ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย

ในการจัดจ้างพัฒนาระบบคอมพิวเตอร์

1. ชื่อโครงการ **การจ้างผู้ให้บริการพัฒนาระบบการคัดกรองผู้ประกอบการและนำเสนอผลิตภัณฑ์ธนาคารผ่านช่องทางออนไลน์ (Customer Filtering & Offering Engine)**

2. หน่วยงานเจ้าของโครงการ **ศูนย์ความเป็นเลิศด้านการค้า**

3. วงเงินงบประมาณที่ได้รับจัดสรร **4,500,000.- บาท (สี่ล้านห้าแสนบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 13 มี.ค. 2564

เป็นเงิน **4,438,300.- บาท (สี่ล้านสี่แสนสามหมื่นแปดพันสามร้อยบาทถ้วน)** ราคา/หน่วย

5. ค่า Hardware - บาท

6. ค่า Software - บาท

7. ค่าพัฒนาระบบ 4,438,300.- บาท

8. ค่าใช้จ่ายอื่นๆ - บาท

9. รายชื่อผู้รับผิดชอบกำหนดราคากลาง

9.1 นางจันทร์ฉาย	พิทักษ์อรรภพ	ผู้ช่วยผู้บริหารศูนย์ความเป็นเลิศด้านการค้า
9.2 นายพีระเดช	มักการุณ	ผู้จัดการส่วนพัฒนาระบบสารสนเทศบริการ 2 ฝ่ายบริหารและพัฒนาเทคโนโลยีสารสนเทศ
9.3 นางสาวขนิษฐา	ฤทธิตา	ผู้ช่วยผู้บริหารส่วนจัดซื้อเทคโนโลยีสารสนเทศ ฝ่ายธุรการ

10. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

10.1 บริษัท ไอบิสซิเนส คอร์ปอเรชั่น จำกัด

10.2 บริษัท คลิกเน็กซ์ จำกัด

10.3 บริษัท อินเทลลิเจ้นท์ เวฟ ไอที จำกัด

10.4 บริษัท จีเอเบิล จำกัด

10.5 บริษัท แอลเอฟฟินเทค จำกัด

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการพัฒนาระบบการคัดกรองผู้ประกอบการและนำเสนอผลิตภัณฑ์ธนาคาร

ผ่านช่องทางออนไลน์ (Customer Filtering & Offering Engine)

---

1. ข้อกำหนดความต้องการทั่วไป

ผู้ยื่นข้อเสนอต้องดำเนินการตามเงื่อนไขและขอบเขตความต้องการของระบบ EXIM CFOE ดังต่อไปนี้

1.1 ต้องดำเนินการ ทดสอบและติดตั้งระบบ EXIM CFOE ตามรายละเอียดและคุณลักษณะเฉพาะด้านความต้องการ (Functional Requirement) ที่แนบ **ตามภาคผนวก 1 ก.** และรายละเอียดคุณลักษณะเฉพาะด้านเทคนิค (Technical Requirement) ที่แนบ **ตามภาคผนวก 1 ข.**

1.2 ระบบ EXIM CFOE ที่นำเสนอ ต้องสามารถทำงานร่วมกับระบบสารสนเทศและระบบเครือข่ายของธนาคารในปัจจุบันได้

1.3 ต้องรับประกันคุณภาพ (Warranty) ระบบ EXIM CFOE พร้อมให้การสนับสนุนในระหว่างการรับประกันคุณภาพตามข้อ 2. (ผนวก 1) เป็นระยะเวลาไม่น้อยกว่า 1 ปี นับถัดจากวันที่ธนาคารตรวจรับมอบงานงวดสุดท้ายเป็นที่เรียบร้อยแล้ว

1.4 กรณีระบบ EXIM CFOE ที่เสนอมีความจำเป็นต้องใช้งานร่วมกับโปรแกรมอื่น ๆ ผู้ยื่นข้อเสนอต้องจัดให้มีโปรแกรมต่าง ๆ ที่เกี่ยวข้อง พร้อมทั้งสิทธิ์การใช้งาน (Software License) และจำนวนสิทธิ์ทั้งหมดที่ถูกต้องตามกฎหมาย (ถ้ามี) ให้ครบถ้วน รวมทั้งบริการ (Support) เป็นระยะเวลา 1 ปี นับถัดจากวันที่ธนาคารตรวจรับมอบงานงวดสุดท้ายเป็นที่เรียบร้อยแล้ว

2. การให้บริการสนับสนุนระหว่างการรับประกันคุณภาพ (Support)

2.1 ต้องจัดให้มีเจ้าหน้าที่ประสานงานที่มีความรู้ความเชี่ยวชาญ พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้สะดวกเพื่อรับแจ้งเหตุขัดข้อง ให้คำปรึกษา ตอบข้อซักถาม ให้ความช่วยเหลือหรือแก้ไขปัญหาเบื้องต้น (On Phone Support) รวมถึงช่องทางอื่นที่ธนาคารสามารถติดต่อขอรับคำปรึกษาได้ ในวันทำการของธนาคาร (วันจันทร์ถึงวันศุกร์ ตั้งแต่เวลา 7.00 – 20.00 น.) ตลอดระยะเวลา 1 ปี

2.2 กรณีไม่สามารถให้คำปรึกษา/แก้ไขปัญหาทางโทรศัพท์หรือช่องทางอื่นได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องตอบรับปัญหาเป็นลายลักษณ์อักษรผ่านทาง Email หรืออื่นๆ ภายใน 4 ชั่วโมงทำการนับจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร

2.3 กรณีไม่สามารถให้คำปรึกษา/แก้ไขปัญหาทางโทรศัพท์หรือช่องทางอื่นได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องจัดส่งพนักงานเข้ามาแก้ไขปัญหาหรือเหตุขัดข้อง ณ สถานที่ติดตั้งใช้งานระบบ เพื่อให้ใช้งานได้ภายในวันทำการถัดไป

2.4 ผู้ยื่นข้อเสนอซึ่งได้รับการคัดเลือกจะต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปัญหาเหตุขัดข้องและ/หรือความชำรุดบกพร่องของระบบ ให้แก่ธนาคารทันทีที่สามารถดำเนินการได้ และผู้ยื่นข้อเสนอซึ่งได้รับการคัดเลือกตกลงเป็นผู้รับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

2.5 ต้องจัดให้มีเจ้าหน้าที่เข้าตรวจสอบและบำรุงรักษาระบบไม่น้อยกว่า 2 ครั้ง/ปี พร้อมทั้งจัดทำรายละเอียดและขั้นตอนการตรวจเช็ค

3. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการตามขอบเขตงานที่กำหนดอย่างน้อย ดังต่อไปนี้

3.1 ด้านการติดตั้ง/ ทดสอบ และการดำเนินการอื่น ๆ ในระหว่างการติดตั้ง

3.1.1 ต้องดำเนินการติดตั้งและทดสอบความถูกต้องของระบบ EXIM CFOE ร่วมกับธนาคารในขั้นตอนการทำ UAT

3.1.2 ต้องให้คำแนะนำในการประยุกต์ใช้ และการดำเนินงานอื่น ๆ ที่จำเป็น เพื่อให้ธนาคารสามารถใช้ระบบ EXIM CFOE ได้อย่างมีประสิทธิภาพ

3.1.3 ต้องจัดให้มีการประชุมร่วมกันหรือรายงานความคืบหน้ากับคณะทำงานโครงการของธนาคารอย่างน้อย 2 สัปดาห์ต่อครั้ง พร้อมทั้งนำเสนอรายงานความก้าวหน้าของโครงการ (Project Status) เป็นประจำทุกสัปดาห์ให้ธนาคารทราบจนกว่างานจะแล้วเสร็จ

3.1.4 ต้องจัดให้มีบุคลากรที่จะให้การสนับสนุนธนาคารในระหว่างดำเนินโครงการจนแล้วเสร็จตามระยะเวลาที่กำหนด และต้องเป็นบุคคลที่สามารถสื่อสารภาษาไทยได้

3.1.5 ต้องติดตั้งและทดสอบความถูกต้องของระบบงาน รวมทั้งให้การสนับสนุนในการนำระบบขึ้นใช้งาน (Go-Live)

3.2 ด้านเอกสาร

ต้องจัดทำเอกสารส่งมอบเป็นภาษาไทย รวมทั้งจัดทำข้อมูลในรูปแบบอิเล็กทรอนิกส์ (Soft File) เช่น CD ROM, DVD, Thumb Drive เป็นต้น และบันทึกลงอุปกรณ์จัดเก็บข้อมูลอิเล็กทรอนิกส์ จำนวนอย่างละ 1 ชุด ดังนี้

3.2.1 ต้องจัดทำแผนการดำเนินงานและขั้นตอนการดำเนินงาน (Project Plan) ประกอบด้วยตารางการปฏิบัติงาน ขั้นตอนในการดำเนินงาน/ขั้นตอนในการปฏิบัติงาน ผู้รับผิดชอบงานแต่ละขั้นตอน งานที่ส่งมอบในแต่ละขั้นตอน ระยะเวลาที่ใช้ในแต่ละขั้นตอน โดยนำเสนอในรูปแบบ Gantt Chart เพื่อใช้ในการบริหารและติดตามผลการดำเนินงานให้ธนาคารก่อนเริ่มดำเนินการ

3.2.2 ต้องจัดทำเอกสาร ดังนี้

3.2.2.1 Project Plan

3.2.2.2 MOM Vendor Kickoff

3.2.2.3 Risk Assessment

3.2.3 ต้องจัดทำเอกสารการวิเคราะห์และออกแบบระบบงาน และเอกสารอื่น ๆ ที่เกี่ยวข้อง (กรณีที่มีการเพิ่มเติมจากระบบงานหลัก) ดังนี้

3.2.3.1 Business Requirement Document : BRD

3.2.3.2 Software Requirement Specification : SRS

3.2.3.3 Software Design Specification : SDS

3.2.4 ต้องจัดทำเอกสารการทดสอบระบบ ดังนี้

3.2.4.1 Unit Test (Test Case/ Test Script/ Test Result/ Defect Report)

3.2.4.2 SIT Test (System Test and System integration Test) (Test Case/ Test Script/Test Result/ Defect Report)

3.2.4.3 Performance Test (Test Case / Test Script/ Test Result/ Defect Report)

3.2.4.4 UAT Test (Test Case/ Test Script/ Test Result/ Defect Report)

3.2.4.5 Security Test (Test Case/ Test Script/ Test Result/ Defect Report)

3.2.5 ต้องจัดทำเอกสารคู่มือ Infrastructure ของระบบ 6 เล่ม ดังนี้

3.2.5.1 คู่มือการทำงานของระบบ (System Detail & Diagram)

3.2.5.2 คู่มือการติดตั้งระบบ (Installation & Configuration Manual)

3.2.5.3 คู่มือตรวจสอบการทำงานของระบบ (Monitoring Manual)

3.2.5.4 คู่มือการสำรองข้อมูล และกู้คืนระบบ (Backup & Recovery Manual)

3.2.5.5 คู่มือการใช้งานระบบสำหรับผู้ดูแลระบบ (Operation Manual Administrator, Operator)

3.2.5.6 คู่มือการแก้ไขปัญหาเบื้องต้น (Trouble Shooting Manual)

3.2.6 ต้องจัดทำเอกสารคู่มือการใช้งานระบบ ดังนี้

3.2.6.1 คู่มือการใช้งานระบบสำหรับผู้ใช้ระบบงาน (User Manual)

3.2.6.2 คู่มือการใช้งานระบบสำหรับผู้ดูแลระบบ (Administrator Manual)

3.2.7 ต้องจัดทำเอกสารประกอบการติดตั้ง

3.2.7.1 Deployment Readiness Check List

3.2.8 ต้องจัดทำเอกสาร Post Implementation Support ดังนี้

3.2.8.1 เอกสารการแก้ไขปัญหา

3.2.8.2 เอกสารรายงานการสนับสนุนการขึ้นใช้งานระบบ (Post-Go-Live Support Document)

3.3 ด้าน Software

3.3.1 ต้องส่งมอบ Source Code ที่ดำเนินการพัฒนาในโครงการ (ถ้าเป็น Software Packet ให้ส่งมอบ Source code ที่ดำเนินการ Customize) ในรูปแบบอิเล็กทรอนิกส์ กรณีที่มีลิขสิทธิ์ต้องส่งมอบลิขสิทธิ์ให้ธนาคารด้วย

3.4 ด้านการฝึกอบรม

3.4.1 ต้องจัดฝึกอบรมเกี่ยวกับการใช้งานและการดูแลระบบ EXIM CFOE พร้อมจัดทำเอกสารการฝึกอบรม โดยการอบรมจะดำเนินการอบรมในห้องอบรมหรืออบรมผ่านช่องทางออนไลน์ที่ธนาคารกำหนดให้แก่เจ้าหน้าที่ธนาคาร โดยรองรับผู้เข้ารับการฝึกอบรม ดังนี้

3.4.1.1 สำหรับผู้ใช้ระบบงาน จำนวน 2 รอบ รอบละไม่น้อยกว่า 5 คน

3.4.1.2 สำหรับผู้ดูแลระบบ จำนวน 1 รอบ รอบละไม่น้อยกว่า 2 คน

ภาคผนวก 1 ก.

รายละเอียดและคุณลักษณะเฉพาะด้านความต้องการ (Functional Requirement)
การจ้างผู้ให้บริการพัฒนาระบบการคัดกรองผู้ประกอบการและนำเสนอผลิตภัณฑ์ธนาคาร
ผ่านช่องทางออนไลน์ (Customer Filtering & Offering Engine)

ผู้ยื่นข้อเสนอต้องดำเนินการตามเงื่อนไขและขอบเขตความต้องการของระบบ EXIM CFOE ดังต่อไปนี้

1. ขอบเขตความต้องการหลักของระบบ

1.1 ระบบสามารถคัดกรองผู้ประกอบการจากข้อมูลงบการเงิน และนำเสนอผลิตภัณฑ์ธนาคารให้กับผู้ใช้งานระบบ Thailand Export Readiness Assessment & Knowledge Management (EXAC-TERAK) และทำการนำเข้าข้อมูลผู้ประกอบการที่สนใจผลิตภัณฑ์เข้าสู่ระบบ CRM

1.1.1 ระบบต้องรองรับการจัดการค่าเริ่มต้นของระบบ โดยสามารถแก้ไข แสดงข้อมูล ค้นหา และเก็บประวัติการแก้ไขหลักเกณฑ์การพิจารณาได้

1.1.2 ระบบต้องรองรับการบริหารจัดการข้อมูลผลิตภัณฑ์ของธนาคาร โดยสามารถสร้าง/ลบ/แก้ไข แสดงข้อมูล ค้นหาข้อมูล และเก็บประวัติการสร้าง/ลบ/แก้ไขข้อมูลผลิตภัณฑ์ในระบบได้

1.2 ระบบต้องรองรับการนำเข้าข้อมูลการพิจารณาจัดทำ CA และข้อมูลพิจารณาสินเชื่อ พร้อมเหตุผลในการอนุมัติหรือปฏิเสธ จากระบบ LOS และ CRM ในรูปแบบ CSV หรือ Excel ได้

1.3 ระบบต้องสามารถดึงข้อมูล (API) จากระบบดังต่อไปนี้

- ระบบ Thailand Export Readiness Assessment & Knowledge Management (EXAC-TERAK)
- ระบบ Loan Origination System (LOS)
- ระบบ Customer Relationship Management (CRM)

ซึ่งเป็นระบบของธนาคารเพื่อนำข้อมูลมาประมวลผลในระบบตามที่ธนาคารกำหนด

1.4 ระบบสามารถกำหนดสิทธิ์การเข้าใช้งาน หรือเสนอแนวทางรวมถึงวิธีการใช้งานของเจ้าหน้าที่ธนาคารให้มีการยืนยันสิทธิ์เข้าใช้งาน เพื่อความเหมาะสมและปลอดภัย

1.5 ระบบกรอกข้อมูลและเงื่อนไขของลูกค้าให้กับพนักงานธนาคาร เพื่อจัดทำข้อมูลและคุณสมบัติต่าง ๆ ของลูกค้าที่เหมาะสม และส่งข้อมูลกลับไปยังระบบ Thailand Export Readiness Assessment & Knowledge Management (EXAC-TERAK) เพื่อนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมให้กับลูกค้า

1.6 พัฒนาระบบ Matching ระหว่างคุณสมบัติลูกค้าและผลิตภัณฑ์และบริการของธนาคาร เพื่อประมวลผลและลูกค้าได้รับข้อเสนอจากผลิตภัณฑ์และบริการที่เหมาะสมและดีที่สุด

1.7 พัฒนาระบบสรุปผลการอนุมัติหรือปฏิเสธการขอสินเชื่อหรือบริการต่าง ๆ ของลูกค้าสำหรับลูกค้าที่สนใจ

1.8 ระบบสามารถเก็บข้อมูลนำไปประมวลผลและแสดงผลในรูปแบบ Dashboard โดยการทำ Data analytics เบื้องต้น เพื่อธนาคารนำไปใช้ในการวิเคราะห์ประเภทลูกค้า พฤติกรรมลูกค้า และสามารถนำไปวางแผนในการนำเสนอผลิตภัณฑ์และบริการใหม่ ๆ ที่เหมาะสมให้กับลูกค้าแต่ละประเภท รวมถึงปรับปรุงนโยบายที่เกี่ยวข้องให้มีประสิทธิภาพยิ่งขึ้น

1.9 ระบบต้องรองรับการส่ง email แจ้งเตือนต่างๆ ได้ ตามที่ธนาคารกำหนด

2. ระบบสามารถแสดงผลเว็บไซต์แบบ Responsive เพื่อแสดงบน Device ต่าง ๆ ได้ เช่น PC, Notebook, Mobile, Tablet ฯลฯ เพื่อให้แสดงผลได้อย่างถูกต้องสวยงาม
3. การพัฒนาและติดตั้งโปรแกรม ต้องสามารถติดตั้งบน Environment ที่ธนาคารได้จัดเตรียมไว้
4. ระบบที่ออกแบบและพัฒนาต้องเป็นไปตามแนวทางการพัฒนาเว็บที่ทุกคนเข้าถึงได้ (WEB Content Accessibility Guidelines 2.0 (WCAG2.0) ของ W3C) อย่างน้อย Level A
5. ระบบที่พัฒนาต้องใช้หลักการของ OWASP (The Open Web Application Security Project) Top 10 Version ล่าสุดที่มีการประกาศในการใช้งาน ณ วันที่ประกาศผลการจัดจ้าง

ภาคผนวก 1 ข.

รายละเอียดและคุณลักษณะเฉพาะด้านเทคนิค (Technical Requirement)

การจ้างผู้ให้บริการพัฒนาระบบการคัดกรองผู้ประกอบการและนำเสนอผลิตภัณฑ์ธนาคาร ผ่านช่องทางออนไลน์ (Customer Filtering & Offering Engine)

ข้อกำหนดความต้องการด้านเทคนิคของระบบงาน

1. ด้าน System Architecture

1.1 ระบบงานต้องทำงานแบบ 3-tier Architecture

1.2 ระบบงานที่ให้บริการต้องเป็นลักษณะ Web-Base Application

1.3 ระบบสามารถทำงานบนระบบปฏิบัติการ (Operating System) Windows Server 2019, Linux RHEL (Version ไม่ต่ำกว่า 8.0) ได้อย่างใดอย่างหนึ่ง

1.4 ระบบสามารถทำงานบนฐานข้อมูลเชิงสัมพันธ์ (Relational Database) ต้องรองรับ Microsoft SQL Server 2016, Maria DB (Version ไม่ต่ำกว่า 10.5) ได้อย่างใดอย่างหนึ่ง

1.5 ระบบสามารถทำงานบน Web Server IIS หรือ Apache ได้อย่างใดอย่างหนึ่ง

1.6 ระบบมีการแบ่งแยกการเข้าใช้งานระบบ รวมถึงสามารถกำหนดสิทธิในการเข้าถึงระดับต่างๆ ได้ เช่น User, Operation, Admin, Super admin เป็นต้น

1.7 ต้องสนับสนุนการใช้สิทธิ์เข้าใช้ระบบด้วย AD (Active Directory) ของธนาคาร

1.8 ต้องทำการทดสอบ Performance Test (Load Test) จาก Testing Tool โดยการทดสอบต้องรองรับปริมาณผู้ใช้ระบบงานพร้อมกัน (Concurrent Users) ไม่น้อยกว่า 100 คน

1.9 ระบบที่นำเสนอต้องสามารถบันทึกรายการ (Log) เพื่อการตรวจสอบ และผู้ใช้ระบบงานต้องไม่สามารถ Delete และ Insert ได้ แบ่งเป็น

- บันทึกการเข้าออกระบบ (Access Logs)
- บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Transection Logs)
- บันทึกเมื่อเกิด Application Error (Exception Logs) (ถ้ามี)

1.10 ผู้รับจ้างต้องดำเนินการติดตั้งระบบ และข้อมูลทั้งหมดของโครงการให้มาอยู่ภายใต้ Server ที่ธนาคารกำหนด

2. ด้านมาตรฐานการรักษาความปลอดภัยของระบบ (System & Web Application) อย่างน้อยดังนี้

2.1 เว็บไซต์ของระบบต้องมีความปลอดภัยในการทำธุรกรรม โดยใช้ Protocol ที่เข้ารหัสลับในการรับส่งข้อมูลระหว่างผู้ใช้บริการกับ Web Server เช่น HTTPs

2.2 รูปแบบการสื่อสารต้องใช้ Protocol (SSL 3.0/TLS 1.2) เป็นอย่างน้อย

2.3 มีการใช้ใบรับรองแบบ-Wildcard SSL Certificate

2.4 มีการทำ End-to-End Encryption ที่ระดับ Application Layer เพื่อรักษาความลับและความปลอดภัยข้อมูลผู้ใช้บริการ เช่น รหัสผ่านของผู้ใช้บริการ

2.5 มีการเข้ารหัสข้อมูลรหัสผ่านของผู้ใช้บริการ ที่จัดเก็บในฐานข้อมูลที่ใช้ในการพิสูจน์ตัวตน (Authentication Database) ด้วยมาตรฐานการเข้ารหัสที่เป็นที่ยอมรับสากล โดยเลือกอัลกอริทึมในการเข้ารหัสแบบย้อนกลับไม่ได้ (Irreversible Encryption หรือ Hashing) และมีความมั่นคงปลอดภัย

2.6 ต้องมีการ SCAN ระบบ โดยต้องครอบคลุม และปิดความเสี่ยงของ OWASP TOP 10 ในปีล่าสุด

2.7 มีการควบคุมให้ข้อความแจ้งเตือน (Error Message) เป็นหน้ากลางที่มีรูปแบบเดียวกันทั้งหมด โดยข้อความจะต้องสื่อสารให้ลูกค้าเกิดความเข้าใจที่ถูกต้อง และจะต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อ และ version ของ Web Application, Debug Message, Stack Trace, IP Address, Path เป็นต้น และควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด

2.8 มีมาตรฐานในการเพิ่มความมั่นคงปลอดภัยให้กับรหัสผ่านของระบบ
- ต้องมีความยาวอย่างน้อย 8 ตัวอักษร และต้องประกอบด้วย ตัวหนังสือ ตัวเลข ตัวอักษรพิมพ์ใหญ่ และตัวอักษรสัญลักษณ์ อย่างน้อย 1 ตัวอักษร

2.9 ต้องไม่ให้มีการใช้ค่าเริ่มต้นของ รหัสผ่าน ที่มากับการตั้งโปรแกรมครั้งแรก

2.10 ตรวจสอบและจัดการลบ บัญชีผู้ที่ไม่ได้ใช้งาน ออกจากระบบทั้งหมด (จากขั้นตอนทดสอบ) ก่อนขึ้น Go-Live ระบบ

2.11 ปิด Services ต่าง ๆ ที่ไม่จำเป็นบนเครื่องที่ให้บริการระบบ

2.12 มีการควบคุมไม่ให้มีการจัดเก็บข้อมูลที่ใช้ในการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการ เช่น User ID หรือ รหัสผ่าน ไว้ใน Cookie หรือ ใน Web Browser

2.13 มีการบริหารจัดการ Session การใช้งานอย่างเหมาะสม โดยอย่างน้อยให้มีการควบคุมที่ลดความเสี่ยงจาก Man in-the-Middle Attack และ Man-in-the-Browser Attack

2.14 มีการควบคุมไม่ให้มีการเก็บข้อมูลที่สำคัญของลูกค้าไว้ใน Session และมีการสร้าง Session Key ใหม่เมื่อมีการเข้าสู่ระบบ

2.15 มีการกำหนด Time-Out ของ Session

2.16 หน้าเว็บไซต์ (Browser) ควรออกแบบให้สามารถป้องกันการ key เดาสุ่มข้อมูลสำคัญ เช่น User ID/Password การสืบค้นข้อมูลบัญชีของลูกค้า เป็นต้น

2.17 ระบบงานสามารถควบคุมไม่ให้ Username เดียวกันเข้าใช้งานระบบพร้อมกัน (Concurrent Session)

2.18 ระบบสามารถระงับการใช้งานของบัญชีผู้ใช้ระบบงานเป็นการชั่วคราว เมื่อมีการใส่ข้อมูลการพิสูจน์ตัวตนผิด เกิน 5 ครั้ง และปลดระงับให้ผู้ใช้ระบบงานสามารถ log in ได้อีกครั้งหลังจาก 5 นาที (สามารถเปลี่ยนแปลง ได้ในอนาคตตามนโยบายที่ธนาคารกำหนด) นับจากการใส่ข้อมูลการพิสูจน์ตัวตนผิดครั้งสุดท้าย

2.19 ระบบสามารถเข้ารหัสข้อมูลที่รับส่งด้วยมาตรฐานการเข้ารหัสที่มีความมั่นคงปลอดภัย โดยใช้วิธีการเข้ารหัส แบบ 256 bit หรือสูงกว่า โดยใช้ใบรับรองความปลอดภัยตามที่ธนาคารกำหนด และธนาคารสามารถเปลี่ยนใบรับรองความปลอดภัยได้ในอนาคต

3. การควบคุมมาตรฐานความปลอดภัยของระบบฐานข้อมูล (Database) อย่างน้อยดังนี้

3.1 ไม่ใช้สิทธิ์ในการเข้าถึงจาก Active Directory ให้สร้างบัญชีผู้ใช้ระบบงานภายในฐานข้อมูล และกำหนดสิทธิ์ การใช้งาน และควบคุมการเข้าถึงให้เหมาะสมกับหน้าที่ของผู้ใช้ระบบงาน

3.2 ไม่ใช้บัญชีที่มีสิทธิ์สูงสุดของฐานข้อมูลในการเข้าถึงฐานข้อมูลโดยแอปพลิเคชัน

3.3 ต้องกำหนดสิทธิ์ของแอปพลิเคชันในการเข้าถึง ฐานข้อมูล ให้เหมาะสม เช่น มีสิทธิ์ในการ Insert, Update, Delete ข้อมูลใน Table เท่านั้น

3.4 ตรวจสอบและทบทวนบัญชีผู้ใช้ภายในฐานข้อมูล และลบบัญชีที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูลก่อนขึ้นใช้งานระบบ

3.5 ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งฐานข้อมูลครั้งแรก หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ดังกล่าว

3.6 ต้องกำหนดรหัสผ่านในการเข้าถึงระบบฐานข้อมูลให้มีความมั่นคงปลอดภัยดังต่อไปนี้เป็นอย่างน้อย (โดยให้เป็นไปตามนโยบายที่ธนาคารกำหนด)
- ต้องมีความยาวอย่างน้อย 8 ตัวอักษร และต้องประกอบด้วย ตัวหนังสือ ตัวเลข ตัวอักษรพิมพ์ใหญ่ และตัวอักษรสัญลักษณ์ แต่ละชนิด อย่างน้อย 1 ตัวอักษร

3.7 กำหนดค่าติดตั้งระบบฐานข้อมูลเพื่อไม่อนุญาตให้ใช้งานรหัสผ่านที่มีค่าว่า (Null password)

3.8 ต้องอัพเดต Patch โปรแกรมระบบฐานข้อมูลให้เป็นเวอร์ชั่นล่าสุด ในกรณีที่จำเป็น และอธิบายถึงผลกระทบในการอัพเดต Patch ให้ธนาคารทราบเพื่อเป็นข้อมูลประกอบการตัดสินใจ Patch

3.9 รหัสผ่านที่เก็บในฐานข้อมูล ต้องมีการเข้ารหัสของรหัสผ่านเสมอ

3.10 ไม่ใช้วิธีการระบุบัญชีผู้ใช้ระบบงาน และรหัสผ่านของระบบฐานข้อมูลใน Configuration ไฟล์ โดยไม่ผ่านการเข้ารหัสรักษาความปลอดภัย

3.11 ต้องนำเสนอการสำรองข้อมูลของระบบฐานข้อมูล (Backup Database) เพื่อหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย โดยสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้

4. ด้าน Web Application

4.1 ระบบสามารถทำงานบน Browser ดังนี้ ได้เป็นอย่างน้อย

4.1.1 แสดงผลผ่านเว็บบราวเซอร์บน Smart Phone และ Tablet ได้ดังนี้

- Google Chrome
- Safari

4.1.2 แสดงผลผ่านเว็บบราวเซอร์บนเครื่องคอมพิวเตอร์ (Desktop) ได้ดังนี้

- Google Chrome
- Microsoft Edge
- Safari สำหรับ Mac OS

4.2 รูปแบบธีมของระบบงานจะต้องสอดคล้องกับมาตรฐาน/รูปแบบที่ธนาคารกำหนด

จันทร์ลอย