ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการสิทธิการใช้งาน** Supply Chain Finance Platform

2. หน่วยงานเจ้าของโครงการ **ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ**

3. วงเงินงบประมาณที่ได้รับจัดสรร 1,800,000.00 **บาท (หนึ่งล้านแปดแสนบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ..7 สิงหาคม 2566...

   เป็นเงิน 1,000,000.00 **บาท (หนึ่งล้านบาทถ้วน)**

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท เจเนอรัล อิเลคทรอนิค คอมเมอร์ซ เซอร์วิสเซส จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายมานิต	พรประสิทธิ์	ผู้ช่วยผู้บริหารฝ่ายบริหารและพัฒนาเทคโนโลยีสารสนเทศ / ฝ่ายพส.
6.2 นายนินาท	มรุตัณฑ์	ผู้ช่วยผู้บริหารส่วนพัฒนากระบวนการด้านเทคโนโลยีสารสนเทศ / ฝ่ายพส.
6.3 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการสิทธิการใช้งาน Supply Chain Finance Platform

---

ผู้ยื่นข้อเสนอต้องเสนอรายละเอียดการให้บริการสิทธิการใช้งาน EXIM SCF ตามขอบเขตงานที่ธนาคารกำหนด โดยมีรายละเอียดดังต่อไปนี้

1. ข้อกำหนดความต้องการทั่วไป

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องเสนอการให้บริการสิทธิการใช้งาน EXIM SCF เป็นระยะเวลา 12 เดือน (ตั้งแต่วันที่ 1 กันยายน 2566 ถึงวันที่ 31 สิงหาคม 2567) ตามขอบเขตงานที่กำหนดดังต่อไปนี้

1.1 ระบบ EXIM SCF ที่นำเสนอต้องมีคุณสมบัติตามรายละเอียดและคุณลักษณะเฉพาะด้านความต้องการ (Functional Requirement) ตามข้อ 3. และรายละเอียดคุณลักษณะเฉพาะด้านเทคนิค (Technical Requirement) ตามข้อ 4.

1.2 ระบบ EXIM SCF ที่นำเสนอ ต้องสามารถทำงานร่วมกับระบบสารสนเทศ และระบบเครือข่ายของธนาคารในปัจจุบันได้

1.3 กรณีระบบ EXIM SCF ที่เสนอมีความจำเป็นต้องใช้งานร่วมกับโปรแกรมอื่น ๆ ผู้ยื่นข้อเสนอต้องจัดให้มีโปรแกรมต่าง ๆ ที่เกี่ยวข้อง พร้อมทั้งสิทธิการใช้งาน (Software License) และจำนวนสิทธิทั้งหมดที่ถูกต้องตามกฎหมาย (ถ้ามี) ให้ครบถ้วน รวมทั้งบริการ (Support) ตลอดระยะเวลาที่สัญญาสิทธิการใช้งานระบบมีผลบังคับ

2. การให้บริการสนับสนุนระหว่างการใช้บริการ (Support)

ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องให้บริการ**สนับสนุนระหว่างการใช้บริการ (Support)** ตลอดระยะเวลาการใช้บริการ เป็นระยะเวลา 12 เดือน (ตั้งแต่วันที่ 1 กันยายน 2566 ถึงวันที่ 31 สิงหาคม 2567) โดยมีรายละเอียดดังนี้

2.1 ต้องจัดให้มีเจ้าหน้าที่ประสานงานที่มีความรู้ความเชี่ยวชาญพร้อมเบอร์โทรศัพท์ที่สามารถติดต่อได้สะดวก เพื่อรับแจ้งเหตุขัดข้อง ให้คำปรึกษา ตอบข้อซักถาม ให้ความช่วยเหลือหรือแก้ไขปัญหาเบื้องต้น (On Phone Support) รวมถึงช่องทางอื่นที่ธนาคารสามารถติดต่อขอรับคำปรึกษาได้ ในแบบ 10 x 5 (วันจันทร์ถึงวันศุกร์ ตั้งแต่เวลา 8.30 - 18.30 น.)

2.2 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องดำเนินการแก้ไขปัญหาเบื้องต้นให้แล้วเสร็จภายในกำหนด<u>ระยะเวลาทำการ</u>นับจากที่ได้รับแจ้งผ่านทาง e-mail ตามระดับผลกระทบที่มีต่อธุรกิจ หรือ การทำงาน (Severity) ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาการแก้ไขปัญหาเบื้องต้นนับจากที่ได้รับแจ้ง (Workaround)
Critical : ระบบมีปัญหาในส่วนที่เป็นหน้าที่หลัก หรือมีผลกระทบต่อลูกค้าสูง เช่น การ Login เข้าใช้งานระบบ การยื่นคำขอใช้ทำธุรกรรม เป็นต้น	5 ชม.
Urgent : ระบบมีปัญหาในส่วนที่ไม่ใช่หน้าที่หลัก เช่น การลงทะเบียนลูกค้า การแก้ไขเปลี่ยนแปลงข้อมูลลูกค้า เป็นต้น	24 ชม.
Error : ระบบมีปัญหาในส่วนที่ไม่ใช่หน้าที่หลัก และไม่มีผลกระทบต่อธุรกิจ แต่ยังสามารถใช้งานได้ เช่น รายงาน และ Inquiry เป็นต้น	48 ชม.

ทั้งนี้ กรณีเกิดข้อผิดพลาดจากระบบอื่นที่มีการเชื่อมโยงกันจะไม่รวมอยู่ตามตารางที่ระบุข้างต้น โดยระยะเวลาการแก้ไขจะขึ้นอยู่กับทางธนาคารและผู้เสนอราคาจะพิจารณากำหนดร่วมกัน และให้ถือความเห็นของธนาคารเป็นที่สุด

2.3 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องดำเนินการแก้ไขปัญหาให้เสร็จสิ้นแบบถาวร (Permanent Fix) ภายในกำหนดระยะเวลา 20 วัน นับจากที่ได้รับแจ้งผ่านทาง e-mail

2.4 ต้องจัดทำรายละเอียดและขั้นตอนการแก้ไขปัญหาเหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบ EXIM SCF อย่างละเอียดให้แก่ธนาคารในทันทีที่สามารถดำเนินการได้ (ไม่รวมปัญหาเหตุขัดข้องที่เกิดจาก Infrastructure ของธนาคาร) และผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกตกลงเป็นผู้รับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

2.5 ผู้ยื่นข้อเสนอต้องดำเนินการการให้บริการสนับสนุนระหว่างการใช้บริการ (Support) ตามที่ธนาคารร้องขอ โดยไม่มีการจำกัดจำนวนครั้งในการให้บริการ และหรือระยะเวลาในการให้บริการ

2.6 กรณีธนาคารตรวจพบช่องโหว่ของระบบงาน EXIM SCF ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกให้เป็นคู่สัญญาต้องดำเนินแก้ไขปิดช่องโหว่โดยไม่มีค่าใช้จ่ายเพิ่มเติม โดยมีระยะเวลาในการดำเนินการ ดังนี้

2.6.1 ช่องโหว่ที่มีความรุนแรงระดับสูง (High/Critical) ภายใน 15 วัน นับจากที่ได้รับแจ้ง

2.6.2 ช่องโหว่ที่มีความรุนแรงระดับปานกลาง (Medium) ภายใน 30 วัน นับจากที่ได้รับแจ้ง

2.6.3 ช่องโหว่ที่มีความรุนแรงระดับต่ำ (Low) ภายใน 45 วัน นับจากที่ได้รับแจ้ง

ทั้งนี้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปิดช่องโหว่ดังกล่าวอย่างละเอียดให้แก่ธนาคารในทันทีที่สามารถดำเนินการได้โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

3. รายละเอียดและคุณลักษณะเฉพาะด้านความต้องการ (Functional Requirement)

3.1 <u>ภาพรวมของระบบงาน</u>

เป็นบริการที่ให้ความสะดวกแก่ลูกค้าของธนาคารในห่วงโซ่ทางการผลิต (Supply Chain) ในการขอใช้บริการสินเชื่อ โดยระบบ EXIM SCF จะให้บริการ การ Upload Invoice โดย Sponsor เพื่อให้คู่ค้าทำ

ธุรกรรมขอสินเชื่อ การยื่นขอทำธุรกรรมเพื่อขอสินเชื่อ การสืบค้นรายการที่ทำธุรกรรม และรายงานการทำธุรกรรม ในส่วนของการให้บริการสินเชื่อฝั่งผู้ขาย (Supplier Financing) ผ่านทางออนไลน์

3.2 ขอบเขตความต้องการระบบ

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการตามเงื่อนไขและขอบเขตความต้องการของระบบ EXIM SCF ดังต่อไปนี้

3.2.1 ส่วนที่ 1 ขอบเขตความต้องการหลักของระบบ

3.2.1.1 ระบบต้องรองรับการจัดการค่าเริ่มต้นของระบบได้

3.2.1.1.1 สามารถสร้าง แก้ไข หรือลบ Bank Holiday ในระบบได้

3.2.1.1.2 สามารถกำหนด User/Password Policy ตามที่ธนาคารกำหนดได้

3.2.1.1.3 สามารถกำหนดเวลาในการทำงานของ Batch Job ต่าง ๆ ได้

3.2.1.1.4 ระบบต้องมีการเก็บประวัติการทำธุรกรรมและกิจกรรมอื่น ๆ ในระบบ

3.2.1.2 ระบบต้องรองรับการจัดการ User ในระบบได้

3.2.1.2.1 รองรับการสร้าง/การลบ/การแก้ไขสิทธิ์ User ทั้งฝั่งลูกค้า และเจ้าหน้าที่ธนาคาร (กรณี User เป็นเจ้าหน้าที่ธนาคารต้องมีการใช้ผ่านระบบ User/Password ของธนาคาร)

3.2.1.2.2 รองรับการสร้างบทบาท (Role) ของ User และกำหนดสิทธิ์ในการทำธุรกรรม สิทธิ์ในการเรียกดูรายการหรือรายงาน และสิทธิ์ในการใช้งานอื่น ๆ ได้

3.2.1.2.3 รองรับการกำหนดสถานะของ User ในระบบได้ (Active/Inactive)

3.2.1.2.4 ระบบต้องมี Authorization ในขั้นตอนที่ลูกค้าอนุมัติการทำธุรกรรม

3.2.1.2.5 ระบบต้องแสดงรายชื่อ User ทั้งหมดของระบบและสิทธิ์การใช้งานได้

3.2.1.3 ระบบต้องมีการแจ้งเตือนการทำธุรกรรมของลูกค้าผ่านทาง E-Mail เป็นอย่างน้อย

3.2.1.4 ระบบต้องมีการเก็บประวัติการทำธุรกรรมของลูกค้า เพื่อใช้ในการติดตามแก้ไขปัญหาที่อาจจะเกิดขึ้นได้

3.2.1.5 ระบบสามารถบันทึกข้อมูลและแสดงผลได้ทั้งภาษาไทยและภาษาอังกฤษ

3.2.2 ส่วนที่ 2 ขอบเขตความต้องการของระบบฝั่งผู้ขาย (Supplier Financing)

3.2.2.1 ระบบรองรับการนำเข้าเอกสาร AP Document เข้าระบบ อย่างน้อย 1 ช่องทาง คือ

3.2.2.1.1 Web Browser

3.2.2.2 ระบบต้องรองรับไฟล์ข้อมูลบนเอกสาร AP Document ได้อย่างน้อย 2 ประเภท คือ

3.2.2.2.1 Delimited format เช่น csv

3.2.2.2.2 Fixed Length format เช่น txt

3.2.2.3 ระบบต้องรองรับการนำเข้าข้อมูลจากลูกค้าที่มี Layout Fields ที่แตกต่างกันเข้าระบบได้

3.2.2.4 ระบบต้องรองรับการแสดงผลของข้อมูลที่นำเข้าตามความต้องการของลูกค้าที่แตกต่างกันได้

3.2.2.5 ระบบต้องมีการตรวจสอบการนำเข้าข้อมูลเบื้องต้นได้ เช่น Field ที่เป็น Mandatory ต้องมีข้อมูล Field ที่กำหนดเป็นตัวเลข ต้องมีข้อมูลเป็นตัวเลข เป็นต้น

3.2.2.6 ระบบต้องรายงานผลการนำเข้าได้ว่าสำเร็จหรือไม่สำเร็จกี่รายการ จำนวนเท่าไหร่ และแจ้งเหตุผลในรายการที่ไม่สำเร็จ

3.2.2.7 ระบบต้องรองรับการเพิ่ม แก้ไขชนิดของเอกสาร Upload เช่น Invoice, Credit Note, Debit Note เป็นต้น

3.2.2.8 ระบบต้องรองรับเงื่อนไขการแสดงผลของลูกค้าได้หลากหลายประเภท เช่น สามารถกำหนดได้ว่าต้องการให้ระบบแสดงข้อมูล Invoice ที่ Over Due หรือไม่ก็ได้ ตามความต้องการของธนาคารและลูกค้า

3.2.2.9 ระบบต้องรองรับการทำธุรกรรมของลูกค้าที่แตกต่างกันได้ เช่น

3.2.2.9.1 ลูกค้าสามารถขอเบิกกู้แบบเต็มจำนวนตาม Invoice

3.2.2.9.2 ลูกค้าสามารถขอเบิกกู้แบบบางส่วนจากจำนวนเต็มของ Invoice นั้น

3.2.2.9.3 ลูกค้าสามารถทำรายการโดยเลือกจากหลาย ๆ Invoice ต่อการขอเบิกกู้ 1 ครั้ง

3.2.2.9.4 ลูกค้าสามารถกำหนดวันที่ขอเบิกกู้โดยเลือกจากระบบได้ว่าจะขอเบิกกู้วันที่ทำรายการทันที หรือตั้งเวลาล่วงหน้า ตามความต้องการของลูกค้า

3.2.2.9.5 ลูกค้าสามารถตรวจสอบประวัติการทำธุรกรรมย้อนหลังได้

3.2.2.9.6 ลูกค้าสามารถเลือกได้ว่าต้องการรับ E-Mail แจ้งเตือนการทำธุรกรรมหรือไม่

3.2.2.9.7 ระบบต้องรองรับการกำหนด/เปลี่ยนแปลงระยะเวลาที่ลูกค้าสามารถขอทำธุรกรรม หากเกินระยะเวลาของบริการที่ธนาคารกำหนด (Cut off time) ระบบจะต้องแจ้งเตือนลูกค้าทราบ และไม่สามารถทำรายการต่อไปได้

3.2.2.10 ระบบต้องรองรับการจัดการ Profile ของลูกค้าในระบบได้

3.2.2.10.1 สามารถสร้าง แก้ไข หรือลบ Profile ของลูกค้าได้

3.2.2.10.2 สามารถสร้าง แก้ไข หรือลบ Bank Account ของลูกค้าได้

3.2.2.10.3 สามารถสร้าง แก้ไข หรือลบ Trading Partner ระหว่างลูกค้าได้

3.2.2.10.4 สามารถกำหนด Level of Authorize ได้ว่า ในการทำธุรกรรมจะต้องมี Checker มาตรวจสอบข้อมูลก่อนหรือไม่

3.2.2.11 ระบบสามารถเรียกดูข้อมูล (Inquiry) และรายงาน (Report) สำหรับลูกค้าและเจ้าหน้าที่ธนาคารตามที่ธนาคารกำหนด

3.2.2.12 ระบบสามารถจัดทำสัญญา/เอกสารทางการเงิน/คำขอ ตามรูปแบบที่ธนาคารกำหนดได้ผ่านระบบ และสามารถเรียกดูเอกสารตัวอย่างได้ก่อนการอนุมัติรายการ

3.2.2.13 ระบบต้องสามารถแนบเอกสารประกอบการเบิกกู้ผ่านการ Upload file ได้ (Attach file)

3.2.2.14 ระบบต้องสามารถ Accept รายการ หรือ Reject รายการธุรกรรมที่ทางธนาคารไม่ปล่อยกู้ พร้อมทั้งแจ้งเหตุผลให้กับทางลูกค้าทราบ

3.2.2.15 มีการตรวจสอบวงเงินที่เหลือตามที่ธนาคารกำหนดในระบบได้

3.2.2.16 ระบบต้องมีรายงานประจำวัน แสดง Due date ของ Sponsor รายงานประจำวันแสดงรายการขอกู้ โดยแยกตาม Supplier และ Invoice

3.2.2.17 ระบบต้องสามารถแสดงรายการทั้งหมดที่เจ้าหน้าที่ธนาคารต้องดำเนินการเบิกกู้ โดยรายการแสดงแยกเป็น 2 ส่วน คือ รายการที่ต้องดำเนินการในวันนั้น และรายการที่ต้องดำเนินการในวันถัดไป

4. รายละเอียดและคุณลักษณะเฉพาะด้านเทคนิค (Technical Requirement)

4.1 ด้าน System Architecture

4.1.1 ระบบงานต้องทำงานแบบ 3-tier Architecture

4.1.2 ระบบงานที่ให้บริการสิทธิ์ต้องเป็นลักษณะ Web-Base Application

4.1.3 ระบบสามารถทำงานบนระบบปฏิบัติการ (Operating System) Windows Server 2019, Linux RHEL (Version ไม่ต่ำกว่า 7.2) ได้อย่างใดอย่างหนึ่ง

4.1.4 ระบบสามารถทำงานบนฐานข้อมูลเชิงสัมพันธ์ (Relational Database) ต้องรองรับ Microsoft SQL Server 2016, MySQL (Version ไม่ต่ำกว่า 5.7) ได้อย่างใดอย่างหนึ่ง

4.1.5 ระบบมีการแบ่งแยกการเข้าใช้งานระบบสำหรับลูกค้า และ สำหรับพนักงาน

4.1.6 ต้องสนับสนุนการใช้สิทธิ์เข้าใช้ระบบด้วย AD ของธนาคาร

4.1.7 ต้องสนับสนุนการทำงานสิ้นวันด้วยระบบแบตช์ (End of day Batch Job's process) รวมถึงการออกรายงานประจำวันด้วยระบบงานแบตช์ภายในหรือภายนอก

4.1.8 ต้องทำการทดสอบ Performance Test (Load Test) จาก Testing Tool โดยการทดสอบต้องมีผู้ใช้ระบบงานพร้อมกัน (Concurrent Users) จำนวน 30 Users หลังจากผ่านการทดสอบระบบก่อนการใช้งานจริงโดยมีเงื่อนไขตามตารางดังต่อไปนี้

ฟังก์ชั่น	เกณฑ์ที่ต้องผ่าน
Display Report and screen	< 10 second
Analysis & Calculation Process	< 30 second
Inquiry Data	< 10 second
Add/Update/Delete Data	< 10 second

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

4.1.9.1 ข้อมูลเหตุการณ์การใช้งานสารสนเทศ (Audit logging)

4.1.9.2 ข้อมูลการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)

4.1.9.3 ข้อมูลเหตุการณ์การประมวลผลของระบบ (Application Log)

4.1.10 ผู้รับจ้างต้องดำเนินการติดตั้งแอพพลิเคชั่น และข้อมูลทั้งหมดของโครงการให้มาอยู่ภายใต้ Server ที่ธนาคารกำหนด

4.2 <u>ด้านมาตรฐานการรักษาความปลอดภัยของระบบ (System & Web Application) อย่างน้อยดังนี้</u>

4.2.1 เว็บไซต์ของระบบต้องมีความปลอดภัยในการทำธุรกรรม โดยใช้ Protocol ที่เข้ารหัสลับในการรับส่งข้อมูลระหว่างผู้ใช้บริการกับ Web Server เช่น HTTPs

4.2.2 รูปแบบการสื่อสารต้องใช้ Protocol (SSL 3.0/TLS 1.2) เป็นอย่างน้อย

4.2.3 มีการใช้ ใบรับรองแบบ EV SSL certificate

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

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

4.2.6 ต้องมีการ SCAN ระบบ โดยต้องครอบคลุมและปิดความเสี่ยงของ OWASP TOP 10 ในปีล่าสุด

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

4.2.8 มีมาตรฐานในการเพิ่มความมั่งคงปลอดภัยให้กับรหัสผ่าน ของ Application

4.2.8.1 ต้องมีความยาวอย่างน้อย 8 ตัวอักษร และต้องประกอบด้วย ตัวหนังสือ ตัวเลข ตัวอักษรพิมพ์ใหญ่ และตัวอักษรสัญลักษณ์ อย่างน้อย 1 ตัวอักษร

4.2.8.2 การระงับการใช้งาน Application เมื่อใส่รหัสผ่านผิด

4.2.9 จัดหมวดหมู่ของสารบบ (Directory) ที่ใช้เก็บไฟล์ข้อมูล เว็บเพจ ระบบปฏิบัติการ โปรแกรมสำหรับให้บริการเว็บ และโปรแกรมอื่นๆ โดยจะต้องมีการกำหนดสิทธิในการเข้าถึงสารบบที่เกี่ยวข้องทั้งหมด

4.2.10 ต้องไม่ให้มีการใช้ค่าเริ่มต้นของรหัสผ่าน ที่มากับการตั้งโปรแกรมครั้งแรก

4.2.11 ปิด Services ต่าง ๆ ที่ไม่จำเป็นบนเครื่องที่ให้บริการระบบ

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

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

4.2.14 มีการควบคุมไม่ให้มีการเก็บข้อมูลที่สำคัญของลูกค้าไว้ใน Session และมีการสร้าง Session Key ใหม่เมื่อมีการเข้าสู่ระบบ

4.2.15 มีการตรวจสอบลำดับของขั้นตอนการทำธุรกรรมอย่างเหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถข้ามขั้นตอนใดขั้นตอนหนึ่งได้ หากพบว่ามีการกระทำดังกล่าว จะต้องมีกระบวนการในการยับยั้งการทำธุรกรรม เช่น ทำให้ Session หมดอายุ หรือ Logout ผู้ใช้บริการออกจากระบบ

4.2.16 มีการกำหนด Time-Out ของ Session

4.2.17 หน้าเวบไซต์ (Browser) ควรออกแบบให้สามารถป้องกันการ key เดาสุ่มข้อมูลสำคัญ เช่น User ID/Password การสืบค้นข้อมูลบัญชีของลูกค้า เป็นต้น

4.2.18 ผู้รับจ้างต้องดำเนินการแก้ไขและปรับปรุงระบบตามข้อเสนอแนะของผู้ให้บริการทางด้านการทดสอบเจาะระบบ (Penetration Testing) ที่ธนาคารมอบหมายให้ดำเนินการทดสอบเจาะระบบ โดยการปิดช่องโหว่ที่อาจส่งผลกระทบต่อระดับความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

4.2.19 ระบบงานสามารถควบคุมไม่ให้ Username เดียวกันเข้าใช้งานระบบพร้อมกัน (Concurrent Session)

4.2.20 ระบบสามารถบังคับให้ผู้ใช้ระบบงานเปลี่ยนรหัสผ่านเมื่อเข้าใช้งานครั้งแรก หรือเมื่อได้รับรหัสผ่านใหม่

4.2.21 ระบบสามารถระงับการใช้งานของบัญชีผู้ใช้ระบบงานเป็นการชั่วคราว เมื่อมีการใส่ข้อมูลการพิสูจน์ตัวตนผิดเกิน 5 ครั้ง และปลดระงับให้ผู้ใช้ระบบงานสามารถ log in ได้อีกครั้งหลังจาก 5 นาที (สามารถเปลี่ยนแปลงได้ในอนาคตตามนโยบายที่ธนาคารกำหนด) นับจากการใส่ข้อมูลการพิสูจน์ตัวตนผิดครั้งสุดท้าย

4.2.22 ระบบสามารถเข้ารหัสข้อมูลด้วยมาตรฐานการเข้ารหัสที่มีความมั่นคงปลอดภัย โดยใช้วิธีการเข้ารหัสแบบ 256 bit หรือสูงกว่า โดยใช้ใบรับรองความปลอดภัยตามที่ธนาคารกำหนด และธนาคารสามารถเปลี่ยนใบรับรองความปลอดภัยได้ในอนาคต

4.3 <u>การควบคุมมาตรฐานความปลอดภัยของระบบฐานข้อมูล (Database) อย่างน้อยดังนี้</u>

4.3.1 ไม่ใช้สิทธิในการเข้าถึงจาก Active Directory ให้สร้างบัญชีผู้ใช้ระบบงานภายในฐานข้อมูล และกำหนดสิทธิการใช้งาน และควบคุมการเข้าถึงให้เหมาะสมกับหน้าที่ของผู้ใช้ระบบงาน

4.3.2 ไม่ใช้บัญชีที่มีสิทธิสูงสุดของฐานข้อมูลในการเข้าถึงฐานข้อมูลโดย Application

4.3.3 ต้องกำหนดสิทธิของ Application ในการเข้าถึง ฐานข้อมูล ให้เหมาะสม เช่น มีสิทธิ ในการ Insert, Update, Delete ข้อมูล ใน Table เท่านั้น

4.3.4 ตรวจสอบและทบทวนบัญชีผู้ใช้ภายในฐานข้อมูล และลบบัญชีที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูลก่อนขึ้นใช้งานระบบ

4.3.5 ปิดบัญชีผู้ที่มาพร้อมกับการติดตั้งฐานข้อมูลครั้งแรก หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ดังกล่าว

4.3.6 ต้องกำหนดรหัสผ่านในการเข้าถึงระบบฐานข้อมูลให้มีความมั่นคงปลอดภัยดังต่อไปนี้เป็นอย่างน้อย (โดยให้เป็นไปตามนโยบายที่ธนาคารกำหนด)

4.3.6.1 ต้องมีความยาวอย่างน้อย 8 ตัวอักษร และต้องประกอบด้วย ตัวหนังสือ, ตัวเลข, ตัวอักษรพิมพ์ใหญ่ และตัวอักษรสัญลักษณ์ แต่ละชนิด อย่างน้อย 1 ตัวอักษร

4.3.7 กำหนดค่าติดตั้งระบบฐานข้อมูลเพื่อไม่อนุญาตให้ใช้งานรหัสฝ่ายที่มีค่าว่า (Null password)

4.3.8 ต้องอัพเดต Patch โปรแกรมระบบฐานข้อมูลให้เป็นเวอร์ชั่นล่าสุด ในกรณีที่จำเป็น และอธิบายถึงผลกระทบในการอัพเดต Patch ให้ธนาคารทราบเพื่อเป็นข้อมูลประกอบการตัดสินใจ Patch

4.3.9 รหัสผ่านที่เก็บในฐานข้อมูล ต้องมีการเข้ารหัสของรหัสผ่านเสมอ

4.3.10 ไม่ใช้วิธีการระบุบัญชีผู้ใช้ระบบงาน และรหัสผ่านของระบบฐานข้อมูลใน Configuration ไฟล์ โดยไม่ผ่านการเข้ารหัสรักษาความปลอดภัย

4.4 <u>ด้าน Web Application</u>

4.4.1 ระบบสามารถทำงานบน Browser ดังนี้ ได้เป็นอย่างน้อย

4.4.1.1 Chrome Version 58.0 หรือสูงกว่า

4.4.2 ระบบงานสามารถแสดงผลได้ทั้งภาษาไทยและภาษาอังกฤษ

4.4.3 ระบบสามารถเชื่อมต่อกับระบบของธนาคาร ได้ดังนี้

4.4.3.1 ระบบ Mail Server

4.4.3.2 ระบบจัดเก็บ Username และ Password ของธนาคาร โดยธนาคารเป็นผู้จัดเตรียมช่องทางการเชื่อมต่อ

4.4.3.3 ระบบอื่นๆ (ถ้ามี)

4.4.4 ระบบสามารถแสดงผลเว็บไซต์แบบ Responsive เพื่อแสดงบน Device ต่างๆ ได้ เช่น PC, Notebook, Mobile, Tablet ฯลฯ เพื่อให้แสดงผลได้อย่างถูกต้องสวยงาม

4.4.5 รูปแบบธีมของระบบงานจะต้องสอดคล้องกับมาตฐาน/รูปแบบที่ธนาคารกำหนด

4.4.6 ระบบ EXIM SCF ต้องมี Database เพื่อเก็บข้อมูลที่เกี่ยวข้องกับระบบ EXIM SCF