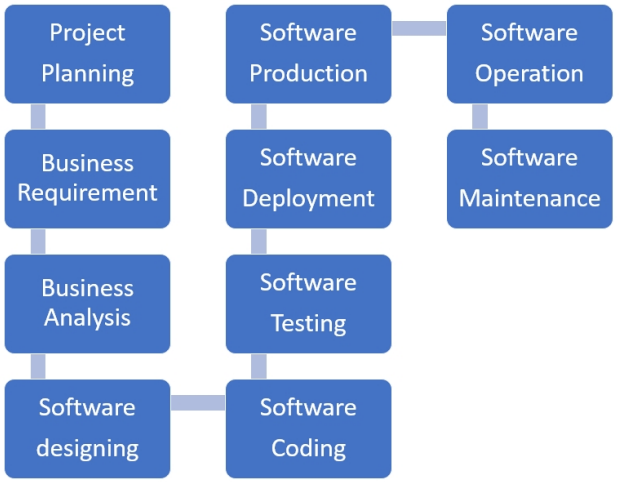
แบบประเมินความสอดคล้องด้วยตนเอง
ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ELECTRONIC VOTING SYSTEM)
ตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (ขมธอ. 26-2564) เวอร์ชัน 2.0

ชื่อระบบ	SpaceVote
ผู้ประเมินความสอดคล้องด้วยตนเอง (ชื่อบริษัท)	บริษัท วันสเปซ คอร์ปอเรชั่น จำกัด
ช่องทางการติดต่อผู้ให้บริการ	อีเมล hi@onespace.co.th, โทร. 02-257-7000
วันที่ประเมินความสอดคล้อง	21 มิ.ย. 66
วันที่ครบกำหนดการทบทวน	20 มิ.ย. 67
ประเภทของระบบการให้บริการ	☒ On Cloud ☐ On Premise ☐ อื่น ๆ โปรดระบุ
การใช้งานระบบการลงคะแนน	☒ ร่วมกับระบบการประชุมฯ ☒ แยกกับระบบการประชุมฯ
มาตรฐานที่ได้รับการรับรอง	☐ ISO/IEC 27001 ☐ ISO/IEC 27701 ☐ อื่น ๆ
ขอบข่ายการประเมินความสอดคล้องด้วยตนเอง	ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ SpaceVote ประกอบด้วยส่วนผู้ควบคุมระบบการลงคะแนน ที่สร้าง ควบคุม แก้ไข หัวข้อการลงคะแนน ออกรายงานผลรวมการลงคะแนน และส่วนผู้ลงคะแนน ที่ทำการลงคะแนน ตรวจสอบผลรวมการลงคะแนน และทำการยืนยันตัวตนก่อนการเข้าใช้งาน และส่วนการบันทึกผลการลงคะแนนบนบล็อกเชน

หมายเหตุ : สพธอ ไม่เกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
ข้อกำหนดเกี่ยวกับฟังก์ชันการทำงาน		
1. การออกแบบระบบ (System Design) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการออกแบบที่สามารถดำเนินการตามกระบวนการการลงคะแนนอย่างถูกต้อง ครบถ้วน และมีประสิทธิภาพ**		
1.1 – ระบบการลงคะแนนมีการออกแบบให้สอดคล้องตามกระบวนการลงคะแนนที่กฎหมายหรือหลักเกณฑ์กำหนด	ระบบการลงคะแนนมีฟังก์ชันการทำงานที่จำเป็นตามกระบวนการลงคะแนนที่ กฎหมายหรือหลักเกณฑ์กำหนด ซึ่งครอบคลุมการเตรียมข้อมูลสำหรับการลงคะแนน การตรวจสอบระบบการลงคะแนนก่อนการลงคะแนน การเปิดลงคะแนน การลงคะแนน การส่งผลลงคะแนน การปิดลงคะแนน การนับคะแนน และการรายงานผลรวมของการลงคะแนน	ระบบการลงคะแนน SpaceVote มีการออกแบบฟังก์ชันการทำงานที่จำเป็นตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วย ระบบการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ ของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ดังนี้ - ฟังก์ชันการเตรียมข้อมูลสำหรับลงคะแนน - ฟังก์ชันการเปิดลงคะแนน - ฟังก์ชันการลงคะแนน - ฟังก์ชันการส่งผลลงคะแนน - ฟังก์ชันการปิดลงคะแนน - ฟังก์ชันการนับคะแนน - ฟังก์ชันการรายงานผลรวมของการลงคะแนน ในรูปแบบของ Dashboard และไฟล์

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		เอกสาร ทั้งนี้ ระบบการลงคะแนนมีฟังก์ชั่น Service Check ตรวจสอบการทำงานในส่วนต่าง ๆ ของระบบ ตลอดการทำงาน โดยจะมีแจ้งเตือนผ่าน Line Notify ของทีมดูแลระบบ และแจ้งเตือนผู้ใช้ผ่าน Web Portal
1.2 – ระบบการลงคะแนนมีการออกแบบให้ทำงานอย่างถูกต้องในสภาวะการทำงานจริง	ระบบการลงคะแนนมีการตรวจสอบความถูกต้องน่าเชื่อถือ (system accuracy and reliability) การทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด (maximum volume) ในสภาวะที่ใกล้เคียงกับการใช้งานจริงในกระบวนการลงคะแนน และการทดสอบสมรรถนะการทำงานของระบบในภาวะวิกฤต (stress testing)	ระบบการลงคะแนนมีการทดสอบ ดังนี้ - ระบบมีการทดสอบขีดความสามารถของระบบในการรองรับปริมาณธุรกรรมสูงสุด โดยทำการ Load Testing จำลองการใช้งานจริงในกระบวนการลงคะแนน โดยสามารถรองรับ transaction สูงสุด 25,000 ต่อวินาที คือการรับรองคนเข้าลงคะแนนพร้อมกันทั้งหมด 25,000 คนต่อวินาที - ระบบมีการจัดทำ Testcase ในทุกฟังก์ชั่นทั้งหมดของระบบการลงคะแนน
1.3 – ระบบการลงคะแนนมีการทดสอบคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำรายงานผลการทดสอบระบบ (test report) ที่ดำเนินการโดยผู้ทดสอบซอฟต์แวร์ (software tester) ของผู้พัฒนาระบบการลงคะแนน	ระบบ SpaceVote มีการจัดทำ Testcase รายงานผลการทดสอบโดยดำเนินการทดสอบด้วย ทีม software tester ภายในองค์กรเพื่อยืนยันคุณสมบัติว่าเป็นไปตามที่ระบุไว้ในการออกแบบระบบ
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)	ระบบการลงคะแนนมีการพัฒนาตามมาตรฐาน ISO/IEC 29110: Systems and Software Life Cycle Profiles and Guidelines for Very Small Entities (VSEs) ซึ่งเป็นบริษัทขนาดเล็ก ได้พัฒนาตามลำดับขั้นดังนี้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		
2.2 – โครงสร้างของระบบการลงคะแนนเป็นแบบแยกส่วน(modular)	ระบบการลงคะแนนมีการออกแบบโครงสร้างเป็นแบบแยกส่วน โดยแต่ละส่วนหรือโมดูล (module) มีฟังก์ชันการทำงานเฉพาะที่สามารถทดสอบและตรวจสอบได้โดยไม่ขึ้นกับส่วนที่เหลือ	ระบบการลงคะแนนมีการออกแบบการทำงานแยกเป็นส่วนต่าง ๆ ผ่าน API ดังนี้ - ส่วนหัวข้อการลงคะแนน - ส่วนตัวเลือกการลงคะแนน - ส่วนกระบวนการลงคะแนน - ส่วนผลการลงคะแนน - ส่วนผู้ใช้งานในระบบ
2.3 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ของกระบวนการและข้อมูลในซอฟต์แวร์	กระบวนการและข้อมูลของระบบการลงคะแนนใช้แนวปฏิบัติที่ดีสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ดที่มีความมั่นคงปลอดภัย ซึ่งไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้ (self-modifying code)	ระบบการลงคะแนนมีกระบวนการและแนวปฏิบัติสำหรับการรักษาความครบถ้วนของซอฟต์แวร์และการเขียนซอร์สโค้ด ดังนี้ - มีการใช้ ซอฟต์แวร์ควบคุม Container ในการ deploy ระบบในแต่ละ version - มีการใช้ Git: Version Control เฉพาะขององค์กร เพื่อใช้สำหรับ ติดตาม ตรวจสอบ พัฒนา และแก้ไขซอร์ซโค้ด ให้เป็นไปตามแนวปฏิบัติที่ดี และมีความปลอดภัย ไม่เป็นโค้ดที่สามารถแก้ไขตัวเองได้
2.4 – ระบบการลงคะแนนจัดการข้อผิดพลาดและกู้คืนจากความล้มเหลวได้อย่างมีประสิทธิภาพ	ระบบการลงคะแนนมีความสามารถจัดการและกู้คืนจากข้อผิดพลาด รวมถึงความล้มเหลวในการทำงานของอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องกับระบบการลงคะแนน	ระบบการลงคะแนนทำงานอยู่บนคลาวด์ของ INET ที่รับประกันมาตรฐาน SLA 99.90% มีการออกแบบ infrastructure เพื่อให้ระบบสามารถทำงานได้ในกรณีที่มีอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้องเกิดการผิดพลาด และยังมีการจัดทำ Backup โดยทำการ Snapshot VM ไว้เพื่อสำรองข้อมูล และมีการทดสอบ Restore Snapshot VM ที่ได้ Backup ไว้เพื่อเป็นการยืนยันว่าข้อมูลที่ Backup สามารถนำมากู้คืนระบบได้จริง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
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)	ระบบ SpaceVote มีการจัดทำเอกสารเกี่ยวกับระบบซึ่งรวบรวมรายละเอียดทั้งหมดโดยแยกเป็นหมวดหมู่ดังนี้ (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)
3.2 – ข้อมูลกระบวนการและธุรกรรมที่เกี่ยวข้องกับระบบการลงคะแนน เตรียมไว้พร้อมสำหรับการตรวจสอบระบบ	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการตรวจสอบ (inspection) ว่าระบบการลงคะแนนได้รับ<u>การติดตั้งและตั้งค่า</u>อย่างถูกต้อง และวิธีการเฝ้าระวังการทำงานของระบบ	ระบบ SpaceVote ให้บริการผ่าน Web Portal (Software as a Serivce) ผู้ใช้ไม่จำเป็นต้องทำการติดตั้งแอปพลิเคชัน installation หรือตั้งค่าระบบใด ๆ อย่างไรก็ตามจะมีเอกสารสำหรับตรวจสอบการตั้งค่าระบบ รวมถึงการทดสอบการทำงาน เพื่อตรวจสอบการลงคะแนนเสียงอย่างถูกต้องตามที่ต้องการ
3.3 – บุคคลที่เกี่ยวข้องกับระบบการลงคะแนนสามารถเข้าใจและตรวจสอบการทำงานของระบบการลงคะแนนได้ตลอดกระบวนการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนจัดทำเอกสารที่อธิบายวิธีการบันทึกเหตุการณ์ (event logging) ของระบบการลงคะแนน และรูปแบบของบันทึกเหตุการณ์ (log format)	ระบบ SpaceVote มีเอกสารอธิบายบันทึก log ของระบบการลงคะแนน ซึ่งมีการจัดเก็บข้อมูลเกี่ยวกับเหตุการณ์ที่ผู้ใช้กระทำกับระบบทั้งหมด โดยมีบันทึกเหตุการณ์ event log การเข้าใช้งานของระบบ โดยจะมีการบันทึก log ทุกครั้งที่มีการเรียกใช้ Service API ของระบบการลงคะแนน และจัดเก็บข้อมูลลงบนฐานข้อมูล MongoDB ในรูปแบบ JSON โดยมีรูปแบบ (log format) ดังภาพ

<table>
<tr><th>ข้อกำหนด</th><th>คำอธิบาย</th><th>ความสามารถของระบบการลงคะแนน</th></tr>
<tr><td></td><td></td><td><pre>{
    "_id" : ObjectId("641a087b02df302ee787d1a5"),
    "user_type" : "",
    "request_user" : {
        "user_id" : "81[redacted]"
    },
    "request_data" : {
        "choice_selected" : [
            {
                "name" : "ไม่เห็นด้วย",
                "key" : "2",
                "value" : NumberInt(1),
                "description" : ""
            }
        ]
    },
    "event_path" : "/voting-transaction/create-update",
    "status" : "Success",
    "ip_address" : "1[redacted]",
    "status_detail" : "",
    "created_at " : ISODate("2023-03-21T23:41:47.927+0000")
}</pre>รูปที่ 1 ภาพบันทึก log ของระบบการลงคะแนน</td></tr>
<tr><td colspan="3">4. การเข้าถึงอย่างเท่าเทียม (Equitable Access)
<u>วัตถุประสงค์</u> เพื่อให้ผู้ลงคะแนนสามารถใช้งานระบบการลงคะแนนได้อย่างสอดคล้องและเท่าเทียม</td></tr>
<tr><td>4.1 – ผู้ลงคะแนนมีประสบการณ์ใช้งานที่สอดคล้องกันตลอดกระบวนการลงคะแนนด้วยวิธีการลงคะแนนทุกรูปแบบ</td><td>ในวิธีการลงคะแนนผ่านสื่ออิเล็กทรอนิกส์ (เช่น การลงคะแนนผ่านคอมพิวเตอร์ หรือการลงคะแนนผ่านโทรศัพท์เคลื่อนที่) ผู้ลงคะแนนต้องเข้าถึงรูปแบบการแสดงผล (display format) (รวมถึงการแสดงภาพและเสียง) และรูปแบบการมีปฏิสัมพันธ์ (interaction mode) (เช่น การคลิกปุ่ม การแตะสัมผัสบนหน้าจอ) ในลักษณะที่สอดคล้องกัน</td><td>ระบบการลงคะแนนมีการแสดงผลแบบ Web Responsive ซึ่งสามารถเข้าใช้งานผ่าน Browser ปัจจุบัน เช่น Google Chrome, Microsoft Edge, Safari, Firefox Web โดย ผู้ลงคะแนนจะได้รับประสบการณ์ใช้งานที่สอดคล้องกันตลอดการลงคะแนน ทั้งในการลงคะแนนผ่านคอมพิวเตอร์ หรือผ่านโทรศัพท์เคลื่อนที่</td></tr>
<tr><td>4.2 – ผู้ลงคะแนนได้รับข้อมูลและตัวเลือกลงคะแนนที่เท่าเทียมกันในการลงคะแนนทุกรูปแบบ</td><td>รูปแบบการแสดงผล (display format) แสดงข้อมูลและตัวเลือกลงคะแนนทั้งหมดที่เกี่ยวข้องกับการลงคะแนนอย่างเท่าเทียมกัน และไม่ทำให้เกิดอคติกับตัวเลือกลงคะแนนใด ๆ ที่นำเสนอต่อผู้ลงคะแนน เช่น ตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน</td><td>ระบบการลงคะแนนออกแบบให้ตัวเลือกลงคะแนนทั้งหมดแสดงผลด้วยแบบอักษรที่มีขนาด สี และลักษณะเหมือนกัน</td></tr>
</table>

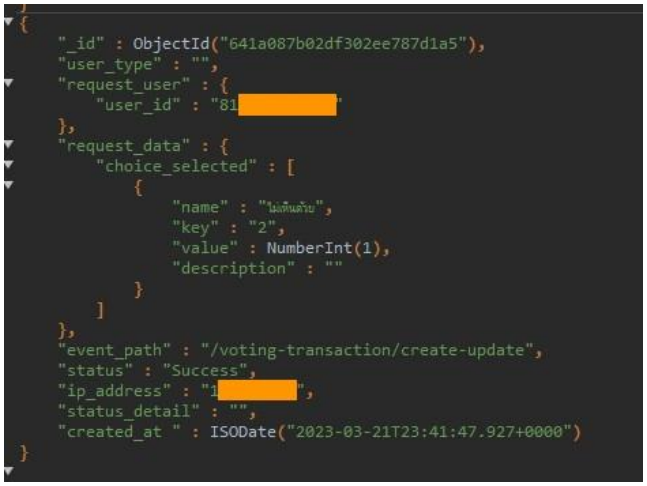
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
5. การลงคะแนนตรงตามเจตนา (Cast as Intended) **<u>วัตถุประสงค์</u> เพื่อให้การแสดงข้อมูลและตัวเลือกลงคะแนนมีการแสดงผลที่มองเห็นชัดเจน เข้าใจได้ และดำเนินการได้ และผู้ลงคะแนนทุกคนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้**		
5.1 – ระบบการลงคะแนนมีการตั้งค่าเริ่มต้นให้สามารถใช้งานได้เหมาะสมที่สุดกับผู้ลงคะแนน และผู้ลงคะแนนสามารถปรับการตั้งค่าส่วนบุคคล (preference setting) ให้ตรงกับความต้องการของผู้ลงคะแนน	ระบบการลงคะแนนมีการตั้งค่าเริ่มต้น (default setting) ที่เหมือนกันสำหรับผู้ลงคะแนนทุกคนในครั้งแรก และการตั้งค่าส่วนบุคคล (preference setting) ตามความต้องการของผู้ลงคะแนน เช่น การปรับขนาดตัวอักษร และสีของภาพ	ระบบการลงคะแนน SpaceVote ยังไม่ได้มีการตั้งค่าส่วนบุคคล (preference setting) ในส่วนของการปรับขนาดตัวอักษร และสีของภาพ แต่มีการตั้งค่าเริ่มต้นที่สามารถใช้งานได้ ดังนี้ 1. ผู้ใช้งานสามารถเห็นเฉพาะหัวข้อลงคะแนนที่มีสิทธิ์ลงคะแนนเท่านั้น 2. สามารถลงคะแนนได้ 3. สามารถให้ความเห็นในระหว่างการลงคะแนนได้ 4. สามารถดูผลรวมการลงคะแนนได้หลังประกาศผลการลงคะแนน 5. ดูรายการที่ได้ลงคะแนนทั้งหมดย้อนหลังได้
5.2 – ผู้ลงคะแนนสามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนนและการส่งผลลงคะแนนได้โดยตรง	ในระหว่างการลงคะแนน ผู้ลงคะแนนสามารถควบคุมการลงคะแนนของตนเองได้โดยตรง เช่น รูปแบบการแสดงผลของข้อมูล (display format) การเลือกหรือเปลี่ยนตัวเลือกลงคะแนน การเปลี่ยนหน้าจอไปหน้าถัดไป/ก่อนหน้า การเลื่อนหน้าจอขึ้น/ลง และการใช้ท่าทางสัมผัสบนหน้าจอ (touch screen gestures) รวมถึงระบบการลงคะแนนมีการควบคุมเพื่อป้องกันการเปิดใช้งานโดยไม่ตั้งใจ (accidental activation) เช่น การให้ผู้ลงคะแนนยืนยันเจตนาในการลงคะแนนก่อนส่งผลลงคะแนน หรือการแจ้งสถานะของการลงคะแนนให้ผู้ลงคะแนนทราบ	ระบบการลงคะแนนออกแบบให้ผู้ลงคะแนนสามารถ สามารถควบคุมการเปลี่ยนตัวเลือกลงคะแนน การแสดงความคิดเห็น การส่งผลลงคะแนน ได้โดยตรง และมีแจ้งเตือนให้ยืนยันอีกครั้งก่อนส่งผลลงคะแนน เพื่อยืนยันเจตนาในการลงคะแนนของผู้ใช้
5.3 – ผู้ลงคะแนนสามารถเข้าใจข้อมูลทั้งหมดเกี่ยวกับการลงคะแนนตามที่เสนอ รวมถึงกฎกติกาของการลงคะแนน คำแนะนำ ข้อความจากระบบ และข้อความแสดงข้อผิดพลาด	ระบบการลงคะแนนมีการแสดงข้อมูลทั้งหมดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน คำแนะนำ และข้อความจากระบบด้วยภาษาที่ชัดเจนและอ่านง่าย การวางตำแหน่งข้อความที่ไม่ให้เกิดความสับสนในการลงคะแนน การแจ้งจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนมีสิทธิเลือก การแจ้งเตือนผู้ลงคะแนนถึงข้อผิดพลาดในการลงคะแนนก่อนจะส่งผลลงคะแนน (เช่น การพยายามเลือกตัวเลือกมากกว่าจำนวนที่อนุญาต หรือการเลือกตัวเลือกน้อยกว่าจำนวนที่อนุญาต) และการ	ระบบการลงคะแนน มีการแสดงข้อมูลรายละเอียดเกี่ยวกับการลงคะแนน กฎกติกาของการลงคะแนน และคำแนะนำ ผ่าน web portal ในส่วนของหน้าลงคะแนน โดยทางผู้ควบคุมระบบการลงคะแนนสามารถกำหนดข้อความและรายละเอียดต่าง ๆ ได้ด้วยตนเองผ่าน web portal สำหรับผู้ควบคุมระบบการลงคะแนน ระบบการลงคะแนนมีการวางตำแหน่งข้อความในส่วนต่าง ๆ อย่างชัดเจน มีข้อความแสดงจำนวนตัวเลือกสูงสุดที่ผู้ลงคะแนนสามารถเลือกได้ มีการเปลี่ยนของสีตัวเลือกที่ผู้ลงคะแนนได้กดเลือกไว้แล้ว เพื่อให้เกิดความแตกต่างอย่างชัดเจน และเมื่อผู้ลงคะแนนกดส่งผลคะแนน ระบบจะมีแจ้งเตือน popup เพื่อให้ผู้ลงคะแนนยืนยันอีกครั้งในการส่งผลคะแนน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	แสดงข้อความให้ผู้ลงคะแนนทราบเมื่อลงคะแนนสำเร็จแล้ว นอกจากนี้ ระบบมีการแสดงคำแนะนำและข้อความที่ชัดเจนสำหรับผู้ควบคุมระบบการลงคะแนนในการปฏิบัติงานและการบำรุงรักษาระบบ	โดยผู้ลงคะแนนสามารถกด ยกเลิก เพื่อกลับไปเปลี่ยนตัวเลือกลงคะแนน หรือ กดยืนยันเพื่อส่งผลคะแนน โดยหลังจากกดยืนยันส่งผลคะแนน ระบบจะมี popup แจ้งเตือนการลงคะแนนสำเร็จ และแจ้งเตือนข้อผิดพลาด ในกรณีลงคะแนนไม่สำเร็จ ในส่วนของผู้ควบคุมระบบการลงคะแนน ระบบไม่มีส่วนการแสดงคำแนะนำในการใช้งาน แต่มีการจัดทำคู่มือการใช้งานสำหรับผู้ควบคุมระบบการลงคะแนน
6. **ความเหมาะสมต่อการใช้งาน (Usable)** **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการประเมินให้สามารถใช้งานได้อย่างเหมาะสม**		
6.1 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ลงคะแนนที่จะใช้ระบบการลงคะแนน เพื่อให้มั่นใจว่าระบบการลงคะแนนสามารถใช้งานกับผู้คะแนนทุกคน (ซึ่งอาจรวมถึงผู้สูงอายุและบุคคลที่มีความบกพร่องทางการมองเห็น) ได้อย่างเหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี เช่น มาตรฐาน Web Content Accessibility Guidelines (WCAG) 2.0 ของ World Wide Web Consortium (W3C)	ระบบการลงคะแนนมีการทดสอบความเหมาะสมต่อการใช้งาน โดยอ้างอิงตามกลุ่มเป้าหมายของผู้ใช้งานระดับองค์กร ซึ่งได้ทำการทดสอบกับบุคลากรในองค์กรชาวไทยที่มีช่วงอายุ 22- 55 ปี จำนวน 50 ท่าน ทำการทดสอบในส่วนของผู้ลงคะแนน โดยผลการทดสอบสามารถทำความเข้าใจ และใช้งานได้อย่างเหมาะสม ปัจจุบันระบบไม่รองรับการใช้งานสำหรับผู้ทุพพลภาพบางประเภท เช่น ผู้ใช้ที่มีความบกพร่องทางสายตา
6.2 – ระบบการลงคะแนนผ่านการประเมินความเหมาะสมต่อการใช้งานกับผู้ควบคุมระบบการลงคะแนน	ผู้พัฒนาระบบการลงคะแนนมีการประเมินหรือทดสอบความเหมาะสมต่อการใช้งาน (usability) กับผู้ควบคุมระบบการลงคะแนน ในการตั้งค่าระบบ การทำงานในระหว่างการลงคะแนน และการปิดระบบ เพื่อแสดงให้เห็นว่าผู้ควบคุมระบบการลงคะแนนสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ	ระบบการลงคะแนนมีการทดสอบความเหมาะสมต่อการใช้งานด้วยทีมทดสอบ ภายในองค์กร ซึ่งมีการทดสอบการใช้งานแยกเฉพาะส่วนของผู้ควบคุมระบบการลงคะแนนเพื่อให้ผู้ใช้งานในส่วนของผู้ควบคุมสามารถทำความเข้าใจและปฏิบัติงานได้สำเร็จ
ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ		
6. การทำงานร่วมกัน (Interoperable) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการออกแบบที่รองรับการทำงานร่วมกันกับระบบภายนอก ส่วนประกอบภายในระบบ และข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนน**		
7.1 – ข้อมูลที่เกี่ยวข้องกับระบบการลงคะแนนอยู่ในรูปแบบที่ทำงานร่วมกันได้หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการลงคะแนนที่นำเข้า ส่งออก หรือใช้รายงาน รวมถึงบันทึกเหตุการณ์ (log) อยู่ในรูปแบบที่ทำงานร่วมกันได้ (interoperable format) หรือรูปแบบมาตรฐาน	ข้อมูลทั้งหมดของระบบการคะแนนอยู่ในรูปแบบ JSON ซึ่งอยู่ในรูปแบบที่สามารถทำงานร่วมกันได้ - ระบบนำเข้าในรูปแบบ JSON ผ่านทาง Service API ของระบบ - ระบบส่งออกข้อมูลรายงานผลรวมการลงคะแนนในรูปแบบ xlsx ได้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		- ระบบเก็บบันทึกเห็นการณ์ (log) ในรูปแบบ JSON
7.2 – ระบบการลงคะแนนใช้วิธีการเชื่อมต่อฮาร์ดแวร์และวิธีการติดต่อสื่อสารในรูปแบบมาตรฐาน	วิธีการเชื่อมต่อฮาร์ดแวร์ (hardware interface) และวิธีการติดต่อสื่อสาร (communication protocol) ใช้รูปแบบมาตรฐาน ในการเชื่อมต่อกับระบบภายนอกหรืออุปกรณ์ต่าง ๆ	ระบบการลงคะแนนใช้ผ่านเว็บเบราว์เซอร์ ซึ่งไม่มีการเชื่อมต่อกับฮาร์ดแวร์ หรืออุปกรณ์ภายนอกอื่น ๆ
7. การตรวจสอบ (Auditable) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีหลักฐานสำหรับการตรวจสอบความถูกต้องของผลลงคะแนน**		
8.1 – ผลลงคะแนนสามารถตรวจพบการเปลี่ยนแปลงได้หากมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน	ผลลงคะแนนที่ได้จากการลงคะแนนของผู้ลงคะแนน มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูลได้ (tamper-evidence) ระบบการลงคะแนนเปิดโอกาสให้ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลลงคะแนนที่เลือกไป แจ้งข้อผิดพลาดในผลลงคะแนนที่เกิดจากระบบการลงคะแนน และเริ่มต้นลงคะแนนใหม่หากต้องการแก้ไขข้อผิดพลาดที่พบในผลลงคะแนน (ขึ้นอยู่กับกฎหมายหรือหลักเกณฑ์ที่กำหนด) รวมถึงควรมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ระบบการลงคะแนนต้องสร้างรายงานที่จะช่วยให้ผู้ตรวจสอบภายนอก (external auditor) สามารถตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง รวมถึงผู้พัฒนาระบบการลงคะแนนจัดทำขั้นตอนสำหรับการตรวจสอบว่าผลลงคะแนนถูกนำไปนับคะแนนเป็นผลรวมของการลงคะแนนอย่างถูกต้อง	- ระบบการลงคะแนนมีการบันทึกหลักฐานการลงคะแนนไว้ในบล็อกเชนซึ่งออกแบบให้ไม่สามารถเปลี่ยนแปลงข้อมูลได้ - ระบบการลงคะแนนมีการจัดเก็บหลักฐานการลงคะแนนในฐานข้อมูล และ log ซึ่งหากมีการแก้ไขผลคะแนน สามารถตรวจพบการเปลี่ยนแปลงโดยเปรียบเทียบข้อมูลจากฐานข้อมูล หรือ log กับ ข้อมูลที่อยู่บนบล็อกเชน - ผู้ลงคะแนนสามารถตรวจสอบความถูกต้องของผลการลงคะแนนได้ผ่านรายงานผลการลงคะแนนบน Web Portal ลงคะแนน - ระบบการลงคะแนนมีช่องทางให้ผู้ลงคะแนนแจ้งเหตุขัดข้องที่เกิดขึ้นในระหว่างการลงคะแนน ผ่านการส่งข้อความบน Web Portal ลงคะแนน หรือผ่านช่องทาง Call Center จากเบอร์โทรที่ระบุบน Web Portal ลงคะแนน - ระบบสามารถสร้าง/ดึงรายงานที่สามารถให้ผู้ตรวจสอบภายนอกตรวจสอบได้ในการลงคะแนนทุกครั้ง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
8. ความเป็นส่วนตัวของผู้ลงคะแนน (Voter Privacy) [1] **<u>วัตถุประสงค์</u> เพื่อให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัวและด้วยตนเอง**		
9.1 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้อย่างเป็นส่วนตัว	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ โดยไม่แสดงหรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลอื่นในระหว่างการลงคะแนน เพื่อรักษาความเป็นส่วนตัวของผู้ลงคะแนน	- ผู้เข้าร่วมลงคะแนนต้องยืนยันตัวตนผ่านรหัสผู้ใช้งาน (username, password) หรือ ผ่านเบอร์โทรศัพท์โดยมีการยืนยัน OTP ซึ่งจะเป็นการลงคะแนนส่วนตัวเฉพาะบุคคล - เฉพาะผู้ควบคุมระบบการลงคะแนนที่ได้สร้างหัวข้อลงคะแนนเท่านั้นที่สามารถดูคะแนนของแต่ละคนได้หากเป็นการลงคะแนนแบบเปิดเผย กรณีเป็นลงคะแนนลับจะดูได้เฉพาะคะแนนเสียงเท่านั้น
9.2 – ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ด้วยตนเอง โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น	ระบบการลงคะแนนมีการออกแบบให้ผู้ลงคะแนนสามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนนได้ ตามรูปแบบการตั้งค่าส่วนบุคคล (preference settings) ของผู้ลงคะแนน โดยไม่จำเป็นต้องอาศัยความช่วยเหลือจากบุคคลอื่น เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน	ในส่วนของการลงคะแนน ผู้ลงคะแนน สามารถทำเครื่องหมายลงคะแนน ตรวจสอบตัวเลือกลงคะแนน และส่งผลลงคะแนน ได้ด้วยตนเอง ตามรูปแบบการตั้งค่าเริ่มต้นของเว็บเบราว์เซอร์นั้น ๆ ของผู้ลงคะแนน โดยต้องมีการเข้าสู่ระบบด้วย ชื่อผู้ใช้ และรหัสผ่าน หรือเบอร์โทรศัพท์ พร้อมกับระบุรหัสที่ได้รับจาก SMS OTP เพื่อยืนยันตัวตนก่อนลงคะแนน เพื่อป้องกันบุคคลอื่นแทรกแซงการลงคะแนนของผู้ลงคะแนน
9. ความลับของคะแนนเสียง (Vote Secrecy) **<u>วัตถุประสงค์</u> (กรณีการลงคะแนนลับ) เพื่อให้ระบบการลงคะแนนมีการรักษาความลับในการลงคะแนนของผู้ลงคะแนน**		
10.1 – ระบบการลงคะแนนมีการรักษาความลับของผลลงคะแนนตลอดกระบวนการลงคะแนน	ระบบการลงคะแนนต้องไม่นำข้อมูลส่วนบุคคลของผู้ลงคะแนน เช่น ชื่อบุคคล ที่อยู่ หรือเลขประจำตัว มาประมวลผล จัดเก็บ หรือแสดงในลักษณะที่เชื่อมโยงกับผลลงคะแนนของผู้ลงคะแนนดังกล่าว	ระบบการลงคะแนนรองรับการลงคะแนนลับ ซึ่งจะไม่จัดเก็บและแสดงข้อมูลส่วนบุคคลของผู้ลงคะแนนไว้ในระบบ
10.2 – ระบบการลงคะแนนไม่จัดทำข้อมูลเกี่ยวกับผู้ลงคะแนนหรือข้อมูลอื่น ๆ ที่สามารถใช้เชื่อมโยงอัตลักษณ์ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน	ระบบการลงคะแนนต้องไม่มีการเชื่อมโยงโดยตรง (direct voter association) ระหว่างอัตลักษณ์ (identity) ของผู้ลงคะแนนกับผลลงคะแนนของผู้ลงคะแนน นอกจากนี้ ผลลงคะแนนและผลรวมของการลงคะแนนต้องไม่มีข้อมูลที่ระบุตัวผู้ลงคะแนนและข้อมูลที่สามารถใช้หาลำดับของการส่งผลลงคะแนนได้ อย่างไรก็ตาม ในกรณีที่ให้ผู้ลงคะแนนส่งผลลงคะแนนก่อนจะตรวจสอบการมีสิทธิลงคะแนนของผู้ลงคะแนน ระบบการลงคะแนน<u>สามารถใช้การเชื่อมโยงโดยอ้อม</u> (indirect voter association) ที่	ระบบการลงคะแนนรองรับการลงคะแนนลับ การลงคะแนนลับระบบจะใช้การเชื่อมโยงโดยอ้อมเพื่อตรวจสอบสิทธิ์การลงคะแนน แต่ไม่ได้จัดเก็บข้อมูลส่วนบุคคลของผู้ลงคะแนนผลคะแนนจึงไม่สามารถเชื่อมโยงโดยตรงระหว่างผู้ลงคะแนนกับผลคะแนนได้

[1] ความเป็นส่วนตัวของผู้ลงคะแนน ในที่นี้หมายถึง ความเป็นส่วนตัวที่เกิดขึ้นภายในระบบการลงคะแนนเท่านั้น

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	เชื่อมโยงผู้ลงคะแนนกับผลลงคะแนนที่ถูกเข้ารหัสลับไว้ โดยหลังจากตรวจสอบแล้วว่าผู้ลงคะแนนมีสิทธิลงคะแนน ระบบการลงคะแนนต้องลบการเชื่อมโยงโดยอ้อมระหว่างผู้ลงคะแนนกับผลลงคะแนนออก จากนั้น จึงถอดรหัสลับผลลงคะแนนที่ถูกเข้ารหัสลับและนำไปนับคะแนนเป็นผลรวมของการลงคะแนน	
10. การควบคุมการเข้าถึง (Access Control) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการยืนยันตัวตนของผู้ใช้งานและการควบคุมการเข้าถึงให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้น**		
11.1 – ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน	ระบบการลงคะแนนมีการบันทึกกิจกรรมและการเข้าถึงของบัญชีผู้ใช้งานที่เกิดขึ้นในระบบการลงคะแนน เพื่อให้มีหลักฐานสำหรับตรวจสอบในกรณีที่มีข้อผิดพลาดหรือภัยคุกคามเกิดขึ้น ระบบการลงคะแนนป้องกันไม่ให้มีการปิดใช้งาน เปลี่ยนแปลงแก้ไขโดยไม่สามารถตรวจพบได้ และลบบันทึกเหตุการณ์ (log) เพื่อรักษาความครบถ้วน (integrity) ของบันทึกเหตุการณ์ รวมถึงระบบการลงคะแนนให้สิทธิผู้ควบคุมระบบการลงคะแนนในการเข้าถึงบันทึกเหตุการณ์ เพื่อให้สามารถตรวจสอบและทบทวนสิทธิการเข้าถึงอย่างต่อเนื่อง	ระบบการลงคะแนนมีการบันทึกกิจกรรม และการเข้าถึงของบัญชีผู้ใช้งาน ในรูปแบบของ log ในฐานข้อมูลเพื่อเป็นหลักฐานในการตรวจสอบดังรูป  รูปที่ 1 แสดง log เข้าสู่ระบบ  รูปที่ 2 log การลงคะแนน

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		- ระบบมีการจัดเก็บ Logs การเข้าใช้งานของแต่ละ User ว่าเข้ามาใช้งานเมื่อไร จาก IP ไหน เพื่อสามารถตรวจสอบย้อนหลังได้ - ระบบการลงคะแนนจะเก็บบันทึก Logs ทั้งหมด บนที่เก็บข้อมูลที่ไม่สามารถเปลี่ยนแปลงหรือลบได้
11.2 – ระบบการลงคะแนนมีการจำกัดสิทธิของผู้ใช้งานและบทบาทของผู้ใช้งาน ในการเข้าถึงฟังก์ชันการทำงานและข้อมูลที่เฉพาะเจาะจงตามสิทธิการเข้าถึงของแต่ละบุคคล	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบการลงคะแนน และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดบัญชีผู้ใช้งานที่ได้รับอนุญาต กำหนดบทบาทของผู้ใช้งาน และกำหนดสิทธิการเข้าถึงให้กับแต่ละบทบาทของผู้ใช้งาน	ระบบการลงคะแนนมีการจำกัดสิทธิ์การเข้าใช้งานดังนี้ - ผู้ลงคะแนน สามารถลงคะแนน แสดงความคิดเห็น และตรวจสอบผลการลงคะแนน - ผู้ควบคุมระบบการลงคะแนน สามารถสร้างหัวข้อลงคะแนน ตัวเลือกการลงคะแนน และกำหนดสิทธิ์ของบัญชีผู้ใช้ที่จะได้รับอนุญาตให้ลงคะแนนในหัวข้อที่ผู้ควบคุมได้สร้างขึ้นเท่านั้น โดยสิทธิ์ผู้ควบคุมระบบการลงคะแนน ทางบริษัทฯ จะเป็นผู้ดำเนินการตรวจสอบข้อมูล และกำหนดสิทธิ์ให้บัญชีผู้ใช้งาน
11.3 – ระบบการลงคะแนนรองรับวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน	ระบบการลงคะแนนใช้วิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน เพื่อตรวจสอบว่าเป็นผู้ใช้งานที่ได้รับอนุญาตจริง และใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สำหรับผู้ควบคุมระบบการลงคะแนน เพื่อตรวจสอบว่าเป็นผู้ที่มีสิทธิเข้าถึงการดำเนินการที่สำคัญ (เช่น การเปิดลงคะแนน การปิดลงคะแนน) ทั้งนี้ วิธีการพิสูจน์และยืนยันตัวตนอาจพิจารณาข้อกำหนดตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) จากมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ระบบการลงคะแนนต้องเก็บรักษาข้อมูลยืนยันตัวตน (เช่น รหัสผ่าน) โดยมีการรักษาความลับ (confidentiality) และความครบถ้วน (integrity) ของข้อมูล และหากระบบการลงคะแนนใช้วิธีการยืนยันตัวตนด้วยรหัสผ่าน ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดความเข้มงวดและการหมดอายุของรหัสผ่าน	ระบบการลงคะแนนรองรับวิธีการพิสูจน์และยืนยันตัวตนที่มั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมถึงวิธีการยืนยันตัวตนแบบหลายปัจจัยสำหรับผู้ควบคุมระบบ ดังนี้ ผู้ลงคะแนน - ต้องยืนยันตัวตนในการเข้าสู่ระบบด้วย ชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) หรือ เบอร์โทรศัพท์โดยมีการยืนยัน OTP ผู้ควบคุมระบบการลงคะแนน - ต้องยืนยันตัวตนในการเข้าสู่ระบบด้วย ชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) หรือ เบอร์โทรศัพท์โดยมีการยืนยัน OTP - ระบบมีการกำหนดสิทธิ์ในส่วนของผู้ควบคุมระบบการลงคะแนนโดยรองรับการพิสูจน์จากระดับความน่าเชื่อถือของบัญชี (LOA) 4 Level 1. ยืนยันอีเมล 2. ยืนยันเบอร์มือถือ 3. ยืนยันตัวตนผ่านระบบ Ekyc By ID Card 4. ใบรับรองอิเล็กทรอนิกส์

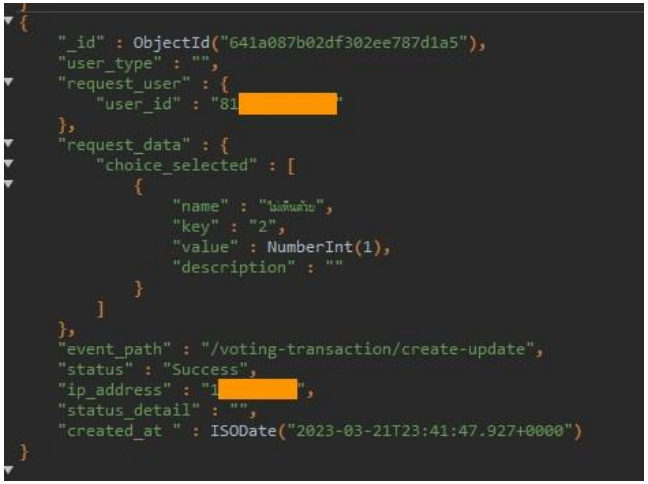
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
11.4 – ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่สอดคล้องตามหลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น และการแบ่งแยกหน้าที่	ระบบการลงคะแนนใช้นโยบายการควบคุมการเข้าถึงที่ใช้หลักการของการกำหนดสิทธิการเข้าถึงตามความจำเป็น (least privilege) โดยลดสิทธิการเข้าถึงภายในระบบให้เหลือเฉพาะที่จำเป็น และการแบ่งแยกหน้าที่ (separation of duties) โดยจำกัดบทบาทไม่ให้ผู้ใช้งานกลุ่มใดกลุ่มหนึ่งมีสิทธิการเข้าถึงที่เกินจำเป็น	ระบบการลงคะแนนมีการกำหนดสิทธิการเข้าถึงระบบ โดยมีการจำกัดบทบาทตามสิทธิที่ได้รับ ดังนี้ - ผู้ควบคุมระบบการลงคะแนน สามารถสร้าง ควบคุม แก้ไข หัวข้อการลงคะแนนและออกรายงานผลรวมการลงคะแนน - ผู้ลงคะแนน สามารถลงคะแนนเสียงและตรวจสอบผลรวมการลงคะแนน
11.5 – ระบบการลงคะแนนยกเลิกการเข้าถึงระบบของผู้ใช้งานเมื่อไม่มีการใช้งาน	ระบบการลงคะแนนให้ผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาของเซสชัน (session) และระยะเวลาในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด (inactivity timeout) โดยระบบการลงคะแนนต้องให้ผู้ใช้งานยืนยันตัวตนซ้ำ (reauthentication) หลังจากครบระยะเวลาที่กำหนด หากผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด ระบบการลงคะแนนควรระงับการใช้งาน (account lockout) ของผู้ใช้งานเป็นระยะเวลาหนึ่งก่อนจะให้ยืนยันตัวตนครั้งต่อไป และต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนสามารถกำหนดระยะเวลาระงับการใช้งาน (lockout duration) เพื่อจะช่วยป้องกันการใช้งานโดยไม่ได้รับอนุญาต หากระบบถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล	ระบบการลงคะแนนมีการกำหนดระยะเวลาของเซสชัน (session) ในกรณีผู้ใช้งานไม่ทำกิจกรรมใด ๆ ภายในระยะเวลาที่กำหนด โดยมีระยะเวลาเซสชัน 3 ชั่วโมงหลังจากนั้นผู้ใช้ต้องมีการเข้าสู่ระบบเพื่อยืนยันตันตนอีกครั้ง กรณีผู้ใช้งานยืนยันตัวตนผิดพลาดต่อเนื่องระบบไม่มีการจำกัดจำนวนความผิดพลาดต่อเนื่อง แต่ได้มีการใช้ Google reCAPTCHA ในการป้องกันการที่บอท Login ซ้ำๆและสามารถป้องกันบุคคลที่มีพฤติกรรมคล้ายบอทในการ Login reCAPTCHA คือบริการที่ปกป้องเว็บไซต์จากสแปมและการละเมิด ใช้เทคนิคการวิเคราะห์ความเสี่ยงขั้นสูงเพื่อแยกมนุษย์และบ็อตออกจากกัน  reCAPTCHA โดยปัจจุบัน SpaceVote ใช้ reCAPTCHA v3 ป้องกันในส่วนของการเข้าสู่ระบบ โดยเมื่อผู้ใช้กด "เข้าสู่ระบบ" จะมีการเรียกใช้ script ของ reCAPTCHA ซึ่งจะมีการ generate token ขึ้นมา และเมื่อเรานำ token ที่ได้ไป verify ผ่าน API ของ reCAPTCHA กรณี verify success เราจะได้ข้อมูล เกี่ยวกับ hostname ของไซต์ที่เรียกใช้ และ ข้อมูลคะแนน (0.0 - 1.0) โดยระดับคะแนน จะขึ้นอยู่กับการวิธีการเข้างานในส่วนที่มีการป้องกันของ reCAPTCHA ไว้ ซึ่งถ้าคะแนนต่ำกว่า 0.5 จะเป็นการบ่งบอกถึงการเข้าใช้ที่ผิดปกติ ซึ่งจะเกิดขึ้นได้ในกรณีต่าง ๆ เช่น การ Brute Force Attack, การส่งข้อมูลจำนวนหลาย ๆ ครั้งภายในระยะเวลาเดียวกัน แต่ในกรณีเข้าใช้งานทั่วไป คะแนนจะอยู่ในระดับที่มากกว่าหรือเท่ากับ 0.5 ขึ้นไปโดยระบบ SpaceVote จะอนุญาตให้เข้าสู่ระบบได้ เมื่อผลคะแนนที่ได้จากการ verify reCAPTCHA มากกว่าหรือเท่ากับ 0.5 ขึ้นไป

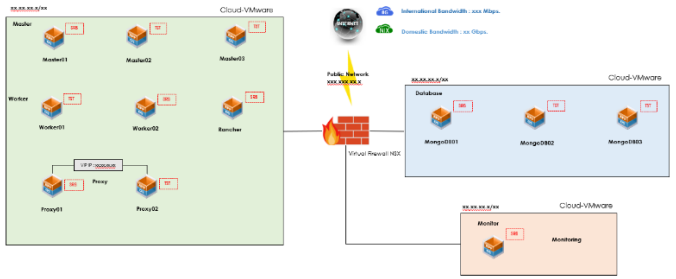
ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		ระบบมีการกำหนด Account Logout โดยมีการตั้งค่าดังต่อไปนี้ - Account lockout data : วันที่เริ่มปิดใช้งานยูสเซอร์ชั่วคราว - Account lockout duration: ระยะเวลาเป็นนาทีที่ทำการปิดใช้งานยูสเซอร์ชั่วคราว โดยระบบจะมีตั้งค่าที่ระยะเวลา 5 นาที - Account status: สถานะใช้งานของยูสเซอร์ กรณีสถานะเปิดใช้งาน ยูสเซอร์จะสามารถเข้าได้งานได้ต่อเมื่อ Account lockout duration มีค่าเป็น 0 กรณีสถานะปิดใช้งาน ยูสเซอร์จะไม่สามารถเข้าใช้งานระบบได้
11. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการป้องกันหรือตรวจจับความพยายามที่จะทำให้ฮาร์ดแวร์ของระบบการลงคะแนนเกิดความเสียหาย**		
12.1 – ระบบการลงคะแนนรองรับการตรวจจับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ	ระบบการลงคะแนนมีวิธีการตรวจจับการเข้าถึงทางกายภาพ (physical access) เช่น การบันทึกหลักฐานหรือการแจ้งเตือน หากมีเหตุการณ์การเข้าถึงโดยไม่ได้รับอนุญาตหรือการถูกตัดการเชื่อมต่อทางกายภาพเกิดขึ้นกับส่วนประกอบที่สำคัญของระบบการลงคะแนนในระหว่างเปิดใช้งานระบบการลงคะแนน ผู้พัฒนาระบบการลงคะแนนมีการรักษาความมั่นคงปลอดภัยสำหรับสภาพแวดล้อมทางกายภาพ เช่น ระบบล็อคที่มั่นคงปลอดภัย หรือระบบไฟฟ้าสำรองเมื่อเกิดเหตุไฟฟ้าดับ	- ระบบการลงคะแนนมีการใช้บริการ Monitoring ตรวจสอบความผิดปกติที่เกิดขึ้นภายในระบบ และแจ้งเตือนทันทีเมื่อตรวจพบความผิดปกติ - ระบบการลงคะแนนใช้บริการคลาวด์ ของ INET ซึ่งเป็นผู้ให้บริการที่มีการรักษา ความมั่นคงปลอดภัย รวมถึงการรับรองตามมาตรฐาน รายละเอียดตาม Link: https://inet.co.th/services.php?s=cloud https://www.inet.co.th/services.php?s=security โดยใช้บริการคลาวด์ในรูปแบบ laaS cloud ของ iNET, ประกอบด้วยดังนี้ 1. ส่วนของ virtual Machine (CPU/RAM/Disk) 2. ส่วนของ IP Network สำหรับ virtual Machine 3. ส่วนของ Security ของ Virtual Machine ได้แก่ Antivirus, SOC, VA Scan และ Pentest 4. ส่วนของ Monitoring สำหรับ virtual Machine 5. ส่วนของ Support แจ้งเคสและติดตามเคส
12. การคุ้มครองข้อมูล (Data Protection) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการคะแนนมีการปกป้องข้อมูลจากการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต**		
13.1 – ระบบการลงคะแนนมีการปกป้องข้อมูลการตั้งค่า (configuration) หรือบันทึกการลงคะแนน จากการเข้าถึงหรือการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ระบบการลงคะแนนต้องอนุญาตให้เฉพาะผู้ควบคุมระบบการลงคะแนนที่ยืนยันตัวตนแล้วเท่านั้นสามารถเข้าถึงหรือแก้ไขไฟล์การตั้งค่า (configuration file) ของระบบการลงคะแนนและระบบเครือข่าย รวมถึง	ระบบการลงคะแนนมีการป้องกันการปกป้องข้อมูลการตั้งค่า หรือบันทึกการลงคะแนน ดังนี้ 1. ระบบมีการจำกัดสิทธิของผู้ควบคุมระบบการลงคะแนน โดยผู้ควบคุมระบบการลงคะแนน สามารถตั้งค่า และจัดการเกี่ยวกับหัวข้อการลงคะแนนเฉพาะที่ตนเองเป็นผู้สร้าง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ระบบการลงคะแนนต้องมีการรักษาความครบถ้วน (integrity) ของบันทึกการลงคะแนน (vote records) จากการแก้ไขเปลี่ยนแปลง	เท่านั้น ผ่าน Web Portal ส่วนผู้ควบคุมระบบการลงคะแนน 2. ผู้ควบคุมระบบการลงคะแนนต้องยืนยันตัวตนก่อนเข้าใช้งานระบบทุกครั้งด้วย ชื่อผู้ใช้และรหัสผ่าน หรือเบอร์โทรศัพท์โดยมีการยืนยัน OTP 3. ระบบออกแบบให้ผู้ควบคุมระบบการลงคะแนนไม่สามารถเข้าถึงการตั้งค่าเครือข่าย หรือการแก้ไขผลคะแนน 4. บันทึกการลงคะแนนถูกจัดเก็บบนบล็อกเชน ที่ออกแบบให้ไม่สามารถแก้ไขข้อมูลได้
13.2 – บันทึกการลงคะแนนสามารถตรวจสอบความครบถ้วนของข้อมูลได้	ระบบการลงคะแนนสามารถตรวจสอบความครบถ้วนของผลลงคะแนนที่ได้รับมาจากผู้ลงคะแนน บันทึกและแสดงข้อผิดพลาดในการตรวจสอบผลลงคะแนนที่ได้รับมาในทันที และจัดเก็บบันทึกการลงคะแนนให้อยู่ในรูปแบบที่สามารถแสดงผลลงคะแนนที่ได้รับมาให้ปรากฏอย่างถูกต้องได้	ระบบการลงคะแนนมีการจัดการความครบถ้วนของข้อมูลดังนี้ - ระบบมีการตรวจสอบข้อผิดพลาดและแจ้งเตือนผู้ใช้ทันทีเมื่อเกิดข้อผิดพลาดโดยการลงคะแนนที่ไม่สำเร็จจะไม่ถูกบันทึกลงบนระบบ - ระบบมีการจัดเก็บบันทึกผลการลงคะแนนที่ได้รับไว้บนฐานข้อมูลระบบ และบนบล็อกเชน ที่ข้อมูลไม่สามารถเปลี่ยนแปลง ซึ่งสามารถนำบันทึกของทั้งสองส่วนมาตรวจสอบความถูกต้องและครบถ้วนของข้อมูลได้
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	ระบบการลงคะแนนมีการดำเนินการเกี่ยวกับการเข้ารหัสลับ ดังนี้ - มีการใช้ SSL/TLS v1.2 สำหรับ http protocol ในการเข้ารหัสขณะรับส่งข้อมูล (data-in-transit encryption) - มีการเข้ารหัสข้อมูลส่วนบุคคล ชื่อ, นามสกุล, เบอร์ติดต่อ, email, เลขบัตรประชาชน ด้วยวิธี AES-256 โดยผู้มีสิทธิเท่านั้นที่สามารถเข้าถึงได้
13.4 – ระบบการลงคะแนนมีการรักษาความครบถ้วน (integrity) ความถูกต้องแท้จริง (authenticity) และความลับ (confidentiality) ของข้อมูลสำคัญที่ส่งผ่านเครือข่ายคอมพิวเตอร์ทั้งหมด	การติดต่อสื่อสารของระบบการลงคะแนนผ่านเครือข่ายคอมพิวเตอร์ทั้งหมดต้องเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย (mutually-authenticated secure channel) นอกจากนี้ ระบบการลงคะแนนต้องมีการรักษาความครบถ้วนและความลับของข้อมูลทั้งหมดที่ส่งผ่านเครือข่ายคอมพิวเตอร์ด้วยกระบวนการเข้ารหัสลับ (cryptography)	ระบบมีการใช้ SSL/TLS ในการเข้ารหัสขณะรับส่งข้อมูลระหว่าง Server กับ Client
13. การรักษาความครบถ้วนของระบบ (System Integrity) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีการทำงานอย่างถูกต้องครบถ้วนตามฟังก์ชันการทำงาน และไม่มีการแทรกแซงการทำงานของระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะโดยตั้งใจหรือโดยไม่ตั้งใจ**		
14.1 – ระบบการลงคะแนนใช้การควบคุมหลายระดับชั้น (multiple layers of	เอกสารเกี่ยวกับระบบการลงคะแนนมีรายละเอียดของการประเมินความเสี่ยง (risk assessment) และวิธีการ	ระบบการลงคะแนนมีเอกสารที่มีรายละเอียดของการประเมินความเสี่ยง

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
controls) เพื่อรับมือภัยคุกคามหรือช่องโหว่ด้านความมั่นคงปลอดภัย	ควบคุมเพื่อรับมือหรือลดความเสี่ยงจากภัยคุกคามแต่ประเภทซึ่งอาจส่งผลกระทบต่อการทำงานของระบบการลงคะแนน รวมถึงอธิบายวิธีการควบคุมหลายระดับชั้น (multiple layers of controls) เพื่อป้องกันบรรเทา และตอบสนองต่อการโจมตีระบบการลงคะแนน เช่น กระบวนการเข้ารหัสลับ (cryptography) การป้องกันมัลแวร์ (malware) การตั้งค่าไฟร์วอลล์ (firewall) และการตั้งค่าระบบ (system configurations)	(Risk Assessment) โดยมี 3 ด้าน CIA (Confidential, Integrity, Availability) และผลกระทบทั้ง 3 ด้าน (Operation, Compliance, Service) สรุปผลจากการประเมินความเสี่ยง 6 ประเภท คือ Hardware, Software, Logical, Information, People, External ทั้งหมดจำนวน 53 รายการ พบว่ามีความเสี่ยง ดังนี้ แดง = 19 รายการ , เหลือง = 14 รายการ , เขียว= 20 รายการ หลังจากมีแผนลดความเสี่ยง RTP (Risk Treatment Plan) ทำให้ความเสี่ยงคงเหลือ ดังนี้ แดง = 0 รายการ , เหลือง = 23 รายการ , เขียว = 30 รายการ ซึ่งต้องมีการ Monitor และทบทวนความเสี่ยงที่จะเกิดต่อไปอย่างน้อยปีละ 1ครั้ง อ้างอิงมาตรฐาน ISO27001 (Risk Assessment_spacevote_FM-SC-41) Risk Profile ผลกระทบ(Impact) สูงมาก 5 10 15 20 25 สูง 4 8 12 16 (Intolerable) 20 ปานกลาง 3 6 9 (Tolerance) 12 15 น้อย 2 4 (Appetite) 6 8 10 น้อยมาก 1 2 3 4 5 น้อยมาก น้อย ปานกลาง สูง สูงมาก โอกาส(Likelihood) ระดับ / ความหมาย สีเขียว: ระดับความเสี่ยงอยู่ในระดับที่องค์กรยอมรับ (Acceptable) สีเหลือง: ระดับความเสี่ยงเกินกว่าระดับที่องค์กรยอมรับแต่ยังอยู่ในค่าความเบี่ยงเบนที่กำหนด (Torrable) สีแดง: ระดับความเสี่ยงเกินกว่าระดับที่องค์กรยอมรับได้ (Intolerable) การระบุถึงระดับความเสียหายที่อาจจะเกิดขึ้นได้จากการประเมินระดับความเสี่ยงแต่ละปัจจัย (ระดับความเสี่ยง = ระดับผลกระทบของความเสี่ยง x ระดับโอกาสของการเกิดความเสี่ยง) มีการควบคุมกระบวนการเข้ารหัสลับ (cryptography) อ้างอิงตามระเบียบปฏิบัติการ (Cryptography Control) และระเบียบปฏิบัติงาน (User Access Management) -. ด้านการ กู้คืนข้อมูล หากระบบมีผลกระทบทำให้ฐานข้อมูลผิดปกติ จะมีการกู้คืนข้อมูลโดยการนำ Snapshot/ฐานข้อมูลที่ Backup ไว้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		-. ด้านการ ทำ Business Continuity Plan มีการทำแผนและทดสอบBCP ปีละ 2 ครั้ง ด้าน Security ดังนี้ - Policy Firewall – NSX ทำหน้าที่ตรวจสอบการเข้าถึง IP ของ VM และ กำหนด Allow หรือ Deny Policy และ Port การเข้าถึงให้เป็นไปตามนโยบายความปลอดภัยตามมาตรฐาน ISO 27001 - จำกัดการเข้าถึง Cluster Policy Firewall ที่มีการ Run VM โดยการเข้าถึงระบบด้วย VPN authentication และ ควบการเข้าถึงของ User ด้วยระบบ AD - มีการป้องกัน Anti-malware ด้วยโปรแกรม Deep Security ทั้งนี้ระบบการลงคะแนน ได้มีการจัดทำ VA Scan, Penetration Testing และ SOC บนระบบปฏิบัติการ Windows และ Linux โดยเป็นการทดสอบความปลอดภัยของระบบเว็บไซต์โดยอ้างอิงจาก OWASP (Web Security Testing Guide) ใช้การทดสอบแบบ Gray Box ซึ่งไม่พบช่องโหว่ที่มีนัยสำคัญ
14.2 – ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสการโจมตี (attack surface) โดยหลีกเลี่ยงซอร์สโค้ดและการเชื่อมต่อเครือข่ายที่ไม่จำเป็น	ระบบการลงคะแนนป้องกันการติดตั้งหรือการสั่งประมวลผลกระบวนการที่ไม่เกี่ยวข้อง และปิดใช้งานการเชื่อมต่อเครือข่ายและคุณสมบัติอื่น ๆ ที่ไม่จำเป็นต่อการทำงานของระบบการลงคะแนน ซอฟต์แวร์ของระบบการลงคะแนนต้องไม่มีซอร์สโค้ดที่ไม่ถูกเรียกใช้งาน (unused code) หรือถูกเรียกใช้งานแต่ผลลัพธ์ไม่ถูกนำไปใช้งาน (dead code) และต้องเรียกใช้คลังโปรแกรม (software library) เฉพาะส่วนที่จำเป็นเท่านั้น	ระบบการลงคะแนนมีการออกแบบเพื่อลดโอกาสในการโจมตี ดั้งนี้ - มีการใช้ Firewall บล็อกการเชื่อมต่อจาก IP ที่ไม่ได้รับอนุญาต - มีการเปิดใช้งาน port เฉพาะที่จำเป็นในการเชื่อมต่อเท่านั้น - มีการตรวจสอบเรื่อง unused code, software library ที่จำเป็น และปรับปรุงแก้ไข issue อย่างสม่ำเสมอ
14. การตรวจจับและการเฝ้าระวัง (Detection and Monitoring) **<u>วัตถุประสงค์</u> เพื่อให้ระบบการลงคะแนนมีมาตรการตรวจจับและเฝ้าระวังพฤติกรรมที่ผิดปกติหรือเป็นอันตรายต่อระบบการลงคะแนน**		
15.1 – ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ	ระบบการลงคะแนนต้องสามารถบันทึกเหตุการณ์ (event logging) ที่เกิดขึ้นในระบบการลงคะแนน ซึ่งประกอบด้วยเหตุการณ์ที่เกี่ยวข้องกับสถานะการทำงานและความผิดปกติของระบบ การยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน การจัดการระบบเครือข่าย การจัดการซอฟต์แวร์ และฟังก์ชันการลงคะแนน เป็นอย่างน้อย	ระบบการลงคะแนนมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบ ดังนี้ 1. สถานการณ์ทำงาน และความผิดปกติของระบบ ระบบ SpaceVote ได้ใช้ Zabbix monitor และบริการ monitor service ของ INET โดยจะมีทีม monitor คอยสังเกตปัญหาที่เกิดขึ้นในระบบ และโทรแจ้งเตือนกับทีมผู้ดูแลระบบในกรณีที่ตรวจพบความผิดปกติ 

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		รูปที่ 1 แสดง Zabbix monitor 2. ยืนยันตัวตนและการเข้าถึงของผู้ใช้งาน ระบบมีการบันทึก log ในการยืนยันตัวตนและการเข้าถึงของผู้ใช้งานดังรูป  รูปที่ 2 แสดง log การเข้าสู่ระบบ 3. การจัดการระบบเครือข่าย ระบบมีการจัดการระบบเครือข่ายบน Virtual Firewall NSX ของ INET 4. การจัดการซอฟต์แวร์ ระบบได้มีการใช้ Rancher ในการจัดการซอฟต์แวร์ในส่วนของ Web Portal และ Service API ของระบบลงคะแนน 5. ฟังก์ชันการลงคะแนน ระบบมีการบันทึก log ของการเรียกใช้งาน ฟังก์ชั่นการลงคะแนนดังรูป  รูปที่ 3 แสดง log ฟังก์ชั่นลงคะแนน
15.2 – ระบบการลงคะแนนมีการสร้าง จัดเก็บ และรายงานข้อความแสดงข้อผิดพลาดทั้งหมดที่เกิดขึ้น	เมื่อมีข้อผิดพลาดเกิดขึ้นในระบบการลงคะแนน ระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ใช้งานในทันที บันทึกข้อผิดพลาดทั้งหมดที่เกิดขึ้น และสร้างรายงาน	ระบบการลงคะแนนมีการจัดการข้อผิดพลาดที่เกิดขึ้นดังนี้ - ระบบมีการแจ้งเตือนผู้ใช้งาน เมื่อระบบการลงคะแนนเกิดข้อผิดพลาด เช่น เข้าสู่ระบบไม่สำเร็จ ลงคะแนนไม่สำเร็จ

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
	ข้อผิดพลาด (error report) รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการจัดการข้อผิดพลาดในระบบการลงคะแนน	- ระบบมีการบันทึกข้อผิดพลาดที่เกิดขึ้นในรูปแบบของ error log และสามารถออกรายงานข้อผิดพลาดได้ - เอกสารที่เกี่ยวข้องกับระบบการลงคะแนน มีขั้นตอนสำหรับการจัดการข้อผิดพลาดในระบบการลงคะแนน
15.3 – ระบบการลงคะแนนมีการออกแบบให้ป้องกันมัลแวร์ (malware)	ระบบการลงคะแนนต้องมีมาตรการป้องกันมัลแวร์ (malware) โดยระบบการลงคะแนนต้องสามารถแจ้งเตือนผู้ควบคุมระบบการลงคะแนนในทันทีเมื่อตรวจพบมัลแวร์ บันทึกเหตุการณ์ที่ตรวจพบมัลแวร์ แจ้งเตือนเมื่อมีการกำจัดหรือแก้ไขมัลแวร์สำเร็จ และบันทึกเหตุการณ์ของกิจกรรมการแก้ไขมัลแวร์ รวมถึงเอกสารเกี่ยวกับระบบการลงคะแนนมีขั้นตอนสำหรับการอัปเดตมาตรการป้องกันมัลแวร์	ระบบการลงคะแนนมีการติดตั้ง anti-malware โดยใช้โปรแกรม Deep Security มีการตั้ง schedule ให้ run full scan 1 ครั้งต่อสัปดาห์ และ มีการ set update virus signature ทุกวัน ระบบการลงคะแนนมีการ monitoring ด้วยทีม operation ของ INET ซึ่งจะมีการแจ้งเตือนเมื่อพบสิ่งผิดปกติ
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	ระบบการลงคะแนนที่เชื่อมต่อเครือข่ายใช้วิธีการป้องกันการโจมตีทางเครือข่าย ที่เหมาะสมและสอดคล้องกับแนวปฏิบัติที่ดี ดังนี้ - มีการใช้ SSL/TLS ในการเข้ารหัสขณะรับส่งข้อมูลระหว่าง Server กับ Client - มีการป้องกันเครือข่ายด้วย Virtual Firewall มีการทำ DNAT และเปิดใช้งาน Policy Port เฉพาะที่จำเป็นเท่านั้น - มีการนำระบบ VA Scan หาช่องโหว่ของระบบ เซิร์ฟเวอร์ และเครือข่าย - มีการทำ Pentest เพื่อทดสอบทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบ -ติดตั้ง Agent SOC เพื่อ Monitor ความผิดปกติของการเข้าถึง  รูป ตัวอย่าง SpaceVote Network Diagram - ตามรูปแบบ Diagram การใช้ Firewall มีความปลอดภัยตามมาตรฐาน เนื่องจากมีการกำหนดและ Review Policy ต่างๆที่ Virtual Firewall ก่อนนำขึ้น Solution โดยรายละเอียดของ Firewall ที่ใช้ คือ Virtual Firewall NSX Dedicate มีรายละเอียดดังนี้

ข้อกำหนด	คำอธิบาย	ความสามารถของระบบการลงคะแนน
		- Firewall Throughput 9.7Gbps - Max sessions 1.0 Million - สามารถทำงานบนระบบเครือข่าย IPv4 ได้ - สามารถทำ SSL-VPN (Client To Site) ได้ - สามารถทำ IPSEC-VPN (Site To Site) ได้ - สามารถทำ Load balancing rule บน Destination network address translation เพื่อใช้สำรองเครื่องปลายทาง โดยสามารถทำงานในรูปแบบ Round Robin, First Alive เป็นอย่างน้อยโดยสามารถใช้งาน health check เพื่อตรวจสอบ Service ผ่าน Port โดยใช้ Protocol TCP ได้ ในส่วนของ Security configuration มีการตั้งค่าโดยอิงตามนโยบายความปลอดภัย มาตรฐาน ISO 27001 ตามหัวข้อดังนี้ ● SP-SC-76_02_Patch management ● WI-SC-02_07_Clock Synchronization ● SP-SC-20_08_Backup Management ● SP-SC-21_08_Network Security Control ทั้งนี้ยังทำส่วนของ OS Hardening Checklist เช่น ● ติดตั้ง Anti-virus Anti-Malware ● เปิด Port เท่าที่จำเป็นเพื่อใช้งาน โดยทดสอบ VASCAN อีกครั้ง ● เปิด Firewall ระบบ OS ● Limit การเข้าถึงของ User ● Update Patch ตามหัวข้อ Patch Management