกรมอนามัยในการดูแลค่าใช้จ่ายของการลงทุนเกี่ยวกับการเชื่อมต่อระบบอินเทอร์เน็ตของศูนย์ต่าง ๆ ของกรมอนามัย	ข้อเสนอแนะ ควรจะมีการรวมกันระหว่างศูนย์ต่าง ๆ กับทางส่วนกลางในการวางแผนการเชื่อมต่อระบบเครือข่ายภายในของศูนย์ต่าง ๆ กับระบบอินเทอร์เน็ตที่มีการใช้งบประมาณในการลงทุนที่ไม่ซับซ้อนกัน หรืออาจจะจัดทำโครงการการเชื่อมต่อระบบอินเทอร์เน็ตของศูนย์ต่าง ๆ ภายในกรมอนามัย

๔. Best Practice ทั้งในประเทศ/ต่างประเทศ

๔.๑ ระบบบริการศูนย์กลางข้อมูลกรมนามัย (Cloud Storage Service)

ระบบบริการศูนย์กลางข้อมูลกรมนามัย (Cloud Storage Service) นั้น จึงเป็นระบบที่สำคัญอย่างยิ่งในการดำเนินงาน สามารถเป็นศูนย์กลางให้บริการประชาชน และให้บริการข้อมูลระบบสารสนเทศของหน่วยงานสังกัด รองรับระบบสุขภาพ Health Data Center (HDC) และยังเพิ่มประสิทธิภาพในการสำรองข้อมูลและกู้คืนข้อมูล พร้อมรองรับการทำงานของผู้ใช้งานในทุกๆ ด้านไม่ว่าจะเป็นระบบเครือข่าย การจัดเก็บข้อมูล การทดสอบระบบหรือติดตั้งฐานข้อมูล หรือการใช้งานซอฟต์แวร์เฉพาะด้านในการปฏิบัติงานด้านต่างๆ โดยที่ผู้ใช้งานไม่ต้องติดตั้งระบบทั้งฮาร์ดแวร์และซอฟต์แวร์ไว้ที่สำนักงานให้ยุ่งยาก แต่สามารถใช้งานในสิ่งที่ต้องการได้ด้วยการเชื่อมต่อกับระบบ Cloud Computing ผ่านอินเทอร์เน็ต ในการเชื่อมต่อกับระบบหรือการใช้งานผ่าน Cloud เป็นการเชื่อมต่อกับศูนย์ข้อมูลคอมพิวเตอร์หรือ Data Center ของกรมนามัย ซึ่งศูนย์ข้อมูล (ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย กรมนามัย) อยู่ภายใต้ระบบที่มีมาตรฐานและความปลอดภัยสูง ไม่เพียงเท่านั้น สามารถเชื่อมต่อและใช้งานระบบได้ผ่านอินเทอร์เน็ตทำให้การทำงานไม่ถูกจำกัดอยู่ในสถานที่หนึ่ง แต่สามารถทำงานได้ทุกที่ทุกเวลาผ่านอุปกรณ์ต่างๆ

ตารางที่ ๑๔ ประเด็นเทียบเคียงและผลการดำเนินงานของหน่วยงาน/ประเทศเทียบเคียง

ลำดับ	ประเด็นเทียบเคียง	ผลการดำเนินงานเทียบเคียง	
		ศูนย์เทคโนโลยีสารสนเทศ กระทรวงสาธารณสุข	กรมอนามัย กระทรวงสาธารณสุข
การขอใช้บริการของแต่ละเครื่อง			
๑	ขนาดความจุ) Hard disk)	๑๐ GB	๒๐๐ GB
๒	ขนาดหน่วยความจำหลัก (RAM)	๔ GB	๔ GB
๓	จำนวน Core CPU	๒ Core	๔ Core
การบริการระบบจัดเก็บไฟล์ข้อมูล (File Server)			
๕	พื้นที่การให้บริการ	-	๒ GB
การให้บริการสำรองข้อมูล			
๖	ลักษณะการสำรองข้อมูล*	Manual	Automatic

หมายเหตุ : ลักษณะการสำรองข้อมูล*

- Manual คือ การทำงานโดยผู้ดูแลระบบเป็นผู้ดำเนินการเอง
- Automatic คือ การทำงานโดยใช้ชุดโปรแกรมในการควบคุมการทำงาน ลดภาระงานของผู้ดูแลระบบ

๔.๒ ปรับปรุงระบบเครือข่ายคอมพิวเตอร์กรมอนามัย

กรมอนามัยได้ดำเนินการปรับปรุงสายสัญญาณระบบเครือข่ายคอมพิวเตอร์เนื่องจาก สายสัญญาณ ที่ใช้งานอยู่ในปัจจุบันเริ่มชำรุดเสียหายและมีการใช้งานเพิ่มขึ้น จึงจำเป็นต้องเพิ่มจุดให้บริการครอบคลุมพื้นที่ ปฏิบัติงานของอาคารกรมอนามัย และเพื่อพัฒนาระบบบริการเครือข่ายไร้สายครอบคลุมพื้นที่ปฏิบัติงานของ อาคารกรมอนามัย อีกทั้งยังรองรับการเชื่อมโยงระบบเครือข่ายความเร็วสูง 10 GB ของกระทรวงสาธารณสุข ในปีงบประมาณ ๒๕๖๓

ตารางที่ ๑๕ ประเด็นเทียบเคียงและผลการดำเนินงานของหน่วยงาน/ประเทศเทียบเคียง

ลำดับ	ประเด็นเทียบเคียง	ผลการดำเนินงานเทียบเคียง	
		ศูนย์เทคโนโลยีสารสนเทศ กระทรวงสาธารณสุข	กรมอนามัย
โครงสร้างระบบเครือข่ายคอมพิวเตอร์			
๑	ความเร็วในการรับ-ส่งข้อมูลเส้นทางเครือข่ายหลัก (Backbone)	๑ Gbps	๑๐ Gbps
๒	ชนิดสายสัญญาณ (LAN)	CAT ๕E	CAT ๖
๓	ชนิดสายสัญญาณอุปกรณ์กระจายสัญญาณ Core Switch	Fiber	Fiber
๔	ชนิดสายสัญญาณอุปกรณ์กระจายสัญญาณ Access Switch	UTP	UTP
๕	ชนิดสายสัญญาณอุปกรณ์กระจายสัญญาณ Distribution Switch*	UTP	Fiber

หมายเหตุ : สายสัญญาณแบบ Fiber มีความเร็วในการรับส่งข้อมูลมากกว่า สายสัญญาณแบบUTP

๕. บทสรุป

จาก ๘ ด้านพบว่าสถานภาพปัจจุบันยังมีการใช้งานและรองรับการทำงานในอนาคตพอสมควร แต่ก็ยังคงต้องไปวิเคราะห์กับเป้าหมายของกรมอนามัยที่ได้กำหนดขึ้น ที่จะขับเคลื่อนไปยัง (กรมอนามัย ๔.๐ เพื่อคนไทย ๔.๐) โดยมีเป้าหมายเพื่อคนไทยมีความรอบรู้ด้านสุขภาพสามารถ เข้าถึง เข้าใจ เรียนรู้ ข้อมูลและความรู้ด้านสุขภาพที่ถูกต้อง ตัดสินใจ นำไปใช้ปรับเปลี่ยนพฤติกรรมสุขภาพได้อย่างเหมาะสมตามบริบทของตนเองและสามารถบอกต่อผู้อื่นได้ และได้มีการจัดประชุมในการวางแผน Road Map เพื่อให้คนไทยมีอายุคาดเฉลี่ยของการมีสุขภาพดีที่ ๗๒ ปี ในระยะ ๒๐ ปี โดยได้มีการแบ่งเป้าประสงค์ออกเป็น ๔ ช่วง เพื่อที่จะได้มีการพัฒนาโครงสร้างพื้นฐานและระบบสารสนเทศของกรมอนามัยทั้งส่วนกลางและส่วนภูมิภาคในศูนย์ต่าง ๆ ทางด้านเป้าหมายเชิงเทคนิคและข้อจำกัด ซึ่งจะเป็หัวข้อในการวิเคราะห์ความต้องการดังนี้

๑. การรองรับการขยายตัวในอนาคต (Scalability) โดยมีข้อเสนอแนะ ควรที่จะมีการกำหนดรูปแบบการเชื่อมต่อเครือข่ายภายในของศูนย์ต่าง ๆ ให้เป็นไปในรูปแบบเดียวกัน โดยมีส่วนกลางเป็นผู้ช่วยในการดูแลและพัฒนาระบบเครือข่ายของศูนย์ต่าง ๆ เพื่อที่จะทำให้เกิดการรองรับการขยายตัวของระบบเครือข่ายไปในแนวทางเดียวกันของทุกศูนย์
๒. การทำงานอย่างต่อเนื่องไม่หยุดชะงัก (Availability) โดยมีข้อเสนอแนะ ควรที่จะต้องทำการสำรองระบบสารสนเทศของแต่ละศูนย์ฯ ไว้ที่กรมอนามัย ซึ่งจะทำหน้าที่เป็น ศูนย์ข้อมูลและระบบงานสำรอง (DR Site) เพื่อที่รองรับการทำงานของระบบงานและข้อมูลของศูนย์ต่าง ๆ ได้ตลอด ๒๔ ชม. โดยควรที่จะวางแผนงานในการจัดตั้งศูนย์สำรองระบบงานและข้อมูล กับกรมอนามัยในส่วนกลางในรูปแบบระดับ Warm Site
๓. การส่งข้อมูลอย่างรวดเร็ว (Performance) โดยมีข้อเสนอแนะ
 - ในเรื่องการรับส่งข้อมูลในระบบเครือข่ายที่ไม่ราบรื่นในการรับส่งข้อมูลภายในเครือข่ายกรมอนามัย กล่าวคือเมื่อมีการใช้งานระบบสาย LAN ที่มีหัวในการเชื่อมต่อจะอุปกรณ์ patch panel ที่เชื่อมสายแลนเกิดความเสื่อมสภาพ ในการใช้งาน โดยปกติ patch panel ในการเชื่อมต่อจะมีอายุการใช้งานประมาณ ๑๔ ปี ในสถานะการใช้งานทั่วไป จึงต้องมีการซ่อมบำรุงโดยการเข้าโดยการทำความสะอาดและเข้าสายแลนใหม่ เพื่อให้พร้อมในการใช้งาน
 - ควรที่จะมีการจำกัดปริมาณ Bandwidth ที่มีการใช้งาน ซึ่งโดยปกติในการใช้งานทั่วไป ปริมาณ Bandwidth ที่มีการใช้งานกันอย่างราบรื่นในการรับส่งข้อมูลควรอยู่ที่ ๔ – ๕ Mbps โดยในปริมาณ Bandwidth ดังกล่าวจะสามารถใช้งาน Application แบบ video streaming ได้ที่ ๗๒๐p เป็นต้น
๔. ความปลอดภัยของข้อมูล (Security) โดยมีข้อเสนอแนะ
 - จัดทำโครงการตรวจสอบระบบความปลอดภัยของระบบสารสนเทศและการสื่อสารของกรมอนามัย (penetration test) ในส่วนของระบบงานการให้บริการหรือระบบงานที่ต้องการทำการเผยแพร่ข้อมูลของศูนย์ต่าง ๆ ของกรมอนามัย และโครงการเสริมสร้างความแข็งแกร่งของระบบสารสนเทศและการสื่อสาร (Hardening System) เพื่อช่วยการป้องกันการโจมตีจากผู้ที่ไม่ประสงค์ดีได้อย่างมีประสิทธิภาพ

- การให้ความรู้ทางด้านความมั่นคงปลอดภัย ควรจะมีการอบรมด้านระบบความปลอดภัยขั้นพื้นฐานในการใช้งานระบบเครือข่ายอินเทอร์เน็ต เพื่อให้เจ้าหน้าที่ได้มีความตระหนักถึงการป้องกันตัวเองและองค์กรต่อการโจมตีของผู้บุกรุกในรูปแบบต่าง ๆ บนระบบเครือข่ายอินเทอร์เน็ต เป็นประจำทุกปี
 - ๕. การบริหารจัดการ (Manageability) โดยมีข้อเสนอแนะ ควรจะมีการจัดอบรมในเรื่องระบบเครือข่ายขั้นพื้นฐานในการดูแลระบบเครือข่ายไม่ว่าจะเป็นระบบแลน หรือระบบเครือข่ายไร้สายให้แก่เจ้าหน้าที่ของศูนย์ ฯ ของกรมอนามัยเพื่อที่จะสามารถและดูแลระบบเครือข่ายเบื้องต้นได้อย่างมีประสิทธิภาพ
 - ๖. การใช้งานง่ายและสะดวก (Usability) โดยมีข้อเสนอแนะ ควรจะมีการแจ้งข่าวสารผ่านทางระบบอีเมล หรือ ช่องที่เป็นประชาสัมพันธ์ของกรมอนามัยเพื่อที่จะทำให้เจ้าหน้าที่ผู้ใช้งานในระบบสารสนเทศและการสื่อสารได้รับข่าวสารอย่างทั่วถึง
 - ๗. การรองรับการเปลี่ยนแปลงในอนาคต (Adaptability) โดยมีข้อเสนอแนะ ในการรองรับการเปลี่ยนแปลงที่จะก้าวไปสู่นิยามที่ว่า “กรมอนามัย 4.0” นั้นจะต้องมีการรองรับการเพิ่มขึ้นของปริมาณข้อมูลที่มีใช้งานในระบบสารสนเทศและการสื่อสารจึงควรที่จะมี โครงการจัดทำการบูรณาการข้อมูลรองรับกรมอนามัย 4.0 บนระบบการประมวลผลแบบกลุ่มเมฆ (Cloud computing system)
 - ๘. ต้นทุนค่าใช้จ่ายที่เหมาะสม (Affordability) โดยมีข้อเสนอแนะ ควรจะมีการรวมกันระหว่างศูนย์ต่าง ๆ กับทางส่วนกลางในการวางแผนการเชื่อมต่อระบบเครือข่ายภายในของศูนย์ต่าง ๆ กับระบบอินเทอร์เน็ตที่มีการใช้งบประมาณในการลงทุนที่ไม่ซับซ้อนกัน หรืออาจจะจัดทำโครงการการเชื่อมต่อระบบอินเทอร์เน็ตของศูนย์ต่าง ๆ ภายในกรมอนามัย
- โดยได้ทำการนำเอาผลจากการศึกษาและวิเคราะห์มาทำการออกแบบทั้ง Logical Design และ Physical Design ของกรมอนามัย รวมทั้งโดยมีการระบุ คุณลักษณะ (Specification) ของอุปกรณ์ที่ใช้ในเครือข่ายเพื่อนำไปใช้เป็นข้อมูลในการจัดหาอุปกรณ์ เพิ่มเติมสำหรับเครือข่ายของกรมอนามัยต่อไป รวมไปถึงองค์ความรู้ที่จำเป็นต่อบุคลากรของกรมอนามัย