แบบประเมินความสอดคล้องด้วยตนเอง

ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ELECTRONIC VOTING SYSTEM)

ตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ขมธอ. 26-2564) เวอร์ชัน 2.0

ชื่อระบบ	Inventech Connect
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท)	บริษัท อินเวนท์เทค ซิสเท็มส์ (ประเทศไทย) จำกัด
ช่องทางการติดต่อผู้ให้บริการ	**ผู้ติดต่อ :** นายอรรถกร ธารามหากูล **เบอร์ติดต่อ :** 082-998-6299 **Email :** Sales@inventech.co.th
วันที่ประเมินความสอดคล้อง	*วันที่ 29 มกราคม 2568*
วันที่ครบกำหนดการทบทวน	*วันที่ 28 มกราคม 2569*
ประเภทของระบบการให้บริการ	☒ On Cloud ☐ On Premise ☐ อื่น ๆ โปรดระบุ
การใช้งานระบบการลงคะแนน	☒ ร่วมกับระบบการประชุมฯ ☒ แยกกับระบบการประชุมฯ
มาตรฐานที่ได้รับการรับรอง	☒ ISO/IEC 27001 ☐ ISO/IEC 27701 ☐ อื่น ๆ โปรดระบุ
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง	ระบบ Inventech Connect มีรูปแบบการให้บริการ On Cloud ครอบคลุมการประชุมทั้งภาพและเสียง, การนับองค์ประชุม, การลงคะแนนวาระ, การสรุปผลองค์ประชุมผ่านระบบออนไลน์ และมีการสรุปรายงานองค์ประชุม, รายงานผลคะแนนรายวาระ, รายงานผู้เข้าร่วมประชุมและข้อมูลจราจรทางอิเล็กทรอนิกส์ได้ทันทีหลังเสร็จสิ้นการประชุม

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	ระบบการลงคะแนนมีการออกแบบฟังก์ชันการใช้งานตามกระบวนการลงคะแนนตามข้อกำหนดและหลักเกณฑ์ของกระทรวงพาณิชย์ ดังนี้ 1. สามารถกำหนดเงื่อนไขของการประชุม และสามารถกำหนดเงื่อนไขของแต่ละวาระได้ 2. ระบบรองรับการนำเข้าข้อมูล โดยมีการนำเข้าไฟล์ Excel ที่มีการกำหนดรายชื่อผู้มีสิทธิเข้าร่วมประชุมและจำนวนเสียงที่สามารถออกเสียงลงคะแนนได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		3. การเปิด - ปิดลงคะแนน ผู้เข้าร่วมประชุมสามารถทำการลงคะแนนล่วงหน้าได้จนกว่าวาระนั้นจะปิดรับผลการลงคะแนน ซึ่งระบบสามารถกำหนดระยะเวลาการปิดการลงคะแนนได้ 4. การลงคะแนน หลังจากผู้เข้าร่วมประชุมมีการยืนยันตัวตนแล้ว ผู้เข้าร่วมประชุมสามารถดำเนินการลงคะแนนได้ตามความประสงค์ ซึ่งการลงคะแนนหรือการแก้ไขผลคะแนนจะต้องมีการยืนยันทุกครั้ง โดยสามารถแก้ไขการออกเสียงลงคะแนนได้ตลอดเวลา จนกว่าวาระนั้นจะปิดรับผลคะแนน 5. การส่งผลลงคะแนน ระบบมีปุ่มสำหรับการเลือกลงคะแนนตามความประสงค์ดังนี้ 5.1 ปุ่ม “เห็นด้วย” 5.2 ปุ่ม “ไม่เห็นด้วย” 5.3 ปุ่ม “งดออกเสียง” 5.4 ปุ่ม “ยกเลิกการลงคะแนนเสียง” 6. การปิดลงคะแนน ระบบมีการควบคุมการปิดรับผลการลงคะแนน เมื่อเจ้าหน้าที่ทำการกดปุ่ม เลือกวาระและบันทึกการผ่านมติวาระ หลังจากขั้นตอนนี้จะทำให้ผู้เข้าร่วมประชุมไม่สามารถทำการลงคะแนนเสียงในวาระที่ทำการเลือกได้และเมื่อมีการปิดรับผลคะแนนเรียบร้อยแล้ว ระบบจะคำนวณผลคะแนนให้อัตโนมัติ 7. การรายงานผลรวมของการลงคะแนน ระบบมีการแสดงข้อมูลผลรวมของการลงคะแนน ดังนี้ 7.1 แสดงผ่านระบบอิเล็กทรอนิกส์ ที่ใช้ในการควบคุมระบบการประชุม ซึ่งหน้าจอจะแสดงให้ผู้เข้าร่วมประชุมทราบผ่านการถ่ายทอดสัญญาณการประชุม 7.2 แสดงผ่านระบบ e-Voting ที่ผู้เข้าร่วมประชุมใช้งาน ซึ่งหน้าจอจะแสดงให้ผู้เข้าร่วมประชุมทราบ จากการกดเลือกวาระการประชุม หลังจากมีการปิดรับผลคะแนนในวาระนั้นแล้ว โดยผู้ใช้งานสามารถตรวจสอบสรุปผลคะแนนของตนเอง และสรุปผลคะแนนรวมรายวาระ 7.3 ระบบสามารถทำการออกรายงานสรุปผลการลงคะแนนเป็นไฟล์

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		เอกสารในรูปแบบ PDF / Excel จากเจ้าหน้าที่ควบคุมการประชุม
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ (system accuracy and reliability) การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) ในสภาวะที่ใกล้เคียงกับการใช้งานจริงในกระบวนการลงคะแนน และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)	ระบบการลงคะแนนมีการทดสอบและจัดเก็บข้อมูลการทดสอบ ดังนี้ 1. มีการจัดทำ Test case และจัดเก็บ Test log เพื่อทดสอบ และประเมินความสามารถในการใช้งานระบบ Inventech Connect 2. ทดสอบจากการใช้งานจริงพร้อมกับการทดสอบขีดความสามารถของระบบและ Server โดยการทำ Load test หรือ Performance test ตามการใช้งานจริงในกระบวนการลงคะแนน และประมวลผลคะแนน ซึ่งสามารถรองรับปริมาณธุรกรรมสูงสุดตามจำนวนที่ให้บริการ
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบซอฟต์แวร์ (software tester) ของผู้พัฒนาระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำรายงานผลการทดสอบ โดยมีการจัดทำรายงาน Test case เพื่อยืนยันการทดสอบคุณสมบัติของระบบว่าเป็นไปตามที่ผู้พัฒนาออกแบบ โดยกำหนดให้ทดสอบ ทุกเดือนธันวาคมของทุกปี เพื่อนำระบบไปใช้ในปีถัดไป
2. การพัฒนาระบบ (System Development) <u>วัตถุประสงค์</u> 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)	ระบบการลงคะแนนถูกพัฒนาในโปรแกรมภาษาที่ผู้พัฒนาภาษายังรองรับการใช้งาน ณ ปัจจุบัน ดังนี้ - React - Dotnet core ซึ่งมีการออกแบบให้ผู้ใช้งาน ใช้งานได้ง่าย ไม่ซับซ้อน โดยออกแบบระบบลงคะแนนให้มีความสอดคล้องกับกฎหมายและหลักเกณฑ์ที่กำหนด โดยมีการพัฒนาตามหลัก SDLC 7 ขั้นตอน ในรูปแบบของ Agile Model ดังนี้ 1.Planning Stage 2.Feasibility or Requirements of Analysis Stage

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		3.Design and Prototyping Stage 4.Software Development Stage 5.Software Testing Stage 6.Implementation and Integration 7.Operations and Maintenance Stage
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน (modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ	ระบบการลงคะแนนมีการแยกส่วนการทำงานที่ชัดเจนผ่าน API ทั้งหมด โดยส่วนที่แยกออกมา คือ 1.ข้อมูลผู้ถือหุ้น 2.ข้อมูลการลงทะเบียน 3.ข้อมูลการลงคะแนน และ 4.ข้อมูลการประมวลผล
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้ (self-modifying code)	- ระบบการลงคะแนนมีการกำหนดเวอร์ชัน Control โดยเก็บรายละเอียดว่าในเวอร์ชันนั้นๆ มีการปรับปรุง/เพิ่มเติม หรือแก้ไขอะไรไปบ้าง - โดยชุดคำสั่งการทำงานจะถูกออกแบบให้ทำงานเฉพาะเจาะจงเท่านั้น - ระบบการลงคะแนนออกแบบให้มีการเข้ารหัสข้อมูลการเข้าถึงก่อนส่ง API เพื่อปกป้องข้อมูลที่อยู่ในระบบให้มีความปลอดภัย
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน	- ระบบการลงคะแนนมีการบันทึกข้อผิดพลาด ให้ผู้พัฒนาทราบ ในกรณีเกิดเหตุไม่พึงประสงค์ - ระบบมีการจัดทำ Replication เพื่อรองรับกรณี ที่ Application หรือ Database เกิดปัญหาในการทำงาน รายละเอียดการดำเนินการ 1. ส่ง SMS แจ้งเหตุขัดข้อง และ email แจ้งเหตุขัดข้อง 1 2. ทำการถอด Replication ของงานประชุม 3. แก้ไขการเชื่อมต่อ 4. แจ้งประสานงานหน้างาน เพื่อดำเนินการประชุมต่อไป - ระบบมีการกำหนดนโยบาย “การตอบสนองต่อเหตุการณ์ที่ผิดปกติ” ตามมาตรฐาน ISO 27001:2022

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
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)	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารเกี่ยวกับระบบการลงคะแนน เพื่อให้สามารถอ่านและทำความเข้าใจได้อย่างครบถ้วน 1. Data Dictionary 2. Functional Specification 3. ER-Diagram 4. ภาพรวมของระบบ (system overview) 5. ประสิทธิภาพของระบบ (system performance) 6. ความมั่นคงปลอดภัยของระบบ (system security) 7. การติดตั้งซอฟต์แวร์ (software installation) 8. การทำงานของระบบ (system operations) 9. คู่มือการใช้งาน (user manual) โดยคู่มือยถูกแบ่งออกเป็น 2 สิทธิ์การใช้งาน คือ 9.1 User Manual สำหรับผู้เข้าร่วมประชุม 9.2 User Manual สำหรับผู้ควบคุมระบบ ที่ระบุถึงวิธีการรายละเอียดของระบบลงคะแนน และวิธีการคำนวณ ระบบการลงคะแนนสามารถตรวจสอบความถูกต้องของที่มา ของผลคะแนนได้ในแต่ละวาระ โดยมีรายงานประกอบสำหรับการตรวจสอบ ส่งให้กับผู้ใช้บริการ (ลูกค้า)
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการ	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ	ผู้พัฒนาระบบการลงคะแนนมีการจัดทำเอกสารวิธีการติดตั้ง ตั้งค่าและการตรวจสอบค่าของการทำงานอย่างถูกต้อง โดยมีกระบวนการ ดังนี้ 1. เอกสารวิธีการติดตั้งระบบ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ลงคะแนน เตรียมไว้พร้อมสำหรับการตรวจสอบระบบ		2. เอกสารการตั้งค่าระบบ 3. เอกสารการตรวจสอบการใช้งานระบบ โดยบริษัทเป็นผู้ดำเนินการติดตั้ง ตั้งค่าและตรวจสอบระบบ
3.3 – บุคคลที่เกี่ยวข้องกับระบบการลงคะแนนสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)	เจ้าหน้าที่ควบคุมระบบสามารถออกรายงานข้อมูลจราจรอิเล็กทรอนิกส์ เพื่อตรวจสอบการลงคะแนน และเหตุการณ์ในการใช้งานระบบของผู้เข้าร่วมประชุม ซึ่งมีการจัดเก็บข้อมูลทุกการกระทำที่ผู้ใช้งานกระทำกับระบบ เช่น View, Insert, Update แยกเป็นรายบุคคลโดยมีการอธิบายรูปแบบของการบันทึกเหตุการณ์ทั้งหมด
4. การเข้าถึงอย่างเท่าเทียม (Equitable Access) <u>วัตถุประสงค์</u> เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม		
4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงภาพและเสียง) และรูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัสบนหน้าจอ) ในลักษณะที่สอดคล้องกัน	ระบบการลงคะแนนมีฟังก์ชันในการลงคะแนนและตรวจสอบผลการลงคะแนน โดยมีการแสดงผล และมีปฏิสัมพันธ์ที่สอดคล้องกัน คือระบบมีการแสดงปุ่มการออกเสียงลงคะแนนให้ทราบ และเมื่อมีการยืนยันผลการลงคะแนนระบบจะแสดงแจ้งเตือนข้อมูลเพื่อแจ้งให้ทราบถึงการดำเนินการ เพื่อให้ผู้เข้าร่วมประชุมยืนยัน และแสดงผลลัพธ์ได้อย่างถูกต้อง โดยผู้ใช้งานสามารถเข้าใช้ผ่าน Web browser (web responsive) ทำให้สามารถเข้าใช้งานได้ทุกอุปกรณ์ เช่น คอมพิวเตอร์ หรือโทรศัพท์เคลื่อนที่
4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ	รูปแบบการแสดงผล (display format) แสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน และไม่ทำให้เกิดอคติกับตัวเลือกลงคะแนนใด ๆ ที่นำเสนอต่อผู้ลงคะแนน เช่น ตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน	ระบบมีการแสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน โดยระบบมีการออกแบบปุ่มและแบบอักษรลักษณะเดียวกัน
5. การลงคะแนนตรงตามเจตนา (Cast as Intended) <u>วัตถุประสงค์</u> เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้		
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล	ระบบมีการกำหนดการตั้งค่าส่วนบุคคล เช่น ส่วนของการเปลี่ยนภาษา โดยค่าเริ่มต้น (default setting) ของระบบมีการกำหนดค่าเป็นภาษาไทย โดยระบบใช้งานผ่าน Web

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
เหมาะสมที่สุดกับผู้ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงกับความต้องการของผู้ลงคะแนน	(preference setting) ตามความต้องการของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษร และสีของภาพ	browser ทำให้สามารถปรับเพิ่ม - ลด ขนาดหน้าจอและตัวอักษร ตามความต้องการของผู้ใช้งานระบบ
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง เช่น รูปแบบการแสดงผลของข้อมูล (display format) การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้าถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ (touch screen gestures) รวมถึงระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) เช่น การให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนน หรือการแจ้งสถานะของการลงคะแนนให้ผู้ลงคะแนนทราบ	ผู้ใช้งานสามารถเลือกลงคะแนนตามวาระได้ด้วยตนเอง โดยผู้ใช้งานสามารถลงคะแนนเสียง เห็นด้วย ไม่เห็นด้วย งดออกเสียง และยกเลิกการลงคะแนนเสียง ซึ่งระบบจะแสดงตัวเลือกล่าสุดให้ผู้ใช้งานตรวจสอบความถูกต้อง โดยผู้ใช้งานสามารถเปลี่ยนตัวเลือกการลงคะแนนเสียงได้จนกว่าระบบปิดรับการลงคะแนน และสามารถเข้าใช้งานเมนูอื่น ๆ ได้ตามสิทธิการใช้งาน ซึ่งระบบมีการควบคุมการเปิดใช้งานโดยไม่ตั้งใจ โดยผู้ใช้งานจะต้องมีการยืนยันการกระทำกับระบบ โดยระบบมีการแจ้งเตือนให้ผู้ใช้งาน รับทราบและยืนยันการกระทำเพื่อป้องกันการกระทำที่ไม่ได้ตั้งใจ
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน คำแนะนำ และข้อความจากระบบด้วยภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งข้อความที่ไม่ให้เกิดความสับสนในการลงคะแนน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต หรือการเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) และการแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว นอกจากนี้ระบบมีการแสดงคำแนะนำและข้อความที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ	ระบบมีการออกแบบให้ผู้ใช้งานสามารถเข้าใจและใช้งานได้ง่าย โดยมีการแยกเมนูการใช้งานอย่างชัดเจน รวมถึงมีการแสดงข้อความแจ้งเตือนเป็นลักษณะ Pop-up เช่น แจ้งเตือนเพื่อยืนยันการลงคะแนน และแจ้งเตือนเมื่อทำการลงคะแนนสำเร็จ ให้ทราบตามสิทธิของผู้เข้าร่วมประชุม
6. ความเหมาะสมต่อการใช้งาน (Usable)		

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
วัตถุประสงค์ 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)	ผู้พัฒนามีการออกแบบให้ระบบใช้งานอย่างไม่ซับซ้อนเพื่อลดปัญหาในการใช้งานของทุกกลุ่มเป้าหมาย โดยใช้ภาษาที่ชัดเจนอ่านง่าย และใช้การแสดงตำแหน่งข้อมูล ที่เหมาะสม ซึ่งระบบมีการรองรับภาษาในการใช้งานทั้งภาษาไทยและอังกฤษ ทางผู้พัฒนามีการประเมินจากกลุ่มผู้ใช้งานในปี 2565 จำนวน 141 งาน รวมผู้ใช้งานจำนวน 4,275 ราย โดยมีการจัดทำตัวอย่างข้อมูลช่วงอายุของผู้ใช้งาน ดังนี้ ช่วงที่ 1 อายุไม่เกิน 40 ปี ช่วงที่ 2 อายุ 40-60 ปี และ ช่วงที่ 3 อายุ 60 ปี ขึ้นไป โดยผู้ใช้งานทั่วไปอยู่ในกลุ่มช่วงที่ 2และ 3 ไม่พบปัญหาการใช้งานในส่วนหน้าจอลงคะแนน หรือวิธีการลงคะแนน (อ้างอิงจาก Call Center Log หมวดหมู่การใช้งาน e-Vote) โดยในปัจจุบันมีการปรับปรุงระบบจาก feedback ที่ได้รับเช่น ต้องใช้งานแยกระหว่างระบบโหวตและระบบถ่ายทอดสด ทำให้ต้องสลับไปมา จึงมีการพัฒนาให้ผู้ใช้ login เข้าใช้งานครั้งเดียวและสามารถรับชมการประชุมและโหวตคะแนนได้ในระบบเดียว ซึ่งการพัฒนาระบบจะดำเนินการพัฒนาจากระบบงานเดิมโดยมีการแยกจาก Version ที่ใช้งาน ทำให้มีการเก็บทั้ง Version เดิม และ Version ที่จะใช้ในปีถัดไป
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ	ผู้พัฒนามีการออกแบบขั้นตอนการดำเนินงานของระบบที่เหมาะสมและครอบคลุมการใช้งาน เพื่อช่วยให้ผู้ควบคุมระบบสามารถใช้งานได้ง่าย และมีการแจ้งเตือนการกระทำที่ไม่ได้ตั้งใจ โดยผู้ควบคุมการลงคะแนนตรวจสอบจาก Activity Log ของหน้าการลงคะแนน ซึ่งมีการแสดงผลลัพธ์การลงคะแนนเป็นสำเร็จ (Success) และระบบผ่านการประเมินความเหมาะสมต่อการใช้งานโดยผู้ควบคุมระบบการลงคะแนนแล้ว
ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ		
7. การทำงานร่วมกัน (Interoperable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน		

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนอยู่ในรูปแบบที่ทำงานร่วมกันได้หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐาน	- ระบบมีการนำเข้าข้อมูล ในรูปแบบไฟล์ Excel เช่น ไฟล์รายชื่อผู้เข้าร่วมประชุม - ระบบรองรับการส่งออกข้อมูลรายงาน ในรูปแบบไฟล์ PDF และ Excel เช่น รายงาน Activity Log และรายงานสรุปผลการลงคะแนน
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้รูปแบบมาตรฐาน ในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่าง ๆ	ระบบไม่มีการรองรับการเชื่อมต่อกับฮาร์ดแวร์อื่น หรือเครื่องลงคะแนนอิเล็กทรอนิกส์อื่น เนื่องจากระบบมีการใช้งานผ่าน Web browser เท่านั้น
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 หากพบข้อผิดพลาดในระบบระหว่างการลงคะแนน ระบบจะมีการโหลดหน้าการใช้งานใหม่ (reload) เพื่อให้ผู้เข้าร่วมประชุมสามารถกลับไปทำการลงคะแนนอีกครั้ง โดยระบบการลงคะแนนมีช่องทางการติดต่อสำหรับการแจ้งเหตุขัดข้องที่เกิดขึ้นระหว่างการลงคะแนน โดยมีการจัดเก็บหลักฐานในรูปแบบของรายงาน Activity Log ซึ่งผู้ตรวจสอบสามารถออกรายงานจากระบบเพื่อตรวจสอบข้อผิดพลาดที่เกิดขึ้นได้ - ระบบสามารถตรวจสอบผลการลงคะแนน และออกรายงานสรุปผลคะแนนได้อย่างถูกต้อง - ระบบมีช่องทางการตรวจสอบข้อมูลการลงคะแนนของผู้ตรวจสอบภายนอก (external auditor) โดยมีการกำหนดสิทธิให้สามารถตรวจสอบความถูกต้องของผลคะแนน ผ่านระบบหรือจากการออกรายงานได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
9. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy) [1] วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง		
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่แสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน	ผู้เข้าร่วมประชุมมีการยืนยันตัวตนผ่านรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับการเข้าใช้ระบบลงคะแนน ทำให้การลงคะแนนเสียงเป็นการลงคะแนนเสียงเฉพาะบุคคลไม่มีการเปิดเผยข้อมูลต่อบุคคลอื่น เพื่อรักษาความเป็นส่วนตัวของผู้เข้าร่วมประชุม
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่าส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนมีการออกแบบให้ผู้เข้าร่วมประชุมเข้าใจได้ง่าย โดยสามารถเข้ามาเลือกวาระที่ต้องการลงคะแนน มีการแสดงแจ้งเตือนยืนยันการลงคะแนน และสามารถตรวจสอบผลการลงคะแนนได้ด้วยตนเอง
10. ความลับของคะแนนเสียง (Vote Secrecy) วัตถุประสงค์ (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน		
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	ระบบการลงคะแนนต้องไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มาประมวลผล จัดเก็บ หรือแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว	การลงคะแนน ระบบจะสรุปผลการลงคะแนนโดยแสดงข้อมูลสรุปเฉพาะข้อมูลผลการลงคะแนน และ/หรือ จำนวนผู้ออกเสียงลงคะแนนในแต่ละวาระ โดยแยกตามการออกเสียงลงคะแนน “เห็นด้วย, ไม่เห็นด้วย, งดออกเสียง, บัตรเสีย, ไม่ออกเสียงลงคะแนน , ไม่มีสิทธิออกเสียงลงคะแนน” โดยไม่มีข้อมูลส่วนบุคคลใดๆของผู้ลงคะแนนมาแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว
10.2 – ระบบการลงคะแนนไม่จัดทำข้อมูลเกี่ยวกับผู้ลงคะแนน	ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับผล	การลงคะแนน ระบบจะใช้การเชื่อมโยงโดยอ้อมเพื่อตรวจสอบสิทธิของผู้ลงคะแนน โดยข้อมูลส่วนบุคคลดังกล่าวจะถูกทำการเข้ารหัส (Encryption) ไว้ และระบบจะทำการ

[1] ความเป็นส่วนตัวของผู้ลงคะแนน ในที่นี้หมายถึง ความเป็นส่วนตัวที่เกิดขึ้นภายในระบบการลงคะแนนเท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
หรือข้อมูลอื่น ๆ ที่สามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน	ลงคะแนนของผู้ลงคะแนน นอกจากนี้ ผลลงคะแนนและผลรวมของการลงคะแนนต้องไม่มีข้อมูลที่ระบุตัวผู้ลงคะแนนและข้อมูลที่สามารถใช้หาลำดับของการส่งผลลงคะแนนได้ อย่างไรก็ตาม ในกรณีที่ให้ผู้ลงคะแนนส่งผลลงคะแนนก่อนจะตรวจสอบการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนนสามารถใช้การเชื่อมโยงโดยอ้อม (indirect voter association) ที่เชื่อมโยงผู้ลงคะแนนกับผลลงคะแนนที่ถูกเข้ารหัสลับไว้ โดยหลังจากตรวจสอบแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้น จึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับ และนำไปนับคะแนนเป็นผลรวมของการลงคะแนน	สร้างชุดเลขที่ให้โดยอัตโนมัติ (Unique Number) เพื่อใช้แทนอัตลักษณ์ของผู้ลงคะแนน ทำให้ไม่สามารถเชื่อมโยงโดยตรงระหว่างผู้ลงคะแนนกับผลคะแนนได้ เว้นแต่หน่วยงานบังคับใช้กฎหมายและผู้ตรวจสอบที่ได้รับสิทธิเท่านั้น ที่สามารถเรียกดูข้อมูลรายงานการลงคะแนน ที่แสดงคะแนนเสียงเป็นรายบุคคลได้ โดยสามารถร้องขอได้ภายในระยะเวลา 14 วัน หลังสิ้นการประชุม ตามมาตรฐานการให้บริการของทางบริษัท เว้นแต่ผู้จัดจ้างจะกำหนดระยะเวลาให้เป็นอย่างอื่น
11. การควบคุมการเข้าถึง (Access Control) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น		
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน เพื่อให้มีหลักฐานสำหรับตรวจสอบในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งาน เปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และลบบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง	- ระบบมีการเข้าสู่ระบบ (login) เข้าใช้งานด้วยรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) เพื่อเข้าใช้งานระบบลงคะแนนเสียง โดยผู้พัฒนามีการออกแบบให้ 1 รหัสผู้ใช้งานสามารถเข้าสู่ระบบ (login) ได้เพียงเครื่องเดียวเท่านั้น ซึ่งการเข้าสู่ระบบ (login) จะมีการเก็บการบันทึกเหตุการณ์ (activity log) ที่เกิดขึ้นทั้งหมดของการใช้งาน - ระบบมีการเก็บบันทึกเหตุการณ์ (log) ซึ่งไม่สามารถแก้ไขเปลี่ยนแปลงหรือลบบันทึกของเหตุการณ์ได้ โดยมีการกำหนดสิทธิเพื่อเข้าถึงรายงาน Activity Log เฉพาะผู้ควบคุมระบบที่ได้รับมอบหมายจากบริษัท
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและ	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนน และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดบัญชีผู้ใช้งานที่ได้รับ	ระบบการลงคะแนนเสียงมีการจำกัดสิทธิการเข้าใช้งาน ดังนี้ - ผู้ควบคุมระบบ ทำหน้าที่ควบคุมการประชุมและออกรายงานที่เกี่ยวข้องกับการประชุม - ผู้เข้าร่วมประชุม สามารถลงคะแนนเสียง ตรวจสอบการลงคะแนน และสอบถามคำถาม

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	อนุญาต กำหนดบทบาทของผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละบทบาทของผู้ใช้งาน	- ผู้ตรวจสอบภายนอก (external auditor) มีการกำหนดสิทธิให้สามารถตรวจสอบความถูกต้องของผลคะแนน ผ่านระบบหรือจากการออกรายงานได้
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	- ระบบการลงคะแนนมีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัย สำหรับผู้ใช้งานก่อนเข้าใช้งาน ซึ่งพิจารณาข้อกำหนดตามระดับ ความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL1) และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL1) จากมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล - ผู้ใช้งานระบบมีการลงคะแนนด้วยวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ดังนี้ 1. การยืนยันตัวตนด้วยรหัสผ่าน โดยผู้เข้าร่วมประชุมจะต้องนำ รหัสผู้ใช้งาน (username) และรหัสผ่าน (password) ที่ได้รับจากอีเมล 2. การยืนยันตัวตนด้วยการขอรับ OTP โดยผู้เข้าร่วมประชุมจะต้องกรอกเบอร์โทรศัพท์ เพื่อขอรับรหัส OTP สำหรับเข้าสู่ระบบ - ผู้ควบคุมระบบมีการลงคะแนนใช้วิธีการยืนยันตัวตนแบบ 2 ชั้น (two-factor authentication) ดังนี้ 1. มีการ Login ด้วยรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) จากนั้นต้องกรอกรหัส OTP เพื่อยืนยันตัวตนอีกครั้ง - ระบบการลงคะแนนสามารถกำหนดหรือตั้งค่าความเข้มงวดและการหมดอายุของรหัสผ่านได้ - ตั้งค่าความเข้มงวดของรหัสผ่าน สามารถระบุความยาวของรหัสผ่านได้สูงสุด 14 หลักได้ - โดยตั้งค่า default ความยาวของรหัสผ่านไว้ที่ความยาว 8 หลัก และระยะเวลาของ OTP 5 นาที - การหมดอายุของรหัสผ่านสามารถตั้งค่าได้จากระบบหลังบ้านโดยดำเนินการรีเซ็ตรหัสผ่านและสร้างระผ่านผ่านใหม่พร้อมทั้งส่งอีเมลแจ้งผู้เข้าใช้งานตามสิทธิ์อัตโนมัติ - การหมดอายุของ OTP สามารถกำหนดจากผู้ให้บริการ OTP โดยสามารถกำหนดเวลาหมดอายุของ OTP ได้ ขั้นต่ำคือ 5 **นาที หรือตามความต้องการของลูกค้า**
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลด	ระบบมีการกำหนดสิทธิการเข้าถึงระบบการลงคะแนนเสียงของผู้เข้าร่วมประชุม โดยมีการจำกัดบทบาทการลงคะแนนเสียงตามสิทธิที่ได้รับสำหรับการประชุม ดังนี้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	สิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่ (separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น	- ผู้ควบคุมระบบ ทำหน้าที่ควบคุมการประชุมและออกรายงานที่เกี่ยวข้องกับการประชุม - ผู้เข้าร่วมประชุม สามารถลงคะแนนเสียง ตรวจสอบการลงคะแนน และสอบถามคำถาม - ผู้ตรวจสอบภายนอก (external auditor) มีการกำหนดสิทธิให้สามารถตรวจสอบความถูกต้องของผลคะแนน ผ่านระบบหรือจากการออกรายงานได้
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด หากผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนควรระงับการใช้งาน (account lockout) ของผู้ใช้งานเป็นระยะเวลาหนึ่งก่อนจะให้ยืนยันตัวตนครั้งต่อไป และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล	- ระบบมีการกำหนดระยะเวลาของเซสชัน (session) ในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด หลังจากนั้นผู้เข้าร่วมประชุมต้องมีการกรอก ผู้ใช้งาน (username) และรหัสผ่าน (password) เพื่อยืนยันตัวตนอีกครั้ง - ผู้ควบคุมระบบสามารถกำหนดระยะเวลาการตั้งค่าของการหมดอายุเซสชัน (session) ได้ - หากมีการยืนยันตัวตนผิดพลาดต่อเนื่องระบบไม่มีการจำกัดจำนวนความผิดพลาดต่อเนื่อง เนื่องจากมีผลกับการเข้าร่วมประชุมและการควบคุมการประชุม เช่น การลงทะเบียน และการลงคะแนนเสียงตามเวลาที่กำหนด
12. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย		
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐาน หรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาตหรือการถูกตัดการเชื่อมต่อทางกายภาพ เกิดขึ้นกับส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน	- ระบบการลงคะแนนติดตั้งและให้บริการบนระบบคลาวด์ของผู้ให้บริการที่มีการรักษาความมั่นคงปลอดภัย - ระบบอำนวยความสะดวก : มีเครื่องสำรองไฟ (UPS) และผลิตกระแสไฟฟ้า (generator set) ห้องควบคุมอุณหภูมิ ระบบตรวจจับความชื้น และระบบป้องกันอัคคีภัยที่ได้มาตราฐานสากล

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ผู้พัฒนาระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อคที่มั่นคงปลอดภัย หรือระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ	- ระบบความปลอดภัย : ด้าน Network Security มีความปลอดภัยสูงด้วย ระบบป้องกันเครือข่าย (Firewall) ทั้ง Hardware Software และ Policy Security ตามมาตรฐาน ISO 27001 , ISO 27001 และ ISO 27001 ข้อมูลอ้างอิงจากผู้ให้บริการ : https://www.inet.co.th/th/brochure
13. การคุ้มครองข้อมูล (Data Protection) วัตถุประสงค์ เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต		
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนน จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนนและระบบเครือข่าย รวมถึงระบบการลงคะแนนต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง	- ระบบมีการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลการตั้งค่า การลงคะแนนเสียง โดยไม่ได้รับอนุญาตจากรายละเอียด ดังนี้ 1. การยืนยันตัวตนของผู้ควบคุมระบบแบบ 2 ชั้น (two-factor authentication) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ก่อนการเข้าใช้งานระบบลงคะแนน 2. มีการกำหนดสิทธิการเข้าใช้งานและการเข้าถึงข้อมูลของผู้ควบคุมระบบ โดยสามารถจำกัดสิทธิของผู้ควบคุมระบบเป็นรายบุคคล และต้องมีการยืนยันตัวตนก่อนการเข้าใช้งาน 3. การแก้ไขผลคะแนนจะสามารถทำได้เฉพาะสิทธิของผู้ควบคุมระบบที่ได้รับมอบหมายจากบริษัท
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับมาจากผู้ลงคะแนน บันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที และจัดเก็บบันทึกการลงคะแนนให้อยู่ในรูปแบบที่สามารถแสดงผลลงคะแนนที่ได้รับมาให้ปรากฏอย่างถูกต้องได้	- ระบบออกแบบให้บันทึกผลการลงคะแนนของผู้เข้าร่วมประชุม ทันทีที่มีการยืนยันการออกเสียงลงคะแนน โดยระบบสามารถตรวจสอบได้ว่าผู้เข้าร่วมประชุมมีการลงคะแนนแล้วหรือไม่ หากมีการลงคะแนนไปในทิศทางใด หรือหากกรณีลงคะแนนเสียงมีข้อผิดพลาดหรือไม่สำเร็จระบบจะแจ้งเตือนผู้เข้าร่วมประชุม และการออกเสียงลงคะแนนนั้นจะไม่ถูกบันทึกลงระบบ
13.3 – ระบบการลงคะแนนใช้อัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่เป็นมาตรฐาน	กุญแจเข้ารหัส โมดูลการเข้ารหัสลับ (cryptographic module) และอัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่ใช้ในกระบวนการเข้ารหัสลับของระบบการลงคะแนนต้องเป็นไปตามมาตรฐาน เช่น FIPS 140 Security Requirements for	Inventech Connect มีการทำ Database Encryption คือการใช้ SSL เข้ารหัสลับของข้อมูลการลงคะแนนในแต่ละการประชุม โดยจะทำการเข้ารหัสก่อนทำการส่งข้อมูลระหว่างเครือข่าย และเมื่อข้อมูลไปยังปลายทาง จึงทำการถอดรหัส ซึ่งบริษัทมีนโยบายด้านการเข้ารหัสลับข้อมูลที่ระบุถึงการเข้ารหัสลับข้อมูล ดังนี้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	Cryptographic Modules และ NIST Special Publication 800-57 Part 1 Recommendation for Key Management: Part 1 – General	1. data-in-transit encryption : ระบบมีการใช้ SSL/TLS ในการเข้ารหัสขณะรับส่งข้อมูลระหว่าง server กับ client โดยมีการติดตั้ง SSL Certificate ของ www.globalsign.com (SHA256-RSA) 2. data-at-rest encryption : ฐานข้อมูลระบบจะมีการเข้ารหัสข้อมูลส่วนบุคคล ชื่อ, นามสกุล, เบอร์ติดต่อ, email, เลขบัตรประชาชน และ เลขทะเบียนผู้ถือหุ้นโดยการเข้ารหัสด้วยวิธี AES-256 ซึ่ง Key แต่ละ Key จะถูกสร้างโดยระบบการจัดการเฉพาะ และ สามารถเข้าได้เฉพาะผู้มีสิทธิเท่านั้น
13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด	การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายคอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)	ระบบมีการใช้ SSL/TLS ในการเข้ารหัสขณะรับส่งข้อมูลระหว่าง server กับ client โดยมีการติดตั้ง SSL Certificate ของ www.globalsign.com (SHA256-RSA)
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) เพื่อป้องกัน บรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน เช่น กระบวนการเข้ารหัสลับ (cryptography) การป้องกันมัลแวร์ (malware) การตั้งค่าไฟร์วอลล์ (firewall) และการตั้งค่าระบบ (system configurations)	- มีเอกสารการปฏิบัติหรือการประเมินความเสี่ยง สำหรับระบบการลงคะแนน โดยมีการจัดทำเอกสาร Load test performance เพื่อวิเคราะห์ความเสี่ยง - ระบบการลงคะแนนมีการควบคุมทั้งหมด 5 ชั้น 1. Data Layer - มีการเข้ารหัสข้อมูลที่จำเป็น, และมีการบันทึก Log การใช้งานทั้งฝั่งผู้ดูแลระบบ และ ผู้ใช้งานทั่วไป 2. Application Stack Layer – มีการ update patch และติดตามเวอร์ชันของ Application stack ที่ใช้อยู่ตลอดเวลา 3. Server Stack Layer - โดยมีการติดตั้ง Antivirus ,malware ,Microsusaoft .Net framework package , Report viewer , SQL และการตั้งค่า Port Firewall , การเปิด

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		Port Firewall รวมถึง Webserver IIS, DNS, WDS , WSUS , FTP , Window Remote services 4. Network Stack Layer - ข้อมูลส่วนนี้ระบบมีการเช่าใช้ cloud server ของ Internet Thailand (i-Net) 5. Policies Layer - การเข้าถึง Server ต้องมีการเข้ารหัสก่อนด้วย username และ password
14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น	ระบบการลงคะแนนป้องกันการติดตั้งหรือการสั่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง และปิดใช้งานการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน ซอฟต์แวร์ของระบบการลงคะแนนต้องไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และต้องเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น	- ระบบมีการติดตั้งเฉพาะการประมวลผลที่เกี่ยวข้อง และเปิดเฉพาะการเชื่อมต่อที่จำเป็น เท่านั้น - ซอฟต์แวร์ระบบการลงคะแนนมีการตรวจสอบเรื่อง unused code อยู่ตลอด และมีการเรียกใช้ software library ที่น่าเชื่อถือเท่านั้น และยังติดตาม issue หรือปรับปรุงเวอร์ชันอย่างสม่ำเสมอ
15. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน		
15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ	ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งประกอบด้วยเหตุการณ์ที่เกี่ยวข้องกับสถานะการทำงานและความผิดปกติของระบบ การยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน การจัดการระบบเครือข่าย การจัดการซอฟต์แวร์และฟังก์ชันการลงคะแนน เป็นอย่างน้อย	- ระบบลงคะแนนมีการแสดงหลักฐาน การบันทึกเหตุการณ์ที่เกิดขึ้นในระบบลงคะแนน โดยสามารถมีการบันทึกเหตุการณ์ (activity log) ของการใช้งานทั้งในการทำงานปกติและผิดปกติของระบบลงคะแนน มีการยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน และมีฟังก์ชันในการปิดการลงคะแนน ซึ่งระบบสามารถออกรายงานที่เกิดขึ้นในรูปแบบไฟล์ PDF
15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ใช้งานในทันที บันทึกข้อผิดพลาดทั้งหมดที่เกิดขึ้น และสร้างรายงานข้อผิดพลาด (error report) รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการจัดการข้อผิดพลาดในระบบการลงคะแนน	- ระบบการลงคะแนนมีการแจ้งเตือนผู้ใช้งาน เมื่อระบบลงคะแนนเกิดข้อผิดพลาด และสามารถออกรายงานข้อผิดพลาดได้ เช่น การเข้าสู่ระบบไม่สำเร็จ และการแจ้งเตือนเมื่อทำการลงคะแนนไม่สำเร็จ โดยสามารถทำการออกรายงานข้อผิดพลาดได้ - มีเอกสารที่เกี่ยวข้องกับระบบการลงคะแนน ซึ่งมีการระบุขั้นตอนในการจัดการข้อผิดพลาดในระบบการลงคะแนน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	ระบบการลงคะแนนต้องมีมาตรการป้องกันมัลแวร์ (malware) โดยระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ บันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ และบันทึกเหตุการณ์ของกิจกรรมการแก้ไขมัลแวร์ รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการอัปเดตมาตรการป้องกันมัลแวร์	- ระบบลงคะแนนมีการติดตั้งลงบน server ที่มีการติดตั้ง antivirus คือ trend micro deep security ซึ่งมีการป้องกันได้ถึง (ransomware) และมีการแจ้งเตือนหากพบสิ่งผิดปกติ
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	Inventech Connect มีการเชื่อมต่อสื่อสารระหว่างผู้ประชุมมีการใช้ช่องทางการสื่อสารที่ปลอดภัย มีการใช้ SSL และมีการเข้ารหัสข้อมูลแบบ Symmetric – key โดยกุญแจที่ใช้ในการเข้ารหัสลับข้อมูลในแต่ละการประชุมจะถูกเปลี่ยนทุกครั้งในแต่ละการประชุมไม่ซ้ำกัน ระหว่างโอนย้ายข้อความ และข้อมูลอื่น ๆ เพื่อป้องกันการเข้าถึงข้อมูล ซึ่งมีนโยบาย ดังนี้ - นโยบายด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย และขั้นตอนปฏิบัติเพื่อควบคุมและป้องกันการถ่ายโอนข้อมูล ครอบคลุมเรื่องการเข้ารหัสลับข้อมูลระหว่างโอนย้ายข้อมูล ตามมาตรฐาน ISO 27001 และ ISO 27017 ระบบมีการเช่าใช้ cloud server ของ Internet Thailand (i-Net) โดยมีการ backup snapshot ข้อมูลทุกๆ 7 วัน