# บันทึกข้อความ

**ส่วนราชการ** ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ฝ่ายบริหารทั่วไป โทร. ๐ ๒๒๘๑ ๒๗๑๔

**ที่** กษ ๐๔๐๓/ว ๙๖ **วันที่** ๒๓ กุมภาพันธ์ ๒๕๖๗

**เรื่อง** เอกสารแจ้งเวียน

เรียน อธิบดีกรมตรวจบัญชีสหกรณ์
รองอธิบดีกรมตรวจบัญชีสหกรณ์
ผู้อำนวยการสำนัก ผู้อำนวยการศูนย์ และ ผู้อำนวยการกอง
ผู้อำนวยการสำนักงานตรวจบัญชีสหกรณ์ที่ ๑ – ๑๐
หัวหน้ากลุ่มพัฒนาระบบบริหาร และ หัวหน้ากลุ่มตรวจสอบภายใน
หัวหน้าสำนักงานตรวจบัญชีสหกรณ์ทุกจังหวัด

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ขอส่งสำเนา ☑ หนังสือ ☐ คำสั่ง ☐ ระเบียบ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มระบบเครือข่ายคอมพิวเตอร์ ที่ กษ ๐๔๐๓/๓๙ ลงวันที่ ๒๑ กุมภาพันธ์ ๒๕๖๗ เรื่อง แจ้งเวียนประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๓ ฉบับ

จึงเรียนมาเพื่อ ☐ โปรดทราบ
☐ โปรดทราบและดำเนินการต่อไป
☑ โปรดทราบและถือปฏิบัติต่อไป
☐ โปรดทราบและแจ้งผู้เกี่ยวข้องทราบ

(นางสาวกนกพรรณ ชำนาญกิจ)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

มาตราฐาน กสมช

# บันทึกข้อความ

**ส่วนราชการ** ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มระบบเครือข่ายคอมพิวเตอร์ โทร. ๔๓๒๖
**ที่** กษ ๐๔๐๓/๓๙ **วันที่** ๒๑ กุมภาพันธ์ ๒๕๖๗
**เรื่อง** แจ้งเวียนประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๓ ฉบับ

เรียน ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (Department Chief Information Officer : DCIO)

**๑. เรื่องเดิม**

ตามหนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ สกมช ๐๙๐๐/ว ๔๒๘ ลงวันที่ ๖ กุมภาพันธ์ ๒๕๖๗ เรื่อง แจ้งเวียนประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๓ ฉบับ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทราบถึงผลบังคับใช้ วัตถุประสงค์ รายละเอียดสาระสำคัญ รวมทั้งสามารถนำไปปฏิบัติได้อย่างถูกต้อง ครบถ้วนและสอดคล้องตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) นั้น

**๒. ข้อเท็จจริง**

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มระบบเครือข่ายคอมพิวเตอร์ เห็นว่าประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีความสำคัญ ควรประชาสัมพันธ์ให้ทราบเกี่ยวกับมาตรฐานต่างๆ โดยสรุปสาระสำคัญของประกาศทั้ง ๓ ฉบับ ดังนี้

๑) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ มีผลบังคับใช้ตั้งแต่วันที่ ๑๘ มกราคม ๒๕๖๘ เป็นต้นไป โดยมีวัตถุประสงค์เพื่อให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถกำหนดความสำคัญของข้อมูล/ระบบสารสนเทศ นำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมทำให้ประชาชนได้รับบริการที่มีประสิทธิภาพและมีความมั่นคงปลอดภัยทางไซเบอร์อันจะส่งผลให้ธุรกิจหรือบริการภายในประเทศได้รับความเชื่อมั่นมากยิ่งขึ้น อย่างคุ้มค่า

๒) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ มีผลบังคับใช้ตั้งแต่วันที่ ๑๘ มกราคม ๒๕๖๘ เป็นต้นไป โดยมีวัตถุประสงค์เพื่อให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำได้อย่างเหมาะสม คุ้มค่า ลดมาตรการควบคุม และค่าใช้จ่ายที่เกิดความจำเป็น อันเป็นการช่วยประหยัดงบประมาณแผ่นดินของประเทศ

๓) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ มีผลบังคับใช้ตั้งแต่วันที่ ๑๙ มกราคม ๒๕๖๗ เป็นต้นไป โดยมีวัตถุประสงค์ เพื่อส่งเสริมธุรกิจและการให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้มีคุณภาพและได้รับการยอมรับจากผู้ใช้บริการทั้งในและต่างประเทศ ส่งผลให้ประเทศมีอำนาจในการแข่งขันมากยิ่งขึ้น รวมทั้งผู้ใช้บริการสามารถเลือกผู้ให้บริการที่เหมาะสมกับตนและได้มาตรฐาน ทั้งนี้ ประกาศ กมช. ฉบับนี้ ใช้บังคับกับบุคคลธรรมดา คณะบุคคล และนิติบุคคล ที่เป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

**๓. กฎหมาย....**

๓. **กฎหมาย ระเบียบที่เกี่ยวข้อง**

พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๒

๔. **ข้อพิจารณา**

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พิจารณาแล้วเห็นควรแจ้งเวียนประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๓ ฉบับ เพื่อสร้างความรู้ความเข้าใจและเตรียมการดำเนินการต่าง ๆ ให้เป็นไปตามที่กฎหมายกำหนดต่อไป

๕. **ข้อเสนอแนะ** -

จึงเรียนมาเพื่อโปรดพิจารณา

กนกพรรณ ช.

(นางสาวกนกพรรณ ชำนาญกิจ)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

เห็นชอบตามเสนอ

๒๑ ก.พ. ๒๕๖๗

(นางรพีพร กลั่นเนียม)
รองอธิบดีกรมตรวจบัญชีสหกรณ์ ปฏิบัติราชการแทน
อธิบดีกรมตรวจบัญชีสหกรณ์

# 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) ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรงมากให้จัดเป็นผลกระทบระดับสูง

ในกรณีที่การดำเนินการของหน่วยงานอาจเปิดเผยข้อมูลที่ถูกกำหนดชั้นความลับตามระเบียบว่าด้วยการรักษาความลับของทางราชการและระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ ให้จัดเป็นผลกระทบระดับต่ำเป็นอย่างน้อย

(๒) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก ให้จัดเป็นผลกระทบระดับกลางเป็นอย่างน้อย

(๓) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๘ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ในการรักษาความถูกต้องครบถ้วนตามข้อ ๔ (๒) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๙ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ในการรักษาสภาพพร้อมใช้งานตามข้อ ๔ (๓) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๑๐ การกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ ในกรณีที่ระบบสารสนเทศมีข้อมูลหลายประเภทข้อมูล ให้หน่วยงานดำเนินการ ดังต่อไปนี้

(๑) ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อ 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 การตีความและคำวินิจฉัยของประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
## เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ
## พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรกำหนดมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

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

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"หน่วยงาน" หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

"มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการที่กำหนดขึ้นเพื่อดำเนินการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) สำหรับข้อมูลหรือระบบสารสนเทศ

"ประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐาน" หมายความว่า ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๔ ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ ซึ่งพิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในเรื่องการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน และได้ระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์แต่ละเรื่องเป็นระดับต่ำ ระดับกลาง หรือระดับสูง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศแล้ว ให้หน่วยงานกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศนั้นในแต่ละระดับตามหัวข้อของประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานที่กำหนดในตารางท้ายประกาศนี้ ทั้งนี้ โดยพิจารณาจากคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

(๑) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับต่ำ ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อต่อไปนี้

(ก) การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)

(ข) แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) (ทั้งในส่วนของประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐาน)

(ค) การจัดการทรัพย์สิน (Asset Management)

(ง) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(จ) การควบคุมการเข้าถึง (Access Control)

(ฉ) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(ช) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(ซ) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(ฌ) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(ญ) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

(๒) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับกลาง ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อ ต่อไปนี้

(ก) ให้ดำเนินการตามข้อ (๑)

(ข) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)

(ค) การเชื่อมต่อระยะไกล (Remote Connection)

(ง) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(๓) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับสูง ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อ ต่อไปนี้

(ก) ให้ดำเนินการตามข้อ (๒)

(ข) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(ค) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(ง) การแบ่งปันข้อมูล (Information Sharing)

(จ) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

ข้อ ๕ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ตารางหัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ
สำหรับข้อมูลหรือระบบสารสนเทศ
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

| หัวข้อในการกำหนด<br>มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ<br>สำหรับข้อมูลหรือระบบสารสนเทศ | ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ | | |
|---|---|---|---|
| | ต่ำ | กลาง | สูง |
| **ประมวลแนวทางปฏิบัติ** | | | |
| องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) | | ● | ● |
| องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) | ● | ● | ● |
| องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) | ● | ● | ● |
| **กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** | | | |
| **๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)** | | | |
| ๑.๑ การจัดการทรัพย์สิน (Asset Management) | ● | ● | ● |
| ๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy) | ● | ● | ● |
| ๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) | | | ● |
| ๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) | | | ● |
| **๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)** | | | |
| ๒.๑ การควบคุมการเข้าถึง (Access Control) | ● | ● | ● |
| ๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) | ● | ● | ● |
| ๒.๓ การเชื่อมต่อระยะไกล (Remote Connection) | | ● | ● |
| ๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) | | ● | ● |
| ๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) | ● | ● | ● |
| ๒.๖ การแบ่งปันข้อมูล (Information Sharing) | | | ● |
| **๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)** | | | |
| ๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) | ● | ● | ● |

| หัวข้อในการกำหนด<br>มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ<br>สำหรับข้อมูลหรือระบบสารสนเทศ | ระดับคุณลักษณะ<br>ความมั่นคงปลอดภัยไซเบอร์<br>ของข้อมูลหรือระบบสารสนเทศ | | |
|---|---|---|---|
| | ต่ำ | กลาง | สูง |
| **๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)** | | | |
| ๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์<br>(Cybersecurity Incident Response Plan) | ● | ● | ● |
| ๔.๒ แผนการสื่อสารในภาวะวิกฤต<br>(Crisis Communication Plan) | ● | ● | ● |
| ๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์<br>(Cybersecurity Exercise) | ● | ● | ● |
| **๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)** | | | |
| ๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์<br>(Cybersecurity Resilience and Recovery) | | | ● |

# ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการ
เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๖

---

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงสมควรกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการรับรองคุณภาพของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำหนดแนวทางส่งเสริมพัฒนาการให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

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

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

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์” หมายความว่า ผู้ให้บริการที่เกี่ยวข้องกับการระบุ ป้องกัน ตรวจสอบ เฝ้าระวัง รับมือ ลดความเสี่ยง รักษาและฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์

“การรับรองคุณภาพ” หมายความว่า กระบวนการตรวจสอบและรับรองการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นกระบวนการดำเนินงาน ระบบหรือเครื่องมือที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงาน ว่ามีคุณภาพเป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

“คณะทำงานตรวจประเมิน” หมายความว่า คณะทำงานที่สำนักงานแต่งตั้งขึ้นเพื่อทำหน้าที่ตรวจสอบคุณภาพเกี่ยวกับการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ไม่ว่าจะเป็นกระบวนการดำเนินงาน ระบบหรือเครื่องมือที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงาน

"องค์กรที่ทำหน้าที่ตรวจคุณภาพ" หมายความว่า หน่วยงานที่ให้บริการตรวจสอบคุณภาพเกี่ยวกับการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นกระบวนการดำเนินงาน ระบบหรือเครื่องมือ ที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงาน

ข้อ ๔ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์และป้องกันความเสียหายอันอาจเกิดขึ้นจากการดำเนินงานของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์หรือจากภัยคุกคามทางไซเบอร์ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการยอมรับว่ามีมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องเป็นผู้ให้บริการที่ได้รับการรับรองคุณภาพตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดในประกาศนี้ ทั้งนี้ การรับรองคุณภาพดังกล่าว ไม่ใช่การอนุญาตการเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๕ การรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์มี ๓ ระดับ ได้แก่

(๑) การรับรองคุณภาพขั้นต้น

(๒) การรับรองคุณภาพขั้นก้าวหน้า

(๓) การรับรองคุณภาพขั้นสูง

การรับรองคุณภาพตามวรรคหนึ่ง (๑) หรือ (๒) สำนักงานอาจรับรองให้แก่บุคคลธรรมดา คณะบุคคล หรือนิติบุคคลก็ได้ แต่การรับรองคุณภาพตามวรรคหนึ่ง (๓) ให้สำนักงานรับรองให้แก่นิติบุคคลเท่านั้น

สำนักงานอาจจัดให้มีการรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง สำหรับประเภทบริการที่ขอรับการรับรองเฉพาะบางประเภทบริการหรือบางระดับก็ได้ ทั้งนี้แล้วแต่ความพร้อมของสำนักงานในการรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๖ ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์รายใดประสงค์ได้รับการรับรองคุณภาพให้ยื่นคำขอต่อสำนักงานตามแบบที่สำนักงานกำหนด พร้อมทั้งเอกสารหรือหลักฐาน ดังต่อไปนี้

(๑) เอกสารแสดงความเชี่ยวชาญของบุคลากรของผู้ยื่นคำขอที่สอดคล้องกับประเภทบริการที่ขอรับการรับรอง ได้แก่ เอกสารแสดงวุฒิการศึกษา หนังสือรับรองประสบการณ์การทำงาน และเอกสารที่แสดงว่าได้รับการรับรองตามมาตรฐานสำหรับประเภทบริการที่ขอรับการรับรองตามที่สำนักงานประกาศกำหนดในกรณีที่ผู้ยื่นคำขอเป็นนิติบุคคล ผู้ยื่นคำขอต้องยื่นเอกสารแสดงความเชี่ยวชาญของบุคลากรสำหรับการรับรองคุณภาพในแต่ละระดับ ตามจำนวนที่กำหนด โดยบุคลากรดังกล่าวต้องเป็นบุคลากรที่ทำงานเต็มเวลาตามจำนวนที่กำหนด ดังต่อไปนี้

| ระดับการรับรองคุณภาพ | จำนวนบุคลากรที่ต้องยื่นเอกสารแสดงความเชี่ยวชาญ | จำนวนบุคลากรที่ทำงานเต็มเวลา |
|---|---|---|
| ขั้นต้น | อย่างน้อย ๑ คน | อย่างน้อย ๑ คน |
| ขั้นก้าวหน้า | อย่างน้อย ๒ คน | อย่างน้อย ๒ คน |
| ขั้นสูง | อย่างน้อย ๕ คน | อย่างน้อย ๓ คน |

ทั้งนี้ บุคลากรที่ทำงานเต็มเวลาอย่างน้อยหนึ่งคนต้องมีเอกสารที่แสดงว่าได้รับการรับรองตามมาตรฐานสำหรับประเภทบริการที่ขอรับการรับรองคุณภาพตามที่สำนักงานประกาศกำหนด และหากขอรับการรับรองคุณภาพขั้นสูง ผู้ยื่นคำขอต้องแสดงเอกสารการรับรองด้านกระบวนการตามมาตรฐานสากลของหน่วยงานผู้ยื่นคำขอด้วย

(๒) เอกสารแสดงประสบการณ์การทำงานในประเภทบริการที่ขอรับการรับรอง โดยอย่างน้อยต้องมีเอกสารแสดงประสบการณ์ในโครงการที่ดำเนินการแล้วเสร็จตามเป้าหมาย สำหรับการขอรับรองคุณภาพขั้นต้น การรับรองคุณภาพขั้นก้าวหน้า และการรับรองคุณภาพขั้นสูง เป็นจำนวนไม่น้อยกว่าหนึ่งโครงการ สามโครงการ และห้าโครงการ ตามลำดับ

(๓) เอกสารการรับรองตนเองตามแบบที่สำนักงานกำหนดที่แสดงว่าผู้ยื่นคำขอเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ปฏิบัติตามมาตรฐานที่กำหนดในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (เฉพาะในกรณีที่ผู้ยื่นคำขอเป็นนิติบุคคล)

การยื่นคำขอตามวรรคหนึ่งให้ดำเนินการโดยวิธีการทางอิเล็กทรอนิกส์เป็นหลัก โดยต้องมีการพิสูจน์ตัวตน (Identity Assurance Level) ไม่น้อยกว่าระดับ ๒ และใช้การเข้ารหัสด้วยวิธีการ Pretty Good Privacy (PGP) ในกรณีที่ยังไม่สามารถดำเนินการหรือมีเหตุอื่นใดทำให้ไม่สามารถดำเนินการโดยวิธีการทางอิเล็กทรอนิกส์ได้ ให้การดำเนินการดังกล่าวกระทำ ณ สำนักงาน

ผู้ยื่นคำขอตามข้อนี้ต้องชำระค่าธรรมเนียมตามที่สำนักงานกำหนด

ข้อ ๗ ประกาศสำนักงานตามข้อ ๖ (๑) ต้องมีรายละเอียดเกี่ยวกับประเภทบริการ รายละเอียดการตรวจประเมินบริการแต่ละประเภท และรายชื่อมาตรฐานหรือประกาศนียบัตรที่สามารถใช้เป็นหลักฐานในการขอรับการรับรองคุณภาพการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์แต่ละประเภทบริการสำหรับการรับรองคุณภาพขั้นต้น การรับรองคุณภาพขั้นก้าวหน้า และการรับรองคุณภาพขั้นสูง โดยให้พิจารณากำหนดรายชื่อมาตรฐานและประกาศนียบัตรในการรับรองคุณภาพแต่ละระดับโดยคำนึงถึงปัจจัย ดังต่อไปนี้

(๑) ระดับความยากง่ายของมาตรฐานหรือประกาศนียบัตร

(๒) การใช้ทักษะเฉพาะทาง

(๓) การทดสอบแบบลงมือปฏิบัติจริง

(๔) การได้รับการยอมรับ

ทั้งนี้ มาตรฐานหรือประกาศนียบัตรที่สามารถใช้เป็นหลักฐานในการขอรับการรับรองคุณภาพขั้นสูงต้องเป็นมาตรฐานหรือประกาศนียบัตรที่แสดงให้เห็นได้ว่าผู้ที่ได้รับจะต้องมีความเชี่ยวชาญเฉพาะด้านที่เกี่ยวข้องกับประเภทบริการนั้นเป็นที่ประจักษ์

ข้อ ๘ เมื่อได้รับคำขอรับการรับรองคุณภาพ ให้สำนักงานตรวจสอบคำขอรวมทั้งเอกสารหรือหลักฐานว่าถูกต้องและครบถ้วนหรือไม่ หากไม่ถูกต้องหรือไม่ครบถ้วน ให้สำนักงานแจ้งให้ผู้ยื่นคำขอแก้ไขเพิ่มเติมคำขอ หรือจัดส่งเอกสารหรือหลักฐาน ให้ถูกต้องและครบถ้วนภายในระยะเวลา

ที่สำนักงานกำหนด ในกรณีที่ผู้ยื่นคำขอไม่แก้ไขเพิ่มเติมคำขอ หรือไม่จัดส่งเอกสารหรือหลักฐานให้ครบถ้วนภายในระยะเวลาที่สำนักงานกำหนด ให้ถือว่าผู้ยื่นคำขอไม่ประสงค์จะให้ดำเนินการต่อไป และให้สำนักงานจำหน่ายเรื่องออกจากสารบบ

ในกรณีที่คำขอรับการรับรองคุณภาพ รวมทั้งเอกสารหรือหลักฐานครบถ้วน ให้สำนักงานมอบหมายองค์กรที่ทำหน้าที่ตรวจคุณภาพที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ความเห็นชอบ หรือแต่งตั้งคณะทำงานตรวจประเมิน เพื่อทำหน้าที่ในการตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานเพื่อการรับรองคุณภาพของผู้ยื่นคำขอ จำนวนอย่างน้อยสามคน ประกอบด้วยบุคคลที่ไม่มีผลประโยชน์ที่อาจทำให้การตรวจสอบไม่เป็นกลาง และเป็นผู้ที่มีความเชี่ยวชาญหรือประสบการณ์ในด้าน ดังต่อไปนี้

(๑) การรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) การรับรองคุณภาพตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง

(๓) ความเชี่ยวชาญเฉพาะทางที่เกี่ยวข้องกับบริการที่ขอรับการรับรอง

การแต่งตั้งคณะทำงานตรวจประเมินตามวรรคสอง สำนักงานจะแต่งตั้งคณะทำงานตรวจประเมินโดยจำแนกตามประเภทบริการที่ขอรับการรับรองก็ได้ โดยให้ทำหน้าที่คราวละสามปี ซึ่งคณะทำงานตรวจประเมินอย่างน้อยหนึ่งคนต้องเป็นผู้ที่มีประกาศนียบัตรแสดงถึงระดับความเชี่ยวชาญเฉพาะทางที่เกี่ยวข้องกับประเภทบริการที่ทำการตรวจประเมิน

ข้อ ๙ เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินตามข้อ ๘ ได้รับคำขอรับการรับรองคุณภาพ พร้อมทั้งเอกสารหรือหลักฐานของผู้ยื่นคำขอจากสำนักงานแล้ว ให้ดำเนินการ ดังต่อไปนี้

(๑) กรณีขอรับการรับรองคุณภาพขั้นต้น ให้ตรวจสอบข้อมูลในคำขอรับการรับรองคุณภาพและเอกสารหรือหลักฐาน หากพิจารณาแล้วเห็นว่าผู้ยื่นคำขอเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ปฏิบัติตามมาตรฐานที่กำหนดในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเอกสารหรือหลักฐานที่ผู้ยื่นคำขอเป็นเอกสารที่ถูกต้อง ให้แจ้งผลการตรวจสอบให้สำนักงานทราบภายในเจ็ดวันนับแต่วันตรวจสอบแล้วเสร็จ ทั้งนี้ องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องดำเนินการให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่ได้รับคำขอพร้อมด้วยเอกสารหรือหลักฐานครบถ้วนจากสำนักงาน

(๒) กรณีขอรับการรับรองคุณภาพขั้นก้าวหน้า ให้ตรวจสอบข้อมูลในคำขอรับการรับรองคุณภาพและเอกสารหรือหลักฐาน หากพิจารณาแล้วเห็นว่าผู้ยื่นคำขอเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ปฏิบัติตามมาตรฐานที่กำหนดในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเอกสารหรือหลักฐานที่ผู้ยื่นคำขอเป็นเอกสารที่ถูกต้อง ให้องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินดำเนินการตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการด้วยวิธีการสัมภาษณ์

โดยให้เรียกเก็บค่าธรรมเนียมได้ไม่เกินสามวัน และองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องดำเนินการตรวจสอบให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่ได้รับคำขอพร้อมด้วยเอกสารหรือหลักฐานครบถ้วนจากสำนักงาน ทั้งนี้ เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินได้ตรวจสอบแล้วว่าข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ยื่นคำขอถูกต้องและได้มาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้แจ้งผลการตรวจสอบให้สำนักงานทราบภายในเจ็ดวันนับแต่วันตรวจสอบแล้วเสร็จ

(๓) กรณีขอรับการรับรองคุณภาพขั้นสูงให้ดำเนินการตาม (๒) โดยองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องตรวจสอบด้วยว่าผู้ขอรับการรับรองคุณภาพขั้นสูงเป็นผู้ที่ได้รับการรับรองด้านกระบวนการตามมาตรฐานสากล และให้องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินดำเนินการตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการ ณ สถานประกอบการหรือสถานที่ให้บริการของผู้ยื่นคำขอด้วย โดยผู้ยื่นคำขอต้องเตรียมความพร้อมทั้งบุคลากร เอกสารหรือหลักฐาน สถานที่และเครื่องมือที่จำเป็นในการตรวจสอบ รวมทั้งอำนวยความสะดวกแก่องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินในการเข้าถึงระบบสารสนเทศที่เกี่ยวข้อง โดยให้เรียกเก็บค่าธรรมเนียมได้ไม่เกินห้าวัน ทั้งนี้ เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินได้ตรวจสอบแล้วว่าข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ยื่นคำขอถูกต้องและได้มาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้แจ้งผลการตรวจสอบให้สำนักงานทราบภายในเจ็ดวันนับแต่วันตรวจสอบแล้วเสร็จ

ในการดำเนินการตามวรรคหนึ่ง (๑) (๒) หรือ (๓) องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินอาจแจ้งให้ผู้ยื่นคำขอส่งข้อมูลหรือเอกสารที่จำเป็นเพิ่มเติมก็ได้ ในการนี้มิให้นับระยะเวลาตั้งแต่วันที่แจ้งจนถึงวันที่ได้รับข้อมูลหรือเอกสารดังกล่าวจากผู้ยื่นคำขอรวมเข้าเป็นระยะเวลาที่องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องดำเนินการตรวจสอบให้แล้วเสร็จ

ข้อ ๑๐ เมื่อสำนักงานได้รับแจ้งผลการตรวจสอบตามข้อ ๙ วรรคหนึ่ง (๑) (๒) หรือ (๓) แล้ว ให้สำนักงานแต่งตั้งคณะทำงานรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์จำนวนอย่างน้อยสามคน เพื่อพิจารณาผลการตรวจสอบว่าข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ยื่นคำขอถูกต้องและได้มาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรองจริง และให้แจ้งให้สำนักงานออกใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้า หรือใบรับรองคุณภาพขั้นสูง แล้วแต่กรณี ให้แก่ผู้ยื่นคำขอ

ข้อ ๑๑ ให้ใบรับรองคุณภาพมีอายุนับตั้งแต่วันที่ออกใบรับรองคุณภาพ ดังต่อไปนี้

| ระดับใบรับรองคุณภาพ | อายุใบรับรองคุณภาพ |
|---|---|
| ขั้นต้น | ๒ ปี |
| ขั้นก้าวหน้า | ๓ ปี |
| ขั้นสูง | ๓ ปี |

นอกจากการสิ้นอายุใบรับรองคุณภาพตามวรรคหนึ่ง ใบรับรองคุณภาพ จะสิ้นอายุเมื่อมีเหตุดังต่อไปนี้

(๑) ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์เลิกประกอบกิจการ

(๒) ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ตาย เลิกคณะบุคคล หรือสิ้นสภาพการเป็นนิติบุคคล

(๓) สำนักงานเพิกถอนใบรับรองคุณภาพ

ข้อ ๑๒ ภายหลังการออกใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้า หรือใบรับรองคุณภาพขั้นสูงตามข้อ ๑๐ เมื่อสำนักงานหรือคณะทำงานตรวจประเมินได้รับการร้องเรียนหรือมีเหตุสงสัยว่า มีการปฏิบัติไม่เป็นไปตามมาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้สำนักงานหรือคณะทำงานตรวจประเมินมีอำนาจเรียกให้ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์จัดส่งเอกสารหรือหลักฐานตามที่สำนักงานหรือคณะทำงานตรวจประเมินกำหนดเพื่อตรวจสอบรวมถึงมีอำนาจเข้าไปตรวจสอบข้อมูลขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ และหากปรากฏว่าการให้บริการของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ไม่เป็นไปตามมาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้สำนักงานเพิกถอนใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้า หรือใบรับรองคุณภาพขั้นสูง แล้วแต่กรณี

ในระหว่างใบรับรองคุณภาพยังไม่สิ้นอายุ ในกรณีที่ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์มีการเปลี่ยนแปลงขั้นตอนหรือกระบวนการ บุคลากร หรือเทคโนโลยีที่ใช้ในกระบวนการของบริการที่ได้รับการรับรองคุณภาพแล้ว ให้ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าวมีหน้าที่แจ้งให้สำนักงานทราบภายในสามสิบวันนับแต่วันที่มีการเปลี่ยนแปลง และให้สำนักงานแจ้งให้คณะทำงานตรวจประเมินเพื่อดำเนินการตรวจสอบว่าการให้บริการของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ยังคงเป็นไปตามมาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรองหรือไม่ หากปรากฏว่าผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ไม่ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดในประกาศนี้ สำหรับประเภทบริการที่ขอรับการรับรอง ให้สำนักงานเพิกถอนใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้า หรือใบรับรองคุณภาพขั้นสูง แล้วแต่กรณี และลบรายชื่อผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าวออกจากรายชื่อที่ได้ประกาศตามข้อ ๑๐ วรรคสอง

การเปลี่ยนแปลงขั้นตอนหรือกระบวนการ บุคลากร หรือเทคโนโลยีที่ต้องแจ้งตามวรรคสอง ให้รวมถึงกรณีที่ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ได้ควบรวมกิจการหรือรับโอนกิจการจากบุคคลอื่นในส่วนที่เกี่ยวกับบริการที่ขอรับการรับรอง

ข้อ ๑๓ ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับใบรับรองคุณภาพรายใดประสงค์จะต่ออายุใบรับรองคุณภาพ ให้ยื่นคำขอต่อสำนักงานไม่น้อยกว่าหนึ่งร้อยยี่สิบวันก่อนใบรับรองคุณภาพสิ้นอายุ โดยให้ดำเนินการตามข้อ ๖ และให้สำนักงานดำเนินการตามข้อ ๘ ทั้งนี้ หากผู้ให้บริการด้านความมั่นคง

ปลอดภัยไซเบอร์ไม่ยื่นขอต่ออายุใบรับรองคุณภาพภายในระยะเวลาที่กำหนดข้างต้น ให้ถือว่าผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ไม่ประสงค์ต่ออายุใบรับรองคุณภาพ

เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินได้รับคำขอรับการรับรองคุณภาพ พร้อมทั้งเอกสารหรือหลักฐานของผู้ยื่นคำขอจากสำนักงานแล้ว ให้ดำเนินการตามข้อ ๙ ทั้งนี้ ในกรณีขอรับการรับรองคุณภาพขั้นก้าวหน้าหรือใบรับรองคุณภาพขั้นสูงตามข้อ ๙ วรรคหนึ่ง (๒) หรือ (๓) คณะทำงานตรวจประเมินอาจตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานของผู้ยื่นคำขอโดยใช้วิธีการสุ่มตรวจก็ได้

ข้อ ๑๔ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

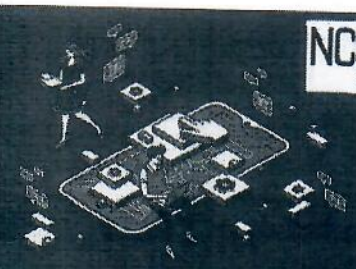
ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจตีความและวินิจฉัยชี้ขาด แล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบ ทั้งนี้ การตีความและคำวินิจฉัยของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)



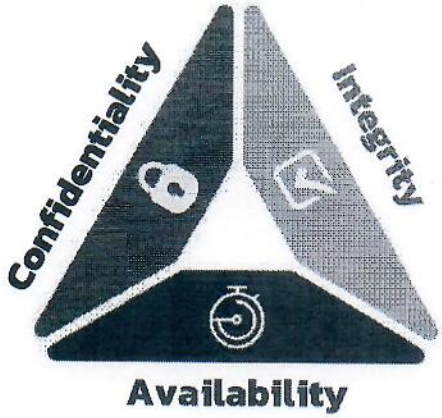
**ประกาศในราชกิจจานุเบกษา 18 มกราคม 2567** | **มีผลใช้บังคับ 18 มกราคม 2568** → มีผลบังคับใช้กับ GOV REG และ CII

## Security Categorization

เพื่อให้ GOV REG และ CII สามารถกำหนดความสำคัญของข้อมูล/ระบบสารสนเทศ นำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม ทำให้ประชาชนได้รับบริการที่มีประสิทธิภาพและมีความมั่นคงปลอดภัยทางไซเบอร์อันจะส่งผลให้ธุรกิจหรือบริการภายในประเทศได้รับความเชื่อมั่นมากยิ่งขึ้น อย่างคุ้มค่า

## 1 STEP

**กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์** ให้แก่ข้อมูลหรือระบบสารสนเทศ **โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objectives)** ดังนี้




## 2 STEP

**ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้น โดยพิจารณาผลกระทบในแต่ละด้าน** ดังนี้


## 3 STEP

**จัดระดับผลกระทบที่อาจเกิดขึ้นเป็น 3 ระดับ**

| ระดับต่ำ | ระดับกลาง | ระดับสูง |
|---|---|---|

| ระดับผลกระทบ | การรักษาความลับ (Confidentiality) | การรักษาความถูกต้องครบถ้วน (Integrity) | สภาพพร้อมใช้งาน (Availability) |
|---|---|---|---|
| ระดับต่ำ | **ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับ** | **การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด** | **กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด** |
| ระดับกลาง | **ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับมาก** | **การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรง** | **กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรง** |
| ระดับสูง | **ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับที่สุด** | **การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก** | **กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก** |

**หมายเหตุ**

- **กรณีระบบสารสนเทศมีข้อมูลหลายประเภทข้อมูล** ให้กำหนดคุณลักษณะ โดย**ใช้ผลกระทบของข้อมูลที่มีระดับมากที่สุด**
- **หน่วยงานต้องพิจารณาทบทวนการกำหนดคุณลักษณะทุก 3 ปีเป็นอย่างน้อย** หรือทบทวนเมื่อข้อมูล ระบบสารสนเทศ หรือหน้าที่ของหน่วยงานเปลี่ยนแปลงอย่างมีนัยสำคัญ

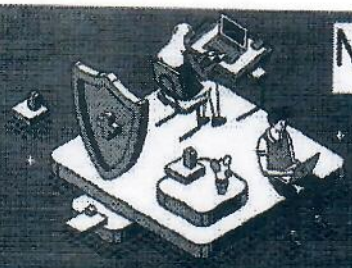
**จัดทำโดย :** สำนักกฎหมาย สกมช.

ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะฯ


**ติดต่อสอบถามเพิ่มเติม**

โทร : 0 2502 7826
อีเมล : cii@ncsa.or.th

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
**เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566**
(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)



NCSA สกมช.

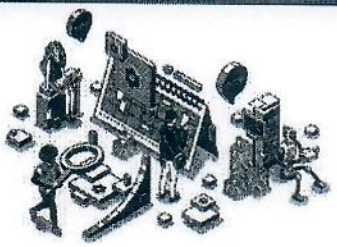
**ประกาศในราชกิจจานุเบกษา**
**18 มกราคม 2567**

**มีผลใช้บังคับ**
**18 มกราคม 2568**

**มีผลบังคับใช้กับ**
GOV REG และ CII

**Security Baselines**

เพื่อให้ GOV REG และ CII สามารถกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำได้อย่างเหมาะสมคุ้มค่า
ลดมาตรการควบคุมและค่าใช้จ่ายที่เกินความจำเป็น ช่วยประหยัดงบประมาณแผ่นดินของประเทศ



ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์
และได้ระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศแล้ว
**ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ**
สำหรับข้อมูลหรือระบบสารสนเทศในแต่ละระดับ ดังนี้

**ผลกระทบระดับต่ำ** = SET A

**ผลกระทบระดับกลาง** = SET A + SET B

**ผลกระทบระดับสูง** = SET A + SET B + SET C

## ประมวลแนวทางปฏิบัติ

## กรอบมาตรฐานด้าน Cybersecurity

### SET A

- **การประเมินความเสี่ยง** ด้าน Cybersecurity
- **แผนการรับมือ** ภัยคุกคามทางไซเบอร์

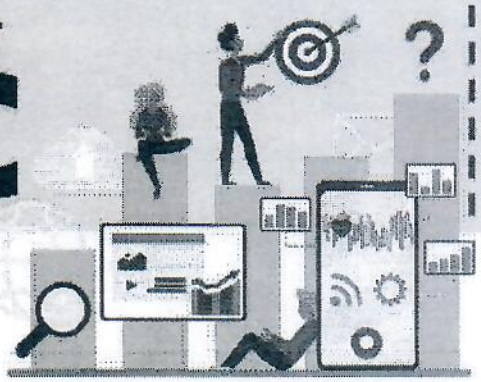
- **การระบุความเสี่ยง** (Identify)
  - การจัดการทรัพย์สิน
  - การประเมินความเสี่ยงและกลยุทธ์
- **มาตรการตรวจสอบและเฝ้าระวัง** (Detect)
  - การตรวจสอบและเฝ้าระวัง
- **มาตรการป้องกัน** (Protect)
  - การควบคุมการเข้าถึง
  - การทำให้ระบบมีความแข็งแกร่ง
  - การสร้างความตระหนักรู้
- **มาตรการเผชิญเหตุ** (Respond)
  - แผนการรับมือ
  - แผนการสื่อสารในภาวะวิกฤต
  - การฝึกซ้อม

### SET B

- **แผนการตรวจสอบ** ด้าน Cybersecurity

- **มาตรการป้องกัน** (Protect)
  - การเชื่อมต่อระยะไกล
  - สื่อเก็บข้อมูลแบบถอดได้

### SET C



- **การระบุความเสี่ยง** (Identify)
  - การประเมินช่องโหว่และการทดสอบเจาะระบบ
  - การจัดการผู้ให้บริการภายนอก
- **มาตรการป้องกัน** (Protect)
  - การแบ่งปันข้อมูล
- **มาตรการรักษาและฟื้นฟูความเสียหาย** (Recover)
  - การรักษาและฟื้นฟูความเสียหายที่เกิด


**ติดต่อสอบถามเพิ่มเติม**
โทร : 0 2502 7826
อีเมล : cii@ncsa.or.th



**จัดทำโดย :** สำนักกฎหมาย สกมช.


ประกาศ คมช. เรื่อง มาตรฐานขั้นต่ำฯ

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

**ประกาศในราชกิจจานุเบกษา** 18 มกราคม 2567 | **มีผลใช้บังคับ** 19 มกราคม 2567

บุคคลธรรมดา คณะบุคคล หรือนิติบุคคล ที่เป็นผู้ให้บริการ Cyber Security

เพื่อส่งเสริมธุรกิจและการให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้มีคุณภาพและได้รับการยอมรับจากผู้ใช้บริการทั้งในและต่างประเทศ ส่งผลให้ประเทศมีอำนาจในการแข่งขันมากยิ่งขึ้น รวมทั้งผู้ใช้บริการสามารถเลือกผู้ให้บริการที่เหมาะสมกับตนและได้มาตรฐาน


เลือกขั้นที่ประสงค์ขอรับรองคุณภาพ

## การรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์มี 3 ระดับ

ขั้นต้น | ขั้นก้าวหน้า | ขั้นสูง

### ประเภทผู้ได้รับการรับรอง

บุคคลธรรมดา | คณะบุคคล | นิติบุคคล

นิติบุคคล

### เอกสาร/หลักฐานในการยื่นคำขอรับรอง

**เอกสารแสดงความเชี่ยวชาญ** ของบุคลากรของผู้ยื่นคำขอ

**เอกสารแสดงประสบการณ์การทำงาน** ในประเภทบริการที่ขอรับการรับรอง

**เอกสารการรับรองตนเอง** ว่าปฏิบัติตามมาตรฐานที่กำหนดในประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ (เฉพาะผู้ยื่นคำขอเป็นนิติบุคคล)

### การตรวจรับรองคุณภาพ

- ✓ ตรวจเอกสาร/หลักฐาน

- ✓ ตรวจเอกสาร/หลักฐาน
- ✓ สัมภาษณ์

- ✓ ตรวจเอกสาร/หลักฐาน
- ✓ ตรวจมาตรฐานสากล
- ✓ สัมภาษณ์
- ✓ ตรวจ ณ สถานประกอบการหรือสถานที่ให้บริการ

### อายุใบรับรอง

3 ปี

2 ปี

## ขั้นตอนการดำเนินการ


ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมฯ

ติดต่อสอบถามเพิ่มเติม

โทร : 0 2502 7825

อีเมล : Research@ncsa.or.th

จัดทำโดย : สำนักกฎหมาย สกมช.