

ด่วนที่สุด

ที่ พจ ๐๐๓๓.๐๐๒/๓๖๗



สำนักงานสาธารณสุขจังหวัดพิจิตร
ถนนคลองคะเชนทร์ พจ. ๖๖๐๐๐

๒๐ เมษายน ๒๕๖๖

เรื่อง ย้ำเตือนให้หน่วยงานปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด

เรียน ผู้อำนวยการโรงพยาบาลพิจิตร, ผู้อำนวยการโรงพยาบาลชุมชนทุกแห่ง และสาธารณสุขอำเภอทุกแห่ง

อ้างถึง หนังสือสำนักงานสาธารณสุขจังหวัดพิจิตรที่ พจ ๐๐๓๓.๐๐๒/๓๖๖ ลงวันที่ ๕ เมษายน ๒๕๖๖

สิ่งที่ส่งมาด้วย มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ จำนวน ๑ ชุด

ตามหนังสือที่อ้างถึง สำนักงานสาธารณสุขจังหวัดพิจิตร ขอให้หน่วยงานดำเนินการตามแนวทางในการป้องกันและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยบริการในจังหวัดพิจิตร เพื่อเป็นการป้องกันและรับมือจากภัยคุกคามทางไซเบอร์ ซึ่งปัจจุบันยังคงพบช่องโหว่ทางไซเบอร์ของหลายหน่วยงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ได้แจ้งและย้ำเตือนมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข ฉบับที่ ๑ เพื่อให้ทุกหน่วยงานดำเนินการตามมาตรการโดยเคร่งครัด

ในการนี้ สำนักงานสาธารณสุขจังหวัดพิจิตร ขอให้หน่วยงานทุกแห่ง ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อทราบและปฏิบัติตามมาตรการอย่างเคร่งครัดต่อไป

ขอแสดงความนับถือ

(นายวิศิษฎ์ อภิสิทธิ์วิทยา)
นายแพทย์สาธารณสุขจังหวัดพิจิตร

กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข

โทร. ๐ ๕๖๙๙ ๐๓๕๒-๘ ต่อ ๑๒๒

โทรสาร ๐ ๕๖๙๙ ๐๓๕๓

e-office



มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข

ฉบับที่ ๑

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลบังคับใช้เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที มิให้เกิดผลกระทบต่อความมั่นคงปลอดภัยทางด้านสาธารณสุขของประเทศ

ในการนี้ เพื่อให้หน่วยงานในสังกัดกระทรวงสาธารณสุขสามารถดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม กระทรวงสาธารณสุขจึงได้กำหนดมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข ฉบับที่ ๑ ให้ทุกหน่วยงานปฏิบัติโดยเคร่งครัดและต่อเนื่อง ดังต่อไปนี้

๑. มาตรการระดับประเทศ

กระทรวงสาธารณสุข พร้อมให้ความร่วมมือกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานที่เกี่ยวข้อง รวมถึงให้การสนับสนุนนโยบายในระดับประเทศ ในการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. มาตรการจากส่วนกลาง

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CERT) ดำเนินการ ดังนี้

- ๑) จัดทำทะเบียนกลางของกระทรวง รวบรวมชื่อเว็บไซต์และชื่อโดเมนระบบงานต่างๆ ที่หน่วยงานในสังกัดกระทรวงสาธารณสุขใช้งาน เพื่อการกำกับดูแล
- ๒) สำรวจสถานะความพร้อมด้านเครือข่ายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานในสังกัดกระทรวงสาธารณสุข
- ๓) เผื่อระวังภัยคุกคามทางไซเบอร์ ตรวจสอบค้นหาช่องโหว่ของหน่วยงานในสังกัดกระทรวงสาธารณสุขในเบื้องต้น
- ๔) ดำเนินการปิดการเข้าถึงผ่านชื่อโดเมนในทันทีที่ตรวจพบภัยคุกคามทางไซเบอร์ และประสานแจ้งพร้อมให้ความช่วยเหลือหน่วยงานเจ้าของเว็บไซต์หรือระบบงานให้ดำเนินการปิดช่องโหว่หรือแก้ไขให้แล้วเสร็จภายใน ๒๔ ชั่วโมง
- ๕) เป็นหน่วยงานกลางในการสร้าง Community การรักษาความมั่นคงปลอดภัยไซเบอร์ โดยรวมทีม CIRT (Cyber Incident Response Team) ของหน่วยงานในสังกัดกระทรวงสาธารณสุข

๖) กำหนดช่องทางติดต่อ Health CERT

- โทรศัพท์ ๐๘ ๓๐๖๔ ๙๘๖๗, ๐ ๒๕๙๐ ๑๑๖๙, ๐ ๒๕๙๐ ๑๒๐๐
- อีเมล: health-cirt@moph.go.th
- Line Official: @health-cirt
- เว็บไซต์แจ้งเหตุการณ์ไซเบอร์: <https://health-cirt.moph.go.th>
- เว็บไซต์เผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารทางไซเบอร์:
<https://cyber.moph.go.th/>

๓. มาตรการภายในหน่วยงาน

หน่วยงานในสังกัดกระทรวงสาธารณสุข ให้ดำเนินการตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ โดยเคร่งครัด และให้ดำเนินการตามมาตรการเร่งด่วน ดังนี้

๑) **สำรวจเว็บไซต์และระบบงานในความดูแลของหน่วยงาน และจัดทำทะเบียนชื่อเว็บไซต์และชื่อโดเมน และ IP Address** เช่น ict-ops-moph.moph.go.th ๒๐๓.๑๕๗.xxx.xxx เป็นต้น และจัดส่งสำเนาไฟล์ไปยัง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ. อีเมล ictmoph@moph.go.th เพื่อนำไปจัดทำทะเบียนกลางของกระทรวงสาธารณสุข ให้ Health CERT ใช้ในการกำกับดูแลต่อไป

๒) **ปิดเว็บไซต์และระบบงานที่ไม่ได้ใช้งาน รวมถึงเว็บไซต์และระบบงานที่พบความเสี่ยงทั้งหมดในทันที เพื่อลดความเสี่ยงในการถูกคุกคามทางไซเบอร์จากผู้ไม่หวังดี**

๓) **ดูแล Environments** ทั้งหมดที่เกี่ยวข้อง ของเว็บไซต์ และอัปเดตให้ทันสมัย เช่น อัปเดตเวอร์ชันและ Patch ของ ระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบัน เป็นต้น

๔) **ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์** เช่น Firewall, Web Application Firewall และ Antivirus เป็นต้น พร้อมตั้งค่าให้ถูกต้อง เหมาะสมกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

๕) **เผื่อระวางภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง** โดยต้องจัดให้มีเจ้าหน้าที่ปฏิบัติงานเป็นประจำอย่างน้อย ๑ คน และต้องสามารถประสานงานกับ Health CERT ได้ตลอดเวลา

๖) **ก่อนเผยแพร่ข้อมูลส่วนบุคคลในทุกช่องทางทั้งระบบอินเทอร์เน็ตและอินเทอร์เน็ต จะต้องได้รับความเห็นชอบหรืออนุญาต** (อย่างมีหลักฐาน) จากผู้บริหารสูงสุดของหน่วยงาน

๗) **เว็บไซต์และระบบงาน ควรใช้ชื่อโดเมนของกระทรวงสาธารณสุข** (xxxx.moph.go.th) โดยแจ้งความประสงค์เป็นหนังสือราชการถึงศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.

๘) ตรวจสอบรายการปัจจัยเสี่ยงที่ทำให้เกิดช่องโหว่ทางไซเบอร์ ดังต่อไปนี้ หากพบให้จัดการปิดช่องโหว่ทันทีหรือโดยเร็วที่สุด

- ๘.๑ มีการอัปเดตไฟล์ที่มีความสำคัญขึ้นบนหน้าเว็บไซต์ทั้งภายใต้โดเมน (moph.go.th) และภายนอก (Development Platform ต่างๆ เช่น github) ทำให้ผู้โจมตีใช้ประโยชน์ได้ เช่น ไฟล์ที่ประกอบด้วย Username Password สำหรับเข้าใช้งานระบบ, Source code ของระบบ Token ในการยืนยันตัวตน
- ๘.๒ ขาดการอัปเดตซอฟต์แวร์ที่ใช้งานให้เป็นเวอร์ชันปัจจุบัน
- ๘.๓ มี CMS Plugins ที่ไม่ได้ใช้งานแล้วแต่ยังไม่ถอนการติดตั้ง
- ๘.๔ ขาดการทำ Data Encryption เพื่อการรับ-ส่งข้อมูลสำคัญทำได้จากคนที่มี Key เท่านั้น
- ๘.๕ ไม่มีการปิดกั้นการ exposed ของ website configuration, database configuration, website directory หรือเปิดให้เข้าถึงไฟล์ได้จากอินเทอร์เน็ตโดยไม่มีการตรวจสอบ เช่น เปิดหน้า Index Directory ไว้ ทำให้เห็นไฟล์ต่างๆ
- ๘.๖ ไม่ได้กำหนด IP Address ที่จะเข้าถึง Service จากระยะไกลที่มีความอ่อนไหว เช่น Database และ Network Protocol ต่าง ๆ
- ๘.๗ ไม่ได้กำหนด Rate-Limitation ในการเข้าถึง Service ว่าหากเกิด Connection failed บ่อยๆ จะต้องถูกปิดกั้น
- ๘.๘ ไม่มีการทำตรวจสอบ User Input ทำให้สามารถพัฒนาเป็นช่องโหว่ที่ใช้โจมตีได้ เช่น SQL Injection, XSS Attack
- ๘.๙ ไม่มีการปิด Error ที่ระบบตอบกลับ ทำให้ผู้โจมตีตรวจสอบได้ว่า Payload ที่ใช้สามารถทำงานได้หรือไม่
- ๘.๑๐ เปิดให้เชื่อมต่อ Database จากสาธารณะ เช่น เปิด Port ๓๓๐๖ โดยไม่ผ่าน VPN
- ๘.๑๑ มีการแชร์ไฟล์ที่มีข้อมูลส่วนบุคคลในพื้นที่สาธารณะ (Public File Sharing) เช่น google drive , OneDrive โดยไม่เข้ารหัสไฟล์ หรือแชร์เฉพาะบุคคล
- ๘.๑๒ ขาดการตรวจสอบ Username และ Permission บนระบบที่อยู่ภายใต้การดูแลให้ถูกต้อง หากพบความผิดปกติ ควรแก้ไขโดยทันที
