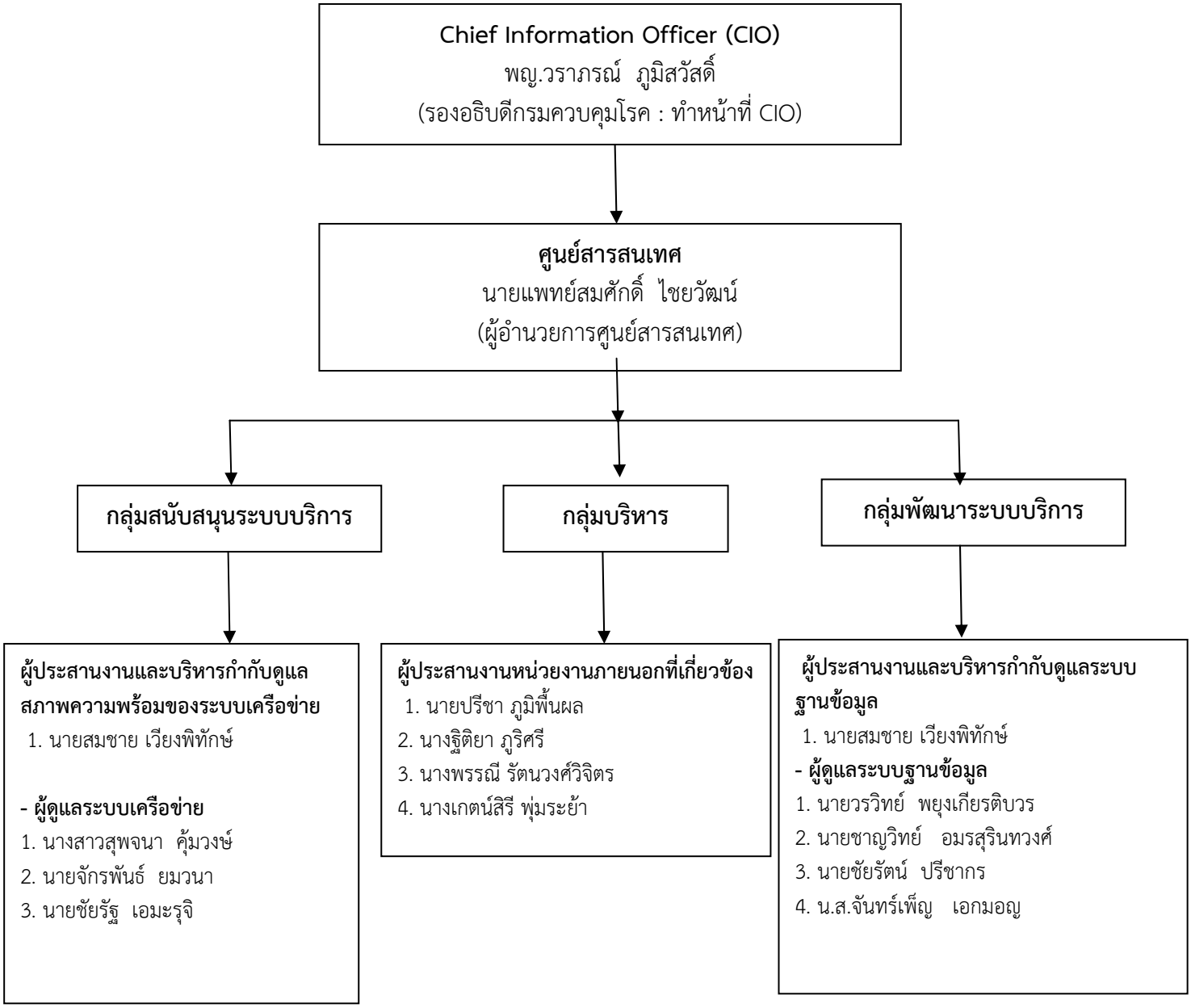
(ฉบับร่าง)

<u>แผนปฏิบัติการเมื่อเกิดสภานการณ์ภาวะฉุกเฉิน</u>

<u>หรือการใช้งานระบบเครือข่ายขัดข้อง (Contingency Plan)</u>

<u>แผนการสั่งการ</u>



การจัดองค์กรปฏิบัติการฉุกเฉินในระบบสารสนเทศกรมควบคุมโรคเมื่อเกิดเหตุฉุกเฉิน

การจัดองค์กรปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา (Lines of authority) เมื่อเกิดเหตุฉุกเฉิน

๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

๑.๑.๑ เป็นผู้ประกาศใช้แผนเมื่อเกิดเหตุสถานการณ์ฉุกเฉินและยุติการปฏิบัติการตามแผนเมื่อเข้าสู่สภาวะปกติ

๑.๑.๒ กำหนดนโยบายให้ศูนย์สารสนเทศ

๑.๑.๓ ให้คำปรึกษาแก่ผู้อำนวยการศูนย์สารสนเทศในฐานะประธานศูนย์ฯ

๑.๒ ผู้อำนวยการศูนย์สารสนเทศ

๑.๒.๑ เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๑.๒.๒ มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๑.๒.๓ มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

๑.๒.๔ ประชุมหารือกับคณะกรรมการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง

๑.๒.๕ ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

๑.๒.๖ รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริการเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

๑.๓ ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย

๑.๓.๑ วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการศูนย์สารสนเทศ

๑.๓.๒ มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

๑.๓.๓ สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

๑.๓.๔ ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ท่านผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

๑.๓.๕ ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

๑.๓.๖ รายงานให้ผู้อำนวยงานระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

๑.๓.๗ กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

๑.๓.๘ ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุการณ์

รายละเอียดโดยสรุปเกี่ยวกับ
แผนป้องกันและแก้ไขปัญหาเมื่อเกิดสถานการณ์ฉุกเฉิน
ศูนย์สารสนเทศ กรมควบคุมโรค

ศูนย์สารสนเทศ กรมควบคุมโรค ได้มีมาตรการในการป้องกันและแก้ไขปัญหาเมื่อเกิดสถานการณ์ฉุกเฉินและการรักษาความปลอดภัยที่อาจเกิดขึ้น ซึ่งจะสร้างความเสียหายแก่ทรัพย์สินของทางราชการ รวมทั้งระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ รวมถึงแนวทางปฏิบัติของบุคลากรเมื่อเกิดสถานการณ์ฉุกเฉิน มีจำนวน ๓ สถานการณ์ ดังนี้

๑. ระบบป้องกันและการแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

๒. ระบบป้องกันและการแก้ไขปัญหาเมื่อเกิดอัคคีภัย

๓. ระบบป้องกันและการแก้ไขปัญหาเมื่อเกิดการโจรกรรม

รายละเอียดแผนการป้องกันและการแก้ไขปัญหาจากสถานการณ์ฉุกเฉินข้างต้น มีรายละเอียด ดังนี้

๑. ระบบป้องกันและการแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความจำเป็นต้องใช้กระแสไฟฟ้าในกระบวนการทำงาน สิ่งที่มักจะเกิดขึ้นและยากที่จะหลีกเลี่ยงได้ ก็คือ ผลกระทบต่างๆ ที่เกิดขึ้นจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลที่สำคัญแยกตามสถานการณ์ดังนี้

๑.๑ ไฟฟ้าตก (Sag หรือ Brownout)

ไฟฟ้าตก คือ สภาวะที่แรงดันไฟฟ้าลดต่ำลงจากปกติในช่วงเวลาสั้นๆเป็นปัญหาทางไฟฟ้าที่พบบ่อยที่สุด

สาเหตุ เกิดจากการเปิดสวิตช์อุปกรณ์บางชนิดที่ต้องการใช้กระแสไฟฟ้ามาก เช่น เครื่องปรับอากาศ ลิฟต์ และเครื่องมือเครื่องจักร เป็นต้น อุปกรณ์เหล่านี้ต้องการกระแสไฟฟ้ามากในการติดเครื่อง เมื่อเทียบกับการทำงานในภาวะปกติ ส่งผลให้แรงดันไฟฟ้าในสายส่งการไฟฟ้าฯลดต่ำลง

ผลกระทบคือ หากไม่มีเครื่องสำรองไฟฟ้า(UPS) อาจทำให้เครื่องคอมพิวเตอร์เกิดความเสียหายหรือข้อมูลที่ทำงานอยู่ในขณะนั้นเกิดสูญหาย

๑.๒ ไฟฟ้าดับ (Blackout)

ไฟฟ้าดับ คือ สภาวะที่กระแสไฟฟ้าหยุดไหล

สาเหตุ เกิดจากความต้องการกระแสไฟฟ้าจากสายส่งการไฟฟ้าฯที่มากเกินไป เกิดไฟฟ้าลัดวงจรในสายส่ง พายุฟ้าคะนอง แผ่นดินไหว และปัญหาที่เกิดกับสายส่งการไฟฟ้าฯ เช่น เสาไฟฟ้าล้ม หรือหม้อแปลงระเบิด ถูกตัดไฟ ฯลฯ ซึ่งส่งผลให้ไม่สามารถจ่ายไฟจากการไฟฟ้าได้

ผลกระทบ คือ เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ ทำให้เกิดข้อมูลสูญหายได้

ศูนย์สารสนเทศ กรมควบคุมโรค ได้มีการป้องกันปัญหาจากกระแสไฟฟ้าดังกล่าวโดยการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply; UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อให้บริการอินเตอร์และระบบงานต่างๆ ของกรมควบคุมโรค ซึ่งอยู่ภายในศูนย์สารสนเทศ เพื่อให้บุคลากรของศูนย์สารสนเทศสามารถดำเนินการแก้ไขปัญหาหรือรักษาอุปกรณ์คอมพิวเตอร์ได้ ทั้งนี้หากไฟฟ้าดับหรือถูกตัดสายหลัก ภายใน ๒๐ นาที ในกรณีที่ทำให้ไฟฟ้าดับเกิน ๒๐ นาทีขึ้นไป ศูนย์สารสนเทศจำเป็นต้องปิดระบบของเครื่องเครือข่ายและระบบงานต่างๆ ทั้งหมด เพื่อป้องกันการสูญหายของข้อมูลและอุปกรณ์เครือข่ายชำรุด

<u>หลักปฏิบัติของบุคลากรเมื่อเกิดปัญหาจากกระแสไฟฟ้า</u>

เพื่อป้องกันมิให้เกิดความเสียหายอันเกิดจากกระแสไฟฟ้า และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดปัญหาจากกระแสไฟฟ้า จึงกำหนดหลักปฏิบัติของบุคลากรในสังกัดกรมควบคุมโรค ดังนี้

๑) เปิดใช้งานเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์ทั้งเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล

๒) เมื่อเกิดกระแสไฟฟ้าดับ เครื่องสำรองไฟฟ้า (UPS) ยังคงให้กระแสไฟฟ้ากับอุปกรณ์คอมพิวเตอร์ตามสมรรถนะของเครื่อง ให้บุคลกรรีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่น

๓) หากไม่มีเครื่องสำรองไฟฟ้า บุคลากรควรทำการ save ข้อมูลที่กำลังดำเนินการอยู่อย่างต่อเนื่อง และควรมีการสำรองข้อมูล (back up) ข้อมูลทั้งหมดเพื่อป้องกันการสูญหายของข้อมูลที่จำเป็น

๒. ระบบการป้องกันและการแก้ไขปัญหาเมื่อเกิดอัคคีภัย

กรมควบคุมโรค ได้มีการซ้อมแผนตามโครงการอบรมเชิงปฏิบัติการ เรื่องการป้องกันและระงับอัคคีภัย ของสำนักงานเลขานุการกรม ให้บุคลากรสังกัดกรมควบคุมโรคปฏิบัติตามที่ได้รับการอบรมดังนี้

<u>หลักปฏิบัติของบุคลากรเมื่อเกิดอัคคีภัย</u>

เพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติของบุคลากรใน ศูนย์สารสนเทศ ดังนี้

๑) ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๒) ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

๓) ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบดูทางออกฉุกเฉินไม่ปิดตาย หรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉินทั้งสองทาง เพื่อให้ไปถึงทางหนีฉุกเฉินได้ ถึงแม้ว่าจะดับหรือปกคลุมไปด้วยควัน

๔) เมื่อเกิดเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นหนีจากอาคารแล้วโทรศัพท์แจ้งหน่วยดับเพลิง โทร ๑๙๙ ทันที หรือแจ้ง ๑๖๖๙

๕) เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

๖) ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันที รีบแจ้งฝ่ายอาคารและสถานที่ เพื่อโทรศัพท์แจ้งหน่วยดับเพลิงต่อไป

๗) ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อยๆ ปิดประตู แล้วหนีไปยังทางหนีไฟฉุกเฉินที่อยู่ใกล้ที่สุด

๘) ถ้าเพลิงไหม้อยู่บริเวณใกล้ๆ ประตูจะมีความร้อน ห้ามเปิดประตูเด็ดขาด ให้รีบโทรศัพท์เรียกหน่วยดับเพลิงและแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งถูกเพลิงไหม้ หาผ้าเช็ดตัวเปียกๆ ปิดทางเข้าของควัน ปิดพัดลมและเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๙) เมื่อต้องเผชิญกับควันไฟที่ปกคลุม ให้ใช้วิธีคลานหนีไปทางฉุกเฉินเพราะอากาศบริสุทธิ์จะอยู่ด้านล่าง (เหนือพื้นห้อง) นำกุญแจห้องทำงานไปด้วยหากหมดหนทางหนีจะได้สามารถกลับเข้าห้องได้

๑๐) ห้ามใช้ลิฟท์ขณะเกิดเพลิงไหม้

ศูนย์สารสนเทศจะปฏิบัติงานดังนี้

๑. กลุ่มงานบริหาร นำเอกสารที่จำเป็นออกนอกสถานที่ พร้อมไฟล์ข้อมูลที่สำคัญของศูนย์ที่ทำการสำรองไว้

๒. กลุ่มสนับสนุนระบบบริการ และกลุ่มพัฒนาระบบบริการ ทำการปิดระบบทั้งหมดและนำข้อมูลที่สำรองไว้จาก Server และรีบออกจากสถานที่

๓. ระบบป้องกันและการแก้ไขปัญหาเมื่อเกิดการโจรกรรม

เนื่องด้วยที่ตั้งของศูนย์สารสนเทศ กรมควบคุมโรค ในปัจจุบันตั้งอยู่ที่ ๘๘/๒๑ อาคาร ๒ ชั้น ๓ ถ.ติวานนท์ ต.ตลาดขวัญ อ.เมือง จ.นนทบุรี จึงมีระบบป้องกันการโจรกรรมตามระเบียบของทางราชการเกี่ยวกับการดูแลรักษาสถานราชการระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ บทที่ ๕ การรักษาความปลอดภัยอันเกี่ยวกับสถานที่ รวมทั้งตามระเบียบและมาตรฐานของทางนิติบุคคลอาคารชุดดังนี้

๑) ดำเนินการในส่วนที่เกี่ยวข้องตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

๒) ให้มีการรายงานการเปิดปิดห้องทำงานทุกวัน และนำส่งแก่งานบริหารของศูนย์สารสนเทศ ทุกสิ้นเดือน

๓) ห้ามผู้ที่ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้องคอมพิวเตอร์แม่ข่าย

๔) จัดให้มีเวรยามรักษาการณ์ ตลอด ๒๔ ชั่วโมง

๕) นิติบุคคลอาคารชุดจัดให้มีระบบควบคุมการเข้าออกอาคารในวันหยุด หรือนอกเวลาราชการ

<u>หลักปฏิบัติของบุคลากรเมื่อเกิดการโจรกรรม</u>

เพื่อป้องกันการโจรกรรม จึงกำหนดหลักปฏิบัติของบุคลากรในสังกัดศูนย์สารสนเทศ กรมควบคุมโรค ดังนี้

๑) ปฏิบัติตนให้เป็นไปตามระเบียบของทางราชการในส่วนที่เกี่ยวข้องกับการดูแลรักษาสถานที่ราชการ และระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

๒) เฝ้าระวัง และสอดส่องดูแลเพื่อป้องกันมิให้เกิดการโจรกรรมขึ้น ทั้งนี้หากพบเห็นเหตุการณ์หรือบุคคลซึ่งคาดว่าจะนำไปสู่การโจรกรรมทรัพย์สินของทางราชการ หรือข้อมูลสารสนเทศต่างๆ ให้รีบรายงานให้ผู้บังคับบัญชาทราบโดยด่วนที่สุด เพื่อจะได้ประสานงานกับเจ้าหน้าที่ที่เกี่ยวข้อง หรือเจ้าหน้าที่ตำรวจในการที่จะระงับ หรือจับกุมผู้ที่จะกระทำการดังกล่าวต่อไป

<u>สิ่งที่ควรปฏิบัติต่อเครื่องคอมพิวเตอร์ก่อนออกจากสถานที่</u>

<u>กรณีเครื่องลูกข่าย</u>

๑. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่ศูนย์สารสนเทศของหน่วยงานทราบหรือกรณีมีเหตุอันทำให้ศูนย์สารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์สารสนเทศจะต้องประกาศให้ทุกหน่วยงานในสังกัดกรมควบคุมโรคทราบ

๒. ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๓. ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด

๔. ขนย้ายเครื่องไปไว้ในที่ปลอดภัย (เฉพาะเครื่องที่สามารถเคลื่อนย้ายได้)

๕. หากเป็นหน่วยงานที่พบเหตุฉุกเฉินโปรดแจ้งหรือประสานงาน ด้วยโทรศัพท์เคลื่อนที่ เพื่อให้เจ้าหน้าที่ในกรมฯทราบโดยทั่วกัน

<u>กรณีเครื่องแม่ข่ายที่ให้บริการ (Server) และอุปกรณ์เครือข่าย</u>

๑. ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๒. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับดังนี้

๒.๑ ระยะเวลาที่ไฟฟ้าดับ

๒.๒ หากดับเกิน ๒๐ นาที ซึ่งเกินขีดความสามารถของเครื่องสำรองไฟฟ้าของศูนย์สารสนเทศ จะลำดับความสำคัญของระบบงาน และทำการปิดระบบงานทีละระบบเพื่อรักษาข้อมูลและเครื่องคอมพิวเตอร์แม่ข่ายไว้

๓. ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้ น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔. รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย (เฉพาะเครื่องที่สามารถเคลื่อนย้ายได้)

๕. ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖. ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗. ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์สารสนเทศทราบโดยเร็วที่สุด

เบอร์โทรติดต่อเมื่อเกิดสถานการณ์ภาวะฉุกเฉิน

ชื่อผู้ประสานงาน	ตำแหน่ง	หมายเลขโทรศัพท์	รับผิดชอบระบบงาน
นายสมศักดิ์ ไชยวัฒน์	ผู้อำนวยการศูนย์สารสนเทศ	๐๘๑๙๑๔๐๖๐๘	ผู้บริหาร
นายสมชาย เวียงพิทักษ์	นักวิชาการสาธารณสุขชำนาญการ	๐๘๔-๑๖๔-๒๕๖๘	ระบบงานเครือข่ายคอมพิวเตอร์
น.ส.สุพจนา คุ้มวงษ์	นักวิชาการคอมพิวเตอร์	๐๘๕-๙๙๔-๓๓๒๘	
นายจักรพันธ์ ยมวนา	นักวิชาการคอมพิวเตอร์	๐๙๔-๔๘๗-๗๓๑๓	
นายชัยรัฐ เอมะรุจิ	เจ้าพนักงานคอมพิวเตอร์	๐๘๒-๙๘๙-๐๐๖๗	
นายพงษ์อมร	บริษัทที่จ้างดูแลระบบ (dxp)	๐๘๑-๙๐๔-๔๖๖๙	
นายวรวิทย์ พยุงเกียรติบวร	นักวิชาการคอมพิวเตอร์	๐๘๑-๗๕๕-๘๐๘๐	งานดูแลฐานข้อมูลและเว็บไซต์
นายชาญวิทย์ อมรสุรินทวงศ์	นักวิชาการคอมพิวเตอร์	๐๘๖-๕๕๓-๘๓๗๒	
นายชัยรัตน์ ปรีชากร	นักวิชาการคอมพิวเตอร์	๐๘๖-๕๒๐-๖๒๗๖	
น.ส.จันทร์เพ็ญ เอกมอญ	นักวิชาการคอมพิวเตอร์	๐๘๖-๕๗๐-๙๓๖๘	