แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ

กรมสนับสนุนบริการสุขภาพ

พ.ศ. ๒๕๖๔ - ๒๕๖๖

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

คำนำ

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ได้จัดทำ “แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ - ๒๕๖๖” ขึ้นเพื่อเป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับผู้บริหาร บุคลากรภายในกรมสนับสนุนบริการสุขภาพ ตามแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศด้วยมาตรฐานการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ และมาตรฐานสากล เช่น NIST เพื่อให้กรมสนับสนุนบริการสุขภาพได้รับความเชื่อมั่นและมีความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ รวมทั้งส่งเสริมการทำธุรกรรมอิเล็กทรอนิกส์ด้านระบบบริการสุขภาพ ตามนโยบายก้าวสู่เศรษฐกิจดิจิทัล (Digital Economy)

หวังเป็นอย่างยิ่งว่าแผนยุทธศาสตร์ฉบับนี้ จะเป็นประโยชน์ต่อผู้บริหาร บุคลากรและผู้เกี่ยวข้องด้านเทคโนโลยีสารสนเทศภายในกรมสนับสนุนบริการสุขภาพ ต่อไป

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข
๑ ตุลาคม ๒๕๖๓

สารบัญ

สารบัญแผนภาพ / ตาราง

หน้า

แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. ๒๕๖๔ – ๒๕๖๖

ชื่อหน่วยงาน กรมสนับสนุนบริการสุขภาพ

๑. หลักการและเหตุผลการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง ที่กรมสนับสนุนบริการสุขภาพเป็นหน่วยงานหลัก (Main Regulator) ในการควบคุม กำกับ ดูแลการดำเนินกิจการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสุขภาพ (CII : Critical Information Infrastructure in Healthcare Service) ที่มีผลกระทบต่อประชาชนโดยตรง (Impact Security Risk และ Economics Public Health) จากการเชื่อมโยงข้อมูลสารสนเทศ (Interconnected Information System) เพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการ ข้อมูลสารสนเทศจำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ

กรมสนับสนุนบริการสุขภาพ มีภารกิจในการคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพและส่งเสริมผู้ประกอบการด้านระบบบริการสุขภาพ จากการขึ้นทะเบียนและออกใบอนุญาตสถานพยาบาลและสถานประกอบการเพื่อสุขภาพ (e-Registration) เป็นหน่วยงานที่เกี่ยวข้องกับการเก็บรักษาข้อมูลส่วนบุคคล (Data Privacy Protection) ด้านธุรกิจบริการสุขภาพระหว่างภาครัฐและเอกชน สนับสนุนการทำธุรกรรมอิเล็กทรอนิกส์ (e-Commerce) ด้านระบบบริการสุขภาพทั้งภายในและต่างประเทศ ส่งเสริมการพัฒนานวัตกรรมดิจิทัล (Digital Innovation) รวมทั้งเป็นหน่วยงานควบคุม กำกับมาตรฐานระบบบริการสุขภาพ ด้านที่ ๙ การรักษาความมั่นคงปลอดภัยไซเบอร์

ดังนั้น **“เพื่อให้กรมสนับสนุนบริการสุขภาพได้รับความเชื่อมั่นและมีความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ รวมทั้งส่งเสริมการทำธุรกรรมอิเล็กทรอนิกส์ด้านระบบบริการสุขภาพ”** ในการติดตาม ควบคุมกำกับความมั่นคงปลอดภัย (Enterprise Risk Management) ของระบบสารสนเทศ ที่กำหนดให้กรมสนับสนุนบริการสุขภาพผ่านเกณฑ์ประเมินมาตรฐานความมั่นคงปลอดภัยสารสนเทศ[๑] รวมทั้งเป็นการดำเนินงานตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ ที่ประกาศในราชกิจจานุเบกษา เมื่อวันที่ ๒๗ พฤษภาคม พ.ศ.๒๕๖๒ แล้วนั้น **เป็นการเพิ่มขีดความสามารถในการแข่งขัน การพัฒนาเศรษฐกิจดิจิทัลในการขับเคลื่อนยุทธศาสตร์ชาติ** อันเป็นนโยบายสำคัญเร่งด่วนของรัฐบาลและเพิ่มรายได้สู่ประเทศ ตามนโยบายก้าวสู่**เศรษฐกิจดิจิทัล (Digital Economy)**

๒. วิสัยทัศน์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

“กรมสนับสนุนบริการสุขภาพ ผ่านการประเมินมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ภายใน ปี พ.ศ. ๒๕๖๖”

๓. พันธกิจการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑. สร้างความมั่นคงปลอดภัยด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ รวมทั้งส่งเสริมการทำธุรกรรมอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพตามมาตรฐาน

๒. ส่งเสริม สนับสนุนการพัฒนาความรู้ ความสามารถของบุคลากรทุกระดับ กรมสนับสนุนบริการสุขภาพในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓. สร้างความเชื่อมั่นในการเข้าถึงและใช้ประโยชน์จากข้อมูลสารสนเทศของกรมสนับสนุนบริการสุขภาพ

[๑] มาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ตามมติ คณะกรรมการเทคโนโลยีสารสนเทศ (ICT) กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๕๗

๔. วัตถุประสงค์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑. เพื่อให้กรมสนับสนุนบริการสุขภาพมีแนวทางการดำเนินงานตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ

๒. เพื่อให้ผู้บริหารและบุคลากรทุกระดับของกรมสนับสนุนบริการสุขภาพ มีความรู้ ความเข้าใจและทักษะในการรักษาความมั่นคงปลอดภัยสารสนเทศ

๓. เพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการที่เกี่ยวข้องกับข้อมูลสารสนเทศด้านระบบบริการสุขภาพ รวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ของกรมสนับสนุนบริการสุขภาพ

๕. แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑: ๒๐๑๓ ในประเด็นที่เกี่ยวข้อง ดังนี้

๑. ด้านบุคลากร (People) ได้กำหนดการพัฒนาศักยภาพบุคลากร กรมสนับสนุนบริการสุขภาพ ตามแนวทางการพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ ของสำนักงานคณะกรรมการข้าราชการพลเรือน (กพ.) (Cyber Security Liteacy) ได้แก่

๑.๑ การฝึกซ้อมรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber drill) สำหรับบุคลากรทุกระดับ

๑.๒ การพัฒนาความรู้พื้นฐาน ในการสร้างความตระหนักและการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Awareness) สำหรับผู้ใช้งาน (User)

๑.๓ การพัฒนาความรู้ความสามารถในการตรวจสอบ วิเคราะห์ เจาะระบบเทคโนโลยีสารสนเทศด้วยวิธีการตรวจสอบช่องโหว่ Vulnerability Assessment (Web Application Hacking) และการเจาะระบบ (Penetration Testing) สำหรับผู้ดูแลระบบ (System Administrator)

๑.๔ การเตรียมความพร้อมของบุคลากร ในการจัดตั้ง “ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ (HSS SOC Team : Health Service Support Security Operation Center)” ในการเป็นศูนย์รวมของทั้งหน่วยงานจริงและในรูปแบบเสมือนในการทดสอบระบบเชิงยุทธศาสตร์ ตรวจสอบภัยคุกคาม แจ้งเตือน กู้คืนเอื้อต่อการตอบสนองด้านความปลอดภัยและเหตุการณ์ฉุกเฉิน (IDR: ป้องกันภัยคุกคามและความเสี่ยง) รวมทั้งเฝ้าระวังและแจ้งเตือนสถานพยาบาล ตามแนวทางมาตรฐานสถานพยาบาลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ด้านการบริหารจัดการ (Process) การบริหารจัดการความเสี่ยง (Risk Management) ตามแนวทางมาตรฐานที่กำหนดให้เป็นไปในแนวปฏิบัติเดียวกัน เพื่อให้ผ่านการประเมินมาตรฐานความมั่นคงปลอดภัยสารสนเทศตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ (Cyber Security) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) รวมทั้งกฎหมายที่เกี่ยวข้อง

๓. ด้านเทคโนโลยี (Technology) ครุภัณฑ์ การจัดเก็บรวบรวมครุภัณฑ์คอมพิวเตอร์ (Asset Management) เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment/Risk Management)

๔. การจัดสรรงบประมาณ (Budget) สำหรับการดำเนินงานให้ประสบผลสำเร็จตามเป้าหมาย รวมทั้งการตรวจประเมินมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ด้วยมาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๑๓ หรือมาตรฐานอื่นตามนโยบายที่กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุขกำหนด

ในปีงบประมาณ พ.ศ.๒๕๖๒ - ๒๕๖๓ กรมสนับสนุนบริการสุขภาพ ได้เตรียมความพร้อมตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ในประเด็นบุคลากร (People) ด้วยการพัฒนาศักยภาพบุคลากรเกี่ยวกับการสร้างความตระหนักและการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Awareness for User) ผ่านกระบวนการฝึกซ้อมรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber drill) การพัฒนาความรู้พื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ และสำหรับผู้ดูแลระบบ (System Administrators) และกระบวนการทำงาน (Process) ในด้านการ

ตรวจสอบระบบเทคโนโลยีสารสนเทศด้วยวิธีการตรวจสอบช่องโหว่ (Vulnerability Assessment) เช่น Web Application Hacking การเจาะระบบ (Penetration Testing) และผลการวิเคราะห์ช่องว่างมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (Gap Assessment) เพื่อเตรียมความพร้อมในการตรวจประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

เพื่อให้การดำเนินงานมีประสิทธิภาพ และเกิดประสิทธิผลตามเป้าหมาย จึงได้กำหนดการดำเนินงานเป็น ๔ ระยะ จำแนกเป็น ๕ ขั้นตอน ดังนี้

Phase I: Scoping & Planning ประกอบด้วย ขั้นตอนที่ ๑ กำหนดวัตถุประสงค์การดำเนินงาน สอดคล้องตามนโยบาย ประกอบด้วย การทบทวน กำหนด รายละเอียด ขั้นตอนของการดำเนินงานสอดคล้องตามนโยบาย

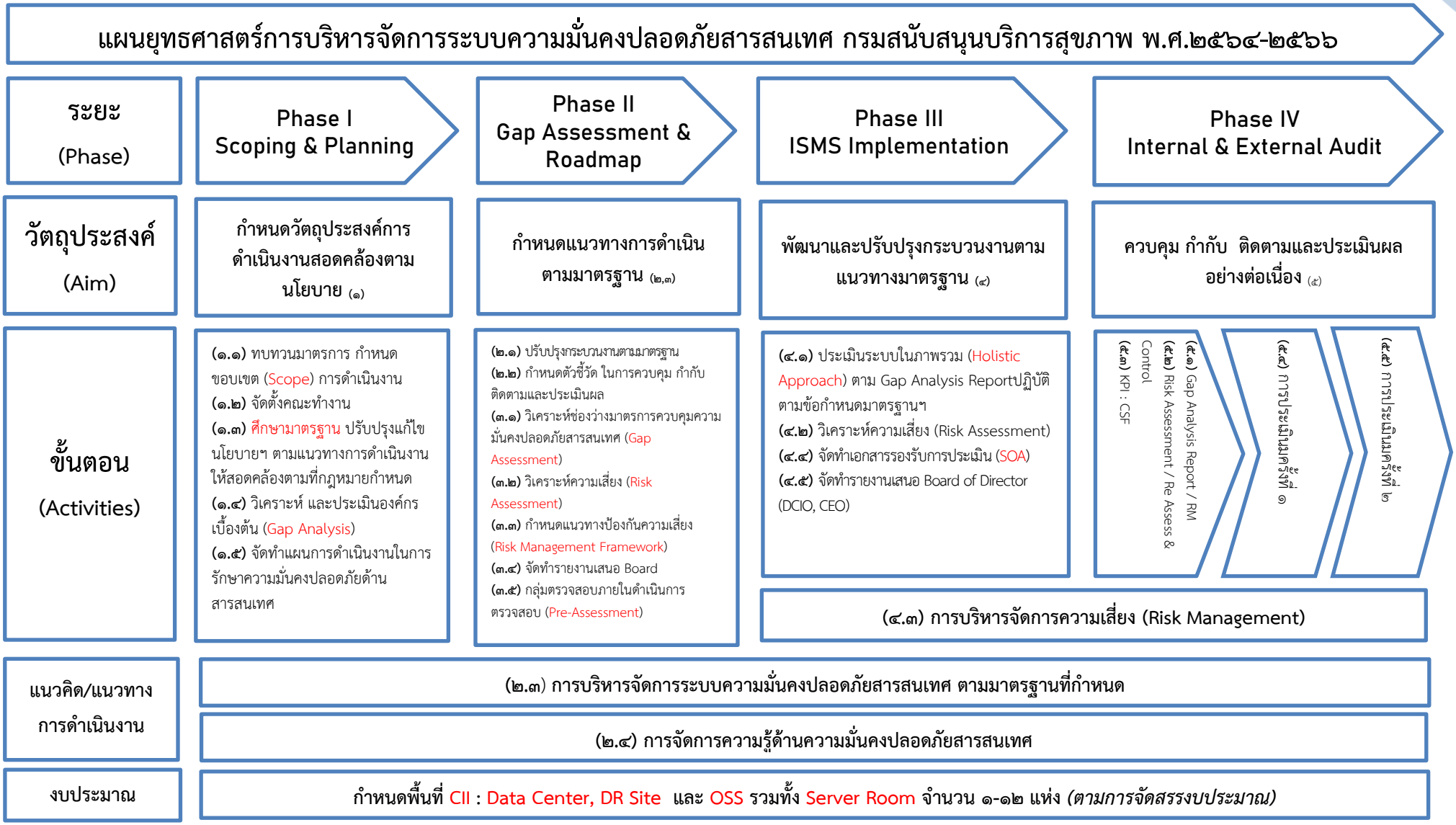
Phase II: Gap Assessment & Roadmap ประกอบด้วย ขั้นตอนที่ ๒ กำหนดแนวทางการดำเนินงานตามมาตรฐาน ประกอบด้วย การทำความเข้าใจกับกระบวนการ วางแผนการดำเนินงาน กำหนดตัวชี้วัด และขั้นตอนที่ ๓ วิเคราะห์ หาสาเหตุ โดยการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๑๓ (Gap Assessment)

Phase III: ISMS Implementation ประกอบด้วย ขั้นตอนที่ ๔ พัฒนาและปรับปรุงกระบวนงานตามมาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๑๓

Phase IV: Internal & External Audit ประกอบด้วย ขั้นตอนที่ ๕ ควบคุม กำกับ ติดตาม และประเมินผลอย่างต่อเนื่อง

ดังแผนภาพที่ ๑ แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ พ.ศ. ๒๕๖๔ – ๒๕๖๖

แผนภาพที่ ๑ แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ พ.ศ.๒๕๖๔ – ๒๕๖๖



ขั้นตอนที่ ๑ กำหนดวัตถุประสงค์การดำเนินงาน สอดคล้องตามนโยบาย ประกอบด้วย การทบทวน กำหนดรายละเอียด ขั้นตอนของการดำเนินงานสอดคล้องตามนโยบาย

๑.๑ ทบทวนมาตรการ กำหนดขอบเขตการทำงาน (Scope)

๑.๑.๑ กำหนดขอบเขตการดำเนินงาน Server & Network (HSS Net) ซึ่งประกอบด้วย

๑) กระบวนการทำงาน (Process)

๒) ข้อมูลและสารสนเทศ (Information)

๓) ฮาร์ดแวร์ (Hardware)

๔) การบริหารจัดการทรัพย์สิน (Asset management)

๕) ซอฟต์แวร์ (Software)

๖) เครือข่ายคอมพิวเตอร์ (Network)

๗) เครื่องแม่ข่ายเสมือน (Virtual Machine)

๘) บุคลากร (Personnel)

๙) สถานที่และระบบสนับสนุน (Site)

๑.๑.๒ ภายนอกขอบเขต Server & Network (HSS Net)

๑) ระบบงาน ที่ไม่เกี่ยวข้องกับระบบงานของกรมสนับสนุนบริการสุขภาพ (HSS Net)

๒) เครือข่ายคอมพิวเตอร์ระหว่างผู้ใช้บริการที่ไม่เกี่ยวข้องกับระบบงานของ กรมสนับสนุนบริการสุขภาพที่กำกับดูแลโดยผู้ให้บริการภายนอกองค์กร

๑.๒ ดำเนินการจัดตั้งคณะทำงาน IT Security Steering หรือ IT Security Working Group ซึ่งต้องมีการทบทวนทุกปี จากการเปลี่ยนแปลงโครงสร้างองค์กร และประชุมชี้แจงแนวทางการดำเนินงานให้บุคลากรทุกระดับทราบ

๑.๓ ศึกษามาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๑๓ อย่างละเอียดทบทวนและปรับปรุงแก้ไขนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย มาตรการควบคุม ๑๔ หัวข้อ

๑.๓.๑ นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information security policies)

๑.๓.๒ โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร (Organization of information security)

๑.๓.๓ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบุคลากร (Human resource security)

๑.๓.๔ การบริหารจัดการทรัพย์สิน (Asset management)

๑.๓.๕ การควบคุมการเข้าถึง (Access control)

๑.๓.๖ การเข้ารหัสข้อมูล (Cryptography)

๑.๓.๗ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

๑.๓.๘ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านการดำเนินการ (Operations security)

๑.๓.๙ ความมั่นคงปลอดภัยทางด้านการสื่อสาร (Communications security)

๑.๓.๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

๑.๓.๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

๑.๓.๑๒ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสนเทศ (Information security incident management)

๑.๓.๑๓ ประเด็นด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

๑.๓.๑๔ การปฏิบัติตามข้อกำหนด (Compliance)

๑.๔ วิเคราะห์และประเมินองค์กรเบื้องต้น ในประเด็นการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Gap Analysis) เพื่อดำเนินการขับเคลื่อนนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ได้มีประสิทธิภาพ

๑.๕ จัดทำแผนการดำเนินงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑.๕.๑ แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑.๕.๒ นโยบายและแนวปฏิบัติในการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑๕.๓ แผนบริหารความต่อเนื่องในสภาวะวิกฤตสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑๕.๔ แผนบริหารความเสี่ยงด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑๕.๕ ทบทวนผลการดำเนินงานตามแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ขั้นตอนที่ ๒ กำหนดแนวทางการดำเนินงานตามมาตรฐาน ประกอบด้วย การทำความเข้าใจกับกระบวนการวางแผนการดำเนินงาน และกำหนดตัวชี้วัดในการควบคุม กำกับ ติดตามและประเมินผล

๒.๑ ปรับปรุงกระบวนงานตามมาตรฐาน การพัฒนาองค์กรด้านความมั่นคงปลอดภัยสารสนเทศให้รองรับการตรวจประเมินด้วยมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๒.๑.๑ บริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ประกอบด้วย ๑๔ ข้อกำหนด (Control Area) ๓๔ ข้อควบคุม (Control Objectives) และ ๑๑๔ มาตรการควบคุม (Control Points)

(๑) ISMS Scope

(๒) IT Security Steering Committee

(๓) Internal ISMS Workshop / ISMS Framework / ISMS Framework / ISMS Guideline

(๔) Holistic Approach :

(๔.๑) Gap Analysis

(๔.๒) Gap Assessment

(๔.๓) Risk Assessment and Control

(๔.๔) Risk Management

(๕) Review and Monitor with SOA Statement of Applicability

(๖) Pre Assessment by Internal Auditor

(๗) Assessment by External Auditor for Certify

(๘) ISMS Control / Re - Audit

๒.๑.๒ พัฒนาระบบบำรุงรักษา

(๑) ครุภัณฑ์คอมพิวเตอร์ (Hardware / Software)

(๒) ครุภัณฑ์ระบบเครือข่ายคอมพิวเตอร์ (Computer System Network)

(๓) ครุภัณฑ์โครงข่ายเทคโนโลยีการสื่อสาร (Communication Network)

(๔) อุปกรณ์จัดเก็บข้อมูล (Data Storage Devices) ได้แก่

(๔.๑) สื่อเก็บข้อมูลแบบจานแม่เหล็ก (Magnetic Disk Device) เช่น Hard disk

(๔.๒) สื่อเก็บข้อมูลชนิดแสง (Optical Storage Devices) เช่น CD Rom, CD-R, CD-RW, DVD Rom, DVD-R, DVD-RW

(๔.๓) สื่อเก็บข้อมูลแบบเทป (Tape Devices)

(๔.๔) หน่วยความจำแบบแฟลช (Flash Memory)

(๔.๕) อุปกรณ์จัดเก็บข้อมูลชนิดพกพา (External Hard disk)

(๔.๖) อุปกรณ์จัดเก็บข้อมูลชนิดพกพาที่ไม่มีจานหมุน (Solid-State Drive)

(๕) เซิร์ฟเวอร์ (Server)

(๕.๑) File Server จัดเก็บไฟล์แบบรวมศูนย์ : Centralized Disk Storage

(๕.๒) Print Server สำหรับ Printer ราคาแพงบางรุ่น

(๕.๓) Database Server เพื่อจัดการฐานข้อมูล (Database Management System)

(๕.๔) Application Server เพื่อจัดการโปรแกรมประยุกต์ เช่น Mail Server, Proxy Server หรือ Web Server

๒.๑.๓ ระบบทำลายข้อมูลจากอุปกรณ์จัดเก็บข้อมูลของส่วนราชการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๑.๔ บริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว ในประเด็นต่อไปนี้

(๑) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์

(๒) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล

(๓) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ

(๔) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๕) กำหนดมาตรการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

(๕.๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๕.๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๕.๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๕.๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕.๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

๒.๑.๕ บริหารจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อการคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

(๑) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงทีเกี่ยวข้องกับข้อมูลส่วนบุคคล

(๒) กำหนดหน้าที่ของหน่วยงานที่มีหน้าที่ควบคุม กำกับ ข้อมูลส่วนบุคคล

(๓) กำหนดระดับของข้อมูลส่วนบุคคล พร้อมทั้งรายละเอียดของมาตรการป้องกันข้อมูลส่วนบุคคล

(๔) วิเคราะห์สถานการณ์ และประเมินผลกระทบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

(๕) กำหนดมาตรการจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

(๕.๑) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๕.๒) มาตรการตรวจสอบและเฝ้าระวังการละเมิดข้อมูลส่วนบุคคล

(๕.๓) มาตรการเผชิญเหตุเมื่อมีการตรวจพบการละเมิดข้อมูลส่วนบุคคล

(๕.๔) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากการละเมิดข้อมูลส่วนบุคคล

๒.๑.๖ บริหารจัดการโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศด้านระบบบริการสุขภาพ

(๑) จัดหา ซื้อ เช่าครุภัณฑ์เทคโนโลยีสารสนเทศ (ทดแทน /จัดหา) Software ลิขสิทธิ์ พร้อมครุภัณฑ์คอมพิวเตอร์ทดแทน

(๒) พัฒนาเครือข่ายคอมพิวเตอร์ โครงข่ายการสื่อสาร และการเชื่อมโยงข้อมูลของศูนย์ข้อมูลด้านระบบบริการสุขภาพตามเขตบริการสุขภาพ (Health Care Sectors)

๒.๑.๗ การพัฒนาทักษะ องค์ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy) สำหรับบุคลากร กรมสนับสนุนบริการสุขภาพ

(๑) การพัฒนาศักยภาพบุคลากรขั้นพื้นฐาน (Digital Government Capacity Building)

(๑.๑) การพัฒนาศักยภาพด้านการใช้ระบบเครือข่ายคอมพิวเตอร์

(๑.๒) การพัฒนาศักยภาพด้านการใช้โครงข่ายเทคโนโลยีการสื่อสาร

(๑.๓) การพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy)

(๑.๔) การพัฒนาทักษะความรู้และสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ใช้งาน (User Awareness in Cyber Security)

(๒) การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยสารสนเทศ ชั้นสูง

(๒.๑) การบริหารจัดการระบบคอมพิวเตอร์ (System Administrator)

(๒.๒) การบริหารจัดการระบบเครือข่ายสารสนเทศ (Network Administrator)

(๒.๓) การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Administrator)

(๒.๓.๑) การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

(๒.๓.๒) การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

(๒.๓.๓) การรักษาความปลอดภัยการแผ่รังสี (Emission Security)

(๒.๓.๔) การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

(๒.๓.๕) การรักษาความปลอดภัยเครือข่าย (Network Security)

(๒.๓.๖) การรักษาความปลอดภัยข้อมูล (Information Security)

๒.๑.๘ การพัฒนาศักยภาพบุคลากรเฉพาะทาง

(๑) การพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๑.๑) พัฒนาทักษะบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๑.๑.๑) ผู้บริหารเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

(๑.๑.๒) ผู้เชี่ยวชาญและจัดการเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

(๑.๑.๓) ผู้ประเมินความเสี่ยงและช่องโหว่ระบบเทคโนโลยีสารสนเทศ

(๑.๑.๔) ผู้ตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์

(๑.๑.๕) ผู้ประเมินความเสี่ยงและช่องโหว่ระบบเทคโนโลยีสารสนเทศ

(๑.๑.๖) นักทดสอบช่องโหว่และภัยคุกคามระบบเทคโนโลยีสารสนเทศ

- การตรวจสอบระบบเทคโนโลยีสารสนเทศด้วยวิธีการตรวจสอบ ช่องโหว่ Vulnerability Assessment (Web Application Hacking)
- การเจาะระบบ (Penetration Testing)

(๑.๑.๗) นักวิจัยและวิเคราะห์งานเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

(๑.๒) สนับสนุนการผ่านการประเมินด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ISEC : Information Security Expert Certification, CISSP : Certified Information System Security Professional, CISA, CASP, CISM, CSX, CompTIA เป็นต้น

๒.๑.๙ บริหารจัดการบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ (Human Resource Management)

(๑) เสนอขออนุมัติจัดจ้างผู้เชี่ยวชาญภายนอก

(๑.๑) ด้านการบริหารจัดการระบบคอมพิวเตอร์ (Computer System Administrator)

(๑.๒) ด้านการบริหารจัดการระบบเครือข่ายสารสนเทศ (Network Administrator)

(๑.๓) ด้านการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Administrator)

๒.๑.๑๐ เสนอกรอบอัตรากำลังบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๑) เสนอโครงสร้างบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๒) เสนอขอจัดสรร/ทดแทน อัตรากำลัง ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ

(๓) วิเคราะห์กรอบอัตรากำลัง เสนอต่อกลุ่มบริหารงานบุคคล เพื่อเสนอต่อคณะอนุกรรมการสามัญกรมสนับสนุนบริการสุขภาพ (อกพ.) พิจารณา

(๔) กำหนดเส้นทางความก้าวหน้าในวิชาชีพสายความมั่นคงปลอดภัยสารสนเทศ

๒.๒ กำหนดตัวชี้วัดในการควบคุม กำกับ ติดตามและประเมินผล

ตัวชี้วัด (CSF) คือ **ระดับความสำเร็จของการการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ** (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ)

ตัวชี้วัดที่ ๑.๑ ระดับความสำเร็จของการการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ : Process Indicator)

ตัวชี้วัดที่ ๒.๑ ร้อยละ ๘๐ ของบุคลากรพึงพอใจต่อการพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy) (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ : Process Indicator)

ตัวชี้วัดที่ ๒.๒ จำนวนบุคลการผ่านเกณฑ์ประเมินมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Cirtification) (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ : Process Indicator)

ผลสัมฤทธิ์ : ประชาชนมีความเชื่อมั่น ในการเข้าใช้ประโยชน์จากข้อมูลด้านระบบบริการสุขภาพที่มีความมั่นคงปลอดภัย (CIA) : ทั้งการรักษาความลับ (Confidentiality) ความถูกต้อง แม่นยำ ครบถ้วน (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) รวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ ของกรมสนับสนุนบริการสุขภาพ

๒.๓ การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐานที่กำหนด

๒.๔ การจัดการความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

ขั้นตอนที่ ๓ หมายถึง วิเคราะห์ หาสาเหตุ โดยการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ (Gap Assessment)

๓.๑ วิเคราะห์ช่องว่างมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Gap Assessment) พบว่ากรมสนับสนุนบริการสุขภาพ มีความพร้อมรองรับตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๓.๒ วิเคราะห์ความเสี่ยง (Risk Assessment)

๓.๒.๑ วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๒.๒ วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๓.๒.๓ วิเคราะห์ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

๓.๓ กำหนดแนวทางป้องกันความเสี่ยง วางแผนป้องกันความเสี่ยง (Risk Management Framework)

๓.๓.๑ วางแผนป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๒.๒ วางแผนป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๓.๒.๓ วางแผนป้องกันความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

๓.๔ จัดทำรายงานและนำเสนอต่อ Board of Director เพื่อผู้บริหารระดับสูงเข้าใจในปัญหาที่เกิดขึ้น และดำเนินการแก้ไขข้อบกพร่องจากการที่องค์กรยังไม่ได้ปฏิบัติตามมาตรฐานฯ ดังกล่าวอย่างเป็นรูปธรรม (Corrective Action)

๓.๕ กลุ่มตรวจสอบภายในดำเนินการตรวจสอบ (Pre-Assessment) ระดับ Internal Auditor

ขั้นตอนที่ ๔ พัฒนา ปรับปรุงกระบวนงานตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๔.๑ ประเมินระบบความมั่นคงปลอดภัยสารสนเทศในภาพรวม (Gap Analysis Holistic Approach) ด้วยการนำเสนอ Gap Analysis Report ใน ๓ มุมมอง

๔.๑.๑ มุมมองด้านบุคลากร (People)

๔.๑.๒ มุมมองด้านกระบวนการ (Process)

๔.๑.๓ มุมมองด้านเทคโนโลยี (Technology)

๔.๒ วิเคราะห์ความเสี่ยง ประเมินและปรับปรุงความเสี่ยงตามแผนการดำเนินงานที่กำหนด (Risk Assessment)

๔.๓ การบริหารจัดการความเสี่ยง ควบคุมตามแผนที่ได้กำหนดไว้ (Risk Management) เช่น Vulnerability Assessment, Penetration Testing, Hardening เป็นต้น

๔.๔ จัดทำเอกสารรองรับการประเมิน ในรูปแบบ Statement of Applicability (SOA) เพื่อรองรับการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๔.๕ จัดทำรายงานเสนอ Board of Director (DCIO, CEO)

ขั้นตอนที่ ๕ ควบคุม กำกับ ติดตาม และประเมินผลอย่างต่อเนื่อง

๕.๑ ควบคุม กำกับ (Control) สอบทาน (Review) และการเฝ้าระวัง (Monitor) เตรียมพร้อมรองรับการตรวจประเมินมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (Gap Analysis Report)

๕.๑.๑ การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ

๕.๑.๒ การจัดการความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๒ การจัดการและควบคุมความเสี่ยง (Risk Assessment & Re-Assessment & Control)

๕.๓ สรุปรายงานผลการดำเนินงานการพัฒนา / ติดตาม / ประเมินผลตามตัวชี้วัดที่กำหนด (KPI / CSF)

๕.๔ ดำเนินการตรวจประเมิน ครั้งที่ ๑ (Assessment) โดย External Auditor ด้วยการ Outsource ไปยัง Manage Security Service Provider หรือ MSSP ที่ถือเป็นการ “Transfer Risk”

๕.๕ ดำเนินการตรวจประเมิน ครั้งที่ ๒ (Re - Assessment) โดย External Auditor ทุก ๓ ปี

โดยมีแนวทางการดำเนินงาน เพื่อทำให้กรมสนับสนุนบริการสุขภาพมีการรักษาความมั่นคงปลอดภัยสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร รวมทั้งนโยบายการเข้าใช้งานระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ ตามแผนภาพที่ ๒ แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

แผนภาพที่ ๒ แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ.๒๕๖๔ – ๒๕๖๖

ตารางที่ ๑ แสดงขั้นตอนการดำเนินงาน “การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ - ๒๕๖๖” (รายละเอียดตาม ภาคผนวก ก)

ขั้นตอนการดำเนินงาน	ระยะเวลาดำเนินงาน (เดือนที่)																																		
	๑	๒	๓	๔	๕	๖	๗	๘	๙	๑๐	๑๑	๑๒	๑๓	๑๔	๑๕	๑๖	๑๗	๑๘	๑๙	๒๐	๒๑	๒๒	๒๓	๒๔	๒๕	๒๖	๒๗	๒๘	๒๙	๓๐	๓๑	๓๒	๓๓	๓๔	๓๕	๓๖
ขั้นตอนที่ ๑. กำหนดวัตถุประสงค์การดำเนินงาน สอดคล้องตามนโยบาย ประกอบด้วย การทบทวน กำหนด รายละเอียด ขั้นตอนของการดำเนินงานสอดคล้องตามนโยบาย																																			
ทบทวน กำหนดรายละเอียดขั้นตอนการดำเนินงาน	✓	✓	✓																																
ขั้นตอนที่ ๒ กำหนดแนวทางการดำเนินงานตามมาตรฐาน ประกอบด้วย การทำความเข้าใจกับกระบวนการ วางแผนการดำเนินงาน กำหนดตัวชี้วัด																																			
ทำความเข้าใจกับกระบวนการวางแผนการดำเนินงาน กำหนดตัวชี้วัด		✓	✓	✓																															
ขั้นตอนที่ ๓ วิเคราะห์ หาสาเหตุ โดยการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ (Gap Assessment)																																			
วิเคราะห์ หาสาเหตุ ประเมินตามมาตรฐาน				✓	✓	✓																													
ขั้นตอนที่ ๔ พัฒนา ปรับปรุงกระบวนงานตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓																																			
ดำเนินงานตามมาตรฐานบริหารจัดการความเสี่ยง					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
ขั้นตอนที่ ๕ ควบคุม กำกับ ติดตาม และประเมินผลอย่างต่อเนื่อง																																			
ควบคุม ติดตามปรับปรุงต่อเนื่อง			✓			✓			✓			✓			✓			✓			✓			✓			✓			✓			✓			✓
ประเมินตามเกณฑ์มาตรฐาน											✓	✓ ✓											✓	✓ ✓											✓	✓ ✓
ปรับปรุง ตรวจสอบ ควบคุม รายงานผล				✓			✓			✓			✓			✓			✓			✓			✓			✓			✓			✓	✓

หมายเหตุ : ✓ หมายถึง การรับการประเมินจากกลุ่มงานตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ (Internal Surveyor)

✓✓ หมายถึง การรับการประเมินจาก MSSP : Managed Security Service Provider

๖. ประเด็นยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ภายใต้ โครงการขับเคลื่อนคุณภาพมาตรฐานสถานพยาบาลโดยการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๔ - ๒๕๖๖ ตามแผนยุทธศาสตร์การพัฒนาดิจิทัลเพื่อระบบบริการสุขภาพและระบบสุขภาพภาคประชาชน ระยะ ๕ ปี ของกรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๘

ประเด็นยุทธศาสตร์ที่ ๑ พัฒนาองค์กรให้รองรับการตรวจประเมินระบบด้วย ISO/ COBITS /ITILS หรืออื่นๆ ที่เป็นมาตรฐานสากล ที่กรมสนับสนุนบริการสุขภาพกำหนด

กิจกรรม /การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๑-๑ การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (ISMS: Information Security Management System) : ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ และที่แก้ไขเพิ่มเติมภายหลัง เพื่อรองรับการประเมินมาตรฐาน ๑.๑.๑ ISMS Scope ๑.๑.๒ IT Security Steering Committee ๑.๑.๓ Internal ISMS Workshop / ISMS Framework / ISMS Framework / ISMS Guideline ๑.๑.๔ Holistic Approach ๑.๑.๔.๑ Gap Analysis ๑.๑.๔.๒ Gap Assessment ๑.๑.๔.๓ Risk Assessment and Control ๑.๑.๔.๔ Risk Management ๑.๑.๕ Review and Monitor with SOA Statement of Applicability ๑.๑.๖ Pre Assessment by Internal Auditor ๑.๑.๗ Assessment by External Auditor for Certify ๑.๑.๘ ISMS Control / Re - Audit	กทส./ทุกหน่วยงาน
กิจกรรมที่ ๑-๒ การพัฒนาระบบบำรุงรักษา ๑. ครุภัณฑ์คอมพิวเตอร์ (Hardware / Software) ๒. ครุภัณฑ์ระบบเครือข่ายคอมพิวเตอร์ (Computer Sysytem Network) ๓. ครุภัณฑ์โครงข่ายเทคโนโลยีการสื่อสาร (Communication Network) ๔. อุปกรณ์จัดเก็บข้อมูล (Data Storage Devices) ได้แก่ ๔.๑. สื่อเก็บข้อมูลแบบจานแม่เหล็ก (Magnetic Disk Device) เช่น Floppy Disk, Harddisk ๔.๒. สื่อเก็บข้อมูลชนิดแสง (Optical Storage Devices) เช่น CD Rom, CD-R, CD-RW, DVD Rom, DVD-R, DVD-RW ๔.๓. สื่อเก็บข้อมูลแบบเทป (Tape Devices) ๔.๔. หน่วยความจำแบบแฟลช (Flash Memory) ๕. เซิร์ฟเวอร์ (Server) ๕.๑. File Server จัดเก็บไฟล์แบบรวมศูนย์: Centerized Disk Storage	กทส.

กิจกรรม /การดำเนินงาน	หน่วยงานที่รับผิดชอบ
๕.๒. Print Server สำหรับ Printer ราคาแพงบางรุ่น ๕.๓. Database Server เพื่อจัดการฐานข้อมูล (Database Management System) ๕.๔. Application Server เพื่อจัดการโปรแกรมประยุกต์ เช่น Mail Server, Proxy Server หรือ Web Server	
กิจกรรมที่ ๑-๓ ระบบทำลายข้อมูลจากอุปกรณ์จัดเก็บข้อมูลของส่วนราชการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ	กทส.

ประเด็นยุทธศาสตร์ที่ ๒ การรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

กิจกรรม /การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๒ การบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒.๑ กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ๒.๒ กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล ๒.๓ กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ๒.๔ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ๒.๕ กำหนดมาตรการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ๒.๕.๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล ๒.๕.๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น ๒.๕.๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ๒.๕.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ ๒.๕.๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	กทส./ทุกหน่วยงาน

ประเด็นยุทธศาสตร์ที่ ๓ การคุ้มครองข้อมูลส่วนบุคคล

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๓ การบริหารจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล ๓.๑ กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงทีเกี่ยวข้องกับข้อมูลส่วนบุคคล ๓.๒ กำหนดหน้าที่ของหน่วยงานที่มีหน้าที่ควบคุม กำกับ ข้อมูลส่วนบุคคล ๓.๓ กำหนดระดับของข้อมูลส่วนบุคคล พร้อมทั้งรายละเอียดของมาตรการป้องกันข้อมูลส่วนบุคคล	กทส./ทุกหน่วยงาน *(ขึ้นกับความพร้อมและนโยบายฯ)*

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
๓.๔ การวิเคราะห์สถานการณ์ และประเมินผลกระทบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ๓.๕ กำหนดมาตรการจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล ๓.๕.๑ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น ๓.๕.๒ มาตรการตรวจสอบและเฝ้าระวังการละเมิดข้อมูลส่วนบุคคล ๓.๕.๓ มาตรการเผชิญเหตุเมื่อมีการตรวจพบการละเมิดข้อมูลส่วนบุคคล ๓.๕.๔ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากการละเมิดข้อมูลส่วนบุคคล	

ประเด็นยุทธศาสตร์ที่ ๔ การบริหารจัดการโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศด้านระบบบริการสุขภาพ

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๔-๑ การจัดหา ซื้อ เช่าครุภัณฑ์เทคโนโลยีสารสนเทศ (ทดแทน /จัดหา) Software ลิขสิทธิ์ พร้อมครุภัณฑ์คอมพิวเตอร์ทดแทน	กทส./ทุกหน่วยงาน
กิจกรรมที่ ๔-๒ การพัฒนาเครือข่ายคอมพิวเตอร์ โครงข่ายการสื่อสาร และการเชื่อมโยงข้อมูลของศูนย์ข้อมูลด้านระบบบริการสุขภาพเชิงรุก ตามเขตบริการสุขภาพ (HealthCare Sectors)	กทส./ศบส.๑-๑๒/ สสม.๕ แห่ง

ประเด็นยุทธศาสตร์ที่ ๕ การพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy)

๕.๑ การพัฒนาศักยภาพบุคลากรขั้นพื้นฐาน (Digital Government Capacity Building)

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๕-๑-๑ การพัฒนาศักยภาพด้านการใช้อุปกรณ์คอมพิวเตอร์พื้นฐาน	กทส./ทุกหน่วยงาน
กิจกรรมที่ ๕-๑-๒ การพัฒนาศักยภาพด้านการใช้ระบบเครือข่ายคอมพิวเตอร์	กทส./ทุกหน่วยงาน
กิจกรรมที่ ๕-๑-๓ การพัฒนาศักยภาพด้านการใช้โครงข่ายเทคโนโลยีการสื่อสาร	กทส./ทุกหน่วยงาน
กิจกรรมที่ ๕-๑-๔ การพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy) ๑. สร้างการรับรู้ กระตุ้นให้บุคลากรทุกระดับ เกิดความสนใจในการพัฒนาทักษะความเข้าใจและการใช้เทคโนโลยีดิจิทัล ๒. กำหนดให้การพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ เป็นนโยบายของส่วนราชการ ๓. สร้างบรรยากาศการทำงานแบบความมั่นคงปลอดภัยสารสนเทศ ๔. พัฒนาบุคลากรภายในองค์กรทุกระดับ ๕. ติดตามผลการพัฒนาบุคลากรภายในองค์กรทุกระดับ ๖. ประมวลผลการพัฒนาในภาพรวมขององค์กร ๗. รายงานผลการพัฒนาทักษะความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศเสนอต่อผู้บริหาร	กทส.
กิจกรรมที่ ๕-๑-๕ การพัฒนาทักษะความรู้และสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ สำหรับผู้ใช้งาน (User Awareness in Cyber Security)	กทส.

๕.๒ การพัฒนาศักยภาพบุคลากรขั้นสูง

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๕-๒-๑ การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยสารสนเทศ ชั้นสูง เช่น ๑. การบริหารจัดการระบบคอมพิวเตอร์ (System Administrator) ๒. การบริหารจัดการระบบเครือข่ายสารสนเทศ (Network Administrator) ๓. การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Administrator) ๓.๑ การรักษาความปลอดภัยด้านกายภาพ (Physical Security) ๓.๒ การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security) ๓.๓ การรักษาความปลอดภัยการแผ่รังสี (Emission Security) ๓.๔ การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security) ๓.๕ การรักษาความปลอดภัยเครือข่าย (Network Security) ๓.๖ การรักษาความปลอดภัยข้อมูล (Information Security)	กทส.

๕.๓ การพัฒนาศักยภาพบุคลากรเฉพาะทาง

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๕-๓-๑ การพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ ๑. การพัฒนาทักษะบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ ๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์ ๑.๒ ผู้เชี่ยวชาญและจัดการเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์ ๑.๓ ผู้ประเมินความเสี่ยงและช่องโหว่ระบบเทคโนโลยีสารสนเทศ ๑.๔ ผู้ตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์ ๑.๕ ผู้ประเมินความเสี่ยงและช่องโหว่ระบบเทคโนโลยีสารสนเทศ ๑.๖ นักทดสอบช่องโหว่และภัยคุกคามระบบเทคโนโลยีสารสนเทศ - การตรวจสอบระบบเทคโนโลยีสารสนเทศด้วยวิธีการตรวจสอบช่องโหว่ Vulnerability Assessment (Web Application Hacking) - การเจาะระบบ (Penetration Testing) ๑.๗ นักวิจัยและวิเคราะห์งานเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์ ๒. สนับสนุนการผ่านการประเมินด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ISEC (Information Security Expert Cirtification), CISSP (Certified Information System Security Professional), CISA, CASP, CISM, CSX เป็นต้น	กทส.

ประเด็นยุทธศาสตร์ที่ ๖ การบริหารจัดการอัตรากำลัง/บุคลากร (Human Resource Management)

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
กิจกรรมที่ ๖-๑ เสนอขออนุมัติจัดจ้างผู้เชี่ยวชาญภายนอก เช่น ๑. ด้านการบริหารจัดการระบบคอมพิวเตอร์ (Computer System Administrator) ๒. ด้านการบริหารจัดการระบบเครือข่ายสารสนเทศ (Network Administrator)	กทส. / กบค.

กิจกรรม / การดำเนินงาน	หน่วยงานที่รับผิดชอบ
๓. ด้านการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Administrator)	
กิจกรรมที่ ๖-๒ เสนอขออนุมัติจัดสรรกรอบอัตรากำลัง (ใหม่) เพื่อสนับสนุนการปฏิบัติงานของหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศ ๑. เสนอโครงสร้างบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ ๒. เสนอขอจัดสรร/ทดแทน อัตรากำลัง ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ ๓. กำหนดเส้นทางความก้าวหน้าในวิชาชีพสายความมั่นคงปลอดภัยสารสนเทศ	กทส. /กบค.

๗. การติดตามและประเมินผลการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ด้านการติดตาม ประเมินผลที่สำคัญ คือ ๑) ต้องรู้ความจริง ๒) ต้องทันเวลา ไม่ก่อให้เกิดความเสียหาย หรือเสียหายน้อยที่สุด ๓) ต้องสร้างสรรค์ สร้างขวัญและกำลังใจ ๔) ต้องส่งเสริมการพัฒนาตนเอง และ ๕) ต้องมีประสิทธิภาพสูงเพื่อให้การบริหารจัดการบรรลุผลสำเร็จตามเป้าหมาย ที่สอดคล้องตามแนวทาง การดำเนินงานของกรมสนับสนุนบริการสุขภาพ โดยได้กำหนดผลสัมฤทธิ์การดำเนินงาน (Critical Success Factors) ในการรักษาความมั่นคงปลอดภัยสารสนเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายสำคัญของประเทศ ทำให้กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข มีความมั่นคงปลอดภัยไซเบอร์ในระดับสูง โดยกำหนดผลสำเร็จและผลสัมฤทธิ์ของการดำเนินงาน ได้ดังนี้

๑. กรมสนับสนุนบริการสุขภาพมีแนวทางการดำเนินงานตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ

๒. ผู้บริหารและบุคลากรทุกระดับของกรมสนับสนุนบริการสุขภาพ มีความรู้ ความเข้าใจและทักษะในการรักษาความมั่นคงปลอดภัยสารสนเทศ

๓. ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการที่เกี่ยวข้องกับข้อมูลสารสนเทศด้านระบบบริการสุขภาพรวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ของกรมสนับสนุนบริการสุขภาพ

ภาพรวมความสำเร็จที่สำคัญ	แผนงานและตัวชี้วัด ตัวดำเนินงาน
๑. การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	**๑. แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๖** **๑. ระดับความสำเร็จของการการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ** ๑.๑ ระดับความสำเร็จของการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ
๒. การพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ	
๒.๑ การพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy)	๒.๑ แผนพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ ๒.๑ ร้อยละ ๘๐ ของบุคลากรพึงพอใจต่อการพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ
๒.๒ บุคลากรผ่านเกณฑ์ประเมินมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Certification)	๒.๒ แผนพัฒนาศักยภาพบุคลากรเฉพาะทางด้านความมั่นคงปลอดภัยสารสนเทศ ๒.๒ จำนวนบุคลากรผ่านเกณฑ์ประเมินมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

กรมสนับสนุนบริการสุขภาพได้จัดทำ “แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศกรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๖” เพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการข้อมูลสารสนเทศของกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข รวมทั้งการเพิ่มมูลค่าการทำธุรกรรมอิเล็กทรอนิกส์ที่สามารถสร้างรายได้สู่ประเทศ ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลของประชาชนหรือผลประโยชน์ที่สำคัญของประเทศ ต่อไป

(ลงชื่อ) ..... ผู้เสนอ
(นายอภินันท์ นิลฉาย)
ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ

(ลงชื่อ) ..... ผู้เห็นชอบ
(นายภานุวัฒน์ ปานเกตุ)
ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

(ลงชื่อ) ..... ผู้อนุมัติ
(นายธเรศ กรัษนัยรวิวงศ์)
อธิบดีกรมสนับสนุนบริการสุขภาพ

เอกสารอ้างอิง

๑. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

๒. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๔. แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ระยะ ๕ ปี (พ.ศ. ๒๕๖๐ – ๒๕๖๔)

๕. แผนยุทธศาสตร์ชาติ ระยะ ๒๐ ปี (ด้านสาธารณสุข) กระทรวงสาธารณสุข : ระบบบริหารจัดการ (Governance Excellence) ประเด็นระบบข้อมูลและเทคโนโลยีสารสนเทศ

๖. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๗. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๘. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒

๙. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ และที่เกี่ยวข้อง

๑๐. แผนยุทธศาสตร์การพัฒนาดิจิทัลเพื่อระบบบริการสุขภาพและระบบสุขภาพภาคประชาชน ระยะ ๕ ปี ของกรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๘

ภาคผนวก ก

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
1	**ขั้นตอนที่ 1 : ทำการประเมินในภาพรวม (Plan : Holistic Approach, Policy)**														
	1.1 รวบรวมกฎหมาย กฎระเบียบด้านเทคโนโลยีสารสนเทศที่ต้องปฏิบัติ	1) กฎระเบียบด้านความมั่นคงปลอดภัยสารสนเทศที่มีต่อหน่วยงานที่เกี่ยวข้อง (Cybersecurity roles and responsibilities for the entire workforce and third party stakeholder)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										
	1.2 รวบรวมข้อมูลเอกสารความรู้ และศึกษามาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO27001:2013		งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										
	1.3 รวบรวมวัสดุ ครุภัณฑ์ รวมทั้งข้อมูลที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (Asset Management)		งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→				←	→				←	→
	1.3.1 การจัดการวัสดุครุภัณฑ์ (Assset Management)	1) ด้านอุปกรณ์และระบบที่ใช้ภายในองค์กร (Physical devices and systems within the organization are inventoried)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→				←	→			

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		2) ด้านระบบปฏิบัติการและแอพลิเคชั่นต่างๆ (Software Platforms and applications)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→					←	→		
		3) ด้านการสื่อสารภายในองค์กร (Organizational communication and Data flows are mapped)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→					←	→		
		4) ด้านการสื่อสารภายนอกองค์กร (External information systems are catalougued)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→					←	→		
		5) ทรัพยากรที่เกี่ยวข้องกับงาน (Resources are prioritized based on their classification, criticalty and business value)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→					←	→		
2	**ขั้นตอนที่ 2 การกำหนดขอบเขต ตัวชี้วัดและแนวทางการดำเนินงาน (Do ; Implement, Operate ,Measure)**														
	2.1 ระบบบริหารจัดการองค์กร (Business Environment)	1) การกำหนดกรอบในการจัดทำวัตถุประสงค์ (Objectives) รวมถึงทิศทางและหลักการในการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										
		2) การคำนึงถึงข้อกำหนดทางธุรกิจและกฎหมาย รวมถึงข้อบังคับตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		3) การกำหนดนโยบายการบริหารความเสี่ยงให้สอดคล้องตามพันธกิจขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										
		4) การบริหารจัดการความเสี่ยงเชิงกลยุทธ์ขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→	→									
		5) การกำหนดมาตรการบริหารจัดการความสี่ยงและผลกระทบที่เกิดขึ้น	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→	→									
		6) แต่งตั้งคณะกรรมการอำนวยการและคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศกรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										
	2.2 นโยบายองค์กร (Governance Policy)	1) การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									
		2) การกำหนดนโยบายการบริหารจัดการความเสี่ยงตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→								
		3) การกำหนดข้อกฎหมายและระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→								

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
	2.3 นโยบายการจัดการความเสี่ยง (Risk Management Strategy)	1) การระบุความเสี่ยงและการจัดลำดับความสำคัญ ซึ่งสามารถใช้เป็นหลักฐาน ตามลักษณะโครงสร้างพื้นฐานขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	—	—	→			←	—	→			
		2) การดำเนินการจัดการเกี่ยวกับการคุกคามจากสื่อแหล่งต่างๆ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT				←	→				←	→		
		3) การจัดทำเอกสารการบริหารจัดการกรณีเกิดการบุกรุกจากภายในและภายนอกองค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT								←	→			
		4) การระบุผลกระทบจากภัยคุกคามและความเสี่ยงที่ส่งผลกระทบต่อองค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT								←	→			
		5) การระบุผลกระทบทางธุรกิจที่อาจจะเกิดขึ้นและแนวทางแก้ไข	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	—	—	—	—	—	—	—	—	—	—	→
	2.4 อนุมัตินโยบายโดยผู้บริหารเทคโนโลยีสารสนเทศ ระดับกรม (DCIO) / อธิบดีกรมสนับสนุนบริการสุขภาพ (CEO)		DCIO/CEO	←	→										

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
3	**ขั้นตอนที่ 3 การดำเนินงานตามแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Check : Monitor, Review and Analysis)**														
	3.1 การสร้างการรับรู้ ทำความเข้าใจให้บุคลากรในทุกระดับ (Mind Set)	1) ประชุมคณะกรรมการอำนวยการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Steering Committee)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)					↔				↔			
		3) ประชุมคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Working Group)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)				↔		↔				↔		
	(โดยการจัดจ้างบุคคลภายนอก)	4) ประชุมเชิงปฏิบัติการ : พัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)						↔			↔			
	3.2 ทำการประเมินระบบสารสนเทศในภาพรวม (Holistic Approach) โดยใช้เทคนิค Gap Analysis ตามมาตรฐาน ISO/IEC 27001 (ดำเนินการปีงบประมาณ 25XX)	1) ประเมินผลกระทบทางธุรกิจซึ่งอาจเกิดจากความล้มเหลวในความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/	←	-	-	-	-	-	-	-	-	-	-	→
		2) ประเมินโอกาสในการเกิดขึ้นของความล้มเหลวที่มีต่อความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)	←	-	-	-	-	-	-	-	-	-	-	→

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		3) การคำนวณระดับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)	←	---	---	---	---	---	---	---	---	---	---	→
		4) การพิจารณาความสามารถในการยอมรับความเสี่ยงในเกณฑ์ที่ยอมรับได้	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)	←	---	---	---	---	---	---	---	---	---	---	→
		5) การประเมินความคุ้มค่าคุ้มทุนจากการดำเนินงานตามนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศส่วนกลาง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)	←	---	---	---	---	---	---	---	---	---	---	→
	3.3 ดำเนินการตามแผนจัดการความเสี่ยง (Risk Management) ใน 3 มุมมอง คือ ด้านบุคลากร ด้านกระบวนการและด้านเทคโนโลยี	1) ดำเนินการตรวจจับความผิดพลาดของผลลัพธ์ที่ได้จากการประมวลผล และทบทวนวิธีการปฏิบัติงาน เช่น การทำ Hardening, การจัดฝึกอบรม Security Awareness Training หรือ การจัดทำระบบ centralized Log Management	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)				←	---	→						

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		2) ทบทวนประสิทธิผลของการดำเนินงานตามนโยบายความมั่นคงปลอดภัยสารสนเทศ ตามที่กำหนด เช่น Vulnerability Assessment, Penetration Testing, Hardening, การติดตั้ง patch	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)						←	→					
		3) วัดประสิทธิผลของการดำเนินงานตามแผนจัดการความเสี่ยง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)	←											→
		4) ทบทวนการประเมินความเสี่ยงตามแผนจัดการความเสี่ยง (Continuous Audit)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)	←											→
4	**ขั้นตอนที่ 4 การปรับปรุงการดำเนินงานตามแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Act : Maintain and Improve)**														
	4.1 การตรวจประเมินโดยกลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ (Pre Assessment by Internal Auditor)	1) การประเมินผลตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท) /กลุ่มตรวจสอบภายใน										←	→	
		2) การแก้ไขข้อบกพร่องจากการตรวจประเมินตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
	4.2 การตรวจประเมินจากผู้เชี่ยวชาญภายนอก (Pre Assessment by External Auditor)	1) การประเมินผลตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)/กลุ่มตรวจสอบภายใน									← - - - - - →			
		2) การแก้ไขข้อบกพร่องจากการตรวจประเมินตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)											← - - - - - →	
	4.3 ผู้บริหารระดับสูงตัดสินใจสนับสนุนในการปฏิบัติตามมาตรฐาน ISO/IEC 27001	1) ดำเนินการแก้ไขข้อบกพร่องจากองค์กรที่ยังไม่ได้ปฏิบัติตามมาตรฐานอย่างเป็นรูปธรรม (Corrective Action)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	← ——— →											
	4.4 การจัดเตรียมเอกสารแสดงการประยุกต์ใช้งาน (SOA : Statement of Applicability)	1) เป็นเอกสารที่แสดงถึงรายการของหัวข้อในการควบคุม (Control) วัตถุประสงค์ในการควบคุม (Control Objectives) และเหตุผลในการเลือกหัวข้อในการควบคุม	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท) / ทุกหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ					← - →							

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
5	**ขั้นตอนที่ 5 การควบคุม กำกับ ติดตาม (Control)**														
	5.1 การควบคุมกำกับ	1) นโยบายความมั่นคงปลอดภัย : โดยจะต้องได้รับการอนุมัติจากผู้บริหารระดับสูง เผยแพร่อย่างทั่วถึง มีการมอบนโยบายการดูแลความมั่นคงปลอดภัย : ผู้บริหารระดับสูง จะต้องให้การสนับสนุนอย่างเต็มที่ / มีการกำหนดทิศทางชัดเจน / มีการมอบหมายงานและสร้างการรับรู้ รวมถึงการสร้างรูปแบบการประสานงานภายในองค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)			↔			↔			↔			↔
		2) การจัดการทรัพย์สิน : สิ่งใดๆ ที่มีคุณค่ากับองค์กร ซึ่งจะรวมไปถึงเครื่องมือ อุปกรณ์ ฮาร์ดแวร์ ซอฟท์แวร์ ฐานข้อมูล บุคลากร สาธารณูปโภคต่างๆ จะต้องมีการจัดทำบัญชีทรัพย์สินทั้งหมดตามมาตรฐาน	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)			↔			↔			↔			↔

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		3) ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร : มีการกำหนดบทบาทหน้าที่ความรับผิดชอบของบุคลากร พนักงาน รวมทั้งหน่วยงานภายนอกที่ชัดเจน โดยจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		←	→									
		4) ความมั่นคงปลอดภัยทางกายภาพ : มีการกำหนดพื้นที่ มีการกำหนดแนวปฏิบัติตามมาตรฐานความมั่นคงปลอดภัย รวมทั้งแนวทางการทำลายตามมาตรฐานด้วย	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		←	→									
		5) การบริหารการสื่อสารและการดำเนินการ : มีการจัดทำเอกสารวิธีการปฏิบัติงาน มีการแบ่งหน้าที่ความรับผิดชอบ เพื่อลดโอกาสการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือมีการใช้ผิดวัตถุประสงค์ของทรัพย์สินขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)/ Info Security gr.		←	→									

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		6) การควบคุมการเข้าถึงระบบ (Access Control) มีการกำหนดนโยบายในการเข้าถึงระบบ (Access Control Policy) มีการจัดทำเอกสารชัดเจนและมีการทบทวนความต้องการขององค์กรและข้อกำหนดความมั่นคงปลอดภัย	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ Info Security gr.			↔			↔			↔		↔	
		7) การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ : องค์กรต้องจัดให้มีการวิเคราะห์และระบุถึงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศหรือเมื่อมีการปรับปรุงระบบที่มีอยู่ในปัจจุบัน ตลอดจนมาตรการที่เหมาะสมในการจัดการความเสี่ยง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)			↔			↔			↔		↔	
		8) การจัดการเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ : มีการรายงานผ่านช่องทางการรายงานอย่างเหมาะสมด้วยความรวดเร็วเป็นไปได้ ตามบทบาทหน้าที่ความรับผิดชอบที่ชัดเจน	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→

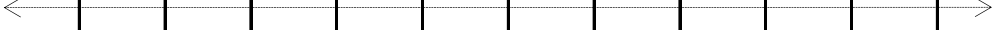
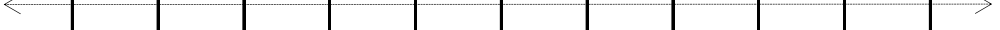
ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		9) การบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity) : องค์กรมีการจัดกระบวนการในการสร้างความต่อเนื่องทางธุรกิจ มีแผนมีการนำไปปฏิบัติและมีการปรับปรุงแผนอย่างต่อเนื่อง สอดคล้องตามข้อกำหนด (Compliance) : การดำเนินการให้สอดคล้องตามข้อกฎหมาย ตามนโยบายความมั่นคงปลอดภัยสารสนเทศและการดำเนินการตรวจประเมินระบบสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	→
	5.2 ความตระหนักและการฝึกอบรมของบุคลากรกรมสนับสนุนบริการสุขภาพ	1) การลงทะเบียนเพื่อเข้าใช้งานในระบบ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		2) การสร้างความรู้ ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับบุคลากรและผู้เกี่ยวข้อง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)						←	—	→				

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		3) ผู้บริหารระดับสูงของกรมสนับสนุนบริการสุขภาพมีความรู้ความเข้าใจ เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)												
	5.3 ความปลอดภัยของข้อมูล	1) ข้อมูลสารสนเทศได้รับการป้องกันตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)												
		2) การส่งต่อข้อมูลได้รับการป้องกันตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)												
		3) การบริหารจัดการครุภัณฑ์ที่เกี่ยวข้องตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)												
		4) การบำรุงรักษาครุภัณฑ์ตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)												
		5) การตรวจสอบความถูกต้องในการใช้เฟิร์มแวร์และความสมบูรณ์ของข้อมูล	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)												
		6) การจัดสภาพแวดล้อมในการพัฒนาระบบสารสนเทศ ออกจากสภาพปกติ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)												

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
	5.4 กระบวนการและขั้นตอนในการป้องกันข้อมูล	1) การออกแบบระบบในการดูแลปกป้องข้อมูลตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		2) การประเมินและปรับปรุงข้อมูลตามแผนความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		3) การควบคุม กำกับ ดูแลระบบพื้นที่ห้อง Sever และครุภัณฑ์	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		4) การดำเนินการสำรองข้อมูลและการทดสอบเป็นระยะตามเกณฑ์ที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		5) การปฏิบัติตามนโยบาย ระเบียบ ข้อบังคับที่เกี่ยวข้องกับสภาพแวดล้อมในการบริหารทรัพย์สินขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		6) การทำลายข้อมูลตามแนวทางนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		7) การปรับปรุงแนวทางการป้องกันข้อมูลที่มีประสิทธิภาพอย่างต่อเนื่อง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		8) การกำหนดแผนบริหารจัดการต่อการตอบสนองเหตุการณ์ผิดปกติและแผนฟื้นฟู กู้คืนจากภัยพิบัติ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)				←	→							
	5.5 การซ่อมบำรุง (Maintainance)	1) การจัดหา ซ่อมแซมสินทรัพย์ขององค์กรตามข้อกำหนดรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	-	-	-	-	-	-	-	-	-	-	→
		2) การควบคุม กำกับ สินทรัพย์ครุภัณฑ์คอมพิวเตอร์ ที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	-	-	-	-	-	-	-	-	-	-	→
	5.6 ระบบการป้องกัน (Protective Technology)	1) การเก็บบันทึกข้อมูล เอกสารการดำเนินงาน ทบทวนตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	.	.	.	.	.	.	.	.	.	.	→
		2) แนวทางในการปกป้องข้อมูลจาก Removable media ตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)				←	-	→						
		3) การมีระบบควบคุม กำกับทรัพย์สิน ครุภัณฑ์คอมพิวเตอร์ตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	.	.	.	.	.	.	.	.	.	.	→

ภาคผนวก ก รายละเอียด แนวทางการดำเนินงานบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ISO 27001:2013 and NIST)

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. 2564 - 2566

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.XX-1	พย.	ธค.	มค.XX	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.XX
		4) การควบคุมเครือข่ายการสื่อสารและระบบเชื่อมต่อตามเกณฑ์ที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
	5.7 การรวบรวม Incident ของระบบสารสนเทศ เช่น ระบบล่ม, รายงานปัญหาไวรัส มัลแวร์ต่างๆ เป็นต้น	1) การรวบรวม Incident ของระบบสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		2) การกำหนดแนวทางและมาตรการในการป้องกันแก้ไข ตามแนวทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)				↔	↔							
		3) การวิเคราะห์ความเสี่ยงและสาเหตุของผลกระทบที่มีโอกาสเกิดขึ้นในระบบ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)						↔					↔	
		4) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→

หมายเหตุ : แนวทางการดำเนินงานสามารถเปลี่ยนแปลงได้ตามนโยบายกรมสนับสนุนบริการสุขภาพ

ภาคผนวก ข

สารบัญ

๑. วัตถุประสงค์

คู่มือปฏิบัติงานฉบับนี้จัดทำขึ้น เพื่อใช้เป็นแนวทางให้เจ้าหน้าที่ผู้รับผิดชอบปฏิบัติงานตามกระบวนการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ ในสังกัดกรมสนับสนุนบริการสุขภาพ ปฏิบัติงานให้เป็นไปตามมาตรฐานอย่างเป็นระบบเดียวกัน และสอดคล้องกับแนวทางมาตรฐานการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) ที่ส่งผลกระทบต่อประชาชนโดยตรง (Impact Security Risk and Economics Public Health) จากการเชื่อมโยงข้อมูล (Interconnected Information System) รวมทั้งการเป็นหน่วยงานหลักในการควบคุมกำกับมาตรฐานระบบบริการสุขภาพ ด้านที่ ๙ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ และเพื่อให้กรมสนับสนุนบริการสุขภาพ **“ได้รับความเชื่อมั่นและมีความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ รวมทั้งส่งเสริมการทำธุรกรรมอิเล็กทรอนิกส์ด้านระบบบริการสุขภาพ”** เป็นการเพิ่มความสามารถในการแข่งขันการพัฒนาเศรษฐกิจดิจิทัลในการขับเคลื่อนยุทธศาสตร์ชาติตามนโยบายก้าวสู่เศรษฐกิจดิจิทัล (Digital Economy)

๒. ผังกระบวนการ

กระบวนการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ

ลำดับ	กระบวนงาน	รายละเอียด	จุดควบคุมความเสี่ยง	ระยะเวลา (นาที)	ผู้รับผิดชอบ
๑	ศึกษา วิเคราะห์ รวบรวม ข้อมูลสถานการณ์สภาพแวดล้อม	- ศึกษา วิเคราะห์ รวบรวมข้อมูลที่เกี่ยวข้อง -รายงานผลการตรวจสอบจากการปฏิบัติงานภาคสนาม	๑.๑ การคิดเชิงวิเคราะห์ ๑.๒ การคิดเชิงสร้างสรรค์ ๑.๓ การคิดเชิงบูรณาการ ๑.๔ การคิดในภาพรวมเชิงระบบ	๑๘,๓๖๐	งานพัฒนาระบบเทคโนโลยีสารสนเทศ
๒	จัดทำแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	- จัดทำแนวทางการดำเนินงาน - บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ - บริหารจัดการระบบฯ ตามแนวทางมาตรฐานฯ ที่กำหนด	๒.๑ คำสั่งแต่งตั้งฯ ๒.๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๒.๓ แผนบริหารความสี่ยงในสภาวะวิกฤตด้านสารสนเทศ	๑๘,๗๕๙.๖๐	งานพัฒนาระบบเทคโนโลยีสารสนเทศ
๓	ดำเนินการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (ต่อ)	-ประชุมชี้แจงแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ดำเนินงานตามแนวทางมาตรฐานฯ ที่กรมสนับสนุนบริการสุขภาพกำหนด	๓.๑ Gap Analysis ๓.๒ Gap Assessment ๓.๓ Risk Assessment ๓.๔ Risk Management	๓๘,๗๐๐	งานพัฒนาระบบเทคโนโลยีสารสนเทศ

๒. ผังกระบวนการ

กระบวนการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ (ต่อ)

ลำดับ	กระบวนงาน	รายละเอียด	จุดควบคุมความเสี่ยง	ระยะเวลา (นาที)	ผู้รับผิดชอบ
๔	ติดตามผลการบริหารจัดการระบบความมั่นคงปลอดภัย	- ติดตามผลการดำเนินงานจากคณะทำงานฯ - รายงานผลให้คณะกรรมการอำนวยการ / อธิบดีทราบ	๔.๑ ติดตามตรวจสอบ แก้ไขตามข้อกำหนดมาตรฐานฯ ๔.๒ ติดตามผลการดำเนินงานตามตัวชี้วัดที่กำหนด (Process Indicators)	๓,๕๒๘	งานพัฒนาระบบเทคโนโลยีสารสนเทศ
๕	ประเมินผลการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	- Internal Audit by กลุ่มตรวจสอบภายใน - External Audit by MSSP : ISMS Certification - สรุปผลการดำเนินงาน	๕.๑ สรุปผลการดำเนินงานตามตัวชี้วัดที่กำหนด	๑,๗๖๔	งานพัฒนาระบบเทคโนโลยีสารสนเทศ
		รวมระยะเวลา		**๘๑,๑๑๑.๖๐ นาที**	

๓. ขอบเขต รายละเอียดลักษณะงานและการปฏิบัติงาน

๓.๑ กำหนดขั้นตอนการปฏิบัติงานจากการศึกษา วิเคราะห์ รวบรวม ข้อมูลสถานการณ์สภาพแวดล้อมของการเพิ่มขีดความสามารถในการสร้างความเชื่อมั่นในการเข้าถึงข้อมูลด้านระบบบริการสุขภาพ กรมสนับสนุนบริการสุขภาพ และมาตรฐานในการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ใน ๑๔ ประเด็น

๓.๒ กำหนดขอบเขตการดำเนินงาน Server & Network (HSS Net) ซึ่งประกอบด้วย

๓.๒.๑ ภายในของเขตการดำเนินงาน

๑) กระบวนการทำงาน (Process)

๒) ข้อมูลและสารสนเทศ (Information)

๓) ฮาร์ดแวร์ (Hardware)

๔) การบริหารจัดการทรัพย์สิน (Asset management)

๕) ซอฟต์แวร์ (Software)

๖) เครือข่ายคอมพิวเตอร์ (Network)

๗) เครื่องแม่ข่ายเสมือน (Virtual Machine)

๘) บุคลากร (Personnel)

๙) สถานที่และระบบสนับสนุน (Site)

๓.๒.๑ ภายนอกขอบเขตการดำเนินงาน

๑) ระบบงาน ที่ไม่เกี่ยวข้องกับระบบงานของกรมสนับสนุนบริการสุขภาพ (HSS Net)

๒) เครือข่ายคอมพิวเตอร์ระหว่างผู้ใช้บริการที่ไม่เกี่ยวข้องกับระบบงานของกรมสนับสนุนบริการสุขภาพที่กำกับดูแลโดยผู้ให้บริการภายนอกองค์กร

๓.๓ กำหนดการดำเนินงานเป็น ๔ ระยะ จำแนกเป็น ๕ ขั้นตอน ดังนี้

๓.๑ Phase I : Scoping & Planning ประกอบด้วย ขั้นตอนที่ ๑ ทบทวน กำหนด รายละเอียด ขั้นตอนของการดำเนินงาน

๓.๒ Phase II : Gap Assessment & Roadmap ประกอบด้วย ขั้นตอนที่ ๒ กำหนดแนวทางการดำเนินงานตามมาตรฐาน กำหนดตัวชี้วัด และขั้นตอนที่ ๓ วิเคราะห์ หาสาเหตุ โดยการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๓.๓ Phase III : ISMS Implementation ประกอบด้วย ขั้นตอนที่ ๔ พัฒนาและปรับปรุงกระบวนงานตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๓.๔ Phase IV : Internal & External Audit ประกอบด้วย ขั้นตอนที่ ๕ ควบคุม กำกับ ติดตาม และประเมินผลอย่างต่อเนื่อง

๔. หน้าที่และความรับผิดชอบของบุคลากร

๔.๑ “ผู้บริหารระดับสูงสุด” (Chief Executive Officer : CEO) หมายความว่า อธิบดีกรมสนับสนุนบริการสุขภาพ

๔.๒ “ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม” (Department Chief Information Officer: DCIO) หมายความว่า รองอธิบดีหรือผู้ซึ่งได้รับมอบหมายให้รับผิดชอบงานด้านระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๔.๓ “ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ” หมายความว่า ผู้กำกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการใดวิธีการหนึ่ง ด้วยหนังสือเวียนภายในองค์กร ระบบเครือข่ายภายใน (Intranet) หนังสือเวียนอิเล็กทรอนิกส์ หรือเว็บไซต์ภายในและภายนอก กรมสนับสนุนบริการสุขภาพ

๔.๔ “คณะกรรมการ” หมายความว่า คณะกรรมการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๔.๕ “ผู้ดูแลระบบ” (System Administrator) หมายความว่า บุคลากรกรมสนับสนุนบริการสุขภาพผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ ของระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๔.๖ “เจ้าของระบบ” (System Owner) หมายความว่า สำนัก/กอง/กลุ่ม/กลุ่มงาน/ศูนย์ ที่เป็นผู้รับผิดชอบในการพัฒนาระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อสนับสนุนภารกิจการปฏิบัติงานของหน่วยงานให้เกิดประสิทธิภาพ ต่อกรมสนับสนุนบริการสุขภาพในภาพรวม หรือตามที่อธิบดีให้ดำเนินงาน หรือมีหน้าที่อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User)

๔.๗ “ผู้ใช้งาน” (User) หมายความว่า บุคลากรกรมสนับสนุนบริการสุขภาพทุกระดับ ซึ่งเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอก ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายและโปรแกรมประยุกต์หรือแอพพลิเคชั่นของ และ/หรือเกี่ยวข้องกับการใช้ประโยชน์จากระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๕. คำจำกัดความ

๕.๑ “สบส.” หมายความว่า กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

๕.๒ “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไป ตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

(๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๓) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๔) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และและที่แก้ไขเพิ่มเติม

(๕) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๖) กฎหมายอื่นๆ ทั้งในและต่างประเทศที่เกี่ยวข้อง

๕.๓ “แนวปฏิบัติ” หมายความว่า ขั้นตอน วิธีการหรือข้อกำหนดให้ผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ สบส. ได้ถือปฏิบัติตามนโยบาย ข้อ ๓ (๕)

๕.๔ “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของ สบส.

๕.๕ “สินทรัพย์” (asset) หมายความว่า ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของ สบส. ประกอบด้วย

๕.๕.๑ ฮาร์ดแวร์ (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใด อย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งแบบเครื่องแม่ข่ายปกติ (Rack Server) และเครื่องแม่ข่ายแบบชุด (Blade Server)

- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Laptop) อุปกรณ์สื่อสารแบบพกพา (Tablet/Smart phone) รวมถึงอุปกรณ์สนับสนุน เครื่องพิมพ์ (printer/Scanner) และอุปกรณ์สำรองข้อมูลของกรม สบส.

- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

๕.๕.๒ โปรแกรมประยุกต์หรือแอพพลิเคชั่น (Program or Operation System) หมายความว่า ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบประเภท, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ในหัวข้อ Hardware

๕.๕.๓ เครือข่าย (Network and Communication) หมายความว่า ระบบเทคโนโลยีด้านการสื่อสารโทรคมนาคม ของ สบส.

๕.๕.๔ “ระบบสารสนเทศ” หมายความว่า ระบบงานคอมพิวเตอร์ เช่น เว็บไซต์ (Website) เว็บพอร์ทัล (Portal Web) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนา หรือติดตั้ง หรือการนำมาประบุกต์ใช้ เพื่อสนับสนุนการปฏิบัติงานของ สบส.

๕.๕.๕ “ข้อมูลสารสนเทศ” หมายความว่า ข้อมูล (Data) หรือ สารสนเทศ (Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (Files) ฐานข้อมูล (Database) หรือเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (e-Document) เป็นต้น ของ สบส.

๕.๖ “พื้นที่ปฏิบัติงานทั่วไป” (General Working Area) หมายความว่า พื้นที่สำหรับการปฏิบัติงานภายใน สบส. ซึ่งได้มีการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์ลูกข่ายเสมือน เครื่องคอมพิวเตอร์พกพา อุปกรณ์ต่อพ่วงและเครือข่ายแบบมีสาย (LAN) และไร้สาย (Wireless)

๕.๗ “ศูนย์ข้อมูลและสารสนเทศ” หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะ เพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน ประกอบด้วย

๕.๗.๑ “ศูนย์กลางข้อมูล” (DC : Data Center) หมายความว่า ศูนย์กลางข้อมูลและสารสนเทศ ของ สบส. ตั้งอยู่ที่ชั้น ๒ อาคาร สบส.

๕.๗.๒ “ศูนย์สำรองข้อมูล” (DR Site : Disaster Recovery Site) หมายความว่า ศูนย์กลางสำรองข้อมูลและสารสนเทศ ของ สบส. ตั้งอยู่ที่ ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี

๕.๗.๓ “ศูนย์บริการแบบเบ็ดเสร็จ” (OSS One Stop Service) หมายความว่า หน่วยให้บริการข้อมูลด้านระบบบริการสุขภาพแบบเบ็ดเสร็จครบวงจร ณ จุดเดียว ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒ ตั้งอยู่ที่ชั้น ๑ อาคาร สบส.

๕.๗.๔ “ห้องเซิร์ฟเวอร์” (Server Room) หมายความว่า ศูนย์ข้อมูลและสารสนเทศของ สบส. ตั้งอยู่ที่ศูนย์สนับสนุนบริการสุขภาพ หรือ ศูนย์พัฒนาการสาธารณสุขมูลฐาน ของ สบส. จำนวน ๑๒ แห่ง

๕.๘ “เครือข่าย” (Network System) หมายถึง ระบบเครือข่ายที่เชื่อมโยงกับอุปกรณ์ในหัวข้อ Hardware, Software และระบบเทคโนโลยีสารสนเทศของ สบส. ทั้งแบบใช้สายและไร้สาย

๕.๙ “ระบบงาน” หมายถึง ระบบฐานข้อมูลที่สนับสนุนการดำเนินงานของ สบส.

๕.๙.๑ งานคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ

๕.๙.๒ งานสนับสนุนการบริหารจัดการและกำกับมาตรฐานระบบบริการสุขภาพ

๕.๙.๓ งานวิศวกรรมการแพทย์และเครื่องมือแพทย์

๕.๙.๔ งานแบบมาตรฐานอาคารด้านระบบบริการสุขภาพ

๕.๙.๕ งานการมีส่วนร่วมภาคประชาชน

๕.๙.๕.๑ งานสุขศึกษา

๕.๙.๕.๒ งานสนับสนุนสุขภาพภาคประชาชน

๕.๙.๖ “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดแนวปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

๖. ขั้นตอนการปฏิบัติงาน

ตามมติ คณะกรรมการเทคโนโลยีสารสนเทศ (ICT) กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๕๗ ได้กำหนดให้กรมสนับสนุนบริการสุขภาพผ่านเกณฑ์ประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ เพื่อให้การดำเนินงานมีประสิทธิภาพและเกิดประสิทธิผลตามเป้าหมายที่กำหนดตามยุทธศาสตร์ ใน ๕ ขั้นตอน ดังนี้

ขั้นตอนที่ ๑ ทบทวน กำหนด รายละเอียด ขั้นตอนของการดำเนินงาน
ขั้นตอนที่ ๒ กำหนดแนวทางการดำเนินงานตามมาตรฐาน กำหนดตัวชี้วัด
ขั้นตอนที่ ๓ วิเคราะห์ หาสาเหตุ โดยการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓
ขั้นตอนที่ ๔ พัฒนาและปรับปรุงกระบวนงานตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓
ขั้นตอนที่ ๕ ควบคุม กำกับ ติดตาม และประเมินผลอย่างต่อเนื่อง

ขั้นตอนที่ ๑ กำหนดวัตถุประสงค์การดำเนินงาน สอดคล้องตามนโยบาย ประกอบด้วย การทบทวน กำหนดรายละเอียด ขั้นตอนของการดำเนินงานสอดคล้องตามนโยบาย

๑.๑ ทบทวนมาตรการ กำหนดขอบเขตการทำงาน (Scope)

๑.๑.๑ กำหนดขอบเขตการดำเนินงาน Server & Network (HSS Net) ซึ่งประกอบด้วย

๑) กระบวนการทำงาน (Process)
๒) ข้อมูลและสารสนเทศ (Information)
๓) ฮาร์ดแวร์ (Hardware)
๔) การบริหารจัดการทรัพย์สิน (Asset management)
๕) ซอฟต์แวร์ (Software)
๖) เครือข่ายคอมพิวเตอร์ (Network)
๗) เครื่องแม่ข่ายเสมือน (Virtual Machine)
๘) บุคลากร (Personnel)
๙) สถานที่และระบบสนับสนุน (Site)

๑.๑.๒ ภายนอกขอบเขต Server & Network (HSS Net)

๑) ระบบงาน ที่ไม่เกี่ยวข้องกับระบบงานของกรมสนับสนุนบริการสุขภาพ (HSS Net)
๒) เครือข่ายคอมพิวเตอร์ระหว่างผู้ใช้บริการที่ไม่เกี่ยวข้องกับระบบงานของกรมสนับสนุนบริการสุขภาพที่กำกับดูแลโดยผู้ให้บริการภายนอกองค์กร

๑.๒ ดำเนินการจัดตั้งคณะทำงาน IT Security Steering หรือ IT Security Working Group ซึ่งต้องมีการทบทวนทุกปี จากการเปลี่ยนแปลงโครงสร้างองค์กร และประชุมชี้แจงแนวทางการดำเนินงานให้บุคลากรทุกระดับทราบ

๑.๓ ศึกษามาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๑๓ อย่างละเอียดทบทวนและปรับปรุงแก้ไขนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย มาตรการควบคุม ๑๔ หัวข้อ

๑.๓.๑ นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information security policies)

๑.๓.๒ โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร (Organization of information security)

๑.๓.๓ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบุคลากร (Human resource security)

๑.๓.๔ การบริหารจัดการทรัพย์สิน (Asset management)

๑.๓.๕ การควบคุมการเข้าถึง (Access control)

๑.๓.๖ การเข้ารหัสข้อมูล (Cryptography)

๑.๓.๗ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

๑.๓.๘ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านการดำเนินการ (Operations security)

๑.๓.๙ ความมั่นคงปลอดภัยทางด้านการสื่อสาร (Communications security)

๑.๓.๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

๑.๓.๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

๑.๓.๑๒ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสนเทศ (Information security incident management)

๑.๓.๑๓ ประเด็นด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

๑.๓.๑๔ การปฏิบัติตามข้อกำหนด (Compliance)

๑.๔ วิเคราะห์และประเมินองค์กรเบื้องต้น ในประเด็นการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Gap Analysis) เพื่อดำเนินการขับเคลื่อนนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ได้มีประสิทธิภาพ

๑.๕ จัดทำแผนการดำเนินงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑.๕.๑ แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑.๕.๒ นโยบายและแนวปฏิบัติในการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑๕.๓ แผนบริหารความต่อเนื่องในสภาวะวิกฤตสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑๕.๔ แผนบริหารความเสี่ยงด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑๕.๕ ทบทวนผลการดำเนินงานตามแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ขั้นตอนที่ ๒ กำหนดแนวทางการดำเนินงานตามมาตรฐาน ประกอบด้วย การทำความเข้าใจกับกระบวนการ วางแผนการดำเนินงาน และกำหนดตัวชี้วัดในการควบคุม กำกับ ติดตามและประเมินผล

๒.๑ ปรับปรุงกระบวนงานตามมาตรฐาน การพัฒนาองค์กรด้านความมั่นคงปลอดภัยสารสนเทศให้รองรับการตรวจประเมินด้วยมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๒.๑.๑ บริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ประกอบด้วย ๑๔ ข้อกำหนด (Control Area) ๓๔ ข้อควบคุม (Control Objectives) และ ๑๑๔ มาตรการควบคุม (Control Points)

(๑) ISMS Scope

(๒) IT Security Steering Committee

(๓) Internal ISMS Workshop / ISMS Framework / ISMS Framework / ISMS Guideline

(๔) Holistic Approach :

(๔.๑) Gap Analysis

(๔.๒) Gap Assessment

(๔.๓) Risk Assessment and Control

(๔.๔) Risk Management

(๕) Review and Monitor with SOA Statement of Applicability

(๖) Pre Assessment by Internal Auditor

(๗) Assessment by External Auditor for Certify

(๘) ISMS Control / Re - Audit

๒.๑.๒ พัฒนาระบบบำรุงรักษา

(๑) ครุภัณฑ์คอมพิวเตอร์ (Hardware / Software)

(๒) ครุภัณฑ์ระบบเครือข่ายคอมพิวเตอร์ (Computer System Network)

(๓) ครุภัณฑ์โครงข่ายเทคโนโลยีการสื่อสาร (Communication Network)

(๔) อุปกรณ์จัดเก็บข้อมูล (Data Storage Devices) ได้แก่

(๔.๑) สื่อเก็บข้อมูลแบบจานแม่เหล็ก (Magnetic Disk Device) เช่น Hard disk

(๔.๒) สื่อเก็บข้อมูลชนิดแสง (Optical Storage Devices) เช่น CD Rom, CD-R, CD-RW, DVD Rom, DVD-R, DVD-RW

(๔.๓) สื่อเก็บข้อมูลแบบเทป (Tape Devices)

(๔.๔) หน่วยความจำแบบแฟลช (Flash Memory)

(๔.๕) อุปกรณ์จัดเก็บข้อมูลชนิดพกพา (External Hard disk)

(๔.๖) อุปกรณ์จัดเก็บข้อมูลชนิดพกพาที่ไม่มีจานหมุน (Solid-State Drive)

(๕) เซิร์ฟเวอร์ (Server)

(๕.๑) File Server จัดเก็บไฟล์แบบรวมศูนย์ : Centralized Disk Storage

(๕.๒) Print Server สำหรับ Printer ราคาแพงบางรุ่น

(๕.๓) Database Server เพื่อจัดการฐานข้อมูล (Database Management System)

(๕.๔) Application Server เพื่อจัดการโปรแกรมประยุกต์ เช่น Mail Server, Proxy Server หรือ Web Server

๒.๑.๓ ระบบทำลายข้อมูลจากอุปกรณ์จัดเก็บข้อมูลของส่วนราชการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๑.๔ บริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว ในประเด็นต่อไปนี้

(๑) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์

(๒) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล

(๓) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ

(๔) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๕) กำหนดมาตรการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

(๕.๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๕.๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๕.๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๕.๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕.๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

๒.๑.๕ บริหารจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อการคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

(๑) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงทีเกี่ยวข้องกับข้อมูลส่วนบุคคล

(๒) กำหนดหน้าที่ของหน่วยงานที่มีหน้าที่ควบคุม กำกับ ข้อมูลส่วนบุคคล

(๓) กำหนดระดับของข้อมูลส่วนบุคคล พร้อมทั้งรายละเอียดของมาตรการป้องกันข้อมูลส่วนบุคคล

(๔) วิเคราะห์สถานการณ์ และประเมินผลกระทบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

(๕) กำหนดมาตรการจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

(๕.๑) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๕.๒) มาตรการตรวจสอบและเฝ้าระวังการละเมิดข้อมูลส่วนบุคคล

(๕.๓) มาตรการเผชิญเหตุเมื่อมีการตรวจพบการละเมิดข้อมูลส่วนบุคคล

(๕.๔) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากการละเมิดข้อมูลส่วนบุคคล

๒.๑.๖ บริหารจัดการโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศด้านระบบบริการสุขภาพ

(๑) จัดหา ซื้อ เช่าครุภัณฑ์เทคโนโลยีสารสนเทศ (ทดแทน /จัดหา) Software ลิขสิทธิ์ พร้อมครุภัณฑ์คอมพิวเตอร์ทดแทน

(๒) พัฒนาเครือข่ายคอมพิวเตอร์ โครงข่ายการสื่อสาร และการเชื่อมโยงข้อมูลของศูนย์ข้อมูลด้านระบบบริการสุขภาพตามเขตบริการสุขภาพ (Health Care Sectors)

๒.๑.๗ การพัฒนาทักษะ องค์ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy) สำหรับบุคลากร กรมสนับสนุนบริการสุขภาพ

(๑) การพัฒนาศักยภาพบุคลากรขั้นพื้นฐาน (Digital Government Capacity Building)

(๑.๑) การพัฒนาศักยภาพด้านการใช้ระบบเครือข่ายคอมพิวเตอร์

(๑.๒) การพัฒนาศักยภาพด้านการใช้โครงข่ายเทคโนโลยีการสื่อสาร

(๑.๓) การพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy)

(๑.๔) การพัฒนาทักษะความรู้และสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ สำหรับผู้ใช้งาน (User Awareness in Cyber Security)

(๒) การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยสารสนเทศ ชั้นสูง

(๒.๑) การบริหารจัดการระบบคอมพิวเตอร์ (System Administrator)

(๒.๒) การบริหารจัดการระบบเครือข่ายสารสนเทศ (Network Administrator)

(๒.๓) การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Administrator)

(๒.๓.๑) การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

(๒.๓.๒) การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

(๒.๓.๓) การรักษาความปลอดภัยการแผ่รังสี (Emission Security)

(๒.๓.๔) การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

(๒.๓.๕) การรักษาความปลอดภัยเครือข่าย (Network Security)

(๒.๓.๖) การรักษาความปลอดภัยข้อมูล (Information Security)

๒.๑.๘ การพัฒนาศักยภาพบุคลากรเฉพาะทาง

(๑) การพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๑.๑) พัฒนาทักษะบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๑.๑.๑) ผู้บริหารเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

(๑.๑.๒) ผู้เชี่ยวชาญและจัดการเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

(๑.๑.๓) ผู้ประเมินความเสี่ยงและช่องโหว่ระบบเทคโนโลยีสารสนเทศ

(๑.๑.๔) ผู้ตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์

(๑.๑.๕) ผู้ประเมินความเสี่ยงและช่องโหว่ระบบเทคโนโลยีสารสนเทศ

(๑.๑.๖) นักทดสอบช่องโหว่และภัยคุกคามระบบเทคโนโลยีสารสนเทศ

- การตรวจสอบระบบเทคโนโลยีสารสนเทศด้วยวิธีการตรวจสอบ ช่องโหว่ Vulnerability Assessment (Web Application Hacking)
- การเจาะระบบ (Penetration Testing)

(๑.๑.๗) นักวิจัยและวิเคราะห์งานเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

(๑.๒) สนับสนุนการผ่านการประเมินด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ISEC : Information Security Expert Certification, CISSP : Certified Information System Security Professional, CISA, CASP, CISM, CSX, CompTIA เป็นต้น

๒.๑.๙ บริหารจัดการบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ (Human Resource Management)

(๑) เสนอขออนุมัติจัดจ้างผู้เชี่ยวชาญภายนอก

(๑.๑) ด้านการบริหารจัดการระบบคอมพิวเตอร์ (Computer System Administrator)

(๑.๒) ด้านการบริหารจัดการระบบเครือข่ายสารสนเทศ (Network Administrator)

(๑.๓) ด้านการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Administrator)

๒.๑.๑๐ เสนอกรอบอัตรากำลังบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๑) เสนอโครงสร้างบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

(๒) เสนอขอจัดสรร/ทดแทน อัตรากำลัง ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ

(๓) วิเคราะห์กรอบอัตรากำลัง เสนอต่อกลุ่มบริหารงานบุคคล เพื่อเสนอต่อคณะอนุกรรมการสามัญกรมสนับสนุนบริการสุขภาพ (อกพ.) พิจารณา

(๔) กำหนดเส้นทางความก้าวหน้าในวิชาชีพสายความมั่นคงปลอดภัยสารสนเทศ

๒.๒ กำหนดตัวชี้วัดในการควบคุม กำกับ ติดตามและประเมินผล

ตัวชี้วัด (CSF) คือ **ระดับความสำเร็จของการการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ** (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ)

ตัวชี้วัดที่ ๑.๑ ระดับความสำเร็จของการการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ : Process Indicator)

ตัวชี้วัดที่ ๒.๑ ร้อยละ ๘๐ ของบุคลากรพึงพอใจต่อการพัฒนาองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy) (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ : Process Indicator)

ตัวชี้วัดที่ ๒.๒ จำนวนบุคลการผ่านเกณฑ์ประเมินมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Certification**)** (ตัวชี้วัดทางตรง ด้านการบริหารจัดการ : Process Indicator)

ผลสัมฤทธิ์ : ประชาชนมีความเชื่อมั่น ในการเข้าใช้ประโยชน์จากข้อมูลด้านระบบบริการสุขภาพที่มีความมั่นคงปลอดภัย (CIA) : ทั้งการรักษาความลับ (Confidentiality) ความถูกต้อง แม่นยำ ครบถ้วน (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) รวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ ของกรมสนับสนุนบริการสุขภาพ

๒.๓ การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐานที่กำหนด

๒.๔ การจัดการความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

ขั้นตอนที่ ๓ หมายถึง วิเคราะห์ หาสาเหตุ โดยการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ (Gap Assessment)

๓.๑ วิเคราะห์ช่องว่างมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Gap Assessment) พบว่ากรมสนับสนุนบริการสุขภาพ มีความพร้อมรองรับตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๓.๒ วิเคราะห์ความเสี่ยง (Risk Assessment)

๓.๒.๑ วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๒.๒ วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๓.๒.๓ วิเคราะห์ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

๓.๓ กำหนดแนวทางป้องกันความเสี่ยง วางแผนป้องกันความเสี่ยง (Risk Management Framework)

๓.๓.๑ วางแผนป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๒.๒ วางแผนป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๓.๒.๓ วางแผนป้องกันความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

๓.๔ จัดทำรายงานและนำเสนอต่อ Board of Director เพื่อผู้บริหารระดับสูงเข้าใจในปัญหาที่เกิดขึ้น และดำเนินการแก้ไขข้อบกพร่องจากการที่องค์กรยังไม่ได้ปฏิบัติตามมาตรฐานฯ ดังกล่าวอย่างเป็นรูปธรรม (Corrective Action)

๓.๕ กลุ่มตรวจสอบภายในดำเนินการตรวจสอบ (Pre-Assessment) ระดับ Internal Auditor

ขั้นตอนที่ ๔ พัฒนา ปรับปรุงกระบวนงานตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๔.๑ ประเมินระบบความมั่นคงปลอดภัยสารสนเทศในภาพรวม (Gap Analysis Holistic Approach) ด้วยการนำเสนอ Gap Analysis Report ใน ๓ มุมมอง

๔.๑.๑ มุมมองด้านบุคลากร (People)

๔.๑.๒ มุมมองด้านกระบวนการ (Process)

๔.๑.๓ มุมมองด้านเทคโนโลยี (Technology)

๔.๒ วิเคราะห์ความเสี่ยง ประเมินและปรับปรุงความเสี่ยงตามแผนการดำเนินงานที่กำหนด (Risk Assessment)

๔.๓ การบริหารจัดการความเสี่ยง ควบคุมตามแผนที่ได้กำหนดไว้ (Risk Management) เช่น Vulnerability Assessment, Penetration Testing, Hardening เป็นต้น

๔.๔ จัดทำเอกสารรองรับการประเมิน ในรูปแบบ Statement of Applicability (SOA) เพื่อรองรับการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๔.๕ จัดทำรายงานเสนอ Board of Director (DCIO, CEO)

ขั้นตอนที่ ๕ ควบคุม กำกับ ติดตาม และประเมินผลอย่างต่อเนื่อง

๕.๑ ควบคุม กำกับ (Control) สอบทาน (Review) และการเฝ้าระวัง (Monitor) เตรียมพร้อมรองรับการตรวจประเมินมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (Gap Analysis Report)

๕.๑.๑ การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ

๕.๑.๒ การจัดการความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๒ การจัดการและควบคุมความเสี่ยง (Risk Assessment & Re-Assessment & Control)

๕.๓ สรุปรายงานผลการดำเนินงานการพัฒนา / ติดตาม / ประเมินผลตามตัวชี้วัดที่กำหนด (KPI / CSF)

๕.๔ ดำเนินการตรวจประเมิน ครั้งที่ ๑ (Assessment) โดย External Auditor ด้วยการ Outsource ไปยัง Manage Security Service Provider หรือ MSSP ที่ถือเป็นการ “Transfer Risk”

๕.๕ ดำเนินการตรวจประเมิน ครั้งที่ ๒ (Re - Assessment) โดย External Auditor ทุก ๓ ปี

๗. กฎหมาย มาตรฐาน และเอกสารที่เกี่ยวข้อง

๗.๑ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๗.๒ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๗.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๗.๔ พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม

๗.๕ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และที่แก้ไขเพิ่มเติม

๗.๖ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๗.๗ ประกาศกระทรวงสาธารณสุข เรื่อง การกำหนดลักษณะของสถานพยาบาลและมาตรฐานซึ่งได้รับการยกเว้นไม่ต้องอยู่ในบังคับกฎหมายว่าด้วยสถานพยาบาล (ฉบับที่ ๒) ในมาตรา ๕ วรรคสอง แห่งพระราชบัญญัติสถานพยาบาล พ.ศ.๒๕๔๑ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติสถานพยาบาล (ฉบับที่ ๔) พ.ศ. ๒๕๕๙

๗.๘ กฎหมายอื่นๆ ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพ

๘. การจัดเก็บและเข้าถึงเอกสาร

๘.๑ การจัดเก็บ

ชื่อเอกสาร	สถานที่เก็บ	ผู้รับผิดชอบ	ระยะเวลา
๑.คำสั่งคณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ	เลขานุการคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	๑๐ ปี
๒. แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ	เลขานุการคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	๑๐ ปี
๓. นโยบายและแนวปฏิบัติในการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ	เลขานุการคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	๑๐ ปี
๔ .แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ	เลขานุการคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	๑๐ ปี
๕. แผนบริหารความเสี่ยงด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ	เลขานุการคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	๑๐ ปี

๘. การจัดเก็บและเข้าถึงเอกสาร (ต่อ)

๘.๑ การจัดเก็บ

ชื่อเอกสาร	สถานที่เก็บ	ผู้รับผิดชอบ	ระยะเวลา
๖. ผลการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ	เลขานุการคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ	๑๐ ปี

๘.๒ ผู้มีสิทธิเข้าถึง

๘.๒.๑ คณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๘.๒.๒ ผู้เกี่ยวข้องกับการดำเนินงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ที่ขอเข้าถึงเอกสารฯ ดังกล่าว

๙. ระบบการติดตามและประเมินผล

๙.๑ มีการติดตาม ประเมินผลการดำเนินงาน โดย เลขานุการคณะทำงาน/เลขานุการคณะกรรมการอำนวยการในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๙.๒ ร้อยละ ๘๐ ของความสำเร็จในการดำเนินงาน สามารถปฏิบัติงานได้ตามขั้นตอนของคู่มือปฏิบัติงานการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศได้อย่างถูกต้อง

๙.๓ กลวิธีการเข้าถึง

๙.๓.๑ ผู้บริหาร/ผู้รับผิดชอบให้ความสำคัญและเข้าใจในการดำเนินงานตามขั้นตอนของคู่มือ

๙.๓.๒ เผยแพร่คู่มือ ให้ผู้เกี่ยวข้องทราบ

๑๐. ภาคผนวก

๑๐.๑ แผนภาพแสดงการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑๐.๒ การวิเคราะห์ภาระงานของบุคลากรในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๑. บันทึกการปรับปรุงแก้ไขเอกสาร (Version History)

เวอร์ชั่น	วันที่ปรับปรุงแก้ไข	หน้า	รายละเอียดการปรับปรุงแก้ไข	ผู้รับผิดชอบ
๑	๑ ตุลาคม ๒๕๖๓	ทั้งหมด	เอกสารใหม่	เลขานุการคณะทำงานในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

ภาคผนวก ก. แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรม สบส.

ระยะ (Phase)	Phase I Scoping & Planning	Phase II Gap Assessment & Roadmap	Phase III Implementation	Phase IV Internal & External Audit
วัตถุประสงค์ (Aim)	กำหนดวัตถุประสงค์การดำเนินงานสอดคล้องตามนโยบาย (1)	กำหนดแนวทางการดำเนินตามมาตรฐาน (2,3)	พัฒนาและปรับปรุงกระบวนงานตามแนวทางมาตรฐาน (4)	ควบคุม กำกับ ติดตามและประเมินผล ตามแนวทางมาตรฐาน (5)
ขั้นตอน (Activities)	(1.1) ทบทวนมาตรการ **กำหนดขอบเขต (Scope)** การดำเนินงาน (1) (1.2) จัดตั้งคณะทำงาน (1.3) **ศึกษามาตรฐาน** ปรับปรุงแก้ไขนโยบายฯ ตามแนวทางการดำเนินงานให้สอดคล้องตามที่กฎหมายกำหนด (2) (1.4) วิเคราะห์ และประเมินองค์กรเบื้องต้น **(Gap Analysis)** (3) (1.5) จัดทำแผนยุทธศาสตร์ฯ /นโยบายและแนวปฏิบัติฯ /แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ	(2.1) ปรับปรุงกระบวนงานตามมาตรฐาน (2.2) กำหนดตัวชี้วัด ควบคุม กำกับ ติดตามและประเมินผล (3.1) วิเคราะห์ช่องว่างมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ **(Gap Assessment)** (3.2) วิเคราะห์ความเสี่ยง **(Risk Assessment)** (3.3) กำหนดแผนบริหารความเสี่ยง **(Risk Management Framework)** (3.4) จัดทำรายงานเสนอ Board (3.5) กลุ่มตรวจสอบภายในดำเนินการตรวจสอบ **(Pre-Assessment)**	(4.1) ประเมินระบบในภาพรวม **(Holistic Approach)** ตาม Gap Analysis Report ปฏิบัติตามข้อกำหนดมาตรฐานฯ (4.2) ประเมินความเสี่ยงตามแผนการดำเนินงานที่กำหนด (Risk Assessment) (4.4) จัดทำเอกสารรองรับการประเมิน **(SOA)** (4.5) จัดทำรายงานเสนอ Board of Director (DCIO, CEO)	(5.1) Gap Analysis Report (5.2) Risk Assessment / Re Assess & Control (5.2) KPI : CSF (5.4) การประเมินครั้งที่ 1 (5.5) การประเมินครั้งที่ 2
แนวคิด/แนวทางการดำเนินงาน	(4.3) การบริหารจัดการความเสี่ยง (Risk Management) (2.3) การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ ตามมาตรฐานที่กำหนด (2.4) การจัดการความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy) / SOC Team			
งบประมาณ	กำหนดพื้นที่ CII : Data Center, DR Site และ OSS รวมทั้ง Data Room ของ ศบส.ที่ 1-12			

ภาคผนวก ข. การวิเคราะห์ภาระงานของบุคลากรในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ พ.ศ. ....

ลำดับ	แนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศ	ประเด็นในการดำเนินงาน ปีงบประมาณ พ.ศ.	หน่วยนับ	ระยะเวลาในการทำงานและขั้นตอน		ระยะเวลาในการทำงาน ต่อ ๑ หน่วยนับ (นาที)	ผลงาน/ปริมาณงาน ปี		อัตรำลังที่คำนวณได้	บุคลากรที่เกี่ยวข้องในงาน (X)			กรอบอัตรากำลังที่เหมาะสมในการปฏิบัติงาน
				ตัวเลข	หน่วย		ตัวเลข	หน่วย		ขรก.	พรก.	ลจป.	

ภาคผนวก ค

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support

รายชื่อคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ ๒๕๖๓

ลำดับ	รายชื่อ	ตำแหน่ง	หมายเหตุ
๑.	ดร.นพ.ภานุวัฒน์ ปานเกตุ	ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (DCIO) รองอธิบดีกรมสนับสนุนบริการสุขภาพ	ประธานฯ
๒.	นายอภินันท์ นิลฉาย	ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม	คณะทำงาน
๓.	นางสาวชวันธร สัมฤทธิ์	เจ้าพนักงานธุรการปฏิบัติงาน สำนักงานเลขานุการกรม	คณะทำงาน
๔.	นายทวิช เทียนคำ	นักวิชาการเผยแพร่ชำนาญการพิเศษ สำนักงานเลขานุการกรม	คณะทำงาน
๕.	นางสาวสิริลักษณ์ จุทิ่น	นักวิเคราะห์นโยบายและแผนชำนาญการ กองกฎหมาย	คณะทำงาน
๖.	นายวุฒิศักดิ์ ชูตน	วิศวกรโยธาชำนาญการ กองแบบแผน	คณะทำงาน
๗.	นายธันวา โทนวิรัตน์	นายช่างเทคนิคชำนาญงาน กองวิศวกรรมการแพทย์	คณะทำงาน
๘.	นางสาวรัตนา สังข์เพชร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองวิศวกรรมการแพทย์	คณะทำงาน
๙.	นายพิศณุพงศ์ ศรีงามเมือง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองสถานประกอบการเพื่อสุขภาพ	คณะทำงาน
๑๐.	นายธนัท บุญสังข์	นักวิชาการสาธารณสุขชำนาญการ กองสถานพยาบาลและการประกอบโรคศิลปะ	คณะทำงาน
๑๑.	นายอุดร อมรไทยสุนทร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองสถานพยาบาลและการประกอบโรคศิลปะ	คณะทำงาน
๑๒.	นายชนินทร์ ห่านตระกูล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองสนับสนุนสุขภาพภาคประชาชน	คณะทำงาน
๑๓.	ว่าที่ ร.ต.หญิงชนิศรา ผาคำ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองสุขศึกษา	คณะทำงาน
๑๔.	นางณัฐณิชา กลัมพสุต	นักวิชาการตรวจสอบภายในชำนาญการพิเศษ กลุ่มตรวจสอบภายใน	คณะทำงาน
๑๕.	นายทศพล คล้ายขำ	นักวิเคราะห์นโยบายและแผน กลุ่มพัฒนาระบบบริหาร	คณะทำงาน
๑๖.	นายศุภชัย กันทาใจ	นักทรัพยากรบุคคลชำนาญการพิเศษ กลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม	คณะทำงาน

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support

รายชื่อคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ ๒๕๖๓

ลำดับ	รายชื่อ	ตำแหน่ง	หมายเหตุ
๑๗.	นายสุรชัย สมิงรัมย์	นักทรัพยากรบุคคลปฏิบัติการ กลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม	คณะทำงาน
๑๘.	จ่าอากาศโทอธิปพงศ์ ขานไข	นักทรัพยากรบุคคลปฏิบัติการ กลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม	คณะทำงาน
๑๙.	นายวิรัลพัชร กรชญา	เจ้าพนักงานธุรการปฏิบัติงาน กลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม	คณะทำงาน
๒๐.	นางสาวบุศรินทร์ ศรีชาติ	นักทรัพยากรบุคคล กลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม	คณะทำงาน
๒๑.	นายสุพจน์ สว่างดี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กลุ่มแผนงาน สำนักงานเลขานุการกรม	คณะทำงาน
๒๒.	นางสิริกร เสนีย์วงศ์ ณ อยุธยา	เจ้าพนักงานธุรการชำนาญงาน กลุ่มงานคุ้มครองจริยธรรม	คณะทำงาน
๒๓.	นางสาวศิรินภา สระทองหน	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กองสุขภาพระหว่างประเทศ	คณะทำงาน
๒๔.	นายเอกลักษณ์ คุ้มเมือง	นักจัดการงานทั่วไป กองสุขภาพระหว่างประเทศ	คณะทำงาน
๒๕.	นายทัตเทพ เมืองวงศ์	นักวิเคราะห์นโยบายและแผน กองสุขภาพระหว่างประเทศ	คณะทำงาน
๒๖.	นางสาวอารยา สุขบุญเกิด	นักวิชาการสาธารณสุข ศูนย์คุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ	คณะทำงาน
๒๗.	นางสาวยุวลักษณ์ ขันอาสา	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ ผู้แทนสำนักผู้เชี่ยวชาญ	คณะทำงาน
๒๘.	นางก่อกุล ใสสกุล	นักวิเคราะห์นโยบายและแผนชำนาญการ ศูนย์บริการแบบเบ็ดเสร็จ	คณะทำงาน
๒๙.	นางสาวกมลพร พันหล้อ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑ (จังหวัดเชียงใหม่)	คณะทำงาน

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support

รายชื่อคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ ๒๕๖๓

ลำดับ	รายชื่อ	ตำแหน่ง	หมายเหตุ
๓๐.	นายศรุต ม่วงศิริ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๒ (จังหวัดพิษณุโลก)	คณะทำงาน
๓๑.	นายวัชรินทร์ นาคมี	ปฏิบัติงานด้านคอมพิวเตอร์ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๓ (จังหวัดนครสวรรค์)	คณะทำงาน
๓๒.	นางสาววรรณภา สอนจันทร์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๔ (จังหวัดนนทบุรี)	คณะทำงาน
๓๓.	นายสมยศ หลวงผาด	นายช่างเทคนิคชำนาญงาน ศูนย์สนับสนุนบริการสุขภาพ ที่ ๕ (จังหวัดราชบุรี)	คณะทำงาน
๓๔.	นางสาวพัชราวลี แจ่มศรี	ปฏิบัติงานด้านคอมพิวเตอร์ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๕ (จังหวัดราชบุรี)	คณะทำงาน
๓๕.	นายทศพงษ์ ตรีเนตร	นายช่างเทคนิคอาวุโส ศูนย์สนับสนุนบริการสุขภาพ ที่ ๖ (จังหวัดชลบุรี)	คณะทำงาน
๓๖.	นายไชยวัฒน์ พงษ์พิสิฐวงศ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๖ (จังหวัดชลบุรี)	คณะทำงาน
๓๗.	นายธันวา เชาว์โคกสูง	ปฏิบัติงานด้านคอมพิวเตอร์ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๗ (จังหวัดขอนแก่น)	คณะทำงาน
๓๘.	นายปัญญา บุญราวิกุล	ปฏิบัติงานด้านคอมพิวเตอร์ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๘ (จังหวัดอุดรธานี)	คณะทำงาน
๓๙.	นายเอกวิทย์ เทียบทรง	นายช่างเทคนิคปฏิบัติงาน ศูนย์สนับสนุนบริการสุขภาพ ที่ ๙ (จังหวัดนครราชสีมา)	คณะทำงาน
๔๐.	นายสมยศ บุรีรักษ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๙ (จังหวัดนครราชสีมา)	คณะทำงาน

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support

รายชื่อคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ ๒๕๖๓

ลำดับ	รายชื่อ	ตำแหน่ง	หมายเหตุ
๔๑.	นายราชชสาส์น อินสิงห์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๐ (จังหวัดอุบลราชธานี)	คณะทำงาน
๔๒.	นายชาญศิลป์ แสงอรุณ	ช่างฝีมือโรงงาน (ลจป.) ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๑ (จังหวัดสุราษฎร์ธานี)	คณะทำงาน
๔๓.	นางสาวภาวินี ยาวิราช	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๒ (จังหวัดสงขลา)	คณะทำงาน
๔๔	นางเพ็ญศรี โตเทศ	นักวิชาการสาธารณสุขชำนาญการ ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคเหนือ จังหวัดนครสวรรค์	คณะทำงาน
๔๕.	นายมฤคราช ไชยภาพ	นักวิชาการสาธารณสุขปฏิบัติการ ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคเหนือ จังหวัดนครสวรรค์	คณะทำงาน
๔๖.	นายกฤษณชัย กิมชัย	นักวิชาการสาธารณสุขชำนาญการ ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น	คณะทำงาน
๔๗.	นางวริษฐา ทรัพย์ธรณี	นักจัดการงานทั่วไปชำนาญการ ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น	คณะทำงาน
๔๘.	นายอภิสิทธ์ ปะสาวะเท	ปฏิบัติงานด้านคอมพิวเตอร์ ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น	คณะทำงาน
๔๙.	นางรุ่งอรุณ บูรณะ	เจ้าพนักงานการเงินปฏิบัติงาน ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคกลาง จังหวัดชลบุรี	คณะทำงาน
๕๐.	จ.อ.ศุภปกรณ์ ขวัญใจ	เจ้าพนักงานโสตทัศนศึกษาชำนาญงาน ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคใต้ จังหวัดนครศรีธรรมราช	คณะทำงาน
๕๑.	นางสาววลัยลักษณ์ ทะบุตร	เจ้าพนักงานพัสดุปฏิบัติงาน ศูนย์พัฒนาการสาธารณสุขมูลฐานชายแดนใต้ จังหวัดยะลา	คณะทำงาน

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support

รายชื่อคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ปีงบประมาณ ๒๕๖๓

ลำดับ	รายชื่อ	ตำแหน่ง	หมายเหตุ
๕๒.	นายธีรพงศ์ เรือนน้อย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม	คณะทำงาน
๕๓.	นางสาวนรารัตน์ มุลจันดา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม	คณะทำงาน
๕๔.	นายนันทชัย นุ่มน้อย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม	คณะทำงาน
๕๕.	นางสาวธนิมา สังข์สุวรรณ์	นักวิชาการสาธารณสุขชำนาญการ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม	คณะทำงานและเลขานุการฯ

ภาคผนวก ง

Critical Services ด้านสาธารณสุข – Health [HSS เสนอเพิ่ม Patient ID : 19 March,2020]

ด้านการให้บริการสุขภาพ (Health Services) (ใน-ระหว่าง รพ.)	ด้านยา เวชภัณฑ์ และ เครื่องมือแพทย์	ด้านการให้บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา	ด้านข้อมูลสุขภาพดิจิทัล (Digital Health)
Regulator : • กรมสนับสนุนบริการสุขภาพ (Main) • กรมการแพทย์ (Sub) • กรมควบคุมโรค (Sub) Critical Operator :	Regulator : • สำนักงานคณะกรรมการอาหารและยา Critical Operator :	Regulator : • กรมวิทยาศาสตร์การแพทย์ (Main) • สำนักงานพลังงานปรมาณูเพื่อสันติ (Sub) Critical Operator :	Regulator : • สำนักงานปลัดกระทรวงสาธารณสุข Critical Operator :
Critical Services	Critical Services	Critical Services	Critical Services
▪ *บริการข้อมูลผู้ป่วย การยืนยันตัวตน (Patient ID) เสนอเพิ่ม* ▪ บริการทางการแพทย์ในสถานพยาบาล (ห้องฉุกเฉิน ห้องผ่าตัด ห้องคลอด ห้องผู้ป่วยวิกฤต หอผู้ป่วยใน / ระบบสนับสนุน (ก๊าซทางการแพทย์ ไฟฟ้า ประปา ขนส่ง) ▪ ระบบการควบคุมการแพร่กระจายเชื่อโรค ใน รพ.	▪ บริการผลิตยา / วัคซีน ▪ บริการผลิตเวชภัณฑ์ ▪ บริการผลิตเครื่องมือแพทย์	▪ บริการการตรวจวิเคราะห์ทางการแพทย์ (Analyzer) ▪ บริการทางรังสีวิทยา ▪ บริการทางกัมตรังสี	▪ บริการด้านการเงินการคลังสุขภาพ (ด้านสวัสดิการ ,หลักประกันสุขภาพ, ประมวลผลข้อมูลเพื่อการเบิกจ่าย) ▪ บริการรับส่งข้อมูลเบิกจ่ายค่ารักษาพยาบาล (Health Data Clearing House Services)
▪ บริการส่งต่อผู้ป่วยระหว่างสถานพยาบาล (Referral Services) ▪ บริการการแพทย์ฉุกเฉินนอกสถานพยาบาล ▪ บริการทางห้องปฏิบัติการ ▪ บริการทางรังสีวิทยา ▪ บริการโลหิตและคลังเลือด ▪ การควบคุมโรคติดต่อ	▪ บริการนำเข้า กระจายและจำหน่ายยา ▪ บริการนำเข้า กระจายและจำหน่ายเวชภัณฑ์ ▪ บริการนำเข้า กระจายและจำหน่ายเครื่องมือแพทย์		▪ บริการคลังข้อมูลสุขภาพ (คลังข้อมูลสุขภาพที่อยู่นอกหน่วยบริการ) ▪ บริการระบบสุขภาพดิจิทัล (บริการโทรเวชกรรม, บริการติดตามข้อมูลสุขภาพรายบุคคล, บริการตรวจวิเคราะห์ข้อมูลสุขภาพดิจิทัล, บริการ Wearable device

มาตรฐานที่เกี่ยวข้อง : ISO 27001, ISO 27799, HIPAA (NIST 800-66), Joint Commission International หัวข้อ Management of Information, Healthcare Accreditation หัวข้อ I-4.2

สาระสำคัญของ พ.ร.บ. ไซเบอร์ ในประเด็นการกำหนดแนวทางปฏิบัติและกรอบมาตรฐานฯ [HSS]

“มาตรา 3 ในพระราชบัญญัตินี้

CI [Critical Infrastructure] : “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้กิจการ (CS : Critical Services) ของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

CII [Critical Information Infrastructure] : “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Regulator : “หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจ ในการควบคุมหรือ กำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ : Critical Information Infrastructure (CII)

[HSS]

คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) อำนาจหน้าที่ มาตรา 9

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) อำนาจหน้าที่ มาตรา 11

คณะกรรมการบริหารสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)
สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อำนาจหน้าที่ มาตรา 22

Regulator

ประมวลแนวทางปฏิบัติ/ตรวจสอบการปฏิบัติ

มาตรา 53 (หน่วยงานควบคุมหรือกำกับ ดูแล)
- ตรวจสอบมาตรฐานขั้นต่ำ
- สั่งให้แก้ไข
- รายงาน กกม. (ถ้าเพิกเฉย)

กรมสนับสนุนบริการสุขภาพ

HSS SOC Team : ศูนย์ปฏิบัติการเฝ้าระวังการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรม สบส.

สถานพยาบาล

Operator

แผนรับมือ : COBIT/ISO27001/NIST

มาตรา 54 (หน่วยงานโครงสร้างพื้นฐาน)
- ประเมินความเสี่ยง
- ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้ง

หน่วยงานเฝ้าระวัง ติดตาม ตรวจสอบ เผชิญเหตุ
- Health CERT
- ICS-CERT
- National Health-ISAC

มาตราที่เกี่ยวข้อง	ม.44,45,46,52 ม.53 ม.56,57 ม.59	ม.44, 45,46,52 ม.54 ม.56,57 ม.58
บทลงโทษ	ม.73,ม.77,ม.49 (7) ด้านสาธารณสุข	

- หน่วยงานตรวจประเมินความเสี่ยงระบบ (IS Audit)
- ประมวลแนวทางปฏิบัติ (ตามแผนชาติ)

ภาพรวมการดำเนินการ [HSS]

CII Sector Critical Service

1. กำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (CII Sector)

2. กำหนดปัจจัยและเกณฑ์การคัดเลือก Critical Service จากบริการที่ใช้งานจริง

3. กำหนด Regulator ของแต่ละ Sector

ก.DE/สกมช./กกม.

Identify Critical Service

4. กำหนดรายการบริการที่สำคัญทางสารสนเทศ (Critical Service)

5. กำหนด Critical Service ของหน่วยงานตามปัจจัยและเกณฑ์

6. กำหนดมาตรฐานที่เกี่ยวข้อง

หน่วยงาน Regulator/CII

Identify CII Assets related to Critical Service

7. ประเมินความเสี่ยง กระบวนการของสินทรัพย์ทางสารสนเทศ (Critical Asset) ที่เกี่ยวข้องกับ Critical Service

หน่วยงาน CII

Policy and Practice, IR Respond

8. จัดทำแผนปฏิบัติการด้านการรับมือภัยคุกคามไซเบอร์โดยอ้างอิงตาม ม.13 (4)

9. ดำเนินการตามแผนปฏิบัติการฯ

หน่วยงาน CII

Developing and Internal IR Respond plan

10. ทบทวน ตรวจสอบแผนปฏิบัติการฯ เป็นประจำ

11. ทบทวนรายการหน่วยงาน CII / Critical Asset / Critical Service

หน่วยงาน Regulator/CII

สมรรถนะเป็นฐาน
สร้างสรรค์สิ่งใหม่
บริการด้วยใจ
ใฝ่สามัคคี