

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์
ให้แก่ข้อมูลหรือระบบสารสนเทศ

พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ เพื่อประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศอันจะนำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ประเภทข้อมูล” หมายความว่า หมวดหมู่ข้อมูลที่ถูกกำหนดขึ้นโดยหน่วยงานตามแนวทางที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนด

“ระบบสารสนเทศ” หมายความว่า ระบบหรือชุดทรัพยากรด้านสารสนเทศที่ถูกใช้สำหรับการเก็บรวบรวม การประมวลผล การบำรุงรักษา การใช้ การเผยแพร่ หรือการทำลายข้อมูล

“คุณลักษณะความมั่นคงปลอดภัยไซเบอร์” (Security category) หมายความว่า ลักษณะเฉพาะของข้อมูลหรือระบบสารสนเทศในด้านความมั่นคงปลอดภัยไซเบอร์ ตามการประเมินและจัดระดับผลกระทบต่อการดำเนินงานของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือความปลอดภัยของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงาน หรือประชาชน ที่อาจเกิดขึ้นเมื่อข้อมูลลับของหน่วยงานรั่วไหล ข้อมูลของหน่วยงานถูกลบถูกบิดเบือน หรือถูกทำลาย หรือข้อมูลหรือระบบสารสนเทศของหน่วยงานไม่อยู่ในสภาพพร้อมใช้งาน

“การรักษาความลับ” (Confidentiality) หมายความว่า การรักษาหรือสงวนไว้ ซึ่งการจำกัดการเข้าถึงหรือการเปิดเผยข้อมูลให้แก่บุคคล หน่วยงานอื่น หรือชุดคำสั่งที่ไม่ได้รับอนุญาต

“การรักษาความถูกต้องครบถ้วน” (Integrity) หมายความว่า การรักษาหรือสงวนไว้ ซึ่งความถูกต้องและความครบถ้วนของข้อมูล

“การรักษาสภาพพร้อมใช้งาน” (Availability) หมายความว่า การดำเนินการ เพื่อให้บุคคล หน่วยงาน หรือชุดคำสั่งที่ได้รับอนุญาตสามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ตามต้องการและได้อย่างมีประสิทธิภาพ

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๔ ให้หน่วยงานกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objectives) ในเรื่องดังต่อไปนี้

- (๑) การรักษาความลับ (Confidentiality)
- (๒) การรักษาความถูกต้องครบถ้วน (Integrity)
- (๓) การรักษาสภาพพร้อมใช้งาน (Availability)

ในกรณีที่ข้อมูลหรือระบบสารสนเทศได้เผยแพร่ต่อสาธารณะแล้ว หน่วยงานไม่ต้องพิจารณาวัตถุประสงค์ตามวรรคหนึ่ง (๑)

ข้อ ๕ การพิจารณาวัตถุประสงค์ตามข้อ ๔ วรรคหนึ่ง (๑) (๒) และ (๓) ให้ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นเป็นสามระดับ ได้แก่ ระดับต่ำ ระดับกลาง และระดับสูง

ข้อ ๖ การจัดระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับตามข้อ ๕ ให้หน่วยงานพิจารณาการประเมินผลกระทบในแต่ละด้าน ดังต่อไปนี้

- (๑) ผลกระทบต่อมูลค่าความเสียหายทางการเงินหรือทรัพย์สิน หรือต่อชื่อเสียงของหน่วยงาน
- (๒) ผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงาน หรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด
- (๓) ผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน
- (๔) ผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

ในกรณีหน่วยงานที่จัดระดับผลกระทบที่อาจเกิดขึ้นเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลกำหนดแนวทางการประเมินผลกระทบตามวรรคหนึ่งให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ในกรณีที่สถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์เปลี่ยนแปลงไป หน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดผลกระทบเพิ่มเติม หรือยกเว้นหรือยกเลิกผลกระทบข้อใดข้อหนึ่งหรือหลายข้อก็ได้

ข้อ ๗ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ในการรักษาความลับตามข้อ ๔ (๑) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัดให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อ การดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก ให้จัดเป็น ผลกระทบระดับสูง

ในกรณีที่มีการดำเนินการของหน่วยงานอาจเปิดเผยข้อมูลที่ถูกกำหนดชั้นความลับตามระเบียบ ว่าด้วยการรักษาความลับของทางราชการและระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัย แห่งชาติ ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ ให้จัดเป็นผลกระทบ ระดับต่ำเป็นอย่างน้อย

(๒) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก ให้จัดเป็นผลกระทบ ระดับกลางเป็นอย่างน้อย

(๓) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด ให้จัดเป็นผลกระทบ ระดับสูง

ข้อ ๘ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ ในการรักษาความถูกต้องครบถ้วนตามข้อ ๔ (๒) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่มีการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อ การดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีที่มีการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อ การดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่มีการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อ การดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๙ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ ในการรักษาสภาพพร้อมใช้งานตามข้อ ๔ (๓) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อ การดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด ให้จัดเป็น ผลกระทบระดับต่ำ

(๒) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อ การดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อ การดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๑๐ การกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ ในกรณี ที่ระบบสารสนเทศมีข้อมูลหลายประเภทข้อมูล ให้หน่วยงานดำเนินการ ดังต่อไปนี้

(๑) ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ด้านความมั่นคง ปลอดภัยไซเบอร์ตามข้อ ๔ ให้แก่แต่ละประเภทข้อมูล

(๒) พิจารณากำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ โดยใช้ระดับผลกระทบของประเภทข้อมูลตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อ ๔ ในแต่ละเรื่องที่มีระดับผลกระทบมากที่สุด

หน่วยงานอาจดำเนินการกำหนดประเภทข้อมูลตามหลักเกณฑ์ของหน่วยงาน หรือตามแนวทางในประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยแนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

ข้อ ๑๑ ให้หน่วยงานพิจารณาทบทวนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศทุก ๓ ปีเป็นอย่างน้อย หรือทบทวนเมื่อข้อมูล ระบบสารสนเทศ หรือหน้าที่ของหน่วยงานมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ และบันทึกผลการพิจารณาทบทวนพร้อมเหตุผลในการคงไว้ หรือแก้ไขเปลี่ยนแปลงระดับผลกระทบที่อาจเกิดขึ้นของวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ ตามข้อ ๔ ในแต่ละเรื่องด้วย

ข้อ ๑๒ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้เป็นที่สิ้นสุด

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖

ภูมิธรรม เวชยชัย

รองนายกรัฐมนตรี ปฏิบัติหน้าที่

ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ