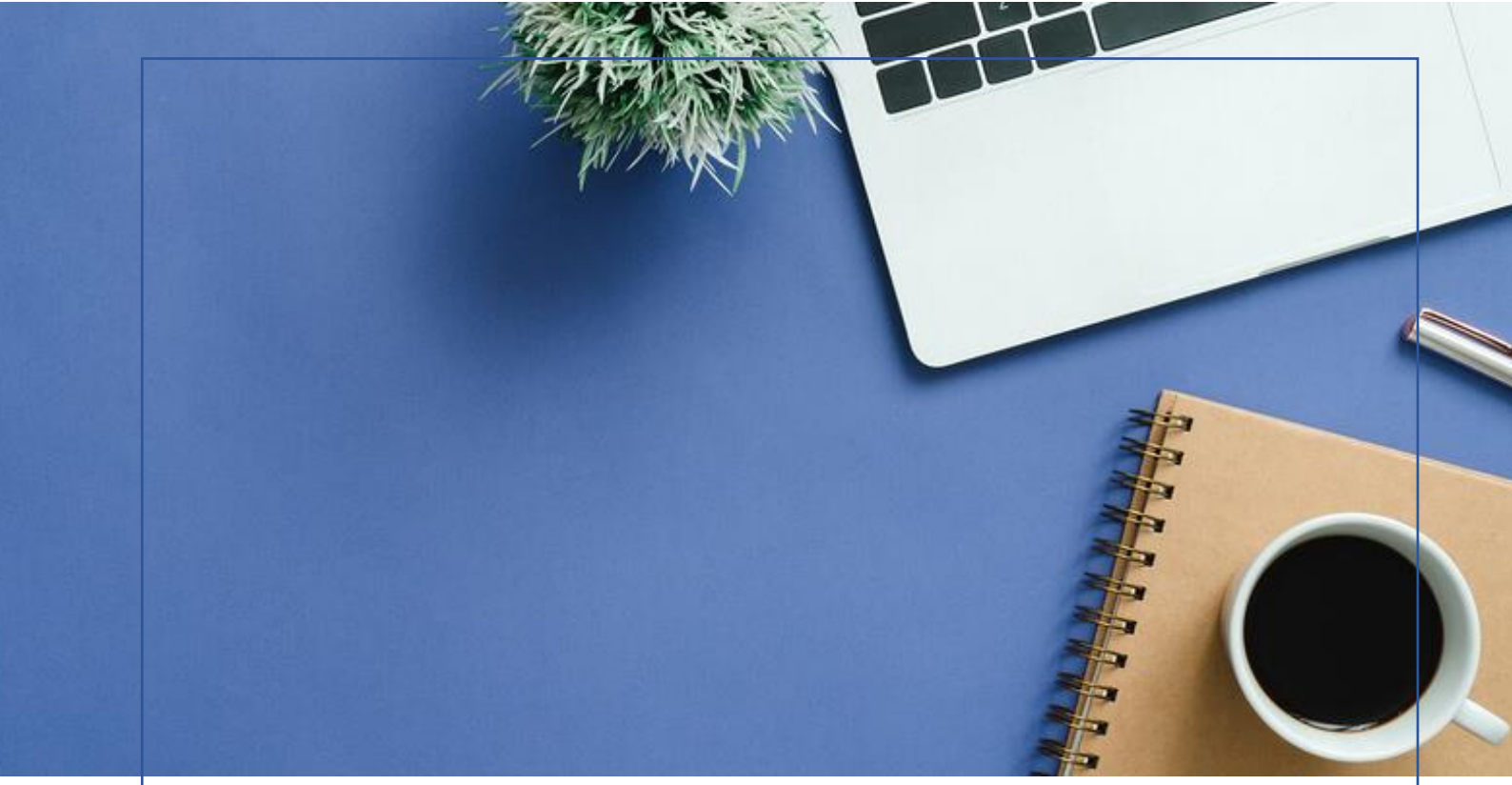

# แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ

พ.ศ. ๒๕๖๓

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข



# แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ

# ของกรมสนับสนุนบริการสุขภาพ

# สารบัญ

**หน้า**

# แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ
# กรมสนับสนุนบริการสุขภาพ

## ๑. บทนำ

ตามที่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ รวมทั้งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพ ในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีผลกระทบต่อประชาชนโดยตรง จากการเชื่อมโยงข้อมูลกับหน่วยงานที่เกี่ยวข้อง ควรต้องผ่านเกณฑ์มาตรฐานเพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการในระบบบริการสุขภาพรวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

กรมสนับสนุนบริการสุขภาพ ได้วิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศ โดยพิจารณาจากเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) และภัยพิบัติหรือสถานการณ์อื่นๆ รวมถึงได้กำหนดแนวทางการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต การสำรองและการกู้คืนข้อมูลสารสนเทศ เพื่อจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ อย่างน้อยปีละ ๑ ครั้ง สำหรับใช้เป็นแนวทางปฏิบัติงานต่อไป

## ๒. วัตถุประสงค์

๒.๑ เพื่อให้ กรมสนับสนุนบริการสุขภาพมีแนวทางในการระบุและประเมินความเสี่ยงด้านสารสนเทศ รวมถึงการกำหนดแนวทางบริหารความเสี่ยงด้านสารสนเทศ ในการป้องกัน จัดการและลดความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้และทำให้กรมสนับสนุนบริการสุขภาพสามารถดำเนินงานได้อย่างต่อเนื่อง

๒.๒ เพื่อให้ กรมสนับสนุนบริการสุขภาพมีแนวทางในการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศและสามารถเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤตที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงมีแนวปฏิบัติในการบริหารจัดการ กำกับ ตรวจสอบ และดูแลรักษาระบบคอมพิวเตอร์และระบบสารสนเทศให้มีความมั่นคง ปลอดภัย มีเสถียรภาพและพร้อมใช้งานตลอดเวลา

๒.๓ เพื่อให้ กรมสนับสนุนบริการสุขภาพมีแนวทางในการสำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ โดยสามารถกู้คืนระบบและข้อมูลดังกล่าวได้ทันที เพื่อให้ผู้ใช้งาน (User) สามารถปฏิบัติงานได้อย่างต่อเนื่อง

## ๓. ขอบเขต

แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๓ ฉบับนี้ เพื่อรองรับสถานการณ์ฉุกเฉินในสภาวะวิกฤตในพื้นที่ของกรมสนับสนุนบริการสุขภาพ ดังนี้

๓.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People)

๓.๑.๑ บุคลากรของกรมสนับสนุนบริการสุขภาพ

๓.๑.๒ บุคคลภายนอก ผู้ไม่ประสงค์ดี

๓.๒ เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process)

๓.๒.๑ การโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)

๓.๒.๒ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค

๓.๒.๓ เหตุการณ์ไฟฟ้าดับ

๓.๒.๔ เหตุการณ์อัคคีภัย

๓.๒.๕ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง

๓.๓ เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology)

๓.๓.๑ ทรัพย์สิน ครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี

๓.๓.๒ การสื่อสารและเครือข่ายสารสนเทศ

๓.๓.๓ โครงข่ายสารสนเทศ

๓.๓.๔ ข้อมูลสารสนเทศ

**๔. การวิเคราะห์ความเสี่ยงด้านสารสนเทศ**

กรมสนับสนุนบริการสุขภาพ มีภารกิจการคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพและส่งเสริมผู้ประกอบการด้านบริการสุขภาพเพื่อประชาชนมีศักยภาพในการพึ่งพาตนเอง มีระบบขึ้นทะเบียนและออกใบอนุญาตสถานพยาบาลและสถานประกอบการเพื่อสุขภาพ เป็นหน่วยงานที่เกี่ยวข้องกับการเก็บรักษาข้อมูลส่วนบุคคล ด้านธุรกิจบริการสุขภาพรองรับการดำเนินงานระหว่างภาครัฐและเอกชน ที่สนับสนุนการทำธุรกรรมอิเล็กทรอนิกส์ด้านระบบบริการสุขภาพทั้งภายในและต่างประเทศ การพัฒนานวัตกรรมดิจิทัลด้านระบบบริการสุขภาพตามนโยบายเศรษฐกิจดิจิทัล (Digital Economy) และภารกิจกรมสนับสนุนบริการสุขภาพมีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่ต้องผ่านเกณฑ์มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งการบริหารราชการของกรมสนับสนุนบริการสุขภาพ ด้านขับเคลื่อนการพัฒนารัฐบาลดิจิทัล (Digital Government)

ผลจากการวิเคราะห์ดังกล่าว พบว่าความเสี่ยงที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และสารสนเทศ รวมถึงข้อมูลสารสนเทศ มีดังนี้

๔.๑ ความเสี่ยงที่เกิดจากบุคคล (People) ดังนี้

๔.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร กรมสนับสนุนบริการสุขภาพ หมายถึง บุคลากรของ กรมสนับสนุนบริการสุขภาพ ขาดความรู้ ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ เช่น ด้านฮาร์ดแวร์ ด้านซอฟท์แวร์ และด้านเครือข่าย รวมถึงการใช้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศที่ไม่เหมาะสม

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

๔.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) ดังนี้

๔.๒.๑ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) หมายถึง ผู้ที่ลักลอบเข้าไปโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ หากศูนย์ข้อมูลดังกล่าวไม่ได้รับการป้องกันที่ดี เช่น มาตรการในการเข้าถึงห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ เครื่องอ่านบัตรแถบแม่เหล็ก กล้องวงจรปิด และเจ้าหน้าที่รักษาความปลอดภัย เป็นต้น

๔.๒.๒ ความเสี่ยงที่เกิดจากด้านเทคนิค หมายถึง เหตุการณ์หรือภัยที่เกิดจากอุปกรณ์ ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ทำงานไม่เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้ เช่น อุปกรณ์ประมวลผลข้อมูล (Process Device) ชำรุด เสียหาย เนื่องจากอุปกรณ์บางรายการเสื่อมสภาพตามอายุการใช้งาน ระบบปรับอากาศชำรุดส่งผลให้ อุณหภูมิภายในห้องสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ที่ให้บริการหยุดการทำงาน ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถใช้งานได้ หรืออาจได้รับความเสียหาย

๔.๒.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ

๔.๒.๓.๑ เหตุการณ์ไฟฟ้าดับ หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟฟ้าดับ ซึ่งส่งผลให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ไม่มีแหล่งพลังงานที่ใช้ในการเปิด ระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับให้บริการ เช่น สายไฟฟ้าขาด ไฟฟ้าช็อต หม้อแปลงไฟฟ้าที่ติดตั้งบริเวณกรมสนับสนุนบริการสุขภาพ หรือภายในกระทรวงสาธารณสุขระเบิดเสียหาย

๔.๒.๓.๒ เหตุการณ์อัคคีภัย หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟไหม้ ซึ่งเป็นเหตุการณ์ที่สร้างความเสียหายร้ายแรงที่สุด ทำให้ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ถูกไฟไหม้จนทำให้ไม่สามารถปฏิบัติงานได้ ซึ่งเกิดได้หลายสาเหตุ เช่น ไฟฟ้าลัดวงจร หรือไฟไหม้บริเวณอื่นแล้วไหม้ลุกลามมาที่ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์

๔.๒.๓.๓ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง หมายถึง อันเกิดจากภัยตามธรรมชาติหรือสถานการณ์ที่เกิดจากกลุ่มบุคคล ซึ่งอาจไม่เกิดผลกระทบโดยตรงต่อการให้บริการของระบบคอมพิวเตอร์และระบบสารสนเทศ แต่จะเกิดผลกระทบต่อการเข้าไปปฏิบัติงานภายในพื้นที่ กรมสนับสนุนบริการสุขภาพ

๔.๓ ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) เช่น

๔.๓.๑ ทรัพย์สินครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software)

๔.๓.๒ เครือข่ายสารสนเทศ และเครือข่ายเสมือน (Information Network and Virtual Machine)

๔.๓.๓ โครงข่ายการสื่อสาร (Communication Network)

๔.๓.๔ ข้อมูลและสารสนเทศ (Information)

**๕. การประเมินความเสี่ยงด้านสารสนเทศ**

การประเมินความเสี่ยงด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ได้ประเมินความเสี่ยงที่เกิดจากบุคคล จากทางด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ ตามข้อ ๓ และ ๔ เป็นแนวทางในการดำเนินงาน โดย กรมสนับสนุนบริการสุขภาพ ได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพแล้ว ปรากฏ ดังนี้

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕.๑ ความเสี่ยงที่เกิดจากบุคคล (People) | | | | | | |
| (๑) เหตุการณ์หรือภัยที่เกิดจากบุคลากร ภายในกรมสนับสนุนบริการสุขภาพ | - ระบบคอมพิวเตอร์ติดไวรัส หรือหนอนอินเทอร์เน็ตจากอินเตอร์เน็ต หรือไฟล์ที่คัดลอกจากอุปกรณ์ บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk, Storage ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศประมวลผล ข้อมูลได้ช้าลงหรืออาจทำงานผิดพลาดได้ | ๕ | ๕ | ๒๕ | สูง | - ผู้ดูแลระบบ (System Administrator) ตัดการเชื่อมต่อเครื่องที่ติดไวรัสดังกล่าว ออกจากระบบเครือข่าย ภายใน และดำเนินการสแกนไวรัสเพื่อกำจัดไวรัสเครื่องดังกล่าว<br>- หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) |
| (๒) เหตุการณ์หรือภัย ที่เกิดจากผู้ไม่ประสงค์ดี | - ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบหน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์ และระบบสารสนเทศล่มได้ | ๕ | ๕ | ๒๕ | สูง | ตรวจพอร์ตทั้งหมดที่ใช้เชื่อมต่อแล้วให้ปิดพอร์ตที่ไม่ได้ใช้งาน โดยทันที |
| ๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) | | | | | | |
| (๑) เหตุการณ์หรือภัย ที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) | - อุปกรณ์ประมวลผลข้อมูล (Process Device) สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ กรมสนับสนุนบริการสุขภาพ | ๓ | ๕ | ๑๕ | ค่อนข้างสูง | - ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป<br>- ผู้ดูแลระบบ (System Administrator) ตรวจสอบความครบถ้วนและความเสียหาย |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| | โดยเฉพาะข้อมูลที่เป็นความลับ<br>- ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถให้บริการได้เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้ | | | | | ของอุปกรณ์ประมวลผลข้อมูล (Process Device) และผลกระทบต่อระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ |
| (๒) เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค | - อุปกรณ์ประมวลผลข้อมูล (Process Device) บางรายการหยุดทำงานชั่วขณะหรือใช้งาน ระบบคอมพิวเตอร์และระบบสารสนเทศ ได้ไม่เต็มประสิทธิภาพ<br>- ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิในห้องศูนย์ข้อมูลและสารสนเทศสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้รับความเสียหาย | ๑ | ๕ | ๕ | ค่อนข้างต่ำ | - ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป<br>- ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ ประมวลผลข้อมูล (Process Device) หรือระบบปรับอากาศที่ได้รับความเสียหาย หากเสียหายเล็กน้อย ให้ดำเนินการแก้ไขและเปิดใช้งาน ระบบคอมพิวเตอร์และระบบสารสนเทศต่อไป |
| (๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ | (๓.๑) เหตุการณ์ไฟฟ้าดับ<br>- อุปกรณ์ประมวลผลข้อมูล (Process Device) บางรายการหยุดทำงานชั่วขณะหรือใช้งาน ระบบคอมพิวเตอร์และระบบสารสนเทศ ได้ไม่เต็มประสิทธิภาพ | ๑ | ๕ | ๕ | ค่อนข้างต่ำ | - ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป<br>- ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| (๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | - ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิในห้องศูนย์ข้อมูลและสารสนเทศสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้รับความเสียหาย | | | | | และระบบปรับอากาศ พร้อมทั้ง รายงานให้ DCIO ทราบ เพื่อสั่งการต่อไป<br>- DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการชั่วคราวเนื่องจากไฟฟ้าดับ<br>- DCIO ประสานงานกับกลุ่มเทคโนโลยีสารสนเทศเพื่อสอบถามปัญหา และระยะเวลา การแก้ไขที่จะสามารถกลับมาให้บริการได้<br>- ผู้ดูแลระบบ (System Administrator) เปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมทั้งรายงานให้ DCIO และ อธิบดีทราบตามลำดับ<br>- DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้ปกติ |
| | (๓.๒) เหตุการณ์อัคคีภัย<br>- สินทรัพย์ (Asset) ที่ย้ายไม่ทันอาจถูกไฟไหม้<br>- อุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ไม่สามารถให้บริการได้ | ๑ | ๕ | ๕ | ค่อนข้างต่ำ | แนวทางปฏิบัติตามแผนป้องกันและระงับอัคคีภัย ในการรักษาความมั่นคงปลอดภัยสารสนเทศ<br><u>กรณีที่ ๑</u> ไฟเริ่มไหม้หรือสามารถดับไฟได้<br>- ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| (๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | (๓.๒) เหตุการณ์อัคคีภัย (ต่อ) | | | | | - ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ และให้แจ้งให้อธิบดีทราบโดยเร็ว<br>- ผู้ดูแลระบบ (System Administrator) ประเมินสถานการณ์ในเบื้องต้นว่า ควรหยุดให้บริการระบบคอมพิวเตอร์ และระบบสารสนเทศหรือไม่<br>- ถ้าหยุดให้บริการ DCIO สั่งการให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการ ชั่วคราวเนื่องจากเหตุไฟไหม้<br>- ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ พร้อมทั้งรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ DCIO และอธิบดีทราบตามลำดับชั้น และสั่งการต่อไป<br>- หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ (System Administrator) ดำเนินการ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| (๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | (๓.๒) เหตุการณ์อัคคีภัย (ต่อ) | | | | | แก้ไข และเปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ<br>- DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้แล้ว<br>- หากเสียหายมากให้ผู้ดูแลระบบ (System Administrator) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยี และ DCIO ทราบ ตามลำดับชั้นและสั่งการต่อไป<br><br><u>กรณีที่ ๒</u> ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง<br>- ให้ผู้พบเหตุโทรแจ้งหน่วยดับเพลิง เป็นลำดับแรก และแจ้งให้ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ และ DCIO ทราบโดยเร็ว<br>- ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณไฟที่เริ่มลุกลามและบริเวณโดยรอบ หากไม่สามารถระงับเหตุได้ ให้ออกจากพื้นที่โดยเร็ว<br>-DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุด ให้บริการเนื่องจากเหตุไฟไหม้ |

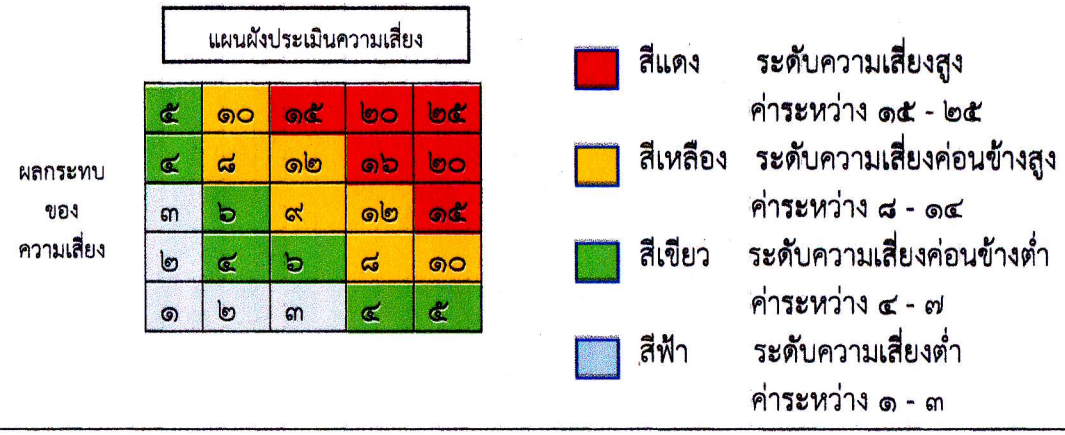
| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ) | | | | | | |
| (๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ) | (๓.๓) เหตุการณ์ที่เกิดจาก ภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง<br>- เช่น กรณีการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง อาจถูกปิดกั้นการเข้าออกและอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำบริเวณกระทรวงสาธารณสุข ซึ่งส่งผลกระทบต่อห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ หรือสถานที่ปฏิบัติงานบริเวณอาคาร กรมสนับสนุนบริการสุขภาพ | ๑ | ๕ | ๕ | ค่อนข้างต่ำ | - หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยี และ DCIO ทราบ ตามลำดับชั้นและสั่งการต่อไป<br>- หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยี และ DCIO ทราบ ตามลำดับชั้นและสั่งการต่อไป<br>- ถ้าเกิดเหตุการณ์ไฟฟ้าดับ ให้ดำเนินการตามแนวทางแก้ไขตาม ข้อ ๕<br>- กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย ตามที่ กรมสนับสนุนบริการสุขภาพกำหนด |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕.๓ ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) | | | | | | |
| ๕.๓.๑ ทรัพย์สินครุภัณฑ์ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software) | - ไม่เพียงพอต่อการใช้งาน<br>- ไม่พร้อมใช้งาน | ๒ | ๕ | ๑๐ | ค่อนข้างสูง | - จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ<br>- สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งานตามแผนที่กำหนด<br>- กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง<br>- ปรับปรุงระบบการยืม-คืน เมื่อนำอุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอกสำนักงาน<br>- ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |
| ๕.๓.๒ เครือข่ายสารสนเทศ และเครือข่ายเสมือน (Information Network and Virtual Machine) | - ไม่เพียงพอต่อการใช้งาน<br>- ไม่พร้อมใช้งาน | ๒ | ๕ | ๑๐ | ค่อนข้างสูง | - กำหนดแนวทางการควบคุม กำกับติดตามประเมินผลการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง<br>- ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสเกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕.๓ ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) (ต่อ) | | | | | | |
| ๕.๓.๓ โครงข่ายการสื่อสาร (Communication Network) | - ไม่เพียงพอต่อการใช้งาน<br>- ไม่พร้อมใช้งาน | ๒ | ๕ | ๑๐ | ค่อนข้างสูง | - กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง<br>- ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |
| ๕.๓.๔ ข้อมูลและสารสนเทศ (Information) | - ไม่พร้อมใช้งาน | ๒ | ๕ | ๑๐ | ค่อนข้างสูง | - กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัส<br>- ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ |

<u>หมายเหตุ</u> เกณฑ์การประเมินการให้คะแนนโอกาสที่จะเกิดและผลกระทบ

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



**๖. การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต**

เนื่องจากเหตุการณ์ที่เป็นความเสี่ยงด้านสารสนเทศข้างต้น กรมสนับสนุนบริการสุขภาพ จึงได้ดำเนินการจัดทำแนวทางการเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต เพื่อป้องกันภัยจากเหตุการณ์หรือภัยที่จะเกิดขึ้น ดังนี้

๖.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People)

๖.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากรของกรมสนับสนุนบริการสุขภาพ มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) กำหนดให้ปฏิบัติตามประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) การสร้างความรู้ความเข้าใจในการใช้ระบบคอมพิวเตอร์และระบบสารสนเทศเบื้องต้น โดยการจัดอบรมให้กับบุคลากร หรือส่งไปอบรมร่วมกับหน่วยงานภายนอกที่จัดขึ้น เพื่อลดความเสี่ยงด้านสารสนเทศ

(๓) มีการประชาสัมพันธ์ให้ความรู้แก่บุคลากรผ่านช่องทางสื่อสารต่างๆ ตามความเหมาะสม เช่น ผ่านระบบ Website ติดบอร์ดประชาสัมพันธ์ e-Mail, Line, Chat, Facebook หรือสื่อ Social Media อื่นๆ ของกลุ่มเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ เป็นต้น

๖.๑.๒ เหตุการณ์หรือภัยที่เกิดจากบุคคลภายนอก ผู้ไม่ประสงค์ดี มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งและใช้งาน Firewall เพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์ และระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device)

(๒) ติดตั้งซอฟต์แวร์ป้องกันไวรัส (Anti Virus)/ หนอนคอมพิวเตอร์ (Worm) หรือโปรแกรมไม่ประสงค์ดี (Anti Malware) ที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๖.๒ เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process)

๖.๒.๑ การโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) มีมาตรการควบคุมการเข้า - ออกห้องศูนย์ข้อมูล (Data Center) ดังนี้

(๑.๑) ปฏิบัติตามหลักเกณฑ์สำหรับการปฏิบัติงานภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ ตามที่ กรมสนับสนุนบริการสุขภาพกำหนด

(๑.๒) การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ ต้องได้รับอนุมัติจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ ก่อนเริ่มดำเนินการทุกครั้ง

(๑.๓) ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ เว้นแต่ได้รับอนุญาตจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ

(๑.๔) ผู้ใช้งาน (User) หรือบุคคลภายนอก

(๑.๔.๑) ต้องติดบัตรแสดงตนตลอดระยะเวลา ที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (System Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอกตลอดเวลา

(๑.๔.๒) ต้องไม่นำอาหารหรือเครื่องดื่มเข้าไปในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์

(๑.๔.๓) ห้ามสูบบุหรี่ ในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์

(๑.๕) มีเจ้าหน้าที่รักษาความปลอดภัยตลอด ๒๔ ชั่วโมง

(๑.๖) มีการติดตั้งระบบควบคุมการเข้าถึง (Access Control) ห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ด้วยระบบอิเล็กทรอนิกส์

(๑.๗) มีการติดตั้งกล้องวงจรปิดบันทึกเหตุการณ์บริเวณทางเข้าและภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์เพื่อเฝ้าระวังเหตุการณ์หรือภัยที่จะเกิดขึ้น

๖.๒.๒ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) มีการตรวจความพร้อมอุปกรณ์ประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพและด้านเทคนิคให้พร้อมใช้งานอยู่เสมออย่างน้อยเดือนละ ๑ ครั้ง หากพบอุปกรณ์ประมวลผลข้อมูล (Process Device)

หรืออุปกรณ์ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ชำรุดเสียหาย หรือใกล้เสื่อมสภาพการใช้งาน ให้รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อรายงานตามลำดับชั้นและสั่งการแก้ไข ด้วยการซ่อมแซม หรือจัดซื้อ ทดแทนต่อไป

(๒) มีการตรวจสอบปริมาณการเข้าถึงเครือข่ายภายนอก (Internet) เพื่อสังเกตปริมาณ การใช้งาน อัตราความเร็วของข้อมูล เพื่อเฉลี่ยแบนด์วิดท์ (Bandwidth) ให้ทั่วถึงทั้งองค์กร และป้องกัน ไม่ให้ผู้ใช้งาน (User) มีการใช้แบนด์วิดท์ (Bandwidth) มากเกินไป

๖.๒.๓ เหตุการณ์ไฟฟ้าดับ มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

มีการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) จำนวน ๒ เครื่อง ขนาด ๓๐ KVA และ ๒๐ KVA เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงอุปกรณ์ประมวลผลข้อมูล (Process Device) โดยทั้ง ๒ เครื่อง สามารถสำรองไฟฟ้า ได้เป็นเวลาประมาณ ๓๐ นาที ซึ่งเพียงพอต่อการจัดเก็บและสำรองข้อมูลสารสนเทศในกรณีที่เกิดไฟฟ้าดับ

๖.๒.๔ เหตุการณ์อัคคีภัย มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) มีการติดตั้งอุปกรณ์ตรวจจับควัน กรณีเกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้น ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือน เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุทราบและเข้ามาระงับเหตุฉุกเฉินก่อนเกิดอัคคีภัยได้อย่างทันท่วงที เพราะเป็นภัยที่มีผลกระทบรุนแรงที่สุด

(๒) มีการติดตั้งถังดับเพลิงชนิดที่ใช้สารเคมีไม่ทำอันตรายต่ออุปกรณ์ประมวลผลข้อมูล (Process Device) ไว้ในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ จำนวน ๑ ถัง และห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ จำนวน ๒ ถัง เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุใช้ระงับเหตุก่อนไฟเริ่มลุกลามถึงขั้นรุนแรง

๖.๒.๕ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ให้ผู้ใช้งาน (User) สำรองข้อมูลสารเทศส่วนตัวลงในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk

(๒) มีเจ้าหน้าที่รักษาความปลอดภัยตลอด ๒๔ ชั่วโมง เพื่อป้องกันไม่ให้บุคคลภายนอกเข้าไปภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์โดยไม่ได้รับอนุญาต

(๓) ตรวจสอบการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เพื่อให้ผู้ใช้งาน ( User) ปฏิบัติงานจากภายนอกกรมสนับสนุนบริการสุขภาพ (Teleworking) โดยผ่านเครือข่ายภายนอก (Internet) ได้

(๔) ตรวจสอบความพร้อมของข้อมูลสารสนเทศที่ได้สำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ได้บันทึกลงในตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใด สำหรับเตรียมนำไปกู้คืน จากศูนย์สำรองข้อมูล (Disaster Recovery Site : DR Site) ณ ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี หรือตามที่ผู้บริหารเห็นชอบ หากเกิดเหตุการณ์ฉุกเฉินในสภาวะวิกฤตจนส่งผลให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต้องปิดระบบการให้บริการถูกปิดลง

(๕) เมื่อ กรมสนับสนุนบริการสุขภาพ ได้รับแจ้งว่าจะเกิดเหตุชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมืองบริเวณกระทรวงสาธารณสุข ซึ่งอาจถูกปิดกั้นการเข้าออก และอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำให้ผู้ดูแลระบบ (System Administator) นำตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใด ที่สำรองข้อมูลไว้ไปเก็บในสถานที่ปลอดภัย

๖.๓ เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology)

๖.๓.๑ ทรัพย์สิน ครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี

๖.๓.๒ การสื่อสารและเครือข่ายสารสนเทศ

๖.๓.๓ โครงข่ายสารสนเทศ

๖.๓.๔ ข้อมูลสารสนเทศ

มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ

**๗. กลยุทธ์ความต่อเนื่องในสภาวะวิกฤต**

หากเหตุการณ์หรือภัยได้เกิดขึ้นแล้ว ต้องมีการดำเนินกลยุทธ์ความต่อเนื่องในสภาวะวิกฤต เพื่อให้การปฏิบัติงานของบุคลากร ดำเนินการไปได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุด ดังนี้

| ทรัพยากร | กลยุทธ์ความต่อเนื่อง |
|---|---|
| ๑. สถานที่ปฏิบัติงาน กรมสนับสนุนบริการสุขภาพ | **๑. กำหนดพื้นที่ปฏิบัติงานสำรอง ได้แก่ ห้องคอมพิวเตอร์หรือพื้นที่อื่นๆ** โดยประสานงานและสำรวจความเหมาะสมของสถานที่<br>**๒. ประสานขอใช้พื้นที่กับส่วนราชการอื่นเป็นสถานที่ปฏิบัติงาน สำรองเพิ่มเติม**<br>๓. หากพื้นที่ปฏิบัติงานสำรองมีพื้นที่จำกัด หรืออาจเกิดอันตรายระหว่างเดินทางไปปฏิบัติงาน ให้บุคลากรปฏิบัติงานจากที่พักอาศัย |
| ๒. วัสดุอุปกรณ์ | ๑. จัดหาเครื่องคอมพิวเตอร์สำรองพร้อมอุปกรณ์ในการเข้าถึงระบบเครือข่าย เพื่อให้ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศได้<br>๒. จัดเตรียมอุปกรณ์สารสนเทศสำหรับนำมาใช้ในการปฏิบัติงาน เช่น เครื่องพิมพ์ (Printer) เครื่องสแกนเนอร์ (Scaner) และสายเชื่อมต่อระบบเครือข่ายเฉพาะที่ (Lan)<br>๓. ผู้ใช้งาน (User) สามารถใช้คอมพิวเตอร์แบบพกพาส่วนตัวในการปฏิบัติงานได้ |
| ๓. ระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ | ๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศได้ติดตั้ง และจัดเก็บไว้ใน ณ ห้องศูนย์กลางข้อมูล (Data Center) อาคารกรมสนับสนุนบริการสุขภาพ ชั้น ๒ ซึ่งรองรับการเข้าถึงจากภายนอก โดยการรับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) และมีการเข้ารหัส รักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)<br>๒. ประสานศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี เพื่อจัดเตรียมไซต์สำรอง (Disaster Recovery Site : DR Site) เมื่อเกิดเหตุฉุกเฉินหรือสภาวะวิกฤต<br>๓. กลุ่มเทคโนโลยีสารสนเทศพิจารณาและนำตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใด ที่สำรองระบบคอมพิวเตอร์ ระบบสารสนเทศและข้อมูลสารสนเทศ ณ ห้องศูนย์กลางข้อมูล (Data Center) ไปไว้ในสถานที่ปลอดภัย<br>๔. สำหรับระบบ SMART, GFMIS ซึ่งเป็นระบบสารสนเทศตามภารกิจหลัก เพื่อบริการแก่บุคลากรและส่วนราชการที่เกี่ยวข้อง ได้ติดตั้ง ณ ศูนย์พัฒนาการสาธารณสุขมูลฐานภาคกลาง จังหวัดชลบุรี<br>๕. ให้ผู้ใช้งาน (User) สำรองข้อมูลสารสนเทศที่จำเป็นและสำคัญไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive, Externel Harddisk หรือ Share Drive ที่กรมจัดให้ เช่น GDCC (Cloud Computing Services) |
| ๔. บุคลากร | ๑. หากผู้ดูแลระบบ (System Administrator) มีจำนวนไม่เพียงพอต่อการปฏิบัติหน้าที่ ให้ผู้รับจ้างที่ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศให้การสนับสนุนด้านเทคนิค |

| ทรัพยากร | กลยุทธ์ความต่อเนื่อง |
|---|---|
| | ๒. อนุญาตให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอก กรมสนับสนุนบริการสุขภาพ (Teleworking) โดยเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านระบบคอมพิวเตอร์ ลูกข่ายแบบเสมือน (Virtualization System) |
| ๕. ผู้รับบริการและผู้ที่เกี่ยวข้อง | ๑. แจ้งสถานที่การติดต่อราชการสำรองผ่านทางหน้าเว็บไซต์ของ กรมสนับสนุนบริการสุขภาพ<br>๒. บุคลากรที่มีหน้าที่ปฏิบัติงานร่วมกับหน่วยงานอื่นๆ ให้ประสานงาน ทางโทรศัพท์เคลื่อนที่หรือจดหมายอิเล็กทรอนิกส์ (E - Mail) หรือหาก ระบบคอมพิวเตอร์และระบบสารสนเทศอยู่ระหว่างดำเนินการกู้คืน ให้พิจารณาใช้จดหมายอิเล็กทรอนิกส์ (E - Mail) จากภายนอกที่มีความน่าเชื่อถือ |

**๘. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต**

จากการวิเคราะห์ผลกระทบจากความเสี่ยงในข้อ ๕ เพื่อให้บุคลากรสามารถปฏิบัติงานด้วยความต่อเนื่อง จึงกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต ดังนี้

| กระบวนงาน | ระดับผลกระทบ | ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต | | |
|---|---|---|---|---|
| | | ภายใน ๑ วัน | ภายใน ๗ วัน | มากกว่า ๗ วัน |
| ๘.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People) | | | | |
| ๘.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากรของกรมสนับสนุนบริการสุขภาพ | ค่อนข้างสูง | ✓ | | |
| ๘.๑.๒ เหตุการณ์หรือภัยที่เกิดจากบุคคลภายนอกหรือผู้ไม่ประสงค์ดี | ค่อนข้างสูง | | ✓ | |
| ๘.๒ เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process) | | | | |
| ๘.๒.๑ เหตุการณ์หรือภัย ที่เกิดจากการโจรกรรมอุปกรณ์ ประมวลผลข้อมูล (Process Device) | ค่อนข้างสูง | | ✓ | |
| ๘.๒.๒ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค | ค่อนข้างต่ำ | | ✓ | |
| ๘.๒.๓ เหตุการณ์ไฟฟ้าดับ | ค่อนข้างต่ำ | ✓ | | |
| ๘.๒.๔ เหตุการณ์อัคคีภัย | ค่อนข้างต่ำ | | | ✓ |
| ๘.๒.๕ เหตุการณ์ที่เกิดจาก ภัยพิบัติหรือสถาน การณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง | ค่อนข้างต่ำ | | ✓ | |
| ๘.๓ เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology) | | | | |
| ๘.๓.๑ ทรัพย์สิน ครุภัณฑ์ระบบปฏิบัติการด้านเทคโนโลยี | ค่อนข้างต่ำ | | | ✓ |
| ๘.๓.๒ การสื่อสารและเครือข่ายสารสนเทศ | ค่อนข้างสูง | ✓ | | |
| ๘.๓.๓ โครงข่ายสารสนเทศ | ค่อนข้างสูง | ✓ | | |
| ๘.๓.๔ ข้อมูลสารสนเทศ | ค่อนข้างสูง | ✓ | | |

## ๙. โครงสร้างและทีมบริหารความต่อเนื่อง (BCP Team)

เพื่อให้แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ กรมสนับสนุนบริการสุขภาพ สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ จึงต้องมีการจัดตั้งทีมบริหารความต่อเนื่อง (BCP Team) ซึ่งประกอบด้วยผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ และบุคลากรกลุ่มเทคโนโลยีสารสนเทศ เนื่องจากมีความรู้ความสามารถด้านระบบคอมพิวเตอร์และระบบสารสนเทศ ประกอบกับปฏิบัติหน้าที่ เป็นผู้ดูแลระบบ (System Administrator) ของ กรมสนับสนุนบริการสุขภาพ

๙.๑ หน้าที่ความรับผิดชอบทีมบริหารความต่อเนื่อง (BCP Team) ดังนี้

๙.๑.๑ หัวหน้าทีมและรองหัวหน้าทีม มีหน้าที่ในการพิจารณาแนวทางการแก้ไขปัญหา กำหนดขอบเขต และสั่งการให้ผู้ที่รับผิดชอบดำเนินการแก้ไข พร้อมทั้งรายงานให้คณะผู้บริหารระดับสูง กรมสนับสนุนบริการสุขภาพได้รับทราบ

๙.๑.๒ ผู้ประสานงาน มีหน้าที่ในการติดต่อประสานงานภายในและหน่วยงานภายนอก กรมสนับสนุนบริการสุขภาพและจัดเตรียมเอกสารข้อมูลที่เกี่ยวข้อง รวมถึงจัดทำรายงานในแต่ละสถานการณ์

๙.๑.๓ ผู้ดูแลระบบ (System Administrator) มีหน้าที่การพัฒนาและบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัย ดูแลสิทธิของผู้ใช้งาน (User) แก้ไขปัญหาการใช้งาน และดูแลห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์

๙.๒ รายชื่อทีมบริหารความต่อเนื่อง (BCP Team) และหน้าที่ความรับผิดชอบ

| ชื่อ | บทบาท | โทรศัพท์ |
|---|---|---|
| นายอภินันท์ นิลฉาย | หัวหน้าทีมบริหารความต่อเนื่อง (BCP Team) | - ๐๒-๑๙๓-๗๐๐๐ ต่อ ๑๘๒๘๘<br>- ๐๘๑-๘๔๙-๘๕๐๔ |
| นายสรายุทธ ภูตาสืบ | รองหัวหน้าทีมบริหารความต่อเนื่อง ผู้ดูแลระบบ (System Administrator) (บุคลากรหลัก) | - ๐๒-๑๙๓-๗๐๐๐ ต่อ ๑๘๒๐๘<br>- ๐๘๖-๓๙๑-๓๕๕๐ |
| นางสาวนรารัตน์ มุลจันดา | ผู้ดูแลระบบ (System Administrator) (บุคลากรสำรอง) | - ๐๒-๑๙๓-๗๐๐๐ ต่อ ๑๘๒๘๘<br>- ๐๘๕-๑๑๗-๓๔๖๐ |
| นายนันทชัย นุ่มน้อย | ผู้ดูแลครุภัณฑ์คอมพิวเตอร์ (Computer Asset) (บุคลากรหลัก) | - ๐๒-๑๙๓-๗๐๐๐ ต่อ ๑๘๒๐๗<br>- ๐๘๑-๑๒๙-๐๓๕๙ |
| นายสิทธิชัย ศิริรัตน์ | ดูแลระบบฯ กรมสนับสนุนบริการสุขภาพ (Contract Outsource) | ๐๒-๑๙๓-๗๐๐๐ ต่อ ๑๘๒๐๗<br>๐๘๒-๕๕๔-๗๓๓๕ |

## ๑๐. กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree) ตามแนวทางของแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ กรมสนับสนุนบริการสุขภาพ หมายถึง ขั้นตอนการแจ้งเหตุฉุกเฉินหรือการแจ้งปัญหาระบบคอมพิวเตอร์ และระบบสารสนเทศ เพื่อรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้นและสั่งการให้ผู้ที่มีหน้าที่รับผิดชอบ ดำเนินการแก้ไขตามระดับความรุนแรงของเหตุนั้น เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศสามารถ ให้บริการสนับสนุนการปฏิบัติงานแก่บุคลากรได้อย่างต่อเนื่อง ที่กำหนดรายละเอียดไว้ตามรายชื่อทีมบริหาร ความต่อเนื่อง (BCP Team) และหน้าที่ความรับผิดชอบ ทั้งนี้ ในกรณีที่บุคลากรหลักในแต่ละบทบาทไม่สามารถ ปฏิบัติหน้าที่ได้ให้บุคลากรสำรองรับผิดชอบปฏิบัติหน้าที่แทน

**๑๑. การสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ**

เนื่องจากระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศส่วนใหญ่ ถูกติดตั้งและจัดเก็บบนระบบประมวลผลกลาง ณ ห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ซึ่งเป็นการอำนวยความสะดวกแก่ผู้ใช้งาน (User) เป็นอย่างมาก แต่ก็มีความเสี่ยงสูงมากเช่นกัน ซึ่งเป็นผู้ดูแลรับผิดชอบหลัก จึงได้จัดทำแนวปฏิบัติการสำรอง ข้อมูลและกู้คืนข้อมูลสารสนเทศ เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานสามารถให้บริการได้อย่างต่อเนื่อง และสามารถกู้คืนกลับมาใช้งานได้โดยเร็วหากเกิดปัญหา

๑๑.๑ ผู้รับผิดชอบ

รายละเอียดบุคลากรและหน้าที่ความรับผิดชอบ ตามข้อ ๙

๑๑.๒ แนวปฏิบัติในการดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจน อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้มอบหมายให้ผู้ดูแลระบบ (System Administrator) ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนให้ตรวจสอบอุปกรณ์ประมวลผลข้อมูล (Process Device) ณ ห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง หากพบข้อผิดพลาดให้รายงานผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบโดยทันที

๑๑.๓ แนวปฏิบัติในการสำรองข้อมูลสารสนเทศ กำหนดดังนี้

๑๑.๓.๑ ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการสำรองข้อมูลสารสนเทศไว้ในตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองอื่นใด ตามขั้นตอนของโปรแกรมสำรองข้อมูล

๑๑.๓.๒ ผู้ดูแลระบบ (System Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองอื่นใดที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์ หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

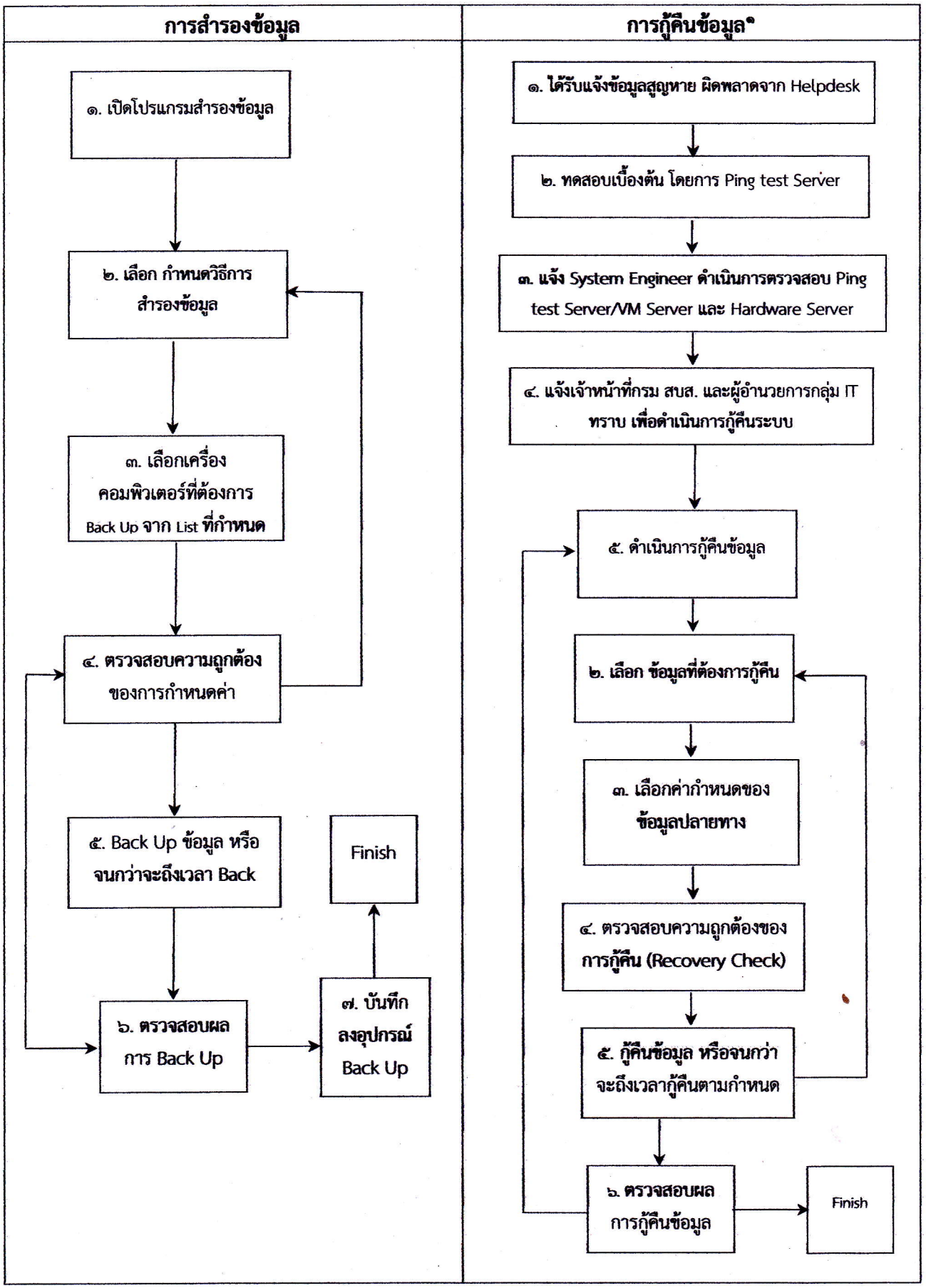
๑๑.๓.๓ รายละเอียดการสำรองข้อมูล กำหนดดังนี้

| ลำดับ | รายการ | จำนวน (หน่วย) | ข้อมูลสำรอง |
|---|---|---|---|
| ๑ | เครื่องคอมพิวเตอร์แม่ข่าย (Rack Server) สำหรับประมวลผล ระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Server Virtualization System) | ๔๓ | Full |
| ๒ | เครื่องคอมพิวเตอร์แม่ข่าย (Tower) สำหรับประมวลผล ระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Server Virtualization System) | ๔ | Full |
| ๓ | เครื่องคอมพิวเตอร์แม่ข่าย (Blade Server) สำหรับประมวลผล ระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Server Virtualization System) | ๑๔ | Full |

๑๑.๔ แนวปฏิบัติการกู้คืนระบบ

หากระบบคอมพิวเตอร์และระบบสารสนเทศเกิดปัญหาไม่สามารถใช้งานได้ หรือข้อมูลสารสนเทศสูญหาย ให้ผู้ดูแลระบบ (System Administrator) ดำเนินการกู้คืนข้อมูลสารสนเทศที่สำรองไว้ในตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองอื่นใด เช่น GDCC (Cloud Computing Services) เพื่อนำข้อมูลสารสนเทศกลับมาใช้งาน

## ๑๑.๕ แผนผังการสำรองและกู้คืนระบบคอมพิวเตอร์และระบบสารสนเทศและข้อมูลสารสนเทศ




* อ้างอิงตามรายงานผลการทดสอบกู้คืนข้อมูลระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ.๒๕๖๒

๑๑.๖ กรมสนับสนุนบริการสุขภาพ ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศและระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง ดังนี้

๑๑.๖.๑ พิจารณาคัดเลือกระบบคอมพิวเตอร์และระบบสารสนเทศที่สำคัญเพื่อดำเนินการทดสอบ พร้อมทั้งเตรียมความพร้อมก่อนการทดสอบ เพื่อมิให้เกิดความเสี่ยงและความเสียหายแก่ทางราชการ

๑๑.๖.๒ จัดทำรายงานเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (DCIO : Department Chief Information Officer) ก่อนดำเนินการทดสอบ

๑๑.๖.๓ ดำเนินการทดสอบระบบคอมพิวเตอร์และระบบสารสนเทศตามที่กำหนดไว้

๑๑.๖.๔ รายงานผลการทดสอบเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

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

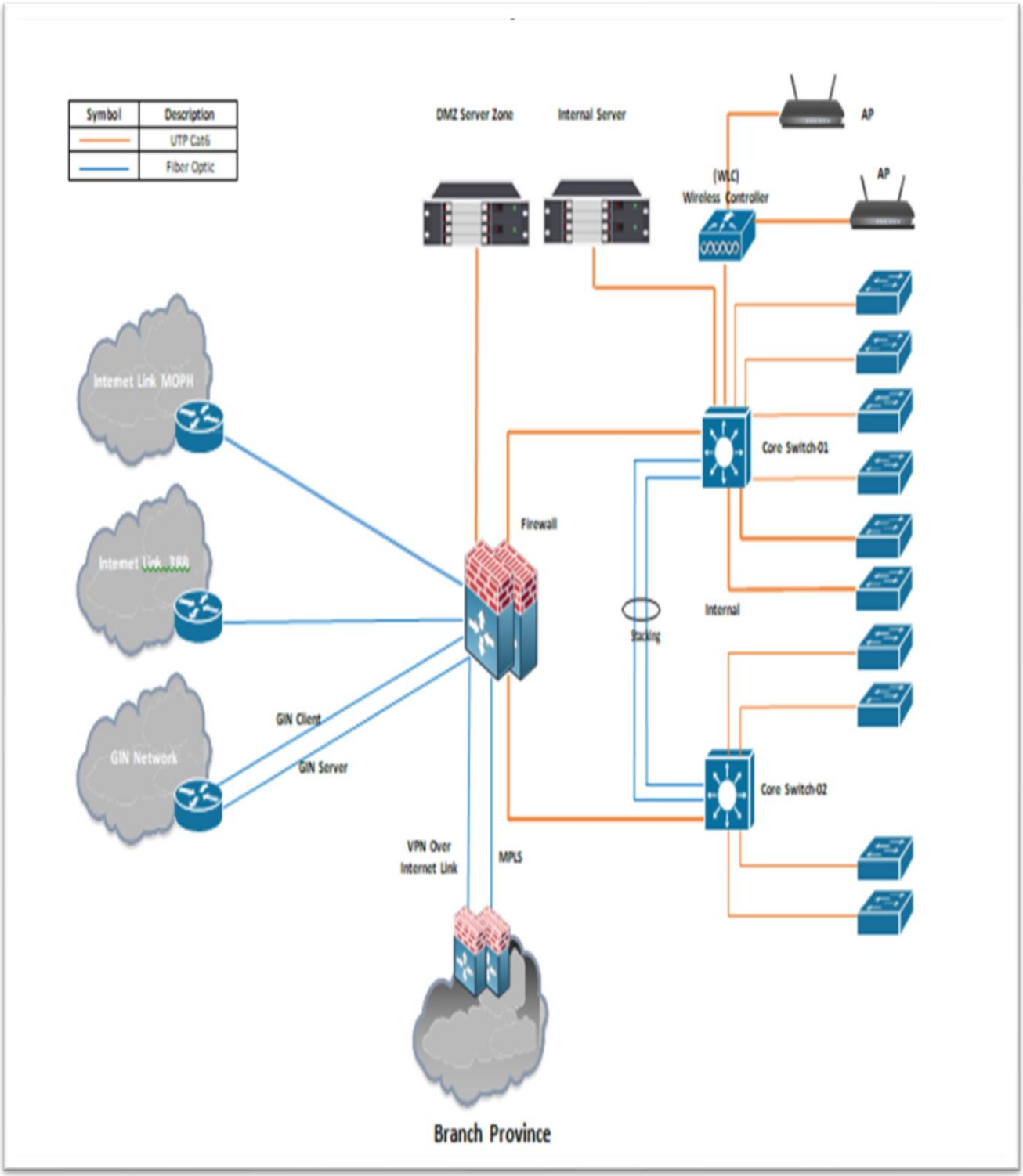
(ลงชื่อ) ..... ผู้เห็นชอบ
(นายภานุวัฒน์ ปานเกตุ)
ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

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

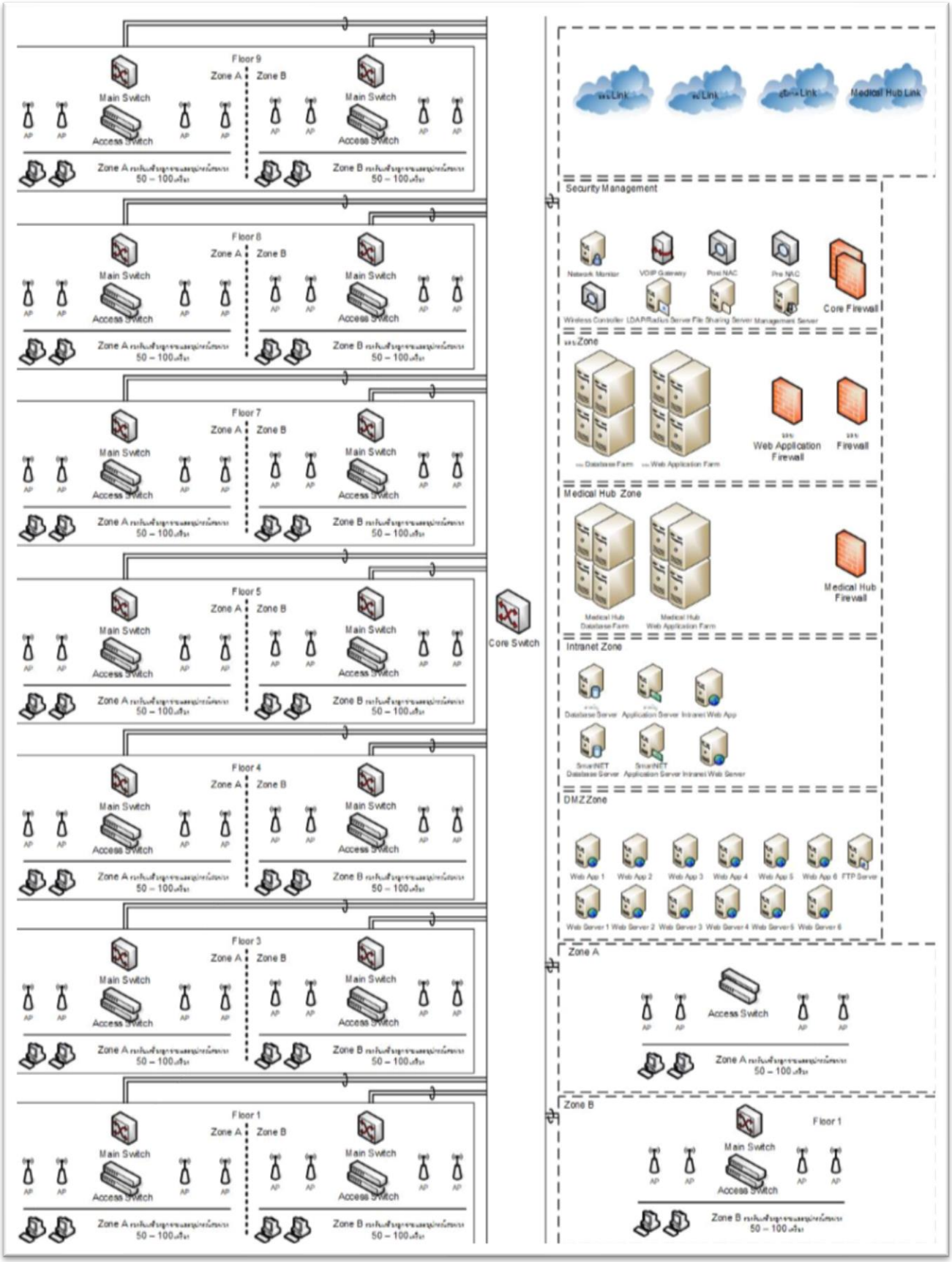
# ภาคผนวก

# ระบบเครือข่ายและการเชื่อมโยงเครือข่าย

**ภาพที่ ๑** ระบบเครือข่ายของกรมสนับสนุนบริการสุขภาพ



**ภาพที่ ๒** การเชื่อมโยงเครือข่ายภายในกรมสนับสนุนบริการสุขภาพ



**๓. ผู้ประสานงานภายนอก**

| ลำดับ | หน่วยงาน | หมายเลขโทรศัพท์ |
|---|---|---|
| ๑ | ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานปลัดกระทรวงสาธารณสุข | ๐๒ – ๕๙๐ - ๑๑๖๙<br>๐๒ – ๕๙๐ - ๑๒๐๐ |
| ๒ | บริษัท ทีโอที จำกัด | ๐๒ – ๕๗๔ – ๘๘๔๘ – ๙<br>หรือสายด่วน ๑๑๐๐ |
| ๓ | บริษัท กสท โทรคมนาคม จำกัด (มหาชน) | ๐๒ – ๑๐๔ – ๔๗๗๖<br>หรือสายด่วน ๑๓๒๒ |
| ๔ | สถานีดับเพลิง เทศบาลนครนนทบุรี | ๐๒ – ๕๘๙ - ๐๔๘๙ |
| ๕ | สถานีตำรวจภูธร จังหวัดนนทบุรี | ๐๒ – ๕๒๗ – ๐๒๓๖-๗ |

# 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