R-NCSA-CAB-03

(ร่าง) ข้อกำหนดทั่วไปในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรอง

General Requirements for Quality Control and maintaining the competence of Conformity Assessment Body

ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ข้อกำหนดทั่วไปในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรอง
พ.ศ. ๒๕๖๙

เพื่อเป็นการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไข ทั่วไปที่ต้องการรวมทั้งการกำหนดหน้าที่และความรับผิดชอบที่จำเป็น เพื่อให้ใช้เป็นแนวทางปฏิบัติในการตรวจสอบคุณสมบัติของหน่วยงานที่ประสงค์จะขึ้นทะเบียนเป็นหน่วยตรวจสอบรับรอง (ผู้ตรวจสอบคุณภาพ) กับ สกมช. ให้มีความชัดเจน ถูกต้องเชื่อถือได้ในทางเทคนิควิชาการ มีความเสี่ยงในระดับที่ยอมรับได้ มีหลักประกันความรับผิดที่เหมาะสม เป็นกลาง มีเอกภาพและเป็นไปตามแนวทางปฏิบัติของอนุกรมมาตรฐาน มอก. 17000 (ISO/IEC 17000 series) ซึ่งเป็นที่ยอมรับในระดับนานาชาติ

อาศัยอำนาจตามความในข้อ ๙ (๔) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังนี้ ข้อกำหนดทั่วไปในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรอง R-NCSA-CAB-03 ไว้ดังมีรายละเอียดตามเอกสารแนบท้ายประกาศนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ข้อกำหนดทั่วไปในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรอง พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ข้อกำหนดทั่วไปในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรอง ให้เป็นไปตามแนบท้ายประกาศนี้

ข้อ ๔ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรักษาการตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้มิได้กำหนดเรื่องใดไว้ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยดังกล่าวให้เป็นที่สุด

ประกาศ ณ วันที่ สิงหาคม พ.ศ. ๒๕๖๙

พลอากาศตรี
(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(ร่าง) ข้อกำหนดทั่วไป ในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรอง

General Requirements for Quality control
and maintaining the competence of
Conformity Assessment Body

R-NCSA-CAB-03

ประวัติการปรับปรุงเอกสาร

ครั้งที่	วันที่ประกาศใช้	รายการปรับปรุง
๑	สิงหาคม ๒๕๖๙	จัดทำเอกสารฉบับแรก

ข้อกำหนดทั่วไป ในการควบคุมคุณภาพ และการรักษาความสามารถ ของหน่วยตรวจสอบรับรอง

๑. วัตถุประสงค์

ข้อกำหนดทั่วไปในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรองนี้ กำหนดขึ้นโดยมีวัตถุประสงค์ ดังนี้

(๑) เพื่อให้วิธีการ รูปแบบ และข้อกำหนดที่ใช้เป็นหลักปฏิบัติในการตรวจประเมินระบบการบริหารจัดการคุณภาพของหน่วยตรวจสอบรับรอง มีความถูกต้อง ชัดเจน เป็นที่ยอมรับ และสอดคล้องกับมาตรฐานระดับประเทศ หรือระดับสากล

(๒) เพื่อใช้เป็นหลักเกณฑ์ข้อกำหนดในการตรวจประเมินระบบบริหารจัดการคุณภาพ ของผู้ยื่นคำขอหรือผู้ได้รับการรับรอง

๒. ขอบเขต

ข้อกำหนดทั่วไปในการควบคุมคุณภาพ และการรักษาความสามารถ ของหน่วยตรวจสอบรับรองนี้ เป็นการกำหนดหลักเกณฑ์ทั่วไปในการตรวจประเมินระบบบริหารจัดการคุณภาพ เพื่อยืนยันความสามารถของหน่วยตรวจสอบรับรอง โดยครอบคลุม การจัดการองค์กร การรักษาความเป็นกลาง การรักษาความลับ สถานะทางการเงิน การทำข้อตกลงระหว่างผู้ใช้บริการ ขั้นตอนกระบวนการในการให้บริการ การควบคุมและเฝ้าระวังผลการตรวจสอบรับรอง ทรัพยากรที่ใช้ในการตรวจประเมิน การควบคุมบันทึก การควบคุมเอกสาร การทบทวนของฝ่ายบริหาร การตรวจประเมินคุณภาพภายใน การวิเคราะห์ข้อมูล การปรับปรุงอย่างต่อเนื่อง การปฏิบัติการแก้ไข และการดำเนินการป้องกัน

๓. เอกสารอ้างอิง

๓.๑ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖

๓.๒ มอก. 17065	การตรวจสอบและรับรอง - ข้อกำหนดสำหรับหน่วยรับรองผลิตภัณฑ์ กระบวนการ และ การบริการ
๓.๒ มอก. 17020	การตรวจสอบและรับรอง - ข้อกำหนดสำหรับหน่วยตรวจ
๓.๓ มอก. 17025	ข้อกำหนดทั่วไปว่าด้วยความสามารถของห้องปฏิบัติการทดสอบ และห้องปฏิบัติการสอบเทียบ
๓.๔ มอก. 17024	การตรวจสอบและรับรอง - ข้อกำหนดทั่วไปสำหรับหน่วยรับรองบุคลากร
๓.๕ มตช. 17021	การตรวจสอบและรับรอง – ข้อกำหนดสำหรับหน่วยตรวจประเมินและให้การรับรองระบบการจัดการ - ส่วนที่ 2 ข้อกำหนดความสามารถสำหรับการตรวจประเมินและการรับรองระบบการจัดการสิ่งแวดล้อม
๓.๖ ISO/IEC 17067	Conformity assessment – Fundamentals of product certification and guildelines for product certification schemes

หมายเหตุ: เอกสารอ้างอิงให้เป็นไปตามข้อกำหนดของมาตรฐาน **ฉบับล่าสุด**

๔. นิยาม

๔.๑ สำนักงาน หมายถึง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๔.๒ หน่วยตรวจสอบรับรอง หมายถึง บุคคล นิติบุคคล หรือส่วนของนิติบุคคลที่มีหน้าที่ในการวัด วิเคราะห์ ทดสอบ ตรวจ ประเมิน สอบ สอบเทียบ ตรวจสอบ รับรอง หรือที่คล้ายกัน อย่างใดอย่างหนึ่งหรือหลายอย่างรวมกัน

๔.๓ ผู้ยื่นคำขอ หมายถึง หน่วยตรวจสอบรับรองที่ประสงค์จะขอขึ้นทะเบียนกับสำนักงาน

๔.๔ ผู้ได้รับการขึ้นทะเบียน หมายถึง หน่วยตรวจสอบรับรองที่ได้รับการพิจารณาตัดสินให้ขึ้นทะเบียนกับสำนักงาน

๕. ข้อกำหนดกิจกรรมในการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรอง

๕.๑ ผู้ยื่นคำขอ และผู้ที่ได้รับการขึ้นทะเบียน ควรจัดให้มีระบบการควบคุมคุณภาพ และการรักษาความสามารถของหน่วยตรวจสอบรับรองอย่างน้อยตามกิจกรรมที่กำหนดต่อไปนี้

ลำดับ	กิจกรรม	หน่วยตรวจสอบรับรอง				
		ห้องทดสอบ/สอบเทียบ	หน่วยตรวจ	หน่วยรับรองผลิตภัณฑ์	หน่วยรับรองระบบการบริหารจัดการ	หน่วยรับรองบุคคล
๑	การจัดการองค์กร	Y	Y	Y	Y	Y
๒	การรักษาความเป็นกลาง	*	Y	Y	Y	Y
๓	การรักษาความลับ	Y	Y	Y	Y	Y
๔	สถานะทางการเงิน	Y	Y	Y	Y	Y
๕	การทำข้อตกลงระหว่างผู้ใช้บริการ	Y	Y	Y	Y	Y
๖	ขั้นตอนกระบวนการในการให้บริการ	Y	Y	Y	Y	Y
	- การตรวจประเมิน (Audit)	Y	Y	Y	Y	
	- การประเมินผลิตภัณฑ์	Y		Y		
	- การทดสอบ / สอบ	Y				
	- การตรวจติดตาม			Y	Y	Y
	- การออกเอกสารผลการตรวจสอบรับรอง	Y	Y	Y	Y	Y
๗	การควบคุมและเฝ้าระวังผลการตรวจสอบรับรอง	Y	Y	Y	Y	Y
๘	ทรัพยากรที่ใช้ในการตรวจประเมิน	Y	Y	Y	Y	Y
	- บุคลากร ผู้ประเมิน ผู้เชี่ยวชาญ	Y	Y	Y	Y	Y
	- การจ้างเหมาช่วง (ถ้ามี)	Y	Y	Y	Y	Y
	- เครื่องมือทดสอบ	Y	Y	Y	Y	Y
๙	การควบคุมบันทึก	Y	Y	Y	Y	Y
๑๐	การควบคุมเอกสาร	Y	Y	Y	Y	Y
๑๑	การทบทวนของฝ่ายบริหาร	Y	Y	Y	Y	Y
๑๒	ทรัพยากรบุคคล	Y	Y	Y	Y	Y
๑๓	การจัดซื้อ	Y				

ลำดับ	กิจกรรม	หน่วยตรวจสอบรับรอง				
		ห้องทดสอบ/ สอบเทียบ	หน่วย ตรวจ	หน่วยรับรอง ผลิตภัณฑ์	หน่วยรับรอง ระบบการ บริหารจัดการ	หน่วยรับรอง บุคคล
๑๔	การตรวจประเมินภายใน	Y	Y	Y	Y	Y
๑๕	การเฝ้าระวัง การวัดและวิเคราะห์ข้อมูล	Y	Y	Y	Y	Y
๑๖	การปรับปรุงอย่างต่อเนื่อง	Y	Y	Y	Y	Y
๑๗	การปฏิบัติการแก้ไข	Y	Y	Y	Y	Y
๑๘	การดำเนินการป้องกัน	Y	Y	Y	Y	Y

หมายเหตุ * การรักษาความเป็นกลางของห้องปฏิบัติการทดสอบ /ห้องปฏิบัติงานสอบเทียบ ตามข้อกำหนด มอก. 17025 เป็นข้อกำหนดที่ต้องการสำหรับนิติบุคคลที่ 3 (3rd party) และเป็นทางเลือกสำหรับนิติบุคคลที่ 1 (1st party) และ นิติบุคคลที่ 2 (2nd party)

๕.๒ ผู้ยื่นคำขอ และผู้ที่ได้รับการขึ้นทะเบียน ต้องมั่นใจว่ามีการเฝ้าระวังและติดตามรายงานที่เกี่ยวกับช่องโหว่ หรือความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ รวมถึงจัดการให้มีการปรับปรุงความรู้ของบุคลากร และเครื่องมือต่างๆ ที่ใช้ในการให้บริการให้ทันสมัยและเหมาะสมกับสภาพการณ์