ด่วนที่สุด

ที่ สธ ๐๒๑๒/ว๑๑๕๓๐



สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๑๓ สิงหาคม ๒๕๖๙

เรื่อง มาตรการเร่งด่วนเพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของระบบสารสนเทศในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

เรียน นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑– ๑๒ ผู้อำนวยการโรงพยาบาลศูนย์ ผู้อำนวยการโรงพยาบาลทั่วไป และผู้อำนวยการโรงพยาบาลชุมชนทุกแห่ง

ด้วยคณะรัฐมนตรีมีมติเห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi - Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThaID) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กมช.) เสนอเมื่อวันที่ ๑๑ สิงหาคม ๒๕๖๙ เพื่อยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัยมากยิ่งขึ้น นำไปสู่การเพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจและนักลงทุน ประเทศไทยมีมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ทัดเทียมกับระดับสากล

สำนักงานปลัดกระทรวงสาธารณสุข พิจารณาแล้วเห็นควรกำหนดมาตรการเร่งด่วนเพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของระบบสารสนเทศในสังกัดกระทรวงสาธารณสุข ตามมติคณะรัฐมนตรีดังกล่าว เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานปลัดกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับนโยบายของรัฐบาลในการอุดช่องโหว่ของระบบสารสนเทศภาครัฐ จึงขอให้ทุกหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ดำเนินการตามมาตรการเร่งด่วน ๓ ประการ ดังต่อไปนี้อย่างเคร่งครัด

๑. การบังคับเปลี่ยนรหัสผ่าน (Force Reset Password) ให้หน่วยงานแจ้งผู้ดูแลระบบดำเนินการบังคับให้ข้าราชการ พนักงานราชการ เจ้าหน้าที่ในสังกัด และผู้ใช้งานทุกราย ทำการเปลี่ยนรหัสผ่านใหม่ทั้งหมดในทุกระดับสิทธิ์ทันที ทั้งนี้ เพื่อเป็นการตัดวงจรภัยคุกคาม และป้องกันมิให้ผู้ไม่ประสงค์ดีนำรหัสผ่านเดิมที่อาจเคยรั่วไหล กลับมาใช้ลักลอบเข้าถึงระบบสารสนเทศของทางราชการ

๒. การทำความสะอาดระบบ (System Cleansing) ให้หน่วยงานเร่งตรวจสอบระบบสารสนเทศ ทรัพยากรระบบ และเว็บไซต์ในความรับผิดชอบทั้งหมด หากพบระบบใดที่เป็น ระบบเก่า หรือ ระบบร้าง ที่ไม่มีการใช้งานแล้ว ให้ดำเนินการ ปิดการเข้าถึงในระดับโครงสร้างระบบ (Back-end) อย่างถาวร ภายใน ๑๕ วัน เพื่อป้องกันการใช้ระบบหลังบ้านที่ถูกทิ้งร้างเป็นช่องโหว่ในการโจมตี

๓. การยกระดับการยืนยันตัวตน (Multi-Factor Authentication: MFA) และการควบคุมการเข้าถึง ให้หน่วยงานนำระบบการยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น การใช้ Digital Identity (ThaID) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย มาใช้กับระบบสารสนเทศอย่างเป็นรูปธรรม โดยให้ยึดหลักเกณฑ์ดังนี้

๓.๑ ระบบที่เปิดให้เข้าถึงผ่านเครือข่ายภายนอกหน่วยงาน (อินเทอร์เน็ต) ต้องบังคับใช้งานระบบ MFA เช่น การใช้ Digital Identity (ThaID) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัยในการเข้าสู่ระบบทุกกรณี

๓.๒ กรณี...

๓.๒ กรณีระบบใดยังไม่สามารถรองรับการใช้งาน MFA เช่น การใช้ Digital Identity (ThaID) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัยได้ ให้หน่วยงานดำเนินการตั้งค่าจำกัดสิทธิ์การเข้าถึง โดยให้ใช้งานได้เฉพาะเครือข่ายภายในหน่วยงาน (Intranet) เท่านั้น ห้ามเผยแพร่หรือเปิดให้เข้าถึงผ่านเครือข่ายอินเทอร์เน็ตโดยเด็ดขาด จนกว่าระบบนั้นจะได้รับการปรับปรุงให้รองรับ MFA เรียบร้อยแล้ว

๔. รายงานการดำเนินการข้อ ๑ – ๓ ไปยังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ภายในวันที่ ๒๘ สิงหาคม ๒๕๖๙ ผ่านแบบฟอร์มที่กำหนด https://moph.link/pzSBhZmTI หรือ QR Code ที่ปรากฏท้ายหนังสือ และมอบหมายให้นางสาวณัฐณิชา จันทร์ทอง ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ โทร. ๐ ๒๕๙๐ ๑๒๐๑ เป็นผู้ประสาน

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการอย่างเคร่งครัดด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายโสภณ เอี่ยมศิริถาวร)
รองปลัดกระทรวงสาธารณสุข
หัวหน้ากลุ่มภารกิจด้านพัฒนาการสาธารณสุข
ปฏิบัติราชการแทนปลัดกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๕๙๐ ๑๒๑๓
ไปรษณีย์อิเล็กทรอนิกส์ ictmoph-datagov@moph.go.th

https://moph.link/pzSBhZmTI
แบบฟอร์มรายงาน