ประกาศคณะกรรมการการมาตรฐานแห่งชาติ

เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดขอบข่าย และการสุ่มตัวอย่างเพื่อการรับรองหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดขอบข่ายและการสุ่มตัวอย่างเพื่อการรับรองหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ เพื่อให้หน่วยรับรองมีแนวทางในการดำเนินการได้อย่างมีประสิทธิภาพ และสร้างความเชื่อมั่นว่าหน่วยรับรองที่ได้รับการรับรองจะดำเนินการได้ตามวัตถุประสงค์และข้อกำหนดของมาตรฐานที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๒๘ วรรคสอง แห่งพระราชบัญญัติการมาตรฐานแห่งชาติ พ.ศ. ๒๕๕๑ ประกอบมติคณะกรรมการการมาตรฐานแห่งชาติ ในการประชุมครั้งที่ ๑๐-๑/๒๕๖๔ เมื่อวันที่ ๑๕ กุมภาพันธ์ ๒๕๖๔ คณะกรรมการการมาตรฐานแห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการมาตรฐานแห่งชาติ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดขอบข่าย และการสุ่มตัวอย่างเพื่อการรับรองหน่วยรับรองระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศคณะกรรมการการมาตรฐานแห่งชาติ ฉบับที่ ๓ (พ.ศ. ๒๕๕๙) เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดสาขาและขอบข่าย และการสุ่มตัวอย่างเพื่อการรับรองระบบงานหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ ลงวันที่ ๗ กรกฎาคม พ.ศ. ๒๕๕๙

ข้อ ๔ การกำหนดขอบข่ายและการสุ่มตัวอย่างเพื่อการรับรองหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ ให้เป็นไปตามรายละเอียดที่แนบท้ายประกาศนี้

ข้อ ๕ บรรดาคำขอที่อยู่ระหว่างดำเนินการ ให้ดำเนินการต่อไปจนกว่าจะแล้วเสร็จ และให้ถือว่าเป็นการดำเนินการตามประกาศนี้

ประกาศ ณ วันที่ ๒๒ เมษายน พ.ศ. ๒๕๖๔
วิษณุ เครืองาม
รองนายกรัฐมนตรี
ประธานกรรมการการมาตรฐานแห่งชาติ

หลักเกณฑ์ วิธีการ และเงื่อนไขสำหรับการกำหนดขอบข่าย และการสุ่มตัวอย่าง เพื่อการรับรองหน่วยรับรองระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ แนบท้ายประกาศคณะกรรมการการมาตรฐานแห่งชาติ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดขอบข่าย และการสุ่มตัวอย่างเพื่อการรับรองหน่วยรับรองระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ 22 เมษายน 2564

1. ขอบข่าย

เอกสารนี้กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการกำหนดขอบข่าย และการสุ่มตัวอย่างเพื่อการรับรองหน่วยรับรองระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เอกสารอ้างอิง นิยาม เงื่อนไขสำหรับผู้ยื่นคำขอและผู้ได้รับใบรับรอง และการตรวจประเมิน การกำหนดขอบข่าย และการสุ่มตัวอย่างโดยสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

2. เอกสารอ้างอิง

2.1 ประกาศคณะกรรมการการมาตรฐานแห่งชาติ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการรับรองหน่วยรับรอง

2.2 ประกาศคณะกรรมการรับรองหน่วยรับรองและหน่วยตรวจ ฉบับที่ 1 (พ.ศ. 2555) เรื่อง การกำหนดสาขาการรับรองหน่วยรับรองเพิ่มเติม

2.3 มอก. 2000 การจัดประเภทอุตสาหกรรมตามกิจกรรมทางเศรษฐกิจทุกประเภทตามมาตรฐานสากล

2.4 ISO/IEC 27006 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

3. นิยาม

ความหมายของคำที่ใช้ในเอกสารนี้ให้เป็นไปตามนิยามที่กำหนดไว้ในหลักเกณฑ์ วิธีการ และเงื่อนไขการรับรองหน่วยรับรอง

4. เงื่อนไขสำหรับผู้ยื่นคำขอและผู้ได้รับใบรับรอง และการตรวจประเมิน

เงื่อนไขสำหรับผู้ยื่นคำขอและผู้ได้รับใบรับรอง และการตรวจประเมิน ให้เป็นไปตามประกาศคณะกรรมการการมาตรฐานแห่งชาติ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขสำหรับการรับรองหน่วยรับรอง

5. การกำหนดขอบข่าย

การกำหนดขอบข่ายในการรับรองหน่วยรับรองระบบการจัดการความปลอดภัยด้านสารสนเทศ จะอ้างอิงตามการแบ่งประเภทอุตสาหกรรมตามกิจกรรมทางเศรษฐกิจ (หมวด A-Q) ที่ระบุไว้ในมาตรฐานเลขที่ มอก. 2000 รายละเอียดการกำหนดขอบข่าย ดังตารางที่ 1

ตารางที่ 1 การกำหนดขอบข่าย

หมวด	กิจกรรมทางเศรษฐกิจ
A	เกษตรกรรม การล่าสัตว์ และการป่าไม้
B	การประมง
C	การทำเหมืองแร่และเหมืองหิน
D	การผลิต
E	การจ่ายไฟฟ้า ก๊าซ และน้ำ
F	การก่อสร้าง
G	การขายส่ง การขายปลีก การซ่อมแซมยานยนต์ รถจักรยานยนต์ ของใช้ส่วนบุคคล และของใช้ภายในบ้าน
H	โรงแรมและภัตตาคาร
I	การขนส่ง การเก็บรักษา และการคมนาคม
J	การเป็นตัวกลางทางการเงิน
K	การค้าอสังหาริมทรัพย์ การให้เช่า และกิจกรรมทางธุรกิจ
L	การบริหารราชการและการป้องกันประเทศ การประกันสังคมแบบบังคับ
M	การศึกษา
N	การบริการเกี่ยวกับสุขภาพและงานสังคมสงเคราะห์
O	การบริการชุมชน สังคม และการบริการส่วนบุคคลอื่น ๆ
P	บ้านส่วนบุคคลพร้อมลูกจ้าง

หมายเหตุ มอก. 2000 แบ่งประเภทอุตสาหกรรมตามกิจกรรมทางเศรษฐกิจของผลิตภัณฑ์และการบริการ โดยแบ่งเป็นหมวด A –Q ทั้งนี้ หมวด Q กิจกรรมองค์การระหว่างประเทศและองค์การต่างประเทศอื่น ๆ และสมาชิก เป็นขอบข่ายที่ไม่ให้การรับรอง

6. การสุ่มตัวอย่าง

6.1 สำนักงานจะพิจารณาตรวจประเมินความสามารถผู้ประเมินของหน่วยรับรองขณะตรวจประเมินผู้ประกอบกิจการ โดยตรวจครบทุกข้อกำหนด (หน่วยรับรองประเมินเพื่อให้การรับรองครั้งแรก หรือประเมินใหม่) เป็นลำดับแรก หากหน่วยรับรองไม่สามารถจัดสรรการประเมินครบทุกข้อกำหนดตามข้างต้นได้ สำนักงานอาจพิจารณาการตรวจติดตามผล (Surveillance) จำนวน 2 ครั้ง และการตรวจติดตามผลในแต่ละครั้งต้องครอบคลุมกระบวนการหลักของผู้ประกอบกิจการ

6.3 สำนักงานสามารถเลือกขอบข่ายและผู้ประเมินที่จะตรวจประเมินความสามารถได้ตามความเหมาะสม

6.3 การสุ่มตัวอย่างเพื่อตรวจประเมินความสามารถผู้ประเมินของหน่วยรับรองขณะประเมินผู้ประกอบกิจการสำหรับการรับรองครั้งแรก การขอขยายขอบข่าย การตรวจติดตามผลและการต่ออายุ ให้สุ่มตัวอย่างอย่างน้อย 1 ตัวอย่าง

6.4 การพิจารณาเลือกสุ่มตัวอย่างเพื่อตรวจประเมินความสามารถผู้ประเมินของหน่วยรับรองขณะประเมิน ผู้ประกอบกิจการจะพิจารณาเลือกตัวอย่างที่มีนัยสำคัญต่อผลกระทบ และ/หรือความเสี่ยงต่อความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นตัวแทนขอบข่ายที่ขอรับการรับรองระบบงาน