แบบประเมินความสอดคล้องด้วยตนเอง
ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ELECTRONIC VOTING SYSTEM)
ตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ขมธอ. 26-2564) เวอร์ชัน 2.0

ชื่อระบบ	AGMNext
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท)	บริษัท เน็กซ์ ดิจิทัล พลัส จำกัด
ช่องทางการติดต่อผู้ให้บริการ	ผู้ติดต่อ: นางสาวกฤษณา อรเนตรพงษ์ เบอร์ติดต่อ : 089-686-3588 Email : sales@agmnext.com
วันที่ประเมินความสอดคล้อง	*วันที่ 15 พ.ค. 69*
วันที่ครบกำหนดการทบทวน	*วันที่ 14 พ.ค. 70*
ประเภทของระบบการให้บริการ	☒ On Cloud ☐ On Premise ☐ อื่น ๆ โปรดระบุ
การใช้งานระบบการลงคะแนน	☒ ร่วมกับระบบการประชุมฯ ☒ แยกกับระบบการประชุมฯ
มาตรฐานที่ได้รับการรับรอง	☒ ISO/IEC 27001 ☐ ISO/IEC 27701 ☐ อื่น ๆ โปรดระบุ
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง	ระบบ AGMNext มีรูปแบบการให้บริการ On Cloud ครอบคลุมการประชุมทั้งภาพและเสียง, การนับองค์ประชุม, การลงคะแนนรายวาระและมีสรุปรายงานองค์ประชุม, รายงานผลการคะแนนรายวาระ , รายงานผู้เข้าร่วมประชุมและบันทึกข้อมูลจราจรทางอิเล็กทรอนิกส์ได้ทันทีหลังเสร็จสิ้นการประชุม

หมายเหตุ : สพธอ ไม่เกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน		
1. การออกแบบระบบ (System Design) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามกระบวนการการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ		
1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด	ระบบการลงคะแนนมีฟังก์ชันการทำงานที่จำเป็นตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด ซึ่งครอบคลุมการเตรียมข้อมูลสำหรับการลงคะแนน การตรวจสอบระบบการลงคะแนนก่อนการลงคะแนน การเปิดลงคะแนน การลงคะแนน การส่งผลลงคะแนน การปิดลงคะแนน การนับคะแนน และการรายงานผลรวมของการลงคะแนน	ระบบลงคะแนน AGMNext ได้รับการออกแบบให้รองรับกระบวนการและหลักเกณฑ์ทางกฎหมายที่เกี่ยวข้องกับการจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ อาทิ การประชุมผู้ถือหุ้น การประชุมผู้ถือหุ้นกู้ การประชุมคณะกรรมการบริษัทหรือสมาคม และการประชุมเจ้าของร่วมในนิติบุคคลหมู่บ้านจัดสรรหรืออาคารชุด โดยมีรายละเอียดการทำงานหลักดังนี้: **1. การเตรียมข้อมูลสำหรับการลงคะแนน** ● การกำหนดเงื่อนไข: รองรับการตั้งค่ารูปแบบการประชุมและหลักเกณฑ์การนับคะแนน ในแต่ละวาระการประชุมได้ ● การจัดการข้อมูลผู้สิทธิออกเสียง: รองรับการนำเข้าข้อมูลรายชื่อผู้มีสิทธิเข้าร่วมประชุม พร้อมระบุจำนวนสิทธิออกเสียง ของผู้เข้าร่วมแต่ละรายเข้าสู่ระบบอย่างถูกต้อง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		2. **การเปิดการลงคะแนน** ระบบรองรับการเปิด-ปิดการรับผลคะแนนในแต่ละวาระ เพื่อให้ผู้เข้าร่วมประชุมดำเนินการภายในระยะเวลาที่กำหนด 3. **การลงคะแนน** ● ผู้เข้าร่วมประชุมสามารถตรวจสอบและยืนยันการลงคะแนน ก่อนส่งข้อมูลเข้าสู่ระบบ ● การแก้ไขผลคะแนน: ผู้เข้าร่วมประชุมสามารถเปลี่ยนแปลงผลการลงคะแนนได้จนกว่าประธานในที่ประชุมหรือผู้ควบคุมระบบจะประกาศปิดรับการลงคะแนนในวาระนั้น 4. **รูปแบบการลงคะแนน** รองรับการลงคะแนนเสียงตามมาตรฐานสากล ได้แก่ "เห็นด้วย", "ไม่เห็นด้วย" และ "งดออกเสียง" 5. **การปิดการลงคะแนน** เมื่อสิ้นสุดการรับผลคะแนนในแต่ละวาระ ระบบจะทำการปิดรับข้อมูลทันที โดยผู้เข้าร่วมประชุมจะไม่สามารถลงคะแนนเพิ่มเติมหรือเปลี่ยนแปลงข้อมูลเดิมได้ 6. **การนับคะแนน** ระบบรองรับการประมวลผลคะแนนอัตโนมัติ ตามเงื่อนไขที่กำหนดไว้ในแต่ละวาระ อาทิ การนับคะแนนตามเสียงจริง หรือการเทคะแนนเสียงโดยจะเริ่มประมวลผลทันทีหลังปิดวาระ 7. **การรายงานผลการลงคะแนน** ● การแสดงผล: รองรับการแสดงผลการลงคะแนนในแต่ละวาระ ผ่านระบบการประชุม (e-Meeting) เพื่อแจ้งให้ที่ประชุมทราบโดยพร้อมเพรียงกัน ● การจัดทำรายงาน: สามารถสรุปผลการลงคะแนนในแต่ละวาระ โดยจัดทำเป็นรายงานในรูปแบบไฟล์อิเล็กทรอนิกส์ (อาทิ PDF หรือ Excel) เพื่อใช้เป็นหลักฐานประกอบรายงานการประชุมต่อไป
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ (system accuracy and reliability) การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) ในสภาวะที่ใกล้เคียงกับการใช้งานจริงในกระบวนการลงคะแนน และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)	ระบบการลงคะแนนมีการทดสอบความถูกต้องและความน่าเชื่อถือ ดังนี้ 1. กำหนดและจัดทำ test case ให้ครอบคลุมการทำงานทั้งหมดของระบบ ได้แก่ ● การลงทะเบียนเข้าประชุม ● การลงคะแนนตามเงื่อนไขของวาระต่างๆ ● การสรุปผลคะแนนรายวาระ ● การออกรายงาน 2. ทดสอบ load test จำลองสภาวะการใช้งานจริงระบบลงคะแนนจริงโดยใช้ JMeter จำลองจำนวนผู้ลงคะแนนตามที่คาดการณ์ไว้เข้ามาใช้งานระบบพร้อมกัน ซึ่งจากการทดสอบระบบสามารถรองรับผู้เข้าร่วมประชุมได้ไม่น้อยกว่า 8,000 ราย โดยการใช้งาน CPU/RAM ของ Server ยังไม่เกิน 70%
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบซอฟต์แวร์ (software tester) ของผู้พัฒนาระบบการลงคะแนน	ระบบลงคะแนนผ่านการทดสอบตาม test case อย่างครบถ้วน ได้แก่ ● การลงทะเบียนเข้าประชุม ● การลงคะแนนตามเงื่อนไขของวาระต่างๆ ● การสรุปผลคะแนนรายวาระ ● การออกรายงาน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		โดยมีการจัดทำรายงานผลการทดสอบเพื่อยืนยันว่าระบบสามารถทำงานได้สอดคล้องกับการออกแบบ
2. การพัฒนาระบบ (System Development) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการพัฒนาระบบโดยใช้แนวปฏิบัติที่ดี		
2.1 – การพัฒนาระบบการลงคะแนนใช้แนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์	ระบบการลงคะแนนใช้ภาษาโปรแกรมและรูปแบบการเขียนโปรแกรมที่เป็นที่ยอมรับ รวมถึงแนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์ 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)	ระบบการลงคะแนนถูกพัฒนาด้วยภาษาโปรแกรมที่ผู้พัฒนายังรองรับการใช้งาน คือ Java และ PHP โดยดำเนินการพัฒนาและปฏิบัติตาม Software Development Life Cycle (SDLC) อ้างอิงตามมาตรฐาน ISO/IEC 29110 ดังต่อไปนี้ 1. Planning 2. Requirement Analysis 3. Design: ออกแบบ System Architecture, Database, UX/UI 4. Development 5. Testing: ทดสอบ Unit Test, Integration Test และ UAT 6. Deployment 7. Maintenance & Support
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน(modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ	ระบบการลงคะแนนมีการออกแบบโครงสร้างแบบ Microservices ผ่าน RESTful API แยกโมดูลการทำงานดังนี้ 1. การจัดการข้อมูลผู้มีสิทธิเข้าร่วมประชุมและจำนวนเสียง 2. การลงทะเบียนและการยืนยันตัวตนเพื่อเข้าร่วมประชุม 3. การจัดการวาระและเงื่อนไขการลงคะแนน 4. การลงคะแนน - ประมวลผลและจัดเก็บผลการลงคะแนน 5. การออกรายงาน โดยแต่ละโมดูลสามารถทดสอบและตรวจสอบได้อิสระจากกัน และ มีการยึดตาม Secure Coding Standard: OWASP เช่น SQL Injection เป็นต้น
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้	ระบบการลงคะแนนใช้ Bitbucket เป็นเครื่องมือในการสนับสนุน Source Code Integrity และ Self-Modifying Code ดังนี้ 1. ระบบการลงคะแนนมีการกำหนด Version Control ของ Source Code โดยมีเก็บรายละเอียดที่ได้มีการพัฒนาหรือปรับปรุงแก้ไข 2. ระบบการลงคะแนนมีการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย โดยไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจาก	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน	ระบบการลงคะแนนได้รับการออกแบบให้รองรับและกู้คืนจากข้อผิดพลาด ดังนี้ 1. มีการออกแบบให้รองรับการจัดทำ data replication เพื่อจัดการและกู้คืนข้อมูลจากข้อผิดพลาดหรือล้มเหลว 2. ใช้บริการของ cloud server provider ที่มีมาตรฐานสากลคือ Google Cloud ที่รองรับการเป็น DR site

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ความล้มเหลวได้อย่างมีประสิทธิภาพ		กรณีระบบงานหลักมีข้อผิดพลาดหรือล้มเหลว 3. กรณีมีข้อผิดพลาดหรือล้มเหลวของระบบ มีกระบวนการบันทึกและแจ้งเตือนให้ผู้รับผิดชอบทราบเมื่อเกิดเหตุ โดยบริษัทมีการจัดทำและซักซ้อมแผน DRP รวมถึงทดสอบการกู้คืนข้อมูลด้วยเป็นประจำทุกปี
3. ความโปร่งใส (Transparent) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนและกระบวนการลงคะแนนมีการออกแบบที่มีความโปร่งใส		
3.1 – เอกสารอธิบายการออกแบบ การทำงาน การเข้าถึง มาตรการความมั่นคงปลอดภัย และรายละเอียดอื่น ๆ ของระบบการลงคะแนนสามารถอ่านและทำความเข้าใจได้	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารเกี่ยวกับระบบการลงคะแนน 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) คู่มือการใช้งาน (user manual)	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารประกอบความครบถ้วน ดังนี้ 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. คู่มือการใช้งาน (user manual) แยกสำหรับผู้ควบคุมระบบและผู้เข้าร่วมประชุม
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนนเตรียมไว้พร้อมสำหรับการตรวจสอบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารวิธีการตั้งค่า การตรวจสอบความพร้อม เช่น จำนวนของผู้มีสิทธิ์ลงคะแนนและความถูกต้องของเงื่อนไขการลงคะแนนของแต่ละวาระ โดย บริษัทเป็นผู้ดำเนินการติดตั้งตั้งค่า และตรวจสอบระบบทั้งหมดก่อนการประชุมทุกครั้ง สำหรับวิธีการเฝ้าระวังการทำงานของระบบการลงคะแนนจะครอบคลุม (1) การใช้งานของระบบ เช่น CPU Memory (2) ความสอดคล้องของของข้อมูล เช่น จำนวนผู้ลงคะแนนต้องสัมพันธ์กับจำนวนคะแนน ซึ่งถ้าพบความผิดปกติจะมีการแจ้งเตือนไปยังผู้ดูแลระบบทันที
3.3 – บุคคลที่เกี่ยวข้องกับระบบการลงคะแนนสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)	ระบบการลงคะแนนมีการบันทึกเหตุการณ์ครอบคลุมดังนี้ 1. Log การเข้าสู่ระบบ 2. Log การลงคะแนน 3. System Log โดยผู้ควบคุมระบบสามารถ Export ข้อมูล Log ที่มีข้อมูล IP Adress, Action และ Timestamp ได้ในรูปแบบ CSV หรือ Excel สำหรับการตรวจสอบ ซึ่งมีการอธิบายรูปแบบ Log Format ไว้ในเอกสารประกอบระบบอย่างครบถ้วน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
4. การเข้าถึงอย่างเท่าเทียม (Equitable Access) วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม		
4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงภาพและเสียง) และรูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัสบนหน้าจอ) ในลักษณะที่สอดคล้องกัน	ระบบการลงคะแนน ใช้วิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ในทุกช่องทางมีฟังก์ชันในการลงคะแนน และการตรวจสอบผลการลงคะแนนที่เหมือนกัน ในทุกอุปกรณ์ เช่น คอมพิวเตอร์ Tablet หรือโทรศัพท์มือถือ โดยสามารถเข้าใช้งานผ่าน browser ซึ่งระบบการลงคะแนนรองรับการแสดงผลแบบ responsive ในทุกอุปกรณ์
4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ	รูปแบบการแสดงผล (display format) แสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน และไม่ทำให้เกิดอคติกับตัวเลือกลงคะแนนใด ๆ ที่นำเสนอต่อผู้ลงคะแนน เช่น ตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน	ระบบการลงคะแนนแสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน โดยตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยด้วยปุ่ม โดยใช้อักษรที่มีขนาด สี และลักษณะเหมือนกัน
5. การลงคะแนนตรงตามเจตนา (Cast as Intended) วัตถุประสงค์ เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่อ งหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้		
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงกับความต้องการของผู้ลงคะแนน	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล (preference setting) ตามความต้องการของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษร และสีของภาพ	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคน โดยไม่รองรับการตั้งค่าส่วนบุคคล (Preference setting) ตามความต้องการของผู้ลงคะแนน อย่างไรก็ตาม ผู้ลงคะแนนสามารถปรับเปลี่ยนขนาดการแสดงผลของหน้าจอและขนาดตัวอักษร เช่น ตัวหนังสือและปุ่มสำหรับลงคะแนน ได้ตามความเหมาะสมผ่านฟังก์ชันของ browser
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือก	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง เช่น รูปแบบการแสดงผลของข้อมูล (display format) การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้า	• ผู้ลงคะแนนสามารถควบคุมการลงคะแนนในวาระที่ต้องการ ได้โดยการเลื่อนหน้าจอขึ้น/ลง โดยการใช้ท่าทางสัมผัสบนหน้าจอ • ผู้ลงคะแนนสามารถควบคุมการลงคะแนนได้โดยตรง สามารถลงคะแนนเสียง (1) เห็นด้วย (2) ไม่เห็นด้วย (3) งดออกเสียง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	ถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ (touch screen gestures) รวมถึงระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) เช่น การให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนน หรือการแจ้งสถานะของการลงคะแนนให้ผู้ลงคะแนนทราบ	• ระบบการลงคะแนนจะแสดงการลงคะแนนล่าสุดให้ผู้ลงคะแนนทราบ • ในกรณีที่ผู้ลงคะแนนต้องการเปลี่ยนแปลงการลงคะแนน สามารถทำได้ด้วยตนเองจนกว่าวาระนั้นจะปิดรับการลงคะแนน ระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ โดยจะแสดงหน้าจอ pop up ให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนนทุกครั้ง
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน คำแนะนำและข้อความจากระบบด้วยภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งข้อความที่ไม่ให้เกิดความสับสนในการลงคะแนน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต หรือการเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) และการแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว นอกจากนี้ ระบบมีการแสดงคำแนะนำและข้อความที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ	ระบบการลงคะแนนมีการออกแบบหน้าจอแสดงเฉพาะข้อมูลที่จำเป็นและไม่ซับซ้อน เพื่อให้ผู้ลงคะแนนสามารถใช้งานได้ง่าย โดย 1. มีการแสดงชื่อวาระและปุ่มให้ผู้ลงคะแนนสามารถเลือกลงคะแนนตามวัตถุประสงค์ได้ทันที 2. มีการแจ้งเตือนผู้ลงคะแนนเพื่อยืนยันการลงคะแนน 3. มีการแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนน เช่น ไม่สามารถลงคะแนนได้หลังจากวาระถูกปิดการลงคะแนนแล้ว เป็นต้น 4. มีการแสดงข้อมูลการลงคะแนนให้ผู้ลงคะแนนทราบ เมื่อลงคะแนนสำเร็จ นอกจากนี้ระบบการลงคะแนนมีการแสดงคำแนะนำและมีขั้นตอนการทำงานที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงาน
6. ความเหมาะสมต่อการใช้งาน (Usable) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้อย่างเหมาะสม		
6.1 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบการลงคะแนน เพื่อให้มั่นใจว่าระบบการลงคะแนนสามารถใช้งานกับผู้คะแนนทุกคน (ซึ่งอาจรวมถึงผู้สูงอายุและบุคคลที่มีความบกพร่องทางการมองเห็น) ได้อย่างเหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี เช่น มาตรฐาน Web Content Accessibility Guidelines (WCAG) 2.0 ของ World Wide Web Consortium (W3C)	ผู้พัฒนาระบบการลงคะแนนมีการประเมินและทดสอบความเหมาะสมต่อการใช้งาน ดังนี้ 1. ทดสอบกับตัวแทนกลุ่มผู้ใช้งานประมาณ 100 ราย ช่วงอายุ 25-70 ปี 2. ไม่พบปัญหาในการใช้งานระบบลงคะแนนในกลุ่มทดสอบดังกล่าว ทั้งนี้ระบบการลงคะแนนยังไม่รองรับสำหรับบุคคลที่มีความบกพร่องทางการมองเห็น โดยบริษัทมีการนำแนวปฏิบัติมาตรฐาน WCAG 2.0 มาเป็นส่วนหนึ่งของการประเมินความเหมาะสมในการใช้งาน เพื่อให้สามารถใช้กับผู้ลงคะแนนทุกกลุ่ม และนำข้อเสนอแนะที่ได้รับจากการประเมินมาปรับปรุง เช่น สามารถปรับเปลี่ยนขนาดของตัวอักษรได้ สำหรับผู้สูงอายุ เป็นต้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ	ผู้พัฒนาระบบการลงคะแนนมีการทดสอบความเหมาะสมต่อการใช้งานสำหรับผู้ควบคุมระบบ ดังนี้ 1. จัดทำขั้นตอนการดำเนินงานที่เข้าใจง่าย พร้อมเอกสารคู่มือสำหรับผู้ควบคุมระบบ 2. จัดฝึกอบรมผู้ควบคุมระบบเป็นประจำ 3. ทดสอบการตั้งค่าระบบ การดำเนินการในระหว่างการประชุม และการปิดระบบ
ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ		
7. การทำงานร่วมกัน (Interoperable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน		
7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนอยู่ในรูปแบบที่ทำงานร่วมกันได้หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐาน	ระบบการลงคะแนนมีการนำข้อมูลเข้าและออกอยู่ในรูปแบบมาตรฐานดังนี้ 1. นำเข้าข้อมูลผู้มีสิทธิลงคะแนนในรูปแบบไฟล์ Excel หรือรูปแบบมาตรฐานอื่นๆ ที่เป็น machine readable 2. ส่งออกข้อมูลการลงคะแนน ข้อมูล Log และรายงานผลการลงคะแนนในรูปแบบไฟล์ PDF CSV หรือ Excel
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้รูปแบบมาตรฐาน ในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่าง ๆ	ระบบการลงคะแนนไม่มีการเชื่อมต่ออุปกรณ์ hardware อื่นๆ ในการลงคะแนน ผู้ลงคะแนนสามารถใช้ผ่านอุปกรณ์ส่วนตัวได้ด้วยตนเอง
8. การตรวจสอบ (Auditable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบความถูกต้องของผลลงคะแนน		
8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	ผลลงคะแนนที่ได้จากการลงคะแนนของผู้ลงคะแนนมีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลได้ (tamper-evidence) ระบบการลงคะแนนเปิดโอกาสให้ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกไป แจ้งข้อผิดพลาดในผลลงคะแนนที่เกิดจากระบบการลงคะแนน และเริ่มต้นลงคะแนนใหม่หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน (ขึ้นอยู่กับกฎหมายหรือหลักเกณฑ์ที่กำหนด) รวมถึงควรมีช่องทางให้ผู้	ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบผลลงคะแนน ดังนี้ 1. ผู้ลงคะแนนสามารถตรวจสอบผลการลงคะแนนของตนเองได้ผ่านหน้าสรุปผลบนระบบ 2. ระบบการลงคะแนนมีการตรวจสอบการลงคะแนนให้แบบอัตโนมัติ โดยจะลงคะแนนได้ไม่เกินคะแนนที่มี 3. ระบบการลงคะแนนมีช่องทาง Call Center แสดงตลอดระยะเวลาประชุม สำหรับแจ้งเหตุขัดข้อง 4. ระบบการลงคะแนนมีการเก็บ log การลงคะแนน เพื่อใช้ในการตรวจสอบการเปลี่ยนแปลงการลงคะแนนได้ 5. ระบบการลงคะแนนสร้างรายงาน Activity Log ให้ผู้ตรวจสอบภายนอก ตรวจสอบผลลงคะแนนและการนับคะแนนได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ระบบการลงคะแนนต้องสร้างรายงานที่จะช่วยให้ผู้ตรวจสอบภายนอก (external auditor) สามารถตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง รวมถึงผู้พัฒนาระบบการลงคะแนนจัดทำขั้นตอนสำหรับการตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง	
9. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy) [1] วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง		
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่แสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน	ระบบการลงคะแนนมีการออกแบบเพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนนดังนี้ 1. ผู้ลงคะแนนต้องยืนยันตัวตนและเข้าใช้ระบบผ่าน URL ที่ถูกกำหนดมาให้เฉพาะผู้ลงคะแนนแต่ละราย 2. การลงคะแนนเป็นรายบุคคลเฉพาะตนเอง ไม่มีการเปิดเผยข้อมูลหรือผลลงคะแนนต่อบุคคลอื่นในระหว่างลงคะแนน
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่าส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนมีการออกแบบหน้าจอแสดงเฉพาะข้อมูลที่จำเป็นและไม่ซับซ้อน เพื่อให้ผู้ลงคะแนนสามารถใช้งานได้ง่าย และสามารถเลือกตัวเลือกลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น
10. ความลับของคะแนนเสียง (Vote Secrecy) วัตถุประสงค์ (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน		
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผล	ระบบการลงคะแนนต้องไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มา	ระบบการลงคะแนนไม่รองรับการลงคะแนนลับ

[1] ความเป็นส่วนตัวของผู้ลงคะแนน ในที่นี้หมายถึง ความเป็นส่วนตัวที่เกิดขึ้นภายในระบบการลงคะแนนเท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ลงคะแนนตลอดกระบวนการลงคะแนน	ประมวลผล จัดเก็บ หรือแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว	
10.2 – ระบบการลงคะแนนไม่จัดทำข้อมูลเกี่ยวกับผู้ลงคะแนนหรือข้อมูลอื่น ๆ ที่สามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน นอกจากนี้ ผลลงคะแนนและผลรวมของการลงคะแนนต้องไม่มีข้อมูลที่ระบุตัวผู้ลงคะแนนและข้อมูลที่สามารถใช้หาลำดับของการส่งผลลงคะแนนได้ อย่างไรก็ตาม ในกรณีที่ให้ผู้ลงคะแนนส่งผลลงคะแนนก่อนจะตรวจสอบการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนน<u>สามารถใช้การเชื่อมโยงโดยอ้อม</u> (indirect voter association) ที่เชื่อมโยงผู้ลงคะแนนกับผลลงคะแนนที่ถูกเข้ารหัสลับไว้ โดยหลังจากตรวจสอบแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้น จึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับ และนำไปนับคะแนนเป็นผลรวมของการลงคะแนน	ระบบการลงคะแนนไม่รองรับการลงคะแนนลับ
11. การควบคุมการเข้าถึง (Access Control) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น		
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนนเพื่อให้มีหลักฐานสำหรับตรวจสอบในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งาน เปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และลบบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงครอบคลุม ดังนี้ 1. ระบบการลงคะแนนมีการจัดเก็บ log กิจกรรมการใช้งานในระบบทั้งหมด ซึ่งมีข้อมูลที่ระบุตัวบุคคล วันและเวลา ซึ่งได้มีการเทียบเวลากับแหล่งเวลาที่เป็นมาตรฐานสากล รวมถึง IP Address ของอุปกรณ์ที่ได้ใช้งาน 2. บันทึก log ถูกกำหนดให้ไม่สามารถแก้ไขเปลี่ยนแปลงหรือลบบันทึกเหตุการณ์ 3. ระบบการลงคะแนนกำหนดสิทธิ์เข้าถึง Log เฉพาะผู้ควบคุมระบบที่ได้รับมอบหมายเท่านั้น และมีการทบทวนสิทธิการเข้าถึงระบบลงคะแนนของผู้ควบคุมระบบเป็นประจำทุก 6 เดือน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนน และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดบัญชีผู้ใช้งานที่ได้รับอนุญาต กำหนดบทบาทของผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละบทบาทของผู้ใช้งาน	ระบบการลงคะแนนมีการจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยมีบทบาทหน้าที่ ดังนี้ ● ผู้ควบคุมระบบ (Admin) ทำหน้าที่ตั้งค่าและดูแลระบบงาน ● ผู้ควบคุมการประชุม ทำหน้าที่ควบคุมการประชุมให้เป็นตามวาระที่กำหนด ● ผู้ตรวจสอบภายนอก ทำหน้าที่ตรวจสอบความถูกต้องของผลคะแนนผ่านระบบและรายงาน ● ผู้เข้าร่วมประชุม สามารถลงคะแนนเสียงและตรวจสอบการลงคะแนน
11.3 – ระบบการลงคะแนนรองรับวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน	ระบบการลงคะแนนใช้วิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน เพื่อตรวจสอบว่าเป็นผู้ใช้งานที่ได้รับอนุญาตจริง และใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน เพื่อตรวจสอบว่าเป็นผู้ที่มีสิทธิเข้าถึงการดำเนินการที่สำคัญ (เช่น การเปิดลงคะแนน การปิดลงคะแนน) ทั้งนี้ วิธีการพิสูจน์และยืนยันตัวตนอาจพิจารณาข้อกำหนดตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) จากมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ระบบการลงคะแนนต้องเก็บรักษาข้อมูลยืนยันตัวตน (เช่น รหัสผ่าน) โดยมีการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล และหากระบบการลงคะแนนใช้วิธีการยืนยันตัวตนด้วยรหัสผ่าน ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดความเข้มงวดและการหมดอายุของรหัสผ่าน	ระบบการลงคะแนนใช้วิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้ 1. ผู้เข้าร่วมประชุม ที่ผ่านการยืนยันตัวตนและได้รับการอนุมัติให้เข้าร่วมประชุม จะได้รับ unique token แบบมั่นคงปลอดภัยเพื่อให้ผู้เข้าร่วมประชุมใช้ในการยืนยันตัวตนด้วยข้อมูลส่วนตัวอีกครั้งเพื่อเข้าใช้งานและมีการจำกัดการเข้าใช้งาน เฉพาะอุปกรณ์และเครือข่ายที่เกี่ยวข้อง ซึ่งระบบจะไม่อนุญาตให้ผู้เข้าร่วมประชุมใช้ token เดียวกันเข้าประชุมในระบบพร้อมกัน 2. ผู้ควบคุมระบบ สามารถเข้าระบบด้วยรหัสผ่านซึ่งมีการกำหนดความเข้มงวดซึ่งต้องประกอบด้วยตัวเลข ตัวอักษร และอักขระพิเศษ และมีการหมดอายุของรหัสผ่านทุก 3 เดือน นอกจากนี้ต้องมียืนยันตัวตนแบบ Multi-Factor Authentication (MFA) ในการดำเนินการที่สำคัญ เช่น รหัสผ่าน และ Email OTP เป็นต้น
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการ	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลดสิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่	ระบบการลงคะแนนมีการกำหนดสิทธิ์การเข้าถึงระบบงานดังนี้ ● ผู้ควบคุมระบบ (Admin) ทำหน้าที่ตั้งค่าและดูแลระบบงาน ● ผู้ควบคุมการประชุม ทำหน้าที่ควบคุมการประชุมให้เป็นตามวาระที่กำหนด ● ผู้ตรวจสอบภายนอก ทำหน้าที่ตรวจสอบความถูกต้องของผลคะแนนผ่านระบบและรายงาน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ของการกำหนดสิทธิการเข้าถึงตามความจำเป็นและการแบ่งแยกหน้าที่	(separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น	● ผู้เข้าร่วมประชุม สามารถลงคะแนนเสียงและตรวจสอบการลงคะแนน
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด หากผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนควรระงับการใช้งาน (account lockout) ของผู้ใช้งานเป็นระยะเวลาหนึ่งก่อนจะให้ยืนยันตัวตนครั้งต่อไป และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล	ระบบการลงคะแนนมีการกำหนดระยะเวลาของเซสชัน (session) ในกรณีผู้ใช้งานไม่ทำกิจกรรมภายในระยะเวลา 30 นาที โดยผู้ใช้งานต้องยืนยันตัวตนซ้ำเพื่อเข้าใช้งานระบบใหม่อีกครั้ง ในกรณีที่ผู้ใช้งานยืนยันตัวตนผิดต่อเนื่องเกิน 5 ครั้ง บัญชีของผู้ใช้งานจะถูกระงับการใช้งานเป็นระยะเวลา 10 นาที
12. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย		
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐานหรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาตหรือการถูกตัดการเชื่อมต่อทางกายภาพ เกิดขึ้นกับส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน ผู้พัฒนาระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อคที่มั่นคงปลอดภัย หรือระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ	ระบบการลงคะแนนถูกติดตั้งและให้บริการผ่านผู้ให้บริการ cloud ซึ่งมีมาตรการรักษาความปลอดภัยทางกายภาพตามมาตรฐานของ google cloud (https://cloud.google.com/security/compliance/iso-27001)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
13. การคุ้มครองข้อมูล (Data Protection) วัตถุประสงค์ เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต		
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนนจากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนนและระบบเครือข่าย รวมถึงระบบการลงคะแนนต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง	ระบบการลงคะแนนมีการปกป้องข้อมูล Configuration และบันทึกการลงคะแนน ดังนี้ 1. เฉพาะผู้ควบคุมระบบที่ผ่านการยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไข Configuration File ได้ 2. ระบบการลงคะแนนมีการกำหนดสิทธิการการเข้าใช้งาน สำหรับผู้ที่สามารถตั้งค่าของระบบการลงคะแนนและการตั้งค่าระบบเครือข่าย 3. ระบบการลงคะแนนมีการรักษาความครบถ้วนของการบันทึกการลงคะแนนด้วยการแฮช
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับมาจากผู้ลงคะแนน บันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที และจัดเก็บบันทึกการลงคะแนนให้อยู่ในรูปแบบที่สามารถแสดงผลลงคะแนนที่ได้รับมาให้ปรากฏอย่างถูกต้องได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของบันทึกการลงคะแนน ดังนี้ 1. ระบบออกแบบให้ผู้ลงคะแนนตรวจสอบตัวเลือกที่เลือกและให้ยืนยันก่อนส่ง 2. แสดงข้อความยืนยันทันทีที่ระบบรับผลลงคะแนนสำเร็จ 3. กรณีเกิดข้อผิดพลาด ระบบจะไม่นำคะแนนนั้นมาประมวลผล และบันทึก Log พร้อม Error Message 4. จัดเก็บบันทึกการลงคะแนนในรูปแบบที่สามารถแสดงผลลงคะแนนได้อย่างถูกต้องครบถ้วน
13.3 – ระบบการลงคะแนนใช้อัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่เป็นมาตรฐาน	กุญแจเข้ารหัส โมดูลการเข้ารหัสลับ (cryptographic module) และอัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่ใช้ในกระบวนการเข้ารหัสลับของระบบการลงคะแนนต้องเป็นไปตามมาตรฐาน เช่น FIPS 140 Security Requirements for Cryptographic Modules และ NIST Special Publication 800-57 Part 1 Recommendation for Key Management: Part 1 – General	ระบบการลงคะแนนมีการใช้ SSL เข้ารหัสลับของข้อมูลการลงคะแนน โดยจะทำการเข้ารหัสก่อนทำการส่งข้อมูลระหว่างเครือข่าย และเมื่อข้อมูลไปยังปลายทาง จึงทำการถอดรหัส ซึ่งบริษัทมีนโยบายด้านการเข้ารหัสลับข้อมูลที่ระบุถึงการเข้ารหัสลับข้อมูล ดังนี้ 1. ข้อมูลที่เกี่ยวข้องบนระบบ และข้อมูลส่วนบุคคลที่เกี่ยวข้อง เช่น เลขบัตรประชาชน, เบอร์ติดต่อ 2. ระบบ มีการทำ Database Encryption ข้อมูลที่เกี่ยวข้องทั้งหมด 3. ระบบมีการ hashing ข้อมูลการลงคะแนนด้วยมาตรฐาน SHA-256 สำหรับเจ้าหน้าที่ผู้ดูแลระบบการลงคะแนนจะต้องมีการเชื่อมต่อผ่าน VPN สำหรับการบริหาร จัดการระบบลงคะแนน
13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่าน	การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายคอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)	ระบบการลงคะแนนมีการเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย โดยการใช้ SSL Certificate ของ Let's Encrypt (SHA256) และมีการรับส่งข้อมูลผ่านช่องทางที่ปลอดภัยด้วยโปรโตคอล HTTPS โดยใช้มาตรฐานการเข้ารหัส TLS1.3

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
เครือข่ายคอมพิวเตอร์ทั้งหมด		
14. การรักษาความครบถ้วนของระบบ (System Integrity) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงาน และไม่มีการแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือโดยไม่ตั้งใจ		
14.1 – ระบบการลงคะแนนใช้การควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อรับมือภัยคุกคามหรือช่องโหว่ด้านความมั่นคงปลอดภัย	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) และวิธีการควบคุมเพื่อรับมือหรือลดความเสี่ยงจากภัยคุกคามแต่ประเภทซึ่งอาจส่งผลกระทบต่อการทำงานของระบบการลงคะแนน รวมถึงอธิบายวิธีการควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อป้องกันบรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน เช่น กระบวนการเข้ารหัสลับ (cryptography) การป้องกันมัลแวร์ (malware) การตั้งค่าไฟร์วอลล์ (firewall) และการตั้งค่าระบบ (system configurations)	1. ระบบการลงคะแนนมีการประเมินความเสี่ยง (risk assessment) ในด้านต่างๆ เช่น operation risk และ cyber-attack risk โดยหลังจากทำ risk migration and control แล้ว ส่งผลให้ความเสี่ยงลดลงอยู่ในระดับต่ำ (Low Impact) และมีโอกาสเกิดน้อย (Low Probability) 2. ระบบการลงคะแนนมีการควบคุมในหลายระดับชั้น เช่น การตั้งค่า firewall และป้องกันมัลแวร์ (malware) ในระดับ Server และ Network Layer ตามมาตรฐานของผู้ให้บริการ cloud https://cloud.google.com/security/products/firewall
14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น	ระบบการลงคะแนนป้องกันการติดตั้งหรือการสั่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง และปิดใช้งานการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน ซอฟต์แวร์ของระบบการลงคะแนนต้องไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และต้องเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น	1. ระบบการลงคะแนนมีการควบคุมการติดตั้ง source code หรือ software รวมถึงการเปิดการเชื่อมต่อเท่าที่จำเป็นเท่านั้น 2. มีการทบทวนตรวจสอบ unused code อย่าสม่ำเสมอ รวมถึงการใช้ภาษาหรือ library ที่ได้มาตรฐานเท่านั้น 3. มีการจัดทำแผนการบริหารจัดการช่องโหว่ โดยการ update patch ที่สำคัญอย่างสม่ำเสมอๆ 4. ระบบ AGMNext มีการทำ Hardening ครอบคลุมทั้งระดับ OS, Network และ Application เพื่อลดโอกาสการถูกโจมตี
15. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน		
15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ	ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งประกอบด้วยเหตุการณ์ที่เกี่ยวข้องกับสถานะการทำงานและความผิดปกติของระบบ การยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน การจัดการระบบเครือข่าย การ	ระบบการลงคะแนนมีการบันทึก event logging ที่เกิดขึ้นในระบบลงคะแนน ดังนี้ 1. System Log บันทึกสถานะการทำงานและความผิดปกติของระบบ 2. Activity Log บันทึกการยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน รวมถึงการลงคะแนนในวาระต่างๆ ทั้งนี้ Log Format ถูกกำหนดให้ต้องมีข้อมูลของ Action, IP Address และ Timestamp และระบบรองรับการนำข้อมูล log ที่บันทึกไว้ออกมาได้ในรูปแบบ csv

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	จัดการซอฟต์แวร์ และฟังก์ชันการลงคะแนน เป็นอย่างน้อย	
15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ใช้งานในทันที บันทึกข้อผิดพลาดทั้งหมดที่เกิดขึ้น และสร้างรายงานข้อผิดพลาด (error report) รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการจัดการข้อผิดพลาดในระบบการลงคะแนน	ระบบการลงคะแนนมีการแจ้งเตือนผู้ใช้งานเมื่อมีข้อผิดพลาดเกิดขึ้น เช่น การลงคะแนนไม่สำเร็จ โดยสามารถสร้างรายงานข้อผิดพลาดได้
15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	ระบบการลงคะแนนต้องมีมาตรการป้องกันมัลแวร์ (malware) โดยระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ บันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ และบันทึกเหตุการณ์ของกิจกรรมการแก้ไขมัลแวร์ รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการอัปเดตมาตรการป้องกันมัลแวร์	ระบบการลงคะแนนมีการใช้งานบน server ของ google cloud ซึ่งมีมาตรการป้องกัน malware โดยมีรูปแบบการสแกนเป็นแบบ schedule scan ทุก 30 นาที และมีการแจ้งเตือนผู้ควบคุมระบบการลงคะแนนทันทีเมื่อตรวจสอบพบ malware
15.4 – ระบบการลงคะแนนที่เชื่อมต่อเครือข่ายใช้วิธีการป้องกันการโจมตีทางเครือข่าย (network-based attack) ที่เหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของสถาปัตยกรรมระบบเครือข่าย (network architecture) ของเครือข่ายคอมพิวเตอร์ภายใน (internal network) ของระบบการลงคะแนน และมีข้อมูลเกี่ยวกับวิธีการปิดใช้งานเครือข่ายไร้สาย (wireless network) ของระบบการลงคะแนน นอกจากนี้ เอกสารเกี่ยวกับระบบการลงคะแนนมีรายการการตั้งค่าความมั่นคงปลอดภัยของระบบเครือข่าย (security configuration) ที่สอดคล้องกับแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย เช่น NIST Special Publication 800-44 Guidelines on Securing Public Web Servers	ระบบการลงคะแนนมีการออกแบบสถาปัตยกรรมระบบเครือข่ายของเครือข่ายภายใน โดยใช้ cloud server ของ google cloud ซึ่งมีนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโอนย้ายข้อมูล ตามมาตรฐาน ISO 27001 และ ISO 27017