



ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานหลักประกันสุขภาพแห่งชาติ ให้เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๓๑ วรรคหนึ่ง และมาตรา ๓๖ (๒) แห่งพระราชบัญญัติหลักประกันสุขภาพแห่งชาติ พ.ศ. ๒๕๔๕ ประกอบมาตรา ๔๔ มาตรา ๔๕ แห่งพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ เมษายน พ.ศ. ๒๕๖๕ เป็นต้นไป

ข้อ ๓ ให้ยกเลิก

(๑) ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ เรื่อง นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ลงวันที่ ๒๓ มิถุนายน พ.ศ. ๒๕๕๗

(๒) ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ลงวันที่ ๑๖ กรกฎาคม พ.ศ. ๒๕๕๗

ข้อ ๔ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานหลักประกันสุขภาพแห่งชาติ และให้หมายความรวมถึงสำนักงานสาขาด้วย

“เลขาธิการ” หมายความว่า เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ

“นโยบาย” หมายความว่า หลักการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“แนวปฏิบัติ” หมายความว่า ข้อปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

/ข้อ ๕...

ข้อ ๕ แผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ประกอบด้วย

- (๑) แผนนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- (๒) แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ใช้งาน
- (๓) แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ดูแลระบบ
- (๔) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

ข้อ ๖ ในกรณีที่กฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ ว่าด้วยการรักษาความมั่นคง
ปลอดภัยด้านสารสนเทศ กำหนดแผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ไว้เป็นอย่างอื่น ให้ถือปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ ว่าด้วยการนั้น

ข้อ ๗ วิธีดำเนินการตามแผนนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- (๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศ
- (๒) การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน
- (๓) การตรวจสอบและประเมินความเสี่ยง
- (๔) การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงาน

- (๕) การรับมือข้อต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศ

ของสำนักงาน

- (๖) การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- (๗) การปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- (๘) การรับมือภัยคุกคามทางไซเบอร์

ข้อ ๘ วิธีปฏิบัติตามแนวทางในการรักษาความปลอดภัยด้านสารสนเทศของผู้ใช้งาน

- (๑) การปฏิบัติหน้าที่ทั่วไป
- (๒) การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย
- (๓) การควบคุมเข้าถึงระบบปฏิบัติการ
- (๔) การใช้งานบัญชีผู้ใช้งาน (Account)
- (๕) การกำหนดรหัสผ่าน (Password) การเปลี่ยนรหัสผ่าน และการใช้งานรหัสผ่าน
- (๖) การป้องกันจากโปรแกรมประสงค์ร้าย (Malware)
- (๗) การใช้ระบบอินเทอร์เน็ต (Internet)
- (๘) การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ของสำนักงาน
- (๙) การจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย
- (๑๐) การเคลื่อนย้ายและการทำสำเนาสารสนเทศ
- (๑๑) การควบคุมอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูล
- (๑๒) การทำลายสื่อบันทึกข้อมูลหรือการทำลายไฟล์ข้อมูลที่มีระดับลับขึ้นไป
- (๑๓) การเข้ารหัสข้อมูลที่มีระดับลับขึ้นไป

ข้อ ๙ วิธีปฏิบัติเพื่อรักษาความปลอดภัยด้านสารสนเทศของผู้ดูแลระบบ

- (๑) การปฏิบัติหน้าที่โดยทั่วไปของผู้ดูแลระบบ
- (๒) การกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

- (๓) การควบคุมการเข้าถึงระบบสารสนเทศ
- (๔) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
- (๕) การควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
- (๖) การควบคุมการเข้าถึงระบบปฏิบัติการ
- (๗) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- (๘) การปฏิบัติเมื่อเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย กรณีการเข้าถึงระบบ

โดยไม่ได้รับอนุญาต

- (๙) การปฏิบัติภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย
- (๑๐) การสำรองข้อมูล
- (๑๑) การสำรองและกู้คืนข้อมูล
- (๑๒) การสร้างความตระหนัก
- (๑๓) การตรวจสอบและการประเมินผล
- (๑๔) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๑๐ วิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

- (๑) การปฏิบัติการเข้าออกพื้นที่ภายในสำนักงาน
- (๒) การกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอก

สำนักงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานได้

ข้อ ๑๑ การปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๑๒ กรณีมีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้เลขาธิการเป็นผู้มีอำนาจวินิจฉัยชี้ขาด โดยอาจมอบคณะกรรมการบริหารนโยบายดิจิทัลของสำนักงาน พิจารณาเสนอความเห็นก่อนก็ได้

ประกาศ ณ วันที่ ๑๗ เมษายน พ.ศ. ๒๕๖๕

นางสาวกัญญาพร นามวงศ์
เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ
นางสาวกัญญาพร นามวงศ์
นางสาวกัญญาพร นามวงศ์



(นายจเด็จ ธรรมธัชอารี)

เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ