



ที่ สธ ๐๒๑๒/ว สด๑๓

สำนักงานปลัดกระทรวงสาธารณสุข

ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๒ เมษายน ๒๕๖๕

เรื่อง ให้นำหน่วยงานปฏิบัติงานให้มีความมั่นคงปลอดภัยไซเบอร์

เรียน นายแพทย์สาธารณสุขจังหวัด, ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไป, ผู้อำนวยการสำนักงานเขตสุขภาพ

ที่ ๑ - ๑๓, ผู้อำนวยการสำนัก/กอง/กลุ่ม/ศูนย์ สังกัดสำนักงานปลัดกระทรวงสาธารณสุข ทุกแห่ง

สิ่งที่ส่งมาด้วย สำเนาคำสั่งกระทรวงสาธารณสุข ที่ ๓๗๘/๒๕๖๕ ลงวันที่ ๒๘ มีนาคม ๒๕๖๕

เรื่อง มอบหมายหน่วยงานปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านสาธารณสุข

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาลและระหว่างโรงพยาบาล ต้องดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้อยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข นั้น

ปัจจุบันพบเหตุการณ์ความเสี่ยงและความไม่ปลอดภัยทางไซเบอร์เกิดขึ้นกับหน่วยงานในสังกัดกระทรวงสาธารณสุขเพิ่มขึ้นอย่างมาก ทั้งจากการบุกรุกโจมตีผ่านทางอินเทอร์เน็ต การเข้าใช้ Web Hosting และ Domain Name ของเอกชน แต่ Domain Name และ IP Address ที่เข้านั้นถูกจัดอยู่ในกลุ่มภัยคุกคามไซเบอร์ ทำให้เว็บไซต์ของหน่วยงานถูกตรวจพบว่าเป็นภัยคุกคามไซเบอร์ ส่งผลต่อความน่าเชื่อถือของหน่วยงาน และส่งผลกระทบต่อภาพลักษณ์ของกระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุข จึงขอให้หน่วยงานปฏิบัติงานให้มีความมั่นคงปลอดภัยไซเบอร์ ในเบื้องต้น ดังนี้

๑. การจดทะเบียนเว็บไซต์ของหน่วยงาน กำหนดให้ใช้ Domain Name ของกระทรวงสาธารณสุข ได้แก่ ชื่อภาษาอังกฤษ.moph.go.th

๒. การใช้ IP Address สำหรับเว็บไซต์และระบบงาน กำหนดให้หน่วยงานที่ได้รับจัดสรรชุดเลข IP Address จากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ใช้ IP Address ที่มีชุดเลขขึ้นต้นด้วย ๒๐๓.๑๕๗.xxx.xxx

๓. ติดตั้ง SSL (https://) เพื่อให้เว็บไซต์มีความปลอดภัยและน่าเชื่อถือเพิ่มขึ้น

๔. ทำการสำรองข้อมูล (Backup) สำคัญทุกวัน และจัดเก็บข้อมูลสำรองไว้ในพื้นที่ที่ปลอดภัยจากการเข้าถึงผ่านเครือข่ายคอมพิวเตอร์ทุกช่องทาง

๕. ตรวจสอบ...

๕. ตรวจสอบช่องโหว่ของระบบงานต่างๆ และเครือข่ายคอมพิวเตอร์ทั้งอินเทอร์เน็ต และ อินทราเน็ต อย่างน้อยสัปดาห์ละครั้ง

๖. กรณีพบภัยคุกคามทางไซเบอร์ ให้ประสานศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) ทันทีได้ทุกช่องทาง ได้แก่ โทรศัพท์ ๐๘ ๓๐๖๔ ๙๘๖๗ อีเมล health-cirt@moph.go.th และ Line Official : @health-cirt ซึ่ง Health CIRT อยู่ในความดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ตามคำสั่งกระทรวงสาธารณสุข ที่ ๓๗๘/๒๕๖๕ ลงวันที่ ๒๘ มีนาคม ๒๕๖๕ รายละเอียดตามสิ่งที่ส่งมาด้วย

การปฏิบัติดังกล่าวข้างต้นจะช่วยให้ Health CIRT เผื่อระวัง ตรวจสอบ และป้องกัน การบุกรุกหรือภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานในสังกัดกระทรวงสาธารณสุขได้ และสามารถประสานความร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National CERT) ได้อย่างรวดเร็วเพื่อให้การช่วยเหลือหน่วยงานต่อไป ทั้งนี้สอบถามเพิ่มเติมเกี่ยวกับการปฏิบัติดังกล่าวข้างต้น ได้ที่กลุ่มคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร ๐ ๒๕๙๐ ๑๒๐๐, ๐ ๒๕๙๐ ๑๑๖๙ หรืออีเมล moph-network@health.moph.go.th

จึงเรียนมาเพื่อโปรดดำเนินการและแจ้งหน่วยงานในกำกับ ให้ปฏิบัติงานให้มีความมั่นคงปลอดภัยไซเบอร์ดังกล่าว โดยเคร่งครัดต่อไปด้วย

ขอแสดงความนับถือ



(นายธงชัย เลิศวิไลรัตนพงศ์)

รองปลัดกระทรวงสาธารณสุข

ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

ประจำกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

กลุ่มบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการ

โทรศัพท์ ๐ ๒๕๙๐ ๑๒๐๘

อีเมล ict-moph@health.moph.go.th





คำสั่งกระทรวงสาธารณสุข  
ที่ ๓๗๔ /๒๕๖๕

เรื่อง มอบหมายหน่วยงานปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ  
ด้านสาธารณสุข

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CI) และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ มีผลบังคับใช้เมื่อ ๒๔ สิงหาคม พ.ศ. ๒๕๖๔ กำหนดให้สำนักงานปลัดกระทรวงสาธารณสุข เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านสาธารณสุข สำหรับหน่วยงานที่มีลักษณะการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านยา เวชภัณฑ์ และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล จึงควรให้มีหน่วยงานขับเคลื่อนการดำเนินงานตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในนามของสำนักงานปลัดกระทรวงสาธารณสุข และมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อประสานงาน ฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข

ฉะนั้น อาศัยอำนาจตามความในมาตรา ๒๑ และมาตรา ๓๘ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ปลัดกระทรวงสาธารณสุข จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข โดยมีหน้าที่และอำนาจ ดังนี้

ข้อ ๑. รับผิดชอบหลักเกี่ยวกับงานควบคุมและกำกับดูแล (Main Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข

ก. ปฏิบัติหน้าที่ที่เกี่ยวข้องกับงานควบคุมและกำกับดูแล ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ข. เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) มีลักษณะ หน้าที่และความรับผิดชอบ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔ ฉบับลงวันที่ ๑๑ สิงหาคม พ.ศ. ๒๕๖๔

ค. ฝ้าระวังความเสี่ยง เตรียมพร้อมรับมือและแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข

ง. ประสาน...



ง. ประสานดำเนินงานร่วมกับหน่วยงานควบคุมและกำกับดูแลเกี่ยวกับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุขที่ให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านยา เวชภัณฑ์ และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา

จ. ประสานความร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (ศปช.สกมช.) (National CERT)

ฉ. รายงานผลเบื้องต้นต่อผู้บังคับบัญชา เพื่อนำเสนอผู้บริหารระดับสูงด้านความปลอดภัยสารสนเทศ (CISO) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ช. ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับเทคโนโลยีสารสนเทศดิจิทัลด้านสุขภาพ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะเกี่ยวกับมาตรฐานความมั่นคงปลอดภัย หรือกรณีอื่นใดเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารด้านธุรกรรมทางอิเล็กทรอนิกส์ด้านสุขภาพ

ข้อ ๒. รับผิดชอบหลักเกี่ยวกับงานควบคุมและกำกับดูแล (Regulator) หน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุขที่ให้บริการข้อมูลสุขภาพดิจิทัล และระบบสุขภาพดิจิทัล

ก. จัดทำข้อเสนอแนะที่เกี่ยวข้องกับมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการพัฒนาบริการข้อมูลสุขภาพดิจิทัล และระบบสุขภาพดิจิทัล

ข. จัดทำข้อเสนอแนะเกี่ยวกับมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการพัฒนาบริการข้อมูลสุขภาพดิจิทัล และระบบสุขภาพดิจิทัล

ข้อ ๓. ในการปฏิบัติตามคำสั่งนี้ หากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจำเป็นต้องออกระเบียบ ประกาศ คำสั่ง แนวทางปฏิบัติ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการจัดทำระเบียบ ประกาศ คำสั่ง แนวทางปฏิบัติเสร็จแล้วให้เสนอผู้มีอำนาจเพื่อพิจารณาลงนามใช้บังคับต่อไป

ทั้งนี้ ตั้งแต่บัดนี้ เป็นต้นไป

สั่ง ณ วันที่ ๒๙ มีนาคม พ.ศ. ๒๕๖๕



(นายเกียรติภูมิ วงศ์รจิต)  
ปลัดกระทรวงสาธารณสุข