สมาคมสโมสรนักลงทุน
INVESTOR CLUB ASSOCIATION
1 อาคาร ทีพี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900 โทร. 02 666 9111
1 TP & T Tower, 12th FL., Vibhavadi Rangsit Rd., Chatuchak, Chatuchak, Bangkok 10900 Tel. 02 666 9111

ประกาศสมาคมสโมสรนักลงทุน เลขที่ IC-PUA 8/2569
เรื่อง สอบราคาโครงการว่าจ้างบริการระบบบริหารจัดการ ติดตาม และประเมินผลตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ

สมาคมสโมสรนักลงทุน ซึ่งต่อไปนี้เรียกว่า “สมาคม” มีความประสงค์จะสอบราคาโครงการว่าจ้างบริการระบบบริหารจัดการ ติดตาม และประเมินผลตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ ในรูปแบบ Software as a Service (SaaS) สำหรับผู้ใช้งานจำนวน 25 สิทธิ (Named User License) พร้อมบริการวิเคราะห์ความต้องการ ติดตั้ง กำหนดค่า ปรับแต่ง ทดสอบ ฝึกอบรม ส่งมอบ เปิดใช้งานจริง (Go-Live) และให้บริการระบบเป็นระยะเวลา 12 เดือน

โดยมีข้อแนะนำและข้อกำหนด ดังต่อไปนี้

1. เอกสารแนบท้ายเอกสารสอบราคา

1.1 ขอบเขตงาน (Terms of Reference: TOR) โครงการว่าจ้างบริการระบบบริหารจัดการ ติดตาม และประเมินผลตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ

1.2 แบบใบเสนอราคา (Pricing Schedule)

1.3 แบบสัญญา

(1) สัญญาหลัก

(2) สัญญารักษาความลับและข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (ตามที่สมาคมกำหนด)

1.4 แบบหนังสือค้ำประกันหลักประกันสัญญา

1.5 แบบบัญชีเอกสาร

(1) บัญชีเอกสารส่วนที่ 1 เอกสารคุณสมบัติและข้อมูลบริษัท

(2) บัญชีเอกสารส่วนที่ 2 ข้อเสนอด้านเทคนิค

ภาคผนวก/เอกสารนโยบายที่เกี่ยวข้อง: IT Policy and Management for Vendor รหัสเอกสาร IT-1PC-02 และเอกสารด้านความมั่นคงปลอดภัยสารสนเทศอื่นตามที่สมาคมกำหนด

2. คุณสมบัติผู้เสนอราคา

ผู้เสนอราคาต้องมีคุณสมบัติดังต่อไปนี้

2.1 เป็นนิติบุคคลที่จดทะเบียนตามกฎหมายไทย มีทุนจดทะเบียนชำระแล้วไม่น้อยกว่า 1,000,000 บาท ณ วันที่ยื่นข้อเสนอ และประกอบกิจการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ คอมพิวเตอร์ ซอฟต์แวร์ หรือ IT Service Management

2.2 เป็นเจ้าของผลิตภัณฑ์ (Product Owner) หรือได้รับการแต่งตั้งเป็นตัวแทนจำหน่าย ตัวแทนให้บริการ หรือพันธมิตรทางธุรกิจอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์ กรณีเสนอซอฟต์แวร์ประเภทโอเพนซอร์ส (Open Source Software) ต้องแสดงหลักฐานความสามารถในการติดตั้ง ปรับแต่ง พัฒนา บำรุงรักษา และให้บริการสนับสนุนตลอดระยะเวลาตามสัญญา รวมทั้งปฏิบัติตามเงื่อนไขของสัญญาอนุญาตการใช้งานที่เกี่ยวข้อง

2.3 มีประสบการณ์ให้บริการ ITSM, Helpdesk, Service Desk หรือ Ticket Management System ไม่น้อยกว่า 3 ปี และมีผลงานอ้างอิงไม่น้อยกว่า 3 โครงการ

2.4 มีบุคลากรที่มีความรู้และประสบการณ์เหมาะสม และมี Project Manager หรือผู้รับผิดชอบหลักประจำโครงการ

2.5 มีทีม Technical Support ในประเทศไทย และมีช่องทางสนับสนุนทางโทรศัพท์ อีเมล หรือระบบออนไลน์

2.6 สามารถให้บริการ Maintenance, Corrective Maintenance, Version Upgrade และ Security Patch ตลอดระยะเวลาสัญญาโดยไม่มีค่าใช้จ่ายเพิ่มเติม

2.7 ไม่มีประวัติถูกบอกเลิกสัญญาเนื่องจากการทิ้งงานหรือไม่ปฏิบัติตามสัญญาอย่างร้ายแรงกับหน่วยงานของรัฐหรือองค์กรเอกชนภายในระยะเวลา 3 ปีที่ผ่านมา

ทั้งนี้ ข้อกำหนดเกี่ยวกับคุณลักษณะระบบ SaaS, Cloud/Data Center, Security, Backup/DR, SLA, Data Portability และการส่งมอบข้อมูล ให้เป็นไปตาม TOR และถือเป็นข้อกำหนดด้านเทคนิค/การให้บริการ มิใช่คุณสมบัติทั่วไปของผู้เสนอราคา เว้นแต่ TOR กำหนดไว้เป็น Mandatory Requirement โดยชัดแจ้ง

3. หลักฐานการเสนอราคา

ผู้เสนอราคาต้องยื่นเอกสารโดยแยกเป็น 3 ส่วน ดังนี้

3.1 ส่วนที่ 1 เอกสารคุณสมบัติและข้อมูลบริษัท อย่างน้อยประกอบด้วย

(1) สำเนาหนังสือรับรองนิติบุคคลที่ออกให้ไม่เกินระยะเวลาตามที่สมาคมกำหนด พร้อมรับรองสำเนาถูกต้อง

(2) เอกสารรายชื่อกรรมการ/ผู้มีอำนาจลงนาม และบัญชีผู้ถือหุ้นตามประเภทนิติบุคคล

(3) หนังสือมอบอำนาจติดอากรแสตมป์ตามกฎหมาย (ถ้ามี)

(4) หลักฐาน Product Owner/Authorized Partner หรือหลักฐานความสามารถกรณี Open Source

(5) หลักฐานประสบการณ์ไม่น้อยกว่า 3 ปี และผลงานอ้างอิงไม่น้อยกว่า 3 โครงการ

(6) ข้อมูล Project Manager และทีมงานหลัก

(7) บัญชีเอกสารส่วนที่ 1

3.2 ส่วนที่ 2 ข้อเสนอด้านเทคนิค อย่างน้อยประกอบด้วย

(1) Technical Compliance Matrix ตอบข้อกำหนด TOR ทุกข้อ โดยระบุ Comply/Partially Comply/Not Comply พร้อมเลขหน้าเอกสารอ้างอิง

(2) รายละเอียดระบบและสถาปัตยกรรม SaaS รวมถึง Cloud/Data Center และประเทศที่จัดเก็บข้อมูล

(3) แผนดำเนินโครงการ Implementation ให้แล้วเสร็จภายใน 60 วันนับถัดจากวันที่ลงนามในสัญญา

(4) แผนการติดตั้ง กำหนดค่า ปรับแต่ง Workflow/SLA/KPI/Dashboard/Report การทดสอบ UAT การฝึกอบรม และ Go-Live

(5) รายละเอียดระบบ ITSM, Asset & Configuration/CMDB, Knowledge Management, KPI Dashboard, Reporting, User/Role/RBAC, Audit Trail และโมดูลอื่นตาม TOR

(6) แผน Support & Maintenance และ SLA โดย System Availability ไม่น้อยกว่า 99.9% ต่อเดือน

(7) รายละเอียด Backup/DR โดย RTO และ RPO ไม่เกิน 24 ชั่วโมง หรือตาม TOR

(8) เอกสารด้าน Security/Privacy/PDPA, ISO/IEC 27001 หรือหลักฐานมาตรการที่เทียบเท่า และข้อมูล Subprocessor/Cloud Provider ตามที่ TOR กำหนด

(9) แนวทาง Security Incident Notification ภายใน 24 ชั่วโมงตาม TOR

(10) แนวทาง Data Portability, Exit Management และ Data Deletion เมื่อสิ้นสุดสัญญา

(11) แผนฝึกอบรม คู่มือ และรายการเอกสารส่งมอบ

(12) ข้อเสนอ/บริการเพิ่มเติม (ถ้ามี)

(13) บัญชีเอกสารส่วนที่ 2

3.3 ส่วนที่ 3 ข้อเสนอด้านราคา

(1) ใบเสนอราคาตามเอกสารแนบ 1.2 ปิดผนึกแยกจากข้อเสนอด้านเทคนิค

(2) ต้องแยกราคา Implementation Service และ SaaS Subscription ระยะเวลา 12 เดือน สำหรับ 25 Named Users

(3) ต้องระบุราคา Additional User License ราคาต่ออายุปีที่ 2–3 หรือหลักเกณฑ์การปรับราคา และ Optional Services ตามแบบ โดยรายการอ้างอิงดังกล่าวไม่นำมารวมในราคาหลัก เว้นแต่สมาคมกำหนดเป็นอย่างอื่น

(4) ราคาหลักที่ใช้ในการพิจารณา ประกอบด้วยค่าดำเนินการติดตั้งและปรับแต่งระบบ (Implementation Service) รวมกับค่าบริการระบบ SaaS ระยะเวลา 12 เดือน สำหรับผู้ใช้งาน 25 สิทธิ โดยเงื่อนไขการจ่ายเงินให้เป็นไปตามข้อ 7 ของ TOR

4. การเสนอราคา

4.1 ผู้เสนอราคาต้องยื่นเสนอราคาตามแบบที่กำหนดไว้ในเอกสารสอบราคานี้ โดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น และจะต้องกรอกข้อความให้ถูกต้องครบถ้วน ลงลายมือชื่อของผู้เสนอราคาให้ชัดเจน จำนวนเงินที่เสนอต้องระบุตรงกันทั้งตัวเลขและตัวอักษร โดยไม่มีการขูดลบหรือแก้ไข หากมีการขูดลบ ตกเติม แก้ไขเปลี่ยนแปลง จะต้องลงลายมือชื่อผู้เสนอราคาพร้อมประทับตรา (ถ้ามี) กำกับไว้ทุกแห่ง

4.2 ผู้เสนอราคาจะต้องเสนอราคาเป็นเงินบาท และเสนอราคาต่อหน่วย และ/หรือต่อรายการตามเงื่อนไขที่ระบุไว้ให้ถูกต้อง ทั้งนี้ ราคารวมที่เสนอจะต้องตรงกันทั้งตัวเลขและตัวหนังสือ ถ้าตัวเลขและตัวหนังสือไม่ตรงกันให้ถือตัวหนังสือเป็นสำคัญ โดยคิดราคารวมทั้งสิ้นซึ่งไม่รวมค่าภาษีมูลค่าเพิ่ม แต่รวมภาษีอากรอื่น ค่าขนส่ง ค่าจดทะเบียน และค่าใช้จ่ายอื่น ๆ ทั้งปวง จนกระทั่งส่งมอบงานทุกอย่างให้ ณ สมาคมสโมสรนักลงทุน เลขที่ 1 อาคาร ทีพี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900

ราคาที่เสนอต้องมีกำหนดยืนราคาไม่น้อยกว่า 60 วันนับแต่วันยื่นซองเสนอราคาโดยภายในกำหนดยืนราคาผู้เสนอราคาต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และจะถอนการเสนอราคามิได้

4.3 ก่อนยื่นซองข้อเสนอ ผู้เสนอราคาควรตรวจดูข้อกำหนด รายละเอียด และขอบเขตงาน ฯลฯ ให้ถี่ถ้วนและเข้าใจเอกสารสอบราคาทั้งหมดเสียก่อนที่จะตกลงยื่นซองสอบราคาตามเงื่อนไขในเอกสารสอบราคา

4.4 ผู้เสนอราคาจะต้องยื่นซองใบเสนอราคาที่ปิดผนึกซองเรียบร้อย จ่าหน้าซองถึง ประธานคณะกรรมการจัดซื้อจัดจ้าง โดยระบุไว้ที่หน้าซองว่า “ใบเสนอราคาตามเอกสารสอบราคาเลขที่ IC-PUA 8/2569” ยื่นต่อพนักงานภายในวันและเวลาที่กำหนด เมื่อพ้นกำหนดเวลายื่นซองสอบราคาแล้วจะไม่รับซองสอบราคาโดยเด็ดขาด

5. หลักเกณฑ์การพิจารณา

5.1 สมาคมจะตรวจสอบคุณสมบัติและความครบถ้วนของเอกสารก่อน ผู้เสนอราคาที่ไม่ผ่าน Mandatory Requirement ที่เป็นสาระสำคัญอาจไม่ได้รับการพิจารณาในขั้นตอนถัดไป

5.2 ผู้ผ่านการตรวจสอบเบื้องต้นต้องนำเสนอรายละเอียดระบบและสาธิตการใช้งานระบบ (Presentation and System Demonstration) ตามสถานการณ์จำลอง (Demo Scenario) เดียวกันที่สมาคมกำหนด โดยกำหนดเวลานำเสนอรายละไม่เกิน 120 นาที และช่วงตอบข้อซักถามไม่เกิน 30 นาที เพื่อให้สามารถเปรียบเทียบข้อเสนอได้อย่างเป็นธรรม

5.3 คะแนนด้านเทคนิคเต็ม 100 คะแนน แบ่งเป็น

(1) คุณสมบัติและประสบการณ์บริษัทและทีมงาน 15 คะแนน

(2) ความสามารถของระบบและการสาธิตระบบ 40 คะแนน

(3) Project Plan, Implementation, Training และ Support 20 คะแนน

(4) Security, PDPA, Backup, DR และ SLA 15 คะแนน

(5) Value Added Features 10 คะแนน

5.4 ผู้เสนอราคาต้องได้คะแนนด้านเทคนิคไม่น้อยกว่า 80 คะแนน จึงจะผ่านเข้าสู่การพิจารณาด้านราคา

5.5 สมาคมจะเปิดและพิจารณาข้อเสนอด้านราคาของผู้ที่ผ่านเกณฑ์ด้านเทคนิค โดยพิจารณาราคารวมของ Implementation Service และ SaaS Subscription ระยะเวลา 12 เดือน ตาม Pricing Schedule และใช้หลักประสิทธิภาพต่อราคา โดยสมาคมไม่จำเป็นต้องเลือกผู้เสนอราคาต่ำสุด

5.6 การตัดสินของคณะกรรมการจัดซื้อจัดจ้างให้ถือเป็นที่สุดภายใต้หลักเกณฑ์และอำนาจของสมาคม

6. การทำสัญญา

6.1 ผู้ชนะการเสนอราคาต้องทำสัญญาจ้างกับสมาคมภายใน 5 วันนับถัดจากวันที่สมาคมได้แจ้งให้ทราบเป็นลายลักษณ์อักษร และหากไม่ไปทำสัญญากับสมาคมภายในระยะเวลาที่กำหนดดังกล่าว สมาคมจะถือว่าเป็นผู้ทิ้งงาน

6.2 ผู้ชนะการเสนอราคาต้องวางหลักประกันสัญญามีมูลค่าร้อยละ 10 (สิบ) ของราคาที่สมาคมตกลงจ้างตลอดอายุสัญญา โดยหลักประกันสัญญาให้ใช้อย่างหนึ่งอย่างใดตามที่สมาคมกำหนด ดังนี้

(1) โอนเงินเข้าบัญชีของสมาคม

(2) หนังสือค้ำประกันของธนาคารภายในประเทศตามแบบที่สมาคมกำหนดไว้

6.3 เอกสารขอบเขตงาน (TOR) เอกสารสอบราคา ข้อเสนอด้านเทคนิค ข้อเสนอด้านราคา และเอกสารชี้แจงหรือเอกสารอื่นที่ผู้ชนะการเสนอราคายื่นต่อสมาคม ให้ถือเป็นภาระผูกพันและเป็นส่วนหนึ่งของสัญญาจ้าง โดยผู้รับจ้างต้องติดตั้งและเปิดใช้งานจริง (Go-Live) ให้แล้วเสร็จภายใน 60 วันปฏิทินนับถัดจากวันที่ลงนามในสัญญา และให้บริการระบบเป็นระยะเวลา 12 เดือนนับจากวัน Go-Live ตามที่ระบุในเอกสารตรวจรับงานงวดที่ 1

6.4 ผู้ชนะการเสนอราคาต้องรับผิดชอบในการดำเนินงานไม่ให้มีการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลใด ๆ ทั้งนี้ หากมีความเสียหายเกิดขึ้น ผู้ชนะการเสนอราคาต้องรับผิดชอบชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมด

6.5 ผู้ชนะการเสนอราคาต้องปฏิบัติตามข้อกำหนดด้าน SLA ความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล การแจ้ง Security Incident ภายใน 24 ชั่วโมง การสำรองและกู้คืนข้อมูล การส่งมอบและทำลายข้อมูลเมื่อสิ้นสุดสัญญา ตลอดจนข้อกำหนดอื่นทั้งหมดตาม TOR และสัญญา

7. กำหนดยื่นซองสอบราคา

วันที่ 13 – 26 สิงหาคม 2569 ระหว่างเวลา 08.30–15.00 น.

ณ แผนกจัดซื้อ สมาคมสโมสรนักลงทุน เลขที่ 1 อาคาร ทีพี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

8. กำหนดผู้เสนอราคานำเสนอข้อเสนอ (Presentation)

วันที่ 1 กันยายน 2569 รูปแบบออนไลน์หรือรูปแบบอื่นตามที่สมาคมกำหนด โดยกำหนดเวลานำเสนอรายละไม่เกิน 120 นาที และช่วงตอบข้อซักถามไม่เกิน 30 นาที

ผู้เสนอราคาต้องนำเสนอข้อเสนอด้านเทคนิค แผนดำเนินโครงการ และสาธิตระบบตาม Demo Scenario ที่สมาคมกำหนด ทั้งนี้ สมาคมจะแจ้งวัน เวลา รูปแบบ และรายละเอียดการสาธิตให้ผู้เสนอราคาที่ผ่านการตรวจสอบคุณสมบัติทราบอีกครั้ง

9. การติดต่อสอบถาม

ผู้สนใจสามารถติดต่อขอทราบรายละเอียดได้ที่ แผนกจัดซื้อ สมาคมสโมสรนักลงทุน โทรศัพท์ 02 666 9111 ต่อ 8006 หรือ 086 612 1183 (คุณเดือนรุ่ง) หรืออีเมล duenrungk@ic.or.th ในวันทำการ วันจันทร์–วันศุกร์ เวลา 09.00–16.00 น. ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ 10 สิงหาคม 2569

(นางสาวกรองกนก มานะกิจจงกล)

ผู้จัดการสมาคมสโมสรนักลงทุน

ขอบเขตงาน (Terms of Reference: TOR)
โครงการว่าจ้างบริการระบบติดตามและการประเมินตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ

1. หลักการและเหตุผล

ปัจจุบันการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศของสมาคมยังอาศัยการบันทึกและติดตามข้อมูลผ่านโปรแกรม Microsoft Word และ Microsoft Excel เป็นหลัก ซึ่งแม้จะสามารถรองรับการดำเนินงานในระดับพื้นฐานได้ แต่มีข้อจำกัดในการควบคุมคุณภาพข้อมูล การติดตามสถานะการดำเนินงานแบบเรียลไทม์ และการประเมินผลการปฏิบัติงานตามข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และตัวชี้วัดผลการดำเนินงาน (Key Performance Indicator: KPI) ส่งผลให้เกิดความเสี่ยงจากความผิดพลาดในการปฏิบัติงาน (Human Error) ความล่าช้าในการติดตามแก้ไขปัญหา และข้อจำกัดในการนำข้อมูลมาใช้ประกอบการตัดสินใจเชิงบริหาร

นอกจากนี้ การดำเนินงานด้านเทคโนโลยีสารสนเทศในปัจจุบันจำเป็นต้องมีระบบที่สามารถรวบรวม ติดตาม วิเคราะห์ และรายงานผลการให้บริการได้อย่างเป็นระบบ โปร่งใส และตรวจสอบได้ เพื่อรองรับการกำกับดูแลที่มีประสิทธิภาพ ตลอดจนการพัฒนาและปรับปรุงคุณภาพการให้บริการอย่างต่อเนื่อง

ดังนั้น สมาคมจึงมีความจำเป็นต้องจัดจ้างบริการระบบติดตามและประเมินผลตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ เพื่อใช้เป็นเครื่องมือกลางในการบริหารจัดการงานบริการไอทีอย่างครบวงจร โดยระบบดังกล่าวจะช่วยเพิ่มประสิทธิภาพในการติดตามสถานะงานและการแก้ไขปัญหา ควบคุมระยะเวลาการให้บริการให้เป็นไปตาม SLA ลดความเสี่ยงจากข้อผิดพลาดในการบันทึกข้อมูล และสนับสนุนการจัดทำรายงานผลการดำเนินงานที่ถูกต้อง ครบถ้วน และเป็นปัจจุบัน

ทั้งนี้ ระบบดังกล่าวยังเป็นกลไกสำคัญในการสนับสนุนการดำเนินงานให้สอดคล้องกับมาตรฐานสากลด้านการบริหารจัดการบริการเทคโนโลยีสารสนเทศ ISO/IEC 20000-1:2018 และมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 ช่วยเสริมสร้างความน่าเชื่อถือของกระบวนการปฏิบัติงาน เพิ่มประสิทธิภาพการกำกับติดตามผลการดำเนินงาน และยกระดับคุณภาพการให้บริการด้านเทคโนโลยีสารสนเทศของสมาคมฯ ให้สามารถรองรับการเติบโตและภารกิจขององค์กรได้อย่างยั่งยืนในอนาคต

2. วัตถุประสงค์

2.1 เพื่อพัฒนาระบบติดตามและประเมินผลการให้บริการด้านเทคโนโลยีสารสนเทศให้เป็นมาตรฐาน มีความถูกต้อง น่าเชื่อถือ และสามารถบริหารจัดการข้อมูล การติดตามสถานะงาน และการรายงานผลได้อย่างเป็นระบบและตรวจสอบได้

2.2 เพื่อเพิ่มประสิทธิภาพการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ โดยลดขั้นตอนการปฏิบัติงาน ลดความเสี่ยงจากความผิดพลาดในการบันทึกข้อมูล (Human Error) และเพิ่มความสามารถในการติดตาม ตรวจสอบ และควบคุมการดำเนินงานได้แบบเรียลไทม์

2.3 เพื่อสนับสนุนการติดตามและประเมินผลการปฏิบัติงานตามข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และตัวชี้วัดผลการดำเนินงาน (Key Performance Indicator: KPI) ให้เป็นไปอย่างมีประสิทธิภาพและสามารถนำข้อมูลไปใช้ประกอบการตัดสินใจเชิงบริหารได้

2.4 เพื่อสนับสนุนการดำเนินงานด้านการบริหารจัดการบริการเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับมาตรฐาน ISO/IEC 20000-1:2018 และ ISO/IEC 27001:2022 รวมถึงรองรับการตรวจประเมินและการพัฒนาองค์กรอย่างต่อเนื่อง

3. คุณสมบัติผู้เสนอราคา

3.1 ผู้เสนอราคาต้องเป็นนิติบุคคลที่จดทะเบียนจัดตั้งตามกฎหมายไทย มีฐานะทางการเงินที่มั่นคง โดยมีทุนจดทะเบียนชำระแล้วไม่น้อยกว่า 1,000,000 บาท ณ วันที่ยื่นข้อเสนอ และมีวัตถุประสงค์ในการประกอบกิจการด้านเทคโนโลยีสารสนเทศ คอมพิวเตอร์ ซอฟต์แวร์ ระบบบริหารจัดการบริการเทคโนโลยีสารสนเทศ (IT Service Management: ITSM) ความมั่นคงปลอดภัยสารสนเทศ หรือกิจการอื่นที่เกี่ยวข้อง

3.2 ผู้เสนอราคาต้องเป็นเจ้าของผลิตภัณฑ์ (Product Owner) หรือได้รับการแต่งตั้งเป็นตัวแทนจำหน่าย ตัวแทนให้บริการ หรือพันธมิตรทางธุรกิจอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์ ทั้งนี้ กรณีเสนอซอฟต์แวร์ประเภทโอเพนซอร์ส (Open Source Software) ผู้เสนอราคาต้องมีความสามารถในการติดตั้ง ปรับแต่ง พัฒนา บำรุงรักษา และให้บริการสนับสนุนซอฟต์แวร์ดังกล่าวตลอดระยะเวลาตามสัญญา โดยต้องปฏิบัติตามเงื่อนไขของสัญญาอนุญาตการใช้งาน (Open Source License) ที่เกี่ยวข้อง และแสดงเอกสารหรือหลักฐานที่แสดงถึงความสามารถในการให้บริการเพื่อประกอบการพิจารณา

3.3 ผู้เสนอราคาต้องมีประสบการณ์ในการให้บริการระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ (ITSM), Helpdesk, Service Desk หรือระบบติดตามและบริหารจัดการคำร้อง (Ticket Management System) ไม่น้อยกว่า 3 ปี และมีผลงานอ้างอิงไม่น้อยกว่า 3 โครงการ

3.4 ผู้เสนอราคาต้องมีบุคลากรที่มีความรู้ ความสามารถ และประสบการณ์ในการติดตั้ง ปรับแต่ง ดูแล และสนับสนุนการใช้งานระบบ โดยมีผู้รับผิดชอบโครงการ (Project Manager) หรือผู้เชี่ยวชาญประจำโครงการที่สามารถประสานงานกับสมาคมฯ ได้ตลอดระยะเวลาดำเนินโครงการ

3.5 ผู้เสนอราคาต้องมีทีมงานสนับสนุนทางเทคนิค (Technical Support) ในประเทศไทย และสามารถให้บริการผ่านช่องทางโทรศัพท์ อีเมล หรือระบบออนไลน์ได้ในวันและเวลาทำการ พร้อมกำหนดกระบวนการรับแจ้งเหตุและระยะเวลาการตอบสนองต่อปัญหา (Response Time) อย่างชัดเจน

3.6 ผู้เสนอราคาต้องสามารถให้บริการบำรุงรักษาระบบ (Maintenance Service) การแก้ไขข้อขัดข้อง (Corrective Maintenance) การอัปเดตเวอร์ชัน (Version Upgrade) และการแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Security Patch) ตลอดระยะเวลาสัญญา โดยไม่มีค่าใช้จ่ายเพิ่มเติม

3.7 ผู้เสนอราคาต้องไม่มีประวัติการถูกบอกเลิกสัญญาเนื่องจากการทิ้งงานหรือไม่ปฏิบัติตามสัญญาอย่างร้ายแรงกับหน่วยงานของรัฐหรือองค์กรเอกชนภายในระยะเวลา 3 ปีที่ผ่านมา

3.8 ระบบที่เสนอจะต้องอยู่ในรูปแบบ Software as a Service (SaaS) และสามารถใช้งานผ่านเครือข่ายอินเทอร์เน็ตได้ โดยไม่จำเป็นต้องติดตั้งระบบหลักภายในศูนย์ข้อมูลของสมาคม

3.9 ผู้เสนอราคาต้องมีใบรับรองมาตรฐาน ISO/IEC 27001:2022 หรือมาตรฐานสากลอื่นที่เทียบเท่า หากไม่มีผู้เสนอราคาต้องจัดส่งเอกสารนโยบายและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เพื่อประกอบการพิจารณาความน่าเชื่อถือของบริการ ทั้งนี้ ผู้เสนอราคาต้องเสนอศูนย์ข้อมูล (Cloud Data Center) ที่ใช้ในการให้บริการ ซึ่งได้รับการรับรองมาตรฐาน ISO/IEC 27001 และ ISO/IEC 27701 หรือมาตรฐานสากลอื่นที่เทียบเท่า

3.10 ผู้เสนอราคาต้องระบุสถานที่ตั้งของศูนย์ข้อมูล (Data Center) และประเทศที่จัดเก็บข้อมูลอย่างชัดเจน รวมทั้งต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และกฎหมายที่เกี่ยวข้อง

3.11 ผู้เสนอราคาต้องรับประกันความพร้อมใช้งานของระบบ (System Availability) ไม่น้อยกว่าร้อยละ 99.9 ต่อเดือน โดยต้องมีระบบเฝ้าระวังและบริหารจัดการเหตุขัดข้องตลอดระยะเวลาการให้บริการ พร้อมรายงานสถิติการให้บริการเมื่อสมาคมร้องขอ

3.12 ผู้เสนอราคาต้องมีมาตรการสำรองข้อมูล (Backup) และศูนย์สำรองระบบ (Disaster Recovery Site) หรือโครงสร้างพื้นฐานสำรองที่สามารถรองรับการให้บริการต่อเนื่องกรณีเกิดเหตุขัดข้อง พร้อมระบุค่า Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) อย่างชัดเจน โดยค่า RTO ต้องไม่เกิน 24 ชั่วโมง และค่า RPO ต้องไม่เกิน 24 ชั่วโมง

3.13 ระบบที่เสนอจะต้องรองรับการกำหนดสิทธิผู้ใช้งานตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) การบันทึกประวัติการใช้งาน (Audit Trail) และสามารถตรวจสอบย้อนหลังได้

3.14 การส่งมอบและการทำลายข้อมูลเมื่อสิ้นสุดสัญญา

3.14.1 เมื่อสัญญาสิ้นสุด ไม่ว่าจะเป็นการครบกำหนดอายุสัญญา การบอกเลิกสัญญา หรือการสิ้นสุดสัญญาก่อนกำหนดด้วยเหตุใดก็ตาม ผู้เสนอราคาต้องส่งมอบข้อมูลทั้งหมดของสมาคมให้แก่ผู้ว่าจ้างภายใน 7 วันทำการ นับจากวันที่สัญญาสิ้นสุด

3.14.2 ข้อมูลที่ส่งมอบต้องอยู่ในรูปแบบมาตรฐาน (Open Standard Format) ที่สามารถนำไปใช้งานต่อ หรืออัปโหลดเข้าสู่ระบบอื่นได้ (Data Portability) โดยอย่างน้อยต้องรองรับรูปแบบ CSV และ XLSX และหากระบบรองรับ ให้สามารถส่งออกข้อมูลในรูปแบบ JSON หรือรูปแบบมาตรฐานอื่นที่สามารถนำเข้าระบบสารสนเทศอื่นได้โดยไม่ต้องแปลงข้อมูลเพิ่มเติมอย่างมีนัยสำคัญ

3.14.3 ผู้เสนอราคาต้องส่งมอบข้อมูลให้ครบถ้วน ถูกต้อง และสามารถนำไปใช้งานได้จริง ตามข้อกำหนดในสัญญา

3.14.4 ภายหลังจากผู้ว่าจ้างตรวจสอบและยืนยันการรับมอบข้อมูลเรียบร้อยแล้ว ผู้เสนอราคาต้องดำเนินการลบหรือทำลายข้อมูลของสมาคมที่จัดเก็บอยู่ในระบบหลัก ระบบสำรองข้อมูล (Backup) และสื่อจัดเก็บข้อมูลอื่นที่เกี่ยวข้อง ภายใน 7 วันทำการ หรือตามระยะเวลาที่กฎหมายกำหนด หากมีกฎหมายกำหนดให้ต้องเก็บรักษาข้อมูลไว้เป็นระยะเวลานานกว่า

3.14.5 การลบหรือทำลายข้อมูลต้องเป็นไปตามกระบวนการที่ปลอดภัย สามารถตรวจสอบได้ และสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง

3.14.6 ภายหลังการลบหรือทำลายข้อมูลแล้ว ผู้เสนอราคาต้องจัดทำหนังสือรับรองการลบหรือทำลายข้อมูล (Certificate of Data Deletion/Destruction) หรือเอกสารหลักฐานอื่นที่เทียบเท่า เพื่อยืนยันว่าข้อมูลของสมาคมได้ถูกลบหรือทำลายเรียบร้อยแล้ว และไม่สามารถกู้คืนกลับมาใช้งานได้อีก

3.15 ผู้เสนอราคาต้องมีมาตรการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศหรือเหตุการณ์ที่ส่งผลกระทบต่อการให้บริการแก่สมาคม และต้องแจ้งให้สมาคมทราบภายใน 24 ชั่วโมงนับจากเวลาที่ตรวจพบเหตุการณ์ พร้อมรายงานสาเหตุ ผลกระทบ และแนวทางแก้ไข

3.16 ผู้เสนอราคาต้องสามารถสนับสนุนการดำเนินงานตามแนวทางมาตรฐาน ISO/IEC 20000-1:2018 และ ISO/IEC 27001:2022 โดยระบบที่เสนอจะต้องรองรับการบริหารจัดการข้อตกลงระดับการให้บริการ (SLA) การวัดผลตัวชี้วัดการปฏิบัติงาน (KPI) การจัดเก็บบันทึกและหลักฐานการดำเนินงาน (Audit Trail) รวมถึงการจัดทำรายงานเพื่อสนับสนุนการตรวจประเมินและการปรับปรุงกระบวนการอย่างต่อเนื่อง

3.17 กรณีผู้เสนอราคาเป็นผู้ให้บริการ Cloud หรือ Software as a Service (SaaS) จากต่างประเทศ หรือใช้โครงสร้างพื้นฐาน Cloud สาธารณะ (Public Cloud) ผู้เสนอราคาควรสามารถแสดงรายงานการตรวจสอบด้านการควบคุมภายในและความมั่นคงปลอดภัยสารสนเทศ เช่น SOC 2 Type II Report, ISO/IEC 27001:2022 หรือมาตรฐานสากลอื่นที่เทียบเท่า เพื่อประกอบการพิจารณาความน่าเชื่อถือของบริการ

3.18 ผู้เสนอราคาต้องดำเนินการติดตั้ง กำหนดค่า ทดสอบระบบ อบรมผู้ดูแลระบบและผู้ใช้งาน พร้อมจัดทำคู่มือการใช้งานและเอกสารประกอบการบริหารจัดการระบบก่อนส่งมอบงาน

3.19 ผู้เสนอราคาต้องเสนอรายละเอียดอัตราค่าบริการสำหรับการต่ออายุการใช้งานระบบภายหลังสิ้นสุดสัญญา รวมทั้งหลักเกณฑ์การปรับราคา (ถ้ามี) และเงื่อนไขการให้บริการภายหลังการต่ออายุ

3.20 ผู้เสนอราคาต้องเสนอรายละเอียดอัตราค่าบริการในการเพิ่มจำนวนผู้ใช้งาน (Additional User License) รวมถึงเงื่อนไข วิธีการ และระยะเวลาในการเพิ่มสิทธิการใช้งาน โดยต้องสามารถดำเนินการได้โดยไม่ส่งผลกระทบต่อการให้บริการของระบบ

3.21 ผู้เสนอราคาจะต้องปฏิบัติตามระเบียบปฏิบัติงานตามนโยบายและการบริหารเทคโนโลยีสารสนเทศฉบับผู้ให้บริการ (IT Policy and Management for Vendor) รหัสเอกสาร: IT-1PC-02 รายละเอียดตามเอกสารแนบท้าย TOR

4. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินการติดตั้ง กำหนดค่า ทดสอบ ส่งมอบ และให้บริการระบบติดตามและประเมินผลตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ ในรูปแบบ Software as a Service (SaaS) โดยระบบที่เสนอจะต้องรองรับการบริหารจัดการงานบริการเทคโนโลยีสารสนเทศตามแนวทางมาตรฐาน ISO/IEC 20000-1:2018 และมาตรฐาน ISO/IEC 27001:2022 รวมถึงมีคุณลักษณะและความสามารถอย่างน้อยดังต่อไปนี้

4.1 ระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ (IT Service Management)

4.1.1 รองรับการบริหารจัดการเหตุการณ์ผิดปกติ (Incident Management) และคำร้องขอรับบริการ (Service Request Management) ผ่าน Web Application หรือ Mobile Application

4.1.2 รองรับการบริหารจัดการปัญหา (Problem Management) เพื่อวิเคราะห์หาสาเหตุที่แท้จริงของปัญหา (Root Cause Analysis) และติดตามแนวทางการแก้ไขปัญหา

4.1.3 รองรับการบริหารจัดการการเปลี่ยนแปลง (Change Management) พร้อมกระบวนการอนุมัติ (Approval Workflow) ที่สามารถกำหนดลำดับการอนุมัติได้

4.1.4 รองรับการบริหารจัดการข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) โดยสามารถกำหนด SLA ตามประเภทบริการ ระดับความสำคัญของงาน และเวลาทำการ (Business Hours) ขององค์กรได้

4.1.5 รองรับการจัดทำ Service Catalog และการจัดหมวดหมู่บริการ เพื่อให้ผู้ใช้งานสามารถเลือกใช้บริการได้อย่างเหมาะสม

4.1.6 รองรับการประเมินความพึงพอใจของผู้รับบริการ (Customer Satisfaction: CSAT) และการสรุปผลการประเมินในรูปแบบรายงาน

4.1.7 รองรับการแจ้งเตือนและการยกระดับเหตุการณ์ (Notification & Escalation) อัตโนมัติ เมื่อใกล้หรือเกิน SLA ที่กำหนด

4.1.8 รองรับระบบ Self-Service Portal เพื่อให้ผู้ใช้งาน (พนักงานสมาคม) สามารถแจ้งปัญหา ติดตามสถานะงาน ค้นหาข้อมูล และประเมินความพึงพอใจได้ด้วยตนเอง

4.2 ระบบบริหารจัดการทรัพย์สินและองค์ประกอบบริการ (Asset & Configuration Management)

4.2.1 รองรับการบริหารจัดการข้อมูลทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) และ

4.2.2 รองรับการจัดเก็บข้อมูล Configuration Item (CI) และระบบฐานข้อมูลการจัดการองค์ประกอบบริการ (Configuration Management Database: CMDB)

4.2.3 รองรับการแสดงความสัมพันธ์ระหว่างอุปกรณ์ ระบบ และบริการในรูปแบบแผนภาพ (Relationship Mapping หรือ Service Topology)

4.3 ระบบควบคุมความมั่นคงปลอดภัยและการเข้าถึงข้อมูล

4.3.1 รองรับการกำหนดสิทธิการเข้าถึงข้อมูลตามบทบาทหน้าที่ (Role-Based Access Control: RBAC)

4.3.2 รองรับหลักการจำกัดสิทธิเท่าที่จำเป็น (Principle of Least Privilege)

4.3.3 รองรับการแยกหน้าที่และความรับผิดชอบ (Segregation of Duties)

4.3.4 รองรับการกำหนดนโยบายรหัสผ่าน (Password Policy) และการกำหนดระยะเวลาหมดอายุของการใช้งานระบบ (Session Timeout)

4.3.5 ข้อมูลที่จัดเก็บและข้อมูลที่รับส่งผ่านเครือข่ายต้องได้รับการเข้ารหัสตามมาตรฐานสากลที่เหมาะสม

4.3.6 รองรับการบันทึกประวัติการใช้งานและการเปลี่ยนแปลงข้อมูล (Audit Trail) โดยสามารถตรวจสอบย้อนหลังได้

4.3.7 รองรับการแนบเอกสาร รูปภาพ วิดีโอ หรือหลักฐานประกอบการปฏิบัติงานในแต่ละรายการ

4.4 ระบบบริหารจัดการองค์ความรู้ด้านการให้บริการเทคโนโลยีสารสนเทศ (IT Service Knowledge Management)

4.4.1 รองรับการจัดเก็บวิธีแก้ไขปัญหาชั่วคราว (Workaround) และวิธีแก้ไขปัญหาถาวร (Known Error Resolution)

4.4.2 รองรับการจัดหมวดหมู่ ค้นหา และเรียกใช้องค์ความรู้เพื่อสนับสนุนการแก้ไขปัญหาและการให้บริการ

4.5 ระบบรายงานผลและแดชบอร์ด

4.5.1 รองรับ Dashboard แบบ Real-Time สำหรับติดตามสถานะการให้บริการ

4.5.2 รองรับ Dashboard สำหรับผู้บริหาร (Executive Dashboard) เพื่อใช้ติดตาม วิเคราะห์ และประเมินผลการดำเนินงานด้านการให้บริการเทคโนโลยีสารสนเทศ โดยสามารถแสดงผลข้อมูลสำคัญ (Key Performance Indicators) ได้แบบ Real-Time หรือใกล้เคียง Real-Time อย่างน้อยประกอบด้วย สถานะการปฏิบัติตาม SLA ผลการดำเนินงานตาม KPI จำนวนและสถานะของ Incident, Service Request, Problem และ Change Management รวมถึงสามารถแสดงผลการปฏิบัติงานในระดับรายบุคคล รายทีม และภาพรวมขององค์กรได้

4.5.3 รองรับการจัดทำรายงานมาตรฐานและรายงานเชิงวิเคราะห์ เช่น

4.5.3.1 SLA Dashboard & Performance Report

4.5.3.2 KPI Performance Report

4.5.3.3 Incident & Service Request Report

4.5.3.4 Problem Analysis Report

4.5.3.5 Asset History Report

4.5.3.6 User Access Log Report

4.5.3.7 Audit Trail Report

4.5.3.8 Vendor & Contract Report

4.5.3.9 Customer Satisfaction Report

4.5.4 สามารถส่งออกรายงานในรูปแบบ Excel, CSV หรือ PDF ได้

4.6 ความต่อเนื่องทางธุรกิจและการคุ้มครองข้อมูล

4.6.1 ผู้รับจ้างต้องมีระบบสำรองข้อมูลและการกู้คืน (Data Backup and Recovery) โดยระบบจะต้องทำการสำรองข้อมูลทุกวัน โดยสามารถกู้คืนข้อมูลย้อนหลังได้ 90 วัน และต้องมีศูนย์สำรองระบบ (Disaster Recovery Site) หรือโครงสร้างพื้นฐานสำรองที่สามารถรองรับการให้บริการต่อเนื่องเมื่อเกิดเหตุขัดข้อง

4.6.2 ผู้รับจ้างต้องกำหนดและแจ้งค่า Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) อย่างชัดเจน เป็นไปตามข้อ 3.12

4.6.3 ผู้รับจ้างต้องมีการทดสอบแผนกู้คืนระบบ (Disaster Recovery Test) อย่างน้อยปีละ 1 ครั้ง และสามารถแสดงหลักฐานการทดสอบได้เมื่อสมาคมร้องขอ

4.6.4 ผู้รับจ้างต้องมีนโยบายการจัดเก็บข้อมูล (Data Retention Policy) และการจัดการ Log ที่สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง

4.6.5 ผู้รับจ้างต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และกฎหมายที่เกี่ยวข้อง

4.6.6 ผู้รับจ้างต้องมีมาตรการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Security Incident Notification) ให้สมาคมทราบภายในระยะเวลาที่กำหนด พร้อมรายงานสาเหตุ ผลกระทบ และแนวทางแก้ไข

4.6.7 เมื่อสิ้นสุดสัญญา ผู้รับจ้างต้องสามารถส่งมอบข้อมูลทั้งหมดของสมาคมในรูปแบบมาตรฐานที่สามารถนำไปใช้งานต่อได้ และดำเนินการลบหรือทำลายข้อมูลตามกระบวนการที่สามารถตรวจสอบได้ พร้อมจัดทำหนังสือรับรองการลบข้อมูล (Certificate of Data Deletion/Destruction)

5. ระยะเวลาดำเนินโครงการ

5.1 ระยะเวลาติดตั้งและส่งมอบระบบ: ผู้รับจ้างต้องดำเนินการวิเคราะห์ความต้องการ ติดตั้ง กำหนดค่า ทดสอบนำเข้าข้อมูล (ถ้ามี) ฝึกอบรม ส่งมอบเอกสาร และเปิดใช้งานจริง (Go-Live) ให้แล้วเสร็จภายใน 60 วัน ปฏิทินนับถัดจากวันลงนามในสัญญา โดยวัน Go-Live ต้องไม่เกินวันสุดท้ายของระยะเวลาดังกล่าว

5.2 ระยะเวลาให้บริการระบบ: 12 เดือน เริ่มนับตั้งแต่วันที่ระบุเป็นวันเปิดใช้งานจริง (Go-Live) ในเอกสารตรวจรับงานงวดที่ 1 และสิ้นสุดเมื่อครบกำหนด 12 เดือนนับจากวันดังกล่าว

6. การส่งมอบงาน

ผู้รับจ้างต้องดำเนินการติดตั้ง กำหนดค่า ทดสอบ ฝึกอบรม และส่งมอบระบบให้พร้อมใช้งานจริง (Go-Live) ตามขอบเขตงานที่กำหนด ภายในระยะเวลาที่กำหนดในสัญญา โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

6.1 จัดเตรียมระบบพร้อมสิทธิการใช้งานตามจำนวนที่กำหนด

6.2 กำหนดค่าระบบพื้นฐาน (System Configuration)

6.3 กำหนดบทบาทและสิทธิการใช้งานตาม Access Control Matrix

6.4 กำหนดค่า SLA, KPI, Workflow และ Dashboard ตามที่ผู้ว่าจ้างกำหนด

6.5 จัดเตรียมระบบสำรองข้อมูล (Backup) และการกู้คืนระบบ (Disaster Recovery)

6.6 จัดทำแผนดำเนินโครงการ (Project Plan)

6.7 ดำเนินการนำเข้าข้อมูล (Data Migration) (ถ้ามี)

6.8 ดำเนินการทดสอบระบบร่วมกับผู้ว่าจ้าง และแก้ไขข้อบกพร่องที่พบ

6.9 จัดส่งรายงานผลการทดสอบระบบ (System Test Report)

6.10 จัดส่งรายงานผลการทดสอบการยอมรับระบบโดยผู้ใช้งาน (User Acceptance Test: UAT)

6.11 จัดส่งรายงานผลการทดสอบการสำรองและกู้คืนข้อมูล (Backup Recovery Test Report)

6.12 ฝึกอบรมผู้ดูแลระบบและผู้ใช้งาน

6.13 ส่งมอบคู่มือการใช้งาน คู่มือผู้ดูแลระบบ เอกสารการตั้งค่าระบบ และรายงานสรุปผลการดำเนินโครงการ รวมทั้งคำอธิบายโครงสร้างข้อมูล (Data Dictionary) และ/หรือเอกสารอธิบายรูปแบบข้อมูล (Data Schema) ที่จำเป็นสำหรับการใช้งาน การบำรุงรักษา และการเชื่อมโยงข้อมูลกับระบบอื่น (ถ้ามี)

6.14 ส่งมอบรายงานการกำหนดสิทธิผู้ใช้งาน (User Role & Permission Configuration Report)

6.15 ส่งมอบหนังสือรับประกันการให้บริการและการบำรุงรักษาระบบ

6.16 เปิดใช้งานระบบจริง (Go-Live) และเริ่มให้บริการตามสัญญา

ทั้งนี้ การส่งมอบงานจะถือว่าแล้วเสร็จเมื่อผู้ว่าจ้างตรวจรับระบบและเอกสารประกอบครบถ้วน และระบบสามารถใช้งานได้จริงตามขอบเขตงานที่กำหนด

7. เงื่อนไขการจ่ายเงิน

การชำระเงินแบ่งออกเป็น 2 ส่วน ดังนี้

7.1 ค่าดำเนินการติดตั้งและปรับแต่งระบบ (Implementation Service)

ผู้ว่าจ้างจะชำระค่าดำเนินการติดตั้งและปรับแต่งระบบ 100% ของค่าดำเนินการติดตั้ง เมื่อผู้รับจ้างดำเนินการส่งมอบงานตามข้อ 6 ครบถ้วน ระบบผ่านการทดสอบการยอมรับจากผู้ใช้งาน (User Acceptance Test: UAT) สามารถเปิดใช้งานจริง (Go-Live) และได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุและการจ้าง

7.2 ค่าบริการระบบรายปี (Subscription / SaaS Service)

ผู้ว่าจ้างจะชำระค่าบริการระบบรายปีเป็น 4 งวด งวดละร้อยละ 25 ของค่าบริการรายปี โดยมีรายละเอียดเงื่อนไขการชำระเงิน ดังนี้

งวดที่ 1 เมื่อผู้รับจ้างเปิดให้บริการระบบ (Go-Live) และให้บริการครบ 3 เดือน พร้อมปฏิบัติตามข้อตกลงระดับการให้บริการ (SLA) และได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุและการจ้าง

งวดที่ 2 เมื่อผู้รับจ้างให้บริการครบ 6 เดือน และปฏิบัติตาม SLA

งวดที่ 3 เมื่อผู้รับจ้างให้บริการครบ 9 เดือน และปฏิบัติตาม SLA

งวดที่ 4 เมื่อผู้รับจ้างให้บริการครบ 12 เดือน และปฏิบัติตาม SLA พร้อมส่งมอบรายงานการให้บริการประจำปี และได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุและการจ้าง

ทั้งนี้ การชำระเงินในแต่ละงวด ผู้รับจ้างต้องไม่มีเหตุผิดสัญญา และต้องปฏิบัติตามข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ตามที่กำหนดไว้ในสัญญา

8. ค่าปรับ

ในกรณีที่ผู้รับจ้างไม่สามารถดำเนินการส่งมอบงานให้แล้วเสร็จภายในระยะเวลาที่กำหนดตามสัญญา และมิใช่เหตุสุดวิสัยหรือเหตุอันเกิดจากผู้ว่าจ้าง ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้างในอัตราร้อยละ 0.10 ของวงเงินตามสัญญาต่อวัน นับถัดจากวันครบกำหนดส่งมอบงานจนถึงวันที่ส่งมอบงานแล้วเสร็จและได้รับการตรวจรับจากผู้ว่าจ้าง

การคิดค่าปรับดังกล่าวไม่ตัดสิทธิของผู้ว่าจ้างในการเรียกร้องค่าเสียหายอื่นใดที่เกิดขึ้นจริงอันเนื่องมาจากการส่งมอบงานล่าช้าของผู้รับจ้าง

9. หลักเกณฑ์การพิจารณาคัดเลือก

9.1 คณะกรรมการจะพิจารณาคุณสมบัติของผู้เสนอราคาตามข้อกำหนดใน TOR หากผู้เสนอราคารายใดมีคุณสมบัติครบถ้วน สมาคมสโมสรนักลงทุนอาจเชิญผู้เสนอราคามานำเสนอรายละเอียดระบบ (Presentation) และสาธิตการใช้งานระบบ (System Demonstration) ต่อคณะกรรมการ โดยกำหนดเวลานำเสนอรายละไม่เกิน 120 นาที และช่วงตอบข้อซักถามไม่เกิน 30 นาที ทั้งนี้ วัน เวลา และสถานที่ สมาคมสโมสรนักลงทุนจะแจ้งให้ทราบต่อไป

9.2 สมาคมสโมสรนักลงทุนจะพิจารณาคัดเลือกจากผู้เสนอราคาที่ได้คะแนนสูงสุดด้านเทคนิคเป็นอันดับแรก ทั้งนี้ การคัดเลือกจะใช้วิธีประสิทธิภาพต่อราคา และขอสงวนสิทธิไม่พิจารณาเลือกจากผู้เสนอราคาต่ำสุด

9.3 ผู้เสนอราคาต้องจัดส่งข้อมูลเพื่อประกอบการพิจารณา อย่างน้อยดังนี้

9.3.1 รายละเอียดบริษัท ประสบการณ์ และผลงานที่เกี่ยวข้อง

9.3.2 รายละเอียดบุคลากรหลัก ผู้จัดการโครงการ และทีมงานที่จะรับผิดชอบโครงการ

9.3.3 รายละเอียดคุณสมบัติเพิ่มเติมของระบบ (Value Added Features) ที่นอกเหนือจากข้อกำหนดขั้นต่ำใน TOR พร้อมระบุว่ามีค่าใช้จ่ายเพิ่มเติมหรือไม่

9.3.4 แผนการดำเนินโครงการ (Project Plan)

9.3.5 เอกสารสถาปัตยกรรมระบบ (System Architecture)

9.3.6 รายละเอียดคุณลักษณะของระบบ (System Functional Specification)

9.3.7 แผนการฝึกอบรมและการถ่ายทอดความรู้

9.3.8 แผนการให้บริการหลังการขาย (Support & Maintenance)

9.4 ผู้เสนอราคาที่จะได้รับการพิจารณาด้านราคา ต้องมีคะแนนด้านเทคนิค ไม่น้อยกว่า 80 คะแนน

9.5 เมื่อผ่านเกณฑ์ตามข้อ 9.4 แล้ว สมาคมสโมสรนักลงทุนจึงจะเปิดซองราคา และจะพิจารณาคัดเลือกจากผู้เสนอราคาที่เสนอราคาไม่เกินวงเงินงบประมาณ โดยใช้หลักประสิทธิภาพต่อราคา ทั้งนี้ การตัดสินของคณะกรรมการถือเป็นที่สุด

เกณฑ์การพิจารณาให้คะแนน	**คะแนนสูงสุด**
1. คุณสมบัติและประสบการณ์ของบริษัทและทีมงาน	15 คะแนน
2. ความสามารถของระบบตาม TOR และการสาธิตการใช้งาน (Presentation & Demonstration)	40 คะแนน
3. แผนการดำเนินโครงการ ทีมงาน การติดตั้ง การอบรม และการสนับสนุนหลังการขาย	20 คะแนน
4. ความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูล และความ	15 คะแนน

เกณฑ์การพิจารณาให้คะแนน	คะแนนสูงสุด
ต่อเนื่องในการให้บริการ (Security, PDPA, Backup, DR, SLA)	
5. คุณสมบัติเพิ่มเติมของระบบและบริการ (Value Added Features)	10 คะแนน
รวมคะแนน	**100 คะแนน**

หมายเหตุ: รายละเอียดหลักเกณฑ์การประเมินหัวข้อ คุณสมบัติเพิ่มเติมของระบบและบริการ (Value Added Features) ให้เป็นไปตาม ภาคผนวก ง เกณฑ์การประเมินข้อเสนอด้านเทคนิค

10. ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)

10.1 ผู้รับจ้างต้องรับประกันความพร้อมใช้งานของระบบ (System Availability) ไม่น้อยกว่าร้อยละ 99.9 ต่อเดือน ตลอดระยะเวลาการให้บริการตามสัญญา โดยไม่นับรวมช่วงเวลาการบำรุงรักษาระบบตามแผนงาน (Scheduled Maintenance) ที่ได้แจ้งให้ผู้ว่าจ้างทราบล่วงหน้าไม่น้อยกว่า 7 วันทำการ

10.2 ผู้รับจ้างต้องจัดให้มีช่องทางรับแจ้งเหตุขัดข้องและให้บริการสนับสนุนทางเทคนิคแก่ผู้ว่าจ้างตลอดระยะเวลาสัญญา โดยอย่างน้อยต้องสามารถติดต่อผ่านโทรศัพท์ อีเมล หรือระบบออนไลน์ได้ในวันและเวลาทำการ (08.30-17.30 น.)

10.3 ผู้รับจ้างต้องดำเนินการตอบสนองและแก้ไขปัญหาตามระดับความรุนแรงของเหตุการณ์ ดังนี้

ระดับความรุนแรง	ลักษณะเหตุการณ์	ระยะเวลาตอบสนอง (Response Time)	ระยะเวลาแก้ไขเบื้องต้น (Resolution Time)
Critical	ระบบไม่สามารถใช้งานได้ทั้งหมด หรือส่งผลกระทบต่อการดำเนินงานหลักขององค์กร	ไม่เกิน 2 ชั่วโมงทำการ	ไม่เกิน 4 ชั่วโมงทำการ
High	ระบบบางส่วนไม่สามารถใช้งานได้ หรือส่งผลกระทบต่อผู้ใช้งานจำนวนมาก	ไม่เกิน 2 ชั่วโมงทำการ	ไม่เกิน 1 วันทำการ
Medium	ระบบมีข้อขัดข้องที่ยังมีแนวทางปฏิบัติงานทดแทนได้	ไม่เกิน 4 ชั่วโมงทำการ	ไม่เกิน 2 วันทำการ
Low	ข้อเสนอแนะ ปัญหาเล็กน้อย หรือการขอคำปรึกษาทั่วไป	ไม่เกิน 6 ชั่วโมงทำการ	ไม่เกิน 3 วันทำการ

10.4 ผู้รับจ้างต้องสามารถจัดทำและส่งมอบรายงานสรุประดับการให้บริการ (Service Level Agreement Report: SLA Report) เป็นรายเดือน โดยอย่างน้อยต้องแสดงข้อมูลดังต่อไปนี้

(1) ระดับความพร้อมใช้งานของระบบ (System Availability)

(2) ระยะเวลาหยุดให้บริการ (Downtime) และสาเหตุของเหตุขัดข้อง

(3) สถิติการรับแจ้งเหตุและการให้บริการ (Incident และ Service Request)

(4) ผลการปฏิบัติตาม SLA ทั้งด้าน Response Time และ Resolution Time

(5) สถิติการใช้งานระบบและข้อมูลที่เกี่ยวข้องกับการให้บริการ

ทั้งนี้ ผู้ว่าจ้างสามารถร้องขอรายงานดังกล่าวได้ตลอดระยะเวลาของสัญญา

10.5 กรณีผู้รับจ้างไม่สามารถรักษาระดับความพร้อมใช้งานของระบบ (System Availability) ได้ตามข้อ 10.1 ผู้รับจ้างต้องชดเชยให้แก่ผู้ว่าจ้างโดยการขยายระยะเวลาการให้บริการเพิ่มเติมโดยไม่มีค่าใช้จ่าย ตามเกณฑ์ดังต่อไปนี้

ระดับความพร้อมใช้งานของระบบต่อเดือน	**การชดเชย**
ตั้งแต่ 99.90% ขึ้นไป	ไม่มีการชดเชย
99.00% - 99.89%	ขยายระยะเวลาการให้บริการ 7 วัน
98.00% - 98.99%	ขยายระยะเวลาการให้บริการ 15 วัน
ต่ำกว่า 98.00%	ขยายระยะเวลาการให้บริการ 30 วัน

10.6 กรณีผู้รับจ้างไม่สามารถปฏิบัติตามระยะเวลาการตอบสนอง (Response Time) หรือระยะเวลาการแก้ไขปัญหา (Resolution Time) ตามข้อ 10.3 ได้เกินกว่า 3 ครั้งภายในรอบระยะเวลา 12 เดือน ผู้ว่าจ้างมีสิทธิเรียกประชุมร่วมกับผู้รับจ้างเพื่อวิเคราะห์สาเหตุของปัญหา (Root Cause Analysis) และจัดทำแผนแก้ไขและปรับปรุงคุณภาพการให้บริการ (Corrective Action Plan) โดยผู้รับจ้างต้องจัดส่งแผนแก้ไขและปรับปรุงคุณภาพการให้บริการเป็นลายลักษณ์อักษรภายใน 15 วันนับจากวันที่ได้รับแจ้งจากผู้ว่าจ้าง ซึ่งอย่างน้อยต้องประกอบด้วย

(1) การวิเคราะห์สาเหตุของปัญหาและผลกระทบที่เกิดขึ้น

(2) มาตรการแก้ไขปัญหาระยะสั้น (Corrective Action)

(3) มาตรการป้องกันไม่ให้เกิดเหตุซ้ำ (Preventive Action)

(4) ระยะเวลาดำเนินการและผู้รับผิดชอบ

(5) ตัวชี้วัดผลสำเร็จของการปรับปรุงคุณภาพการให้บริการ

ในกรณีที่ผู้รับจ้างไม่ดำเนินการตามแผนดังกล่าว หรือยังคงไม่สามารถรักษาระดับการให้บริการตามที่กำหนดได้ ผู้ว่าจ้างมีสิทธิเรียกร้องให้ผู้รับจ้างดำเนินมาตรการแก้ไขเพิ่มเติม เรียกร้องค่าชดเชยตามข้อตกลงระดับการให้บริการ (Service Credit) หรือพิจารณาดำเนินการตามสิทธิและหน้าที่ที่กำหนดไว้ในสัญญา รวมถึงการบอกเลิกสัญญาในกรณีที่มีการผิดสัญญาอย่างมีนัยสำคัญ

10.7 ผู้รับจ้างต้องแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Security Incident) ที่ส่งผลกระทบต่อข้อมูลหรือการให้บริการของผู้ว่าจ้าง ภายใน 24 ชั่วโมงนับจากเวลาที่ตรวจพบเหตุการณ์ พร้อมรายงานสาเหตุ ผลกระทบ และแนวทางการแก้ไขป้องกันไม่ให้เกิดซ้ำ

11. การระงับงานชั่วคราวและการบอกเลิกสัญญา

11.1 ผู้ว่าจ้างมีสิทธิสั่งระงับการดำเนินงานทั้งหมดหรือบางส่วนเป็นการชั่วคราว หากตรวจพบว่าผู้รับจ้างดำเนินงานไม่เป็นไปตามขอบเขตงาน คุณลักษณะเฉพาะ เงื่อนไขของสัญญา หรือมาตรฐานที่กำหนดไว้ และอาจส่งผลกระทบต่อคุณภาพ ความมั่นคงปลอดภัยของข้อมูล หรือการดำเนินงานของผู้ว่าจ้าง

11.2 เมื่อผู้ว่าจ้างมีคำสั่งระงับงาน ผู้รับจ้างต้องดำเนินการแก้ไขข้อบกพร่องหรือข้อไม่สอดคล้องตามที่ได้รับแจ้ง และรายงานผลการแก้ไขให้ผู้ว่าจ้างทราบภายในระยะเวลาที่ผู้ว่าจ้างกำหนด ทั้งนี้ต้องไม่เกิน 15 วันนับถัดจากวันที่ได้รับแจ้ง เว้นแต่ผู้ว่าจ้างจะเห็นชอบให้ขยายระยะเวลาเป็นลายลักษณ์อักษร

11.3 ในกรณีที่ผู้รับจ้างไม่ดำเนินการแก้ไขภายในระยะเวลาที่กำหนด หรือไม่สามารถแก้ไขให้เป็นไปตามข้อกำหนดของสัญญาได้ ผู้ว่าจ้างมีสิทธิคงคำสั่งระงับงานไว้จนกว่าผู้รับจ้างจะดำเนินการแก้ไขแล้วเสร็จ หรือดำเนินการตามสิทธิและหน้าที่ที่กำหนดไว้ในสัญญา รวมถึงการเรียกค่าปรับ การเรียกค่าเสียหาย หรือการบอกเลิกสัญญาแล้วแต่กรณี

11.4 ผู้ว่าจ้างมีสิทธิบอกเลิกสัญญาได้ทั้งหมดหรือบางส่วน โดยไม่ต้องรับผิดชอบค่าเสียหายใด ๆ ต่อผู้รับจ้าง หากเกิดกรณีใดกรณีหนึ่งดังต่อไปนี้

(1) ผู้รับจ้างไม่สามารถดำเนินการติดตั้ง กำหนดค่า ทดสอบ หรือส่งมอบระบบให้แล้วเสร็จภายในระยะเวลาที่กำหนดตามสัญญา และไม่สามารถชี้แจงเหตุผลอันสมควรได้

(2) ผู้รับจ้างไม่สามารถรักษาระดับการให้บริการ (Service Level Agreement: SLA) ตามที่กำหนดไว้ในสัญญาอย่างต่อเนื่อง และไม่ดำเนินการแก้ไขหรือปรับปรุงคุณภาพการให้บริการภายหลังได้รับแจ้งจากผู้ว่าจ้าง

(3) ผู้รับจ้างฝ่าฝืนข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล หรือเงื่อนไขสำคัญอื่นตามสัญญา จนก่อให้เกิดความเสียหายแก่ผู้ว่าจ้าง

(4) ผู้รับจ้างโอนสิทธิ หน้าที่ หรือมอบหมายงานตามสัญญาให้บุคคลอื่นดำเนินการแทนทั้งหมดหรือบางส่วนโดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง

(5) ผู้รับจ้างตกเป็นบุคคลล้มละลาย ถูกพิทักษ์ทรัพย์ หรือมีเหตุอันควรเชื่อได้ว่าไม่สามารถดำเนินการตามสัญญาได้ต่อไป

(6) ผู้รับจ้างยุติการให้บริการผลิตภัณฑ์หรือประกาศเลิกสนับสนุนผลิตภัณฑ์ (End of Support / End of Service) ในระหว่างอายุสัญญา และไม่สามารถจัดหาทางเลือกที่มีคุณสมบัติเทียบเท่าให้แก่ผู้ว่าจ้างได้

11.5 การบอกเลิกสัญญาตามข้อ 11.4 ไม่กระทบต่อสิทธิของผู้ว่าจ้างในการเรียกค่าปรับ ค่าเสียหาย หรือสิทธิอื่นใดตามที่กำหนดไว้ในสัญญาและตามกฎหมาย

12. สิทธิในทรัพย์สินทางปัญญาและความเป็นเจ้าของข้อมูล

12.1 ข้อมูล เอกสาร รายงาน สถิติ ข้อมูลการดำเนินงาน ข้อมูลผู้ใช้งาน และข้อมูลอื่นใดที่ผู้ว่าจ้างบันทึก จัดเก็บ หรือประมวลผลผ่านระบบตามสัญญานี้ ให้ถือเป็นกรรมสิทธิ์ของผู้ว่าจ้างแต่เพียงผู้เดียว

12.2 ผู้รับจ้างไม่มีสิทธิเปิดเผย เผยแพร่ โอน จำหน่าย หรือใช้ประโยชน์จากข้อมูลของผู้ว่าจ้างไม่ว่าทั้งหมดหรือบางส่วน เว้นแต่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง หรือเป็นกรณีที่กฎหมายกำหนด

12.3 ผู้รับจ้างต้องจัดให้ผู้ว่าจ้างสามารถเข้าถึง เรียกดู ส่งออก และรับมอบข้อมูลทั้งหมดของผู้ว่าจ้างได้ตลอดระยะเวลาการให้บริการ และเมื่อสิ้นสุดสัญญาตามเงื่อนไขที่กำหนดไว้ในสัญญา

12.4 ลิขสิทธิ์ สิทธิในทรัพย์สินทางปัญญา สิทธิในซอฟต์แวร์ต้นฉบับ (Source Code) โปรแกรมคอมพิวเตอร์ เครื่องหมายการค้า สิทธิบัตร ฐานข้อมูลเชิงระบบ และองค์ประกอบอื่นใดของระบบที่ผู้รับจ้างเป็นผู้พัฒนาหรือเป็นเจ้าของก่อนวันทำสัญญา ให้ยังคงเป็นกรรมสิทธิ์ของผู้รับจ้างหรือเจ้าของผลิตภัณฑ์ตามกฎหมาย

12.5 การที่ผู้ว่าจ้างได้รับสิทธิใช้งานระบบตามสัญญานี้ ไม่ถือเป็นการโอนกรรมสิทธิ์หรือสิทธิในทรัพย์สินทางปัญญาของซอฟต์แวร์ให้แก่ผู้ว่าจ้าง เว้นแต่จะมีข้อตกลงเป็นลายลักษณ์อักษรระหว่างคู่สัญญาเป็นอย่างอื่น

12.6 ผู้รับจ้างต้องรักษาความลับและความมั่นคงปลอดภัยของข้อมูลของผู้ว่าจ้างตลอดระยะเวลาสัญญาและภายหลังสิ้นสุดสัญญา ตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

12.7 ผู้รับจ้างไม่มีสิทธินำข้อมูลของผู้ว่าจ้างไปใช้เพื่อการวิเคราะห์ การตลาด การพัฒนาแบบจำลองปัญญาประดิษฐ์ (AI Model Training) หรือวัตถุประสงค์อื่นใด เว้นแต่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง

ภาคผนวก ก.

ตารางข้อตกลงระดับการให้บริการ (SLA Matrix)

1. System Availability

รายการ	**ข้อกำหนด**
System Availability	ไม่น้อยกว่า 99.9% ต่อเดือน
Scheduled Maintenance	แจ้งล่วงหน้าไม่น้อยกว่า 7 วันทำการ
SLA Report	จัดส่งเมื่อผู้ว่าจ้างร้องขอ

2. Response Time และ Resolution Time

Severity Level	**รายละเอียด**	**Response Time**	**Resolution Time**
Critical	ระบบไม่สามารถใช้งานได้ทั้งหมด หรือส่งผลกระทบต่อการดำเนินงานหลักขององค์กร	ไม่เกิน 2 ชั่วโมงทำการ	ไม่เกิน 4 ชั่วโมงทำการ
High	ระบบบางส่วนไม่สามารถใช้งานได้ หรือส่งผลกระทบต่อผู้ใช้งานจำนวนมาก	ไม่เกิน 2 ชั่วโมงทำการ	ไม่เกิน 1 วันทำการ
Medium	ระบบมีข้อขัดข้องแต่ยังมีแนวทางปฏิบัติงานทดแทนได้	ไม่เกิน 4 ชั่วโมงทำการ	ไม่เกิน 2 วันทำการ
Low	ข้อเสนอแนะ ปัญหาเล็กน้อย หรือการขอคำปรึกษาทั่วไป	ไม่เกิน 6 ชั่วโมงทำการ	ไม่เกิน 3 วันทำการ

3. Service Credit

Availability ต่อเดือน	**การชดเชย**
ตั้งแต่ 99.90% ขึ้นไป	ไม่มีการชดเชย
99.00% – 99.89%	ขยายระยะเวลาการให้บริการ 7 วัน
98.00% – 98.99%	ขยายระยะเวลาการให้บริการ 15 วัน
ต่ำกว่า 98.00%	ขยายระยะเวลาการให้บริการ 30 วัน

ภาคผนวก ข.

รายการผู้ใช้งานระบบ (License Subscription)

จำนวนผู้ใช้งานรวมทั้งสิ้น 25 สิทธิ (Named User License)

ประเภทผู้ใช้งาน	**จำนวน**
System Administrator	1
IT Manager / Supervisor	2
IT Staff (Technician)	7
User / Branch Staff	15
รวม	**25**

ผู้ว่าจ้างสามารถปรับเปลี่ยนรายชื่อผู้ใช้งานภายในจำนวนสิทธิที่จัดซื้อได้ตลอดอายุสัญญา โดยไม่ถือเป็นการเพิ่มจำนวนสิทธิการใช้งาน

ภาคผนวก ค.

รายการโมดูลที่จัดซื้อ

ระบบที่เสนอจะต้องประกอบด้วยโมดูลอย่างน้อยดังต่อไปนี้

1. Incident Management
2. Service Request Management
3. Problem Management
4. Change Management
5. Service Level Management (SLA)
6. KPI Dashboard & Executive Dashboard
7. Service Catalog
8. Knowledge Management
9. IT Asset Management
10. Fixed Asset Management
11. Configuration Management Database (CMDB)
12. Supplier & Contract Management
13. User & Role Management
14. Audit Trail & Activity Log
15. Reporting & Analytics
16. Self-Service Portal
17. Mobile Application
18. Backup & Disaster Recovery
19. Security Incident Logging
20. Data Export & Data Retention Management

ทั้งนี้ ผู้รับจ้างต้องจัดให้โมดูลทั้งหมดสามารถใช้งานร่วมกันได้ภายใต้แพลตฟอร์มเดียว และรวมอยู่ในค่าบริการตามสัญญาโดยไม่มีค่าใช้จ่ายเพิ่มเติมตลอดระยะเวลาสัญญา

ภาคผนวก ง.

เกณฑ์การประเมินข้อเสนอด้านเทคนิค

หัวข้อที่ 5 คุณสมบัติเพิ่มเติมของระบบและบริการ (Value Added Features)

ลำดับ	รายการพิจารณา	แนวทางการพิจารณา	คะแนน
1	การรองรับการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA)	รองรับโดยไม่มีค่าใช้จ่ายเพิ่มเติม	2
2	การรองรับการยืนยันตัวตนแบบ Single Sign-On (SSO)	รองรับการเชื่อมต่อกับระบบ Identity Provider ขององค์กร	2
3	การเชื่อมต่อระบบผ่าน API	รองรับการเชื่อมต่อกับระบบอื่นผ่านมาตรฐาน API	2
4	สามารถเพิ่มหรือลดจำนวนผู้ใช้งาน (User License) ได้อย่างยืดหยุ่น	โดยไม่มีค่าใช้จ่ายในการเปลี่ยน Edition หรือมีเงื่อนไขที่เป็นประโยชน์	2
5	เงื่อนไขการต่ออายุการใช้บริการ	มีเงื่อนไขที่เป็นประโยชน์ต่อสมาคม เช่น การควบคุมการปรับราคา ส่วนลด หรือสิทธิประโยชน์เพิ่มเติม	2

หมายเหตุ: คณะกรรมการจะพิจารณาให้คะแนนตามรายละเอียดและความเหมาะสมของคุณสมบัติที่ผู้เสนอราคาเสนอ ทั้งนี้ หากผู้เสนอราคามีคุณสมบัติหรือบริการเพิ่มเติมอื่นที่เป็นประโยชน์ต่อสมาคม และไม่มีค่าใช้จ่ายเพิ่มเติม คณะกรรมการอาจนำมาประกอบการพิจารณาภายใต้คะแนนรวมของหัวข้อนี้ได้

แบบใบเสนอราคา (Pricing Schedule)

เรียน ประธานกรรมการจัดซื้อจัดจ้าง

1. ข้าพเจ้า.....อยู่เลขที่.....ถนน.....

ตำบล/แขวง.....อำเภอ/เขต.....จังหวัด.....โทรศัพท์.....
โดย.....ผู้ลงนามข้างท้ายนี้ ได้พิจารณาเงื่อนไขต่าง ๆ ในประกาศสมาคมสโมสรนักลงทุน เลขที่ IC-PUA 8/2569 และเอกสารเพิ่มเติมเลขที่..... (ถ้ามี) โดยตลอดและยอมรับข้อกำหนดและเงื่อนไขนั้นแล้ว รวมทั้งรับรองว่า ข้าพเจ้าเป็นผู้มีคุณสมบัติครบถ้วนตามที่กำหนด

2. ข้าพเจ้าขอเสนอราคา **โครงการว่าจ้างบริการระบบติดตามและการประเมินตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ** ตามข้อกำหนดเงื่อนไขแบบรูปรายการละเอียดแห่งเอกสารสอบราคา ดังนี้

ลำดับที่	รายการ	จำนวน	ราคา/หน่วย	ราคารวม
	โครงการว่าจ้างบริการระบบติดตามและการประเมินตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ			
A	ค่าบริการ Implementation	1 งาน		
B	ค่าบริการ SaaS Subscription ระยะเวลา 12 เดือน	12 เดือน		
			บวก : ภาษีมูลค่าเพิ่ม 7%	
			รวมเป็นเงินทั้งสิ้น	

(.....)

ราคาที่ใช้ในการเปรียบเทียบข้อเสนอของโครงการ ให้พิจารณาจากราคารวมค่าบริการ Implementation และค่าบริการ SaaS Subscription ระยะเวลา 12 เดือน สำหรับผู้ใช้งาน 25 สิทธิ์ ก่อนภาษีมูลค่าเพิ่ม โดยราคาดังกล่าวต้องรวมภาษีอากรอื่น ค่าธรรมเนียม ค่าเดินทาง และค่าใช้จ่ายทั้งปวงที่จำเป็นต่อการส่งมอบงานครบถ้วนตาม TOR

ข้อเสนอด้านราคาเพิ่มเติม

ส่วนที่ 1 ราคาค่าดำเนินการติดตั้งและนำระบบขึ้นใช้งาน Implementation Service

ลำดับ	รายการ	หน่วย	จำนวน	ราคาต่อหน่วย (บาท)	จำนวนเงิน (บาท)
1.1	ค่าติดตั้งและกำหนดค่าระบบ (System Setup & Configuration)	งาน	1		
1.2	ค่ากำหนดและปรับแต่ง Workflow, SLA, KPI, Dashboard และ Report ตาม TOR	งาน	1		
1.3	ค่าตั้งค่า User, Role และสิทธิ์การใช้งาน (User & Access Configuration)	งาน	1		
1.4	ค่านำเข้าหรือย้ายข้อมูล (Data Migration) ตามขอบเขต TOR (ถ้ามี)	งาน	1		
1.5	ค่าทดสอบระบบและสนับสนุนการทดสอบ UAT	งาน	1		
1.6	ค่าฝึกอบรมผู้ดูแลระบบและผู้ใช้งานตาม TOR	งาน	1		
1.7	ค่าจัดทำคู่มือและเอกสารประกอบการส่งมอบ	งาน	1		
1.8	ค่าใช้จ่ายอื่นที่จำเป็นสำหรับการติดตั้งและนำระบบขึ้นใช้งาน (โปรดระบุ)	งาน	1		
	รวมค่าบริการ Implementation (A)				.....

หมายเหตุ: ค่าใช้จ่ายในส่วน Implementation ต้องรวมค่าใช้จ่ายทั้งหมดที่จำเป็นเพื่อให้ระบบสามารถเปิดใช้งานจริง (Go-Live) และผ่านการตรวจรับตาม TOR โดยผู้เสนอราคาต้องไม่เรียกเก็บค่าใช้จ่ายเพิ่มเติมภายหลังสำหรับงานที่อยู่ในขอบเขต TOR

ส่วนที่ 2 ค่าบริการระบบ SaaS Subscription ระยะเวลา 12 เดือน

ลำดับ	รายการ	หน่วย	จำนวน	ราคาต่อหน่วย (บาท)	จำนวนเงิน (บาท)
2.1	ค่าบริการ SaaS Subscription สำหรับ 25 Named User Licenses ระยะเวลา 12 เดือน	ปี	1		
2.2	Cloud Hosting / Data Center	ปี	1		
2.3	Maintenance / Corrective Maintenance	ปี	1		
2.4	Version Upgrade / Software Update / Security Patch	ปี	1		
2.5	Technical Support และบริการตาม SLA	ปี	1		
2.6	Backup & Disaster Recovery Service	ปี	1		
2.7	Security Monitoring/มาตรการด้านความมั่นคงปลอดภัยที่รวมในบริการ	ปี	1		
2.8	ค่าใช้จ่ายอื่นที่จำเป็นต่อการให้บริการตลอด 12 เดือน (โปรดระบุ)	ปี	1		
	รวมค่าบริการ SaaS Subscription 12 เดือน (B)				.....

หมายเหตุ: กรณีค่าใช้จ่ายรายการที่ 2.2–2.7 รวมอยู่ในค่า SaaS Subscription ตามข้อ 2.1 แล้ว ให้ผู้เสนอราคาระบุคำว่า **“รวมอยู่ในค่า SaaS Subscription ไม่มีค่าใช้จ่ายเพิ่มเติม”** โดยไม่ต้องแยกราคา

ส่วนที่ 3 ราคา Additional User License

ราคาส่วนนี้เป็นราคาอ้างอิงสำหรับกรณีสมาคมมีความประสงค์เพิ่มจำนวนผู้ใช้งานภายหลัง และไม่รวมอยู่ในราคาที่ใช้เปรียบเทียบข้อเสนอครั้งนี้ เว้นแต่สมาคมมีการสั่งซื้อเพิ่มเติม

รายการ	หน่วย	ราคาต่อหน่วยก่อน VAT (บาท)	หมายเหตุ
Additional Named User License	User/เดือน		
Additional Named User License	User/ปี		

ผู้เสนอราคาต้องระบุเงื่อนไขการคิดค่าบริการกรณีเพิ่มผู้ใช้งานระหว่างอายุสัญญา เช่น การติดตามสัดส่วนระยะเวลาคงเหลือของสัญญา (Prorate) หรือหลักเกณฑ์อื่นให้ชัดเจน

ส่วนที่ 4 ราคาต่ออายุบริการ SaaS

เพื่อประกอบการวางแผนงบประมาณในอนาคต ผู้เสนอราคาต้องระบุราคาหลักเกณฑ์ราคาหรือหลักเกณฑ์การปรับราคาต่ออายุบริการ ดังนี้

ระยะเวลาต่ออายุ	ราคาก่อน VAT (บาท)	อัตราเพิ่ม/ลดจากปีแรก	หมายเหตุ
ปีที่ 2			
ปีที่ 3			

กรณีไม่สามารถยืนยันราคาคงที่ล่วงหน้าได้ ให้ระบุหลักเกณฑ์หรืออัตราสูงสุดในการปรับราคา (Price Increase

ส่วนที่ 5 ราคาบริการเพิ่มเติม (Optional Services)

ราคาส่วนนี้เป็นราคาอ้างอิงและไม่นำมารวมในการเปรียบเทียบราคาหลัก เว้นแต่รายการใดถูกกำหนดเป็นขอบเขตงานตาม TOR

ลำดับ	รายการ	หน่วย	ราคาต่อหน่วยก่อน VAT (บาท)	หมายเหตุ
5.1	Professional Service	Man-day		
5.2	Additional Training	วัน/ครั้ง		
5.3	Additional Data Migration	Man-day/งาน		
5.4	Integration/API Development	Man-day/งาน		
5.5	Customization นอกเหนือขอบเขต TOR	Man-day/งาน		

5.6	Optional Module (โปรดระบุ)	ปี		
5.7	บริการเพิ่มเติมอื่น (โปรดระบุ)			

ส่วนที่ 6 รายการค่าใช้จ่ายที่รวมอยู่ในราคาที่เสนอ

ผู้เสนอราคาต้องทำเครื่องหมาย ✓ เพื่อยืนยันว่าราคาที่เสนอรวมค่าใช้จ่ายดังต่อไปนี้แล้ว

รายการ	รวมในราคาที่เสนอ	ไม่เกี่ยวข้อง	หมายเหตุ
SaaS License จำนวน 25 Named Users	☐	☐	
Cloud Hosting / Data Center	☐	☐	
Implementation / Configuration	☐	☐	
Workflow / SLA / KPI Configuration	☐	☐	
Dashboard / Report Configuration	☐	☐	
Data Migration ตามขอบเขต TOR	☐	☐	
UAT Support	☐	☐	
Training	☐	☐	
User/Admin Manual	☐	☐	
Maintenance	☐	☐	
Version Upgrade / Software Update	☐	☐	
Security Patch	☐	☐	
Technical Support	☐	☐	
Backup & Recovery	☐	☐	
Disaster Recovery	☐	☐	
SLA Reporting / Service Reporting	☐	☐	
ค่าเดินทางและค่าใช้จ่ายในการปฏิบัติงาน (ถ้ามี)	☐	☐	

ค่าใช้จ่ายอื่นที่จำเป็นเพื่อให้บริการครบตาม TOR	☐	☐	

ส่วนที่ 7 ระยะเวลาดำเนินงานและเงื่อนไขการชำระเงิน

ผู้เสนอราคารับทราบและยอมรับกำหนดระยะเวลาและเงื่อนไขการชำระเงินตาม TOR ดังต่อไปนี้

รายการ	กำหนดเวลา/งวด	สัดส่วนการชำระ	การยืนยัน
ติดตั้ง กำหนดค่า ทดสอบ ฝึกอบรม ส่งมอบเอกสาร และเปิดใช้งานจริง (Go-Live)	ภายใน 60 วันปฏิทินนับถัดจากวันลงนามในสัญญา	100% ของค่า Implementation เมื่อตรวจรับครบถ้วน	☐ ยืนยัน
ค่าบริการระบบ SaaS สำหรับ 25 Named User Licenses	ครบ 3 เดือน	25% ของค่าบริการรายปี	☐ ยืนยัน
ค่าบริการระบบ SaaS สำหรับ 25 Named User Licenses	ครบ 6 เดือน	25% ของค่าบริการรายปี	☐ ยืนยัน
ค่าบริการระบบ SaaS สำหรับ 25 Named User Licenses	ครบ 9 เดือน	25% ของค่าบริการรายปี	☐ ยืนยัน
ค่าบริการระบบ SaaS พร้อมรายงานการให้บริการประจำปี	ครบ 12 เดือน	25% ของค่าบริการรายปี	☐ ยืนยัน

หมายเหตุ: การชำระเงินทุกงวดเป็นไปเมื่อผู้รับจ้างปฏิบัติตาม SLA ไม่มีเหตุผิดสัญญา และได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุและการจ้างตามเงื่อนไขใน TOR

ส่วนที่ 8 คำรับรองของผู้เสนอราคา

ผู้เสนอราคาขอรับรองว่า

1. ราคาที่เสนอได้รวมค่าใช้จ่ายทั้งหมดที่จำเป็นสำหรับการดำเนินงานและการให้บริการให้ครบถ้วนตาม TOR แล้ว เว้นแต่รายการที่ระบุไว้อย่างชัดเจนว่าเป็น Optional Service หรืออยู่นอกขอบเขตงาน
2. ผู้เสนอราคาได้ตรวจสอบและทำความเข้าใจขอบเขตงาน คุณลักษณะของระบบ ระยะเวลาดำเนินงาน การส่งมอบ การตรวจรับ SLA และเงื่อนไขที่เกี่ยวข้องทั้งหมดแล้ว
3. ผู้เสนอราคาจะไม่เรียกเก็บค่าใช้จ่ายเพิ่มเติมสำหรับฟังก์ชัน License บริการ หรือทรัพยากรที่จำเป็นต่อการทำให้ระบบผ่าน Mandatory Requirements และสามารถใช้งานได้ตาม TOR เว้นแต่เป็นการเปลี่ยนแปลงขอบเขตงานที่ได้รับอนุมัติจากสมาคมเป็นลายลักษณ์อักษร
4. ผู้เสนอราคายอมรับเงื่อนไขการจ่ายเงินตามข้อ 7 ของ TOR ระยะเวลาติดตั้งและ Go-Live ภายใน 60 วันปฏิทิน และระยะเวลาให้บริการระบบ 12 เดือนนับจากวัน Go-Live

5. ราคาที่เสนอมีผลยืนราคาไม่น้อยกว่า 60 วัน นับจากวันที่ยื่นซองเสนอราคา และจะถอนการเสนอราคาภายในกำหนดดังกล่าวมิได้

เสนอมา ณ วันที่.....เดือน.....พ.ศ. .....

ลงชื่อ.....ผู้มีอำนาจลงนาม/ผู้รับมอบอำนาจ

(.....)

ตำแหน่ง.....

ประทับตรา (ถ้ามี)

ยกร่างสัญญาจ้างบริการระบบติดตามและการประเมินตัวชี้วัด (KPI)

งานบริการด้านเทคโนโลยีสารสนเทศ

สัญญาฉบับนี้ทำขึ้น ณ สมาคมสโมสรนักลงทุน สำนักงานตั้งอยู่เลขที่ 1 อาคารทีพี แอนด์ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 เมื่อวันที่ ..... ระหว่าง

สมาคมสโมสรนักลงทุน ซึ่งมีสำนักงานใหญ่ตั้งอยู่เลขที่1 อาคารทีพี แอนด์ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โดย นางสาวกรองกนก มานะกิจจงกล ตำแหน่ง ผู้จัดการสมาคมสโมสรนักลงทุน ผู้มีอำนาจกระทำการแทนสมาคม ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้ว่าจ้าง” ฝ่ายหนึ่ง กับ

บริษัท..... จำกัด ซึ่งจดทะเบียนเป็นนิติบุคคล ณ สำนักงานทะเบียนหุ้นส่วนบริษัทกลาง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ มีสำนักงานใหญ่ตั้งอยู่เลขที่ ..... โดย ..... ตำแหน่ง ..... ผู้มีอำนาจลงนามผูกพันนิติบุคคล/ผู้รับมอบอำนาจ (ซึ่งเอกสารประกอบการแสดงตนดังกล่าวมีกำหนดอายุไม่เกิน 6 เดือน นับถึงวันลงนามในสัญญานี้) รายละเอียดปรากฏตามเอกสารแนบท้ายสัญญานี้ ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้รับจ้าง” อีกฝ่ายหนึ่ง

คู่สัญญาทั้งสองฝ่ายได้ตกลงทำสัญญากัน โดยมีข้อความดังต่อไปนี้

ข้อ 1 ข้อตกลงว่าจ้างและขอบเขตแห่งสัญญา

1.1 ผู้ว่าจ้างตกลงจ้างและผู้รับจ้างตกลงรับจ้างดำเนินการวิเคราะห์ความต้องการ จัดหา ติดตั้ง กำหนดค่าปรับแต่ง ทดสอบ นำเข้าข้อมูล (ถ้ามี) ฝึกอบรม ส่งมอบ เปิดใช้งานจริง และให้บริการระบบติดตามและประเมินผลตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ ในรูปแบบ Software as a Service (SaaS) พร้อมสิทธิการใช้งานแบบระบุชื่อ (Named User License) จำนวน 25 (ยี่สิบห้า) สิทธิ เป็นระยะเวลา 12 (สิบสอง) เดือน รวมทั้งบริการบำรุงรักษา สนับสนุนทางเทคนิค สำรองและกู้คืนข้อมูล และบริการอื่นที่เกี่ยวข้อง ตามสัญญา ขอบเขตของงาน (TOR) ลงวันที่ 4 สิงหาคม 2569 และเอกสารแนบท้ายสัญญา

1.1.1 ระบบตามสัญญาต้องประกอบด้วยโมดูลอย่างน้อย 20 รายการ ได้แก่ Incident Management, Service Request Management, Problem Management, Change Management, Service Level Management (SLA), KPI Dashboard & Executive Dashboard, Service Catalog, Knowledge Management, IT Asset Management, Fixed Asset Management, Configuration Management Database (CMDB), Supplier & Contract Management, User & Role Management, Audit Trail & Activity Log, Reporting & Analytics, Self-Service Portal, Mobile Application, Backup & Disaster

Recovery, Security Incident Logging และ Data Export & Data Retention Management โดยทุกโมดูลต้องใช้งานร่วมกันบนแพลตฟอร์มเดียวและรวมอยู่ในค่าจ้างแล้ว

1.2 ผู้รับจ้างตกลงดำเนินงานตามสัญญาด้วยความรู้ ความสามารถ ความชำนาญ และความระมัดระวังตามมาตรฐานวิชาชีพที่พึงคาดหมายจากผู้ประกอบวิชาชีพประเภทเดียวกัน และต้องจัดให้ระบบและบริการเป็นไปตามข้อกำหนดบังคับ (Mandatory Requirements) ตารางแสดงการปฏิบัติตามข้อกำหนดด้านเทคนิค (Technical Compliance Matrix) ข้อตกลงระดับการให้บริการ (SLA) และข้อเสนอด้านเทคนิคของผู้รับจ้างซึ่งผู้ว่าจ้างได้ให้ความเห็นชอบแล้ว

1.3 บรรดาค่าใช้จ่ายทั้งปวงอันจำเป็นเพื่อให้การดำเนินงานและการให้บริการตามสัญญาสำเร็จครบถ้วน รวมถึงแต่ไม่จำกัดเพียง ค่าสิทธิการใช้งาน ค่าบริการระบบคลาวด์ ค่าบำรุงรักษา ค่าปรับปรุงรุ่นซอฟต์แวร์ ค่าปรับปรุงแก้ไขด้านความมั่นคงปลอดภัย ค่าบริการสนับสนุนทางเทคนิค ค่าบริการสำรองและกู้คืนข้อมูล และค่าใช้จ่ายอื่นที่เกี่ยวข้อง ให้ถือว่ารวมอยู่ในค่าจ้างตามสัญญาแล้ว ผู้รับจ้างจะเรียกร้องค่าใช้จ่ายเพิ่มเติมมิได้ เว้นแต่เป็นงานนอกเหนือขอบเขตแห่งสัญญาซึ่งผู้ว่าจ้างได้อนุมัติเป็นหนังสือไว้ก่อนแล้ว

ข้อ 2 เอกสารอันเป็นส่วนหนึ่งของสัญญา

2.1 เอกสารดังต่อไปนี้ให้ถือเป็นส่วนหนึ่งของสัญญาและมีผลผูกพันคู่สัญญาเช่นเดียวกับข้อความในสัญญานี้ ได้แก่

(1) ขอบเขตของงาน (TOR) และภาคผนวก

(2) ประกาศสอบราคาและเอกสารชี้แจงหรือแก้ไขเพิ่มเติม (ถ้ามี)

(3) ข้อเสนอด้านเทคนิคและ Technical Compliance Matrix ของผู้รับจ้าง

(4) ใบเสนอราคาและ Pricing Schedule

(5) ตารางข้อตกลงระดับการให้บริการ (SLA Matrix) และเกณฑ์การชดเชย

(6) เอกสารด้านการรักษาความลับและการประมวลผลข้อมูลส่วนบุคคล (ถ้ามี)

(7) ระเบียบปฏิบัติงานตามนโยบายและการบริหารเทคโนโลยีสารสนเทศ ฉบับผู้ให้บริการ รหัสเอกสาร IT-1PC-02 และ

(8) เอกสารอื่นที่คู่สัญญาตกลงให้เป็นส่วนหนึ่งของสัญญา

2.2 ในกรณีที่ข้อความในเอกสารอันเป็นส่วนหนึ่งของสัญญาขัดหรือแย้งกัน ให้ตีความโดยคำนึงถึงเจตนาและวัตถุประสงค์แห่งสัญญาเป็นสำคัญ และให้ข้อความในสัญญานี้มีผลใช้บังคับก่อน ตามด้วย TOR เอกสารชี้แจงหรือแก้ไขเพิ่มเติม ข้อเสนอด้านเทคนิค และใบเสนอราคา ตามลำดับ

ทั้งนี้ หากข้อเสนอของผู้รับจ้างกำหนดมาตรฐาน คุณภาพ หรือประโยชน์แก่ผู้ว่าจ้างสูงกว่าที่กำหนดไว้ใน TOR โดยไม่ก่อให้เกิดค่าใช้จ่ายเพิ่มเติม ให้ถือปฏิบัติตามข้อเสนอที่เป็นคุณแก่ผู้ว่าจ้างนั้น

ข้อ 3 ระยะเวลาดำเนินงานและระยะเวลาให้บริการ

3.1 ผู้รับจ้างต้องดำเนินการติดตั้ง กำหนดค่า ปรับแต่ง ทดสอบ ฝึกอบรม และเตรียมระบบให้พร้อมเปิดใช้งานจริง (Implementation and Go-Live) ให้แล้วเสร็จภายใน 60 (หกสิบ) วันปฏิทิน นับถัดจากวันลงนามในสัญญา

3.2 ผู้รับจ้างต้องให้บริการระบบ SaaS เป็นระยะเวลา 12 (สิบสอง) เดือน โดยเริ่มนับตั้งแต่วันระบุเป็นวันเปิดใช้งานจริง (Go-Live) ในเอกสารตรวจรับงาน Implementation และสิ้นสุดเมื่อครบกำหนด 12 เดือน นับจากวันดังกล่าว ทั้งนี้ วัน Go-Live ต้องไม่เกินวันสุดท้ายของระยะเวลา 60 วันตามข้อ 3.1

3.3 ระยะเวลาดำเนินงาน Implementation ตามข้อ 3.1 ไม่นับรวมอยู่ในระยะเวลาให้บริการ SaaS ตามข้อ 3.2

ข้อ 4 การส่งมอบงานและเอกสารประกอบ

4.1 ผู้รับจ้างต้องส่งมอบงาน Implementation พร้อมเอกสารและหลักฐานตาม TOR และเอกสารแนบท้ายสัญญา ซึ่งอย่างน้อยต้องประกอบด้วย

- แผนดำเนินโครงการ สถาปัตยกรรมระบบ
- รายละเอียดคุณลักษณะและการกำหนดค่าระบบ
- รายละเอียด Workflow, SLA, KPI, Dashboard
- Report ตารางสิทธิการเข้าถึงระบบ
- รายงานผลการทดสอบระบบ
- รายงาน UAT
- รายงานการทดสอบสำรองและกู้คืนข้อมูล
- หลักฐานการฝึกอบรม
- คู่มือใช้งานและผู้ดูแลระบบ
- เอกสารการตั้งค่าระบบ
- รายการสิทธิการใช้งาน
- รายงานการเปิดใช้งานจริง
- หนังสือรับประกันบริการ

- คำอธิบายโครงสร้างข้อมูล (Data Dictionary) และ/หรือ Data Schema ที่จำเป็นสำหรับการใช้งาน บำรุงรักษา และเชื่อมโยงข้อมูลกับระบบอื่น (ถ้ามี)

4.2 ตลอดระยะเวลาให้บริการ SaaS ผู้รับจ้างต้องจัดทำรายงาน SLA เป็นรายเดือน โดยอย่างน้อยต้องแสดง System Availability, Downtime และสาเหตุ, สถิติ Incident และ Service Request, ผล Response Time และ Resolution Time และสถิติการใช้งานระบบ รวมทั้งจัดทำรายงานผลการให้บริการไตรมาสเพื่อประกอบการตรวจรับแต่ละงวด

4.3 ในงวดสุดท้าย ผู้รับจ้างต้องจัดทำรายงานสรุปผลการให้บริการตลอดอายุสัญญา พร้อมสรุปปัญหาที่ยังคงค้างอยู่ (ถ้ามี) และข้อมูลที่จำเป็นต่อการสิ้นสุดหรือเปลี่ยนผ่านบริการ

ข้อ 5 การตรวจรับงาน

5.1 ผู้ว่าจ้างจะแต่งตั้งคณะกรรมการตรวจรับเพื่อทำหน้าที่ตรวจสอบและพิจารณาผลงานของผู้รับจ้างให้เป็นไปตามสัญญา TOR และเอกสารแนบท้ายสัญญา

5.2 การตรวจรับงาน Implementation จะกระทำเมื่อผู้รับจ้างส่งมอบงานและเอกสารครบถ้วน ระบบผ่านการทดสอบ UAT สามารถใช้งานได้จริงตามข้อกำหนด และเปิดใช้งานจริง (Go-Live) เรียบร้อยแล้ว

5.3 การตรวจรับบริการ SaaS ให้แบ่งเป็น 4 (สี่) งวด งวดละ 3 (สาม) เดือน โดยคณะกรรมการตรวจรับจะพิจารณาจากผลการให้บริการจริง รายงาน SLA รายเดือน รายงานผลการให้บริการรายไตรมาส และหลักฐานอื่นตามที่กำหนด

5.4 หากคณะกรรมการตรวจรับเห็นว่างานหรือบริการไม่ถูกต้องครบถ้วนตามสัญญา ผู้ว่าจ้างมีสิทธิแจ้งให้ผู้รับจ้างแก้ไข เปลี่ยนแปลง หรือดำเนินการเพิ่มเติมให้ถูกต้องครบถ้วนภายในระยะเวลาที่ผู้ว่าจ้างกำหนด โดยผู้รับจ้างไม่มีสิทธิเรียกค่าใช้จ่ายเพิ่มเติม

5.5 การที่ผู้ว่าจ้างตรวจรับงานหรือชำระค่าจ้างแล้ว ไม่เป็นการตัดสิทธิผู้ว่าจ้างที่จะเรียกร้องให้ผู้รับจ้างรับผิดในความชำรุดบกพร่อง ความเสียหาย หรือการผิดสัญญาที่ตรวจพบภายหลัง

ข้อ 6 ค่าจ้างและการชำระเงิน

6.1 คู่สัญญาตกลงค่าจ้างตามสัญญาเป็นจำนวนเงินทั้งสิ้น ..... บาท (.....) [รวม/ไม่รวม] ภาษีมูลค่าเพิ่ม โดยแบ่งเป็น

(1) ค่าดำเนินการติดตั้งและนำระบบขึ้นใช้งาน (Implementation Fee) จำนวน ..... บาท และ

(2) ค่าบริการ SaaS Subscription ระยะเวลา 12 เดือน จำนวน..... บาท

6.2 ผู้ว่าจ้างจะชำระค่าดำเนินการ Implementation ให้แก่ผู้รับจ้างเมื่อผู้รับจ้างดำเนินงานครบถ้วนตามสัญญาและคณะกรรมการตรวจรับได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว

6.3 ค่าบริการ SaaS Subscription ให้แบ่งชำระเป็น 4 (สี่) งวด งวดละร้อยละ 25 (ยี่สิบห้า) ของค่าบริการ SaaS โดยชำระเมื่อผู้รับจ้างให้บริการครบ 3 เดือน 6 เดือน 9 เดือน และ 12 เดือน ตามลำดับ และคณะกรรมการตรวจรับงานในแต่ละงวดเรียบร้อยแล้ว

6.4 ผู้รับจ้างต้องจัดส่งใบแจ้งหนี้และเอกสารประกอบการเบิกจ่ายตามที่ผู้ว่าจ้างกำหนด ผู้ว่าจ้างมีสิทธิหักภาษี ณ ที่จ่าย ค่าปรับ หรือหนี้อื่นใดที่ผู้รับจ้าง มีหน้าที่ต้องชำระแก่ผู้ว่าจ้างออกจากเงินที่ถึงกำหนดชำระได้ตามกฎหมายและสัญญา การชำระเงินแต่ละงวดให้กระทำเมื่อผู้รับจ้างไม่มีเหตุผิดสัญญาและได้ปฏิบัติตาม SLA แล้ว

ข้อ 7 หลักประกันการปฏิบัติตามสัญญา

ผู้รับจ้างต้องนำหลักประกันการปฏิบัติตามสัญญาเป็นจำนวนร้อยละ 10 (สิบ) ของมูลค่าสัญญา มามอบให้แก่ผู้ว่าจ้างในวันทำสัญญา ในรูปแบบที่ผู้ว่าจ้างกำหนด และต้องดำรงหลักประกันดังกล่าวให้มีผลใช้บังคับตลอดระยะเวลาที่ผู้รับจ้างยังมีหน้าที่หรือความรับผิดตามสัญญา ผู้ว่าจ้างจะคืนหลักประกันเมื่อผู้รับจ้างพ้นจากข้อผูกพัน และความรับผิดทั้งปวงตามสัญญาแล้ว

ข้อ 8 ค่าปรับกรณีส่งมอบงานล่าช้า

8.1 หากผู้รับจ้างไม่สามารถส่งมอบงาน Implementation ให้แล้วเสร็จภายในกำหนดเวลาตามข้อ 3.1 และมิใช่เหตุสุดวิสัยหรือเหตุอันเกิดจากผู้ว่าจ้าง ผู้รับจ้างต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นรายวันในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของวงเงินตามสัญญาต่อวัน นับถัดจากวันครบกำหนดส่งมอบจนถึงวันที่ส่งมอบงานแล้วเสร็ จและได้รับการตรวจรับจากผู้ว่าจ้าง ทั้งนี้ การคิดค่าปรับไม่ตัดสิทธิผู้ว่าจ้างในการเรียกค่าเสียหายอื่นที่เกิดขึ้นจริง การใช้สิทธิตามหลักประกัน หรือการบอกเลิกสัญญา

8.2 การชดเชยกรณีความพร้อมใช้งานของระบบไม่เป็นไปตาม SLA หาก System Availability ต่อเดือนต่ำกว่าร้อยละ 99.9 ผู้รับจ้างต้องขยายระยะเวลาการให้บริการโดยไม่มีค่าใช้จ่าย ดังนี้

(1) ตั้งแต่ร้อยละ 99.00 ถึง 99.89 ขยาย 7 วัน

(2) ตั้งแต่ร้อยละ 98.00 ถึง 98.99 ขยาย 15 วัน และ

(3) ต่ำกว่าร้อยละ 98.00 ขยาย 30 วัน การชดเชยดังกล่าวไม่ตัดสิทธิผู้ว่าจ้างในการเรียกให้แก้ไขเรียกค่าเสียหาย หรือใช้สิทธิบอกเลิกสัญญาเมื่อมีการผิดสัญญาอย่างมีนัยสำคัญ

ข้อ 9 ข้อตกลงระดับการให้บริการ (SLA) และการบริหารจัดการ

9.1 ความพร้อมใช้งานของระบบ ผู้รับจ้างต้องรักษาความพร้อมใช้งานของระบบ (Monthly Availability) ไม่น้อยกว่าร้อยละ 99.9 ต่อเดือน โดยวิธีคำนวณ ระยะเวลาบำรุงรักษาตามแผน และข้อยกเว้นให้เป็นไปตาม SLA แนบท้ายสัญญา

9.2 ช่องทางสนับสนุนและรับแจ้งเหตุ ผู้รับจ้าง ต้องจัดให้มีช่องทางรับแจ้งเหตุและสนับสนุนทางเทคนิคอย่างน้อยผ่านโทรศัพท์ อีเมล หรือระบบออนไลน์ ในวันและเวลาทำการ 08:30-17:30 น. และดำเนินการตามระดับความรุนแรงและระยะเวลาที่กำหนดใน SLA แนบท้ายสัญญา

9.3 ผลของการไม่ปฏิบัติตาม SLA หากผู้รับจ้างไม่สามารถรักษา System Availability ได้ตามข้อ 9.1 ผู้รับจ้างต้องขยายระยะเวลาการให้บริการโดยไม่มีค่าใช้จ่ายตามเกณฑ์ในข้อ 8.1 และ TOR การขยายระยะเวลาดังกล่าวไม่ทำให้ผู้รับจ้างพ้นจากหน้าที่แก้ไขปัญหา และไม่ตัดสิทธิผู้ว่าจ้างในการใช้สิทธิอื่นตามสัญญาและกฎหมาย

9.4 หากผู้รับจ้างไม่สามารถปฏิบัติตาม Response Time หรือ Resolution Time เกินกว่า 3 ครั้งภายในรอบ 12 เดือน ผู้รับจ้างต้องจัดทำ Root Cause Analysis และ Corrective Action Plan เป็นลายลักษณ์อักษรภายใน 15 วันนับจากวันที่ได้รับแจ้ง โดยระบุสาเหตุ ผลกระทบ มาตรการแก้ไขและป้องกัน ระยะเวลา ผู้รับผิดชอบ และตัวชี้วัดผลสำเร็จ หากไม่ดำเนินการหรือยังไม่สามารถรักษาระดับบริการได้ ผู้ว่าจ้างมีสิทธิเรียกร้องมาตรการเพิ่มเติมหรือบอกเลิกสัญญาเมื่อเป็นการผิดสัญญาอย่างมีนัยสำคัญ

ข้อ 10 การบำรุงรักษาและการสนับสนุนบริการ

ตลอดอายุสัญญา ผู้รับจ้างต้องจัดให้มีบริการบำรุงรักษา แก้ไขข้อบกพร่อง อัปเดตเวอร์ชัน และติดตั้ง Security Patch โดยไม่คิดค่าใช้จ่ายเพิ่มเติม การเปลี่ยนแปลงต้องไม่ทำให้ความสามารถหรือความมั่นคงปลอดภัยลดลง และ Scheduled Maintenance ต้องแจ้งผู้ว่าจ้างล่วงหน้าไม่น้อยกว่า 7 (เจ็ด) วันทำการ

ข้อ 11 การรักษาความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคล

11.1 ผู้รับจ้างต้องจัดให้มีมาตรการทางเทคนิคและมาตรการเชิงองค์กรที่เหมาะสมเพื่อรักษาความมั่นคงปลอดภัยของระบบและข้อมูล และต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยของผู้ว่าจ้างที่แจ้งให้ทราบ

11.2 ผู้รับจ้างต้องควบคุมสิทธิการเข้าถึงข้อมูลและระบบตามหลักความจำเป็นในการใช้งานและสิทธิเท่าที่จำเป็น รวมทั้งจัดให้มีบันทึกการใช้งานและการตรวจสอบย้อนหลัง (Audit Trail) ตามความเหมาะสม

11.3 เมื่อผู้รับจ้างตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุละเมิดข้อมูลที่มีหรืออาจมีผลกระทบต่อผู้ว่าจ้าง ผู้รับจ้างต้องแจ้งผู้ว่าจ้างโดยไม่ชักช้าและไม่เกิน 24 (ยี่สิบสี่) ชั่วโมงนับแต่ตรวจพบ พร้อมให้ความร่วมมือในการควบคุม แก้ไข ตรวจสอบ วิเคราะห์สาเหตุ และจัดทำรายงานตามที่ผู้ว่าจ้างร้องขอ

ข้อ 12 การสำรองข้อมูล การกู้คืน และความต่อเนื่องของบริการ

ผู้รับจ้างต้องสำรองข้อมูลทุกวันและสามารถกู้คืนข้อมูลย้อนหลังได้ไม่น้อยกว่า 90 วัน พร้อมมีศูนย์สำรองระบบหรือโครงสร้างพื้นฐานสำรอง มี RTO ไม่เกิน 24 ชั่วโมง และ RPO ไม่เกิน 24 ชั่วโมง ต้องแจ้งสถานที่หรือประเทศที่จัดเก็บข้อมูล จัดทำนโยบาย Data Retention และทดสอบแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง พร้อมแสดงหลักฐานเมื่อผู้ว่าจ้างร้องขอ

ข้อ 13 การจ้างช่วงและผู้ประมวลผลช่วง

ผู้รับจ้างจะนำงานอันเป็นสาระสำคัญตามสัญญาไปให้บุคคลอื่นรับจ้างช่วงมิได้ เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากผู้ว่าจ้างก่อน การที่ผู้ว่าจ้างอนุญาตให้จ้างช่วงไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดตามสัญญา และผู้รับจ้างยังคงต้องรับผิดในการกระทำหรือละเว้นการกระทำของผู้รับจ้างช่วง ผู้ให้บริการระบบคลาวด์ หรือผู้ประมวลผลช่วงเสมือนเป็นการกระทำของผู้รับจ้างเอง

ข้อ 14 การรักษาความลับ

ผู้รับจ้างตกลงเก็บรักษาข้อมูล เอกสาร ความลับทางการค้า ข้อมูลระบบ ข้อมูลส่วนบุคคล และข้อมูลอื่นใดของผู้ว่าจ้างซึ่งได้รับรู้หรือเข้าถึงเนื่องจากการปฏิบัติตามสัญญาไว้เป็นความลับ และจะไม่นำไปใช้ เปิดเผย ทำซ้ำ หรือส่งต่อแก่บุคคลใด เว้นแต่เท่าที่จำเป็นต่อการปฏิบัติตามสัญญา ได้รับความยินยอมเป็นหนังสือจากผู้ว่าจ้าง หรือเป็นกรณีที่กฎหมายกำหนด หน้าที่รักษาความลับยังคงมีผลต่อไปภายหลังสัญญาสิ้นสุด

ข้อ 15 กรรมสิทธิ์ในข้อมูลและทรัพย์สินทางปัญญา

15.1 ข้อมูลทั้งหมดที่ผู้ว่าจ้างนำเข้าสู่ระบบ รวมทั้งข้อมูลที่เกิดขึ้นจากการใช้งานระบบของผู้ว่าจ้าง ให้เป็นกรรมสิทธิ์หรืออยู่ภายใต้สิทธิของผู้ว่าจ้างตามกฎหมาย ผู้รับจ้างไม่มีสิทธินำข้อมูลดังกล่าวไปใช้เพื่อประโยชน์อื่นนอกเหนือจากการปฏิบัติตามสัญญา

15.2 สิทธิในซอฟต์แวร์หรือผลิตภัณฑ์ SaaS ที่มีอยู่ก่อนวันทำสัญญาหรือเป็นผลิตภัณฑ์มาตรฐานของผู้รับจ้างหรือเจ้าของผลิตภัณฑ์ ยังคงเป็นของเจ้าของสิทธินั้น ผู้รับจ้างรับรองว่าตนมีสิทธิโดยชอบในการให้บริการและให้สิทธิใช้งานตามสัญญา และการใช้บริการของผู้ว่าจ้างตามสัญญาจะไม่เป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลภายนอก

ข้อ 16 การส่งคืนข้อมูลและการสิ้นสุดบริการ

เมื่อสัญญาสิ้นสุดไม่ว่าด้วยเหตุใด ผู้รับจ้างต้องส่งมอบข้อมูลทั้งหมดของผู้ว่าจ้างภายใน 7 (เจ็ด) วันทำการนับจากวันที่สัญญาสิ้นสุด โดยข้อมูลต้องครบถ้วน ถูกต้อง ใช้งานได้จริง และอยู่ใน Open Standard Format อย่างน้อย CSV และ XLSX และหากระบบรองรับให้ส่งออกเป็น JSON หรือรูปแบบมาตรฐานอื่น พร้อมให้ความร่วมมือในการเปลี่ยนผ่านบริการ ภายหลังผู้ว่าจ้างตรวจสอบและยืนยันการรับมอบแล้ว ผู้รับจ้างต้องลบหรือทำลายข้อมูลในระบบหลัก ระบบสำรอง และสื่อจัดเก็บที่เกี่ยวข้องภายใน 7 (เจ็ด) วันทำการ เว้นแต่กฎหมายกำหนดให้เก็บไว้นานกว่า การลบหรือทำลายต้องปลอดภัย ตรวจสอบได้ และผู้รับจ้างต้องออก Certificate of Data Deletion/Destruction เพื่อยืนยันว่าข้อมูลไม่สามารถกู้คืนได้

ข้อ 17 การตรวจสอบและการบริหารความเสี่ยงของผู้ให้บริการ

ผู้รับจ้างต้องให้ความร่วมมือแก่ผู้ว่าจ้างในการตรวจสอบสถานะ การประเมินความเสี่ยงของผู้ให้บริการภายนอก การประเมินผลการปฏิบัติงาน และการตรวจสอบหลักฐานที่เกี่ยวข้องกับการปฏิบัติตามสัญญา โดยผู้ว่าจ้างมีสิทธิร้องขอข้อมูลหรือหลักฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล ความต่อเนื่องทางธุรกิจ การกู้คืนจากภัยพิบัติ SLA และผู้รับจ้างช่วงตามสมควร หากพบความเสี่ยงหรือผลการประเมินต่ำกว่าเกณฑ์ ผู้รับจ้างต้องทำและดำเนินการตามแผนแก้ไขหรือแผนจัดการความเสี่ยงภายในระยะเวลาที่ตกลงกัน

ข้อ 18 การเปลี่ยนแปลงขอบเขตงาน

การเปลี่ยนแปลงเพิ่มเติมหรือลดทอนขอบเขตงาน การกำหนดค่าระบบ หรือบริการใดที่มีผลต่อราคา ระยะเวลา คุณภาพ ความมั่นคงปลอดภัย หรือระดับการให้บริการ จะกระทำได้ต่อเมื่อได้รับความเห็นชอบจากผู้ว่าจ้างเป็นหนังสือก่อนดำเนินการ ผู้รับจ้างไม่มีสิทธิเรียกร้องค่าจ้างหรือค่าใช้จ่ายสำหรับงานเพิ่มเติมที่ดำเนินการไปโดยมิได้รับอนุมัติเป็นหนังสือจากผู้ว่าจ้าง

ข้อ 19 บุคลากรของผู้รับจ้าง

ผู้รับจ้างต้องจัดให้มีผู้จัดการโครงการและบุคลากรที่มีความรู้ ความสามารถ และประสบการณ์เหมาะสมกับงานตามสัญญา หากมีความจำเป็นต้องเปลี่ยนบุคลากรหลัก ผู้รับจ้างต้องแจ้งให้ผู้ว่าจ้างทราบล่วงหน้าและจัดหาบุคลากรทดแทนที่มีคุณสมบัติไม่ต่ำกว่าบุคลากรเดิม โดยต้องไม่ก่อให้เกิดผลกระทบต่อการดำเนินงานหรือการให้บริการ

19.1 ข้อกำหนดด้านการบริหารบริการและความรับผิดชอบ

19.1.1 ผู้รับจ้างต้องกำหนดผู้รับผิดชอบหลัก ผู้ประสานงาน และช่องทางการติดต่อสำหรับการบริหารสัญญา การบริหารบริการ การรับแจ้งเหตุขัดข้อง การรับคำขอใช้บริการ และการยกระดับปัญหา (Escalation) ให้ชัดเจน และต้องแจ้งผู้ว่าจ้างเป็นหนังสือเมื่อมีการเปลี่ยนแปลงบุคคลหรือช่องทางดังกล่าว

19.1.2 ผู้รับจ้างต้องให้บริการตามข้อกำหนดบริการ (Service Requirements) ขอบเขตบริการ ชั่วโมงให้บริการ ระดับการให้บริการ และหน้าที่ความรับผิดชอบของคู่สัญญาที่กำหนดไว้ใน TOR, SLA และเอกสารแนบท้ายสัญญา และต้องรักษาข้อมูลบริการที่จำเป็นต่อการบริหารและตรวจสอบบริการให้เป็นปัจจุบันตลอดอายุสัญญา

19.1.3 ผู้รับจ้างต้องเข้าร่วมประชุมทบทวนผลการให้บริการตามที่ผู้ว่าจ้างกำหนด เพื่อพิจารณาผลการปฏิบัติงานตาม SLA แนวโน้มปัญหา ความเสี่ยง ข้อร้องเรียน เหตุการณ์ด้านความมั่นคงปลอดภัย การเปลี่ยนแปลงที่สำคัญ และโอกาสในการปรับปรุงบริการ พร้อมดำเนินการตามมติหรือแผนแก้ไขภายในระยะเวลาที่ตกลงกัน

19.2 การจัดการเหตุขัดข้อง คำขอใช้บริการ และปัญหา

19.2.1 ผู้รับจ้างต้องจัดให้มีกระบวนการรับแจ้ง บันทึก จำแนก จัดลำดับความสำคัญ ติดตาม ยกระดับ และปิดเหตุขัดข้อง (Incident) และคำขอใช้บริการ (Service Request) โดยสามารถตรวจสอบสถานะและประวัติย้อนหลังได้

19.2.2 สำหรับเหตุขัดข้องที่มีผลกระทบร้ายแรงหรือเกิดซ้ำ ผู้รับจ้างต้องดำเนินการวิเคราะห์สาเหตุรากของปัญหา (Root Cause Analysis) จัดทำแนวทางแก้ไขถาวรและมาตรการป้องกันการเกิดซ้ำ และรายงานให้ผู้ว่าจ้างทราบตามระยะเวลาที่กำหนดใน SLA

19.2.3 ผู้รับจ้างต้องเก็บรักษาบันทึก Incident, Service Request, Problem, RCA และการดำเนินการแก้ไขไว้ตลอดอายุสัญญาและตามระยะเวลาที่กฎหมายหรือนโยบายของผู้ว่าจ้างกำหนด เพื่อให้สามารถตรวจสอบย้อนหลังได้

19.3 การบริหารการเปลี่ยนแปลง การนำขึ้นใช้งาน และการกำหนดค่าระบบ

19.3.1 การเปลี่ยนแปลงใดที่อาจมีผลกระทบต่อบริการ ข้อมูล ความมั่นคงปลอดภัย SLA การเชื่อมต่อ หรือการดำเนินงานของผู้ว่าจ้าง ต้องผ่านการประเมินผลกระทบและความเสี่ยง การอนุมัติ การทดสอบ และการวางแผนย้อนกลับ (Rollback) ตามความเหมาะสมก่อนนำขึ้นใช้งานจริง

19.3.2 การเปลี่ยนแปลงฉุกเฉินต้องมีเหตุผลและหลักฐานประกอบ และต้องได้รับการทบทวนภายหลังดำเนินการโดยเร็ว

19.3.3 ผู้รับจ้างต้องควบคุมข้อมูลการกำหนดค่าที่สำคัญของระบบ (Configuration Information) และปรับปรุงเอกสารสถาปัตยกรรม การตั้งค่า สิทธิการเข้าถึง และเอกสารที่เกี่ยวข้องให้เป็นปัจจุบันภายหลังการเปลี่ยนแปลง

19.3.4 การนำซอฟต์แวร์ รุ่นใหม่ หรือการเปลี่ยนแปลงสำคัญขึ้นใช้งานต้องมีเกณฑ์การยอมรับและหลักฐานผลการทดสอบที่เหมาะสม และต้องไม่ทำให้ระดับบริการหรือมาตรการความมั่นคงปลอดภัยลดลงต่ำกว่าที่ตกลงไว้

19.4 การบริหารความพร้อมใช้งาน ขีดความสามารถ และความต่อเนื่องของบริการ

19.4.1 ผู้รับจ้างต้องติดตามและบริหารความพร้อมใช้งานและขีดความสามารถของระบบให้เพียงพอต่อปริมาณการใช้งานตามขอบเขตสัญญา และต้องแจ้งผู้ว่าจ้างล่วงหน้าเมื่อพบแนวโน้มที่อาจทำให้บริการไม่เป็นไปตาม SLA

19.4.2 ผู้รับจ้างต้องทบทวนความเสี่ยงที่เกี่ยวข้องกับความพร้อมใช้งาน ความต่อเนื่องของบริการและความมั่นคงปลอดภัยเป็นระยะ และเมื่อมีการเปลี่ยนแปลงสำคัญ พร้อมจัดทำมาตรการจัดการความเสี่ยงตามความเหมาะสม

19.4.3 ผู้รับจ้างต้องจัดให้มีและทดสอบแผนความต่อเนื่องและการกู้คืนบริการตามระยะเวลาที่กำหนดหรืออย่างน้อยปีละหนึ่งครั้งสำหรับบริการที่อยู่ในขอบเขตสัญญา และต้องส่งรายงานผลการทดสอบ ข้อบกพร่องและแผนแก้ไขให้ผู้ว่าจ้างเมื่อร้องขอ

19.5 การบริหารผู้ให้บริการช่วงและห่วงโซ่อุปทาน ICT

19.5.1 ผู้รับจ้างต้องบริหารและติดตามผู้รับจ้างช่วง ผู้ให้บริการคลาวด์ และผู้ประมวลผลช่วงที่เกี่ยวข้องกับบริการ เพื่อให้การให้บริการและการรักษาความมั่นคงปลอดภัยเป็นไปตามข้อกำหนดของสัญญา

19.5.2 ผู้รับจ้างต้องแจ้งผู้ว่าจ้างล่วงหน้าเป็นหนังสือก่อนมีการเพิ่ม เปลี่ยน หรือยกเลิกผู้ให้บริการช่วงที่มีผลกระทบอย่างมีนัยสำคัญต่อสถานที่ประมวลผลหรือจัดเก็บข้อมูล ความมั่นคงปลอดภัย ความต่อเนื่องหรือระดับการให้บริการ และต้องประเมินความเสี่ยงและผลกระทบก่อนดำเนินการ

19.5.3 ผู้รับจ้างยังคงรับผิดชอบต่อการปฏิบัติตามสัญญาของผู้ให้บริการช่วงทุกทอดเสมือนเป็นการกระทำของผู้รับจ้างเอง และต้องกำหนดข้อผูกพันด้านความมั่นคงปลอดภัย การรักษาความลับ การแจ้งเหตุ การคืนและลบข้อมูล และสิทธิการตรวจสอบในข้อตกลงกับผู้ให้บริการช่วงตามความเหมาะสม

19.6 การติดตาม วัดผล ทบทวน และปรับปรุงบริการ

19.6.1 ผู้รับจ้างต้องติดตาม วัดผล วิเคราะห์ และรายงานผลการให้บริการตามตัวชี้วัดและ SLA ที่ตกลงโดยข้อมูลและหลักฐานที่ใช้รายงานต้องถูกต้อง เชื่อถือได้ และสามารถตรวจสอบย้อนหลังได้

19.6.2 เมื่อผลการให้บริการไม่เป็นไปตามข้อกำหนด ผู้รับจ้างต้องดำเนินการแก้ไข ควบคุมผลกระทบ วิเคราะห์สาเหตุ และดำเนินมาตรการแก้ไขเพื่อป้องกันการเกิดซ้ำ พร้อมติดตามประสิทธิผลของการแก้ไข

19.6.3 ผู้รับจ้างต้องให้ความร่วมมือในการประเมินผลการปฏิบัติงานของผู้ให้บริการตามหลักเกณฑ์ของผู้ว่าจ้าง และต้องดำเนินการปรับปรุงบริการอย่างต่อเนื่องตามข้อเสนอแนะ ผลการประเมิน ผลการตรวจสอบ เหตุการณ์ และแนวโน้มผลการให้บริการที่เกี่ยวข้อง

19.7 สิทธิในการตรวจสอบและหลักฐานการปฏิบัติตามข้อกำหนด

19.7.1 ผู้ว่าจ้างหรือผู้ตรวจสอบที่ผู้ว่าจ้างมอบหมายมีสิทธิขอตรวจสอบเอกสาร บันทึก รายงาน และหลักฐานที่เกี่ยวข้องกับการปฏิบัติตามสัญญา SLA ความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล การสำรองและกู้คืนข้อมูล ความต่อเนื่องของบริการ และการบริหารผู้ให้บริการช่วง โดยแจ้งให้ผู้รับจ้างทราบล่วงหน้าตามสมควร เว้นแต่เป็นกรณีเหตุการณ์ร้ายแรงหรือเร่งด่วน

19.7.2 ผู้รับจ้างต้องให้ความร่วมมือและจัดเตรียมหลักฐานที่จำเป็นโดยไม่ชักช้า ทั้งนี้ การตรวจสอบต้องดำเนินการโดยคำนึงถึงการรักษาความลับ ความมั่นคงปลอดภัย และไม่รบกวนการให้บริการเกินสมควร

19.7.3 หากการตรวจสอบพบข้อบกพร่องหรือความไม่สอดคล้องที่อยู่ในความรับผิดชอบของผู้รับจ้าง ผู้รับจ้างต้องจัดทำแผนแก้ไข ระบุผู้รับผิดชอบและกำหนดเวลา และรายงานผลการดำเนินการจนแล้วเสร็จ

19.8 การเก็บรักษาบันทึกและหลักฐาน

ผู้รับจ้างต้องจัดทำ ควบคุม และเก็บรักษาบันทึกและหลักฐานที่จำเป็นต่อการพิสูจน์การปฏิบัติตามสัญญา รวมถึงรายงานบริการ บันทึก SLA เหตุขัดข้อง ปัญหา การเปลี่ยนแปลง การเข้าถึงระบบ เหตุการณ์ด้านความมั่นคงปลอดภัย การสำรองและกู้คืนข้อมูล การทดสอบความต่อเนื่อง และการดำเนินการแก้ไข โดยต้องแก้ไขป้องกันการสูญหาย การแก้ไขโดยมิชอบ และสามารถเรียกดูได้เมื่อผู้ว่าจ้างร้องขอ ภายใต้ระยะเวลาเก็บรักษาที่กฎหมาย สัญญา หรือนโยบายที่เกี่ยวข้องกำหนด

ข้อ 20 เหตุสุดวิสัย

ในกรณีที่คู่สัญญาฝ่ายใดไม่สามารถปฏิบัติหน้าที่ตามสัญญาได้เนื่องจากเหตุสุดวิสัยตามกฎหมาย ฝ่ายนั้นต้องแจ้งให้อีกฝ่ายทราบเป็นหนังสือโดยเร็ว พร้อมแสดงหลักฐานและดำเนินมาตรการตามสมควรเพื่อลดผลกระทบจากเหตุดังกล่าว หากเหตุสุดวิสัยดำเนินต่อเนื่องจนทำให้ไม่อาจบรรลุวัตถุประสงค์แห่งสัญญาคู่สัญญาจะหารือร่วมกันเพื่อกำหนดแนวทางดำเนินการต่อไป ทั้งนี้ ไม่กระทบสิทธิหรือหนี้ที่เกิดขึ้นก่อนเหตุสุดวิสัย

ข้อ 21 ความรับผิดและค่าเสียหาย

ผู้รับจ้างต้องรับผิดชอบต่อความเสียหายที่เกิดแก่ผู้ว่าจ้างอันเนื่องมาจากการไม่ปฏิบัติหรือปฏิบัติไม่ถูกต้องตามสัญญา ความประมาทเลินเล่อ การกระทำโดยมิชอบ หรือการฝ่าฝืนกฎหมายของผู้รับจ้าง ลูกจ้าง ตัวแทน ผู้รับจ้างช่วง หรือผู้ประมวลผลช่วง ทั้งนี้ ตามขอบเขตที่กฎหมายกำหนด การชำระค่าปรับหรือการชดเชยตาม SLA ไม่ตัดสิทธิผู้ว่าในการเรียกค่าเสียหายส่วนที่กฎหมายหรือสัญญาให้สิทธิเรียกร้องได้

ข้อ 22 การผิดสัญญาและการบอกเลิกสัญญา

22.1 หากผู้รับจ้างผิดสัญญาในสาระสำคัญ ผู้ว่าจ้างมีสิทธิแจ้งเป็นหนังสือให้ผู้รับจ้างแก้ไขการผิดสัญญาภายในระยะเวลาที่กำหนด หากผู้รับจ้างไม่ดำเนินการแก้ไขภายในกำหนด ผู้ว่าจ้างมีสิทธิบอกเลิกสัญญาทั้งหมดหรือบางส่วนได้ เว้นแต่เป็นกรณีผิดสัญญาร้ายแรงซึ่งโดยสภาพไม่อาจแก้ไขได้ ผู้ว่าจ้างมีสิทธิบอกเลิกสัญญาได้ทันที

22.2 เหตุแห่งการบอกเลิกสัญญาให้รวมถึงแต่ไม่จำกัดเพียง การไม่ส่งมอบงาน Implementation ภายในกำหนดและไม่แก้ไขภายในระยะเวลาที่ผู้ว่าจ้างแจ้ง การผิด SLA ซ้ำหรือร้ายแรงจนกระทบต่อการดำเนินงาน การฝ่าฝืนหน้าที่ด้านความมั่นคงปลอดภัยหรือข้อมูลส่วนบุคคลอย่างร้ายแรง การหยุดให้บริการโดยไม่มีเหตุอันสมควร การโอนสิทธิหรือมอบหมายงานโดยไม่ได้รับความยินยอม การเลิกกิจการ ล้มละลาย หรือการยุติ/เลิกสนับสนุนผลิตภัณฑ์ (End of Support / End of Service) โดยไม่จัดหาทางเลือกที่มีคุณสมบัติเทียบเท่า

22.3 เมื่อสัญญาสิ้นสุดหรือถูกบอกเลิก ผู้รับจ้างต้องส่งคืนข้อมูลดำเนินการตามแผนสิ้นสุดและเปลี่ยนผ่านบริการและให้ความร่วมมือแก่ผู้ว่าจ้างเพื่อมิให้การดำเนินงานของผู้ว่าจ้างหยุดชะงัก ทั้งนี้ ผู้ว่าจ้างสงวนสิทธิเรียกค่าปรับค่าเสียหาย ใช้สิทธิตามหลักประกันสัญญา และใช้สิทธิอื่นตามกฎหมายและสัญญา

ข้อ 23 การโอนสิทธิและหน้าที่ตามสัญญา

ผู้รับจ้างจะโอนสิทธิ หน้าที่ หรือประโยชน์ใดตามสัญญานี้ทั้งหมดหรือบางส่วนให้แก่บุคคลอื่นมิได้ เว้นแต่ได้รับความยินยอมเป็นหนังสือจากผู้ว่าจ้างก่อน

ข้อ 24 การบอกกล่าว

บรรดาคำบอกกล่าว หนังสือแจ้ง หรือการติดต่อที่มีผลตามสัญญา ให้ทำเป็นหนังสือและส่งไปยังที่อยู่หรือช่องทางอิเล็กทรอนิกส์ที่คู่สัญญาระบุไว้ หากคู่สัญญาฝ่ายใดเปลี่ยนแปลงที่อยู่หรือข้อมูลติดต่อ ต้องแจ้งให้อีกฝ่ายทราบเป็นหนังสือ มิฉะนั้น ให้ถือว่าการส่งไปยังที่อยู่หรือช่องทางเดิมเป็นการส่งโดยชอบ

ข้อ 25 กฎหมายที่ใช้บังคับและการระงับข้อพิพาท

สัญญานี้อยู่ภายใต้บังคับและให้ตีความตามกฎหมายแห่งราชอาณาจักรไทย หากเกิดข้อพิพาท คู่สัญญาจะพยายามเจรจาเพื่อระงับข้อพิพาทโดยสุจริตก่อน หากไม่สามารถตกลงกันได้ ให้ดำเนินการตามกระบวนการยุติธรรมของไทย

ข้อ 26 ข้อกำหนดทั่วไป

การที่คู่สัญญาฝ่ายใดไม่ใช้สิทธิหรือผ่อนผันการใช้สิทธิตามสัญญาในคราวใด ไม่ถือเป็นการสละสิทธินั้น หากข้อกำหนดใดของสัญญาตกเป็นโมฆะหรือไม่อาจใช้บังคับได้ ให้ข้อกำหนดอื่นยังคงมีผลใช้บังคับต่อไป การแก้ไขเพิ่มเติมสัญญาจะมีผลต่อเมื่อทำเป็นหนังสือและลงนามโดยผู้มีอำนาจของคู่สัญญาทั้งสองฝ่าย

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาทั้งสองฝ่ายได้อ่านและเข้าใจข้อความแห่งสัญญาโดยตลอดแล้ว เห็นว่าถูกต้องตรงตามเจตนาของตนทุกประการ จึงได้ลงลายมือชื่อและประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และต่างฝ่ายต่างยึดถือไว้ฝ่ายละหนึ่งฉบับ

ลงชื่อ ..... ผู้ว่าจ้าง

(.....)

ตำแหน่ง .....

ลงชื่อ ..... ผู้รับจ้าง

(.....)

ตำแหน่ง .....

ลงชื่อ ..... พยาน

(.....)

ลงชื่อ ..... พยาน

(.....)

ยกร่างสัญญารักษาความลับและประมวลผลข้อมูลส่วนบุคคล

โครงการว่าจ้างบริการระบบติดตามและการประเมินตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ

สัญญาฉบับนี้ทำขึ้น ณ สมาคมสโมสรนักลงทุน เลขที่ 1 อาคาร ที พี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 เมื่อวันที่ ..... 2569 ระหว่าง

สมาคมสโมสรนักลงทุน ซึ่งมีสำนักงานใหญ่ตั้งอยู่เลขที่ 1 อาคารทีพีแอนด์ทีชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โดย นางสาวกรองกนก มานะกิจจงกล ตำแหน่ง ผู้จัดการสมาคมสโมสรนักลงทุน ซึ่งต่อไปในสัญญาฉบับนี้ เรียกว่า "ผู้ให้ข้อมูล" ฝ่ายหนึ่ง กับ

บริษัท ..... จำกัด (เลขทะเบียนนิติบุคคล .....) โดย.....ตำแหน่ง ..... ผู้มีอำนาจลงนามผูกพันบริษัท ซึ่งจดทะเบียนเป็นนิติบุคคล ณ ..... ปรากฏตามหนังสือรับรองบริษัท เลขที่ ..... ลงวันที่ ..... 2569 รายละเอียดปรากฏตามเอกสารแนบท้ายสัญญานี้ ซึ่งต่อไปในสัญญาฉบับนี้เรียกว่า "ผู้รับข้อมูล" อีกฝ่ายหนึ่ง

โดยที่ผู้รับข้อมูลมีนิติสัมพันธ์กับผู้ให้ข้อมูลตามโครงการว่าจ้างบริการระบบติดตามบริการและการประเมินตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ (ซึ่งต่อไปสัญญาฉบับนี้เรียกว่า “โครงการฯ”) ปรากฏตามสำเนาสัญญาดังกล่าวแนบท้ายสัญญา ซึ่งต่อไปในสัญญาฉบับนี้เรียกว่า "สัญญาหลัก” และถือว่าเป็นส่วนหนึ่งของสัญญาฉบับนี้ด้วย ซึ่งในการปฏิบัติงานตามสัญญาหลักดังกล่าว มีเหตุทำให้ผู้รับข้อมูล และ/หรือบุคลากรของผู้รับข้อมูล ได้รับทราบหรือเข้าถึงข้อมูลอันเป็นความลับของผู้ให้ข้อมูล รวมถึงข้อมูลอันเป็นข้อมูลส่วนบุคคล และข้อมูลที่เกี่ยวข้องกับระบบที่เชื่อมต่อในโครงการฯ หรือข้อมูลอื่นใดของพนักงาน เจ้าหน้าที่ ผู้ใช้บริการ หรือลูกค้าของผู้ให้ข้อมูล เพื่อนำมาใช้ในการวิเคราะห์ เฝ้าระวังภัยคุกคาม หรือปฏิบัติงานภายใต้ขอบเขตงานของสัญญาหลัก

คู่สัญญาตกลงกันว่า ผู้ให้ข้อมูลจะเปิดเผยข้อมูล และผู้รับข้อมูลจะเก็บรักษาข้อมูลที่ได้รับไว้เป็นความลับขั้นสูงสุด ภายใต้ข้อกำหนดและเงื่อนไขที่ระบุไว้ในสัญญาฉบับนี้ ทั้งนี้ ผู้รับข้อมูลได้อ่านและทำความเข้าใจนโยบายเทคโนโลยีสารสนเทศ ฉบับผู้ให้บริการ (IT Policy and Management for Vendor) รหัสเอกสาร: IT-1PC-02 และระเบียบปฏิบัติงานการตรวจสอบการตั้งค่าตามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Secure Configuration Baseline) รหัสเอกสาร: IT-2FM-10 และระเบียบปฏิบัติงาน ตามขั้นตอนการพัฒนาระบบ (System Development Procedure) รหัสเอกสาร: IT-2PR-05 อย่างครบถ้วนแล้ว เพื่อวัตถุประสงค์ในการปฏิบัติงานตามขอบเขตของสัญญาหลัก คู่สัญญาจึงตกลงกันมีข้อความดังต่อไปนี้

ข้อ 1. คำนิยาม

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

"การประมวลผลข้อมูล" หมายความว่า การดำเนินการใด ๆ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลอันเป็นความลับ

"ผู้มีอำนาจ" หมายความว่า ผู้แทน ผู้เข้าทำสัญญา หรือตัวแทนช่วงของคู่สัญญาแต่ละฝ่ายที่จำเป็นอย่างยิ่งที่จะต้องได้รับการเปิดเผยรายละเอียดข้อมูลอันเป็นความลับเพื่อดำเนินการให้สำเร็จตามวัตถุประสงค์แห่งสัญญาหลัก

"ข้อมูลอันเป็นความลับ" หมายความว่า บรรดาข้อความ ข้อมูล วัตถุ สื่อบันทึก หรือเอกสารใด ๆ ซึ่งผู้ให้ข้อมูลจัดหาให้แก่ผู้รับข้อมูลที่เกี่ยวกับการเจรจา หรือธุรกิจ หรือการปฏิบัติงาน ไม่ว่าจะเป็นโดยลายลักษณ์อักษร โดยวาจา หรือในรูปแบบอิเล็กทรอนิกส์ รวมถึงข้อมูลที่ปรากฏอยู่ในระบบคอมพิวเตอร์ของผู้ให้ข้อมูล ข้อมูลการตั้งค่าระบบ ข้อมูลรหัสผ่าน ข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) รายงานเหตุการณ์ภัยคุกคาม (Incident Reports) และข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ว่าจะถูกระบุว่าเป็นข้อมูลอันเป็นความลับหรือไม่ก็ตาม หรือผู้รับข้อมูลควรจะรู้ว่าเป็นความลับโดยลักษณะหรือพฤติการณ์แวดล้อม

"บุคลากร" หมายความว่า กรรมการ เจ้าหน้าที่ พนักงาน ตัวแทน หรือที่ปรึกษาของคู่สัญญาแต่ละฝ่าย ตลอดจนบุคคลหรือนิติบุคคลรวมถึงแต่ไม่จำกัดเฉพาะบริษัทใดภายในกลุ่มของคู่สัญญาแต่ละฝ่ายที่ได้รับมอบหมายให้ปฏิบัติงาน

ข้อ 2. การรักษาความลับและประมวลผลข้อมูลส่วนบุคคล

2.1 ผู้ให้ข้อมูลเป็นผู้มีสิทธิควบคุมข้อมูลอันเป็นความลับ ซึ่งได้รับการเปิดเผยด้วยวาจา ลายลักษณ์อักษร หรือบนสื่อบันทึกข้อมูลใด ๆ รวมทั้งโปรแกรมคอมพิวเตอร์ที่ถูกทำเครื่องหมายหรือระบุไว้ว่าเป็นความลับ ไม่ว่าจะได้รับการเปิดเผยด้วยวิธีใดก็ตาม

2.2 ผู้รับข้อมูลต้องรับผิดชอบรักษาข้อมูลอันเป็นความลับนั้นไว้เป็นความลับตามกฎหมาย ประกาศระเบียบที่เกี่ยวข้อง และตามข้อกำหนดและเงื่อนไขของสัญญาฉบับนี้โดยครบถ้วนและเคร่งครัด

2.3 ผู้รับข้อมูลจะต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลอันเป็นความลับเพียงเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ในสัญญาหลักและสัญญาฉบับนี้เท่านั้น และจะไม่ใช้ หรือพยายามเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลอันเป็นความลับดังกล่าว เพื่อวัตถุประสงค์อื่นใดโดยไม่ได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูลก่อนล่วงหน้า

2.4 ผู้รับข้อมูลสัญญาว่าจะไม่เปิดเผยข้อมูลอันเป็นความลับไม่ว่าทั้งหมดหรือบางส่วนให้แก่บุคคลภายนอก หรือยินยอมให้บุคคลภายนอกใช้ประโยชน์ เว้นแต่จะได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูล

2.5 ผู้รับข้อมูลสัญญาว่าจะไม่ทำซ้ำ ทำสำเนา ทำสรุปย่อ ทำบันทึกรายการ หรือทำการอื่นใดทำนองเดียวกันแก่ข้อมูลอันเป็นความลับไม่ว่าทั้งหมดหรือบางส่วน เว้นแต่เป็นเรื่องที่จำเป็นอย่างยิ่งเพื่อดำเนินการตามวัตถุประสงค์ของสัญญาหลัก และต้องได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูลก่อน และให้ถือว่าเอกสารที่ทำซ้ำหรือสำเนาเหล่านั้นเป็นข้อมูลอันเป็นความลับด้วยเช่นกัน

2.6 ผู้รับข้อมูลต้องแจ้งให้ผู้ให้ข้อมูลทราบทันที และอย่างช้าที่สุดภายใน 24 (ยี่สิบสี่) ชั่วโมง นับแต่ตรวจพบหรือมีเหตุอันควรสงสัยว่ามีการนำข้อมูลอันเป็นความลับหรือข้อมูลส่วนบุคคลใด ๆ ไปใช้ หรือเปิดเผยต่อบุคคลภายนอกโดยไม่ได้รับอนุญาต หรือเกิดเหตุละเมิดข้อมูลอันเป็นความลับ (Data Breach) อีกทั้งผู้รับข้อมูลต้องให้ความร่วมมือกับผู้ให้ข้อมูลอย่างเต็มที่ในการระงับเหตุและเยียวยาความเสียหาย

2.7 ผู้รับข้อมูลต้องใช้มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและเข้มงวดในการเก็บรักษาข้อมูลอันเป็นความลับทั้งหมดตามเกณฑ์มาตรฐานสากล ISO/IEC 27001 และตามที่กฎหมายกำหนด เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

2.8 ผู้รับข้อมูลจะไม่นำข้อมูลอันเป็นความลับไปพัฒนา ต่อยอด หรือใช้ประโยชน์เชิงพาณิชย์อื่นใด โดยไม่ได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูลก่อน

2.9 ในกรณีที่ข้อมูลใด ๆ ที่เกี่ยวข้องกับการปฏิบัติงานตามสัญญาหลักประกอบด้วยข้อมูลส่วนบุคคล คู่สัญญาตกลงจะปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยจัดให้มีมาตรฐานการรักษาความปลอดภัยข้อมูลส่วนบุคคลไม่ต่ำกว่าที่กฎหมายกำหนด

2.10 ผู้รับข้อมูลตกลงที่จะดำเนินการให้บรรดาคู่สัญญา ผู้มีอำนาจ และ/หรือบุคลากรของผู้รับข้อมูลซึ่งเข้าถึงข้อมูล ปฏิบัติตามเงื่อนไขของสัญญาฉบับนี้อย่างเคร่งครัด และต้องจัดให้บุคคลดังกล่าวลงนามในหนังสือรักษาความลับ (NDA) ที่มีเงื่อนไขไม่ต่ำกว่าสัญญาฉบับนี้ก่อนเข้าปฏิบัติงาน

ข้อ 3. ข้อยกเว้นในการเปิดเผยข้อมูลอันเป็นความลับ

ผู้รับข้อมูลไม่ต้องรับผิดในการเปิดเผยข้อมูลอันเป็นความลับเฉพาะในกรณีดังต่อไปนี้:

3.1 มีกฎหมาย คำสั่งศาล หรือหน่วยงานของรัฐที่มีอำนาจตามกฎหมายบังคับให้ต้องเปิดเผย โดยผู้รับข้อมูลต้องแจ้งให้ผู้ให้ข้อมูลทราบเป็นหนังสือล่วงหน้าก่อนการเปิดเผยทุกครั้ง เพื่อให้ผู้ให้ข้อมูลมีโอกาสคัดค้านหรือดำเนินการตามสิทธิ์

3.2 ข้อมูลอันเป็นความลับนั้นได้ถูกเปิดเผยต่อสาธารณชนแล้ว โดยมิได้เกิดจากความผิดหรือความประมาทเลินเล่อของผู้รับข้อมูล หรือบุคลากรของผู้รับข้อมูล

3.3 ผู้รับข้อมูลมีหลักฐานเป็นลายลักษณ์อักษรแสดงว่าตนได้ทราบข้อมูลนั้นอยู่ก่อนแล้ว โดยชอบด้วยกฎหมายก่อนที่ผู้ให้ข้อมูลจะเปิดเผยให้ทราบ

3.4 ผู้รับข้อมูลได้รับข้อมูลนั้นในภายหลังชอบด้วยกฎหมายจากบุคคลภายนอก โดยที่บุคคลภายนอกนั้นไม่มีหน้าที่หรือข้อผูกพันในการรักษาความลับต่อผู้ให้ข้อมูล

3.5 ผู้ให้ข้อมูลอนุญาตเป็นหนังสือให้นำข้อมูลอันเป็นความลับนั้นเปิดเผยต่อสาธารณชนได้

ข้อ 4. ระยะเวลาของสัญญา

สัญญาฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ลงนามเป็นต้นไป โดยข้อตกลงและหน้าที่ในการเก็บรักษาความลับข้อมูลภายใต้สัญญาฉบับนี้ จะยังคงมีผลผูกพันและบังคับใช้ต่อไปอีกเป็นเวลา 5 (ห้า) ปี นับถัดจากวันที่สัญญาหลักสิ้นสุดลง หรือระงับสิ้นไปไม่ว่าด้วยเหตุใดก็ตาม ทั้งนี้ หน้าที่ในการรักษาความลับและการประมวลผลข้อมูลส่วนบุคคลให้มีผลบังคับใช้ต่อไปตลอดระยะเวลาที่กฎหมายกำหนด

ข้อ 5. สิทธิในการควบคุมข้อมูล

คู่สัญญาตกลงให้อำนาจหน้าที่และสิทธิเด็ดขาดในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลอันเป็นความลับ และข้อมูลส่วนบุคคลทั้งหมด รวมถึงสำเนาทั้งหมดเป็นของผู้ให้ข้อมูลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) แต่เพียงผู้เดียว

ข้อ 6. ทรัพย์สินทางปัญญา

สัญญาฉบับนี้ไม่มีผลเป็นการโอนสิทธิ หรือการอนุญาตให้ใช้สิทธิ์ (Licensing) ไม่ว่าโดยตรงหรือโดยอ้อมในสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า หรือทรัพย์สินทางปัญญาใด ๆ ของผู้ให้ข้อมูล ให้แก่ผู้รับข้อมูล บรรดากฎเกณฑ์การตรวจจับ (Detection Rules) หรือกรณีการใช้งาน (Use Cases) ที่พัฒนาร่วมกันในโครงการ ให้ตกเป็นสิทธิ์ของผู้ให้ข้อมูลตามที่กำหนดไว้ในสัญญาหลัก

ข้อ 7. สิทธิของผู้ให้ข้อมูลในการเปิดเผยและการใช้

ผู้ให้ข้อมูลรับรองว่าตนมีสิทธิที่จะเปิดเผยข้อมูลอันเป็นความลับให้แก่ผู้รับข้อมูลเพื่อปฏิบัติการตามวัตถุประสงค์ของสัญญาฉบับนี้ แต่ผู้ให้ข้อมูลไม่ได้ให้คำรับรองเกี่ยวกับความถูกต้องแม่นยำ หรือความครบถ้วนสมบูรณ์ของข้อมูลดังกล่าวในมิติทางเทคนิคเชิงลึกที่เกินกว่าขอบเขตของโครงการ

ข้อ 8. กรณีผิดสัญญา

หากผู้รับข้อมูลกระทำผิดสัญญา หรือฝ่าฝืนข้อกำหนดข้อใดข้อหนึ่งแห่งสัญญาฉบับนี้ ผู้ให้ข้อมูลมีสิทธิเรียกคืนข้อมูลอันเป็นความลับทั้งหมด และระงับการเข้าถึงระบบได้ในทันทีโดยไม่ต้องบอกกล่าวล่วงหน้า และผู้รับข้อมูลตกลงยอมรับผิดชดใช้ค่าเสียหาย ค่าใช้จ่ายในการดำเนินคดี ตลอดจนค่าปรับที่เกิดขึ้นจริงแก่ผู้ให้ข้อมูลเต็มจำนวน และผู้ให้ข้อมูลมีสิทธิบอกเลิกสัญญาหลักได้ทันที

ข้อ 9. การโอนสิทธิ

คู่สัญญาไม่สามารถโอนสิทธิและหน้าที่ตามสัญญาฉบับนี้ให้แก่บุคคลอื่นได้ เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจากคู่สัญญาอีกฝ่ายหนึ่งล่วงหน้า

ข้อ 10. การห้ามเปิดเผยข้อมูลต่อสาธารณชน

ผู้รับข้อมูลตกลงว่าจะเก็บรักษาข้อมูลในการเข้าทำสัญญาฉบับนี้ รายละเอียดของสัญญา การเจรจาต่อรอง และวัตถุประสงค์ของโครงการไว้เป็นความลับ และจะไม่นำชื่อหรือเครื่องหมายการค้าของผู้ให้ข้อมูลไปใช้ในการโฆษณา ประชาสัมพันธ์ หรือเผยแพร่ใด ๆ โดยไม่ได้รับความเห็นชอบเป็นหนังสือจากผู้ให้ข้อมูลก่อนล่วงหน้า

ข้อ 11. ความเกี่ยวพันกับสัญญาหลัก

ให้สัญญาฉบับนี้ถือเป็นเอกสารแนบท้ายและเป็นส่วนหนึ่งของสัญญาหลัก โดยการปฏิบัติผิดสัญญาฉบับนี้ให้ถือเป็นการปฏิบัติผิดสัญญาหลักร้ายแรงด้วยเช่นกัน

ข้อ 12. การชดใช้และการเยียวยาค่าเสียหาย

12.1 ในกรณีที่ผู้รับข้อมูล ผู้มีอำนาจ และ/หรือบุคลากรของผู้รับข้อมูลฝ่าฝืนข้อกำหนดตามสัญญาฉบับนี้ จนก่อให้เกิดความเสียหาย หรือข้อมูลรั่วไหล ผู้รับข้อมูลต้องชดใช้ค่าเสียหายและค่าใช้จ่ายทั้งหมดให้แก่ผู้ให้ข้อมูล ภายใน 15 (สิบห้า) วัน นับแต่วันที่ได้รับหนังสือแจ้งจากผู้ให้ข้อมูล

12.2 กรณีที่ผู้ให้ข้อมูลถูกฟ้องร้อง ดำเนินคดี หรือถูกปรับโดยหน่วยงานรัฐ (เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) อันเนื่องมาจากการที่ผู้รับข้อมูลหรือบุคลากรของผู้รับข้อมูลปฏิบัติหน้าที่บกพร่องหรือผิดสัญญา ผู้รับข้อมูลต้องเป็นผู้รับผิดชอบชดใช้ค่าเสียหาย ค่าปรับ และค่าใช้จ่ายทางกฎหมายต่าง ๆ ทั้งหมดที่เกิดขึ้นแทนผู้ให้ข้อมูล

ข้อ 13. สิทธิในการตรวจสอบ (Right to Audit)

ผู้รับข้อมูลยินยอมให้ผู้ให้ข้อมูล หรือผู้แทนที่ได้รับมอบหมาย (รวมถึงผู้ตรวจประเมินมาตรฐาน ISO) มีสิทธิเข้าตรวจเยี่ยม และตรวจประเมินมาตรการรักษาความปลอดภัยทางกายภาพ และความปลอดภัยทางระบบสารสนเทศ ณ ศูนย์ปฏิบัติการ SOC หรือสถานที่ตั้งระบบของผู้รับข้อมูลได้ โดยแจ้งให้ทราบล่วงหน้าเป็นลายลักษณ์อักษร เพื่อให้สอดคล้องตามมาตรฐาน ISO/IEC 27001 และกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ข้อ 14. การส่งคืน ลบ หรือทำลายข้อมูล (Data Destruction)

เมื่อสิ้นสุดการปฏิบัติงานตามสัญญาหลัก หรือสัญญาหลักสิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ หรือเมื่อได้รับการร้องขอจากผู้ให้ข้อมูล ผู้รับข้อมูลต้องจัดส่งข้อมูลอันเป็นความลับทั้งหมดคืนให้แก่ผู้ให้ข้อมูล หรือทำการลบและทำลายข้อมูลความลับ ข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) และข้อมูลส่วนบุคคลที่ตกค้างอยู่ในระบบคอมพิวเตอร์และสำเนาของผู้รับข้อมูลอย่างถาวรตามมาตรฐานสากลที่ปลอดภัย และต้องจัดส่งหนังสือรับรองการลบทำลายข้อมูล (Certificate of Data Destruction) ให้แก่ผู้ให้ข้อมูลภายใน 15 (สิบห้า) วัน

ข้อ 15. การเปลี่ยนแปลงแก้ไข

การเปลี่ยนแปลง แก้ไข หรือยกเลิกข้อตกลงและเงื่อนไขใด ๆ ของสัญญาฉบับนี้ จะมีผลสมบูรณ์ก็ต่อเมื่อคู่สัญญาทั้งสองฝ่ายได้ตกลงร่วมกัน และจัดทำเป็นลายลักษณ์อักษรพร้อมลงลายมือชื่อโดยผู้มีอำนาจของทั้งสองฝ่ายเรียบร้อยแล้วเท่านั้น

ข้อ 16. สถานะการประมวลผลข้อมูลส่วนบุคคล

16.1 คู่สัญญาตกลงให้ผู้ให้ข้อมูลมีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)” และผู้รับข้อมูลมีสถานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)” ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

16.2 ผู้รับข้อมูลจะดำเนินการประมวลผลข้อมูลส่วนบุคคลได้เฉพาะตามคำสั่งที่ได้รับจากผู้ให้ข้อมูล และภายในขอบเขตที่จำเป็นต่อการปฏิบัติตามวัตถุประสงค์ของสัญญาหลักเท่านั้น

16.3 ผู้รับข้อมูลไม่มีสิทธินำข้อมูลส่วนบุคคลหรือข้อมูลอันเป็นความลับไปใช้เพื่อวัตถุประสงค์อื่น รวมถึงการวิเคราะห์เชิงพาณิชย์ การพัฒนาผลิตภัณฑ์ การฝึกสอนระบบปัญญาประดิษฐ์ (AI Training) การตลาด หรือการจัดทำฐานข้อมูลเปรียบเทียบ เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ให้ข้อมูลก่อนล่วงหน้า

ข้อ 17. การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลและข้อมูลอันเป็นความลับ

17.1 เมื่อผู้รับข้อมูลตรวจพบหรือมีเหตุอันควรเชื่อได้ว่ามีการเข้าถึง ใช้ เปิดเผย สูญหาย แก้ไข เปลี่ยนแปลง หรือทำลายข้อมูลอันเป็นความลับหรือข้อมูลส่วนบุคคลโดยมิชอบ (Data Breach) ผู้รับข้อมูลต้องแจ้งผู้ให้ข้อมูลทันทีโดยไม่ชักช้าและไม่เกิน 24 (ยี่สิบสี่) ชั่วโมงนับแต่ทราบเหตุ

17.2 หนังสือแจ้งเหตุอย่างน้อยต้องประกอบด้วยรายละเอียดดังนี้:

(1) วัน เวลา และลักษณะของเหตุการณ์ที่เกิดขึ้น

(2) ประเภทของข้อมูลและระบบที่ได้รับผลกระทบ

(3) จำนวนข้อมูล หรือจำนวนเจ้าของข้อมูลที่คาดว่าจะได้รับผลกระทบ

(4) ผลกระทบที่อาจเกิดขึ้นกับผู้ให้ข้อมูล

(5) มาตรการควบคุมและแก้ไขสถานการณ์เบื้องต้น

(6) แนวทางและมาตรการป้องกันมิให้เกิดเหตุซ้ำซ้อน

17.3 ผู้รับข้อมูลต้องให้ความร่วมมือแก่ผู้ให้ข้อมูลในการสืบสวน หาหลักฐานดิจิทัล (Digital Forensics) ระงับเหตุ แจ้งหน่วยงานกำกับดูแล และดำเนินการเยียวยาความเสียหายที่เกิดขึ้นโดยพลัน

ข้อ 18. การโอนข้อมูลไปต่างประเทศและการใช้ผู้ประมวลผลช่วง

18.1 ผู้รับข้อมูลจะไม่โอน ส่ง สำรอง จัดเก็บ หรือเปิดให้เข้าถึงข้อมูลส่วนบุคคล ข้อมูลอันเป็นความลับ ข้อมูล Log หรือข้อมูลที่เกี่ยวข้องกับโครงการจากต่างประเทศ เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ให้ข้อมูลก่อนล่วงหน้า

18.2 กรณีที่ผู้รับข้อมูลมีความจำเป็นต้องใช้ผู้รับข้อมูลช่วง หรือผู้ประมวลผลช่วง (Sub-processor) หรือผู้ให้บริการระบบคลาวด์ (Cloud Service Provider) เพื่อสนับสนุนการให้บริการ ผู้รับข้อมูลต้องแจ้งรายละเอียดให้ผู้ให้ข้อมูลพิจารณาอนุมัติล่วงหน้าเป็นลายลักษณ์อักษร

18.3 ผู้รับข้อมูลต้องจัดให้ผู้ประมวลผลช่วงดังกล่าวผูกพันตามข้อกำหนดด้านการรักษาความลับ ความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลในระดับเดียวกันหรือสูงกว่าที่กำหนดไว้ในสัญญาฉบับนี้ และผู้รับข้อมูลยังคงต้องรับผิดชอบต่อการกระทำและการละเว้นการกระทำของผู้ประมวลผลช่วงเสมือนเป็นการกระทำของผู้รับข้อมูลเองทุกประการ

สัญญาฉบับนี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียดแล้ว จึงได้ลงลายมือชื่อพร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญา ต่างฝ่ายต่างยึดถือไว้ฝ่ายละหนึ่งฉบับ

สมาคมสโมสรนักลงทุน	**บริษัท ..... จำกัด**
ลงชื่อ.....ผู้ให้ข้อมูล	ลงชื่อ.....ผู้รับข้อมูล
(นางสาวกรองกนก มานะกิจจงกล)	(.....)
ผู้จัดการสมาคมสโมสรนักลงทุน	ตำแหน่ง.....
ลงชื่อ.....พยาน	ลงชื่อ.....พยาน
(นางสาวปริญญา ศรีอนันต์)	(.....)
หัวหน้าแผนกบริหารระบบคุณภาพ ISO	ตำแหน่ง.....

สมาคมสโมสรนักลงทุน
Investor Club Association

นโยบายและการบริหารเทคโนโลยีสารสนเทศ ฉบับผู้ให้บริการ

(IT Policy and Management for Vendor)

รหัสเอกสาร:	IT-1PC-02
หมายเลขปรับปรุงเอกสาร:	1.0
วันที่เอกสารมีผลบังคับใช้:	27 เมษายน 2569
เจ้าของเอกสาร:	ฝ่ายเทคโนโลยีสารสนเทศ

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ-นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
ผู้จัดทำ	สมโภช เผือกจันทึก	หัวหน้าแผนก บริหารระบบ		24 เมษายน 2569
ผู้ทบทวน	สิริวรรณ ฉลากรไชยา	หัวหน้าฝ่าย เทคโนโลยีสารสนเทศ		24 เมษายน 2569
ผู้อนุมัติ	กรองกนก มานะกิจจงกล	ผู้จัดการ สมาคมสโมสรนักลงทุน		24 เมษายน 2569

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุงเอกสาร (version) :	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข

สารบัญ

เรื่อง หน้า

นโยบายระบบเทคโนโลยีสารสนเทศ

หลักการ

ระบบสารสนเทศ ข้อมูล ทรัพย์สินคอมพิวเตอร์ ซึ่งรวมถึงเครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ การสื่อสารด้วยข้อมูลและเสียง (ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์) เครื่องพิมพ์และอุปกรณ์/ระบบต่อพ่วง ทั้งหมดนี้ถือเป็นทรัพย์สินของสมาคมสโมสรนักลงทุน ผู้ที่ได้รับสิทธิในการใช้ พึงใช้ด้วยความสมเหตุสมผลเพื่อรักษาความถูกต้องของระบบคอมพิวเตอร์ และข้อมูล และเพื่อความปลอดภัยของทรัพย์สิน อนึ่งการใช้ทรัพย์สินเหล่านี้จะต้องใช้เพื่องานที่เกี่ยวข้องกับการดำเนินงานของสมาคม ฯ เท่านั้น

การรับทราบนโยบาย

บุคคลหรือนิติบุคคลที่ได้รับว่าจ้างโดยสมาคมสโมสรนักลงทุน จะต้องอ่านทำความเข้าใจนโยบายระบบเทคโนโลยีสารสนเทศ และลงนามรับทราบในเอกสาร Acknowledgement Statement ก่อนที่จะเข้าใช้ระบบเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน (ดูตัวอย่างตามเอกสารแนบ 1)

บทสงวนสิทธิ

ฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการติดตาม ตรวจสอบ กลั่นกรอง ปกป้องข้อมูลตามความเหมาะสม เพื่อให้สอดคล้องกับนโยบายขององค์กร การเผยแพร่ข้อมูลขององค์กรโดยพละการ การละเมิดสิทธิเข้าใช้งานระบบ และการใช้ประโยชน์จากทรัพย์สินโดยไม่ได้รับอนุญาตถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมายได้

ความปลอดภัยของอุปกรณ์ และข้อมูล

หลักการ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้แนวทางด้านความมั่นคงปลอดภัยของสารสนเทศ โดยพิจารณาองค์ประกอบ 3 ข้อหลัก ได้แก่

องค์ประกอบ	คำอธิบาย
ความลับ (Confidentiality)	การรักษาไว้ซึ่งความลับของสารสนเทศ ไม่ถูกเปิดเผยแก่ระบบ คน และ/หรือ หน่วยงานที่ไม่ได้มีส่วนเกี่ยวข้อง
ความสมบูรณ์ (Integrity)	การรักษาไว้ซึ่งความถูกต้องเสถียรภาพของสารสนเทศ ไม่ถูกแก้ไขหรือนำไปใช้อย่างผิดวิธี และสามารถตรวจสอบความถูกต้องของสารสนเทศก่อนการนำไปใช้งานได้
ความพร้อมใช้ (Availability)	การรักษาไว้ซึ่งความพร้อมใช้งานของสารสนเทศ

โดยองค์ประกอบข้างต้น จะถูกนำมาพิจารณาเป็นมูลค่าของทรัพย์สินสารสนเทศในเชิงความมั่นคงปลอดภัย อันรวมไปถึงทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับสารสนเทศ

เป้าหมายสำคัญของการดำเนินกิจกรรมตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือ การลดและหลีกเลี่ยงปัญหาการละเมิดความมั่นคงปลอดภัยสารสนเทศ อันส่งผลต่อภาพลักษณ์และความเชื่อมั่นของผู้ใช้งานระบบ โดยมีการวางเป้าหมายเชิงธุรกิจ คือ ระบบสารสนเทศของสมาคมสโมสรนักลงทุน ที่เป็นมืออาชีพในการให้บริการด้วยระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย (Information Security)

- การลดความเสี่ยง (Reduce Risk)
- การถ่ายโอนความเสี่ยง (Transfer Risk)
- การหลีกเลี่ยงความเสี่ยง (Avoid Risk)

เมื่อเลือกแนวทางในการจัดการความเสี่ยงได้แล้ว เจ้าของความเสี่ยง จะต้องกำหนดมาตรการควบคุม และแผนการดำเนินงานในการจัดการความเสี่ยง

การรักษาความปลอดภัย

หลักการ

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อแจกแจงระเบียบปฏิบัติสำหรับผู้ใช้อุปกรณ์คอมพิวเตอร์ ข้อห้ามทั่วไปที่จะนำมาประยุกต์ใช้ และอ้างอิงข้อมูลเพิ่มเติมอื่นๆ ที่จะนำมาใช้ในบางสถานการณ์

ขอบเขต

ทรัพยากรที่บริหาร และดูแลโดยฝ่ายเทคโนโลยีสารสนเทศภายใต้นโยบายฉบับนี้ครอบคลุมอุปกรณ์และโปรแกรมคอมพิวเตอร์ เอกสาร และสื่อที่ใช้อ้างอิง ข้อมูลที่เก็บบนอุปกรณ์คอมพิวเตอร์แม่ข่าย ตลอดจนข้อมูลอื่น ๆ ของสมาคมสโมสรนักลงทุนที่เก็บบนสื่ออื่น ๆ เช่น ซีดีรอม เทป รวมถึงอุปกรณ์จัดเก็บประเภทต่าง ๆ ที่อยู่ในการครอบครองของฝ่ายเทคโนโลยีสารสนเทศหรือหน่วยงานใดภายใต้สมาคมสโมสรนักลงทุน

แนวทาง

การเชื่อมต่อทั้งที่เป็นการชั่วคราวและถาวรผ่านระบบเครือข่ายต้องเป็นไปตามที่กำหนดไว้ในนโยบายฉบับนี้ ซึ่งครอบคลุมถึงการเชื่อมต่อถึงในระดับข้อมูลของเครื่องคอมพิวเตอร์แต่ละเครื่องที่ต่อเชื่อมกับเครือข่าย และอุปกรณ์โทรศัพท์ที่ใช้เชื่อมต่อด้วย

อุปกรณ์คอมพิวเตอร์ที่สมาคมสโมสรนักลงทุนไม่ได้เป็นเจ้าของ จะเชื่อมต่อกับระบบเครือข่ายของสมาคม ฯ ได้ให้ติดต่อฝ่ายเทคโนโลยีสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการติดตามเนื้อหาของข้อมูลที่มีการส่งผ่านระบบเครือข่าย

นโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy)

- การอนุญาตให้มีการเข้าถึงระบบและข้อมูลสารสนเทศใด ๆ ก็ตาม ต้องขึ้นอยู่กับความจำเป็นในการทำงาน
- การเข้าถึงระบบและข้อมูลสารสนเทศต้องมีการยืนยันตัวตนก่อนจึงจะเข้าใช้งานได้ เช่น การยืนยันตัวตนโดยใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นต้น
- ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ และต้องมีการกำหนดสิทธิ์ผู้ใช้งานในระดับสูง

- ในการเข้าใช้งานของผู้ใช้งานในระดับสูงจะต้องมีการร้องขอใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงในแต่ละครั้ง
- ผู้ดูแลระบบสามารถถอดสิทธิ์หรือเปลี่ยนแปลงสิทธิ์ในกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการให้บริการระบบและข้อมูลสารสนเทศได้ตามความเหมาะสม
- ไม่อนุญาตให้มีการใช้งานรหัสผ่านตั้งต้น (Default Password) ที่ติดมากับอุปกรณ์หรือที่มีมากับการตั้งค่าจากโรงงาน
- เจ้าของระบบหรือผู้ดูแลระบบควรมีการทบทวนสิทธิที่ได้มีการอนุญาตให้กับผู้ใช้งานอย่างสม่ำเสมอ
- ควรมีการจัดทำเอกสารแสดงสิทธิที่ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศต่างๆ เพื่อใช้ในการทบทวนและตรวจสอบการเข้าถึง
- คู่ค้าที่มีความประสงค์ร้องขอเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Account) ต้องจัดทำแบบฟอร์มร้องขอบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Request Form) (IT-2FM-07)
- ผู้ดูแลระบบบันทึกทะเบียนบัญชีผู้ใช้ที่มีสิทธิสูง (Privileged Account Inventory) (IT-2FM-09) สำหรับใช้ในการอ้างอิง

สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน

ปัจจุบันนี้ฝ่ายเทคโนโลยีสารสนเทศดำเนินการดูแลการปฏิบัติงานระบบคอมพิวเตอร์ภายในองค์กร โดยทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศจะทำหน้าที่ดูแลจัดการสัญญาการว่าจ้างจากภายนอกกับสมาคม ฯ เพื่อให้สัญญาเป็นไปตามเวลาที่กำหนดอย่างมีประสิทธิภาพและต้นทุนที่เหมาะสม โดยคู่ค้าที่ได้รับการอนุมัติให้ดำเนินการต้องปฏิบัติตามข้อกำหนดดังนี้

- ต้องกำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที
- ต้องกำหนดการตั้งรหัสผ่าน (Password Management) ต้องมีรูปแบบดังนี้
    - มีความยาวไม่ต่ำกว่า 8 ตัวอักษร
    - ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว
    - ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กอย่างน้อย 1 ตัว

- ประกอบด้วยตัวเลขอย่างน้อย 1 ตัว
- ต้องเปลี่ยนรหัสผ่านทุก 90 วัน
- รหัสผ่านที่เปลี่ยนใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม

- ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของสมาคมฯ ได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง

บุคคลที่ไม่ใช่พนักงานที่เข้าใช้เครื่องคอมพิวเตอร์โดยลำพัง และไม่มีพนักงานของบริษัทคอยดูแลอยู่ หากถูกพบจะถูกบังคับให้ออกจากระบบทันที โดยที่เครื่องคอมพิวเตอร์ที่ใช้งาน และบัญชีผู้ใช้งานที่เปิดค้างไว้ให้บุคคลใช้อยู่ขณะตรวจพบจะถูกยึด และระงับไม่ให้ใช้งานต่อไป ในเหตุการณ์ดังกล่าว จะต้องแจ้งให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและผู้บริหารของหน่วยงานที่ครอบคลุมอุปกรณ์คอมพิวเตอร์และข้อมูลนั้นรับทราบเพื่อดำเนินการต่อไป

นอกจากนี้ ผู้ใช้งานไม่ควรที่จะถือโอกาสอ่านข้อมูลที่เป็นความลับ อันเนื่องมาจากความบังเอิญ หรือจากความผิดพลาดของผู้ละเมิดเข้าสู่ระบบ หรือจากการถือสิทธิในการเข้าสู่ข้อมูลที่เหนือกว่า เป็นต้น เมื่อทราบว่าข้อมูลที่เป็นความลับถูกเปิดเผยก็ไม่ควรที่จะอ่านต่อ และจะต้องรายงานให้ผู้บริหารของฝ่ายเทคโนโลยีสารสนเทศทราบทันที เช่นเดียวกันการเขียนทับข้อมูลที่ไม่ใช่ของตนโดยตั้งใจ และไม่ได้รับอนุญาต ถือเป็นความผิด

- ต้องควบคุมให้มีมาตรการการปิดบังข้อมูลสารสนเทศเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน และปฏิบัติตามข้อกำหนดทางกฎหมาย กฎหมาย ข้อบังคับและสัญญา

แนวทางและมาตรการความปลอดภัยในการปิดบังข้อมูลเพื่อไม่ให้สามารถระบุตัวตนได้ มีดังนี้

- การปิดบังข้อมูล (Data Masking) เช่น แทนที่เลขบัตรประจำตัวประชาชน 10 หลักแรกด้วยเครื่องหมาย x แสดงเพียง 4 หลักสุดท้าย (x-xxxx-xxxxx-12-3)
- การใช้นามแฝง (Pseudonymization) เช่น แทนที่ชื่อลูกค้าด้วยเลขรหัสลูกค้า (ลูกค้าหมายเลข 12345)

- การทำข้อมูลนิรนาม (Anonymization) เช่น รวมกลุ่มข้อมูลที่มีลักษณะคล้ายคลึงกันเข้าด้วยกัน (ลูกค้ากลุ่มอายุ 20-30 ปี, เพศชาย, อาชีพพนักงานออฟฟิศ)
- การเข้ารหัส (Encryption) เช่น การเข้ารหัสการส่งอีเมล
- การลบหรือเปลี่ยนเป็นค่า null เช่น การลบข้อมูลออกจากระบบ หรือแทนที่ด้วยค่าว่าง (null)
- การแทนที่ (Substitution) เช่น แทนที่ชื่อจริงด้วยชื่อปลอม หรือแทนที่ที่อยู่จริงด้วยที่อยู่ปลอม
- การแทนที่ด้วยค่าแฮช (Hashing) เช่น เก็บรหัสผ่านในรูปแบบค่าแฮช เพื่อป้องกันการถูกขโมยและนำไปใช้

กรรมสิทธิ์ในข้อมูล

หลักการ

ระบบเทคโนโลยีสารสนเทศขององค์กร ข้อมูล รวมถึงสินทรัพย์ต่าง ๆ ในระบบคอมพิวเตอร์ ถือเป็นกรรมสิทธิ์ของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน และถือเป็นทรัพย์สมบัติที่มีค่ายิ่งขององค์กร และข้อมูลทั้งหมดที่เก็บอยู่ในสินทรัพย์เหล่านี้ถือเป็นกรรมสิทธิ์ของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน โดยฝ่ายเทคโนโลยีสารสนเทศมีความรับผิดชอบต่อข้อมูลที่เก็บไว้บนระบบเครือข่าย และระบบข้อมูลกลางอื่น ๆ ที่อยู่ภายใต้การครอบครองและดูแล ในขณะที่ผู้ใช้งานแต่ละคนจะรับผิดชอบข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายคอมพิวเตอร์แต่ละเครื่องที่ตนเองใช้งานอยู่ และอุปกรณ์การจัดเก็บประเภทต่าง ๆ ที่อยู่ในการครอบครอง

แนวทาง

ระบบคอมพิวเตอร์และข้อมูลต่าง ๆ ที่เกี่ยวข้องถือเป็นสินทรัพย์ที่มีมูลค่าขององค์กร และข้อมูลทั้งหมดที่เก็บอยู่ในสินทรัพย์เหล่านี้ถือเป็นสมบัติของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน โดยผู้ใช้งานแต่ละคนจะรับผิดชอบข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายคอมพิวเตอร์แต่ละเครื่องที่ตนเองใช้งานอยู่

การใช้ข้อมูลและระบบสารสนเทศขององค์กรจะทำได้ก็ต่อเมื่อได้รับอนุมัติโดยผู้จัดการของสมาคมสโมสรนักลงทุนเท่านั้น การมอบสิทธิในการเข้าถึงข้อมูลควรสอดคล้องกับหน้าที่และงานที่รับผิดชอบ การเปิดเผยข้อมูลควรเป็นไปตามข้อกำหนดในนโยบายว่าด้วยความลับของสมาคมสโมสรนักลงทุน (โปรดดูข้อตกลงว่าด้วยการรักษาความลับขององค์กร หรือ Mutual Confidentiality Agreement ตามเอกสารแนบ 2) การละเมิดนโยบายดังกล่าวนี้จะต้องรายงานให้คณะอนุกรรมการสารสนเทศของสมาคมสโมสรนักลงทุนหรือฝ่ายเทคโนโลยีสารสนเทศทราบทันที ผู้รับเหมาทุกรายที่ต้องเข้าใช้งานระบบสารสนเทศขององค์กรจะต้องเซ็นยอมรับตามข้อตกลงในเอกสารข้อตกลงว่าด้วยการรักษาความลับขององค์กร (Confidential Agreement)

การควบคุมการเข้าใช้งานแอพพลิเคชั่นและข้อมูล

- การจำกัดการเข้าใช้งานข้อมูล การควบคุมการเข้าถึงแอพพลิเคชั่นต้องเป็นไปตามข้อกำหนดและสอดคล้องกับนโยบายด้านการควบคุมการเข้าถึงของสมาคมสโมสรนักลงทุน กำหนดสิทธิ์ในการเข้าถึงข้อมูลตามความรับผิดชอบในการทำงาน
- การแยกระบบข้อมูลที่มีความสำคัญ ระบบที่มีความสำคัญควรจะแยกออกจากการเข้าถึงของบุคคลทั่วไป การให้บริการของแอพพลิเคชั่นที่มีความสำคัญควรใช้เซิร์ฟเวอร์ที่แยกต่างหาก ในกรณีที่อาจต้องใช้ทรัพยากรร่วมกัน เจ้าของแอพพลิเคชั่นทั้งสองฝ่ายต้องประเมินความสำคัญของข้อมูลก่อนจะตกลงกันเรื่องใช้ทรัพยากรร่วมกัน

การสำรองข้อมูลสำหรับคู่ค้า

ระบบทุกระบบและข้อมูลของผู้ใช้งานในเครื่องแม่ข่ายจะต้องทำการสำรองไว้เป็นประจำทุกวัน และสำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลง โดยข้อมูลสำรองนี้จะถูกจัดเก็บไว้ในที่ที่ปลอดภัย และทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

การบริหารจัดการ Configuration สำหรับคู่ค้า

แนวทางการบริหารจัดการ Configuration มีดังต่อไปนี้

- ต้องจัดให้มีมาตรฐานในการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Configuration Baseline) สำหรับเครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ โดยจัดทำเป็นเอกสาร เพื่อตรวจสอบให้มั่นใจว่ามีการกำหนดค่าการรักษาความมั่นคงปลอดภัยที่จำเป็น

- ต้องกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ เพื่อสามารถตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ การเปลี่ยนแปลงแก้ไข Baseline ของอุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน ต้องผ่านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเพียงพอ และได้รับการอนุมัติก่อนดำเนินการ

การบริหารจัดการคลาวด์

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการบริหารจัดการคลาวด์ เพื่อให้มีกระบวนการที่ชัดเจนสำหรับการเลือกใช้บริการคลาวด์ การจัดการการใช้งาน การควบคุมการเข้าถึง และการยกเลิกการใช้งานให้สอดคล้องกับข้อกำหนดความมั่นคงปลอดภัยของข้อมูลของสมาคมฯ

แนวทาง

นโยบายการใช้บริการคลาวด์สำหรับคู่ค้า

1. หลักการ (Principle)

หน่วยงานกำหนดให้การใช้บริการคลาวด์โดยคู่ค้า (Vendor/Third Party) ที่เกี่ยวข้องกับข้อมูลหรือระบบของหน่วยงาน ต้องอยู่ภายใต้การกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม เพื่อลดความเสี่ยงจากการเข้าถึงการใช้งานและการประมวลผลข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของหน่วยงาน

คู่ค้าจะต้องดำเนินการให้สอดคล้องกับนโยบายมาตรฐานและข้อกำหนดที่หน่วยงานกำหนดรวมถึงกฎหมายและระเบียบที่เกี่ยวข้อง

2. ขอบเขตการบังคับใช้ (Scope)

นโยบายนี้ใช้บังคับกับคู่ค้าทุกรายที่มีการใช้บริการคลาวด์ในลักษณะดังต่อไปนี้

- ให้บริการระบบหรือแอปพลิเคชันแก่หน่วยงานโดยใช้คลาวด์
- มีการจัดเก็บประมวลผลหรือรับส่งข้อมูลของหน่วยงานผ่านคลาวด์
- มีการเชื่อมต่อระบบคลาวด์กับระบบสารสนเทศของหน่วยงาน

3. แนวทางการดำเนินงาน (Policy Statements)

3.1 การเลือกใช้บริการคลาวด์

คู่ค้าต้องพิจารณาเลือกใช้บริการคลาวด์ให้เหมาะสมกับลักษณะของงานและข้อมูลโดยคำนึงถึงระดับความสำคัญของข้อมูลปริมาณข้อมูลและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศทั้งนี้ต้องสามารถอธิบายโครงสร้างระบบ (Architecture) และการไหลของข้อมูล (Data Flow) ที่เกี่ยวข้องได้อย่างชัดเจน

3.2 บทบาทและความรับผิดชอบ

คู่ค้าต้องกำหนดบทบาทและความรับผิดชอบในการบริหารจัดการคลาวด์และการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจนรวมถึงต้องมีผู้รับผิดชอบหลักด้านความมั่นคงปลอดภัยของระบบคลาวด์เพื่อให้สามารถกำกับดูแลและตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ

3.3 การควบคุมการเข้าถึง

การเข้าถึงระบบคลาวด์ต้องอยู่ภายใต้หลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) และต้องมีการกำหนดกระบวนการบริหารจัดการสิทธิ์ผู้ใช้งานอย่างเหมาะสมรวมถึงการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยและการทบทวนสิทธิ์การเข้าถึงเป็นระยะ

3.4 การเฝ้าระวังและการจัดการเหตุการณ์

คู่ค้าต้องมีมาตรการในการเฝ้าระวังตรวจจับและบันทึกเหตุการณ์ที่เกิดขึ้นในระบบคลาวด์อย่างเหมาะสมเพื่อให้สามารถตรวจสอบย้อนหลังได้และต้องดำเนินการแจ้งหน่วยงานโดยไม่ชักช้าเมื่อเกิดเหตุการณ์ที่อาจกระทบต่อความมั่นคงปลอดภัยของข้อมูลหรือระบบรวมถึงต้องมีแนวทางการตอบสนองต่อเหตุการณ์ที่ชัดเจน

3.5 การบริหารความเสี่ยงและการปฏิบัติตามข้อกำหนด

คู่ค้าต้องดำเนินการประเมินและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของการใช้บริการคลาวด์อย่างต่อเนื่องและต้องปฏิบัติตามกฎหมายระเบียบและมาตรฐานที่เกี่ยวข้องโดยต้องสามารถแสดงหลักฐานหรือเอกสารที่เกี่ยวข้องให้หน่วยงานตรวจสอบได้ตามความเหมาะสม

3.6 การคุ้มครองข้อมูล

คู่ค้าต้องจัดให้มีมาตรการคุ้มครองข้อมูลที่เหมาะสมกับระดับความสำคัญของข้อมูล เช่น การเข้ารหัสข้อมูล การสำรองข้อมูลและการกู้คืนข้อมูลรวมถึงต้องกำหนดระยะเวลาในการเก็บรักษาข้อมูลและแนวทางการจัดการข้อมูลให้สอดคล้องกับข้อกำหนดของหน่วยงาน

3.7 การติดตามและประเมินผลการให้บริการ

คู่ค้าต้องมีการติดตามตรวจสอบและประเมินผลการให้บริการคลาวด์อย่างสม่ำเสมอเพื่อให้มั่นใจว่าระบบสามารถให้บริการได้ตามระดับการให้บริการที่ตกลงไว้ และไม่ส่งผลกระทบต่อการดำเนินงานของหน่วยงาน

3.8 การสิ้นสุดการให้บริการและการทำลายข้อมูล

เมื่อสิ้นสุดการให้บริการคู่ค้าต้องดำเนินการส่งมอบข้อมูลทั้งหมดคืนให้แก่หน่วยงานในรูปแบบที่สามารถนำไปใช้งานต่อได้และต้องดำเนินการลบหรือทำลายข้อมูลของหน่วยงานที่อยู่ในระบบคลาวด์ทั้งหมดอย่างถาวร โดยไม่สามารถกู้คืนได้ พร้อมทั้งจัดทำหลักฐานยืนยันการดำเนินการดังกล่าว

4. การกำกับดูแล (Governance)

หน่วยงานขอสงวนสิทธิ์ในการตรวจสอบและประเมินการดำเนินงานของคู่ค้าในด้านการใช้บริการคลาวด์และความมั่นคงปลอดภัยสารสนเทศรวมถึงการขอข้อมูลหรือเอกสารที่เกี่ยวข้องเพื่อให้มั่นใจว่าคู่ค้าปฏิบัติตามนโยบายนี้อย่างเหมาะสม

5. การไม่ปฏิบัติตามนโยบาย (Non-Compliance)

ในกรณีที่คู่ค้าไม่ปฏิบัติตามนโยบายนี้หน่วยงานอาจพิจารณาดำเนินมาตรการที่เหมาะสมตามความรุนแรงของเหตุการณ์ รวมถึงการระงับการให้บริการหรือการยกเลิกสัญญา

นโยบายการใช้ปัญญาประดิษฐ์ภายในสมาคมสโมสรนักลงทุน

บทนำ

สมาคมสโมสรนักลงทุนตระหนักถึงศักยภาพอันยิ่งใหญ่ของปัญญาประดิษฐ์ (AI)ในการเพิ่มประสิทธิภาพการดำเนินงานสร้างสรรค์นวัตกรรมและยกระดับการบริการลูกค้าอย่างไรก็ตาม การใช้ AI อย่างมีความรับผิดชอบและมีจริยธรรมเป็นสิ่งสำคัญยิ่ง เพื่อให้มั่นใจว่าเทคโนโลยีนี้จะถูกนำมาใช้เพื่อประโยชน์สูงสุดของสมาคมและสังคมโดยรวม

การนำ AI มาใช้ในองค์กรอย่างมีประสิทธิภาพจำเป็นต้องอาศัยความร่วมมือจากทุกฝ่ายในองค์กร ตั้งแต่ผู้นำจนถึงพนักงานทุกคน การเปลี่ยนแปลงวัฒนธรรมองค์กร การเสริมสร้างความรู้ความเข้าใจเกี่ยวกับ AI และการปรับตัวให้เข้ากับเทคโนโลยีใหม่ๆ เป็นสิ่งสำคัญที่จะทำให้องค์กรสามารถเดินหน้าไปได้พร้อมกันและมั่นคง

นโยบายการใช้ปัญญาประดิษฐ์ (AI) สำหรับคู่ค้า

1. หลักการ (Principle)

หน่วยงานตระหนักถึงบทบาทของปัญญาประดิษฐ์(Artificial Intelligence: AI) ในการสนับสนุนการดำเนินงาน การวิเคราะห์ข้อมูลและการให้บริการอย่างไรก็ตาม การนำ AI มาใช้โดยคู่ค้าที่เกี่ยวข้องกับข้อมูลหรือระบบของหน่วยงานจำเป็นต้องอยู่ภายใต้การกำกับดูแลที่เหมาะสมเพื่อให้มั่นใจว่าการใช้งานเป็นไปอย่างมีความรับผิดชอบ โปร่งใส เป็นธรรม และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศของหน่วยงาน

คู่ค้าต้องดำเนินการให้สอดคล้องกับนโยบาย มาตรฐาน กฎหมาย และหลักจริยธรรมที่เกี่ยวข้องกับการใช้ AI ที่หน่วยงานกำหนด

2. ขอบเขตการบังคับใช้ (Scope)

นโยบายนี้ใช้บังคับกับคู่ค้าทุกรายที่มีการใช้ AI ในลักษณะดังต่อไปนี้

- ใช้ AI ในการให้บริการหรือพัฒนาระบบแก่หน่วยงาน
- ใช้ AI ในการประมวลผล วิเคราะห์ หรือจัดการข้อมูลของหน่วยงาน

- ใช้ AI ที่มีผลต่อการตัดสินใจ การให้บริการ หรือประสบการณ์ของผู้ใช้ที่เกี่ยวข้องกับหน่วยงาน

3. แนวทางการดำเนินงาน

3.1 การพัฒนาและการใช้งานระบบ AI

การพัฒนาและการนำระบบ AI ไปใช้งานควรอยู่ภายใต้การกำกับดูแลที่เหมาะสม โดยคู่ค้าควรดำเนินการขอความเห็นชอบจากหน่วยงานก่อนการใช้งานจริงรวมถึงต้องมีการทดสอบและประเมินความถูกต้องความเหมาะสม และผลกระทบของระบบอย่างรอบด้าน

นอกจากนี้ควรมีการติดตาม ตรวจสอบ และประเมินผลการทำงานของระบบ AI อย่างต่อเนื่อง เพื่อให้มั่นใจว่าระบบยังคงทำงานได้ตามวัตถุประสงค์และไม่ก่อให้เกิดผลกระทบที่ไม่พึงประสงค์

3.2 การจัดเก็บและประมวลผลข้อมูล

การจัดเก็บ ใช้ และประมวลผลข้อมูลที่เกี่ยวข้องกับ AI ควรดำเนินการให้สอดคล้องกับกฎหมาย มาตรฐาน และข้อกำหนดของหน่วยงาน โดยต้องให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล ความถูกต้องครบถ้วนของข้อมูล และความเหมาะสมของแหล่งข้อมูล

การเข้าถึงข้อมูลควรถูกจำกัดเฉพาะผู้ที่มีหน้าที่เกี่ยวข้องและอยู่ภายใต้การควบคุมสิทธิ์อย่างเหมาะสม เพื่อป้องกันการเข้าถึงหรือใช้งานข้อมูลโดยไม่ได้รับอนุญาต

3.3 การใช้ AI ในการตัดสินใจ

การนำ AI มาใช้ในการสนับสนุนการตัดสินใจควรดำเนินการอย่างรอบคอบ โดยการตัดสินใจที่มีนัยสำคัญไม่ควรมอบหมายให้ AI ดำเนินการโดยลำพัง และควรมีการกำกับดูแลหรือทบทวนโดยมนุษย์อย่างเหมาะสม

ทั้งนี้ ผลลัพธ์หรือข้อเสนอแนะที่ได้จาก AI ควรสามารถอธิบายเหตุผลหรือที่มาได้ในระดับที่เหมาะสม เพื่อสร้างความโปร่งใสและความเชื่อมั่นในการใช้งาน

3.4 การกำกับดูแลและการตรวจสอบ

คู่ค้าควรจัดให้มีกลไกในการกำกับดูแลการใช้ AI ให้สอดคล้องกับนโยบายของหน่วยงาน รวมถึงการติดตาม ตรวจสอบ และประเมินการดำเนินงานอย่างสม่ำเสมอ

ควรมีช่องทางในการรับข้อร้องเรียนหรือข้อเสนอแนะที่เกี่ยวข้องกับการใช้AIและดำเนินการจัดการอย่างเหมาะสม เพื่อให้สามารถปรับปรุงและพัฒนาการใช้งาน AI ได้อย่างต่อเนื่อง

4. การกำกับดูแล (Governance)

หน่วยงานขอสงวนสิทธิ์ในการกำกับดูแล ตรวจสอบ และประเมินการดำเนินงานของคู่ค้าในด้านการใช้ AI รวมถึงการขอข้อมูล เอกสาร หรือหลักฐานที่เกี่ยวข้อง เพื่อให้มั่นใจว่าการดำเนินการเป็นไปตามนโยบายนี้

5. การไม่ปฏิบัติตามนโยบาย (Non-Compliance)

ในกรณีที่คู่ค้าไม่ปฏิบัติตามนโยบายนี้ หน่วยงานอาจพิจารณาดำเนินมาตรการตามความเหมาะสม รวมถึงการระงับการให้บริการหรือการยกเลิกสัญญา

เอกสารแนบ 1

ACKNOWLEDGEMENT STATEMENT

(ตัวอย่าง)

ข้าพเจ้าได้อ่านเอกสารและทำความเข้าใจนโยบายเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน และยืนยันที่จะปฏิบัติตามเงื่อนไขและ/หรือกฎเกณฑ์ที่มีระบุในเอกสารดังกล่าว ข้าพเจ้าเข้าใจเช่นกันว่า การเซ็นรับรองในเอกสารนี้ไม่ถือว่าเป็นการทำสัญญาหรือถูกทำให้เข้าใจว่าเป็นการทำสัญญาในอนาคต แต่เป็นการรับรองว่าข้าพเจ้าได้อ่านและเข้าใจนโยบายและกฎเกณฑ์ต่าง ๆ ที่ได้ระบุในเอกสารดังกล่าวแล้ว

ชื่อ : _____

ลายเซ็น : _____

วันที่ : _____

เอกสารแนบ 2

MUTUAL CONFIDENTIALITY AGREEMENT

(ตัวอย่าง)

ระหว่าง

สมาคมสโมสรนักลงทุน

1 อาคารทีพีแอนด์ที ชั้น 12 ถนนวิภาวดี-รังสิต

แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

และ

_____

_____

_____

เพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับของทั้งสองหน่วยงานในระหว่างการหารือในประเด็นทางธุรกิจหรือระบบเทคโนโลยีสารสนเทศระหว่างกัน ทั้งสองฝ่ายมีข้อตกลงดังต่อไปนี้

1. **คำจำกัดความ**

1.1 “ข้อมูลข่าวสารที่เป็นความลับ” หมายถึงข้อมูลทั้งทางวาจาหรือเอกสารหรือข้อมูลอิเล็กทรอนิกส์ที่มาจากผู้เปิดเผย ทั้งนี้รวมถึงเอกสารและ/หรือ ข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องเช่น โปรแกรมซอฟต์แวร์ ข้อมูลไฟล์อิเล็กทรอนิกส์ต่างๆ คู่มือผู้ใช้งานและคู่มืออื่นๆ

1.2 “ผู้เปิดเผย” หมายถึง องค์กรในสัญญานี้ที่เป็นผู้ให้ข้อมูล

1.3 “ผู้รับ” หมายถึง องค์กรให้สัญญานี้ที่เป็นผู้รับข้อมูล

1.4 “โครงการ” หมายถึง _____

2. **หน้าที่ของผู้รับ**

2.1 ผู้รับจะใช้ข้อมูลข่าวสารที่เป็นความลับเพื่อวัตถุประสงค์เฉพาะโครงการนั้นเท่านั้น และจะไม่ใช้เพื่อวัตถุประสงค์อื่น ๆ ยกเว้นจะได้รับความยินยอมเป็นลายลักษณ์อักษร

2.2 ผู้รับตกลงจะไม่เปิดเผยข้อมูลข่าวสารที่เป็นความลับที่ได้รับจากผู้เปิดเผยในรูปแบบใด ๆ ก็ตาม ทั้งนี้ข้อมูลดังกล่าวจะต้องไม่อยู่ภายใต้ข้อ 2.3

2.3 ข้อตกลงนี้ไม่ผูกมัดเกี่ยวกับข้อมูลข่าวสารที่เป็นความลับกรณี (ก) ข้อมูลดังกล่าวได้รับรู้โดยสาธารณะอันเนื่องจากทางอื่นที่นอกเหนือจากผู้รับ หรือ (ข) ข้อมูลดังกล่าวเป็นข้อมูลที่ผู้รับได้ข้อมูลมาจากทางอื่นก่อนที่จะได้รับจากผู้เปิดเผย หรือ (ค) ข้อมูลดังกล่าวเป็นข้อมูลที่ผู้รับได้รับจากองค์กรอื่นซึ่งไม่เป็นการละเมิดข้อตกลงเกี่ยวกับข้อมูลที่เป็นความลับจากผู้เปิดเผย หรือ (ง) ข้อมูลดังกล่าวได้มาหรือคิดค้นมา โดยอยู่นอกเหนือจากข้อมูลที่อยู่ในข้อตกลงนี้ หรือ (จ) ข้อมูลดังกล่าวจำเป็นต้องเปิดเผยโดยข้อบังคับทางกฎหมาย

2.4 ข้อมูลข่าวสารที่เป็นความลับที่ได้รับมาเป็นทรัพย์สินของผู้เปิดเผยข้อมูล ในกรณีที่ผู้เปิดเผยข้อมูลต้องการข้อมูลดังกล่าวกลับคืนโดยแจ้งมาเป็นลายลักษณ์อักษร ผู้รับจะต้องส่งข้อมูลดังกล่าวคืน หรือทำลายข้อมูลดังกล่าว ซึ่งรวมทั้งสำเนาต่าง ๆ ตามที่ผู้เปิดเผยข้อมูลร้องขอมา

2.5 ทั้งสองฝ่ายยอมรับว่าข้อตกลงนี้ไม่มีผลต่อการโอนย้ายทรัพย์สินทางปัญญาระหว่างฝ่ายใดฝ่ายหนึ่ง

3. ข้อตกลงทั่วไป

3.1 ข้อตกลงนี้ไม่ก่อให้เกิดความสัมพันธ์ทางธุรกิจอื่นใด นอกเหนือจากการเข้าใจร่วมกันในเรื่องการรักษาความลับของข้อมูล

3.2 ผู้รับข้อมูลยอมรับว่าความเสียหายทางการเงินอาจไม่เพียงพอต่อการละเมิดข้อตกลงดังกล่าว และตกลงว่า ผู้เปิดเผยข้อมูลสามารถเสนอทางเลือกหรือแนวทางจ่ายค่าเสียหายในกรณีที่มีการละเมิดข้อตกลงดังกล่าวขึ้น

3.3 ผู้รับข้อมูลยอมรับว่าข้อมูลที่ได้รับจากผู้เปิดเผยข้อมูลไม่ได้เป็นการรับประกันหรือแสดงให้เห็นว่าข้อมูลดังกล่าวมีความถูกต้องหรือครบถ้วนสมบูรณ์ของข้อมูลที่เป็นความลับดังกล่าว

3.4 ผู้รับข้อมูลจะไม่นำส่งข้อมูลดังกล่าวออกนอกประเทศไทยไม่ว่าจะเป็นทางตรงหรือทางอ้อม ยกเว้นจะได้รับการยินยอมเป็นลายลักษณ์อักษรจากผู้เปิดเผยข้อมูล

3.5 ผู้รับข้อมูลจะต้องดำเนินการลบข้อมูลที่เป็นข้อมูล Sensitive ภายในระยะเวลา 3 เดือน หลังจากสิ้นสุดระยะเวลาการดำเนินงานของโครงการและรายงานกลับ เพื่อให้ทราบว่าดำเนินการแล้วตามมาตรฐาน

3.6 การเพิ่มเติมหรือแก้ไขข้อตกลงนี้จะต้องจัดทำเป็นลายลักษณ์อักษรพร้อมทั้งเซ็นรับรองโดยทั้งสองฝ่าย

3.7 ข้อตกลงนี้ถูกจัดทำขึ้นภายใต้กฎหมายข้อบังคับในประเทศไทย

3.8 ทั้งสองฝ่ายยอมรับว่า การเซ็นยินยอมในข้อตกลงนี้และดำเนินการส่งข้อตกลงการส่งด้วยมือทางไปรษณีย์ หรือ ทางอิเล็กทรอนิกส์ เพื่อให้อีกฝ่ายหนึ่งได้รับรู้นั้นเป็นการกระทำที่ยอมรับได้และถือว่ามีผลผูกพันได้ทันที

รับรองโดย _____ **รับรองโดย สมาคมสโมสรนักลงทุน**

ลงนาม: _____ ลงนาม: _____

ชื่อ: _____ ชื่อ: _____

ตำแหน่ง:_____ ตำแหน่ง:_____

วันที่: _____ วันที่: _____

การตรวจสอบการตั้งค่าตามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Secure Configuration Baseline)

หมายเลขเอกสาร : IT-2FM-10 หมายเลขการปรับปรุงเอกสาร : 1.0 ระดับชั้น : ใช้ภายใน วันที่บังคับใช้ : 10 ม.ค. 68 วันที่ทบทวนข้อมูล : xx/xx/xx

* หมายถึง ข้อกำหนดดังกล่าวเป็นข้อแนะนำตามที่นโยบายกำหนด

/ หมายถึง บังคับให้มีการตั้งค่าตามข้อกำหนด | O หมายถึง ไม่บังคับการตั้งค่า

No.	รายละเอียดนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ	IT Policy	Server	Network Device/ Network Security Device	Client	Application
1	* กำหนดให้รหัสผ่านมีความยาวไม่ต่ำกว่า 8 ตัวอักษร ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว ตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กอย่างน้อย 1 ตัว และตัวเลขอย่างน้อย 1 ตัว	การรักษาความปลอดภัย	/	/	/	/
2	* กำหนดให้เปลี่ยนรหัสผ่านทุก 90 วัน	การรักษาความปลอดภัย	/	/	/	/
3	รหัสผ่านที่เปลี่ยนใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม 10 ครั้งล่าสุด		O	O	O	
4	ล็อกสิทธิ์การเข้าถึงของผู้ใช้ 30 นาที เมื่อมีการป้อนรหัสผ่านผิดเกิน 5 ครั้ง		O	O	O	
5	* กำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที	การรักษาความปลอดภัย	/	/		/
6	* ติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัส	การใช้อุปกรณ์คอมพิวเตอร์	/		/	
7	ตรวจสอบการอัปเดตระบบปฏิบัติการ และแพตช์		O	O	O	
8	ตั้งสัญญาณนาฬิกาของระบบเทคโนโลยีสารสนเทศให้ตรงตามมาตรฐานสากล		O	O	O	
9	ปิดการใช้งาน Protocol ที่ไม่มีการเข้ารหัส เช่น "Telnet" และ "HTTP" เว้นแต่จำเป็นสำหรับการดำเนินงาน		O	O		/
10	ต้องจัดให้มีการบันทึกกิจกรรมของผู้ใช้งานระบบสารสนเทศ อุปกรณ์เครือข่าย และเหตุการณ์ความปลอดภัยต่าง ๆ (Logs)		O	O	O	O
11	* เครื่องคอมพิวเตอร์ต้องถูกล็อกหน้าจอเมื่อไม่มีการใช้งานเป็นเวลา 15 นาที	การรักษาความปลอดภัย			/	
12	ตรวจสอบซอฟแวร์ที่ไม่ได้รับอนุญาตให้ติดตั้ง ในเครื่องคอมพิวเตอร์ที่ใช้งานของ IC				O	

"ผู้ดำเนินการตรวจสอบ"

ลงชื่อ .....
ตำแหน่ง (.....)
วันที่ : .....

"ผู้อนุมัติการตรวจสอบ"

ลงชื่อ .....
ตำแหน่ง (.....)
วันที่ : .....

***Reference from CIS Controls V8.1

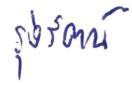
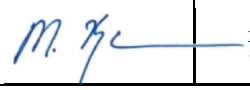
สมาคมสโมสรนักลงทุน
Investor Club Association

ขั้นตอนการพัฒนาระบบ

(System Development Procedure)

รหัสเอกสาร:	IT-2PR-05
หมายเลขปรับปรุงเอกสาร:	1.0
วันที่เอกสารมีผลบังคับใช้:	10 มกราคม 2568
เจ้าของเอกสาร:	ฝ่ายเทคโนโลยีสารสนเทศ

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ-นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
ผู้จัดทำ	รุ่งรัตน์ อุ่นจิตต์	พนักงานพัฒนาระบบสารสนเทศอาวุโส		09/01/2568
ผู้ทบทวน	สิริวรรณ ฉลากรไชยา	หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ		10 มกราคม 2568
ผู้อนุมัติ	กรองกนก มานะกิจจงกล	ผู้จัดการสมาคมสโมสรนักลงทุน		10 มกราคม 2568

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย	คำอธิบายและเหตุผลในการแก้ไข

สารบัญ

เรื่อง **หน้า**

1. บทนำ

1.1 วัตถุประสงค์ (Objective)

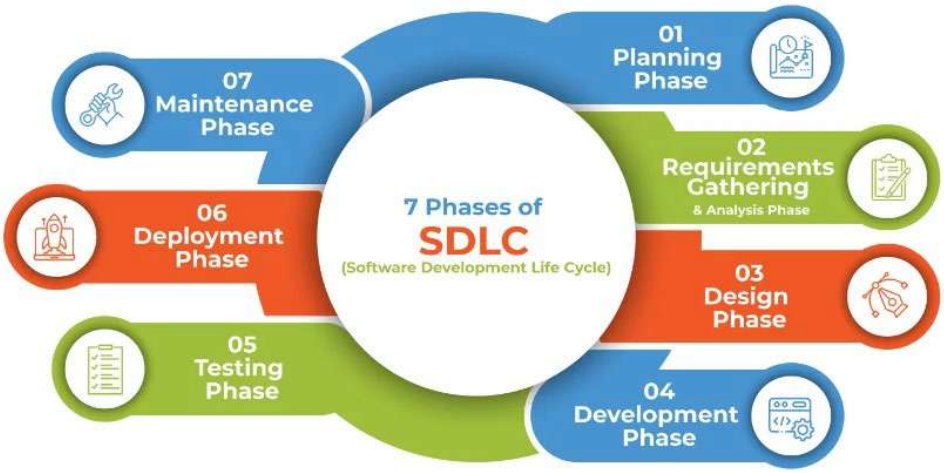
เอกสารฉบับนี้จัดทำขึ้นเพื่ออธิบายกระบวนการดำเนินงานในการจัดหาและการพัฒนาระบบที่นำมาใช้ในสมาคมฯ ให้เป็นไปตามมาตรฐานสากล

1.2 ขอบเขต (Scope)

เอกสารฉบับนี้ จัดทำขึ้นเพื่อใช้ในการกำหนดแนวทางการพัฒนาระบบที่อยู่ภายใต้ขอบเขตการขอรับรองที่อ้างอิงตามเอกสารขอบเขตระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS and ISMS Scope) (ISO-1PC-02) ที่เป็นการพัฒนาโครงการใหม่

2. กรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development Lifecycle)

เพื่อให้การพัฒนาระบบสารสนเทศและซอฟต์แวร์ เป็นไปในแนวทางที่เป็นมาตรฐานและสามารถบริหารจัดการโดยง่าย จึงกำหนดกรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ให้ครอบคลุมกระบวนการ ดังนี้



ภาพที่ 1 กระบวนการพัฒนาระบบสารสนเทศและซอฟต์แวร์

2.1 การวางแผน (Planning)

เป็นการวางแผนการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ของทั้งโครงการ โดยผู้จัดการโครงการ (Project Manager) จะวางแผนด้านระยะเวลาในการพัฒนา (Time) ขอบเขตงาน (Scope) จำนวนคนที่จะใช้ (Resource) รวมถึงวางแผนว่าใครหรือองค์ใดที่จะมีส่วนเกี่ยวข้องกับการพัฒนาบ้าง เนื่องจากบางครั้งอาจต้องอาศัยปัจจัยอื่น เช่น นโยบาย กฎหมาย หรือระเบียบที่เกี่ยวข้องของสมาคมฯ เข้ามาเป็นปัจจัยการออกแบบระบบสารสนเทศหรือซอฟต์แวร์ด้วย Project Manager จะต้องวางแผนให้คลอบคลุมกิจกรรมในการเก็บ

รวบรวมและวิเคราะห์ความต้องการ (Analysis) การออกแบบ (Design) การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development) และการทดสอบ (Testing) โดยการวางแผนงานที่ละเอียดแม่นยำ จะช่วยลดความเสี่ยงของการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ และสามารถพัฒนาสำเร็จตามเวลา และวัตถุประสงค์ที่กำหนดไว้

2.2 การเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis)

ในขั้นตอนนี้ Project Manager หรือ Product Owner หรือ Business Analyst จะเป็นผู้เก็บรวบรวม Requirement จากลูกค้าหรือผู้มีส่วนเกี่ยวข้อง เพื่อเข้าใจความต้องการจากผู้ใช้งานและการทำงานของระบบ โดยอาจจัดทำอยู่ในรูปแบบ Prototyping เพื่อให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบได้ง่ายขึ้น หลังจากการรวบรวม Requirement เสร็จแล้ว ทีมพัฒนา เช่น ผู้พัฒนาระบบ (Developer) หรือ ผู้ตรวจสอบคุณภาพ (Quality Assurance) สามารถช่วยตรวจสอบ Requirement นั้นได้เพื่อใช้ในการออกแบบและประเมินความเสี่ยงและข้อจำกัดของระบบสารสนเทศหรือซอฟต์แวร์ที่อาจเกิดขึ้น

ตัวอย่างขั้นตอนการเก็บรวบรวมและวิเคราะห์ความต้องการสำหรับการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ สามารถพิจารณาได้ดังต่อไปนี้

1) ขั้นตอนการรวบรวมความต้องการ (Requirement Gathering) เป็นขั้นตอนที่ดำเนินการรวบรวมความต้องการที่มีต่อระบบ จากกลุ่มลูกค้าหรือผู้มีส่วนเกี่ยวข้อง โดยการสัมภาษณ์หรือศึกษาปัญหา/ข้อมูลที่มีอยู่ปัจจุบัน
2) ขั้นตอนการวิเคราะห์ความต้องการ (Requirement Analysis) เป็นขั้นตอนที่จะวิเคราะห์ข้อมูลความต้องการที่รวบรวมได้ เพื่อออกแบบการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์โดยมีวัตถุประสงค์ ดังนี้
    - จัดกลุ่มความต้องการตามหมวดหมู่ เช่น ฟังก์ชันการทำงาน ประสิทธิภาพ การรักษาความมั่นคงปลอดภัย
    - ประเมินความสำคัญของความต้องการแต่ละข้อ เช่น ความต้องการข้อใดควรมีการดำเนินการทำก่อน
    - กำหนดลำดับความสำคัญของความต้องการ เช่น ระดับผลกระทบของแต่ละความต้องการ

2.3 การออกแบบระบบสารสนเทศหรือซอฟต์แวร์ (Design)

ขั้นตอนนี้หลัก ๆ แล้ว Developer จะนำ Requirement ที่ได้มาออกแบบ เช่น ออกแบบสถาปัตยกรรมที่จะใช้ (Architects) ออกแบบส่วนต่อประสานผู้ใช้งาน (User Interface) ภาษาที่จะใช้ในการพัฒนา ออกแบบฐานข้อมูล ระบบเครือข่ายและความมั่นคงปลอดภัย เป็นต้น ผลลัพธ์ที่ได้จากขั้นตอนนี้จะได้ System Design Specification ซึ่งสามารถให้ผู้มีส่วนเกี่ยวข้องหรือผู้เชี่ยวชาญตรวจสอบและให้คำแนะนำได้

2.4 การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development)

ขั้นตอนนี้ทีม Developer โดยนำ Requirement และ Design ที่ได้จากขั้นตอนที่ 2.2 และ 2.3 มาพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ โดยมีเครื่องมือต่าง ๆ ตามความต้องการของแต่ละระบบ

2.5 การทดสอบระบบสารสนเทศหรือซอฟต์แวร์ (Testing)

เป็นการประกันคุณภาพของระบบสารสนเทศหรือซอฟต์แวร์ โดยการค้นหาข้อผิดพลาด ป้องกันการเกิดข้อผิดพลาด รวมไปถึงตรวจสอบว่าระบบสารสนเทศหรือซอฟต์แวร์ที่พัฒนานั้นเป็นไปตาม Requirement หรือไม่ ในการทดสอบนั้นจะมีการสร้าง Test Case ซึ่งเป็นสถานการณ์และขั้นตอนที่ผู้ใช้งานจะใช้งานระบบ โดยใน Test Case จะมีการระบุ Expected Results คือผลที่คาดหวังจากการทดสอบโดยผลที่คาดหวังนี้จะอ้างอิงตาม Requirement ที่ได้มาจากขั้นตอนการเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis) ในกรณีที่ระบบสารสนเทศหรือซอฟต์แวร์ทำงานถูกต้องเป็นไปตามผลที่คาดหวัง จะทำให้การทดสอบนั้นผ่าน แต่หากไม่เป็นไปตามผลที่คาดหวัง จะทำให้การทดสอบนั้นไม่ผ่าน ต้องให้ Developer ดำเนินการแก้ไข ผู้ทดสอบอาจเลือกวิธีทดสอบแบบ Automated Test ได้ เพื่อให้การทดสอบสามารถทำได้รวดเร็วมากขึ้น

ในขั้นตอนการทดสอบนี้ Project Manager สามารถเพิ่มเติมรายละเอียดของกิจกรรมของการทดสอบได้ตามความเหมาะสม หรือเปลี่ยนแปลงตามแนวทาง (Methodology) ที่ถูกนำมาใช้ในการพัฒนาระบบสารสนเทศ เช่น Agile Development หรือ Waterfall Methodology เป็นต้น

<u>การกำหนดสภาพแวดล้อม (Environment) ในการพัฒนา ทดสอบ และติดตั้งระบบสารสนเทศและซอฟต์แวร์</u>

กำหนดให้สมาคมฯ แบ่งสภาพแวดล้อมเพื่อรองรับการพัฒนา ทดสอบ และติดตั้งระบบสารสนเทศและซอฟต์แวร์ ดังนี้

1) Development Environment คือ ระบบสารสนเทศและซอฟต์แวร์ ต้องได้รับการควบคุมการเข้าถึงอย่างเคร่งครัด มีระบบเครือข่ายที่สนับสนุนสภาพแวดล้อม ควรเป็นระบบปิดที่ไม่มีการเชื่อมต่อสภาพแวดล้อมของ Production
2) Test Environment คือ ใช้เพื่อการทดสอบระบบสารสนเทศหรือซอฟต์แวร์ หรือการใช้งานอุปกรณ์อื่น ๆ ก่อนการติดตั้งจริง (Deployment) ทั้งนี้ควรเป็นสภาพแวดล้อมที่ใกล้เคียงกับ Production มากที่สุด
3) Production Environment คือ สภาพแวดล้อมจริงที่มีการติดตั้งระบบสารสนเทศหรือซอฟต์แวร์เพื่อใช้งาน

ทั้งนี้การแบ่งแยกสภาพแวดล้อมควรเป็นไปทั้งในลักษณะของระบบเครือข่าย (Network) เครื่องคอมพิวเตอร์แม่ข่าย (Server and System) และพื้นที่เชิงกายภาพ (Area/Room) การกำหนดสภาพแวดล้อมในเครื่องคอมพิวเตอร์แม่ข่ายเดียวกัน (เช่น การใช้งาน Virtualized Machine) ต้องมั่นใจว่าการ

ทดสอบที่ล้มเหลวจะไม่ส่งผลกระทบต่อเครื่องคอมพิวเตอร์แม่ข่ายในระดับกายภาพ (Physical Machine Failure) ห้ามมิให้มีการทดสอบใด ๆ เกิดขึ้นบนสภาพแวดล้อม Production หรือเครื่องคอมพิวเตอร์แม่ข่ายของระบบงานใน Production โดยอ้างอิงตามหัวข้อการแบ่งหน้าที่ในการปฏิบัติงานและการจัดทำเอกสารประกอบการปฏิบัติงาน ของการจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and Operations Management) ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)

2.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment)

เป็นขั้นตอนที่นำระบบสารสนเทศหรือซอฟต์แวร์ที่ผ่านการพัฒนาและทดสอบเรียบร้อยแล้วมาติดตั้งในสภาพแวดล้อม Production เพื่อให้สามารถใช้งานได้จริง ขั้นตอนการติดตั้งนี้จะต้องมีการวางแผนอย่างรอบคอบและมีการเตรียมการเพื่อให้มั่นใจว่าการติดตั้งจะเป็นไปอย่างราบรื่นและไม่ส่งผลกระทบต่อการดำเนินงานปกติขององค์กร อ้างอิงตามหัวข้อนโยบายการบริหารจัดการนำระบบขึ้นใช้งาน (Release & Deployment Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual) และกระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure)

2.7 การบำรุงรักษา (Maintenance)

เป็นขั้นตอนหลังจากที่ระบบสารสนเทศหรือซอฟต์แวร์ถูกติดตั้งใช้งานจริงในสภาพแวดล้อม Production ซึ่งเป็นขั้นตอนในการดูแลและปรับปรุงอย่างต่อเนื่อง เพื่อให้แน่ใจว่าระบบสารสนเทศหรือซอฟต์แวร์สามารถทำงานอย่างถูกต้องโดยไม่มีข้อผิดพลาด และเหมาะสมสอดคล้องกับความต้องการที่เปลี่ยนแปลงของผู้ใช้และองค์กร รวมถึงการป้องกัน Source Code จากภัยคุกคาม นอกจากนี้ การบำรุงรักษา (Maintenance) ยังครอบคลุมถึงการปรับปรุงด้านความมั่นคงปลอดภัย การเพิ่มฟังก์ชันใหม่ และการพัฒนาระบบให้เหมาะสมกับเทคโนโลยีล่าสุดด้วยเช่นกัน โดยขั้นตอนนี้จะต้องดำเนินการอย่างสม่ำเสมอ เพื่อคงคุณภาพกับความน่าเชื่อถือและความมั่นคงปลอดภัยของระบบสารสนเทศและซอฟต์แวร์ในระยะยาว

3. ขั้นตอนการพัฒนาระบบสารสนเทศและซอฟต์แวร์

3.1 การวางแผนโครงการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Project Planning)

ก่อนการดำเนินโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ ต้องกำหนดให้มีการจัดทำแผนงานโครงการอย่างละเอียด โดยใช้มาตรฐานของสมาคมฯ หรือของผู้ให้บริการนั้น ๆ ทั้งนี้ ต้องมีเนื้อหาและรายละเอียดอย่างเป็นลายลักษณ์อักษรตามรายการ ดังต่อไปนี้ โดยอ้างอิงแนวทางที่ใช้ในการดำเนินงานโครงการด้านความมั่นคงปลอดภัยสารสนเทศตามหัวข้อ การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ ในเอกสารนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)

- การกำหนดขอบเขต วัตถุประสงค์ และรายละเอียดภาพรวมของโครงการ
- การระบุแนวทาง และกลยุทธ์ที่ใช้ในการพัฒนา

- การระบุผู้รับผิดชอบโครงการ และสมาชิกในโครงการ
- การระบุความเสี่ยงของโครงการ และแนวทางการรับมือ โดยครอบคลุมความเสี่ยงเชิงธุรกิจและเชิงเทคนิค
- การกำหนดกิจกรรม ระยะเวลา และต้นทุนของโครงการ
- ช่องทางและรูปแบบการรายงานความคืบหน้าของโครงการ
- กระบวนการในการควบคุม Configuration Item ในโครงการ เช่น เอกสาร, Package ของซอฟต์แวร์, องค์ประกอบของซอฟต์แวร์ (Software Component) โดยอ้างอิงแนวทางตามหัวข้อการบริหารจัดการ Configuration ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) และอ้างอิงขั้นตอนปฏิบัติการบริหารจัดการองค์ประกอบของบริการด้านเทคโนโลยีสารสนเทศ ในเอกสารกระบวนการจัดองค์ประกอบ (Configuration Management Procedure)
- เอกสารที่จะถูกผลิตขึ้นระหว่างการดำเนินโครงการ ทั้งเอกสารส่งมอบและเอกสารที่ใช้อ้างอิงระหว่างการดำเนินโครงการ
- เอกสารใด ๆ ที่มีรายละเอียดดังข้างต้น ต้องได้รับการอนุมัติและตรวจสอบโดยพนักงานของสมาคมฯ ตามการแต่งตั้งและบทบาทหน้าที่ความรับผิดชอบ

3.2 การบริหารจัดการความต้องการในการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Requirement Management)

ในการดำเนินโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ ต้องมีเอกสารระบุความต้องการของระบบสารสนเทศหรือซอฟต์แวร์ โดยมีการเก็บข้อมูลจากผู้ใช้งานและผู้ที่เกี่ยวข้อง โดยครอบคลุมรายการ ดังต่อไปนี้

- ความต้องการของระบบสารสนเทศหรือซอฟต์แวร์ (Functional Requirement)
- ความต้องการด้านคุณลักษณะของระบบสารสนเทศหรือซอฟต์แวร์ (Non-functional Requirement) ซึ่งครอบคลุมรายการ ดังต่อไปนี้
    1. ความต้องการด้านความมั่นคงปลอดภัย (Security Requirement) สามารถพิจารณาทั้งระบบหรือจำแนกตามแต่ละ Module ของระบบสารสนเทศหรือซอฟต์แวร์ โดยควรพิจารณาอย่างน้อยดังต่อไปนี้
        1) ระดับความมั่นคงปลอดภัยของสารสนเทศ และระบบสารสนเทศ
        2) เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยในอดีต
        3) ขอบเขตสำหรับการเชื่อมต่อระบบสารสนเทศ
        4) ผลกระทบที่อาจจะเกิดขึ้นกับระบบสารสนเทศอื่น ๆ และภาพรวมของระดับความมั่นคงปลอดภัยสารสนเทศของสมาคมฯ
        5) คุณสมบัติด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย

- การควบคุมการเข้าถึง (Access Control) ประกอบด้วย การระบุและพิสูจน์ตัวตน (Identification and Authentication) การกำหนดสิทธิการเข้าถึง (Authorization) และการจัดการหลักฐานการตรวจสอบและการรับผิดชอบต่อการกระทำ (Auditing and Accountability)
- การควบคุมการประมวลผลสารสนเทศในแอปพลิเคชัน (Correct Processing in Applications) ประกอบด้วย การตรวจสอบข้อมูลนำเข้า (Input Data Validation) การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing) การตรวจสอบความถูกต้องของข้อความ (Message Integrity) และการตรวจสอบข้อมูลนำออก (Output Data Validation)
- การป้องกันข้อมูล (Data Protection) ประกอบด้วย การเข้ารหัสข้อมูลที่จัดเก็บและการเข้ารหัสข้อมูลขณะส่ง
- การสำรองและการกู้คืนระบบ

2. ความต้องการด้านสมรรถนะและประสิทธิภาพ (Performance Requirement) สามารถพิจารณาทั้งระบบหรือจำแนกแต่ละ Module ของระบบสารสนเทศหรือซอฟต์แวร์
3. ความต้องการด้านข้อกฎหมาย เพื่อสร้างความสอดคล้องกับข้อกำหนด นโยบาย หรือกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศหรือซอฟต์แวร์ โดยอ้างอิงกฎหมายและข้อกำหนดที่ต้องปฏิบัติในเอกสาร รายการกฎหมายและข้อบังคับที่ต้องปฏิบัติตาม (List of Law and Regulatory)

- เอกสารสรุปความต้องการในรายการข้างต้น ต้องดำเนินการเป็นลายลักษณ์อักษรและต้องได้รับการอนุมัติและตรวจสอบโดยพนักงานของสมาคมฯ ตามการแต่งตั้งและบทบาทหน้าที่ความรับผิดชอบ
- เอกสารดังกล่าว ต้องได้รับการตรวจสอบและอนุมัติโดย Project Manager และมีการควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ
- การเปลี่ยนแปลงความต้องการ (Requirement Change Management) หรือคุณลักษณะใด ๆ ของระบบสารสนเทศหรือซอฟต์แวร์ ให้ดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) และชี้แจง Project Manager ตามความเหมาะสม

3.3 การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Design and Analysis)

กำหนดให้มีเอกสารใด ๆ ที่ระบุถึงการออกแบบและวิเคราะห์ระบบสารสนเทศหรือซอฟต์แวร์ ดังต่อไปนี้

- การแสดงถึงการวิเคราะห์ความต้องการของหน่วยงาน และองค์ประกอบ (Module) ของระบบสารสนเทศหรือซอฟต์แวร์ เช่น Business Flowchart
- การวิเคราะห์ถึงความสัมพันธ์ระหว่างผู้ใช้งาน และระบบสารสนเทศหรือซอฟต์แวร์ เช่น Use-case Diagram, Conceptual Diagram

- การวิเคราะห์ถึงข้อมูลเข้า/ออก ระหว่างองค์ประกอบของระบบสารสนเทศหรือซอฟต์แวร์ และการบ่งชี้ Data Storage เช่น API design, Database design (สามารถพิจารณาได้หลายระดับชั้น)
- การวิเคราะห์ความต้องการเชิงเทคนิค (Technical Requirement) และการรองรับ (Compatibility) ของระบบสารสนเทศหรือซอฟต์แวร์ รวมถึงองค์ประกอบย่อยของระบบสารสนเทศหรือซอฟต์แวร์ เช่น Product Requirement, Software Specification

เอกสารดังกล่าว ต้องได้รับการตรวจสอบและอนุมัติโดย Project Manager และควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ

การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Secure Engineering Principal) ต้องคำนึงถึงหลักวิศวกรรมด้านความมั่นคงปลอดภัยสารสนเทศ โดยมุ่งเน้นการออกแบบเพื่อรองรับการป้องกันคุณสมบัติของข้อมูลสารสนเทศ ได้แก่ ความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) โดยมีแนวทางการพิจารณา ดังนี้

ตารางที่ 1 หลักวิศวกรรมระบบสารสนเทศ

คุณสมบัติ	เกณฑ์พิจารณา	การออกแบบ	
ความลับ (Confidentiality)	เปิดเผยได้ในที่สาธารณะ	การกำหนดระดับชั้น (Classification)	ข้อมูลทั่วไป
	เปิดเผยได้เพียงบุคคลภายในกลุ่มงานที่เกี่ยวข้อง		ข้อมูลใช้ภายใน
	เปิดเผยได้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับ
	เปิดเผยได้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับมาก
	เปิดเผยได้เฉพาะผู้บริหารระดับสูงหรือบางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับที่สุด
ความถูกต้อง (Integrity)	หากข้อมูลผิดพลาด จะไม่ส่งผลกระทบต่อระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ	ความสำคัญเชิงข้อมูล (Significance)	ต่ำ
	หากข้อมูลผิดพลาด จะส่งผลในการทำงานผิดพลาดเพียงองค์ประกอบ (Function, Module) หนึ่งในระบบสารสนเทศหรือซอฟต์แวร์เท่านั้น		ปานกลาง
	หากข้อมูลผิดพลาด จะส่งผลในการทำงานผิดพลาดหลายองค์ประกอบ (Function, Module) ในระบบสารสนเทศหรือซอฟต์แวร์เท่านั้น		สูง

คุณสมบัติ	เกณฑ์พิจารณา	การออกแบบ	
	หากข้อมูลผิดพลาด จะส่งผลทำให้ระบบสารสนเทศหรือซอฟต์แวร์ล้มเหลวและหยุดชะงัก		สูงมาก
ความพร้อมใช้ (Availability)	หากขาดข้อมูลดังกล่าว จะไม่ส่งผลกระทบต่อระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ	ความสำคัญเชิงข้อมูล (Significance)	ต่ำ
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) หนึ่งในระบบสารสนเทศหรือซอฟต์แวร์หยุดการทำงาน		ปานกลาง
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) มากกว่าหนึ่งองค์ประกอบในระบบสารสนเทศหรือซอฟต์แวร์หยุดการทำงาน		สูง
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) ระบบสารสนเทศทั้งหมดหรือซอฟต์แวร์หยุดการทำงาน		สูงมาก

3.4 การพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development)

ก่อนการพัฒนาระบบหรือซอฟต์แวร์ ให้มีการดำเนินการกำหนดมาตรฐานในการพัฒนา (Coding Standard) ที่มีเนื้อหาครอบคลุมอย่างน้อยดังนี้ โดยอ้างอิงนโยบายการจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual)

- การกำหนดวิธีการตั้งชื่อระหว่างการพัฒนา เช่น การตั้งชื่อตัวแปร, การตั้งชื่อ Package เป็นต้น
- การกำหนดวิธีการสร้างข้อความ Comment
- การกำหนดรูปแบบ (Theme) การแสดงผล (Display) ของระบบสารสนเทศหรือซอฟต์แวร์
- การกำหนดอัลกอริทึม (Algorithm) ที่สามารถนำมาใช้ในการพัฒนา เช่น มาตรฐานการเข้ารหัส, มาตรฐานในการดึงชุดข้อมูลจากฐานข้อมูล
- การกำหนดวิธีการเรียกใช้งานชุดคำสั่งระหว่างองค์ประกอบย่อยของระบบสารสนเทศหรือซอฟต์แวร์ (Function Call)
- การกำหนดชนิดของข้อมูล (Data Type)

- การสร้างชุดคำสั่งต้นแบบและคุณสมบัติการสืบทอด (Inheritance)
- การกำหนดรูปแบบและประเภทของ Log
- กำหนดให้การจัดเก็บ Source Code ของระบบสารสนเทศหรือซอฟต์แวร์ผ่านเครื่องมือควบคุมที่ได้มาตรฐาน โดยมีผู้ที่ได้รับมอบหมายในการบริหารจัดการ

3.5 การทดสอบระบบสารสนเทศและซอฟต์แวร์ (Testing)

กำหนดให้ทุก ๆ ความต้องการ (Requirement) ต้องได้รับการทดสอบ โดยสามารถแบ่งออกได้เป็น 2 ลักษณะ ดังนี้

3.5.1 การทดสอบและตรวจสอบโดยผู้พัฒนา (Verification)

การทดสอบและตรวจสอบโดยผู้พัฒนา มีวัตถุประสงค์เพื่อตรวจสอบความพร้อม ความถูกต้องของระบบสารสนเทศหรือซอฟต์แวร์ เพื่อให้มั่นใจว่าตรงตามความต้องการ โดยประกอบด้วย

- การทดสอบเบื้องต้น (Unit Test)
- การทดสอบการทำงานผสานระหว่างระบบ (System Integration Test)
- การทดสอบความมั่นคงปลอดภัยของระบบ (Security Test) โดยควรครอบคลุมถึง
  - การทดสอบการเข้าถึงข้อมูลและระบบงาน
  - การเข้ารหัสข้อมูล และการปกป้องข้อมูล
  - การตั้งค่าด้านความมั่นคงปลอดภัย เช่น การตั้งค่ารหัสผ่าน การตั้งค่าเวลามาตรฐาน การตั้งค่าการเชื่อมต่อ การจัดเก็บบันทึกเหตุการณ์ (Log) เป็นต้น
  - การทดสอบความมั่นคงปลอดภัยทางเทคนิค ได้แก่ การวิเคราะห์ซอร์สโค้ด (Source Code Analysis) การประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing)

3.5.2 การทดสอบและตรวจสอบโดยผู้ใช้งานในสภาพแวดล้อมจริง (Validation)

เพื่อมั่นใจว่าระบบสารสนเทศหรือซอฟต์แวร์ สามารถถูกนำมาใช้ได้จริงในสภาพแวดล้อมจริง และได้รับการยอมรับจากผู้ใช้งาน จำเป็นต้องมีการทดสอบโดยตัวแทนฝ่ายผู้ใช้งาน (User) สามารถแบ่งได้เป็น

- การทดสอบการยอมรับระบบสารสนเทศหรือซอฟต์แวร์ (User Acceptance Test)
- การทดสอบความพร้อมก่อนการติดตั้งระบบเพื่อใช้งานจริง (Operation Readiness Test)

กำหนดให้ชุดข้อมูลทดสอบ ต้องเป็นข้อมูลจำลองเท่านั้น ในกรณีมีความจำเป็นใช้ข้อมูลจริงที่มีชั้นความลับหรือเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้มีการดำเนินการขออนุมัติอย่างเป็นลายลักษณ์อักษร และจะต้องลบข้อมูลทดสอบทั้งหมดออกจากระบบเมื่อเสร็จสิ้นการทดสอบ

กำหนดเอกสารควบคุมการทดสอบระบบสารสนเทศหรือซอฟต์แวร์ ที่ได้รับการตรวจสอบและอนุมัติโดย Project Manager และควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ โดยมีรายละเอียดครอบคลุม ดังนี้

- ชนิดและประเภทของการทดสอบและรายละเอียดเบื้องต้น เช่น วันที่ทดสอบ ผู้ดำเนินการ
- การกำหนดวิธีการและเกณฑ์การทดสอบ เช่น Key Stopper, Testing Methodology
- การกำหนดขั้นตอนการทดสอบและผลลัพธ์ที่คาดหวัง
- การกำหนดเกณฑ์การพิจารณาผลการทดสอบ เช่น ชนิดของผลการทดสอบ (Defect Type)

3.5.3 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of System Test Data)

เพื่อให้มั่นใจว่าข้อมูลที่นำมาทดสอบได้รับการควบคุมและป้องกันอย่างเหมาะสม ผู้พัฒนาและเจ้าของระบบ ควรควบคุมการใช้ข้อมูลสำหรับทดสอบดังนี้

- กำหนดให้มีการควบคุมการเข้าถึงข้อมูลที่ใช้ในการทดสอบเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ควบคุมมิให้นำข้อมูลที่ใช้ในระบบที่ให้บริการจริงไปใช้สำหรับทำการทดสอบระบบ ทั้งนี้หากมีความจำเป็นต้องใช้ ต้องจัดให้มีการควบคุมอย่างน้อยดังต่อไปนี้
  - ได้รับอนุญาตจากเจ้าของระบบก่อนนำไปใช้ในการทดสอบ
  - ปรับ หรือลบข้อมูลที่มีระดับความลับ “ลับมาก” หรือ “ลับที่สุด”
  - ลบข้อมูลที่ใช้ในการทดสอบภายหลังการทดสอบเสร็จสิ้น
  - มีการบันทึกเหตุการณ์ของการสำเนาข้อมูลจากระบบที่ให้บริการจริงเพื่อใช้ในการทดสอบ

3.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment)

ต้องได้รับความเห็นชอบและอนุมัติผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) ตามหัวข้อนโยบายการบริหารจัดการนำระบบขึ้นใช้งาน (Release & Deployment Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual) และกระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure) อย่างเคร่งครัด

3.7 การปิดโครงการหรือเสร็จสิ้นการพัฒนาโครงการ (Project Closure)

กำหนดพนักงานผู้รับผิดชอบที่ได้รับมอบหมายจากสมาคมฯ ดำเนินการสรุปผลการดำเนินงานทั้งหมด โดยมีเนื้อหาครอบคลุม

- ปัญหาและอุปสรรคที่เกิดขึ้นในโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ การแก้ไขปัญหาหรือองค์ความรู้ใหม่

- ในกรณีที่เป็นการจัดจ้างผู้ให้บริการภายนอก ให้มีการประเมินศักยภาพของผู้ให้บริการภายนอกรายนั้น ๆ
- ข้อมูลอื่น ๆ ตามที่มีร้องขอ

4. การจัดจ้างผู้ให้บริการภายนอก เพื่อการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Outsourcing Development)

กำหนดให้ผู้ให้บริการภายนอกใด ๆ ที่ได้รับการจัดจ้างให้พัฒนาระบบสารสนเทศหรือซอฟต์แวร์ให้แก่สมาคมฯ ต้องดำเนินการให้สอดคล้องและปฏิบัติตามนโยบายของสมาคมฯ อย่างเคร่งครัด โดยอ้างอิงหัวข้อนโยบายการบริหารจัดการผู้ให้บริการ ตามเอกสารกระบวนการบริหารจัดการผู้ให้บริการ (Supplier Management Procedure) ทั้งนี้ ผู้ให้บริการภายนอกจะต้องเป็นผู้เชี่ยวชาญเฉพาะด้าน และในระหว่างการดำเนินโครงการ บุคลากรที่เกี่ยวข้องและเข้าถึงข้อมูลของสมาคมฯ ต้องมีการลงนามข้อตกลงว่าด้วยการรักษาความลับขององค์กร (Mutual Confidentiality Agreement) ที่มีผลทางกฎหมายแม้สิ้นสุดโครงการ

เพื่อให้การตรวจสอบการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์โดยการจัดจ้างผู้ให้บริการภายนอกนั้นเป็นระบบหรือซอฟต์แวร์ที่มีมั่นคงปลอดภัย และมีการพัฒนาที่เป็นไปตามความต้องการขององค์กร ควรกำหนดเกณฑ์ดังต่อไปนี้สำหรับการพิจารณาตรวจรับระบบสารสนเทศหรือซอฟต์แวร์

- ต้องมีการกำหนดข้อตกลงการให้สิทธิ์ใช้งาน การเป็นเจ้าของ Code และสิทธิ์ในทรัพย์สินทางปัญญาที่เกี่ยวข้องกับเนื้อหาที่ว่าจ้างพัฒนา โดยอ้างอิงตามหัวข้อกรรมสิทธิ์ในข้อมูล ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)
- ต้องมีข้อกำหนดหรือสัญญาสำหรับการออกแบบ การเขียนโค้ด และแนวทางการทดสอบที่มั่นคงปลอดภัย
- ต้องมีการทดสอบสิ่งส่งมอบก่อนยอมรับ เพื่อประเมินคุณภาพและความถูกต้องของสิ่งที่ส่งมอบ
- ต้องมีหลักฐานแสดงว่ามีการกำหนดระดับความสามารถด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวขั้นต่ำที่สามารถยอมรับได้
- ต้องมีหลักฐานแสดงว่ามีการทดสอบอย่างเพียงพอ เพื่อป้องกันช่องโหว่ที่ทราบ
- ต้องมีหลักฐานแสดงว่าการดำเนินการพัฒนาเป็นไปตาม Requirement ที่ทางสมาคมฯ ได้กำหนดไว้

5. เอกสารที่เกี่ยวข้อง (Related Documents)

- ISO-1PC-02 ขอบเขตระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS and ISMS Scope)
- ISO-1PC-01 นโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual)
- IT-1PC-01 นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)

- IT-2PR-02 กระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure)
- RMEM-2PR-02 กระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure)
- IT-2PR-03 กระบวนการจัดองค์ประกอบ (Configuration Management Procedure)
- PU-2PR-01 กระบวนการบริหารจัดการผู้ให้บริการ (Supplier Management Procedure)
- ISO-2SD-01 รายการกฎหมายและข้อบังคับที่ต้องปฏิบัติตาม (List of Law and Regulatory)

เอกสารแนบ 1.4

แบบหนังสือค้ำประกัน

(หลักประกันสัญญา)

เลขที่..... วันที่.....

ข้าพเจ้า.....(ชื่อธนาคาร) .....สำนักงานตั้งอยู่เลขที่.....ถนน.....ตำบล/แขวง..... อำเภอ/เขต.....จังหวัด.....โดย.....ผู้มีอำนาจลงนามผูกพันธนาคาร ขอทำหนังสือค้ำประกันฉบับนี้ให้ไว้ต่อสมาคมสโมสรนักลงทุน ซึ่งต่อไปนี้เรียกว่า “ผู้ว่าจ้าง/ผู้ใช้บริการ” ดังมีข้อความต่อไปนี้

1. ตามที่..... (ชื่อบริษัท) .....ซึ่งต่อไปนี้เรียกว่า “ผู้รับจ้าง/ผู้ให้บริการ” ได้ทำสัญญา.....ตามสัญญาลงวันที่.....ซึ่งผู้รับจ้าง/ผู้ให้บริการต้องวางหลักประกันการปฏิบัติตามสัญญาต่อผู้ว่าจ้าง/ผู้ใช้บริการ เป็นจำนวนเงิน.....บาท (.....)

ข้าพเจ้ายอมผูกพันตนโดยไม่มีเงื่อนไขที่จะค้ำประกันชนิดเพิกถอนไม่ได้เช่นเดียวกับลูกหนี้ชั้นต้น ในการชำระเงินให้ตามสิทธิเรียกร้องของผู้ว่าจ้าง/ผู้ใช้บริการ จำนวนไม่เกิน.....บาท (.....) ในกรณีที่ผู้รับจ้าง/ผู้ให้บริการก่อให้เกิดความเสียหายใด ๆ หรือต้องชำระค่าปรับ หรือค่าใช้จ่ายใด ๆ หรือผู้รับจ้าง/ผู้ให้บริการมิได้ปฏิบัติตามภาระหน้าที่ใด ๆ ที่กำหนดในสัญญาดังกล่าวข้างต้นทั้งนี้ โดยข้าพเจ้าจะไม่อ้างสิทธิใด ๆ เพื่อโต้แย้ง และผู้ว่าจ้าง/ผู้ใช้บริการไม่จำเป็นต้องเรียกร้องให้ผู้รับจ้าง/ผู้ให้บริการชำระหนี้นั้นก่อน

2. หากผู้ว่าจ้าง/ผู้ใช้บริการได้ขยายระยะเวลาให้แก่ผู้รับจ้าง/ผู้ให้บริการหรือยินยอมให้ผู้รับจ้าง/ผู้ให้บริการปฏิบัติผิดแผกไปจากเงื่อนไขใด ๆ ในสัญญา ให้ถือว่าข้าพเจ้ายินยอมในกรณีนั้น ๆ ด้วย

3. หนังสือค้ำประกันนี้มีผลใช้บังคับตั้งแต่วันทำสัญญาซื้อขาย/สัญญาว่าจ้างดังกล่าวจนถึงภาระหน้าที่ทั้งหลายของผู้รับจ้าง/ผู้ให้บริการจะได้ปฏิบัติให้สำเร็จลุล่วงไป และข้าพเจ้าจะไม่เพิกถอนการค้ำประกันไม่ว่ากรณีใด ๆ ตราบเท่าที่ผู้รับจ้าง/ผู้ให้บริการยังต้องรับผิดชอบต่อ ผู้ว่าจ้าง/ผู้ใช้บริการตามสัญญาซื้อขาย/สัญญาว่าจ้างอยู่

ข้าพเจ้าได้ลงนามและประทับตราไว้ต่อหน้าพยานเป็นสำคัญ

(ลงชื่อ).....ผู้ค้ำประกัน

(.....)

ตำแหน่ง.....

(ลงชื่อ)..... พยาน

(.....)

(ลงชื่อ)..... พยาน

(.....)

บัญชีเอกสารส่วนที่ 1

เอกสารคุณสมบัติและข้อมูลบริษัท

โครงการว่าจ้างบริการระบบติดตามและการประเมินตัวชี้วัด (KPI) งานบริการด้านเทคโนโลยีสารสนเทศ

ชื่อผู้เสนอราคา .....

ลำดับ	รายการเอกสาร	มี	ไม่มี	จำนวนแผ่น	หมายเหตุ
1	สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล ซึ่งออกให้ไม่เกิน 6 เดือนก่อนวันยื่นข้อเสนอ โดยแสดงรายชื่อกรรมการ ผู้มีอำนาจลงนาม วัตถุประสงค์ที่เกี่ยวข้อง และทุนจดทะเบียนชำระแล้วไม่น้อยกว่า 1,000,000 บาท ณ วันที่ยื่นข้อเสนอ	☐	☐		
2	สำเนาหนังสือบริคณห์สนธิ/เอกสารแสดงวัตถุประสงค์ของนิติบุคคล (กรณีรายละเอียดในหนังสือรับรองนิติบุคคลไม่เพียงพอ)	☐	☐		
3	สำเนาบัญชีรายชื่อผู้ถือหุ้นล่าสุด (บอจ.5) หรือเอกสารเทียบเท่าตามประเภทนิติบุคคล	☐	☐		
4	สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ.20) (ถ้ามี)	☐	☐		
5	สำเนาบัตรประจำตัวประชาชนของผู้มีอำนาจลงนาม พร้อมรับรองสำเนาถูกต้อง	☐	☐		
6	หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมาย พร้อมสำเนาบัตรประจำตัวประชาชนของผู้มอบอำนาจและผู้รับมอบอำนาจ (กรณีมอบอำนาจ)	☐	☐		
7	หลักฐานการเป็นเจ้าของผลิตภัณฑ์ (Product Owner) หรือหนังสือแต่งตั้งเป็นตัวแทนจำหน่าย ตัวแทนให้บริการ หรือพันธมิตรทางธุรกิจอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์ ซึ่งยังมีผลใช้บังคับ ณ วันยื่นข้อเสนอ	☐	☐		
8	กรณีเสนอซอฟต์แวร์ประเภทโอเพนซอร์ส (Open Source Software): หลักฐานแสดงความสามารถในการติดตั้ง ปรับแต่ง พัฒนา บำรุงรักษา และให้บริการสนับสนุนตลอดระยะเวลาตามสัญญา รวมทั้งข้อมูลสัญญาอนุญาตการใช้งานที่เกี่ยวข้อง	☐	☐		
9	เอกสารแสดงประสบการณ์ในการให้บริการระบบ ITSM, Helpdesk, Service Desk หรือ Ticket Management System ไม่น้อยกว่า 3 ปี	☐	☐		
10	บัญชีผลงานอ้างอิงไม่น้อยกว่า 3 โครงการ พร้อมหลักฐาน เช่น สำเนาสัญญา ใบสั่งซื้อ/สั่งจ้าง หนังสือรับรองผลงาน หรือเอกสารอื่นที่ตรวจสอบได้ (ให้ปกปิดข้อมูลที่เป็นความลับได้เท่าที่ไม่กระทบต่อการตรวจสอบสาระสำคัญ)	☐	☐		
11	ประวัติผู้รับผิดชอบโครงการ (Project Manager) และทีมงานหลัก โดยระบุชื่อ ตำแหน่ง บทบาท ประสบการณ์ และช่องทางติดต่อประสานงาน	☐	☐		

ลำดับ	รายการเอกสาร	มี	ไม่มี	จำนวนแผ่น	หมายเหตุ
12	ข้อมูลทีมสนับสนุนทางเทคนิค (Technical Support) ในประเทศไทย ช่องทางรับแจ้งเหตุและวัน/เวลาการให้บริการ	☐	☐		
13	หนังสือรับรองว่าไม่มีประวัติถูกบอกเลิกสัญญาเนื่องจากการทิ้งงานหรือไม่ปฏิบัติตามสัญญาอย่างร้ายแรงกับหน่วยงานของรัฐหรือองค์กรเอกชนภายในระยะเวลา 3 ปีที่ผ่านมา	☐	☐		
14	หนังสือรับรองความถูกต้องครบถ้วนของเอกสารและยินยอมให้สมาคมตรวจสอบข้อมูล (ตามคำรับรองท้ายบัญชีเอกสารฉบับนี้)	☐	☐		
15	เอกสารอื่นตามที่กำหนดใน TOR หรือประกาศสอบราคา สำหรับเอกสารส่วนที่ 1 (โปรดระบุในช่องหมายเหตุ)	☐	☐		

คำรับรองของผู้เสนอราคา

ข้าพเจ้าขอรับรองว่าเอกสารและหลักฐานที่ยื่นประกอบข้อเสนอนี้ถูกต้อง ครบถ้วน เป็นปัจจุบัน และเป็นความจริงทุกประการ สอดคล้องกับ TOR และประกาศสอบราคา พร้อมยินยอมให้สมาคมตรวจสอบข้อมูลและหลักฐานดังกล่าวได้ หากปรากฏภายหลังว่าข้อมูลเป็นเท็จ หรือมีสาระสำคัญไม่ครบถ้วน

ข้าพเจ้ายินยอมให้สมาคมพิจารณาตัดสิทธิหรือดำเนินการตามเงื่อนไขที่กำหนด

ลงชื่อ ..... ผู้เสนอราคา/ผู้มีอำนาจลงนาม

(.....)

ตำแหน่ง .....

วันที่ .....

บัญชีเอกสารส่วนที่ 2

ข้อเสนอด้านเทคนิคและหลักฐานคุณสมบัติเฉพาะ

โครงการว่าจ้างบริการระบบบริหารจัดการ ติดตาม และประเมินผลตัวชี้วัด (KPI)

งานบริการด้านเทคโนโลยีสารสนเทศ

ชื่อผู้เสนอราคา .....

ลำดับ	รายการเอกสาร	มี	ไม่มี	จำนวนแผ่น	หมายเหตุ
1	ข้อเสนอด้านเทคนิค (Technical Proposal) ตาม TOR โดยระบุแนวทางดำเนินงาน ขอบเขตบริการ และข้อสมมติ/ข้อจำกัด (ถ้ามี)	☐	☐		
2	สรุปประสบการณ์ของบริษัท บุคลากรหลัก ผู้จัดการโครงการ และทีมงาน เพื่อประกอบการให้คะแนนด้านเทคนิค (อ้างอิงหลักฐานในเอกสารส่วนที่ 1 ได้)	☐	☐		
3	ตารางตอบข้อกำหนด (Technical Compliance Matrix) แบบข้อ-ต่อ-ข้อ พร้อมระบุหน้าอ้างอิง และข้อแตกต่าง/ข้อยกเว้น (ถ้ามี)	☐	☐		
4	รายละเอียดคุณลักษณะและฟังก์ชันของระบบ (System Functional Specification) พร้อมตารางยืนยันโมดูลตามภาคผนวก ค ครบ 20 โมดูลภายใต้แพลตฟอร์มเดียว	☐	☐		
5	รายละเอียดสิทธิ์ใช้งานระบบแบบ Named User จำนวน 25 สิทธิ์ ตามภาคผนวก ข และความสามารถในการเพิ่ม/ลดผู้ใช้งาน	☐	☐		
6	สถาปัตยกรรมระบบ (System Architecture) รูปแบบ SaaS/Cloud ผู้ให้บริการ Cloud สถานที่จัดเก็บข้อมูล (Data Residency) และการเชื่อมต่อที่เกี่ยวข้อง	☐	☐		
7	รายละเอียดการกำหนดค่า Workflow, SLA, KPI, Dashboard, Report, Audit Trail และการส่งออกข้อมูลตามขอบเขต TOR	☐	☐		
8	แผนดำเนินโครงการและแผนทรัพยากร (Project Plan & Resource Plan) ตั้งแต่ Kick-off ถึง Go-Live ภายใน 60 วัน พร้อม Milestone และผู้รับผิดชอบ	☐	☐		
9	แผนติดตั้ง กำหนดค่า และย้ายข้อมูล (Implementation, Configuration & Data Migration Plan) (กรณีมีการย้ายข้อมูล)	☐	☐		
10	แผนและกรณีทดสอบระบบ รวมถึงการสนับสนุน UAT และเกณฑ์ผ่านการทดสอบ (Test & UAT Plan)	☐	☐		
11	แผนฝึกอบรมและถ่ายทอดความรู้สำหรับผู้ดูแลระบบและผู้ใช้งาน (Training & Knowledge Transfer Plan)	☐	☐		

ลำดับ	รายการเอกสาร	มี	ไม่มี	จำนวนแผ่น	หมายเหตุ
12	บัญชีผลส่งมอบและเอกสารโครงการตาม TOR ข้อ 6 เช่น Test/UAT/Backup Recovery Report, คู่มือ, Configuration, Data Dictionary/Schema และรายงานสิทธิ์ผู้ใช้	☐	☐		
13	แผนบำรุงรักษาและสนับสนุนบริการ ครอบคลุม Corrective Maintenance, Version Upgrade, Security Patch และช่องทาง Technical Support ในประเทศไทย	☐	☐		
14	รายละเอียด SLA ตาม TOR/ภาคผนวก ก ครอบคลุม Availability 99.9%, Scheduled Maintenance, Response/Resolution Time, SLA Report รายเดือน และ Service Credit	☐	☐		
15	รายละเอียดมาตรการความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล ครอบคลุม RBAC/Least Privilege, Encryption, Audit Log, PDPA และการแจ้งเหตุภายใน 24 ชั่วโมง	☐	☐		
16	หลักฐานหรือรายงานมาตรฐานด้าน Cloud/SaaS และความมั่นคงปลอดภัย เช่น ISO/IEC 27001:2022, SOC 2 Type II หรือมาตรฐานเทียบเท่า (ถ้ามี/ตาม TOR)	☐	☐		
17	รายละเอียด Backup & Recovery (สำรองข้อมูลทุกวันและกู้คืนย้อนหลัง 90 วัน), DR Site/Infrastructure, RTO, RPO และแผนทดสอบ DR อย่างน้อยปีละ 1 ครั้ง	☐	☐		
18	รายละเอียด Data Retention, Data Portability/Export, Exit Management การส่งมอบข้อมูลภายใน 7 วันทำการ และการลบ/ทำลายข้อมูลพร้อมหนังสือรับรอง	☐	☐		
19	รายชื่อ Cloud Provider, Subprocessor และผู้รับจ้างช่วงที่เกี่ยวข้อง พร้อมบทบาท สถานที่ประมวลผลข้อมูล และมาตรการควบคุม (ถ้ามี)	☐	☐		
20	แผนการนำเสนอและสาธิตระบบ (Presentation & System Demonstration) โดยเชื่อมโยงกับข้อกำหนดและเกณฑ์ประเมิน ภายในเวลา 120 นาที และตอบข้อซักถาม 30 นาที	☐	☐		
21	ตารางคุณสมบัติเพิ่มเติมของระบบและบริการ (Value Added Features) ตามภาคผนวก ง พร้อมระบุว่าแต่ละรายการมีค่าใช้จ่ายเพิ่มเติมหรือไม่	☐	☐		
22	รายละเอียดอัตราและเงื่อนไขการต่ออายุบริการภายหลังสิ้นสุดสัญญา รวมถึงหลักเกณฑ์การปรับราคา (ไม่รวมราคาไว้ในส่วนนี้ ให้แสดงในซองราคา)	☐	☐		

ลำดับ	รายการเอกสาร	มี	ไม่มี	จำนวนแผ่น	หมายเหตุ
23	รายละเอียดเงื่อนไข วิธีการ และระยะเวลาเพิ่มสิทธิ์ผู้ใช้งาน (Additional User License) โดยไม่กระทบต่อบริการ (ไม่รวมราคาไว้ในส่วนนี้ ให้แสดงในซองราคา)	☐	☐		
24	หนังสือรับรองการปฏิบัติตาม IT Policy and Management for Vendor รหัส IT-1PC-02 และเอกสาร Supplier Risk Assessment ตามที่สมาคมร้องขอ	☐	☐		
25	เอกสารหรือหลักฐานทางเทคนิคอื่นตาม TOR และประกาศสอบราคา (โปรดระบุ)	☐	☐		

หมายเหตุ:

1. เอกสารส่วนที่ 2 ต้องไม่มีตัวเลขราคา มูลค่าค่าบริการ หรือ Pricing Schedule เนื่องจากสมาคมจะพิจารณาข้อเสนอด้านเทคนิคก่อนเปิดซองราคา

2. กรณีข้อมูลหรือหลักฐานใดได้ยื่นไว้ในเอกสารส่วนที่ 1 แล้ว ผู้เสนอราคาอาจระบุเลขรายการและหน้าที่อ้างอิงแทนการแนบซ้ำ แต่ต้องมีข้อมูลเพียงพอต่อการประเมินด้านเทคนิค

3. ผู้เสนอราคาต้องจัดทำสารบัญ/คั่นหมวด และระบุเลขหน้าอ้างอิงใน Technical Compliance Matrix ให้ตรวจสอบได้โดยสะดวก รายการที่ระบุว่า “ถ้ามี/ตาม TOR” ให้ยื่นตามลักษณะผลิตภัณฑ์และบริการที่เสนอ

คำรับรองของผู้เสนอราคา

ข้าพเจ้าขอรับรองว่า เอกสารและหลักฐานที่ยื่นประกอบข้อเสนอด้านเทคนิคนี้ถูกต้อง ครบถ้วน เป็นความจริง และสอดคล้องกับระบบและบริการที่เสนอ โดยยินยอมให้สมาคมตรวจสอบข้อมูล หลักฐาน และทดสอบ/สาธิตคุณสมบัติของระบบได้ตามความเหมาะสม

ลงชื่อ ..... ผู้เสนอราคา/ผู้มีอำนาจลงนาม

(.....)

ตำแหน่ง .....

วันที่ .....