

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

ชื่อระบบ	AGM Voting		
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท)	บจก.เจเวนเจอร์ส		
ช่องทางการติดต่อผู้ให้บริการ	thitithan@jventures.co.th หรือ โทร 095-296-5591		
วันที่ประเมินความสอดคล้อง	21 มีนาคม 2566		
วันที่ครบกำหนดการทบทวน	20 มีนาคม 2567		
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 และวาระการประชุมที่ใช้เทคโนโลยี Blockchain โดยมีระบบสนับสนุนในการพิสูจน์ตัวตน (eKYC) JDID Application ใช้สำหรับผู้มีสิทธิลงคะแนน เพื่อพิสูจน์ตัวตน และมีระบบการยืนยันตัวตน JOIN Application ใช้สำหรับผู้มีสิทธิลงคะแนน เพื่อยืนยันตัวตนแบบ Multi Factor Authentication		

หมายเหตุ : สฟธอ ไม่เกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน		
1. การออกแบบระบบ (System Design)		
วัตถุประสงค์	เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามกระบวนการการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ	
1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด	ระบบการลงคะแนนมีฟังก์ชันการทำงานที่จำเป็นตามกระบวนการลงคะแนนที่ กฎหมายหรือหลักเกณฑ์กำหนด ซึ่งครอบคลุมการเตรียมข้อมูลสำหรับการลงคะแนน การตรวจสอบระบบการลงคะแนนก่อนการลงคะแนน การเปิดลงคะแนน การลงคะแนน การส่งผลลงคะแนน การปิดลงคะแนน การนับคะแนน และการรายงานผลรวมของการลงคะแนน	กระบวนการลงคะแนนทั้งหมดจะควบคุมโดยผู้จัดการประชุม เพื่อให้เป็นไปตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง เช่น ในการประชุมสามัญประจำปีผู้ถือหุ้น จะเป็นไปตามพระราชบัญญัติบริษัทมหาชนจำกัด พ.ศ. 2535 และแนวทางการกำกับดูแลกิจการที่ดี ของตลาดหลักทรัพย์แห่งประเทศไทย ส่วนในการประชุมใหญ่เจ้าของร่วม และการประชุมผู้ถือหุ้นบริษัทตามประมวลกฎหมายแพ่งและพาณิชย์ ฉบับที่ 18 พ.ศ. 2551 การประชุมใหญ่ ในส่วนของการประชุมของอาคารชุดก็จะเป็นไปตามพระราชบัญญัติอาคารชุด (ฉบับที่ 4) พ.ศ.2551 ซึ่งทั้งหมดจะต้องเป็นไปตามพระราชกำหนด ว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 โดยขั้นตอนต่างๆจะเป็นไปดังนี้ 1. การเตรียมข้อมูลสำหรับการลงคะแนน ผู้จัดการประชุมจะเป็นผู้จัดเตรียมข้อมูล

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		2. การตรวจสอบระบบการลงคะแนนก่อนการลงคะแนน ก่อนการประชุมทุกครั้งจะมีการทดสอบระบบลงคะแนนร่วมกับผู้จัดการประชุม 3. การเปิดลงคะแนน ผู้ควบคุมระบบจะเปิดลงคะแนนเมื่อผู้จัดการประชุมประกาศเปิดลงคะแนนในการประชุม 4. การลงคะแนน ผู้เข้าร่วมประชุมออนไลน์จะลงคะแนนพร้อมๆ กันในการประชุม 5. การส่งผลลงคะแนน ระบบจะส่งคะแนนเข้าไปยังฐานข้อมูลของผู้จัดการประชุม ซึ่งจะมีแยกระหว่างคะแนนจากผู้มาร่วมประชุมด้วยตนเอง คะแนนจากผู้ที่มีบัตรผ่าน และคะแนนออนไลน์ 6. การปิดลงคะแนน ผู้ควบคุมระบบจะปิดลงคะแนนเมื่อผู้จัดการประชุมประกาศปิดลงคะแนนในการประชุม 7. การนับคะแนน การนับคะแนนแต่ละวาระจะเป็นไปตามหลักเกณฑ์ของการประชุม เนื่องจากแต่ละวาระจะมีเกณฑ์การนับคะแนนแตกต่างกันโดยเฉพาะคะแนนจากผู้ที่ยกข้อสงสัยลงคะแนน ซึ่งผู้จัดการประชุมจะเป็นผู้เตรียมการนับคะแนนให้ตรงตามหลักเกณฑ์ 8. การรายงานผลรวมของการลงคะแนน ระบบจะส่งคะแนนเข้าไปยังฐานข้อมูลของผู้จัดการประชุม โดยผู้จัดการประชุมจะเป็นผู้รายงานผลการลงคะแนน ทั้งรายงานแยกระหว่างคะแนนจากผู้มาร่วมประชุมด้วยตนเอง คะแนนจากผู้ที่มีบัตรผ่าน และคะแนนออนไลน์ และรายงานผลรวมคะแนนทั้งหมด
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ (system accuracy and reliability) การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) ในสภาวะที่ใกล้เคียงกับการใช้งานจริง ในกระบวนการลงคะแนน และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)	มีการทดสอบขีดความสามารถของระบบในกระบวนการบันทึกค่าแฮช (Hash) ของผู้ลงคะแนนและผลการลงคะแนน พบว่าระบบสามารถรองรับปริมาณธุรกรรมสูงสุด (maximum volume) 371 รายการ/วินาที นอกจากนี้ บริษัทฯ ได้มีการทำ Penetration Testing ของระบบ AGM Voting บนระบบปฏิบัติการ iOS และ Android โดยใช้วิธีการทางเทคนิคแบบ Grey-Box ซึ่งไม่พบช่องโหว่ที่มีนัยสำคัญ
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบซอฟต์แวร์ (software tester) ของผู้พัฒนาระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนได้จัดทำรายงานผลการทดสอบระบบ (test report) ซึ่งได้กำหนด test case ไว้ 14 กรณีครอบคลุมขั้นตอนการใช้งานของระบบของผู้ลงคะแนนและผู้จัดประชุม (ผู้ควบคุมการลงคะแนน) พบว่า ผลการทดสอบเป็นไปตามความคาดหวังของผลลัพธ์ที่กำหนด (Expected Result) ตามเอกสารแนบ AGM Test Result.pdf

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 AGM Test Result.pdf
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)	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 สำหรับระบบสมาชิกและระบบจัดเก็บข้อมูลซึ่งมีฐานข้อมูลเป็น MongoDB อีกทั้งยังใช้วิธีการออกแบบและพัฒนาซอร์สโค้ดแอปพลิเคชันตามมาตรฐาน SDLC – Hybride 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

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ระบบการลงคะแนน (AGM Voting Application) ใช้บริการอื่น ๆ เพื่อเพิ่มประสิทธิภาพการทำงานของระบบ AGM Voting ดังนี้ ● NDID: ใช้สำหรับการพัฒนา Digital ID Platform เพื่อเป็นช่องทางในการพิสูจน์และยืนยันตัวตนของผู้ลงคะแนนแบบไม่พบหน้ากัน อย่างปลอดภัย ● xCHAIN Network: เป็น Blockchain Infrastructure ที่ร่วมก่อตั้งและพัฒนาระหว่างพันธมิตรที่มีความเชี่ยวชาญด้านเทคโนโลยี และองค์กรชั้นนำของประเทศให้เป็น Public Blockchain Infrastructure ในประเทศไทยและเป็นระบบนิเวศแรก (First Ecosystem) ที่ถูกสร้างขึ้นและ นำมาใช้งานจริงที่มี Validator Node เป็นองค์กรที่สาธารณชนรู้จักโดยทั่วไป มีความปลอดภัย โปร่งใสและน่าเชื่อถือระบบนิเวศ xCHAIN ขับเคลื่อนด้วยเหรียญ XTH เพื่อเป็นสื่อกลางแทนค่าใช้จ่ายธุรกรรม (Gas Fee) ที่มีเป้าหมายในการลดความผันผวนของราคาจึงทำให้สามารถประเมินค่าใช้จ่ายได้และมีราคาที่สมเหตุสมผล
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน(modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน functions ดังรูปภาพ Consent Flow with RP (AGM Voting)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		Consent Flow with RP (AGM Voting) <pre>graph TD subgraph 01_JDID_eKYC [01 JDID eKYC] Dipchip[Dipchip service] IAL[Complete IAL 2.3] end subgraph 2_AGM_VOTING [2 AGM VOTING] Register[Register] Submit[Submit AAL 2 request] Confirm[Confirm] end subgraph 3_JOIN [3 join] Notification[Received Notification request for AAL 2] ConfirmAAL[Confirm AAL 2 process NDID menu] Result[Submit Result Back] end Register --> Submit Submit --> Confirm Confirm --> Continue[Continue voting] Confirm --> Result Result --> ConfirmAAL ConfirmAAL --> Notification Notification --> Register</pre> ระบบการลงคะแนนมีการออกแบบโครงสร้าง modules ต่างๆ ออกเป็น 3 application 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 Application ใช้สำหรับผู้มีสิทธิลงคะแนน เพื่อยืนยันตัวตนแบบ Multi Factor Authentication ตามมาตรฐาน AAL 2
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคง	Application ระบบการลงคะแนน (AGM Voting) ได้มีการพัฒนาเขียนซอร์สโค้ดตามมาตรฐาน SDLC – Hybride of Waterfall and Agile methodology ซึ่งเป็นไปตามมาตรฐานสากล (Best Practice) และพัฒนาตาม Guideline ที่เป็นมาตรฐานของทางบริษัทที่จัดวางไว้ (Dev-Ops)

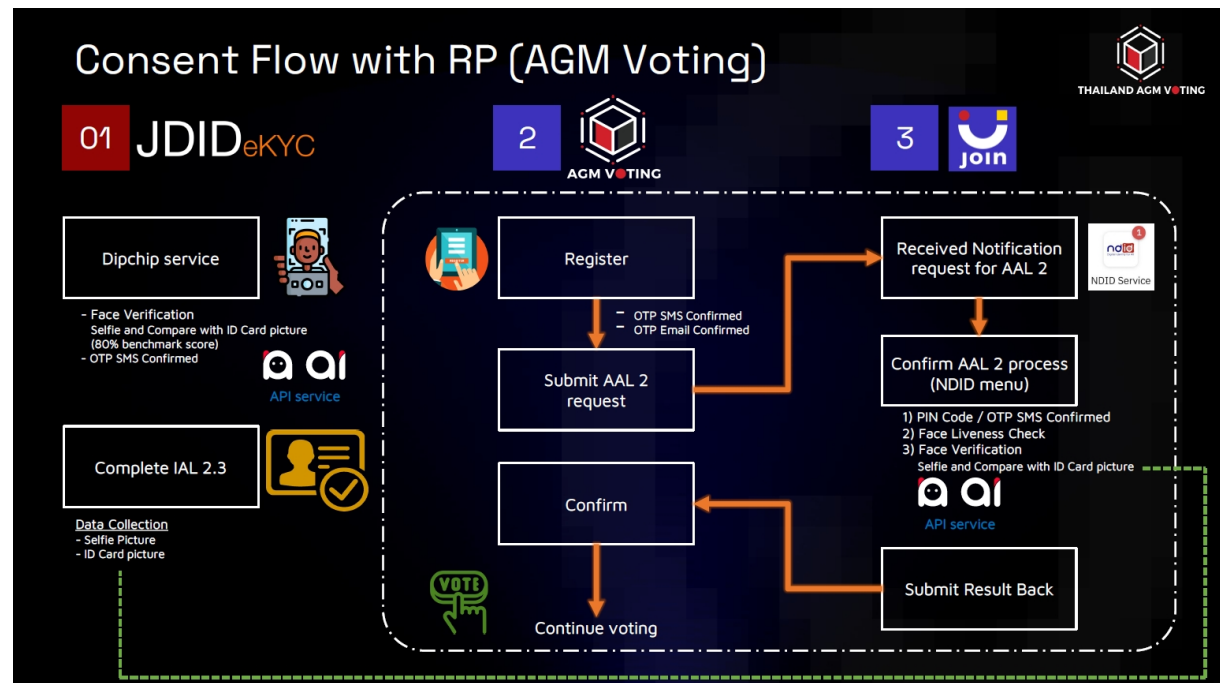
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
(integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	ปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้ (self-modifying code)	ทั้งนี้ จะมีกระบวนการทดสอบการใช้งานในระบบ Development เพื่อให้ยืนยันการทำงานเป็นไปตามที่วางแผนไว้กับทาง Tester ในโครงการ และมีการร่วมวิเคราะห์การเขียน (Analyze Code) จากผู้ที่เชี่ยวชาญจาก Jventures โดยมีการทำ Peer-to-peer source code และ review เป็นการภายในเท่านั้น โดยไม่ได้ใช้ self-modifying การพัฒนาหรือการ Deploy Code ไปที่ระบบ Production บริษัทฯ ใช้ CI/CD ตามมาตรฐานของ GITLAB เพื่อเป็นตัวควบคุมการพัฒนาและการแก้ไขให้เหมาะสมพร้อมมีระบบการตรวจสอบ (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 และมีความโปร่งใส เพื่อให้การเก็บรักษาและการตรวจสอบเป็นไปได้อย่างปลอดภัยและน่าเชื่อถือ
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน	Server ของระบบการลงคะแนน ติดตั้งอยู่บน CS Loxinfo Cloud Center ที่ได้รับมาตรฐานสากล โดยมีการ backup servers ทุกวัน ดังนั้น เมื่อเกิดวิกฤติแล้วต้องทำการกู้คืนข้อมูลต่างๆจะสามารถนำ backup ล่าสุดมา restore เพื่อให้ระบบกลับมาใช้งานได้ โดยมี RPO (Recovery Point Objective) 24 ชม. และ RTO (Recovery Time Objective) 4 ชม. อีกทั้งระบบมีการแจ้งเตือนการ backup สำเร็จ หรือ ไม่สำเร็จ ผ่าน email alert ให้ทุกวัน นอกจากนั้น Hash ของข้อมูลผู้ลงคะแนนและผลการลงคะแนน จะถูกจัดเก็บไว้บน Blockchain จึงทำให้ไม่มีการสูญหาย
3. ความโปร่งใส (Transparent) <u>วัตถุประสงค์</u> 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)

(1) ภาพรวมของระบบ (system overview)



ตามลิงก์ที่แนบ (Link [3.1. AGM Voting Flow on iApp Technology.pdf](#))

(2) ประสิทธิภาพของระบบ (system performance)

มีการทดสอบขีดความสามารถของระบบในกระบวนการบันทึกค่าแฮช (Hash) ของผู้ลงคะแนนและผลการลงคะแนน พบว่าระบบสามารถรองรับปริมาณธุรกรรมสูงสุด (maximum volume) 371 รายการ/วินาที

(3) ความมั่นคงปลอดภัยของระบบ (system security)

บริษัทฯ ใช้มาตรการความมั่นคงตามมาตรฐาน ISO27001-2013 หัวข้อ การควบคุมการเข้าถึง (Access Control) บริษัทฯ จัดทำนโยบายนี้เพื่อเป็นแนวทางในการกำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูลภายใน ข้อมูลลูกค้า ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศขององค์กรเพื่อปกป้องข้อมูล ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศขององค์กร จากการเข้าถึง โดยผู้ที่ไม่ได้รับอนุญาตเพื่อกำหนดกระบวนการในการบริหารจัดการ อนุมัติ/อนุญาต สร้าง เปลี่ยนแปลง ถอดถอน และยกเลิกบัญชีผู้ใช้ และสิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศที่สำคัญ

		1. จัดทำนโยบายควบคุมการเข้าถึงต้องมีการกำหนดจัดทำเป็นลายลักษณ์อักษร และทบทวนทุก 6 เดือน เพื่อให้มั่นใจว่าตรงตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ 2. กำหนดสิทธิ์ ให้ผู้ใช้งานต้องได้รับสิทธิ์ การเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น 3. จัดทำกระบวนการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต 4. ปฏิบัติตามกระบวนการจัดการสิทธิ์ และการถอดถอนสิทธิ์ การเข้าถึงของผู้ใช้งานทุกประเภทและทุกระบบบริการทั้งหมดของบริษัทฯ 5. ดำเนินการตามหลักเกณฑ์ที่กำหนด ให้สอดคล้องกับสิทธิ์ของพนักงานที่เกี่ยวข้อง โดยให้เข้าถึงตามระดับสิทธิ์ ที่ได้รับตามมอบหมาย 6. สิทธิ์ ที่มอบหมายให้พนักงานต้องถูกเป็นความลับห้ามเปิดเผยให้ผู้ที่ไม่เกี่ยวข้องทราบ รวมถึงข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน ซึ่งเป็นข้อมูลลับ 7. จัดให้มีการทบทวนสิทธิ์ การเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้ 8. สิทธิ์ การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อข้อมูลสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องได้รับ การถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน 9. พนักงานต้องดำเนินการตามวิธีปฏิบัติของบริษัทฯ สำหรับการใช้งานข้อมูลการพิสูจน์ตัวตนและต้องจัดเก็บ User และ Password ที่ใช้ในการพิสูจน์ตัวตนให้เป็นข้อมูลลับ 10. การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง โดยห้ามไม่ให้ผู้ไม่มีสิทธิ์เข้าถึง สามารถเข้าถึงสารสนเทศและฟังก์ชัน ยกเว้นจะได้รับการอนุญาตจากผู้มีอำนาจอนุมัติ 11. การเข้าถึงระบบต้องมีการ Login เข้าระบบที่มีความมั่นคงปลอดภัย โดยการ Login เพื่อพิสูจน์ตัวตน หาก Login ไม่ถูกต้อง 5 ครั้ง ระบบจะ Lock และในกรณีที่ผู้ใช้งาน ไม่ได้ใช้งานระบบอย่างต่อเนื่องเป็นระยะเวลา 10 นาที เมื่อต้องการใช้งานต่อ ต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง 12. ระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ
--	--	---

13. ส่วนระบบ Firewall ใช้ระบบ 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 ทำให้สามารถตั้ง Policy เพื่อทำการควบคุมการใช้งาน Application ต่าง ๆ เหล่านั้นได้ เช่น ภายในองค์กรกำหนดสิทธิ์ให้ใช้ระบบผ่าน VPN access และมีการป้องกัน cyber attack เช่น

- IPS (Intrusion Protection System) ระบบตรวจสอบและได้ตอบการบุกรุก เมื่อตรวจพบข้อมูลที่มีลักษณะที่เป็นความเสี่ยงต่อเครือข่าย ก็จะทำการป้องกันข้อมูลนั้น ไม่ให้เข้ามาในเครือข่ายได้
- Antivirus เพื่อเสริมประสิทธิภาพในการป้องกันไวรัสทั่ว ๆ ไป เช่น Malware, Trojan, Spy Ware เป็นต้น ที่จะเข้ามาในระบบเครือข่ายเพื่อทำความเสียหายกับข้อมูลหรือระบบคอมพิวเตอร์
- Firewall ระบบคัดกรองข้อมูลที่พยายามผ่านเข้ามาสู่ระบบเครือข่าย เช่น ข้อมูลชนิดนี้เป็นใคร (Source) ข้อมูลชนิดนี้ทำอะไร (Service) และจะไปที่ไหน (Destination)

(4) การติดตั้งซอฟต์แวร์ (software installation), การทำงานของระบบ (system operations) และ คู่มือการใช้งาน (user manual)

ผู้พัฒนาระบบการลงคะแนน ได้จัดทำเอกสารเกี่ยวกับการติดตั้งซอฟต์แวร์ การทำงานของระบบและคู่มือการใช้งานโดยแบ่งออกเป็นการใช้สำหรับผู้ลงคะแนน ตามเอกสารแนบ คู่มือ JMART – EGM No. 3_2565 และการใช้งานสำหรับผู้จัดประชุม ตามลิงก์ที่แนบ (Link [3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Administrator.pdf](#))



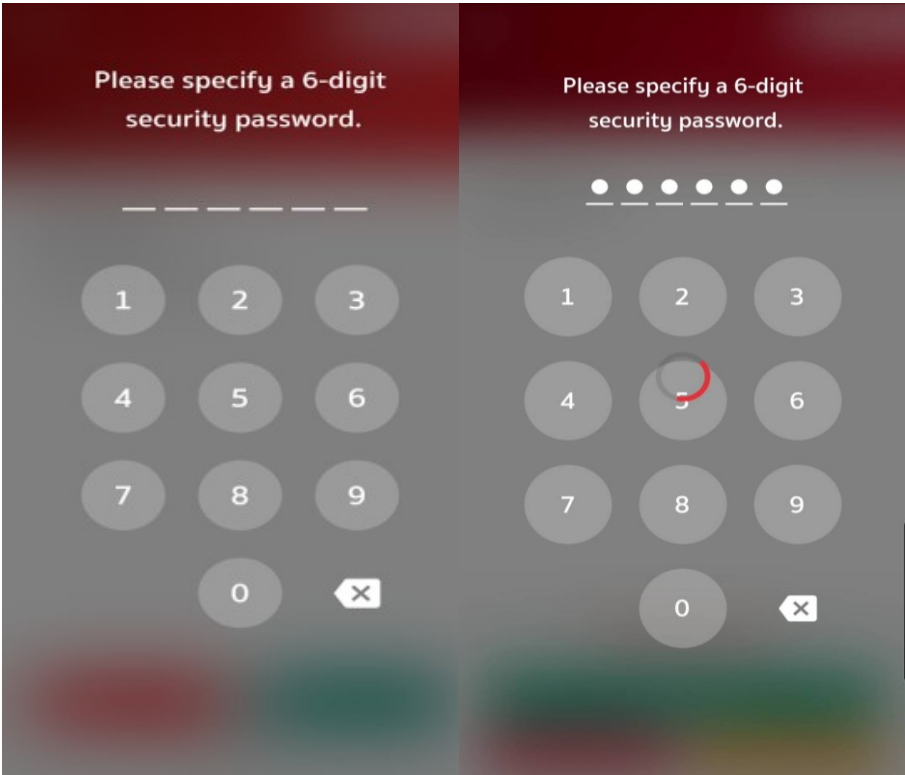
คู่มือ JMART - EGM
No. 3_2565_แนวทางปฏิบัติ

(5) การบำรุงรักษาระบบ (system maintenance)

บริษัทฯ จัดทำเอกสารสำหรับการบำรุงรักษาระบบสารสนเทศ โดยมีการ Upgrading Hardware, System, Software ให้ทันสมัยอยู่เสมอ อีกทั้ง ยังมีการ Monitor servers : โดย Monitoring disk, cpu memory 7*24 hours ผ่านการใช้ Tools ดังนี้ ZABBIX monitoring tool และ ZABBIX monitoring tool warning message ผ่าน LINE Application

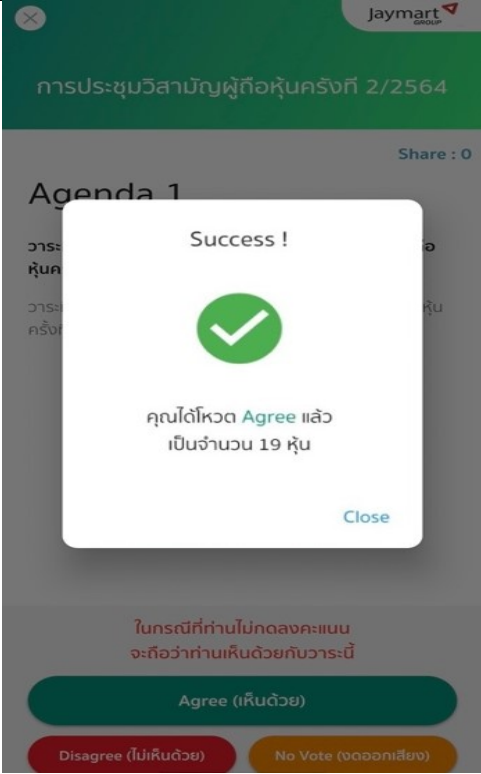
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนนเตรียมไว้พร้อมสำหรับการตรวจสอบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับการติดตั้งและตั้งค่าอย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ	AGM Back Office มีการเฝ้าระวังการทำงานของระบบ AGM Voting ดังนี้ - กรณีมีการจัดประชุม เช่น การประชุมผู้ถือหุ้น จะมีการส่งเจ้าหน้าที่ไป Onsite Support - กรณีผู้จัดประชุมเกิดปัญหาหรือข้อซักถามสามารถติดต่อ J ventures ที่หมายเลข 02-483-6259 หรือ J Ventures Facebook หรือ https://m.me/jventures.jvc - การเฝ้าระวังการทำงานของระบบ (monitor) ทำผ่านระบบ Zabbix application 7x24 Hours โดยมี Notification ผ่าน Line Alert วิธีการตรวจสอบการลงคะแนน ดังนี้ - กำหนดรายชื่อผู้มีสิทธิลงคะแนนทั้งหมดโดยผู้จัดการประชุม - นำรายชื่อผู้ลงทะเบียนออนไลน์สำเร็จในรูปแบบไฟล์ json และ CSV format มาเทียบกับรายชื่อผู้มีสิทธิลงคะแนน - เปิดสิทธิให้ผู้ลงทะเบียนสำเร็จให้สามารถลงคะแนนได้ - นำผลการลงคะแนนแบบออนไลน์รวมกับผลลงคะแนนแบบออฟไลน์ โดยเช็คเทียบกับรายชื่อผู้มีสิทธิลงคะแนนทั้งหมด ทั้งนี้ มีการ Monitor คะแนนในรูปแบบ Realtime โดยมีรายละเอียดเพิ่มเติม ตามเอกสารแนบ คู่มือ AGM Backoffice Manual.pdf  คู่มือ AGM Backoffice Manual.pdf บริษัทฯ มีคู่มือการจัดประชุมระบบลงคะแนนสำหรับ Admin เพื่อผู้จัดประชุมสามารถติดตั้งและตั้งค่าได้อย่างถูกต้อง ตามลิงก์ที่แนบ (Link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Administrator.pdf)
3.3 – บุคคลที่เกี่ยวข้องกับระบบการลงคะแนนสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)	ระบบ AGM voting มีบันทึกเหตุการณ์ (event logging) การเข้าใช้งานทั้งในส่วนของ ผู้ใช้งานระบบ (User) และผู้ดูแลระบบ (Admin) ตามลิงก์ที่แนบ (Link 13.1 ขอบภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบที่ใช้งานจริง.pdf) โดยจัดเก็บข้อมูลไว้ใน MongoDB ซึ่งเป็นในส่วนที่ไม่อยู่ใน smart contract มีรูปแบบการบันทึกเหตุการณ์ (log format) ดังนี้ - ระบบตรวจสอบ User - ถ้ามี User ในระบบจะสร้าง session log - ถ้ามีการสร้าง meeting จะสร้างใน AGMmeetings table

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		4 ถ้ามีการสร้าง meeting agenda จะสร้างใน AGMAgendas table 5 ถ้ามีการ Vote จะสร้างใน AGMmeeting Voters
4. การเข้าถึงอย่างเท่าเทียม (Equitable Access)		
<u>วัตถุประสงค์</u>	เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม	
4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ	ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงผลภาพและเสียง) และรูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัสบนหน้าจอ) ในลักษณะที่สอดคล้องกัน	ปัจจุบันผู้ลงคะแนนสามารถใช้งาน ผ่าน Mobile และ Tablet เท่านั้น โดยแสดงผลหน้าจอเหมือนกันทั้ง 2 อุปกรณ์ โดยผู้ลงคะแนนสามารถกดปุ่ม/สัมผัส ได้ตามฟังก์ชันที่กำหนดบนหน้าจออุปกรณ์ของผู้ลงคะแนน ตามเอกสารแนบ 5.2 รูปแคปเจอร์หน้าจอการแสดงผลบนโทรศัพท์  5.2 รูปแคปเจอร์หน้าจอการแสดงผลบนโทรศัพท์
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  5.2 รูปแคปเจอร์หน้าจอการแสดงผลบนโทรศัพท์
5. การลงคะแนนตรงตามเจตนา (Cast as Intended)		
<u>วัตถุประสงค์</u>	เพื่อให้การแสดงผลข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้	
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting)	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล (preference setting) ตามความต้องการของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษร และสีของภาพ	ระบบการลงคะแนน (AGM Voting) มีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก ตามลักษณะของ Mobile Device (Responsive design) และไม่สามารถปรับแต่งค่าตามความต้องการของผู้ใช้งานรายบุคคลได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ให้ตรงกับความต้องการของผู้ลงคะแนน		
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง เช่น รูปแบบการแสดงผลของข้อมูล (display format) การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้าถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ (touch screen gestures) รวมถึง ระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) เช่น การให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนน หรือการแจ้งสถานะของการลงคะแนนให้ผู้ลงคะแนนทราบ	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 การให้ผู้ลงคะแนนยืนยันเจตนา ก่อนส่งผลลงคะแนนทุกวาระ. โดยการกด PIN ซึ่งเป็นรหัสที่ผู้ใช้งาน/ผู้ลงคะแนนจะทราบแต่เพียงผู้เดียว (Something you know) 

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		รูปที่ 1 แสดงหน้าต่างให้ผู้ลงคะแนนยืนยันเจตนา ก่อนการลงคะแนน หน้าหน้าการยืนยัน กด PIN ก่อนการลงคะแนน
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน คำแนะนำ และข้อความจากระบบด้วยภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งข้อความที่ไม่ให้เกิดความสับสนในการลงคะแนน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต หรือการเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) และการแสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว นอกจากนี้ ระบบมีการแสดงคำแนะนำและข้อความที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ	ระบบมีการแสดงข้อมูลกฎกติกาของการลงคะแนน และคำแนะนำ ผ่านการแจ้งในหนังสือเชิญประชุมผู้ถือหุ้น ดังตัวอย่างตามลิงก์ที่แนบ (Link 5.3 JMART - EGM Notice 3_2565_TH.pdf.pdf) ซึ่งส่งแจ้งทางอีเมลของผู้เข้าร่วมการประชุม ระบบมีการวางวาระตามลำดับไม่ก่อให้เกิดความสับสนในการลงคะแนน ตัวอักษรชัดเจน และอ่านง่าย โดยผู้ลงคะแนนสามารถกดเลือกลงคะแนนได้เพียง 1 ตัวเลือกเท่านั้น โดยมีตัวเลือกดังนี้ Agree (เห็นด้วย) , Disagree (ไม่เห็นด้วย) , No Vote (งดออกเสียง) และระบบจะมีการแจ้งเตือน เมื่อกดเลือกตัวเลือกสำเร็จ หากผู้ลงคะแนนมีความต้องการที่จะเปลี่ยนแปลงผลการลงคะแนน สามารถทำได้จนกว่าผู้จัดประชุมจะปิดวาระนั้น ในกรณีที่ผู้ลงคะแนนไม่กดเลือกปุ่มใด ๆ จนครบระยะเวลาลงคะแนน ระบบจะบันทึกว่าผู้ลงคะแนนเห็นด้วยกับวาระนี้ เมื่อผู้ลงคะแนนทำการลงคะแนนสำเร็จระบบจะแสดงหน้าต่างแจ้งเตือน (popup) การลงคะแนนสำเร็จให้ทราบ ระบบการลงคะแนนสำหรับผู้จัดประชุมไม่มีฟังก์ชันแสดงคำแนะนำในการใช้งาน แต่ทางบริษัทฯ ได้จัดทำคู่มือ แนวทางปฏิบัติงาน และการบำรุงรักษาระบบสำหรับผู้จัดการประชุม (Administrator) ตามลิงก์ที่แนบ (Link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Adminitrator.pdf)

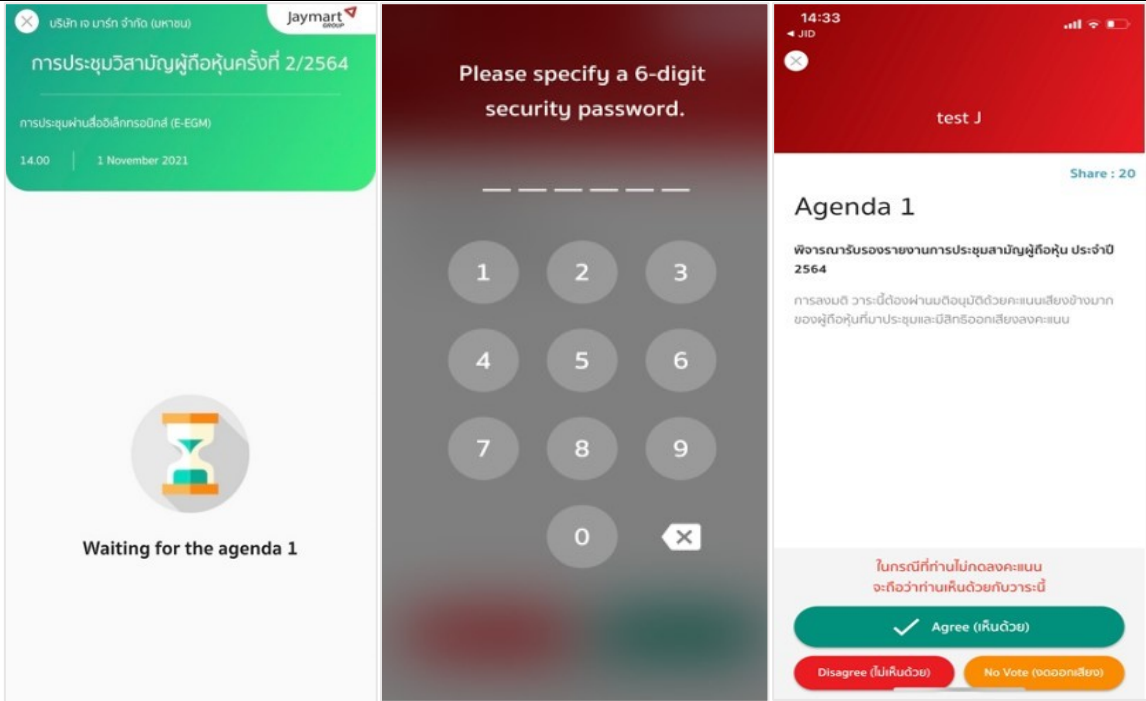
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 รูปที่ 1 แสดงการวางข้อความและตัวเลือกสำหรับการลงคะแนน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 รูปที่ 2 การแจ้งเตือนเมื่อโหวตสำเร็จ ซึ่งแสดงเป็นข้อความผ่าน Popup
6. ความเหมาะสมต่อการใช้งาน (Usable) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้อย่างเหมาะสม		
6.1 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบการลงคะแนน เพื่อให้มั่นใจว่าระบบการลงคะแนนสามารถใช้งานกับผู้ลงคะแนนทุกคน (ซึ่งอาจรวมถึงผู้สูงอายุและบุคคลที่มีความบกพร่องทางการมองเห็น) ได้อย่างเหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี เช่น มาตรฐาน Web Content Accessibility	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบการลงคะแนนการประชุม ซึ่งกลุ่มตัวอย่างมีช่วงอายุอยู่ระหว่าง 20 - 59 ปี จำนวน 25 คน แต่ยังไม่รองรับ “บุคคลที่มีความบกพร่องทางการมองเห็น” ซึ่งบริษัทได้ทดสอบ โดยทดสอบกับระบบปฏิบัติการ Android และระบบปฏิบัติการ iOS

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	Guidelines (WCAG) 2.0 ของ World Wide Web Consortium (W3C)	
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ	ในปัจจุบันบริษัท เจ เวนเจอร์ส บริการลูกค้าโดยการมอบหมายเจ้าหน้าที่ของ เจ เวนเจอร์ส เป็นผู้ควบคุมระบบลงคะแนนในทุกการประชุม โดย บริษัทฯ ได้รับมอบหมายจากนิติบุคคลผู้ว่าจ้างตามใบเสนอราคาที่เรียกเก็บเป็นค่าบริการจาก นิติบุคคล (บริษัท JMART) นั้น ซึ่งหากผู้จัดประชุมต้องการควบคุมระบบการลงคะแนนด้วยตนเอง ทางบริษัทฯ ได้จัดทำคู่มือสำหรับผู้จัดประชุม ซึ่งมีคำแนะนำในการตั้งค่าระบบ วิธีการใช้งานในระหว่างลงคะแนน การเปิด-ปิดระบบการประชุม และมีการฝึกอบรมการใช้งานสำหรับผู้ควบคุมระบบการลงคะแนนเพื่อให้ 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) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) ระบบนำเข้าข้อมูลรายชื่อผู้มีสิทธิลงคะแนนในรูปแบบไฟล์ XLS และส่งออกข้อมูลรายชื่อผู้ลงคะแนนเข้าร่วมการประชุมในรูปแบบไฟล์ CSV และ json format และ XLS ได้ ซึ่งอยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) ตามข้อ 4 ของลิงก์ที่แนบ (Link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Administrator.pdf)
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้รูปแบบมาตรฐาน ในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่าง ๆ	ระบบการลงคะแนนโปรโตคอล TCP/IP ในการติดต่อสื่อสาร (communication protocol) และใช้โปรโตคอล HTTPS ในการเรียกโปรแกรมบราวเซอร์ (Browser Program) เพื่อเรียก Service ภายในต่างๆ ให้ทำงานตาม Request เช่น https://e-kyc.jfin.neteork เป็นต้น
8. การตรวจสอบ (Auditable)		
วัตถุประสงค์	เพื่อให้ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบความถูกต้องของผลลงคะแนน	
8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	ผลลงคะแนนที่ได้จากการลงคะแนนของผู้ลงคะแนน มีคุณสมบัติที่สามารถตรวจพบการ	ระบบมีการบันทึก Hash ของผู้ลงคะแนนและผลการลงคะแนน ไว้บน Blockchain ทำให้ผู้ดูแลระบบสามารถตรวจสอบ transaction ที่เกิดขึ้นย้อนหลังได้ผ่านข้อมูลที่บันทึกบน blockchain นอกจากนี้ยังมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้น ในระหว่างการลงคะแนน โดยแจ้งผ่านฝ่ายนักลงทุนสัมพันธ์ของบริษัท/ผู้จัดการประชุม/ผู้ประสานงานนิติบุคคลอาคารชุด ซึ่งจะส่งปัญหาต่อมายังทีม Support ของผู้ลงคะแนนโหวตโดยเฉพาะ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	เปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลได้ (tamper-evidence) ระบบการลงคะแนนเปิดโอกาสให้ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกไป แจ้งข้อผิดพลาดในผลลงคะแนนที่เกิดจากระบบการลงคะแนน และเริ่มต้นลงคะแนนใหม่ หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน (ขึ้นอยู่กับกฎหมายหรือหลักเกณฑ์ที่กำหนด) รวมถึงควรมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ระบบการลงคะแนนต้องสร้างรายงานที่จะช่วยให้ผู้ตรวจสอบภายนอก (external auditor) สามารถตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง รวมถึงผู้พัฒนาระบบการลงคะแนนจัดทำขั้นตอนสำหรับการตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง	ผู้จัดประชุมสามารถตรวจสอบผลการลงคะแนนเทียบกับผู้มีสิทธิลงคะแนนได้เพื่อตรวจสอบความถูกต้องของยอดผลการลงคะแนนได้ที่หน้าสรุปผลการลงคะแนน ซึ่งจะแสดงเมื่อปิดการประชุม ระบบสามารถส่งออกข้อมูลการลงคะแนนให้ Auditor ตรวจสอบได้ รวมถึงการรวมคะแนนกับคะแนนส่วนอื่นๆ จากฐานข้อมูล (Database) ของบริษัทผู้จัดการประชุมโดยระบบสามารถ Export ไฟล์เป็น CSV หรือ json format
9. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy) ¹		
วัตถุประสงค์	เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง	
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่ต้องแสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน	การลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้โดยไม่ต้องแสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน โดยก่อนทำการโหวตจะต้องทำการยืนยันตัวตน และป้อนรหัส PIN ก่อนกดลงคะแนนในทุกวาระการประชุมเพื่อยืนยันว่าคนที่ทำการลงคะแนนเป็นผู้มีสิทธิลงคะแนนนั้นจริง การแสดงผลการลงคะแนนจะปรากฏเพียงภาพรวมของคะแนน โดยไม่ระบุตัวตนของผู้ลงคะแนน ตามรายละเอียดของลิงก์ที่แนบ ข้อ 5.7-5.9 (link 3.1 คู่มือ AGM Voting แนวทางปฏิบัติสำหรับ Administrator.pdf)

¹ ความเป็นส่วนตัวของผู้ลงคะแนน ในที่นี้หมายถึง ความเป็นส่วนตัวที่เกิดขึ้นภายในระบบการลงคะแนนเท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 รูป แสดงหน้าวาระการประชุม การยืนยันตัวตนเพื่อยืนยันว่าเป็นผู้มีสิทธิลงคะแนนนั้นจริง และแสดงหน้าสำหรับลงคะแนน (จากซ้ายไปขวาตามลำดับ)
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่าส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน	ในการลงคะแนนผู้ลงคะแนน สามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้เอง ตามรูปแบบการตั้งค่าเริ่มต้นของแอปพลิเคชันในโทรศัพท์เครื่องนั้น ๆ ของผู้ลงคะแนน อีกทั้งยังมีการกำหนดให้ยืนยันตัวตนโดยการกด PIN ซึ่งผู้ลงคะแนนเท่านั้นที่จะทราบ ก่อนลงคะแนนในวาระนั้น เพื่อป้องกันบุคคลอื่นในการแทรกแซงการลงคะแนนของผู้ลงคะแนน โดยที่ผู้ดูแลระบบไม่สามารถเข้าถึงหน้าแอปพลิเคชันของผู้ลงคะแนนได้
10. ความลับของคะแนนเสียง (Vote Secrecy) <u>วัตถุประสงค์</u> (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน		

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	ระบบการลงคะแนนต้องไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มาประมวลผล จัดเก็บ หรือแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว	ผลการลงคะแนนจะนำเสนอในรูปแบบคะแนนรวม โดยแยกตามผลการลงคะแนน/ประเภทการลงคะแนน ดังนี้ จำนวนผู้มีสิทธิลงคะแนนทั้งหมด จำนวนผลการลงคะแนนทั้งหมด จำนวนผลการลงคะแนนทั้งหมดที่แบ่งเป็น เห็นด้วย/ไม่เห็นด้วย/งดออกเสียง/เพิกเฉย และจำนวนผู้ไม่มาประชุม ซึ่งไม่มีการนำข้อมูลส่วนบุคคลของผู้ลงคะแนนมาแสดง ดังรูปภาพตัวอย่างที่แนบ วาระการประชุม 1 - Self Assessment ✓ 2 - อื่นๆ ✓ Total voter 1 Total vote 0 Agree (0) เห็นด้วย 0 Disagree (0) ไม่เห็นด้วย 0 No vote (0) งดออกเสียง 0 No action n เพิกเฉย 2,900 Abandon ไม่เข้าร่วม 0 START STOP ↺ รูปที่ 1 แสดงคะแนนรวม โดยแยกตามผลการลงคะแนน/ประเภทการลงคะแนน

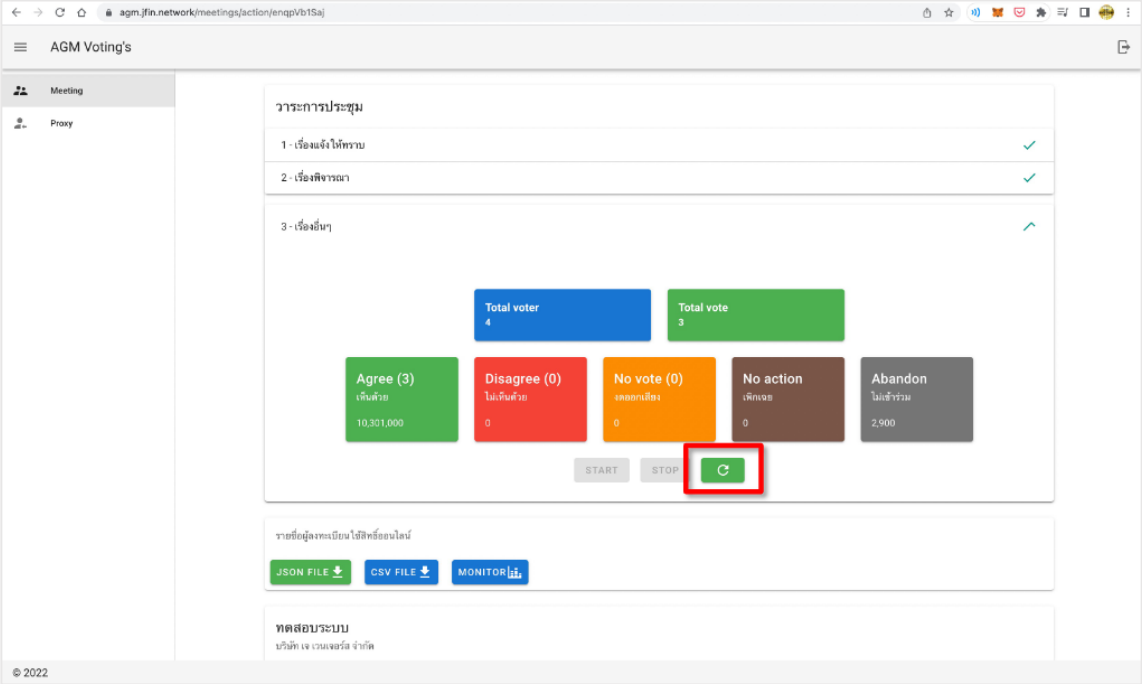
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอัตโนมัติระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้นจึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับ และนำไปนับคะแนนเป็นผลรวมของการลงคะแนน	
11. การควบคุมการเข้าถึง (Access Control)		
วัตถุประสงค์	เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น	
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน เพื่อให้มีหลักฐานสำหรับตรวจสอบในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งาน เปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง	มีการเก็บ log ของทุก activities และ ทุก users รวมทั้งผู้ควบคุมโดยเก็บรายละเอียดใน session table (mongo db) ซึ่งมีความสัมพันธ์ (DB relationship) กันตามลำดับดังนี้ Table User สำหรับเก็บสิทธิ์ของ user , Table session สำหรับเก็บ transaction log , Table AGMeeting สำหรับเก็บ หัวข้อการประชุม , Table AGMAgendars สำหรับเก็บวาระต่างๆในหัวข้อการประชุม และ Table AGMeeingVotes สำหรับเก็บรายละเอียดของผู้ลงคะแนน บริษัทฯ ทำการกำหนดสิทธิ์ให้ Security Admin เป็นผู้เข้าระบบ log ของ database และมีการ hash ข้อมูลซึ่งถูกเก็บใน blockchain หากมีการแก้ไขเหตุการณ์ใด ๆ ระบบจะสามารถตรวจสอบย้อนกลับได้ ตามเอกสารแนบ 13.1 ภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบ 13.1 ขอบภาพแสดงตัวอย่าง Log ของผู้ควบคุม
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนน และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดบัญชีผู้ใช้งานที่ได้รับอนุญาต กำหนดบทบาทของผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละบทบาทของผู้ใช้งาน	ระบบการลงคะแนนกำหนดบทบาทหน้าที่ของผู้ใช้งาน ดังนี้ 1. Super user มีหน้าที่สร้าง user ผู้ควบคุมระบบ 2. ผู้ควบคุมระบบ มีหน้าที่สร้างผู้ใช้งานหรือผู้มีสิทธิลงคะแนน 3. ผู้ใช้งานหรือผู้มีสิทธิลงคะแนน มีสิทธิ์ลงคะแนนตามวาระที่ตัวเองมีสิทธิ์เท่านั้น โดยมีวิธีการสร้างและกำหนดสิทธิ์ ตามเอกสารแนบ AGM Backoffice Manual.pptx AGM Backoffice Manual.pptx

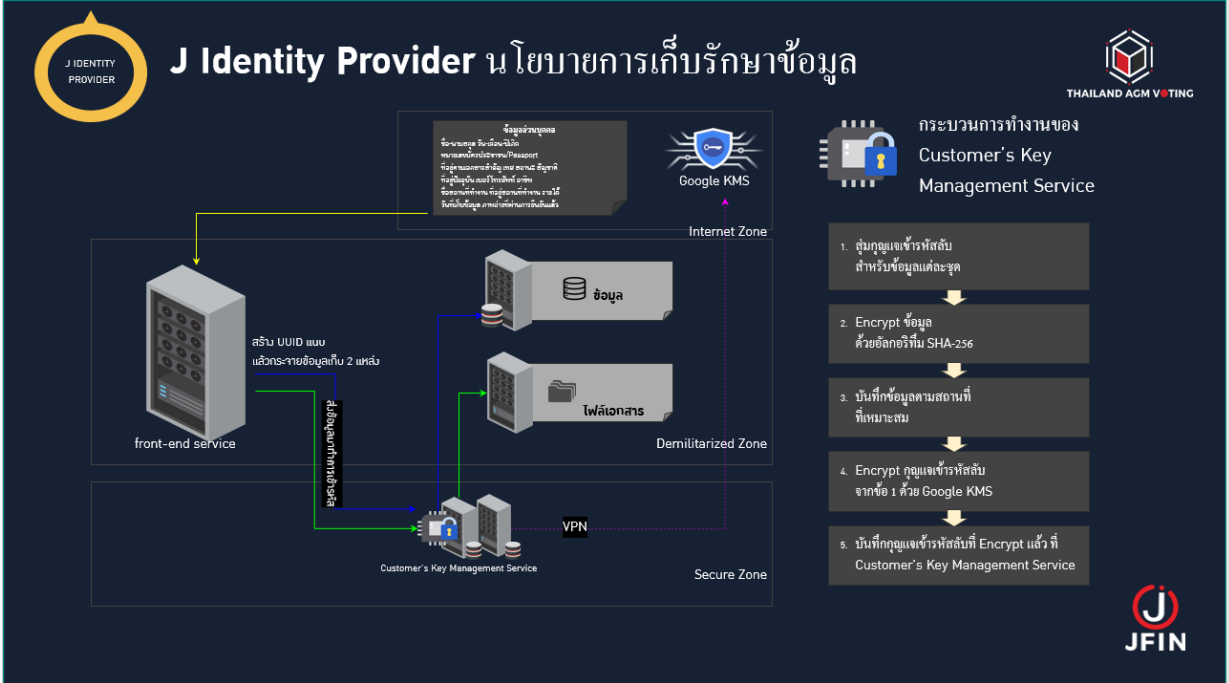
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ผู้ควบคุมระบบที่กำหนดสิทธิ์นั้น เป็นได้ทั้งผู้ให้บริการและผู้ให้บริการ ในกรณีที่ผู้ควบคุมระบบเป็นผู้ถือหุ้น และมีสิทธิ์ออกเสียง ผู้ควบคุมระบบจะ upload รายชื่อและจำนวนคะแนนเข้าระบบ โดยมีตัวแทนการประชุมเช่น โฆษกในงานเป็นผู้ตรวจสอบข้อมูลก่อนนำเข้าระบบ อีกทั้งยังมีการกำหนดสิทธิในส่วน Authorize Matrix ของการใช้งานระบบ มีกระบวนการบริหารจัดการของผู้ให้บริการเอง (Backoffice) เช่น มีการแยกหน้าที่ของทีม Security ทีม Network และทีม Operation เป็นต้น โดยมีตัวอย่าง ตามเอกสารแนบ 14.1 ตารางการกำหนดสิทธิ์รายบุคคล 14.1 ตารางการกำหนดสิทธิ์รายบุคคล.pdf
11.3 – ระบบการลงคะแนนรองรับวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (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 ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการ		The diagram illustrates the 'Consent Flow with RP (AGM Voting)' process. It is divided into three main stages: 01 JDIDeKYC, 2 AGM VOTING, and 3 join. Stage 01 involves 'Dipchip service' (Face Verification, Selfie and Compare with ID Card picture, 80% benchmark score, OTP SMS Confirmed) and 'Complete IAL 2.3' (Data Collection: Selfie Picture, ID Card picture). Stage 2 involves 'Register' (OTP SMS Confirmed, OTP Email Confirmed), 'Submit AAL 2 request', 'Confirm', and 'Continue voting'. Stage 3 involves 'Received Notification request for AAL 2' (NDID Service), 'Confirm AAL 2 process (NDID menu)' (1) PIN Code / OTP SMS Confirmed, 2) Face Liveness Check, 3) Face Verification, Selfie and Compare with ID Card picture), and 'Submit Result Back'. The process is supported by 'AI API service' and 'VOTE' branding. การพิสูจน์และยืนยันตัวตนของระบบการลงคะแนนของผู้ควบคุมการลงคะแนนและผู้ลงคะแนน รวมทั้งผู้ใช้งานของระบบ AGM Voting มีรายละเอียด ดังนี้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ลงคะแนนสามารถกำหนดความเข้มงวดและการหมดอายุของรหัสผ่าน	การพิสูจน์ตัวตนของระบบการลงคะแนน จะต้องทำการพิสูจน์ตัวตนทั้งผู้ควบคุมระบบและผู้ลงคะแนน เป็นไปตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level) IAL2.3 ประกอบด้วย การดึงข้อมูลจากบัตรประจำตัวประชาชน ซึ่งผู้ใช้บริการต้องไปทำการ Dip Chip ด้วยตนเอง ณ จุดบริการสาขา Jaymart พร้อมทั้งตรวจสอบสถานะข้อมูลจากบัตรกับกรมการปกครอง 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 เมื่อผู้ลงคะแนนยืนยันตัวตนผ่านเป็นที่เรียบร้อยแล้ว จึงจะสามารถเข้าประชุมผ่าน Application AGM voting ได้ ผู้ใช้บริการสามารถ download application “JOIN” และ “AGM Voting” จาก App Store หรือ Play Store เพื่อใช้ในการยืนยันตัวตนแบบหลายปัจจัย ก่อนทำการลงคะแนน ระบบการลงคะแนนมีการเก็บรักษาข้อมูลการยืนยันตัวตน โดยมีการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล โดยใช้ Symmetric Key เพื่อเข้ารหัสลับ ซึ่งจะมีความยาว 256 bit ขึ้นไป และใช้ SHA Algorithm (SHA-256) ในการเข้ารหัสลับ และมีการ Hash Voter Address ส่งเข้า blockchain ดังตัวอย่างตามลิงก์ที่แนบ (Link https://exp.xchain.asia/address/0x546Da1e07b8FDC0eCC73e84d717AcCDFC16C75da/transactions)
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลดสิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่ (separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น	การกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยมี ระดับ 1. Super user มีหน้าที่สร้าง Administrator โดยมีการวิธีสร้างตามเอกสารแนบคู่มือ AGM Backoffice Manual.pptx หน้า 3 AGM Backoffice Manual.pptx 2. Administrator หรือ ผู้ควบคุมระบบ มีหน้าที่ในกำหนดสิทธิในการจัดประชุมต่างๆ 3. End User หรือ ผู้ลงคะแนน มีหน้าที่ลงคะแนนในวาระต่างๆ โดยสิทธิระดับ Super user เท่านั้นที่สามารถสร้าง user ผู้ควบคุมระบบได้

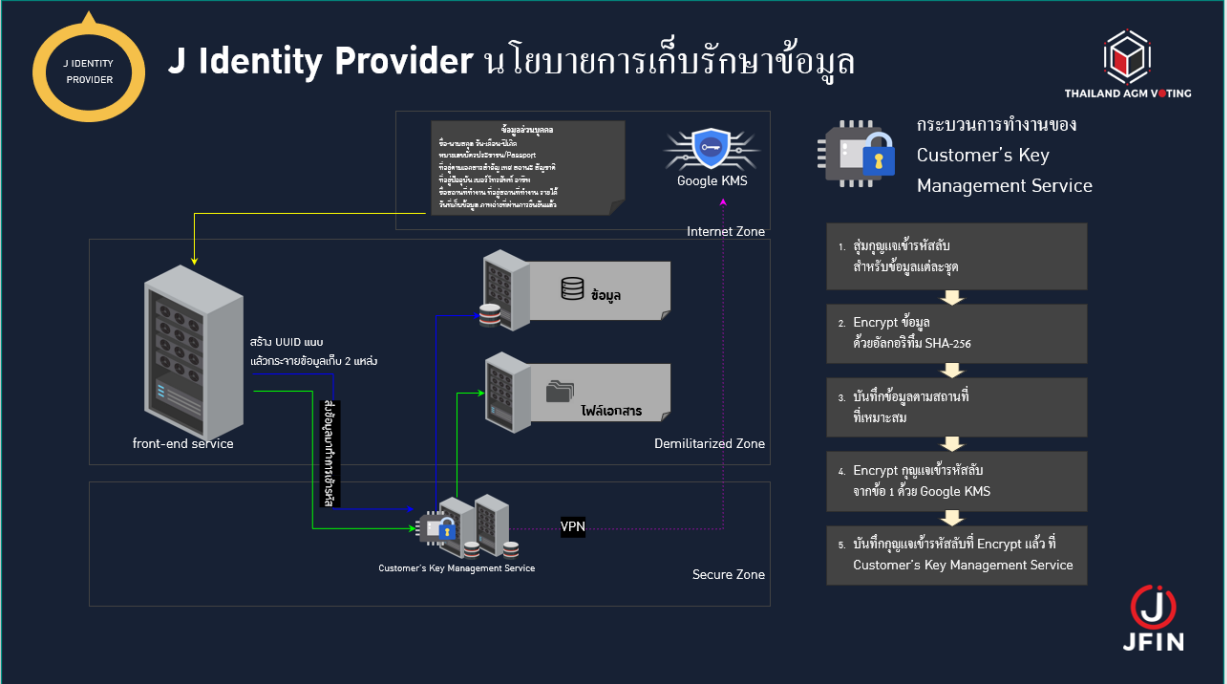
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ทั้งนี้ บริษัทฯ มีการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ของพนักงาน และความรับผิดชอบของตำแหน่งงาน โดยมีการแบ่งเป็นทีม เช่น ทีม security, ทีม Network, ทีม Operation ตามเอกสารแนบ 14.1 ตารางการกำหนดสิทธิ์รายบุคคล  14.1 ตารางการกำหนดสิทธิ์รายบุคคล.pdf
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด หากผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนควรระงับการใช้งาน (account lockout) ของผู้ใช้งานเป็นระยะเวลาหนึ่งก่อนจะให้ผู้ใช้งานยืนยันตัวตนครั้งต่อไป และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาการระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด กรณีผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด 2 ครั้ง ระบบการลงคะแนนจะ lockout และ ผู้ใช้งานต้องทำการ log in เข้าสู่ระบบใหม่ ระยะเวลาการระงับการใช้งาน (lockout duration) ประมาณ 1 นาที
12. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) <u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย		
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษา	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐาน หรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาตหรือการถูกตัดการเชื่อมต่อทางกายภาพ เกิดขึ้นกับ	ระบบการลงคะแนน วางอยู่บน CS Loxinfo Cloud Center – Servers ที่มีมาตรฐาน • ISO/IEC 20000-1: 2018, • CSA STAR CERTIFICATION 2014 • ISO 9001:2005

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน ผู้พัฒนาระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อกที่มั่นคงปลอดภัย หรือระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ	- ISO 22301:2019 - ISO/IEC 27001:2013
13. การคุ้มครองข้อมูล (Data Protection)		
<u>วัตถุประสงค์</u>	เพื่อให้ระบบการลงคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนนจากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนน และระบบเครือข่าย รวมถึงระบบการลงคะแนน ต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง	ระบบการลงคะแนนอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนน ซึ่งหมายถึงผู้ให้บริการเท่านั้น โดยควบคุมระบบจะต้องยืนยันตัวตนแล้วเท่านั้น จึงสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนน (Administrator) และ vote records ถูกเก็บบน Blockchain ทำให้เกิดความครบถ้วนของการลงคะแนนที่สามารถทำการแก้ไขได้ ตัวอย่าง Log Table ของผู้จัดประชุม (ผู้ควบคุมระบบ) โดยมีจำนวน 5 Table ได้แก่ 1. Table user objid เมื่อผู้ควบคุมระบบทำการ log in ใน AGM ด้วย mobile ระบบจะทำการแปลงค่าเป็น objid ใน user table 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 โดยจะถูกกำหนดเป็นตัวแปรเมื่อผู้ควบคุมระบบทำการเพิ่ม 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 โดยมี meetingId เป็น linkage ตามเอกสารแนบ 13.1 ภาพแสดงตัวอย่าง Log ของผู้ควบคุมระบบ  13.1 ขอภาพแสดง ตัวอย่าง Log ของผู้ควบคุม

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับมาจากผู้ลงคะแนน บันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที และจัดเก็บบันทึกการลงคะแนนให้อยู่ในรูปแบบที่สามารถแสดงผลลงคะแนนที่ได้รับมาให้ปรากฏอย่างถูกต้องได้	ผู้จัดการประชุม เป็นผู้ที่มีสิทธิ์ลงคะแนนเข้าระบบ และสามารถตรวจสอบข้อมูลที่มีการบันทึกการลงคะแนนได้ โดยมีการแสดงผลผ่าน Dashboard ของผู้ดูแลระบบ ซึ่งจะสามารถตรวจสอบความครบถ้วนของผลการลงคะแนนที่ได้รับจากผู้ลงคะแนนได้ ดังรูป กรณีที่ระบบมีข้อผิดพลาดแล้วทำให้ user ลงคะแนนไม่ได้ ระบบจะถือว่า user ทำการ “no action” แล้วจะนำคะแนนไปรวมกับ คะแนน “เห็นด้วย” ในการรวมคะแนนวาระ นั้นๆ ซึ่งถูกกำหนดไว้โดยระบบไม่ได้ขึ้นกับเกณฑ์การประชุมของผู้จัดการประชุม (มีการประกาศเตือน โดย โฆษก ก่อนเริ่มการประชุมทุกครั้ง)  รูป การบันทึกการลงคะแนนโดยมีการแสดงผลผ่าน Dashboard
13.3 – ระบบการลงคะแนนใช้อัลกอริทึมการเข้ารหัสลับ (cryptographic)	กฎแฉเข้ารหัส โมดูลการเข้ารหัสลับ (cryptographic module) และอัลกอริทึมการเข้ารหัสลับ (cryptographic algorithm) ที่ใช้ในกระบวนการเข้ารหัสลับของระบบการลงคะแนนต้องเป็นไปตามมาตรฐาน เช่น FIPS 140	ระบบจะใช้ การเข้ารหัส Google KMS ซึ่งเป็น Symmetric Key เพื่อเข้ารหัสลับ โดยจะมีความยาว 256 bit ขึ้นไปและใช้ SHA Algorithm (SHA-256) ในการเข้ารหัสลับ โดยการออกแบบจะใช้วิธีสร้างกุญแจแต่ละบุคคลไม่ซ้ำกัน เพื่อใช้เป็นกุญแจเข้ารหัสลับขั้นแรก แล้วจึงนำข้อมูลที่เข้ารหัสลับแล้วไปบันทึกไว้ จากนั้นนำกุญแจดังกล่าวมาเข้ารหัสลับด้วยกุญแจดอกที่สอง (กุญแจดอกที่สอง จะใช้ดอกเดียวกันกับทั้งระบบ) ที่เก็บไว้ใน Google Cloud KMS แล้วจึงนำกุญแจที่เข้ารหัสลับแล้ว มาบันทึก

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
algorithm) ที่เป็นมาตรฐาน	Security Requirements for Cryptographic Modules และ NIST Special Publication 800-57 Part 1 Recommendation for Key Management: Part 1 – General	ไว้ที่ฐานข้อมูลของ Customer Key Management Service การออกแบบเช่นนี้ จะสามารถแก้ปัญหาเรื่องการเปลี่ยนผู้ให้บริการ Cloud KMS ในอนาคตได้ โดยไม่จำเป็นต้องแตะต้องข้อมูลบุคคลเลย Customer Key Management Service จะเป็นส่วนที่สำคัญที่สุดและไม่สามารถเชื่อมกับอินเทอร์เน็ตได้โดยตรง โดยจะมีการกำหนด Access Control เพื่ออนุญาตให้ใช้งานผ่าน Server ที่อนุญาตเท่านั้น และใช้ฐานข้อมูลแยกจากข้อมูลอื่นๆ ในระบบ ตามรูป  รูป แผนภาพการทำงานของระบบ Secure Storage ภาพถ่ายที่ผ่านการยืนยันแล้ว จะถูกจัดเก็บไว้ที่ระบบ JOIN ซึ่งระบบลงคะแนนจะไม่ได้จัดเก็บข้อมูลชีวมิติ
13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ	การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่าย	บริษัทมีการวางสถาปัตยกรรมระบบเครือข่ายซึ่งมีช่องทางการเชื่อมต่อที่ปลอดภัย (mutually-authenticated secure channel) ต่างๆ ดังนี้ 1. ผู้ลงคะแนนเข้าใช้งานระบบบนมือถือ (mobile) ผ่าน public internet 2. CloudFare มีการใช้งาน load balance และ anti ddos อีกทั้งยังซ่อน IP ปลายทาง มีอุปกรณ์ dns server สำหรับถอดค่า DNS name เป็น public IP ของ Jventures แล้วทำการส่ง package ไปให้ปลายทางตามที่ระบุ 3. CSL Firewall – FortiGate มีหน้าที่ทำการตรวจสอบ incoming IP เพื่ออนุญาต หรือไม่อนุญาต IP ตาม policy ที่ตั้งไว้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
(confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด	คอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)	โดยจะทำการ scan VIRUS ทุกครั้ง ทั้งนี้บริษัทฯ ยังการแบ่งโซนการทดสอบระหว่างขั้นตอน Production กับขั้นตอนการทำ UAT บริษัทมีการจัดทำ Security configuration baseline ซึ่งเป็นแนวทางการตั้งค่านโยบายความมั่นคงปลอดภัยโดยการจำกัดการเข้าถึง (least privilege) ซึ่งประกอบไปด้วยการไม่ให้สิทธิเกินหน้าที่และความจำเป็น การตรวจสอบความปลอดภัยในการเข้าถึงระบบของผู้ดูแลระบบ ซึ่งรวมถึง การติดตั้งการใช้งาน การกำหนดค่าในการบริหารทรัพยากร การกำหนดกลุ่มของผู้ใช้งาน และการใช้งานนโยบายการรักษาความมั่นคงปลอดภัย การดูแลระบบ Security Verify Access เกี่ยวข้องกับงานระดับสูงดังต่อไปนี้ การติดตั้งและกำหนดค่าในการบริหารทรัพยากร การกำหนดคุณลักษณะผู้ใช้งานที่สามารถเข้าถึงได้ ประเภทของการเข้าใช้งาน ระยะเวลาที่สามารถเข้าใช้งานได้ เงื่อนไขที่ต้องปฏิบัติตาม การควบคุมการเข้าถึงของผู้ใช้งานเฉพาะกลุ่ม Access Control List (ACL) การกำหนดกฎในการเข้าถึงของผู้ใช้งาน การอนุญาตให้เข้าถึงข้อมูล รายละเอียดตามรูป
		The diagram illustrates the network architecture for Jventures. It is divided into two main sections: PRODUCTION (top, green border) and UAT/DEV (bottom, red border). A central Cloud (Public Network) and CloudPare (Firewall) act as the hub. On the left, external services like JDID-EKYC, JOIN, and AGM Voting connect to the Cloud. The PRODUCTION environment includes AGM Voting, JOIN, EKYC API, Mail Server, X-Chain Node, OTP, JFINChain Node, and JVEN IDP. The UAT/DEV environment includes VPN & JUMP Host Server, EKYC API UAT, JVEN IDP UAT, JOIN UAT, and X-Chain UAT. Dashed lines represent network connections between these components.
		รูป ตัวอย่าง Jventures Network Diagram

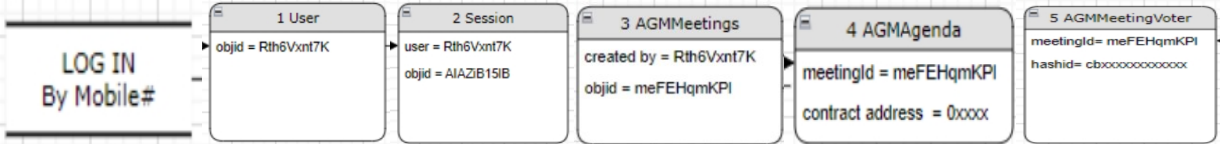
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ในส่วนของ Data in transit ระบบจะใช้ การเข้ารหัส Google KMS ซึ่งเป็น Symmetric Key เพื่อเข้ารหัสลับ โดยจะมีความยาว 256 bit ขึ้นไปและใช้ SHA Algorithm (SHA-256) ในการเข้ารหัสลับ โดยการออกแบบจะใช้วิธีสร้างกุญแจแต่ละบุคคลไม่ซ้ำกัน รายละเอียดตามรูป  J Identity Provider นโยบายการรักษาข้อมูล กระบวนการทำงานของ Customer's Key Management Service 1. กลุ่มกุญแจเข้ารหัสลับสำหรับข้อมูลแต่ละชุด 2. Encrypt ข้อมูล ด้วยอัลกอริทึม SHA-256 3. บันทึกข้อมูลตามสถานที่ที่เหมาะสม 4. Encrypt กุญแจเข้ารหัสลับจากข้อ 1 ด้วย Google KMS 5. บันทึกกุญแจเข้ารหัสลับที่ Encrypt แล้วที่ Customer's Key Management Service
14. การรักษาความครบถ้วนของระบบ (System Integrity)		
<u>วัตถุประสงค์</u>	เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงาน และไม่มี การแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ	
14.1 – ระบบการลงคะแนนใช้การควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อรับมือภัยคุกคามหรือช่องโหว่ด้านความมั่นคงปลอดภัย	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) และวิธีการควบคุมเพื่อรับมือหรือลดความเสี่ยงจากภัยคุกคามแต่ประเภทซึ่งอาจส่งผลกระทบต่อการทำงานของระบบการลงคะแนน รวมถึงอธิบายวิธีการควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อป้องกัน บรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน เช่น กระบวนการเข้ารหัสลับ (cryptography) การ	ระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) ตามมาตรฐาน ISO27001:2013 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 ตามลิงก์ที่แนบ (Link เอกสาร J VENTURES (27K-2013_RECERT_UKAS)_FULL_CER.PDF) โดยมีขอบเขตการประเมินความเสี่ยงด้านความปลอดภัยสารสนเทศ ประกอบด้วย การกำหนดประเภทของความเสี่ยง การจัดลำดับความสำคัญ ความรุนแรง ที่จะมีผลกระทบต่อทรัพยากรและการให้บริการของระบบสารสนเทศ พร้อมทั้งนำข้อมูล

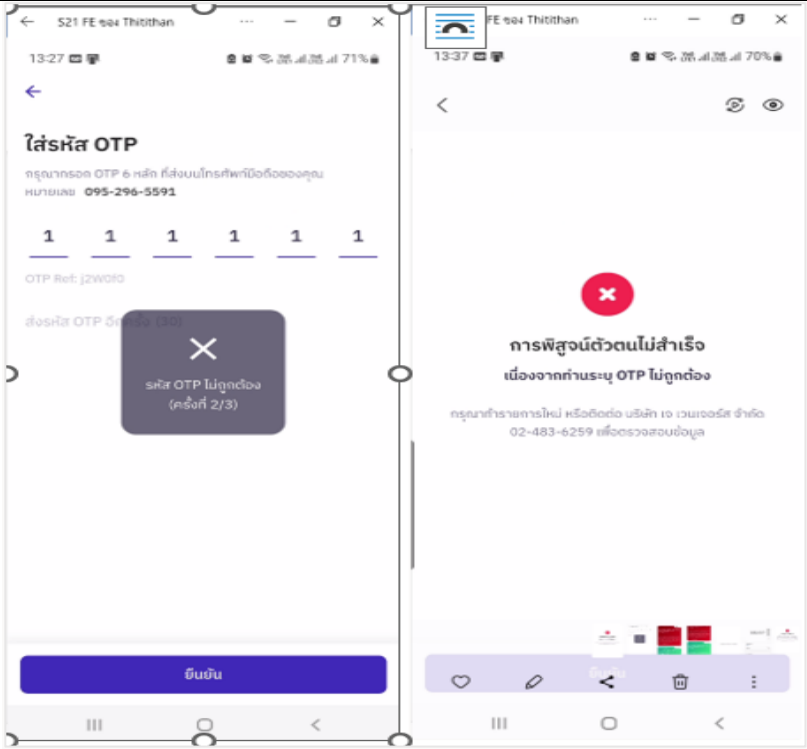
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ป้องกันมัลแวร์ (malware) การตั้งค่าไฟร์วอลล์ (firewall) และการตั้งค่าระบบ (system configurations)	ดังกล่าวมาบริหารจัดการเพื่อลดความเสี่ยงด้านความมั่นคงของระบบสารสนเทศ พร้อมทั้งดำเนินการเฝ้าระวัง และประเมินผล การจัดการความเสี่ยงด้านสารสนเทศเป็นระยะอย่างต่อเนื่อง ตลอดจนการปรับปรุงกระบวนการบริหารจัดการด้านความเสี่ยง สารสนเทศให้มีประสิทธิภาพมากยิ่งขึ้น ระบบมีการออกแบบสถาปัตยกรรมเครือข่าย โดยวิธีการควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อป้องกัน บรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน อีกทั้ง บริษัทฯ ได้มีการจัดทำ Security Configuration baseline ดังนี้ 1 user login mobile ผ่าน public internet 2. CloudFare 2.1.ทำหน้าที่ load balance, และ anti ddos และ ซ่อน ip ปลายทาง 2.2 ทำหน้าที่ dns server จะทำการถอดค่า dns name เป็น public IP ของ Jventures แล้วทำการส่ง package ไปให้ ปลายทางตามที่ระบุ 3. CSL Firewall – FortiGate มีหน้าที่ทำการตรวจสอบ incoming IP เพื่อ allow or not allow ตาม policy ที่ตั้งไว้ โดย จะทำการ scan VIRUS ทุกครั้ง 3.1. CSL = CS loxinfo Cloud Center 3.2 Jventures ทำการแบ่ง zone Production กับ UAT ดังรูป

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		รูป ตัวอย่าง Jventures Network Diagram
14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น	ระบบการลงคะแนนป้องกันการติดตั้งหรือการส่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง 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 Application ผ่าน FortiGate Firewall (NGFW รวม anti-virus and malware) นอกจากนั้นยังมีการ pen test, VA scan รวมทั้ง external IT Audit ทำการตรวจสอบทุกปี (EY) นอกจากนั้นยังใช้วิธีการ peer-to-peer สำหรับ review source code โดยมี Supervisor สุ่มตรวจสอบเป็นบางครั้ง
15. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring)		

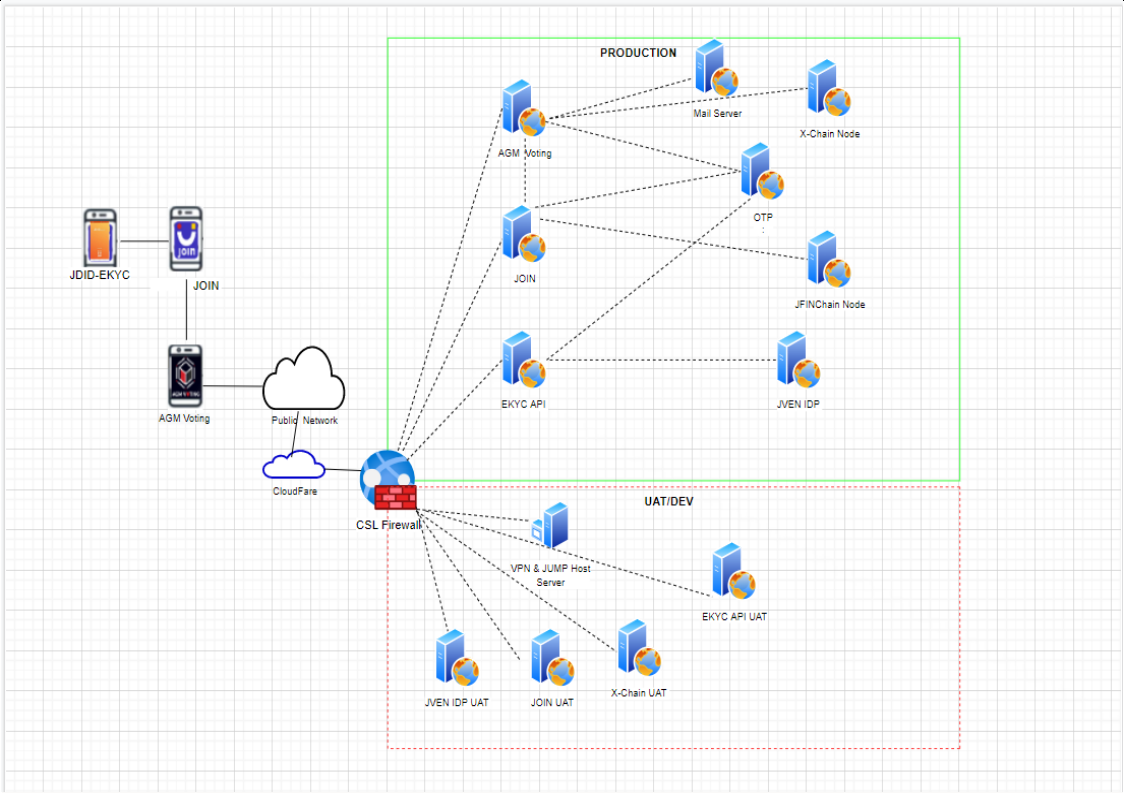
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
<u>วัตถุประสงค์</u>	เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน	
15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ	ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งประกอบด้วยเหตุการณ์ที่เกี่ยวข้องกับสถานะการทำงานและความผิดปกติของระบบการยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน การจัดการระบบเครือข่าย การจัดการซอฟต์แวร์ และฟังก์ชันการลงคะแนน เป็นอย่างน้อย	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) บริษัทได้กำหนดกระบวนการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศ มีการควบคุมการรักษาความปลอดภัย อย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล ISO27001:2013 ตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและไซเบอร์ (ISMS-02 Information Security_Cyber Policy) รูป ISO/IEC 27001:2013 The Operation of Information Security Management System for IT Platform Service, Software as a service and Digital ID Service

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน												
		ระบบการลงคะแนนสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนนได้ดังนี้ 1) สถานะการทำงานปกติ และความผิดปกติของระบบปฏิบัติการ ระบบเครือข่าย ระบบฐานข้อมูล และระบบการลงคะแนนอ ซึ่งบริษัทฯ ใช้ระบบ Zabbix monitor system ในเฝ้าสังเกตปัญหาที่เกิดขึ้นจากระบบ และส่งแจ้งเตือนผ่าน Line application Problem hosts <table><tr><th>Host group ▲</th><th>Without problems</th><th>With problems</th><th>Total</th></tr><tr><td>ACB Group</td><td>8</td><td>1</td><td>9</td></tr><tr><td>AGM Group</td><td>2</td><td></td><td>2</td></tr></table> รูปที่ 1 แสดงปัญหาที่เกิดขึ้นพบในการเฝ้าสังเกตผ่านระบบ Zabbix monitor system JVC-INFRA-NOTI (4) LINE Notify JVC-INFRA-NOTI: OK: Disk I/O is overloaded on LOAN-SUGGEST-PRD-01 Trigger: Disk I/O is overloaded on LOAN-SUGGEST-PRD-01 Trigger status: OK Trigger severity: Warning Trigger URL: Item values: 1. CPU iowait time (LOAN-SUGGEST-PRD-01:system.cpu.util[iowait]): 2.6 % 2. UNKNOWN (*UNKNOWN*:UNKNOWN): UNKNOWN 3. UNKNOWN (*UNKNOWN*:UNKNOWN): UNKNOWN Original event ID: 100156 LINE Notify JVC-INFRA-NOTI: OK: ACB-MCS-PRD-01 have logged in users Trigger: ACB-MCS-PRD-01 have logged in users Trigger status: OK Trigger severity: Information Trigger URL: Item values: 1. Logged in Users (Alert) (ACB-MCS-PRD-01:lastlogin.logged_in_users_alert): 0 2. UNKNOWN (*UNKNOWN*:UNKNOWN): UNKNOWN 3. UNKNOWN (*UNKNOWN*:UNKNOWN): UNKNOWN Original event ID: 100147 รูปที่ 2 แสดงการแจ้งเตือนผ่าน Line application	Host group ▲	Without problems	With problems	Total	ACB Group	8	1	9	AGM Group	2		2
Host group ▲	Without problems	With problems	Total											
ACB Group	8	1	9											
AGM Group	2		2											

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		2) ระบบมีการบันทึก Log การยืนยันตัวตนในการใช้งานระบบ และการเข้าถึงระบบของผู้ใช้งาน ใน Parse ตัวอย่างดังรูป  3) การจัดการระบบเครือข่าย สามารถเปิด และ ปิดการเชื่อมต่อระบบบน FortiGate Firewall (ถ้าจำเป็น) 4) การจัดการซอฟต์แวร์ user สามารถ download application ผ่าน app store และ play store และตั้งค่าตามมาตรฐานทั่วไปของระบบ 5) ผู้ดูแลระบบสามารถเปิดและปิดการลงคะแนนได้ผ่าน AGM Back office โดยผลของการลงคะแนนสามารถนำออก (export Logs) เป็น json และ csv file format
15.2 – ระบบการลงคะแนนมีการสร้างจัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ใช้งานในทันที บันทึกข้อผิดพลาดทั้งหมดที่เกิดขึ้น และสร้างรายงานข้อผิดพลาด (error report) รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการจัดการข้อผิดพลาดในระบบการลงคะแนน	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน จะมีการแจ้งข้อผิดพลาดที่หน้าจอของผู้ใช้งานทันที โดยมีตัวอย่างการแสดงความผิดพลาด Error ผ่าน Popup ดังรูปที่ 1 และจะรวบรวมข้อมูลจัดทำเป็นรายงานข้อผิดพลาด

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		 รูปที่ 1 ตัวอย่างการแสดงความ Error ผ่าน Popup ปัจจุบันผู้ดูแลระบบจะประจำ on site ตามการประชุม VOTING ทุกครั้ง ทำให้รับทราบปัญหาและทำการแก้ไขหน้างาน ส่วนส่วนรายงานข้อผิดพลาด จะจัดทำเป็นรายงาน error report
15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	ระบบการลงคะแนนต้องมีมาตรการป้องกันมัลแวร์ (malware) โดยระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ บันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ และบันทึกเหตุการณ์ของกิจกรรมการแก้ไขมัลแวร์ รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการอัปเดตมาตรการป้องกันมัลแวร์	ระบบการลงคะแนนมีการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware) อ้างอิง ISO27001-2013 หมายเลขเอกสาร ISMS-02 นโยบายการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและไซเบอร์ ดังนี้ 1. ผู้ดูแลระบบ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ 2. ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น thumb drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ 3. ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		4. ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลายถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ มีระบบ FortiGate Firewall เป็น Next-Generation Firewall security for full visibility and threat protection any times สำหรับป้องกัน malware ระบบบันทึกเหตุการณ์ที่ตรวจพบบน servers และเมื่อระบบตรวจพบไฟล์ที่มีไวรัส ระบบจะทำการบล็อกไวรัสดังกล่าวทันที ซึ่งตัวอย่าง Virus ที่ดักจับได้ เช่น PHP/Agent.RZ!tr ระบบมีการป้องกันโดยใช้ Fortinet – Best Practices Version 6.4.0 ซึ่งประกอบไปด้วย โปรแกรมป้องกันไวรัส โดยสามารถเปิดใช้งานเพื่อสแกนไวรัสสำหรับเครือข่ายที่ใช้งานทั้งหมด โดยใช้ FortiClient endpoint antivirus สแกนเพื่อป้องกันภัยคุกคามที่เข้ามาในเครือข่าย ซึ่งสมาชิก FortiGuard AntiVirus ต้องอัปเดตและกำหนดค่า FortiGate ของระบบซึ่งจะทำให้ได้รับการอัปเดตลายเซ็นของโปรแกรมป้องกันไวรัสทันทีที่พร้อมใช้งาน สามารถเปิดการใช้งานเฉพาะโปรโตคอลที่ต้องการตรวจสอบได้ ระบบสามารถทำการตรวจสอบและรายงานการป้องกันไวรัส รวมถึงข้อความบันทึกเป็นระยะๆ ระบบป้องกันการบุกรุก (IPS) สามารถตรวจพบทราฟฟิกที่พยายามใช้ช่องโหว่ นี้ อีกทั้ง IPS ยังอาจตรวจพบตอนที่ระบบติดไวรัส โดยการเปิดใช้งานการสแกน IPS ที่เครือข่ายทั้งหมด โดยใช้ FortiClient endpoint IPS สแกนเพื่อป้องกันภัยคุกคามที่เข้ามาในเครือข่ายของ ซึ่งสมาชิก FortiGuard IPS Updates ต้องอัปเดตและกำหนดค่า FortiGate ของระบบซึ่งจะทำให้ได้รับการอัปเดตลายเซ็นของโปรแกรมป้องกันไวรัสทันทีที่พร้อมใช้งาน ซึ่งเป็นสิ่งสำคัญในการป้องกันการโจมตีบริการที่เผยแพร่สู่สาธารณะ
15.4 – ระบบการลงคะแนนที่เชื่อมต่อเครือข่ายใช้วิธีการป้องกันการโจมตีทางเครือข่าย (network-based attack) ที่เหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของสถาปัตยกรรมระบบเครือข่าย (network architecture) ของ เครือ ข่ า ย คอมพิวเตอร์ภายใน (internal network) ของ ระบบการลงคะแนน และมีข้อมูลเกี่ยวกับวิธีการปิดใช้งานเครือข่ายไร้สาย (wireless network) ของระบบการลงคะแนน นอกจากนี้ เอกสารเกี่ยวกับระบบการลงคะแนนมีรายการการตั้งค่าความมั่นคงปลอดภัยของระบบเครือข่าย (security configuration) ที่สอดคล้องกับแนวปฏิบัติที่ดีในการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย เช่น NIST	1. ผู้ลงคะแนนเข้าใช้งานระบบบนมือถือ (mobile) ผ่าน public internet 2. CloudFare มีการใช้งาน load balance และ anti ddos อีกทั้งยังซ่อน IP ปลายทาง มีอุปกรณ์ dns server สำหรับถอดค่า DNS name เป็น public IP ของ Jventures แล้วทำการส่ง package ไปให้ปลายทางตามที่ระบุ 3. CSL Firewall – FortiGate มีหน้าที่ทำการตรวจสอบ incoming IP เพื่ออนุญาต หรือไม่อนุญาต IP ตาม policy ที่ตั้งไว้ โดย จะทำการ scan VIRUS ทุกครั้ง บริษัทมีการจัดทำ Security configuration baseline ซึ่งเป็นแนวทางการตั้งค่านโยบายความมั่นคงปลอดภัยโดยการจำกัดการเข้าถึง (least privilege) ซึ่งประกอบไปด้วยการไม่ให้สิทธิเกินหน้าที่และความจำเป็น การตรวจสอบความปลอดภัยในการเข้าถึงระบบของผู้ดูแลระบบ ซึ่งรวมถึง การติดตั้งการใช้งาน การกำหนดค่าในการบริหารทรัพยากร การกำหนดกลุ่มของผู้ใช้งาน และการใช้งานนโยบายการรักษาความมั่นคงปลอดภัย การดูแลระบบ Security Verify Access เกี่ยวข้องกับงานระดับสูงดังต่อไปนี้ การติดตั้งและกำหนดค่าในการบริหารทรัพยากร การกำหนดคุณลักษณะผู้ใช้งานที่สามารถเข้าถึงได้ ประเภทของการเข้าใช้งาน ระยะเวลาที่สามารถเข้าใช้งานได้ เงื่อนไขที่ต้องปฏิบัติตาม การควบคุมการเข้าถึงของผู้ใช้งานเฉพาะกลุ่ม Access Control List (ACL) การกำหนดกฎในการเข้าถึงของผู้ใช้งาน การอนุญาตให้เข้าถึงข้อมูล รายละเอียดตามรูป

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	Special Publication 800-44 Guidelines on Securing Public Web Servers	 รูป ตัวอย่าง Jventures Network Diagram ซึ่งการตั้งค่า Security Configuration นี้อ้างอิงตามเอกสาร ISO27001-2013 หมายเลขเอกสาร ISMS-02 นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและไซเบอร์ และเอกสาร Fortinet FortiOS - Best Practices version 6.4.0 ในการ setup Firewall