# แผนบริหารความเสี่ยงด้านสารสนเทศ

กลุ่มเทคโนโลยีสารสนเทศ
สำนักงานเลขานุการกรม

**พ.ศ. ๒๕๖๓**

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

# คำนำ

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข ได้จัดทำ “แผนบริหารความเสี่ยงด้านสารสนเทศ” ขึ้นเพื่อเป็นกรอบแนวทางการปฏิบัติงานในการบริหารความเสี่ยงด้านสารสนเทศ สำหรับผู้บริหาร บุคลากรด้านเทคโนโลยีสารสนเทศภายในกรมสนับสนุนบริการสุขภาพ ตามแนวทางการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ด้วยมาตรฐานการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (ISMS : Information Security Management System) ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ในข้อกำหนดที่ ๗ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) และตามแนวทางการพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวด ๒ การวางแผนเชิงยุทธศาสตร์ SP ๗ ที่กำหนดให้ส่วนราชการต้องมีการวิเคราะห์และจัดทำแผนบริหารความเสี่ยงตามมาตรฐาน COSO (The Committee of Sponsoring Organizations of the Tread way Commission) เพื่อเตรียมรองรับการเปลี่ยนแปลงที่อาจจะเกิดขึ้น จากการดำเนินแผนงาน/โครงการที่สำคัญ ครอบคลุมความเสี่ยงด้านธรรมาภิบาล ให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพและมีประสิทธิผลขององค์กร รวมทั้งมีความรู้ ความเข้าใจในเรื่องการบริหารความเสี่ยงด้านสารสนเทศและสามารถนำไปปฏิบัติได้อย่างมีประสิทธิผลและต่อเนื่อง

หวังเป็นอย่างยิ่งว่า “แผนบริหารความเสี่ยงด้านสารสนเทศ” ฉบับนี้ จะเป็นประโยชน์ต่อผู้บริหาร บุคลากรด้านเทคโนโลยีสารสนเทศภายในกรมสนับสนุนบริการสุขภาพ ในการปฏิบัติงานต่อไป

**กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม**
**กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข**
**๑๑ พฤศจิกายน ๒๕๖๓**

# สารบัญ

# สารบัญ (ต่อ)

# บทที่ ๑

## บทนำ

### ๑.๑ หลักการและเหตุผล

การนำกระบวนการบริหารความเสี่ยงมาใช้ภายในองค์กร โดยอาศัยหลักการพื้นฐานของการกำกับดูแลกิจการขององค์กรที่ดี (Good Governance) ทั้งนี้ เพื่อให้ผู้มีส่วนได้เสียขององค์กรสามารถเชื่อมั่นอย่างสมเหตุสมผลว่าการดำเนินงานเชิงกลยุทธ์ของงานด้านเทคโนโลยีสารสนเทศ มุ่งไปสู่การบรรลุวัตถุประสงค์และเป้าหมายขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล ดังนั้น การพัฒนากระบวนการบริหารความเสี่ยงด้านสารสนเทศให้ประสบผลสำเร็จได้นั้น จำเป็นจะต้องส่งเสริมและผลักดันให้มีการบริหารความเสี่ยงทั่วทั้งองค์กรทุกระดับ รวมทั้งรณรงค์ให้ผู้บริหารและบุคลากรทุกคนตระหนักและเข้าใจถึงความสำคัญของการบริหารความเสี่ยง

กรมสนับสนุนบริการสุขภาพ เป็นหน่วยงานที่มีหน้าที่กำกับ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) ด้านระบบบริการสุขภาพ ที่ส่งผลกระทบต่อประชาชนโดยตรง (Impact Security Risk และ Economics Public Health) จากการเชื่อมโยงข้อมูลด้านระบบบริการสุขภาพ (Interconnected Information System) และหน่วยงานที่เกี่ยวข้องควรต้องผ่านเกณฑ์มาตรฐาน เพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการในระบบบริการสุขภาพรวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ จำเป็นจะต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ

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

การบริหารความเสี่ยง คือ กระบวนการที่เป็นระบบในการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินการต่างๆ เพื่อลดมูลเหตุของโอกาส ที่จะทำให้เกิดความเสียหายจากการดำเนินการที่ไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ ควบคุมได้ และตรวจสอบได้อย่างเป็นระบบ

ความเสี่ยง คือ เหตุการณ์/การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายของแผนงาน/โครงการที่สำคัญในแต่ละประเด็นยุทธศาสตร์ตามที่ระบุในแผนปฏิบัติราชการประจำปีของส่วนราชการเพื่อนำไปใช้เป็นเครื่องมือในการดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และเกิดประโยชน์สูงสุดแก่องค์กร

### ๑.๒ ภาพรวมการบริหารความเสี่ยง

การจัดทำระบบบริหารความเสี่ยงด้านสารสนเทศ ตามเกณฑ์พัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวด ๒ การวางแผนเชิงยุทธศาสตร์ SP ๗ ที่ต้องมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์ประเมิน และจัดการความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงมาตรฐาน COSO คือ

**ขั้นตอนที่ ๑** การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
**ขั้นตอนที่ ๒** การระบุความเสี่ยง (Event Identification)
**ขั้นตอนที่ ๓** การประเมินความเสี่ยง (Risk Assessment)
**ขั้นตอนที่ ๔** กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
**ขั้นตอนที่ ๕** กิจกรรมการบริหารความเสี่ยง (Control Activity)
**ขั้นตอนที่ ๖** ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
**ขั้นตอนที่ ๗** การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

ทั้งนี้ การคิดวิเคราะห์เพื่อระบุความเสี่ยงต่างๆ อาจพิจารณาจากปัจจัยในหลายๆ ด้าน เช่น

**ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S)** เกี่ยวข้องกับการบรรลุเป้าหมายและพันธกิจภาพรวม โดยความเสี่ยงที่อาจจะเกิดขึ้นเป็นความเสี่ยง เนื่องจากการเปลี่ยนแปลงของสถานการณ์และเหตุการณ์ภายนอก ส่งผลต่อกลยุทธ์ที่กำหนดไว้ไม่สอดคล้อง กับประเด็นยุทธศาสตร์/วิสัยทัศน์ หรือเกิดจากการกำหนดกลยุทธ์ที่ขาดการมีส่วนร่วมจากภาคประชาชนหรือการร่วมมือกับองค์กรอิสระ ทำให้โครงการขาดการยอมรับและโครงการไม่ได้นำไปสู่การแก้ไขปัญหาหรือการตอบสนองต่อความต้องการของผู้รับบริการหรือผู้มีส่วนได้เสียอย่างแท้จริง หรือเป็นความเสี่ยงที่เกิดขึ้นจากการตัดสินใจผิดพลาดหรือนำการตัดสินใจนั้นมาใช้อย่างไม่ถูกต้อง

**ความเสี่ยงด้านการดำเนินงาน (Operational Risk: O)** เกี่ยวข้องกับประสิทธิภาพ ประสิทธิผล หรือผลการปฏิบัติงาน โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยงเนื่องจากระบบงานภายในขององค์กร/กระบวนการ เทคโนโลยี หรือนวัตกรรมที่ใช้/บุคลากร/ความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพ ประสิทธิผลในการดำเนินโครงการ

**ความเสี่ยงด้านการเงิน (Financial Risk: F)** เป็นความเสี่ยงเกี่ยวกับการบริหารงบประมาณ และการเงิน เช่น การบริหารการเงินที่ไม่ถูกต้อง ไม่เหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันต่อสถานการณ์ หรือเป็นความเสี่ยงที่เกี่ยวข้องกับการเงินขององค์การ เช่นการประมาณการงบประมาณไม่เพียงพอ และไม่สอดคล้องกับขั้นตอนการดำเนินการ เป็นต้น เนื่องจากขาดการจัดหาข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารงบประมาณ และการเงินดังกล่าว

**ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ (Compliance Risk: C)** เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบต่างๆ โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยงเนื่องจากความไม่ชัดเจน ความไม่ทันสมัยหรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับต่างๆ รวมถึงการทำนิติกรรมสัญญา การร่างสัญญาที่ไม่ครอบคลุมการดำเนินงาน

ในการวิเคราะห์ความเสี่ยง นอกจากส่วนราชการจะพิจารณาปัจจัยเสี่ยงจากด้านต่างๆ แล้ว ต้องนำแนวคิดเรื่องธรรมาภิบาลที่เกี่ยวข้องในแต่ละด้านมาเป็นปัจจัยในการวิเคราะห์ความเสี่ยง เช่น

- **ด้านยุทธศาสตร์** โครงการที่คัดเลือกมานั้นอาจมีความเสี่ยงต่อเรื่อง ประสิทธิผลและการมีส่วนร่วม
- **ด้านการดำเนินการ** อาจมีความเสี่ยงต่อเรื่องประสิทธิภาพและความโปร่งใส
- **ด้านการเงิน** อาจมีความเสี่ยงต่อเรื่องนิติธรรมและภาระรับผิดชอบ
- **ด้านกฎระเบียบ** อาจมีความเสี่ยงต่อเรื่องนิติธรรมและความเสมอภาค

ความเสี่ยงเรื่องธรรมาภิบาลที่อาจเกิดขึ้นจากการดำเนินแผนงาน/โครงการ เพื่อให้เป็นไปตามหลักธรรมาภิบาล (Good Governance) ได้แก่

๑. ประสิทธิผล (Effectiveness)
๒. ประสิทธิภาพ (Efficiency)
๓. การมีส่วนร่วม (Participation)
๔. ความโปร่งใส (Transparency)

๕. การตอบสนอง (Responsiveness)
๖. ภาระรับผิดชอบ (Accountability)
๗. นิติธรรม (Rule of Law)
๘. การกระจายอำนาจ (Decentralization)
๙. ความเสมอภาค (Equity)
๑๐. การมุ่งเน้นฉันทามติ (Consensus Oriented)

เมื่อวิเคราะห์ความเสี่ยงแล้ว ส่วนราชการอาจจัดทำแผนบริหารความเสี่ยงจำแนกตามโครงการ หรือบางกิจกรรมที่สามารถบูรณาการในการดำเนินการได้ ก็สามารถนำมารวมเป็นแผนบริหารความเสี่ยงเดียวกันได้ ทั้งนี้ แผนบริหารความเสี่ยงต้องสอดคล้องกับผลการวิเคราะห์ความเสี่ยงดังกล่าวข้างต้น และมีการกำหนดตัวชี้วัดความสำเร็จของเป้าหมายของแผนอย่างชัดเจน รวมทั้งเกณฑ์การให้คะแนนของค่าเป้าหมายตัวชี้วัด

ในการบริหารความเสี่ยงด้านสารสนเทศ ได้จากการศึกษา วิเคราะห์ รวบรวม ข้อมูลสถานการณ์สภาพแวดล้อมของการเพิ่มขีดความสามารถในการสร้างความเชื่อมั่นในการเข้าถึงข้อมูลด้านระบบบริการสุขภาพตามแนวทางการประเมินระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ ใน ๑๔ ประเด็น ตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC ๒๗๐๐๑ : ๒๐๑๓) รวมทั้งกฎหมายที่เกี่ยวข้องและมาตรฐานสากล เช่น NIST (National Institute of Standard and Technology) GDPR (General Data Protection Regulation) ดังนี้

๑.๑ นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policies)
๑.๒ โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Security)
๑.๓ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบุคลากร (Human Resources Security)
๑.๔ การบริหารจัดการทรัพย์สินขององค์กร (asset Management)
๑.๕ การควบคุมการเข้าถึง (Access Control)
๑.๖ การเข้ารหัสข้อมูล (Cryptography)
๑.๗ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
๑.๘ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านการดำเนินการ (Operation Security)
๑.๙ ความมั่นคงปลอดภัยด้านการสื่อสาร (Communication Security)
๑.๑๐ การจัดหา การพัฒนาและการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)
๑.๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)
๑.๑๒ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)
๑.๑๓ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)
๑.๑๔ การปฏิบัติตามข้อกำหนด (Compliance)

**๑.๓ วัตถุประสงค์**

๑. ผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ มีความรู้ความเข้าใจเรื่องการบริหารความเสี่ยงด้านสารสนเทศ เพื่อนำไปใช้ในการดำเนินงานตามยุทธศาสตร์ และแผนปฏิบัติราชการ ให้บรรลุตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒. ผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ สามารถระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยง และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๓. สามารถนำแผนบริหารความเสี่ยงด้านสารสนเทศไปใช้ในการบริหารงานที่รับผิดชอบ

๔. เพื่อพัฒนาความสามารถของบุคลากรด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ และกระบวนการภายในองค์กรอย่างต่อเนื่อง

๕. ความรับผิดชอบต่อความเสี่ยงและการบริหารความเสี่ยงถูกกำหนดขึ้นอย่างเหมาะสมในการบริหารความเสี่ยง ได้รับการปลูกฝังให้เป็นวัฒนธรรมองค์กร

**๑.๔ ประโยชน์ของการบริหารความเสี่ยงด้านสารสนเทศ**

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น และทำให้หน่วยงานสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้หน่วยงานเกิดความเสียหาย ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

**๑. เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี** การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและควบคุมภายในทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลหน่วยงานได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

**๒. สร้างฐานข้อมูลความรู้ที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในหน่วยงาน** การบริหารความเสี่ยงจะเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ ซึ่งรวมถึงการบริหารความเสี่ยงและตั้งอยู่บนสมมติฐานในการตอบสนองต่อเป้าหมายและภารกิจหลักของหน่วยงาน รวมถึงระดับความเสี่ยงที่ยอมรับได้

**๓. ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด** การบริหารความเสี่ยงจะทำให้บุคลากรภายในหน่วยงานมีความเข้าใจถึงเป้าหมายและภารกิจหลักของหน่วยงาน รวมทั้งตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อหน่วยงานได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงที่มีเหตุทั้งจากปัจจัยภายในหน่วยงาน (เช่น วัฒนธรรม โครงสร้างองค์กร และบุคลากร เป็นต้น) และจากปัจจัยภายนอกหน่วยงาน (เช่น การเมือง สภาวะเศรษฐกิจ และระบบเทคโนโลยีสารสนเทศ เป็นต้น)

**๔. เป็นเครื่องมือที่สำคัญในการบริหารงาน** การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของหน่วยงานเป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่หน่วยงาน

**๕. ช่วยให้การพัฒนาหน่วยงานเป็นไปในทิศทางเดียวกัน** การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานของหน่วยงานมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์ วัตถุประสงค์ของหน่วยงาน และระดับความเสี่ยงอย่างชัดเจน

**๖. ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล** การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูงย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

# บทที่ ๒

## กระบวนการบริหารความเสี่ยงด้านสารสนเทศ

**๒.๑ ความหมายและคำจำกัดความของการบริหารความเสี่ยง**

การนำกระบวนการบริหารความเสี่ยงมาใช้ในองค์กร จะเป็นหลักประกันในระดับหนึ่งว่าการดำเนินงานต่างๆ จะบรรลุเป้าหมายที่วางไว้ เนื่องจากการบริหารความเสี่ยงเป็นการทำนายอนาคตอย่างมีเหตุมีผล มีหลักการและหาทางลดหรือป้องกันความเสียหายในการทำงานแต่ละขั้นตอนไว้ล่วงหน้า หรือในกรณีที่พบกับเหตุการณ์ที่ไม่คาดคิดโอกาสที่จะประสบกับปัญหาน้อยกว่าองค์กรอื่น หรือหากเกิดความเสียหายขึ้นก็จะเป็นความเสียหายที่น้อยกว่าองค์กรที่ไม่มีการนำกระบวนการบริหารความเสี่ยงมาใช้เพราะได้มีการเตรียมการไว้ล่วงหน้า ในขณะที่องค์กรอื่นไม่เคยมีการเตรียมการหรือไม่มีการนำแนวคิดของกระบวนการบริหารความเสี่ยงมาใช้ เมื่อเกิดสถานการณ์วิกฤตขึ้นองค์กรเหล่านั้นจะประสบกับปัญหาและความเสียหายที่ตามมาโดยยากที่จะแก้ไข ดังนั้นการนำกระบวนการบริหารความเสี่ยงมาช่วยเสริมร่วมกับการทำงานจะช่วยให้ภาระงานที่ปฏิบัติการอยู่เป็นไปตามเป้าหมายที่กำหนดไว้ และป้องกันโอกาสที่จะเกิดความเสี่ยงและปัญหาที่จะเป็นอุปสรรคต่อการดำเนินงาน การบริหารความเสี่ยงเป็นส่วนหนึ่งของการบริหารจัดการองค์กร เป็นเรื่องส่วนรวมที่ทุกคนในองค์กรต้องเกี่ยวข้อง ตั้งแต่คณะกรรมการ ผู้บริหารระดับสูง จนถึงบุคลากรทุกคนที่ต้องพิจารณาวิเคราะห์ในเชิงลึก เชิงบูรณาการ และเชื่อมโยงกับการกำหนดกลยุทธ์ นโยบาย แผนงาน แผนปฏิบัติการ กิจกรรมขององค์กร ซึ่งการบริหารความเสี่ยงที่ดีจะเป็นการวัดความสามารถและการดำเนินงานของบุคลากรภายในองค์กร องค์กรที่มีการบริหารจัดการที่ดี จะมีการดำเนินงานบนพื้นฐานของ ๓ องค์ประกอบที่สำคัญ คือ ๑) การตรวจสอบภายใน (Internal Audit) ๒) การควบคุมภายใน (Internal Control) และ ๓) การบริหารความเสี่ยง (Risk Management) ซึ่งสอดคล้องกับหลักการบริหารกิจการบ้านเมืองที่ดี

การบริหารความเสี่ยง คือ กระบวนการที่เป็นระบบในการบริหารปัจจัย และควบคุมกิจกรรมรวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อลดมูลเหตุของโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินการที่ไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่ยอมรับได้ ควบคุมได้ ตรวจสอบได้อย่างเป็นระบบ

ความเสี่ยง คือ เหตุการณ์/การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และส่งผลกระทบ หรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายของแผนงาน/โครงการที่สำคัญในแต่ละประเด็นยุทธศาสตร์ตามที่ระบุไว้ในแผนปฏิบัติราชการของส่วนราชการ

ดังนั้น จึงสรุปได้ว่าความเสี่ยง คือ โอกาสที่เหตุการณ์บางอย่างอาจเกิดขึ้น และมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร

ระดับของความเสี่ยงที่สูงหรือต่ำ สามารถวัดได้จากผลที่ตามมา (Consequence) และโอกาสที่เหตุการณ์ๆ หนึ่งจะเกิดขึ้น (Likelihood)

ผลกระทบ (Consequence) คือ ผลลัพธ์หรือผลกระทบจากเหตุการณ์ๆ หนึ่ง เป็นไปได้ทั้งในทางบวกหรือลบ

การนำระบบบริหารความเสี่ยงมาใช้ ต้องแสดงให้เห็นในเชิงระบบว่าเรามีระบบการวิเคราะห์อย่างไร เป็นแผนงานอย่างไร มีการติดตามอย่างไร และทบทวนปรับปรุงอย่างไร หรือครบถ้วนทั้ง PDCA (Plan –Do-Check-Act) ควรเพิ่มเติมการควบคุม กำกับ (Control)

**๒.๒ กรอบการบริหารความเสี่ยงตามแนวทาง COSO**

การบริหารความเสี่ยงตามแนวทางหรือมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) ใช้หลักการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) คือ กระบวนการที่ได้รับอิทธิพลมาจากคณะกรรมการของกรมสนับสนุนบริการสุขภาพ ผู้บริหาร และบุคลากร เป็นกระบวนการที่จะถูกนำมาเพื่อให้สามารถระบุเหตุการณ์อันอาจเกิดขึ้นและส่งผลกระทบต่อองค์กร เพื่อจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk appetite) การบริหารความเสี่ยงขององค์กรจะทำให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

**ประโยชน์ของ Enterprise Risk Management : ERM**

๑. จัดให้กลยุทธ์ต่างๆ เข้ากันได้กับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

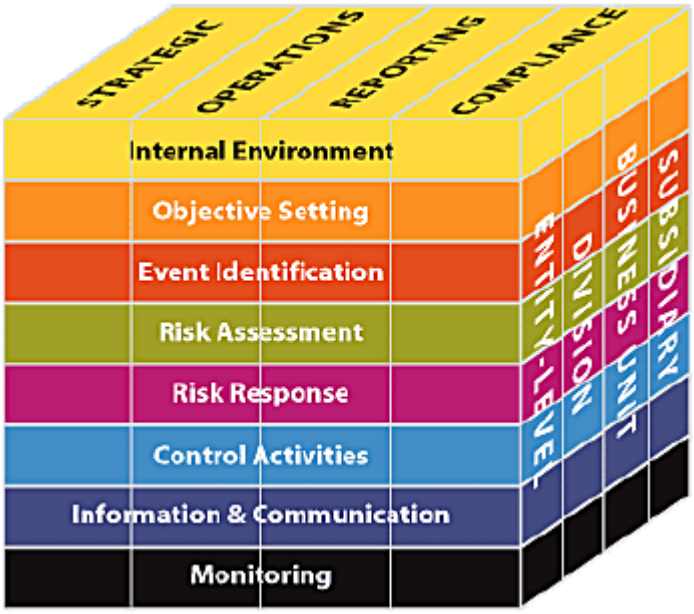
๒. ช่วยให้การตัดสินใจในเรื่องการโต้ตอบกับความเสี่ยงทำได้ดีขึ้น

๓. ลดสิ่งที่ไม่คาดฝันและความสูญเสียที่จะเกิดในการดำเนินงาน

๔. ทำให้การระบุและจัดการความเสี่ยงที่ต่อเนื่อง กันหรือคาบเกี่ยวอย่างทั่วถึงทุกระดับ

๕. การมองถึงเหตุการณ์ในอนาคตที่อาจเกิดขึ้นได้ ทำให้อาจมองเห็นโอกาส และฉวยโอกาสนั้นอย่างเชิงรุกได้

๖. การบริหารและใช้ทรัพยากรได้อย่างเหมาะสม มีประสิทธิภาพและประสิทธิผล




**วัตถุประสงค์ของ Enterprise Risk Management : ERM**

๑. ด้านกลยุทธ์ (Strategic) : เกี่ยวกับการกำหนดเป้าหมายในระดับสูง ซึ่งต้องเป็นแนวทางเดียวกัน และต้องสนับสนุนวัตถุประสงค์ขององค์กร

๒. ด้านการปฏิบัติการ (Operations) : มีการใช้ทรัพยากรขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล

๓. ด้านการรายงาน (Reporting) : การรายงาน (รายงานด้านการเงิน และไม่ใช่ด้านการเงิน) ขององค์กรมีความน่าเชื่อถือ

๔. ด้านการปฏิบัติตามข้อกำหนด (Compliance) : องค์กรได้ปฏิบัติตามข้อกำหนด หรือกฎหมาย ระเบียบต่างๆ ที่ใช้องค์กร

**องค์ประกอบหลักของ ERM**

๑. สภาพแวดล้อมภายในองค์กร (Internal Environment)

- ปรัชญาการบริหารความเสี่ยง
- ระดับความเสี่ยงที่องค์กรยอมรับได้
- ค่านิยมขององค์กร (ความซื่อตรง จริยธรรม)
- คณะกรรมการ
- โครงสร้างองค์กร
- อำนาจหน้าที่และความรับผิดชอบ
- มาตรฐานทรัพยากรบุคคล (หลักเกณฑ์ด้านความรู้ความสามารถของผู้ที่เกี่ยวข้อง)
- การให้ความสำคัญกับการเสริมสร้างขีดความสามารถ (การอบรมพัฒนาบุคลากรมีอะไรบ้าง)

๒. การกำหนดวัตถุประสงค์ (Objective Setting)
   - องค์กรต้องกำหนดวัตถุประสงค์/เป้าหมายการดำเนินงานก่อนที่จะระบุเหตุการณ์ที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์/เป้าหมายนั้นๆ
   - วัตถุประสงค์ต้องสอดคล้องกับการยอมรับในความเสี่ยง (Risk Appetites)

๓. การระบุเหตุการณ์ (Event Identification)
   - การระบุเหตุการณ์ทั้งภายในภายนอกองค์กร รวมทั้งที่องค์กรควบคุมได้และควบคุมไม่ได้ ที่อาจเกิดขึ้นแล้วส่งผลกระทบต่อการบรรลุวัตถุประสงค์ โดยจะต้องแยกแยะให้ออกระหว่างความเสี่ยงกับโอกาส
   - หากมีโอกาสจะต้องสื่อสารกลับไปยังฝ่ายที่จัดการ เพื่อกำหนดวัตถุประสงค์และกลยุทธ์

๔. การประเมินความเสี่ยง (Risk Assessment)
   - การวิเคราะห์ระดับความเสี่ยงจะพิจารณาถึงโอกาส (Likelihood) และผลกระทบ (Impact) ที่จะเกิด เพื่อเป็นพื้นฐานในการที่จะจัดการกับความเสี่ยงนั้นๆ
   - การประเมินความเสี่ยงจะประเมินอยู่บนพื้นฐานของ Inherent risk และ Residual risk

๕. กลยุทธ์ที่ใช้ในการจัดการความเสี่ยง (Risk Response)
   - การยอมรับความเสี่ยง (Task) หากทำการวิเคราะห์แล้วเห็นว่าไม่มีวิธีการจัดการความเสี่ยงใดเลยที่เหมาะสม เนื่องจากต้นทุนการจัดการความเสี่ยงสูงกว่าประโยชน์ที่จะได้รับอาจต้องยอมรับความเสี่ยง แต่ควรมีมาตรการติดตามอย่างใกล้ชิดเพื่อรองรับผลที่จะเกิดขึ้น
   - การลด/ควบคุมความเสี่ยง (Treat) พยายามลดความเสี่ยงโดยการเพิ่มเติม หรือเปลี่ยนแปลงขั้นตอนบางส่วนของกิจกรรมหรือโครงการที่นำไปสู่เหตุการณ์ที่เป็นความเสี่ยง รวมถึงลดความน่าจะเป็นที่เหตุการณ์ที่เป็นความเสี่ยงที่จะเกิดขึ้น
   - การถ่ายโอน/กระจายความเสี่ยง (Transfer ) ยกภาระในการเผชิญหน้ากับเหตุการณ์ และการจัดการกับความเสี่ยงให้ผู้อื่น
   - การหลีกเลี่ยงความเสี่ยง (Terminate) ปฏิเสธและหลีกเลี่ยงโอกาสที่จะเกิดความเสี่ยง โดยการหยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรมหรือโครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง

๖. กิจกรรมการควบคุม (Control Activities)
   เป็นนโยบายและวิธีการต่างๆ ที่กำหนดขึ้นและนำไปปฏิบัติ เพื่อช่วยก่อให้เกิดความเชื่อมั่นได้ว่า ได้มีการดำเนินการกับความเสี่ยงได้อย่างเหมาะสม ซึ่งกิจกรรมการควบคุมสามารถจัดกลุ่มได้ตามลักษณะของวัตถุประสงค์ขององค์กร ทั้งวัตถุประสงค์ด้านกลยุทธ์ ด้านการปฏิบัติงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎระเบียบ

๗. สารสนเทศและการสื่อสาร (information and Communication)
   ต้องระบุสารสนเทศที่จำเป็น รับทราบได้ และสื่อสารไปยังบุคลากรในองค์กรในรูปแบบ และช่วงเวลาที่เหมาะสมเพื่อให้บุคคลกรปฏิบัติหน้าที่ของตนได้

๘. การติดตามประเมินผล (Monitoring)
   มีการติดตามประเมินผลการบริหารความเสี่ยงแบบครบวงจร และมีการปรับแก้ตามความเหมาะสมซึ่งการประเมินอาจทำได้ทั้งขณะดำเนินงานอยู่ (Ongoing Monitoring Activities) หรือการประเมินแยกต่างหาก (Separate Evaluations) หรือทั้ง ๒ แบบ

**กระบวนการในการบริหารความเสี่ยง**

ขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์ ประเมิน และการจัดการความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (The Committee of Sponsoring Organizations of the Tread way Commission) มี ๗ ขั้นตอน ดังนี้

**ขั้นตอนที่ ๑** การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
**ขั้นตอนที่ ๒** การระบุความเสี่ยง (Event Identification)
**ขั้นตอนที่ ๓** การประเมินความเสี่ยง (Risk Assessment)
**ขั้นตอนที่ ๔** กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
**ขั้นตอนที่ ๕** กิจกรรมการบริหารความเสี่ยง (Control Activity)
**ขั้นตอนที่ ๖** ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
**ขั้นตอนที่ ๗** การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

**ขั้นตอนที่ ๑** การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

การกำหนดวัตถุประสงค์การดำเนินการบริหารความเสี่ยง เป็นการกำหนดเป้าหมายการบริหารความเสี่ยง โดยมีการกำหนดหลักเกณฑ์การพิจารณาคัดเลือกโครงการ และการวิเคราะห์รายละเอียดโครงการ ทั้งนี้ การกำหนดวัตถุประสงค์การบริหารความเสี่ยงขึ้นนั้น เพื่อต้องการให้โครงการสำคัญที่มีนัยสำคัญต่อการบรรลุความสำเร็จตามประเด็นยุทธศาสตร์สามารถดำเนินการได้บรรลุเป้าหมายตามที่ตั้งไว้ ซึ่งจะส่งผลให้บรรลุความสำเร็จตามกลยุทธ์ เป้าประสงค์ของประเด็นยุทธศาสตร์

ทั้งนี้ การกำหนดวัตถุประสงค์ของการบริหารความเสี่ยง กำหนดจาก

๑. วิสัยทัศน์และภารกิจขององค์กร
๒. จากเป้าหมายหลักองค์กรให้สอดคล้องกับภารกิจ
๓. เป้าหมายในระดับหน่วยงาน
๔. เป้าหมายของแผนงานโครงการและกิจกรรมที่ทำให้บรรลุเป้าหมายในระดับองค์กร

นอกจากนี้ วัตถุประสงค์ที่จะ SMART ควรจะ

๑. **Specific** (เฉพาะเจาะจง) มีความชัดเจนและกำหนดผลตอบแทน หรือผลลัพธ์ที่ต้องการที่ทุกคนสามารถเข้าใจได้อย่างชัดเจน
๒. **Measurable** (สามารถวัดได้) สามารถวัดผลการบรรลุวัตถุประสงค์ได้
๓. **Achievable** (สามารถบรรลุผลได้) มีความเป็นไปได้ที่จะบรรลุวัตถุประสงค์ภายใต้เงื่อนไขการใช้ทรัพยากรที่มีอยู่ในปัจจุบัน
๔. **Relevant** (มีความเกี่ยวข้อง) มีความสอดคล้องกับกลยุทธ์และเป้าหมายในการดำเนินงานขององค์กร
๕. **Timeless** (มีกำหนดเวลา) สามารถกำหนดระยะเวลาที่ต้องการบรรลุผล

**ขั้นตอนที่ ๒** การระบุความเสี่ยง (Event Identification)

วิธีการระบุความเสี่ยง (Risk Identification) พิจารณาจากข้อมูลภายใน ได้แก่ ความถี่ และความรุนแรงของความสูญเสียในอดีต และการดำเนินงานที่ผ่านมา รวมทั้งการพิจารณาจากข้อมูลภายนอก ได้แก่ ความสูญเสียขององค์การอื่นที่คล้ายคลึงกัน เศรษฐกิจ หรือการเมือง ฯลฯ

**ประเภทความเสี่ยง** มีดังนี้

**ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S)** เกี่ยวข้องกับการบรรลุเป้าหมาย และพันธกิจในภาพรวม โดยความเสี่ยงที่อาจจะเกิดขึ้นเป็นความเสี่ยงเนื่องจาก ๑) การเปลี่ยนแปลงสถานการณ์และเหตุการณ์ภายนอก ส่งผลต่อกลยุทธ์ที่กำหนดไว้ไม่สอดคล้องกับประเด็นยุทธศาสตร์ วิสัยทัศน์ หรือเกิดจาก ๒) การกำหนดกลยุทธ์ที่ขาดการมีส่วนร่วมจากภาคประชาชน หรือการร่วมมือกับองค์กรอิสระ ทำให้โครงการขาดการยอมรับและโครงการไม่ได้นำไปสู่การแก้ไขปัญหา หรือการตอบสนองต่อความต้องการของผู้รับบริการ หรือผู้มีส่วนได้ส่วนเสียอย่างแท้จริง หรือ ๓) เป็นความเสี่ยงที่เกิดขึ้นจากการตัดสินใจผิดพลาด หรือการนำการตัดสินใจมาใช้ไม่ถูกต้อง

**ความเสี่ยงด้านการดำเนินการ (Operational Risk : O)** เกี่ยวข้องกับประสิทธิภาพ ประสิทธิผล หรือผลการปฏิบัติงานโดยความเสี่ยงที่เกิดขึ้นเป็นความเสี่ยงเนื่องจากระบบงานภายในองค์กร/กระบวนการ/เทคโนโลยี หรือนวัตกรรมที่ใช้/บุคลากร/ความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินโครงการ

**ความเสี่ยงด้านการเงิน (Financial Risk : F)** เป็นความเสี่ยงเกี่ยวกับการบริหารงบประมาณและการเงิน เช่น การบริหารการเงินไม่ถูกต้อง ไม่เหมาะสม ทำให้ขาดประสิทธิภาพและไม่ทันต่อสถานการณ์ หรือเป็นความเสี่ยงที่เกี่ยวข้องกับการเงินขององค์การ เช่น การประมาณการงบประมาณไม่เพียงพอ และไม่สอดคล้องกับขั้นตอนการดำเนินงาน เป็นต้น เนื่องจากขาดการจัดหาข้อมูล การวิเคราะห์ การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารงบประมาณและการเงิน

**ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ (Compliance Risk : C)** เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบต่างๆ โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยง เนื่องจากความไม่ชัดเจน ความไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับต่างๆ รวมทั้งนิติกรรมต่างๆ รวมทั้งการทำนิติกรรมสัญญา การร่างสัญญาไม่ครอบคลุมการดำเนินงาน

การระบุกิจกรรมของโครงการ และระบุความเสี่ยงตามหลักธรรมาภิบาล ทั้ง ๑๐ องค์ประกอบ ประกอบด้วย

**๑. หลักประสิทธิผล (Effectiveness)** ต้องมีวิสัยทัศน์เชิงยุทธศาสตร์ เพื่อตอบสนองความต้องการของประชาชนและผู้มีส่วนได้ส่วนเสียทุกฝ่าย ปฏิบัติหน้าที่ตามพันธกิจให้บรรลุวัตถุประสงค์ขององค์การ มีการวางเป้าหมายการปฏิบัติงานที่ชัดเจน และอยู่ในระดับที่ตอบสนองต่อความคาดหวังของประชาชน สร้างกระบวนการปฏิบัติงานอย่างเป็นระบบและมีมาตรฐาน มีการจัดการความเสี่ยงและมุ่งเน้นผลการปฏิบัติงานที่เป็นเลิศ รวมถึงมีการติดตามประเมินผล และพัฒนาปรับปรุงการปฏิบัติงานให้ดีขึ้นอย่างต่อเนื่อง

**๒. หลักประสิทธิภาพ (Efficiency)** ในการปฏิบัติงานต้องมีการใช้ทรัพยากรอย่างประหยัด เกิดประสิทธิภาพ คุ้มค่าการลงทุน และบังเกิดประโยชน์สูงสุดต่อส่วนรวม รวมทั้งต้องมีการลดขั้นตอนและระยะเวลาในการปฏิบัติงาน เพื่ออำนวยความสะดวกและลดภาระค่าใช้จ่าย ตลอดจนยกเลิกภารกิจที่ล้าสมัยไม่มีความจำเป็น

**๓. หลักการมีส่วนร่วม (Participation)** ต้องรับฟังความคิดเห็นของประชาชน รวมทั้งเปิดให้ประชาชนมีส่วนร่วมในการรับรู้ เรียนรู้ ทำความเข้าใจ ร่วมแสดงทัศนะ ร่วมเสนอปัญหา/ประเด็นสำคัญที่เกี่ยวข้อง ร่วมคิดแก้ไขปัญหา ร่วมกระบวนการตัดสินใจและการดำเนินงาน ร่วมตรวจสอบผลการปฏิบัติงาน

**๔. หลักความโปร่งใส (Transparency)** ต้องปฏิบัติงานด้วยความซื่อสัตย์สุจริตตรงไปตรงมา รวมทั้งต้องมีการเปิดเผยข้อมูลข่าวสารที่จำเป็นและเชื่อถือได้ให้ประชาชนได้รับทราบสม่ำเสมอ ตลอดจนวางระบบให้การเข้าถึงข้อมูลข่าวสารเป็นไปโดยง่าย

**๕. หลักการตอบสนอง (Responsiveness)** ต้องสามารถให้บริการได้อย่างมีคุณภาพสามารถดำเนินการแล้วเสร็จภายในระยะเวลาที่กำหนด สร้างความเชื่อมั่นไว้วางใจ รวมถึงตอบสนองความคาดหวัง/ความต้องการของประชาชนผู้รับบริการ และผู้มีส่วนได้ส่วนเสียที่มีความหลากหลาย และมีความแตกต่างกันได้อย่างเหมาะสม

**๖. หลักภาระรับผิดชอบ (Accountability)** ในการปฏิบัติงานต้องสามารถตอบคำถามและชี้แจงได้เมื่อมีข้อสงสัย รวมทั้งต้องมีการวางระบบการรายงานความก้าวหน้าและผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ต่อสาธารณะเพื่อประโยชน์ในการตรวจสอบและการให้คุณให้โทษ ตลอดจนการจัดเตรียมระบบการแก้ไขหรือบรรเทาปัญหา และผลกระทบใดๆ ที่อาจจะเกิดขึ้น

**๗. หลักนิติธรรม (Rule of Law)** ต้องใช้อำนาจของกฎหมาย กฎระเบียบ ข้อบังคับในการปฏิบัติงานอย่างเคร่งครัดด้วยความเป็นธรรม ไม่เลือกปฏิบัติ และคำนึงถึงสิทธิเสรีภาพของผู้มีส่วนได้ส่วนเสียฝ่ายต่างๆ

**๘. หลักการกระจายอำนาจ (Decentralization)** ในการปฏิบัติงานควรมีการมอบอำนาจและกระจายอำนาจความรับผิดชอบในการตัดสินใจ และการดำเนินการให้แก่ผู้ปฏิบัติงานในระดับต่างๆ ได้อย่างเหมาะสม รวมทั้งมีการโอนถ่ายบทบาทและภารกิจให้แก่องค์กรปกครองส่วนท้องถิ่น หรือภาคส่วนอื่นๆ ในสังคม

**๙. การมุ่งฉันทามติ (Consensus Oriented)** ในการปฏิบัติงานต้องมีกระบวนการในการแสวงหาฉันทามติ หรือข้อตกลงร่วมกันระหว่างกลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง โดยเฉพาะกลุ่มที่ได้รับผลกระทบโดยตรง จะต้องไม่มีข้อคัดค้านที่หาข้อยุติไม่ได้ในประเด็นที่สำคัญ

**ขั้นตอนที่ ๓** การประเมินความเสี่ยง (Risk Assessment)

โอกาสที่จะเกิดความเสียหายต่อองค์กร คือ การพิจารณาปัจจัยเสี่ยงแต่ละปัจจัยว่ามีโอกาสที่จะเกิดขึ้นในระดับมากน้อยเพียงใด

ความเสียหายที่จะกระทบต่อองค์กร คือ การพิจารณาปัจจัยเสี่ยงแต่ละปัจจัยว่าหากเกิดขึ้นแล้วมีผลกระทบต่อหน่วยงานมากน้อยแค่ไหน

ความสำคัญของความเสี่ยงที่องค์กรเผชิญอยู่ คือ การลำดับความสำคัญของแต่ละปัจจัยเสี่ยง เพื่อพิจารณาว่าความเสี่ยงใดควรพิจารณาจัดการก่อนหลัง

การประเมินความเสี่ยงประกอบด้วย

๑) มีการกำหนดหลักเกณฑ์การประเมินความเสี่ยง (ความรุนแรง × โอกาส)
๒) ประเมินความเสี่ยงตามหลักเกณฑ์ความรุนแรงและโอกาส
๓) กำหนดกลยุทธ์ที่ใช้ในการจัดการความเสี่ยงและแนวทางการจัดการความเสี่ยง
๔) การจัดทำแผนภูมิความเสี่ยง เพื่อช่วยให้สามารถตัดสินใจในการวางแผนบริหารความเสี่ยงได้อย่างเหมาะสม และสามารถเห็นภาพว่าเมื่อรวมทุกปัจจัยเสี่ยงแล้ว ปัจจัยเสี่ยงใดควรได้รับการจัดการก่อนหลัง

โอกาสที่จะเกิดความเสียหายต่อองค์กร และความเสียหายที่จะกระทบต่อองค์กรพิจารณาได้ ๒ ลักษณะ คือ

๑. วิธีการประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Approach) ซึ่งจะไม่มีการระบุค่าของความเสียหายออกมาเป็นตัวเลข แต่ระบุออกเป็นระดับความรุนแรงของความเสียหาย และระดับของความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น

๒. วิธีการประเมินความเสี่ยงเชิงปริมาณ (Quantitative Approach) ซึ่งจะต้องระบุค่าของความเสียหายออกมาเป็นตัวเลข (โดยเฉพาะเป็นตัวเงิน) และโอกาสที่เหตุการณ์นั้นจะเกิดออกมาในรูปของความน่าจะเป็น (Probability)

**กำหนดหลักเกณฑ์การประเมินความเสี่ยง (ความรุนแรง)**

| ประเด็น/องค์ประกอบที่พิจารณา | ๑ = น้อยมาก | ๒ = น้อย | ๓ = ปานกลาง | ๔ = สูง | ๕ = สูงมาก |
|---|---|---|---|---|---|
| **ความรุนแรงของผลกระทบ (X)** | | | | | |
| มูลค่าความเสียหาย (X ๑) | < ๑ หมื่นบาท | ๑-๕ หมื่นบาท | ๕ หมื่น – ๒.๕ แสนบาท | ๒.๕ – ๕ แสนบาท | > ๕ แสนบาท |
| ความพึงพอใจของผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย (X ๒) | ๑๐๐-๘๐ % | ๘๐-๖๐ % | ๖๐-๔๐ % | ๔๐-๒๐ % | > ๒๐ % |
| จำนวนผู้รับบริการที่ได้รับความเสียหาย/จำนวนผู้มีส่วนได้ส่วนเสียที่ได้รับผลกระทบ (X ๓) | กระทบเฉพาะผู้เกี่ยวข้องโดยตรงบางราย | กระทบเฉพาะกลุ่มผู้ที่เกี่ยวข้องโดยตรงเป็นส่วนใหญ่ | กระทบเฉพาะกลุ่มที่เกี่ยวข้องโดยตรงทั้งหมด | กระทบเฉพาะกลุ่มผู้ที่เกี่ยวข้องโดยตรงทั้งหมดและผู้อื่นบางส่วน | กระทบเฉพาะกลุ่มผู้ที่เกี่ยวข้องโดยตรงทั้งหมดและผู้อื่นมาก |
| จำนวนผู้ร้องเรียน (ต่อระยะเวลาโครงการ) (X ๔) | น้อยกว่า ๑ ราย | ๑-๕ ราย | ๖-๑๐ ราย | ๑๑-๑๕ ราย | มากกว่า ๑๕ ราย |
| **ความรุนแรงของผลกระทบ (X)** | | | | | |
| ความล่าช้าในการดำเนินโครงการ (X๕) | น้อยกว่า ๑ สัปดาห์ | ๑-๒ สัปดาห์ | ๐.๕-๑ เดือน | ๑-๒ เดือน | ๒ เดือน ขึ้นไป |

| ประเด็น/องค์ประกอบที่พิจารณา | ๑ = น้อยมาก | ๒ = น้อย | ๓ = ปานกลาง | ๔ = สูง | ๕ = สูงมาก |
|---|---|---|---|---|---|
| **โอกาสที่จะเกิดความเสียหาย (Y)** | | | | | |
| ระเบียบและคู่มือปฏิบัติ (Y ๑) | มีทั้ง ๒ อย่าง และมีการปฏิบัติตาม | มีอย่างใดอย่างหนึ่งและมีการปฏิบัติตาม | มีทั้ง ๒ อย่าง แต่ปฏิบัติตามอย่างใดอย่างหนึ่งหรือไม่ถือปฏิบัติ | มีอย่างใดอย่างหนึ่งแต่ไม่ถือปฏิบัติ | ไม่มีทั้ง ๒ อย่าง |
| การควบคุม ติดตาม และตรวจสอบของผู้บังคับบัญชา หรือหน่วยงานอื่น (Y ๒) | ทุกสัปดาห์ | ทุก ๒ สัปดาห์ | ทุก ๑ เดือน | ทุก ๓ เดือน | ทุก ๖ เดือน |
| การอบรม/สอนงาน/ทบทวนการปฏิบัติงาน (Y ๓) | ทุกเดือน | ทุก ๓ เดือน | ทุก ๖ เดือน | ทุก ๑ ปี | มากกว่า ๑ ปี |
| ความถี่ในการเกิดความผิดพลาดการปฏิบัติงาน (เฉลี่ย : ปี/ครั้ง) (Y ๔) | ๕ ปี/ครั้ง | ๒-๓ ปี/ครั้ง | ๑ ปี/ครั้ง | ๑-๖ เดือน/ครั้ง หรือมากกว่า | ๑ เดือน/ครั้ง หรือมากกว่า |
| โอกาสที่จะเกิดเหตุการณ์ (Y๕) | ๕ ปี/ครั้ง | ๔ ปี/ครั้ง | ๓ ปี/ครั้ง | ๒ ปี/ครั้ง | ๑ปี/ครั้ง (เกิดแน่นอน) |

**ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงปริมาณ**

| ระดับ | โอกาสที่จะเกิด | คำอธิบาย |
|---|---|---|
| ๕ | สูงมาก | ๑ เดือน/ครั้ง หรือมากกว่า |
| ๔ | สูง | ๑-๖ เดือน/ครั้ง แต่ไม่เกิน ๕ ครั้ง |
| ๓ | ปานกลาง | ๑ ปี/ครั้ง |
| ๒ | น้อย | ๒-๓ ปี/ครั้ง |
| ๑ | น้อยมาก | ๕ ปี/ครั้ง |

**ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงคุณภาพ**

| ระดับ | โอกาสที่จะเกิด | คำอธิบาย |
|---|---|---|
| ๕ | สูงมาก | มีโอกาสในการเกิดเกือบทุกครั้ง |
| ๔ | สูง | มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ |
| ๓ | ปานกลาง | มีโอกาสเกิดบางครั้ง |
| ๒ | น้อย | อาจมีโอกาสเกิดแต่นานๆ ครั้ง |
| ๑ | น้อยมาก | มีโอกาสเกิดน้อยมาก หรือไม่น่าเกิด |

**ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงปริมาณ**

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

**ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงปริมาณ**

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

**ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงคุณภาพ**

| ระดับ | ผลกระทบ | คำอธิบาย |
|---|---|---|
| ๕ | รุนแรงที่สุด | มีการสูญเสียทรัพย์สินอย่างมหันต์ มีการบาดเจ็บถึงชีวิต |
| ๔ | ค่อนข้างรุนแรง | มีการสูญเสียทรัพย์สินมาก มีการบาดเจ็บสาหัสถึงขั้นพักงาน |
| ๓ | ปานกลาง | มีการสูญเสียทรัพย์สินมาก มีการบาดเจ็บสาหัสถึงขั้นหยุดงาน |
| ๒ | น้อย | มีการสูญเสียทรัพย์สินพอสมควร มีการบาดเจ็บรุนแรง |
| ๑ | มาก | มีการสูญเสียทรัพย์สินเล็กน้อย ไม่มีการบาดเจ็บรุนแรง |

**ระดับความรุนแรงของผลกระทบของความเสี่ยงต่อชื่อเสียงขององค์กร**

| ระดับ | ผลกระทบ | คำอธิบาย |
|---|---|---|
| ๕ | สูงมาก | มีการพาดหัวข่าวทั้งจากสื่อภายในและต่างประเทศ |
| ๔ | สูง | มีการเผยแพร่ข่าวในวงกว้างสำหรับสื่อภายในประเทศและมีการเผยแพร่ข่าวในวงจำกัดของสื่อต่างประเทศ |
| ๓ | ปานกลาง | มีการเผยแพร่ข่าวในหนังสือพิมพ์ภายในประเทศหลายฉบับ (๒-๕ วัน) |
| ๒ | น้อย | มีการเผยแพร่ข่าวในวงจำกัดภายในประเทศ (๑ วัน) |
| ๑ | น้อยมาก | ไม่มีการเผยแพร่ข่าว |

**ระดับความรุนแรงของผลกระทบของความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศ**

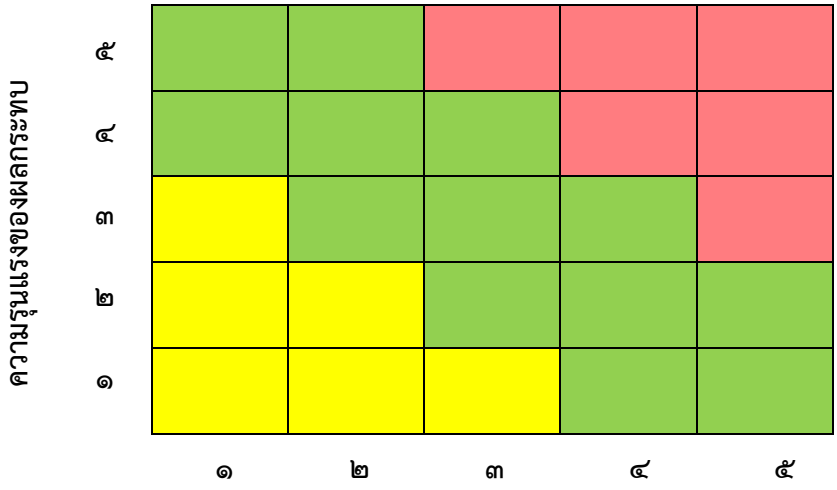
| ระดับ | ผลกระทบ | คำอธิบาย |
|---|---|---|
| ๕ | สูงมาก | เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ |
| ๔ | สูง | เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน |
| ๓ | ปานกลาง | ระบบมีปัญหาและมีความสูญเสียไม่มาก |
| ๒ | น้อย | เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้ |
| ๑ | น้อยมาก | เกิดเหตุร้ายที่ไม่มีความสำคัญ |

**ระดับความรุนแรงของผลกระทบของความเสี่ยงต่อบุคลากร**

| ระดับ | ผลกระทบ | คำอธิบาย |
|---|---|---|
| ๕ | สูงมาก | ถูกเลิกจ้างออกจากงาน และอันตรายต่อร่างกายและชีวิตโดยตรง |
| ๔ | สูง | ถูกลงโทษทางวินัย ตัดเงินเดือน ไม่ได้ขึ้นเงินเดือน |
| ๓ | ปานกลาง | ถูกทำทัณฑ์บน คุณภาพชีวิต และบรรยากาศการปฏิบัติงานที่ไม่เหมาะสม |

| ระดับ | ผลกระทบ | คำอธิบาย |
|---|---|---|
| ๒ | น้อย | ไม่สะดวกต่อการปฏิบัติงานบ่อยครั้ง |
| ๑ | น้อยมาก | ไม่สะดวกต่อการปฏิบัติงานนานๆ ครั้ง |

**แผนภูมิความเสี่ยง**




**หมายเหตุ** : นำรหัสของปัจจัยเสี่ยงใส่ลงในช่องที่มีระดับความเสี่ยง (L) × (I) ที่สอดคล้องกันนั้น

| ระดับความเสี่ยง | เขตสี | มาตรการในปัจจุบัน | มาตรการเพิ่มเติม |
|---|---|---|---|
| **ยอมรับได้** | เขียว | มาตรการในการจัดการความเสี่ยงในปัจจุบันเพียงพอหรือมีการควบคุมที่ดีมากแล้ว | ไม่จำเป็นต้องมีมาตรการจัดการความเสี่ยงเพิ่มเติมอีก หรืออาจจะผ่อนคลายมาตรการเดิม เพื่อให้มีประสิทธิภาพมากขึ้นโดยไม่เกิดการใช้ทรัพยากรมากเกินไป |
| | เหลือง | มาตรการในการจัดการความเสี่ยงในปัจจุบัน อาจจะเพียงพอแล้ว ให้ติดตามการดำเนินการเป็นระยะๆ | ไม่จำเป็นต้องมีมาตรการจัดการความเสี่ยงเพิ่มเติมอีก หรืออาจจะมีได้หากไม่ใช้ทรัพยากรเพิ่มเติมหรือมีแผนงานอื่นรองรับอยู่แล้ว |
| **สูงกว่าระดับที่ยอมรับได้** | แดง | ต้องเฝ้าระวังอย่างต่อเนื่อง และอาจเพิ่มเติมความเข้มข้นในการดำเนินการตามมาตรการในปัจจุบัน | จำเป็นต้องมีการเพิ่มเติมมาตรการ โดยหากมีข้อจำกัดด้านทรัพยากรในการจัดการความเสี่ยงให้มีความสำคัญในระดับที่สูงกว่า และผู้บริหารควรให้ความสำคัญในการติดตามการดำเนินการของมาตรการดังกล่าวอย่างต่อเนื่อง |

**ขั้นตอนที่ ๔** กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

การกำหนดกลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยงมี ๔ กลยุทธ์ (๔T's Strategies) ได้แก่

๑. การยอมรับความเสี่ยง (Take) หากทำการวิเคราะห์แล้วเห็นว่า ไม่มีวิธีการจัดการความเสี่ยงใดที่เหมาะสม เนื่องจากต้นทุนการจัดการความเสี่ยงสูงกว่าประโยชน์ที่จะได้รับ อาจต้องยอมรับความเสี่ยง แต่ควรมีมาตรการติดตามอย่างใกล้ชิดเพื่อรองรับผลที่จะเกิดขึ้น

๒. การลด/ควบคุมความเสี่ยง (Treat) พยายามลดความเสี่ยงโดยการเพิ่มเติม หรือเปลี่ยนแปลงขั้นตอนบางส่วนของกิจกรรม หรือโครงการที่นำไปสู่เหตุการณ์ที่เป็นความเสี่ยง รวมถึงลดความน่าจะเป็นที่เหตุการณ์ที่เป็นความเสี่ยงจะเกิดขึ้น

๓. การถ่ายโอน/กระจายความเสี่ยง (Transfer) ยกภาระในการเผชิญหน้ากับเหตุการณ์ และการจัดการกับความเสี่ยงให้ผู้อื่น

๔. การหลีกเลี่ยงความเสี่ยง (Terminate) ปฏิเสธและหลีกเลี่ยงโอกาสที่จะเกิดความเสี่ยงโดยการหยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรม หรือโครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง

**ขั้นตอนที่ ๕** กิจกรรมการบริหารความเสี่ยง (Control Activities)

การกำหนดกิจกรรมการบริหารความเสี่ยง หรือการจัดทำแผนบริหารความเสี่ยงของโครงการ ประกอบด้วย

๕.๑ การกำหนดกิจกรรมตามแนวทางการจัดการความเสี่ยง เป็นการกำหนดวิธีการต่างๆ ที่นำมาใช้ในการดำเนินงาน เพื่อป้องกันหรือลดความเสี่ยงอย่างมีประสิทธิภาพและประสิทธิผล และให้สามารถบรรลุวัตถุประสงค์ขององค์กร

๕.๒ กำหนดเป้าหมาย/ผลสำเร็จของการดำเนินการกิจกรรมตามแนวทางการจัดการความเสี่ยง

๕.๓ การกำหนดระยะเวลาในการดำเนินการ ผู้รับผิดชอบ และงบประมาณ (ถ้ามี)

**ขั้นตอนที่ ๖** ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

ข้อมูลและการสื่อสารเป็นส่วนสนับสนุนที่สำคัญต่อประสิทธิภาพและประสิทธิผลในการกำหนดกลยุทธ์ ประเมินความเสี่ยง และกิจกรรมการบริหารความเสี่ยง ดังนั้น เมื่อดำเนินการจัดทำแผนบริหารความเสี่ยงของหน่วยงานเรียบร้อยแล้ว จะต้องมีการสื่อสารแผนบริหารความเสี่ยงของหน่วยงานให้บุคลากรในหน่วยงานทราบ เพื่อเข้าใจในหลักการบริหารความเสี่ยง กิจกรรม/มาตรการในการจัดการความเสี่ยง และสามารถนำแผนบริหารความเสี่ยงของหน่วยงานไปปฏิบัติได้

**ขั้นตอนที่ ๗** การติดตามและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

หลังจากจัดทำแผนบริหารความเสี่ยง และมีการดำเนินงานตามแผนแล้ว จะต้องมีการรายงานและติดตามผลเป็นระยะๆ เพื่อให้เกิดความมั่นใจว่าได้มีการดำเนินงานไปอย่างถูกต้องและเหมาะสม โดยมีเป้าหมายในการติดตามผล คือ เป็นการประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการไปแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่ โดยหน่วยงานต้องสอบทานดูว่าวิธีการบริหารจัดการความเสี่ยงใดมีประสิทธิภาพดีก็ให้ดำเนินการต่อไป หรือวิธีการบริหารจัดการความเสี่ยงใดควรปรับเปลี่ยนและนำผลการติดตามรายงานให้ฝ่ายบริหารทราบตามแบบรายงาน ทั้งนี้ กระบวนการสอบทานหน่วยงานอาจกำหนดข้อมูลที่ต้องติดตาม หรืออาจทำ Check list การติดตาม พร้อมกำหนดความถี่ในการติดตามผล โดยสามารถติดตามผลใน ๒ ลักษณะ คือ

๗.๑ การติดตามผลเป็นรายครั้ง (Separate Monitoring) เป็นการติดตามตามรอบระยะเวลาที่กำหนด เช่น ทุก ๓ เดือน ๖ เดือน ๙ เดือน หรือทุกสิ้นปี

๗.๒ การติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring) เป็นการติดตามที่รวมอยู่ในการดำเนินงานต่างๆ ตามปกติของหน่วยงาน

**๒.๓ กรอบการบริหารความเสี่ยงด้านสารสนเทศ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC ๒๗๐๐๑ : ๒๐๑๓)**

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และสารสนเทศรวมถึงข้อมูลสารสนเทศ มีดังนี้

๑. ความเสี่ยงที่เกิดจากบุคคล (People) ดังนี้

๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร หมายถึง บุคลากรของกรมสนับสนุนบริการสุขภาพ ขาดความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ เช่น ด้านฮาร์ดแวร์ ซอฟท์แวร์และด้านเครือข่าย รวมถึงการใช้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศที่ไม่เหมาะสม

๑.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี หมายถึง ผู้ที่หวังก่อกวน เจาะทำลายระบบ เพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ หากไม่ได้รับการป้องกันด้วยเครื่องมือหรืออุปกรณ์ที่มีมาตรฐานและอัพเดทให้ทันสมัย เช่น Firewall ระบบ IPS และระบบป้องกันไวรัส

๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) ดังนี้

๒.๑ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) หมายถึง ผู้ที่ลักลอบเข้าไปโจรกรรมอุปกรณ์ประมวลผลข้อมูลภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์ หากศูนย์ข้อมูลดังกล่าว ไม่ได้รับการป้องกันที่ดี เช่น มาตรการในการเข้าถึงห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์ เครื่องอ่านแถบแม่เหล็ก กล้องวงจรปิดและเจ้าหน้าที่รักษาความปลอดภัย เป็นต้น

๒.๒ ความเสี่ยงที่เกิดจากด้านเทคนิค หมายถึง เหตุการณ์หรือภัยที่เกิดจากอุปกรณ์ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์ ทำงานไม่เต็มประสิทธิภาพ หรือไม่สามารถให้บริการได้ เช่น อุปกรณ์ประมวลผลข้อมูลชำรุด เสียหาย เนื่องจากอุปกรณ์บางรายการเสื่อมสภาพตามอายุการใช้งาน ระบบปรับอากาศชำรุด ส่งผลให้อุณหภูมิภายในห้องสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูลที่ให้บริการหยุดการทำงาน ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถใช้งานได้หรืออาจได้รับความเสียหาย

๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ

๒.๓.๑ เหตุการณ์ไฟฟ้าดับ หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟฟ้าดับ ซึ่งส่งผลให้อุปกรณ์ประมวลผลข้อมูล ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์ไม่มีแหล่งพลังงานที่ใช้ในการเปิดระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับให้บริการ เช่น สายไฟฟ้าขาด ไฟฟ้าช็อต หม้อแปลงไฟฟ้าที่ติดตั้งบริเวณกรมสนับสนุนบริการสุขภาพหรือภายในกระทรวงสาธารณสุขเสียหาย

๒.๓.๒ เหตุการณ์อัคคีภัย หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟไหม้ ซึ่งเป็นเหตุการณ์ที่สร้างความเสียหายร้ายแรงที่สุด ทำให้ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์ ถูกไฟไหม้ จนทำให้ไม่สามารถปฏิบัติงานได้ เช่น ไฟฟ้าลัดวงจรหรือ ไฟไหม้บริเวณอื่น แล้วลุกลามมาที่ห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์

๒.๓.๒ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง หมายถึง เหตุการณ์อันเกิดจากภัยตามธรรมชาติหรือสถานการณ์ที่เกิดจากกลุ่มบุคคล ซึ่งอาจไม่เกิดผลกระทบโดยตรงต่อการให้บริการของระบบคอมพิวเตอร์และระบบสารสนเทศ แต่ละเกิดผลกระทบต่อการเข้าไปปฏิบัติงานภายในพื้นที่ห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์ กรมสนับสนุนบริการสุขภาพ

๓. ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) เช่น

๓.๑ ทรัพย์สินครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software)

๓.๒ เครือข่ายสารสนเทศ และเครือข่ายเสมือน (Information Network and Virtual Network)

๓.๓ โครงข่ายการสื่อสาร (Communication Network)

๓.๔ ข้อมูลและสารสนเทศ (Information)

การวิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศ มีการพิจารณาจากเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) และภัยพิบัติหรือสถานการณ์อื่นๆ รวมถึงได้กำหนดแนวทางการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต การสำรอง และการกู้คืนข้อมูลสารสนเทศ ตามแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓ (ฉบับปรับปรุง ครั้งที่ ๑)[๑] สำหรับใช้เป็นแนวทางในการปฏิบัติงาน

นอกจากนี้ จะต้องมีการจัดทำสรุปรายงานผลและประเมินผลการบริหารความเสี่ยงประจำปี เพื่อให้มั่นใจว่ามีการบริหารความเสี่ยงเป็นไปอย่างเหมาะสม เพียงพอ ถูกต้อง และมีประสิทธิผล มาตรการหรือกลการควบคุมความเสี่ยง (Control Activity) ที่ดำเนินการสามารถลดและควบคุมความเสี่ยงที่เกิดขึ้นได้จริง และอยู่ในระดับที่ยอมรับได้ หรือต้องจัดหามาตรการหรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่หลังมีการจัดการ (Residual Risk) อยู่ในระดับที่ยอมรับได้ และให้หน่วยงานมีการบริหารความเสี่ยงอย่างต่อเนื่องจนเป็นวัฒนธรรมในการดำเนินงาน

[๑] อยู่ระหว่างเสนอสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์พิจารณา

# บทที่ ๓

# ข้อมูลพื้นฐาน

**๓.๑ ความเป็นมาและวัตถุประสงค์**

กรมสนับสนุนบริการสุขภาพ ได้จัดทำแผนปฏิรูปองค์การ ตามมาตรการปรับปรุงประสิทธิภาพในการปฏิบัติราชการประจำปีงบประมาณ พ.ศ. ๒๕๖๑ ได้กำหนดให้ทุกส่วนราชการต้องจัดทำแผนปฏิรูปองค์กรตามองค์ประกอบที่ ๕ (Potential Base) โดยให้วิเคราะห์สถานการณ์ บทบาทภารกิจ ระบบงาน โครงสร้าง อัตรากำลังและจัดทำข้อเสนอการปรับเปลี่ยนบทบาทภารกิจในระยะ ๓ ปี (ปีงบประมาณ พ.ศ. ๒๕๖๒ – ๒๕๖๔)

ตามประกาศกฎกระทรวงแบ่งส่วนราชการ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข พ.ศ. ๒๕๖๓ ในราชกิจจานุเบกษา เล่มที่ ๑๓๗ ตอนที่ ๔๑ ก ลงวันที่ ๙ มิถุนายน ๒๕๖๓ และกรมสนับสนุนบริการสุขภาพ ได้จัดตั้งหน่วยงานภายในขึ้นเป็นส่วนราชการที่มีฐานะเทียบเท่ากอง ตามคำสั่งกรมสนับสนุนบริการสุขภาพ ที่ ๑๐๗๒/๒๕๖๓ ลงวันที่ ๙ มิถุนายน พ.ศ. ๒๕๖๓ และคำสั่งกรมสนับสนุนบริการสุขภาพ ที่ ๑๐๗๖/๒๕๖๓ ลงวันที่ ๙ มิถุนายน พ.ศ. ๒๕๖๓

เพื่อให้การดำเนินงานสัมฤทธิ์ผลตามเป้าหมายและมีประสิทธิภาพ จึงได้ทบทวนภารกิจของหน่วยงานใน ๔ ด้าน คือ

๑. Structure การปรับปรุงโครงสร้างหน่วยงานให้สอดรับกับภารกิจใหม่

๒. Process Redesign การปรับปรุงกระบวนการทำงานให้ง่าย สะดวก ลดต้นทุนค่าใช้จ่ายและตอบโจทย์ประชาชนผู้ใช้บริการบน Digital Platform

๓. Law การปรับปรุงกฎหมายให้เอื้อต่อการปฏิบัติงานในรูปแบบใหม่

๔. People การพัฒนาบุคลากร การจัดสรรอัตรากำลังให้สอดรับกับการปรับบทบาทภารกิจและการปฏิบัติงานในรูปแบบใหม่โดยใช้ Digital Platform

สามารถจำแนกออกเป็น ๓ ภารกิจหลัก และภารกิจระดับพื้นที่ คือ

(๑) ภารกิจที่ ๑ ภารกิจการคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ

(๑.๑) ด้านสถานพยาบาลและการประกอบโรคศิลปะ : กองสถานพยาบาลและการประกอบโรคศิลปะ (สพรศ.)

(๑.๒) ด้านสถานประกอบการเพื่อสุขภาพ : กองสถานประกอบการเพื่อสุขภาพ (กสพส.)

(๑.๓) ด้านกฎหมาย : กองกฎหมาย (กม.)

(๑.๔) ศูนย์คุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ (ศคบ.)

(๒) ภารกิจที่ ๒ ภารกิจยุทธศาสตร์การบริหารจัดการและกำกับมาตรฐานระบบบริการสุขภาพ

(๒.๑) ด้านวิศวกรรมการแพทย์และสาธารณสุข : กองวิศวกรรมการแพทย์ (วศ.)

(๒.๒) ด้านอาคารและสภาพแวดล้อมสาธารณสุข : กองแบบแผน (บ.)

(๒.๓) ด้านการพัฒนาอุตสาหกรรมบริการสุขภาพแบบครบวงจร : กองสุขภาพระหว่างประเทศ (กสป.)

(๒.๔) ด้านบริหารจัดการ

(๒.๔.๑) สำนักงานเลขานุการกรม (สลก.)

(๒.๔.๒) กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม (กทส.)

(๒.๔.๓) กลุ่มบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม (กบค.)

(๒.๔.๔) กลุ่มแผนงาน สำนักงานเลขานุการกรม (กผ.)

(๒.๖) ด้านพัฒนาระบบบริหารจัดการ : กลุ่มพัฒนาระบบบริหารจัดการ (กพร.)

(๒.๗) ด้านตรวจสอบภายใน : กลุ่มตรวจสอบภายใน (ตสน.)

(๒.๘) ด้านคุ้มครองจริยธรรม : กลุ่มงานคุ้มครองจริยธรรม (กคจ.)

(๒.๙) ด้านวิชาการ : สำนักผู้เชี่ยวชาญ (สชช.)

(๓) ภารกิจที่ ๓ ภารกิจส่งเสริมการมีส่วนร่วมภาคประชาชน

(๓.๑) ด้านสุขภาพภาคประชาชน : กองสนับสนุนสุขภาพภาคประชาชน (สช.)

(๓.๒) ด้านพัฒนาพฤติกรรมสุขภาพ : กองสุขศึกษา (ส.)

(๔) ภารกิจที่ ๔ ภารกิจระดับพื้นที่ ด้านสนับสนุนระบบบริการสุขภาพในพื้นที่

(๔.๑) ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑ - ๑๒ (ศบส. ๑ - ๑๒)

(๔.๒) ศูนย์พัฒนาการสาธารณสุขมูลฐาน ๕ ภาค (สสม. ๕ ภาค)

โดยมีการกำหนดรูปแบบวิธีการทำงานแบบใหม่ (Business Model) ให้แต่ละงานที่สำคัญ ดังนี้

(๑) ภารกิจหลักระดับกรมสนับสนุนบริการสุขภาพ :เป็นกรมวิชาการที่มีบทบาทของการส่งเสริม ควบคุม กำกับ รับรอง คุณภาพมาตรฐานเพื่อการคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ (Regulator for Customer Protection) และ ขยายผลไปสู่นโยบายด้านเศรษฐศาสตร์สาธารณสุขในอนาคต (Organizational Transformation Plan to Health Economics) ในการก้าวสู่รัฐบาลดิจิทัล (Digital Government) ประกอบด้วย

(๑.๑) งานคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ

(๑.๒) งานสนับสนุนการบริหารจัดการและกำกับมาตรฐานระบบบริการสุขภาพ

(๑.๓) งานเสริมสร้างการมีส่วนร่วมภาคประชาชน

(๒) ภารกิจระดับพื้นที่ : ดำเนินการ ๓ ภารกิจหลักในระดับภูมิภาค

### ๓.๒ โครงสร้างของระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

#### เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

จากการสำรวจสถานภาพเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ของกรมสนับสนุนบริการสุขภาพ พบว่ามีคอมพิวเตอร์ตั้งโต๊ะ จำนวน ๗๖๖ เครื่อง คอมพิวเตอร์โน๊ตบุ๊ค จำนวน ๒๒๙ เครื่อง เครื่องพิมพ์ จำนวน ๓๓๐ เครื่อง สแกนเนอร์ จำนวน ๖๓ เครื่อง โดยมีจำนวนบุคลากรที่ปฏิบัติงานจริงจำนวน ๑,๓๙๓ คน

**ตารางที่ ๑** สรุปจำนวนข้อมูลเครื่องคอมพิวเตอร์และอุปกรณ์

| รายการ | จำนวนที่มีปัจจุบัน | จำนวนที่ต้องการเพิ่ม | หมายเหตุ |
|---|---|---|---|
| **คอมพิวเตอร์ตั้งโต๊ะ** | ๗๖๖ | ๔๖๙ | ข้าราชการ ๗๗๐ คน |
| **คอมพิวเตอร์โน๊ตบุ๊ค** | ๒๒๙ | ๗๕ | ลูกจ้างประจำ ๒๒๑ คน |
| **เครื่องพิมพ์** | ๓๓๐ | ๕๕ | พนักงานราชการ ๑๘๑ คน |
| **สแกนเนอร์** | ๖๓ | ๒๔ | จ้างเหมาบริการ ๒๒๑ คน |
| **รวม** | **๑,๓๘๘** | **๖๒๓** | **๑,๓๙๓** |

#### เครื่องคอมพิวเตอร์แม่ข่าย [๑]

เครื่องคอมพิวเตอร์แม่ข่าย (Server) สามารถจำแนกตามลักษณะทางกายภาพได้ ๓ ประเภท คือ (๑) Rack Server จำนวน ๔๓ เครื่อง คิดเป็นร้อยละ ๗๐.๕ ของจำนวนเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด (๒) Tower จำนวน ๔ เครื่อง คิดเป็นร้อยละ ๖.๕ (๓) Blade Server จำนวน ๑๔ เครื่อง คิดเป็นร้อยละ ๒๓ และในส่วนของระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (๑) Unix/Linux จำนวน ๔๕ เครื่อง คิดเป็นร้อยละ ๗๓.๗ (๒) Windows Server จำนวน ๑๖ คิดเป็นร้อยละ ๒๖.๓

[1] ข้อมูล ณ เดือนสิงหาคม ๒๕๖๑ จาก แผนปฏิบัติการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม

**ตารางที่ ๒** จำนวนเครื่องคอมพิวเตอร์แม่ข่าย (SERVER) และระบบปฏิบัติการสำหรับเครื่องแม่ข่าย

| ลำดับ | เครื่องแม่ข่าย | ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย | สถานที่ |
|---|---|---|---|
| ๑ | Sun Sparc T-๓ | SunOS ๕.๑๐ | Datacenter |
| ๒ | Sun Sparc T-๓ | SunOS ๕.๑๐ | Datacenter |
| ๓ | HP ProLiant DL๓๘๐ G๗ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๔ | HP ProLiant DL๓๘๐ G๗ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๕ | HP ProLiant DL๓๘๐ G๗ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๖ | HP Proliant DL๓๘๐GS | CentOS | Datacenter |
| ๗ | HP ProLiant DL๓๘๐ G๕ | Microsoft Windows Server ๒๐๐๘ Standard | Datacenter |
| ๘ | Dell PowerEdge ๒๙๐๐ | CentOS ๕.๖ | Datacenter |
| ๙ | HP Proliant ML๓๕๐ | CentOS | Datacenter |
| ๑๐ | IBM System x๓๖๕๐ M๓ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๑๑ | HP ProLiant ML๑๑๐ G๗ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๑๒ | HP ProLiant ML๓๕๐ G๕ | Microsoft Windows Server ๒๐๐๓, Enterprise | Datacenter |
| ๑๓ | HP Proliant DL๓๘๐ G๕ | Microsoft Windows Server ๒๐๐๘ Standard | Datacenter |
| ๑๔ | HP ProLiant DL๓๘๐ G๕ | Microsoft Windows Server ๒๐๐๘ Standard | Datacenter |
| ๑๕ | HP ProLiant DL๓๘๐ G๗ | Microsoft Windows Server ๒๐๐๓, Enterprise | Datacenter |
| ๑๖ | HP ProLiant DL๓๘๐p Gen๘ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๑๗ | Fujitsu RX๓๐๐๐ S๗ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๑๘ | Dell PowerEdge R๗๒๐ | CentOS | Datacenter |
| ๑๙ | HP ProLiant DL๓๘๐p Gen๘ | CentOS (VMWare) | Datacenter |
| ๒๐ | Bladesystem c๗๐๐๐ Enclosure ๑๔ Bay | HP UEFI | Datacenter |
| ๒๑ | HP Proliant BL๔๖๐C Gen๘ (Bay ๑) | Vmware ESXI/CentOS | Datacenter |
| ๒๒ | HP Proliant BL๔๖๐C Gen๘ (Bay ๒) | Vmware ESXI/CentOS | Datacenter |
| ๒๓ | HP Proliant BL๔๖๐C Gen๘ (Bay ๓) | Vmware ESXI/CentOS | Datacenter |

| ลำดับ | เครื่องแม่ข่าย | ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย | สถานที่ |
|---|---|---|---|
| ๒๔ | HP Proliant BL๔๖๐C Gen๘ (Bay ๔) | Vmware ESXI/CentOS | Datacenter |
| ๒๕ | HP Proliant BL๔๒๐C Gen๘ (Bay ๕) | Vmware ESXI/CentOS | Datacenter |
| ๒๖ | HP Proliant BL๔๒๐C Gen๘ (Bay ๖) | Vmware ESXI/CentOS | Datacenter |
| ๒๗ | HP Proliant BL๔๒๐C Gen๘ (Bay ๗) | Vmware ESXI/CentOS | Datacenter |
| ๒๘ | HP Proliant BL๔๒๐C Gen๘ (Bay ๘) | Vmware ESXI/CentOS | Datacenter |
| ๒๙ | HP Proliant BL๔๒๐C Gen๘ (Bay ๙) | Vmware ESXI/CentOS | Datacenter |
| ๓๐ | HP Proliant BL๔๒๐C Gen๘ (Bay ๑๐) | Vmware ESXI/CentOS | Datacenter |
| ๓๑ | HP Proliant BL๔๒๐C Gen๘ (Bay ๑๑) | Vmware ESXI/CentOS | Datacenter |
| ๓๒ | HP Proliant BL๔๒๐C Gen๘ (Bay ๑๒) | Vmware ESXI/CentOS | Datacenter |
| ๓๓ | HP Proliant BL๔๒๐C Gen๘ (Bay ๑๓) | Vmware ESXI/CentOS | Datacenter |
| ๓๔ | HP Proliant BL๔๒๐C Gen๘ (Bay ๑๔) | Vmware ESXI/CentOS | Datacenter |
| ๓๕ | HP Proliant DL๓๘๐p G๘ | Microsoft Windows Server ๒๐๐๘ R๒ Standard | Datacenter |
| ๓๖ | Dell PowerEdge ๒๙๕๐ | Microsoft Windows Server ๒๐๐๓ R๒ | Datacenter |
| ๓๗ | Dell PowerEdge ๒๙๕๐ | Microsoft Windows Server ๒๐๐๓ R๒ | Datacenter |
| ๓๘ | IBMX๒๓๖ | Microsoft Windows Server ๒๐๐๓ | Datacenter |
| ๓๙ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | เชียงใหม่ |
| ๔๐ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | เชียงใหม่ |
| ๔๑ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ชลบุรี |
| ๔๒ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ชลบุรี |
| ๔๓ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ขอนแก่น |
| ๔๔ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ขอนแก่น |
| ๔๕ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครราชสีมา |
| ๔๖ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครราชสีมา |
| ๔๗ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครสวรรค์ |
| ๔๘ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครสวรรค์ |
| ๔๙ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครสวรรค์ |
| ๕๐ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครสวรรค์ |
| ๕๑ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครศรีธรรมราช |
| ๕๒ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นครศรีธรรมราช |
| ๕๓ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ราชบุรี |
| ๕๔ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ราชบุรี |
| ๕๕ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | สงขลา |
| ๕๖ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | สงขลา |
| ๕๗ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | อุบลราชธานี |

| ลำดับ | เครื่องแม่ข่าย | ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย | สถานที่ |
|---|---|---|---|
| ๕๘ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | อุบลราชธานี |
| ๕๙ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ขอนแก่น |
| ๖๐ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | ขอนแก่น |
| ๖๑ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นนทบุรี |
| ๖๒ | Server HP ProLiant DL๓๖๐ Gen๙ | Vmware ESXI/CentOS | นนทบุรี |

นอกจากเครื่องแม่ข่ายจริงแล้ว กรมสนับสนุนบริการสุขภาพ โดยกลุ่มเทคโนโลยีสารสนเทศยังมีการนำระบบคอมพิวเตอร์แม่ข่ายเสมือน (Server Virtualization System) มาจัดสรรทรัพยากรให้ระบบสารสนเทศที่ทำงานบนระบบปฏิบัติการเดียวกัน เป็นการใช้ทรัพยากรร่วมกันได้อย่างเต็มประสิทธิภาพ ประหยัดพลังงาน และลดพื้นที่ในการใช้งานห้องแม่ข่าย ตลอดจนรองรับปัญหาการขาดแคลนเครื่องคอมพิวเตอร์แม่ข่ายที่มีอายุการใช้งานเกินกว่าที่กำหนดหรือที่ไม่สามารถทำงานได้

## ระบบเครือข่าย

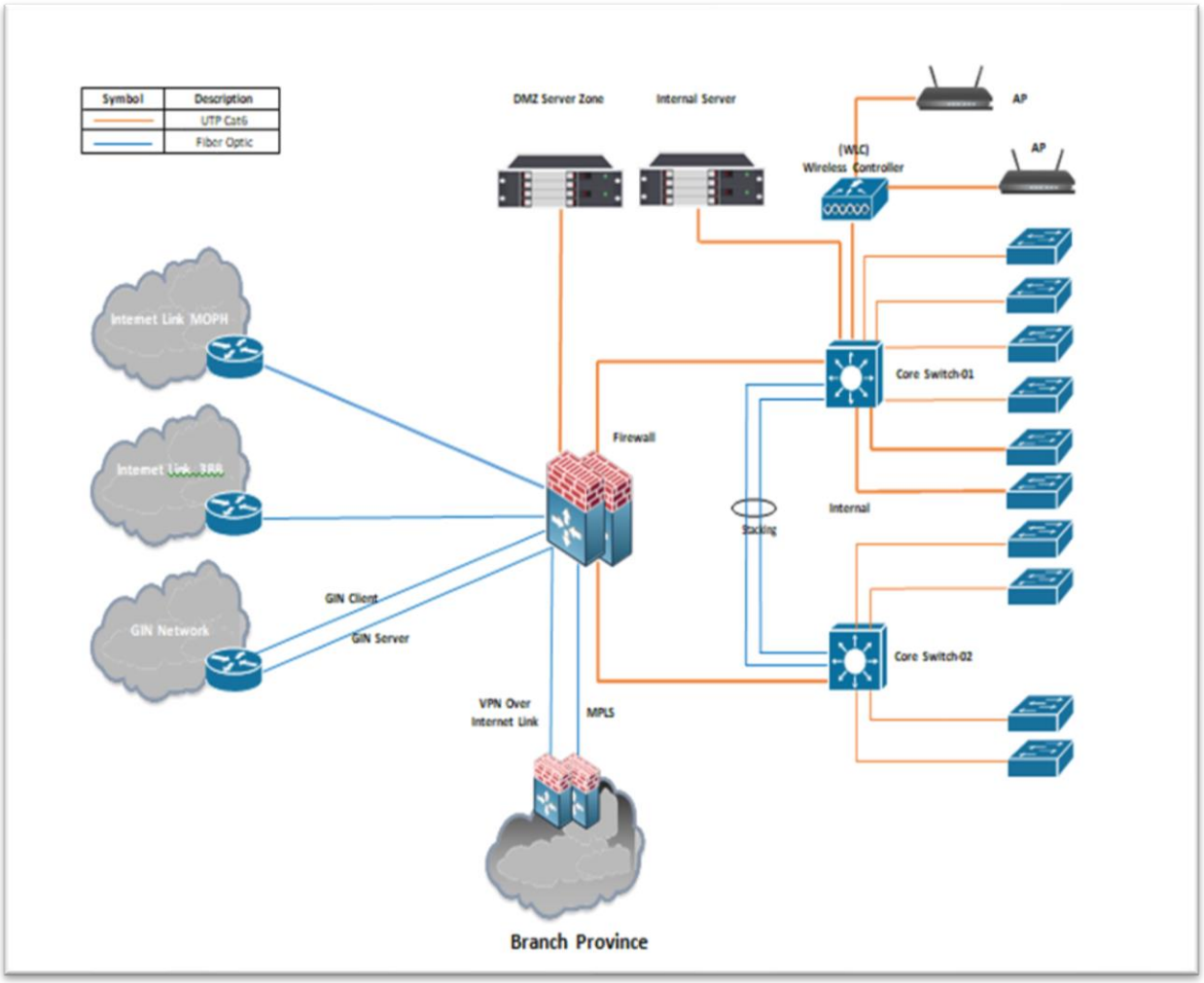
กรมสนับสนุนบริการสุขภาพได้ดำเนินการเชื่อมต่อระบบเครือข่าย (Network) ที่มีความเร็วในการรับ-ส่งข้อมูล ภายในประเทศ (Domestic Bandwidth) ไม่น้อยกว่า ๒๐๐ Mbps และภายนอกประเทศ (International Bandwidth) ที่ความเร็วไม่น้อยกว่า ๑๐๐ Mbps โดยมีบริการระบบเครือข่ายอินเทอร์เน็ตทั้งแบบมีสายและแบบไร้สาย เชื่อมโยงข้อมูลเพื่อให้บริการระบบงานสารสนเทศ แก่หน่วยงานภายใต้สังกัด ประชาชนทั่วไป และมีระบบตรวจจับและยับยั้งการโจมตีจากภัยคุกคามต่างๆ เช่น Virus, Malware รวมถึงควบคุมการเข้าถึงระบบสารสนเทศและระบบฐานข้อมูลตามนโยบายด้านความมั่นคง โดยมีรายละเอียดการเชื่อมโยง ดังตารางที่ ๓

**ตารางที่ ๓** แสดงความเร็วในการรับส่งข้อมูลภายในและภายนอกประเทศของระบบอินเทอร์เน็ต

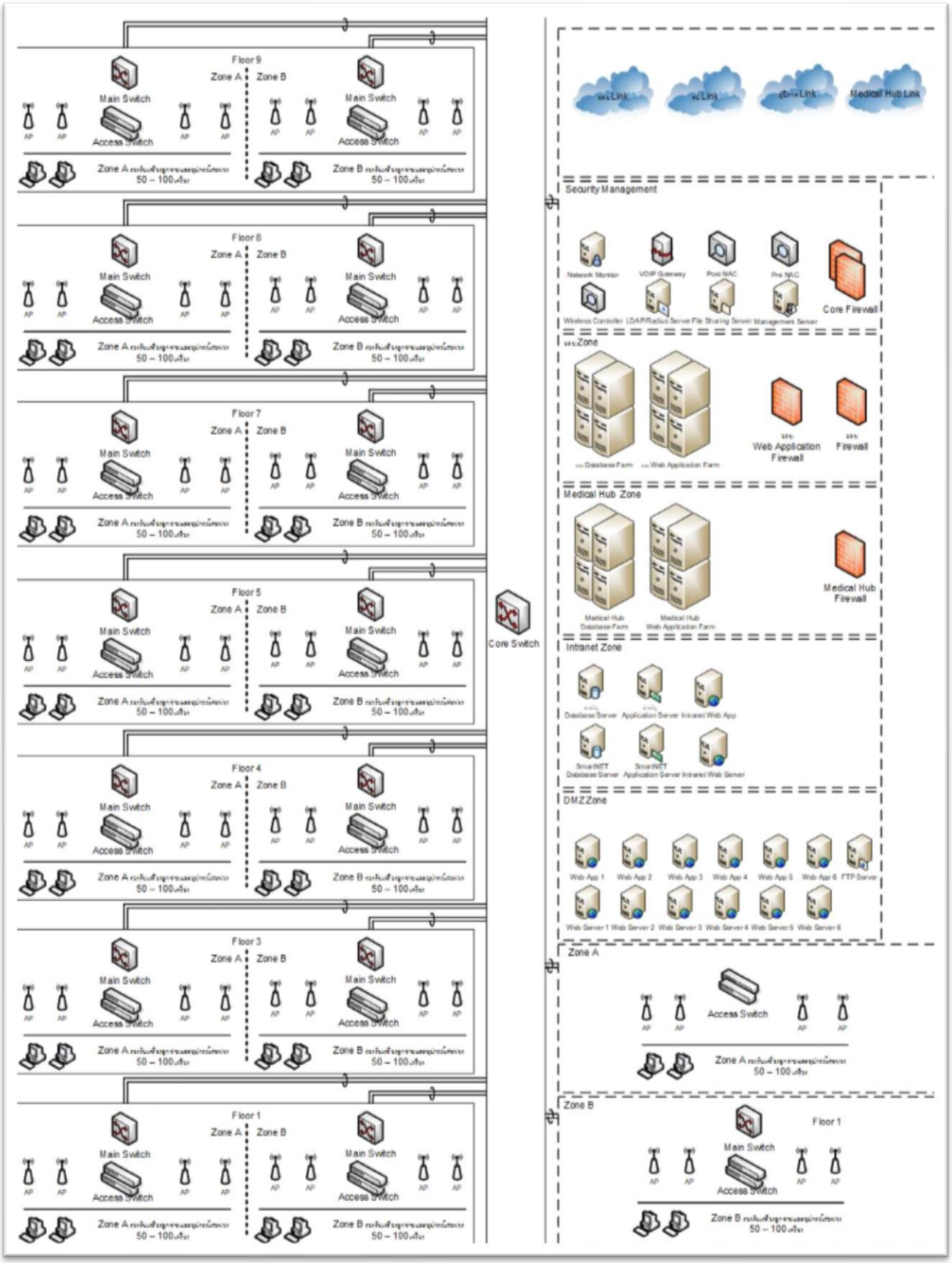
| ลำดับ | สถานที่ตั้ง (Location) | ความเร็ว (Speed) | | |
|---|---|---|---|---|
| | | ๒๕๕๙ | ๒๕๖๐ | ๒๕๖๑ |
| ๑ | กรมสนับสนุนบริการสุขภาพ (Data Center) | ๑๕๐/๕๐ Mbps | ๑๗๐/๗๐ Mbps | ๒๐๐/๑๐๐ Mbps |
| ๒ | กรมสนับสนุนบริการสุขภาพ (อสม.) | ๑๒๐/๑๐ Mbps | ๑๔๐/๒๐ Mbps | ๒๐๐/๔๐ Mbps |
| ๓ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑ (ศูนย์วิศวกรรมการแพทย์ที่ ๖ เชียงใหม่) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๔ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๒ (จังหวัดพิษณุโลก) | | | |
| ๕ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๓ (ศูนย์วิศวกรรมการแพทย์ที่ ๓ นครสวรรค์) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๖ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๔ (สำนักงานสนับสนุนบริการสุขภาพเขต ๔ กองวิศวกรรมการแพทย์) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๗ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๕ (ศูนย์วิศวกรรมการแพทย์ที่ ๑ ราชบุรี) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๘ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๖ | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |

| ลำดับ | สถานที่ตั้ง (Location) | ความเร็ว (Speed) | | |
|---|---|---|---|---|
| | | ๒๕๕๙ | ๒๕๖๐ | ๒๕๖๑ |
| | (Disaster Recovery Site)<br>(ศูนย์วิศวกรรมการแพทย์ที่ ๘ ชลบุรี) | | | |
| ๙ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๗<br>(ศูนย์วิศวกรรมการแพทย์ที่ ๒ ขอนแก่น) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๐ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๘<br>(จังหวัดอุดรธานี) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๑ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๙<br>(ศูนย์วิศวกรรมการแพทย์ที่ ๔ นครราชสีมา) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๒ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๐<br>(ศูนย์วิศวกรรมการแพทย์ที่ ๕ อุบลราชธานี) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๓ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๑<br>(ศูนย์วิศวกรรมการแพทย์ที่ ๙ สุราษฎร์ธานี) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๔ | ศูนย์สนับสนุนบริการสุขภาพ ที่ ๑๒<br>(ศูนย์วิศวกรรมการแพทย์ที่ ๗ สงขลา) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๕ | ศูนย์พัฒนาการสาธารณสุขมูลฐาน<br>ภาคเหนือ จังหวัดนครสวรรค์<br>(ศูนย์ฝึกอบรมและพัฒนาสุขภาพภาค<br>ประชาชน ภาคเหนือ จังหวัดนครสวรรค์) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๖ | ศูนย์พัฒนาการสาธารณสุขมูลฐาน<br>ภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น<br>(ศูนย์ฝึกอบรมและพัฒนาสุขภาพภาค<br>ประชาชน ภาคตะวันออกเฉียงเหนือ จังหวัด<br>ขอนแก่น) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๗ | ศูนย์พัฒนาการสาธารณสุขมูลฐาน<br>ภาคใต้ จังหวัดนครศรีธรรมราช<br>(ศูนย์ฝึกอบรมและพัฒนาสุขภาพภาค<br>ประชาชนภาคใต้ จังหวัดนครศรีธรรมราช) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๘ | ศูนย์พัฒนาการสาธารณสุขมูลฐาน<br>ชายแดนภาคใต้ จังหวัดยะลา<br>(ศูนย์ฝึกอบรมและพัฒนาสุขภาพภาค<br>ประชาชนชายแดนภาคใต้ จังหวัดยะลา) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |
| ๑๙ | ศูนย์พัฒนาการสาธารณสุขมูลฐาน<br>ภาคกลาง จังหวัดชลบุรี<br>(ศูนย์ฝึกอบรมและพัฒนาสุขภาพภาค<br>ประชาชน ภาคกลาง จังหวัดชลบุรี) | ๓๐/๔ Mbps | ๔๐/๘ Mbps | ๕๐/๑๒ Mbps |

**ภาพที่ ๑** ระบบเครือข่ายของกรมสนับสนุนบริการสุขภาพ



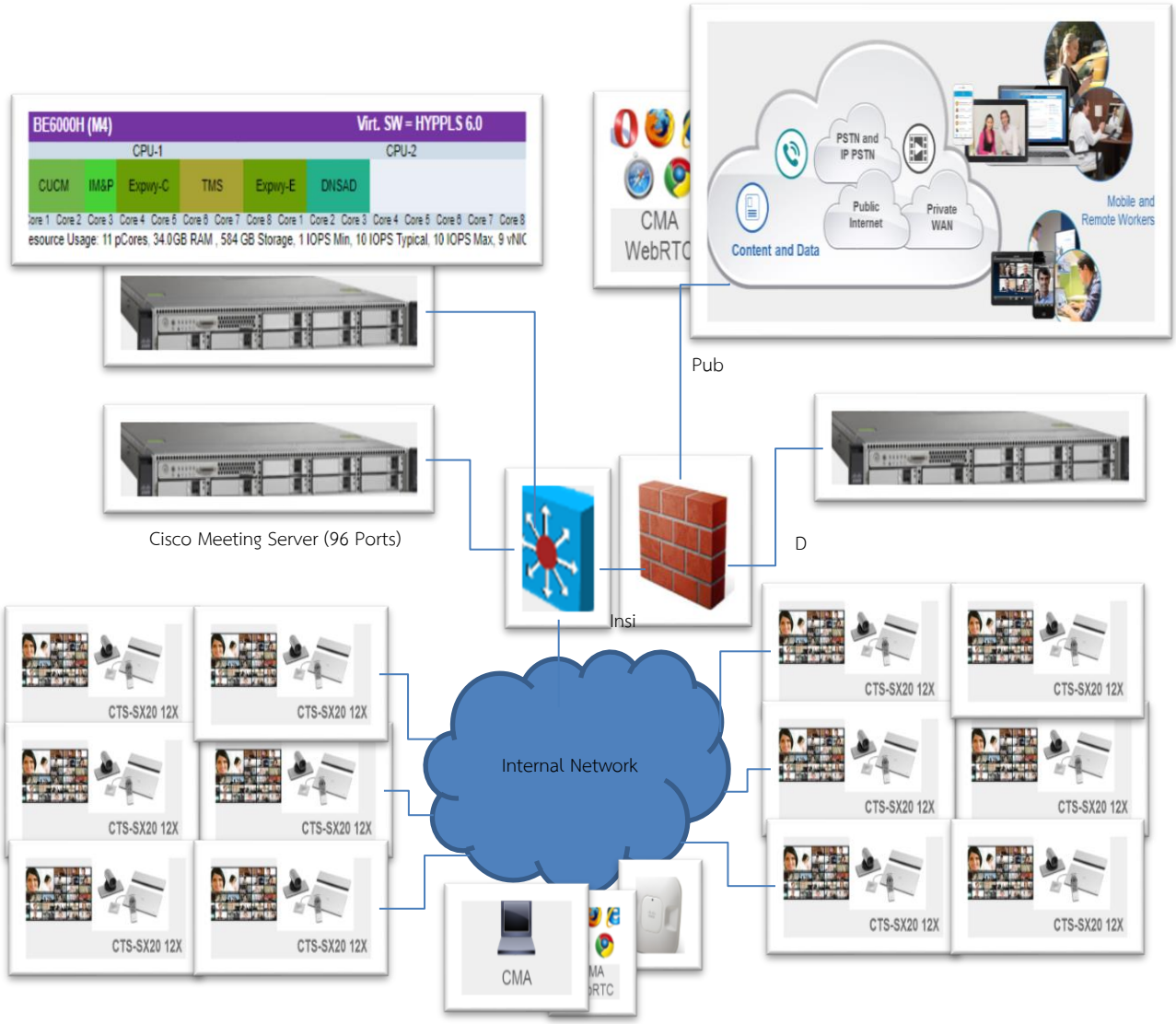
**ภาพที่ ๒** การเชื่อมโยงเครือข่ายภายในกรมสนับสนุนบริการสุขภาพ



## ระบบ VDO Conference และศูนย์ข้อมูล DOC กรมสนับสนุนบริการสุขภาพ

กรมสนับสนุนบริการสุขภาพจัดทำห้องบัญชาการ (War room) ที่สามารถแสดงผลการปฏิบัติงานให้ได้อย่างมีประสิทธิภาพ มีเทคโนโลยีทันสมัย สามารถเชื่อมต่อประชุมทางไกลกับหน่วยงานที่ให้บริการทั้ง ๑๒ เขต ลดภาระค่าใช้จ่ายในการเดินทางมาประชุม และสามารถติดตามงานได้อย่างทันท่วงที รวมถึงใช้เป็นที่บัญชาการในสถานการณ์ฉุกเฉินได้อย่างทันท่วงทีสำหรับการใช้ข้อมูลประกอบการตัดสินใจของผู้บริหารระดับสูง เพื่อตอบสนองการติดตามสถานการณ์ปัจจุบันและข่าวสารอื่น ๆ รวมถึงจัดทำระบบศูนย์ข้อมูล DOC ที่ผู้เข้าร่วมประชุมสามารถ Download เอกสารการประชุมมาใช้งาน ผ่านทาง Application ที่จัดทำ เป็นการลดภาระค่าใช้จ่ายในการจัดเตรียมเอกสารการประชุมให้แก่ผู้เข้าร่วมประชุม อีกทั้งยังสามารถแก้ไขเอกสารผ่านทาง Application ที่จัดทำได้ในขณะที่ประชุม

**ภาพที่ ๓** ระบบ VDO Conference กรมสนับสนุนบริการสุขภาพ



## สถานภาพด้านระบบสารสนเทศและฐานข้อมูล

กรมสนับสนุนบริการสุขภาพได้มีการจัดจ้างพัฒนา และปรับปรุงโปรแกรมต่าง ๆ เพื่อใช้ระบบสารสนเทศสำหรับสนับสนุนการปฏิบัติงาน เมื่อระบบโปรแกรมคอมพิวเตอร์เพิ่มจำนวนขึ้นมาอย่างรวดเร็ว จึงพบปัญหาขาดการบูรณาการและมีความซ้ำซ้อนของข้อมูล เนื่องจากบางระบบมีความจำเป็นเร่งด่วนในการใช้งาน หรือพัฒนาขึ้นใช้งานเฉพาะกิจให้ทันต่อการใช้งานหรือทันต่อเหตุการณ์ของช่วงเวลานั้น และขาดการบำรุงรักษาอย่างต่อเนื่องทำให้การใช้งานโปรแกรมเกิดขัดข้องและไม่สะดวกแก่ผู้ใช้งานและผู้รับบริการ สำนักบริหาร โดย กลุ่มเทคโนโลยีสารสนเทศซึ่งมีหน้าที่หลักในการดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ จึงจำเป็นต้องมีการปรับปรุงระบบสารสนเทศ และวางแนวทางการเชื่อมโยงระบบสารสนเทศอย่างต่อเนื่อง ได้เล็งเห็นความจำเป็นในการจัดหาผู้ดูแลระบบที่มีความเชี่ยวชาญเป็นที่ปรึกษาให้ความรู้แก่บุคลากร และผู้รับบริการตลอดจนบำรุงรักษาโปรแกรมคอมพิวเตอร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ และมีการพัฒนาระบบโปรแกรมให้สอดคล้องกับการเปลี่ยนแปลงที่เกิดขึ้นในปัจจุบัน และอนาคต

**ตารางที่ ๔** ระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ

| ลำดับ | ระบบงาน | หน่วยงานเจ้าของระบบ | URL |
|---|---|---|---|
| ๑ | Website บันทึกข้อมูลการรับบริการของประชาชน | กองสนับสนุนสุขภาพภาคประชาชน | http://203.157.7.124/identity_card/ |
| ๒ | ระบบทะเบียนอาสาสมัครชุมชน | กองสนับสนุนสุขภาพภาคประชาชน | http://www.thaiphc.net |
| ๓ | ระบบข้อมูลอาสาสมัครประจำครอบครัว | กองสนับสนุนสุขภาพภาคประชาชน | http://phc.fv.hss.moph.go.th |
| ๔ | ระบบเก็บข้อมูลองค์กรเอกชนสาธารณประโยชน์ | กองสนับสนุนสุขภาพภาคประชาชน | http://ngo.hss.moph.go.th/ |
| ๕ | ระบบคลังข้อมูลสุขภาพกรมสนับสนุนบริการสุขภาพ | กองสุขศึกษา | http://healthydee.moph.go.th |
| ๖ | ระบบคลังภาพ | กองสุขศึกษา | http://shutterstock.hss.moph.go.th |
| ๗ | ระบบทะเบียนข้อมูลแบบแปลนก่อสร้าง | กองแบบแผน | http://dcd.hss.moph.go.th/ |
| ๘ | ระบบการขอตั้งครรภ์แทน | สำนักสถานพยาบาลและการประกอบโรคศิลปะ | http:// 203.157.7.38 |
| ๙ | ระบบออกตรวจสถานพยาบาลเอกชน | สำนักสถานพยาบาลและการประกอบโรคศิลปะ | (Mobile App) |
| ๑๐ | Website One Stop Service | สำนักสถานพยาบาลและการประกอบโรคศิลปะ | http://bo.mrd.hss.moph.go.th |
| ๑๑ | ระบบตรวจสอบคลินิค/สถานพยาบาลเอกชน | สำนักสถานพยาบาลและการประกอบโรคศิลปะ | http://privatehospital.hss.moph.go.th |
| ๑๒ | ระบบข้อมูลสารสนเทศเพื่อการคุ้มครองผู้บริโภคด้านบริการสุขภาพภาคเอกชน | สำนักสถานพยาบาลและการประกอบโรคศิลปะ | http://privatehospital.hss.moph.go.th |

| ลำดับ | ระบบงาน | หน่วยงานเจ้าของระบบ | URL |
|---|---|---|---|
| ๑๓ | ระบบข้อมูลผู้ดำเนินการและผู้ให้บริการสถานบริการส่งเสริมสุขภาพ | กองสถานประกอบการเพื่อสุขภาพ | http://spa.hss.moph.go.th/ |
| ๑๔ | ระบบออกใบอนุญาตผู้ประกอบการสถานบริการส่งเสริมสุขภาพ | กองสถานประกอบการเพื่อสุขภาพ | http://spa.hss.moph.go.th/ |
| ๑๕ | ระบบข้อมูลสถาบันโรงเรียนสอนหลักสูตรมาตรฐานด้านบริการส่งเสริมสุขภาพ | กองสถานประกอบการเพื่อสุขภาพ | http://spa.hss.moph.go.th/ |
| ๑๖ | ระบบ Web Portal (Medical Hub Thailand) | กองสุขภาพระหว่างประเทศ | http://www.thailandmedicalhub.net |
| ๑๗ | ระบบโปรแกรม Call Center | กองสุขภาพระหว่างประเทศ | Call Center Application |
| ๑๘ | Website QR Code | กองสุขภาพระหว่างประเทศ | https://www.thailandmedicalhub.net/qrcode |
| ๑๙ | Website กลุ่มตรวจสอบภายใน | กลุ่มตรวจสอบภายใน | http://203.157.7.98/audit/ |
| ๒๐ | ระบบ Cockpit กพร. | กลุ่มพัฒนาระบบบริหาร | http://smart.hss.moph.go.th/61/kpi_report2/ |
| ๒๑ | Website สำนักบริหาร | สำนักบริหาร | http://admin.hss.moph.go.th/ |
| ๒๒ | Website กลุ่มงานคลัง | กลุ่มงานคลัง | http://203.157.7.98/store/ |
| ๒๓ | Website กลุ่มบริหารทรัพยากรบุคคล | กลุ่มบริหารทรัพยากรบุคคล | http://hr2.hss.moph.go.th |
| ๒๔ | Website บอร์ดปรึกษาเรื่องกฎหมาย | กองกฎหมาย | http://hss.moph.go.th/law/webboard/ |
| ๒๕ | ระบบรับเรื่องร้องเรียน | กองกฎหมาย | http://crm.hss.moph.go.th/ |
| ๒๖ | Website กลุ่มงานคุ้มครองจริยธรรม | กลุ่มงานคุ้มครองจริยธรรม | http://203.157.7.98/et/ |
| ๒๗ | ระบบบริหารจัดการเว็บไซต์และหน่วยงานในสังกัด กรมสนับสนุนบริการสุขภาพ | กลุ่มเทคโนโลยีสารสนเทศ | http://hss.moph.go.th |
| ๒๘ | ระบบโปรแกรมทะเบียนสินทรัพย์ กรมสนับสนุนบริการสุขภาพ | กลุ่มเทคโนโลยีสารสนเทศ | http://asset.hss.moph.go.th/ |
| ๒๙ | ระบบบริหารแผนงานและงบประมาณ กรมสนับสนุนบริการสุขภาพ (SMART) | กลุ่มเทคโนโลยีสารสนเทศ | http://smart.hss.moph.go.th/ |

| ลำดับ | ระบบงาน | หน่วยงานเจ้าของระบบ | URL |
|---|---|---|---|
| ๓๐ | ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ กรมสนับสนุนบริการสุขภาพ | กลุ่มเทคโนโลยีสารสนเทศ | http://manage.hss.moph.go.th/ |
| ๓๑ | ระบบข้อมูลอัตราค่ารักษาพยาบาลโรงพยาบาลเอกชน | กลุ่มเทคโนโลยีสารสนเทศ | http://hospitalprice.net |
| ๓๒ | ระบบคลังข้อมูล กรมสนับสนุนบริการสุขภาพ | กลุ่มเทคโนโลยีสารสนเทศ | http://dwh2.hss.moph.go.th |
| ๓๓ | ระบบบันทึกงาน Service เจ้าหน้าที่ (Smart Office) | กลุ่มเทคโนโลยีสารสนเทศ | http://203.157.7.16 |
| ๓๔ | Website ร้องเรียน | กลุ่มเทคโนโลยีสารสนเทศ | http://crm.hss.moph.go.th/ |
| ๓๕ | Website ศูนย์ข้อมูลข่าวสารของราชการ | กลุ่มเทคโนโลยีสารสนเทศ | http://hss.moph.go.th/info_act/ |
| ๓๖ | Website หน่วยงาน IT | กลุ่มเทคโนโลยีสารสนเทศ | http://it.hss.moph.go.th |
| ๓๗ | ระบบแบบสอบถามสิทธิประโยชน์ของพนักงานราชการ | กลุ่มเทคโนโลยีสารสนเทศ | http://hr2.hss.moph.go.th/qnform/ |
| ๓๘ | Website ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคเหนือ จังหวัดนครสวรรค์ | ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคเหนือ จังหวัดนครสวรรค์ | http://stb1.hss.moph.go.th:8080 |
| ๓๙ | Website ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี | ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี | http://stb2.hss.moph.go.th:8080 |
| ๔๐ | Website ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น | ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคตะวันออกเฉียงเหนือ จังหวัดขอนแก่น | http://stb3.hss.moph.go.th:8080 |
| ๔๑ | Website ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคใต้ จังหวัดนครศรีธรรมราช | ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคใต้ จังหวัดนครศรีธรรมราช | http://stb4.hss.moph.go.th:8080 |
| ๔๒ | Website ศูนย์พัฒนาการสาธารณสุขมูลฐานชายแดนภาคใต้ จังหวัดยะลา | ศูนย์พัฒนาการสาธารณสุขมูลฐานชายแดนภาคใต้ จังหวัดยะลา | http://stb5.hss.moph.go.th:8080 |

## สถานภาพบุคลากรด้าน สารสนเทศ

กรอบอัตรากำลังบุคลากร ด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ปัจจุบันมีจำนวน ๒๕ อัตรา ประกอบด้วยนักเทคโนโลยีสารสนเทศ จำนวน ๑ คน และนักวิชาการคอมพิวเตอร์ จำนวน ๑๙ คน[๒] ประกอบด้วยข้าราชการ จำนวน ๔ คน และพนักงานราชการ จำนวน ๑๖ คน รวมทั้งการจ้างเหมาบุคลากรภายนอก จำนวน ๕ คน โดยบุคลากรด้านระบบเทคโนโลยีสารสนเทศ มีทักษะ ความรู้ความสามารถในการปฏิบัติงานด้านระบบเทคโนโลยีสารสนเทศ แต่เนื่องจากกรอบอัตรากำลังบุคลากรด้านระบบเทคโนโลยีสารสนเทศในปัจจุบันไม่เพียงพอต่อการขับเคลื่อนระบบงาน จึงจำเป็นต้องมีบุคลากรด้านอื่นร่วมปฏิบัติงาน เพื่อให้เกิดความคล่องตัวในการปฏิบัติงาน เช่น นักวิเคราะห์นโยบายและแผน นักวิชาการสาธารณสุข นักวิชาการตรวจสอบภายใน เป็นต้น จำนวน ๔๙ คน รองรับภาระงานด้านระบบเทคโนโลยีสารสนเทศ เพื่อขับเคลื่อนระบบงานตามนโยบายของกรมสนับสนุนบริการสุขภาพ ตามตารางที่ ๕

[๒] ข้อมูล ณ วันที่ ๑๑ สิงหาคม ๒๕๖๓ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมสนับสนุนบริการสุขภาพ ปีงบประมาณ ๒๕๖๓

**ตารางที่ ๕ แสดงข้อมูลเบื้องต้นบุคลากรด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข [ข้อมูล ณ วันที่ ๑๑ สิงหาคม ๒๕๖๓]**

| ลำดับ | ตำแหน่ง | จำนวน (คน) | คุณวุฒิ | | | | วุฒิบัตรด้าน IT/IS | | | User | SysAdmin |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ปกศ. | ป.ตรี | ป.โท | ป.เอก | ITPE | IS | CCNA/ CSSP | | |
| IT00001 | กลุ่ม IT | 25 | 0 | 22 | 3 | 0 | 1 | 1 | 0 | 0 | 25 |
| IT0011-0101 | นักวิชาการคอมพิวเตอร์ปฏิบัติการ | 2 | | 1 | 1 | | | 1 | | | 2 |
| IT0011-0102 | นักวิชาการคอมพิวเตอร์ชำนาญการ | 1 | | | 1 | | 1 | | | | 1 |
| IT0011-0103 | นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ | | | | | | | | | | |
| IT0011-0104 | นักวิชาการคอมพิวเตอร์ | 16 | | 15 | 1 | | | | | | 16 |
| IT0011-0201 | ปฏิบัติงานด้านคอมพิวเตอร์ | 5 | | 5 | | | | | | | 5 |
| | | | | | | | | | | | |
| IT0012-0101 | นักเทคโนโลยีสารสนเทศปฏิบัติการ | | | | | | | | | | |
| IT0012-0102 | นักเทคโนโลยีสารสนเทศชำนาญการ | | | | | | | | | | |
| IT0012-0103 | นักเทคโนโลยีสารสนเทศชำนาญการพิเศษ | 1 | | 1 | | | | | | | 1 |
| IT0012-0201 | นักเทคโนโลยีสารสนเทศ | | | | | | | | | | |
| IT0012-0401 | ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ | | | | | | | | | | 1 |
| | | | | | | | | | | | |
| IT00002 | กลุ่ม non IT | 50 | 0 | 46 | 3 | 1 | 1 | 1 | 0 | 37 | 13 |
| | **ผู้บริหาร** | | | | | | | | | | |
| IT0021-0101 | อธิบดีกรมสนับสนุนบริการสุขภาพ | 1 | | | 1 | | | | | 1 | |
| IT0021-0102 | รองอธิบดีกรมสนับสนุนบริการสุขภาพ (CIO) | 1 | | | | 1 | 1 | | | 1 | |
| IT0021-0103 | รองอธิบดีกรมสนับสนุนบริการสุขภาพ (CFO) | | | | | | | | | 1 | |
| IT0021-0104 | รองอธิบดีกรมสนับสนุนบริการสุขภาพ (CMO) | | | | | | | | | 1 | |

| ลำดับ | ตำแหน่ง | จำนวน (คน) | คุณวุฒิ | | | | วุฒิบัตรด้าน IT/IS | | | User | SysAdmin |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ปกศ. | ป.ตรี | ป.โท | ป.เอก | ITPE | IS | CCNA/ CSSP | | |
| IT00002 | กลุ่ม non IT | 50 | 0 | 46 | 3 | 1 | 1 | 1 | 0 | 37 | 13 |
| IT0021-0105 | ผู้อำนวยการ (32) | | | | | | | | | | |
| IT0021-0106 | หัวหน้างาน (2) | | | | | | | | | | |
| | บุคลากร | | | | | | | | | | |
| IT0022-0201 | เจ้าพนักงานโสตทัศนศึกษาปฏิบัติงาน | | | | | | | | | | |
| IT0022-0202 | เจ้าพนักงานโสตทัศนศึกษาชำนาญงาน | 1 | | 1 | | | | | | 1 | |
| IT0022-0301 | เจ้าพนักงานโสตทัศนศึกษา | | | | | | | | | | |
| IT0022-0101 | นักวิชาการโสตทัศนศึกษาปฏิบัติการ | 1 | | 1 | | | | | | 1 | |
| IT0022-0102 | นักวิชาการโสตทัศนศึกษาชำนาญการ | 1 | | 1 | | | | | | | 1 |
| | | | | | | | | | | | |
| IT0023-0201 | เจ้าพนักงานธุรการปฏิบัติงาน | 2 | | 2 | | | | | | 2 | |
| IT0023-0202 | เจ้าพนักงานธุรการชำนาญงาน | 1 | | 1 | | | | | | 1 | |
| | | | | | | | | | | | |
| IT0024-0201 | เจ้าพนักงานการเงินปฏิบัติงาน | 1 | | 1 | | | | | | 1 | |
| | | | | | | | | | | | |
| IT0025-0202 | เจ้าพนักงานพัสดุชำนาญงาน | 1 | | 1 | | | | | | 1 | |
| | | | | | | | | | | | |
| IT0026-0102 | นักจัดการงานทั่วไปชำนาญการ | 1 | | 1 | | | | | | 1 | |
| IT0026-0301 | นักจัดการงานทั่วไป | 1 | | 1 | | | | | | 1 | |
| | | | | | | | | | | | |

| ลำดับ | ตำแหน่ง | จำนวน (คน) | คุณวุฒิ | | | | วุฒิบัตรด้าน IT/IS | | | User | SysAdmin |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ปกศ. | ป.ตรี | ป.โท | ป.เอก | ITPE | IS | CCNA/ CSSP | | |
| IT00002 | กลุ่ม non IT | 50 | 0 | 46 | 3 | 1 | 1 | 1 | 0 | 37 | 13 |
| IT0027-0101 | นักทรัพยากรบุคคลปฏิบัติการ | 2 | | 2 | | | | | | 2 | |
| IT0027-0102 | นักทรัพยากรบุคคลชำนาญการ | | | | | | | | | | |
| IT0027-0103 | นักทรัพยากรบุคคลชำนาญการพิเศษ | 1 | | 1 | | | | | | 1 | |
| IT0027-0301 | นักทรัพยากรบุคคล | 1 | | 1 | | | | | | 1 | |
| | | | | | | | | | | | |
| IT0028-0101 | นักวิเคราะห์นโยบายและแผนปฏิบัติการ | 1 | | 1 | | | | | | 1 | |
| IT0028-0102 | นักวิเคราะห์นโยบายและแผนชำนาญการ | 2 | | 2 | | | | | | 2 | |
| IT0028-0103 | นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ | 1 | | 1 | | | | | | 1 | |
| IT0028-0301 | นักวิเคราะห์นโยบายและแผน | 2 | | 2 | | | | | | 2 | |
| | | | | | | | | | | | |
| IT0029-0103 | นักวิชาการเผยแพร่ชำนาญการพิเศษ | 1 | | 1 | | | | | | 1 | |
| | | | | | | | | | | | |
| IT0030-0103 | นักวิชาการตรวจสอบภายในชำนาญการพิเศษ | 1 | | 1 | | | | | | | 1 |
| | | | | | | | | | | | |
| IT0031-0101 | นักวิชาการสาธารณสุขปฏิบัติการ | 1 | | 1 | | | | | | 1 | |
| IT0031-0102 | นักวิชาการสาธารณสุขชำนาญการ | 4 | | 3 | 1 | | 1 | 1 | | 2 | 2 |
| IT0031-0103 | นักวิชาการสาธารณสุขชำนาญการพิเศษ | | | | | | | | | | |
| IT0031-0301 | นักวิชาการสาธารณสุข | 1 | | 1 | | | | | | 1 | |
| | | | | | | | | | | | |

| ลำดับ | ตำแหน่ง | จำนวน (คน) | คุณวุฒิ | | | | วุฒิบัตรด้าน IT/IS | | | User | SysAdmin |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ปกศ. | ป.ตรี | ป.โท | ป.เอก | ITPE | IS | CCNA/ CSSP | | |
| IT00002 | กลุ่ม non IT | 50 | 0 | 46 | 3 | 1 | 1 | 1 | 0 | 37 | 13 |
| IT0041-0201 | นายช่างเทคนิคปฏิบัติงาน | 1 | | 1 | | | | | | | 1 |
| IT0041-0202 | นายช่างเทคนิคชำนาญงาน | 3 | | 3 | | | | | | 1 | 2 |
| IT0041-0203 | นายช่างเทคนิคอาวุโส | 1 | | 1 | | | | | | | 1 |
| | | | | | | | | | | | |
| IT0051-0201 | นายช่างไฟฟ้าปฏิบัติงาน | 1 | | 1 | | | | | | | 1 |
| IT0051-0202 | นายช่างไฟฟ้าชำนาญงาน | 1 | | 1 | | | | | | | 1 |
| IT0041-0001 | ช่างฝีมือโรงงาน | 1 | | 1 | | | | | | | 1 |
| | | | | | | | | | | | |
| IT0052-0602 | วิศวกรโยธาชำนาญการ | 1 | | 1 | | | | | | | 1 |
| | | | | | | | | | | | |
| IT1000-0001 | อื่นๆ | 11 | | 11 | | | | | | 10 | 1 |
| รวมบุคลากรด้าน IT/ปฏิบัติงานด้าน IT | | 74 | 0 | 67 | 6 | 1 | 2 | 2 | 0 | 37 | 37 |

# บทที่ ๔

## แนวทางการบริหารความเสี่ยงด้านสารสนเทศ

### ๔.๑ แนวทางการดำเนินการบริหารความเสี่ยงด้านสารสนเทศ

แนวทางการดำเนินการบริหารความเสี่ยงด้านสารสนเทศ จำแนกได้เป็น ๗ ขั้นตอน ดังนี้

**ขั้นตอนที่ ๑** การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
- แต่งตั้งคณะทำงานบริหารความเสี่ยงด้านสารสนเทศ
- กำหนดนโยบายหรือแนวทางในการบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๒** การระบุความเสี่ยง (Event Identification)
- การวิเคราะห์ความเสี่ยงและระบุปัจจัยความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๓** การประเมินความเสี่ยง (Risk Assessment)
- การประเมินความเสี่ยงด้านสารสนเทศ จากการดำเนินงานเบื้องต้น
- การจัดลำดับความสำคัญปัจจัยเสี่ยงด้านสารสนเทศ จากการดำเนินงานเบื้องต้น

**ขั้นตอนที่ ๔** กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
- จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๕** กิจกรรมการบริหารความเสี่ยง (Control Activity)
- กำหนดกิจกรรมการบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๖** ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
- การสื่อสารทำความเข้าใจเกี่ยวกับแผนความเสี่ยงด้านสารสนเทศให้บุคลากรที่เกี่ยวข้องรับทราบ สามารถนำไปปฏิบัติได้
- รายงานความก้าวหน้าของการดำเนินงานตามแผนบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๗** การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)
- เสนอแนะเพื่อการปรับปรุงแผนบริหารความเสี่ยงด้านสารสนเทศ
- พัฒนากระบวนการบริหารความเสี่ยงด้านสารสนเทศ
- ผลักดันให้มีการบริหารความเสี่ยงด้านสารสนเทศทั่วทั้งหน่วยงาน
- พัฒนาขีดความสามารถของบุคลากรในการดำเนินงานตามกระบวนการบริหารความเสี่ยงด้านสารสนเทศ

### ๔.๒ การบริหารความเสี่ยงด้านสารสนเทศ

ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายและมาตรฐานสากล (NIST : National Institute of Standard and Technology) ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพ

กรมสนับสนุนบริการสุขภาพ มีภารกิจการคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพและส่งเสริมผู้ประกอบการด้านบริการสุขภาพเพื่อประชาชนมีศักยภาพในการพึ่งพาตนเอง มีระบบขึ้นทะเบียนและออกใบอนุญาตสถานพยาบาลและสถานประกอบการเพื่อสุขภาพ เป็นหน่วยงานที่เกี่ยวข้องกับการเก็บรักษาข้อมูลส่วนบุคคล ด้านธุรกิจบริการสุขภาพรองรับการดำเนินงานระหว่างภาครัฐและเอกชน ที่สนับสนุนการทำธุรกรรมอิเล็กทรอนิกส์ด้านระบบบริการสุขภาพทั้งภายในและต่างประเทศ การพัฒนานวัตกรรมดิจิทัลด้านระบบบริการสุขภาพตามนโยบายเศรษฐกิจ

ดิจิทัล (Digital Economy) และภารกิจในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) ที่มีผลกระทบต่อประชาชนโดยตรง จากการเชื่อมโยงข้อมูลกับหน่วยงานที่เกี่ยวข้อง ควรต้องผ่านเกณฑ์มาตรฐานเพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการในระบบบริการสุขภาพรวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ รวมทั้งการบริหารราชการของกรมสนับสนุนบริการสุขภาพ ด้านขับเคลื่อนการพัฒนารัฐบาลดิจิทัล (Digital Government)

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศ อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และสารสนเทศรวมถึงข้อมูลสารสนเทศ ใน ๓ ด้านดังนี้

๑. ความเสี่ยงที่เกิดจากบุคคล (People)

๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process)

๓. ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology)

**๔.๓ นโยบาย วัตถุประสงค์การบริหารความเสี่ยงด้านสารสนเทศ**

**๔.๓.๑ นโยบายการบริหารความเสี่ยงด้านสารสนเทศ**

เพื่อให้กรมสนับสนุนบริการสุขภาพ มีการบริหารความเสี่ยงด้านสารสนเทศ โดยการบริหารปัจจัยเสี่ยงควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อลดมูลเหตุของแต่ละโอกาสที่จะเกิดความเสียหาย ให้ระดับความเสี่ยงและขนาดของความเสี่ยงที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงการบรรลุเป้าหมาย ตามยุทธศาสตร์ที่สำคัญ จึงกำหนดนโยบายการบริหารความเสี่ยงด้านสารสนเทศ ดังนี้

๑. จัดให้มีระบบ และกระบวนการบริหารความเสี่ยงด้านสารสนเทศ โดยมีเอกสารแสดงแนวทางและระบุปัจจัยเสี่ยงด้านสารสนเทศ

๒. การบริหารความเสี่ยงด้านสารสนเทศ จะต้องครอบคลุมทุกหน่วยงานภายในกรมสนับสนุนบริการสุขภาพทั้งที่มีสาเหตุจากปัจจัยภายในและปัจจัยภายนอก เพื่อช่วยให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพ และประสิทธิผล

๓. ให้ทุกหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ รวมทั้งผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เข้าใจและให้ความสำคัญกับการบ่งชี้และการควบคุมความเสี่ยง มีวิธีการ และแนวทางการปฏิบัติงานที่เป็นแนวทางเดียวกันในการประเมิน และการจัดการความเสี่ยงด้านสารสนเทศ

๔. ให้มีการกำหนดกระบวนการบริหารความเสี่ยงด้านสารสนเทศที่เป็นมาตรฐานเดียวกันทั้งองค์กร

๕. ให้มีการบริหารจัดการข้อมูลที่ดี (Data Governance) ตามนโยบายรัฐบาลดิจิทัล (Digital Government)

๖. ให้นำการบริหารความเสี่ยงด้านสารสนเทศไปปฏิบัติให้เป็นส่วนหนึ่งของภารกิจ จนเกิดเป็นวัฒนธรรมองค์กร และเป็นส่วนหนึ่งของการดำเนินงานตามปกติ

๗. ให้มีการติดตามและประเมินผลการบริหารความเสี่ยง มีการทบทวน และปรับปรุงอย่างสม่ำเสมอ

**๔.๓.๒ วัตถุประสงค์การบริหารความเสี่ยงด้านสารสนเทศ**

๑. เพื่อช่วยเพิ่มประสิทธิภาพของการตัดสินใจ โดยคำนึงถึงปัจจัยและความเสี่ยงด้านสารสนเทศ ที่มีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้นก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินการตามแผนที่กำหนดไว้

๒. เพื่อให้กรมสนับสนุนบริการสุขภาพ สามารถลดมูลเหตุของโอกาสที่จะเกิดความเสียหาย และลดขนาดของความเสียหายที่จะเกิดในอนาคตให้อยู่ในระดับความเสี่ยงด้านสารสนเทศที่ยอมรับได้ ควบคุมได้ และตรวจสอบได้

๓. เพื่อให้กรมสนับสนุนบริการสุขภาพ มีผลการดำเนินงานบรรลุเป้าหมายตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ

# บทที่ ๕

## แผนการบริหารความเสี่ยงด้านสารสนเทศ

### ๕.๑ การบริหารความเสี่ยงด้านสารสนเทศ

การบริหารความเสี่ยง เป็นกลยุทธ์ในการดำเนินงานเพื่อขับเคลื่อนองค์กรไปสู่การบริหารแบบบูรณาการอย่างมีคุณค่า (Business Integrity) และการมีคุณธรรมในการบริหาร เช่น การกำหนดกฎเกณฑ์ ระเบียบคำสั่ง การปฏิบัติ การให้คุณให้โทษ เป็นปัจจัยสำคัญ “ที่ผู้บริหารต้องใช้ในการขับเคลื่อนการดำเนินงานเชิงรุก” มีการปฏิบัติการที่มีศักยภาพยั่งยืน ด้วยการเข้าสู่ “การบริหารจัดการความเสี่ยง”

**ขั้นตอนที่ ๑** การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
- แต่งตั้งคณะทำงานบริหารความเสี่ยงด้านสารสนเทศ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม
- กำหนดนโยบายหรือแนวทางในการบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๒** การระบุความเสี่ยง (Event Identification)
- การวิเคราะห์ความเสี่ยงและระบุปัจจัยความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๓** การประเมินความเสี่ยง (Risk Assessment)
- การประเมินความเสี่ยงด้านสารสนเทศ จากการดำเนินงานเบื้องต้น
- การจัดลำดับความสำคัญปัจจัยเสี่ยงด้านสารสนเทศ จากการดำเนินงานเบื้องต้น

**ขั้นตอนที่ ๔** กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
- จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๕** กิจกรรมการบริหารความเสี่ยง (Control Activity)
- กำหนดกิจกรรมการบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๖** ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
- การสื่อสารทำความเข้าใจเกี่ยวกับแผนความเสี่ยงด้านสารสนเทศให้บุคลากรที่เกี่ยวข้องรับทราบ สามารถนำไปปฏิบัติได้
- รายงานความก้าวหน้าของการดำเนินงานตามแผนบริหารความเสี่ยงด้านสารสนเทศ

**ขั้นตอนที่ ๗** การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)
- เสนอแนะเพื่อการปรับปรุงแผนบริหารความเสี่ยงด้านสารสนเทศ
- พัฒนากระบวนการบริหารความเสี่ยงด้านสารสนเทศ
- ผลักดันให้มีการบริหารความเสี่ยงด้านสารสนเทศทั่วทั้งหน่วยงาน
- พัฒนาขีดความสามารถของบุคลากรในการดำเนินงานตามกระบวนการบริหารความเสี่ยงด้านสารสนเทศ

### ๕.๒ ผลการบริหารความเสี่ยงด้านสารสนเทศ

ในปี พ.ศ. ๒๕๖๒ – ๒๕๖๓ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม ได้ดำเนินการวิเคราะห์และจัดทำแผนบริหารความเสี่ยงด้านสารสนเทศ เพื่อรองรับสภาวะการเปลี่ยนแปลงที่จะเกิดขึ้นตามประเด็นผลกระทบสูงต่อการบรรลุความสำเร็จของการดำเนินงานตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ มีการดำเนินงานดังนี้

**ขั้นตอนที่ ๑ การกำหนดเป้าหมายการบริหารความเสี่ยง**

๑.๑ การศึกษา วิเคราะห์ รวบรวม ข้อมูลสถานการณ์สภาพแวดล้อมของการสร้างความเชื่อมั่นในการเข้าถึงข้อมูลด้านระบบบริการสุขภาพตามแนวทางการประเมินระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ ใน ๑๔ ประเด็น ตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งกฎหมายที่เกี่ยวข้องและมาตรฐานสากล เช่น NIST (National Institute of Standard and Technology)

๑.๒ 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)

๑.๓ ภายนอกขอบเขต Server & Network (HSS Net)

๑) ระบบงาน ที่ไม่เกี่ยวข้องกับระบบงานของกรมสนับสนุนบริการสุขภาพ (HSS Net)

๒) เครือข่ายคอมพิวเตอร์ระหว่างผู้ใช้บริการที่ไม่เกี่ยวข้องกับระบบงานของกรมสนับสนุนบริการสุขภาพที่กำกับดูแลโดยผู้ให้บริการภายนอกองค์กร

๑.๔ การแต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับกรม กรมสนับสนุนบริการสุขภาพ[๑] ให้สอดคล้องตามภารกิจการขับเคลื่อนกรมสนับสนุนบริการสู่การเป็นรัฐบาลดิจิทัล (Digital Government)

๑.๕ การแต่งตั้งคณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ[๒]

๑.๖ การจัดทำแผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ - ๒๕๖๖[๓] ได้กำหนดงานที่ต้องผ่านการประเมิน มาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓[๔] คือ

๑.๖.๑ ศูนย์กลางข้อมูลด้านระบบบริการสุขภาพ (DC : Data Center) ตั้งอยู่ที่ ชั้น ๒ อาคารกรมสนับสนุนบริการสุขภาพ โดยได้กำหนดให้ประเมินผ่านมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ภายในปี ๒๕๖๔

๑.๖.๒ ศูนย์สำรองข้อมูล (DR Site : Data Recovery Center) ตั้งอยู่ที่ศูนย์พัฒนาการสาธารณสุขมูลฐาน ภาคตะวันออก จังหวัดชลบุรี โดยได้กำหนดให้ประเมินผ่านมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ภายในปี ๒๕๖๔

๑.๖.๓ ศูนย์บริการแบบเบ็ดเสร็จ (OSS : One Stop Service) ตั้งอยู่ที่ ชั้น ๑ อาคารกรมสนับสนุนบริการสุขภาพ โดยได้กำหนดให้ประเมินผ่านมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ภายในปี ๒๕๖๕

๑.๖.๔ ศูนย์ข้อมูลด้านระบบบริการสุขภาพ (Server Room ๑ – ๑๒) ตั้งอยู่ใน ๑๒ ภูมิภาค โดยได้กำหนดให้ประเมินผ่านมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ภายในปี ๒๕๖๖

---

[๑] คำสั่งกรมสนับสนุนบริการสุขภาพ ที่ ๘๕๑/๒๕๖๓ ลงวันที่ ๑๒ พฤษภาคม ๒๕๖๓

[๒] คำสั่งกรมสนับสนุนบริการสุขภาพ ที่ ๑๒๓๑/๒๕๖๓ ลงวันที่ ๒๖ มิถุนายน ๒๕๖๓

[๓] อยู่ระหว่างเสนออนุมัติ (๑๗ สิงหาคม ๒๕๖๓)

[๔] ขึ้นกับงบประมาณที่ได้รับการจัดสรร

๑.๗ การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓ (ฉบับปรับปรุง ครั้งที่ ๑) อยู่ระหว่างเสนอสำนักงานพัฒนาธุกรรมอิเล็กทรอนิกส์ พิจารณา (วันที่ ๙ มิถุนายน ๒๕๖๓)

๑.๘ การจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓ (ฉบับปรับปรุง ครั้งที่ ๑) อยู่ระหว่างเสนอสำนักงานพัฒนาธุกรรมอิเล็กทรอนิกส์ พิจารณา (เมื่อวันที่ ๙ มิถุนายน ๒๕๖๓)

**ขั้นตอนที่ ๒ ระบุความเสี่ยงด้านสารสนเทศ**

การระบุความเสี่ยงด้านสารสนเทศ สามารถจัดหมวดหมู่ว่าด้วยความมั่นคงปลอดภัยสำหรับข้อมูลและระบบข้อมูล (Based on security objectives)[๕] ตามการจัดหมวดหมู่ความปลอดภัย (CIA) ประกอบด้วยการรักษาความลับ (Confidentiality) ความสมบูรณ์ถูกต้อง ครบถ้วน (Integrity) และความรุนแรงที่ส่งผลกระทบต่อความพร้อมในการใช้งาน (Availability) ตามแผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๖ ในประเด็นต่างๆ ดังนี้

๒.๑ นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policies)

๒.๒ โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Security)

๒.๓ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

๒.๔ การบริหารจัดการทรัพย์สินขององค์กร (asset Management)

๒.๕ การควบคุมการเข้าถึง (Access Control)

๒.๖ การเข้ารหัสข้อมูล (Cryptography)

๒.๗ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๒.๘ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านการดำเนินการ (Operation Security)

๒.๙ ความมั่นคงปลอดภัยด้านการสื่อสาร (Communication Security)

๒.๑๐ การจัดหา การพัฒนาและการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

๒.๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

๒.๑๒ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)

๒.๑๓ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

๒.๑๔ การปฏิบัติตามข้อกำหนด (Compliance)

**ขั้นตอนที่ ๓ การประเมินความเสี่ยงด้านสารสนเทศ**

๑. ประเมินตามระดับของผลกระทบ หากมีการละเมิดความปลอดภัย (Level of impact if a security breach)

๑.๑ ระดับต่ำ (Low) ผลกระทบที่จำกัดต่อการดำเนินงานขององค์กร สินทรัพย์องค์กรหรือบุคคล (a limited adverse effect on organizational operations, organizational assets, or individuals)

๑.๒ ระดับปานกลาง (Moderate) ผลกระทบร้ายแรงต่อการดำเนินงานขององค์กร สินทรัพย์ขององค์กรหรือบุคคล (serious adverse effect on organizational operations, organizational assets, or individuals)

๑.๓ ระดับสูง (High) ผลกระทบรุนแรงหรือเป็นความหายนะต่อการดำเนินงานขององค์กรสินทรัพย์ขององค์กรหรือบุคคล (a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals)

๒. ประเมินจากบริการที่สำคัญ

[5] ENISA: European Union Agency for Network and Information Security Agency,2014

๒.๑ พิจารณาจากขอบเขตของผลกระทบ

๒.๒ พิจารณาจากผลกระทบหรือระดับความรุนแรงที่จะตามมา

๒.๓ พิจารณาจากระยะเวลาที่กระทบต่อการให้บริการ.

รายละเอียด ดังตารางที่ ๗

**ตารางที่ ๗** ปัจจัยและเกณฑ์การคัดเลือกบริการที่สำคัญ (Critical Service)

| ปัจจัย | ผลกระทบระดับต่ำ | ผลกระทบระดับกลาง | ผลกระทบระดับสูง | ผลการประเมิน |
|---|---|---|---|---|
| ๑. ผลกระทบต่อประชาชน | ไม่มีผู้ใช้บริการได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย | ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย > ๑ คน ≤ ๑,๐๐๐ คน | ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย > ๑,๐๐๐ คน หรือ ต่อชีวิตตั้งแต่ ๑ คน | |
| ๒. ผลกระทบเชิงความหนาแน่นของประชากร | กระทบต่อชีวิตหรือการปฏิบัติงานของประชาชน < ๑๐ % ของประชากรในพื้นที่ระดับจังหวัดหรือเขตบริหาร | กระทบต่อชีวิตหรือการปฏิบัติงานของประชาชน ๑๐% ≤ X ≤๓๐% ของประชากรในพื้นที่ระดับจังหวัด หรือเขตบริหาร | กระทบต่อชีวิตหรือการปฏิบัติงานของประชาชน > ๓๐% ของประชากรในพื้นที่ระดับจังหวัดหรือเขตบริหาร | |
| ๓. ผลกระทบทางเศรษฐกิจ | ≤ ๑ ล้านบาท | > ๑ ล้านบาท ≤ ๑๐๐ ล้านบาท | > ๑๐๐ ล้านบาท | |
| ๔. ผลกระทบต่อความเชื่อมั่นขององค์กรหรือต่อประเทศ | ไม่มีผลกระทบต่อภาพลักษณ์ขององค์กรหรือต่อประเทศ | เกิดผลกระทบต่อภาพลักษณ์ในระดับกลาง | เกิดผลกระทบรุนแรงต่อภาพลักษณ์ | |
| ๕. ผลกระทบด้านความสัมพันธ์ระหว่างประเทศ | เกิดผลกระทบระดับต่ำด้านความสัมพันธ์ระหว่างประเทศ | เกิดผลกระทบระดับกลางด้านความสัมพันธ์ระหว่างประเทศ | เกิดผลกระทบระดับรุนแรงด้านความสัมพันธ์ระหว่างประเทศ | |
| ๖. ผลกระทบต่อความสงบเรียบร้อยในสังคม | เกิดผลกระทบระดับต่ำต่อความสงบเรียบร้อยในสังคม หรือเป็นภัยต่อความมั่นคงของชาติ | เกิดผลกระทบระดับกลางต่อความสงบเรียบร้อยในสังคม หรือเป็นภัยต่อความมั่นคงของชาติ | เกิดผลกระทบรุนแรงต่อความสงบเรียบร้อยในสังคม หรือเป็นภัยต่อความมั่นคงของชาติ | |
| ๗. ผลกระทบต่อการดำเนินชีวิตประจำวันของประชาชน | กระทบต่อการใช้ชีวิตของประชาชน < ๑๐,๐๐๐ ราย | กระทบต่อการใช้ชีวิตของประชาชน ๑๐,๐๐๐ ≤ X ≤ ๑๐,๐๐๐ | กระทบต่อการใช้ชีวิตของประชาชน > ๑๐๐,๐๐๐ ราย | |
| ๘. ผลกระทบต่อ CII อื่น หรือ Sector อื่น | < ๓ บริการ | = ๓ | > ๓ บริการ | |
| ๙. ผลกระทบต่อสิ่งแวดล้อม | ไม่รุนแรง | รุนแรงปานกลาง | รุนแรงมาก | |

**ขั้นตอนที่ ๔ กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยงด้านสารสนเทศ**

๔.๑ หลักเกณฑ์การให้คะแนนโอกาสที่จะเกิดความเสียหาย (L) และความรุนแรงของผลกระทบ (C)

| ประเด็น/องค์ประกอบที่พิจารณา | | ระดับคะแนน | | | | |
|---|---|---|---|---|---|---|
| | | **๑=น้อยมาก** | **๒=น้อย** | **๓=ปานกลาง** | **๔=สูง** | **๕=สูงมาก** |
| **โอกาสที่จะเกิดความเสียหาย (Likelihood: L)** | | | | | | |
| - ระเบียบและคู่มือปฏิบัติ | L๑ | มีทั้ง ๒ อย่าง และ มีการปฏิบัติ | มีอย่างใดอย่างหนึ่งและ มีการปฏิบัติ | มีทั้ง ๒ อย่างแต่ปฏิบัติตาม อย่างใดอย่างหนึ่ง | มีอย่างใดอย่างหนึ่ง แต่ไม่ถือปฏิบัติ | ไม่มีทั้ง ๒ อย่างและ ไม่ถือปฏิบัติ |
| - การควบคุม ติดตาม และตรวจสอบของ ผู้บังคับบัญชาหรือหน่วยงานอื่น | L๒ | ๒ สัปดาห์ | ๑ เดือน | ๓ เดือน | ๖ เดือน | ≥ เท่ากับ ๑ ปี |
| - การอบรม/สอนงาน/ทบทวนการปฏิบัติงาน | L๓ | ทุกเดือน | ทุก ๓ เดือน | ทุก ๖ เดือน | ทุก ๑ ปี | มากกว่า ๑ ปี |
| - ความถี่ในการเกิด | L๔ | ๕ ปี/ครั้ง | ๒-๓ ปี/ครั้ง | ๑ ปี/ครั้ง | ๑-๖ เดือน/ครั้ง ไม่เกิน ๕ ครั้ง/ปี | ๑ เดือน/ครั้งหรือมากกว่า เกิดขึ้นแน่นอนตั้งแต่ ๒ ครั้ง/ปี ขึ้นไป |
| - โอกาสที่จะเกิดเหตุการณ์* | L๕ | น้อยที่สุด | น้อย | ปานกลาง | สูง | เกิดขึ้นแน่นอน |
| - ความถี่ในการเปลี่ยนแปลง | L๖ | ๔ ปี/ครั้ง | ๓ ปี/ครั้ง | ๒ ปี/ครั้ง | ๑ ปี/ครั้ง | ตั้งแต่ ๒ ครั้ง/ปีขึ้นไป |
| **ความรุนแรงของผลกระทบ (Consequent: C)** | | | | | | |
| - มูลค่าความเสียหาย | C๑ | < ๑ หมื่นบาท | ๑-๕ หมื่นบาท | ๕ หมื่น-๒.๕แสนบาท | ๒.๕ แสน-๑๐ ล้านบาท | > ๑๐ ล้านบาท |
| - อันตรายต่อชีวิต | C๒.๑ | เดือนร้อน | บาดเจ็บเล็กน้อย | บาดเจ็บต้องรักษาแพทย์ | บาดเจ็บสาหัส | |
| - ระดับความปลอดภัย | C๒.๒ | น้อยมาก | น้อย | ปานกลาง | สูง | สูงมาก |
| - ผลกระทบต่อภาพลักษณ์ | C๓.๑ | น้อยมาก | น้อย | ปานกลาง | สูง | สูงมาก |
| - ความพึงพอใจ | C๓.๒ | พึงพอใจ > ๘๐% | > ๖๐-๘๐% | > ๔๐-๖๐% | > ๒๐-๔๐% | ≤ เท่ากับ ๒๐% |
| - ข่าวสารจากสื่อในทางลบ | C๓.๓ | ๑ ข่าว/เดือน | ๒ ข่าว/เดือน | ๓ ข่าว/เดือน | ๔ ข่าว/เดือน | ≥ เท่ากับ ๕ ข่าว/เดือน |
| - ผู้รับบริการได้รับความเสียหาย หรือผู้ได้รับผลกระทบ* | C๔ | กระทบเฉพาะกลุ่ม ผู้เกี่ยวข้องโดยตรงบางราย | กระทบเฉพาะกลุ่ม ผู้เกี่ยวข้องโดยตรงเป็นส่วน ใหญ่ | กระทบเฉพาะกลุ่ม ผู้เกี่ยวข้องโดยตรงทั้งหมด | กระทบกลุ่มผู้เกี่ยวข้อง โดยตรงทั้งหมดและผู้อื่น บางส่วน | กระทบกลุ่มผู้เกี่ยวข้องโดยตรง ทั้งหมดและผู้อื่นมากราย |
| - จำนวนผู้ร้องเรียน | C๕ | น้อยกว่า ๑ราย (ต่อเดือน) | ๑-๒ ราย (ต่อเดือน) | ๓-๕ ราย (ต่อเดือน) | ๕-๖ ราย (ต่อเดือน) | ๗ รายขึ้นไป (ต่อเดือน) |

๔.๒ กลยุทธ์ที่ใช้สำหรับจัดการแต่ละความเสี่ยง มีดังนี้

| **กลยุทธ์จัดการความเสี่ยง** | **คำอธิบาย** |
|---|---|
| การหลีกเลี่ยงความเสี่ยง | - ปฏิเสธและหลีกเลี่ยงโอกาสที่จะเกิดความเสี่ยง โดยการหยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรม หรือโครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง |
| การควบคุมความเสี่ยง | - พยายามลดความเสี่ยงโดยการเพิ่มเติม หรือเปลี่ยนแปลงขั้นตอนบางส่วนของกิจกรรมหรือโครงการที่นำไปสู่เหตุการณ์ที่เป็นความเสี่ยง รวมถึงลดความน่าจะเป็นความเสี่ยงจะเกิดขึ้น |
| การรับความเสี่ยงไว้เอง | หากทำการวิเคราะห์แล้วเห็นว่าไม่มีวิธีการจัดการความเสี่ยงใดเลยที่เหมาะสม เนื่องจากต้นทุนการจัดการความเสี่ยงสูงกว่าประโยชน์ที่จะได้รับ อาจต้องยอมรับความเสี่ยง แต่ควรมีมาตรการติดตามอย่างใกล้ชิดเพื่อรองรับผลที่จะเกิดขึ้น |
| การถ่ายโอนความเสี่ยง | ยกภาระในการเผชิญหน้ากับเหตุการณ์ที่เป็นความ และการจัดการกับความเสี่ยงให้ผู้อื่น |

**ขั้นตอนที่ ๕ กิจกรรมการบริหารความเสี่ยงด้านสารสนเทศ**

๕.๑ นำความเสี่ยงที่ระบุ มาแยกประเภทของความเสี่ยงที่เกี่ยวข้องและวิเคราะห์หาปัจจัยเสี่ยง กลยุทธ์และแนวทางการจัดการความเสี่ยง

**ตารางที่ ๖** ตารางแสดงการประเมินความเสี่ยงด้านสารสนเทศ

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๑. ความเสี่ยงที่เกิดจากบุคคล (People) | | | | | | |
| ๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากรภายใน กรม สบส. | ๑.๑.๑ ระบบคอมพิวเตอร์ติด Virus, Malware ,Worm (หนอนอินเทอร์เน็ต) หรือ Ransomware หรือไฟล์ที่คัดลอกจากอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive หรือ External Hard disk, Storage ส่งผลให้ระบบคอมพิวเตอร์ และระบบสารสนเทศประมวลผลข้อมูลได้ช้าลง หรืออาจทำงานผิดพลาดได้ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | (๑) ผู้ดูแลระบบ (System Administrator) ตัดการเชื่อมต่อทางเครือข่ายสำหรับ<br>(๑.๑) เครื่องคอมพิวเตอร์ที่ติด Malware ออกจากเครือข่ายภายในเพื่อป้องกันการกระจายไปยังระบบสารสนเทศอื่น<br>(๑.๒) ระบบสำรองข้อมูล รวมถึงการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอก เพื่อป้องกันข้อมูลสำรองถูกเข้ารหัสลับ<br>(๑.๓) ระบบสารสนเทศที่อยู่ในเครือข่ายเดียวกัน เพื่อป้องกันการกระจาย Malware ไประบบดังกล่าว<br>(๒) สำรองข้อมูลที่ยังใช้งานได้จากเครื่องคอมพิวเตอร์ที่ติด Malware และดำเนินการสแกนไวรัส เพื่อกำจัดไวรัสเครื่องคอมพิวเตอร์ดังกล่าว |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๑. ความเสี่ยงที่เกิดจากบุคคล (People) (ต่อ) | | | | | | |
| | | | | | | (๓) หากไวรัสไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)<br>(๔) แจ้งเหตุไปยังสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ (Thai CERT) และ ปอท.(สำนักงานป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์) เป็นต้น<br>(๕) เปลี่ยนรหัสผ่านที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ติด Malware รวมถึงรหัสผ่านที่ใช้งาน ผ่านระบบควบคุมบัญชีผู้ใช้งานทั้งหมด<br>(๖) ตรวจสอบสายพันธุ์ของ Malware (กรณีเป็น Ransomware)[๖] โดยอาศัยข้อมูล ที่ปรากฏในเครื่องคอมพิวเตอร์ที่ติด Malware เช่น นามสกุลของ File ที่เปลี่ยนไป ข้อความที่ปรากฏหน้าจอในการเรียกค่าไถ่ เพื่อประเมินวิธีการแก้ไขปัญหา เช่น การกู้คืนข้อมูล |

[6] Data from https://www.cyber-security.in.th

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๑. ความเสี่ยงที่เกิดจากบุคคล (People) (ต่อ) | | | | | | |
| ๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากรภายใน กรม สบส. (ต่อ) | | | | | | (๗) หากมีความประสงค์ในการใช้เครื่องมือถอดรหัสลับข้อมูล ควรทำในสภาพแวดล้อมที่ไม่มีการเชื่อมต่อทางเครือข่าย เพื่อลดความเสี่ยงที่อาจเกิดจากการใช้เครื่องมือดังกล่าว<br>(๘) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ทราบเพื่อดำเนินการกู้คืนข้อมูล ตามแผนการสำรองและกู้คืนข้อมูล กรมสนับสนุนบริการสุขภาพ<br>(๙) รายงานผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (DCIO) และอธิบดีกรมสนับสนุนบริการสุขภาพ (CEO) ทราบแล้วแต่กรณี |
| ๑.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี | ๑.๒.๑ ระบบคอมพิวแตอร์และระบบสารสนเทศ อาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบหน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศล่มได้ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | (๑) ผู้ดูแลระบบ (System Administrator) ตรวจสอบ Log files เพื่อวิเคราะห์ระบบ จัดเก็บข้อมูล การประมวลผลข้อมูล การรายงานผล<br>(๒) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ทราบเพื่อดำเนินการกู้คืนข้อมูล ตามแผนการ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๑. ความเสี่ยงที่เกิดจากบุคคล (People) (ต่อ) | | | | | | |
| ๑.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี (ต่อ) | ๑.๒.๑ ระบบคอมพิวแตอร์และระบบสารสนเทศ อาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบหน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศล่มได้ (ต่อ) | | | | | สำรองและกู้คืนข้อมูล กรมสนับสนุนบริการสุขภาพ<br>- รายงานผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (DCIO) และอธิบดีกรมสนับสนุนบริการสุขภาพ (CEO) ทราบ แล้วแต่กรณี |
| | ๑.๒.๒ ระบบคอมพิวเตอร์ติด Virus, Malware ,Worm (หนอนอินเทอร์เน็ต) หรือ Ransomware หรือไฟล์ที่คัดลอกจากอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive หรือ External Hard disk, Storage ส่งผลให้ระบบคอมพิวเตอร์ และระบบสารสนเทศประมวลผลข้อมูลได้ช้าลง หรืออาจทำงานผิดพลาดได้ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | เช่นเดียวกับเหตุการณ์ ข้อ ๑.๑ |
| ๑.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล | ๑.๓.๑ การเปลี่ยนแปลงแก้ไขข้อมูล ที่ส่งผลให้ข้อมูลขาดความเชื่อถือ<br>ข้อมูลที่ดี (Data Governance) ประกอบด้วย<br>(๑) Data Security<br>(๑.๑) การรักษาความลับ (Confidentiality)<br>(๑.๒) การกำหนดสิทธิของผู้เกี่ยวข้องกับข้อมูล (Integrity) | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | (๑) ผู้พบเหตุ รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป<br>(๒) ผู้ดูแลระบบตรวจสอบความครบถ้วนและความเสียหายของอุปกรณ์ประมวลผลข้อมูลและผลกระทบต่อระบบคอมพิวเตอร์ระบบสารสนเทศรวมทั้งข้อมูลสารสนเทศ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๑. ความเสี่ยงที่เกิดจากบุคคล (People) (ต่อ) | | | | | | |
| ๑.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (ต่อ) | (๑.๓) ความพร้อมใช้งานของข้อมูล (Availability)<br>(๒) Data Privacy<br>(๒.๑) การขอความยินยอมจากเจ้าของข้อมูล (Consent)<br>(๒.๒) การไม่เปิดเผยข้อมูลโดยไม่มีเหตุอันสมควร<br>(๓) Data Quality<br>(๓.๑) การทำให้ข้อมูลมีความถูกต้อง (Accuracy)<br>(๓.๒) ข้อมูลมีความครบถ้วน (Completeness)<br>(๓.๓) ข้อมูลมีความเป็นปัจจุบัน (Timeliness)<br>(๓.๔) ข้อมูลมีมาตรฐานเดียวกัน (Consistency)<br>(๓.๕) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) | | | | | (๓) ผู้ดูแลระบบ (System Administrator) ตรวจสอบ Log files เพื่อวิเคราะห์ระบบ จัดเก็บข้อมูล การประมวลผลข้อมูล การรายงานผล<br>(๔) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ทราบเพื่อดำเนินการกู้คืนข้อมูล ตามแผนการสำรองและกู้คืนข้อมูล กรมสนับสนุนบริการสุขภาพ<br>(๕) รายงานผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (DCIO) และอธิบดีกรมสนับสนุนบริการสุขภาพ (CEO) ทราบ แล้วแต่กรณี |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) | | | | | | |
| ๒.๑ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล | ๒.๑.๑ อุปกรณ์ประมวลผลข้อมูลสูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล ซึ่งส่งผลกระทบต่อกรมสนับสนุนบริการสุขภาพ โดยเฉพาะข้อมูลที่เป็นความลับ | ๑ | ๕ | ๕ | ค่อนข้างต่ำ | (๑) ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ทราบเพื่อรายงานตามลำดับชั้นและสั่งการต่อไป<br>(๒) ผู้ดูแลระบบตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูลหรือระบบปรับอากาศได้รับความเสียหาย หากเสียหายเล็กน้อยให้ดำเนินการแก้ไขและเปิดใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศต่อไป<br>(๓) ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป |
| ๒.๒ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค | ๒.๒.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถให้บริการได้เต็มประสิทธิภาพ หรือไม่สามารถให้บริการได้ | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | - เช่นเดียวกับเหตุการณ์ ข้อ ๒.๑.๑ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| | ๒.๒.๒ อุปกรณ์ประมวลผลข้อมูล บางรายการหยุดทำงานชั่วขณะหรือใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศไม่เต็มประสิทธิภาพ | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | - เช่นเดียวกับเหตุการณ์ ข้อ ๒.๑.๑ |
| ๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ | ๒.๓.๑ เหตุการณ์ไฟฟ้าดับ ทำให้อุปกรณ์ประมวลผลข้อมูล บางรายการหยุดทำงานชั่วขณะหรือใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศไม่เต็มประสิทธิภาพ | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | (๑) ผู้ดูแลระบบตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูลหรือระบบปรับอากาศได้รับความเสียหายเล็กน้อยให้ดำเนินการแก้ไขและเปิดใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ<br>(๒) หากเหตุการณ์ร้ายแรง ไม่สามารถแก้ไขได้ ให้รายงาน DCIO รับทราบ เพื่อประชาสัมพันธ์ให้บุคลากร กรม สบส.<br>รับทราบ ถึงการหยุดให้บริการชั่วคราวเนื่องจากไฟฟ้าดับ<br>(๓) DCIO ประสานงานกับกลุ่มเทคโนโลยีสารสนเทศ เพื่อติดตามปัญหา ระยะเวลา การแก้ไขที่สามารถกลับมาให้บริการได้<br>(๔) เมื่อสามารถแก้ไขแล้วเสร็จ ผู้ดูแลระบบเปิดการใช้งานระบบ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| ๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | ๒.๓.๑ เหตุการณ์ไฟฟ้าดับ ทำให้อุปกรณ์ประมวลผลข้อมูล บางรายการหยุดทำงานชั่วขณะหรือใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศไม่เต็มประสิทธิภาพ (ต่อ) | | | | | คอมพิวเตอร์และระบบสารสนเทศ รวมทั้งรายงานให้ DCIO และอธิบดี กรม สบส. ทราบ<br>(๕) DCIO ประชาสัมพันธ์ให้บุคลากร กรม สบส. ทราบว่างานระบบคอมพิวเตอร์และระบบสารสนเทศสามารถกลับมาใช้งานได้ตามปกติ |
| | ๒.๓.๒ ระบบปรับอากาศชำรุด ส่งผลให้อุณหภูมิในห้องศูนย์ข้อมูลสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูลได้รับความเสียหาย | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | - เช่นเดียวกับเหตุการณ์ ข้อ ๒.๓.๑ |
| | ๒.๓.๓ เหตุการณ์อัคคีภัย<br>- สินทรัพย์ (Asset) ที่ย้ายไม่ทัน อาจถูกไฟไหม้<br>- อุปกรณ์ประมวลผลข้อมูล ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ไม่สามารถให้บริการได้ | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | ดำเนินการตามแนวทางในการปฏิบัติตามแผนป้องกันและระงับอัคคีภัย (มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ) กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข<br><br><u>กรณีที่ ๑</u> ไฟเริ่มไหม้สามารถดับไฟได้<br>(๑.๑) ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับ<br>(๑.๒) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| ๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | | | | | | (๑.๓) ผู้ดูแลระบบ ประเมินสถานการณ์ในเบื้องต้นว่า ควรหยุดให้บริการระบบคอมพิวเตอร์และระบบสารสนเทศหรือไม่<br>(๑.๔) ถ้าหยุดให้บริการ DCIO สั่งการให้บุคลากรได้รับทราบถึงการหยุดให้บริการชั่วคราว เนื่องจากเหตุไฟไหม้<br>(๑.๕) ผู้ดูแลระบบ ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล ระบบปรับอากาศ และสภาพภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์<br>(๑.๖) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ DCIO และอธิบดีฯ ทราบ<br>(๑.๗) หากเสียหายเล็กน้อย ให้ผู้ดูแลระบบดำเนินการแก้ไขและเปิดการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| ๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | ๒.๓.๓ เหตุการณ์อัคคีภัย (ต่อ) | | | | | (๑.๘) DCIO ประชาสัมพันธ์ให้บุคลากร กรม สบส. ทราบว่างานระบบคอมพิวเตอร์และระบบสารสนเทศสามารถกลับมาใช้งานได้ตามปกติ<br><br><u>กรณีที่ ๒</u> ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง<br>(๒.๑) ผู้พบเหตุ โทรแจ้งหน่วยดับเพลิงเป็นลำดับแรก และแจ้งให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ DCIO และอธิบดี กรม สบส.ทราบโดยเร็ว<br>(๒.๒) ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นเริ่มลุกลามโดยรอบ หากไม่สามารถระงับเหตุได้ ให้ออกจากพื้นที่โดยเร็ว<br>(๒.๓) DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการ เนื่องจากเหตุไฟไหม้<br>(๒.๔) หากสามารถระงับเหตุได้ ผู้ดูแลระบบ ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งาน |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| ๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | ๒.๓.๓ เหตุการณ์อัคคีภัย (ต่อ) | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | ของอุปกรณ์ประมวลผลข้อมูล ระบบปรับอากาศ และสภาพภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ พร้อมทั้งรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ DCIO และอธิบดี กรม สบส.ทราบ<br>(๒.๕) หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ รายงานผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ DCIO และอธิบดี กรม สบส.ทราบตามลำดับ<br>(๒.๖) ถ้าเกิดเหตุการณ์ไฟฟ้าดับให้ดำเนินการตามข้อ (๒.๕)<br>(๒.๗) กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่สำรองหรือที่พักตามที่กำหนด |
| | ๒.๓.๔ เหตุการณ์ที่เกิดจากภัยพิบัติ หรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง อาจถูกปิดกั้นการเข้าออกและอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำ บริเวณกระทรวงสาธารณสุข ซึ่งส่งผล | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | (๑) หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ ประมวลผลขอมูล ระบบปรับอากาศ และสภาพภายในภายในห้องศูนย์กลางข้อมูล |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| ๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | กระทบต่อห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูลและห้องเซิร์ฟเวอร์ไม่สามารถให้บริการได้ หรือสถานที่ปฏิบัติงานบริเวณอาคารกรมสนับสนุนบริการสุขภาพ | | | | | ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์<br>(๒) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยี และ DCIO ทราบตามลำดับชั้นและสั่งการต่อไป |
| ๓. ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) | | | | | | |
| ๓.๑ ทรัพย์สินครุภัณฑ์ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software) | ๓.๑.๑ ไม่เพียงพอต่อการใช้งาน<br>๓.๑.๒ ไม่พร้อมใช้งาน | (L๕) ๒ | (C๔) ๕ | ๑๐ | ค่อนข้างสูง | (๑) จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ (e-Asset)<br>(๒) สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งาน ตามแผนที่กำหนด<br>(๓) กำหนดแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง<br>(๔) ปรับปรุงระบบการยืม-คืน เมื่อนำอุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอกสำนักงาน<br>(๕) ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๓. ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) (ต่อ) | | | | | | |
| ๓.๒ เครือข่ายสารสนเทศและเครือข่ายเสมือน (Information Network and Virtual Machine) | ๓.๒.๑ ไม่เพียงพอต่อการใช้งาน<br>๓.๒.๒ ไม่พร้อมใช้งาน | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | (๑) จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ (e-Asset)<br>(๒) สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งาน ตามแผนที่กำหนด<br>(๓) กำหนดแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครือข่ายสารสนเทศและเครือข่ายเสมือนให้ครบทุกเครื่อง<br>(๔) ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |
| ๓.๓ โครงข่ายการสื่อสาร Communication Network) | ๓.๓.๑ ไม่เพียงพอต่อการใช้งาน<br>๓.๓.๒ ไม่พร้อมใช้งาน | (L๕) ๑ | (C๔) ๕ | ๕ | ค่อนข้างต่ำ | (๑) จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ<br>(๒) สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งาน ตามแผนที่กำหนด<br>(๓) กำหนดแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งาน การเข้ารหัสโครงข่ายการสื่อสารให้ครบทุกเครื่อง<br>(๔) ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๓. ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) (ต่อ) | | | | | | |
| ๓.๔ ข้อมูลและสารสนเทศ (Information) | - ด้าน Data Security<br>- ด้าน Data Privacy<br>- ด้าน Data Quality | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | (๑) กำหนดแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งานข้อมูลและสารสนเทศ ตามแนวทางการจัดการข้อมูลที่ดี (Data Governance)<br>(๒) ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |

<u>หมายเหตุ</u> เกณฑ์การประเมิน การให้คะแนนโอกาสที่จะเกิดและผลกระทบ

ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด
ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย
ระดับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง
ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก
ระดับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด

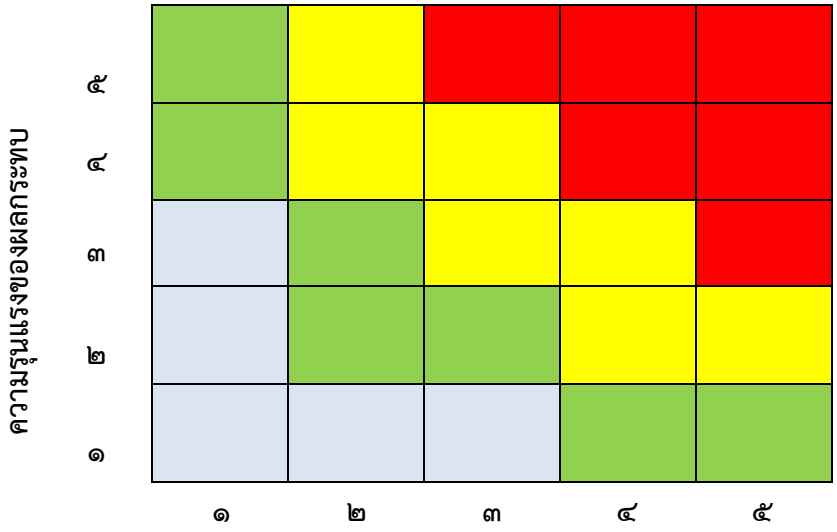
แผนผังประเมินความเสี่ยง

| ผลกระทบของความเสี่ยง | | | | | |
|---|---|---|---|---|---|
| ๕ | ๑๐ | ๑๕ | ๒๐ | ๒๕ | |
| ๔ | ๘ | ๑๒ | ๑๖ | ๒๐ | |
| ๓ | ๖ | ๙ | ๑๒ | ๑๕ | |
| ๒ | ๔ | ๖ | ๘ | ๑๐ | |
| ๑ | ๒ | ๓ | ๔ | ๕ | |

สีแดง ระดับความเสี่ยงสูง ค่าระหว่าง ๑๕ - ๒๕
สีเหลือง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง ๘ - ๑๔
สีเขียว ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง ๔ - ๗
สีฟ้า ระดับความเสี่ยงต่ำ ค่าระหว่าง ๑ - ๓

**๕.๒ การจัดทำแผนภูมิความเสี่ยง**

การจัดทำแผนภูมิความเสี่ยงเพื่อช่วยให้สามารถตัดสินใจวางแผนบริหารความเสี่ยงได้อย่างเหมาะสม และสามารถเห็นภาพว่าเมื่อรวมทุกปัจจัยเสี่ยงแล้ว ปัจจัยเสี่ยงใดควรได้รับการจัดการก่อนหลัง กำหนดให้คะแนนประเมินความเสี่ยงที่จะต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๐ คะแนนขึ้นไป) ส่วนปัจจัยเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๐ คะแนน ถือว่ามีความเสี่ยงค่อนข้างต่ำไม่นำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยง




**ขั้นตอนที่ ๖ ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง**

การสื่อสารทำความเข้าใจเกี่ยวกับแผนความเสี่ยงด้านสารสนเทศให้บุคลากรที่เกี่ยวข้องทราบสามารถนำไปปฏิบัติได้ และรายงานความก้าวหน้าของการดำเนินงานตามแผนบริหารความเสี่ยงด้านสารสนเทศ ตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC ๒๗๐๐๑ : ๒๐๑๓) ใน ๓ ด้าน คือ

๖.๑ ด้านการสร้างความตระหนักของการบริหารความเสี่ยงด้านสารสนเทศ สำหรับผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศ โดยการพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ **(People)** ได้ดำเนินการ

๖.๒.๑ สร้างความตระหนักและการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Awareness) สำหรับผู้ใช้งาน (User) และวิธีการตรวจสอบช่องโหว่ Vulnerability Assessment (Web Application Hacking) และการเจาะระบบ (Penetration Testing) สำหรับผู้ดูแลระบบ (System Administrator)

(๑) ผลการประเมินความพึงพอใจในการพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ มากกว่าร้อยละ ๘๐ [๗]

(๒) กรมสนับสนุนบริการสุขภาพ ไม่มีบุคลากรผู้เชี่ยวชาญ

(๒.๑) ด้านความมั่นคงปลอดภัยสารสนเทศ (Information/Cyber Security Person) และไม่เพียงพอต่อการปฏิบัติงานในการเป็นหน่วยงานหลัก การกำกับมาตรฐานระบบบริการสุขภาพ ด้านที่ ๙ “การรักษาความมั่นคงปลอดภัยไซเบอร์”

(๒.๒) ด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)

กรมสนับสนุนบริการสุขภาพ ควรต้องต้องเสนอขอจัดสรรอัตรากำลัง หรือจัดจ้างบุคลากรภายนอก (Contract Outsource) เพิ่มเติม

[๗] ดำเนินการแล้วเสร็จ วันที่ ๒๘ มีนาคม พ.ศ. ๒๕๖๓

๖.๒.๒ การฝึกซ้อมรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber drill) เพื่อให้บุคลากรและผู้บริหาร กรมสนับสนุนบริการสุขภาพมีการเตรียมความพร้อมรับสถานการณ์การโจมตี (Cyber Drill) มีความเข้าใจ และตระหนักถึงภัยจากการโจมตีทางอิเล็กทรอนิกส์ที่อยู่ใกล้ตัว เพราะเมื่อการโจมตีเกิดขึ้นจะได้ไม่ตกเป็นเหยื่อโดยรู้เท่าไม่ถึงการณ์ ที่การบริหารความมั่นคงปลอดภัยขององค์การในอนาคตต้องมีรูปแบบเป็น “Cyber Resilience” ซึ่งหมายถึง ระบบต้องมีความสามารถในการรองรับการโจมตีและจะต้องสามารถทำงานหรือให้บริการได้อย่างต่อเนื่องไม่ทำให้เกิดความเสียหายต่อภารกิจและภาพลักษณ์ขององค์การ ภาพลักษณ์ของผู้บริหาร ดังนั้นแนวคิดของ Information Security Management ในรูปแบบเดิมๆ จึงไม่ครอบคลุม เพียงพอ จำเป็นต้องนำแนวคิด Cyber Security Resilience Framework (Cyber Security Centric and Cyber Resilience in Action) มาปรับใช้ในองค์กรด้วย

๖.๒ ด้านกระบวนการ **(Process)** ได้วิเคราะห์แนวทางการประเมินความเสี่ยงระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ (Gap Assessment) [๘] พบว่าต้องมีการพัฒนาในภาพรวม จากร้อยละ ๑๙.๗๒๕ ให้ผ่านการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๖.๒.๑ การดำเนินการวิเคราะห์ช่องว่างมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Gap Assessment) เพื่อกำหนดแนวทางการพัฒนาตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ โดยมีเกณฑ์การตรวจประเมินและผลการตรวจประเมิน ที่แสดงถึงรายละเอียดข้อบกพร่องที่ค้นพบและได้ให้ข้อเสนอแนะในการพัฒนาปรับปรุงระบบเทคโนโลยีสารสนเทศให้ผ่านการประเมินตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓

๖.๒.๒ การตรวจสอบระบบเทคโนโลยีสารสนเทศด้วยวิธีการตรวจสอบช่องโหว่ Vulnerability Assessment (Web Application Hacking) และการเจาะระบบ (Penetration Testing) สำหรับผู้ดูแลระบบ (System Administrator) พบว่าการตรวจสอบช่องโหว่ของเครื่องแม่ข่ายจากภายนอกและภายในองค์กร (External and Internal Vulnerability Assessment) ซึ่งช่องโหว่ที่พบเกิดจาก ซอฟต์แวร์ที่ทำงานบนเซิร์ฟเวอร์สำหรับให้บริการผ่านระบบเครือข่ายภายนอก ไม่ได้รับการอัพเกรด (System Patch) โดยส่งผลกระทบต่อองค์กรในด้านของความน่าเชื่อถือขององค์กร (Reputation)และ กระทบต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นต้น

๖.๓ ด้านเทคโนโลยี **(Technology)** ความปลอดภัยมาใช้เพื่อการป้องกันปัญหาต่างๆ ที่เป็นความเสี่ยงในระบบจากบุคลากรที่มีศักยภาพ และแนวคิดการจัดการเชิงระบบ ที่ขึ้นกับการเลือกใช้วิธีการใด ในการกำจัดความเสี่ยงให้พิจารณาจากงบประมาณ,ความคุ้มค่า,กฎหมายที่เกี่ยวข้องและผลกระทบต่อเนื่องกับธุรกิจ[๙]

**ขั้นตอนที่ ๗ การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ**

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม มีการติดตามและเฝ้าระวังความเสี่ยงด้านสารสนเทศในปี พ.ศ. ๒๕๖๓ ดังนี้

๑. การตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ (สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

๒. การสื่อสารประชาสัมพันธ์ผ่านสื่อสังคมออนไลน์ (Social Media) เช่น

๒.๑ Line Group ID: http://line.me/ti/g/Hiooge6PGV ,

๒.๒ e-Mail**:** isms@hss.mail.go.th

๓. การสนับสนุน ส่งเสริมการเรียนรู้ด้วยตนเอง e-Learning สำหรับบุคลากรด้านเทคโนโลยีสารสนเทศเพื่อให้มีการปฏิบัติงานตามปกติและเป็นวัฒนธรรมองค์กร นอกจากนี้ ได้มีการติดตามผลการบริหารความเสี่ยง การประเมินผลการบริหารความเสี่ยง และการสรุปผลการดำเนินงานจากการบริหารความเสี่ยงเป็นรายไตรมาส ตลอดจนจัดทำรายงานสรุปผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านสารสนเทศ ข้อดี ข้อเสีย ปัญหาและอุปสรรค ในการดำเนินงานตามแผนบริหารความเสี่ยงด้านสารสนเทศ รวมทั้งข้อเสนอแนะ เพื่อการปรับปรุงแผนบริหารความเสี่ยง

[๘] ภาคผนวก ก ประเมินโดย บริษัท เอเชี่ยน อินเทลลิเจนท์ อินฟอร์เมชั่น เทคโนโลยี จำกัด,๒๕๖๒

[๙] ไม่ได้มีการประเมิน เนื่องจากข้อจำกัดด้านงบประมาณ,๒๕๖๒

ด้านสารสนเทศ เพื่อรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับกรม และอธิบดีกรมสนับสนุนบริการสุขภาพรับทราบ ทั้งนี้ เพื่อให้การบริหารความเสี่ยงสามารถเพิ่มมูลค่าการปฏิบัติงานแก่บุคลากรด้านเทคโนโลยีสารสนเทศ ได้อย่างแท้จริงและยั่งยืน

การรายงานความก้าวหน้าของการดำเนินงาน พ.ศ. ๒๕๖๓ การบริหารความเสี่ยงด้านสารสนเทศ ตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑:๒๐๑๓ มีดังนี้

**หมวดที่ ๑ นโยบาย** : ได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓ เพื่อให้ผู้ปฏิบัติงานทราบถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการ พ.ศ. ๒๕๖๓

**หมวดที่ ๒ โครงสร้าง** : มีกลไกในการขับเคลื่อนการรักษาความมั่นคงปลอดภัยที่ชัดเจน ตามแผนยุทธศาสตร์การบริหารจัดการระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ.๒๕๖๔ - ๒๕๖๖ และได้มีการแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ และระดับหน่วยงานเพื่อเป็นกลไกเชื่อมโยงสอดคล้อง ในการขับเคลื่อนนโยบายที่กรมกำหนด มีการมอบหมายบุคลากรที่ชัดเจนเป็นลายลักษณ์อักษร มีการแบ่งความรับผิดชอบที่ชัดเจน ส่วนแผนผังโครงสร้างด้าน IT อันเป็นกลไกการสั่งการ ควบคุม กำกับ สื่อสารให้ทราบถึงขั้นตอนสายการบังคับบัญชา ได้จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓ หากเกิดเหตุการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยจะทำให้การสั่งการมีประสิทธิภาพ

**หมวดที่ ๓ มาตรการด้านบุคลากร** : ได้รวบรวมจำนวนบุคลากรด้านเทคโนโลยีสารสนเทศและบุคลากรด้านอื่นๆ ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อจัดทำกรอบอัตรากำลังเสนอต่อผู้บริหารฯ พิจารณารองรับภารกิจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และการประเมินมาตรฐานสถานพยาบาลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งรองรับการจัดตั้ง “ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ : HSS SOC Team (Security Operations Center)” สำหรับหน่วยงานอื่นๆ ยังไม่มีการกำหนดมาตรการด้านบุคลากรไว้ชัดเจนเนื่องจากข้อจำกัดด้านกรอบอัตรากำลังมีเพียงการคัดเลือกบุคลากรตามระเบียบพัสดุและการบริหารทรัพยากรเท่านั้น

**หมวดที่ ๔ การบริหารจัดการสินทรัพย์ด้าน IT**: ได้มีการจัดทำทะเบียนคุมทรัพย์สินตามระเบียบพัสดุ ซึ่งอยู่ระหว่างปรับปรุงระบบรวมทั้งมีแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง และมีระบบการยืม-คืน เมื่อนำอุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอกสำนักงาน

**หมวดที่ ๕ การควบคุมการเข้าถึง** : ได้มีการจดรหัสการเข้าถึงไว้ในบัญชีรหัสผ่านแต่ไม่มีการปรับปรุงและให้ง่าย สะดวกในการนำมาใช้งานด้วยระบบอัตโนมัติ ยังไม่มีการกำหนดสิทธิในการเข้าถึงระบบ ส่วนในระบบเครือข่ายมีการกำหนดสิทธิของผู้บริหารจัดการดูแลระบบรหัสเดียวแต่ใช้รวมกันทั้งทีมงาน เพื่อความสะดวกในการแก้ไขปัญหา มีการถอนถอดสิทธิในการเข้าถึงระบบแต่ยังไม่ครอบคลุม ยังไม่มีระบบควบคุมการเข้าถึงรหัส (Password) มีการเก็บรหัสผ่านที่ยังไม่ดีพอด้านความมั่นคงปลอดภัยสารสนเทศมีการเก็บในรูปแบบ Plain Text และผู้ใช้งานไม่สามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง โดยได้จัดอบรมให้เกิดความตระหนักรู้เกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคล[๑๐] คิดเป็นร้อยละ ๑๐ ของบุคลากรทั้งหมด

**หมวดที่ ๖ การเข้ารหัสข้อมูล** : ได้กำหนดในแผนการพัฒนาระบบเทคโนโลยีสารสนเทศ เพื่อให้เป็นแนวทางในการปฏิบัติงานที่ชัดเจนและมีความมั่นคงปลอดภัยด้านสารสนเทศ

**หมวดที่ ๗ ทางกายภาพ** : มีการแบ่งพื้นที่การรักษาความปลอดภัยเป็นสัดส่วน มีการควบคุมการเข้าถึงโดยมี รปภ.มีกุญแจเข้าในแต่ละชั้นของพื้นที่อาคาร มีการกำหนดผู้รับผิดชอบถือกุญแจคนละดอก มีการติดกล้องวงจรปิดแต่สถานที่ที่กำหนดว่ารักษาความมั่นคงปลอดภัยยังเสี่ยงต่อการโจรกรรมได้ แต่ยังไม่ได้ปฏิบัติให้ครบถ้วนตามมาตรฐาน ยังไม่มีการลงทะเบียนการเข้าออกในพื้นที่เฉพาะ (Restrict Area) ยังไม่ครอบคลุมทุกพื้นที่ มีเครื่องดับเพลิงไว้พร้อมใช้งาน

[๑๐] พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

**หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)**

การติดตั้งโปรแกรมป้องกันไวรัสไม่ครบทุกเครื่อง มีแนวทางการตรวจสอบโปรแกรมไม่พึงประสงค์และการตรวจสอบโปรแกรมอรรถประโยชน์ที่ไม่มีลิขสิทธิ รวมทั้งการนำเทคโนโลยีใหม่ๆ มาปรับใช้ในงาน บางครั้งพบว่าผู้ปฏิบัติงานสามารถติดตั้งโปรแกรมใช้งานได้เองซึ่งเสี่ยงต่อการนำโปรแกรมไม่พึงประสงค์ เช่น ไวรัส มัลแวร์ หนอนไวรัสเข้ามาสู่ระบบได้ ส่วนการสำรองข้อมูลได้กำหนดแนวทางการปฏิบัติฯ แล้ว

**หมวดที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล** (Communications Security) มีการกำหนดผู้ดูแล Firewall และคอยบริหารจัดการ User ที่ผ่านเข้าออก Firewall แต่การส่งข้อมูลผ่านระบบเครือข่ายมีการกำหนด Policy จาก IT กรมฯ หน่วยงานมีหน้าที่ดูแลเพียงรหัสผ่านเข้าออกและอีเมล์ของผู้ใช้งานภายในหน่วยงาน ผู้ใช้งานสามารถใช้ Free e-Mail จากเอกชนได้ ยังไม่มีมาตรการควบคุมในการใช้งานเครือข่าย มีเฉพาะการจัดเก็บ Log file ที่ IT กรมฯ ติดตั้งให้แต่ไม่ได้รับมอบสิทธิและความรู้ในการดูแลเฝ้าระวังระบบ ทำให้การดูแลระบบไม่ครอบคลุม เมื่อเกิดปัญหาจะมีการรายงานเข้ามายังส่วนกลาง และได้รับการแก้ไขจากผู้ดูแลระบบ จากส่วนกลางได้จัดจ้างไว้ อีกทั้งมีการเตรียมความพร้อมบุคลากรผู้ดูแลระบบ (System Administrator) โดยการจัดอบรมพัฒนาศักยภาพด้านความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Literacy) การวิเคราะห์ระบบ (Vulnerability Assessment) และเจาะระบบ (Penetration Testing)

**หมวดที่ ๑๐ การพัฒนาระบบ** : ได้กำหนดในแผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๖ และแผนยุทธศาสตร์การพัฒนาดิจิทัลเพื่อระบบบริการสุขภาพและระบบสุขภาพภาคประชาชน ระยะ ๕ ปี ของกรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๘

**หมวดที่ ๑๑ การรับบริการผู้รับจ้างภายนอก** : ได้กำหนดแนวทางปฏิบัติการควบคุมกำกับผู้รับจ้างและการกำหนด TOR ไว้แล้ว

**หมวดที่ ๑๒ การบริหารจัดการปัญหา** : ได้พัฒนาแนวทางการบริหารจัดการปัญหา กระบวนการขั้นตอนการให้บริการช่วยเหลือ การแก้ไขปัญหา ช่องทางการรับปัญหาและดำเนินการแก้ไขปัญหา อยู่ระหว่างจัดทำรายงานดิจิทัล (Digital Form) การจดบันทึกปัญหาหรือสาเหตุ/แนวทางการแก้ไขปัญหา รวมทั้งการรวบรวม สรุป วิเคราะห์ปัญหาอย่างเป็นระบบและประเภทปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อการวางแผนดำเนินการเชิงระบบในการแก้ปัญหาอย่างครอบคลุม

**หมวดที่ ๑๓ การบริหารความต่อเนื่องในการให้บริการ** : กรมสนับสนุนบริการสุขภาพได้จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓ เพื่อเตรียมความพร้อมรองรับให้บริการความต่อเนื่อง เช่น การบำรุงรักษาเครื่องมือระบบคอมพิวเตอร์และเครือข่าย การเฝ้าระวัง การสำรองข้อมูล เป็นต้น

**หมวดที่ ๑๔ การปฏิบัติงานความสอดคล้องกับกฎหมายที่เกี่ยวข้อง** : มีการวางแผนวิเคราะห์ระบบงานให้สอดคล้องกับกฎหมาย เพื่อให้การปฏิบัติงานไม่ละเมิดต่อกฎหมายที่เกี่ยวข้อง [๑๑]

นอกจากนี้ กรมสนับสนุนบริการสุขภาพ ได้ปรับปรุงประกาศกระทรวงสาธารณสุข เรื่อง กำหนดลักษณะของสถานพยาบาลและมาตรฐานซึ่งได้รับการยกเว้นไม่ต้องอยู่ในบังคับตามกฎหมายว่าด้วยสถานพยาบาล (ฉบับที่ ๒ ) อาศัยอำนาจตามความในมาตรา ๕ วรรคสอง แห่งพระราชบัญญัติสถานพยาบาล พ.ศ. ๒๕๔๑ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติสถานพยาบาล (ฉบับที่ ๔) พ.ศ. ๒๕๕๙ และมาตรา ๖ วรรคหนึ่งแห่งพระราชบัญญัติสถานพยาบาล พ.ศ.๒๕๔๑ ตามข้อ ๓ (๓) “จัดให้มีมาตรฐานระบบบริการสุขภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์” เพื่อใช้ในการควบคุม กำกับมาตรฐานสถานพยาบาลภาครัฐและภาคเอกชนที่อยู่ภายใต้พระราชบัญญัติฉบับนี้ ให้ผ่านเกณฑ์มาตรฐานฯ

จากผลการดำเนินงานข้างต้นนี้ ทำให้กรมสนับสนุนบริการสุขภาพ มีระบบเทคโนโลยีสารสนเทศด้านระบบบริการสุขภาพที่ทันสมัย มีความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ มีความมั่นคงปลอดภัยไซเบอร์ในระดับสูง สร้างความเชื่อมั่นให้ผู้รับบริการ ตลอดจนการควบคุม กำกับสถานพยาบาลภาครัฐและเอกชนให้ผ่านเกณฑ์

[๑๑] การวิเคราะห์ช่องว่างด้านความมั่นคงปลอดภัยสารสนเทศ (Gap Assessment)

มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ อีกทั้งจัดทำข้อเสนอเชิงนโยบายในการจัดตั้ง “ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ[๑๒] : HSS SOC Team (Security Operations Center of Health Service Support Department)” เพื่อการตรวจสอบภัยคุกคาม แจ้งเตือน กู้คืน เอื้อต่อการตอบสนองด้านความปลอดภัยและเหตุการณ์ฉุกเฉิน รวมทั้งเฝ้าระวังและแจ้งเตือนสถานพยาบาล ตามแนวทางมาตรฐานสถานพยาบาลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งผลให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการข้อมูลสารสนเทศ เพิ่มโอกาสการเข้าถึงและใช้ประโยชน์จากบริการข้อมูลด้านระบบบริการสุขภาพเชิงรุกรองรับนโยบายรัฐบาลดิจิทัล (Digital Government) การเพิ่มมูลค่าการทำธุรกรรมอิเล็กทรอนิกส์ ที่สามารถสร้างรายได้สู่ประเทศเพิ่มขึ้น รวมทั้งการคุ้มครองประชาชนหรือผลประโยชน์ที่สำคัญของประเทศ

[๑๒] https://www.nstdaacademy.com

**แบบฟอร์มการรายงานผลความก้าวหน้าการดำเนินงานตามแผนบริหารความเสี่ยงเชิงยุทธศาสตร์ กรมสนับสนุนบริการสุขภาพ**
**ประจำปีงบประมาณ พ.ศ. ๒๕๖๓ (ตามแนวทาง SP๗)**

☐ **รอบ ๙ เดือน** ☐ **รอบ ๑๒ เดือน**

**แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ในยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล**

อ้างตามโครงการฯ ปีงบประมาณ ๒๕๖๒ ดำเนินการแล้วเสร็จ วันที่ ๒๘ มีนาคม ๒๕๖๓ (ไม่มีโครงการฯ ในปีงบประมาณ ๒๕๖๓)

**ชื่อโครงการ** โครงการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ปีงบประมาณ พ.ศ. ๒๕๖๒

๑. กำหนดกิจกรรมที่ต้องดำเนินการ แล้วนำมาระบุความเสี่ยงตามมิติธรรมาภิบาล ๑๐ องค์ประกอบ ดังนี้

| กิจกรรม | มิติธรรมาภิบาลที่เกี่ยวข้อง | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | ประสิทธิผล | ประสิทธิภาพ | ตอบสนอง | รับผิดชอบ | โปร่งใส | มีส่วนร่วม | กระจายอำนาจ | นิติธรรม | เสมอภาค | ฉันทามติ |
| ๑. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | ✓ | | ✓ | ✓ | ✓ | ✓ | | | | ✓ |
| ๒. การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | |

หมายเหตุ : - สามารถศึกษาแนวทางปฏิบัติฯ ได้จากเอกสารรายละเอียดของเกณฑ์ PMQA หมวด 2 SP7

๒. นำความเสี่ยงที่ระบุมาแยกประเภทของความเสี่ยงที่เกี่ยวข้องและวิเคราะห์หาปัจจัยเสี่ยง กลยุทธ์และแนวทางการจัดการความเสี่ยง

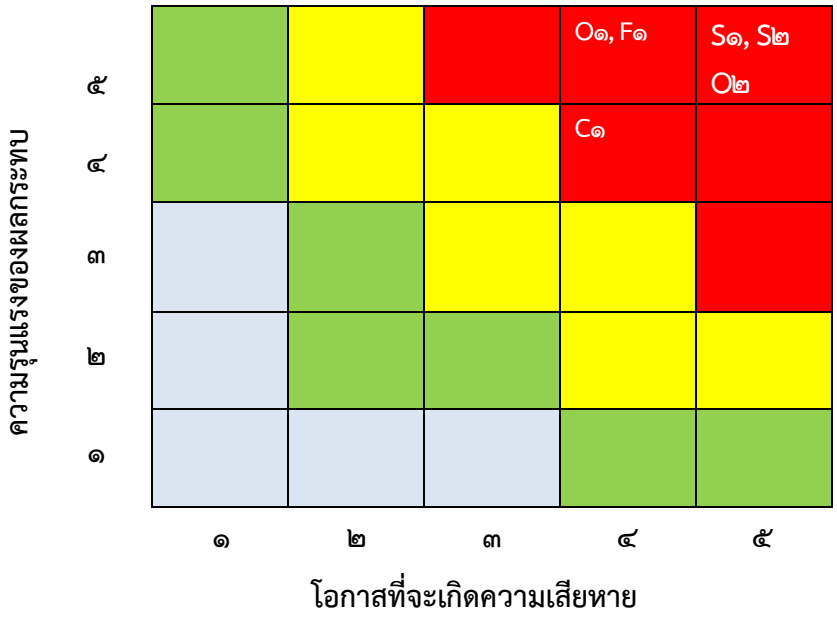
| ประเภทของความเสี่ยงที่เกี่ยวข้อง | กิจกรรม | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (C) | ระดับความเสี่ยง (L) x (C) | กลยุทธ์ที่ใช้จัดการกับความเสี่ยง | แนวทางการจัดการความเสี่ยง |
|---|---|---|---|---|---|---|---|
| ด้านกลยุทธ์ (Strategic Risk : S) | ๑. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | S๑) ความพร้อมรองรับการตรวจประเมิน | ๕ (L๕) | ๕ (C๓.๑) | ๒๕ | การควบคุมความเสี่ยง | ๑.๑) จัดทำแผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ โดยคณะทำงานฯ เสนอต่อผู้บริหารพิจารณาอนุมัติ<br>๑.๒) ปรับปรุงและประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑.๓) จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑.๔) จัดจ้างองค์กรภายนอก (Manage Security Service Provider หรือ MSSP) ดำเนินการรักษาความมั่นคงปลอดภัยสารสนเทศ |
| | ๒. การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้วยการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ | S๒) ความเชื่อมั่นในการเข้าถึงข้อมูลด้านระบบบริการสุขภาพ | ๕ (L๕) | ๕ (C๓.๑) | ๒๕ | การกระจายความเสี่ยง | ๑.๑) จัดจ้างผู้ปฏิบัติงาน/ผู้เชี่ยวชาญด้านระบบความมั่นคงปลอดภัยสารสนเทศ<br>๑.๒) พัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ |

| ประเภทของความเสี่ยงที่เกี่ยวข้อง | กิจกรรม | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (C) | ระดับความเสี่ยง (L) x (C) | กลยุทธ์ที่ใช้จัดการกับความเสี่ยง | แนวทางการจัดการความเสี่ยง |
|---|---|---|---|---|---|---|---|
| ด้านการดำเนินงาน (Operation Risk : O) | ๑.การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | O๑) ความพร้อมรองรับการตรวจประเมิน | ๔ (L๕) | ๕ (C๓.๑) | ๒๐ | การควบคุมความเสี่ยง | ๑.๑) ดำเนินงานตามนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ<br>๑.๒) ติดตามและประเมินผลการดำเนินงานตามนโยบายการบริหารจัดการระบบความมั่นคง สารสนเทศ ทุก ๓ เดือน |
| | ๒. การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้วยการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ | O๒) ศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ | ๕ (L๕) | ๕ (C๓.๑) | ๒๕ | การควบคุมความเสี่ยง | ๒.๑) พัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ<br>๒.๒) ติดตามและประเมินผลการพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ |
| ด้านการเงิน (Financial Risk : F) | ๑.การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้วยการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ | F๑) งบประมาณไม่เพียงพอในการดำเนินงาน | ๕ (L๕) | ๔ (C๑) | ๒๐ | การควบคุมความเสี่ยง | ๑.๑) เสนอแนวทางการดำเนินงานที่ชัดเจนต่อทีมผู้บริหารในการพิจารณาจัดสรรงบประมาณ<br>๑.๒) ประเมินความคุ้มค่า คุ้มทุนจากการดำเนินงานตามนโยบายฯ |
| ด้านการปฏิบัติตามกฎหมาย/ระเบียบ (Compliance Risk :C) | ๑. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | C๑) การเปลี่ยนแปลงกฎเกณฑ์ กฎระเบียบในการดำเนินงาน | ๔ (L๕) | ๔ (C๓.๑) | ๑๖ | การควบคุมความเสี่ยง | ๑) รวบรวม เสนอการปรับปรุงกฎเกณฑ์กฎระเบียบข้อกฎหมายที่เกี่ยวข้องกับนโยบายรัฐบาลดิจิทัลด้านระบบบริการสุขภาพ<br>๒) ดำเนินงานตามกฎ ระเบียบของทางราชการ<br>๓) ติดตาม ควบคุม กำกับ ประเมินผลการดำเนินงานทุก ๓ เดือน |

**๓. การจัดทำแผนภูมิความเสี่ยง**

การจัดทำแผนภูมิความเสี่ยงเพื่อช่วยให้สามารถตัดสินใจวางแผนบริหารความเสี่ยงได้อย่างเหมาะสม และสามารถเห็นภาพว่าเมื่อรวมทุกปัจจัยเสี่ยงแล้ว ปัจจัยเสี่ยงใดควรได้รับการจัดการก่อนหลัง โดยกำหนดให้คะแนนประเมินความเสี่ยงที่จะต้องนำมาดำเนินการจัดการความเสี่ยงใน คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๐ คะแนนขึ้นไป) ส่วนปัจจัยเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๐ คะแนน ถือว่ามีความเสี่ยงค่อนข้างต่ำไม่นำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยง

- **แผนภูมิความเสี่ยงโครงการการพัฒนายุทธศาสตร์ภายในประเทศ**



**ตารางที่ ๗ การบริหารความเสี่ยงเชิงยุทธศาสตร์**

| กิจกรรมภายใต้โครงการที่มีโอกาสเกิดความเสี่ยง | รายการความเสี่ยง/สาเหตุความเสี่ยง | ประเภทความเสี่ยง | | | | | | | | | | | | | | คะแนนความเสี่ยง | | | กลยุทธ์/แนวทางการจัดการความเสี่ยง |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ด้าน | | | | มิติธรรมาภิบาล (๑๐ หลัก) | | | | | | | | | | โอกาส (ค่าคะแนน ๑-๕) | ผลกระทบ (ค่าคะแนน ๑-๕) | คะแนนความเสี่ยง | |
| | | กลยุทธ์ | การดำเนินการ | การเงิน | กฎหมาย/ระเบียบ | ประสิทธิผล | ประสิทธิภาพ | ตอบสนอง | รับผิดชอบ | โปร่งใส | มีส่วนร่วม | กระจายอำนาจ | นิติธรรม | เสมอภาค | หลักนิติธรรม | | | | |
| **โครงการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ปีงบประมาณ พ.ศ. ๒๕๖๒** | | | | | | | | | | | | | | | | | | | |
| ๑. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | **S๑)** ความพร้อมรองรับการตรวจประเมิน | ✓ | - | - | - | ✓ | - | ✓ | ✓ | ✓ | ✓ | - | - | - | ✓ | ๕ | ๕ | ๒๕ | ควบคุมความเสี่ยง |
| ๒. การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ | **S๒)** ความเชื่อมั่นในการเข้าถึงข้อมูลด้านระบบบริการสุขภาพ | ✓ | - | - | - | - | ✓ | ✓ | ✓ | ✓ | ✓ | - | - | ✓ | - | ๕ | ๕ | ๒๕ | กระจายความเสี่ยง |
| ๓. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | **O๑)** ความพร้อมรองรับการตรวจประเมิน | - | ✓ | - | - | ✓ | - | ✓ | ✓ | ✓ | ✓ | - | - | - | ✓ | ๔ | ๕ | ๒๐ | ควบคุมความเสี่ยง |

| กิจกรรมภายใต้โครงการที่มีโอกาสเกิดความเสี่ยง | รายการความเสี่ยง/สาเหตุความเสี่ยง | ประเภทความเสี่ยง | | | | | | | | | | | | | | คะแนนความเสี่ยง | | | กลยุทธ์/แนวทางการจัดการความเสี่ยง |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ด้าน | | | | มิติธรรมาภิบาล (๑๐ หลัก) | | | | | | | | | | โอกาส (ค่าคะแนน ๑-๕) | ผลกระทบ (ค่าคะแนน ๑-๕) | คะแนนความเสี่ยง | |
| | | กลยุทธ์ | การดำเนินการ | การเงิน | กฎหมาย/ระเบียบ | ประสิทธิผล | ประสิทธิภาพ | ตอบสนอง | รับผิดชอบ | โปร่งใส | มีส่วนร่วม | กระจายอำนาจ | นิติธรรม | เสมอภาค | ฉันทามติ | | | | |
| **โครงการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ปีงบประมาณ พ.ศ. ๒๕๖๒** | | | | | | | | | | | | | | | | | | | |
| ๔. การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ | O๒) ความเชื่อมั่นในการเข้าถึงข้อมูลด้านระบบบริการสุขภาพ | - | ✓ | - | - | - | ✓ | ✓ | ✓ | ✓ | ✓ | - | - | ✓ | - | ๕ | ๕ | ๒๕ | ควบคุมความเสี่ยง |
| ๕. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | F๑) ความพร้อมรองรับการตรวจประเมิน | - | - | ✓ | - | ✓ | - | ✓ | ✓ | ✓ | ✓ | - | - | - | ✓ | ๔ | ๕ | ๒๐ | ควบคุมความเสี่ยง |
| ๖. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ | C๑) ความพร้อมรองรับการตรวจประเมิน | - | - | - | ✓ | ✓ | - | ✓ | ✓ | ✓ | ✓ | - | - | - | ✓ | ๔ | ๔ | ๑๖ | ควบคุมความเสี่ยง |

**ตารางที่ ๘ ผลสำเร็จการบริหารความเสี่ยงเชิงยุทธศาสตร์**

| ประเด็นความเสี่ยง | กิจกรรมตามแนวทางการจัดการความเสี่ยง | เป้าหมาย/ผลสำเร็จของการดำเนินการกิจกรรมตามแนวทางการจัดการความเสี่ยง | ผู้รับผิดชอบ | ผลการจัดการความเสี่ยง | ระดับความเสี่ยงหลังการจัดการ | คำอธิบายเพิ่มเติมของความเสี่ยงหลังการจัดการ (ความเสี่ยงที่คงเหลืออยู่) |
|---|---|---|---|---|---|---|
| ๑. การเตรียมความพร้อมรองรับการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (S๑, O๑, F๑, C๑) | - การเตรียมความพร้อมรองรับการตรวจประเมิน | - จัดการประชุมระดมแนวคิดเพื่อให้บุคลากรที่เกี่ยวข้องมีส่วนร่วม<br>- ใช้การขอความเห็นผ่านการสื่อสาร Online<br>- นำประเด็นยุทธศาสตร์มาเป็นกรอบในการดำเนินงาน<br>- การผลักดันให้แผนงาน/โครงการฯ บรรลุตามนโยบาย | กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม | ใช้กลยุทธ์ **การควบคุมความเสี่ยง** | พิจารณาระดับความเสี่ยง คือ โอกาสที่จะเกิดความเสียหาย (ระดับ ๕) และความรุนแรงของผลกระทบ (ระดับ ๕) ระดับความเสี่ยงคือ ๒๕ หลังการดำเนินการพบว่า ระดับความเสี่ยงหลังการจัดการมีค่าลดลง คือ ความรุนแรงของผลกระทบมีค่าลดลง (ระดับ ๒๐) | - เป็นนโยบาย ที่ผู้บริหารระดับสูงพิจารณา<br>- ข้อจำกัดด้านกรอบอัตรากำลังบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเพียงพอ |
| ๒. การยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (S๒, O๒) | - เสนอกรอบอัตรากำลัง<br>- การจัดหาผู้เชี่ยวชาญภายนอก | - จัดจ้างผู้เชี่ยวชาญภายนอกดำเนินการ<br>- ปรับลดกิจกรรมตามงบประมาณที่ได้รับ<br>- ติดตามผลการดำเนินงานทุก ๑ เดือน | กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม | ใช้กลยุทธ์ **การกระจายความเสี่ยง** | พิจารณาระดับความเสี่ยง คือ โอกาสที่จะเกิดความเสียหาย (ระดับ ๕) และความรุนแรงของผลกระทบ (ระดับ ๕) ระดับความเสี่ยงคือ ๒๕ หลังการดำเนินการพบว่า ระดับความเสี่ยงหลังการจัดการมีค่าลดลง คือ ความรุนแรงของผลกระทบมีค่าลดลง (ระดับ ๒๐) | - ข้อจำกัดของระบบเทคโนโลยีสารสนเทศที่ กรม สบส ใช้อยู่เดิม ไม่สามารถ Upgrade Software ได้เพราะมีผลกระทบต่อระบบงานเดิม<br>- บุคลากรมีข้อจำกัดในการเรียนรู้ด้านความมั่นคงปลอดภัยสารสนเทศ |

**ตารางที่ ๙** ตารางแสดงการประเมินความเสี่ยงด้านสารสนเทศ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓[๑๓]

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๑ นโยบาย** | | | | | | |
| ๑. แผนบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ | - การจัดทำแผนยุทธศาสตร์ล่าช้า<br>- การดำเนินงานไม่เป็นไปตามแผนที่กำหนด | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๑.๑ จัดทำและประกาศใช้ แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ - ๒๕๖๖<br>๑.๒ ทบทวนและประกาศใช้ คำสั่งแต่งตั้งคณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑.๓ ทบทวนและประกาศใช้ นโยบายและแนวปฏิบัติในการบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑.๔ ทบทวนและประกาศใช้ แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑.๕ ทบทวนและประกาศใช้ แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑.๖ ทบทวน จัดทำและประกาศใช้ คู่มือ ขั้นตอนการปฏิบัติงาน แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑.๗ จัดทำข้อเสนอเชิงนโยบายในการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ (HSS SOC Team) |

[๑๓] ไม่มีโครงการในปีงบประมาณ พ.ศ.๒๕๖๓

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๒ โครงสร้าง** | | | | | | |
| ๒. โครงสร้างกลุ่มเทคโนโลยีสารสนเทศ | - มีโครงสร้างองค์กรไม่ชัดเจน จากการเป็นการจัดตั้งหน่วยงานภายในของกรมสนับสนุนบริการสุขภาพ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๒.๑ เสนอแนวทางการดำเนินงานในการขับเคลื่อนกรมสนับสนุนบริการสุขภาพ ในการขับเคลื่อนการพัฒนารัฐบาลดิจิทัลระดับกรม เพื่อจัดตั้งโครงสร้างองค์กรที่ชัดเจน<br>๒.๒ จัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ (HSS SOC Team) ในการเป็นศูนย์รวมของทั้งหน่วยงานจริงและในรูปแบบเสมือนในการทดสอบระบบเชิงยุทธศาสตร์ ตรวจสอบภัยคุกคาม แจ้งเตือน กู้คืน เอื้อต่อการตอบสนองด้านความปลอดภัยและเหตุการณ์ฉุกเฉิน (IDR: ป้องกันภัยคุกคามและความเสี่ยง) รวมทั้งเฝ้าระวังและแจ้งเตือนสถานพยาบาล ตามแนวทางมาตรฐานสถานพยาบาลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์<br>๒.๓ จัดจ้างองค์กรภายนอก (Manage Security Service Provider หรือ MSSP) ดำเนินการรักษาความมั่นคงปลอดภัยสารสนเทศ (กระจายความเสี่ยง) |
| **หมวดที่ ๓ มาตรการด้านบุคลากร** | | | | | | |
| ๓. ภาระงานไม่สอดคล้องกับกรอบอัตรากำลังที่ได้รับ | - อัตรากำลังไม่เพียงพอในการปฏิบัติงาน | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๓.๑ วิเคราะห์ภาระงาน (FTE) ให้สอดคล้องกับภารกิจที่เหมาะกับการปฏิบัติงานให้มีประสิทธิภาพ<br>๓.๒ เสนอกรอบอัตรากำลังที่เหมาะสมในการปฏิบัติงาน<br>๓.๓ จัดจ้าง/จัดหา ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ จากหน่วยงานภายนอก เพื่อดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๓ มาตรการด้านบุคลากร** (ต่อ) | | | | | | |
| ๓. ภาระงานไม่สอดคล้องกับกรอบอัตรากำลังที่ได้รับ (ต่อ) | | | | | | ๓.๔ การเตรียมพร้อมบุคลากร รองรับการจัดตั้ง “ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ: HSS SOC Team (Security Operations Center)” |
| **หมวดที่ ๔ การบริหารจัดการสินทรัพย์ด้าน IT** | | | | | | |
| ๔. การบริหารจัดการสินทรัพย์ด้าน IT ไม่ครบถ้วน | - การวิเคราะห์ความเสี่ยงระบบสารสนเทศไม่ครบถ้วน | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๔.๑ รวบรวมข้อมูลสินทรัพย์ด้าน IT ให้ครบถ้วน ผ่าน ระบบ e-Asset ที่กรม สบส. จัดเตรียมไว้<br>๔.๒ วิเคราะห์ความเสี่ยงจากสินทรัพย์ด้าน IT<br>๔.๓ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ |
| **หมวดที่ ๕ การควบคุมการเข้าถึง** | | | | | | |
| ๕. การควบคุมการเข้าถึงระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ | ๕.๑ ความรู้ความเข้าใจ ของบุคลากรในการเข้าถึงระบบสารสนเทศ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๕.๑.๑ การสร้างความตระหนักและการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Awareness) สำหรับผู้ใช้งาน (User) |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๕ การควบคุมการเข้าถึง** (ต่อ) | | | | | | |
| ๕. การควบคุมการเข้าถึงระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ (ต่อ) | ๕.๑ ความรู้ความเข้าใจ ของบุคลากรในการเข้าถึงระบบสารสนเทศ (ต่อ)<br>๕.๒ การใช้รหัสผ่านที่ไม่ปลอดภัย | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๕.๑.๒ การฝึกซ้อมรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber drill)<br>๕.๒.๑ การกำหนดแนวทางการใช้รหัสผ่านที่ปลอดภัย<br>๕.๒.๒ การกำหนดสิทธิในการเข้าถึงระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ<br>๕.๒.๓ การใช้งานรหัสผ่านด้วยระบบอัตโนมัติ<br>๕.๒.๔ การกำหนดสิทธิในการเข้าถึงระบบ<br>๕.๒.๕ การถอนถอดสิทธิในการเข้าถึงระบบ<br>๕.๒.๖ การควบคุมการเข้าถึงรหัส (Password)<br>๕.๒.๗ การเก็บรหัสผ่านที่ดีด้านความมั่นคงปลอดภัยสารสนเทศ หลีกเลี่ยงการเก็บในรูปแบบ Plain Text<br>๕.๒.๘ ให้ผู้ใช้งานไม่สามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง |
| | ๕.๓ การเข้าใช้งานผ่านเครือข่ายที่ไม่ปลอดภัย | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๕.๓.๑ การตรวจสอบระบบเทคโนโลยีสารสนเทศด้วยวิธีการตรวจสอบช่องโหว่ Vulnerability Assessment (Web Application Hacking) และการเจาะระบบ (Penetration Testing) สำหรับผู้ดูแลระบบ (SysAdmin)<br>๕.๓.๒ การจัดหาระบบเครือข่ายที่ปลอดภัยมาใช้งาน (ขึ้นกับความจำเป็นและงบประมาณที่ได้รับ) |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๖ การเข้ารหัสข้อมูล** | | | | | | |
| ๖. เสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดีภายนอกและภายใน | - สูญเสียข้อมูลสำคัญของกรมสนับสนุนบริการสุขภาพ<br>- ข้อมูลรั่วไหล (Data Breach)<br>- กรมสนับสนุนบริการสุขภาพ ขาดความน่าเชื่อถือ สูญเสียภาพลักษณ์องค์กร | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๖.๑ ติดตั้งระบบบรองรับการเข้ารหัสข้อมูล<br>๖.๒ ส่งเสริมให้บุคลากรมีความรู้ในการใช้งาน<br>๖.๓ ติดตามผลจากข้อมูลรั่วไหล |
| **หมวดที่ ๗ ทางกายภาพ** | | | | | | |
| ๗. เสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดีภายนอกและภายใน | - สูญเสียข้อมูลสำคัญของกรมสนับสนุนบริการสุขภาพ<br>- ข้อมูลรั่วไหล (Data Breach)<br>- กรมสนับสนุนบริการสุขภาพ ขาดความน่าเชื่อถือ สูญเสียภาพลักษณ์องค์กร | (L๕) ๒ | (C๔) ๕ | ๑๐ | ต่ำ | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๗.๑ มีการแบ่งพื้นที่การรักษาความปลอดภัยเป็นสัดส่วน มีการควบคุมการเข้าถึง<br>๗.๒ มี รปภ.มีกุญแจเข้าในแต่ละชั้นของพื้นที่อาคาร<br>๗.๓ มีการกำหนดผู้รับผิดชอบถือกุญแจคนละดอก<br>๗.๔ มีการติดกล้องวงจรปิด<br>๗.๕ มีการปฏิบัติให้ครบถ้วนตามมาตรฐานที่กำหนด<br>๗.๖ การลงทะเบียนการเข้าออกในพื้นที่เฉพาะ (Restrict Area)<br>๗.๗ มีเครื่องดับเพลิงไว้พร้อมใช้งาน |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)** | | | | | | |
| ๘. เสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดีภายนอกและภายใน | ๘.๑ การรั่วไหลของข้อมูลสำคัญ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๘.๑.๑ การสร้างความตระหนักและการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Awareness) สำหรับผู้ใช้งาน (User)<br>๘.๑.๒ การฝึกซ้อมรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber drill)<br>๘.๑.๓ การสำรองข้อมูลตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ |
| | ๘.๒ การแพร่กระจายของโปรแกรมไม่พึงประสงค์ภายในระบบของกรมสนับสนุนบริการสุขภาพ เช่น Ransomware | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๘.๒.๑ ตรวจสอบความผิดปกติในการใช้งานผ่านเครือข่ายตลอดเวลา (Monitor around the clock)<br>๘.๒.๒ หากพบความผิดปกติให้ตัดการเชื่อมต่อทันทีและหาสาเหตุที่เกิดขึ้น<br>๘.๒.๓ ดำเนินงานตามแผนการสำรองข้อมูลและกู้คืนข้อมูล |
| | ๘.๓ การติดตั้งโปรแกรมไม่ถูกลิขสิทธิ์ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๘.๓.๑ การติดตั้งโปรแกรมป้องกันไวรัสไม่ครบทุกเครื่อง<br>๘.๓.๒ การกำหนดสิทธิ์การใช้งานผ่านณะบบเครือข่าย (Firewall Policy) |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)** (ต่อ) | | | | | | |
| ๘. เสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดีภายนอกและภายใน (ต่อ) | | | | | | ๘.๓.๓ กำหนดแนวทางการตรวจสอบโปรแกรมไม่พึงประสงค์และการตรวจสอบโปรแกรมอรรถประโยชน์ที่ไม่มีลิขสิทธิ<br>๘.๓.๔ การนำเทคโนโลยีใหม่ๆ มาปรับใช้ในงาน<br>๘.๓.๕ จำกัดการอนุญาตให้ผู้ปฏิบัติงานสามารถติดตั้งโปรแกรมใช้งานได้เองซึ่งเสี่ยงต่อการนำโปรแกรมไม่พึงประสงค์ เช่น ไวรัส มัลแวร์ หนอนไวรัสเข้ามาสู่ระบบได้<br>๘.๓.๖ การสำรองข้อมูลตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ |
| **หมวดที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)** | | | | | | |
| ๙. เสี่ยงต่อข้อมูลรั่วไหล | - มีมาตรการควบคุมในการใช้งานเครือข่าย แต่หน่วยงานระดับเขตยังไม่ได้รับมอบสิทธิและความรู้ในการดูแลเฝ้าระวังระบบ ทำให้การดูแลระบบไม่ครอบคลุม | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๙.๑ ควรมีการกำหนดผู้ดูแลระดับเขต ในการกำหนด Firewall Policy และคอยบริหารจัดการ User ที่ผ่านเข้าออก Firewall<br>๙.๒ มีการกำหนดแนวทางการส่งข้อมูลผ่านระบบเครือข่าย<br>๙.๓ ผู้ใช้งานควรใช้ Official e-Mail ในการติดต่อประสานงาน แต่สามารถใช้ Free e-Mail จากเอกชนได้ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)** (ต่อ) | | | | | | |
| ๙. เสี่ยงต่อข้อมูลรั่วไหล (ต่อ) | | | | | | ๙.๔ มีการจัดเก็บ Log file ที่ IT กรมฯ และเขตที่ได้รับมอบหมาย<br>๙.๕ เมื่อเกิดปัญหาจะมีการรายงานเข้ามายังส่วนกลาง และได้รับการแก้ไขจากผู้ดูแลระบบจากส่วนกลางได้จัดจ้างไว้ อีกทั้งมีการเตรียมความพร้อมบุคลากรผู้ดูแลระบบ (System Administrator)<br>๙.๖ ได้ดำเนินการประเมิน Gap Assessment<br>๙.๗ ได้ดำเนินการประเมิน Gap Analysis<br>๙.๘ ได้ดำเนินการวิเคราะห์ เจาะระบบดูช่องโหว่ของระบบ เพื่อดำเนินการปิดช่องโหว่ |
| **หมวดที่ ๑๐ การพัฒนาระบบ** | | | | | | |
| ๑๐. ข้อจำกัดด้านงบประมาณ และบุคลากร | - ไม่มีกรอบอัตรากำลัง<br>- งบประมาณได้รับการจัดสรรไม่เพียงพอ (ในปี ๒๕๖๒ และไม่ได้รับการจัดสรรงบประมาณ ในปี ๒๕๖๓) ส่งผลให้การดำเนินงานไม่เป็นไปตามเป้าหมายที่กำหนด<br>- ระบบไม่ได้รับการดูแลเพียงพอ จากข้อจำกัดฯ ดังกล่าว | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | ๑๐.๑ จัดทำแผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔ – ๒๕๖๖<br>๑๐.๒ จัดทำคำสั่งคณะกรรมการอำนวยการและคณะทำงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข<br>๑๐.๓ วิเคราะห์ภาระงาน “การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” (FTE)<br>๑๐.๔ วิเคราะห์คุณสมบัติตามตำแหน่ง จากข้อมูลบุคลากรด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๒ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๑๐ การพัฒนาระบบ** (ต่อ) | | | | | | |
| ๑๐. ข้อจำกัดด้านงบประมาณ และบุคลากร (ต่อ) | | | | | | ๑๐.๕ ควบคุม กำกับผลการดำเนินงานและแผนกำกับการจ้างดำเนินการยกระดับความเชื่อมั่นและสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๒ (ดำเนินการแล้วเสร็จ เมื่อวันที่ ๓๑ มีนาคม ๒๕๖๓ เนื่องจากกระบวนการจัดจ้างล่าช้า)<br>๑๐.๖ สนับสนุนการพัฒนาศักยภาพบุคลากรทั้ง User และ System Administrator ด้วยวิธีการ Training on the Job และ e-Learning ศึกษาด้วยตนเอง<br>๑๐.๗ ทบทวนแนวทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ แล้วเสร็จเมื่อวันที่ ๙ มีนาคม ๒๕๖๓<br>๑๐.๘ จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓ แล้วเสร็จ เมื่อวันที่ ๙ มีนาคม ๒๕๖๓ |
| **หมวดที่ ๑๑ การรับบริการผู้รับจ้างภายนอก** | | | | | | |
| ๑๑. การไม่สามารถปฏิบัติได้ตามข้อตกลงที่กำหนด | - การรั่วไหลของข้อมูล | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑๑.๑ การกำหนดแนวทางปฏิบัติการควบคุมกำกับผู้รับจ้างและการกำหนด TOR ไว้ชัดเจน<br>๑๑.๒ การกำกับ ดูแลผู้รับจ้างภายนอก |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๑๒ การบริหารจัดการปัญหา** | | | | | | |
| ๑๒. การจัดการปัญหาได้ทันท่วงที | - ความล่าช้าในการแก้ไขปัญหา<br>- ประชาชนขาดความเชื่อถือในการเข้าใช้บริการข้อมูลสารสนเทศ จากกรมสนับสนุนบริการสุขภาพ | (L๕) ๕ | (C๔) ๕ | ๒๕ | สูง | การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑๒.๑ การบริหารจัดการปัญหา กระบวนการขั้นตอนการให้บริการช่วยเหลือ การแก้ไขปัญหา ช่องทางการรับปัญหาและดำเนินการแก้ไขปัญหา<br>๑๒.๒ จัดทำรายงานดิจิทัล (Digital Platform) ในการจดบันทึกปัญหาหรือสาเหตุ/แนวทางการแก้ไขปัญหา<br>๑๒.๓ การรวบรวม สรุป วิเคราะห์ปัญหาอย่างเป็นระบบและประเภทปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อการวางแผนดำเนินการเชิงระบบในการแก้ปัญหาอย่างครอบคลุม |
| **หมวดที่ ๑๓ การบริหารความต่อเนื่องในการให้บริการ** | | | | | | |
| ๑๓. เสี่ยงต่อการดำเนินงานไม่ต่อเนื่องในการให้บริการ | - ประชาชนขาดความเชื่อถือในการเข้าใช้บริการข้อมูลสารสนเทศ จากกรมสนับสนุนบริการสุขภาพ | (L๕) ๔ | (C๔) ๕ | ๒๐ | ค่อนข้างสูง | ๑๓.๑ จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ<br>๑๓.๒ เตรียมความพร้อมรองรับให้บริการความต่อเนื่อง เช่น การบำรุงรักษาเครื่องมือระบบคอมพิวเตอร์และเครือข่าย การเฝ้าระวัง การสำรองข้อมูล เป็นต้น |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| **หมวดที่ ๑๔ การปฏิบัติงานความสอดคล้องกับกฎหมายที่เกี่ยวข้อง** | | | | | | |
| ๑๔. เสี่ยงต่อความไม่ถูกต้องตามกฎหมาย | - ประชาชนขาดความเชื่อถือในการเข้าใช้บริการข้อมูลสารสนเทศ จากกรมสนับสนุนบริการสุขภาพ | (L๕) ๔ | (C๔) ๕ | ๒๐ | ค่อนข้างสูง | ๑๔.๑ มีการวางแผนวิเคราะห์ระบบงานให้สอดคล้องกับกฎหมาย ได้แก่<br>๑๔.๑.๑ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม<br>๑๔.๑.๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒<br>๑๔.๑.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒<br>๑๔.๑.๔ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม<br>๑๔.๑.๕ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐<br>๑๔.๒ การปฏิบัติงานไม่ละเมิดต่อกฎหมายที่เกี่ยวข้อง |

<u>หมายเหตุ</u> เกณฑ์การประเมิน การให้คะแนนโอกาสที่จะเกิดและผลกระทบ

ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด
ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย
ระดับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง
ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก
ระดับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด

แผนผังประเมินความเสี่ยง

| ผลกระทบของความเสี่ยง | | | | |
|---|---|---|---|---|
| ๕ | ๑๐ | ๑๕ | ๒๐ | ๒๕ |
| ๔ | ๘ | ๑๒ | ๑๖ | ๒๐ |
| ๓ | ๖ | ๙ | ๑๒ | ๑๕ |
| ๒ | ๔ | ๖ | ๘ | ๑๐ |
| ๑ | ๒ | ๓ | ๔ | ๕ |

สีแดง ระดับความเสี่ยงสูง ค่าระหว่าง ๑๕ - ๒๕
สีเหลือง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง ๘ - ๑๔
สีเขียว ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง ๔ - ๗
สีฟ้า ระดับความเสี่ยงต่ำ ค่าระหว่าง ๑ - ๓

# ภาคผนวก

หมายเหตุ เอกสารภายใน กรมสนับสนุนบริการสุขภาพ
จัดเก็บที่ งานพัฒนาระบบเทคโนโลยีสารสนเทศ
กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข
Tel.: +๖๖ ๒ ๑๙๓ ๗๐๐๐ ต่อ ๑๘๒๐๘
e-Mail: isms@hss.mail.go.th

# บันทึกข้อความ

**ส่วนราชการ** งานพัฒนาระบบเทคโนโลยีสารสนเทศ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม โทร. ๑๘๒๐๘

**ที่** สธ ๐๗๐๑.๔/๒๑๔๙ **วันที่** ๑๖ พฤศจิกายน ๒๕๖๓

**เรื่อง** ขออนุมัติเผยแพร่ข้อมูลด้านการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ

เรียน ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม

ตามที่ งานพัฒนาระบบเทคโนโลยีสารสนเทศ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม ได้รับผิดชอบภารกิจด้านการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ตามมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศ (ISMS : Information Security Management System) มาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ นั้น

ในการนี้ งานพัฒนาระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเอกสารที่เกี่ยวข้องเสร็จเรียบร้อยแล้ว เห็นควรเสนอการเผยแพร่ข้อมูลที่ URL https://hss.moph.go.th เพื่อให้บุคลากรภายในหน่วยงานและผู้เกี่ยวข้องรับทราบข้อมูลและยึดถือเป็นแนวปฏิบัติเป็นไปในแนวเดียวกัน ในหัวข้อ (Topic) “DCIO ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม” จากเดิม คือ หัวข้อ “CIO กรม” จำนวน ๕ เรื่อง รายละเอียดดังนี้

เรื่องที่ ๑ ๒๐๒๐ คำสั่งผู้บริหารเทคโนโลยีสารสนเทศระดับกรม กรมสนับสนุนบริการสุขภาพ

เรื่องที่ ๒ ๒๐๒๑ แผนยุทธศาสตร์การบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๔-๒๕๖๖

เรื่องที่ ๓ ๒๐๒๐ แผนบริหารความเสี่ยงด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ.๒๕๖๓

เรื่องที่ ๔ ๒๐๒๑ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

เรื่องที่ ๕ ๒๐๒๑ แผนบริหารความต่อเนื่องด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

รายละเอียดตาม QR Code แนบท้าย

จึงเรียนมาเพื่อทราบ และได้โปรดแจ้งผู้เกี่ยวข้องดำเนินการต่อไปด้วย จะเป็นพระคุณ

(นางสาวธนิมา สังข์สุวรรณ์)
นักวิชาการสาธารณสุขชำนาญการ

(นายอภินันท์ นิลฉาย)
ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ

**ข้อมูลสำหรับ Topic : DCIO**

สมรรถนะเป็นฐาน
สร้างสรรค์สิ่งใหม่
บริการด้วยใจ
ใฝ่สามัคคี