ภาคผนวก ก

ข้อกำหนดหลักเกณฑ์การคัดกรองการให้ตราสัญลักษณ์ dSURE

ด้านความปลอดภัยในการใช้งาน (Safety)

ผลิตภัณฑ์ที่จะได้รับการอนุญาตให้ใช้ตราสัญลักษณ์ dSURE ๑ ดาว ต้องผ่านหลักเกณฑ์การคัดกรองด้านความปลอดภัยในการใช้งาน (Safety) ดังนี้

๑) ผลิตภัณฑ์มีความสอดคล้องกับมาตรฐาน มอก. ๖๒๓๖๘-๑ หรือเทียบเท่า โดยผ่านการตรวจสอบจากหน่วยตรวจสอบรับรองตามประกาศสำนักงานกำหนด

๒) แบตเตอร์รี่ และ/หรือ อะแดปเตอร์ ที่ใช้ร่วมกับผลิตภัณฑ์ ต้องผ่านการรับรองมาตรฐาน มอก. ที่เกี่ยวข้องหรือเทียบเท่า

๓) ผลิตภัณฑ์ต้องผ่านมาตรฐานบังคับที่เกี่ยวข้องตามที่สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรมกำหนด

๔) ผลิตภัณฑ์มีเอกสารหลักฐานอื่นๆ อันยืนยันถึงความสามารถ ประสิทธิภาพ คุณภาพ ตามที่ระบุ หรือข้อเสนอวิธีการตรวจสอบหรือพิสูจน์ทราบ รวมถึงเอกสารเกี่ยวกับความปลอดภัยทางไซเบอร์ (cyber security) (ถ้ามี) โดยคณะทำงานพิจารณาการคัดกรองผลิตภัณฑ์เพื่อขอรับตราสัญลักษณ์ dSURE พิจารณาให้ความเห็นชอบ

ภาคผนวก ข

ข้อกำหนดหลักเกณฑ์การคัดกรองการให้ตราสัญลักษณ์ dSURE

ด้านความสามารถในการทำงาน (Functionality)

ผลิตภัณฑ์ที่จะได้รับการอนุญาตให้ใช้ตราสัญลักษณ์ dSURE ๒ ดาว ต้องผ่านหลักเกณฑ์การคัดกรอง ๒ ด้าน ได้แก่ ๑) ด้านความปลอดภัยในการใช้งาน (Safety) ตามภาคผนวก ก และ ๒) ด้านความสามารถในการทำงาน (Functionality) ดังนี้

ผลิตภัณฑ์สามารถทำงานได้จริงตามรายการคุณลักษณะผลิตภัณฑ์ (specification) ที่ระบุไว้ในเอกสารหรือสื่อต่างๆ ที่เกี่ยวข้องกับผลิตภัณฑ์ โดยเฉพาะในส่วนที่เกี่ยวข้องกับเทคโนโลยีและนวัตกรรมดิจิทัล ได้แก่ กระบวนการรับส่งข้อมูล กระบวนการบันทึกและอ่านข้อมูล กระบวนการประมวลผล กระบวนการควบคุมสั่งการ รวมถึงคุณสมบัติอื่นๆ ที่มีความจำเป็นและส่งผลกระทบต่อการทำงานของผลิตภัณฑ์และความเชื่อมั่นของผู้บริโภค โดยจะต้องผ่านการตรวจสอบจากหน่วยตรวจสอบรับรองตามประกาศสำนักงานกำหนด

ภาคผนวก ค

ข้อกำหนดหลักเกณฑ์การคัดกรองการให้ตราสัญลักษณ์ dSURE

ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

ผลิตภัณฑ์ที่จะได้รับการอนุญาตให้ใช้ตราสัญลักษณ์ dSURE ๓ ดาว ต้องผ่านหลักเกณฑ์การคัดกรอง ๓ ด้าน ได้แก่ ๑) ด้านความปลอดภัยในการใช้งาน (Safety) ตามภาคผนวก ก ๒) ด้านความสามารถในการทำงาน (Functionality) ตามภาคผนวก ข และ ๓) ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ดังนี้

๑) ข้อมูลเกี่ยวกับผลิตภัณฑ์และการใช้งานผลิตภัณฑ์ต้องถูกจัดเก็บในประเทศไทย โดยหากผลิตภัณฑ์มีการเชื่อมโยงกับผู้ให้บริการรับ ส่ง จัดเก็บ และประมวลผลข้อมูล เช่น cloud service, data center จะต้องเป็นผู้ให้บริการที่มีการจดทะเบียนจัดตั้งในประเทศไทย มีสถานที่ตั้งอยู่ในประเทศไทย และมีระบบรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity) ตามประกาศสำนักงานกำหนด

๒) ผลิตภัณฑ์ต้องผ่านการทดสอบด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ในหัวข้อต่อไปนี้จากหน่วยตรวจสอบรับรองตามประกาศสำนักงานกำหนด

ลำดับ	หัวข้อการทดสอบ	เกณฑ์การทดสอบ	เกณฑ์การตัดสิน	มาตรฐาน/ข้อกำหนดที่เกี่ยวข้อง	คำอธิบาย/ประโยชน์
๑	เปิดพอร์ตเฉพาะที่จำเป็น	ตรวจสอบพอร์ตและบริการในอุปกรณ์เทียบกับเอกสารจากผู้ผลิตระบุพอร์ตที่เปิดและบริการที่ใช้งานพอร์ตนั้น	ต้องไม่พบการเปิดพอร์ต/บริการนอกเหนือจากที่ระบุไว้	OWASP ISVS ข้อ ๓.๒.๒	การเปิดบริการ/พอร์ตที่ไม่จำเป็นเป็นการเพิ่มความเสี่ยงที่บริการนั้นจะเกิดช่องโหว่ด้านความปลอดภัย ผู้ไม่หวังดีอาจใช้ช่องโหว่ของบริการนั้นเข้าสู่ระบบได้ โดยเฉพาะอย่างยิ่งบริการที่ผู้ผลิตไม่ได้แจ้งไว้ในเอกสารผลิตภัณฑ์
๒	หลีกเลี่ยงการใช้บริการที่ไม่ปลอดภัย	ตรวจหาการเปิดให้บริการที่ไม่ปลอดภัย อาทิ FTP(๒๑), Telnet(๒๓), HTTP	ไม่พบการเปิดบริการที่ไม่ปลอดภัย	OWASP ISVS ข้อ ๓.๒.๓	บริการที่ไม่ปลอดภัย คือ บริการที่ไม่มีการเข้ารหัสข้อมูลที่แน่นหนาเพียงพอ ทำให้ขณะการรับส่งข้อมูลผ่านบริการดังกล่าวอาจถูกผู้ไม่หวังดีลอบนำข้อมูลสำคัญไปใช้ได้

ลำดับ	หัวข้อการทดสอบ	เกณฑ์การทดสอบ	เกณฑ์การตัดสิน	มาตรฐาน/ข้อกำหนดที่เกี่ยวข้อง	คำอธิบาย/ประโยชน์
๓	Network มีความปลอดภัย	ตรวจสอบการเชื่อมต่อระหว่างอุปกรณ์กับเครือข่ายผ่าน HTTPS, SFTP, SSH, SRTP, SRTCP และ/หรือ SCURL เท่านั้น	ไม่พบการใช้การเชื่อมต่อที่ไม่ปลอดภัย	OWASP ISVS ข้อ ๓.๒.๓	การเชื่อมต่อเครือข่ายที่มีความปลอดภัย จะมีการเข้ารหัสในการรับส่งข้อมูลที่แน่นหนาเพียงพอ ทำให้ยากต่อผู้ไม่หวังดีในการนำข้อมูลไปใช้
๔	การเข้ารหัสในการรับส่งผ่าน network	ตรวจสอบการเข้ารหัส network ขั้นต่ำ AES ๒๕๖ bits, TDES double-length keys, RSA ๒๐๔๘ bits, ECC ๑๖๐ bits, TLS ๑.๒	ใช้การเข้ารหัส network ที่ปลอดภัย	OWASP ISVS ข้อ ๔.๑.๑	ปัจจุบันคอมพิวเตอร์มีประสิทธิภาพสูง สามารถถอดรหัสได้โดยง่าย ดังนั้นหากวิธีการเข้ารหัสไม่แน่นหนาเพียงพอ อาจไม่สามารถป้องกันข้อมูลจากผู้ไม่หวังดี
๕	การส่งข้อมูล streaming มีความปลอดภัย (*เฉพาะอุปกรณ์ที่มี streaming)	ตรวจสอบการเข้ารหัสส่งข้อมูล streaming อาทิ HLS Encryption with AES-๑๒๘, DASH, RTMPE	ใช้การเข้ารหัสที่ปลอดภัย	OWASP ISVS ข้อ ๔.๑.๑	การส่งข้อมูลแบบ streaming (ข้อมูลที่ต้องการความต่อเนื่อง) ที่มีความปลอดภัย จะมีการเข้ารหัสในการรับส่งข้อมูลที่แน่นหนาเพียงพอ ทำให้ยากต่อผู้ไม่หวังดีในการนำข้อมูลไปใช้ในทางมิชอบ
๖	แจ้งเตือนผู้ใช้เมื่อมีการอัปเดตซอฟต์แวร์ (*เฉพาะอุปกรณ์ที่มีการ interface)	ตรวจสอบการแจ้งเตือนผู้ใช้งานผ่านช่องทางที่กำหนดไว้เมื่อมีซอฟต์แวร์เวอร์ชั่นใหม่	สามารถแจ้งเตือนผู้ใช้งานผ่านช่องทางที่กำหนดไว้	OWASP ISVS ข้อ ๓.๔.๒	การใช้งานซอฟต์แวร์อาจพบข้อบกพร่อง บางครั้งเป็นข้อบกพร่องด้านความปลอดภัย ดังนั้นซอฟต์แวร์ควรมีการอัพเดทอยู่เสมอ และเมื่อมีการอัพเดทควรแจ้งให้ผู้ใช้งานทราบ
๗	ฟังก์ชันการอัปเดตซอฟต์แวร์ที่ใช้งานได้และมีความปลอดภัย	ตรวจสอบฟังก์ชันการอัปเดตซอฟต์แวร์	สามารถอัปเดตซอฟต์แวร์ได้ โดยมีกระบวนการตรวจสอบ	OWASP ISVS ข้อ ๓.๔.๒	อุปกรณ์ IoT มักจะพัฒนาฟังก์ชันในการอัพเดทซอฟต์แวร์ของตนเอง ดังนั้นจึงควรตรวจสอบว่าฟังก์ชัน

ลำดับ	หัวข้อการทดสอบ	เกณฑ์การทดสอบ	เกณฑ์การตัดสิน	มาตรฐาน/ ข้อกำหนด ที่เกี่ยวข้อง	คำอธิบาย/ประโยชน์
			firmware เวอร์ชั่นใหม่ว่าทำงานได้อย่างถูกต้องก่อนอนุญาตให้ใช้งานจริง		นั้นทำงานอย่างถูกต้อง เพื่อให้แน่ใจว่า เมื่ออัพเดทซอฟต์แวร์แล้วอุปกรณ์ยังสามารถทำงานได้
๘	ช่องทางการส่งซอฟต์แวร์มีความปลอดภัย	ตรวจสอบการเข้ารหัสที่ใช้ในการส่งซอฟต์แวร์	ใช้การเข้ารหัสตามข้อ ๕ เท่านั้น	OWASP ISVS ข้อ ๓.๔.๑	ช่องทางเข้ารหัสที่ปลอดภัยจะช่วยทำให้มั่นใจในความถูกต้องแท้จริงของซอฟต์แวร์ที่ดาวน์โหลดมามากขึ้น
๙	หากมีการเก็บรักษาข้อมูลส่วนบุคคลต้องเก็บเท่าที่จำเป็นระบุวัตถุประสงค์การนำไปใช้งานให้ผู้ใช้ทราบ และต้องได้รับความยินยอมจากผู้ใช้ก่อน	ตรวจสอบการแจ้งเตือนและการให้ความยินยอมของผู้ใช้	พบการแจ้งและ/หรือ ขอความยินยอมจากผู้ใช้งาน (แล้วแต่กรณีตามความเหมาะสม)	MSTG-ARCH-๑๒, PDPA	เพื่อให้สอดคล้องกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล
๑๐	หากมีการจัดเก็บข้อมูลส่วนบุคคลเพิ่มเติม และ/หรือนำไปใช้ในวัตถุประสงค์อื่นนอกเหนือจากที่ผู้ใช้เคยให้ความยินยอมต้องแจ้งรายการข้อมูล และ/หรือวัตถุประสงค์ให้ผู้ใช้ทราบอีกครั้ง และ/หรือ มีการขอความยินยอมจากผู้ใช้ก่อน	ตรวจสอบการแจ้งเตือนผู้ใช้และผู้ใช้สามารถเลือกที่จะให้ความยินยอมในแต่ละวัตถุประสงค์/ข้อมูลได้	พบการแจ้งและ/หรือ ขอความยินยอมจากผู้ใช้งาน	MSTG-ARCH-๑๒, PDPA	เพื่อให้สอดคล้องกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล
๑๑	ผู้ใช้สามารถเข้าถึงสำเนาข้อมูลได้	ตรวจสอบวิธีการแสดงข้อมูลส่วนบุคคลที่เก็บไว้และ	พบวิธีการ	MSTG-ARCH-๑๒, PDPA	เพื่อให้สอดคล้องกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล

ลำดับ	หัวข้อการทดสอบ	เกณฑ์การทดสอบ	เกณฑ์การตัดสิน	มาตรฐาน/ ข้อกำหนด ที่เกี่ยวข้อง	คำอธิบาย/ประโยชน์
		การให้ผู้ใช้นำข้อมูลออกมาได้			
๑๒	ผู้ใช้มีสิทธิลบข้อมูลที่ถูกเก็บรวบรวมไว้ได้	ตรวจสอบวิธีการให้ผู้ใช้ลบข้อมูลส่วนบุคคลของตน	พบวิธีการ	MSTG-ARCH-๑๒, PDPA	เพื่อให้สอดคล้องกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล
๑๓	สามารถติดต่อผู้ผลิตได้ในกรณีการจัดการข้อมูลส่วนบุคคล	ตรวจสอบเอกสารนโยบายและขั้นตอนการคุ้มครองข้อมูลส่วนบุคคลของบริษัท	พบที่ติดต่อ (อีเมล์ ที่อยู่ หรือเบอร์โทรศัพท์) ของผู้รับผิดชอบในนโยบายการคุ้มครองข้อมูลส่วนบุคคล	MSTG-ARCH-๑๒, PDPA	เพื่อให้สอดคล้องกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล
๑๔	มีมาตรการการรับ/ส่ง/เก็บรักษาข้อมูลผ่านช่องทางที่ปลอดภัย	ตรวจสอบมาตรการการรับ/ส่ง/เก็บรักษาข้อมูล	พบมาตรการ	OWASP ISVS ข้อ ๔.๑.๑	ผู้ผลิตควรประกาศนโยบายการรับส่ง จัดเก็บ จัดการข้อมูลอย่างปลอดภัยเพื่อสร้างความเชื่อมั่นให้กับผู้บริโภค
๑๕	ไม่รัน service โดยใช้ user ที่มีสิทธิ root หรือ admin	ตรวจเฟิร์มแวร์ต้องไม่พบการเรียกใช้บริการโดยใช้บัญชีผู้ใช้ที่มีสิทธิเทียบเท่าผู้ดูแลระบบ	ไม่พบการเปิดบริการที่ใช้สิทธิเทียบเท่าผู้ดูแลระบบ	OWASP ISVS ข้อ ๒.๒.๓	การเรียกใช้บริการผ่านบัญชีผู้ใช้ที่มีสิทธิของผู้ดูแลระบบ (root/admin) เป็นสิ่งที่ไม่สมควรอย่างยิ่ง หากผู้ไม่หวังดีเจาะระบบผ่านบริการนั้น อาจมีสิทธิเทียบเท่ากับผู้ดูแลระบบได้
๑๖	ฟังก์ชันติดตามรายงานสถานะการทำงานของอุปกรณ์ผ่านเครือข่าย	ตรวจสอบสถานะอุปกรณ์	มีฟังก์ชันและใช้งานได้จริง	ISO ๒๕๐๔๐, IEEE/IEC ๒๙๑๑๙-๒	อุปกรณ์โดยเฉพาะด้านความปลอดภัยควรมีการแจ้งสถานะการทำงานของอุปกรณ์ (online/offline) ให้ผู้ใช้ทราบเมื่อเกิดปัญหาจะได้แก้ไขได้ทันท่วงที

ลำดับ	หัวข้อการทดสอบ	เกณฑ์การทดสอบ	เกณฑ์การตัดสิน	มาตรฐาน/ ข้อกำหนด ที่เกี่ยวข้อง	คำอธิบาย/ประโยชน์
๑๗	มีแจ้งเตือนเมื่อเกิดความผิดปกติกับอุปกรณ์	ตรวจสอบการรายงานสถานะอุปกรณ์ สามารถแจ้งเตือนไปยังแอปพลิเคชันหรืออุปกรณ์ เมื่อเกิดความผิดปกติขึ้นกับอุปกรณ์ ในทางกลับกัน แอปพลิเคชันสามารถแจ้งเตือนเมื่อไม่สามารถติดต่อกับอุปกรณ์ภายในระยะเวลาที่กำหนด	มีฟังก์ชันและใช้งานได้จริง อ้างอิงตามกรณีทดสอบ FA๐๕	ISO ๒๕๐๔๐, IEEE/IEC ๒๙๑๑๙-๒	อุปกรณ์โดยเฉพาะด้านความปลอดภัยควรมีการแจ้งสถานะความผิดปกติของอุปกรณ์ เช่น กล้องถูกบังไม่สามารถบันทึกได้ เพื่อให้ผู้ใช้ทราบว่าเกิดปัญหาจะได้แก้ไขได้ทันท่วงที
18	คู่มือแนะนำวิธีการติดตั้งภาษาไทย	ตรวจสอบคู่มือควรมีเนื้อหาเกี่ยวกับขั้นตอนการติดตั้ง เชื่อมต่อ การตั้งค่าความปลอดภัยทั้งทางกายภาพและทางไซเบอร์	พบเอกสาร	depa recommendation	คู่มือภาษาไทยจะช่วยให้ผู้ใช้ทำความเข้าใจได้ง่ายขึ้น และควรแนะนำวิธีการตั้งค่าเพื่อให้อุปกรณ์มีความปลอดภัยมากยิ่งขึ้น
19	คู่มือแนะนำวิธีการใช้งานภาษาไทย	ตรวจสอบคู่มือควรมีเนื้อหาเกี่ยวกับวิธีการใช้งาน ตรวจสอบความปลอดภัยทางไซเบอร์ แก้ไขข้อผิดพลาด	พบเอกสาร	depa recommendation	คู่มือภาษาไทยจะช่วยให้ผู้ใช้ทำความเข้าใจได้ง่ายขึ้น เพื่อให้สามารถใช้งานได้อย่างถูกวิธีและทำให้เกิดความปลอดภัยมากขึ้น
20	ผู้ใช้สามารถเข้าถึงความช่วยเหลือในช่องทางต่างๆ ได้	ตรวจสอบฟังก์ชันช่วยเหลือผู้ใช้งานเกี่ยวกับขั้นตอนการตั้งค่า ตรวจสอบความปลอดภัยทางไซเบอร์	พบเอกสาร	depa recommendation	ซอฟต์แวร์ควรมีฟังก์ชันช่วยเหลือ กรณีผู้ใช้งานเกิดข้อสงสัยสามารถขอความช่วยเหลือจากเมนูของซอฟต์แวร์ได้

ลำดับ	หัวข้อการทดสอบ	เกณฑ์การทดสอบ	เกณฑ์การตัดสิน	มาตรฐาน/ข้อกำหนดที่เกี่ยวข้อง	คำอธิบาย/ประโยชน์
๒๑	การระบุตัวตนอย่างปลอดภัย	ตรวจสอบการระบุตัวตนเพื่อเข้าแอปพลิเคชัน เช่น username/pass, MFA, Biometric	มีฟังก์ชันและใช้งานได้จริง	ISO ๒๕๐๔๐, IEEE/IEC ๒๙๑๑๙-๒	เพื่อป้องกันการเข้าถึงบัญชีผู้ใช้งานโดยไม่ได้รับอนุญาต ควรมีระบุ/ยืนยันตัวตนผู้ใช้งานก่อนใช้งานแอปพลิเคชัน