แผนการบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
สำนักงานสาธารณสุขจังหวัดพิจิตร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

คำนำ

สำนักงานสาธารณสุขจังหวัดพิจิตร ในฐานะที่เป็นหน่วยงานด้านการควบคุมนโยบาย แผนงาน กำกับ ดูแล ประเมินผล การปฏิบัติงานของหน่วยงานในสังกัดสำนักงานสาธารณสุขจังหวัดพิจิตร ให้ดำเนินงานไปอย่างมีประสิทธิภาพ โดยใช้ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) กระทรวงสาธารณสุข เป็นเครื่องมือขับเคลื่อนและผลักดันการดำเนินงานของหน่วยงานภายในสังกัด ให้สามารถนำยุทธศาสตร์ไปสู่การปฏิบัติได้อย่างมีประสิทธิภาพ และบรรลุตามเป้าประสงค์ของแผนยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) กระทรวงสาธารณสุข

การนำเทคโนโลยีสารสนเทศ มาใช้สนับสนุนการปฏิบัติงานและให้บริการแก่ประชาชน จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดพิจิตร ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ จึงเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และใช้เป็นแนวทางหรือมาตรการควบคุมป้องกันหรือลดความเสี่ยง เพื่อให้หน่วยงานในสังกัดบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม บุคลากรทุกระดับของหน่วยงานในสังกัดสำนักงานสาธารณสุขจังหวัดพิจิตร จึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ระดับที่สามารถรองรับได้ และทำให้การดำเนินงานของสำนักงานสาธารณสุขจังหวัดพิจิตร บรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น

สำนักงานสาธารณสุขจังหวัดพิจิตรหวังเป็นอย่างยิ่งว่า แม่บทและแผนการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ นี้จะช่วยลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลให้กระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของแม่บทและแผนการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพที่ดียิ่งขึ้น

สำนักงานสาธารณสุขจังหวัดพิจิตร

สารบัญ

ประกาศนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
สำนักงานสาธารณสุขจังหวัดพิจิตร

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙(๒) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จัดทำเพื่อเป็นแนวทางการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) ของสำนักงานสาธารณสุขจังหวัดพิจิตร ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็วมีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ใช้หลักการตามแนวทางการปฏิบัติที่ดีที่ใช้กันแพร่หลายทั่วโลกรวมถึงประเทศไทย ซึ่งคือหลักการกำกับดูแลการบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) ประกอบด้วย ๓ หลักการ ดังนี้

๑. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

๑.๑ จัดโครงสร้างองค์กร พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ตามหลักการควบคุมกำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ โดยมีผู้ที่ทำหน้าที่ควบคุมกำกับ ตรวจสอบ และสามารถทำหน้าที่ได้อย่างมีประสิทธิผล

๑.๒. กำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักงานสาธารณสุขจังหวัดพิจิตร จัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์ โดยมีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อย ดังนี้

๑. มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

๒. มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)

๓. บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการหน่วยงานเป็นวาระประจำ

๔. ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๕. ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

๒. การบริหารความเสี่ยง (Risk Management)

๒.๑ จัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร กรอบจะรวมถึง :

(ก) วิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(ข) การเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒.๒ เก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk register) ที่เกี่ยวข้องกับบริการที่สำคัญของสำนักงานสาธารณสุขจังหวัดพิจิตร

๒.๓ ติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอ เพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้

๓. นโยบายและแนวปฏิบัติ (Policies and Guidelines)

๓.๑ กำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของสำนักงานสาธารณสุขจังหวัดพิจิตรจากภัยคุกคามทางไซเบอร์ นโยบาย มาตรฐาน และแนวปฏิบัติจะต้อง :

(ก) สอดคล้องกับหลักประมวลแนวทางปฏิบัตินี้ ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ส่วนกลางกำหนด

(ข) เผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของสำนักงานสาธารณสุขจังหวัดพิจิตร

๓.๒ ทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของสำนักงานสาธารณสุขจังหวัดพิจิตร ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละหนึ่งครั้ง โดยนับถัดจากวันที่มีการทบทวนครั้งสุดท้าย หรือวันที่มีผลบังคับใช้ของนโยบาย มาตรฐาน หรือแนวปฏิบัติแต่ละข้อ

ทั้งนี้ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานสาธารณสุขจังหวัดพิจิตรนี้มีผลบังคับใช้นับถัดจากวันที่ประกาศ

ประกาศ ณ วันที่ ๙ พฤศจิกายน ๒๕๖๕

(นายแพทย์วิศิษฎ์ อภิสิทธิ์วิทยา)
นายแพทย์สาธารณสุขจังหวัดพิจิตร

บทที่ ๑
บทนำ

ยุทธศาสตร์สำนักงานสาธารณสุขจังหวัดพิจิตร ปีงบประมาณ พ.ศ. ๒๕๖๖ – ๒๕๗๐ มีเป้าหมายให้ประชาชนทุกคนในเขตเครือข่ายบริการได้รับบริการที่มีคุณภาพมาตรฐานทุกระดับและเข้าถึงเทคโนโลยีที่ทันสมัยในเขตเครือข่ายบริการได้ กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข สำนักงานสาธารณสุขจังหวัดพิจิตร จึงได้จัดทำแผนบริหารความเสี่ยงขึ้นเพื่อใช้เป็นแนวทางปฏิบัติในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร การบริหารงานจึงต้องมีการดำเนินการตาม IT Governance เพื่อให้เกิดการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศ ที่ส่งผลต่อการพัฒนาองค์กร

IT Governance คือหน้าที่และความรับผิดชอบในการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศควบคู่กับความสามารถด้านอื่นๆ ของคณะกรรมการและผู้บริหารระดับสูงที่ใช้เป็นกรอบในกระบวนการบริหารงานภายใน การปฏิบัติตามนโยบาย กลยุทธ์เพื่อสร้างศักยภาพ เพิ่มคุณค่าและการเติบโตอย่างยั่งยืนให้กับองค์กร โดยดำเนินการควบคู่ไปกับการกำกับดูแลที่ดี การบริหารความเสี่ยงตามองค์ประกอบของการจัดการด้าน IT เริ่มตั้งแต่การวางแผน การจัดองค์กร การดำเนินการและการควบคุม ทำให้เกิดการบริหารและบูรณาการที่เป็นระบบระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน ลดความเสี่ยง เพิ่มศักยภาพ โดยสามารถทำงานข้ามสายงานและประสานงานระหว่างองค์กรได้อย่างรวดเร็ว ทันเวลา มีประสิทธิภาพ สอดคล้องกับการดำเนินงานระดับต่างๆ จากการใช้ความสามารถและศักยภาพของเทคโนโลยีสารสนเทศ และทรัพยากรต่างๆ เพื่อผลักดันความสำเร็จของการจัดการองค์กรอย่างทั่วถึงเป็นกระบวนการ

เทคโนโลยีสารสนเทศ สร้างความเสี่ยงใหม่ๆ รวมทั้งการสูญเสียโอกาสที่ส่งผลต่อประสิทธิภาพประสิทธิผลในการดำเนินการ นอกจากนี้ยังกระทบต่อความน่าเชื่อถือและความถูกต้องในการตรวจสอบและการจัดทำรายงาน ซึ่งเป็นหัวใจของการบริหารและควบคุมภายในในการบริหารงานระดับต่างๆ ขององค์กร ดังนั้น การผสมผสานความสามารถด้านต่างๆ ขององค์กรกับศักยภาพของระบบงานและการจัดการเทคโนโลยีสารสนเทศที่ดี จึงเป็นทั้งหน้าที่และความรับผิดชอบที่ไม่อาจหลีกเลี่ยงของคณะกรรมการและผู้บริหารระดับสูงขององค์กรในปัจจุบันสำนักงานปลัดกระทรวงสาธารณสุขได้นำเทคโนโลยีสารสนเทศเข้ามาใช้ในการปฏิบัติงานหลายด้าน จึงตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเกิดขึ้นในระบบบริหารงาน การสั่งการและการปฏิบัติงาน การดำเนินงานดังกล่าวทำให้ข้อมูลและสารสนเทศต่าง ๆ ที่ใช้ในการบริหารงานมีปริมาณที่มากมาย มีความเคลื่อนไหวตลอดเวลา โดยเฉพาะอย่างยิ่งข้อมูลและสารสนเทศที่ใช้ในการให้บริการประชาชนทางด้านสาธารณสุข รวมทั้งข้อมูลและสารสนเทศที่สำนักงานสาธารณสุขจังหวัดพิจิตรต้องรับผิดชอบ กระบวนประมวลผลข้อมูลตามนโยบายสำคัญต่าง ๆ จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้นและเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด สำนักงานสาธารณสุขจังหวัดพิจิตรจึงได้จัดทำแผนบริหารความเสี่ยงขึ้นเพื่อใช้เป็นแนวทางปฏิบัติ เพื่อลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงาน

/๑. วัตถุประสงค์...

๑. วัตถุประสงค์

๑.๑ เพื่อให้ทุกกลุ่มงาน ในสำนักงานสาธารณสุขจังหวัดพิจิตร เข้าใจหลักการและกระบวนการบริหารความเสี่ยงของสำนักงานสาธารณสุขจังหวัดพิจิตร

๑.๒ เพื่อให้ผู้ปฏิบัติได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นได้ และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้อง

๑.๓ เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๑.๔ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับกลยุทธ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๕ เพื่อใช้เป็นเครื่องมือในการสร้างวัฒนธรรมการบริหารความเสี่ยงในทุก ๆ ระดับของสำนักงานสาธารณสุขจังหวัดพิจิตร

๒. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบเทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดพิจิตร มีความพร้อมใช้งานตอบสนองความต้องการของบุคลากรในการปฏิบัติงานอย่างต่อเนื่อง โดยมีระบบข้อมูลและสารสนเทศ เครื่องมืออุปกรณ์ด้านฮาร์ดแวร์ที่เกี่ยวข้องกับการรวบรวม ประมวลผล เก็บรักษา และเผยแพร่ข้อมูล สารสนเทศที่ช่วยในการสื่อสารได้อย่างรวดเร็วและครอบคลุม เช่น ใช้ระบบสารบรรณอิเล็กทรอนิกส์และเว็บไซต์เผยแพร่และแจ้งเวียนหนังสือ/เอกสารรายงานการประชุม ข้อสั่งการ แผนยุทธศาสตร์ และแผนปฏิบัติการต่าง ๆ รายงานผลการดำเนินงานประจำปี มีการใช้ email, Line และ Facebook สื่อสารไปยังกลุ่มเป้าหมาย และผู้ปฏิบัติในทุกระดับ สำหรับสถานการณ์เร่งด่วนจะใช้ระบบประชุมทางไกล (e-Conference) ด้วยระบบ Zoom หรือ Webex มีการจัดโครงสร้างพื้นฐานด้านเครือข่ายเทคโนโลยีสารสนเทศให้บริการแก่บุคลากรผู้ปฏิบัติงานทุกระดับ และเพื่อรองรับการจัดการระบบข้อมูลและสารสนเทศจากหน่วยงานในสังกัด (LAN/Wireless LAN) โดยใช้ INTERNET ความเร็ว ๕๐๐ Mbps ในการใช้ข้อมูลและสารสนเทศเพื่อการดำเนินงานจากระบบงานภายใน ปีงบประมาณ พ.ศ.๒๕๖๖ โดยมีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ทุกกลุ่มงานถือปฏิบัติเป็นแนวทางเดียวกัน มีการติดตั้งระบบรักษาความปลอดภัย (Network Security System) ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เพื่อให้ข้อมูลและสารสนเทศ Hardware และ Software มีความปลอดภัย นอกจากนี้ยังมีกลุ่มงานข้อมูลสารสนเทศ ทำหน้าที่บำรุงรักษา/เฝ้าระวัง/ตรวจสอบ/ปรับปรุงเพิ่มประสิทธิภาพการทำงานของ Network System ให้มีความทันสมัยเหมาะสมกับปริมาณความต้องการใช้ข้อมูลและสารสนเทศในปัจจุบัน การ Update ฐานข้อมูลสารสนเทศของหน่วยงานสังกัดสำนักงานสาธารณสุขจังหวัดพิจิตรทุกปี

๒.๑ ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software)

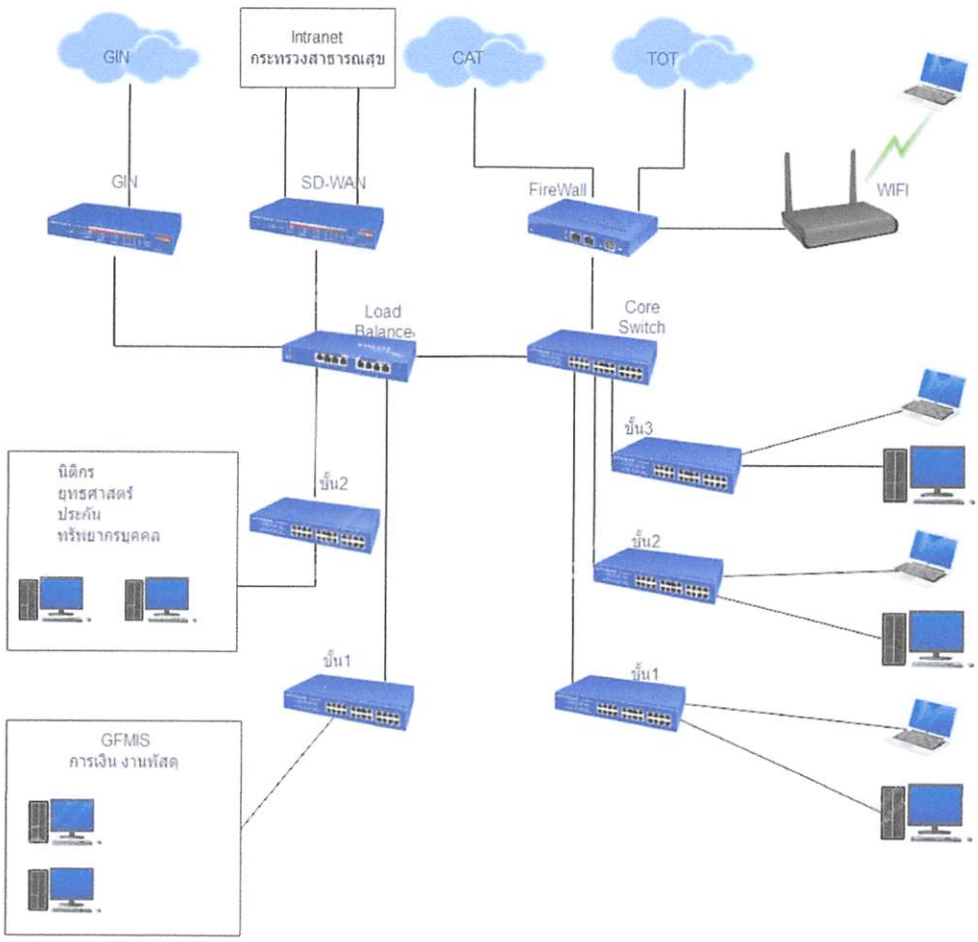
ลำดับ	ระบบงาน	ผู้รับผิดชอบ
๑	ระบบสารบรรณอิเล็กทรอนิกส์ (e-office)	กลุ่มงานธุรการและยานพาหนะ
๒	ระบบ Pay slip	กลุ่มงานการเงิน และกลุ่มงานพัฒนายุทธศาสตร์ฯ
๓	ระบบลาออนไลน์	กลุ่มงานบริหารทรัพยากรบุคคล

/๒. ระบบเครือข่าย...

๒.๒ ระบบเครือข่าย

ลักษณะทั่วไปของระบบเครือข่ายของสำนักงานสาธารณสุขจังหวัดพิจิตร เป็นระบบเครือข่ายคอมพิวเตอร์ในรูปแบบ LAN มีเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) มีการเช่าใช้เครือข่ายอินเตอร์เน็ตของบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เชื่อมต่อรูปแบบ Intranet ไปยังกระทรวงสาธารณสุข และใช้เครือข่าย GIN เป็นเครือข่ายสารสนเทศกลางของภาครัฐที่เชื่อมโยงหน่วยงานของภาครัฐเข้าด้วยกัน ระบบป้องกันความปลอดภัยมีระบบ Firewall ทำหน้าที่ตรวจสอบข้อมูลที่ผ่านเข้า-ออกระบบเครือข่าย มีการจัดเก็บ Log ทั้งภายในและภายนอก มีการรายงานสรุปการบุกรุกเครือข่ายทุกสัปดาห์

ผังเครือข่ายสำนักงานสาธารณสุขจังหวัดพิจิตร



๓. นโยบายการบริหารความเสี่ยง

เพื่อสร้างความตระหนักและกระตุ้นให้บุคลากรในสำนักงานสาธารณสุขจังหวัดพิจิตรเห็นถึงความจำเป็นในการระมัดระวังต่อสถานการณ์ที่คุกคามต่อประสิทธิภาพการปฏิบัติงาน การบริหารงาน และอาจทำให้เกิดความเสียหายต่อระบบฐานข้อมูลสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญในการให้บริการประชาชน และการตัดสินใจของผู้บริหาร แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนทศและการสื่อสาร สำนักงานสาธารณสุขจังหวัดพิจิตร จะทำให้บุคลากรทุกคนที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ ซึ่งจะถือเป็นส่วนหนึ่งของการดำเนินงาน การปฏิบัติงานเพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายต่างๆ ที่อาจเกิดขึ้น ซึ่งการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารให้มีประสิทธิภาพนั้นสำนักงานสาธารณสุขจังหวัดพิจิตร

/ใช้นโยบาย...

ใช้นโยบายความมั่นคงและปลอดภัยของระบบตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๔.๑ ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อระบบเทคโนโลยีสารสนเทศที่ใช้ในการบริหารงานและปฏิบัติการโดยเฉพาะอย่างยิ่งการบริการประชาชน

๔.๒ การควบคุม (Control หมายถึง ขั้นตอนการปฏิบัติ กระบวนการดำเนินงานหรือกลไกการปฏิบัติงานซึ่งกำหนดขึ้นเพื่อให้มั่นใจว่าการบริหารงานจะสามารถบรรลุวัตถุประสงค์ที่ได้กำหนดไว้

๔.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ ประเมิน จัดการและติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หรือกระบวนการดำเนินงานของหน่วยงาน รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้

๔.๔ การบริหารความเสี่ยงสำนักงานสาธารณสุขจังหวัดพิจิตรโดยรวม (Organization Wide Risk Management) หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการปฏิบัติงานต่างๆ โดยต้องลดมูลเหตุของแต่ละโอกาสที่จะทำให้สำนักงานสาธารณสุขจังหวัดพิจิตรเสียหาย

๔.๕ ระบบเทคโนโลยีสารสนเทศและการสื่อสารหมายถึง ระบบเครือข่ายคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์ ระบบเครื่องสื่อสาร ระบบฐานข้อมูล และอุปกรณ์ ประกอบระบบต่าง ๆ รวมทั้งอาคารสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด

๔.๖ ฐานข้อมูลสารสนเทศ หมายถึง ฐานข้อมูลที่สำนักงานสาธารณสุขจังหวัดพิจิตรใช้ในการปฏิบัติหน้าที่ซึ่งประกอบด้วย

๔.๖.๑ ฐานข้อมูลเพื่อการบริการประชาชน

๔.๖.๒ ฐานข้อมูลเพื่อการบริหารงานภายใน

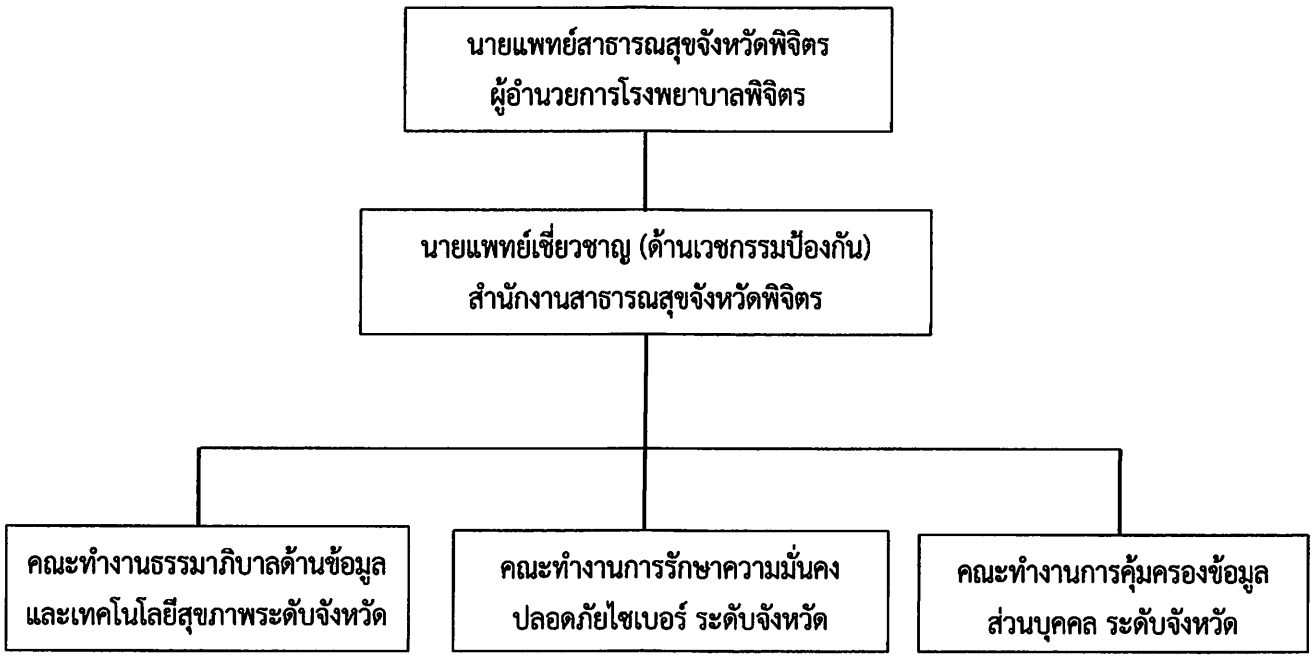
๔.๗ องค์ประกอบของความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔.๗.๑ ความน่าจะเป็น โอกาส หรือ ความไม่แน่นอน

๔.๗.๒ ผู้กระทำ (อาจเป็นได้ทั้งคน และที่ไม่ใช่คนเช่น อุบัติเหตุ ไฟฟ้าดับ ภัยธรรมชาติ)

/๕. โครงสร้าง...

๕. โครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดพิจิตร



ตามที่กระทรวงสาธารณสุขมีนโยบายมุ่งเน้น ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ประเด็นธรรมาภิบาลการพัฒนาระบบเทคโนโลยีสารสนเทศ (ICT) เป็นศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน ซึ่งการดำเนินงานให้ศูนย์ข้อมูลกลางด้านสุขภาพของประชาชนมีประสิทธิภาพและมีความมั่นคงปลอดภัยทางไซเบอร์ พร้อมให้บริการข้อมูลสุขภาพส่วนบุคคลแก่ประชาชนผู้เป็นเจ้าของข้อมูลและใช้ข้อมูลสุขภาพในการส่งเสริมการปรับพฤติกรรมสุขภาพด้วยการให้ความรู้สุขภาพ (Health Literacy) ผ่านระบบดิจิทัล สำนักงานสาธารณสุขจังหวัดพิจิตร จึงแต่งตั้งคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ การรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลระดับจังหวัด โดยมีองค์ประกอบ หน้าที่และอำนาจ ดังนี้

๕.๑ คณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพระดับจังหวัด

หน้าที่และอำนาจ

๑. นำนโยบายจากส่วนกลางไปสู่การปฏิบัติ และกำกับติดตาม ช่วยเหลือและแก้ปัญหาการดำเนินงาน ดังนี้

๑.๑ ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

๑.๒ การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

๑.๓ การเชื่อมโยงข้อมูลระหว่างระบบสถานพยาบาลและผู้รับบริการ ผ่าน HIS gateway

๑.๔ โครงการ 3-Refer

๑.๕ คุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล (HA IT)

๑.๖ IPD Paperless

/๒. กำหนดแนวทาง...

๒. กำหนดแนวทางและกำกับติดตาม การใช้ประโยชน์ข้อมูลสุขภาพส่วนบุคคลร่วมกันได้อย่างไร้รอยต่อ ภายใต้กฎหมายที่เกี่ยวข้อง การรับส่งข้อมูลตามมาตรฐานที่ตกลงร่วมกัน และการนำข้อมูลสุขภาพไปใช้ประโยชน์ในการให้บริการแก่ประชาชนในรูปแบบต่างๆ อย่างมีธรรมาภิบาลข้อมูล (Data Governance) ให้สอดคล้อง กับแนวทางจากส่วนกลาง และจัดให้มีการประชุมนำเสนอปัญหาอุปสรรคและผลการดำเนินงานในที่ประชุมผู้บริหารระดับจังหวัดเป็นประจำ

๓ ให้คำปรึกษาแนะนำ ช่วยเหลือและแก้ปัญหาการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) การคุ้มครองข้อมูลส่วนบุคคล (PDPA) ให้แก่หน่วยงานในสังกัดสำนักงานสาธารณสุขจังหวัดพิจิตร

๕.๒ คณะทำงานการรักษาความมั่นคงปลอดภัยไซเบอร์ ระดับจังหวัด

หน้าที่และอำนาจ

๑. ดูแลรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ให้มีประสิทธิภาพยิ่งขึ้น

๒. กำหนดมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากการบุกรุกโจมตีไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงหน่วยงาน

๕.๓ คณะทำงานการคุ้มครองข้อมูลส่วนบุคคลระดับจังหวัด

หน้าที่และอำนาจ

๑. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

๒. ตรวจสอบและการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

๓. รักษาความลับข้อมูลส่วนบุคคล

๔. กรณีมีปัญหาการเก็บรวบรวม ใช้ เปิดเผยข้อมูล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการจัดการปัญหาต่างๆ

/บทที่ ๒...

บทที่ ๒
การบริหารความเสี่ยง

๑. การเตรียมการและวางแผน

กำหนดความเสี่ยงที่มีโอกาสเกิดขึ้นต่อวัตถุประสงค์ ภารกิจ ความสำเร็จ สำนักงานสาธารณสุขจังหวัดพิจิตร มีพันธกิจคือการสร้างเสริมและปลูกฝังพฤติกรรมสุขภาพให้ประชาชน มีสุขภาพและจิตสำนึกที่ดีด้านสุขภาพ พัฒนาระบบสุขภาพให้คุณภาพ ประสิทธิภาพ ทั่วถึงและเป็นธรรม ส่งเสริมและสนับสนุนให้ภาคีเครือข่ายจากทุกภาคส่วนมีส่วนร่วมในการพัฒนาด้านสุขภาพ ค่านิยมองค์กร ซึ่งระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสิ่งหนึ่งที่จะช่วยสนับสนุนให้พันธกิจของสำนักงานสาธารณสุขจังหวัดพิจิตรไปถึงเป้าหมายบริการได้อย่างมีประสิทธิภาพ

๒. วิเคราะห์ปัญหาหรือโอกาสในองค์กร

ปัญหาหรือโอกาสในการบริหารความเสี่ยงของสำนักงานสาธารณสุขจังหวัดพิจิตร

<u>โอกาส</u> คือสิ่งที่จะมีส่วนช่วยให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ

ปัจจัยแห่งความสำเร็จ (Key Success Factors) เพื่อให้การดำเนินการตามกรอบนโยบายสำนักงานสาธารณสุขจังหวัดพิจิตรบรรลุผลตามเป้าหมาย สามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม คือ

๒.๑ ปัจจัยด้านอุปกรณ์ (Hardware)

๑. พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนการพัฒนาระบบสุขภาพของจังหวัดพิจิตร

๒. มีเครื่องมือในการเก็บรวบรวมข้อมูลที่มีประสิทธิภาพ สามารถเก็บรวบรวมข้อมูลได้ครบถ้วน มีคุณภาพตอบสนองความต้องการในการให้บริการสาธารณสุข และด้านบริหารจัดการของผู้บริหาร

๒.๒ ปัจจัยด้านซอฟต์แวร์ (Software)

๑. สร้างเสริมนวัตกรรมบริการและการวิจัยระบบ เครื่องมือและอุปกรณ์เพื่อเพิ่มประสิทธิภาพระบบบริการสาธารณสุข

๒. ประยุกต์ใช้เทคโนโลยีในกระบวนการจัดการและการให้บริการสาธารณสุข

๓. พัฒนาระบบเทคโนโลยีสารสนเทศการจัดการความรู้ด้านการแพทย์และสุขภาพสำหรับประชาชน

๔. พัฒนามาตรฐานในด้านการเชื่อมโยงแลกเปลี่ยนข้อมูล (Standard and Interoperability)

๒.๓ ปัจจัยด้านโครงข่ายเทคโนโลยีสารสนเทศ (ICT)

๑. สถานบริการสาธารณสุขทุกแห่งสามารถเข้าถึงบริการอินเตอร์เน็ตความเร็วสูงหรือการสื่อสารรูปแบบอื่นที่เป็น Broadband ได้อย่างทั่วถึง สะดวกและรวดเร็วโดยปลอดภัย

๒. ระบบ ICT ของสำนักงานสาธารณสุขจังหวัดพิจิตรมีความทันสมัย รวดเร็วทันต่อความก้าวหน้าของเทคโนโลยีและความเปลี่ยนแปลง สามารถรองรับกับการขยายตัวของการให้บริการ

/๔. ปัจจัยด้านบุคลากร...

๒.๔ ปัจจัยด้านบุคลากร

ผู้บริหารองค์กร

ผู้บริหารมีวิสัยทัศน์ ให้ความสำคัญ สนับสนุนและส่งเสริมการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการพัฒนาองค์กรรวมทั้งให้ความสำคัญต่อการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

ผู้ใช้งาน

๑. บุคลากรผู้ใช้งานส่วนใหญ่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศในระดับที่ใช้งานได้บุคลากรผู้ใช้งานมีความสนใจ และกระตือรือร้นในการใช้เทคโนโลยีสารสนเทศช่วยในการปฏิบัติงาน

๒. บุคลากรทุกคนสามารถใช้ E-mail และ Internet ในการประสานงานและสืบค้นข้อมูลเพื่อปฏิบัติงานในภารกิจได้อย่างมีประสิทธิภาพ

๓. บุคลากรทุกคนเห็นความสำคัญและให้ความร่วมมือในการปฏิบัติตามแผนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

ผู้ปฏิบัติงานด้าน ICT

๑. ผู้ปฏิบัติงานด้าน ICT ส่วนใหญ่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศในระดับที่ใช้งานได้

๒. ผู้ปฏิบัติงานด้าน ICT มีความสนใจ และกระตือรือร้นในการใช้เทคโนโลยีสารสนเทศช่วยในการปฏิบัติงาน

๓. ผู้ปฏิบัติงานด้าน ICT ให้ความร่วมมือในการปฏิบัติตามแผนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

๒.๕ ปัจจัยด้านข้อมูลสารสนเทศ

๑. พัฒนาระบบข้อมูลข่าวสารสุขภาพ มีคลังข้อมูล (Data Center) ซึ่งรวบรวมข้อมูลข่าวสารสุขภาพในระดับจังหวัด โดยเป็นข้อมูลที่สามารถนำไปใช้ประโยชน์ได้จริง ข้อมูลสามารถเชื่อมโยงและแลกเปลี่ยนกันได้

๒. มีการพัฒนารูปแบบการให้บริการข้อมูลขององค์กรในลักษณะสื่อสองทาง (Interactive) และส่งเสริมการมีส่วนร่วมของภาคประชาชน และบุคลากรผ่านระบบอินเทอร์เน็ต

๒.๖ ปัจจัยด้านการบริหารจัดการ

๑. มีการแต่งตั้งคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานสาธารณสุขจังหวัดพิจิตรเพื่อกำหนดทิศทางการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒. มีการใช้เทคโนโลยีสารสนเทศในการปฏิบัติงาน ทำให้สามารถลดขั้นตอน ระยะเวลาปฏิบัติงาน

๒.๗ ปัจจัยด้านงบประมาณ

ได้รับการสนับสนุนด้านงบประมาณอย่างต่อเนื่อง

๒.๘ ปัญหา/อุปสรรค

๑. ปัญหา/อุปสรรค ที่พบในระบบเทคโนโลยีสารสนเทศ

๑.๑ กระบวนการบริหารจัดการและบูรณาการทางด้านการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศภายในหน่วยงานยังไม่เป็นเอกภาพเท่าที่ควร

๑.๒ กระบวนการบริหารจัดการด้านความปลอดภัยยังไม่เป็นรูปธรรมเท่าที่ควร

/๒. ปัญหา/อุปสรรค...

๒. ปัญหา/อุปสรรคที่พบในความน่าเชื่อถือของข้อมูล

๑. ความไม่ชัดเจนของเอกสารเช่น เขียนไม่ชัดเจน

๒. เจ้าหน้าที่นำเข้าข้อมูลพิมพ์ผิด โดยไม่ได้สังเกต

๓. กำหนดขอบเขต

ขอบเขตของการบริหารความเสี่ยงสำนักงานสาธารณสุขจังหวัดพิจิตร ที่มีความสำคัญต่อวัตถุประสงค์ ภารกิจ สถานะ หรือความสำเร็จ

๔. กำหนดตัวบุคลากร

ใช้คณะกรรมการบริหารงานระบบข้อมูลและเทคโนโลยีสารสนเทศและการสื่อสาร (CHIEF INFORMATION OFFICER : CIO) จังหวัดพิจิตร ที่ ๙๔/๒๕๖๕ ลงวันที่ ๔ พฤศจิกายน ๒๕๖๕ และคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ การรักษาความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคลระดับจังหวัด ที่ ๑๖๖/๒๕๖๔ สั่ง ณ วันที่ ๒๗ ธันวาคม ๒๕๖๔

๕. จัดการรายละเอียดด้านกำหนดการ ส่วนสนับสนุนและอำนวยความสะดวก

เจ้าหน้าที่ผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยงเพื่อให้การดำเนินงานตามแผนเป็นไปอย่างรวดเร็วทันต่อการดำเนินการ โดยกำหนดให้เจ้าหน้าที่งานข้อมูลสารสนเทศเป็นผู้รับผิดชอบดำเนินการกำกับดูแล ควบคุมการดำเนินการ และจัดการความเสี่ยง

๕.๑ คณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ การรักษาความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคลระดับจังหวัด

บทบาทและความรับผิดชอบหลัก มีความเข้าใจถึงความเสี่ยงที่อาจมีผลกระทบร้ายแรงต่อองค์กร และทำให้มั่นใจว่ามีการดำเนินการที่เหมาะสมเพื่อจัดการความเสี่ยงนั้นๆ ติดตามกระบวนการบ่งชี้และประเมินความเสี่ยง ประเมินและอนุมัติแผนการจัดการความเสี่ยง

๕.๒ คณะกรรมการบริหารงานระบบข้อมูลและเทคโนโลยีสารสนเทศและการสื่อสาร (CHIEF INFORMATION OFFICER : CIO) จังหวัดพิจิตร

บทบาทและความรับผิดชอบหลัก ติดตามความเสี่ยงที่สำคัญทั้งองค์กร และมีแผนการจัดการที่เหมาะสม ส่งเสริมนโยบายการบริหารความเสี่ยงและปฏิบัติทั่วทั้งหน่วยงาน

๕.๓ หัวหน้าฝ่าย

บทบาทและความรับผิดชอบหลัก ระบุและรายงานความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงาน ร่วมจัดทำแผนจัดการความเสี่ยงและนำแผนไปปฏิบัติ

๕.๔ เจ้าหน้าที่ผู้ปฏิบัติงานในหน่วยงาน

บทบาทความรับผิดชอบหลัก ปฏิบัติตามแผน และนโยบายการบริหารความเสี่ยง

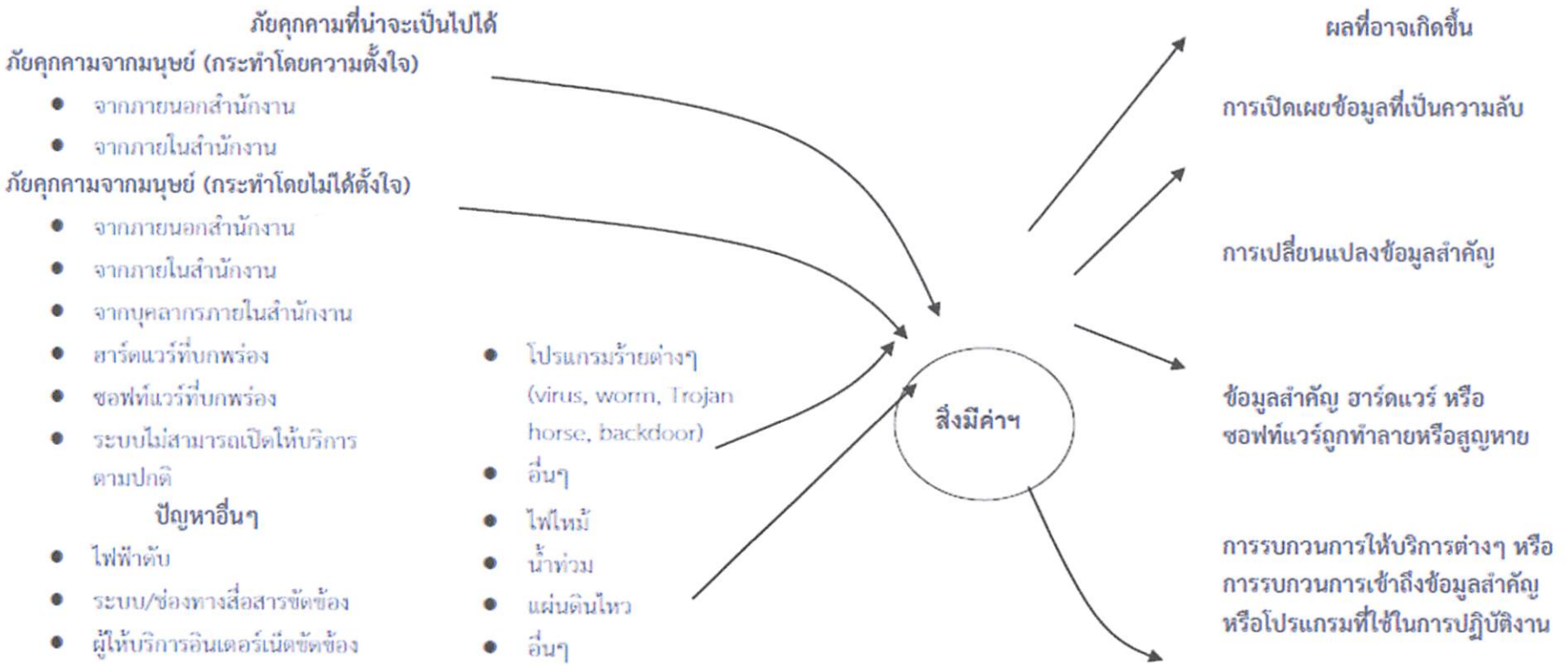
๕.๕ เจ้าหน้าที่งานข้อมูลสารสนเทศ

บทบาทความรับผิดชอบหลัก กำกับดูแล ควบคุมการดำเนินการ และจัดการความเสี่ยง

/๖. บ่งชี้ปัจจัยความเสี่ยง...

๖. บ่งชี้ปัจจัยความเสี่ยง

ผังเหตุการณ์หรือสถานการณ์ที่น่าจะเป็นภัยคุกคามต่อสิ่งมีค่า



/วิเคราะห์ความเสี่ยง...

๗. วิเคราะห์ความเสี่ยง

ตารางที่ ๑ ระบุความเสี่ยงและผลกระทบด้านต่างๆ ที่จะเกิดขึ้น

ปัจจัยเสี่ยง	ผลกระทบด้านต่างๆ			
	ชื่อเสียง	เวลา	การบริการ	บุคลากร
๑. ระบบงานและข้อมูล (System & Information) ทำงานไม่ได้ เสียหายและถูกทำลาย	๑. เจ้าหน้าที่ภายในหน่วยงานวิจารณ์ ๒. เจ้าหน้าที่ขาดความเชื่อมั่นต่อระบบเครือข่ายของหน่วยงาน	๑. เจ้าหน้าที่ในหน่วยงานไม่สามารถใช้ระบบงานและข้อมูลได้ ๒. เสียเวลาในการกู้คืนระบบงานและข้อมูล	เจ้าหน้าที่ไม่สามารถใช้ระบบงานและข้อมูลในการปฏิบัติงาน และการให้บริการ	๑. เจ้าหน้าที่ถูกตำหนิ ๒. เจ้าหน้าที่ดูแลระบบถูกตำหนิในเรื่องความสามารถในการดูแลระบบ
๒. ระบบให้บริการ Internet ล่ม	๑. เจ้าหน้าที่ภายในหน่วยงานวิจารณ์ ๒. เจ้าหน้าที่ขาดความเชื่อมั่นต่อระบบเครือข่ายของหน่วยงาน	๑. ทำให้ระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานไม่สามารถทำงานได้ ๒. ทำให้ไม่สามารถรับส่งข้อมูลที่สำคัญในการปฏิบัติงานอิเล็คทรอนิกส์	๑. เจ้าหน้าที่ไม่สามารถใช้ระบบสารสนเทศในการปฏิบัติงาน ๒. ประชาชนไม่สามารถใช้บริการผ่านระบบอินเตอร์เน็ต	เจ้าหน้าที่ถูกตำหนิในเรื่องความสามารถในการดูแลระบบ
๓. เครื่อง Server/Client ติดไวรัส	ถูกวิจารณ์ถึงประสิทธิภาพการทำงาน	๑. ทำให้ระบบสารสนเทศทำงานได้ช้าหรือทำงานไม่ได้ ๒. คอมพิวเตอร์ของเจ้าหน้าที่หยุดชะงัก ไม่สามารถทำงานได้	เจ้าหน้าที่ในหน่วยงานไม่สามารถปฏิบัติงานได้ คอมพิวเตอร์ไม่สามารถทำงานได้ปกติ	๑. เจ้าหน้าที่ถูกตำหนิในเรื่องการดูแลความปลอดภัยของระบบ ๒. การดำเนินงานของเจ้าหน้าที่หยุดชะงัก เสียเวลาในการจัดการกับไวรัส

/ตารางที่ ๑...

ตารางที่ ๑ ระบุความเสี่ยงและผลกระทบด้านต่างๆ ที่จะเกิดขึ้น (ต่อ)

ปัจจัยเสี่ยง	ผลกระทบด้านต่างๆ			
	ชื่อเสียง	เวลา	การบริการ	บุคลากร
๔. การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่	๑. เป็นข่าวในสื่อต่างๆ ๒. ประชาชนวิจารณ์ถึงประสิทธิภาพการทำงานของหน่วยงาน	ใช้เวลาในการทบทวนติดตาม/ตรวจสอบข้อมูลรวมทั้งเวลาในการเรียกคืนความเชื่อมั่นจากผู้รับบริการ	ไม่สามารถให้บริการข้อมูลที่ผิดพลาดจากความเป็นจริง	เจ้าหน้าที่ถูกตำหนิในการเสนอข้อมูลไม่ระมัดระวัง/ไม่ดูแลรักษาความลับของข้อมูล
๕. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ถูกวิจารณ์ถึงประสิทธิภาพการทำงาน	การทำงานหยุดชะงัก	เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	ผู้ดูแลระบบถูกตำหนิ
๖. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เช่น ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ	เป็นข่าวในสื่อต่างๆ	ระบบเสียหาย การทำงานหยุดชะงัก และต้องใช้เวลาในการกู้คืนและปรับปรุงระบบนาน	ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหาย ต้องดำเนินการตัดกระแสไฟฟ้า และไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	ถูกตำหนิในเรื่องความสามารถในการป้องกันและเตรียมการในการดูแลระบบ
๗. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในพื้นที่	-	ต้องใช้เวลาในการดำเนินงานและปรับปรุงระบบในช่วงเวลาที่ไม่สามารถดำเนินการได้	บุคลากรไม่สามารถปฏิบัติงานและให้บริการได้ตามปกติ	บุคลากรไม่สามารถปฏิบัติงานและให้บริการได้ตามปกติ

/๘. วางแผนการรับมือ...

๘. วางแผนการรับมือกับความเสี่ยง

ตารางที่ ๒ แนวทางในการจัดการ/ควบคุมความเสี่ยง

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	แนวทางการควบคุม
๑. ระบบงานและข้อมูล (System & Information) ทำงานไม่ได้ เสียหาย หรือถูกทำลาย	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน/โดน Virus โจมตี/ Hacker/Cracker	๑. เจ้าหน้าที่ในหน่วยงานไม่สามารถใช้ระบบงานและข้อมูลได้ ๒. ไม่สามารถให้บริการผู้ที่ต้องการใช้ระบบงานและข้อมูลได้ ทำให้เจ้าหน้าที่/ผู้ดูแลระบบถูกตำหนิ	๑. จัดทำระบบงานและขอมูลสำรองให้ทำงานแทนเมื่อระบบหลักเกิดปัญหา (ระบบ Database Backup) ๒. หน่วยงานมีผู้ดูแลระบบงานและข้อมูล ๓. มีการจัดอบรมเพื่อให้ความรู้ด้านการดูแลรักษาความปลอดภัยของระบบงานและข้อมูลแก่ผู้ใช้ระบบ
๒. ระบบให้บริการ Internet ล่ม	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	หน่วยงานไม่สามารถให้บริการผ่านทางอินเตอร์เน็ต	จัดให้มีการเชื่อมต่อกับ Internet service provider (ISP) สำรอง
๓. การนำเสนอข้อมูลผิดพลาด/ข้อมูลสำคัญที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือเผยแพร่	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ประชาชนไม่มั่นใจในกระบวนการรักษาความปลอดภัยของข้อมูลของหน่วยงาน ทำให้ตกเป็นข่าวในสื่อต่างๆ	๑. จัดทำและประกาศใช้นโยบายการดูแลและการใช้งานข้อมูลที่เป็นความลับขององค์กร ๒. จัดทำระบบรักษาความปลอดภัยของข้อมูลที่มีระดับชั้นความลับสูง ๓. จัดอบรมให้ความรู้ด้านความปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ทุกระดับ

/ตารางที่ ๒...

ตารางที่ ๒ แนวทางในการจัดการ/ควบคุมความเสี่ยง (ต่อ)

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	แนวทางการควบคุม
๔. เครื่อง Server ติดไวรัส	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ระบบสารสนเทศ ระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้	๑. จัดหาระบบป้องกันความปลอดภัย Firewall ๒. จัดทำและประกาศใช้นโยบายการป้องกันไวรัส ๓. ติดตั้งระบบป้องกันไวรัสในส่วนของ Sever ๔. ทำการ update virus signature อย่างสม่ำเสมอ ๕. ให้ความรู้เกี่ยวกับการป้องกันไวรัสและการใช้งานระบบสารสนเทศอย่างปลอดภัยให้แก่ผู้ดูแลระบบ
๕. เครื่อง Client ติดไวรัส	ความเสี่ยงจากผู้ปฏิบัติงานนำอุปกรณ์เคลื่อนที่ (Smart Phone, Tablet PC) ส่วนตัวเข้ามาเชื่อมต่อ รวมถึงการดาวน์โหลดโปรแกรมหรือไฟล์จากอินเตอร์เน็ตโดยขาดความระมัดระวัง	๑. ส่งผลกระทบต่อการใช้งานระบบเครือข่าย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย ๒. ทำให้เครื่องของเจ้าหน้าที่ทำงานไม่ได้	๑. ฝึกอบรม เผยแพร่และประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องของความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากร ๒. จัดทำและประกาศใช้นโยบายการป้องกันไวรัสและติดตั้งระบบป้องกันไวรัสในเครื่องของ User และให้ทำการ update virus อย่างสม่ำเสมอ ๓. กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง ๔. กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

/ตารางที่ ๒...

ตารางที่ ๒ แนวทางในการจัดการ/ควบคุมความเสี่ยง (ต่อ)

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	แนวทางการควบคุม
๖. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ทำให้ระบบสารสนเทศ ระบบสำคัญทำงานได้ช้า หรือทำงานไม่ได้ ระบบงาน/ข้อมูลเสียหรือสูญหาย	๑. บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ ๒. เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล ๓. เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในหน่วยงานด้วย ๔. ให้ความรู้และความเข้าใจแก่บุคลากรของหน่วยงานในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ

/ตารางที่ ๒...

ตารางที่ ๒ แนวทางในการจัดการ/ควบคุมความเสี่ยง(ต่อ)

ปัจจัยเสี่ยง	ที่มาของปัจจัยเสี่ยง	ความเสียหายที่อาจเกิดขึ้น	แนวทางการควบคุม
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ)	๑. ไฟไหม้จากอุบัติเหตุ ไฟฟ้าลัดวงจร การวางเพลิง ๒. ภัยธรรมชาติ	ทำให้เครื่องคอมพิวเตอร์ถูกทำลายหรือเสียหาย	๑. มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของหน่วยงาน ๒. มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนฯ
๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในพื้นที่	ชุมนุมประท้วง ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เช่น การจลาจลการก่อการร้าย	การเกิดสถานการณ์ ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๑. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง ๒. จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ ๓. สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด

/๙. แนวทางในการจัดการ...

๙. แนวทางในการจัดการ/ควบคุมความเสี่ยง

ตารางที่ ๓ แนวทางการจัดทำแผนลดความเสี่ยงในระดับยุทธศาสตร์ ด้านเทคโนโลยีสารสนเทศ (ปี ๒๕๖๖ – ๒๕๗๐)

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (ปีงบประมาณ พ.ศ.)				
		๒๕๖๖	๒๕๖๗	๒๕๖๘	๒๕๖๙	๒๕๗๐
๑. บุคลากร	๑. จัดอบรมพัฒนาศักยภาพบุคลากรที่ดูแลระบบสารสนเทศของหน่วยงาน	/				
	๒. บุคลากรที่ดูแลระบบสารสนเทศของหน่วยงาน ได้รับการอบรมพัฒนาศักยภาพจากส่วนกลาง Onsite หรือ Online	/	/	/	/	/
๒. ยุทธศาสตร์ความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	กำหนดยุทธศาสตร์ความปลอดภัยของระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับยุทธศาสตร์และเป้าหมายของหน่วยงาน โดยกำหนดให้มีการทบทวนตามระยะเวลาที่กำหนด ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข	/				
๓. การบริหารเกี่ยวกับความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	๑. จัดทำงบประมาณสำหรับกิจกรรมด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อเสนออนุมัติจากผู้บริหาร โดยกำหนดกิจกรรมที่จำเป็นด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศในหน่วยงาน ๒. จัดให้มีการประชุมทบทวนกระบวนการบริหารความเสี่ยงของหน่วยงานหลังจากที่ได้เริ่มบริหารความสี่ยงแล้วจัดทำรายงานต่อฝ่ายบริหารเมื่อเกิดปัญหาด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศในหน่วยงาน	/	/	/	/	/

/ตารางที่ ๓...

ตารางที่ ๓ แนวทางการจัดทำแผนลดความเสี่ยงในระดับยุทธศาสตร์ ด้านเทคโนโลยีสารสนเทศ (ปี ๒๕๖๖ – ๒๕๗๐) (ต่อ)

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (ปีงบประมาณ พ.ศ.)				
		๒๕๖๖	๒๕๖๗	๒๕๖๘	๒๕๖๙	๒๕๗๐
๓.๑ ความปลอดภัยทางกายภาพ	๑. ประกาศมาตรการที่ใช้ในการป้องกันรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	/				
	๒. กำหนดแผนรับมือกรณีเกิดภัยคุกคาม	/	/	/	/	/
	๓. อุดช่องโหว่ทางกายภาพ	/	/	/	/	/
	๔. ส่งบุคลากรเข้ารับการอบรมเกี่ยวกับความปลอดภัยทางกายภาพ	/	/	/	/	/
	๕. ตรวจสอบข้อมูลปัญหาทางด้านกายภาพที่เกิดขึ้นในปัจจุบัน	/	/	/	/	/
	๖. กำหนดงบประมาณสำหรับการรักษาความปลอดภัยทางกายภาพของหน่วยงานโดยดูจากระดับความรุนแรงของปัญหาด้านความปลอดภัยที่ผ่านมา	/	/	/	/	/
	๗. ทบทวนนโยบายและระเบียบของหน่วยงานว่าเพียงพอสำหรับการรักษาความปลอดภัยทางกายภาพของหน่วยงานให้อยู่ในระดับที่เหมาะสมหรือไม่ โดยดูจากปัญหาที่ผ่านมาและปรับปรุงนโยบายและระเบียบที่มีการประกาศใช้	/	/	/	/	/
	๘. หมั่นตรวจสอบข้อมูลปัจจุบันที่เกี่ยวกับความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	/	/	/	/	/
๓.๒ ความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	๑. หมั่นตรวจสอบข้อมูลปัจจุบันที่เกี่ยวกับความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	/	/	/	/	/
	๒. กำหนดงบประมาณสำหรับการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ โดยดูจากปัญหาที่ผ่านมา	/	/	/	/	/

/ตารางที่ ๓...

ตารางที่ ๓ แนวทางการจัดทำแผนลดความเสี่ยงในระดับยุทธศาสตร์ ด้านเทคโนโลยีสารสนเทศ (ปี ๒๕๖๖ – ๒๕๗๐) (ต่อ)

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (ปีงบประมาณ พ.ศ.)				
		๒๕๖๖	๒๕๖๗	๒๕๖๘	๒๕๖๙	๒๕๗๐
๓.๒ ความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	๓. กำหนดนโยบายและระเบียบของหน่วยงานทางด้านการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศของหน่วยงาน และทบทวนเพื่อปรับปรุงนโยบายและระเบียบของหน่วยงานตามวาระ	/	/	/	/	/
	๔. กำหนดและแต่งตั้งผู้รับผิดชอบหลักในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	/				
๓.๓ การปฏิบัติของบุคลากร	๑. จัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการปฏิบัติงานในเรื่องความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	/				
	๒. กำหนดงบประมาณสำหรับการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศโดยดูจากปัญหาที่ผ่านมา	/	/	/	/	/
	๓. กำหนดนโยบายและระเบียบของหน่วยงานทางด้านการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศของหน่วยงาน และทบทวนเพื่อปรับปรุงนโยบายและระเบียบของหน่วยงานตามวาระ	/	/	/	/	/
	๔. กำหนดและแต่งตั้งผู้รับผิดชอบหลักในการรักษาความปลอดภัยทางระบบเทคโนโลยีสารสนเทศ	/				

/ตารางที่ ๓...

ตารางที่ ๓ แนวทางการจัดทำแผนลดความเสี่ยงในระดับยุทธศาสตร์ ด้านเทคโนโลยีสารสนเทศ (ปี ๒๕๖๖ – ๒๕๗๐) (ต่อ)

หัวข้อหลัก	หัวข้อย่อย	เป้าหมาย (ปีงบประมาณ พ.ศ.)				
		๒๕๖๖	๒๕๖๗	๒๕๖๘	๒๕๖๙	๒๕๗๐
๔. นโยบายและระเบียบปฏิบัติด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงาน	๑. กำหนดนโยบายด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงาน และทำสำเนาแจกจ่ายให้กับทุกกลุ่มงานทราบและปฏิบัติ	/				
	๒. ตรวจสอบกฎหมาย, พ.ร.บ. หรือระเบียบใด ๆ ที่เกี่ยวข้องกับความปลอดภัยของระบบเทคโนโลยีสารสนเทศและนำมาปรับใช้เป็นแนวทางปฏิบัติ	/				
	๓. ประกาศใช้นโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศภายในหน่วยงาน และกำหนดให้มีการทบทวนนโยบายให้สอดคล้องกับกฎหมาย, พ.ร.บ. หรือระเบียบแนวทางปฏิบัติ	/				
๕. ความร่วมมือในการบริหารความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	๑. กำหนดนโยบายด้านความปลอดภัยในการปกป้องข้อมูลเมื่อปฏิบัติงานร่วมกับหน่วยงานอื่นหรือผู้ใช้บริการโดยการกำหนดเป็นข้อตกลงร่วมกันไว้เป็นลายลักษณ์อักษร	/				
	๒. มีกระบวนการตรวจสอบว่าหน่วยงานมีการปกป้องข้อมูลและระบบที่สำคัญอย่างเหมาะสมหรือไม่	/	/	/	/	/
	๓. สรุปข้อมูลการตรวจสอบการปกป้องข้อมูลและระบบที่สำคัญ แล้วนำมาเทียบเคียงกับปัญหาเกิดขึ้น แล้วปรับปรุงวิธีการตรวจสอบ	/	/	/	/	/

/ตารางที่ ๓...