แผนการบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ

สำนักงานปลัดกระทรวงสาธารณสุข
ประจำปีงบประมาณ ๒๕๕๗

iCT @MOPH Key of Success
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข

คำนำ

สำนักงานปลัดกระทรวงสาธารณสุข ในฐานะที่เป็นหน่วยงานด้านการควบคุมนโยบาย แผนงาน กำกับ ดูแล ประเมินผล การปฏิบัติงานของหน่วยงานในสังกัดกระทรวงสาธารณสุข ให้ดำเนินงานไปอย่างมีประสิทธิภาพ โดยใช้ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) กระทรวงสาธารณสุข เป็นเครื่องมือขับเคลื่อนและผลักดันการดำเนินงานขององค์กรภายในสังกัด ให้สามารถนำยุทธศาสตร์ไปสู่การปฏิบัติได้อย่างมีประสิทธิภาพ และบรรลุตามเป้าประสงค์ของแผนยุทธศาสตร์การพัฒนาระบบราชการไทย

การนำเทคโนโลยีสารสนเทศ มาใช้สนับสนุนการปฏิบัติงานและให้บริการแก่ประชาชน จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข ประจำปีงบประมาณ พ.ศ. ๒๕๕๗ จึงเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และใช้เป็นแนวทางหรือมาตรการควบคุมป้องกันหรือลดความเสี่ยง เพื่อให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม บุคลากรทุกระดับในสำนักงานปลัดกระทรวงสาธารณสุข จึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ระดับที่สามารถรองรับได้ และทำให้การดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุข บรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น

สำนักงานปลัดกระทรวงสาธารณสุขหวังเป็นอย่างยิ่งว่า แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๕๗ นี้จะช่วยลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลให้กระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุขมีประสิทธิภาพที่ดียิ่งขึ้น

(นายแพทย์สุเทพ วัชรปิยานันทน์)
ผู้ช่วยปลัดกระทรวงสาธารณสุข
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
สำนักงานปลัดกระทรวงสาธารณสุข

๖ สิงหาคม ๒๕๕๗

สารบัญ

หน้า

บทที่ ๑ บทนำ

ยุทธศาสตร์กระทรวงสาธารณสุข พ.ศ. ๒๕๕๗ – ๒๕๖๐ มีเป้าหมายให้ประชาชนทุกคนในเขตเครือข่ายบริการได้รับบริการที่มีคุณภาพมาตรฐานทุกระดับและเข้าถึงเทคโนโลยีที่ทันสมัยในเขตเครือข่ายบริการได้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจึงได้จัดทำแผนบริหารความเสี่ยงขึ้นเพื่อใช้เป็นแนวทางปฏิบัติในการลดความเสียหายต่างๆที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร การบริหารงานจึงต้องมีการดำเนินการตาม IT Governance เพื่อให้เกิดการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศที่ส่งผลต่อการพัฒนาองค์กร

IT Governance คือหน้าที่และความรับผิดชอบในการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศควบคู่กับความสามารถด้านอื่นๆ ของคณะกรรมการและผู้บริหารระดับสูงที่ใช้เป็นกรอบในกระบวนการบริหารงานภายใน การปฏิบัติตามนโยบาย กลยุทธ์เพื่อสร้างศักยภาพ เพิ่มคุณค่าและการเติบโตอย่างยั่งยืนให้กับองค์กร โดยดำเนินการควบคู่ไปกับการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงตามองค์ประกอบของการจัดการด้าน IT เริ่มตั้งแต่การวางแผน การจัดองค์กร พนักงาน การดำเนินการและการควบคุม

IT Governance ทำให้เกิดการบริหารและบูรณาการที่เป็นระบบ ระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน ลดความเสี่ยง เพิ่มศักยภาพ โดยสามารถทำงานข้ามสายงานและประสานงานระหว่างองค์กรได้อย่างรวดเร็ว ทันเวลา มีประสิทธิภาพ สอดประสานกับการดำเนินงานระดับต่างๆ จากการใช้ความสามารถและศักยภาพของเทคโนโลยีสารสนเทศ และทรัพยากรต่างๆ เพื่อผลักดันความสำเร็จของการจัดการองค์กรอย่างทั่วถึงเป็นกระบวนการ

เทคโนโลยีสารสนเทศ สร้างความเสี่ยงใหม่ๆ รวมทั้งการสูญเสียโอกาสที่ส่งผลต่อประสิทธิภาพ ประสิทธิผลในการดำเนินการ นอกจากนี้ยังกระทบต่อความน่าเชื่อถือและความถูกต้องในการตรวจสอบและการจัดทำรายงาน ซึ่งเป็นหัวใจของการบริหารและควบคุมภายในในการบริหารงานระดับต่างๆ ขององค์กร ดังนั้น การผสมผสานความสามารถด้านต่างๆ ขององค์กรกับศักยภาพของระบบงานและการจัดการเทคโนโลยีสารสนเทศที่ดี จึงเป็นทั้งหน้าที่และความรับผิดชอบที่ไม่อาจหลีกเลี่ยงของคณะกรรมการและผู้บริหารระดับสูงขององค์กรในปัจจุบัน

สำนักงานปลัดกระทรวงสาธารณสุขได้นำเทคโนโลยีสารสนเทศเข้ามาใช้ในการปฏิบัติงานหลายด้าน จึงตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเกิดขึ้นในระบบบริหารงาน การสั่งการและการปฏิบัติงานเพื่อการบำบัดทุกข์ บำรุงสุขประชาชนทั่วประเทศ การดำเนินงานดังกล่าวทำให้ข้อมูลและสารสนเทศต่าง ๆ ที่ใช้ในการบริหารงานมีปริมาณที่มากมาย มีความเคลื่อนไหวตลอดเวลา โดยเฉพาะอย่างยิ่งข้อมูลและสารสนเทศที่ใช้ในการให้บริการประชาชนทางด้านสาธารณสุข รวมทั้งข้อมูลและสารสนเทศที่สำนักงานปลัดกระทรวงสาธารณสุขต้องรับผิดชอบกระบวนประมวลผลข้อมูลตามนโยบายสำคัญต่าง ๆ ของรัฐบาล จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้นและเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด สำนักงานปลัดกระทรวงสาธารณสุขจึงได้จัดทำแผนบริหารความเสี่ยงขึ้นเพื่อใช้เป็นแนวทางปฏิบัติ เพื่อลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานของสำนักงานปลัดกระทรวงสาธารณสุข

๑. วัตถุประสงค์

๑.๑ เพื่อให้ฝ่ายบริหาร/ฝ่ายปฏิบัติการของทุกหน่วยงานในสำนักงานปลัดกระทรวงสาธารณสุขเข้าใจหลักการและกระบวนการบริหารความเสี่ยงของสำนักงานปลัดกระทรวงสาธารณสุข

๑.๒ เพื่อให้ผู้ปฏิบัติได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นได้และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้อง

๑.๓ เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๑.๔ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับกลยุทธ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๕ เพื่อใช้เป็นเครื่องมือในการสร้างวัฒนธรรมการบริหารความเสี่ยงในทุก ๆ ระดับของสำนักงานปลัดกระทรวงสาธารณสุข

๒. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุขมีความพร้อมใช้งานตอบสนองความต้องการของบุคลากรในปฏิบัติงานอย่างต่อเนื่อง โดยมีระบบข้อมูลและสารสนเทศ เครื่องมืออุปกรณ์ด้านฮาร์ดแวร์ที่เกี่ยวข้องกับการรวบรวม ประมวล เก็บรักษา และเผยแพร่ข้อมูลและสารสนเทศที่ช่วยในการสื่อสารได้อย่างรวดเร็วและครอบคลุม เช่น ใช้ระบบสารบรรณอิเล็กทรอนิกส์และเว็บไซต์ เผยแพร่และแจ้งเวียนหนังสือ/เอกสารรายงานการประชุม ข้อสั่งการ แผนยุทธศาสตร์และแผนปฏิบัติการต่าง ๆ รายงานผลการดำเนินงานประจำปี มีการใช้ email และ LINE สื่อสารไปยังกลุ่มเป้าหมายเฉพาะ มีการใช้ Facebook และ twitter สื่อสารไปยังผู้ปฏิบัติในทุกระดับ สำหรับประเด็นร้อนและสถานการณ์เร่งด่วน จะใช้ระบบประชุมทางไกล (e-Conference) ทั้ง Skype Web Conference และระบบอุปกรณ์ VDO ซึ่งสื่อสารสองทางได้ชัดเจนและรวดเร็ว ดังเช่น การประชุม War Room ทุกสัปดาห์ (ความถี่ในการประชุมขึ้นอยู่กับความรุนแรงของสถานการณ์ต่าง ๆ) เพื่อบริหารจัดการด้านสุขภาพและสาธารณสุขในสถานการณ์อุทกภัย โรคไข้หวัดใหญ่ โรคคอตีบ และโรคไข้เลือดออกที่ผ่านมา ทำให้ผู้บริหารได้ทราบปัญหาและอุปสรรคในการปฏิบัติงานจากหน่วยงานบริการสาธารณสุขทั่วประเทศ จึงทำให้สามารถตัดสินใจแก้ไขปัญหา มอบนโยบายและสั่งการได้อย่างทันเหตุการณ์ สามารถควบคุมสถานการณ์การวิกฤติต่าง ๆ ได้เป็นอย่างดี มีการจัดโครงสร้างพื้นฐานด้านเครือข่ายเทคโนโลยีสารสนเทศให้บริการแก่บุคลากรผู้ปฏิบัติงานทุกระดับ และเพื่อรองรับการจัดการระบบข้อมูลและสารสนเทศจากหน่วยงานในสังกัด ทั้งส่วนกลาง(LAN/Wireless LAN)และส่วนภูมิภาค(MPLS Network) ครอบคลุมทุกจังหวัด โดยใช้ INTRANET ความเร็ว ๕ Gbps ในการใช้ข้อมูลและสารสนเทศเพื่อการดำเนินงานจากระบบงานภายใน ปีงบประมาณ พ.ศ.๒๕๕๗ จะดำเนินการขยาย Band Width เส้นทางการใช้ Internet สำหรับกรมต่างๆ ขยายเพิ่มเป็น ๖๐๐/๑๐๐ Mbps (ในประเทศ/ต่างประเทศ) และขยาย Band Width เส้นทางการใช้ Internet สำหรับหน่วยงานภายในอาคาร สป. ขยายเพิ่มเป็น ๖๐๐/๑๐๐Mbps (ในประเทศ/ต่างประเทศ)

นอกจากนี้ยังสนับสนุนอุปกรณ์คอมพิวเตอร์สำนักงาน(Hardware) เช่น PC Notebook Printer Scanner และระบบงาน(Software) ที่จำเป็นใช้งานและมีลิขสิทธิ์ถูกกฎหมายให้แก่บุคลากรทุกระดับใช้ปฏิบัติงานและเพิ่มพูนความรู้พัฒนาทักษะของตนเอง สนับสนุน Server ให้แก่หน่วยงานเพื่อรองรับโปรแกรมระบบงานและเว็บไซต์ โดยมีการจัดทำแนวปฏิบัติในการรักษาความมั่นคง

ปลอดภัยด้านสารสนเทศ และ IT Contingency Plan ให้ทุกหน่วยงานในสังกัดถือปฏิบัติเป็นแนวทางเดียวกัน มีการติดตั้งระบบรักษาความปลอดภัย(Network Security System) ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เพื่อให้ข้อมูลและสารสนเทศ Hardware และ Software มีความปลอดภัย นอกจากนี้ยังมีศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทำหน้าที่บำรุงรักษา/เฝ้าระวัง/ตรวจสอบ/ปรับปรุง(Upgrade & Update Patch) เพิ่มประสิทธิภาพการทำงานของ Network System ให้มีความทันสมัยเหมาะสมกับปริมาณความต้องการใช้ข้อมูลและสารสนเทศในปัจจุบัน การ Update ฐานข้อมูลผลสำรวจข้อมูลสารสนเทศด้านเทคโนโลยีสารสนเทศของหน่วยงานสังกัดสำนักงานปลัดกระทรวงสาธารณสุขทุกปี ก็สนับสนุนให้เชื่อถือได้ว่าระบบจัดการข้อมูลและสารสนเทศพร้อมอุปกรณ์ที่เกี่ยวกับสารสนเทศมีความทันสมัย เหมาะสม มีความปลอดภัย และมีคุณภาพพร้อมใช้งานตลอดเวลา ด้วยสำนักงานปลัดกระทรวงสาธารณสุขเป็นองค์กรขนาดใหญ่ที่มีหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค การนำเสนอข้อมูล สารสนเทศ และความรู้จึงใช้เว็บไซต์เป็นส่วนใหญ่ เพื่อให้บุคลากรได้นำไปใช้สนับสนุนการปฏิบัติงานได้ทุกระดับ และเพื่อให้ผู้รับบริการและผู้มีส่วนได้ส่วนเสียรวมทั้งองค์กรอื่นที่เกี่ยวข้องหรือสนใจ มีช่องทางในการค้นหาและเข้าถึงข้อมูลสารสนเทศและความรู้ที่ต้องการได้อย่างสะดวก รวดเร็ว และเว็บไซต์ยังเป็นช่องทางหนึ่งที่ผู้ใช้ข้อมูลสารสนเทศและความรู้จะได้มีส่วนร่วมในการตรวจสอบความถูกต้องของข้อมูล แลกเปลี่ยนข้อมูลซึ่งกันและกัน ทำให้ได้ข้อมูลสารสนเทศและความรู้ที่น่าเชื่อถือ ทันสมัย ครอบคลุมและเชื่อมโยงกับหน่วยงานอื่นที่เกี่ยวข้อง แสดงให้เห็นได้ว่าข้อมูลสารสนเทศและความรู้ของสำนักงานปลัดกระทรวงสาธารณสุขมีความพร้อมใช้และสามารถเข้าถึงได้ตามสิทธิ์

๑.ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software)

ลำดับ	กอง/สำนัก	ชื่อระบบงาน	ผู้รับผิดชอบ	เบอร์โทรศัพท์
๑	สถาบันพระบรมราชชนก	ระบบการจัดการศึกษาสำหรับวิทยาลัยในสังกัด	นส.น้ำฝน เอี่ยมวิริยาวัฒน์	๐๘๗๑๑๐๘๙๖๔
๒		ระบบสารบรรณอิเล็กทรอนิคส์	กลุ่มอำนวยการ	๐๒๕๙๐๑๙๘๑
๓		ระบบบุคลากร	กลุ่มอำนวยการ	๐๒๕๙๐๑๙๘๑
๔		ระบบมาตรฐานการศึกษา	กลุ่มพัฒนาการศึกษา	๐๒๕๙๐๑๘๗๒
๕	กลุ่มประกันสุขภาพ	การบริหารการเงินการคลัง โดยตัวชี้วัด FAI (Financial Administration Index and Uni	นางอมรรัตน์ พีระพล	๐๒๕๙๐๑๗๙๗
๖		การจัดทำต้นทุนของหน่วยบริการ	นางอมรรัตน์ พีระพล	๐๒๕๙๐๑๗๙๗
๗		รายงานการเงินของหน่วยบริการ	นางอมรรัตน์ พีระพล	๐๒๕๙๐๑๗๙๗
๘		กองทุนบุคคลที่มีปัญหาสถาณะและสิทธิ	นางหิรัญญา ปะดุกา	๐๒๕๙๐๑๕๗๗
๙		กองทุนผู้ประกันตนคนต่างด้าว	นางหิรัญญา ปะดุกา	๐๒๕๙๐๑๕๗๗
๑๐		เว็บไซต์กลุ่มประกันสุขภาพ	นางสาวอโณทัย ไชยปาละ	๐๒๕๙๐๒๔๑๘
๑๑		PlanFin	นางอมรรัตน์ พีระพล	๐๒๕๙๐๑๗๙๗

ลำดับ	กอง/สำนัก	ชื่อระบบงาน	ผู้รับผิดชอบ	เบอร์โทรศัพท์
๑๒	กลุ่มประกันสุขภาพ(ต่อ)	ศูนย์บริหารจัดการข้อมูล กลุ่มประกันสุขภาพ สำนักงานปลัดกระทรวงสาธารณสุข	นางสาวศิญาภัสร์ จำรัสอธิวัฒน์	๐๒๕๙๐๑๗๙๗
๑๓		Intranet	นางสาวอโณทัย ไชยปาละ	๐๒๕๙๐๒๔๑๘
๑๔	สำนักการสาธารณสุขระหว่างประเทศ	ระบบฐานข้อมูลความร่วมมือระหว่างประเทศ	นายปวร จงแจ่ม	๐๒๕๙๐๑๙๗๒
๑๕	สำนักสารนิเทศ	website สำนักสารนิเทศ	นาวสาวณัฏฐ์ภัสสร เปรมปรีดิ์	๐๒๕๙๐๑๓๑๓
๑๖	กลุ่มบริหารทั่วไป	การจองห้องประชุม	มัธรี ชูบรรจง	๐๒๕๙๐๑๑๙๖
๑๗		ระบบงานสารบรรณ	นางสาวสุภิสสา วรธนาคม	๐๒๕๙๐๑๑๗๒
๑๘		ระบบงานห้องสมุด	นางมัธรี ชูบรรจง	๐๒๕๙๐๑๓๑๘
๑๙	สำนักบริหารการสาธารณสุข	โปรแกรมงานชันสูตรพลิกศพ	นางกนกนาถ หงส์สกุล	๐๒๕๙๐๑๗๔๑
๒๐		website ของสำนักบริหารการสาธารณสุข	นางจิราพรรณ ลุยะพันธุ์	๐๒๕๙๐๑๗๕๘
๒๑		โปรแกรมพัฒนาดัชนีชี้วัดข้อมูลงานบริการสุขภาพรายบุคคล	นางอรสา เข็มปัญญา	๐๒๕๙๐๑๗๕๘
๒๒		โปรแกรมพัฒนาระบบรายงานข้อมูลสนับสนุนงานทันตสาธารณสุข	ทพ.จารุวัฒน์ บุษราคัมรุหะ	๐๒๕๙๐๑๗๖๒
๒๓		โปรแกรมระบบรายงานเด็กและสตรีที่ถูกกระทำรุนแรง	นางบุญพลอย ตุลาพันธุ์	๐๒๕๙๐๑๗๔๑
๒๔		ระบบรายงานศูนย์ประสิทธิภาพระบบบริการ	นางสุพรรณี มิ่งขวัญ	๒๕๙๐๑๗๕๘
๒๕		โปรแกรมสังคมสงเคราะห์	นางสาวอชิมา วิไลสกุล	๐๒๕๙๐๑๗๔๑
๒๖		โปรแกรมทรัพยากรสุขภาพ	นายจารุวัฒน์ บุษราคัมรุหะ	๐๒๕๙๐๑๗๕๒
๒๗		โปรแกรมระบบรายงานด้านข้อมูลบริหารเวชภัณฑ์ (offline,online)	ภญ.ไพทิพย์ เหลือเรืองรอง	๐๒๕๙๐๑๖๔๑
๒๘	สำนักนโยบายและยุทธศาสตร์	ข้อมูลการบริการทางการแพทย์และสาธารณสุข	นายเผด็จ ชมชื่น	๒๕๘๐๒๔๐๐
๒๙		ข้อมูลการรับบริการทางการแพทย์และสาธารณสุขรายบุคคล	เผด็จ ชมชื่น	๐๒๕๘๐๒๔๐๐
๓๐	สำนักตรวจและประเมินผล	Website สำนักตรวจและประเมินผล	นายถาวร โฮมแพน	๐๒๕๙๐๑๖๗๖

ลำดับ	กอง/สำนัก	ชื่อระบบงาน	ผู้รับผิดชอบ	เบอร์โทรศัพท์
๓๑	ศูนย์เทคโนสารสนเทศและการสื่อสาร	ระบบสมาชิกอินเตอร์เน็ต สธ.	นายชวลิต ลิ้มปิยินทรากูล	๐๒๕๙๐๑๒๐๑
๓๒		ระบบติดตามโครงการจัดหาคอมพิวเตอร์ปี ๕๗	นายราชิ ปาลือชา	๐๒๕๙๐๑๒๑๓
๓๓		ระบบสมาชิกอินเตอร์เน็ต สธ.	นายชวลิต ลิ้มปิยินทรากูล	๐๒๕๙๐๑๒๐๑
๓๔		ระบบขอใช้รถยนต์ส่วนกลาง ศทส.	นางปัทมา มโนมัธย์	๐๒๕๙๐๑๑๖๙
๓๕		ระบบร้องเรียนร้องทุกข์ ศทส.	นางปัทมา มโนมัธย์	๐๒๕๙๐๑๒๐๔
๓๖		ระบบข้อมูลแผนการฝึกอบรม	นางปัทมา มโนมัธย์	๐๒๕๙๐๑๒๐๗
๓๗		เว็บไซต์กระทรวงสาธารณสุข	นายชวลิต ลิ้มปิยินทรากูล	๐๒๕๙๐๑๒๐๑
๓๘		เว็บไซต์สำนักงานปลัดกระทรวงสาธารณสุข	นส.หทัยทิพย์ พรหมมาศ	๐๒๕๙๐๑๒๐๐
๓๙		เว็บไซต์ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	นางสาวจิลาวัลย์ มีสังข์	๐๒๕๙๐๑๒๐๗
๔๐		ระบบวันลาออนไลน์	นายพิษณุเดช ปักกุนนัน	๐๒๕๙๐๑๒๐๙
๔๑		ระบบลงทะเบียนออนไลน์	น.ส.หทัยทิพย์ พรหมมาศ	๐๒๕๙๐๑๑๖๗
๔๒		รายงานผลจัดหาระบบคอมพิวเตอร์ รพ.สต. ตามแผนปฏิบัติการไทยเข้มแข็ง ๒๕๕๕	นายราชิ ปาลือชา	๐๒๕๙๐๑๑๖๙
๔๓	กลุ่มบริหารงานบุคคล	PIS (ส่วนภูมิภาค)	นางสินีนาฏ พรัดมะลิ	๐๒๕๙๐๑๒๐๙ / ๑๔๔๘
๔๔		ระบบ GIS (ระบบภูมิศาสตร์สารสนเทศด้านกำลังคน)	นางสินีนาฏ พรัดมะลิ	๐๒๕๙๐๑๒๐๙
๔๕		ระบบ HR (ส่วนกลาง)	นางมัธยัสถ์ เหล่าสุรสุนทร	๐๒๕๙๐๑๓๕๖ / ๑๔๔๘
๔๖		ระบบจัดสรรนักเรียนทุนรัฐบาลแพทย์/ทันตแพทย์/เภสัชกร	นางกนกวรรณ มาป้อง	๐๒๕๙๐๑๒๐๔
๔๗		ระบบย้ายหมุนเวียน แพทย์/ทันตแพทย์/เภสัชกร	น.ส.จริยา มอบนรินทร์	๐๒๕๙๐๑๒๐๔
๔๘		ระบบข้อมูลลูกจ้างชั่วคราว	น.ส.อุจนีย์ พรชัยสุขศิริ	๐๒๕๙๐๑๒๐๙ / ๑๓๕๐
๔๙	สำนักสาธารณสุขฉุกเฉิน	ข้อมูลรถพยาบาลของโรงพยาบาลในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข	รสสุคนธ์ กิ่งอุบล	๐๒๕๙๐ ๑๘๕๑

๒.ระบบเครือข่าย

ในช่วงที่ผ่านมากระทรวงสาธารณสุข กระทรวงสาธารณสุขได้มีการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศ กระทรวงสาธารณสุขมาแล้วหลายฉบับ ทุกฉบับได้วางแนวทางการพัฒนาโครงสร้างพื้นฐานด้านเครือข่ายคอมพิวเตอร์ไว้อย่างดี โดยเน้นให้ทุกหน่วยงานต้องมีระบบเครือข่ายคอมพิวเตอร์ (LAN) และเชื่อมต่อมายังส่วนกลางเพื่อให้เกิดระบบเครือข่ายอินทราเน็ต กระทรวงสาธารณสุข เพื่อใช้ในการแลกเปลี่ยนข้อมูลข่าวสารและการค้นหาความรู้ในโลกของอินเตอร์เน็ต แต่ในทางปฏิบัติแล้วไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพมากนักอันเนื่องมาจากโครงการต่างๆ ในการพัฒนาเครือข่ายคอมพิวเตอร์จำเป็นต้องใช้เงินลงทุนด้าน Hardware Software และโครงข่ายด้านสาธารณูปโภค เป็นจำนวนมากซึ่งปีใดได้งบประมาณมาอย่างเพียงพอ การพัฒนาเครือข่ายก็สามารถทำได้ตรงตามเป้าหมายที่ต้องการ ปีใดที่ได้รับงบประมาณไม่เพียงพอ การพัฒนาก็ต้องหยุดชะงัก

อย่างไรก็ตาม การพัฒนาเครือข่ายคอมพิวเตอร์ของกระทรวงสาธารณสุขก็ได้รับความสำเร็จมาระดับหนึ่ง ปัจจุบันมีขนาดที่ใหญ่ขึ้นกว่าเดิมหลายสิบเท่า ระบบเครือข่ายมีความซับซ้อนมากขึ้น การพัฒนาระบบเครือข่ายในแบบเดิม ๆ ที่ใช้วิธีเติมทีละส่วน ตามงบประมาณที่ได้รับในแต่ละปี จะเป็นอุปสรรคอย่างมากต่อการขยายเครือข่ายที่มีขนาดใหญ่ในอนาคต ประกอบกับความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีสารสนเทศ ทำให้ระบบเครือข่ายคอมพิวเตอร์เดิมไม่สามารถรองรับเทคโนโลยีใหม่ ๆ ได้ ปริมาณความต้องการใช้งานและระบบงานต่าง ๆที่เปลี่ยนไปใช้เทคโนโลยีทางด้าน Web base และ Multimedia ซึ่งต้องใช้ Bandwidth ขนาดใหญ่และความเร็วในการ Access ข้อมูล รวมทั้งระบบความปลอดภัยบนเครือข่าย ก็จะต้องเป็นสิ่งที่ต้องคำนึงถึงในการพัฒนาระบบเครือข่ายกลางของกระทรวงสาธารณสุขในระยะต่อ ๆ ไป

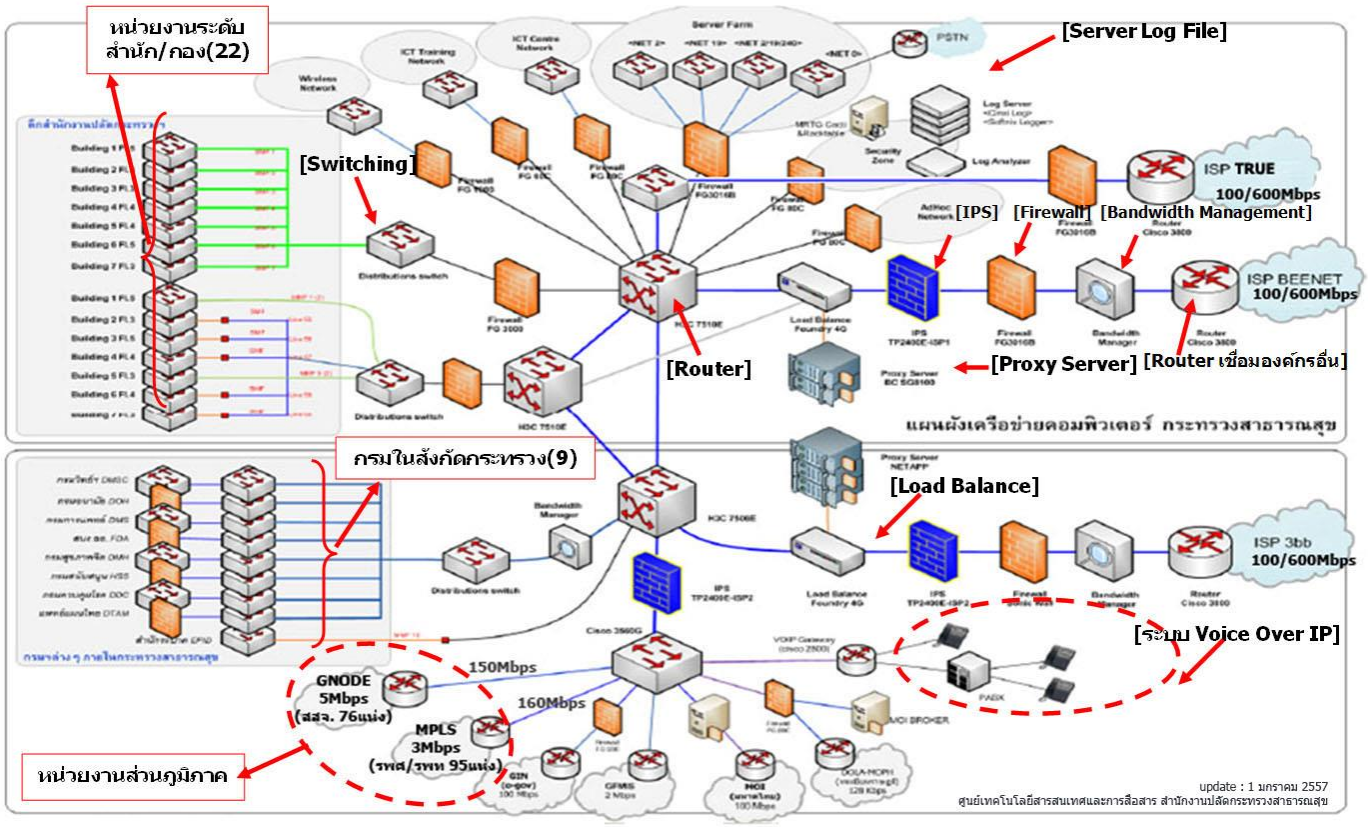
การศึกษาวิเคราะห์ระบบเครือข่ายให้เห็นปัญหา จุดอ่อน และจุดแข็งของระบบเครือข่ายที่เป็นอยู่ เพื่อจะได้เป็นข้อมูลในการออกแบบระบบเครือข่ายใหม่ที่มีประสิทธิภาพมีความปลอดภัยมากขึ้นกว่าเดิมรวมทั้งมีมาตรการรักษาความปลอดภัยและการบริหารความเสี่ยงที่มีประสิทธิภาพสามารถรองรับการขยายเครือข่ายคอมพิวเตอร์ของกระทรวงได้ในอนาคต

ลักษณะทั่วไปของระบบเครือข่ายของหน่วยงานต่าง ๆ ภายในกระทรวงสาธารณสุข จัดทำเป็นแผนภาพดังปรากฏในรูปภาพที่ ๑ พบว่าระบบเครือข่ายกลางของกระทรวงสาธารณสุขมีการเลือกใช้เทคโนโลยีการเชื่อมต่อที่มีความหลากหลาย และเลือกใช้ให้เหมาะกับสภาพพื้นที่ของหน่วยงาน และเงินงบประมาณที่ได้รับอย่างจำกัด ซึ่งสามารถจำแนกออกเป็น ๔ เครือข่ายหลัก ๆ ได้แก่ เครือข่ายในส่วนกลาง เครือข่ายในส่วนภูมิภาค เครือข่ายอินเตอร์เน็ต และเครือข่ายต่างกระทรวง

การออกแบบสถาปัตยกรรมของระบบเครือข่ายกลาง (Backbone) กระทรวงสาธารณสุข ในการออกแบบระบบเครือข่าย Backbone กระทรวงสาธารณสุข คำนึงถึงหลักการออกแบบ ดังนี้

- Reliability ต้องการให้ระบบเครือข่ายมีความน่าเชื่อถือได้มากที่สุด โดยพยายามลดจุดที่เสี่ยงต่อการทำให้ระบบล่มสลาย (Single point of failure)
- Scalability ต้องการให้ระบบสามารถรองรับต่อการขยายขนาดของระบบในอนาคตได้
- Manageability ต้องการให้ระบบง่ายต่อการบริหารและจัดการนอกจากนี้ยังต้องคำนึงถึงความปลอดภัยบนระบบเครือข่าย แนวทางการจัดการไวรัส availability บนเครือข่าย

ประสิทธิภาพบนเครือข่าย การจัดการ IP routing และ addressing, แผนการในการทำงานของ



เครือข่ายใหม่ และงบประมาณโดยประมาณในการสร้างเครือข่ายใหม่ก็ล้วนเป็นกุญแจสำคัญ

รูปภาพที่ ๑ แสดงผังระบบเครือข่ายกระทรวงสาธารณสุข

๓. นโยบายการบริหารความเสี่ยง

เพื่อสร้างความตระหนักและกระตุ้นให้ข้าราชการในสำนักงานปลัดกระทรวงสาธารณสุขเห็นถึงความจำเป็นในการระมัดระวังต่อสถานการณ์ที่คุกคามต่อประสิทธิภาพการปฏิบัติงาน การบริหารงานและอาจทำให้เกิดความเสียหายต่อระบบฐานข้อมูลสารสนเทศซึ่งเป็นเครื่องมือที่สำคัญที่สุดในการให้บริการประชาชนและการตัดสินใจของผู้บริหารสำนักงานปลัดกระทรวงสาธารณสุขตลอดจนคณะรัฐบาล ผู้บริหารประเทศ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข จะทำให้เจ้าหน้าที่ทุกคนที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ ซึ่งจะถือเป็นส่วนหนึ่งของการดำเนินงาน การปฏิบัติงานเพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายต่าง ๆ ที่อาจเกิดขึ้นต่อระบบปฏิบัติราชการของสำนักงานปลัดกระทรวงสาธารณสุข

ซึ่งการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารให้มีประสิทธิภาพนั้นสำนักงานปลัดกระทรวงสาธารณสุขใช้นโยบายความมั่นคงและปลอดภัยของระบบ ICT สป. ที่ได้รับการอนุมัติจาก CIO มี Acceptable Use Policy - Wireless Policy - Firewall Policy - E-mail Policy - Internet Security Policy - Access control Policy - IDS/IPS Policy (Intrusion Detection System/Intrusion Prevention System) มีแผนรักษาความมั่นคงและ

ปลอดภัยของระบบ ICT ของสป. มีคู่มือการปฏิบัติและแนวทางการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และมีระบบ Access Right ที่ถูกต้องและทันสมัย

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๓.๑ ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้สำนักงานปลัดกระทรวงสาธารณสุขไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อระบบเทคโนโลยีสารสนเทศที่สำนักงานปลัดกระทรวงสาธารณสุขใช้ในการบริหารงานและปฏิบัติการโดยเฉพาะอย่างยิ่งการบริการประชาชน

๓.๒ การควบคุม (Control) หมายถึง ขั้นตอนการปฏิบัติ กระบวนการดำเนินงานหรือกลไกการปฏิบัติงาน ซึ่งสำนักงานปลัดกระทรวงสาธารณสุขกำหนดขึ้นเพื่อให้มั่นใจว่าการบริหารงานจะสามารถบรรลุวัตถุประสงค์ที่ได้กำหนดไว้

๓.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ ประเมิน จัดการและติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหน่วยงาน หรือกระบวนการดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุข รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้

๓.๔ การบริหารความเสี่ยงสำนักงานปลัดกระทรวงสาธารณสุขโดยรวม (Organization Wide Risk Management) หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการปฏิบัติงานต่าง ๆ โดยต้องลดมูลเหตุของแต่ละโอกาสที่จะทำให้สำนักงานปลัดกระทรวงสาธารณสุขเสียหาย

๓.๕ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ระบบเครือข่ายคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์ ระบบเครื่องสื่อสาร ระบบฐานข้อมูล และอุปกรณ์ประกอบระบบต่าง ๆ รวมทั้งอาคารสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด

๓.๖ ฐานข้อมูลสารสนเทศ หมายถึง ฐานข้อมูลที่สำนักงานปลัดกระทรวงสาธารณสุขใช้ในการปฏิบัติหน้าที่ซึ่งประกอบด้วย

๓.๖.๑ ฐานข้อมูลเพื่อการบริการประชาชน

๓.๖.๒ ฐานข้อมูลเพื่อการบริหารงานภายใน

๓.๗ องค์ประกอบของความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓.๗.๑ ความน่าจะเป็น โอกาส หรือ ความไม่แน่นอน

๓.๗.๒ ผู้กระทำ (อาจเป็นได้ทั้งคน และที่ไม่ใช่คน เช่น อุบัติเหตุ ไฟฟ้าดับ ภัยธรรมชาติ)

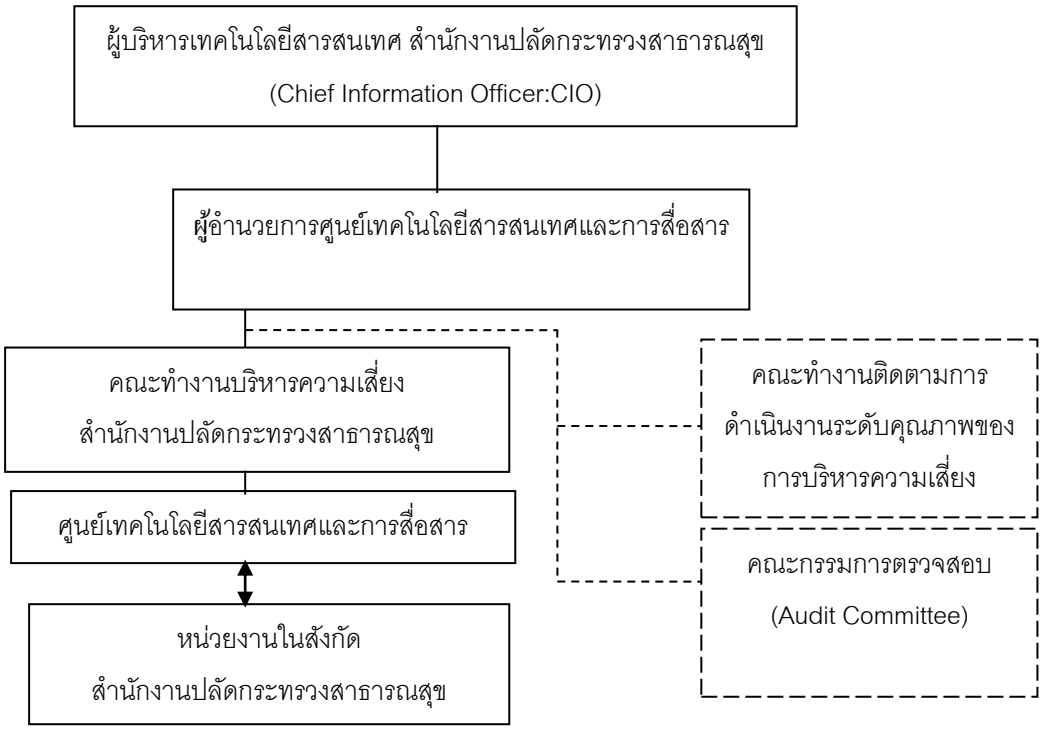
๓.๗.๓ การกระทำ (ถ้าผู้กระทำเป็นคนส่วนนี้จะเป็นการกระทำ ถ้าผู้กระทำไม่ใช่คน ส่วนนี้จะเป็นการเกิดของเหตุการณ์)

๓.๗.๔ ผ่านช่องทางที่มี

๓.๗.๕ ผลกระทบกับวัตถุประสงค์, ภารกิจ, สถานะ หรือ ความสำเร็จ ขององค์กรหรือบุคคล

๕. โครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข

๕.๑ คณะทำงานบริหารความเสี่ยง สำนักงานปลัดกระทรวงสาธารณสุข



<u>คำอธิบาย</u>

ใช้คำสั่งสำนักงานปลัดกระทรวงสาธารณสุขที่ ๖๔๘ /๒๕๕๗ เรื่อง แต่งตั้งคณะทำงานพัฒนาปรับปรุงสารสนเทศส่วนกลางของสำนักงานปลัดกระทรวงสาธารณสุข ประจำปีงบประมาณ พ.ศ.๒๕๕๗ สั่ง ณ วันที่ ๑๘ มีนาคม พ.ศ.๒๕๕๗ ลงนามโดย นายสุเทพ วัชรปิยานันทน์ ผู้ช่วยปลัดกระทรวงสาธารณสุข

<u>อำนาจหน้าที่</u>

๑. ถ่ายทอดแนวทางปฏิบัติ รณรงค์ และกระตุ้นเตือนให้บุคลากรในหน่วยงาน มีความรู้ความเข้าใจ และปฏิบัติตามกฎ ระเบียบด้านการรักษาความปลอดภัยของระบบสารสนเทศอย่างเคร่งครัด

๒. ดำเนินการให้หน่วยงานมีระบบฐานข้อมูลที่สนับสนุนการปฏิบัติงานตามภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ และระบบเครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงสาธารณสุขมีความมั่นคงปลอดภัย

๓. ติดตาม ควบคุมกำกับการดำเนินงานตัวชี้วัดระดับความสำเร็จของการพัฒนาสมรรถนะองค์การด้านทุนสารสนเทศ (IT) ของหน่วยงาน และการพัฒนาประสิทธิภาพระบบสารสนเทศภาครัฐของสำนักงานปลัดกระทรวงสาธารณสุข

๔. รายงานผลการดำเนินงานและข้อเสนอแนะแนวทางแก้ไขปัญหา

๕. ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

โดยมีหน้าที่และความรับผิดชอบในการวางระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศดังต่อไปนี้

๑. กำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อเสนอต่อคณะกรรมการ บริหารความเสี่ยงระดับยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข

๒. วางกลยุทธ์การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายการบริหารความเสี่ยงระดับยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข

๓. พิจารณากรอบแนวทางของระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (วัด ประเมิน ตรวจสอบและควบคุม) ให้สอดคล้องกับแนวทางการดำเนินงานการพัฒนาคุณภาพการบริหารจัดการภาครัฐ

๔. ดูแล ตรวจสอบ ติดตามกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข

๕. จัดทำรายงานความก้าวหน้าในการจัดวางระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อรวบรวมเสนอคณะกรรมการบริหารความเสี่ยงระดับยุทธศาสตร์ ของสำนักงานปลัดกระทรวงสาธารณสุข

๗. นำระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุขที่กำหนดไว้ไปปฏิบัติ โดยกำหนดเป็นนโยบาย วิธีการ แนวทางปฏิบัติงาน หรือระเบียบปฏิบัติ

คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

<u>อำนาจหน้าที่</u>

๑. ถ่ายทอดแนวทางปฏิบัติ รณรงค์ และกระตุ้นเตือนให้บุคลากรในหน่วยงาน มีความรู้ความเข้าใจ และปฏิบัติตามกฎ ระเบียบด้านการรักษาความปลอดภัยของระบบสารสนเทศอย่างเคร่งครัด

๒. ดำเนินการให้หน่วยงานมีระบบฐานข้อมูลที่สนับสนุนการปฏิบัติงานตามภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ และระบบเครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงธารณสุขมีความมั่นคงปลอดภัย

๓. ติดตาม ควบคุมกำกับการดำเนินงานตัวชี้วัดระดับความสำเร็จของการพัฒนาสมรรถนะองค์การด้านทุนสารสนเทศ (IT) ของหน่วยงาน และการพัฒนาประสิทธิภาพระบบสารสนเทศภาครัฐของสำนักงานปลัดกระทรวงสาธารณสุข

๔. รายงานผลการดำเนินงานและข้อเสนอแนะแนวทางแก้ไขปัญหา

๕. ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

๖. การกำหนดเกณฑ์การประเมินความเสี่ยง

๑. การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิญปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒. การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัย

เสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับความรุนแรงของผลกระทบ เชิงปริมาณ(ในแง่ของงบประมาณ)

ผลกระทบ	ความสูญเสีย	ระดับ
สูงมาก	> ๑๐ ล้าน	๕
สูง	> ๒.๕ แสนบาท – ๑๐ ล้าน	๔
ปานกลาง	> ๕๐,๐๐๐-๒.๕ แสนบาท	๓
น้อย	> ๑๐,๐๐๐-๕๐,๐๐๐ บาท	๒
น้อยมาก	ไม่เกิน ๑๐,๐๐๐ บาท	๑

ระดับของความรุนแรง (ผลกระทบของความเสี่ยงต่อชื่อเสียงขององค์กร)

ระดับของความรุนแรง	ผลกระทบของความเสียหาย	คะแนน
สูงมาก	มีการพาดหัวข่าวทั้งจากสื่อภายในและต่างประเทศ	๕
สูง	มีการเผยแพร่ข่าวในวงกว้างสำหรับสื่อภายในประเทศและมีการเผยแพร่ข่าวในวงจำกัดของสื่อต่างประเทศ	๔
ปานกลาง	มีการเผยแพร่ข่าวในหนังสือพิมพ์ภายในประเทศหลายฉบับ (๒-๕ วัน)	๓
น้อย	มีการเผยแพร่ข่าวในวงจำกัดภายในประเทศ (๑ วัน)	๒
น้อยมาก	ไม่มีการเผยแพร่ข่าว	๑

ระดับของความรุนแรง (ผลกระทบของความเสี่ยงต่อระบบเทคโนโลยีและสารสนเทศ)

ระดับของความรุนแรง	ผลกระทบของความเสียหาย	คะแนน
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลลูกค้าหรือข้อมูลธุรกิจ	๕
สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน	๔
ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก	๓
น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้	๒
น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ	๑

ระดับของความรุนแรง (ผลกระทบของความเสี่ยงต่อการต่อเนื่องของการดำเนินงาน)

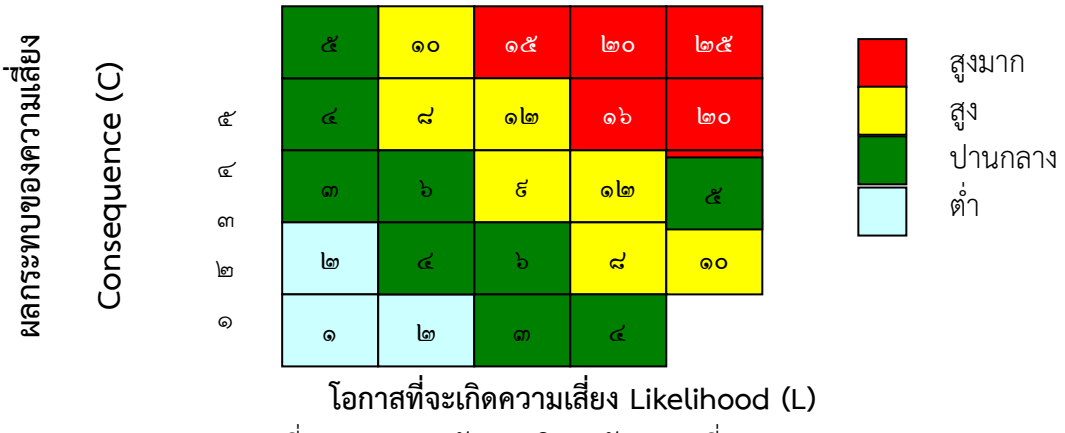
ระดับของความรุนแรง	มูลค่าความเสียหาย	คะแนน
สูงมาก	การหยุดดำเนินการขององค์กรและกระบวนการ เป็นเวลา ๒ เดือน	๕
สูง	มีผลกระทบต่อกระบวนการและการดำเนินงานขององค์กรอย่างรุณแรง เช่น การหยุดดำเนินงาน ๑ เดือน	๔
ปานกลาง	มีการชะงักงันอย่างมีนัยสำคัญของกระบวนการและการดำเนินงานขององค์กร	๓
น้อย	มีผลกระทบเล็กน้อยต่อกระบวนการและการดำเนินงานขององค์กร	๒
น้อยมาก	ไม่มีการชะงักงันของกระบวนการและการดำเนินงานขององค์กร	๑

หมายเหตุ : ผลกระทบของความเสียหาย เป็นเพียงตัวอย่างการนำไปใช้ ควรมีการกำหนดให้เหมาะสมกับขนาดภารกิจและลักษณะการดำเนินงานขององค์กร

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง เป็นดังนี้

โอกาสที่จะเกิดความเสี่ยง	**ความถี่โดยเฉลี่ย**	**ระดับ**
สูงมาก	มีโอกาสเกิดเกือบทุกครั้ง (๑ เดือนต่อครั้งหรือมากกว่า)	๕
สูง	มีโอกาสเกิดค่อนข้างสูงหรือบ่อย ๆ (๑-๖ เดือนต่อครั้งแต่ไม่เกิน ๕ ครั้ง)	๔
ปานกลาง	มีโอกาสเกิดบางครั้ง (๑ ปีต่อครั้ง)	๓
น้อย	อาจมีโอกาสเกิด แต่นาน ๆ ครั้ง (๒-๓ ปีต่อครั้ง)	๒
น้อยมาก	มีโอกาสเกิดน้อยมาก หรือไม่น่าเกิด (๕ ปีต่อครั้ง)	๑

๓. การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังแผนผังประเมินระดับความเสี่ยงรูปที่ ๒



รูปที่ ๒ แสดงแผนผังประเมินระดับความเสี่ยง

ระดับความเสี่ยง หมายถึงโอกาสในการเกิดความเสี่ยง X ความรุนแรงของผลกระทบ โดยแบ่งพื้นที่ออกเป็น ๔ ส่วน ดังนี้

ก. ระดับความเสี่ยงต่ำ คะแนนระดับความเสี่ยง ๑ - ๒ หมายถึงว่าความเสี่ยงที่เกิดมีโอกาสเกิดขึ้นน้อย หากเกิดขึ้นแล้วส่งผลกระทบต่อองค์กรต่ำ เราสามารถที่จะยอมรับความเสี่ยงนั้น กำหนดเป็นสีฟ้า

ข. ระดับความเสี่ยงปานกลาง คะแนนระดับความเสี่ยง ๓ - ๖ หมายถึงว่าความเสี่ยงนั้นมีโอกาสเกิดขึ้นบ้าง หากเกิดขึ้นแล้วส่งผลกระทบต่อองค์กรไม่มากนัก เราสามารถที่จะยอมรับความเสี่ยงนั้น แต่ต้องมีแผนควบคุมความเสี่ยง กำหนดเป็นเขียว

ค. ระดับความเสี่ยงสูง คะแนนระดับความเสี่ยง ๕ – ๑๒ หมายถึงว่าความเสี่ยงนั้นมีโอกาสเกิดขึ้นมาก หากเกิดขึ้นแล้วส่งผลกระทบต่อองค์กรแม้ไม่มากนักก็จัดได้ว่ามีความเสี่ยงสูงในขณะเดียวกันแม้โอกาสที่จะเกิดขึ้นน้อย แต่หากเกิดขึ้นแล้วส่งผลกระทบมาก ก็ถือว่าเสี่ยงสูง เราไม่สามารถที่จะยอมรับความเสี่ยงนั้นได้ จำเป็นต้องมีแผนควบคุมความเสี่ยง กำหนดเป็นเหลือง

ง. ระดับความเสี่ยงสูงมาก คะแนนระดับความเสี่ยง ๑๕ – ๒๕ หมายถึงว่าความเสี่ยงนั้นมีโอกาสเกิดขึ้นมากที่สุด หากเกิดขึ้นแล้วส่งผลกระทบต่อองค์กรในระดับสูง เราไม่สามารถที่จะยอมรับความเสี่ยงนั้นได้ จำเป็นต้องมีแผนควบคุมความเสี่ยงกำหนดเป็นแดง

ขั้นที่ ๔ ระบุและจัดลำดับความเสี่ยง

- ประเมินความเสี่ยง

ขั้นที่ ๕ วางแผนการรับมือกับความเสี่ยง

๕.๑ สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง

๕.๒ แนวทางในการจัดการ/ควบคุมความเสี่ยง

ขั้นที่ ๖ รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง

- การติดตามกิจกรรมการจัดการความเสี่ยง
- การประเมินผลการจัดการความเสี่ยง
- สรุปผลการดำเนินงานจากการบริหารความเสี่ยง

บทที่ ๒ การบริหารความเสี่ยง

ขั้นที่ ๑ การเตรียมการและวางแผน

ขั้น๑.๑ กำหนดความเสี่ยงที่มีโอกาสเกิดขึ้นต่อวัตถุประสงค์ ภารกิจ ความสำเร็จ

สำนักงานปลัดกระทรวงสาธารณสุข เป็นองค์กรที่เป็นเลิศด้านการบริหาร บริการ และวิชาการ ทางการแพทย์และสาธารณสุขที่มีมาตรฐาน ครอบคลุมและเป็นธรรม เพื่อคนไทยสุขภาพดี มีพันธกิจพัฒนาระบบบริหารจัดการตามหลักธรรมาภิบาล พัฒนาระบบบริการทางการแพทย์และสาธารณสุขให้มีคุณภาพและมาตรฐาน พัฒนาระบบการจัดการความรู้ทางการแพทย์และสาธารณสุขให้มีประสิทธิภาพ ซึ่งระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญที่จะช่วยสนับสนุนให้พันธกิจของสำนักงานปลัดกระทรวงสาธารณสุขไปถึงเป้าหมายบริการได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ ภารกิจ ความสำเร็จด้านเทคโนโลยีสารสนเทศและการสื่อสาร	ความเสียหายที่ยอมรับได้
๑. พัฒนาการเชื่อมโยงเครือข่ายระบบสาธารณสุข	การเชื่อมโยงเครือข่ายระหว่างกรมไม่สามารถดำเนินการได้ ๑ กรม
๒. ให้ความสำคัญกับระบบความปลอดภัยด้าน ICT	ระยะเวลา Downtime ของระบบเครือข่ายไม่เกินร้อยละ ๕ ของเวลาทั้งปี (นาที)
๓. ความมีประสิทธิภาพของระบบเทคโนโลยีสารสนเทศสุขภาพ (ระบบงานและข้อมูล (System &Information)	ร้อยละไม่ต่ำกว่า ๕๐ ของหน่วยงานระดับจังหวัดใช้ระบบเทคโนโลยีสารสนเทศสุขภาพที่สำนักงานปลัดกระทรวงสาธารณสุขได้พัฒนาขึ้น
๔. ผู้รับบริการมีความพึงพอใจต่อบริการด้าน ICT	ร้อยละของระดับความพึงพอใจของผู้ใช้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ลดลงจากเดิมไม่เกิน ๒๐ %

สถานะ ชื่อเสียงขององค์กร	ความเสียหายที่ยอมรับได้
๑. ความเชื่อมั่นของประชาชนผู้ใช้บริการฯ	๑. จำนวนผู้ใช้บริการระบบเทคโนโลยีสารสนเทศสำนักงานปลัดกระทรวงสาธารณสุข ไม่เพิ่มขึ้นจากเดิมแต่ไม่ลดลงจากเดิม ๒. ผู้บริหารเรียกให้ชี้แจงข้อมูล
๒. ความเชื่อมั่นต่อบริการด้านเทคโนโลยีและการสื่อสารของหน่วยงานในส่วนภูมิภาค	๑. การส่งรายงานของระบบรายงานต่าง ๆ จากหน่วยงานส่วนภูมิภาคลดลงจากเดิมไม่เกิน ๒๐ % ๒. หน่วยงานในส่วนภูมิภาค มีความคลางแคลงใจ โดยการสอบถามข้อมูลผ่านโทรศัพท์หรือทางอีเมล์เป็นจำนวนมาก
๓. ความเชื่อมั่นต่อบริการด้านเทคโนโลยีและการสื่อสารของหน่วยงานในส่วนกลาง	๑. หน่วยงานในส่วนกลางมีการสอบถามข้อเท็จจริงที่เกิดขึ้น แต่ยังใช้บริการอยู่เช่นเดิม

ขั้น ๑.๒

วิเคราะห์ปัญหาหรือโอกาสในองค์กร

ปัญหาหรือโอกาสในการบริหารความเสี่ยงของสำนักงานปลัดกระทรวงสาธารณสุข

โอกาส – สิ่งที่จะมีส่วนช่วยให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ
ปัจจัยแห่งความสำเร็จ (Key Success Factors) เพื่อให้การดำเนินการตามกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุขบรรลุผลตามเป้าหมาย สามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม คือ **๑. ปัจจัยด้านอุปกรณ์ (Hardware)** (๑) พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนการพัฒนาระบบสุขภาพของประเทศ (๒) มีเครื่องมือในการเก็บรวบรวมข้อมูลที่มีประสิทธิภาพ สามารถเก็บรวบรวมข้อมูลได้ครบถ้วนมีคุณภาพตอบสนองความต้องการในการให้บริการสาธารณสุข และด้านบริหารจัดการของผู้บริหาร **๒. ปัจจัยด้านซอฟต์แวร์(Software)** (๑) สร้างเสริมนวัตกรรมบริการและการวิจัยระบบ เครื่องมือและอุปกรณ์เพื่อเพิ่มประสิทธิภาพระบบบริการสาธารณสุข (๒) ประยุกต์ใช้เทคโนโลยีในการในกระบวนการจัดการและการให้บริการสาธารณสุข (๓) พัฒนาระบบเทคโนโลยีสารสนเทศการจัดการความรู้ด้านการแพทย์และสุขภาพสำหรับประชาชน (๔) พัฒนามาตรฐานในด้านการเชื่อมโยงแลกเปลี่ยนข้อมูล (Standard and Interoperability) **๓. ปัจจัยด้านโครงข่ายเทคโนโลยีสารสนเทศ (ICT)** (๑) สถานบริการสาธารณสุขทุกแห่งทั่วประเทศสามารถเข้าถึงบริการอินเตอร์เน็ตความเร็วสูงหรือการสื่อสารรูปแบบอื่นที่เป็น Broadband ได้อย่างทั่วถึง สะดวกและรวดเร็วโดยปลอดภัย (๒) ระบบ ICT ของกระทรวงสาธารณสุขมีความทันสมัย รวดเร็วทันต่อความก้าวหน้าของเทคโนโลยีและความเปลี่ยนแปลงของสังคมโลก สามารถรองรับกับการขยายตัวของการให้บริการและ (๓) โครงข่าย ICT ของกระทรวงสาธารณสุขมีศักยภาพพัฒนาไปสู่โครงข่ายสมัยใหม่ (Next Generation Network : NGN) ที่สามารถบูรณาการการใช้งานร่วมกันได้อย่างทั่วถึง (๔) ใช้เทคโนโลยีการออกแบบสถาปัตยกรรมโปรแกรมระบบงานที่ทันสมัย มีความยืดหยุ่นในการเปลี่ยนแปลง ง่ายต่อการดูแลบำรุงรักษาโดยเจ้าหน้าที่ของหน่วยงาน **๔. ปัจจัยด้านบุคลากร** - **<u>ผู้บริหารองค์กร</u>** (๑) ผู้บริหารมีวิสัยทัศน์ ให้ความสำคัญ สนับสนุนและส่งเสริมการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการพัฒนาองค์กรรวมทั้งให้ความสำคัญต่อการบริหารความ

โอกาส – สิ่งที่จะมีส่วนช่วยให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ
เสี่ยงของระบบเทคโนโลยีสารสนเทศ - **ผู้ใช้งาน** (๒) บุคลากรผู้ใช้งานส่วนใหญ่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศในระดับที่ใช้งานได้บุคลากรผู้ใช้งานมีความสนใจ และกระตือรือร้นในการใช้เทคโนโลยีสารสนเทศช่วยในการปฏิบัติงาน (๑) บุคลากรทุกคนสามารถใช้ E-mail, Internet และ Intranet ในการประสานงานและสืบค้นข้อมูลเพื่อปฏิบัติงานในภารกิจได้อย่างมีประสิทธิภาพ (๒) บุคลากรทุกคนเห็นความสำคัญและให้ความร่วมมือในการปฏิบัติตามแผนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ - **ผู้ปฏิบัติงานด้าน ICT** (๑) ผู้ปฏิบัติงานด้าน ICT ส่วนใหญ่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศในระดับที่ใช้งานได้ (๒) ผู้ปฏิบัติงานด้าน ICT มีความสนใจ และกระตือรือล้นในการใช้เทคโนโลยีสารสนเทศช่วยในการปฏิบัติงาน (๓) ผู้ปฏิบัติงานด้าน ICT ให้ความร่วมมือในการปฏิบัติตามแผนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ **๕. ปัจจัยด้านข้อมูลสารสนเทศ** (๑) พัฒนาระบบข้อมูลข่าวสารสุขภาพ มีคลังข้อมูล (Data Center) ซึ่งรวบรวมข้อมูลข่าวสารสุขภาพในระดับจังหวัดและส่วนกลาง โดยเป็นข้อมูลที่สามารถนำไปใช้ประโยชน์ได้จริง ข้อมูลสามารถเชื่อมโยงและแลกเปลี่ยนกันได้ ประชาชนสามารถเข้าถึงข้อมูลสุขภาพของตนได้จากทุกแห่งและทุกเวลา (๒) มีการพัฒนารูปแบบการให้บริการข้อมูลขององค์กรในลักษณะสื่อสองทาง (Interactive) และส่งเสริมการมีส่วนร่วมของภาคประชาชน และบุคลากรผ่านระบบอินเทอร์เน็ต (๓) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นแหล่งให้บริการในช่องทางการเข้าถึงข้อมูลสารสนเทศสุขภาพและเป็นศูนย์กลางในการสะท้อนความต้องการ ปัญหาและข้อเสนอแนะจากภาคประชาชน **๖. ปัจจัยด้านการบริหารจัดการ** (๑) มีการจัดตั้งกลุ่มงานฯ/งาน/บุคลากร เพื่อเป็นหน่วยสนับสนุนและกำกับดูแลงานด้านเทคโนโลยีสารสนเทศภายในกอง/สำนักฯ (๒) มีการแต่งตั้ง คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข เพื่อกำหนดทิศทางการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงสาธารณสุข (๓) มีการแต่งตั้ง คณะอนุกรรมการบริหารการจัดหาระบบคอมพิวเตอร์ เพื่อทำหน้าที่บริหารการจัดหาระบบคอมพิวเตอร์ของสำนักงานปลัดกระทรวงสาธารณสุข ให้เป็นไปอย่างมีประสิทธิภาพและเหมาะสม (๔) มีการใช้เทคโนโลยีสารสนเทศในการปฏิบัติงาน ทำให้สามารถลดขั้นตอน ระยะเวลา

โอกาส – สิ่งที่จะมีส่วนช่วยให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ
และค่าใช้จ่ายในการดำเนินงาน **๗. ปัจจัยด้านงบประมาณ** (๑) ได้รับการสนับสนุนด้านงบประมาณอย่างต่อเนื่อง

ปัญหา – สิ่งที่จะขัดขวางมิให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ
ปัญหา/อุปสรรค ที่พบในระบบเทคโนโลยีสนเทศ ในภาพรวมของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ๑.กระบวนการบริหารจัดการและบูรณาการทางด้านการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศภายในองค์กรยังไม่เป็นเอกภาพเท่าที่ควร ๒. กระบวนการบริหารจัดการด้านความปลอดภัยยังไม่เป็นรูปธรรมเท่าที่ควร
ปัญหา/อุปสรรคที่พบในความน่าเชื่อถือของข้อมูล ๑. ความไม่ชัดเจนของเอกสาร เช่น เขียนไม่ชัดเจน ๒. เจ้าหน้าที่นำเข้าข้อมูลพิมพ์ผิด โดยไม่ได้สังเกต

ขั้น ๑.๓

กำหนดขอบเขต

- ขอบเขตของการบริหารความเสี่ยงสำนักงานปลัดกระทรวงสาธารณสุข ที่มีความสำคัญต่อวัตถุประสงค์ ภารกิจ สถานะ หรือ ความสำเร็จ

หน่วยงานขององค์กรที่จะจัดให้มีกระบวนการบริหารความเสี่ยง
ทุกกอง/สำนักของสำนักงานปลัดกระทรวงสาธารณสุข

ขั้นที่ ๑.๔

กำหนดตัวบุคลากร

ใช้คำสั่งสำนักงานปลัดกระทรวงสาธารณสุขที่ ๖๔๘ /๒๕๕๗ เรื่อง แต่งตั้งคณะทำงานพัฒนาปรับปรุงสารสนเทศส่วนกลางของสำนักงานปลัดกระทรวงสาธารณสุข ประจำปีงบประมาณ พ.ศ.๒๕๕๗ สั่ง ณ วันที่ ๑๘ มีนาคม พ.ศ.๒๕๕๗ (รายละเอียดดังหน้า ๑๑)

ขั้นที่ ๑.๕

จัดการรายละเอียดด้านกำหนดการ ส่วนสนับสนุนและอำนวยความสะดวก

เจ้าหน้าที่ผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยง

เพื่อให้การดำเนินงานตามแผนฯ เป็นไปอย่างรวดเร็วทันต่อการดำเนินการ จึงกำหนด ให้เจ้าหน้าที่ต่อไปนี้เป็นผู้รับผิดชอบดำเนินการจัดการความเสี่ยงที่เกิดขึ้น ให้กลุ่มคอมพิวเตอร์และเครือข่ายเป็นผู้รับผิดชอบดำเนินการ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำกับดูแล ควบคุมการดำเนินการ

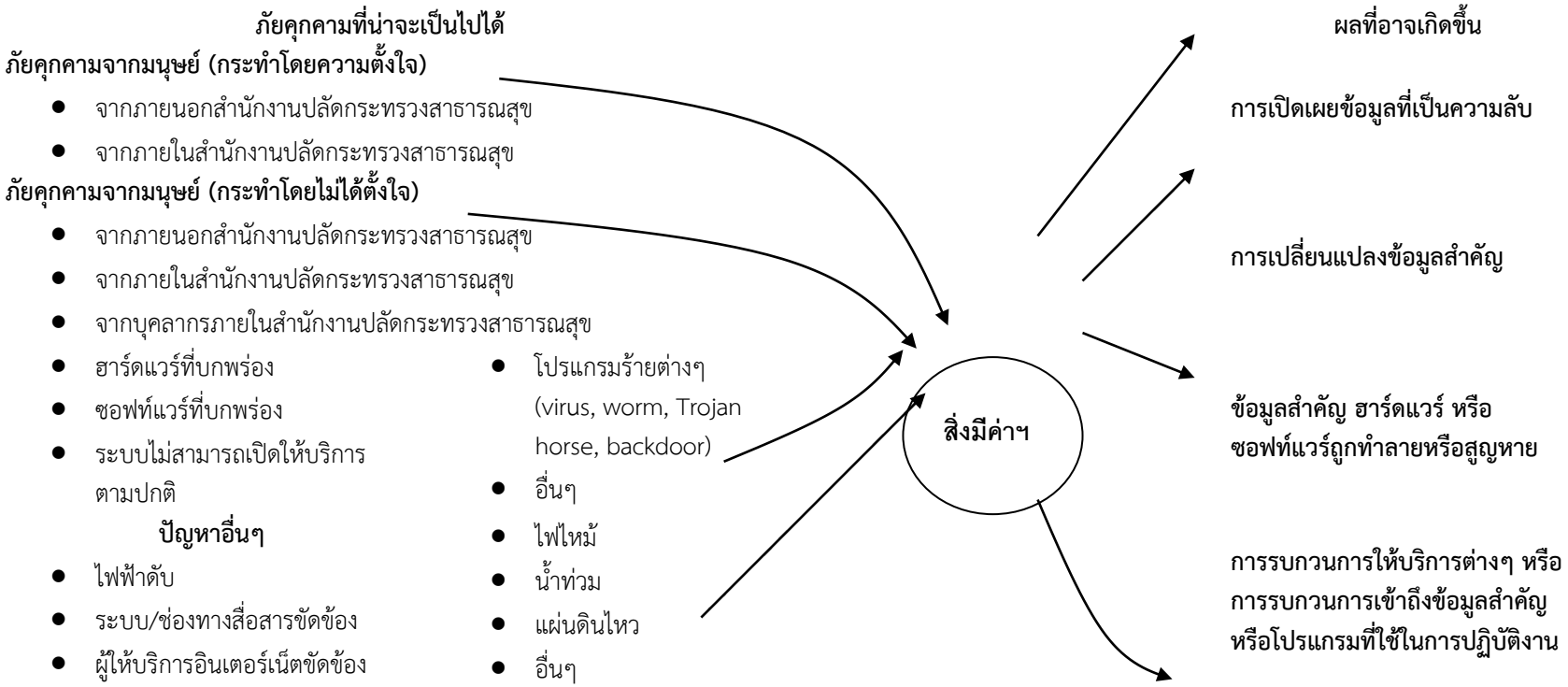
การรายงานผล

กำหนดให้ผู้รับผิดชอบดำเนินการรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีที่ระบุไว้

ผู้เกี่ยวข้อง	บทบาทและความรับผิดชอบหลัก
คณะกรรมการ	มีความเข้าใจถึงความเสี่ยงที่อาจมีผลกระทบร้ายแรงต่อองค์กร และทำให้มั่นใจว่ามีการดำเนินการที่เหมาะสมเพื่อจัดการความเสี่ยงนั้น ๆ
คณะกรรมการตรวจสอบ	● ทำให้มั่นใจว่ามีการควบคุมภายในที่เหมาะสมเพื่อจัดการความเสี่ยงทั่วทั้งองค์กร ● กำกับดูแลและติดตามการบริหารความเสี่ยงอย่างเป็นอิสระ ● ติดตามประสิทธิภาพการทำงานของหน่วยงานตรวจสอบภายใน ● รายงานต่อคณะกรรมการและผู้ถือหุ้นเกี่ยวกับประสิทธิภาพและประสิทธิผลของการควบคุมภายใน ● สื่อสารกับคณะกรรมการบริหารความเสี่ยงเพื่อให้เข้าใจความเสี่ยงที่สำคัญและเชื่อมโยงกับระบบการควบคุมภายใน
คณะกรรมการบริหารความเสี่ยง	● พิจารณาและอนุมัตินโยบายและกรอบการบริหารความเสี่ยง ● ติดตามการพัฒนากรอบการบริหารความเสี่ยง ● ติดตามกระบวนการบ่งชี้และประเมินความเสี่ยง ● ประเมินและอนุมัติแผนการจัดการความเสี่ยง ● รายงานต่อคณะกรรมการเกี่ยวกับความเสี่ยง และการจัดการความเสี่ยง ● สื่อสารกับคณะกรรมการตรวจสอบ เกี่ยวกับความเสี่ยงที่สำคัญ
CIO	● ติดตามความเสี่ยงที่สำคัญทั้งองค์กร และทำให้มั่นใจได้ว่ามีแผนการจัดการที่เหมาะสม ● ส่งเสริมนโยบายการบริหารความเสี่ยง และทำให้มั่นใจว่ากระบวนการบริหารความเสี่ยงได้รับการปฏิบัติทั่วทั้งองค์กร ● ติดตามความเสี่ยงทางกลยุทธ์และความเสี่ยงด้านการปฏิบัติการที่สำคัญและทำให้มั่นใจ ได้ว่ามีแผนการจัดการความเสี่ยงที่เหมาะสม ● ส่งเสริมวัฒนธรรมการบริหารความเสี่ยง และทำให้มั่นใจได้ว่า ผู้อำนวยการกอง/สำนักฯให้ความสำคัญกับการบริหารความเสี่ยงในฝ่ายของตน
ผู้อำนวยการกอง/สำนักฯ	● ทำให้มั่นใจว่าการปฏิบัติงานรายวันมีการประเมิน จัดการและรายงานความเสี่ยงอย่างเพียงพอ ● ส่งเสริมพนักงานในฝ่ายงานให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยง
หัวหน้าฝ่าย	● ระบุและรายงานความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานต่อผู้อำนวยการกอง/สำนักฯ และเข้าร่วมในการจัดทำแผนจัดการความเสี่ยง และนำแผนไปปฏิบัติ

ผู้เกี่ยวข้อง	บทบาทและความรับผิดชอบหลัก
หน่วยงานหรือผู้รับผิดชอบการบริหารความเสี่ยง	● ปฏิบัติหน้าที่ประจำวันแทนคณะกรรมการบริหารความเสี่ยง ● จัดทำนโยบายความเสี่ยง กรอบ และกระบวนการให้กับหน่วยธุรกิจและเสนอคณะกรรมการบริหารความเสี่ยงเพื่ออนุมัติ ● ให้การสนับสนุนและแนะนำกระบวนการบริหารความเสี่ยงแก่หน่วยงานต่างๆ ภายในองค์กรตามที่มีการร้องขอ
ผู้ตรวจสอบภายใน	● ทำให้มั่นใจว่ามีการควบคุมภายในที่เหมาะสมต่อการจัดการความเสี่ยงและการควบคุมเหล่านั้นได้รับการปฏิบัติตามภายในองค์กร ● ทำให้มั่นใจว่าได้มีการนำระบบการบริหารความเสี่ยงมาปรับใช้อย่างเหมาะสมและมีการปฏิบัติตามทั่วทั้งองค์กร ● สอบทานการปฏิบัติงานของหน่วยงานการบริหารความเสี่ยง ● สื่อสารกับหน่วยงานการบริหารความเสี่ยงเพื่อทำความเข้าใจเกี่ยวกับความเสี่ยงและดำเนินการตรวจสอบภายในตามแนวความเสี่ยง (Risk based auditing)

ขั้นที่ ๒ บ่งชี้ปัจจัยความเสี่ยง
ผังเหตุการณ์หรือสถานการณ์ที่น่าจะเป็นภัยคุกคามต่อสิ่งมีค่า



(และหากภัยคุกคามเหล่านี้เกิดขึ้นจริงจะมีผลกระทบอย่างไรกับสำนักงานปลัดกระทรวงสาธารณสุข)

ขั้นที่ ๓ วิเคราะห์ความเสี่ยง

ตารางที่ ๑ ระบุความเสี่ยงและผลกระทบด้านต่างๆ ที่จะเกิดขึ้น

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
ที่มาความเสี่ยง /ปัจจัยเสี่ยง	**ผลกระทบด้านต่างๆ**			
	ชื่อเสียง	**เวลา**	**การบริการ**	**บุคลากร**
๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย (R๐๑)	- ถูกเจ้าหน้าที่ภายในกระทรวงวิจารณ์ - เจ้าหน้าที่ขาดความเชื่อมั่นในระบบเครือข่าย	- ทำให้เจ้าหน้าที่ในสำนักงานปลัดกระทรวงสาธารณสุขไม่สามารถใช้ระบบงานและข้อมูลได้ - เสียเวลาในการกู้คืนระบบงานและข้อมูล	- บุคลากรสาธารณสุขไม่สามารถใช้ระบบงานและข้อมูลในการปฏิบัติงาน และให้บริการ	- บุคลากรสาธารณสุขถูกตำหนิ - เจ้าหน้าที่ดูแลระบบถูกตำหนิในเรื่องความสามารถในการดูแลระบบ
๒.ระบบให้บริการ Internet ล่ม (R๐๒)	- ถูกเจ้าหน้าที่ภายในกระทรวงวิจารณ์ - เจ้าหน้าที่ขาดความเชื่อมั่นในระบบเครือข่าย	- ทำให้ระบบเทคโนโลยีสารสนเทศต่างๆ ของกระทรวงสาธารสุขไม่สามารถทำงานได้	- บุคลากรสาธารณสุขไม่สามารถใช้ระบบสารสนเทศในการปฏิบัติงาน - ประชาชนไม่สามารถใช้บริการผ่านระบบอินเตอร์เน็ต	- เจ้าหน้าที่ถูกตำหนิในเรื่องความสามารถในการดูแลระบบ
		- ทำให้ไม่สามารถรับส่งข้อมูลที่สำคัญในการปฏิบัติงานอิเล็คทรอนิกส์		
๓.เครื่อง Server ติดไวรัส (R๐๓)	- ถูกวิจารณ์ถึงประสิทธิภาพการทำงาน	- ทำให้ระบบสารสนเทศทำงานได้ช้าหรือทำงานไม่ได้	เจ้าหน้าที่หน่วยงานต่างๆ ไม่สามารถทำงานได้	- เจ้าหน้าที่ถูกตำหนิในเรื่องการดูแลความปลอดภัยของระบบ

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
ที่มาความเสี่ยง /ปัจจัยเสี่ยง	**ผลกระทบด้านต่างๆ**			
	ชื่อเสียง	**เวลา**	**การบริการ**	**บุคลากร**
๔.เครื่อง Client ติดไวรัส (R๐๔)		- เครื่องของเจ้าหน้าที่ทำงานไม่ได้ทำให้งานหยุดชะงัก	ทำให้เครื่องคอมพิวเตอร์บางเครื่องไม่สามารถให้บริการได้ตามปกติ	-การดำเนินงานของเจ้าหน้าที่หยุดชะงักเสียเวลาในการจัดการกับไวรัส
๕.การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่) (R๐๕)	- เป็นข่าวในหน้าหนังสือพิมพ์ภายในประเทศ และต่างประเทศ ๒ – ๓ วัน - ถูกประชาชนวิจารณ์ถึงประสิทธิภาพการทำงานของกระทรวงฯ	ใช้เวลาในการทบทวนติดตาม/ตรวจสอบข้อมูลรวมทั้งเวลาในการเรียกคืนความเชื่อมั่นจากผู้รับบริการ	ไม่สามารถให้บริการข้อมูลที่ผิดพลาดจากความเป็นจริง	เจ้าหน้าที่ถูกตำหนิในการเสนอข้อมูลไม่ระมัดระวัง/ไม่ดูแลรักษาความลับของข้อมูล
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ (R๐๖)	ถูกวิจารณ์ถึงประสิทธิภาพการทำงาน	การทำงานหยุดชะงัก	เครื่องแม่ข่ายคอมพิวเตอร์ ถูกปิดโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	ผู้ดูแลระบบถูกตำหนิ
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (R๐๗) - ไฟไหม้ จากอุบัติเหตุไฟฟ้า	- เป็นข่าวในหนังสือพิมพ์/ Social Media	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติทำให้ระบบเสียหาย	ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหาย ต้องดำเนินการตัดกระแสไฟฟ้า	ถูกตำหนิในเรื่องความสามารถในการป้องกันและเตรียมการในการดูแลระบบ

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
ที่มาความเสี่ยง /ปัจจัยเสี่ยง	**ผลกระทบด้านต่างๆ**			
	ชื่อเสียง	**เวลา**	**การบริการ**	**บุคลากร**
ลัดวงจร การวางเพลิง - ภัยธรรมชาติ		การทำงานหยุดชะงักและต้องใช้เวลาในการกู้คืนและปรับปรุงระบบนาน	และไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อย ในบ้านเมือง (R๐๘)	-	ต้องใช้เวลาในการดำเนินงานและปรับปรุงระบบในช่วงเวลาที่ไม่สามารถดำเนินการได้	บุคลากรไม่สามารถปฏิบัติงานและให้บริการได้ตามปกติ	บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ

ขั้นที่ ๔ ระบุและจัดลำดับความเสี่ยง

ตารางที่ ๒ การประเมินความเสี่ยง

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
ปัจจัยเสี่ยง	**รายละเอียดความสูญเสีย**	**โอกาส**	**ผลกระทบ**	**ระดับความเสี่ยง**
๑.ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย (R๐๑)	- เจ้าหน้าที่ในสำนักงานปลัดกระทรวงสาธารณสุข ไม่สามารถใช้งานระบบสารสนเทศภายในได้ - เจ้าหน้าที่ลงรับหนังสือไม่สามารถให้บริการผู้ที่มาติดต่อได้ ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๓	๔	๑๒
๒. ระบบให้บริการ Internet ล่ม (R๐๒)	- ทำให้กระทรวงฯ ไม่สามารถให้บริการผ่านทางอินเตอร์เน็ต	๓	๔	๑๒
๓.การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่) (R๐๓)	- ทำให้ประชาชนไม่มั่นใจในคุณภาพข้อมูลของกระทรวงฯ/ขาดความเชื่อมั่นในความปลอดภัยของข้อมูล - ทำให้ตกเป็นข่าวในหนังสือพิมพ์ในประเทศ และต่างประเทศ	๓	๕	๑๕
๔.เครื่อง Server ติดไวรัส(R๐๔)	- ทำให้ระบบสารสนเทศ/ระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้	๓	๔	๑๒
๕.เครื่อง Client ติดไวรัส(R๐๕)	- ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	๔	๓	๑๒
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่(R๐๖)	- เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๒	๕	๑๐

ขั้นที่ ๔ ระบุและจัดลำดับความเสี่ยง (ต่อ)

ตารางที่ ๒ การประเมินความเสี่ยง

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
ปัจจัยเสี่ยง	**รายละเอียดความสูญเสีย**	**โอกาส**	**ผลกระทบ**	**ระดับความเสี่ยง**
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (R๐๗) - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	- การเกิดไฟไหม้อาคาร หรือแผ่นดิน ไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วน หรือทั้งหมด หรือการเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	๒	๕	๑๐
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง(R๐๘)	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๒	๕	๑๐
๘. ความเสี่ยงจากสถานการณ์ ความไม่สงบเรียบร้อยในบ้านเมือง	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๒	๕	๑๐

รูปที่ ๓ ผังแสดงผลการประเมินระดับความเสี่ยง

ผลการประเมินพบว่าความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศสำนักงานปลัดกระทรวงสาธารณสุขทุกระบบไม่ว่าจะเป็นการนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่) / ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย ,ระบบให้บริการ Internet ล่ม เครื่อง Serverและเครื่อง Client ติดไวรัส กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ ภัยหรือสถานการณ์ฉุกเฉิน สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง มีระดับความเสี่ยงสูง คะแนนระดับความเสี่ยง (๑๐ – ๑๕) ไม่สามารถที่จะยอมรับความเสี่ยงนั้นได้ จำเป็นต้องมีแผนควบคุมความเสี่ยง

ขั้นที่ ๕ วางแผนการรับมือกับความเสี่ยง

๕.๑ สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง

ตารางที่ ๓ สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข					
๑.ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลกระทบต่อการทำงานของระบบงานและข้อมูลซึ่งจำเป็นต้องให้บริการและมีการใช้งานอย่างต่อเนื่อง			
	ควบคุม	- จัดสร้างระบบงานสำรองเพื่อทำงานแทนเมื่อระบบหลักเกิดปัญหา(กรณีที่เป็นระบบงานและข้อมูลที่มีความสำคัญและส่งผลกระทบต่อองค์กรมาก) - หน่วยงานมีผู้ดูแลระบบงานและข้อมูล - มีการจัดอบรมเพื่อให้ความรู้แก่ผู้ใช้ระบบ	- เกิดค่าใช้จ่ายในการจัดหาจัดจ้างเพื่อพัฒนาระบบงานสำรอง	- การดำเนินงานของสำนักงานปลัดกระทรวงสาธารณสุข เป็นไปได้อย่างต่อเนื่อง	
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๒. ระบบให้บริการ Internet ล่ม	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียมาก			
	ควบคุม	- จัดทำระบบ Internet Zone ให้เป็น High Availability - จัดให้มีการเชื่อมสำรองต่อกับ ISP รายที่สองเพื่อให้การบริการเครือข่ายสามารถ	- เกิดค่าใช้จ่ายในการจัดหาอุปกรณ์ระบบเครือข่ายสำรองและการจัดหา ISP รายที่สอง	- การให้บริการประชาชนทางอินเตอร์เน็ตเป็นไปได้อย่างต่อเนื่อง	

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๒. ระบบให้บริการ Internet ล่ม (ต่อ)	ควบคุม (ต่อ)	ดำเนินการได้อย่างต่อเนื่อง (ทดแทนกรณีที่ ISP หลักเกิดปัญหา)			ควบคุม
	ถ่ายโอน	- จัดจ้างหน่วยงานภายนอกดูแลระบบเครือข่าย Internet - จัดให้มีการเชื่อมสำรองต่อกับ ISP รายที่สอง	- เกิดค่าใช้จ่ายในการจัดจ้าง Outsource ทั้งตัวระบบและการดูแลระบบ		
๓.การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่)	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียมาก			
	ควบคุม	- จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ	- เกิดค่าใช้จ่ายในการจัดทำระบบป้องกันความปลอดภัยของข้อมูล		
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๔.เครื่อง Server ติดไวรัส	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียมาก - จัดหาระบบป้องกันความปลอดภัย			

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๔.เครื่อง Server ติดไวรัส (ต่อ)	ควบคุม	- จัดทำและประกาศใช้นโยบายการป้องกัน ไวรัส - ติดตั้งระบบป้องกันไวรัสในส่วนของ Server - ทำการ update virus signature อย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ	- เกิดต้นทุนทางทรัพยากร - บุคคลและต้นทุนทางการจัดการ	- ระบบ Server ทำงานได้อย่างต่อเนื่อง	
	ถ่ายโอน	ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๕.เครื่อง Client ติดไวรัส	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้	- เกิดต้นทุนทางทรัพยากรบุคคลและต้นทุนทางการจัดการ	- ระบบคอมพิวเตอร์ของผู้ใช้ทำงานได้อย่างต่อเนื่อง	ควบคุม
	ยอมรับ	- สามารถยอมรับความเสี่ยงนี้ได้			
	ควบคุม	- จัดทำและประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในส่วนของ Client - ทำการ update virus signature อย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ใช้งาน			
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	หลีกเลี่ยง	- ไม่สามารถยกเลิกระบบนี้ได้			ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้ เนื่องจากมีผลเสียมาก - ระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ			

ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ต้นทุน	ผลประโยชน์	ทางเลือกที่เหมาะสม
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ (ต่อ)	ควบคุม	- ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) - เช่าเครื่องปั่นไฟฟ้ามาใช้ในการให้บริการเครือข่ายเป็นรายครั้ง	เกิดต้นทุนในการจัดหาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) และการเช่าเครื่องปั่นไฟฟ้า	เพื่อป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์	ควบคุม
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	หลีกเลี่ยง	- ไม่สามารถหลีกเลี่ยงได้	การจัดหาระบบสำรองและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด เกิดต้นทุนและค่าใช้จ่ายในการดำเนินการ	- ระบบงานทุกอย่างสามารถทำงานได้อย่างต่อเนื่อง	ควบคุม
	ยอมรับ	- ไม่สามารถยอมรับความเสี่ยงนี้ได้			
	ควบคุม	- จัดทำแผน Business Continuity Plan (BCP) จัดหาระบบสำรองและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด			
	ถ่ายโอน	- ไม่สามารถถ่ายโอนให้ผู้อื่นได้			
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	หลีกเลี่ยง	- ไม่สามารถหลีกเลี่ยงได้	การจัดหาระบบสำรองและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด เกิดต้นทุนและค่าใช้จ่ายในการดำเนินการ	- ระบบงานทุกอย่างสามารถทำงานได้อย่างต่อเนื่อง	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 สำนักงานปลัดกระทรวงสาธารณสุข						
๑.ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหาย หรือถูกทำลาย	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน/ โดน Virus โจมตี/ Hacker/Cracker	- บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุข ไม่สามารถใช้ระบบงานและข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๓	๔	๑๒	- จัดทำระบบงานและข้อมูลสำรองให้ทำงานแทนเมื่อระบบหลักเกิดปัญหา (ระบบ Database Backup) - หน่วยงานมีผู้ดูแลระบบงานและข้อมูล - มีการจัดอบรมเพื่อให้ความรู้ด้านการดูแลรักษาความปลอดภัยของระบบงานและข้อมูลแก่ผู้ใช้ระบบ
๒. ระบบให้บริการ Internet ล่ม	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	สำนักงานปลัดกระทรวงสาธารณสุข ไม่สามารถให้บริการผ่านทางอินเตอร์เน็ต	๓	๔	๑๒	- จัดทำระบบ Internet Zone ให้เป็น High Availability - จัดให้มีการเชื่อมสำรองต่อกับ ISP รายที่สอง
๓. การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่)	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาความปลอดภัยของข้อมูลของกระทรวงฯ ทำให้ตกเป็นข่าวในหนังสือพิมพ์ในประเทศและต่างประเทศ	๓	๕	๑๕	- จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	โอกาสที่จะเกิด (๑)	ผลกระทบเสียหาย (๒)	ระดับความเสี่ยง (๑) X (๒)	แนวทางการควบคุม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๔. เครื่อง Server ติดไวรัส	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้	๓	๔	๑๒	- จัดหาระบบป้องกันความปลอดภัย - จัดทำและประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในส่วนของ Server - ทำการ update virus signature อย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ
๕. เครื่อง Client ติดไวรัส	ความเสี่ยงจากผู้ปฏิบัติงานนำเอาอุปกรณ์เคลื่อนที่ (Smart Phone, Tablet PC) ส่วนตัวเข้ามาเชื่อมต่อ รวมถึงการดาวน์โหลดโปรแกรมหรือไฟล์จากอินเตอร์เน็ตโดยขาดความระมัดระวัง	-ส่งผลกระทบต่อการใช้งานระบบเครือข่าย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย -ทำให้เครื่องของเจ้าหน้าที่ทำงานไม่ได้	๔	๓	๑๒	- ฝึกอบรม เผยแพร่และประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องของความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากร - จัดทำและประกาศใช้นโยบายการป้องกันไวรัสและติดตั้งระบบป้องกันไวรัสในเครื่องของ User และให้ทำการ update virus อย่างสม่ำเสมอ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	โอกาสที่จะเกิด (๑)	ผลกระทบเสียหาย (๒)	ระดับความเสี่ยง (๑) X (๒)	แนวทางการควบคุม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้ ระบบงาน/ข้อมูลเสียหรือสูญหาย	๒	๕	๑๐	- บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล - สำนักงานปลัดกระทรวงสาธารณสุขมีการเช่าเครื่องปั่นไฟฟ้ามาใช้ในการให้บริการเครือข่าย - เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย(Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในหน่วยงานด้วย - ให้ความรู้และความเข้าใจแก่บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุขในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	โอกาสที่จะเกิด (๑)	ผลกระทบเสียหาย (๒)	ระดับความเสี่ยง (๑) X (๒)	แนวทางการควบคุม
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ)	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ทำให้เครื่องคอมพิวเตอร์ถูกทำลายหรือเสียหาย	๒	๕	๑๐	- มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของสำนักงานปลัดกระทรวงสาธารณสุข - มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เช่น การชุมนุมประท้วง จลาจลการก่อการร้าย	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	๒	๕	๑๐	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด

ตารางที่ ๕ แบบรายการกิจกรรมในการจัดการความเสี่ยง

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหาย หรือถูกทำลาย	- บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุข ไม่สามารถใช้ระบบงานและข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๑๒	- จัดทำระบบความมั่นคงปลอดภัยของระบบงานและข้อมูล - จัดสร้างระบบงานสำรองเพื่อทำงานแทนเมื่อระบบหลักเกิดปัญหา(กรณีที่เป็นระบบงานและข้อมูลที่มีความสำคัญและส่งผลกระทบต่อองค์กรมาก)	- จัดประชุมฝ่าย security และ Application - จัดจ้างที่ปรึกษาเพื่อออกแบบระบบป้องกันความปลอดภัยของข้อมูล - จัดซื้อจัดจ้างระบบป้องกันความปลอดภัยของข้อมูล - จัดอบรมให้ความรู้ด้านความปลอดภัย
๒. ระบบให้บริการ Internet ล่ม	- ทำให้กระทรวงฯไม่สามารถให้บริการผ่านทางอินเตอร์เน็ต	๑๒	- จัดทำระบบ Internet Zone ให้เป็น High Availability - จัดให้มีการเชื่อมสำรองต่อกับ ISP รายที่สอง	- เก็บข้อมูล และจัดทำรายละเอียดค่าใช้จ่ายในการจัดทำระบบ Internet Zone ให้เป็น High Availability - เก็บข้อมูล และจัดทำรายละเอียดค่าใช้จ่ายในการเพิ่ม internet link สำรอง - จัดประชุมทีมงานฝ่ายดูแลเครือข่ายสารสนเทศ
๓. การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่)	- ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาข้อมูลของกระทรวงฯ ทำให้ตกเป็นข่าวในหนังสือพิมพ์ในประเทศ และต่างประเทศ	๑๕	- จัดให้มีระบบป้องกันความปลอดภัยของข้อมูล - จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง	- หน่วยงานมีผู้ดูแลระบบงานและข้อมูล - ดำเนินการจัดทำระบบงานสำรอง (ขึ้นกับความสำคัญของระบบงานและงบประมาณ) - จัดตั้งคณะทำงานเกี่ยวกับการป้องกันความปลอดภัยของข้อมูล

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
๓. การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่) (ต่อ)				- จัดทำและประกาศใช้นโยบายป้องกันข้อมูลรั่วไหล - จัดการอบรมให้ความรู้เกี่ยวกับการป้องกันความปลอดภัยของข้อมูลในองค์กร
๔. เครื่อง Server ติดไวรัส	- ทำให้ระบบสารสนเทศ/ระบบงานสำคัญทำงานได้ช้าหรือทำงานไม่ได้	๑๒	- จัดหาระบบป้องกันความปลอดภัย - ประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในส่วนของ Server - ทำการ update virus signature อย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ดูแลระบบ	- จัดทำและประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในเครื่อง Server ทุกเครื่อง - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ
๕. เครื่อง Client ติดไวรัส	- ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	๑๒	- ประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในส่วนของ Client - ทำการ update virus signature อย่างสม่ำเสมอ - ให้ความรู้เกี่ยวกับการป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้กับผู้ใช้งาน	- จัดทำและประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในเครื่อง Client ทุกเครื่อง - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ใช้งาน

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้ ระบบงาน/ข้อมูลเสียหรือสูญหาย	๑๐	- การติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply:UPS) - เช่าเครื่องปั่นไฟฟ้า	- บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที - เช่าเครื่องปั่นไฟฟ้ามาใช้ในการให้บริการเครือข่ายเป็นรายครั้ง - ให้ความรู้และความเข้าใจแก่บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุขในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ทำให้เครื่องคอมพิวเตอร์ถูกทำลายหรือเสียหาย	๑๐	- มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของสำนักงานปลัดกระทรวงสาธารณสุข - มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ	- เมื่อเกิดภัยพิบัติ เช่น อัคคีภัย ให้ผู้ใช้งานรีบเก็บแผ่น CD ซึ่งบรรจุข้อมูลสำรองซึ่งมีความสำคัญไปด้วยแล้วดำเนินการตามหลักปฏิบัติ/ขั้นตอนในแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ - เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบ และดำเนินการประสานผู้ที่

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
				เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า ๑ วัน ในการดำเนินการแก้ไข ให้ออกประกาศแจ้งแก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น ๓. เมื่อเกิดกรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบทำการแก้ไขแล้วเสร็จ ๔. เมื่อเกิดกรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบทำการตรวจสอบเหตุแห่งความเสียหายนั้นในเบื้องต้น พร้อมรายงานให้ผู้บังคับบัญชาทราบ พบว่าหากมีแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมาได้ ให้ดำเนินการโดยด่วน ทั้งนี้อาจประสานงานขอความช่วยเหลือจากผู้ที่ชำนาญในเรื่องดังกล่าวเพื่อดำเนินการด้วยก็ได้ หากไม่สามารถกู้คืนข้อมูลกลับมาได้ให้นำข้อมูลที่สำรองไว้มาใช้แทน กรณีที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไปเมื่อเกิดเหตุอุปกรณ์จัดเก็บข้อมูลเสียหาย ให้รายงานผู้บังคับบัญชาของตนทราบแล้วแจ้งกลุ่มคอมพิวเตอร์เพื่อตรวจสอบเหตุแห่งความเสียหายนั้น

ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	ระดับความเสี่ยง	แนวทางการจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข				
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	๑๐	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสารองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สารองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด

ขั้นที่ ๖ รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง

ตารางที่ ๖ การติดตามกิจกรรมการจัดการความเสี่ยง

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**

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

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรคและแนวทางการแก้ไข
- จัดทำระบบความมั่นคงปลอดภัยของระบบงานและข้อมูล					
- ทำการ Back up ระบบ					
- จัดประชุมฝ่าย security และ Application					
- จัดซื้อจัดจ้างระบบป้องกันความปลอดภัยของข้อมูล					
- จัดอบรมให้ความรู้ด้านความปลอดภัย					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**

รายงานความเสี่ยง **๒. ระบบให้บริการ Internet ล่ม**

วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	%	ปัญหา
๑. ขยาย Band Width เส้นทางการใช้ Internet สำหรับกรมต่างๆ					
๒. ขยาย Band Width เส้นทางการใช้ Internet สำหรับหน่วยงานภายในอาคาร สป.					
๓. จัดให้มีบริการ Internet Link สำรอง					
๔. ดำเนินการตามแผนปฏิบัติ การรักษาความมั่นคงปลอดภัยของระบบระบบเครือข่ายเทคโนโลยีสารสนเทศ					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**
รายงานความเสี่ยง **๓.ความปลอดภัยของข้อมูล**
วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรคและแนวทางการแก้ไข
๑. จัดหาอุปกรณ์ป้องกันรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์					
๒. ติดตั้งโปรแกรม Antivirus					
๓. จัดทำแผนการตรวจสอบช่องโหว่					
๔. จัดทำคู่มือการตรวจหาและจัดการไวรัสคอมพิวเตอร์					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**
รายงานความเสี่ยง **๔.เครื่อง Server ติดไวรัส**
วันที่.....ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์ของกิจกรรม	กำหนดการ	ระยะเวลาดำเนินการ	% ความคืบหน้า	ปัญหาอุปสรรคและแนวทางการแก้ไข
๑. จัดหาอุปกรณ์ป้องกันรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์					
๒. ติดตั้งโปรแกรม Antivirus					
๓. จัดทำแผนการตรวจสอบช่องโหว่					
๔. จัดทำคู่มือการตรวจหาและจัดการไวรัสคอมพิวเตอร์					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**
รายงานความเสี่ยง **๕.เครื่อง Client ติดไวรัส**
วันที่.....ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	%	ปัญหา
๑. จัดหาอุปกรณ์ป้องกันรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์					
๒. ติดตั้งโปรแกรม Antivirus					
๓. จัดทำคู่มือการตรวจหาและจัดการไวรัสคอมพิวเตอร์					
๔. จัดหาช่างผู้มีความเชี่ยวชาญเฉพาะด้านการซ่อมบำรุงคอมพิวเตอร์คอยให้บริการ					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**
รายงานความเสี่ยง **๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่**
วันที่..... ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	%	ปัญหา
- บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ					
- ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS)					
- เช่าเครื่องปั่นไฟฟ้ามาใช้ในการให้บริการเครือข่ายเป็นรายครั้ง					
- ให้ความรู้และความเข้าใจแก่บุคลากรในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**
รายงานความเสี่ยง **๗. ภัยหรือสถานการณ์ฉุกเฉิน**
วันที่.....ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	%	ปัญหา
- จัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan)					
- ประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ					

<u>รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง</u>

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้าน**การใช้เทคโนโลยี**
รายงานความเสี่ยง **๘. สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง**
วันที่.....ผู้รับผิดชอบ.....

กิจกรรม	ผลลัพธ์	กำหนด	ระยะเวลา	%	ปัญหา
- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (BCP)					
- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ และสำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด					

ตารางที่ ๗ การประเมินผลการจัดการความเสี่ยง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๑.	เครื่อง Client ติดไวรัส	ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	- จัดทำและประกาศใช้นโยบายการป้องกันไวรัส -ติดตั้งระบบป้องกันไวรัสในเครื่อง Client ทุกเครื่อง - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ใช้งาน			
๒.	ระบบงานและข้อมูล (System & Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	- บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุข ไม่สามารถใช้ระบบงานและข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	- จัดประชุมฝ่าย security และ Application - จัดจ้างที่ปรึกษาเพื่อออกแบบระบบป้องกันความปลอดภัยของข้อมูล - จัดซื้อจัดจ้างระบบป้องกันความปลอดภัยของข้อมูล - จัดอบรมให้ความรู้ด้านความปลอดภัยแก่ผู้ดูแลระบบ			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๒) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๓.	เครื่อง Server ติดไวรัส	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้	- จัดทำและประกาศใช้นโยบายการป้องกันไวรัส -ติดตั้งระบบป้องกันไวรัสในเครื่อง Server ทุกเครื่อง - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ			
๔.	ระบบให้บริการ Internet ล่ม	ทำให้กระทรวงฯไม่สามารถให้บริการผ่านทางอินเตอร์เน็ต	- เก็บข้อมูล และจัดทำรายละเอียดค่าใช้จ่ายในการจัดทำระบบ Internet Zone ให้เป็น High Availability - เก็บข้อมูล และจัดทำรายละเอียดค่าใช้จ่ายในการเพิ่ม internet link สำรอง -จัดประชุมทีมงานฝ่ายดูแลเครือข่ายสารสนเทศ			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๓) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๕.	การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่)	ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาข้อมูลของกระทรวงฯ ทำให้ตกเป็นข่าวในหนังสือพิมพ์ในประเทศและต่างประเทศ	- จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร - จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง - หน่วยงานมีผู้ดูแลระบบงานและข้อมูล - ดำเนินการจัดทำระบบงานสำรอง - จัดการอบรมให้ความรู้เกี่ยวกับการป้องกันความปลอดภัยของข้อมูลในองค์กร			
๖	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/ แรงดันไฟฟ้าไม่คงที่	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้ ระบบงาน/ข้อมูลเสียหรือสูญหาย	- บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS)			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	รายละเอียดการจัดการ	โอกาสที่จะเกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยงคงเหลือ (๑) X (๒)
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๖	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/ แรงดันไฟฟ้าไม่คงที่ (ต่อ)		- เช่าเครื่องปั่นไฟฟ้ามาใช้ในการให้บริการเครือข่ายเป็นรายครั้ง - ให้ความรู้และความเข้าใจแก่บุคลากรในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ			
๗	ภัยหรือสถานการณ์ฉุกเฉิน	ทำให้เครื่องคอมพิวเตอร์ถูกทำลายหรือเสียหาย	- มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของสป. - มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ			
๘	สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ และสำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด			

ตารางที่ ๘ สรุปผลการดำเนินงานจากการบริหารความเสี่ยง

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๑.	เครื่อง Client ติดไวรัส	ทำให้เครื่องของเจ้าหน้าที่บางท่านทำงานไม่ได้	- จัดทำและประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในเครื่อง Client ทุกเครื่อง - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ใช้งาน			
๒.	ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	- บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุขไม่สามารถใช้ระบบงานและข้อมูลได้ - ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	- จัดทำระบบความมั่นคงปลอดภัยของระบบงานและข้อมูล - จัดสร้างระบบงานสำรองเพื่อทำงานแทนเมื่อระบบหลักเกิดปัญหา - จัดประชุมคณะทำงานความมั่นคงปลอดภัย - จัดอบรมให้ความรู้ด้านความปลอดภัย			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๓.	เครื่อง Server ติดไวรัส	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้าหรือทำงานไม่ได้	- จัดทำและประกาศใช้นโยบายการป้องกันไวรัส - ติดตั้งระบบป้องกันไวรัสในเครื่อง Server ทุกเครื่อง - ให้การอบรมให้ความรู้เกี่ยวกับป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้ดูแลระบบ			
๔.	ระบบให้บริการ Internet ล่ม	ทำให้กระทรวงฯไม่สามารถให้บริการผ่านทางอินเตอร์เน็ต	- เก็บข้อมูล และจัดทำรายละเอียด ค่าใช้จ่ายในการจัดทำระบบ Internet Zone ให้เป็น High Availability - เก็บข้อมูล และจัดทำรายละเอียด ค่าใช้จ่ายในการเพิ่ม internet link สำรอง - จัดประชุมทีมงานฝ่ายดูแลเครือข่ายสารสนเทศ			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๕.	การนำเสนอข้อมูลผิดพลาด/ ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่)	ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาข้อมูลของกระทรวงฯ ทำให้ตกเป็นข่าวในหนังสือพิมพ์ในประเทศ และต่างประเทศ	- จัดตั้งคณะทำงานเกี่ยวกับการป้องกันความปลอดภัยของข้อมูล - จัดทำและประกาศใช้นโยบายป้องกันข้อมูลรั่วไหล -จัดการอบรมให้ความรู้เกี่ยวกับการป้องกันความปลอดภัยของข้อมูลในองค์กร			
๖	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่	ทำให้ระบบสารสนเทศระบบสำคัญทำงานได้ช้าหรือทำงานไม่ได้ ระบบงานและข้อมูลเสียหายหรือสูญหาย	- บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ - ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC)			
๗	ภัยหรือสถานการณ์ฉุกเฉิน	ทำให้เครื่องคอมพิวเตอร์ถูกทำลายหรือเสียหาย เช่น ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง	- มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของสำนักงานปลัดกระทรวง			

ลำดับความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	รายละเอียดการจัดการ	ระดับความเสี่ยงคงเหลือ	ผลจากการใช้มาตรการจัดการความเสี่ยง	หมายเหตุ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข						
๗	ภัยหรือสถานการณ์ฉุกเฉิน (ต่อ)	ทำให้เครื่องคอมพิวเตอร์ถูกทำลายหรือเสียหาย เช่น ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ	- มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของสำนักงานปลัดกระทรวงสาธารณสุข - มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ			
๘	สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสารองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด			

บทที่ ๓ แนวทางการจัดทำแผนลดความเสี่ยงในระดับยุทธศาสตร์
: ด้านเทคโนโลยีสารสนเทศ (ปี ๒๕๕๗ - ๖๑)

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๑. จิตสำนึกและการให้ความรู้ด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	- ขอตั้งงบประมาณในการอบรมเกี่ยวกับความปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่บุคลากรที่ดูแลระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อเพิ่มจิตสำนึกด้านความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศแก่บุคลากร	✓	✓	✓	✓	✓
	- ส่งบุคลากรที่ทำหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุขไปอบรมเพื่อให้มีความชำนาญและมีความรู้เพิ่มขึ้น	✓	✓	✓	✓	✓
๒. ยุทธศาสตร์ความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	- กำหนดยุทธศาสตร์ความปลอดภัยของระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับยุทธศาสตร์และเป้าหมายของสำนักงานปลัดกระทรวงสาธารณสุข โดยกำหนดให้มีการทบทวนตามระยะเวลาที่กำหนด ตาม แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข ประกาศ ณ วันที่ ๗ มกราคม ๒๕๕๖	✓				

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๒. ยุทธศาสตร์ความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ต่อ)	- จัดทำทะเบียนเอกสารที่ระบุยุทธศาสตร์ เป้าหมายและวัตถุประสงค์ด้านความปลอดภัยของความปลอดภัยของระบบเทคโนโลยีสารสนเทศสำนักงานปลัดกระทรวงสาธารณสุข โดยจัดเก็บต้นฉบับไว้ที่แผนกควบคุมเอกสารและทำสำเนาและแจกจ่ายไปยังทุกแผนกเช่นกับเอกสารในระบบ	✓				
๓. การบริหารในเรื่องที่เกี่ยวกับความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	- จัดทำงบประมาณสำหรับกิจกรรมด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อเสนออนุมัติจากผู้บริหาร โดยกำหนดกิจกรรมที่จำเป็นด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศในสำนักงานปลัดกระทรวงสาธารณสุข	✓	✓	✓	✓	✓
	- จัดให้มีการประชุมทบทวนกระบวนการบริหารความเสี่ยงของสำนักงานปลัดกระทรวงสาธารณสุขหลังจากที่ได้เริ่มบริหารความเสี่ยงแล้วจัดทำรายงานต่อฝ่ายบริหารเมื่อเกิดปัญหาด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศในสำนักงานปลัดกระทรวงสาธารณสุข	✓	✓	✓	✓	✓
๓.๑ ความปลอดภัยทางกายภาพ	- ติดตั้งทีวีวงจรปิดเพื่อตรวจจับการเข้าถึงทางเครือข่าย	✓				
	- ประกาศมาตรการที่ใช้ในการป้องกัน	✓				
	- กำหนดแผนรับมือกรณีเกิดภัยคุกคาม	✓	✓	✓	✓	✓
	- อุดช่องโหว่ทางกายภาพ	✓	✓	✓	✓	✓

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๓.๑ ความปลอดภัยทางกายภาพ(ต่อ)	- ส่งบุคลากรเข้ารับการอบรมเกี่ยวกับความปลอดภัยทางกายภาพ		✓			
	- หมั่นตรวจสอบข้อมูลปัญหาทางด้านกายภาพที่เกิดขึ้นในปัจจุบัน	✓	✓	✓	✓	✓
	- กำหนดงบประมาณสำหรับการรักษาความปลอดภัยทางกายภาพของสำนักงานปลัดกระทรวงสาธารณสุขโดยดูจากระดับความรุนแรงของปัญหาด้านความปลอดภัยที่ผ่านมา		✓			
	- ทบทวนนโยบายและระเบียบของสำนักงานปลัดกระทรวงสาธารณสุขว่าเพียงพอสำหรับการรักษาความปลอดภัยทางกายภาพของสำนักงานปลัดกระทรวงสาธารณสุขให้อยู่ในระดับที่เหมาะสมหรือไม่ โดยดูจากปัญหาที่ผ่านมาและปรับปรุงนโยบายและระเบียบที่มีการประกาศใช้		✓			
	- กำหนดและประกาศแต่งตั้งผู้รับผิดชอบหลักในการรักษาความปลอดภัยทางกายภาพ	✓				
	- กำหนดและประกาศแต่งตั้งผู้รับผิดชอบหลักของแต่ละแผนกในการรักษาความปลอดภัยทางกายภาพ	✓				
	- จัดทำข้อตกลงว่าจ้างผู้เชี่ยวชาญจากนอกสำนักงานปลัดกระทรวงสาธารณสุขที่สามารถให้คำปรึกษาและสามารถให้ความช่วยเหลือด้านความปลอดภัยทางกายภาพกรณีเกิดปัญหาที่ไม่สามารถแก้ไขได้ด้วยบุคลากรในสำนักงานปลัดกระทรวงสาธารณสุข โดยให้บุคลากรแผนกไอทีเป็นผู้ติดต่อประสานงานเพื่อแจ้งความต้องการด้านความปลอดภัยทางกายภาพ และให้มีการตรวจสอบโดยบุคลากรแผนกไอทีว่าสำนักงานปลัดกระทรวงสาธารณสุขได้รับความ		✓			

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๓.๑ ความปลอดภัยทางกายภาพ (ต่อ)	ช่วยเหลือที่เป็นไปตามความต้องการนั้นหรือไม่จากผลลัพธ์ที่เกิดขึ้น					
๓.๒ ความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	- หมั่นตรวจสอบข้อมูลปัจจุบันที่เกี่ยวกับความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	✓	✓	✓	✓	✓
	- กำหนดงบประมาณสำหรับการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ โดยดูจากปัญหาที่ผ่านมา	✓	✓	✓	✓	✓
	กำหนดนโยบายและระเบียบของสำนักงานปลัดกระทรวงสาธารณสุขทางด้านการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข และทบทวนเพื่อปรับปรุงนโยบายและระบียบของสำนักงานปลัดกระทรวงสาธารณสุขตามวาระ	✓				
	- กำหนดและแต่งตั้งผู้รับผิดชอบหลักและผู้รับผิดชอบแต่ละกอง/สำนักฯ ในการรักษาความปลอดภัยของทางระบบเทคโนโลยีสารสนเทศ	✓				

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๓.๒ ความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ (ต่อ)	- จัดทำข้อตกลงว่าจ้างผู้เชี่ยวชาญจากนอกสำนักงานปลัดกระทรวงสาธารณสุขที่สามารถให้คำปรึกษาและสามารถให้ความช่วยเหลือด้านความปลอดภัยทางกายภาพกรณีเกิดปัญหาที่ไม่สามารถแก้ไขได้ด้วยบุคลากรในสำนักงานปลัดกระทรวงสาธารณสุข โดยให้บุคลากรแผนกไอทีเป็นผู้ติดต่อประสานงานเพื่อแจ้งความต้องการด้านความปลอดภัยทางกายภาพ และให้มีการตรวจสอบโดยบุคลากรแผนกไอที ว่าสำนักงานปลัดกระทรวงสาธารณสุขได้รับความช่วยเหลือที่เป็นไปตามความต้องการนั้นหรือไม่จากผลลัพธ์ที่เกิดขึ้น		✓			
๓.๓ การปฏิบัติของบุคลากร	- จัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการปฏิบัติงานในเรื่องความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	✓	✓			
	- กำหนดงบประมาณสำหรับการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศโดยดูจากปัญหาที่ผ่านมา	✓				

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๓.๓ การปฏิบัติของบุคลากร (ต่อ)	- กำหนดนโยบายและระเบียบของสำนักงานปลัดกระทรวงสาธารณสุขทางด้านการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข และทบทวนเพื่อปรับปรุงนโยบายและระบียบของสำนักงานปลัดกระทรวงสาธารณสุขตามวาระ	✓				
	- กำหนดและแต่งตั้งผู้รับผิดชอบหลักและผู้รับผิดชอบแต่ละแผนกในการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	✓	✓			
	- จัดทำข้อตกลงว่าจ้างผู้เชี่ยวชาญจากนอกสำนักงานปลัดกระทรวงสาธารณสุขที่สามารถให้คำปรึกษาและสามารถให้ความช่วยเหลือด้านความปลอดภัยทางกายภาพกรณีเกิดปัญหาที่ไม่สามารถแก้ไขได้ด้วยบุคลากรในสำนักงานปลัดกระทรวงสาธารณสุข โดย		✓			
	ให้บุคลากรแผนกไอทีเป็นผู้ติดต่อประสานงานเพื่อแจ้งความต้องการด้านความปลอดภัยทางกายภาพ และให้มีการตรวจสอบโดยบุคลากรแผนกไอที ว่าสำนักงานปลัดกระทรวงสาธารณสุขได้รับความช่วยเหลือที่เป็นไปตามความต้องการนั้นหรือไม่จากผลลัพธ์ที่เกิดขึ้น	✓				

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๔. นโยบายและระเบียบปฏิบัติด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข	- กำหนดนโยบายด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข โดยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศและอนุมัติโดยผู้บริหารระดับสูง จัดเก็บเอกสารต้นฉบับไว้และทำสำเนาแจกจ่ายให้กับทุกแผนก	✓				
	- หมั่นตรวจสอบกฎหมายหรือระเบียบใด ๆ ที่เกี่ยวข้องกับความปลอดภัยของระบบเทคโนโลยีสารสนเทศในเว็บไซต์ของสำนักงานปลัดกระทรวงสาธารณสุขและนำมาปรับใช้เป็นแนวทางปฏิบัติ	✓	✓	✓	✓	✓
	- ประกาศใช้นโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศภายในสำนักงานปลัดกระทรวงสาธารณสุขและกำหนดให้มีการทบทวนนโยบายให้สอดคล้องกับกฎหมายและการปฏิบัติ	✓				
๕. ความร่วมมือในการบริหารความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	- กำหนดนโยบายด้านความปลอดภัยในการปกป้องข้อมูลเมื่อปฏิบัติงานร่วมกับหน่วยงานอื่นหรือผู้ใช้บริการ โดยการกำหนดเป็นข้อตกลงร่วมกันไว้เป็นลายลักษณ์อักษร	✓				

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๕. ความร่วมมือในการบริหารความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ต่อ)	- กำหนดให้มีกระบวนการตรวจสอบจากภายนอกว่าสำนักงานปลัดกระทรวงสาธารณสุขนั้นมีการปกป้องข้อมูลและระบบที่สำคัญอย่างเหมาะสมหรือไม่ โดยใช้แบบสอบถามหรือมีการสัมภาษณ์		✓			
	- สรุปข้อมูลการตรวจสอบจากแบบสอบถามหรือการสัมภาษณ์ แล้วนำมาเทียบเคียงกับปัญหาเกิดขึ้น แล้วปรับปรุงวิธีการตรวจสอบ		✓			
๖. แผนฉุกเฉินและการฟื้นฟูจากหายนะ	- กำหนดแผนการปฏิบัติงานกรณีเกิดภาวะฉุกเฉินเป็นลายลักษณ์อักษร กำหนดแผนการซ้อมและจัดให้มีการซ้อมการดำเนินการตามแผน	✓	✓			
๗. แผนลดความเสี่ยงจากปัญหาของระบบเทคโนโลยีสารสนเทศ	- กำหนดแผนการฟื้นฟูจากหายนะเป็นลายลักษณ์อักษร กำหนดแผนการทดสอบและจัดให้มีการทดสอบตามแผน	✓				
	- จัดตั้งคณะทำงานกรณีเกิดภาวะฉุกเฉินและกำหนดผู้รับผิดชอบของแต่ละแผนกในกรณีที่เกิดภาวะฉุกเฉิน	✓				
	- กำหนดให้มีการตรวจเช็คระบบเทคโนโลยีสารสนเทศตามระยะเวลา - กำหนดให้มีการบำรุงรักษาระบบเทคโนโลยีสารสนเทศเชิงป้องกัน	✓				

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๗. แผนลดความเสี่ยงจากปัญหาของระบบเทคโนโลยีสารสนเทศ (ต่อ)	- กำหนดให้มีการสำรองข้อมูลหรืออุปกรณ์ที่จำเป็น - Upgrade Software ที่ใช้ - พิจารณาผลที่ได้รับจากการปฏิบัติตามแผนลดความเสี่ยงว่าสามารถป้องกันการเข้าถึงโดยทางกายภาพได้หรือไม่	✓				
๘. แผนลดความเสี่ยงจากปัญหาอื่นๆ	- หมั่นตรวจสอบข้อมูลด้านความปลอดภัยอื่นที่อาจก่อให้เกิดความเสียหาย	✓				
	- กำหนดแผนป้องกันมิให้ภัยคุกคามหรือขอความร่วมมือจากส่วนที่เกี่ยวข้อง - กำหนดแผนการฟื้นฟูจากภัยคุกคาม - กำหนดมาตรการรับมือกรณีเกิดเหตุฉุกเฉินและจัดซ้อมตามแผนประจำปี		✓			
๙. เฝ้าดูและแก้ไขปรับปรุงกระบวนการบริหารความเสี่ยง	**-** เฝ้าดูสถานะของแผนการรับมือกับความเสี่ยงด้านเทคโนโลยีสารสนเทศฯ ต่อการปฏิบัติตามแผนการรับมือกับความเสี่ยง - เฝ้าดูและสังเกตผลที่ได้รับจากการรับมือกับความเสี่ยง - เฝ้าดูความเสี่ยงใหม่ๆ เพื่อตรวจหาความเสี่ยงใหม่ๆ ที่มีต่อระบบข้อมูลสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข	✓				

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (พ.ศ.)				
		๒๕๕๗	๒๕๕๘	๒๕๕๙	๒๕๖๐	๒๕๖๑
๙. เฝ้าดูและแก้ไขปรับปรุงกระบวนการบริหารความเสี่ยง (ต่อ)	- เฝ้าดูการเปลี่ยนแปลงของความเสี่ยงเดิมโดยดูระดับความเสี่ยงที่อาจเพิ่มขึ้นหรือลดลง - การแก้ปัญหาในการรับมือกับความเสี่ยงที่ได้ดำเนินการไปแล้ว	✓				
	- การเปลี่ยนแปลงสถานะของความเสี่ยงที่มีต่อสำนักงานปลัดกระทรวงสาธารณสุข และเพิ่มเติมแผนการรับมือกับความเสี่ยงที่มีอยู่เพื่อรับมือกับความเปลี่ยนแปลงที่เกิดขึ้น		✓			

แหล่งอ้างอิง

สำนักงานคณะกรรมการพัฒนาระบบราชการ. คู่มือเทคนิคและวิธีการบริหารจัดการสมัยใหม่ตามแนว ทางการบริหารกิจการบ้านเมืองที่ดีเรื่องการวิเคราะห์และการบริหารความเสี่ยง. พิมพ์ครั้งที่ 2. กรุงเทพฯ : สหมิตรพริ้นติ้ง, 2549

Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004: Enterprise Risk Management – Integrated Framework Executive Summary.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, U.S. Department of Commerce, 2001

Government of Canada, Guide to Security Risk Management for Information Technology Systems, 1996

New South Wales Government, Commonwealth of Australia, Information Security Guidelines, Part I, Jun 2003

Krause, Micki and Harold F. Tipton, Handbook of Information Security Management: Risk Management and Business Continuity Planning, http://www.cccure.org/Documents/HISM/ewtoc.html

Treasury Board of Canada Secretariat, Integrated Risk Management Framework, http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp Dana Goulston, Presentation of Risk Management based on PMBOK