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

ชื่อระบบ	ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ELECTRONIC VOTING SYSTEM)
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท)	บริษัท ไอแอพพ์เทคโนโลยี จำกัด
ช่องทางการติดต่อผู้ให้บริการ	80/359 หมู่ที่ 3 ซอยคลองหลวง 26 ตำบลคลองหนึ่ง อำเภอคลองหลวง จ.ปทุมธานี โทร. 06-5979-6788, 09-4557-4066 อีเมล info@iapp.co.th, supap@iapp.co.th, amornrat@iapp.co.th
วันที่ประเมินความสอดคล้อง	*12 พฤษภาคม 2569*
วันที่ครบกำหนดการทบทวน	*11 พฤษภาคม 2570 (นับถัดจากวันที่ประเมินความสอดคล้อง 1 ปี)*
ประเภทของระบบการให้บริการ	☒ On Cloud ☒ On Premise ☒ อื่น ๆ โปรดระบุ...เช่าบริการ
การใช้งานระบบการลงคะแนน	☐ ร่วมกับระบบการประชุมฯ ☒ แยกกับระบบการประชุมฯ
มาตรฐานที่ได้รับการรับรอง	☐ ISO/IEC 27001 ☐ ISO/IEC 27701 ☐ อื่น ๆ โปรดระบุ
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง	

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 และการรายงานผลรวมของการ	ระบบการลงคะแนนมีการออกแบบฟังก์ชันการใช้งานให้รองรับกระบวนการลงคะแนนตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องกับการประชุมผู้หุ้น ประชุมคณะกรรมการบริษัท/สมาคม/หน่วยงานราชการ รัฐวิสาหกิจ ประชุมเจ้าของร่วมหมู่บ้าน/นิติบุคคลอาคารชุด เป็นต้น โดยมีรายละเอียดดังนี้ 1. การเตรียมข้อมูลสำหรับการลงคะแนน หน่วยงานจะเป็นผู้จัดเตรียมข้อมูล ข้อกำหนด คำอธิบาย ความสามารถของระบบการลงคะแนน 2. ผู้ใช้งาน (User) ภายในระบบ แบ่งออกเป็น 3 บทบาท ได้แก่

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ลงคะแนน	2.1 ผู้ดูแลระบบ (System Administrator) 2.2 ผู้ควบคุมการลงคะแนน (Vote Controller) 2.3 ผู้มีสิทธิ์การลงคะแนน 3. การตั้งค่าของระบบประกอบด้วยฟังก์ชันการทำงาน ดังนี้ 3.1 มีฟังก์ชันในการบริหารจัดการผู้ใช้งาน (user management) ของระบบ 3.2 มีฟังก์ชันในการบริหารจัดการเทมเพลตของการลงคะแนน (vote templates) 3.3 มีฟังก์ชันในการกำหนดวันเวลา เปิด-ปิด การเลือกตั้ง 3.4 มีฟังก์ชันรูปแบบการยืนยันตัวตนเพื่อเข้าสู่ระบบ - ผ่านฐานข้อมูลกรมการปกครอง - ผ่านฐานข้อมูลหน่วยงาน - ผ่านฐานข้อมูลในระบบ - OTP ผ่านหมายเลขโทรศัพท์ 3.5 มีฟังก์ชันการกำหนดข้อความ SMS ได้แก่ - ข้อความ OTP ยืนยันเข้าสู่ระบบ - ข้อความ เชิญเลือกตั้ง - ข้อความเลือกตั้งสำเร็จ - ข้อความเลือกตั้งไม่สำเร็จ 3.6 ฟังก์ชันกำหนดพื้นหลัง และข้อความการเลือกตั้ง 3.7 ฟังก์ชันกำหนดข้อมูลการติดต่อ 3.8 ฟังก์ชันเพิ่มบัตรเลือกตั้ง 3.9 ฟังก์ชันข้อมูลรายชื่อผู้มีสิทธิ์เลือกตั้ง 3.10 ฟังก์ชันรายงานสถิติการเลือกตั้ง 3.11 ฟังก์ชันรายการแจ้งคำร้องเรียน 3.12 ฟังก์ชันการตั้งค่าผู้ใช้งานระบบ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		3.13 ฟังก์ชันสร้าง Public Key และ Private Key จากข้อมูลบัตรสรรหาและรายชื่อผู้มีสิทธิเลือกตั้ง รวมทั้งการเก็บ Private Key เพื่อความปลอดภัยและเป็นการรับประกันความลับของข้อมูลการเลือกตั้ง
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ (system accuracy and reliability) การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) ในสภาวะที่ใกล้เคียงกับการใช้งานจริงในกระบวนการลงคะแนน และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)	ระบบการลงคะแนนมีการทดสอบ ดังนี้ - ระบบมีการทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด โดยการทดสอบยิง Request ผ่าน Amazon Webservice - ระบบมีการจัดทำ Load Test หรือ Performance Test โดยจำลองการใช้งานเหมือนจริง ตั้งแต่กระบวนการลงคะแนน และประมวลผลคะแนน ของผู้เลือกตั้ง ทั้งนี้ระบบสามารถรองรับผู้เลือกตั้งได้ไม่น้อยกว่า 1,000 concurrent ต่อ นาที
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบซอฟต์แวร์ (software tester) ของผู้พัฒนาระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำรายงานผลการทดสอบ โดยมีการจัดทำรายงาน Test Case เพื่อยืนยันการทดสอบคุณสมบัติของระบบว่าเป็นไปตามที่ผู้พัฒนาออกแบบโดยกำหนดให้ทดสอบทุกครั้ง เพื่อนำไปใช้ในปีถัดไป
2. การพัฒนระบบ (System Development) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการพัฒนาระบบโดยใช้แนวปฏิบัติที่ดี		
2.1 – การพัฒนาระบบการลงคะแนนใช้แนวปฏิบัติที่ดีใน การพัฒนาซอฟต์แวร์	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)	ระบบการลงคะแนนถูกพัฒนาในโปรแกรมภาษาที่ผู้พัฒนาภาษายังรองรับการใช้งาน ณ ปัจจุบันดังนี้ - Nextjs - Nodejs ซึ่งมีการออกแบบให้ผู้ใช้งาน ใช้งานง่ายไม่ซับซ้อน โดยออกแบบระบบลงคะแนน ให้มีความสอดคล้องกับกฎหมายและหลักเกณฑ์ที่กำหนด โดยมีการพัฒนาตามมาตรฐาน ISO/IEC 29110-4-1:2008 และหลัก SDLC 7 ขั้นตอน ในรูปแบบ Agile Model ดังนี้ 1. ขั้นตอนการวางแผน (Planning Stage) 2. ความเป็นไปได้หรือข้อกำหนดของขั้นตอนการวิเคราะห์ (Feasibility or Requirements of Analysis Stage) 3. ขั้นตอนการออกแบบและการสร้างต้นแบบ (Design and Prototyping Stage) 4. ขั้นตอนการพัฒนาซอฟต์แวร์ (Software Development Stage) 5. ขั้นตอนการทดสอบซอฟต์แวร์ (Software Testing Stage)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		6. การดำเนินการและการรวมระบบ (Implementation and Integration) 7. ขั้นตอนการปฏิบัติการและบำรุงรักษา (Operations and maintenance Stage)
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน(modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ	ระบบการลงคะแนน มีการแยกส่วนการทำงานที่ชัดเจนผ่าน API ทั้งหมด โดยแยกส่วนออกมาคือ 1. ข้อมูลผู้มีสิทธิเลือกตั้งลงคะแนน 2. ข้อมูลสถิติรายวัน โดยระบบแสดงข้อมูลดังนี้ - แสดงข้อมูลจำนวนผู้มาใช้สิทธิเลือกตั้งทั้งหมด ● จำนวนผู้มาใช้สิทธิเลือกตั้งทั้งหมด /คน ● จำนวนผู้ยังไม่ได้ใช้สิทธิเลือกตั้ง /คน - จำนวนผู้มาใช้สิทธิเลือกตั้งวันนี้ /คน - จำนวนผู้มีสิทธิเลือกตั้ง - แสดงข้อมูลจำนวนผู้มาใช้สิทธิเลือกตั้งรายวัน - แสดงข้อมูลจำนวนผู้มาใช้สิทธิเลือกตั้งรายชั่วโมง - จำนวนผู้ทำการเลือกตั้งสำเร็จ ต่อจำนวนการเข้าใช้งาน ● จำนวนการเข้าใช้งานทั้งหมด /คน ● จำนวนผู้ที่ทำการเลือกตั้งสำเร็จ /คน - จำนวน SMS ที่ทำการส่ง - ค่าเฉลี่ยผู้มาใช้สิทธิเลือกตั้ง ต่อวัน/ชั่วโมง 3. นับคะแนนการเลือกตั้งแบบอิเล็กทรอนิกส์ (E-Voting) 4. แจ้งคำร้องเรียน 5. การตั้งค่าผู้ใช้งาน (รายชื่อผู้ใช้งาน) 6. Generate Key
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้ (self-modifying code)	- ระบบการลงคะแนนมีการกำหนดเวอร์ชัน และควบคุมระบบโดยเก็บรายละเอียดในแต่ละเวอร์ชัน มีการปรับปรุง/แก้ไข หรือเพิ่มเติม อะไรบ้าง - การทำงานของระบบมีชุดคำสั่งการทำงาน ที่ถูกออกแบบให้ทำงานเฉพาะเจาะจงเท่านั้น - ระบบการลงคะแนนออกแบบให้มีการเข้ารหัสก่อน การเข้าถึงข้อมูลก่อนส่ง API เพื่อปกป้องข้อมูลที่อยู่ในระบบให้มีความปลอดภัย

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน	- ระบบการลงคะแนนมีการจัดทำ Disaster Recovery Site เพื่อรองรับกรณีที่ Application หรือ Database ที่ Primary Site ไม่สามารถใช้งานได้ เพื่อป้องกันการหยุดชะงักของการ ดำเนินงาน มีการกำหนดแผนในการทำ Disaster Recovery ระหว่างทีม Infrastructure, ทีม Network และทีม Application จากการทดสอบมีการกำหนดระยะเวลาในการกู้คืน ระบบดังต่อไปนี้ • Recovery Time Objective (RTO) 10 นาที • Recovery Point Objective (RPO) 5 นาที
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)	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารเกี่ยวกับระบบการลงคะแนนเพื่อให้สามารถอ่านและทำความเข้าใจได้อย่างครบถ้วน 1. Functional Specification 2. ภาพรวมของระบบ (system overview) 3. ประสิทธิภาพของระบบ (system performance) 4. ความมั่นคงปลอดภัยของระบบ (system security) 5. การติดตั้งซอฟต์แวร์ (software installation) 6. การทำงานของระบบ (system operations) 7. คู่มือการใช้งาน (user manual) ระบบการลงคะแนนสามารถตรวจสอบความถูกต้องของที่มาของผลคะแนนได้ในแต่ละขั้นตอนโดยมีรายงานประกอบสำหรับการตรวจสอบ ส่งให้กับผู้ใช้บริการ (ลูกค้า)
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนน เตรียมไว้พร้อมสำหรับการตรวจสอบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ	มีการจัดทำเอกสารวิธีการติดตั้ง / ตั้งค่า และวิธีการตรวจสอบการทำงาน โดยทางบริษัท เป็นผู้ดำเนินการติดตั้ง ตั้งค่าและการตรวจสอบระบบทั้งหมด

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
3.3 – บุคคลที่เกี่ยวข้องกับระบบการลงคะแนนสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)	เจ้าหน้าที่ควบคุมระบบสามารถออกรายงานข้อมูลอิเล็กทรอนิกส์ได้ เพื่อตรวจสอบ การลงคะแนน และเหตุการณ์ในการใช้งานระบบของผู้ใช้งานซึ่งมีการจัดเก็บข้อมูลทุกการกระทำที่ผู้ใช้งานกระทำกับระบบ เช่น View, Insert, Update แยกเป็น รายบุคคลโดยมีการอธิบายรูปแบบของการบันทึกเหตุการณ์ทั้งหมด
4. การเข้าถึงอย่างเท่าเทียม (Equitable Access) วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม		
4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงภาพและเสียง) และรูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัสบนหน้าจอ) ในลักษณะที่สอดคล้องกัน	ระบบการลงคะแนนมีฟังก์ชันในการลงคะแนน และตรวจสอบผลการลงคะแนน โดยมีการแสดงผลและมีปฏิสัมพันธ์ที่สอดคล้องกัน คือระบบมีการแสดงปุ่มการออกเสียง ลงคะแนนให้ทราบ และเมื่อมีการยืนยันผลการลงคะแนนระบบจะแสดงแจ้งเตือนข้อมูล เพื่อแจ้งให้ผู้ใช้งานทราบถึงการดำเนินการลงคะแนนเสียงสำเร็จ และแสดงผลลัพธ์ได้อย่างถูกต้อง โดยผู้ใช้งานสามารถเข้าใช้ผ่าน Web browser (web responsive) ทำให้สามารถเข้าใช้งานได้ทุกอุปกรณ์ เช่น คอมพิวเตอร์ หรือโทรศัพท์เคลื่อนที่
4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ	รูปแบบการแสดงผล (display format) แสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน และไม่ทำให้เกิดอคติกับตัวเลือกลงคะแนนใด ๆ ที่นำเสนอต่อผู้ลงคะแนน เช่น ตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน	ระบบมีการแสดงข้อมูล และตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนน อย่างเท่าเทียมกัน โดยระบบมีการออกแบบปุ่มและแบบอักษรลักษณะเดียวกัน
5. การลงคะแนนตรงตามเจตนา (Cast as Intended) วัตถุประสงค์ เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบ ตัวเลือกลงคะแนน และส่งผลลงคะแนนได้		
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล (preference setting) ตามความต้องการ	ระบบการลงคะแนน (E-Voting) มีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก ตามลักษณะของ Mobile Device (Responsive design) และไม่สามารถปรับแต่งค่าตามความต้องการของผู้ใช้งานรายบุคคลได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงกับความต้องการของผู้ลงคะแนน	ของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษร และสีของภาพ	
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง เช่น รูปแบบการแสดงผลของข้อมูล (display format) การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้าถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ (touch screen gestures) รวมถึงระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) เช่น การให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนน หรือการแจ้งสถานะของการลงคะแนนให้ผู้ลงคะแนนทราบ	ระบบการลงคะแนนออกแบบให้ผู้ลงคะแนนสามารถ สามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนน หรืองดออกเสียงได้โดยตรง และมีแจ้งเตือนให้ยืนยันอีกครั้งก่อนส่งผลลงคะแนน เพื่อยืนยันเจตนาในการ ลงคะแนนของผู้ใช้
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน คำแนะนำ และข้อความจากระบบด้วยภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งข้อความที่ไม่ให้เกิดความสับสนในการลงคะแนน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต หรือการเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) และการแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว นอกจากนี้ ระบบมีการแสดงคำแนะนำและข้อความที่ชัดเจนสำหรับผู้ควบคุม	ระบบมีการออกแบบให้ผู้ใช้งานสามารถเข้าใจและใช้งานได้ง่าย โดยมีการแยกเมนูการใช้งานอย่างชัดเจน รวมถึงมีการแสดงข้อความแจ้งเตือนเป็นลักษณะ Pop-up หรือ Toast Notifications เช่น แจ้งเตือนเพื่อยืนยันการลงคะแนน และแจ้งเตือนเมื่อทำการลงคะแนนสำเร็จ ให้ทราบตามสิทธิของผู้ใช้งาน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ	
6. ความเหมาะสมต่อการใช้งาน (Usable)		
6.1 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบการลงคะแนน เพื่อให้มั่นใจว่าระบบการลงคะแนนสามารถใช้งานกับผู้คะแนนทุกคน (ซึ่งอาจรวมถึงผู้สูงอายุและบุคคลที่มีความบกพร่องทางการมองเห็น) ได้อย่างเหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี เช่น มาตรฐาน Web Content Accessibility Guidelines (WCAG) 2.0 ของ World Wide Web Consortium (W3C)	ผู้พัฒนามีการออกแบบให้ระบบใช้งานอย่างไม่ซับซ้อน เพื่อลดปัญหาในการใช้งานของทุกกลุ่มเป้าหมาย โดยใช้ภาษาที่ชัดเจนอ่านง่าย และใช้การแสดงตำแหน่งข้อมูลที่เหมาะสม ซึ่งระบบมีการรองรับภาษาในการใช้งานทั้งภาษาไทยและอังกฤษ ทางผู้พัฒนามีการประเมินจากกลุ่มผู้ใช้งาน โดยมีการจัดทำตัวอย่างข้อมูลช่วงอายุของผู้ใช้งาน ดังนี้ - ช่วงที่ 1 อายุ ไม่เกิน 40 ปี ช่วงที่ 2 อายุ 40-60 ปี และ ช่วงที่ 3 อายุ 60 ปี ขึ้นไป โดยผู้ใช้งานทั่วไปไม่พบปัญหาการใช้งานในส่วนหน้าจอ ลงคะแนน หรือวิธีการลงคะแนน (อ้างอิง การใช้งาน Evoting) ซึ่งการพัฒนาระบบจะดำเนินการพัฒนาจากระบบงานเดิม โดยมีการแยกจาก Version ที่ ใช้งาน ทำให้มีการเก็บทั้ง Version เดิม และ Version ที่จะใช้ในปีถัดไป
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ	ผู้พัฒนามีการออกแบบขั้นตอนการดำเนินงานของระบบที่เหมาะสม และครอบคลุม การใช้งาน เพื่อช่วยให้ผู้ควบคุมระบบสามารถใช้งานได้ง่าย โดยผู้ควบคุมการลงคะแนนตรวจสอบจาก Activity Log ของ หน้าการลงคะแนน ซึ่งมีการแสดงผลลัพธ์การลงคะแนนเป็นสำเร็จ (Success) และระบบผ่านการประเมินความเหมาะสมต่อการใช้งานโดยผู้ควบคุมระบบการลงคะแนนแล้ว
ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ		
7. การทำงานร่วมกัน (Interoperable) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน		
7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนอยู่ในรูปแบบที่ทำงานร่วมกันได้หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐาน	- ระบบมีการนำเข้าข้อมูล ในรูปแบบไฟล์ Excel เช่น ไฟล์รายชื่อผู้ใช้งานที่มีสิทธิในการลงคะแนน - ระบบรองรับการส่งออกข้อมูลรายงาน ในรูปแบบไฟล์ Excel เช่น รายงาน Activity Log และรายงานสรุปผลการลงคะแนน
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้	ระบบไม่มีการรองรับการเชื่อมต่อกับฮาร์ดแวร์อื่น หรือเครื่องลงคะแนนอิเล็กทรอนิกส์อื่น เนื่องจากระบบมีการใช้งานผ่าน Web browser เท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	รูปแบบมาตรฐาน ในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่าง ๆ	
8. การตรวจสอบ (Auditable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบความถูกต้องของผลลงคะแนน		
8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	ผลลงคะแนนที่ได้จากการลงคะแนนของผู้ลงคะแนน มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลได้ (tamper-evidence) ระบบการลงคะแนนเปิดโอกาสให้ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกไป แจ้งข้อผิดพลาดในผลลงคะแนนที่เกิดจากระบบการลงคะแนน และเริ่มต้นลงคะแนนใหม่หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน (ขึ้นอยู่กับกฎหมายหรือหลักเกณฑ์ที่กำหนด) รวมถึงควรมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ระบบการลงคะแนนต้องสร้างรายงานที่จะช่วยให้ผู้ตรวจสอบภายนอก (external auditor) สามารถตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง รวมถึงผู้พัฒนาระบบการลงคะแนนจัดทำขั้นตอนสำหรับการตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง	- ระบบออกแบบให้มีการตรวจสอบข้อผิดพลาดที่เกิดขึ้น จะมีติดต่อสำหรับการแจ้งเหตุขัดข้องที่เกิดขึ้นระหว่างการลงคะแนนได้ โดยมีการจัดเก็บหลักฐานในรูปแบบของรายงาน Activity Log ซึ่งผู้ตรวจสอบสามารถออกรายงานจากระบบเพื่อตรวจสอบข้อผิดพลาดที่เกิดขึ้นได้ - ระบบสามารถตรวจสอบผลการลงคะแนน และออกรายงานสรุปผลคะแนน ได้อย่างถูกต้อง
9. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy) วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง		
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่แสดงหรือเปิดเผยข้อมูล	ระบบรองรับการยืนยันตัวตนสำหรับผู้เข้าร่วมลงคะแนนที่หลากหลาย ตาม Solution ของหน่วยงาน ได้แก่ ● ผ่านฐานข้อมูลกรมการปกครอง (หน่วยงานจัดเตรียมข้อมูล) ● ผ่านฐานข้อมูลหน่วยงาน (หน่วยงานจัดเตรียมข้อมูล)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	ดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน	• ผ่านฐานข้อมูลในระบบ • OTP ผ่านหมายเลขโทรศัพท์ สำหรับการเข้าใช้ระบบลงคะแนน ทำให้การลงคะแนนเสียงเป็นการลงคะแนนเสียงเฉพาะบุคคลไม่มีการเปิดเผยข้อมูลต่อบุคคลอื่น เพื่อรักษาความเป็น ส่วนตัวของผู้เข้าร่วมลงทะแนน
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่าส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนมีการออกแบบให้ผู้เข้าร่วมลงคะแนนเข้าใจได้ง่าย โดยสามารถเข้ามาเลือกวาระที่ต้องการลงคะแนน ได้โดยมี SMS ข้อความแจ้งเตือนแจ้งไปยังมือถือผู้เข้าร่วมลงทะเบียนเ ทำการลงคะแนน ยืนยันการลงคะแนน และสามารถตรวจสอบผลการลงคะแนนได้ด้วยตนเอง
10. ความลับของคะแนนเสียง (Vote Secrecy) <u>วัตถุประสงค์</u> (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน		
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	ระบบการลงคะแนนต้องไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มาประมวลผล จัดเก็บ หรือแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว	การลงคะแนน ระบบจะสรุปผลการลงคะแนนโดยแสดงข้อมูลสรุปเฉพาะข้อมูลผลการ ลงคะแนน และจำนวนผู้ออกเสียงลงคะแนน โดยแยกตามหมายเลขผู้สมัครที่ได้คะแนน และจำนวนผู้งดออกเสียง/ไม่ประสงค์ลงคะแนน โดยไม่มีข้อมูลส่วนบุคคลใดๆของผู้ลงคะแนนมาแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว
10.2 – ระบบการลงคะแนนไม่จัดทำข้อมูลเกี่ยวกับผู้ลงคะแนนหรือข้อมูลอื่น ๆ ที่สามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน นอกจากนี้ ผลลงคะแนนและผลรวมของการลงคะแนนต้องไม่มีข้อมูลที่ระบุตัวผู้ลงคะแนนและข้อมูลที่สามารถใช้หาลำดับของการส่งผลลงคะแนนได้ อย่างไรก็ตาม ในกรณีที่ให้ผู้ลงคะแนนส่งผลลงคะแนนก่อนจะตรวจสอบการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนน<u>สามารถใช้การเชื่อมโยงโดยอ้อม</u> (indirect voter association) ที่เชื่อมโยงผู้ลงคะแนนกับ	การลงคะแนน ระบบจะ Generate สร้างชุดเลขที่ให้โดยอัตโนมัติ (Unique Number) เพื่อใช้แทนอัตลักษณ์ของผู้ลงคะแนน ทำให้ไม่สามารถเชื่อมโยงโดยตรงระหว่างผู้ลงคะแนนกับผลคะแนนได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ผลลงคะแนนที่ถูกเข้ารหัสลับไว้ โดยหลังจากตรวจสอบแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้น จึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับ และนำไปนับคะแนนเป็นผลรวมของการลงคะแนน	
11. การควบคุมการเข้าถึง (Access Control) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น		
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน เพื่อให้มีหลักฐานสำหรับตรวจสอบในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งาน เปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และลบบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง	- ระบบมีการยืนยันตัวตนสำหรับผู้เข้าร่วมลงคะแนนที่หลากหลาย ตาม Solution ของหน่วยงาน ได้แก่ ● ผ่านฐานข้อมูลกรมการปกครอง (หน่วยงานจัดเตรียมข้อมูล) ● ผ่านฐานข้อมูลหน่วยงาน (หน่วยงานจัดเตรียมข้อมูล) ● ผ่านฐานข้อมูลในระบบ ● OTP ผ่านหมายเลขโทรศัพท์ เพื่อเข้าใช้งานระบบลงคะแนนเสียง โดยผู้พัฒนามีการออกแบบ ให้ 1 Solution สามารถเข้าสู่ระบบ (login) ได้เพียงเครื่องเดียวเท่านั้น ซึ่งการเข้าสู่ ระบบ (login) จะมีการเก็บการบันทึกเหตุการณ์ (activity log) ที่เกิดขึ้นของการใช้งาน - ระบบมีการเก็บบันทึกเหตุการณ์ (log) ซึ่งไม่สามารถแก้ไขเปลี่ยนแปลงหรือลบบันทึกของเหตุการณ์ได้ โดยมีการกำหนดสิทธิเพื่อเข้าถึงรายงาน Activity Log เฉพาะผู้ควบคุมระบบที่ได้รับมอบหมายจากบริษัท
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนน และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดบัญชีผู้ใช้งานที่ได้รับอนุญาต กำหนดบทบาทของผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละบทบาทของผู้ใช้งาน	ระบบการลงคะแนนเสียงมีการจำกัดสิทธิการเข้าใช้งาน ดังนี้ - ผู้ควบคุมระบบ ทำหน้าที่ควบคุมการลงคะแนน และออกรายงานที่เกี่ยวข้องกับการลงคะแนน - ผู้เข้าร่วมลงคะแนน สามารถลงคะแนนเสียง ตรวจสอบการลงคะแนน และสอบถามคำถามเพิ่มเติมจากผู้ควบคุมระบบ หรือสอบถามคำถาม - ผู้ตรวจสอบภายนอก (external auditor) มีการกำหนดสิทธิให้สามารถตรวจสอบความถูกต้องของผลคะแนน ผ่านระบบหรือจากการออกรายงานได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
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	ระบบมีการยืนยันตัวตนของผู้ใช้งาน (ผู้ลงคะแนน) และผู้ควบคุมระบบ เป็นแบบ multi-factor authentication โดยมีรายละเอียดดังนี้: **1) วิธีการพิสูจน์ตัวตน** - ผู้ใช้งานระบบมีการลงคะแนนด้วยวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ดังนี้ • พิสูจน์ข้อมูลจากบัตรประชาชนผ่านฐานข้อมูลกรมการปกครอง • พิสูจน์ข้อมูลเลขที่สมาชิก, ชื่อและนามสกุล, เบอร์โทรศัพท์, E-mail และ/หรือเลขบัตรประชาชน ผ่านฐานข้อมูลหน่วยงาน (หน่วยงานจัดเตรียมข้อมูล) • พิสูจน์ OTP ผ่านหมายเลขโทรศัพท์หรืออีเมล์ **ซึ่งเป็นไปตามมาตรฐาน IAL2** ข้อมูลที่สามารถใช้ในการยืนยันตัวตนได้จากหลายแหล่ง โดยสามารถยืนยันตัวตนได้ผ่านการตรวจสอบข้อมูลจากแหล่งข้อมูลหลายๆ แห่ง (เช่น ข้อมูลที่อ้างอิงจากฐานข้อมูลรัฐบาลหรือหน่วยงานที่น่าเชื่อถือ) และการใช้งานรหัสผ่านร่วมกับ OTP **2) การยืนยันตัวตน** - การยืนยันตัวตนผ่านฐานข้อมูลกรมการปกครอง โดยการกรอก ชื่อนามสกุล วันเดือนปีเกิด เลขบัตรประจำตัวประชาชน รหัสหลังบัตร - การยืนยันตัวตนผ่านฐานข้อมูลหน่วยงาน โดยการกรอกข้อมูลตามที่หน่วยงานกำหนด เช่น เลขบัตรประจำตัวประชาชน เลขสมาชิก - การยืนยันตัวตนผ่านฐานข้อมูลในระบบ โดยการกรอกข้อมูลที่ตรงกับระบบ เช่น รหัสการเลือกตั้ง Username & Password เป็นต้น - การยืนยันตัวตนด้วยการขอรับ OTP โดยการกรอกหมายเลขเบอร์โทรศัพท์ (เบอร์โทรศัพท์ 1 หมายเลข ต่อ 1 การเลือกตั้ง)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ระบบการลงคะแนนจะเก็บรักษาข้อมูลยืนยันตัวตน (เช่น รหัสผ่าน) โดยการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล ด้วยการใช้เทคนิคการ Salt และ Hashing ในฐานข้อมูล (เพื่อไม่ให้เก็บรหัสผ่านในรูปแบบที่สามารถใช้งานได้โดยตรง) นอกจากนี้ หากระบบการลงคะแนนใช้วิธีการยืนยันตัวตนด้วยรหัสผ่าน ระบบจะอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนเท่านั้นที่สามารถกำหนดความเข้มงวดและการหมดอายุของรหัสผ่านได้ นอกจากนี้ ระบบสามารถตั้งค่าความเข้มงวดของ OTP สามารถระบุความยาวของรหัสผ่านได้ โดยระบบตั้งค่า Default ความยาวของรหัสผ่านไว้ที่ความยาว 6 หลัก และระยะเวลาของ OTP ไม่เกิน 5 นาที จากการที่ระบบนี้ใช้ OTP และรหัสผ่าน ซึ่งถือเป็นการยืนยันตัวตนที่มีหลายปัจจัย (multi-factor authentication) **ซึ่งเป็นไปตามมาตรฐาน AAL2** เนื่องจากเป็นการยืนยันตัวตนผ่านรหัสผ่านและ OTP ที่ส่งไปยังโทรศัพท์มือถือ ซึ่งให้การยืนยันตัวตนที่ปลอดภัยขึ้นจากการใช้เพียงรหัสผ่านอย่างเดียว
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลดสิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่ (separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น	ระบบมีการกำหนดสิทธิการเข้าถึงระบบการลงคะแนนเสียงของผู้เข้าร่วมลงคะแนน โดยมีการจำกัดบทบาทการลงคะแนนเสียงตามสิทธิที่ได้รับสำหรับเลือกตั้ง ดังนี้ - ผู้ควบคุมระบบ ทำหน้าที่ควบคุมการลงคะแนน และออกรายงานที่เกี่ยวข้องกับการลงคะแนน - ผู้เข้าร่วมลงคะแนน สามารถลงคะแนนเสียง ตรวจสอบการลงคะแนน และสอบถามคำถาม - ผู้ตรวจสอบภายนอก (external auditor) มีการกำหนดสิทธิให้สามารถตรวจสอบความถูกต้องของผลคะแนนผ่านระบบหรือจากการออกรายงานได้
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการ	- ระบบมีการกำหนดระยะเวลาของเซสชัน (session) ในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด หลังจากนั้นผู้เข้าร่วมลงคะแนนต้องมียืนยันตัวตนตามรูปแบบที่กำหนด เพื่อยืนยันตัวตนอีกครั้ง - ผู้ควบคุมระบบสามารถกำหนดระยะเวลาการตั้งค่าของการหมดอายุเซสชัน (session) ได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด หากผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนควรระงับการใช้งาน (account lockout) ของผู้ใช้งานเป็นระยะเวลาหนึ่งก่อนจะให้ยืนยันตัวตนครั้งต่อไป และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล	- หากมีการยืนยันตัวตนผิดพลาดต่อเนื่อง ระบบไม่มีการจำกัดจำนวนความผิดพลาดต่อเนื่อง เนื่องจากมีผลกับการเข้าร่วมลงทะเบียน และการควบคุมการลงทะเบียน เช่น การ ลงทะเบียน และการลงคะแนนเสียงตามเวลาที่กำหนด
12. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย		
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐาน หรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาตหรือการถูกตัดการเชื่อมต่อทางกายภาพ เกิดขึ้นกับส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน ผู้พัฒนาระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อคที่มั่นคงปลอดภัย หรือระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ	ระบบการลงคะแนนติดตั้งให้บริการทั้งหมดบนระบบคลาวด์ Google Cloud หรือ Huawei Cloud (ขึ้นอยู่กับลูกค้าสำหรับลูกค้าบางท่านที่ต้องการให้ Server การเลือกตั้งอยู่ในประเทศไทยทั้งหมด) ซึ่งทั้งคู่ใช้ระบบรักษาความปลอดภัยทางกายภาพที่มีหลายชั้นเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต **Google Cloud** **มาตรการความปลอดภัยทางกายภาพในศูนย์ข้อมูลของ Google** 1. การควบคุมการเข้าถึงหลายชั้น: รวมถึงการใช้บัตรประจำตัวอิเล็กทรอนิกส์ที่ออกแบบเฉพาะ, ระบบสแกนม่านตา, เครื่องตรวจจับโลหะ, และอุปสรรคสำหรับยานพาหนะ เพื่อจำกัดการเข้าถึงพื้นที่สำคัญ 2. การตรวจสอบและเฝ้าระวัง: มีการติดตั้งกล้องวงจรปิดความละเอียดสูงทั้งภายในและภายนอกอาคาร พร้อมระบบตรวจจับความร้อนและการลาดตระเวนโดยเจ้าหน้าที่รักษาความปลอดภัยที่ผ่านการตรวจสอบประวัติและฝึกอบรม 3. การควบคุมการเข้าถึงพื้นที่เซิร์ฟเวอร์: การเข้าถึงพื้นที่เซิร์ฟเวอร์ต้องผ่านช่องทางที่มีการควบคุมอย่างเข้มงวด โดยใช้บัตรประจำตัวและการสแกนม่านตาเท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		4. การทำลายข้อมูลที่ปลอดภัย: มีห้องที่ออกแบบมาเพื่อทำลายอุปกรณ์จัดเก็บข้อมูลอย่างปลอดภัย เพื่อป้องกันการกู้คืนข้อมูลที่อาจถูกละเมิด **มาตรการความมั่นคงของสภาพแวดล้อมทางกายภาพ** Google ให้ความสำคัญกับความมั่นคงของสภาพแวดล้อมทางกายภาพ โดยมีมาตรการดังนี้: • ระบบจ่ายไฟฟ้าสำรอง: ศูนย์ข้อมูลมีระบบจ่ายไฟฟ้าสำรอง เช่น เครื่องกำเนิดไฟฟ้าฉุกเฉิน และระบบ UPS เพื่อให้บริการต่อเนื่องแม้เกิดเหตุไฟฟ้าดับ • การควบคุมสภาพแวดล้อม: มีการควบคุมอุณหภูมิและความชื้นในศูนย์ข้อมูลอย่างเข้มงวด เพื่อป้องกันความเสียหายต่ออุปกรณ์และข้อมูล **Ref:** https://cloud.google.com/docs/security/physical-to-logical-space **Huawei Cloud** **มาตรการความปลอดภัยทางกายภาพของ Huawei Cloud** 1. การควบคุมการเข้าถึงหลายชั้น: ศูนย์ข้อมูลของ Huawei Cloud ใช้ระบบควบคุมการเข้าถึงที่มีหลายชั้น เช่น การใช้บัตรประจำตัวอิเล็กทรอนิกส์, ระบบสแกนลายนิ้วมือ, และการตรวจสอบด้วยไบโอเมตริกซ์ เพื่อจำกัดการเข้าถึงพื้นที่สำคัญเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น 2. การเฝ้าระวังและตรวจสอบ: มีการติดตั้งกล้องวงจรปิดความละเอียดสูงทั้งภายในและภายนอกอาคาร พร้อมระบบตรวจจับความร้อนและการลาดตระเวนโดยเจ้าหน้าที่รักษาความปลอดภัยที่ผ่านการตรวจสอบประวัติและฝึกอบรม เพื่อเฝ้าระวังและตรวจสอบการเข้าถึงพื้นที่สำคัญตลอด 24 ชั่วโมง 3. การป้องกันภัยพิบัติและการกู้คืน: ศูนย์ข้อมูลของ Huawei Cloud มีแผนการป้องกันภัยพิบัติและการกู้คืนที่ครอบคลุม เช่น การสำรองข้อมูลในหลายภูมิภาค และการใช้ระบบจ่ายไฟฟ้าสำรอง เช่น เครื่องกำเนิดไฟฟ้าฉุกเฉิน และระบบ UPS เพื่อให้บริการต่อเนื่องแม้เกิดเหตุไฟฟ้าดับ 4. การควบคุมสภาพแวดล้อม: มีการควบคุมอุณหภูมิและความชื้นในศูนย์ข้อมูลอย่างเข้มงวด เพื่อป้องกันความเสียหายต่ออุปกรณ์และข้อมูล และมีการตรวจสอบสภาพแวดล้อมอย่างต่อเนื่องเพื่อรักษาความมั่นคงของสภาพแวดล้อมทางกายภาพ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		Ref: https://www.huaweicloud.com/intl/en-us/securecenter/security/datacenter.html Ref: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/SecurityWhitepaper_intl_en.pdf Ref: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/Best%20Practices/DataSecurityWhitepaper_intl_en.pdf
13. การคุ้มครองข้อมูล (Data Protection) วัตถุประสงค์ เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต		
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนน จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนนและระบบเครือข่าย รวมถึงระบบการลงคะแนนต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง	ระบบลงคะแนนมีระบบ Admin สำหรับกำหนดสิทธิ์อนุญาตให้เฉพาะผู้ควบคุมระบบการ ลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนนและระบบเครือข่าย รวมถึงระบบการลงคะแนนมีการรักษาความ ครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง มีการจัดเก็บ Log การแก้ไขและเปลี่ยนแปลง
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับมาจากผู้ลงคะแนน บันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที และจัดเก็บบันทึกการลงคะแนนให้อยู่ในรูปแบบที่สามารถแสดงผลลงคะแนนที่ได้รับมาให้ปรากฏอย่างถูกต้องได้	ระบบออกแบบให้บันทึกผลการลงคะแนนของผู้เข้าร่วมลงคะแนน ทันทีที่มีการยืนยัน การออกเสียงลงคะแนน ระบบสามารถตรวจสอบได้ว่าผู้เข้าร่วมลงคะแนน มีการลงคะแนนแล้วหรือไม่ หรือหากกรณีลงคะแนนเสียง มีข้อผิดพลาดหรือไม่สำเร็จระบบจะแจ้งเตือนให้ผู้เข้าร่วมลงคะแนนทราบ และการออกเสียง ลงคะแนนนั้นจะไม่ถูกบันทึกลงระบบ
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	ระบบการลงคะแนนมีอัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่เป็น มาตรฐาน ดังนี้ 1. SSL 2. Database Encryption โดยใช้ algorithm การเข้ารหัสข้อมูลที่จัดเก็บด้วย RSA 4096-bits สำหรับการเข้ารหัสบัตรเลือกตั้ง และ El-Gamal ใช้เข้ารหัสเพิ่มเติมในกระบวนการประมวลผล/จัดเก็บ

<table>
<tr><th>ข้อกำหนด</th><th>คำอธิบาย</th><th>ความสามารถของระบบการลงคะแนน</th></tr>
<tr><td></td><td>Recommendation for Key Management: Part 1 – General</td><td></td></tr>
<tr><td>13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด</td><td>การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายคอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)</td><td>ระบบมีการใช้ SSL/TLS ในการเข้ารหัสขณะรับส่งข้อมูลระหว่าง Server กับ Client</td></tr>
<tr><td colspan="3">14. การรักษาความครบถ้วนของระบบ (System Integrity)
<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงาน และไม่มีการแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือโดย ไม่ตั้งใจ</td></tr>
<tr><td>14.1 – ระบบการลงคะแนนใช้การควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อรับมือภัยคุกคามหรือช่องโหว่ด้านความมั่นคงปลอดภัย</td><td>เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) และวิธีการควบคุมเพื่อรับมือหรือลดความเสี่ยงจากภัยคุกคามแต่ประเภทซึ่งอาจส่งผลกระทบต่อการทำงานของระบบการลงคะแนน รวมถึงอธิบายวิธีการควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อป้องกัน บรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน เช่น กระบวนการเข้ารหัสลับ (cryptography) การป้องกันมัลแวร์ (malware) การตั้งค่าไฟร์วอลล์ (firewall) และการตั้งค่าระบบ (system configurations)</td><td>ระบบการลงคะแนนมีการควบคุมดูแลระบบหลายระดับชั้นเพื่อลดความเสี่ยงจากภัยคุกคาม ที่อาจเกิดขึ้น เช่น การจัดการระบบ Firewall, การป้องกันมัลแวร์, การควบคุมการเข้าถึง ข้อมูล, การสำรองข้อมูล (Backup) และการอัพเดทระบบให้ปลอดภัยสม่ำเสมอ และมีการ ทำเอกสารประเมินความเสี่ยง (Risk Management) ตัวอย่างการประเมินความเสี่ยงของระบบ E-Voting
<table>
<tr><th>ความเสี่ยง</th><th>ปัจจัยเสี่ยง</th><th>แนวทางการควบคุมความเสี่ยง</th></tr>
<tr><td>ระบบใช้งานไม่ได้ หรือ ทำงานช้าจนใช้งานไม่ได้</td><td>มีผู้ใช้งานระบบในเวลาเดียวกันเป็นจำนวนมาก</td><td>เพิ่มระบบ Load balancer และ Web server ของระบบการลงคะแนน จำนวน 2 instance และ database 1 instance</td></tr>
<tr><td>ระบบไม่สามารถเข้าใช้ งานได้ผ่าน Internet</td><td>เครือข่ายของผู้ ให้บริการ Internet มี ปัญหา เช่น สาย Fiber ขาด ทำให้เชื่อมต่อกับ Data Center ไม่ได้</td><td>ผู้ใช้งานเปลี่ยนไปใช้งานระบบบนเครือข่าย อื่นที่ใช้งานได้ชั่วคราว ระหว่างรอผู้ใช้บริการ Internet แก้ไขปัญหาเครือข่าย</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>ข้อกำหนด</th><th>คำอธิบาย</th><th colspan="3">ความสามารถของระบบการลงคะแนน</th></tr>
<tr><td></td><td></td><td>Data Center ไม่สามารถ ให้บริการได้ ทำให้ระบบ ไม่สามารถใช้งานได้</td><td>เกิดภัยพิบัติต่างๆ กระทันหัน จาก ธรรมชาติหรืออื่นๆ เช่น ไฟดับเป็นเวลานาน , สาย Fiber ขาด , Virus Computer / Ransomware</td><td>เตรียมเจ้าหน้าที่คอยประสานงานกับ Data Center หากปัญหาที่เกิดไม่สามารถ แก้ปัญหาได้ภายใน 24 ชั่วโมง จะพิจารณา นำข้อมูลที่ Backup ไว้มาเปิดใช้งานที่ Site สำรองแทน</td></tr>
<tr><td></td><td></td><td>ข้อมูลการลงคะแนนเสียหายหรือสูญหาย</td><td>ฐานข้อมูลไม่สามารถ เปิดใช้งานได้ / Hard disk ที่เก็บข้อมูลบน ระบบ Cloud เสียหาย</td><td>- Restore สำรองข้อมูลรายวัน
- Data Center มีระบบแจ้งเตือนหากพบ Hard disk เสีย และให้เจ้าหน้าที่เปลี่ยน disk ใหม่ โดยที่ข้อมูลไม่สูญหาย</td></tr>
<tr><td>14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น</td><td>ระบบการลงคะแนนป้องกันการติดตั้งหรือการสั่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง และปิดใช้งานการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน
ซอฟต์แวร์ของระบบการลงคะแนนต้องไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และต้องเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น</td><td colspan="3">ระบบการลงคะแนนทำงานมีการป้องกันการโจมตีแบบต่างๆ เช่น SQL injection, Crosssite scripting (XSS) และมีการตั้งค่า Firewall โดยการเปิด port เฉพาะที่จำเป็นต่อการใช้ งาน และจำกัดการเชื่อมต่อเฉพาะ IP Address ที่ได้รับอนุญาตเท่านั้น</td></tr>
<tr><td colspan="5">15. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring)
<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน</td></tr>
<tr><td>15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ</td><td>ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งประกอบด้วยเหตุการณ์ที่เกี่ยวข้องกับสถานะการทำงานและความผิดปกติของระบบ การยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน การจัดการระบบเครือข่าย การจัดการซอฟต์แวร์ และฟังก์ชันการลงคะแนน เป็นอย่างน้อย</td><td colspan="3">ระบบลงคะแนนมีการแสดงหลักฐาน การบันทึกเหตุการณ์ที่เกิดขึ้นในระบบลงคะแนน โดยสามารถมีการบันทึกเหตุการณ์ (activity log) ของการใช้งานของระบบลงคะแนน มีการยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน และมีฟังก์ชันในการปิดการลงคะแนน และระบบสามารถออกรายงานที่เกิดขึ้นในรูปแบบไฟล์ Excel</td></tr>
</table>

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ใช้งานในทันที บันทึกข้อผิดพลาดทั้งหมดที่เกิดขึ้น และสร้างรายงานข้อผิดพลาด (error report) รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการจัดการข้อผิดพลาดในระบบการลงคะแนน	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบจะแสดงข้อความแจ้งเตือนให้ผู้ใช้งาน ทราบทันที และมีการบันทึกข้อผิดพลาดเก็บไว้ในฐานข้อมูล เช่น การยืนยันตัวตนไม่สำเร็จ, การส่งผลลงคะแนนไม่สำเร็จ โดยสามารถส่งออกในรูปแบบไฟล์ Excel (.xlsx) เพื่อจัดทำ เป็นรายงานข้อผิดพลาด (error report) ได้
15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	ระบบการลงคะแนนต้องมีมาตรการป้องกันมัลแวร์ (malware) โดยระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ บันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ และบันทึกเหตุการณ์ของกิจกรรมการแก้ไขมัลแวร์ รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการอัปเดตมาตรการป้องกันมัลแวร์	ระบบลงคะแนนมีการติดตั้ง Malware Scanner บนระบบคลาวด์ ซึ่งผู้ดูแลระบบจะทำ การ Scan เพื่อตรวจสอบหา Malware เป็นระยะๆ โดยหากตรวจพบความผิดปกติหรือ Malware/Virus ผู้ดูแลระบบจะดำเนินการกำจัดหรือแก้ไข Malware ทันที และทำการ Scan เพื่อตรวจสอบซ้ำอีกครั้ง
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	ระบบการลงคะแนนมีแนวทางปฏิบัติในการป้องกันการโจมตีทางเครือข่าย ดังนี้ • กำหนดนโยบาย Firewall เพื่ออนุญาตการเข้าถึงหรือไม่อนุญาตเข้าถึง ตามนโยบายที่กำหนดไว้ • ระบบ Firewall มีการกำหนด Rate limit เพื่อการจำกัดจำนวนการเชื่อมต่อต่อวินาที หรือจำนวนข้อมูลที่สามารถส่งผ่านได้ต่อนาทีเพื่อป้องกันการโจมตีแบบ DDoS (Distributed Denial of Service) • เปิดเฉพาะ Port ที่จำเป็นสำหรับการเชื่อมต่อเท่านั้น • ระบบสำรองข้อมูลรายวัน • มีนโยบายกำหนดสิทธิ์เฉพาะผู้รับผิดชอบในการเข้าถึงระบบ และกำหนดสิทธิ์ไม่มาก เกินความจำเป็น • ระบบมีการเก็บกิจกรรมต่างๆ (Logs) เพื่อใช้ในการวิเคราะห์เหตุการณ์และการ ตรวจสอบต่อไป

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		• มีการอัพเดทซอฟท์แวร์บนระบบคลาวด์สม่ำเสมอ เพื่อป้องกันช่องโหว่ใหม่ๆ และเพิ่ม ความปลอดภัยให้สูงสุด