

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

ชื่อระบบ	OJ E-AGM
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท)	บริษัท โอเจ อินเตอร์เนชั่นแนล จำกัด
ช่องทางการติดต่อผู้ให้บริการ	ผู้ติดต่อ : นายปรัชญา เสือทองคำ เบอร์ติดต่อ : 089-527-5588 Email : sales@ojconsultinggroup.com
วันที่ประเมินความสอดคล้อง	20 มกราคม 2569
วันที่ครบกำหนดการทบทวน	19 มกราคม 2570
ประเภทของระบบการให้บริการ	☒ On Cloud ☐ On Premise ☐ อื่น ๆ โปรดระบุ
การใช้งานระบบการลงคะแนน	☒ ร่วมกับระบบการประชุมฯ ☒ แยกกับระบบการประชุมฯ
มาตรฐานที่ได้รับการรับรอง	☒ ISO/IEC 27001 ☐ ISO/IEC 27701 ☐ อื่น ๆ:
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง	ระบบ OJ E-AGM มีรูปแบบการให้บริการ On Cloud ครอบคลุมการประชุมทั้งภาพและเสียง, การนัดบ่งชี้ประชุม, การลงคะแนนวาระ, การสรุปผลองค์ประชุมผ่านระบบออนไลน์ และมีการสรุปรายงานองค์ประชุม , รายงานผลคะแนนรายวาระ , รายงานผู้เข้าร่วมประชุมและข้อมูลจราจรทางอิเล็กทรอนิกส์ได้ทันทีหลังเสร็จสิ้นการประชุม

หมายเหตุ : สฟธอ ไม่เกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน		
1. การออกแบบระบบ (System Design)		
<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามกระบวนการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ		
1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด	ระบบการลงคะแนนมีฟังก์ชันการทำงานที่จำเป็นตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด ซึ่งครอบคลุมการเตรียมข้อมูลสำหรับการลงคะแนน การตรวจสอบระบบการลงคะแนนก่อนการลงคะแนน การเปิดลงคะแนน การลงคะแนน การส่งผลลงคะแนน การปิดลงคะแนน การนับคะแนน และการรายงานผลรวมของการลงคะแนน	ระบบการลงคะแนนมีการออกแบบฟังก์ชันการใช้งานให้รองรับกระบวนการลงคะแนนตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องกับการประชุมผู้หุ้น ประชุมคณะกรรมการบริษัท/สมาคม ประชุมเจ้าของร่วมหมู่บ้าน/นิติบุคคลอาคารชุด เป็นต้น โดยมีรายละเอียดดังนี้ การเตรียมข้อมูลสำหรับการลงคะแนน - รองรับการกำหนดเงื่อนไขของการประชุมและเงื่อนไขการนับของแต่ละวาระได้ - รองรับการนำเข้าข้อมูลรายชื่อผู้มีสิทธิเข้าร่วมประชุมและจำนวนเสียงที่สามารถออกเสียงลงคะแนน เข้าสู่ระบบ การเปิดการลงคะแนน รองรับการทำหนดเวลาที่จะให้ผู้เข้าร่วมประชุมสามารถลงคะแนนได้จนกว่าวาระนั้นจะปิดรับการลงคะแนน การลงคะแนน รองรับการลงคะแนน โดยระบบจะมีให้ผู้เข้าร่วมประชุมยืนยันการ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ลงคะแนนก่อนทุกครั้ง และสามารถเปลี่ยนแปลงการลงคะแนนเสียงได้จนกว่าวาระนั้นจะปิดรับการลงคะแนน 4. การส่งผลลงคะแนน รองรับการลงคะแนนเสียงแบบมาตรฐานดังนี้ ● เห็นด้วย ● ไม่เห็นด้วย ● งดออกเสียง 5. การปิดลงคะแนน รองรับการปิดรับการลงคะแนน โดยหลังจากวาระถูกปิดรับการลงคะแนนแล้ว ผู้เข้าร่วมประชุมจะไม่สามารถลงคะแนนหรือเปลี่ยนแปลงผลการลงคะแนนในวาระนั้นได้อีก 6. การนับคะแนน รองรับการนับคะแนนตามเงื่อนไขที่ถูกกำหนดในแต่ละวาระ เช่น การนับคะแนนตามจริง หรือ การทะเลาะกันเสียง เป็นต้น โดยเมื่อมีการปิดลงคะแนนแล้ว ระบบจะนับคะแนนให้อัตโนมัติ 7. การรายงานผลรวมของการลงคะแนน รองรับการแสดงผลรวมของการลงคะแนนและรายงานสรุปผลรวมของการลงคะแนนทุกวาระ โดยมีรายละเอียดดังนี้ ● แสดงผ่านหน้าจอให้ผู้เข้าร่วมประชุมทราบผ่าน ระบบประชุม (E-Meeting) ● แสดงรายงานสรุปผลการลงคะแนนเป็นไฟล์เอกสารรูปแบบ PDF/Excel
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ (system accuracy and reliability) การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) ในสภาวะที่ใกล้เคียงกับการใช้งานจริงในกระบวนการลงคะแนน และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)	ระบบการลงคะแนนมีการทดสอบ ดังนี้ 1. จัดทำ Test case ให้ครอบคลุมเงื่อนไขการลงคะแนนต่างๆ และมีการทำ regression test ระบบงานทุกครั้ง เมื่อมีการปรับปรุงหรือเพิ่ม feature ใหม่ 2. ทดสอบ Load Test โดยจำลองจากการใช้งานเสมือนจริงในกระบวนการลงคะแนนของผู้เข้าร่วมประชุม โดยสามารถรองรับผู้เข้าร่วมประชุมได้ไม่น้อยกว่า 3,000 ราย
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบซอฟต์แวร์ (software tester) ของผู้พัฒนาระบบการลงคะแนน	ระบบการลงคะแนนมีการทดสอบโดยทีมงานขององค์กรซึ่ง มีการจัดทำรายงานผลการทดสอบตาม Test Case ที่ครอบคลุมเงื่อนไขทั้งหมดในระบบ ซึ่งรวมถึง Regression Test ด้วยเมื่อมีการพัฒนาหรือแก้ไขส่วนที่กระทบระบบงานหลัก
2. การพัฒนาระบบ (System Development) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการพัฒนาระบบโดยใช้แนวปฏิบัติที่ดี		
2.1 – การพัฒนาระบบการลงคะแนนใช้แนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์	ระบบการลงคะแนนใช้ภาษาโปรแกรมและรูปแบบการเขียนโปรแกรมที่เป็นที่ยอมรับ รวมถึงแนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์ เช่น มาตรฐาน ISO/IEC/IEEE 12207 Systems and software engineering – Software life cycle	ระบบการลงคะแนนถูกพัฒนาด้วยภาษา Java ซึ่งเป็นภาษาที่ผู้พัฒนาภาษายังรองรับการใช้งานอยู่ โดยมีการนำเอามาตรฐาน ISO/IEC 29110 Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs) มาใช้เป็นแนวปฏิบัติที่ดีในการพัฒนาระบบการลงคะแนน ดังนี้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	processes และ ISO/IEC 29110 Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs)	1. Initiation 2. Requirement Analysis 3. Architect and Detailed Design 4. Development 5. Integration and Test 6. Delivery
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน (modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ	ระบบการลงคะแนนถูกพัฒนามีการใช้ MVC framework ในการพัฒนา ซึ่งมีการแยกส่วนของ Logic การประมวลผลและการแสดงผลออกจากกัน ซึ่งสามารถทดสอบและตรวจสอบระบบแบบแยกแต่ละส่วนได้
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้ (self-modifying code)	1. ระบบการลงคะแนนมีการกำหนด Version Control ของ Source Code โดยมีเก็บรายละเอียดที่ได้มีการพัฒนาหรือปรับปรุงแก้ไข 2. ระบบการลงคะแนนมีการเข้ารหัสข้อมูลที่ระบบส่งผ่านเครือข่าย internet เพื่อป้องกันการถูกแก้ไขโดยไม่ได้รับอนุญาต 3. ระบบการลงคะแนนมีการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย โดยไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน	1. ระบบการลงคะแนนมีการออกแบบให้รองรับการจัดการ data replication เพื่อจัดการและกู้คืนข้อมูลจากข้อผิดพลาดหรือล้มเหลว 2. ระบบการลงคะแนนมีการใช้ google cloud ซึ่งเป็น cloud server provider ที่รองรับการเป็น DR site กรณีระบบงานหลักมีข้อผิดพลาดหรือล้มเหลว 3. มีการบันทึกข้อผิดพลาดหรือล้มเหลวของระบบ และแจ้งเตือนให้ผู้รับผิดชอบทราบเมื่อเกิดเหตุ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
3. ความโปร่งใส (Transparent) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนและกระบวนการลงคะแนนมีการออกแบบที่มีความโปร่งใส		
3.1 – เอกสารอธิบายการออกแบบ การทำงาน การเข้าถึงมาตรการความมั่นคงปลอดภัย 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)	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารดังนี้ 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) ● สำหรับผู้เข้าร่วมประชุม ● สำหรับผู้ควบคุมระบบ
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนน เตรียมไว้พร้อมสำหรับการตรวจสอบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารวิธีการตั้งค่า การตรวจสอบความพร้อมและการเฝ้าระวังการทำงานของระบบการลงคะแนน โดยบริษัทเป็นผู้ดำเนินการทั้งหมด
3.3 – บุคคลที่เกี่ยวข้องกับระบบการลงคะแนนสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)	1. ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) และรูปแบบของบันทึกเหตุการณ์ (log format) ของระบบการลงคะแนนโดยระบบการลงคะแนนสามารถออกรายงานข้อมูล activity log เพื่อตรวจสอบเหตุการณ์การลงคะแนนของผู้เข้าร่วมประชุมรายบุคคลได้ตลอดกระบวนการลงคะแนน 2. มีการจัดทำเอกสารที่อธิบายรายละเอียดของ log format ดังนี้ (1) Timestamp (2) ข้อมูลผู้ลงคะแนน (3) ประเภทของ activity log (4) IP Address (5) รายละเอียดของแต่ละ activity

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
4. การเข้าถึงอย่างเท่าเทียม (Equitable Access) <u>วัตถุประสงค์</u> เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม		
4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงผลภาพและเสียง) และรูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัสบนหน้าจอ) ในลักษณะที่สอดคล้องกัน	ระบบการลงคะแนน ใช้วิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ในทุกช่องทางมีฟังก์ชันในการลงคะแนน และการตรวจสอบผลการลงคะแนนที่เหมือนกัน โดยเข้าใช้งานผ่าน browser ที่รองรับการแสดงผลแบบ responsive ในทุกอุปกรณ์ ไม่ว่าจะเป็นคอมพิวเตอร์ Tablet หรือโทรศัพท์มือถือ
4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ	รูปแบบการแสดงผล (display format) แสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน และไม่ทำให้เกิดอคติกับตัวเลือกลงคะแนนใด ๆ ที่นำเสนอต่อผู้ลงคะแนน เช่น ตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน	ระบบการลงคะแนนมีการแสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน โดยตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยด้วยปุ่ม โดยใช้อักษรที่มีขนาด สี และลักษณะเหมือนกัน
5. การลงคะแนนตรงตามเจตนา (Cast as Intended) <u>วัตถุประสงค์</u> เพื่อให้การแสดงผลข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้		
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงตามความต้องการของผู้ลงคะแนน	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล (preference setting) ตามความต้องการของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษร และสีของภาพ	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคน ไม่รองรับการตั้งค่าส่วนบุคคล (Preference setting) ตามความต้องการของผู้ลงคะแนน แต่สามารถปรับเพิ่มลดขนาดการแสดงผลของหน้าจอ เช่น ตัวหนังสือและปุ่มสำหรับลงคะแนนได้ตามต้องการผ่าน browser
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง เช่น รูปแบบการแสดงผลของข้อมูล (display format) การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้าถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ (touch screen gestures) รวมถึงระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) เช่น การให้ผู้ลงคะแนนยืนยันเจตนาในการ	- ผู้ลงคะแนนสามารถควบคุมการลงคะแนนในวาระที่ต้องการ ได้โดยการเลื่อนหน้าจอขึ้น/ลง โดยการใช้ท่าทางสัมผัสบนหน้าจอ - ผู้ลงคะแนนสามารถควบคุมการลงคะแนนได้โดยตรง สามารถลงคะแนนเสียง (1) เห็นด้วย (2) ไม่เห็นด้วย (3) งดออกเสียง - ระบบการลงคะแนนจะแสดงการลงคะแนนล่าสุดให้ผู้ลงคะแนนทราบ - ในกรณีที่ผู้ลงคะแนนต้องการเปลี่ยนแปลงการลงคะแนน สามารถทำได้ด้วยตนเองจนกว่าวาระนั้นจะปิดรับการลงคะแนน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ลงคะแนนก่อนส่งผลลงคะแนน หรือการแจ้งสถานะของการลงคะแนนให้ผู้ลงคะแนนทราบ	ระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ โดยการให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนนทุกครั้ง
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน คำแนะนำ และข้อความจากระบบด้วยภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งข้อความที่ไม่ให้เกิดความสับสนในการลงคะแนน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต หรือการเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) และการแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว นอกจากนี้ ระบบมีการแสดงคำแนะนำ และข้อความที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ	ระบบการลงคะแนนมีการออกแบบหน้าจอแสดงเฉพาะข้อมูลที่จำเป็นและไม่ซับซ้อน เพื่อให้ผู้ลงคะแนนสามารถใช้งานได้ง่าย โดย 1. มีการแสดงชื่อวาระและปุ่มให้ผู้ลงคะแนนสามารถเลือกลงคะแนนตามวัตถุประสงค์ได้ทันที 2. มีการแจ้งเตือนผู้ลงคะแนนเพื่อยืนยันการลงคะแนน 3. มีการแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนน เช่น ไม่สามารถลงคะแนนได้ หลังจากการระงับปิดการลงคะแนนแล้ว เป็นต้น 4. มีการแสดงข้อมูลการลงคะแนนให้ผู้ลงคะแนนทราบ เมื่อลงคะแนนสำเร็จ นอกจากนี้ระบบการลงคะแนนมีการแสดงคำแนะนำและมีขั้นตอนการทำงานที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงาน
6. ความเหมาะสมต่อการใช้งาน (Usable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้เหมาะสม		
6.1 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบการลงคะแนน เพื่อให้มั่นใจว่าระบบการลงคะแนนสามารถใช้งานกับผู้ลงคะแนนทุกคน (ซึ่งอาจรวมถึงผู้สูงอายุ และบุคคลที่มีความบกพร่องทางการมองเห็น) ได้อย่างเหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี เช่น มาตรฐาน Web Content Accessibility Guidelines (WCAG) 2.0 ของ World Wide Web Consortium (W3C)	ผู้พัฒนาระบบการลงคะแนนมีการออกแบบและพัฒนาหน้าจอเพื่อให้ทุกคนสามารถเข้าถึงและใช้งานได้อย่างเท่าเทียมกัน รวมถึงผู้สูงอายุ (ยังไม่รองรับสำหรับบุคคลที่มีความบกพร่องทางการมองเห็น) โดยหน้าจอจะแสดงข้อความที่อ่านง่ายและชัดเจน รองรับทั้งภาษาไทยและภาษาอังกฤษ รวมถึงมีวิธีการลงคะแนนที่สะดวกไม่ซับซ้อน ซึ่งผ่านการประเมินหรือทดสอบความเหมาะสมต่อการใช้งานมาแล้วมากกว่า 1,000 ราย โดยมีผู้งานที่เป็นผู้สูงอายุคิดเป็นประมาณ 10%
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ	ผู้พัฒนาระบบการลงคะแนนมีการออกแบบขั้นตอนการดำเนินงานสำหรับผู้ควบคุมระบบการลงคะแนน ครอบคลุมการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ ซึ่งผ่านการประเมินหรือทดสอบความเหมาะสมต่อการใช้งานโดย บริษัทมหาชน บริษัทจำกัด สมาคมต่างๆ และนิติบุคคลที่ดูแลอาคารชุดหรือหมู่บ้านในการประชุมและลงคะแนน ด้วยการใช้งานจริงมาแล้วมากกว่า 500 ครั้ง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ		
7. การทำงานร่วมกัน (Interoperable)		
<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน		
7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนอยู่ในรูปแบบที่ทำงานร่วมกันได้หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐาน	ระบบการลงคะแนนมีการนำข้อมูลเข้าและออกอยู่ในรูปแบบมาตรฐานดังนี้ - นำเข้าข้อมูลผู้มีสิทธิลงคะแนนในรูปแบบไฟล์ Excel หรือรูปแบบมาตรฐานอื่นๆ ที่เป็น machine readable - ส่งออกข้อมูลการลงคะแนน ข้อมูล Log และรายงานผลการลงคะแนนในรูปแบบไฟล์ PDF และ Excel
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้รูปแบบมาตรฐาน ในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่างๆ	ระบบการลงคะแนนไม่มีการเชื่อมต่ออุปกรณ์ hardware อื่นๆ ในการลงคะแนน
8. การตรวจสอบ (Auditable)		
<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบความถูกต้องของผลลงคะแนน		
8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	ผลลงคะแนนที่ได้จากการลงคะแนนของผู้ลงคะแนน มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลได้ (tamper-evidence) ระบบการลงคะแนนเปิดโอกาสให้ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกไป แจ้งข้อผิดพลาดในผลลงคะแนนที่เกิดจากระบบการลงคะแนนและเริ่มต้นลงคะแนนใหม่หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน (ขึ้นอยู่กับกฎหมายหรือหลักเกณฑ์ที่กำหนด) รวมถึงควรมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ระบบการลงคะแนนต้องสร้างรายงานที่จะช่วยให้ผู้ตรวจสอบภายนอก (external auditor) สามารถตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง รวมถึงผู้พัฒนาระบบการลงคะแนนจัดทำขั้นตอนสำหรับการตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง	- ระบบการลงคะแนนมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ผ่านช่องทาง Call Center ซึ่งจะมีแสดงข้อมูลเบอร์ Call Center ตลอดระยะเวลาประชุม - ระบบการลงคะแนนมีการตรวจจับความผิดพลาดของการลงคะแนนโดยจะลงคะแนนได้ไม่เกินคะแนนที่ผู้ลงคะแนนมี โดยอัตโนมัติ - ระบบการลงคะแนนมีการเก็บ log การลงคะแนนของผู้ลงคะแนนทั้งหมด เพื่อใช้ในการตรวจสอบประวัติการเปลี่ยนแปลงการลงคะแนนได้ โดย log การลงคะแนนจะถูกเก็บในระบบในรูปแบบ read only ไม่สามารถแก้ไขได้ - ระบบการลงคะแนนมีรายงานแสดงข้อมูลผลการลงคะแนนแบบละเอียดที่จะช่วยให้ผู้ตรวจสอบภายนอกสามารถตรวจสอบได้ ผ่านการกำหนดสิทธิ์ของระบบ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
9. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy) ¹ <u>วัตถุประสงค์</u> เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง		
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่แสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนเข้าใช้งานระบบผ่าน URL เฉพาะของผู้ลงคะแนนแต่ละราย ทำให้การส่งผลลงคะแนนเป็นการดำเนินการเฉพาะบุคคล โดยไม่แสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่าส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน	1. ระบบการลงคะแนนมีการออกแบบหน้าจอแสดงเฉพาะข้อมูลที่จำเป็นและไม่ซับซ้อน เพื่อให้ผู้ลงคะแนนสามารถใช้งานได้ง่าย และสามารถทำได้ตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น 2. การแสดงผลมีความชัดเจน เมื่อผู้ใช้งานเข้าสู่ระบบและกดปุ่ม e-voting จะแสดงชื่อวาระและทางเลือกในการลงคะแนนที่ชัดเจน เมื่อมีการลงคะแนนระบบจะมีข้อความให้กดยืนยันการลงคะแนน เป็นการจบขั้นตอนการใช้งาน
10. ความลับของคะแนนเสียง (Vote Secrecy) <u>วัตถุประสงค์</u> (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน		
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	ระบบการลงคะแนนต้องไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มาประมวลผล จัดเก็บ หรือแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว	ระบบการลงคะแนนไม่รองรับการลงคะแนนเสียงลับ
10.2 – ระบบการลงคะแนนไม่จัดทำข้อมูลเกี่ยวกับผู้ลงคะแนนหรือข้อมูลอื่น ๆ ที่สามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน นอกจากนี้ ผลลงคะแนนและผลรวมของการลงคะแนนต้องไม่มีข้อมูลที่ระบุตัวผู้ลงคะแนนและข้อมูลที่สามารถใช้หาลำดับของการส่งผลลงคะแนนได้ อย่างไรก็ตาม ในกรณีที่ให้ผู้ลงคะแนนส่งผลลงคะแนนก่อนจะตรวจสอบการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนนสามารถใช้การเชื่อมโยงโดยอ้อม (indirect voter association) ที่เชื่อมโยงผู้ลงคะแนนกับผลลงคะแนน	ระบบการลงคะแนนไม่รองรับการลงคะแนนเสียงลับ

¹ ความเป็นส่วนตัวของผู้ลงคะแนน ในที่นี้หมายถึง ความเป็นส่วนตัวที่เกิดขึ้นภายในระบบการลงคะแนนเท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ที่ถูกเข้ารหัสลับไว้ โดยหลังจากตรวจสอบแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้น จึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับ และนำไปนับคะแนนเป็นผลรวมของการลงคะแนน	
11. การควบคุมการเข้าถึง (Access Control) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น		
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน เพื่อให้มีหลักฐานสำหรับตรวจสอบในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งานเปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และลบบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง	1. ระบบการลงคะแนนมีการจัดเก็บ log กิจกรรมการใช้งานในระบบทั้งหมด ซึ่งมีข้อมูลที่ระบุตัวบุคคล วันและเวลา ซึ่งได้มีการเทียบเวลากับแหล่งเวลาที่เป็นมาตรฐานสากล รวมถึง IP Address ของอุปกรณ์ที่ได้ใช้งาน 2. บันทึก log ถูกกำหนดให้ไม่สามารถแก้ไขเปลี่ยนแปลงหรือลบบันทึก 3. ระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึก log เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เกี่ยวข้องเฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนน และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดบัญชีผู้ใช้งานที่ได้รับอนุญาต กำหนดบทบาทของผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละบทบาทของผู้ใช้งาน	ระบบการลงคะแนนมีการจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยมีบทบาทหน้าที่ดังนี้ ● ผู้ควบคุมระบบ ทำหน้าที่ตั้งค่าและดูแลระบบงาน รวมถึงเป็นคนกำหนดบัญชีผู้ใช้งานที่ได้รับอนุญาต โดยจะสร้างให้เฉพาะผู้ที่เกี่ยวข้องและรับผิดชอบในแต่ละบทบาทหน้าที่เท่านั้น ● ผู้ควบคุมการประชุม ทำหน้าที่ควบคุมการประชุมให้เป็นตามวาระที่กำหนด ● ผู้ตรวจสอบภายนอก ทำหน้าที่ตรวจสอบความถูกต้องของผลคะแนนผ่านระบบและรายงาน ● ผู้เข้าร่วมประชุม สามารถลงคะแนนเสียงและตรวจสอบการลงคะแนน
11.3 – ระบบการลงคะแนนรองรับวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน	ระบบการลงคะแนนใช้วิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน เพื่อตรวจสอบว่าเป็นผู้ใช้งานที่ได้รับอนุญาตจริง และใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน เพื่อตรวจสอบว่าเป็นผู้ที่มีสิทธิเข้าถือการดำเนินการที่สำคัญ (เช่น การเปิดลงคะแนน การปิด	1. ระบบการลงคะแนนมีการพิสูจน์และยืนยันตัวตนที่ปลอดภัยสำหรับผู้ใช้งาน โดยผู้เข้าร่วมประชุมได้รับการอนุมัติให้เข้าร่วมประชุม จะได้รับ unique token แบบมั่นคงปลอดภัยส่งให้ทางอีเมล เพื่อให้ผู้เข้าร่วมประชุมใช้ในการยืนยันตัวตนด้วยข้อมูลส่วนตัวอีกครั้งเพื่อเข้าใช้งานและมีการจำกัดการเข้าใช้งาน เฉพาะอุปกรณ์และเครือข่ายที่เกี่ยวข้อง ซึ่งระบบจะไม่อนุญาตให้ผู้เข้าร่วมประชุมใช้ token เดียวกันเข้าประชุมในระบบพร้อมกัน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
authentication) สำหรับผู้ควบคุมระบบการลงคะแนน	ลงคะแนน) ทั้งนี้ วิธีการพิสูจน์และยืนยันตัวตนอาจพิจารณาข้อกำหนดตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) จากมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ระบบการลงคะแนนต้องเก็บรักษาข้อมูลยืนยันตัวตน (เช่น รหัสผ่าน) โดยมีการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล และหากระบบการลงคะแนนใช้วิธีการยืนยันตัวตนด้วยรหัสผ่าน ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดความเข้มงวดและการหมดอายุของรหัสผ่าน	2. ระบบการลงคะแนนมีการใช้วิธีการยืนยันตัวตนแบบ multi-factor authentication สำหรับผู้ควบคุมการลงคะแนน โดยใช้ (1) username password (2) รหัส OTP 6 หลักที่จะถูกจัดส่งไปที่อีเมลของผู้ควบคุมการลงคะแนน เมื่อมีการใช้งานระบบโดยจะต้องใช้งานภายใน 5 นาที
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลดสิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่ (separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น	ระบบการลงคะแนนมีการกำหนดสิทธิการเข้าถึงระบบงานดังนี้ ● ผู้ควบคุมระบบ ทำหน้าที่ตั้งค่าและดูแลระบบงาน ● ผู้ควบคุมการประชุม ทำหน้าที่ควบคุมการประชุมให้เป็นตามวาระที่กำหนด ● ผู้ตรวจสอบภายนอก ทำหน้าที่ตรวจสอบความถูกต้องของผลคะแนนผ่านระบบและรายงาน ● ผู้เข้าร่วมประชุม สามารถลงคะแนนเสียงและตรวจสอบการลงคะแนน
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด หากผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนควรระงับการใช้งาน (account lockout) ของผู้ใช้งานเป็นระยะเวลาหนึ่งก่อนจะให้นับยืนยันตัวตนครั้งต่อไป และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาการระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล	ระบบการลงคะแนนมีการกำหนดระยะเวลาของเซสชัน (session) ในกรณีผู้ใช้งานไม่ทำกิจกรรมภายในระยะเวลาที่กำหนด ผู้ใช้งานต้องทำการเข้างานระบบใหม่อีกครั้ง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
12. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย		
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐาน หรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาต หรือการถูกตัดการเชื่อมต่อทางกายภาพ เกิดขึ้นกับส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน ผู้พัฒนาระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อกที่มั่นคงปลอดภัย หรือระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ	ระบบการลงคะแนนถูกติดตั้งและให้บริการผ่านผู้ให้บริการ cloud ซึ่งมีมาตรการรักษาความปลอดภัยทางกายภาพตามมาตรฐานของ google cloud (https://cloud.google.com/security/compliance/iso-27001)
13. การคุ้มครองข้อมูล (Data Protection) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต		
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนน จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนน และระบบเครือข่าย รวมถึงระบบการลงคะแนนต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง	1. ระบบการลงคะแนนมีการกำหนดสิทธิการการเข้าใช้งาน สำหรับผู้ที่สามารถตั้งค่าของระบบการลงคะแนนและการตั้งค่าระบบเครือข่าย 2. ระบบการลงคะแนนมีการรักษาความครบถ้วนของการบันทึกการลงคะแนนด้วยการแฮชอัลกอริทึม (SHA256)
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับจากผู้ลงคะแนน บันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที และจัดเก็บบันทึกการลงคะแนนให้อยู่ในรูปแบบที่สามารถแสดงผลลงคะแนนที่ได้รับมาให้ปรากฏอย่างถูกต้องได้	ระบบการลงคะแนนออกแบบให้มีการบันทึกผลการลงคะแนนของผู้ลงคะแนน โดยระบบจะแสดงผลการลงคะแนนให้ผู้ลงคะแนนตรวจสอบทันที กรณีที่ระบบตรวจพบข้อผิดพลาดต้องไม่นำคะแนนมานับเป็นผลรวม
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 เข้ารหัสลับของข้อมูลการลงคะแนนในแต่ละการประชุม ผ่าน https protocol โดยจะทำการเข้ารหัสก่อนทำการส่งข้อมูลระหว่างเครือข่าย และเมื่อข้อมูลไปยังปลายทางจึงทำการถอดรหัส (data in transit) ซึ่งบริษัทมีนโยบายด้านการเข้ารหัสลับข้อมูลทุกระดับถึงการเข้ารหัสลับข้อมูล ดังนี้ 1. ข้อมูลที่เกี่ยวข้องบนระบบ และข้อมูลส่วนบุคคลที่เกี่ยวข้อง เช่น เลขบัตรประชาชน, เบอร์ติดต่อ 2. ระบบ มีการทำ Database Encryption ข้อมูลที่เกี่ยวข้องทั้งหมด (encryption at rest) อ้างอิงตาม https://cloud.google.com/docs/security/encryption/default-encryption

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด	การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายคอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)	ระบบการลงคะแนนมีการเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย โดยใช้ SSL Certificate ของ Let's Encrypt (SHA256) สำหรับเจ้าหน้าที่ผู้ดูแลระบบการลงคะแนนจะต้องมีการเชื่อมต่อผ่าน VPN สำหรับการบริหารจัดการระบบลงคะแนน
14. การรักษาความครบถ้วนของระบบ (System Integrity) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงาน และไม่มีการแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ		
14.1 – ระบบการลงคะแนนใช้การควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อรับมือภัยคุกคามหรือช่องโหว่ด้านความมั่นคงปลอดภัย	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) และวิธีการควบคุมเพื่อรับมือหรือลดความเสี่ยงจากภัยคุกคามแต่ละประเภทซึ่งอาจส่งผลกระทบต่อการทำงานของระบบการลงคะแนน รวมถึงอธิบายวิธีการควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อป้องกัน บรณา 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 ส่งผลให้ความเสี่ยงในด้านต่างๆ ลดลงอยู่ในระดับต่ำ (Low Impact) และมีโอกาสเกิดน้อย (Low Probability) 2. ระบบการลงคะแนนมีการควบคุมในหลายระดับชั้น เช่น การเข้ารหัสลับ (cryptography) ในระดับ Database Layer และป้องกันมัลแวร์ (malware) ในระดับ Server และ Network Layer
14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น	ระบบการลงคะแนนป้องกันการติดตั้งหรือการส่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง และปิดใช้งานการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน ซอฟต์แวร์ของระบบการลงคะแนนต้องไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และต้องเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น	1. ระบบการลงคะแนนมีการควบคุมการติดตั้ง source code หรือ software รวมถึงการเปิดการเชื่อมต่อเท่าที่จำเป็นเท่านั้น 2. มีการทบทวนตรวจสอบ unused code อย่างสม่ำเสมอ รวมถึงการใช้ภาษาหรือ library จากแหล่งที่น่าเชื่อถือและได้มาตรฐานเท่านั้น 3. มีการจัดทำแผนการบริหารจัดการช่องโหว่ โดยการ update patch ที่สำคัญอย่างสม่ำเสมอ ๆ
15. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน		
15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ	ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งประกอบด้วย	ระบบการลงคะแนนมีการบันทึก log ที่เกิดขึ้นในระบบลงคะแนน ตั้งแต่การเข้ามาในระบบงาน รวมถึงการลงคะแนนในวาระต่างๆ ซึ่งระบบรองรับการนำออก log ที่ขึ้นได้ในรูปแบบ csv

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	เหตุการณ์ที่เกี่ยวข้องกับสถานะการทำงานและความผิดปกติของระบบ การยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน การจัดการระบบเครือข่าย การจัดการซอฟต์แวร์ 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 และมีการแจ้งเตือนผู้ควบคุมระบบการลงคะแนนทันทีเมื่อตรวจสอบพบ malware อ้างอิง https://cloud.google.com/architecture/mitigating-ransomware-attacks#security-and-resiliency-controls-in-google-cloud
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	1. ระบบการลงคะแนนมีการออกแบบสถาปัตยกรรมระบบเครือข่ายของเครือข่ายภายใน โดยใช้ cloud server ของ google cloud รูปแบบ IaaS พร้อมติดตั้ง firewall โดยกำหนด firewall rule เฉพาะเจาะจงสำหรับระบบงาน เพื่อป้องกันระบบเครือข่ายภายใน 2. มีการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูลครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโอนย้ายข้อมูล ตามมาตรฐาน ISO 27001 และ ISO 27017 นอกจากนี้ระบบมีการ backup ข้อมูลทุกวัน มีการกำหนด security configuration อ้างอิงตาม practice ของ google cloud https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf