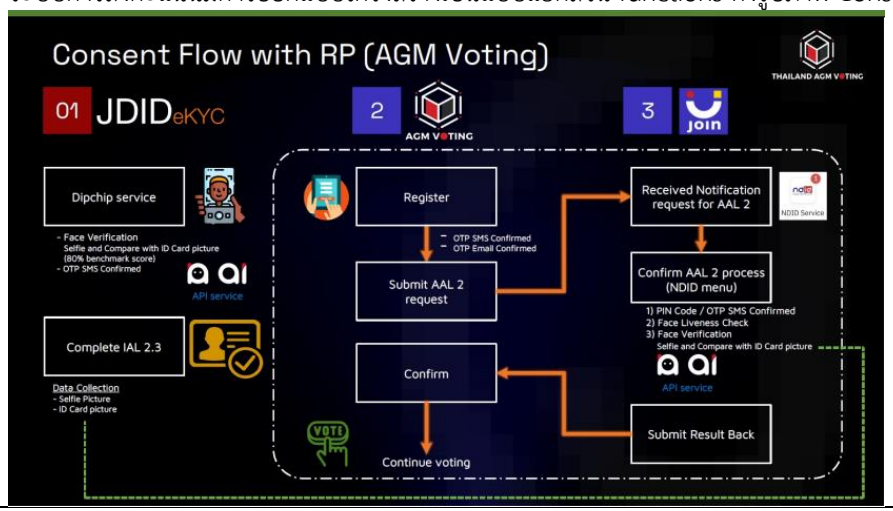
แบบประเมินความสอดคล้องด้วยตนเอง
ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ELECTRONIC VOTING SYSTEM)
ตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ขมธอ. 26-2564) เวอร์ชัน 2.0

ชื่อระบบ	AGM Voting
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท)	บจก.เจเวนเจอร์ส
ช่องทางการติดต่อผู้ให้บริการ	thitithan@J Ventures.co.th หรือ โทร 095-296-5591
วันที่ประเมินความสอดคล้อง	31 มกราคม 2568
วันที่ครบกำหนดการทบทวน	30 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 AGM Voting ซึ่งเป็นระบบการลงคะแนน และแสดงข้อมูลการประชุม และวาระการประชุมที่ใช้เทคโนโลยีBlockchain โดยมีระบบสนับสนุนในการพิสูจน์ตัวตน (eKYC) JDID Application ใช้สำหรับผู้มีสิทธิลงคะแนน เพื่อพิสูจน์ตัวตน และมีระบบการยืนยันตัวตน JOIN Application ใช้สำหรับผู้มีสิทธิลงคะแนน เพื่อยืนยันตัวตนแบบ Multi Factor Authentication

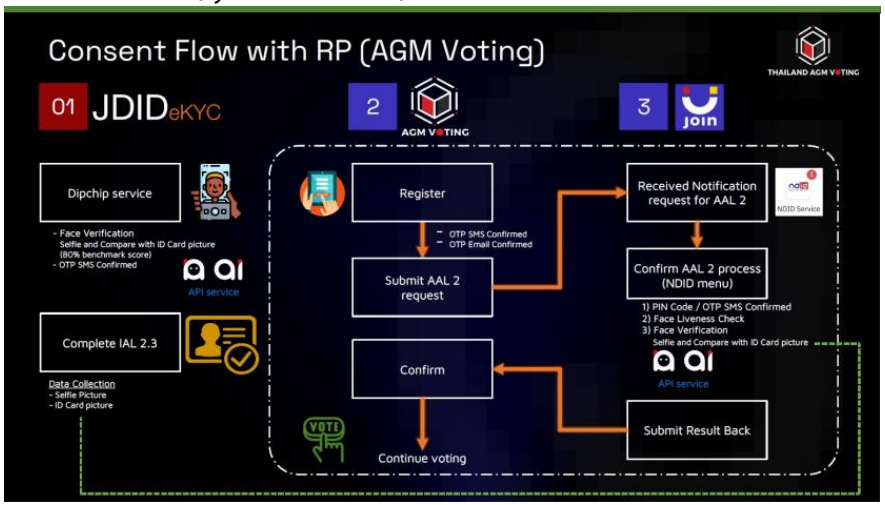
หมายเหตุ : สพธอ ไม่เกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน		
1. การออกแบบระบบ (System Design) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามกระบวนการการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ		
1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด	ระบบการลงคะแนนมีฟังก์ชันการทำงานที่จำเป็นตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด ซึ่งครอบคลุมการเตรียมข้อมูลสำหรับการลงคะแนน การตรวจสอบระบบการลงคะแนนก่อนการลงคะแนน การเปิดลงคะแนนการลงคะแนน การส่งผลลงคะแนน การปิดลงคะแนน การนับคะแนน และการรายงานผลรวมของการลงคะแนน	กระบวนการลงคะแนนทั้งหมดจะควบคุมโดยผู้จัดการประชุม เพื่อให้เป็นไปตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง เช่น ใน การประชุมสามัญประจำปีผู้ถือหุ้น จะเป็นไปตามพระราชบัญญัติบริษัทมหาชนจำกัด พ.ศ. 2535 และแนวทางการกำกับดูแล กิจการที่ดี ของตลาดหลักทรัพย์แห่งประเทศไทย ส่วนในการประชุมใหญ่เจ้าของร่วม และ การประชุมผู้ถือหุ้นบริษัทตามประมวล กฎหมายแพ่งและพาณิชย์ ฉบับที่ 18 พ.ศ. 2551 การประชุมใหญ่ ในส่วนของการประชุมของอาคารชุดก็จะเป็นไปตาม พระราชบัญญัติอาคารชุด (ฉบับที่ 4) พ.ศ.2551 ซึ่งทั้งหมดจะต้องเป็นไปตามพระราชกำหนด ว่าด้วยการประชุมผ่านสื่อ อิเล็กทรอนิกส์ พ.ศ. 2563 โดยขั้นตอนต่างๆจะเป็นไปดังนี้ 1. การเตรียมข้อมูลสำหรับการลงคะแนน ผู้จัดการประชุมจะเป็นผู้จัดเตรียมข้อมูล ข้อกำหนด คำอธิบาย ความสามารถของระบบการลงคะแนน 2. การตรวจสอบระบบการลงคะแนนก่อนการลงคะแนน ก่อนการประชุมทุกครั้งจะมีการทดสอบระบบลงคะแนนร่วมกับ ผู้จัดการประชุม 3. การเปิดลงคะแนน ผู้ควบคุมระบบจะเปิดลงคะแนนเมื่อผู้จัดการประชุมประกาศเปิดลงคะแนนในการประชุม 4. การลงคะแนน ผู้เข้าร่วมประชุมออนไลน์จะลงคะแนนพร้อมๆ กันในการประชุม 5. การส่งผลลงคะแนน ระบบจะส่งคะแนนเข้าไปยังฐานข้อมูลของผู้จัดการประชุม ซึ่งจะมีแยกระหว่างคะแนนจากผู้ มาร่วมประชุมด้วย

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ตนเอง คะแนนจากผู้ที่มอบฉันทะ และคะแนนออนไลน์ 6. การปิดลงคะแนน ควบคุมระบบจะปิดลงคะแนนเมื่อผู้จัดการประชุมประกาศปิดลงคะแนนในการประชุม 7. การนับคะแนน การนับคะแนนแต่ละวาระจะเป็นไปตามหลักเกณฑ์ของการประชุม เนื่องจากแต่ละวาระจะมีเกณฑ์การ นับคะแนนแตกต่างกันโดยเฉพาะคะแนนจากผู้ที่งดออกเสียงลงคะแนน ซึ่งผู้จัดการประชุมจะเป็นผู้จัดเตรียมการนับ คะแนนให้ตรงตามหลักเกณฑ์ 8. การรายงานผลรวมของการลงคะแนน ระบบจะส่งคะแนนเข้าไปยังฐานข้อมูลของผู้จัดการประชุม โดยผู้จัดการประชุม จะเป็นผู้รายงานผลการลงคะแนน ทั้งรายงานแยกระหว่างคะแนนจากผู้มาร่วมประชุมด้วยตนเอง คะแนนจากผู้ที่มอบ ฉันทะ และคะแนนออนไลน์ และรายงานผลรวมคะแนนทั้งหมด
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ (system accuracy and reliability) การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) ในสภาวะที่ใกล้เคียงกับการใช้งานจริงในกระบวนการลงคะแนน และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)	มีการทดสอบขีดความสามารถของระบบในกระบวนการบันทึกค่าแฮช (Hash) ของผู้ลงคะแนนและผลการลงคะแนน พบว่า ระบบสามารถรองรับปริมาณธุรกรรมสูงสุด (maximum volume) 371 รายการ/วินาที นอกจากนี้ บริษัทฯ ได้มีการทำ Penetration Testing ของระบบ AGM Voting บนระบบปฏิบัติการ iOS และ Android โดย ใช้วิธีการทางเทคนิคแบบ Grey-Box ซึ่งไม่พบช่องโหว่ที่มีนัยสำคัญ
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบซอฟต์แวร์ (software tester) ของผู้พัฒนาระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนได้จัดทำรายงานผลการทดสอบระบบ (test report) ซึ่งได้กำหนด test case ไว้ 14 กรณี ครอบคลุมขั้นตอนการใช้งานของระบบของผู้ลงคะแนนและผู้จัดประชุม (ผู้ควบคุมการลงคะแนน) พบว่า ผลการทดสอบเป็นไป ตามความคาดหวังของผลลัพธ์ที่กำหนด (Expected Result) ตามเอกสารแนบ AGM Test Result.pdf ตาม link ด้านล่าง; AGM Test Result.pdf
2. การพัฒนาระบบ (System Development) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการพัฒนาระบบโดยใช้แนวปฏิบัติที่ดี		
2.1 – การพัฒนาระบบการลงคะแนนใช้แนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์	ระบบการลงคะแนนใช้ภาษาโปรแกรมและรูปแบบการเขียนโปรแกรมที่เป็นที่ยอมรับ รวมถึงแนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์ เช่น มาตรฐาน ISO/IEC/IEEE 12207 Systems and software	ระบบการลงคะแนน (AGM Voting Application) ใช้ภาษาและมีรูปแบบการเขียนโปรแกรม ดังนี้ • Flutter: ใช้สำหรับการพัฒนา Mobile Application Framework ของ Android และ iOS • Nuxt.js: ใช้สำหรับการพัฒนา Web Application Framework บน Web Dashboard ให้ผู้ดูแลระบบใช้งาน • NodeJS: ใช้สำหรับการพัฒนา API Framework สำหรับจัดทำ API เชื่อมต่อทุกระบบเข้าด้วยกัน • Parse: ใช้สำหรับการพัฒนา Back-end as a Service ที่มีประสิทธิภาพสูง สำหรับระบบสมาชิกและระบบจัดเก็บข้อมูล ซึ่งมีฐานข้อมูลเป็น MongoDB

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	engineering – Software life cycle processes และ ISO/IEC 29110 Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs)	อีกทั้งยังใช้วิธีการออกแบบและพัฒนาซอร์สโค้ดแอปพลิชันตามมาตรฐาน SDLC – Hybridge of Waterfall and Agile methodology โดยมีการพัฒนาตาม Phase ดังนี้ 1. Definition phase - กำหนดขอบเขตและเป้าหมายใหญ่ของ project 2. Requirement phase - กำหนดรายละเอียดของความต้องการใน project แบบละเอียด 3. Design phase – ออกแบบระบบ ให้ตรงตาม Requirement ทุกประการ 4. Construction Phase - ทำการพัฒนาระบบตาม Designed ที่ได้รับการอนุมัติแล้ว 5. Testing – SIT and UAT phase - ทำการ test ระบบตาม design และ ตรวจสอบว่าตรงตาม requirement ถ้าไม่ตรงให้ ลง log แล้วกลับไปแก้ที่ root cause เช่น requirement, design หรือ coding แล้วทำการปรับระบบเพื่อกลับมา test ใหม่ 6. Production Phase เมื่อระบบทำ UAT และ sign off ให้นำขึ้น production 7. Support after live phase - ทำการ monitor ระบบ ถ้าไม่ถูกต้องให้ลง Incident log เพื่อเริ่มกระบวนการ Incident Management ระบบการลงคะแนน (AGM Voting Application) ใช้บริการอื่น ๆ เพื่อเพิ่มประสิทธิภาพการทำงานของระบบ AGM Voting ดังนี้ • NDID: ใช้สำหรับการพัฒนา Digital ID Platform เพื่อเป็นช่องทางในการพิสูจน์และยืนยันตัวตนของผู้ลงคะแนน แบบไม่พบหน้ากัน อย่างปลอดภัย • JFINCHAIN Network: เป็น Blockchain Infrastructure ที่ร่วมก่อตั้งและพัฒนาระหว่างพันธมิตรที่มีความเชี่ยวชาญด้านเทคโนโลยี และองค์กรชั้นนำของประเทศให้เป็น Public Blockchain Infrastructure ในประเทศไทยและเป็นระบบนิเวศ(ecosystem) ที่ถูกสร้างขึ้นและ นำมาใช้ งานจริงที่มี Validator Node เป็นองค์กรที่สาธารณชนรู้จักโดยทั่วไป มีความปลอดภัย โปร่งใสและน่าเชื่อถือระบบนิเวศ JFINCHAIN ขับเคลื่อนด้วยเหรียญ JFIN เพื่อเป็นสื่อกลางแทนค่าใช้จ่ายธุรกรรม (Gas Fee) ที่มีเป้าหมายในการลดความผันผวนของราคาจึงทำให้สามารถประเมินค่าใช้จ่ายได้และมีราคาที่สมเหตุสมผล Link : https://exp.jfinchain.com/txs
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน (modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน functions ดังรูปภาพ Consent Flow with RP (AGM Voting) 

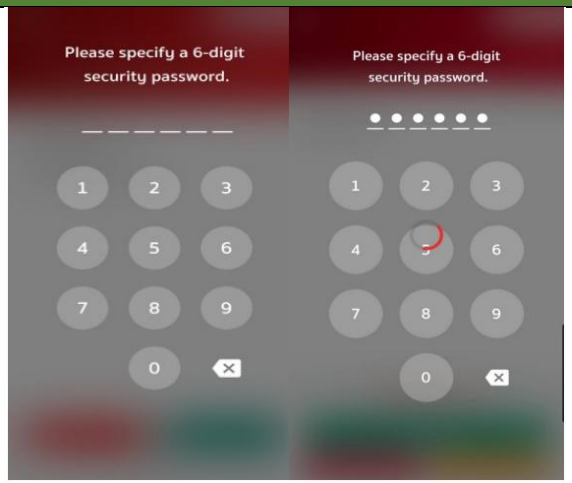
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ระบบการลงคะแนนมีการออกแบบโครงสร้าง modules ต่างๆ ออกเป็น 3 applications ซึ่งแยกจากกันอย่างอิสระ ดังนี้ • ระบบหลัก - AGM Voting Application เป็นระบบการลงคะแนน และแสดงข้อมูลการประชุม และวาระการประชุม • ระบบสนับสนุน - การพิสูจน์ตัวตน (eKYC) JDID Application ใช้สำหรับผู้มีสิทธิลงคะแนน เพื่อพิสูจน์ตัวตนโดยทำการแสดงตนและ dip chip ต่อหน้าเจ้าหน้าที่สาขา ตามมาตรฐาน IAL 2.3 - การยืนยันตัวตน JOIN Applicationใช้สำหรับผู้มีสิทธิลงคะแนน เพื่อยืนยันตัวตนแบบ Multi Factor Authentication ตามมาตรฐาน AAL 2
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้ (self-modifying code)	Applicationระบบการลงคะแนน (AGM Voting) ได้มีการพัฒนาเขียนซอร์สโค้ดตามมาตรฐาน SDLC – Hybridge of Waterfall and Agile methodology ซึ่งเป็นไปตามมาตรฐานสากล (Best Practice) และพัฒนาตาม Guideline ที่เป็น มาตรฐานของทางบริษัทที่จัดวางไว้ (Dev-Ops) ทั้งนี้ จะมีกระบวนการทดสอบการใช้งานในระบบ Development เพื่อให้ยืนยันการทำงานเป็นไปตามที่วางแผนไว้กับทาง Tester ในโครงการ และมีการร่วมวิเคราะห์การเขียน (Analyze Code) จากผู้ที่เชี่ยวชาญจาก J Ventures โดยมีการทำ Peer-to-peer source code และ review เป็นการภายในเท่านั้น โดยไม่ได้ใช้ self-modifying การพัฒนาหรือการ Deploy Code ไปที่ระบบ Production บริษัทฯ ใช้ CI/CD ตามมาตรฐานของ GITLAB เพื่อเป็นตัวควบคุม การพัฒนาและการแก้ไขให้เหมาะสมพร้อมมีระบบการตรวจสอบ (Tracking) หรือ การเทียบการเปลี่ยนแปลงของซอร์สโค้ด (Code Compare) อีกด้วย รวมไปถึงส่วนของการพัฒนาการเชื่อมต่อตามมาตรฐานสากล ด้วย HTTPS และ TLS 1.2 สำหรับ Transport Layer Security ระหว่างฝั่ง Client และ Server และในส่วนของการเก็บรักษาข้อมูลการลงคะแนนของระบบ AGM Voting ใช้เทคโนโลยี Blockchain ที่มีความปลอดภัยสูงไม่สามารถแก้ไขได้ และมีความโปรงใส เพื่อให้การเก็บรักษาและการ ตรวจสอบเป็นไปได้อย่างปลอดภัยและน่าเชื่อ หมายเหตุ : ในปี 2568 ทาง J Ventures กำลังดำเนินการขอรับรองมาตรฐาน ISO 29110 เป็นมาตรฐานที่มุ่งเน้นให้การรับรองคุณภาพการบริหารงานหรือผลิตภัณฑ์ซอฟต์แวร์
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน	Servers ของระบบการลงคะแนน ติดตั้งอยู่บน Amazon Web Services (AWS) ที่ได้รับมาตรฐานสากล โดยมีการ backup servers ทุกวัน ดังนั้นเมื่อเกิดวิกฤติแล้วต้องทำการกู้คืนข้อมูลต่างๆจะสามารถนำ backup ล่าสุดมา restore เพื่อให้ระบบกลับมาใช้งานได้ โดยมี RPO (Recovery Point Objective) 24 ชม. และ RTO (Recovery Time Objective) 1 ชม. อีกทั้งระบบมีการแจ้งเตือนการ backup สำเร็จ หรือ ไม่สำเร็จ ผ่าน email alert ให้ทุกวัน นอกจากนั้น Hash ของข้อมูลผู้ ลงคะแนนและผลการลงคะแนน จะถูกจัดเก็บไว้บน Blockchain จึงทำให้ไม่มีการสูญหาย

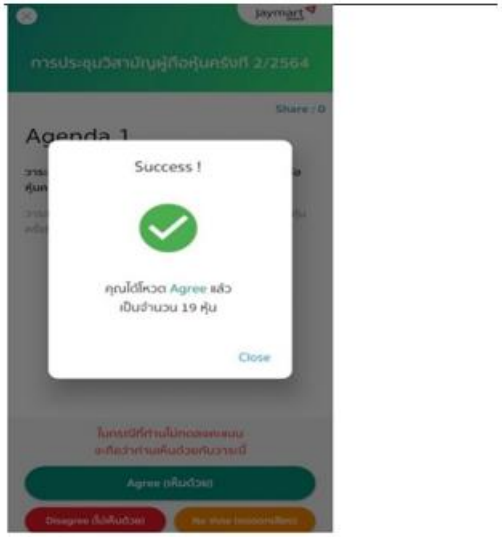
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
3. ความโปร่งใส (Transparent) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนและกระบวนการลงคะแนนมีการออกแบบที่มีความโปร่งใส		
3.1 – เอกสารอธิบายการออกแบบ การทำงาน การเข้าถึง มาตรการความมั่นคงปลอดภัย และรายละเอียดอื่น ๆ ของระบบการลงคะแนน สามารถอ่านและทำความเข้าใจได้	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารเกี่ยวกับระบบการลงคะแนน 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)	**(1) ภาพรวมของระบบ (system overview)**  ตามลิงก์ที่แนบ3.1. AGM Voting Flow on iApp Technology **(2) ประสิทธิภาพของระบบ (system performance)** มีการทดสอบขีดความสามารถของระบบในกระบวนการบันทึกค่าแฮช (Hash) ของผู้ลงคะแนนและผลการลงคะแนน พบว่าระบบสามารถรองรับปริมาณธุรกรรมสูงสุด (maximum volume) 371 รายการ/วินาที **(3) ความมั่นคงปลอดภัยของระบบ (system security)** บริษัทฯ ใช้มาตรการความมั่นคงตามมาตรฐาน ISO27001-2022 หัวข้อ การควบคุมการเข้าถึง (Access Control) บริษัทฯ จัดทำนโยบายนี้เพื่อเป็นแนวทางในการกำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูลภายใน ข้อมูลลูกค้า ระบบเครือข่าย และ ระบบเทคโนโลยีสารสนเทศขององค์กรเพื่อปกป้องข้อมูล ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศขององค์กร จากการเข้าถึง โดยผู้ที่ไม่ได้รับอนุญาตเพื่อกำหนดกระบวนการในการบริหารจัดการ อนุมัติ/อนุญาต สร้าง เปลี่ยนแปลง ถอดถอน และ ยกเลิกบัญชีผู้ใช้และสิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศที่สำคัญ
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนน เตรียม	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ	1. จัดทำ นโยบายควบคุมการเข้าถึงต้องมีการกำหนดเป็นลายลักษณ์อักษร และทบทวนทุก 6 เดือน เพื่อให้มั่นใจว่าตรงตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ 2. กำหนดให้สิทธิ์ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น 3. จัดทำกระบวนการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต 4. ปฏิบัติตามกระบวนการจัดการสิทธิ์และการถอดถอนสิทธิ์การเข้าถึงของผู้ใช้งานทุกประเภทและทุกระบบบริการทั้งหมดของบริษัทฯ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ไว้พร้อมสำหรับการตรวจสอบระบบ		5. ดำเนินงานตามหลักเกณฑ์ที่กำหนด ให้สอดคล้องกับสิทธิ์ของพนักงานที่เกี่ยวข้อง โดยให้เข้าถึงตามระดับสิทธิ์ที่ได้รับตามมอบหมาย 6. สิทธิ์ที่มอบหมายให้พนักงานต้องถูกเป็นความลับห้ามเปิดเผยให้ผู้ที่ไม่เกี่ยวข้องทราบ รวมถึงข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน ซึ่งเป็นข้อมูลลับ 7. จัดให้มีการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้ 8. สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อข้อมูลสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับ การถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน 9. พนักงานต้องดำเนินงานตามวิธีปฏิบัติของบริษัทฯ สำหรับการใช้งานข้อมูลการพิสูจน์ตัวตนและต้องจัดเก็บ User และPassword ที่ใช้ในการพิสูจน์ตัวตนให้เป็นข้อมูลลับ 10. การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง โดยห้ามไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงสามารถเข้าถึงสารสนเทศและฟังก์ชัน ยกเว้นจะได้รับการอนุญาตจากผู้มีอำนาจอนุมัติ 11. การเข้าถึงระบบต้องมีการ Login เข้าระบบที่มีความมั่นคงปลอดภัย โดยการ Login เพื่อพิสูจน์ตัวตน หาก Login ไม่ถูกต้อง 5 ครั้ง ระบบจะ Lock และในกรณีที่ผู้ใช้งาน ไม่ได้ใช้งานระบบอย่างต่อเนื่องเป็นระยะเวลา 10 นาที เมื่อ ต้องการเข้าใช้งานต่อ ต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง 12. ระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ 13. ส่วนระบบ Firewall ใช้ระบบ AWS Security Group ร่วมกับ FortiGate (Next-Generation Firewall- NGFW) Ultra-fast security, end to end defensive system โดย Next Generation Firewall (NGFW) เป็น Firewall ที่มีประสิทธิภาพสูง และสามารถรับมือภัยคุกคามที่ซับซ้อน โดยฟังก์ชันต่าง ๆ ที่เพิ่มเข้าไปมีความแตกต่างจาก Firewall ทั่วไป คือ การเข้าถึงระดับ Application Layer สามารถแยกการใช้งานของ Application Layer ว่าเป็นการใช้โปรแกรม ประเภทอะไร ทำให้ สามารถตั้ง Policy เพื่อทำการควบคุมการใช้งาน Application ต่าง ๆ เหล่านั้นได้ เช่น ภายในองค์กรกำหนดสิทธิ์ให้ใช้ ระบบผ่าน VPN access และมีการป้องกัน cyber attack เช่น • IPS (Intrusion Protection System) ระบบตรวจสอบและโต้ตอบการบุกรุก เมื่อตรวจพบข้อมูลที่มีลักษณะที่ เป็นความเสี่ยงต่อเครือข่าย ก็จะทำการป้องกันข้อมูลนั้น ไม่ให้เข้ามาในเครือข่ายได้ • Antivirus เพื่อเสริมประสิทธิภาพในการป้องกันไวรัสทั่ว ๆ ไป เช่น Malware, Trojan, Spy Ware เป็นต้น ที่จะ เข้ามาในระบบเครือข่ายเพื่อทำความเสียหายกับข้อมูลหรือระบบคอมพิวเตอร์ • Firewall ระบบคัดกรองข้อมูลที่พยายามผ่านเข้ามาสู่ระบบเครือข่าย เช่น ข้อมูลชนิดนี้เป็นใคร (Source) ข้อมูล ชนิดนี้ทำอะไร (Service) และจะไปที่ไหน (Destination) **(4) การติดตั้งซอฟต์แวร์ (software installation),** การทำงานของระบบ (system operations) และ คู่มือการใช้งาน (user manual) ผู้พัฒนาระบบการลงคะแนน ได้จัดทำเอกสารเกี่ยวกับการติดตั้งซอฟแวร์ การทำงานของระบบและคู่มือการใช้งานโดยแบ่ง 4.1 การใช้งานสำหรับผู้จัดประชุม คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Administrator (Link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Adminitrator) 4.2 คู่มือการใช้งานโดยแบ่งออกเป็นการใช้สำหรับผู้ลงคะแนน ตามเอกสารแนบ คู่มือ JMART – EGM No. 3_2565 (Link 5.3 JMART - EGM Notice 3_2565_TH.pdf.pdf)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		(5) การบำรุงรักษาระบบ (system maintenance) บริษัทฯ จัดทำเอกสารสำหรับการบำรุงรักษาระบบสารสนเทศ โดยมีการ Upgrading Hardware, System, Software ให้ ทันสมัยอยู่เสมอ อีกทั้ง ยังมีการ Monitor servers: โดย Monitoring Disk, CPU และ Memory 7*24 hours ผ่านการใช้ Tools ดังนี้ AWS Cloud Watch monitoring warning message ผ่าน LINE Notification
	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)	ขอภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบที่ใช้งานจริงแล้ว ตาม Link ด้านล่าง 13.1 ขอภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบที่ใช้งานจริงแล้ว.pdf
4. การเข้าถึงอย่างเท่าเทียม (Equitable Access) วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม		
4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงภาพและเสียง) และรูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัสบนหน้าจอ) ในลักษณะที่สอดคล้องกัน	ปัจจุบันผู้ลงคะแนนสามารถใช้งาน ผ่าน Mobile และ Tablet เท่านั้น โดยแสดงผลหน้าจอเหมือนกันทั้ง 2 อุปกรณ์ โดยผู้ ลงคะแนนสามารถกดปุ่ม/สัมผัส ได้ตามฟังก์ชันที่กำหนดบนหน้าจออุปกรณ์ของผู้ลงคะแนน ตามเอกสารแนบ 5.2 รูปแคปเจอร์ หน้าจอการแสดงผลบนโทรศัพท์ ตาม Link ด้านล่าง 5.2 รูปแคปเจอร์หน้าจอการแสดงผลบนโทรศัพท์มือถือ และรูปภาพแสดงผลการใช้งานบนแทปเล็ต .pdf
4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ	รูปแบบการแสดงผล (display format) แสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน และไม่ทำให้เกิดอคติกับตัวเลือกลงคะแนนใด ๆ ที่นำเสนอต่อผู้ลงคะแนน เช่น ตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน	รูปแบบการแสดงผลของระบบการลงคะแนน จะแสดงผลตัวเลือกการลงคะแนนทั้งหมดด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกันทุก ๆ อุปกรณ์ ทั้ง IOS และ Android application (Responsive) ตามเอกสารแนบ 5.2 รูปแคปเจอร์หน้าจอการแสดงผลบนโทรศัพท์ Link ด้านล่าง 5.2 รูปแคปเจอร์หน้าจอการแสดงผลบนโทรศัพท์มือถือ และรูปภาพแสดงผลการใช้งานบนแทปเล็ต .pdf

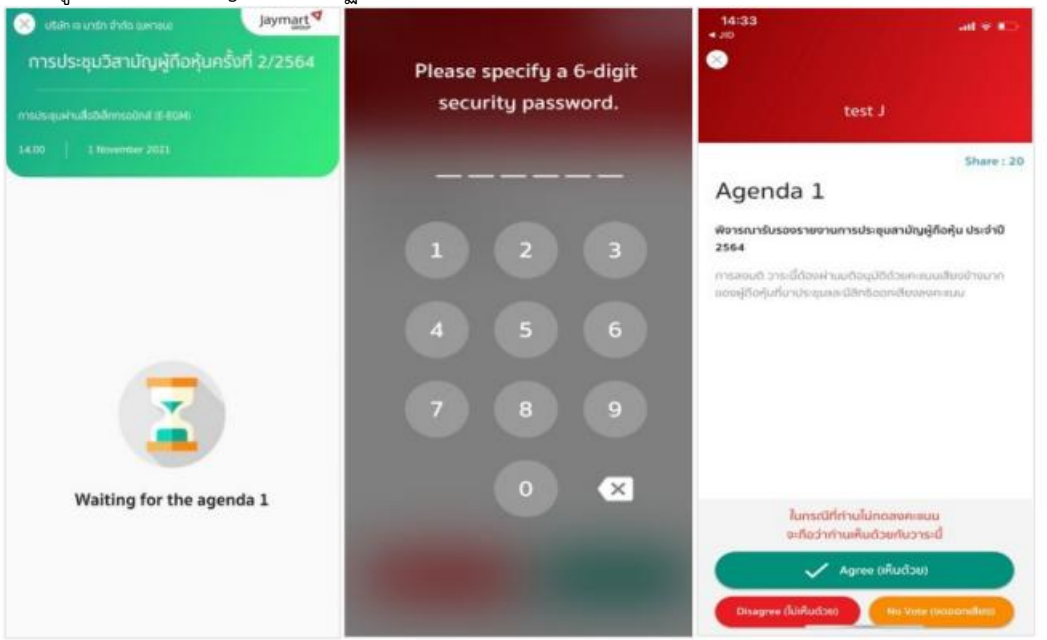
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
5. การลงคะแนนตรงตามเจตนา (Cast as Intended) วัตถุประสงค์ เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้		
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงกับความต้องการของผู้ลงคะแนน	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล (preference setting) ตามความต้องการของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษร และสีของภาพ	ระบบการลงคะแนน (AGM Voting) มีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก ตามลักษณะของ Mobile Device (Responsive design) และไม่สามารถปรับแต่งค่าตามความต้องการของผู้ใช้งานรายบุคคลได้
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนน และการส่งผลลงคะแนนได้โดยตรง	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง เช่น รูปแบบการแสดงผลของข้อมูล (display format) การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้าถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ (touch screen gestures) รวมถึงระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) เช่น การให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนน	ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง ผ่านท่าทางการสัมผัสบนหน้าจอ (touch screen gestures) หรือเป็นไปตามคุณสมบัติของโทรศัพท์มือถือ. โดยมีรูปแบบการแสดงผลข้อมูล (display format) ดังนี้ - การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน สามารถกด Agree (เห็นด้วย) , Disagree (ไม่เห็นด้วย) , No Vote (งดออกเสียง) ได้ - การเปลี่ยนหน้าจอ สามารถกดดูหน้าถัดไป/ก่อนหน้าได้ - การเลื่อนหน้าจอขึ้น/ลง สามารถเลื่อนหน้าจอขึ้น/ลงเพื่อดูรายละเอียดของวาระได้ ระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) คือ การให้ผู้ลงคะแนนยืนยันเจตนาก่อนส่งผลลงคะแนนทุกวาระ. โดยการกด PIN ซึ่งเป็นรหัสที่ผู้ใช้งาน/ผู้ลงคะแนนจะทราบแต่เพียงผู้เดียว (Something you know)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	หรือการแจ้งสถานะของการลงคะแนนให้ผู้ลงคะแนนทราบ	 รูปที่ 1 แสดงหน้าต่างให้ผู้ลงคะแนนยืนยันเจตนาก่อนการลงคะแนนหน้าหน้าการยืนยัน กด PIN ก่อนการลงคะแนน
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน คำแนะนำ และข้อความจากระบบด้วยภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งข้อความที่ไม่ให้เกิดความสับสนในการลงคะแนน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต หรือการเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) และการแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว นอกจากนี้ ระบบมีการแสดงคำแนะนำและข้อความที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนน	ระบบมีการแสดงข้อมูลกฎกติกาของการลงคะแนน และคำแนะนำ ผ่านการแจ้งในหนังสือเชิญประชุมผู้ถือหุ้น ดังตัวอย่างตาม ลิงก์ด้านล่าง ซึ่งส่งแจ้งทางอีเมลของผู้เข้าร่วมการประชุม (Link 5.3 JMART - EGM Notice 3_2565_TH.pdf.pdf) ระบบมีการวางวาระตามลำดับไม่ก่อให้เกิดความสับสนในการลงคะแนน ตัวอักษรชัดเจน และอ่านง่าย โดยผู้ลงคะแนนสามารถ กดเลือกลงคะแนนได้เพียง 1 ตัวเลือกเท่านั้น โดยมีตัวเลือกดังนี้ Agree (เห็นด้วย) , Disagree (ไม่เห็นด้วย) , No Vote (งดออก เสียง) และระบบจะมีการแจ้งเตือน เมื่อกดเลือกตัวเลือกสำเร็จ หากผู้ลงคะแนนมีความต้องการที่จะเปลี่ยนแปลงผลการ ลงคะแนน สามารถทำได้จนกว่าผู้จัดประชุมจะปิดวาระนั้น ในกรณีที่ผู้ลงคะแนนไม่กดเลือกปุ่มใด ๆ จนครบระยะเวลาลงคะแนน ระบบจะบันทึกว่าผู้ลงคะแนนเห็นด้วยกับวาระนี้เมื่อผู้ลงคะแนนทำการลงคะแนนสำเร็จระบบจะแสดงหน้าต่างแจ้งเตือน (popup) การลงคะแนนสำเร็จให้ทราบ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ในการปฏิบัติงานและการบำรุงรักษาระบบ	 รูปที่ 1 แสดงการวางข้อความและตัวเลือกสำหรับการลงคะแนน  รูปที่ 2 การแจ้งเตือนเมื่อโหวตสำเร็จ ซึ่งแสดงเป็นข้อความผ่าน Popup ระบบการลงคะแนนสำหรับผู้จัดประชุมไม่มีฟังก์ชันแสดงคำแนะนำในการใช้งาน แต่ทางบริษัทฯ ได้จัดทำคู่มือ แนวทางปฏิบัติ งาน และการบำรุงรักษาระบบสำหรับผู้จัดการประชุม (Administrator) ตามลิงก์ด้านล่าง (Link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Adminitrator)
6. ความเหมาะสมต่อการใช้งาน (Usable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้อย่างเหมาะสม		
6.1 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบการลงคะแนน เพื่อให้มั่นใจว่าระบบการลงคะแนนสามารถใช้งานกับผู้คะแนนทุกคน (ซึ่งอาจรวมถึงผู้สูงอายุและบุคคลที่มีความบกพร่องทางการมองเห็น) ได้อย่างเหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี เช่น มาตรฐาน Web Content Accessibility Guidelines (WCAG)	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบ การลงคะแนนการประชุม ซึ่งกลุ่มตัวอย่างมีช่วงอายุอยู่ระหว่าง 20 - 59 ปีจำนวน 25 คน แต่ยังไม่รองรับ “บุคคลที่มีความ บกพร่องทางการมองเห็น” ซึ่งบริษัทได้ทดสอบ โดยทดสอบกับระบบปฏิบัติการ Android และระบบปฏิบัติการ iOS

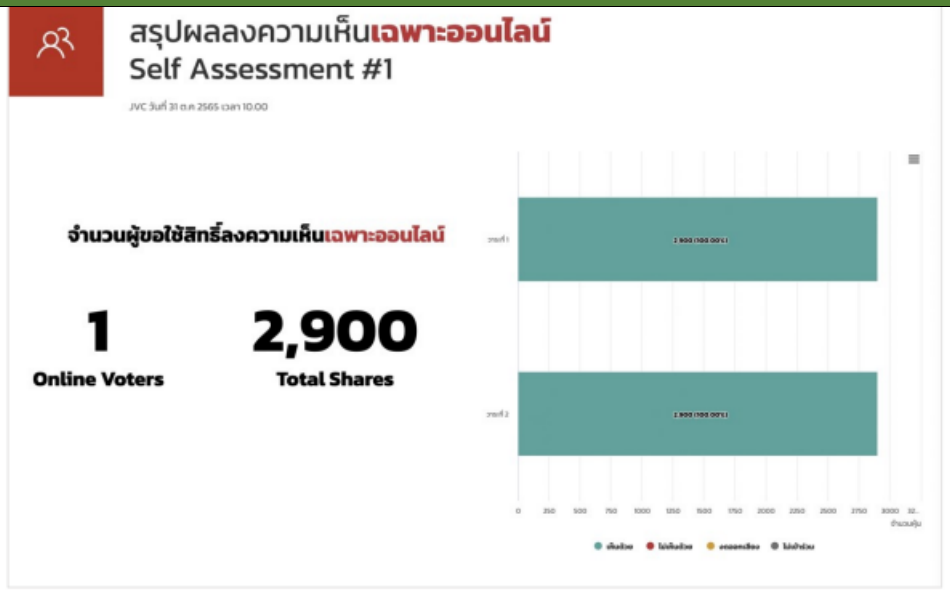
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	2.0 ของ World Wide Web Consortium (W3C)	
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ	ในปัจจุบันบริษัท เจ เวนเจอร์ส บริการลูกค้าโดยการมอบหมายเจ้าหน้าที่ของ เจ เวนเจอร์ส เป็นผู้ควบคุมระบบลงคะแนนในทุก การประชุม โดยบริษัทฯ ได้รับมอบหมายจากนิติบุคคลผู้ว่าจ้างตามใบเสนอราคาที่เรียกเก็บเป็นค่าบริการจาก นิติบุคคล (บริษัท JMART) นั้น ซึ่งหากผู้จัดประชุมต้องการควบคุมระบบการลงคะแนนด้วยตนเอง ทางบริษัทฯ ได้จัดทำคู่มือสำหรับผู้จัดประชุม ซึ่ง มีคำแนะนำในการตั้งค่าระบบ วิธีการใช้งานในระหว่างลงคะแนน การเปิด-ปิดระบบการประชุม และมีการฝึกอบรมการใช้งาน สำหรับผู้ควบคุมระบบการลงคะแนนเพื่อให้ ผู้ควบคุมการประชุมปฏิบัติงานได้สำเร็จ
ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ		
7. การทำงานร่วมกัน (Interoperable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน		
7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนอยู่ในรูปแบบที่ทำงานร่วมกันได้หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงาน ร่วมกันได้ (interoperable format) ระบบนำเข้าข้อมูลรายชื่อผู้มีสิทธิลงคะแนนในรูปแบบไฟล์ XLS และส่งออกข้อมูลรายชื่อผู้ ลงทะเบียนเข้าร่วมการประชุมในรูปแบบไฟล์ CSV และ json format และ XLS ได้ ซึ่งอยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) ตามข้อ 4 ของลิงก์ที่แนบ (Link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Adminitrator)
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้รูปแบบมาตรฐาน ในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่าง ๆ	ระบบการลงคะแนนโปรโตคอล TCP/IP ในการติดต่อสื่อสาร (communication protocol) และใช้โปรโตคอล HTPPS ในการ เรียกโปรแกรมบราวเซอร์ (Browser Program) เพื่อเรียก Service ภายในต่างๆ ให้ทำงานตาม Request เช่น https://ekyc.jfin.neteork เป็นต้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
8. การตรวจสอบ (Auditable) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบความถูกต้องของผลลงคะแนน		
8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	ผลลงคะแนนที่ได้จากการลงคะแนนของผู้ลงคะแนน มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลได้ (tamper-evidence) ระบบการลงคะแนนเปิดโอกาสให้ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกไป แจ้งข้อผิดพลาดในผลลงคะแนนที่เกิดจากระบบการลงคะแนน และเริ่มต้นลงคะแนนใหม่หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน (ขึ้นอยู่กับกฎหมายหรือหลักเกณฑ์ที่กำหนด) รวมถึงควรมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ระบบการลงคะแนนต้องสร้างรายงานที่จะช่วยให้ผู้ตรวจสอบภายนอก (external auditor) สามารถตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง รวมถึงผู้พัฒนาระบบการลงคะแนนจัดทำขั้นตอนสำหรับการตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง	ระบบมีการบันทึก Hash ของผู้ลงคะแนนและผลการลงคะแนน ไว้บน Blockchain ทำให้ผู้ดูแลระบบสามารถตรวจสอบ transaction ที่เกิดขึ้นย้อนหลังได้ผ่านข้อมูลที่บันทึกบน blockchain นอกจากนี้ยังมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้น ในระหว่างการลงคะแนน โดยแจ้งผ่านฝ่ายนักลงทุนสัมพันธ์ของ บริษัท/ผู้จัดการประชุม/ผู้ประสานงานนิติบุคคลอาคารชุด ซึ่งจะส่งปัญหาต่อมายังทีม Support ของผู้ลงคะแนนโหวตโดยเฉพาะ ผู้จัดประชุมสามารถตรวจสอบผลการลงคะแนนเทียบกับผู้มีสิทธิ์ลงคะแนนได้เพื่อตรวจสอบความถูกต้องของยอดผลการ ลงคะแนนได้ที่หน้าสรุปผลการลงคะแนน ซึ่งจะแสดงเมื่อปิดการประชุม ระบบสามารถส่งออกข้อมูลการลงคะแนนให้ Auditor ตรวจสอบได้ รวมถึงการรวมคะแนนกับคะแนนส่วนอื่นๆ จากฐานข้อมูล (Database) ของบริษัทผู้จัดการประชุมโดยระบบสามารถ Export ไฟล์เป็น CSV หรือ json format

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
9. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy) [1] วัตถุประสงค์ เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง		
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่แสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน	การลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผล ลงคะแนนได้โดยไม่ต้องแสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน โดยก่อนทำการโหวตจะต้องทำการ ยืนยันตัวตน และป้อนรหัส PIN ก่อนกดลงคะแนนในทุกวาระการประชุมเพื่อยืนยันว่าคนที่ทำการลงคะแนนเป็นผู้มีสิทธิ ลงคะแนนนั้นจริง การแสดงผลการลงคะแนนจะปรากฏเพียงภาพรวมของคะแนน โดยไม่ระบุตัวตนของผู้ลงคะแนน ตามรายละเอียดของลิงก์ที่ แนบ ข้อ 5.7-5.9 (Link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Adminitrator)  รูป แสดงหน้าวาระการประชุม การยืนยันตัวตนเพื่อยืนยันว่าเป็นผู้มีสิทธิลงคะแนนนั้นจริง และแสดงหน้าสำหรับลงคะแนน (จากซ้ายไปขวาตามลำดับ)
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่า	ในการลงคะแนนผู้ลงคะแนน สามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้เอง ตาม รูปแบบการตั้งค่าเริ่มต้นของแอปพลิเคชันในโทรศัพท์เครื่องนั้น ๆ ของผู้ลงคะแนน อีกทั้งยังมีการกำหนดให้ยืนยันตัวตนโดยการ กด PIN ซึ่งผู้ลงคะแนนเท่านั้นที่จะทราบ ก่อนลงคะแนนในวาระนั้น เพื่อป้องกันบุคคลอื่นในการแทรกแซงการลงคะแนนของผู้ ลงคะแนน โดยที่ผู้ดูแลระบบไม่สามารถเข้าถึงหน้าแอปพลิเคชันของผู้ลงคะแนนได้

[1] ความเป็นส่วนตัวของผู้ลงคะแนน ในที่นี้หมายถึง ความเป็นส่วนตัวที่เกิดขึ้นภายในระบบการลงคะแนนเท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน	
10. ความลับของคะแนนเสียง (Vote Secrecy) วัตถุประสงค์ (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน		
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	ระบบการลงคะแนนต้องไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มาประมวลผล จัดเก็บ หรือแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว	ผลการลงคะแนนจะนำเสนอในรูปแบบคะแนนรวม โดยแยกตามผลการลงคะแนน/ประเภทการลงคะแนน ดังนี้จำนวนผู้มีสิทธิ ลงคะแนนทั้งหมด จำนวนผลการลงคะแนนทั้งหมด จำนวนผลการลงคะแนนทั้งหมดที่แบ่งเป็น เห็นด้วย/ไม่เห็นด้วย/งดออก เสียง/เพิกเฉย และจำนวนผู้ไม่มาประชุม ซึ่งไม่มีการนำข้อมูลส่วนบุคคลของผู้ลงคะแนนมาแสดง ดังรูปภาพตัวอย่างที่แนบ  รูปที่ 1 แสดงคะแนนรวม โดยแยกตามผลการลงคะแนน/ประเภทการลงคะแนน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 รูปที่ 2 แสดง Dashboard ของผลการลงคะแนน
10.2 – ระบบการลงคะแนนไม่จัดทำข้อมูลเกี่ยวกับผู้ลงคะแนนหรือข้อมูลอื่น ๆ ที่สามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน นอกจากนี้ ผลลงคะแนนและผลรวมของการลงคะแนนต้องไม่มีข้อมูลที่ระบุตัวผู้ลงคะแนนและข้อมูลที่สามารถใช้หาลำดับของการส่งผลลงคะแนนได้ อย่างไรก็ตาม ในกรณีที่ให้ผู้ลงคะแนนส่งผลลงคะแนนก่อนจะตรวจสอบการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนน<u>สามารถใช้การเชื่อมโยงโดยอ้อม</u> (indirect voter association) ที่	ระบบการลงคะแนนใช้การเชื่อมโยงโดยอ้อม (indirect voter association) ที่เชื่อมโยงผู้ลงคะแนนกับผลลงคะแนนที่ถูก เข้ารหัสลับไว้โดยเมื่อผู้ลงคะแนนผ่านขั้นตอนการตรวจสอบว่ามีสิทธิลงคะแนนและยืนยันตนเข้าใช้งานแล้ว ระบบจะสร้าง object ID และ Hash ID (เลขบัตรประชาชนที่ผ่าน Hash Function) ใหม่ทุกครั้ง เพื่อใช้ในการลงคะแนนแทน อัตลักษณ์ของผู้ ลงคะแนนโดยตรง ทำให้ไม่สามารถเชื่อมโยงการลงคะแนนย้อนกลับไปยังอัตลักษณ์ของผู้ลงคะแนนโดยตรงได้

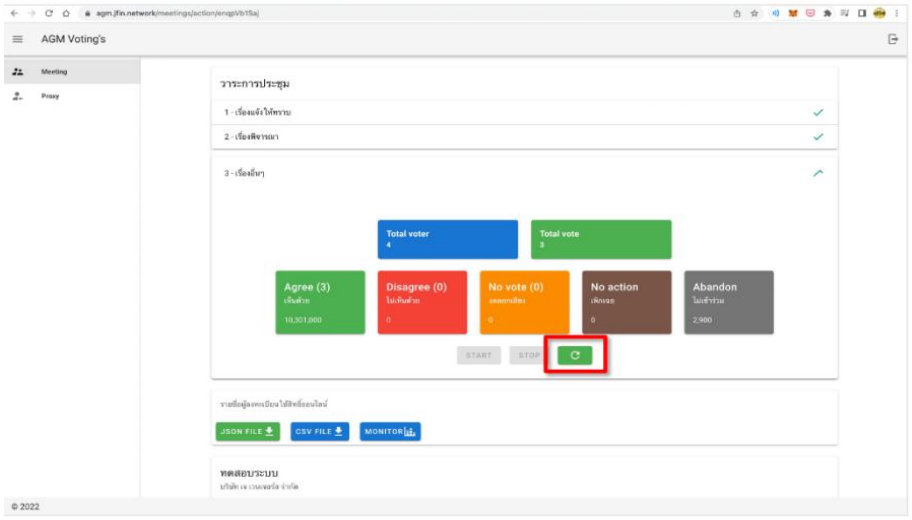
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	เชื่อมโยงผู้ลงคะแนนกับผลลงคะแนนที่ถูกเข้ารหัสลับไว้ โดยหลังจากตรวจสอบแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้น จึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับและนำไปนับคะแนนเป็นผลรวมของการลงคะแนน	
11. การควบคุมการเข้าถึง (Access Control) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น		
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน เพื่อให้มีหลักฐานสำหรับตรวจสอบในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งาน เปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และลบบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง	มีการเก็บ log ของทุก activities และ ทุก users รวมทั้งผู้ควบคุมโดยเก็บรายละเอียดใน session table (mongo db) ซึ่งมี ความสัมพันธ์(DB relationship) กันตามลำดับดังนี้Table User สำหรับเก็บสิทธิ์ของ user , Table session สำหรับเก็บ transaction log , Table AGMeeting สำหรับเก็บ หัวข้อการประชุม , Table AGMAgendars สำหรับเก็บวาระต่างๆในหัวข้อ การประชุม และ Table AGMeeingVotes สำหรับเก็บรายละเอียดของผู้ลงคะแนน บริษัทฯ ทำการกำหนดสิทธิ์ให้ Security Admin เป็นผู้เข้าระบบ log ของ database และมีการ hash ข้อมูลซึ่งถูกเก็บใน blockchain หากมีการแก้ไขเหตุการณ์ใด ๆ ระบบจะสามารถตรวจสอบย้อนกลับได้ตามเอกสารแนบ 13.1 ภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบ ตาม link ด้านล่าง 13.1 ขอภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบที่ใช้งานจริงแล้ว.pdf

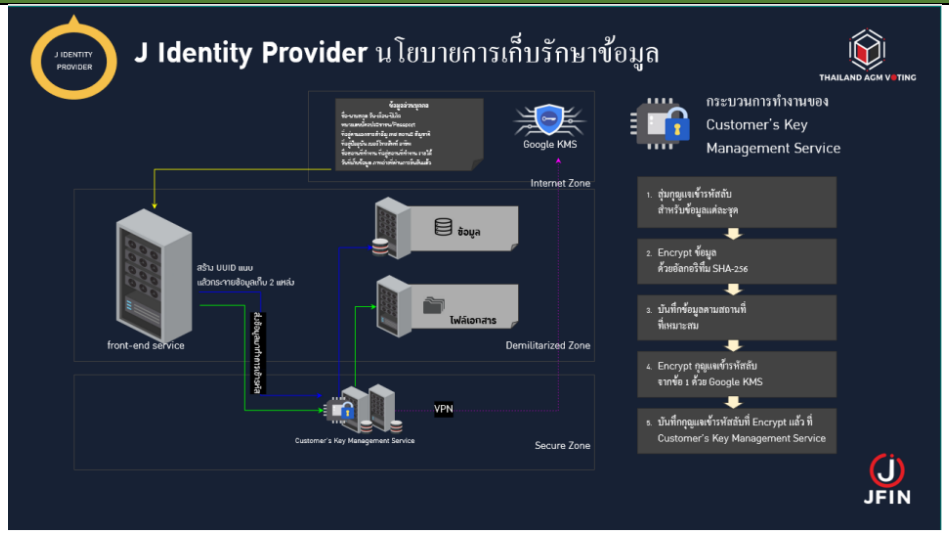
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนนและต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดบัญชีผู้ใช้งานที่ได้รับอนุญาต กำหนดบทบาทของผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละบทบาทของผู้ใช้งาน	ระบบการลงคะแนนกำหนดบทบาทหน้าที่ของผู้ใช้งาน ดังนี้ 1. Super user มีหน้าที่สร้าง user ผู้ควบคุมระบบ 2. ผู้ควบคุมระบบ มีหน้าที่สร้างผู้ใช้งานหรือผู้มีสิทธิลงคะแนน 3. ผู้ใช้งานหรือผู้มีสิทธิลงคะแนน มีสิทธิ์ลงคะแนนตามวาระที่ตัวเองมีสิทธิ์เท่านั้น โดยมีวิธีการสร้างและกำหนดสิทธิ์ตามเอกสารแนบ AGM Backoffice Manual.pdf ตาม link ด้านล่าง AGM Backoffice Manual.pdf ผู้ควบคุมระบบที่กำหนดสิทธินั้น เป็นได้ทั้งผู้ให้บริการและผู้ใช้บริการ ในกรณีที่ผู้ควบคมระบบเป็นผู้ถือหุ้น และมีสิทธิ์ออกเสียง ผู้ควบคุมระบบจะ upload รายชื่อและจำนวนคะแนนเข้าระบบ โดยมีตัวแทนการประชุมเช่น โฆษกในงานเป็นผู้ตรวจข้อมูลก่อนนำเข้าระบบ อีกทั้งยังมีการกำหนดสิทธิในส่วน Authorize Matrix ของการเข้าใช้งานระบบ มีกระบวนการบริหารจัดการของผู้ให้บริการเอง (Backoffice) เช่น มีการแยกหน้าที่ของทีม Security ทีม Network และทีม Operation เป็นต้น โดยมีตัวอย่าง ตามเอกสาร link ด้านล่าง 14.1 ตารางการกำหนดสิทธิ์รายบุคคล.pdf
11.3 – ระบบการลงคะแนนรองรับวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน	ระบบการลงคะแนนใช้วิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน เพื่อตรวจสอบว่าเป็นผู้ใช้งานที่ได้รับอนุญาตจริง และใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน เพื่อตรวจสอบว่าเป็นผู้ที่มีสิทธิเข้าถึงการดำเนินการที่สำคัญ (เช่น การเปิดลงคะแนน การปิดลงคะแนน) ทั้งนี้วิธีการพิสูจน์และยืนยันตัวตนอาจพิจารณาข้อกำหนดตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) จาก	การพิสูจน์และยืนยันตัวตนของระบบการลงคะแนนของผู้ควบคุมการลงคะแนนและผู้ลงคะแนน รวมทั้งผู้ใช้งานของระบบ AGM Voting มีรายละเอียด ดังนี้ การพิสูจน์ตัวตนของระบบการลงคะแนน จะต้องทำการพิสูจน์ตัวตนทั้งผู้ควบคุมระบบและผู้ลงคะแนน เป็นไปตามระดับความ น่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level) IAL2.3 ประกอบด้วย การดึงข้อมูลจากบัตรประจำตัวประชาชน ซึ่ง ผู้ใช้บริการต้องไปทำการ Dip Chip ด้วยตนเอง ณ จุดบริการสาขา Jaymart พร้อมกับตรวจสอบสถานะข้อมูลจากบัตรกับ กรมการปกครอง และมีการใช้เทคโนโลยีชีวมิติในการเทียบเพื่อตรวจสอบใบหน้า ซึ่งขั้นตอนนี้ผู้ลงคะแนนจะมีบัญชีผู้ใช้งานอยู่ที่ Application JOIN การยืนยันตัวตนของระบบลงคะแนน จะเป็นไปตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level) AAL2 ประกอบด้วย 2 ปัจจัย (Two Factors Authentication) ได้แก่ ใส่รหัส PIN (Something you know) และ OTP (Something you have) ซึ่งมีการกำหนดอายุของการกรอก OTP ไว้ด้วย ขั้นตอนการยืนยันตัวตนนี้ ผู้ลงคะแนนต้องยืนยันผ่าน Application JOIN ซึ่งจะ re-direct link มาจาก Application AGM voting เมื่อผู้ลงคะแนนยืนยันตัวตนผ่านเป็นที่เรียบร้อย แล้ว จึงจะสามารถเข้าประชุมผ่าน Application AGM voting ได้ ผู้ใช้บริการสามารถ download application “JOIN” และ “AGM Voting” จาก App Store หรือ Play Store เพื่อใช้ใน การยืนยันตัวตนแบบหลายปัจจัย ก่อนทำการลงคะแนน ระบบการลงคะแนนมีการเก็บรักษาข้อมูลการยืนยันตัวตน โดยมีการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล โดยใช้ Symmetric Key เพื่อเข้ารหัสลับ ซึ่งจะมีความยาว 256 bit ขึ้นไป และใช้ SHA Algorithm (SHA256) ในการเข้ารหัสลับ และมีการ Hash Voter Address ส่งเข้า blockchain ดังตัวอย่างตาม Link : https://jfinscan.com/txs

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	มาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ระบบการลงคะแนนต้องเก็บรักษาข้อมูลยืนยันตัวตน (เช่น รหัสผ่าน) โดยมีการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล และหากระบบการลงคะแนนใช้วิธีการยืนยันตัวตนด้วยรหัสผ่าน ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดความเข้มงวดและการหมดอายุของรหัสผ่าน	
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลดสิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่ (separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น	การกำหนดสิทธิการเข้าถึงตามควาจำเป็น (least privilege) โดยมีระดับ 1. Super user มีหน้าที่สร้าง Administrator โดยมีการวิธีสร้างตามเอกสารแนบคู่มือ หน้า 3 AGM Backoffice Manual.pdf Link : AGM Backoffice Manual.pdf 2. Administrator หรือ ผู้ควบคุมระบบ มีหน้าที่ในกำหนดสิทธิ์ในการจัดประชุมต่างๆ 3. End User หรือ ผู้ลงคะแนน มีหน้าที่ลงคะแนนในวาระต่างๆ โดยสิทธิระดับ Super user เท่านั้นที่สามารถสร้าง user ผู้ควบคุมระบบได้ ข้อกำหนด คำอธิบาย ความสามารถของระบบการลงคะแนน ทั้งนี้ บริษัทฯ มีการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ของพนักงานและความรับผิดชอบของตำแหน่งงาน โดย มีการแบ่งเป็นทีม เช่น ทีม security, ทีม Network, ทีม Operation ตามเอกสารแนบ 14.1 ตารางการกำหนดสิทธิ์รายบุคคล.pdf 14.1 ตารางการกำหนดสิทธิ์รายบุคคล.pdf
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งาน	1. ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณี ผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตน ซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด 2. กรณีผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด 2 ครั้ง ระบบการลงคะแนนจะ lockout และ ผู้ใช้งานต้องทำ การ log in เข้าระบบใหม่ 3. ระยะเวลาระงับการใช้งาน (lockout duration) ประมาณ 1 นาที

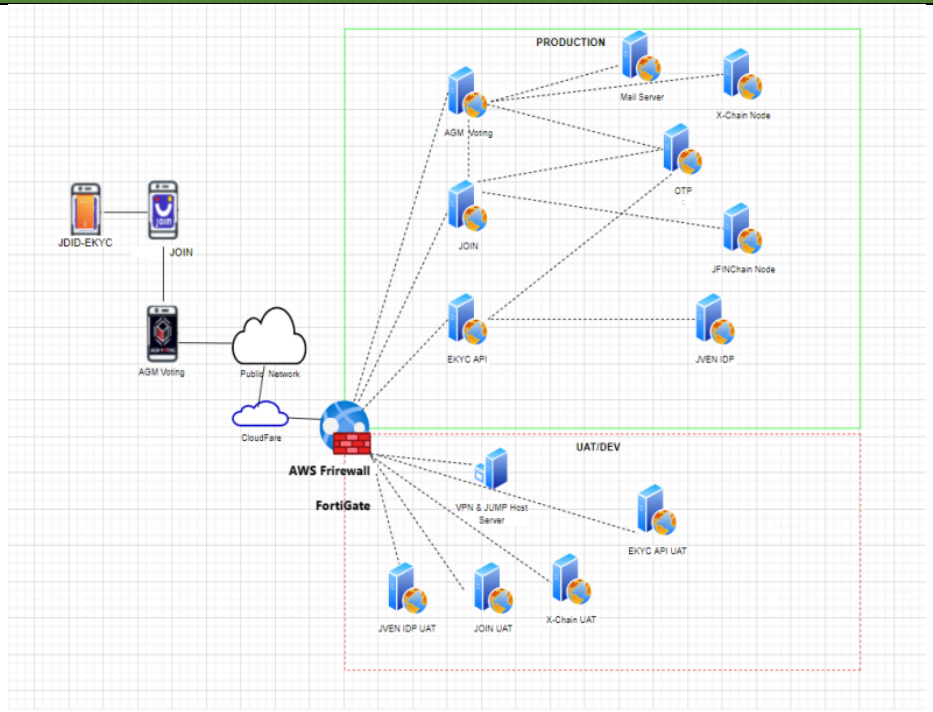
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด หากผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนควรระงับการใช้งาน (account lockout) ของผู้ใช้งานเป็นระยะเวลาหนึ่งก่อนจะให้ยืนยันตัวตนครั้งต่อไป และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล	
12. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย		
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐาน หรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาตหรือการถูกตัดการเชื่อมต่อทางกายภาพเกิดขึ้นกับส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน ผู้พัฒนาระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อคที่มั่นคงปลอดภัย	ระบบการลงคะแนน วางอยู่บน AWS Cloud Service ที่มีมาตรฐานดังนี้; มาตรฐานความปลอดภัยและการปฏิบัติตามกฎหมาย ISO/IEC 27001: ระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล (ISMS) ISO/IEC 27017: แนวปฏิบัติความปลอดภัยสำหรับบริการคลาวด์ ISO/IEC 27018: การคุ้มครองข้อมูลส่วนบุคคลในคลาวด์ SOC 1, SOC 2, SOC 3: การควบคุมความปลอดภัยและกระบวนการในการให้บริการ PCI DSS: มาตรฐานมาตรฐานความต่อเนื่องทางธุรกิจและการบริหารความเสี่ยง ISO 22301: มาตรฐานระบบบริหารความต่อเนื่องทางธุรกิจ ISO 31000: การบริหารจัดการความเสี่ยงความปลอดภัยข้อมูลสำหรับอุตสาหกรรมบัตรเครดิต CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry): มาตรฐานความปลอดภัยของบริการคลาวด์ C5 (Cloud Computing Compliance Controls Catalogue): มาตรฐานความปลอดภัยสำหรับเยอรมนี MTCS (Multi-Tier Cloud Security): มาตรฐานสำหรับบริการคลาวด์ในสิงคโปร์

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	หรือระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ	
13. การคุ้มครองข้อมูล (Data Protection) วัตถุประสงค์ เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต		
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนน จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนนและระบบเครือข่าย รวมถึงระบบการลงคะแนนต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง	ระบบการลงคะแนนอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนน ซึ่งหมายถึงผู้ให้บริการเท่านั้น โดยควบคุมระบบจะต้องยืนยันตัวตนแล้วเท่านั้น จึงสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนน (Administrator) และ vote records ถูกเก็บบน Blockchain ทำให้เกิดความครบถ้วนของการลงคะแนนที่มาสามารถทำการ. แก้ไขได้ตัวอย่าง Log Table ของผู้จัดประชุม (ผู้ควบคุมระบบ) โดยมีจำนวน 5 Table ได้แก่ 1. Table user objid เมื่อผู้ควบคุมระบบทำการ log in ใน AGM ด้วย mobile ระบบจะทำการแปลงค่าเป็น objid ใน usertable เป็นตัวแปรค่าหนึ่ง 2. Table Session objid เมื่อผู้ควบคุมระบบทำการ log in ใน AGM ผ่านด้วย mobile ผ่านระบบจะทำการสร้าง log ใน Session table โดยมี user เป็นตัวแปรอีกค่าหนึ่ง ซึ่งเป็น linkage 3. Table AGMMeetings objid จะถูกกำหนดเป็นตัวแปรค่าหนึ่งที่ระบุด้วย created by โดยจะถูกกำหนดเป็นตัวแปร เมื่อผู้ควบคุมระบบทำการเพิ่ม หัวข้อการประชุมใน AGM ระบบจะทำการสร้าง Meeting ID โดยมี user เป็น linkage 4. เมื่อผู้ควบคุมระบบเพิ่ม agenda ใน AGM ระบบจะทำการสร้าง Contractaddress ในตาราง Table AGMAgendars โดยมี meetingId เป็น linkage 5. เมื่อผู้ลงคะแนนใน AGM ระบบจะทำการสร้าง hashId ในตาราง Table AGMMeetingVoter โดยมีmeetingId เป็น linkage ตามเอกสารแนบ 13.1 ภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบ ภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบ ตาม link ด้านล่าง 13.1 ขอภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบที่ใช้งานจริงแล้ว.pdf
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับมาจากผู้ลงคะแนน บันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที และจัดเก็บบันทึกการลงคะแนนให้อยู่ในรูปแบบที่สามารถแสดงผลลงคะแนนที่ได้รับมาให้ปรากฏอย่างถูกต้องได้	ผู้จัดการประชุม เป็นผู้ที่นำข้อมูลผู้ที่มีสิทธิลงคะแนนเข้าระบบ และสามารถตรวจสอบข้อมูลที่มีการบันทึกการลงคะแนนได้ โดยมีการแสดงผลผ่าน Dashboard ของผู้ดูแลระบบ ซึ่งจะสามารถตรวจความครบถ้วนของผลการลงคะแนนที่ได้รับจากผู้ ลงคะแนนได้ ดังรูป กรณีที่ระบบมีข้อผิดผลาดแล้วทำให้ user ลงคะแนนไม่ได้ ระบบจะถือว่า user ทำการ “no action” แล้วจะนำคะแนนไป รวมกับ คะแนน “เห็นด้วย” ในการรวมคะแนนวาระ นั้นๆ ซึ่งถูกกำหนดไว้โดยระบบไม่ได้ขึ้นกับเกณฑ์การประชุมของผู้จัด ประชุม (มีการประกาศเตือน โดย โฆษก ก่อนเริ่มการประชุมทุกครั้ง)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 รูป การบันทึกการลงคะแนนโดยมีการแสดงผลผ่าน Dashboard
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	ระบบจะใช้การเข้ารหัส Google KMS ซึ่งเป็น Symmetric Key เพื่อเข้ารหัสลับ โดยจะมีความยาว 256 bit ขึ้นไปและใช้ SHA Algorithm (SHA-256) ในการเข้ารหัสลับ โดยการออกแบบจะใช้วิธีสร้างกุญแจแต่ละบุคคลไม่ซ้ำกัน เพื่อใช้เป็นกุญแจ เข้ารหัสลับชั้นแรก แล้วจึงนำข้อมูลที่เข้ารหัสลับแล้วไปบันทึกไว้ จากนั้นนำกุญแจดังกล่าวมาเข้ารหัสลับด้วยกุญแจดอกที่สอง (กุญแจดอกที่สอง จะใช้ดอกเดียวกันกันทั้งระบบ) ที่เก็บไว้ใน Google Cloud KMS แล้วจึงนำกุญแจที่เข้ารหัสลับแล้ว มาบันทึก ไว้ที่ฐานข้อมูลของ Customer Key Management Service การออกแบบเช่นนี้จะสามารถแก้ปัญหาเรื่องการเปลี่ยนผู้ให้ บริการ Cloud KMS ในอนาคตได้ โดยไม่จำเป็นต้องแตะต้องข้อมูลบุคคลเลย Customer Key Management Service จะเป็น ส่วนที่สำคัญที่สุดและไม่สามารถเชื่อมกับอินเทอร์เน็ตได้โดยตรง โดยจะมีการกำหนด Access Control เพื่ออนุญาตให้เข้าใช้งาน ผ่าน Server ที่อนุญาตเท่านั้น และใช้ฐานข้อมูลแยกจากข้อมูลอื่นๆ ในระบบ ตามรูป

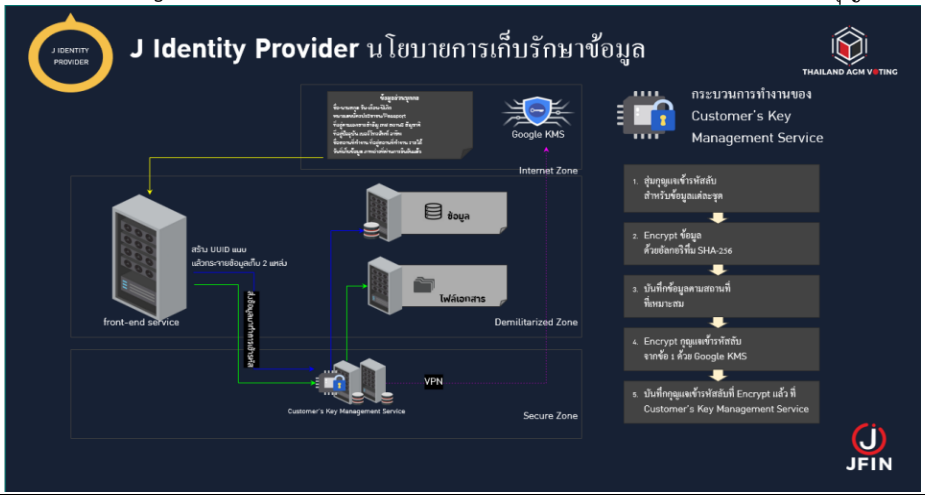
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 ภาพถ่ายที่ผ่านการยืนยันแล้ว จะถูกจัดเก็บไว้ที่ระบบ JOIN ซึ่งระบบลงคะแนนจะไม่ได้จัดเก็บข้อมูลชีวมิติ
13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด	การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายคอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)	บริษัทมีการวางสถาปัตยกรรมระบบเครือข่ายซึ่งมีช่องทางในการเชื่อมต่อที่ปลอดภัย (mutually-authenticated secure channel) ต่างๆ ดังนี้ 1. ผู้ลงคะแนนเข้าใช้งานระบบบนมือถือ (mobile) ผ่าน public internet 2. Cloudflare มีการใช้งาน load balance และ anti ddos อีกทั้งยังซ่อน IP ปลายทาง มีอุปกรณ์ dns server สำหรับถอด ค่า DNS name เป็น public IP ของ J Ventures แล้วทำการส่ง package ไปให้ปลายทางตามที่ระบุ 3. AWS Firewall – FortiGate มีหน้าที่ทำการตรวจสอบ incoming IP เพื่ออนุญาต หรือไม่อนุญาต IP ตาม policy ที่ตั้งไว้ โดยจะทำการ scan VIRUS ทุกครั้ง ทั้งนี้บริษัทฯ ยังการแบ่งโซนการทดสอบระหว่างขั้นตอน Production กับขั้นตอนการทำ UAT บริษัทมีการจัดทำ Security configuration baseline ซึ่งเป็นแนวทางการตั้งค่านโยบายความมั่นคงปลอดภัยโดยการจำกัด การเข้าถึง (least privilege) ซึ่งประกอบไปด้วยการไม่ให้สิทธิเกินหน้าที่และความจำเป็น การตรวจสอบความปลอดภัยใน การเข้าถึงระบบของผู้ดูแลระบบ ซึ่งรวมถึง การติดตั้งการใช้งาน การกำหนดค่าในการบริหารทรัพยากร การกำหนดกลุ่มของ ผู้ใช้งาน และการใช้งานนโยบายการรักษาความมั่นคงปลอดภัย การดูแลระบบ Security Verify Access เกี่ยวข้องกับงานระดับสูงดังต่อไปนี้การติดตั้งและกำหนดค่าในการบริหาร ทรัพยากร การกำหนดคุณลักษณะผู้ใช้งานที่สามารถเข้าถึงได้ ประเภทของการเข้าใช้งาน ระยะเวลาที่สามารถเข้าใช้งานได้ เงื่อนไขที่ต้องปฏิบัติตาม การควบคุมการเข้าถึงของผู้ใช้งานเฉพาะกลุ่ม Access Control List (ACL) การกำหนดกฎในการ เข้าถึงของผู้ใช้งาน การอนุญาตให้เข้าถึงข้อมูล รายละเอียดตามรูป

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน

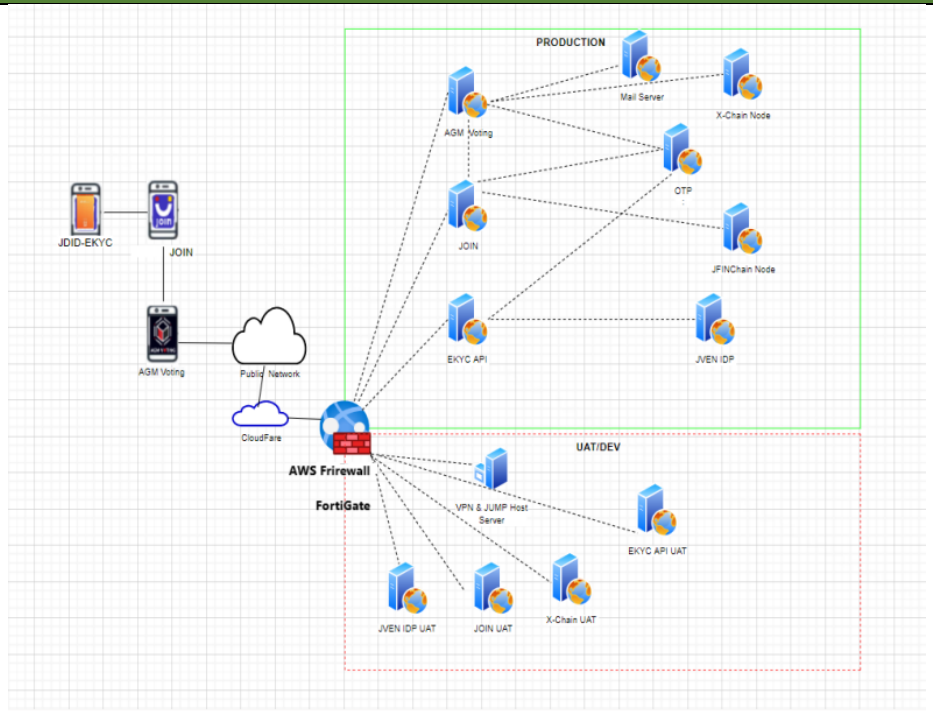


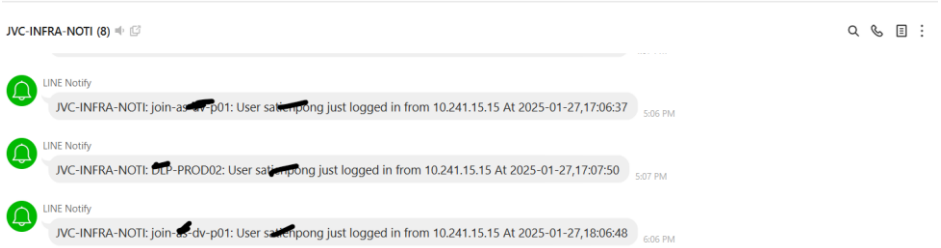
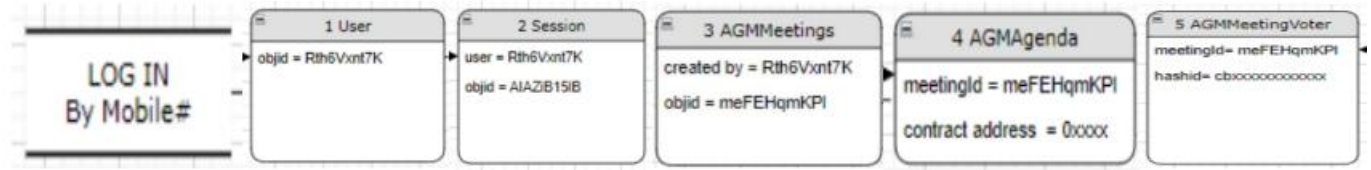
รูป ตัวอย่าง Jventures Network Diagram

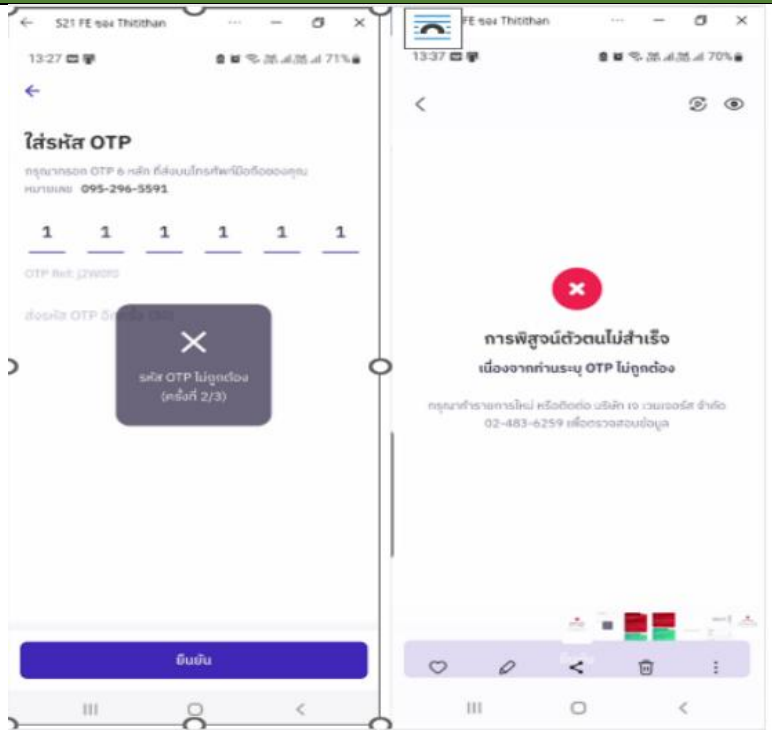
ในส่วนของ Data in transit ระบบจะใช้ การเข้ารหัส Google KMS ซึ่งเป็น Symmetric Key เพื่อเข้ารหัสลับ โดยจะมีความ ยาว 256 bit ขึ้นไป และใช้ SHA Algorithm (SHA-256) ในการเข้ารหัสลับ โดยการออกแบบจะใช้วิธีสร้างกุญแจแต่ละบุคคล ไม่ซ้ำกัน รายละเอียดตามรูป



ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
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)	1. ระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) ตามมาตรฐาน ISO27001:2022 ซึ่งมี Scope of certification คือ THE OPERATION OF INFORMATION SECURITY MANAGEMENT SYSTEM FOR IT PLATFORM SERVICE, SOFTWARE AS A SERVICE AND DIGITAL ID SERVICE STATEMENT OF APPLICABILITY: REVISION 0, 01 SEPTEMBER 20 ซึ่งครอบคลุมระบบ AGM Voting ซึ่งเป็น software as a service 2. โดยมีขอบเขตการประเมินความเสี่ยงด้านความปลอดภัยสารสนเทศ ประกอบด้วย การกำหนดประเภทของความเสี่ยง การ จัดลำดับความสำคัญ ความรุนแรง ที่จะมีผลกระทบต่อทรัพยากรและการให้บริการของระบบสารสนเทศ พร้อมทั้งนำข้อมูลดังกล่าวมาบริหารจัดการเพื่อลดความเสี่ยงด้านความมั่นคงของระบบสารสนเทศ พร้อมทั้งดำเนินการเฝ้าระวัง และประเมินผล การจัดการความเสี่ยงด้านสารสนเทศเป็นระยะอย่างต่อเนื่อง ตลอดจนการปรับปรุงกระบวนการบริหารจัดการด้านความเสี่ยง สารสนเทศให้มีประสิทธิภาพมากยิ่งขึ้น ระบบมีการออกแบบสถาปัตยกรรมเครือข่าย โดยวิธีการควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อป้องกัน บรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน อีกทั้ง บริษัทฯ ได้มีการจัดทำ Security Configuration baseline ดังนี้ 2.1 user login mobile ผ่าน public internet 2.2 Cloudflare 2.2.1 ทำหน้าที่ load balance, และ anti ddos และ ซ่อน ip ปลายทาง 2.2.2 ทำหน้าที่ dns server จะทำการถอดค่า dns name เป็น public IP ของ J Ventures แล้วทำการส่ง package ไปให้ปลายทางตามที่ระบุ 2.2.3. AWS Firewall และ FortiGate ทำการตรวจสอบ incoming IP เพื่อ allow or not allow ตาม policy ที่ตั้งไว้ โดย จะทำการ scan VIRUS ทุกครั้ง โดย J Ventures ทำการแบ่ง zone Production กับ UAT ดังรูป

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 รูป ตัวอย่าง Jventures Network Diagram
14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น	ระบบการลงคะแนนป้องกันการติดตั้งหรือการสั่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง และปิดใช้งานการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน ซอฟต์แวร์ของระบบการลงคะแนนต้องไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และต้องเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น	บริษัทฯ ทำการสร้างความปลอดภัยให้แก่ระบบแบบหลายระดับ ไม่ว่าจะเป็น Network Zoning, DMZ, Network Gateway รวมไปถึง Firewall on Host และ Applicationผ่าน FortiGate Firewall (NGFW รวม anti-virus and malware) นอกจากนั้น ยังมีการ pen test, VA scan รวมทั้ง external IT Audit ทำการตรวจสอบทุกปี (EY) นอกจากนั้นยังใช้วิธีการ peer-to-peer สำหรับ review source code โดยมี Supervisor สุ่มตรวจสอบเป็นบางครั้ง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
15. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring) วัตถุประสงค์ เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน		
15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ	ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งประกอบด้วยเหตุการณ์ที่เกี่ยวข้องกับสถานะการทำงานและความผิดปกติของระบบ การยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน การจัดการระบบเครือข่าย การจัดการซอฟต์แวร์ และฟังก์ชันการลงคะแนน เป็นอย่างน้อย	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) บริษัทได้ กำหนดกระบวนการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศ มีการควบคุมการรักษาความปลอดภัย อย่าง รัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล ISO27001:2022 ตามนโยบายการรักษาความมั่นคงปลอดภัยของ ระบบเทคโนโลยีสารสนเทศและไซเบอร์(ISMS-02 Information Security_Cyber Policy) ระบบการลงคะแนนสามารถบันทึกเหตุการณ์(event logging) ที่เกิดขึ้นในระบบการลงคะแนนได้ดังนี้ 1) สถานะการทำงานปกติและความผิดปกติของระบบปฏิบัติการ ระบบเครือข่าย ระบบฐานข้อมูล และระบบการลงคะแนนอ ซึ่ง บริษัทฯ ใช้ระบบ AWS Cloud Watch monitoring system เฝ้าสังเกตปัญหาที่เกิดขึ้นจากระบบ และส่งแจ้งเตือนผ่าน Line application  2) ระบบมีการบันทึก Log การยืนยันตัวตนในการเข้าใช้งานระบบ และการเข้าถึงระบบของผู้ใช้งาน ใน Parse ตัวอย่างดังรูป  3) การจัดการระบบเครือข่าย สามารถเปิด และ ปิดการเชื่อมต่อระบบบน FortiGate Firewall (ถ้าจำเป็น) 4) การจัดการซอฟต์แวร์ user สามารถ download application ผ่าน app store และ play store และตั้งค่าตามมาตรฐาน ทั่วไปของระบบ 5) ผู้ดูแลระบบสามารถเปิดและปิดการลงคะแนนได้ผ่าน AGM Back office โดยผลของการลงคะแนนสามารถนำออก (export Logs) เป็น json และ csv file format
15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ใช้งานในทันที บันทึกข้อผิดพลาดทั้งหมดที่เกิดขึ้น และสร้างรายงานข้อผิดพลาด (error report) รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับ	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน จะมีการแจ้งข้อผิดพลาดที่หน้าจอของผู้ใช้งานทันที โดยมีตัวอย่างการแสดง ข้อความ Error ผ่าน Popup ดังรูปที่ 1 และจะรวบรวมข้อมูลจัดทำเป็นรายงานข้อผิดพลาด

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	การจัดการข้อผิดพลาดในระบบการลงคะแนน	 รูปที่ 1 ตัวอย่างการแสดงข้อความ Error ผ่าน Popup ปัจจุบันผู้ดูแลระบบจะประจำ on site ตามการประชุม VOTING ทุกครั้ง ทำให้รับทราบปัญหาและทำการแก้ไขหน้างาน ส่วน ส่วนรายงานข้อผิดพลาด จะจัดทำเป็นรายงาน error report
15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	ระบบการลงคะแนนต้องมีมาตรการป้องกันมัลแวร์ (malware) โดยระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ บันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ และบันทึกเหตุการณ์ของกิจกรรมการแก้ไขมัลแวร์ รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการอัปเดตมาตรการป้องกันมัลแวร์	ระบบการลงคะแนนมีการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware) อ้างอิง ISO27001-2022 หมายเลขเอกสาร ISMS-02 นโยบายการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและไซเบอร์ ดังนี้ 1. ผู้ดูแลระบบ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ 2. ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น thumb drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ 3. ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน 4. ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบ คอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลายถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ มีระบบ FortiGate Firewall เป็น Next-Generation Firewall security for full visibility and threat protection any times สำหรับป้องกัน malware ระบบบันทึกเหตุการณ์ที่ตรวจพบบน servers และเมื่อระบบตรวจพบไฟล์ที่มีไวรัส ระบบจะทำ การบล็อคไวรัสดังกล่าวทันทีซึ่งตัวอย่าง Virus ที่ดักจับได้เช่น PHP/Agent.RZ!tr ระบบมีการป้องกันโดยใช้ C – Best Practices Version 7.4.3 ซึ่งประกอบไปด้วย โปรแกรมป้องกันไวรัส โดยสามารถเปิดใช้งานเพื่อสแกนไวรัสสำหรับเครือข่ายที่ใช้งานทั้งหมด โดยใช้ FortiClient endpoint antivirus สแกนเพื่อป้องกันภัยคุกคามที่เข้ามาในเครือข่าย ซึ่งสมาชิก FortiGuard AntiVirus ต้องอัปเดตและกำหนดค่า FortiGate ของระบบซึ่งจะทำให้ได้รับการอัปเดตลายเซ็นของโปรแกรม

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ป้องกันไวรัสทันทีที่พร้อมใช้งาน สามารถเปิดการใช้งาน เฉพาะโปรโตคอลที่ต้องการตรวจสอบได้ ระบบสามารถทำการตรวจสอบและรายงานการป้องกันไวรัส รวมถึงข้อความบันทึกเป็น ระยะๆ ระบบป้องกันการบุกรุก (IPS) สามารถตรวจพบทราฟฟิกที่พยายามใช้ช่องโหว่นี้ อีกทั้ง IPS ยังอาจตรวจพบตอนที่ระบบติด ไวรัส โดยการเปิดใช้งานการสแกน IPS ที่เครือข่ายทั้งหมด โดยใช้ FortiClient endpoint IPS สแกนเพื่อป้องกันภัยคุกคามที่เข้า มาในเครือข่ายของ ซึ่งสมาชิก FortiGuard IPS Updates ต้องอัปเดตและกำหนดค่า FortiGate ของระบบซึ่งจะทำให้ได้รับ การอัปเดตลายเซ็นของโปรแกรมป้องกันไวรัสทันทีที่พร้อมใช้งาน ซึ่งเป็นสิ่งสำคัญในการป้องกันการโจมตีบริการที่เผยแพร่สู่ สาธารณะ
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. ผู้ลงคะแนนเข้าใช้งานระบบบนมือถือ (mobile) ผ่าน public internet 2. Cloudflare มีการใช้งาน load balance และ anti ddos อีกทั้งยังซ่อน IP ปลายทาง มีอุปกรณ์ dns server สำหรับถอดค่า DNS name เป็น public IP ของ J Ventures แล้วทำการส่ง package ไปให้ปลายทางตามที่ระบุ 3. AWS Firewall และ FortiGate มีหน้าที่ทำการตรวจสอบ incoming IP เพื่ออนุญาต หรือไม่อนุญาต IP ตาม policy ที่ตั้งไว้ โดย จะทำการ scan VIRUS ทุกครั้ง บริษัทมีการจัดทำ Security configuration baseline ซึ่งเป็นแนวทางการตั้งค่านโยบายความมั่นคงปลอดภัยโดยการจำกัดการเข้าถึง (least privilege) ซึ่งประกอบไปด้วยการไม่ให้สิทธิเกินหน้าที่และความจำเป็น การตรวจสอบความปลอดภัยในการเข้าถึง ระบบของผู้ดูแลระบบ ซึ่งรวมถึง การติดตั้งการใช้งาน การกำหนดค่าในการบริหารทรัพยากร การกำหนดกลุ่มของผู้ใช้งาน และ การใช้งานนโยบายการรักษาความมั่นคงปลอดภัย การดูแลระบบ Security Verify Access เกี่ยวข้องกับงานระดับสูงดังต่อไปนี้ การติดตั้งและกำหนดค่าในการบริหารทรัพยากร การกำหนดคุณลักษณะผู้ใช้งานที่สามารถเข้าถึงได้ ประเภทของการเข้าใช้งาน ระยะเวลาที่สามารถเข้าใช้งานได้ เงื่อนไขที่ต้อง ปฏิบัติตาม การควบคุมการเข้าถึงของผู้ใช้งานเฉพาะกลุ่ม Access Control List (ACL) การกำหนดกฎในการเข้าถึงของผู้ใช้งาน การอนุญาตให้เข้าถึงข้อมูล การตั้งค่า Security Configuration นี้อ้างอิงตามเอกสาร IS027001-2022 หมายเลขเอกสาร ISMS-02 นโยบายการรักษา ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและไซเบอร์และเอกสาร Fortinet FortiOS - Best Practices version 7.4.3 ในการ setup Firewall