แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๕

การบริหารจัดการความเสี่ยงด้านสารสนเทศ
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

หลักการและเหตุผล

การนำกระบวนการบริหารความเสี่ยงมาใช้ภายในองค์กร โดยอาศัยหลักการพื้นฐานของการกำกับดูแลกิจการขององค์กรที่ดี (Good Governance) เพื่อให้ผู้มีส่วนได้เสียขององค์กรสามารถเชื่อมั่นอย่างสมเหตุสมผลว่าการดำเนินงานเชิงกลยุทธ์ของงานด้านเทคโนโลยีสารสนเทศ มุ่งไปสู่การบรรลุวัตถุประสงค์และเป้าหมายขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล ดังนั้นการพัฒนากระบวนการบริหารความเสี่ยงทั่วทั้งองค์กรทุกระดับ รวมทั้งรณรงค์ให้ผู้บริหารละบุคลากรทุกคนตระหนักและเข้าใจถึงความสำคัญของการบริหารความเสี่ยง

กรมสนับสนุนบริการสุขภาพ เป็นหน่วยงานที่มีหน้าที่กำกับ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) ด้านระบบบริการสุขภาพ ที่ส่งผลกระทบต่อประชาชนโดยตรง (Impact Security Risk และ Economics Public Health) จากการเชื่อมโยงข้อมูลด้านระบบบริหารสุขภาพ (Interconnected Information System) และหน่วยงานที่เกี่ยวข้องควรต้องผ่านเกณฑ์มาตราฐาน เพื่อให้ประชาชนมีความปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม ได้จัดทำ “แผนบริหารความเสี่ยงด้านสารสนเทศ” ตามแนวทางการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศด้วยมาตรฐานการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑:๒๐๑๓ ในข้อกำหนดที่ ๗ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) และตามแนวทางการพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวดที่ ๒ การวางแผนเชิงยุทธศาสตร์ SP ๗ ที่กำหนดให้ส่วนราชการต้องมีการวิเคราะห์และจัดทำแผนบริหารความเสี่ยงตามมาตรฐาน COSO (The Committee of Sponsoring Organizations of the Tread way Commission) ให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพและมีประสิทธิผลขององค์กร สามารถนำไปปฏิบัติได้อย่างมีประสิทธิผลและต่อเนื่องจนเป็นวัฒนธรรมขององค์กร

ความหมายของการบริหารความเสี่ยง

การบริหารความเสี่ยง คือ กระบวนการที่เป็นระบบในการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินการต่างๆ เพื่อลดมูลเหตุของโอกาส ที่จะทำให้เกิดความสียหายจากการดำเนินการที่ไม่เป็นไปตามแผน เพื่อให้ระดับความเสี่ยงและผลกระทบที่เกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ ควบคุมได้และตรวจสอบได้อย่างเป็นระบบ

ความเสี่ยง คือ เหตุการณ์/การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาส ที่จะบรรลุเป้าหมายของแผนงาน/โครงการที่สำคัญในแต่ละประเด็นยุทธศาสตร์ตามที่ระบุในแผนปฏิบัติราชการประจำปีของส่วนราชการ เพื่อนำไปใช้เป็นเครื่องมือในการดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และเกิดประโยชน์สูงสุดแก่องค์กร

๑. วัตถุประสงค์

๑.๑ เพื่อให้ผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ มีความรู้ความเข้าใจเรื่องการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ

๑.๒ เพื่อให้ผู้บริหารและบุคลากรได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นได้และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้อง

๑.๓ เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๑.๔ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับกลยุทธ์ความต่อเนื่องด้านเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ

๑.๕ เพื่อเป็นเครื่องมือในการปลูกฝังและสร้างวัฒนธรรมการบริหารความเสี่ยงในทุกระดับของกรมสนับสนุนบริการสุขภาพ

๒. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

สถานภาพปัจจุบันด้านระบบเทคโนโลยีสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ แบ่งได้เป็น ๓ ด้าน ประกอบด้วย (๑) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (๒) ระบบสารสนเทศและฐานข้อมูล (๓) บุคลากรด้านเทคโนโลยีสารสนเทศ

๒.๑ โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

เครื่องคอมพิวเตอร์แม่ข่าย (Server)

สามารถจำแนกตามลักษณะทางกายภาพได้ ๓ ประเภท ได้แก่

(๑) Rack Server จำนวน ๔๓ เครื่อง

(๒) Tower จำนวน ๔ เครื่อง

(๓) Blade Server จำนวน ๑๔ เครื่อง

นอกจากเครื่องแม่ข่ายจริงแล้ว กลุ่มเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ยังมีการนำระบบคอมพิวเตอร์แม่ข่ายเสมือน (Server Virtualization System) มาจัดสรรทรัพยากรให้ระบบสารสนเทศที่ทำงานบนระบบปฏิบัติการเดียวกัน เป็นการใช้ทรัพยากรร่วมกันได้อย่างเต็มประสิทธิภาพ ประหยัดพลังงานและลดพื้นที่ในการใช้งานห้องศูนย์ข้อมูล Data Center ในส่วนของระบบปฏิบัติการ (OS) ของระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ ได้แก่

(๑) Unix/Linux จำนวน ๙๙ เครื่อง

(๒) Windows Server จำนวน ๑๕ เครื่อง

เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของกรมสนับสนุนบริการสุขภาพ พบว่ามี เครื่องคอมพิวเตอร์ตั้งโต๊ะ(PC) และคอมพิวเตอร์พกพา(Notebook) จำนวน ๑,๓๐๐ เครื่อง เครื่องพิมพ์ จำนวน ๒๐๐ เครื่อง และเครื่องสแกนเนอร์ จำนวน ๔๐ เครื่อง โดยประมาณ

ระบบเครือข่าย (Network)

กรมสนับสนุนบริการสุขภาพ ได้ดำเนินการเชื่อมต่อระบบเครือข่าย (Network) ให้บริการแก่บุคลากรผู้ปฏิบัติงานทุกระดับ ร่วมถึงประชาชนทั่วไป และเพื่อรองรับการจัดการระบบข้อมูลสารสนเทศจากหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ทั้งส่วนกลางและส่วนภูมิภาค ที่ความเร็วในการ รับ-ส่งข้อมูลภายในประเทศ (Domestic Bandwidth) ความเร็วไม่น้อยกว่า ๒๐๐ Mbps และภายนอกประเทศ (International Bandwidth) ความเร็วไม่น้อยกว่า ๑๐๐ Mbps โดยมีบริการระบบเครือข่าย Internet ทั้งแบบมีสายและแบบไร้สาย เพื่อเชื่อมโยงข้อมูลให้บริการระบบงานสารสนเทศ พร้อมระบบตรวจจับและยับยั้งการโจมตีจากภัยคุกคามต่างๆ เช่น Virus, Malware รวมถึงควบคุมการเข้าถึงระบบสารสนเทศ และระบบฐานข้อมูลตามนโยบายด้านความมั่นคงปลอดภัย

ระบบ VDO Conference และศูนย์ข้อมูล DOC

กรมสนับสนุนบริการสุขภาพจัดทำห้องบัญชาการ (War Room) ที่สามารถแสดงผลการปฏิบัติงานให้ได้อย่างมีประสิทธิภาพ มีเทคโนโลยีที่ทันสมัย สามารถเชื่อมต่อประชุมทางไกลกับหน่วยงานให้บริการในส่วนภูมิภาค ลดภาระค่าใช้จ่ายในการเดินทางมาประชุม และสามารถติดตามงานได้อย่างทันท่วงที รวมถึงใช้เป็นที่บัญชาการในสถานการณ์ฉุกเฉิน สำหรับการใช้ข้อมูลประกอบการตัดสินใจของผู้บริหารระดับสูง เพื่อตอบสนองการติดตามสถานการณ์ปัจจุบันและข่าวสารอื่นๆ รวมถึงจัดทำระบบศูนย์ข้อมูล DOC ที่ผู้เข้าร่วมประชุมสามารถ Download เอกสารการประชุมมาใช้ ผ่าน Application ที่จัดทำเป็นการลดภาระค่าใช้จ่ายในการจัดเตรียมเอกสารประชุมการประชุมให้แก่ผู้เข้าร่วมประชุม

ระบบสารสนเทศและฐานข้อมูล

กรมสนับสนุนบริการสุขภาพ ได้มีการจัดจ้างพัฒนาและปรับปรุงระบบสารสนเทศต่างๆ เพื่อสนับสนุนการปฏิบัติงานขององค์กรและอำนวยความสะดวกให้แก่ผู้รับบริการ เมื่อระบบสารสนเทศมีจำนวนเพิ่มขึ้น ทำให้พบว่าข้อมูลมีความซ้ำซ้อนและขาดการบูรณาการ เนื่องจากบางระบบพัฒนาขึ้นแบบเร่งด่วนเพื่อใช้งานเฉพาะกิจตามช่วงเวลานั้นๆ และขาดการบำรุงรักษาอย่างต่อเนื่องทำให้การใช้งานโปรแกรมเกิดขัดข้องและไม่สะดวก แก่ผู้ใช้งาน โดยกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม มีหน้าที่ในการดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ จำเป็นต้องมีการปรับปรุงระบบสารสนเทศและวางแนวทางการเชื่อมโยงระบบสารสนเทศอย่างต่อเนื่องให้สอดคล้องกับการเปลี่ยนแปลงที่จะเกิดขึ้นในปัจจุบันและอนาคต โดย ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการภายในกรมสนับสนุนบริการสุขภาพ มีทั้งหมด ๑๑๘ ระบบ (รายละเอียดตามภาคผนวก)

๒.๒ บุคลากรด้านเทคโนโลยีสารสนเทศ

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม มีอัตรากำลังบุคลากรในตำแหน่งนักวิชาการคอมพิวเตอร์ที่ปฏิบัติงานอยู่ทั้งหมดจำนวน ๗ คน และมีอัตรากำลังบุคลากรในตำแหน่งนักวิชาการคอมพิวเตอร์ ที่ปฏิบัติงานอยู่ภายใต้หน่วยงานอื่นๆ และหน่วยงานส่วนภูมิภาค ของกรมสนับสนุนบริการสุขภาพ จำนวน ๑๓ คน ซึ่งปัจจุบันได้มีคำสั่ง กรมสนับสนุนบริการสุขภาพ ที่ ๒๕๗/๒๕๖๔ ลงวันที่ ๘ กุมภาพันธ์ ๒๕๖๔ เรื่องให้ข้าราชการปฏิบัติหน้าที่ราชการ (อีกหน้าที่หนึ่ง) ในตำแหน่งนักวิชาการคอมพิวเตอร์ จำนวน ๑๓ คน เพื่อสนับสนุนการดำเนินงานต่างๆ ของกลุ่มเทคโนโลยีสารสนเทศ ซึ่งบุคลากรในตำแหน่งนักวิชาการคอมพิวเตอร์ ต้องมีความรู้ความสามารถและทักษะในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อรองรับภารกิจต่างๆ ของกรมสนับสนุนบริการสุขภาพและตอบสนองความต้องการของผู้รับบริการได้อย่างครบถ้วน

๓. นโยบายการบริหารความเสี่ยง

กรมสนับสนุนบริการสุขภาพ มีดำเนินการบริหารความเสี่ยงด้านสารสนเทศ โดยการบริหารปัจจัยเสี่ยงและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อลดมูลเหตุของแต่ละโอกาสที่จะเกิดความเสียหาย ซึ่งกำหนดให้ระดับความเสี่ยงและขนาดของความเสี่ยงที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงการบรรลุเป้าหมาย ตามยุทธศาสตร์ที่สำคัญ จึงกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศดังนี้

๓.๑ จัดให้มีระบบและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมีเอกสารกำหนดแนวทางและระบุปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓.๒ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องครอบคลุมทุกหน่วยงานภายในสังกัดกรมสนับสนุนบริการสุขภาพ โดยรวบรวมสาเหตุความเสี่ยงที่มีทั้งปัจจัยภายในและปัจจัยภายนอก เพื่อช่วยให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพและมีประสิทธิผล

๓.๓ ทุกหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ รวมทั้งผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เข้าใจและให้ความสำคัญกับการบ่งชี้และการควบคุมความเสี่ยง มีวิธีการ และแนวทางการปฏิบัติงานที่เป็นแนวทางเดียวกัน ในการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศสารสนเทศ

๓.๔ กำหนดกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นมาตรฐานเดียวกันทั้งองค์กร

๓.๕ การบริการจัดการข้อมูลที่ดี (Data Governance) ตามนโยบายรัฐบาลดิจิทัล (Digital Government)

๓.๖ ส่งเสริมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศสู่การปฏิบัติ โดยกำหนดให้เป็นส่วนหนึ่งในภารกิจ เพื่อให้หน่วยงานภายในสังกัดกรมสนับสนุนบริการสุขภาพ ยึดถือปฏิบัติเป็นวัฒนธรรมองค์กร

๓.๗ ติดตามและประเมินผลการบริหารความเสี่ยง รวมถึงทบทวนและปรับปรุงการบริหารความเสี่ยงอย่างสม่ำเสมอ

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๑ ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาสเป็นผลทำให้กรมสนับสนุนบริการสุขภาพ ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อองค์กร โดยเฉพาะอย่างยิ่งระบบที่ให้บริการสำหรับประชาชน และระบบเทคโนโลยีสารสนเทศที่ใช้ในการบริหารจัดการและปฏิบัติงานต่างๆ ที่สำคัญของกรมสนับสนุนบริการสุขภาพ

๔.๒ การควบคุม (Control) หมายถึง กระบวนการดำเนินงาน ขั้นตอนการปฏิบัติงานหรือกลไกการปฏิบัติงาน ซึ่งกรมสนับสนุนบริการสุขภาพ กำหนดขึ้นเพื่อให้มั่นใจว่าการบริหารงานจะสามารถบรรลุวัตถุประสงค์ที่ได้ตามที่กำหนดไว้

๔.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ จัดการ ติดตามและประเมินความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหรือกระบวนการดำเนินงานของกรมสนับสนุนบริการสุขภาพ รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้

๔.๔ การบริหารความเสี่ยงขององค์กรโดยรวม (Enterprise Wide Risk Management) หมายถึง การบริหารความเสี่ยงโดยมี โครงสร้างองค์กร กระบวนการ และวัฒนธรรมองค์กร รวมเข้าด้วยกันและมีลักษณะสำคัญดังนี้

๔.๔.๑ ผสมผสานและเป็นส่วนหนึ่งขององค์กร เพราะเป็นกลไกส่วนหนึ่งของการขับเคลื่อนไปสู่การกำกับดูแลกิจการที่ดี เพื่อบรรลุวัตถุประสงค์ที่กำหนดไว้

๔.๔.๒ การบริหารความเสี่ยงควรสอดคล้องกับแผนการดำเนินงานต่างๆ ขององค์กร เพื่อบรรลุวัตถุประสงค์ มีการตัดสินใจ และสามารถนำไปใช้กับองค์ประกอบอื่นๆ ในการบริหารขององค์กรได้เป็นอย่างดี

๔.๔.๓ พิจารณาความเสี่ยงทั้งหมด โดยครอบคลุมความเสี่ยงทั้งองค์กร ไม่ว่าจะเป็นความเสี่ยงเกี่ยวกับกลยุทธ์ การดำเนินงาน การปฏิบัติตามกฎระเบียบ และการเงิน ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหาย ความไม่แน่นอน การเสียโอกาส และการมีผลกระทบต่อวัตถุประสงค์ที่กำหนดไว้

๔.๔.๔ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ระบบเครือข่ายคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์ ระบบเครื่องสื่อสาร ระบบฐานข้อมูล และอุปกรณ์ประกอบระบบต่างๆ รวมทั้งอาคารสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด

๔.๕ ฐานข้อมูลสารสนเทศ หมายถึง ฐานข้อมูลที่กรมสนับสนุนบริการสุขภาพใช้ในการปฏิบัติหน้าที่ซึ่งประกอบด้วย

๔.๕.๑ ฐานข้อมูลเพื่อการบริการประชาชนทั่วไป

๔.๕.๒ ฐานข้อมูลเพื่อการบริหารงานภายในองค์กร

๔.๖ องค์ประกอบของความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔.๖.๑ ความน่าจะเป็น โอกาส หรือความไม่แน่นอน

๔.๖.๒ ผู้กระทำ (อาจเป็นได้ทั้งสิ่งมีชีวิต และไม่มีชีวิต เช่น อุบัติเหตุต่างๆ)

๔.๖.๓ การกระทำ (ถ้าผู้กระทำเป็นสิ่งมีชีวิตจะเป็นการกระทำ ถ้าผู้กระทำไม่มีชีวิต ส่วนนี้จะเป็นการเกิดของเหตุการณ์)

๔.๖.๔ ช่องทางที่มีในการเข้าถึงข้อมูล

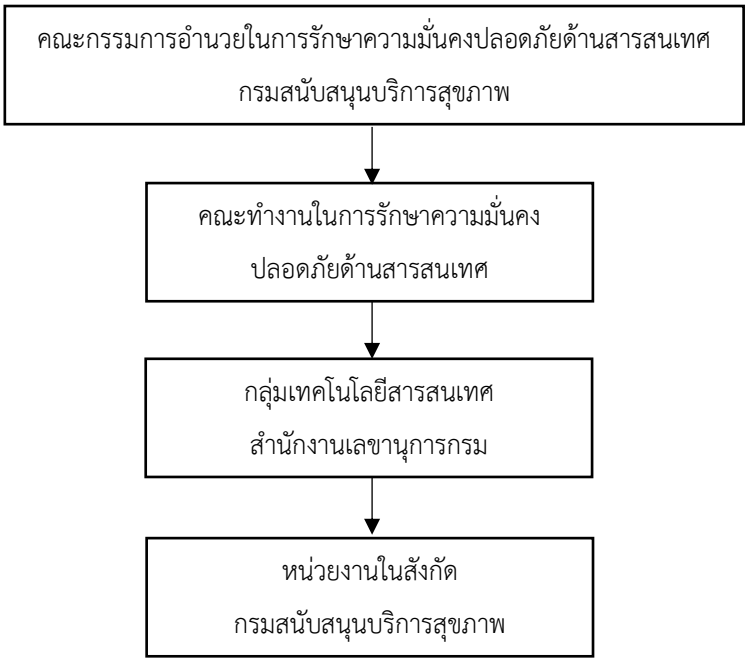
๔.๖.๕ ผลกระทบกับวัตถุประสงค์ ภารกิจ สถานะ หรือความสำเร็จขององค์กร

๕. โครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ตามคำสั่งกรมสนับสนุนบริการสุขภาพที่ ๒๘๔๐/๒๕๖๔ เรื่องแต่งตั้งคณะกรรมการอำนวยและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ลงวันที่ ๑๙ พฤศจิกายน ๒๕๖๔ โดยมีอำนาจหน้าที่ในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

๑. ถ่ายทอดแนวทางปฏิบัติ รณรงค์ และกระตุ้นเตือนให้บุคลากรในหน่วยงาน มีความรู้ความเข้าใจ และแนวปฏิบัติตามกฎ ระเบียบด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งคัด

๒. ดำเนินการสนับสนุนให้หน่วยงานในสังกัด มีระบบฐานข้อมูลที่สนับสนุนการปฏิบัติงานตามภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ และระบบเครือข่ายคอมพิวเตอร์ของกรมสนับสนุนบริการสุขภาพมีความมั่นคงปลอดภัยปลอดภัย



บทที่ ๒ การบริหารความเสี่ยง

ขั้นที่ ๑ การเตรียมการและวางแผน

๑.๑ กำหนดความเสี่ยงที่มีโอกาสเกิดขึ้นต่อวัตถุประสงค์ ภารกิจ ความสำเร็จ

กรมสนับสนุนบริการสุขภาพ เป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุขที่ให้บริการด้านระบบบริการสุขภาพให้กับประชาชน โดยกรมสนับสนุนบริการสุขภาพได้จัดทำและพัฒนาระบบเทคโนโลยีสารสนเทศขึ้นเพื่ออำนวยความสะดวกในการใช้บริการของประชาชน ซึ่งระบบเทคโนโลยีสารสนเทศและการสื่อสารเหล่านั้น เป็นปัจจัยสำคัญที่จะช่วยสนับสนุนภารกิจของกรมสนับสนุนบริการสุขภาพ ให้สำเร็จตามเป้าหมายได้อย่างมีประสิทธิภาพ จำเป็นต้องดำเนินการบริหารจัดการความเสี่ยงเพื่อปกป้องข้อมูลของประชาชนที่ใช้บริการระบบสารสนเทศและการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งรวมถึงข้อมูลต่างๆ ที่เชื่อมโยงกับหน่วยงานภาครัฐอื่นๆ ให้มีมั่นคงปลอดภัยพร้อมทั้งเสริมสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการ ดังนั้นกรมสนับสนุนบริการสุขภาพจำเป็นต้องมีความมั่นคงปลอดภัยทางสารสนเทศในระดับสูงเพื่อคุ้มครองข้อมูลของประชาชนและประโยชน์ที่สำคัญของประเทศ

วัตถุประสงค์ ภารกิจ ความสำเร็จ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	**ความเสียหายที่ยอมรับได้**
๑. พัฒนาการเชื่อมโยงเครือข่ายระบบสาธารณสุข	การเชื่อมโยงเครือข่ายระหว่างกรมไม่สามารถดำเนินการได้ ๑ กรม
๒. ให้ความสำคัญกับระบบความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร	ระยะเวลา Downtime ของระบบเครือข่ายไม่เกินร้อยละ ๕ ของเวลาทั้งปี (นาที)
๓. ความมีประสิทธิภาพของระบบเทคโนโลยีสารสนเทศหรือระบบงานและข้อมูล	ร้อยละไม่ต่ำกว่า ๕๐ ของหน่วยงานระดับจังหวัดใช้ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ได้พัฒนาขึ้น
๔. ผู้ใช้บริการมีความพึงพอใจต่อบริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร	ร้อยละของระดับความพึงพอใจของผู้ใช้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ลดลงจากเดิมไม่เกิน ๒๐ %

สถานะ ชื่อเสียงขององค์กร	ความเสียหายที่ยอมรับได้
๑. ความเชื่อมั่นของประชาชนผู้ใช้บริการ	๑. จำนวนผู้ใช้บริการระบบเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ ไม่เพิ่มขึ้นจากเดิม แต่ไม่ลดลงจากเดิม ๒. ผู้บริหารเรียกให้ชี้แจงข้อมูล
๒. ความเชื่อมั่นต่อบริการด้านเทคโนโลยีและการสื่อสารของหน่วยงานภายนอกกรมฯ	๑. การส่งรายงานของระบบรายงานต่าง ๆ จากหน่วยงานภายนอกกรมฯ จากเดิมไม่เกิน ๒๐ % ๒. หน่วยงานภายนอกกรมฯ มีความคลางแคลงใจ โดยการสอบถามข้อมูลผ่านโทรศัพท์หรือทางอีเมล์หรือแอปพลิเคชั่น เป็นจำนวนมาก
๓. ความเชื่อมั่นต่อบริการด้านเทคโนโลยีและการสื่อสารของหน่วยงานในสังกัดกรมฯ	๑. หน่วยงานในสังกัดกรมฯ สอบถามข้อเท็จจริงที่เกิดขึ้น แต่ยังใช้บริการอยู่เช่นเดิม

๑.๒ วิเคราะห์ปัญหาหรือโอกาสในองค์กรโอกาสหรือสิ่งที่จะมีส่วนช่วยให้ระบวนการบริหารความเสี่ยงประสบผลสำเร็จ

ปัจจัยแห่งความสำเร็จ เพื่อให้การดำเนินการตามกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร กรมสนับสนุนบริการสุขภาพ บรรลุผลตามเป้าหมาย สามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม ได้แก่

๑. ปัจจัยด้านอุปกรณ์ (Hardware)

(๑) พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อสนับสนุนการพัฒนาระบบบริการสุขภาพ

(๒) เครื่องมือในการเก็บรวบรวมข้อมูลที่มีประสิทธิภาพ สามารถเก็บรวบรวมข้อมูลได้ครบถ้วน มีคุณภาพ ตอบสนองความต้องการในการให้บริการสาธารณสุข และด้านบริหารจัดการของผู้บริหาร

๒. ปัจจัยด้านซอฟต์แวร์ (Software)

(๑) ส่งเสริมและพัฒนา นวัตกรรมบริการ การจัดการระบบ เครื่องมือพร้อมอุปกรณ์เพื่อเพิ่มประสิทธิภาพระบบบริการสุขภาพ

(๒) ประยุกต์ใช้เทคโนโลยีในกระบวนการบริหารจัดการและการให้บริการ

(๓) พัฒนาระบบเทคโนโลยีสารสนเทศการจัดการความรู้ด้านการสนับสนุนบริการสุขภาพสำหรับประชาชน

(๔) พัฒนามาตรฐานในด้านการเชื่อมโยงแลกเปลี่ยนข้อมูล

๓. ปัจจัยด้านโครงข่ายเทคโนโลยีสารสนเทศ (Network)

(๑) หน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ทุกหน่วยงานสามารถเข้าถึงบริการอินเทอร์เน็ตความเร็วสูงหรือการสื่อสารรูปแบบอื่นที่เป็น Broadband ได้อย่างทั่วถึง สะดวกและรวดเร็วโดยปลอดภัย

(๒) ระบบเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพมีความทันสมัย รวดเร็วทันต่อการการเปลี่ยนแปลงของเทคโนโลยีและปรับเปลี่ยนไปตามความต้องการของสังคม ซึ่งสามารถรองรับกับการขยายตัวของการให้บริการได้

(๓) โครงข่ายเทคโนโลยีสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ พัฒนาศักยภาพไปสู่โครงข่ายโทรคมนาคมยุคหน้า (Next Generation Network : NGN) ที่สามารถบูรณาการการใช้งานร่วมกันได้อย่างทั่วถึง

(๔) ใช้เทคโนโลยีการออกแบบสถาปัตยกรรมโปรแกรมระบบงานที่ทันสมัย มีความยืดหยุ่นในการเปลี่ยนแปลง ง่ายต่อการดูแลบำรุงรักษาโดยเจ้าหน้าที่ของหน่วยงาน

๔. ปัจจัยด้านบุคลากร

<u>ผู้บริหารองค์กร</u>

(๑) ผู้บริหารมีวิสัยทัศน์ ให้ความสำคัญ สนับสนุนและส่งเสริมการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการพัฒนาองค์กร รวมทั้งให้ความสำคัญต่อการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

<u>ผู้ใช้งาน</u>

(๑) บุคลากรผู้ใช้งานส่วนใหญ่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศในระดับที่ใช้งานได้ บุคลากรผู้ใช้งานมีความสนใจ และกระตือรือร้นในการใช้เทคโนโลยีสารสนเทศช่วยในการปฏิบัติงาน

(๒) บุคลากรทุกคนสามารถใช้ อีเมล์ , อินเทอร์เน็ต และ อินทราเน็ต ในการประสานงานและ

สืบค้นข้อมูลเพื่อปฏิบัติงานในภารกิจได้อย่างมีประสิทธิภาพ

(๓) บุคลากรทุกคนตระหนักถึงความสำคัญและให้ความร่วมมือในการปฏิบัติตามแผนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

(๑) ผู้ปฏิบัติงานมีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศ

(๒) ผู้ปฏิบัติงานมีความสนใจ และพัฒนาตนเองในการใช้เทคโนโลยีสารสนเทศช่วยในการปฏิบัติงาน

(๓) ผู้ปฏิบัติงานตระหนักถึงความสำคัญและให้ความร่วมมือในการปฏิบัติตามแผนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

๕. ปัจจัยด้านข้อมูลสารสนเทศ

(๑) มีการพัฒนารูปแบบการให้บริการข้อมูลขององค์กรในลักษณะสื่อสองทางและส่งเสริมการมีส่วนร่วมของภาคประชาชน และบุคลากรผ่านระบบอินเทอร์เน็ต

(๒) กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม เป็นหน่วยให้บริการในช่องทางการเข้าถึงข้อมูลสารสนเทศและสามารถรับข้อเสนอแนะ/แก้ไขปัญหาอุปสรรคจากผู้ใช้งาน

๖. ปัจจัยด้านการบริหารจัดการ

(๑) หน่วยงาน/บุคลากร เพื่อเป็นหน่วยสนับสนุนและกำกับดูแลงานด้านเทคโนโลยีสารสนเทศภายในกรมสนับสนุนบริการสุขภาพ ทั้งส่วนกลางและส่วนภูมิภาค

(๒) การแต่งตั้ง คณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ เพื่อทำหน้าที่ บริหารจัดหา ติดตามการทำงาน การจัดการข้อมูล และระบบคอมพิวเตอร์ของกรมสนับสนุนบริการสุขภาพ รวมทั้งควบคุม ตรวจสอบ และประเมินผล การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ ให้เป็นไปอย่างมีประสิทธิภาพและเหมาะสม

(๓) การใช้เทคโนโลยีสารสนเทศทำให้สามารถลดขั้นตอน ระยะเวลา ลดค่าใช้จ่ายที่เกิดขึ้นในการปฏิบัติงาน

๗. ปัจจัยด้านงบประมาณ

(๑) การได้รับสนับสนุนด้านงบประมาณอย่างต่อเนื่อง

- **ปัญหาหรือสิ่งที่จะขัดขวางมิให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ**

๑. กระบวนการบริหารจัดการและบูรณาการทางด้านการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศภายในองค์กร ไม่ได้รับความร่วมมือเท่าที่ควร

๒. การให้ความรู้เรื่องบริหารความเสี่ยงไม่เพียงพอเท่าที่ควร กล่าวคือ บุคลากรในองค์กรทุกคนจะต้องได้รับความรู้เกี่ยวกับการบริหารความเสี่ยง เพื่อให้มีความเข้าใจกรอบการบริหารความเสี่ยงและความรับผิดชอบของแต่ละบุคคลในการจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๓. ชุดข้อมูลไม่สอดคล้องตามวัตถุประสงค์ เนื่องจากมีรายละเอียดของข้อมูลไม่ชัดเจน หรือมีการนำเข้าข้อมูลที่ไม่มีคุณภาพ

๑.๓ กำหนดขอบเขต

ขอบเขตของการบริหารความเสี่ยงกรมสนับสนุนบริการสุขภาพ ที่มีความสำคัญต่อวัตถุประสงค์ภารกิจ สถานะ หรือความสำเร็จ

- หน่วยงานขององค์กรที่จะจัดให้มีกระบวนการบริหารความเสี่ยง

- ทุกหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ

๑.๔ กำหนดบุคลากรในการดำเนินงาน

คณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ตามคำสั่งเลขที่ ๒๘๔๐/๒๕๖๔ ลงวันที่ ๑๙ พฤศจิกายน ๒๕๖๔

๑.๕ การจัดการรายละเอียดด้านกำหนดการ ส่วนสนับสนุนและอำนวยความสะดวกเจ้าหน้าที่ผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยง

เพื่อให้การดำเนินงานตามแผนฯ เป็นไปอย่างรวดเร็วทันต่อการดำเนินการ จึงกำหนดให้ เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการจัดการความเสี่ยงที่เกิดขึ้น และให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ กำกับ ดูแล ควบคุมการดำเนินการจัดการความเสี่ยง

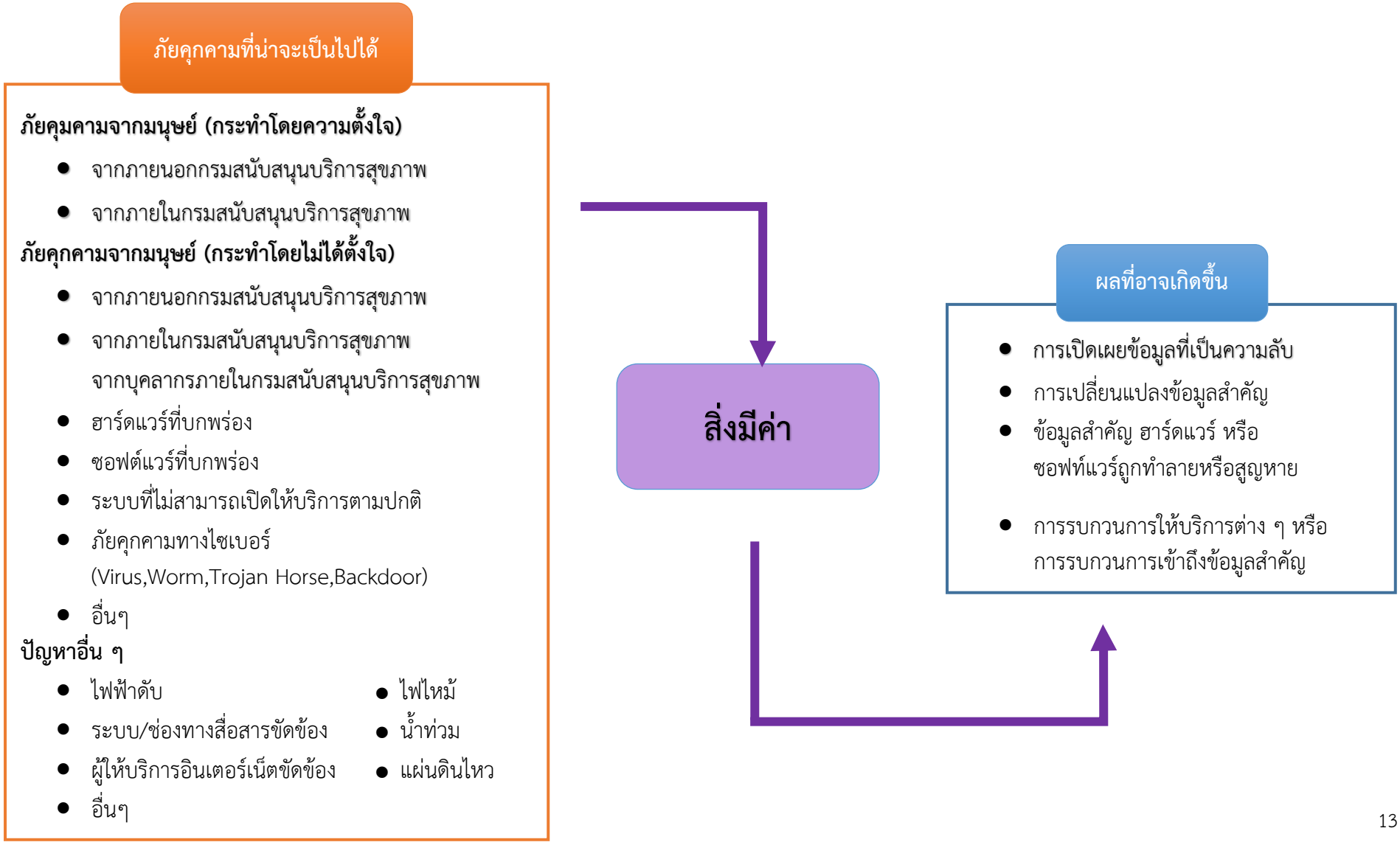
การรายงานผล

กำหนดให้ผู้รับผิดชอบดำเนินการรวบรวมรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบ อย่างน้อยปีละ ๑ ครั้ง ในกรณีตรวจพบปัญหาเร่งด่วนให้รายงานการเกิดปัญหาและผลการแก้ไขให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบโดยทันที

ผู้เกี่ยวข้อง	บทบาทและความรับผิดชอบหลัก
กลุ่มเทคโนโลยีสารสนเทศ	● มีความเข้าใจถึงความเสี่ยงที่อาจมีผลกระทบร้ายแรงต่อองค์กร ● ทำให้มั่นใจว่ามีการควบคุมภายในที่เหมาะสมเพื่อจัดการความเสี่ยงทั่วทั้งองค์กร ● กำกับดูแลและติดตามการบริหารความเสี่ยง ● รายงานต่อคณะทำงานติดตามการดำเนินงาน เกี่ยวกับประสิทธิภาพและประสิทธิผลของการควบคุมภายใน ● สื่อสารกับคณะทำงานติดตามการดำเนินงาน เพื่อให้เข้าใจความเสี่ยงที่สำคัญ และเชื่อมโยงกับระบบการควบคุมภายใน
คณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	● พิจารณาและอนุมัตินโยบายและกรอบการบริหารความเสี่ยง ● ติดตามการพัฒนากรอบการบริหารความเสี่ยง ● ติดตามกระบวนการบ่งชี้และประเมินความเสี่ยง ● ประเมินและอนุมัติแผนการจัดการความเสี่ยง ● รายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เกี่ยวกับความเสี่ยงและการจัดการความเสี่ยง ● สื่อสารกับกลุ่มเทคโนโลยีสารสนเทศ ตรวจสอบเกี่ยวกับความเสี่ยงที่สำคัญ

ผู้เกี่ยวข้อง	บทบาทและความรับผิดชอบหลัก
คณะกรรมการอำนวยการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	● ติดตามความเสี่ยงที่สำคัญทั้งองค์กร และทำให้มั่นใจได้ว่ามีแผนการจัดการที่ เหมาะสม ● ส่งเสริมนโยบายการบริหารความเสี่ยง และทำให้มั่นใจว่ากระบวนการบริหาร ความเสี่ยงได้รับการปฏิบัติทั่วทั้งองค์กร ● ติดตามความเสี่ยงทางกลยุทธ์และความเสี่ยงด้านการปฏิบัติการที่สำคัญและทำให้มั่นใจ ได้ว่ามีแผนการจัดการความเสี่ยงที่เหมาะสม ส่งเสริมวัฒนธรรมการบริหารความเสี่ยง และทำให้มั่นใจได้ว่าผู้อำนวยการหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ให้ความสำคัญกับการบริหารความเสี่ยงในหน่วยงานของตน
ผู้อำนวยการหน่วยงานในสังกัดกรมฯ	● ทำให้มั่นใจว่าการ จัดการและรายงานความเสี่ยง อย่างเพียงพอ ● ส่งเสริมเจ้าหน้าที่ในหน่วยงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง
งานเทคโนโลยีสารสนเทศ	● ระบุและจัดทำรายงานความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานหน่วยงาน เสนอต่อผู้อำนวยการฯ และเข้าร่วมในการจัดทำแผนจัดการความเสี่ยง และนำแผนไปปฏิบัติต่อไป
หน่วยงานหรือ ผู้รับผิดชอบการบริหารความเสี่ยง	● จัดทำนโยบายความเสี่ยง กรอบ และกระบวนการให้กับหน่วยงาน และเสนอต่อคณะทำงานฯ เพื่อพิจารณาอนุมัติ ● ให้การสนับสนุนและแนะนำกระบวนการบริหารความเสี่ยงแก่หน่วยงาน ต่าง ๆ ภายในองค์กรตามที่มีการร้องขอ
ผู้ตรวจสอบ ภายใน	● ตรวจสอบความเหมาะสมของการจัดการความเสี่ยงและการปฏิบัติตามภายในองค์กร ● ติดตามแผนการบริหารความเสี่ยงในการนำมาปรับใช้และการปฏิบัติตามแผนฯขององค์กร

ขั้นที่ ๒ บ่งชี้ปัจจัยความเสี่ยง
ผังเหตุการณ์หรือสถานการณ์ที่น่าจะเป็นภัยคุกคามต่อสิ่งมีค่า



ขั้นที่ ๓ วิเคราะห์ความเสี่ยง

ตารางที่ ๑ ระบุความเสี่ยงและผลกระทบด้านต่าง ๆ ที่จะเกิดขึ้น

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
ที่มาความเสี่ยง / ปัจจัยเสี่ยง	**ผลกระทบด้านต่าง ๆ**			
	ชื่อเสียง	**เวลา**	**การบริการ**	**บุคลากร**
๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	- ได้รับคำตำหนิจากเจ้าหน้าที่ - เจ้าหน้าที่ขาดความเชื่อมั่นในระบบ	- เจ้าหน้าที่ไม่สามารถใช้ระบบงานและข้อมูลได้ - ใช้ระยะเวลานานในการกู้คืนระบบงานและข้อมูล	- เจ้าหน้าที่ไม่สามารถใช้ระบบงานและข้อมูลในการปฏิบัติงาน และให้บริการได้	- เจ้าหน้าที่ผู้ปฏิบัติงาน/ผู้ดูแลระบบถูกตำหนิ
๒. ระบบให้บริการอินเทอร์เน็ตขัดข้อง	- ได้รับคำตำหนิจากเจ้าหน้าที่ - เจ้าหน้าที่ขาดความเชื่อมั่นในระบบ	- ทำให้ระบบเทคโนโลยีสารสนเทศต่าง ๆ ของกรมสนับสนุนบริการสุขภาพไม่สามารถทำงานได้ - ทำให้ไม่สามารถรับ-ส่งข้อมูลทางอิเล็กทรอนิกส์	- เจ้าหน้าที่ไม่สามารถใช้ระบบสารสนเทศในการปฏิบัติงาน - ประชาชนไม่สามารถใช้บริการระบบผ่านอินเทอร์เน็ต	- เจ้าหน้าที่ผู้ปฏิบัติงาน/ผู้ดูแลระบบถูกตำหนิ
๓. เครื่องแม่ข่ายถูกโจมตี	- เจ้าหน้าที่ถูกวิจารณ์ถึงการทำงานในการดูแลเครื่องแม่ข่าย	- ทำให้ระบบสารสนเทศไม่สามารถทำงานได้อย่างปกติ	เจ้าหน้าที่หน่วยงานต่าง ๆ ไม่สามารถทำงานได้	- เจ้าหน้าที่ถูกตำหนิถึงการทำงานในการดูแลเครื่องแม่ข่าย

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
ที่มาความเสี่ยง / ปัจจัยเสี่ยง	**ผลกระทบด้านต่าง ๆ**			
	ชื่อเสียง	**เวลา**	**การบริการ**	**บุคลากร**
๔. เครื่องลูกข่าย ถูกโจมตี	-	- เครื่องของเจ้าหน้าที่ไม่สามารถใช้งานได้ตามปกติ	- เครื่องของเจ้าหน้าที่ไม่สามารถให้บริการได้ตามปกติ	-การดำเนินงานของเจ้าหน้าที่หยุดชะงัก เนื่องจากใช้ระยะเวลานานในการจัดการแก้ไขปัญหา
๕. การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่	- เป็นข่าวในสื่อภายในประเทศ และต่างประเทศ - ถูกประชาชนวิจารณ์ถึงประสิทธิภาพการทำงานของกรมสนับสนุนบริการสุขภาพ	- ใช้เวลาในการทบทวนติดตาม/ตรวจสอบข้อมูล รวมทั้งเวลาในการเรียกคืนความเชื่อมั่นจากผู้รับบริการ	- ไม่สามารถให้บริการเปิดเผยหรือเผยแพร่ข้อมูลที่ผิดพลาดจากความเป็นจริง	- เจ้าหน้าที่ถูกตำหนิในการเผยแพร่ข้อมูลอย่างไม่ระมัดระวัง/ไม่เก็บรักษาข้อมูลสำคัญให้เป็นความลับ
๖. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- ได้รับคำตำหนิจากผู้ใช้งานระบบสารสนเทศ - ผู้ใช้งานขาดความเชื่อมั่นในระบบ	- ทำให้ระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพไม่สามารถทำงานได้ - ทำให้ไม่สามารถรับ-ส่งข้อมูลทางอิเล็กทรอนิกส์	- เจ้าหน้าที่ไม่สามารถใช้ระบบสารสนเทศในการปฏิบัติงาน - ประชาชนไม่สามารถใช้บริการระบบสารสนเทศได้	- เจ้าหน้าที่ผู้ปฏิบัติงาน/ผู้ดูแลระบบถูกตำหนิ

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
ที่มาความเสี่ยง /ปัจจัยเสี่ยง	**ผลกระทบด้านต่าง ๆ**			
	ชื่อเสียง	**เวลา**	**การบริการ**	**บุคลากร**
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ ฯลฯ	- เป็นข่าวในหนังสือพิมพ์/ Social Media	- ทำให้ระบบเสียหายการทำงานหยุดชะงักและต้องใช้เวลานานในการกู้คืนและปรับปรุงระบบ	- ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้	- ถูกตำหนิในเรื่องการป้องกันและเตรียมการในการดูแลระบบ
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อย ในบ้านเมือง	-	- ทำให้ระยะเวลาในการดำเนินงานและปรับปรุงระบบเพิ่มมากขึ้น	- ไม่สามารถปฏิบัติงานและให้บริการได้ตามปกติ	- เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้ตามปกติ

ขั้นที่ ๔ ระบุและจัดลำดับความเสี่ยง

ตารางที่ ๒ การประเมินความเสี่ยง

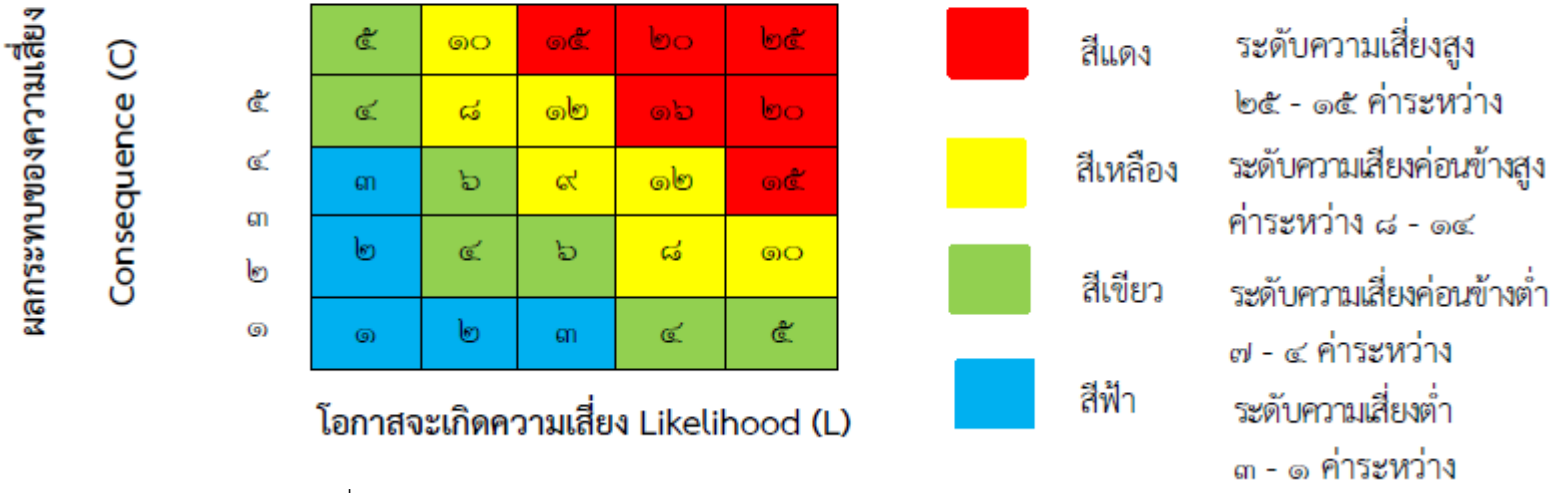
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
ปัจจัยเสี่ยง	**รายละเอียดความสูญเสีย**	**โอกาส**	**ผลกระทบ**	**ระดับความเสี่ยง**
๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	- เจ้าหน้าที่ในกรมสนับสนุนบริการสุขภาพ ไม่สามารถใช้งานระบบสารสนเทศภายในได้ - เจ้าหน้าที่ลงรับหนังสือไม่สามารถให้บริการผู้ที่มาติดต่อได้ ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๓	๔	๑๒
๒. ระบบให้บริการอินเทอร์เน็ตขัดข้อง	- ทำให้กรมสนับสนุนบริการสุขภาพ ไม่สามารถให้บริการผ่านทางอินเทอร์เน็ต	๓	๔	๑๒
๓. การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหลถูกเปิดเผยหรือเผยแพร่)	- ทำให้ประชาชนไม่มั่นใจในคุณภาพข้อมูลของกรมสนับสนุนบริการสุขภาพ/ขาดความเชื่อมั่นใน ความปลอดภัยของข้อมูล - ทำให้ตกเป็นข่าวในประเทศ และต่างประเทศ	๓	๕	๑๕
๔. เครื่องแม่ข่ายถูกโจมตี	- ทำให้ระบบสารสนเทศ/ระบบสำคัญทำงานได้ช้ำ หรือทำงานไม่ได้	๓	๔	๑๒
๕. เครื่องลูกข่ายถูกโจมตี	- ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	๓	๓	๙
๖. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๓	๕	๑๕

ขั้นที่ ๔ ระบุและจัดลำดับความเสี่ยง (ต่อ)

ตารางที่ ๒ การประเมินความเสี่ยง

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
ปัจจัยเสี่ยง	**รายละเอียดความสูญเสีย**	**โอกาส**	**ผลกระทบ**	**ระดับความเสี่ยง**
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	- การเกิดไฟไหม้อาคาร หรือแผ่นดิน ไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วน หรือทั้งหมด หรือการเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	๑	๕	๕
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๑	๕	๕

ผลการประเมินระดับความเสี่ยง



ผลการประเมินพบว่าความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพทุกระบบไม่ว่าจะเป็นการนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่) / ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย,ระบบให้บริการ Internet ล่ม เครื่อง Server และเครื่อง Client ติดไวรัส กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ ภัยหรือสถานการณ์ฉุกเฉิน สถานการณ์ความไม่สงบเรียบร้อย ในบ้านเมือง มีระดับความเสี่ยงสูง คะแนนระดับความเสี่ยง (๑๐ – ๑๕) ไม่สามารถที่จะยอมรับความเสี่ยงนั้นได้ จำเป็นต้องมีแผนควบคุมความเสี่ยง

ขั้นที่ ๕ วางแผนการรับมือกับความเสี่ยง

๕.๑ สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง

ตารางที่ ๓ สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ					
๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลกระทบต่อการทำงานของระบบงานและข้อมูลซึ่งจำเป็นต้องให้บริการและมีการใช้งานอย่างต่อเนื่อง			
	ควบคุม	- จัดสร้างระบบงานสำรองเพื่อทำงานแทนเมื่อระบบหลักเกิดปัญหา (กรณีที่เป็นระบบงานและข้อมูลที่มีความสำคัญและส่งผลกระทบต่อองค์กรมาก) - หน่วยงานมีผู้ดูแลระบบงานและข้อมูล - มีการจัดอบรมเพื่อให้ความรู้แก่ผู้ใช้ระบบ	- เกิดค่าใช้จ่ายในการจัดหาจัดจ้างเพื่อพัฒนาระบบงานสำรอง	- การดำเนินงานของกรมสนับสนุนบริการสุขภาพ เป็นไปได้อย่างต่อเนื่อง	
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๒. ระบบให้บริการอินเทอร์เน็ตขัดข้อง	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสีย			
	ควบคุม	- จัดให้มีการเชื่อมสำรองต่อผู้ให้บริการโครงข่าย (ISP) รายที่สองเพื่อให้การบริการเครือข่ายสามารถดำเนินการได้อย่างต่อเนื่อง (ทดแทนกรณีที่ ผู้ให้บริการโครงข่าย (ISP) หลัก เกิดปัญหา)	- เกิดค่าใช้จ่ายในการจัดหาอุปกรณ์ระบบเครือข่ายสำรองและการจัดหา ผู้ให้บริการโครงข่าย (ISP) รายที่สอง	- การให้บริการประชาชนทางอินเทอร์เน็ตได้อย่างต่อเนื่อง	
	ถ่ายโอน	- จัดจ้างหน่วยงานภายนอกดูแลระบบเครือข่าย Internet - จัดให้มีการเชื่อมสำรองต่อกับ ISP รายที่สอง	- เกิดค่าใช้จ่ายในการจัดจ้าง Outsource ทั้งตัวระบบและการดูแลระบบ		

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๓. การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่)	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียมาก			
	ควบคุม	- จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ	- เกิดค่าใช้จ่ายในการจัดทำระบบป้องกันความปลอดภัยของข้อมูล - เกิดค่าใช้จ่ายการจัดอบรม	ประชาชนมีความเชื่อมั่นต่อใช้บริการระบบสารสนเทศที่น่าเชื่อถือและปลอดภัย	
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๔. เครื่องแม่ข่ายถูกโจมตี	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม ,ถ่ายโอน
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียมาก			
	ควบคุม	- จัดทำและประกาศใช้นโยบายการป้องกันการถูกโจมตี - ติดตั้งระบบป้องกันการถูกโจมตีในส่วนของ Server - ทำการอัพเดทระบบป้องกันอย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ	- เกิดค่าใช้จ่ายในการจัดหาระบบป้องกันการโจมตี - เกิดค่าใช้จ่ายการจัดอบรม	- ระบบเครื่องแม่ข่ายทำงานได้ อย่างต่อเนื่อง -ข้อมูลภายในเครื่องแม่ข่ายมีความมั่นคงปลอดภัย	
	ถ่ายโอน	- จัดให้มีเครื่องแม่ข่ายสำรอง (DR-site) - จัดจ้างหน่วยงานภายนอกดูแลเครื่องแม่ข่าย	- เกิดค่าใช้จ่ายในการจัดจ้าง Outsource	- ระบบเครื่องแม่ข่ายทำงานได้ อย่างต่อเนื่อง -ข้อมูลภายในเครื่องแม่ข่ายมีความมั่นคงปลอดภัย	

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๕. เครื่องลูกข่ายโจมตี	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้	- เกิดค่าใช้จ่ายในการจัดหาระบบป้องกันการโจมตี - เกิดค่าใช้จ่ายการจัดอบรม	- ระบบคอมพิวเตอร์ของผู้ใช้ทำงานได้อย่างต่อเนื่อง - ข้อมูลภายในเครื่องลูกข่าย ปลอดภัย	ควบคุม
	ยอมรับ	- สามารถยอมรับความเสี่ยงนี้ได้			
	ควบคุม	- จัดทำและประกาศใช้นโยบายการป้องกันการถูกโจมตี - ติดตั้งระบบป้องกันการถูกโจมตีในส่วนของเครื่องลูกข่ายโจมตี - ทำการอัพเดทระบบป้องกันอย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ			
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๖. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียมาก - ระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ			
	ควบคุม	- ติดตั้งเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) และเครื่องปั่นไฟ(Generator) เพื่อป้องกันความเสียหายที่อาจเกิด ขึ้นกับอุปกรณ์ ทั้งในส่วนของเครื่องคอมพิวเตอร์ แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC)	- เกิดค่าใช้จ่ายในการจัดหาเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้า อัตโนมัติ (UPS)และ เครื่องปั่นไฟ (Generator)	- เพื่อป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหาย แก่ระบบสารสนเทศและ ระบบคอมพิวเตอร์	
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	หลีกเลี่ยง	- ไม่สามารถหลีกเลี่ยงได้	การจัดหาระบบสำรองและฐานข้อมูลเก็บไว้ใน DR Site เกิดต้นทุนและค่าใช้จ่าย ในการดำเนินการ	- ระบบสารสนเทศสามารถทำงานได้อย่างต่อเนื่อง	ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้			
	ควบคุม	- จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤต จัดหาระบบสำรองและฐานข้อมูลเก็บไว้ใน DR Site			
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	หลีกเลี่ยง	- ไม่สามารถหลีกเลี่ยงได้	การจัดหาระบบสำรองและฐานข้อมูลเก็บไว้ใน DR Site เกิดต้นทุนและค่าใช้จ่าย ในการดำเนินการ	- ระบบสารสนเทศสามารถทำงานได้อย่างต่อเนื่อง	ยอมรับความเสี่ยง
	ยอมรับ	- จำเป็นต้องยอมรับความเสี่ยงนี้ได้			
	ควบคุม	- ไม่สามารถควบคุม			
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			

๕.๒ แนวทางในการจัดการ/ควบคุมความเสี่ยง

ตารางที่ ๔ แบบสรุปการจัดการความเสี่ยง

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	โอกาสที่จะเกิด (๑)	ผลกระทบเสียหาย (๒)	ระดับความเสี่ยง (๑)X ๒)	แนวทางการควบคุม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๑.ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหาย หรือถูกทำลาย	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน/ โดน Virus โจมตี/ Hacker/Cracker	- เจ้าหน้าที่กรมสนับสนุนบริการสุขภาพไม่สามารถใช้ระบบงาน และข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๓	๔	๑๒	- จัดทำระบบงานและข้อมูลสำรองให้ทำงานแทนเมื่อระบบหลักเกิดปัญหา (ระบบ Database Backup) - หน่วยงานมีผู้ดูแลระบบงานและข้อมูล - มีการจัดอบรมเพื่อให้ความรู้ด้านการดูแลรักษาความปลอดภัยของระบบงานและข้อมูลแก่ผู้ใช้ระบบ
๒. ระบบให้บริการอินเทอร์เน็ตขัดข้อง	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	- เจ้าหน้าที่กรมสนับสนุนบริการสุขภาพไม่สามารถใช้บริการ Internet ได้ - ไม่สามารถให้บริการผู้ใช้งานระบบได้ ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๓	๔	๑๒	- จัดให้มีการเชื่อมสำรองต่อผู้ให้บริการโครงข่าย (ISP) รายที่สองเพื่อให้การบริการเครือข่ายสามารถดำเนินการได้อย่างต่อเนื่อง (ทดแทนกรณีที่ ผู้ให้บริการโครงข่าย (ISP) หลัก เกิดปัญหา)
๓. การนำเสนอข้อมูล ผิดพลาด/ข้อมูลสำคัญที่เป็นความลับ รั่วไหล ถูกเปิดเผย หรือเผยแพร่)	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาความปลอดภัยของข้อมูล	๓	๕	๑๕	- จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	โอกาสที่จะเกิด (๑)	ผลกระทบเสียหาย (๒)	ระดับความเสี่ยง (๑) X (๒)	แนวทางการควบคุม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๔. เครื่องแม่ข่ายถูกโจมตี	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ระบบสารสนเทศ/ระบบสำคัญทำงานได้ช้าหรือทำงานไม่ได้	๓	๔	๑๒	- จัดทำและประกาศใช้นโยบายการป้องกันการถูกโจมตี - ติดตั้งระบบป้องกันการถูกโจมตีในส่วนของ Server - ทำการอัพเดทระบบป้องกันอย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ
๕. เครื่องลูกข่ายถูกโจมตี	ความเสี่ยงจากผู้ปฏิบัติงานนำอุปกรณ์เคลื่อนที่ (Smart Phone, Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อ รวมถึงการดาวน์โหลดโปรแกรมหรือไฟล์จากอินเทอร์เน็ตโดยขาดความระมัดระวัง	-ส่งผลกระทบต่อการใช้งานระบบเครือข่าย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย -ทำให้เครื่องของเจ้าหน้าที่ไม่สามารถทำงานได้	๓	๓	๙	- ฝึกอบรม เผยแพร่และประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องของความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากร - ส่งเสริมให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด - กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	โอกาสที่จะเกิด (๑)	ผลกระทบเสียหาย (๒)	ระดับความเสี่ยง (๑) X (๒)	แนวทางการควบคุม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านเทคนิค	- ทำให้ระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพไม่สามารถทำงานได้ - ทำให้ไม่สามารถรับ-ส่งข้อมูลทางอิเล็กทรอนิกส์	๓	๕	๑๕	- บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล - เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย(Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในหน่วยงานด้วย - ให้ความรู้และความเข้าใจแก่เจ้าหน้าที่กรมสนับสนุนบริการสุขภาพตามแนวทางปฏิบัติที่กรมฯกำหนด

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	โอกาสที่จะเกิด (๑)	ผลกระทบเสียหาย (๒)	ระดับความเสี่ยง (๑) X (๒)	แนวทางการควบคุม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ)	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ทำให้เครื่องคอมพิวเตอร์ถูกทำลายหรือเสียหาย	๑	๕	๕	- มีการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตจัดหาระบบสำรองและฐานข้อมูลเก็บไว้ใน DR Site - มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เช่น การชุมนุมประท้วง จลาจลการก่อการร้าย	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย ส่งผลให้เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้ตามปกติ	๑	๕	๕	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ใน DR Site

ตารางที่ ๕ แบบรายการกิจกรรมในการจัดการความเสี่ยง

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหาย หรือถูกทำลาย	- บุคลากรของสำนักงานกรมสนับสนุนบริการสุขภาพไม่สามารถใช้ระบบงานและข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องกำรใช้ระบบงานและข้อมูลได้ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๑๒	- จัดทำระบบความมั่นคงปลอดภัยของระบบงานและข้อมูล - จัดสร้างระบบงานสำรองเพื่อทำงานแทนเมื่อระบบหลักเกิดปัญหา (กรณีที่เป็นระบบงานและข้อมูลที่มีความสำคัญและส่งผลกระทบต่อองค์กรมาก)	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - จัดจ้างหน่วยงานภายนอกเฝ้าระวังระบบงาน - จัดซื้อจัดจ้างระบบป้องกันความปลอดภัยของข้อมูล - จัดอบรมให้ความรู้ด้านความปลอดภัย
๒. ระบบให้บริการอินเทอร์เน็ตขัดข้อง	- ทำให้ประชาชนไม่สามารถใช้บริการระบบผ่านทางอินเทอร์เน็ต	๑๒	- จัดให้มีการเชื่อมสำรองต่อผู้ให้บริการโครงข่าย (ISP) รายที่สองเพื่อให้การบริการเครือข่ายสามารถดำเนินการได้อย่างต่อเนื่อง (ทดแทนกรณีที่ ผู้ให้บริการโครงข่าย (ISP) หลัก เกิดปัญหา)	- จัดประชุมทีมงานฝ่ายดูแลเครือข่ายสารสนเทศ เพื่อจัดหาผู้ให้บริการโครงข่าย(ISP) รายที่สอง (ทดแทนกรณีที่ ผู้ให้บริการโครงข่าย (ISP) หลัก เกิดปัญหา)
๓. การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่	- ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาข้อมูลของ กรมสนับสนุนบริการสุขภาพ ทำให้ตกเป็นข่าวใน หนังสือพิมพ์ในประเทศ และ ต่างประเทศ	๑๕	- จัดให้มีระบบป้องกันความปลอดภัยของข้อมูล - จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง	- จัดทำและประกาศใช้นโยบายการดูแลและ การใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มี ระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
๔. เครื่องแม่ข่ายถูกโจมตี	- ทำให้ระบบสารสนเทศ/ระบบงานสำคัญทำงานได้ช้าหรือทำงานไม่ได้	๑๒	- จัดทำและประกาศใช้นโยบายการป้องกันการถูกโจมตี - ติดตั้งระบบป้องกันการถูกโจมตีในส่วนของเครื่องแม่ข่าย - ทำการอัพเดทระบบป้องกันอย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ
๕. เครื่องลูกข่ายถูกโจมตี	- ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	๙	- จัดทำและประกาศใช้นโยบายการป้องกันการถูกโจมตี - ติดตั้งระบบป้องกันการถูกโจมตีในส่วนของเครื่องลูกข่ายโจมตี - ทำการอัพเดทระบบป้องกันอย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ
๖. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้า ไม่คงที่	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้ ระบบงาน/ข้อมูลเสียหรือสูญหาย	๑๕	- ติดตั้งเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติ(UPS) และเครื่องปั่นไฟ(Generator) เพื่อป้องกันความเสียหายที่อาจเกิด ขึ้นกับอุปกรณ์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC)	- บำรุงรักษาเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติ และ เครื่องปั่นไฟให้อยู่ในสภาพพร้อมใช้งาน อยู่เสมอ

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
				- ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที - ให้ความรู้และความเข้าใจแก่บุคลากรของกรมสนับสนุนบริการสุขภาพในการใช้งานเครื่องสำรองไฟฟ้า(UPS)อย่างมีประสิทธิภาพ
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	- ทำให้ระบบเสียหายการทำงานหยุดชะงักและต้องใช้เวลานานในการกู้คืนและปรับปรุงระบบ	๕	- มีการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตจัดหาระบบสำรองและฐานข้อมูลเก็บไว้ใน DR Site - มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบ

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
				และดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า ๑ วัน ในการดำเนินการแก้ไข ให้ออกประกาศแจ้งแก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น -กรณีที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไปเมื่อเกิดเหตุอุปกรณ์จัดเก็บข้อมูลเสียหาย ให้รายงานผู้บังคับบัญชาของตนทราบแล้วแจ้งกลุ่มคอมพิวเตอร์เพื่อตรวจสอบเหตุแห่งความเสียหายนั้น

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ				
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำ ให้บุคลากรสามารถปฏิบัติงานได้ ตามปกติ	๕	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - ทำการสำรองข้อมูลและฐานข้อมูลเก็บไว้ใน DR Site	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลและฐานข้อมูลเก็บไว้ใน DR Site

ขั้นที่ ๖ รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง

ตารางที่ ๖ การติดตามกิจกรรมการจัดการความเสี่ยง

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

รายงานความเสี่ยง **๑.ระบบงานและข้อมูล (System & information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย**

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรคและแนวทางการแก้ไข
๑. จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัย					
๒.จัดจ้างหน่วยงานภายนอกเฝ้าระวัง					
๓.จัดซื้อจัดจ้างระบบป้องกันความปลอดภัยของข้อมูล					
๔.จัดอบรมให้ความรู้ด้านความปลอดภัย					

<u>รายงานผลลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

รายงานความเสี่ยง **๒.ระบบให้บริการอินเทอร์เน็ตขัดข้อง**

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	%	ปัญหา
๑. จัดประชุมทีมงานฝ่ายดูแลเครือข่ายสารสนเทศ เพื่อจัดหาผู้ให้บริการโครงข่าย(ISP) รายที่สอง (ทดแทนกรณีที่ผู้ให้บริการโครงข่าย (ISP) หลักเกิดปัญหา)					
๒. ดำเนินการตามแผนปฏิบัติ การรักษาความมั่นคงปลอดภัยของระบบระบบเครือข่ายเทคโนโลยีสารสนเทศ					

<u>รายงานการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

รายงานความเสี่ยง **๓.การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่**

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรคและแนวทางการแก้ไข
๑. จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับของ					
๒. จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง					
๓. จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ					

<u>รายงานการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี
รายงานความเสี่ยง **๔.เครื่องแม่ข่ายถูกโจมตี**
วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรคและแนวทางการแก้ไข
๑. จัดหาอุปกรณ์ป้องกันรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์					
๒. จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ					
๓. จัดอบรมให้ความรู้เกี่ยวกับ ป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี
รายงานความเสี่ยง **๕.เครื่องลูกข่ายถูกโจมตี**
วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	% ความคืบหน้า	ปัญหา
๑. จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ					
๒. จัดอบรมให้ความรู้เกี่ยวกับป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ใช้งาน					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี
รายงานความเสี่ยง **๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่**
วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	% ความคืบหน้า	ปัญหา
๑. บำรุงรักษาเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติ และ เครื่องปั่นไฟให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ					
๒. ติดตั้งเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติและ เครื่องปั่นไฟ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที					
๓. ให้ความรู้และความเข้าใจแก่บุคลากรของกรมสนับสนุนบริการสุขภาพในการใช้งานเครื่องสำรองไฟฟ้า(UPS)อย่างมีประสิทธิภาพ					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

รายงานความเสี่ยง **๗. ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน,ไฟไหม้,ไฟฟ้าลัดวงจร,การวางเพลิง,ภัยธรรมชาติ**

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	% ความคืบหน้า	ปัญหา
๑.จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ					
๒. เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบและดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไขทั้งนี้ หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า ๑ วัน ในการดำเนินการแก้ไขให้ออกประกาศแจ้งแก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

รายงานความเสี่ยง **๘. สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง**

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	% ความคืบหน้า	ปัญหา
๑.จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ					
๒. สำรองข้อมูลและฐานข้อมูลเก็บไว้ใน DR Site					
๓.จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้					

ตารางที่ ๗ การประเมินผลการจัดการความเสี่ยง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความ เสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๑.	การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับ รั่วไหล ถูกเปิดเผยหรือเผยแพร่	- ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาข้อมูลของกรมสนับสนุนบริการสุขภาพ ทำให้ตกเป็นข่าวในหนังสือพิมพ์ในประเทศ และต่างประเทศ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับ ป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ			
๒.	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/ แรงดันไฟฟ้าไม่คงที่	- ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้า หรือทำงาน ไม่ได้ ระบบงาน/ข้อมูลเสียหรือ สูญหาย	- บำรุงรักษาเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติ และ เครื่องปั่นไฟให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้า อัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจ เกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการ ประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของ เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที - ให้ความรู้และความเข้าใจแก่บุคลากรของกรมสนับสนุนบริการสุขภาพในการใช้งานเครื่องสำรองไฟฟ้า(UPS)อย่างมีประสิทธิภาพ			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๓.	ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหาย หรือถูกทำลาย	- บุคลากรของสำนักงานกรมสนับสนุนบริการสุขภาพไม่สามารถใช้ระบบงานและข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ทำให้ เจ้าหน้าที่/	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - จัดจ้างหน่วยงานภายนอกเฝ้าระวังระบบงาน - จัดซื้อจัดจ้างระบบป้องกันความปลอดภัยของข้อมูล - จัดอบรมให้ความรู้ด้านความปลอดภัย			
๔.	ระบบให้บริการอินเทอร์เน็ตขัดข้อง	- ทำให้ประชาชนไม่สามารถใช้บริการระบบผ่านทางอินเทอร์เน็ต	- จัดประชุมทีมงานฝ่ายดูแลเครือข่ายสารสนเทศ เพื่อจัดหาผู้ให้บริการโครงข่าย(ISP) รายที่สอง (ทดแทนกรณีที่ผู้ให้บริการโครงข่าย (ISP) หลัก เกิดปัญหา)			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๕.	เครื่องแม่ข่ายถูกโจมตี	- ทำให้ระบบสารสนเทศ/ระบบงานสำคัญทำงานได้ช้าหรือทำงานไม่ได้	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ			
๖	เครื่องลูกข่ายถูกโจมตี	-ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบและผู้ใช้งาน			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๗	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุ ไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	- ทำให้ระบบเสียหายการทำงานหยุดชะงักและต้องใช้เวลานานในการกู้คืนและปรับปรุงระบบ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบ และดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า ๑ วัน ในการดำเนินการแก้ไข ให้ออกประกาศแจ้งแก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น -กรณีที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไปเมื่อเกิดเหตุอุปกรณ์จัดเก็บข้อมูลเสียหาย ให้รายงาผู้บังคับบัญชาของตนทราบแล้วแจ้งกลุ่มคอมพิวเตอร์เพื่อตรวจสอบเหตุแห่งความเสียหายนั้น			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๘	ความเสี่ยงจากสถานการณ์ความไม่ สงบเรียบร้อยใน บ้านเมือง	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำ ให้บุคลากรสามารถปฏิบัติงานได้ ตามปกติ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศ สามารถทำงานได้ - สำรองข้อมูลและฐานข้อมูลเก็บไว้ใน DR Site			

ตารางที่ ๘ สรุปผลการดำเนินงานจากการบริหารความเสี่ยง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยง	ผลจากการใช้มาตรการจัดการ ความ	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๑.	การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่	- ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาข้อมูลของ กรมสนับสนุนบริการสุขภาพ ทำให้ตกเป็นข่าวใน หนังสือพิมพ์ในประเทศ และต่างประเทศ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับ ป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ			
๒.	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่	-ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้าหรือทำงาน ไม่ได้ ระบบงาน/ข้อมูลเสียหรือ สูญหาย	- บำรุงรักษาเครื่องสำรองไฟฟ้าปรับแรงดันไฟฟ้าอัตโนมัติ และ เครื่องปั่นไฟให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้า อัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจ เกิดขึ้นกับอุปกรณ์ คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของ เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่อง คอมพิวเตอร์ส่วนบุคคล(PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที - ให้ความรู้และความเข้าใจแก่บุคลากรของกรมสนับสนุนบริการสุขภาพในการใช้งานเครื่องสำรองไฟฟ้า(UPS)อย่างมีประสิทธิภาพ			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๓.	ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหาย หรือถูกทำลาย	- บุคลากรของสำนักงานกรมสนับสนุนบริการสุขภาพไม่สามารถใช้ระบบงานและข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - จัดจ้างหน่วยงานภายนอกเฝ้าระวังระบบงาน - จัดซื้อจัดจ้างระบบป้องกันความ ปลอดภัยของข้อมูล - จัดอบรมให้ความรู้ด้านความปลอดภัย			
๔.	ระบบให้บริการอินเทอร์เน็ตขัดข้อง	- ทำให้ประชาชนไม่สามารถใช้บริการระบบผ่านทางอินเทอร์เน็ต	- จัดประชุมทีมงานฝ่ายดูแลเครือข่าย สารสนเทศ เพื่อจัดหาผู้ให้บริการโครงข่าย(ISP) รายที่สอง (ทดแทนกรณีที่ผู้ให้บริการโครงข่าย (ISP) หลัก เกิดปัญหา)			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๕	เครื่องแม่ข่ายถูกโจมตี	- ทำให้ระบบสารสนเทศ/ระบบงานสำคัญทำงานได้ช้า หรือทำงานไม่ได้	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ			
๖	เครื่องลูกข่ายถูกโจมตี	-ทำให้เครื่องของเจ้าหน้าที่บาง ท่านทำงานไม่ได้	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันการถูกโจมตีและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบและผู้ใช้งาน			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๗	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	- ทำให้ระบบเสียหายการทำงานหยุดชะงักและต้องใช้เวลานานในการกู้คืนและปรับปรุงระบบ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบและดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า ๑ วัน ในการดำเนินการแก้ไข ให้ออกประกาศแจ้งแก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น -กรณีที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไปเมื่อเกิดเหตุอุปกรณ์จัดเก็บข้อมูลเสียหายให้รายงาผู้บังคับบัญชาของตนทราบแล้วแจ้งกลุ่มคอมพิวเตอร์เพื่อตรวจสอบเหตุแห่งความเสียหายนั้น			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ						
๘	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำ ให้บุคลากรสามารถปฏิบัติงานได้ ตามปกติ	- จัดประชุมคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลและฐานข้อมูลเก็บไว้ใน DR Site			

ภาคผนวก

รายการระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ

ลำดับ	ชื่อระบบสารสนเทศ	Domain name	ผู้ดูแล	สถานะ
๑	เว็บไซต์กรมสนับสนุนบริการสุขภาพ	https://hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๒	ระบบ สมาร์ท อสม.	https://www.smart-osm.com/	กลุ่มเทคโนโลยีสารสนเทศ/สช.	ใช้งาน
๓	ระบบ สามหมอรู้จักคุณ	https://๓doctor.hss.moph.go.th/main/	กลุ่มเทคโนโลยีสารสนเทศ/สช.	ใช้งาน
๔	ระบบ สปา	https://spa.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๕	ระบบ one stop service	http://oss.hss.moph.go.th/auth/login	กลุ่มเทคโนโลยีสารสนเทศ/OSS	ใช้งาน
๖	ระบบ กิจการดูแลผู้สูงอายุหรือผู้มีภาวะพึ่งพิง	https://esta.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗	ระบบ คลังความรู้เพื่อสุขภาพ	https://healthydee.moph.go.th/	กองสุขศึกษา	ใช้งาน
๘	ระบบ บริหารแผนงานและงบประมาณ	https://smart.hss.moph.go.th/๖๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙	ระบบ จองห้องประชุม	http://meeting.hss.moph.go.th/room/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐	ระบบ จองรถยนต์ราชการ	http://asset.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑	ระบบ ทะเบียนสินทรัพย์	http://asset.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๒	ระบบ สารบรรณอิเล็กทรอนิกส์	http://saraban.hss.moph.go.th:๒๘๐๘๐/archive/login.jsp	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๓	ระบบ คิวออนไลน์	http://queue.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ/OSS	ใช้งาน
๑๔	ระบบ ประเมินมาตรฐานระบบบริการสุขภาพ	https://hs๔.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๕	เว็บไซต์ กลุ่มเทคโนโลยีสารสนเทศ	https://ict.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๖	เว็บไซต์สำนักงานเลขานุการกรม	http://admin.hss.moph.go.th/	เลขานุการกรม	ใช้งาน
๑๗	เว็บไซต์กองวิศวกรรมการแพทย์	http://medi.moph.go.th/	กองวิศวกรรมการแพทย์	ใช้งาน
๑๘	เว็บไซต์กองสุขศึกษา	http://www.hed.go.th/	กองสุขศึกษา	ใช้งาน
๑๙	เว็บไซต์กองสนับสนุนสุขภาพภาคประชาชน	http://phc.moph.go.th/www_hss/frontend/theme/index.php	สช.	ใช้งาน
๒๐	เว็บไซต์กองสถานประกอบเพื่อนสุขภาพ	http://www.thaispa.go.th/spa๒๐๑๓/web/web_new/index.php	กสพส.	ใช้งาน
๒๑	เว็บไซต์กองสุขภาพระหว่างประเทศ	https://www.thailandmedicalhub.net/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๒๒	เว็บไซต์กองแบบแผน	https://dcd.hss.moph.go.th/	กองแบบแผน	ใช้งาน
๒๓	เว็บไซต์กลุ่มแผนงาน	http://hssplan.hss.moph.go.th/	กลุ่มแผนงาน	ใช้งาน
๒๔	เว็บไซต์กองสถานพยาบาลและการประกอบโรคศิลปะ	https://mrd.hss.moph.go.th/	สพ.รศ	ใช้งาน
๒๕	เว็บไซต์กลุ่มประชาสัมพันธ์	http://prgroup.hss.moph.go.th/	กลุ่มประชาสัมพันธ์	ใช้งาน

รายการระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ (ต่อ)

ลำดับ	ชื่อระบบสารสนเทศ	Domain name	ผู้ดูแล	สถานะ
๒๖	เว็บไซต์กลุ่มคลัง	http://๒๐๓.๑๕๗.๗.๙๘/store/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๒๗	เว็บไซต์กลุ่มพัฒนาระบบบริหาร	http://opdc.hss.moph.go.th/	กลุ่มพัฒนาระบบบริหาร	ใช้งาน
๒๘	เว็บไซต์กลุ่มตรวจสอบภายใน	http://auditer.hss.moph.go.th/web_Audit/	กลุ่มตรวจสอบภายใน	ใช้งาน
๒๙	เว็บไซต์กลุ่มคุ้มครองจริยธรรม	http://ethics.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๓๐	เว็บไซต์กองกฎหมาย	http://law.hss.moph.go.th/	กองกฎหมาย	ใช้งาน
๓๑	เว็บไซต์กลุ่มบริหารทรัพยากรบุคคล	http://hr๒.hss.moph.go.th/	กบค.	ใช้งาน
๓๒	เว็บไซต์ศูนย์คุ้มครองผู้บริโภค	https://sites.google.com/view/hsscrm/	ศูนย์คุ้มครองผู้บริโภค	ใช้งาน
๓๓	เว็บไซต์สำนักผู้เชี่ยวชาญ	https://sites.google.com/view/hssexpert/	สำนักผู้เชี่ยวชาญ	ใช้งาน
๓๔	เว็บไซต์ศูนย์บริการแบบเบ็ดเสร็จ	http://ossc.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๓๕	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๑	http://do๑.new.hss.moph.go.th:๘๐๘๐/	ศบส. ๑	ใช้งาน
๓๖	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๒	http://do๒.new.hss.moph.go.th:๘๐๘๐/	ศบส. ๒	ใช้งาน
๓๗	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๓	http://do๓.new.hss.moph.go.th:๑๘๐๘๐/	ศบส. ๓	ใช้งาน
๓๘	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๔	https://do๔.hss.moph.go.th/	ศบส. ๔	ใช้งาน
๓๙	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๕	http://www.hss๐๕.com/	ศบส. ๕	ใช้งาน
๔๐	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๖	http://do๖.new.hss.moph.go.th:๘๐๘๐/	ศบส. ๖	ใช้งาน
๔๑	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๗	http://do๗.new.hss.moph.go.th:๘๐๘๐/	ศบส. ๗	ใช้งาน
๔๒	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๘	http://do๘.new.hss.moph.go.th:๘๐๘๐/	ศบส. ๘	ใช้งาน
๔๓	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๙	http://do๙.new.hss.moph.go.th:๘๐๘๐/index.php	ศบส. ๙	ใช้งาน
๔๔	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐	http://do๑๐.hss.moph.go.th:๘๐๘๑/DO๑๐WEB/	ศบส. ๑๐	ใช้งาน
๔๕	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑	http://do๑๑.new.hss.moph.go.th:๘๐๘๐/	ศบส. ๑๑	ใช้งาน
๔๖	เว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๑๒	http://do๑๒.new.hss.moph.go.th:๘๐๘๐/	ศบส. ๑๒	ใช้งาน
๔๗	เว็บไซต์ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคเหนือ	http://phcn.hss.moph.go.th/	สสม.ภาคเหนือ	ใช้งาน
๔๘	เว็บไซต์ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง	http://phce.hss.moph.go.th/index.php	สสม.ภาคกลาง	ใช้งาน
๔๙	เว็บไซต์ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคตะวันออกเฉียงเหนือ	https://www.esanphc.net/frontend๓/	สสม.ภาคตะวันออกเฉียงเหนือ	ใช้งาน
๕๐	เว็บไซต์ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคใต้	http://phcsn.hss.moph.go.th/	สสม.ภาคใต้	ใช้งาน

รายการระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ (ต่อ)

ลำดับ	ชื่อระบบสารสนเทศ	Domain name	ผู้ดูแล	สถานะ
๕๑	เว็บไซต์ศูนย์พัฒนาการสาธารณสุขมูลฐานชายแดนใต้	http://phcs.hss.moph.go.th/index.php	สสม.ชายแดนใต้	ใช้งาน
๕๒	ระบบศูนย์รับเรื่องร้องเรียน	http://www.crm.hss.moph.go.th/	ศูนย์รับเรื่องร้องเรียน	ใช้งาน
๕๓	ระบบแบบประเมินตนเอง	https://access.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๕๔	ระบบศูนย์ Oxygen	http://oxygen.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๕๕	ระบบลงทะเบียนสอบออนไลน์	http://register.hss.moph.go.th/tcm/register	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๕๖	ระบบสารสนเทศงานสุขภาพภาคประชาชน	https://www.thaiphc.net/new๒๐๒๐/	สช	ใช้งาน
๕๗	ระบบสมาชิก อสค.	http://fv.phc.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ/สช	ใช้งาน
๕๘	ระบบตรวจสอบค่ารักษาพยาบาล	http://hospitalprice.net/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๕๙	ระบบศูนย์ปฏิบัติการฉุกเฉินโควิด-๑๙	http://hsscovid.com/	กลุ่มเทคโนโลยีสารสนเทศ/สกพส	ใช้งาน
๖๐	ระบบติดตามแผนงานกองแบบแผน	http://tracking.hss.moph.go.th/	กองแบบแผน	ใช้งาน
๖๑	ระบบประเมินตัวเอง สถานพยาบาล	https://rdumrd.hss.moph.go.th/	สพ.รศ	ใช้งาน
๖๒	ระบบรายงานข้อมูลการปฏิบัติงาน อสม.	http://phccovid.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ/สช	ใช้งาน
๖๓	ระบบตรวจสอบสถานพยาบาลเอกชน	http://privatehospital.hss.moph.go.th/	สพ.รศ	ใช้งาน
๖๔	ระบบทะเบียนแปลนแบบ	https://dcdplan.hss.moph.go.th/newplan/home/index.php	กองแบบแผน	ใช้งาน
๖๕	โปรแกรม DPIS กบค.	http://๒๐๓.๑๕๗.๗.๓๕:๘๐๘๐/admin/index.html	กบค	ใช้งาน
๖๖	ระบบองค์กรเอกชนสาธารณประโยชน์	http://ngo.hss.moph.go.th/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๖๗	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๑	http://do๑.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๖๘	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๒	http://do๒.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๖๙	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๓	http://do๓.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๐	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๔	http://do๔.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๑	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๕	http://do๕.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๒	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๖	http://do๖.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๓	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๗	http://do๗.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๔	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๘	http://do๘.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๕	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๙	http://do๙.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน

รายการระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ (ต่อ)

ลำดับ	ชื่อระบบสารสนเทศ	Domain name	ผู้ดูแล	สถานะ
๗๖	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๑๐	http://do๑๐.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๗	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๑๑	http://do๑๑.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๘	ระบบสปาศูนย์สนับสนุนบริการสุขภาพที่ ๑๒	http://do๑๒.spa.hss.moph.go.th:๑๐๘๑/	กลุ่มเทคโนโลยีสารสนเทศ/กสพส.	ใช้งาน
๗๙	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๑	http://do๑.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๐	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๒	http://do๒.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๑	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๓	http://do๓.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๒	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๔	http://do๔.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๓	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๕	http://do๕.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๔	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๖	http://do๖.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๕	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๗	http://do๗.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๖	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๘	http://do๘.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๗	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๙	http://do๙.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๘	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐	http://do๑๐.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๘๙	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑	http://do๑๑.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๐	ระบบอศค. ศูนย์สนับสนุนบริการสุขภาพที่ ๑๒	http://do๑๒.phc.hss.moph.go.th:๑๐๘๐/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๑	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๑	http://do๑.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๒	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๒	http://do๒.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๓	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๓	http://do๓.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๔	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๔	http://do๔.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๕	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๕	http://do๕.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๖	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๖	http://do๖.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๗	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๗	http://do๗.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๘	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๘	http://do๘.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๙๙	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๙	http://do๙.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๐	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐	http://do๑๐.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน

รายการระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ (ต่อ)

ลำดับ	ชื่อระบบสารสนเทศ	Domain name	ผู้ดูแล	สถานะ
๑๐๑	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑	http://do๑๑.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๒	ระบบตรวจสอบค่ารักษาพยาบาล ศูนย์สนับสนุนบริการสุขภาพที่ ๑๒	http://do๑๒.hp.hss.moph.go.th:๑๐๘๕/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๓	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๑	http://do๑.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๔	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๒	http://do๒.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๕	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๓	http://do๓.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๖	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๔	http://do๔.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๗	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๕	http://do๕.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๘	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๖	http://do๖.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๐๙	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๗	http://do๗.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑๐	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๘	http://do๘.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑๒	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๙	http://do๙.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑๓	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐	http://do๑๐.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑๔	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑	http://do๑๑.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑๕	ระบบบริหารสินทรัพย์ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๒	http://do๑๒.asset.hss.moph.go.th:๑๐๘๓/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑๖	ระบบ อินทราเน็ต กองสุขศึกษา	http://hedintranet.hss.moph.go.th/backend/	กองสุขศึกษา	ใช้งาน
๑๑๗	ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ กรมสนับสนุนบริการสุขภาพ	http://๒๐๓.๑๕๗.๗.๑๒๒/smart_office/	กลุ่มเทคโนโลยีสารสนเทศ	ใช้งาน
๑๑๘	ระบบฐานข้อมูลการให้บริการเกี่ยวกับเทคโนโลยีช่วยการเจริญพันธุ์ทางการแพทย์	https://icmart.hss.moph.go.th/	สพรส	ใช้งาน