ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. [x-xxxx]

ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

ELECTRONIC VOTING SYSTEM

เวอร์ชัน 0.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.240.99

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

ขมธอ. [x-xxxx]

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ กรุณาเลือกวันที่ประกาศ

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นายกำชัย จัตตานนท์	
นายนิรันดร์ ประจวบเหมาะ	กรมสรรพากร
นางสุภิดา บรรเทาทุกข์	
นายคงฤทธิ์ จันทริก	สภาผู้ส่งสินค้าทางเรือแห่งประเทศไทย
นายภาวุธ พงษ์วิทยภานุ	สมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทย
นายธานินทร์ ตันกิติบุตร	สมาคมผู้ให้บริการอินเทอร์เน็ตไทย
นายวรพจน์ ธาราศิริสกุล	สมาคมฟินเทคประเทศไทย
นายปกรณ์ ลี้สกุล	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงานและเลขานุการ

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ
ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

นางพงศ์พล ไผ่อรุณรัตน์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายณัชพล วรกิจปรีดา	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดของระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เพื่อให้ผู้ให้บริการระบบการลงคะแนนมีแนวทางในการพัฒนาระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศเป็นมาตรฐานเดียวกัน

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
อีเมล: estandard.center@etda.or.th
เว็บไซต์: www.etda.or.th

คำนำ

ด้วยปัจจุบัน การประชุมผ่านสื่ออิเล็กทรอนิกส์สามารถดำเนินการได้ตามที่พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 กำหนดรับรองไว้ โดยข้อกำหนดหนึ่งตามกฎหมายดังกล่าวกำหนดให้ผู้มีหน้าที่จัดการประชุมต้องจัดให้ผู้ร่วมประชุมสามารถลงคะแนนได้ ทั้งการลงคะแนนโดยเปิดเผยและการลงคะแนนลับ ทั้งนี้ ผู้มีหน้าที่จัดการประชุมอาจใช้ระบบควบคุมการประชุม และ/หรือระบบการลงคะแนน ของตนเองหรือของผู้ให้บริการ ในกรณีที่จัดให้มีการลงคะแนนผ่านระบบการลงคะแนน ผู้มีหน้าที่จัดการประชุมต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้อง โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความครบถ้วน และการรักษาสภาพพร้อมใช้งาน ตามความในประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 และที่แก้ไขเพิ่มเติม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้จัดทำข้อเสนอแนะมาตรฐานระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เพื่อเป็นข้อกำหนดสำหรับผู้ให้บริการระบบการลงคะแนนในการพัฒนาระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศเป็นมาตรฐานเดียวกัน และเพื่อสร้างความมั่นใจให้กับผู้ใช้งานในการใช้บริการระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความน่าเชื่อถือ

ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์สามารถนำมาใช้กับการลงคะแนนในการประชุมผ่านสื่ออิเล็กทรอนิกส์ หรือการลงคะแนนที่เป็นอิสระจากการประชุมผ่านสื่ออิเล็กทรอนิกส์ก็ได้ ตัวอย่างของการประชุมที่สามารถอาศัยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์เพื่ออำนวยความสะดวกให้ผู้ลงคะแนนสามารถลงคะแนนจากสถานที่ใดก็ได้ เช่น การประชุมผู้ถือหุ้นของบริษัทจำกัดหรือบริษัทมหาชนจำกัด การประชุมใหญ่ของนิติบุคคลอาคารชุดและนิติบุคคลหมู่บ้านจัดสรร การประชุมใหญ่ของสมาคมตามกฎหมายแพ่งและพาณิชย์ หรือการประชุมอื่น ๆ ที่มีผู้ร่วมประชุมจำนวนมาก

สารบัญ

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

เพื่อเป็นข้อกำหนดของระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เพื่อให้ผู้ให้บริการระบบการลงคะแนนมีแนวทางในการพัฒนาระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศเป็นมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๕ (๕) แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เลขที่ ขมธอ. [x-xxxx] ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ [กรุณาระบุวันที่ประกาศ]

( )

ผู้อำนวยการ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นข้อกำหนดของระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เพื่อให้ผู้ให้บริการระบบการลงคะแนนมีแนวทางในการพัฒนาระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความสามารถด้านฟังก์ชันการทำงานและความมั่นคงปลอดภัยด้านสารสนเทศเป็นมาตรฐานเดียวกัน นอกจากนี้ ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ที่มีความน่าเชื่อถือจะช่วยสร้างความมั่นใจให้กับผู้ใช้งานในการใช้บริการระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นเพียงแนวทางในการพัฒนาและปรับใช้ในการออกแบบระบบการลงคะแนนเพื่อให้สามารถใช้งานได้ครบถ้วนเท่านั้น ซึ่งผู้ให้บริการระบบการลงคะแนนหรือผู้ควบคุมระบบการลงคะแนนของแต่ละหน่วยงานสามารถนำไปปรับใช้ได้ตามความเหมาะสม อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้อาจไม่ครอบคลุมทุกประเด็นของการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ เนื่องจากระบบการลงคะแนนหรือการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ของแต่ละหน่วยงานอาจจะมีข้อกำหนดอื่น ๆ เพิ่มเติมตามกฎหมายหรือหลักเกณฑ์ที่กำหนดไว้เป็นการเฉพาะ เช่น การรองรับการลงคะแนนจากหลายช่องทาง การลงคะแนนที่ผู้ลงคะแนนมีสิทธิลงคะแนนไม่เท่ากัน หรือการอนุญาตให้เปลี่ยนตัวเลือกลงคะแนนหรือส่งผลลงคะแนนได้หลายครั้งจนกว่าจะปิดลงคะแนน ดังนั้น แต่ละหน่วยงานควรดำเนินการตามข้อกำหนดอื่น ๆ ที่เกี่ยวข้องด้วย

ข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้ได้กับ

- ระบบการลงคะแนนสำหรับการลงคะแนนในการประชุมผ่านสื่ออิเล็กทรอนิกส์
- ระบบการลงคะแนนสำหรับการลงคะแนนที่เป็นอิสระจากการประชุมผ่านสื่ออิเล็กทรอนิกส์
- ระบบการลงคะแนนสำหรับการลงคะแนนโดยเปิดเผย ซึ่งใช้วิธีการที่สามารถระบุตัวผู้มีสิทธิลงคะแนนและสามารถทราบเจตนาในการลงคะแนนของบุคคลดังกล่าวได้
- ระบบการลงคะแนนสำหรับการลงคะแนนลับ ซึ่งใช้วิธีการที่สามารถทราบจำนวนของผู้ลงคะแนนและผลรวมของการลงคะแนน โดยไม่สามารถระบุตัวของผู้ลงคะแนนได้เป็นการทั่วไป

ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้จะไม่ครอบคลุมถึง

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

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 ระบบการลงคะแนน หมายถึง ระบบเครือข่ายคอมพิวเตอร์ และ/หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เชื่อมโยงกันเป็นเครือข่ายและมีการสื่อสารข้อมูลกันโดยใช้เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือการโทรคมนาคม หรือวิธีการอื่นในลักษณะทำนองเดียวกัน เพื่อให้ผู้ลงคะแนนสามารถใช้งานสำหรับการลงคะแนนได้ [1] ทั้งนี้ ระบบการลงคะแนนจะไม่รวมถึงฮาร์ดแวร์ของผู้ลงคะแนน เช่น เครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ของผู้ลงคะแนน

2.2 ผู้ควบคุมระบบการลงคะแนน หมายถึง ผู้ทำหน้าที่ดูแลและบริหารจัดการระบบการลงคะแนน โดยอาจเป็นบุคคลเดียวกับผู้ทำหน้าที่ดูแลและบริหารจัดการระบบควบคุมการประชุมหรือไม่ก็ได้ [1]

3. ข้อกำหนดของระบบการลงคะแนน

ข้อกำหนดของระบบการลงคะแนนแบ่งออกเป็น 15 หมวด ซึ่งครอบคลุมทั้งข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน (จำนวน 6 หมวด) และข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ (จำนวน 9 หมวด) ดังต่อไปนี้

<u>ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน</u>

(1) การออกแบบระบบ (system design)
(2) การพัฒนาระบบ (system implementation)
(3) ความโปร่งใส (transparent)
(4) การเข้าถึงอย่างเท่าเทียมของผู้ลงคะแนน (equivalent voter access)
(5) การลงคะแนนตรงตามเจตนาของผู้ลงคะแนน (cast as intended)
(6) การใช้งานได้ (usable)

<u>ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ</u>

(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)

ข้อกำหนดของระบบการลงคะแนนทั้งหมด 15 หมวด มีรายละเอียดเป็นไปตามหัวข้อ 0 - 3.15

3.1 การออกแบบระบบ (System Design)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามขั้นตอนการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ

ข้อกำหนด	คำอธิบาย
3.1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามหลักเกณฑ์ของกระบวนการลงคะแนน	ระบบการลงคะแนนมีฟังก์ชันการทำงานที่จำเป็น ซึ่งครอบคลุมการเตรียมข้อมูลสำหรับการลงคะแนน การตั้งค่าและตรวจสอบระบบการลงคะแนน การเปิดลงคะแนน การลงคะแนน การบันทึกตัวเลือกลงคะแนน การปิดลงคะแนน และการรายงานผลรวมของการลงคะแนน
3.1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมจำนวนมาก (maximum volume) และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)
3.1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้ให้บริการระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบ (tester) ของผู้ให้บริการระบบการลงคะแนน

3.2 การพัฒนาระบบ (System Implementation)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการพัฒนาระบบโดยใช้แนวปฏิบัติที่ดี

ข้อกำหนด	คำอธิบาย
3.2.1 – การพัฒนาระบบการลงคะแนนใช้แนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์	ระบบการลงคะแนนใช้ภาษาโปรแกรมและรูปแบบการเขียนโปรแกรมที่เป็นที่ยอมรับในการพัฒนาซอฟต์แวร์ให้มีความถูกต้องสมบูรณ์และความมั่นคงปลอดภัย
3.2.2 - โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน (modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ
3.2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้ (self-modifying code)
3.2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน

3.3 ความโปร่งใส (Transparent)

<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนและกระบวนการลงคะแนนมีการออกแบบที่มีความโปร่งใส

ข้อกำหนด	คำอธิบาย
3.3.1 – เอกสารอธิบายการออกแบบ การทำงาน การเข้าถึง มาตรการความมั่นคงปลอดภัย และรายละเอียดอื่น ๆ ของระบบการลงคะแนนสามารถอ่านและทำความเข้าใจได้	ผู้ให้บริการระบบการลงคะแนนจัดทำเอกสารเกี่ยวกับระบบการลงคะแนน โดยมีรายละเอียดดังต่อไปนี้ (1) ภาพรวมของระบบ (system overview) (2) ประสิทธิภาพของระบบ (system performance) (3) ความมั่นคงปลอดภัยของระบบ (system security) (4) การติดตั้งซอฟต์แวร์ (software installation) (5) การทำงานของระบบ (system operations) (6) การบำรุงรักษาระบบ (system maintenance) (7) การฝึกอบรม (training)
3.3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนนทั้งทางกายภาพและดิจิทัล เตรียมไว้พร้อมสำหรับการตรวจสอบระบบ	ผู้ให้บริการระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ
3.3.3 – บุคคลภายนอกสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	ผู้ให้บริการระบบการลงคะแนนจัดทำเอกสารสำหรับเปิดเผยต่อสาธารณะ โดยอธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)

3.4 การเข้าถึงอย่างเท่าเทียมของผู้ลงคะแนน (Equivalent Voter Access)

<u>วัตถุประสงค์</u> เพื่อให้ผู้ลงคะแนนทุกคนสามารถเข้าถึงและใช้งานระบบการลงคะแนนได้อย่างเท่าเทียม

ข้อกำหนด	คำอธิบาย
3.4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงภาพและเสียง) รูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัส) ในลักษณะที่สอดคล้องกัน
3.4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ	รูปแบบการแสดงผล (display format) แสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน และไม่ทำให้เกิดอคติกับตัวเลือกลงคะแนนใด ๆ ที่นำเสนอต่อผู้ลงคะแนน

3.5 การลงคะแนนตรงตามเจตนาของผู้ลงคะแนน (Cast as Intended)

<u>วัตถุประสงค์</u> เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้

ข้อกำหนด	คำอธิบาย
3.5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนนที่มีความหลากหลาย และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงกับความต้องการของผู้ลงคะแนน	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล (preference setting) ตามความต้องการของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษรและสีของภาพ
3.5.2 – ผู้ลงคะแนนและผู้ควบคุมระบบการลงคะแนนสามารถใช้การควบคุมฟังก์ชันการทำงานได้อย่างถูกต้อง และผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการทำงานของระบบ เช่น รูปแบบการแสดงผลของข้อมูล การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้าถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ นอกจากนี้ ผู้ลงคะแนนและผู้ควบคุมระบบการลงคะแนนต้องสามารถใช้การควบคุมฟังก์ชันการทำงานได้อย่างถูกต้อง รวมถึงระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ
3.5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงคำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน คำแนะนำ และข้อความจากระบบ ด้วยภาษาที่ชัดเจนและอ่านง่าย รวมถึงการป้องกันการวางตำแหน่งที่อาจทำให้เกิดความสับสน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต การเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) ก่อนจะส่งผลลงคะแนน การแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว และการแสดงคำแนะนำและข้อความที่ชัดเจนและเข้าใจได้สำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ

3.6 การใช้งานได้ (Usable)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้จริง

ข้อกำหนด	คำอธิบาย
3.6.1 – ระบบการลงคะแนนมีการประเมินความสามารถด้านการใช้งานกับตัวแทนของผู้ลงคะแนนที่มีความหลากหลาย	ผู้ให้บริการระบบการลงคะแนนมีการทดสอบความสามารถด้านการใช้งาน (usability testing) กับตัวแทนของผู้ลงคะแนนที่จะใช้ระบบการลงคะแนน รวมถึงกิจกรรมทั้งหมดของผู้ลงคะแนนในกระบวนการลงคะแนน ทั้งนี้ การทดสอบกับตัวแทนของผู้ลงคะแนนที่มีความหลากหลาย ซึ่งอาจรวมถึงบุคคลที่มีความบกพร่องทางการมองเห็น ทำให้มั่นใจได้ว่าระบบการลงคะแนนสามารถใช้งานได้จริงสำหรับผู้คะแนนทุกคน
3.6.2 – ระบบการลงคะแนนมีการประเมินความสามารถด้านการใช้งานกับตัวแทนของผู้ควบคุมระบบการลงคะแนน	ผู้ให้บริการระบบการลงคะแนนมีการทดสอบความสามารถด้านการใช้งาน (usability testing) กับตัวแทนของผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถเรียนรู้ ทำความเข้าใจ และปฏิบัติงานได้สำเร็จ

3.7 การทำงานร่วมกัน (Interoperable)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน

ข้อกำหนด	คำอธิบาย
3.7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐานที่ใช้กันอย่างแพร่หลาย	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐานที่ใช้กันอย่างแพร่หลาย
3.7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐานที่ใช้กันอย่างแพร่หลาย	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้รูปแบบมาตรฐานที่ใช้กันอย่างแพร่หลายในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่าง ๆ

3.8 การตรวจสอบ (Auditable)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนสามารถตรวจสอบได้และมีหลักฐานของการลงคะแนน

ข้อกำหนด	คำอธิบาย
3.8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	ผลลงคะแนนที่ได้จากการบันทึกตัวเลือกลงคะแนนของผู้ลงคะแนน มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลได้ (tamper-evidence) ระบบการลงคะแนนเปิดโอกาสให้ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกไป แจ้งข้อผิดพลาดที่เกิดขึ้นกับผลลงคะแนน และเริ่มต้นลงคะแนนใหม่หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน ระบบการลงคะแนนต้องสร้างรายงานที่จะช่วยให้ผู้ตรวจสอบภายนอก (external auditor) สามารถตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนอย่างถูกต้อง รวมถึงผู้ให้บริการระบบการลงคะแนนจัดทำเอกสารขั้นตอนสำหรับใช้ตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนอย่างถูกต้อง

3.9 ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy)

วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและเป็นอิสระ

ข้อกำหนด	คำอธิบาย
3.9.1 – กระบวนการลงคะแนนมีการรักษาความเป็นส่วนตัวของผู้ลงคะแนนในการทำเครื่องหมายลงคะแนน การตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนน	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่เปิดเผยตัวเลือกลงคะแนนหรือรูปแบบการแสดงผลต่อบุคคลอื่น เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน
3.9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นอิสระ โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่าส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น

3.10 ความลับของคะแนนเสียง (Vote Secrecy)

<u>วัตถุประสงค์</u> (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการปกป้องความลับในการลงคะแนนของผู้ลงคะแนน

ข้อกำหนด	คำอธิบาย
3.10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	กรณีการลงคะแนนลับ ระบบการลงคะแนนต้องไม่รับ ประมวลผล จัดเก็บ หรือแสดงข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว ในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว
3.10.2 – ระบบการลงคะแนนไม่จัดเก็บหรือจัดทำข้อมูลเกี่ยวกับผู้ลงคะแนนหรือข้อมูลอื่น ๆ ซึ่งสามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับเจตนาหรือตัวเลือกลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับตัวเลือกลงคะแนน อย่างไรก็ตาม ในกรณีที่ต้องการพิจารณาการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนนสามารถใช้การเชื่อมโยงโดยอ้อม (indirect voter association) ที่เชื่อมโยงผู้ลงคะแนนกับตัวเลือกลงคะแนนที่ถูกเข้ารหัสลับไว้เท่านั้น หลังจากพิจารณาแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน (เช่น พิจารณาจากการตรวจสอบลายมือชื่อดิจิทัล) ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับตัวเลือกลงคะแนนออก จากนั้น จึงถอดรหัสลับตัวเลือกลงคะแนนที่ถูกเข้ารหัสลับ และนำไปนับคะแนนเป็นผลรวมของการลงคะแนน ระบบการลงคะแนนต้องไม่มีข้อมูลใด ๆ ที่สามารถนำมาใช้เพื่อหาลำดับของการส่งผลลงคะแนน หรือข้อมูลใด ๆ ที่ระบุตัวผู้ลงคะแนนได้ นอกจากนี้ ผลรวมของการลงคะแนนต้องไม่มีข้อมูลที่ระบุตัวผู้ลงคะแนน และต้องไม่สามารถสร้างลำดับของการส่งผลลงคะแนนกลับมาใหม่ได้

3.11 การควบคุมการเข้าถึง (Access Control)

<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ควบคุมระบบการลงคะแนน ผู้ใช้งาน และอุปกรณ์ ก่อนจะอนุญาตให้มีสิทธิเข้าถึงฟังก์ชันการทำงานที่สำคัญ

ข้อกำหนด	คำอธิบาย
3.11.1 – ระบบการลงคะแนนสามารถบันทึก เฝ้าระวัง ทบทวน และปรับเปลี่ยนสิทธิการเข้าถึง บัญชีผู้ใช้งาน กิจกรรม และการอนุญาตให้เข้าถึง	ระบบการลงคะแนนมีการบันทึก เฝ้าระวัง ทบทวน และปรับเปลี่ยนตามความจำเป็น เกี่ยวกับสิทธิการเข้าถึง บัญชีผู้ใช้งาน กิจกรรม และการอนุญาตให้เข้าถึง เพื่อให้มีหลักฐานสำหรับพิจารณาในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งาน เปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และลบบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้

ข้อกำหนด	คำอธิบาย
	สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถเฝ้าระวังและทบทวนการควบคุมการเข้าถึงอย่างต่อเนื่อง
3.11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนน และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดรายชื่อผู้ใช้งานที่ได้รับอนุญาต กำหนดกลุ่มหรือบทบาทให้กับผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละกลุ่มหรือบทบาทของผู้ใช้งาน
3.11.3 – ระบบการลงคะแนนรองรับวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย เพื่อยืนยันตัวตนของผู้ใช้งานที่ได้รับอนุญาต และรวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับการดำเนินการที่สำคัญ	ระบบการลงคะแนนใช้วิธีการควบคุมการเข้าถึง เพื่ออนุญาตการเข้าถึงให้เฉพาะที่ได้รับอนุญาตหรือป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และรวมถึงต้องสามารถใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) เพื่อตรวจสอบว่าผู้ใช้งานมีสิทธิเข้าถึงการดำเนินการที่สำคัญ (เช่น การเปิดลงคะแนน การปิดลงคะแนน) และเพื่อยืนยันตัวตนของผู้ควบคุมระบบการลงคะแนน หากระบบการลงคะแนนใช้วิธีการยืนยันตัวตนด้วยรหัสผ่าน (password) ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดความเข้มงวดและการหมดอายุของรหัสผ่าน และระบบการลงคะแนนต้องเก็บรักษาข้อมูลยืนยันตัวตน (เช่น รหัสผ่าน) โดยมีการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล
3.11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลดสิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่ (separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น
3.11.5 – ระบบการลงคะแนนมีการเพิกถอนสิทธิการเข้าถึงข้อมูลเมื่อไม่ต้องการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด ระบบการลงคะแนนระงับการใช้งาน (lockout) ของบทบาทหรือผู้ใช้งานหลังจากการยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่สามารถกำหนดระยะเวลาระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล

3.12 ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย

ข้อกำหนด	คำอธิบาย
3.12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐาน หรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาตหรือการถูกตัดการเชื่อมต่อทางกายภาพ เกิดขึ้นกับส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน ระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อคที่มั่นคงปลอดภัย หรือ ระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ

3.13 การคุ้มครองข้อมูล (Data Protection)

วัตถุประสงค์ เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึง แก้ไขเปลี่ยนแปลง หรือลบโดยไม่ได้รับอนุญาต

ข้อกำหนด	คำอธิบาย
3.13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) บันทึกการลงคะแนน ข้อมูลที่ส่งออก หรือบันทึกการตรวจสอบ จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนนและระบบเครือข่าย รวมถึงต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) หรือบันทึกการตรวจสอบ (audit records) จากการแก้ไขเปลี่ยนแปลงเมื่อมีการจัดเก็บข้อมูลภายในระบบการลงคะแนน
3.13.2 – บันทึกการลงคะแนนสามารถตรวจสอบแหล่งที่มาและความครบถ้วนของข้อมูลได้	ผลลงคะแนนมีการลงลายมือชื่อดิจิทัลโดยผู้ลงคะแนนเมื่อจัดเก็บและก่อนส่งออกข้อมูล เพื่อให้สามารถตรวจสอบแหล่งที่มาของผลลงคะแนนได้ นอกจากนี้ ระบบการลงคะแนนต้องตรวจสอบลายมือชื่อดิจิทัลของผู้ลงคะแนนและตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับมาจากผู้ลงคะแนนด้วยกระบวนการเข้ารหัสลับ (cryptography) รวมถึงมีการบันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที

ข้อกำหนด	คำอธิบาย
3.13.3 – ระบบการลงคะแนนใช้อัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่เป็นมาตรฐาน	กุญแจเข้ารหัส โมดูลการเข้ารหัสลับ (cryptographic module) และอัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่ใช้ในกระบวนการเข้ารหัสลับของระบบการลงคะแนนต้องเป็นไปตามมาตรฐาน เช่น FIPS 140-2 Security Requirements for Cryptographic Modules และ NIST SP 800-57 Part 1 Recommendation for Key Management: Part 1 – General
3.13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด	การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายคอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)

3.14 การรักษาความครบถ้วนของระบบการลงคะแนน (System Integrity)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงานที่กำหนด ไม่มีการดัดแปลงหรือแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือโดยไม่ตั้งใจ

ข้อกำหนด	คำอธิบาย
3.14.1 – ระบบการลงคะแนนใช้การควบคุมหลายด้าน (multiple layers of controls) เพื่อรับมือการโจมตีหรือช่องโหว่ด้านความมั่นคงปลอดภัย	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) ซึ่งอธิบายวิธีการควบคุมเพื่อรับมือหรือลดความเสี่ยงจากภัยคุกคามแต่ประเภทที่จะส่งผลกระทบต่อการทำงานของระบบการลงคะแนน และอธิบายการใช้วิธีการควบคุมด้านกายภาพ ด้านเทคนิค และด้านการปฏิบัติงาน ร่วมกันเพื่อป้องกัน บรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน เช่น การเข้ารหัสลับ การป้องกันมัลแวร์ (malware) การตั้งค่าไฟร์วอลล์ (firewall) และการตั้งค่าระบบ
3.14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น และใช้การควบคุมทางเทคนิคอื่น ๆ	ระบบการลงคะแนนป้องกันการติดตั้งหรือการสั่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง และปิดใช้งานการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีคำแนะนำสำหรับการตั้งค่าระบบที่มั่นคงปลอดภัย ซอฟต์แวร์ของระบบการลงคะแนนต้องไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และต้องเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น

3.15 การตรวจจับและการเฝ้าระวัง (Detection and Monitoring)

วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน

ข้อกำหนด	คำอธิบาย
3.15.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมที่สำคัญด้วยวิธีการบันทึกเหตุการณ์ ซึ่งอยู่ในรูปแบบที่เหมาะสมสำหรับการประมวลผลอัตโนมัติ	ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ที่เกิดขึ้น (event logging) ในระบบการลงคะแนนและสามารถส่งออกบันทึกเหตุการณ์ (log) ทั้งนี้ ระบบการลงคะแนนต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับฟังก์ชันการทำงานทั่วไปของระบบ การจัดการระบบเครือข่าย การจัดการซอฟต์แวร์ และฟังก์ชันการลงคะแนน เป็นอย่างน้อย นอกจากนี้ เมื่อผู้ควบคุมระบบการลงคะแนนเข้าถึงไฟล์การตั้งค่า (configuration file) ระบบการลงคะแนนต้องบันทึกข้อมูลที่ระบุตัวผู้ใช้งาน กลุ่มหรือบทบาทของผู้ใช้งานที่เข้าถึงไฟล์นั้น
3.15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ใช้งานในทันที บันทึกข้อผิดพลาดทั้งหมดที่เกิดขึ้น และสร้างรายงานข้อผิดพลาด (error report) รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการจัดการข้อผิดพลาดในระบบการลงคะแนน
3.15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	ระบบการลงคะแนนต้องมีมาตรการป้องกันมัลแวร์ (malware) โดยระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ บันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ และบันทึกเหตุการณ์ของกิจกรรมการแก้ไขมัลแวร์ รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีกระบวนการและขั้นตอนสำหรับการอัปเดตมาตรการป้องกันมัลแวร์
3.15.4 – ระบบการลงคะแนนที่เชื่อมต่อเครือข่ายใช้วิธีการป้องกันการโจมตีทางเครือข่าย (network-based attack) ที่เหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของสถาปัตยกรรมระบบเครือข่าย (network architecture) ของเครือข่ายคอมพิวเตอร์ภายใน (internal network) ของระบบการลงคะแนน และมีข้อมูลเกี่ยวกับวิธีการปิดใช้งานเครือข่ายไร้สาย (wireless network) ของระบบการลงคะแนน นอกจากนี้ เอกสารเกี่ยวกับระบบการลงคะแนนมีรายการการตั้งค่าความมั่นคงปลอดภัยของระบบเครือข่าย (security configuration) ที่สอดคล้องกับแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย

บรรณานุกรม

[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.