คู่มือการประเมินความสอดคล้องด้วยตนเอง **สำหรับระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์**

ตามข้อเสนอแนะมาตรฐานฯ
ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ขมธอ. 26-2564)

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม
ETDA

คำนำ

ตามที่ สพธอ. ได้ประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (Electronic Voting System) ขมธอ.26-2564 เวอร์ชัน 2.0 เพื่อเป็นข้อกำหนดสำหรับผู้พัฒนาระบบการลงคะแนนในการพัฒนาระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ ที่มีความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศเป็นมาตรฐานเดียวกัน และเพื่อสร้างความมั่นใจให้กับผู้ใช้งานหรือใช้บริการระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความน่าเชื่อถือ

สพธอ. จึงได้จัดทำ คู่มือการประเมินความสอดคล้องด้วยตนเองสำหรับระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เพื่อเป็นแนวทางให้ผู้พัฒนาหรือผู้ให้บริการระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์สามารถปฏิบัติได้อย่างสอดคล้องตามวัตถุประสงค์และข้อกำหนดของ ขมธอ.26-2564 เวอร์ชัน 2.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สารบัญ

วัตถุประสงค์

คู่มือการประเมินความสอดคล้องด้วยตนเองสำหรับระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ฉบับนี้เป็นการอธิบายข้อกำหนดภายใต้ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (Electronic Voting System) ขมธอ.26-2564 เวอร์ชัน 2.0 สำหรับการพัฒนาระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศ โดยแบ่งออกเป็น 15 หมวด ซึ่งครอบคลุมทั้งข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน (จำนวน 6 หมวด) และข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ (จำนวน 9 หมวด) ดังต่อไปนี้

ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน

(1) การออกแบบระบบ (system design)
(2) การพัฒนาระบบ (system development)
(3) ความโปร่งใส (transparent)
(4) การเข้าถึงอย่างเท่าเทียม (equitable access)
(5) การลงคะแนนตรงตามเจตนา (cast as intended)
(6) ความเหมาะสมต่อการใช้งาน (usable)

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

(7) การทำงานร่วมกัน (interoperable)
(8) การตรวจสอบ (auditable)
(9) ความเป็นส่วนตัวของผู้ลงคะแนน (voter privacy)
(10) ความลับของคะแนนเสียง (vote secrecy)
(11) การควบคุมการเข้าถึง (access control)
(12) ความมั่นคงปลอดภัยทางกายภาพ (physical security)
(13) การคุ้มครองข้อมูล (data protection)
(14) การรักษาความครบถ้วนของระบบ (system integrity)
(15) การตรวจจับและการเฝ้าระวัง (detection and monitoring)

เพื่อเป็นการชักชวนความเข้าใจแก่ผู้พัฒนาระบบหรือผู้ให้บริการระบบการลงคะแนน และเป็นการช่วยอำนวยความสะดวกแก่ผู้พัฒนาระบบหรือผู้ให้บริการระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ให้สามารถปฏิบัติได้อย่างสอดคล้องตามข้อกำหนดและแนวปฏิบัติของข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (Electronic Voting System) ซึ่งครอบคลุมการความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศ ที่ช่วยสร้างความน่าเชื่อถือและสร้างความมั่นใจให้กับผู้ใช้งานหรือใช้บริการระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

การใช้งานคู่มือ

คู่มือการประเมินความสอดคล้องด้วยตนเองสำหรับระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ฉบับนี้แบ่งออกเป็น 2 ส่วน ได้แก่

- ส่วนที่ 1 ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน
- ส่วนที่ 2 ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

ซึ่งเป็นการอธิบายเพื่อขยายความเพิ่มเติมจากข้อกำหนดและแนวปฏิบัติ ที่ปรากฏข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (Electronic Voting System) ในข้อ 3. ข้อกำหนดของระบบการลงคะแนนที่คำนึงถึงความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ผู้พัฒนาระบบหรือผู้ให้บริการระบบการลงคะแนน**นำมาพิจารณาเป็นแนวทางในการดำเนินการ**

การแสดงคำอธิบายใช้รูปแบบตาราง โดยผู้อ่านสามารถเปรียบเทียบวัตถุประสงค์และข้อกำหนดตามข้อเสนอแนะมาตรฐานฯ ได้ดังนี้

ข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์	คู่มือการประเมินความสอดคล้องด้วยตนเองสำหรับระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์
ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน	
3.1 การออกแบบระบบ (System Design)	1 การออกแบบระบบ (System Design)
3.2 การพัฒนาระบบ (System Development)	2 การพัฒนาระบบ (System Development)
3.3 ความโปร่งใส (Transparent)	3 ความโปร่งใส (Transparent)
3.4 การเข้าถึงอย่างเท่าเทียม (Equitable Access)	4 การเข้าถึงอย่างเท่าเทียม (Equitable Access)
3.5 การลงคะแนนตรงตามเจตนา (Cast as Intended)	5 การลงคะแนนตรงตามเจตนา (Cast as Intended)
3.6 ความเหมาะสมต่อการใช้งาน (Usable)	6 ความเหมาะสมต่อการใช้งาน (Usable)
ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ	
3.7 การทำงานร่วมกัน (Interoperable)	7 การทำงานร่วมกัน (Interoperable)
3.8 การตรวจสอบ (Auditable)	8 การตรวจสอบ (Auditable)
3.9 ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy)	9 ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy)
3.10 ความลับของคะแนนเสียง (Vote Secrecy)	10 ความลับของคะแนนเสียง (Vote Secrecy)
3.11 การควบคุมการเข้าถึง (Access Control)	11 การควบคุมการเข้าถึง (Access Control)
3.12 ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)	12 ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)
3.13 การคุ้มครองข้อมูล (Data Protection)	13 การคุ้มครองข้อมูล (Data Protection)
3.14 การรักษาความครบถ้วนของระบบ (System Integrity)	14 การรักษาความครบถ้วนของระบบ (System Integrity)
3.15 การตรวจจับและการเฝ้าระวัง (Detection and Monitoring)	15 การตรวจจับและการเฝ้าระวัง (Detection and Monitoring)

คำอธิบาย

แนวทางการประเมินความสอดคล้องด้วยตนเองสำหรับระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

ตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (Electronic Voting System)

ส่วนที่ 1 ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงานข้อกำหนด

1. การออกแบบระบบ (System Design)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามกระบวนการการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ

ข้อกำหนด	คำอธิบาย
1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด	• ผู้พัฒนาระบบต้องแสดงให้เห็นถึงการนำกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนดมาใช้ในการพัฒนาระบบ • ระบบการลงคะแนนมีการออกแบบให้มีฟังก์ชันอย่างน้อย ดังนี้ 1) การเตรียมข้อมูลสำหรับการลงคะแนน โดยรองรับการนำเข้าข้อมูลที่เกี่ยวข้องกับการลงคะแนน เช่น ข้อมูลตัวเลือกการลงคะแนน ผู้มีสิทธิลงคะแนน เงื่อนไขการลงคะแนน เป็นต้น 2) การเปิดลงคะแนน 3) การลงคะแนน 4) การส่งผลลงคะแนน 5) การปิดลงคะแนน 6) การนับคะแนน 7) การรายงานผลรวมของการลงคะแนน
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	• ระบบผ่านการทดสอบดังนี้ 1) มี test case ที่ครอบคลุมการทดสอบความถูกต้อง (system accuracy) รวมถึงการจำลองความล้มเหลวในส่วนต่าง ๆ โดยการทำ unit test และ integration test 2) ทดสอบการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) และการทำงานของระบบในภาวะวิกฤต (stress testing) โดยการทำ load test หรือ Performance test ตามที่กล่าวอ้าง
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	• มีรายงานผลการทดสอบระบบ (test report) ที่มีข้อมูลอย่างน้อยดังนี้ 1) ความต้องการและฟังก์ชันที่ถูกทดสอบ 2) เกณฑ์การผ่าน-ไม่ผ่าน การทดสอบในแต่ละความต้องการและฟังก์ชัน 3) หลักฐานการทดสอบ ทั้งข้อมูลตั้งต้น ผลลัพธ์คาดหวังในแต่ละความต้องการ และฟังก์ชัน 4) ขั้นตอนและกระบวนการที่ใช้ในการทดสอบ โดยครอบคลุมเงื่อนไขการทดสอบ การเตรียมข้อมูลตั้งต้น ข้อมูลประกอบใน

ข้อกำหนด	คำอธิบาย
	การทดสอบ ข้อมูลผลลัพธ์ที่ถูกบันทึก และวิธีการแปลผลให้ได้เป็นผลการทดสอบ 5) รายงานผลการทดสอบจริง 6) รายละเอียดอธิบายกรณีที่การทดสอบไม่ผ่าน

2. การพัฒนาระบบ (System Development)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการพัฒนาระบบโดยใช้แนวปฏิบัติที่ดี

ข้อกำหนด	คำอธิบาย
2.1 – การพัฒนาระบบการลงคะแนนใช้แนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์	• ภาษาที่ใช้ในการเขียนโปรแกรมเป็นภาษาที่ผู้พัฒนาภาษายังรองรับการใช้งานอยู่ (not deprecated) • ผู้พัฒนาระบบปฏิบัติตามกระบวนการพัฒนาระบบที่ดี เช่น มาตรฐาน ISO/IEC/IEEE 12207 Systems and software engineering – Software life cycle processes และ ISO/IEC 29110 Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs) เป็นต้น
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน(modular)	• ผู้พัฒนาระบบออกแบบโครงสร้างโปรแกรมเป็นแบบแยกส่วนตาม function ในการทำงาน หรือมีการใช้ model view controller framework ในการเขียนโปรแกรม
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	• ผู้พัฒนาระบบมีการทำ version control ของซอร์สโค้ด • ซอร์สโค้ดของโปรแกรมการลงคะแนนมีความน่าเชื่อถือ และต้องไม่สามารถแก้ไขตัวเองได้ • ข้อมูลที่เกี่ยวข้องกับการลงคะแนนในโปรแกรม เช่น ข้อมูลตัวเลือกการลงคะแนน ผู้มีสิทธิลงคะแนน เงื่อนไขการลงคะแนน และข้อมูลผลการลงคะแนน เป็นต้น มีการป้องกันการแก้ไขโดยไม่ได้รับอนุญาต
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	• ระบบมีความสามารถในการกู้คืนการทำงาน ในกรณีเกิดเหตุไม่พึงประสงค์ • ระบบมีการ maintain log ของข้อผิดพลาด รวมถึงความล้มเหลวในการทำงาน เช่น กรณีระบบล่มทั้งในระดับ infrastructure level และ application level เป็นต้น

3. ความโปร่งใส (Transparent)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนและกระบวนการลงคะแนนมีการออกแบบที่มีความโปร่งใส

ข้อกำหนด	คำอธิบาย
3.1 – เอกสารอธิบายการออกแบบการทำงาน การเข้าถึง มาตรการความมั่นคงปลอดภัย และรายละเอียดอื่น ๆ ของระบบการลงคะแนนสามารถอ่านและทำความเข้าใจได้	• มีเอกสารเกี่ยวกับระบบการลงคะแนน ที่มีรายละเอียดดังนี้ 1) ภาพรวมของระบบ (system overview) เช่น การออกแบบระบบ ความสามารถของระบบ ส่วนประกอบของระบบ เป็นต้น

ข้อกำหนด	คำอธิบาย
	2) ประสิทธิภาพของระบบ (system performance) เช่น ปริมาณธุรกรรมสูงสุดที่รองรับได้ จำนวนผู้ใช้งานสูงสุด ระยะเวลาทำงานต่อเนื่องสูงสุด เป็นต้น 3) ความมั่นคงปลอดภัยของระบบ (system security) เช่น การเข้ารหัสลับข้อมูล การป้องกันการเข้าถึง เป็นต้น 4) การติดตั้งซอฟต์แวร์ (software installation) 5) การทำงานของระบบ (system operations) 6) การบำรุงรักษาระบบ (system maintenance) 7) คู่มือการใช้งาน (user manual)
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนน เตรียมไว้พร้อมสำหรับการตรวจสอบระบบ	• มีเอกสารอธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ
3.3 – บุคคลที่เกี่ยวข้องกับระบบการลงคะแนนสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	• มีเอกสารอธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และคำอธิบายรูปแบบของบันทึกเหตุการณ์ (log format)

4. การเข้าถึงอย่างเท่าเทียม (Equitable Access)

วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม

ข้อกำหนด	คำอธิบาย
4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	• ระบบการลงคะแนนในทุกช่องทางอิเล็กทรอนิกส์ต้องมีฟังก์ชันในการลงคะแนน และการตรวจสอบผลการลงคะแนนที่เหมือนกัน โดย ○ มีการแสดงผล (display format) ที่สอดคล้องกัน ○ มีปฏิสัมพันธ์ (interaction mode) ที่สอดคล้องกัน
4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ	• การแสดงผล (display format) ข้อมูลและตัวเลือกลงคะแนนแต่ละตัวเลือก ใช้แบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน

5. การลงคะแนนตรงตามเจตนา (Cast as Intended)

วัตถุประสงค์ เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้

ข้อกำหนด	คำอธิบาย
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงกับความต้องการของผู้ลงคะแนน	• ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับการใช้งานครั้งแรก • ระบบลงคะแนนรองรับการตั้งค่าเฉพาะบุคคลโดยผู้ลงคะแนนได้อย่างไรบ้าง เช่น รองรับการปรับขนาดตัวอักษร การปรับ theme สีของจอแสดงผล เป็นต้น

ข้อกำหนด	คำอธิบาย
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	• ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง • ระบบมีกลไกป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation)
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	• ระบบการลงคะแนนมีการแสดงข้อมูลที่เกี่ยวข้องกับการลงคะแนนด้วยภาษาที่ชัดเจนและอ่านง่าย อย่างน้อย ดังนี้ 1) กฎกติกาของการลงคะแนน 2) จำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก 3) การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน 4) การแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จ 5) คำแนะนำสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ

6. ความเหมาะสมต่อการใช้งาน (Usable)

<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้อย่างเหมาะสม

ข้อกำหนด	คำอธิบาย
6.1 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ลงคะแนน	• มีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับทุกกลุ่มเป้าหมายผู้ลงคะแนน • ระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) เกี่ยวกับการแสดงข้อมูล เช่น การใช้ภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งการแสดงข้อมูล เป็นต้น
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	• มีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบให้เหมาะสมสำหรับการควบคุมระบบการลงคะแนน

ส่วนที่ 2 ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

7. การทำงานร่วมกัน (Interoperable)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน

ข้อกำหนด	คำอธิบาย
7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนอยู่ในรูปแบบที่ทำงานร่วมกันได้หรือรูปแบบมาตรฐาน	• ข้อมูลนำเข้า ส่งออกจากระบบการลงคะแนน เช่น ข้อมูลผู้มีสิทธิลงคะแนน ข้อมูลการลงคะแนน ข้อมูลรายงานผลการลงคะแนน และข้อมูล log ควรมีรูปแบบข้อมูลที่เป็นมาตรฐาน เช่น รูปแบบ PDF, CSV , JSON เป็นต้น กรณีข้อมูลไม่เป็นรูปแบบมาตรฐานต้องมีกระบวนการหรือเครื่องมือเพื่อแปลงให้ข้อมูลนั้นอยู่ในรูปแบบมาตรฐานหรือรูปแบบที่ทำงานร่วมกันได้
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	• ระบบการลงคะแนนที่มีการใช้ฮาร์ดแวร์ในการลงคะแนน เช่น เครื่องลงคะแนนอิเล็กทรอนิกส์ (direct-recording electronic voting machine) หรืออุปกรณ์สำหรับลงคะแนนโดยเฉพาะที่ผู้ให้บริการจัดหาให้ เป็นต้น ต้องมีวิธีการเชื่อมต่อ และใช้โปรโตคอลการสื่อสารที่เป็นมาตรฐาน เช่น IEEE (Wifi, Bluetooth, USB) เป็นต้น

8. การตรวจสอบ (Auditable)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบความถูกต้องของผลลงคะแนน

ข้อกำหนด	คำอธิบาย
8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	• ระบบการลงคะแนนต้องมีความสามารถในการตรวจจับและบันทึกข้อผิดพลาดของระบบการลงคะแนนที่เกิดขึ้นในระหว่างการลงคะแนนได้ • รูปแบบการลงคะแนนที่จัดเก็บต้องสามารถตรวจสอบการเปลี่ยนแปลงได้ • ระบบลงคะแนนต้องมีกระบวนการให้ผู้ลงคะแนนตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกได้ และมีกระบวนการให้ผู้ลงคะแนนสามารถเริ่มต้นลงคะแนนใหม่ได้ ก่อนยืนยันผลการลงคะแนน • ระบบการลงคะแนนต้องมีกระบวนการให้ผู้ลงคะแนนตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกได้ และแจ้งข้อผิดพลาดที่เกิดขึ้นจากระบบลงคะแนน ซึ่งผู้ลงคะแนนสามารถเริ่มต้นลงคะแนนใหม่หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน • ควรมีคู่มือหรือคำอธิบายถึงช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน • ระบบการลงคะแนนต้องสร้างรายงานแสดงข้อมูลผลการลงคะแนนที่สามารถตรวจสอบได้ • ผู้ให้บริการต้องมีเอกสารขั้นตอนการนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง

9. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy)

วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง

ข้อกำหนด	คำอธิบาย
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	• ระบบลงคะแนนต้องแสดงให้เห็นถึงการรักษาความเป็นส่วนตัวโดยไม่แสดงหรือเปิดเผยข้อมูลต่อบุคคลอื่น ตลอดช่วงเวลาลงคะแนน เช่น มีกระบวนการรักษาความลับตลอดขั้นตอนการลงลงคะแนน
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	• ระบบการลงคะแนนต้องออกแบบให้ผู้ลงคะแนนสามารถเข้าใจ ใช้งานได้ง่าย และสามารถทำได้ด้วยตนเอง ทั้งเครื่องหมายการลงคะแนน ตัวเลือกสำหรับลงคะแนน และการส่งผลลงคะแนน • ระบบการลงคะแนนควรสามารถให้ผู้ลงคะแนนสามารถตั้งค่าการแสดงผลส่วนบุคคล(preference settings) ที่เกี่ยวกับเครื่องหมายลงคะแนน ตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ เช่น การปรับขนาดและสีตัวอักษร หรือ การตัดสินใจส่งผลการลงคะแนน

10. ความลับของคะแนนเสียง (Vote Secrecy)

วัตถุประสงค์ (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน

ข้อกำหนด	คำอธิบาย
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	• ระบบลงคะแนนต้องแสดงให้เห็นถึงการประมวลผล การจัดเก็บผลการลงคะแนน และการแสดงผลการลงคะแนนที่ไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มาประมวลผลและแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนตลอดกระบวนการลงคะแนน • ข้อมูลผลการลงคะแนนที่จัดเก็บไม่สามารถเชื่อมโยงข้อมูลส่วนบุคคลของผู้ลงคะแนนได้โดยตรง • ผลการลงคะแนนต้องไม่สามารถเชื่อมโยง หรือ ปรากฏข้อมูลส่วนบุคคลของผู้ลงคะแนน
10.2 – ระบบการลงคะแนนไม่จัดทำข้อมูลเกี่ยวกับผู้ลงคะแนนหรือข้อมูลอื่น ๆ ที่สามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนขอลชงผู้ลงคะแนน	• ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับผลลงคะแนน เช่น การเชื่อมโยงผลการลงคะแนนกับหมายเลขบัตรประชาชน หรือหมายเลขใบขับขี่ ชื่อและนามสกุล บัญชีผู้ใช้งาน(User account) และ e-mail address เป็นต้น รวมถึงข้อมูลอื่น ๆ ที่สามารถระบุระหว่างอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนได้ • ข้อมูลผลการลงคะแนนจะต้องมีการเข้ารหัสลับเพื่อรักษาความลับของผลการลงคะแนน • กรณีที่ให้ผู้ลงคะแนนส่งผลลงคะแนนก่อนจะตรวจสอบการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนนสามารถใช้การเชื่อมโยงโดยอ้อม (indirect voter association) ที่เชื่อมโยงผู้ลงคะแนนกับ

ข้อกำหนด	คำอธิบาย
	ผลลงคะแนนที่ถูกเข้ารหัสลับไว้ โดยหลังจากตรวจสอบแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้น จึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับ และนำไปนับคะแนนเป็นผลรวมของการลงคะแนน

11. การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

ข้อกำหนด	คำอธิบาย
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	• ต้องมีการตั้งค่าให้มีการจัดเก็บ log ที่เกี่ยวข้องกับการเข้าถึงและกิจกรรมที่ดำเนินการของผู้ใช้งาน โดยอย่างน้อยต้องประกอบด้วยข้อมูลที่สามารถระบุตัวบุคคลหรือชื่อผู้ใช้งาน (Username) วันและเวลาของการเข้าถึงระบบลงคะแนน (ทั้งล้มเหลวและสำเร็จ) เวลาลงคะแนน และเวลาออกจากระบบลงคะแนน รวมถึงมีการเทียบเวลากับแหล่งเวลาที่เป็นมาตรฐานสากล • ต้องแสดงหลักฐานให้เห็นว่ามีการป้องกันการเปลี่ยนแปลงและการเข้าถึงที่ไม่ได้รับอนุญาตต่อข้อมูล log • ต้องแสดงหลักฐานให้เห็นถึงการจำกัดการเข้าถึงข้อมูล log • ต้องจัดเก็บข้อมูลการดำเนินการที่เกี่ยวข้องกับข้อมูล log ในระบบลงคะแนน เช่น การแก้ไขเปลี่ยนแปลง การลบ การปิดการใช้งาน เป็นต้น โดยครอบคลุมข้อมูลผู้ที่ดำเนินการ วันเวลา และวัตถุประสงค์ในการดำเนินการเป็นอย่างน้อย
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งานในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	• ระบบลงคะแนนต้องมีการจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น • ระบบต้องสามารถแยกบทบาทหน้าที่ของผู้ใช้งานได้อย่างชัดเจน เช่น ผู้ควบคุมระบบ ผู้ใช้งานหรือผู้มีสิทธิลงคะแนน เจ้าหน้าที่ปฏิบัติงานที่เกี่ยวข้อง เป็นต้น รวมถึงต้องแสดงหลักฐานให้เห็นถึงการกำหนดสิทธิดังกล่าว เช่น Authorize Matrix เป็นต้น • ผู้ควบคุมระบบต้องสามารถกำหนดสิทธิสำหรับบัญชีของผู้ใช้งานได้ตามบทบาทหน้าที่ของผู้ใช้งาน เช่น การสร้าง แก้ไข และเพิกถอน เป็นต้น
11.3 – ระบบการลงคะแนนรองรับวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน	• ระบบการลงคะแนนต้องมีวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งานก่อนเข้าใช้งาน ซึ่งอาจพิจารณาข้อกำหนดตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) จากมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล • ระบบการลงคะแนนต้องกำหนดให้ผู้ควบคุมระบบลงคะแนนใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor authentication)

ข้อกำหนด	คำอธิบาย
	• ระบบการลงคะแนนต้องมีกระบวนการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูลยืนยันตัวตน เช่น การเข้ารหัส การแฮช เป็นต้น • หากระบบการลงคะแนนใช้วิธีการยืนยันตัวตนด้วยรหัสผ่าน ระบบการลงคะแนนต้องสามารถกำหนดหรือตั้งค่าความเข้มงวดและการหมดอายุของรหัสผ่านได้ • ควรจัดทำนโยบายหรือเอกสารที่ระบุการตั้งค่ารหัสผ่านที่มั่นคงปลอดภัย
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	• ต้องแสดงนโยบายการควบคุมการเข้าถึงที่เกี่ยวกับการกำหนดสิทธิการเข้าถึงของระบบการลงคะแนน • ต้องกำหนดกระบวนการควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิพิเศษอย่างเข้มงวด • ต้องแสดงหลักฐานให้เห็นถึงสิทธิการเข้าถึงของสิทธิพิเศษ โดยจะต้องปฏิเสธการเข้าถึงฟังก์ชันและข้อมูล เว้นแต่จะได้รับอนุญาตอย่างชัดเจน • ระบบการลงคะแนนต้องสามารถแยกบทบาทหน้าที่ของผู้ใช้งานได้อย่างชัดเจน เช่น ผู้ควบคุมระบบ ผู้ใช้งานหรือผู้มีสิทธิลงคะแนน เจ้าหน้าที่ปฏิบัติงานที่เกี่ยวข้อง เป็นต้น • ต้องแสดงหลักฐานให้เห็นถึงการกำหนดสิทธิการเข้าถึงในแต่ละบทบาทของผู้ใช้งาน เช่น Authorize Matrix เป็นต้น
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	• ระบบการลงคะแนนต้องสามารถกำหนดระยะเวลาของเซสชันและระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมภายในระยะเวลาที่กำหนด • ระบบการลงคะแนนต้องกำหนดให้ผู้ใช้งานยืนยันตัวตนซ้ำ กรณีครบกำหนดระยะเวลาของเซสชันและผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) • กรณีที่มีการยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนต้องสามารถตั้งค่าระงับการยืนยันตัวตนในช่วงระยะเวลาหนึ่งได้ ก่อนจะให้ยืนยันตัวตนครั้งต่อไป เช่น เมื่อใส่รหัสผ่านผิด 3 ครั้ง ระบบจะระงับการใช้งานทันที โดยจะสามารถยืนยันตัวตนใหม่ได้เมื่อครบ 3 นาที • ระบบการลงคะแนนต้องสามารถกำหนดให้ผู้ควบคุมระบบตั้งค่าระยะเวลาระงับการใช้งาน (lockout duration) ระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ได้

12. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย

ข้อกำหนด	คำอธิบาย
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	• ต้องมีมาตรการป้องกันการเข้าถึงทางกายภาพของระบบสารสนเทศที่เกี่ยวข้องกับระบบการลงคะแนน • ต้องแสดงหลักฐานให้เห็นว่ามีการรักษาความมั่นคงปลอดภัยด้านสภาพแวดล้อมทางกายภาพที่เกี่ยวข้องกับระบบลงคะแนน เช่น ขั้นตอนสำหรับการปฏิบัติงานในพื้นที่มั่นคงปลอดภัยที่เกี่ยวข้องกับระบบลงคะแนน ระบบล็อคที่มั่นคงปลอดภัย ระบบสัญญากันขโมย สัญญาณแจ้งเตือนเมื่อเกิดเหตุเพลิงไหม้ ถังดับเพลิง ระบบกล้องวงจรปิด ระบบป้องกันน้ำท่วม ระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับและอื่น ๆ เป็นต้น

13. การคุ้มครองข้อมูล (Data Protection)

วัตถุประสงค์ เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

ข้อกำหนด	คำอธิบาย
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนน จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	• มีการจำกัดผู้ที่สามารถปรับแต่งการตั้งค่าของระบบการลงคะแนนและการตั้งค่าระบบเครือข่าย • ผู้ให้บริการควรมีกระบวนการควบคุม/จัดการสิทธิผู้ควบคุมระบบการลงคะแนน โดยมีกระบวนการพิสูจน์และยืนยันตัวตนในการเข้าใช้งานระบบลงคะแนน • มีการรักษาความครบถ้วนของบันทึกการลงคะแนน (vote records) เช่น การแฮช และการเข้ารหัสลับ
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	• ระบบการลงคะแนนต้องมีการตรวจสอบความครบถ้วนของผลลงคะแนนที่ถูกเข้ารหัสลับไว้ • ระบบการลงคะแนนต้องมีการบันทึกและแสดงข้อผิดพลาดที่ตรวจพบได้ • กรณีตรวจพบข้อผิดพลาดต้องไม่นำคะแนนมานับเป็นผลรวม
13.3 – ระบบการลงคะแนนใช้อัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่เป็นมาตรฐาน	• ระบบการลงคะแนนต้องมีการกำหนดโมดูลการเข้ารหัสลับ (cryptographic module) ให้เป็นไปตามมาตรฐาน เช่น FIPS 140 Security Requirements for Cryptographic Modules • อัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่ใช้ในกระบวนการเข้ารหัสลับของระบบลงคะแนน และการบริหารจัดการกุญแจ ต้องเป็นไปตามมาตรฐาน เช่น NIST Special Publication 800-57 Part 1 Recommendation for Key Management: Part 1 – General
13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality)	• ควรกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่ายครอบคลุมการเข้ารหัสลับข้อมูลทั้งหมดระหว่างการรับส่งผ่านเครือข่าย • ต้องมีการเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย (data-in-transit encryption)

ข้อกำหนด	คำอธิบาย
ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด	• การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย เช่น มีการเทคโนโลยีการเข้ารหัสข้อมูล TLS เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน หรือมีการใช้ IPsec VPN สำหรับป้องกันการเชื่อมต่อเครือข่ายภายในสำหรับระบบการลงคะแนน รวมถึงกรณีการใช้ SSL VPN สำหรับเจ้าหน้าที่ผู้ดูแลระบบสำหรับบริหารจัดการระบบการลงคะแนน

14. การรักษาความครบถ้วนของระบบ (System Integrity)

<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงาน และไม่มีการแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือโดยไม่ตั้งใจ

ข้อกำหนด	คำอธิบาย
14.1 – ระบบการลงคะแนนใช้การควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อรับมือภัยคุกคามหรือช่องโหว่ด้านความมั่นคงปลอดภัย	• ต้องแสดงหลักฐานให้เห็นว่า มีขั้นตอนการปฏิบัติหรือวิธีการประเมินความเสี่ยง (risk assessment) สำหรับระบบการลงคะแนน และจัดทำเป็นเอกสาร โดยควรครอบคลุมหัวข้ออย่างน้อยดังนี้ 1) การกำหนดเกณฑ์การประเมินความเสี่ยง 2) การกำหนดเกณฑ์การยอมรับความเสี่ยง 3) การระบุความเสี่ยงด้านความมั่นคงปลอดภัย 4) วิธีการควบคุมที่มีในปัจจุบัน (Existing Control) 5) ระบุผู้เป็นเจ้าของความเสี่ยง 6) การวิเคราะห์ความเสี่ยงโดยการประเมินผลกระทบและโอกาสที่จะเกิดขึ้นรวมถึงกำหนดระดับค่าความเสี่ยง 7) กำหนดเกณฑ์และมาตรการในการจัดการความเสี่ยง (Risk Treatment) • การควบคุมในหลายระดับชั้น (multiple layers of controls) ซึ่งครอบคลุมระดับ ข้อมูล เครือข่าย แอปพลิเคชัน โดยอาจใช้วิธีการควบคุมทางกายภาพ ทางเทคนิค หรือกระบวนการ เช่น กระบวนการเข้ารหัสลับ (cryptography) การป้องกันมัลแวร์ (malware) การตั้งค่าไฟร์วอลล์ (firewall) และการตั้งค่าระบบ (system configurations) รวมถึงมาตรการด้านการบริหารจัดการกระบวนการอื่น ๆ ที่เกี่ยวข้องกับระบบการลงคะแนน • ต้องแสดงหลักฐานให้เห็นว่า มีการดำเนินการตามขั้นตอนการปฏิบัติหรือวิธีการประเมินความเสี่ยง (risk assessment) สำหรับระบบการลงคะแนน
14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น	• ต้องแสดงหลักฐานให้เห็นว่า ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) อย่างน้อยควรมีการควบคุมดังนี้

	1) การติดตั้งซอร์สโค้ด ซอฟต์แวร์ หรือสั่งการประมวลผลกระบวนการที่ไม่เกี่ยวข้อง รวมถึงการทบทวนซอร์สโค้ด (Source code review) 2) ปิดการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน 3) ปฏิบัติตามข้อแนะนำการตั้งค่าด้านความปลอดภัย(Secure configuration and hardening documentation) ทั้งในระบบปฏิบัติการ เครือข่าย และแอปพลิเคชัน • มีการทบทวนซอฟต์แวร์เพื่อตรวจสอบว่าไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และ มีการเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น หรือ ส่วนที่ต้องการเรียกใช้เท่านั้น • ต้องมีแผนการบริการจัดการช่องโหว่ที่เป็นที่รู้จัก ซึ่งควรมีขั้นตอนอย่างน้อย ได้แก่ วิธีการระบุและจัดการกับช่องโหว่ การเปิดเผยช่องโหว่ที่พบ แผนการจัดการแพตช์ (patch management plan) และการรับ-ส่งรายงานช่องโหว่ที่พบให้ผู้ที่เกี่ยวข้องทราบ

15. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring)

<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน

ข้อกำหนด	คำอธิบาย
15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ	• ต้องแสดงหลักฐานให้เห็นว่า ระบบการลงคะแนนสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งต้องครอบคลุมเหตุการณ์ที่เกี่ยวข้องดังต่อไปนี้เป็นอย่างน้อย 1) สถานะการทำงานปกติและความผิดปกติของระบบปฏิบัติการ ระบบเครือข่าย ระบบฐานข้อมูล และระบบการลงคะแนน 2) การยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน 3) การจัดการระบบเครือข่าย เช่น การเปิด และ ปิดการเชื่อมต่อ 4) การจัดการซอฟต์แวร์ เช่น การติดตั้ง อัปเดต การแก้ไขไฟล์ตั้งค่า 5) ฟังก์ชันการลงคะแนน เช่น การเปิดและปิดการลงคะแนน การยกเลิกการลงคะแนน การลงคะแนนสำเร็จและไม่สำเร็จ • ระบบการลงคะแนนต้องสามารถนำออกบันทึกเหตุการณ์ (export Logs) ที่เกิดขึ้นได้ในรูปแบบที่สามารถอ่านได้ (สัมพันธ์กับข้อ 3.8.1)
15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	• ต้องแสดงหลักฐานให้เห็นว่า มีการแจ้งเตือนเพื่อแจ้งผู้ใช้งานในทันทีกรณีระบบการลงคะแนนข้อผิดพลาดเกิดขึ้น และสามารถสร้างรายงานข้อผิดพลาด (error report) ได้ • ต้องแสดงหลักฐานให้เห็นว่า มีการแจ้งเตือนเพื่อแจ้งผู้ดูแลระบบกรณีระบบการลงคะแนนข้อผิดพลาดเกิดขึ้น และสามารถสร้างรายงานข้อผิดพลาด (error report) ได้

ข้อกำหนด	คำอธิบาย
	• เอกสารเกี่ยวกับระบบการลงคะแนน ต้องมีขั้นตอนการจัดการข้อผิดพลาดในระบบการลงคะแนน ทั้งสำหรับผู้ใช้งาน ผู้ดูแลระบบ และผู้ควบคุมระบบการลงคะแนน
15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	• ต้องแสดงหลักฐานให้เห็นว่า ระบบการลงคะแนนมีมาตรการป้องกันมัลแวร์ (malware) เช่น การติดตั้งและปรับปรุงความสามารถของระบบป้องกันและตรวจจับมัลแวร์อย่างสม่ำเสมอเพียงพอต่อความเสี่ยงและภัยคุกคาม • ต้องแสดงหลักฐานให้เห็นว่า มีการจัดทำเอกสารคู่มือเกี่ยวกับการบริหารจัดการหรือการรับมือมัลแวร์ สำหรับผู้ดูแลระบบการลงคะแนน • ต้องแสดงหลักฐานให้เห็นว่า ระบบการลงคะแนนสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ • ต้องแสดงหลักฐานให้เห็นว่า ระบบการลงคะแนนสามารถบันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ
15.4 – ระบบการลงคะแนนที่เชื่อมต่อเครือข่ายใช้วิธีการป้องกันการโจมตีทางเครือข่าย (network-based attack) ที่เหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี	• ต้องแสดงหลักฐานให้เห็นว่า มีสถาปัตยกรรมระบบเครือข่าย (network architecture) ทั้งภายในและระบบที่มาเชื่อมต่อระบบการลงคะแนน • ต้องแสดงหลักฐานให้เห็นว่า มีการจัดทำเอกสารหรือคู่มือการตั้งค่าความมั่นคงปลอดภัยเครือข่าย เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต เช่น • การปิดการเชื่อมต่อเครือข่ายที่ไม่จำเป็น หรือปฏิบัติตามแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย เช่น NIST Special Publication 800-44 Guidelines on Securing Public Web Servers เป็นต้น • ต้องแสดงหลักฐานให้เห็นว่า ระบบการลงคะแนนมีการกำหนด Rule และ Policy บนระบบหรืออุปกรณ์เครือข่าย เช่น ไฟล์วอล (Firewall) IDS IPS WAF และปรับปรุงอย่างสม่ำเสมอสอดคล้องตามความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้น

เอกสารอ้างอิง

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (Electronic Voting System) ขมธอ. 26-2564