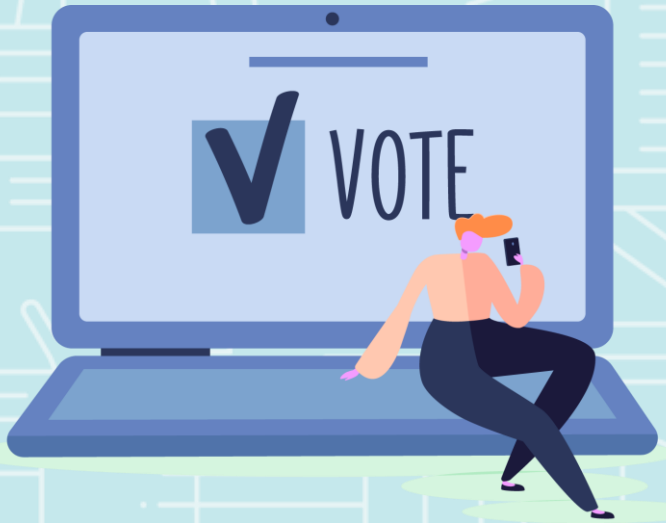
(ร่าง) ข้อเสนอแนะมาตรฐานฯ

ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

(Electronic Voting System)



มาตรฐานระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้เป็น**ข้อกำหนดของระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์**

- เพื่อให้ผู้ให้บริการระบบการลงคะแนนมีแนวทางในการพัฒนาระบบการลงคะแนนที่มีความสามารถด้าน**ฟังก์ชันการทำงาน**และ**ความมั่นคงปลอดภัยด้านสารสนเทศ**เป็นมาตรฐานเดียวกัน
- เพื่อสร้างความมั่นใจให้กับผู้ใช้งานในการใช้บริการระบบการลงคะแนน

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นเพียงแนวทางในการพัฒนาและปรับใช้ในการออกแบบระบบการลงคะแนนเพื่อให้สามารถใช้งานได้ครบถ้วนเท่านั้น ซึ่งแต่ละหน่วยงานสามารถนำไปปรับใช้ได้ตามความเหมาะสม

อย่างไรก็ตาม อาจไม่ครอบคลุมทุกประเด็นของการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เนื่องจากแต่ละหน่วยงานอาจจะมีข้อกำหนดอื่น ๆ เพิ่มเติมตามกฎหมายหรือหลักเกณฑ์ที่กำหนดไว้เป็นการเฉพาะ เช่น

- การรองรับการลงคะแนนจากหลายช่องทาง
- การลงคะแนนที่ผู้ลงคะแนนมีสิทธิลงคะแนนไม่เท่ากัน
- การอนุญาตให้เปลี่ยนตัวเลือกลงคะแนนหรือส่งผลลงคะแนนได้หลายครั้งจนกว่าจะปิดลงคะแนน

มาตรฐานระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

สามารถใช้ได้กับ ระบบการลงคะแนนสำหรับ :

- การลงคะแนนในการประชุมผ่านสื่ออิเล็กทรอนิกส์
- การลงคะแนนที่เป็นอิสระจากการประชุมผ่านสื่ออิเล็กทรอนิกส์
- การลงคะแนนโดยเปิดเผย ซึ่งใช้วิธีการที่สามารถระบุตัวผู้มีสิทธิลงคะแนนและสามารถทราบเจตนาในการลงคะแนนของบุคคลดังกล่าวได้
- การลงคะแนนลับ ซึ่งใช้วิธีการที่สามารถทราบจำนวนของผู้ลงคะแนนและผลรวมของการลงคะแนน โดยไม่สามารถระบุตัวของผู้ลงคะแนนได้เป็นการทั่วไป

ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้จะ**ไม่ครอบคลุมถึง**

- ข้อกำหนดเกี่ยวกับเครื่องลงคะแนนอิเล็กทรอนิกส์ (direct-recording electronic voting machine) หรือฮาร์ดแวร์ของผู้ลงคะแนน เช่น เครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ของผู้ลงคะแนน
- การเลือกตั้งระดับชาติ การเลือกตั้งระดับท้องถิ่น และการออกเสียงประชามติ ที่ดำเนินการโดยสำนักงานคณะกรรมการการเลือกตั้ง
- การเลือกตั้งสมาชิกสภาท้องถิ่นและผู้บริหารท้องถิ่น ที่ดำเนินการโดยกรมส่งเสริมการปกครองท้องถิ่น

โครงสร้างของเอกสาร

1. **ขอบข่าย**
2. **บทนิยาม**
3. **ข้อกำหนดของระบบการลงคะแนน**

ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน

3.1 การออกแบบระบบ
3.2 การพัฒนาระบบ
3.3 ความโปร่งใส
3.4 การเข้าถึงอย่างเท่าเทียมของผู้ลงคะแนน
3.5 การลงคะแนนตรงตามเจตนาของผู้ลงคะแนน
3.6 การใช้งานได้

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.7 การทำงานร่วมกัน
3.8 การตรวจสอบ
3.9 ความเป็นส่วนตัวของผู้ลงคะแนน
3.10 ความลับของคะแนนเสียง
3.11 การควบคุมการเข้าถึง
3.12 ความมั่นคงปลอดภัยทางกายภาพ
3.13 การคุ้มครองข้อมูล
3.14 การรักษาความครบถ้วนของระบบการลงคะแนน
3.15 การตรวจจับและการเฝ้าระวัง

อ้างอิง

[1] (ร่าง) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2564.

[2] United States Election Assistance Commission, "Voluntary Voting System Guidelines Version 2.0", 2021.

[3] United States Election Assistance Commission, "Voluntary Voting System Guidelines Version 1.1 Volume 1", 2015.

[4] Council of Europe, "E-voting handbook", October 2010.

ข้อกำหนดของระบบการลงคะแนน

แบ่งออกเป็น 15 หมวด

ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน

(จำนวน 6 หมวด)

1 

การออกแบบระบบ
(system design)

2 

การพัฒนาระบบ
(system implementation)

3 

ความโปร่งใส
(transparent)

4 

การเข้าถึงอย่างเท่าเทียมของผู้ลงคะแนน
(equivalent voter access)

5 

การลงคะแนนตรงตามเจตนาของผู้ลงคะแนน
(cast as intended)

6 

การใช้งานได้
(usable)

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

(จำนวน 9 หมวด)

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 

การรักษาความครบถ้วนของระบบการลงคะแนน
(system integrity)

15 

การตรวจจับและการเฝ้าระวัง
(detection and monitoring)

ข้อกำหนดเกี่ยวกับฟังชันการทำงาน

3.1 การออกแบบระบบ (System Design)

เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามขั้นตอนการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ

3.1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามหลักเกณฑ์ของกระบวนการลงคะแนน

3.1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง

3.1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ

3.2 การพัฒนาระบบ (System Implementation)

เพื่อให้ระบบการลงคะแนนมีการพัฒนาระบบโดยใช้แนวปฏิบัติที่ดี

3.2.1 – การพัฒนาระบบการลงคะแนนใช้แนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์

3.2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน (modular)

3.2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์

3.2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ

ข้อกำหนดเกี่ยวกับฟังชันการทำงาน

3.3 ความโปร่งใส (Transparent)

เพื่อให้ระบบการลงคะแนนและกระบวนการลงคะแนนมีการออกแบบที่มีความโปร่งใส

3.3.1 – เอกสารอธิบายการออกแบบ การทำงาน การเข้าถึง มาตรการความมั่นคงปลอดภัย และรายละเอียดอื่น ๆ ของระบบการลงคะแนนสามารถอ่านและทำความเข้าใจได้

3.3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนนทั้งทางกายภาพและดิจิทัล เตรียมไว้พร้อมสำหรับการตรวจสอบระบบ

3.3.3 – บุคคลภายนอกสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน

3.4 การเข้าถึงอย่างเท่าเทียมของผู้ลงคะแนน (Equivalent Voter Access)

เพื่อให้ผู้ลงคะแนนทุกคนสามารถเข้าถึงและใช้งานระบบการลงคะแนนได้อย่างเท่าเทียม

3.4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ

3.4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ

ข้อกำหนดเกี่ยวกับฟังชันการทำงาน

3.5 การลงคะแนนตรงตามเจตนาของผู้ลงคะแนน (Cast as Intended)

เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้

3.5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนนที่มีความหลากหลาย และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคลให้ตรงกับความต้องการของผู้ลงคะแนน

3.5.2 – ผู้ลงคะแนนและผู้ควบคุมระบบการลงคะแนนสามารถใช้การควบคุมฟังก์ชันการทำงานได้อย่างถูกต้อง และผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง

3.5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงคำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด

3.6 การใช้งานได้ (Usable)

เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้จริง

3.6.1 – ระบบการลงคะแนนมีการประเมินความสามารถด้านการใช้งานกับตัวแทนของผู้ลงคะแนนที่มีความหลากหลาย

3.6.2 – ระบบการลงคะแนนมีการประเมินความสามารถด้านการใช้งานกับตัวแทนของผู้ควบคุมระบบการลงคะแนน

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.7 การทำงานร่วมกัน (Interoperable)

เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน

3.7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐานที่ใช้กันอย่างแพร่หลาย

3.7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐานที่ใช้กันอย่างแพร่หลาย

3.8 การตรวจสอบ (Auditable)

เพื่อให้ระบบการลงคะแนนสามารถตรวจสอบได้และมีหลักฐานของการลงคะแนน

3.8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.9 ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy)

เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและเป็นอิสระ

3.9.1 – กระบวนการลงคะแนนมีการรักษาความเป็นส่วนตัวของผู้ลงคะแนนในการทำเครื่องหมายลงคะแนน การตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนน

3.9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นอิสระ โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น

3.10 ความลับของคะแนนเสียง (Vote Secrecy)

(กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการปกป้องความลับในการลงคะแนนของผู้ลงคะแนน

3.10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน

3.10.2 – ระบบการลงคะแนนไม่จัดเก็บหรือจัดทำข้อมูลเกี่ยวกับ ผู้ลงคะแนนหรือข้อมูลอื่น ๆ ซึ่งสามารถใช้เชื่อมโยงอัตลักษณ์ของ ผู้ลงคะแนนกับเจตนาหรือตัวเลือกลงคะแนนของผู้ลงคะแนน

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.11 การควบคุมการเข้าถึง (Access Control)

เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ควบคุมระบบการลงคะแนน ผู้ใช้งาน และอุปกรณ์ก่อนจะอนุญาตให้มีสิทธิเข้าถึงฟังก์ชันการทำงานที่สำคัญ

3.11.1 – ระบบการลงคะแนนสามารถบันทึก เฝ้าระวัง ทบทวน และปรับเปลี่ยนสิทธิการเข้าถึง บัญชีผู้ใช้งาน กิจกรรม และการอนุญาตให้เข้าถึง

3.11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล

3.11.3 – ระบบการลงคะแนนรองรับวิธีการยืนยันตัวตน ที่มั่นคงปลอดภัย เพื่อยืนยันตัวตนของผู้ใช้งานที่ได้รับอนุญาต และรวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับการดำเนินการที่สำคัญ

3.11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่

3.11.5 – ระบบการลงคะแนนมีการเพิกถอนสิทธิการเข้าถึงข้อมูลเมื่อไม่ต้องการใช้งาน

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.12 ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย

3.12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ

3.13 การคุ้มครองข้อมูล (Data Protection)

เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึง แก้ไขเปลี่ยนแปลง หรือลบโดยไม่ได้รับอนุญาต

3.13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) บันทึกการลงคะแนน ข้อมูลที่ส่งออก หรือบันทึกการตรวจสอบ จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

3.13.2 – บันทึกการลงคะแนนสามารถตรวจสอบแหล่งที่มาและความครบถ้วนของข้อมูลได้

3.13.3 – ระบบการลงคะแนนใช้อัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่เป็นมาตรฐาน

3.13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.14 การรักษาความครบถ้วนของระบบการลงคะแนน (System Integrity)

เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงานที่กำหนด ไม่มีการดัดแปลงหรือแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือโดยไม่ตั้งใจ

3.14.1 – ระบบการลงคะแนนใช้การควบคุมหลายด้าน (multiple layers of controls) เพื่อรับมือการโจมตีหรือช่องโหว่ด้านความมั่นคงปลอดภัย

3.14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น และใช้การควบคุมทางเทคนิคอื่น ๆ

ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.15 การตรวจจับและการเฝ้าระวัง (Detection and Monitoring)

เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน

3.15.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมที่สำคัญด้วยวิธีการบันทึกเหตุการณ์ ซึ่งอยู่ในรูปแบบที่เหมาะสมสำหรับการประมวลผลอัตโนมัติ

3.15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น

3.15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)

3.15.4 – ระบบการลงคะแนนที่เชื่อมต่อเครือข่ายใช้วิธีการป้องกันการโจมตีทางเครือข่าย (network-based attack) ที่เหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี