R-NCSA-03

(ร่าง) ข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์

General Requirements for Product Quality Control

ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ข้อกำหนดทั่วไปในการควบคุมคุณภาพผลิตภัณฑ์
พ.ศ. ๒๕๖๙

เพื่อเป็นการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไข ทั่วไปที่ต้องการรวมทั้งการกำหนดหน้าที่และความรับผิดชอบที่จำเป็น เพื่อให้ใช้เป็นแนวทางปฏิบัติในการตรวจประเมินความสามารถในการควบคุมคุณภาพผลิตภัณฑ์ของหน่วยงานที่ประสงค์จะขอรับการรับรองคุณภาพผลิตภัณฑ์กับ สกมช. ให้มีความชัดเจน ถูกต้องเชื่อถือได้ในทางเทคนิควิชาการ และเป็นไปตามแนวทางปฏิบัติของมาตรฐานที่เกี่ยวข้อง

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

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ข้อกำหนดทั่วไปในการควบคุมคุณภาพผลิตภัณฑ์ พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ข้อกำหนดทั่วไปในการควบคุมคุณภาพผลิตภัณฑ์ 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 ในการควบคุมคุณภาพผลิตภัณฑ์

General Requirements for
Product Quality control
R-NCSA-03

ประวัติการปรับปรุงเอกสาร

ครั้งที่	วันที่ประกาศใช้	รายการปรับปรุง
๑	สิงหาคม ๒๕๖๙	จัดทำเอกสารฉบับแรก

ข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์

General Requirements for Product Quality control

๑. วัตถุประสงค์

ข้อกำหนดทั่วไปในการควบคุมคุณภาพนี้ กำหนดขึ้นโดยมีวัตถุประสงค์ ดังนี้

(๑) เพื่อให้วิธีการ รูปแบบ และข้อกำหนด ที่ใช้เป็นหลักปฏิบัติในการตรวจประเมินระบบการควบคุมคุณภาพผลิตภัณฑ์ บริการ กระบวนการ ด้านความมั่นคงปลอดภัยไซเบอร์ มีความถูกต้อง ชัดเจน เป็นที่ยอมรับและสอดคล้องกับมาตรฐานระดับประเทศ หรือระดับสากล

(๒) เพื่อใช้เป็นหลักเกณฑ์ข้อกำหนดในการตรวจประเมินระบบการควบคุมคุณภาพผลิตภัณฑ์ บริการ กระบวนการ ด้านความมั่นคงปลอดภัยไซเบอร์ ของผู้ยื่นคำขอหรือผู้ได้รับการรับรอง

๒. ขอบข่าย

ข้อกำหนดทั่วไปในการควบคุมคุณภาพนี้ เป็นการกำหนดหลักเกณฑ์ทั่วไปในการควบคุมคุณภาพลิตภัณฑ์ บริการ กระบวนการ ด้านความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมตั้งแต่ นโยบาย การชี้บ่งและการประเมินความเสี่ยง การวางแผน การควบคุมในระหว่างกระบวนการออกแบบและพัฒนา การควบคุมการให้บริการ การควบคุมทรัพย์สิน การควบคุมการเฝ้าระวังภัยคุกคามทางไซเบอร์ การควบคุมบันทึก การควบคุมเอกสาร การทบทวนของฝ่ายบริหาร ทรัพยากรบุคคล การจัดซื้อ การตรวจประเมินภายใน การวิเคราะห์ข้อมูล การปรับปรุงอย่างต่อเนื่อง การปฏิบัติการแก้ไข และการดำเนินการเชิงป้องกัน

๓. เอกสารอ้างอิง

๓.๑ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖

๓.๒ มอก. 9001 ระบบการบริหารงานคุณภาพ - ข้อกำหนด

๓.๓ มตช. 27001 ความมั่นคงปลอดภัยด้านสารสนเทศ ความมั่นคงปลอดภัยทางไซเบอร์ และการปกป้องความ เป็นส่วนตัว - ระบบการจัดการความมั่นคงปลอดภัย ด้านสารสนเทศ - ข้อกำหนด

๓.๔ 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 ผลิตภัณฑ์ หมายถึง ผลิตภัณฑ์ หรือกระบวนการ หรือบริการ ด้านความมั่นคงปลอดภัยไซเบอร์ หรือ ผลิตภัณฑ์ หรือกระบวนการ หรือบริการที่มีผลต่อความมั่นคงปลอดภัยไซเบอร์

หมายเหตุ ผลิตภัณฑ์ในที่นี้ตั้งใจให้หมายรวมถึง ผลิตภัณฑ์ กระบวนการ และบริการตามขอบเขต และนิยามของมาตรฐาน มอก. 17065

๔.๓ ผู้ยื่นคำขอ หมายถึง บุคคลธรรมดา คณะบุคคล หรือนิติบุคคลที่ประสงค์จะขอรับการรับรองกับสำนักงาน

หมายเหตุ: สำหรับบุคคลธรรมดา หากมีความสามารถดำเนินการ อาจตีความว่าเป็นนิติบุคคลได้ ....

๔.๔ ผู้ได้รับการรับรอง หมายถึง ผู้ยื่นคำขอที่ผ่านการตรวจประเมินและได้รับการรับรอง จากสำนักงาน หรือจากหน่วยตรวจสอบรับรองที่สำนักงานให้การยอมรับ

๔.๕ การตรวจประเมิน หมายถึง กิจกรรมการตรวจประเมินเพื่อตรวจสอบความสามารถและคุณสมบัติของผู้ยื่นคำขอ ตามขอบข่ายที่ยื่นความประสงค์ไว้ ด้วยวิธีการและหลักเกณฑ์ตามที่สำนักงานกำหนด

๔.๖ ผู้ตรวจประเมิน หมายถึง บุคคลหรือคณะบุคคล ที่ได้รับการมอบหมายจากสำนักงาน ให้ทำหน้าที่ในการตรวจประเมินความสามารถและคุณสมบัติของผู้ยื่นคำขอหรือผู้ได้รับการรับรอง

๕. ข้อกำหนดกิจกรรมในการควบคุมคุณภาพผลิตภัณฑ์

๕.๑ ผู้ยื่นคำขอ ควรจัดให้มีระบบการควบคุมคุณภาพอย่างน้อยตามกิจกรรมที่กำหนดต่อไปนี้

กิจกรรม[1]		รูปแบบการรับรอง (Certification Scheme)								
		1a	1b	2	3	4	5	6	7	N[๒]
๑	มีระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์			Y	Y	Y	Y	Y	Y	*
๒	การชี้บ่งและประเมินความเสี่ยง			Y	Y	Y	Y	Y	Y	*
๓	การวางแผนการรับมือภัยคุกคาม			Y	Y	Y	Y	Y	Y	*
๔	การควบคุมวัตถุดิบ/ทรัพยากรที่ใช้ในกระบวนการผลิต			Y	Y	Y	Y			*
๕	การตรวจสอบเฝ้าระวังเครื่องมือ/อุปกรณ์ที่ใช้			Y	Y	Y	Y	Y	Y	*
๖	การออกแบบและพัฒนา			Y	Y	Y	Y	Y	Y	*
๗	การควบคุมกระบวนการ			Y	Y	Y	Y	Y		*
๘	การควบคุมผลิตภัณฑ์/บริการที่ไม่เป็นไปตามข้อกำหนด			Y	Y	Y	Y	Y		*
๙	การดูแลรักษาผลิตภัณฑ์			Y	Y	Y	Y			*
๑๐	การควบคุมระดับคุณภาพในการให้บริการ							Y		*
๑๑	การควบคุมทรัพย์สิน			Y	Y	Y	Y	Y	Y	*
๑๒	การควบคุมการเฝ้าระวังภัยคุกคามทางไซเบอร์			Y	Y	Y	Y	Y	Y	*
๑๓	การควบคุมบันทึก			Y	Y	Y	Y	Y	Y	*
๑๔	การควบคุมเอกสาร			Y	Y	Y	Y	Y	Y	*
๑๕	การทบทวนของฝ่ายบริหาร			Y	Y	Y	Y	Y	Y	*
๑๖	ทรัพยากรบุคคล			Y	Y	Y	Y	Y	Y	*
๑๗	การจัดซื้อ / การจัดหาผู้ให้บริการภายนอก			Y	Y	Y	Y	Y	Y	*
๑๘	การตรวจประเมินภายใน			Y	Y	Y	Y	Y	Y	*
๑๙	การเฝ้าระวัง การวัดและวิเคราะห์ข้อมูล			Y	Y	Y	Y	Y	Y	*
๒๐	การปรับปรุงอย่างต่อเนื่อง			Y	Y	Y	Y	Y	Y	*

กิจกรรม[1]		รูปแบบการรับรอง (Certification Scheme)								
		1a	1b	2	3	4	5	6	7	N[๒]
๒๑	การปฏิบัติการแก้ไข			Y	Y	Y	Y	Y	Y	*
๒๒	การดำเนินการเชิงป้องกัน			Y	Y	Y	Y	Y	Y	*

หมายเหตุ (๑) ตัวอย่างการดำเนินการ/มาตรการที่ใช้ได้ในการควบคุมคุณภาพผลิตภัณฑ์ แสดงไว้ในภาคผนวก ก

(๒) รูปแบบการรับรอง N สำหรับผลิตภัณฑ์ที่มีลักษณะเฉพาะ ที่ต้องกำหนดรูปแบบการรับรองนอกเหนือจากรูปแบบ 1a - 7 โดยสำนักงานจะพิจารณากำหนดรูปแบบ และระบุกิจกรรมที่ตรวจประเมินที่เหมาะสม รายละเอียดให้เป็นไปตามข้อกำหนดเฉพาะในการรับรองคุณภาพผลิตภัณฑ์นั้น ๆ

๕.๒ ผู้ยื่นคำขอ และผู้ที่ได้รับการรับรอง ต้องมั่นใจว่ามีการเฝ้าระวังและติดตามรายงานที่เกี่ยวกับช่องโหว่หรือความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ รวมถึงจัดการให้มีการปรับปรุงความรู้ของบุคลากรและเครื่องมือต่าง ๆ ที่ใช้ในการให้บริการให้ทันสมัยและเหมาะสมกับสภาพการณ์

ภาคผนวก ก.

ตัวอย่างการดำเนินการตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์

ผู้ยื่นคำขอหรือผู้ได้รับการรับรอง ควรจัดให้มีระบบการควบคุมคุณภาพผลิตภัณฑ์ ให้เป็นไปตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์ ดังต่อไปนี้

๑.	**มีระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๑.๑	การกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ เป็นลายลักษณ์อักษร
๑.๒	มีทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์
๑.๓	มีการสื่อสารนโยบาย กระบวนการ มาตรการด้านความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิผล
๒.	**การชี้บ่งและประเมินความเสี่ยง**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๒.๑	จัดทำขั้นตอน วิธีการในการบริหารความเสี่ยงดานการรักษาความมั่นคงปลอดภัยไซเบอร โดยต้องประกอบด้วยรายละเอียดอยางนอย ดังตอไปนี้ ก. การประเมินความเสี่ยง (Risk Assessment) ข. การจัดการความเสี่ยง (Risk Treatment) ค. การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ง. การรายงานความเสี่ยง (Risk Reporting)
๒.๒	จัดเก็บบันทึกผลการประเมิน
๓.	**การวางแผนการรับมือภัยคุกคาม**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๓.๑	จัดทำแผนการรับมือภัยคุกคามทางไซเบอร (Cybersecurity Incident Response Plan)
๓.๒	สื่อสารแผนการรับมือภัยคุกคามทางไซเบอรไปยังบุคลากรที่เกี่ยวของทั้งหมด อยางมีประสิทธิผล
๓.๓	ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง ให้ทันต่อเหตุการณ์
๓.๔	จัดเก็บบันทึกแผนและผลการทบทวน
๔.	**การควบคุมวัตถุดิบ/ทรัพยากรที่ใช้ในกระบวนการผลิต (สำหรับผลิตภัณฑ์ อุปกรณ์ไอที)**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๔.๑	แสดงรายการวัตถุดิบ ส่วนประกอบทั้งหมดที่ใช้ กำหนดรายละเอียดวิธีการตรวจรับ เกณฑ์การยอมรับ ข้อกำหนดมาตรฐานที่ใช้อ้างอิง เพื่อให้มั่นใจว่าวัตถุดิบส่วนประกอบ มีคุณภาพ และมีความมั่นคงปลอดภัย
๔.๒	จัดเก็บบันทึกผลการตรวจสอบ ทดสอบวัตถุดิบ ส่วนประกอบ *กรณีผู้ยื่นคำขอเป็นบุคคลธรรมดา อาจใช้วิธีการควบคุมอื่นๆ ที่เหมาะสม เช่น การตรวจสอบความปลอดภัยของ Library หรือ Open Source ที่นำมาใช้
๕	**การตรวจสอบเฝ้าระวังเครื่องมือ/อุปกรณ์ที่ใช้**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๕.๑	จัดทำทะเบียนรายการเครื่องมือ อุปกรณ์ รวมถึงซอฟต์แวร์ แพลตฟอร์ม ระบบต่าง ๆ ที่ใช้ในการผลิต การออกแบบและพัฒนา
๕.๒	กำหนดวิธีการตรวจสอบ เกณฑ์การยอมรับ สำหรับเครื่องมือ อุปกรณ์ที่ใช้
๕.๓	ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอรของบริการของเครื่องมือ อุปกรณ์ที่ใช้ อย่างสม่ำเสมอ
๕.๔	จัดเก็บทะเบียนรายการเครื่องมือ อุปกรณ์ และผลการประเมินความเสี่ยง

ตัวอย่างการดำเนินการตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์ (ต่อ)

๖.	**การออกแบบและการพัฒนา**
๖.๑	**การวางแผนการออกแบบและการพัฒนา**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๖.๑.๑	วางแผนและควบคุมการออกแบบและการพัฒนาผลิตภัณฑ์/บริการ
๖.๑.๒	ระหว่างการวางแผนการออกแบบและการพัฒนา ควรกำหนด
ก.	ลำดับขั้นตอนของการออกแบบและการพัฒนา
ข.	การทบทวน ทวนสอบ และรับรองที่เหมาะสมสำหรับแต่ละลำดับขั้นตอน
ค.	อำนาจหน้าที่และความรับผิดชอบ
๖.๑.๓	จัดการประสานงานระหว่างกลุ่มต่างๆ ที่มีส่วนร่วม เพื่อให้มั่นใจได้ว่า การสื่อสารเกิดประสิทธิผลและมีการมอบหมายความรับผิดชอบชัดเจน
๖.๑.๔	ปรับแผนให้เป็นปัจจุบันตามความเหมาะสมตามสถานะความคืบหน้าของการออกแบบและการพัฒนา
๖.๒	**ปัจจัยในการออกแบบและการพัฒนา**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๖.๒.๑	กำหนดปัจจัยที่เกี่ยวกับข้อกำหนดของผลิตภัณฑ์/บริการ ที่ครอบคลุมด้านความมั่นคงปลอดภัย
๖.๒.๒	เก็บรักษาบันทึกผลที่เกี่ยวข้อง
๖.๒.๓	ปัจจัยดังกล่าวรวมถึง
ก.	ข้อกำหนดการทำงานและสมรรถนะด้านความมั่นคงปลอดภัยของผลิตภัณฑ์/บริการ
ข.	ข้อกำหนดตามกฎระเบียบที่เกี่ยวข้อง
ค.	ข้อมูลจากการออกแบบที่คล้ายคลึงกันในครั้งก่อนๆ
ง.	ข้อกำหนดอื่นๆ ที่จำเป็นต่อการออกแบบและการพัฒนา
๖.๒.๔	ทบทวนว่ามีปัจจัยดังกล่าวอย่างเพียงพอ
๖.๒.๕	ข้อกำหนดต่างๆ ควรมีความสมบูรณ์ ไม่คลุมเครือ และไม่ขัดแย้งซึ่งกันและกัน
๖.๓	**ผลที่ได้จากการออกแบบและการพัฒนา**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๖.๓.๑	นำผลที่ได้จากการออกแบบและพัฒนามาจัดให้อยู่ในรูปแบบที่สามารถทวนสอบกับปัจจัยในการออกแบบและการพัฒนาได้
๖.๓.๒	อนุมัติผลที่ได้จากการออกแบบและพัฒนาก่อนที่จะนำไปใช้งาน
๖.๓.๓	ผลที่ได้จากการออกแบบและการพัฒนา ควร
ก.	มีความสอดคล้องกับปัจจัยในการออกแบบและการพัฒนา
ข.	ให้ข้อมูลที่เหมาะสมสำหรับการจัดเตรียมทรัพยากรที่ต้องใช้ในกระบวนการผลิต/บริการ
ค.	ระบุหรืออ้างถึงเกณฑ์การยอมรับผลิตภัณฑ์/บริการ
ง.	กำหนดคุณลักษณะเฉพาะที่สำคัญด้านความมั่นคงปลอดภัยและการใช้งานที่ถูกต้องของผลิตภัณฑ์/บริการ
๖.๔	**การทบทวนการออกแบบและการพัฒนา**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๖.๔.๑	ทบทวนการออกแบบและพัฒนาอย่างเป็นระบบ ตามลำดับขั้นตอนที่ได้วางแผนไว้ เพื่อประเมินความสามารถว่าผลที่ได้จากการออกแบบและพัฒนาสอดคล้องกับข้อกำหนด และสามารถระบุปัญหาพร้อมเสนอแนวทางการดำเนินการที่จำเป็น
๖.๔.๒	ผู้เข้าร่วมควรรวมถึงผู้แทนจากหน่วยงานต่างๆ ที่เกี่ยวข้องกับการทบทวนในลำดับขั้นตอนนั้น
๖.๔.๓	เก็บรักษาบันทึกผลการทบทวนและผลการดำเนินการ

ตัวอย่างการดำเนินการตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์ (ต่อ)

๖.	**การออกแบบและการพัฒนา (ต่อ)**
๖.๕	**การทวนสอบการออกแบบและการพัฒนา**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร ดำเนินการทวนสอบตามแผนที่วางไว้ เพื่อให้มั่นใจว่าผลที่ได้สอดคล้องกับปัจจัยของการออกแบบและพัฒนา และต้องเก็บรักษาบันทึกผลการทดสอบสอบและผลการดำเนินการ
๖.๖	**การรับรองการออกแบบและการพัฒนา**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
ก.	ดำเนินการรับรองตามแผนที่วางไว้ เพื่อให้มั่นใจได้ว่าผลิตภัณฑ์เป็นไปตามข้อกำหนด เพื่อสร้างความเชื่อมั่นว่าผลิตภัณฑ์/บริการที่เป็นผลลัพธ์มีขีดความสามารถตามข้อกำหนดเฉพาะตรงตามวัตถุประสงค์การใช้งาน
ข.	ดำเนินการรับรองให้เสร็จสิ้นก่อนส่งมอบหรือก่อนนำผลิตภัณฑ์ไปใช้งาน (ถ้าทำได้)
ค.	เก็บรักษาบันทึกผลการรับรองและผลการดำเนินการ
๖.๗	**การควบคุมการเปลี่ยนแปลงการออกแบบและการพัฒนา**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๖.๗.๑	ชี้บ่งและจัดเก็บบันทึกการเปลี่ยนแปลง
๖.๗.๒	ทบทวน ทวนสอบ และรับรอง(ตามเหมาะสม) และอนุมัติการเปลี่ยนแปลงนั้นๆ ก่อนนำออกใช้
๖.๗.๓	การควบคุมการเปลี่ยนแปลงการออกแบบและพัฒนาควรครอบคลุมถึงการประเมินผลกระทบจากการเปลี่ยนแปลงนั้นๆ ที่มีต่อส่วนประกอบ และผลิตภัณฑ์ ที่ได้ส่งมอบไปแล้ว
๖.๗.๔	เก็บรักษาบันทึกผลการทบทวนการเปลี่ยนแปลงการออกแบบและพัฒนา และผลการดำเนินการ
๗.	**การควบคุมในระหว่างกระบวนการ**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรองควร
๗.๑	**จัดเตรียมความพร้อมสำหรับการผลิต/บริการ อาทิ การมอบหมายหน้าที่ จัดทำวิธีการปฏิบัติงาน (ถ้าจำเป็น) กำหนดเครื่องมือ อุปกรณ์ที่ใช้อย่างเหมาะสม**
๗.๒	**ดำเนินการตรวจวัดและเฝ้าติดตามการควบคุมกระบวนการผลิตและการบริการ ตามวิธีการและหลักเกณฑ์ที่กำหนดไว้**
๗.๓	**ระบุรายละเอียดการดำเนินการอนุมัติปล่อย (Release) การส่งมอบ และกิจกรรมหลังการส่งมอบ**
๗.๔	**รับรองกระบวนการผลิตและการบริการ** กรณีที่ไม่สามารถทวนสอบผลที่ได้จากกระบวนการโดยการตรวจวัดหรือการเฝ้าติดตามในกระบวนการนั้น โดยรวมถึงกระบวนการที่อาจพบข้อบกพร่องได้ก็ต่อเมื่อผลิตภัณฑ์ถูกนำไปใช้งานหรือส่งมอบการบริการไปแล้ว เพื่อแสดงให้เห็นถึงความสามารถของกระบวนการในการบรรลุผลตามแผนที่วางไว้ ซึ่งควรประกอบด้วย
ก.	การกำหนดเกณฑ์ในการทบทวนและอนุมัติกระบวนการต่างๆ
ข.	การอนุมัติอุปกรณ์และคุณสมบัติของบุคลากร
ค.	การใช้วิธีการและขั้นตอนการปฏิบัติงานที่กำหนด
ง.	บันทึกผลการดำเนินการที่เกี่ยวข้อง
จ.	การดำเนินการรับรองซ้ำ
๗.๕	**มีการชี้บ่งผลิตภัณฑ์ด้วยวิธีการที่เหมาะสมตลอดกระบวนการผลิต/พัฒนา เมื่อมีความจำเป็น ดังนี้**
ก.	ชี้บ่งสถานะของผลิตภัณฑ์ ระหว่างการผลิต/พัฒนา เช่น การกำหนดรหัส เวอร์ชั่นซอฟต์แวร์ ฯลฯ
ข.	ควบคุมและบันทึกการชี้บ่งผลิตภัณฑ์อย่างเป็นเอกลักษณ์ (unique) หากจำเป็นต้องสอบกลับ

ตัวอย่างการดำเนินการตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์ (ต่อ)

๘.	**การควบคุมผลิตภัณฑ์/บริการที่ไม่เป็นไปตามข้อกำหนด**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๘.๑	มั่นใจได้ว่าผลิตภัณฑ์/บริการ ที่ไม่เป็นไปตามข้อกำหนด มีการชี้บ่งและควบคุมเพื่อป้องกันการนำไปใช้งานหรือส่งมอบโดยไม่ตั้งใจ
๘.๒	จัดทำเอกสารขั้นตอนการปฏิบัติงานที่ระบุถึงการควบคุมดังกล่าว ตลอดจนอำนาจหน้าที่และความรับผิดชอบในการจัดการกับผลิตภัณฑ์/บริการที่ไม่เป็นไปตามข้อกำหนด
๘.๓	จัดการกับผลิตภัณฑ์/บริการที่ไม่เป็นไปตามข้อกำหนดด้วยวิธีการหนึ่งวิธีการที่เหมาะสม
๘.๔	เก็บรักษาบันทึกที่แสดงถึงความไม่เป็นไปตามข้อกำหนด และผลการดำเนินการตลอดจนการได้รับความเห็นชอบไว้
๘.๕	กรณีผลิตภัณฑ์/บริการ ที่ไม่เป็นไปตามข้อกำหนดได้รับการแก้ไขแล้ว ควรได้รับทวนสอบซ้ำเพื่อแสดงให้เห็นว่าผลิตภัณฑ์นั้นเป็นไปตามข้อกำหนดแล้วไม่นำไปใช้หรือประยุกต์ใช้ตามวัตถุประสงค์การใช้งานเดิม
๘.๖	กรณีที่พบผลิตภัณฑ์ที่/บริการไม่เป็นไปตามข้อกำหนด หลังการส่งมอบหรือหลังจากได้เริ่มนำไปใช้งานแล้ว ควรดำเนินการอย่างเหมาะสมกับผลกระทบทั้งที่เกิดขึ้นและอาจเกิดขึ้นอันเนื่องมาจากความไม่เป็นไปตามข้อกำหนดนั้น *กรณีผู้ยื่นคำขอเป็นบุคคลธรรมดา อาจใช้วิธีการควบคุมอื่นๆ ที่เหมาะสม เช่น การบันทึกข้อผิดพลาด (Bugs/Errors) และแนวทางการจัดการก่อนส่งมอบ
๙.	**การดูแลรักษาผลิตภัณฑ์**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร ก. ดูแลรักษาผลิตภัณฑ์ให้เป็นไปตามข้อกำหนดตลอดการดำเนินการภายในสถานประกอบการ จนกระทั่งส่งมอบไปถึงจุดหมายปลายทาง ข. การดูแลรักษาผลิตภัณฑ์ครอบคลุม การชี้บ่ง การเคลื่อนย้าย การบรรจุ การจัดเก็บ การป้องกัน รวมถึงส่วนประกอบของผลิตภัณฑ์
๑๐.	**การควบคุมระดับคุณภาพในการให้บริการ**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควรดูแลรักษาระดับคุณภาพบริการให้เป็นไปตามข้อกำหนด ตลอดระยะเวลาการให้บริการ
๑๑.	**การควบคุมทรัพย์สิน**
๑๑.๑	ทรัพย์สินขององค์กร ก. จัดทำทะเบียนทรัพยสิน (Inventory) ที่ระบุทรัพยสินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพยสินให้เปนปัจจุบัน ข. ระบุขอบเขตเครือขายของบริการที่สำคัญ และระบบคอมพิวเตอรที่เชื่อมตอโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) ค. ตรวจสอบทะเบียนทรัพยสินอยางนอยปละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพยสินของบริการที่สำคัญใหปรับปรุงทะเบียนทรัพยสินดังกลาวดวย ง. ประเมินความเสี่ยงดานการรักษาความมั่นคงปลอดภัยของบริการที่สำคัญตามรายการที่ระบุไวในทะเบียนทรัพยสิน อยางนอยปละ ๑ ครั้ง
๑๑.๒	ทรัพย์สินลูกค้า ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร ก. ดูแลทรัพย์สินลูกค้าด้วยความระมัดระวังในระหว่างที่อยู่ภายใต้การดูแลหรือระหว่างการนำไปใช้งาน ข. ชี้บ่ง ทวนสอบ ปกป้อง และดูแลรักษาทรัพย์สินที่ลูกค้าจัดหาให้ เพื่อนำมาใช้หรือประกอบเป็นส่วนหนึ่งของผลิตภัณฑ์หรือบริการ ค. กรณีที่ทรัพย์สินของลูกค้าผลต่อด้านความมั่นคงปลอดภัย ต้องประเมินความเสี่ยงด้วย ง. กรณีทรัพย์สินลูกค้าสูญหาย ชำรุด หรือไม่เหมาะต่อการใช้งาน ต้องแจ้งให้ลูกค้าทราบและบันทึกไว้เป็นหลักฐาน <u>หมายเหตุ</u> ทรัพย์สินลูกค้าครอบคลุมถึงทรัพย์สินทางปัญญาด้วย
๑๒.	**การควบคุมการเฝ้าระวังภัยคุกคามทางไซเบอร์**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควรเฝ้าระวังและติดตามรายงานที่เกี่ยวกับช่องโหว่ หรือความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ รวมถึงจัดการให้มีการปรับปรุงความรู้ของบุคลากร และเครื่องมือต่างๆ ที่ใช้ในการให้บริการให้ทันสมัยและเหมาะสมกับสภาพการณ์

ตัวอย่างการดำเนินการตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์ (ต่อ)

๑๓.	**การควบคุมบันทึก**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๑๓.๑	จัดทำและคงรักษาไว้ซึ่งบันทึก เพื่อแสดงถึงความสอดคล้องกับข้อกำหนดและการปฏิบัติงานในระบบอย่างมีประสิทธิผล
๑๓.๒	บันทึกควรอยู่ในสภาพที่อ่านได้ง่าย ชี้บ่ง และนำมาใช้งานได้ทันท่วงที
๑๓.๓	ผู้จัดทำเอกสารขั้นตอนการปฏิบัติงานการควบคุมบันทึก เพื่อระบุการควบคุมที่จำเป็นสำหรับการชี้บ่ง การอ่านได้ง่าย การเก็บรักษา การป้องกัน การนำไปใช้และการเรียกคืน ระยะเวลาการจัดเก็บ และการทำลายบันทึก
๑๔.	**การควบคุมเอกสาร**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๑๔.๑	จัดทำเอกสารขั้นตอนการปฏิบัติงานการควบคุมเอกสารทั้งหมดที่เกี่ยวข้องกับข้อกำหนดของหลักเกณฑ์ข้อกำหนดทั่วไปในการควบคุมคุณภาพผลิตภัณฑ์ฉบับนี้ รวมถึงเอกสารจากภายนอกที่จำเป็น เช่น มาตรฐานข้อกำหนด โดยเอกสารทั้งหมดควรมีการควบคุมตามขั้นตอนการปฏิบัติงานการควบคุมเอกสารที่จำเป็นดังต่อไปนี้
	ก. อนุมัติเอกสารตามความเหมาะสมก่อนนำออกใช้
	ข. ทบทวน ปรับปรุงเอกสารให้ทันสมัยตามความจำเป็น รวมถึงการอนุมัติเอกสารที่ได้ปรับแก้
	ค. ชี้บ่งการเปลี่ยนแปลงและสถานะการปรับปรุงปัจจุบันของเอกสาร
	ง. มีเอกสารที่จำเป็นและเกี่ยวข้องอยู่ที่จุดปฏิบัติงาน
	จ. เอกสารอยู่ในสภาพที่อ่านได้ง่าย และชี้บ่งได้สะดวก
	ฉ. เอกสารจากภายนอกมีการชี้บ่งและควบคุมการแจกจ่าย
	ช. ชี้บ่งเอกสารยกเลิกที่เหมาะสม กรณีที่เก็บไว้เพื่อวัตถุประสงค์อื่น ป้องกันการนำไปใช้งานโดยไม่ตั้งใจ
	<u>หมายเหตุ</u> เอกสารที่จัดทำขึ้นอาจอยู่ในรูปแบบหรือสื่อใดก็ได้ *กรณีผู้ยื่นคำขอเป็นบุคคลธรรมดา อาจใช้วิธีการควบคุมอื่นๆ ที่เหมาะสม เช่น ใช้ระบบ Version Control (เช่น Git) เพื่อสร้าง Traceability ของเอกสาร
๑๕.	**การทบทวนของฝ่ายบริหาร**
๑๕.๑	ผู้บริหารระดับสูงทบทวนระบบตามช่วงเวลาที่กำหนด เพื่อให้มั่นใจได้ว่าระบบมีความเหมาะสม และมีประสิทธิผลอย่างต่อเนื่อง
๑๕.๒	การทบทวนครอบคลุมถึงการประเมินโอกาสเพื่อปรับปรุง และความจำเป็นในการเปลี่ยนแปลงระบบการบริหารงานคุณภาพ นโยบายคุณภาพ และวัตถุประสงค์คุณภาพ
๑๕.๓	เก็บรักษาบันทึกการทบทวนของฝ่ายบริหารไว้เป็นหลักฐาน
๑๕.๔	ข้อมูลในการทบทวนของฝ่ายบริหารอย่างน้อยควรครอบคลุมถึง
	ก. ผลการตรวจประเมิน
	ข. ข้อมูลการตอบกลับจากลูกค้า
	ค. สมรรถนะของกระบวนการและความสอดคล้องกับข้อกำหนดของผลิตภัณฑ์/บริการ
	ง. สถานะการปฏิบัติการแก้ไขและป้องกัน
	จ. การติดตามผลการทบทวนครั้งที่ผ่านมา
	ฉ. การเปลี่ยนแปลงที่อาจกระทบต่อระบบการบริหารงานคุณภาพ
	ช. ข้อแนะนำต่างๆ สำหรับการปรับปรุง
๑๕.๕	ผลของการทบทวนของฝ่ายบริหารควรรวมถึงการตัดสินใจและการดำเนินการที่เกี่ยวข้องกับ
	ก. การปรับปรุงประสิทธิผลของระบบการบริหารงานคุณภาพ และกระบวนการต่างๆ ในระบบ
	ข. การปรับปรุงผลิตภัณฑ์ที่เกี่ยวข้องกับข้อกำหนดของลูกค้า
	ค. ความต้องการด้านทรัพยากร *กรณีผู้ยื่นคำขอเป็นบุคคลธรรมดา อาจใช้วิธีการควบคุมอื่นๆ ที่เหมาะสม เช่น เปลี่ยนเป็นการจัดทำ Log การทบทวนผลดำเนินงานด้วยตนเอง (Self-Log)

ตัวอย่างการดำเนินการตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์ (ต่อ)

๑๖.	**ทรัพยากรบุคคล**
๑๖.๑	บุคลากรที่ปฏิบัติงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัย ต้องมีความสามารถและคุณสมบัติเหมาะสมเพียงพอทั้งในด้าน
ก.	การศึกษา
ข.	การฝึกอบรม
ค.	ทักษะ
ง.	ประสบการณ์
๑๖.๒	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
ก.	กำหนดความสามารถที่จำเป็นสำหรับบุคลากรที่ปฏิบัติงานที่มีผลกระทบทางด้านความมั่นคงปลอดภัย
ข.	จัดฝึกอบรมหรือวิธีการอื่นใด เพื่อให้บุคลากรมีความสามารถและคุณสมบัติที่จำเป็นตามที่กำหนด
ค.	ประเมินประสิทธิผลของวิธีการต่างๆ
ง.	มั่นใจว่าบุคลากรตระหนักถึงความเกี่ยวข้องและความสำคัญของกิจกรรมที่ตนปฏิบัติอยู่ต่อการบรรลุวัตถุประสงค์คุณภาพ
จ.	เก็บรักษาบันทึกต่างๆ ของบุคลากรด้านการศึกษา การฝึกอบรม ทักษะ และประสบการณ์ที่เกี่ยวข้อง
	*กรณีผู้ยื่นคำขอเป็นบุคคลธรรมดา อาจใช้วิธีการควบคุมอื่นๆ ที่เหมาะสม เช่น แสดงหลักฐานความสามารถ (Competence) (เอกสารรับรอง(Certificate)/ประวัติอบรม) ของตนเอง
๑๗.	**การจัดซื้อ / การจัดหาผู้ให้บริการภายนอก**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควรจัดทำขั้นตอนการดำเนินการจัดซื้อ จัดหา ที่ครอบคลุมดังนี้
ก.	ประเมินและคัดเลือกผู้ขาย/ผู้ให้บริการ โดยพิจารณาจากความสามารถในการส่งมอบตามที่องค์กรกำหนด
ข.	กำหนดเกณฑ์การคัดเลือก การประเมิน ที่ครอบคลุมด้านความมั่นคงปลอดภัย และการประเมินสมรรถนะเป็นระยะๆ
ค.	เก็บรักษาบันทึกผลการประเมินและผลการดำเนินการ
	*กรณีผู้ยื่นคำขอเป็นบุคคลธรรมดา อาจใช้วิธีการควบคุมอื่นๆ ที่เหมาะสม เช่น การตรวจสอบความปลอดภัยของ Cloud Service Provider หรือ Sub-contractor
๑๘.	**การตรวจประเมินภายใน**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๑๘.๑	ตรวจประเมินภายในตามช่วงเวลาที่กำหนด เพื่อพิจารณาว่า
ก.	ระบบการบริหารงานคุณภาพที่จัดทำขึ้นยังคงสอดคล้องกับการดำเนินการที่วางแผนไว้ และข้อกำหนดระบบการบริหารงานคุณภาพที่องค์กรจัดทำขึ้น
ข.	มีการนำไปปฏิบัติและคงรักษาไว้อย่างมีประสิทธิผล
๑๘.๒	วางแผนการตรวจประเมินภายในโดยพิจารณาถึงสถานะและความสำคัญของกระบวนการต่างๆ ขอบเขตที่ตรวจ และผลการตรวจประเมินที่ผ่านมา
๑๘.๓	กำหนดเกณฑ์ ขอบข่าย ความถี่ และวิธีการที่จะใช้ในการตรวจประเมิน
๑๘.๔	การคัดเลือกผู้ตรวจประเมินและการตรวจประเมินควรมั่นใจได้ว่ากระบวนการตรวจประเมินมีความเป็นธรรม และเป็นกลาง รวมทั้งไม่ตรวจงานที่ตนรับผิดชอบ
๑๘.๕	ระบุความรับผิดชอบและข้อกำหนดใน การวางแผนและการตรวจประเมิน การรายงานผลและการบันทึกไว้ในเอกสารขั้นตอนการปฏิบัติงาน
๑๘.๖	ผู้บริหารที่รับผิดชอบพื้นที่ที่ถูกตรวจประเมินควรมั่นใจได้ว่ามีการดำเนินการจัดการข้อบกพร่องที่ตรวจพบและสาเหตุ
๑๘.๗	การตรวจติดตามผลควรครอบคลุมถึงการทวนสอบผลการดำเนินการแก้ไขและการรายงานผลการทวนสอบ
	*กรณีผู้ยื่นคำขอเป็นบุคคลธรรมดา อาจใช้วิธีการควบคุมอื่นๆ ที่เหมาะสม เช่น ใช้ผู้เชี่ยวชาญในสาขาเดียวกัน ตรวจสอบความถูกต้อง ความน่าเชื่อถือ (Peer Review) หรือจ้างหน่วยงานภายนอก (Outsource)

ตัวอย่างการดำเนินการตามข้อกำหนดทั่วไป ในการควบคุมคุณภาพผลิตภัณฑ์ (ต่อ)

๑๙.	**การเฝ้าระวัง การวัดและวิเคราะห์ข้อมูล**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๑๙.๑	กำหนด รวบรวม และวิเคราะห์ข้อมูลที่เกี่ยวข้อง ซึ่งแสดงถึงระบบการบริหารงานคุณภาพที่เหมาะสมและ มีประสิทธิผล ตลอดจนประเมินว่ายังสามารถปรับปรุงระบบการบริหารงานคุณภาพอย่างต่อเนื่องได้
๑๙.๒	การดำเนินการดังกล่าวควรครอบคลุมถึงข้อมูลที่ได้จากการเฝ้าติดตาม การตรวจวัด และจากแหล่งอื่นๆ ที่เกี่ยวข้อง
๑๙.๓	จัดเตรียมข้อมูลเกี่ยวกับสิ่งต่อไปนี้
ก.	ความพึงพอใจของลูกค้า
ข.	ความเป็นไปตามข้อกำหนดของผลิตภัณฑ์/บริการ
ค.	คุณลักษณะและแนวโน้มต่างๆ ของกระบวนการและผลิตภัณฑ์ ตลอดจนโอกาสในการดำเนินการเชิงป้องกัน
ง.	ผู้ขาย
๒๐.	**การปรับปรุงอย่างต่อเนื่อง**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควรปรับปรุงประสิทธิผลของระบบการบริหารงานคุณภาพอย่างต่อเนื่อง โดยอาศัย
ก.	นโยบายคุณภาพ
ข.	วัตถุประสงค์คุณภาพ
ค.	ผลการตรวจประเมิน
ง.	การวิเคราะห์ข้อมูล
จ.	การดำเนินการเชิงแก้ไขและป้องกัน
ฉ.	การทบทวนของฝ่ายบริหาร
๒๑.	**การปฏิบัติการแก้ไข**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๒๑.๑	ดำเนินการเพื่อกำจัดสาเหตุของความไม่เป็นไปตามข้อกำหนดเพื่อป้องกันไม่ให้เกิดซ้ำ การดำเนินการเชิงแก้ไขควรเหมาะสมกับผลกระทบของความไม่เป็นไปตามข้อกำหนดนั้นๆ
๒๑.๒	จัดทำเอกสารขั้นตอนการปฏิบัติงานเพื่อระบุถึงข้อกำหนดในการ
ก.	ทบทวนความไม่เป็นไปตามข้อกำหนด (รวมถึงข้อร้องเรียนของลูกค้า)
ข.	การหาสาเหตุของความไม่เป็นไปตามข้อกำหนด
ค.	การประเมินความจำเป็นในการดำเนินการเพื่อให้ มั่นใจว่าความไม่เป็นไปตามข้อกำหนดนั้นๆ จะไม่เกิดขึ้นอีก
ง.	การกำหนดและการดำเนินการแก้ไข
จ.	บันทึกผลการปฏิบัติการแก้ไข
ฉ.	การทบทวนการปฏิบัติการแก้ไขที่ได้ดำเนินการไป
๒๒.	**การดำเนินการเชิงป้องกัน**
	ผู้ยื่นคำขอ/ผู้ได้รับการรับรอง ควร
๒๒.๑	กำหนดการดำเนินการเพื่อกำจัดสาเหตุของความไม่เป็นไปตามข้อกำหนดที่มีแนวโน้มว่าอาจเกิดขึ้น เพื่อป้องกันไม่ให้เกิดขึ้น โดยการดำเนินการป้องกันควรเหมาะสมกับผลกระทบของปัญหาที่มีแนวโน้มว่าอาจเกิดขึ้น
๒๒.๒	จัดทำเอกสารขั้นตอนการปฏิบัติงานเพื่อระบุข้อกำหนดในการ
ก.	กำหนดสาเหตุและความไม่เป็นไปตามข้อกำหนดที่มีแนวโน้มว่าอาจเกิดขึ้น
ข.	ประเมินความจำเป็นในการดำเนินการเพื่อป้องกันไม่ให้ข้อบกพร่องเกิดขึ้น
ค.	กำหนดและดำเนินการปฏิบัติเชิงป้องกัน
ง.	บันทึกผลการปฏิบัติเชิงป้องกัน
จ.	ทบทวนผลการปฏิบัติเชิงป้องกัน