ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการสิทธิการใช้งานและบริการ e-Mail and Corporation Tool (M365)**

2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ

3. วงเงินงบประมาณที่ได้รับจัดสรร **52,000,000.- บาท (ห้าสิบสองล้านบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 12 ธ.ค. 2567

   เป็นเงิน **48,058,240.00 บาท (สี่สิบแปดล้านห้าหมื่นแปดพันสองร้อยสี่สิบบาทถ้วน)**

   ราคา/หน่วย.....

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   สืบราคาจากตัวแทนจำหน่าย จำนวน 5 ราย

   (1) บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน)

   (2) บริษัท เอ็นทีที (ประเทศไทย) จำกัด

   (3) บริษัท เมโทรซิสเต็มส์ คอร์ปอเรชั่น จำกัด (มหาชน)

   (4) บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

   (5) บริษัท ฟูจิตสึ (ประเทศไทย) จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายประสิทธิ์	แซ่เบ๊	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
6.2 นายเดชา	ปริญญาสุข	ผู้ช่วยผู้บริหารฝ่ายธุรการ
6.3 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่าย ปส.

ผนวก 1

รายละเอียดข้อกำหนดสินค้าและบริการด้านเทคนิคและขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการสิทธิการใช้งานและบริการ e-Mail and Corporation Tool (M365)

ผู้ยื่นข้อเสนอต้องให้บริการสิทธิการใช้งานและบริการ e-Mail and Corporation Tool (M365) โดยมีขอบเขตการดำเนินงาน ดังต่อไปนี้

1. บริการด้านเทคนิค(Technical Requirements)

ระบบ Microsoft 365 Enterprise Plan E3 ต้องมีคุณลักษณะเฉพาะและคุณสมบัติทางด้านเทคนิค อย่างน้อยดังต่อไปนี้

1.1 ต้องเสนอสิทธิ์การใช้งานซอฟต์แวร์ลิขสิทธิ์ Microsoft 365 ME3 หรือดีกว่า ที่ถูกต้องตามกฎหมาย

1.2 สามารถติดตั้งและใช้งานโปรแกรม Office 365 บนเครื่องคอมพิวเตอร์ PC หรือ Mac หรือเครื่อง แท็บเล็ต หรือสมาร์ทโฟน จำนวนรวมไม่น้อยกว่า 5 เครื่อง ต่อ 1 ลิขสิทธิ์

1.3 สามารถป้องกันความปลอดภัย (Security) เช่น Windows Defender ATP อย่างน้อยดังต่อไปนี้

1.3.1 Microsoft Threat Protection ต้องสามารถเชื่อมต่อทำงานร่วมกันกับ Azure Advanced Threat Protection, Microsoft Intune และแบบ end-to-end เพื่อช่วยในด้านความปลอดภัยจากการโจมตีแบบ attack surface, securing identities, endpoints.

1.3.2 สามารถทำ Attack surface reduction โดยที่ผู้ดูแลระบบทางด้าน Security สามารถกำหนดค่าอุปกรณ์ด้วย advanced web protection และ สามารถกำหนด ว่าจะ allow หรือ deny รายการ ของ URLs และ IP address ที่ระบุเฉพาะเจาะจงได้ รวมถึงสามารถควบคุม ปกป้อง ransomware, credential misuse การโจมตีที่ถูกส่งมาผ่านทาง removable storage.

1.3.3 สามารถทำ antivirus โดยใช้รูปแบบ advanced machine learning และ AI models ในการป้องกันจากพวก Apex attackers โดยการใช้เทคนิคแบบ innovative vulnerability exploitและ malware.

1.3.4 สามารถทำ antivirus โดยใช้รูปแบบ advanced machine learning และ AI models ในการป้องกันจากพวก Apex attackers โดยการใช้เทคนิคแบบ innovative vulnerability exploitและ malware

1.4 สามารถทำ Password-less login เพื่อเพิ่มความปลอดภัยมากยิ่งขึ้น รองรับการทำ multi-factor authentication ด้วยการ authentication แบบ FIDO2, Web Authentication (WebAuth) และ Microsoft Authenticator ได้

1.5 สามารถปกป้องข้อมูลของ BitLocker ได้

1.6 สามารถปกป้องข้อมูลของ Azure Information Protection ได้

1.7 สามารถป้องกันการสูญหายของข้อมูลของ Office 365 ได้ (Office 365 DLP)

1.8 สามารถสร้าง, ปรับปรุง, ลบชื่อบัญชีผู้ใช้งาน (Username) บน Cloud Service สำหรับ Cloud identity ได้

1.9 สามารถใช้งานในระบบ Azure Active Directory อย่างไม่จำกัดจำนวน (Unlimited)

1.10 มีระบบบริหารจัดการเอกสารอิเล็กทรอนิกส์ โดยสามารถกำหนดสิทธิ์การเข้าถึงเอกสาร รวมทั้งสามารถเปิดไฟล์เอกสารอิเล็กทรอนิกส์ประเภท .docx, .xlsx, .pptx และ .pdf ได้เป็นอย่างน้อย

1.11 มีโปรแกรม Microsoft Office ซึ่งประกอบด้วย Word, PowerPoint, Excel, Outlook, OneNote, Publisher และ Access สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ได้

1.12 สามารถเข้าถึงแอปพลิเคชันและเอกสาร Office ได้จาก iPad และสมาร์ทโฟนทั่วไปได้ เช่น iOS, Android

1.13 มีพื้นที่เก็บเอกสารส่วนตัวแบบออนไลน์ ไม่น้อยกว่า 5 TB ต่อผู้ใช้หนึ่งราย (OneDrive for Business) และสามารถแชร์ไปยังบุคคลภายในและภายนอกองค์กรได้รวมถึงสามารถควบคุมการแชร์ข้อมูลได้ว่าจะสามารถ ดู ได้หรือแก้ไขได้ในแต่ละไฟล์ และเข้าใช้งานจากที่ไหนก็ได้ ได้ทุกๆอุปกรณ์

1.14 สามารถใช้งาน Office Online ผ่าน web edition เช่น Outlook, Word, Excel และ PowerPoint เพื่อสร้าง แก้ไข แชร์ และทำงานเอกสารร่วมกันได้

1.15 สามารถใช้งานร่วมกับระบบปฏิบัติการ Microsoft Windows 10, Windows Server 2016 เป็นอย่างน้อย รวมถึง เบราว์เซอร์ ดังต่อไปนี้ Microsoft Edge, Safari, Chrome และ Firefox เวอร์ชันปัจจุบัน

1.16 สามารถทำ Cloud identity, Federated identity หรือ Multi-factor authentication ได้

1.17 สามารถทำ Directory Sync tool ได้

1.18 สามารถให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) โดยมีพื้นที่จัดเก็บข้อมูลไม่น้อยกว่า 100 GB ต่อ 1 บัญชีผู้ใช้ รวมทั้งสามารถแนบเอกสาร attachments ได้ถึงขนาด 150 MB โดยสามารถใช้งานได้จากทั้ง desktop หรือ web browser โดยต้องสามารถจัดเก็บ Log file การใช้งานได้อย่างน้อย 90 วัน โดยมีรายละเอียดตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ตามจำนวนสิทธิการใช้งาน ทั้งนี้ ผู้ยื่นข้อเสนอต้องระบุหรือแสดงตัวอย่างวิธีการจัดเก็บ Log file ให้เพียงพอต่อการพิจารณาของธนาคาร

1.19 สามารถทำ archiving และ legal hold ด้วยพื้นที่ไม่น้อยกว่า 1.5 TB สำหรับเรื่องสนับสนุนนโยบายเรื่อง data loss prevention (DLP) สำหรับการทำ compliance บังคับใช้เพิ่มเติมใน email

1.20 สามารถกำหนด Custom Email Domain Address เป็นของตัวเองได้

1.21 สามารถทำการควบคุมการเข้าถึงเอกสาร และ email โดยสามารถระบุเป็นคนๆ ได้ และป้องกันการเข้าถึงข้อมูลจากบุคคลอื่นๆ จากการ viewing และ editing ถึงแม้ข้อมูลเหล่านี้จะถูกส่งออกไป จากองค์กร (Rights Management Services)

1.22 สามารถทำการเข้ารหัสข้อมูล (Message Encryption) ในการกำหนดนโยบาย เช่น Encrypt Only และ Do Not Forward และ การป้องกันการอ่าน messages ใน Outlook ได้

1.23 สามารถแสดงรายงานในรูปแบบต่างๆ ได้ เช่น

- รายงาน Active และ inactive mailboxes หรือ New, deleted mailboxes/groups
- รายงาน Mailbox usage, Sent received mail และ Top senders and recipients
- รายงาน Spam, Malware detections
- รายงาน Top DLP policy matches for mail หรือ DLP policy matches by severity for mail

1.24 รองรับ Protocol ทั้งแบบ IPv4 และ IPv6

1.25 รองรับมาตรฐานกลางด้าน Compliance ดังต่อไปนี้ EU Model, Clauses, SAS 70 / SSAE16 Assessments ISO 27001 certified, HIPAA-Business Associate Agreement, PCI-governed PAN data เป็นต้น

1.26 สามารถทำการ Online Meetings แบบ audio, HD video, และ web conferencing ผ่านทางInternet ซึ่งสามารถเข้าร่วมการเข้าประชุมจากเครื่อง smartphone, tablet หรือ PC ได้ และสามารถกำหนดผู้เข้าร่วมประชุมได้

1.27 สามารถทำการ Broadcast meetings บน Internet ไปยัง 10,000 คนได้ โดยสามารถเข้าร่วมด้วย browser ได้

1.28 สามารถทำการ Instant messaging ติดต่อสื่อสารกันผ่านข้อมูลตัวอักษร, voice calls, และ video calls รวมทั้งสามารถแสดงสถานะว่า ว่าง Online อยู่หรือไม่

1.29 สามารถสนับสนุนการทำงานเป็นทีม ติดต่อเชื่อมต่อกันภายในทีมงาน ไม่ว่าจะเป็น Chat, Content, คน และเครื่องมือ ทำงานร่วมกัน ในการเข้าถึงแหล่งข้อมูลต่างๆ ได้ทันที ตามที่ต้องการ

1.30 สามารถทำ Intranet และ team sites ภายในองค์กรได้ เพื่อการ แชร์แหล่งข้อมูลต่าง ๆ

1.31 สามารถทำ Information protection ได้ เช่น Rights management, data loss prevention, และ การเข้ารหัส encryption สำหรับ Exchange Online และ SharePoint Online เพื่อช่วยปกป้องข้อมูล Content ให้ปลอดภัยในรูปแบบ email

1.32 สามารถรองรับคุณสมบัติ Azure Active Directory Plan 1, Windows Hello, Credential Guard และ Direct access ได้

1.33 ระบบ Office 365 ต้องมีชุดคุณสมบัติ Feature ในการเชื่อมต่อกันภายในองค์กร ไม่ว่าจะเป็นในการสร้าง จัดเก็บ และบริหารจัดการ unifying digital content ด้วยเครื่องมือที่มีมาให้ และแชร์ข้อมูลระหว่างผู้ใช้งานร่วมกันได้อย่างน้อยดังต่อไปนี้

- Microsoft Flow
- Microsoft Forms
- Microsoft Graph API
- Microsoft PowerApps
- Microsoft Planner
- Microsoft Stream
- Microsoft Sway
- Microsoft Teams
- Delve
- Office 365 Groups

1.34 ต้องเป็นการรวมชุดของระบบต่างๆ เข้าด้วยกันดังต่อไปนี้

1.34.1 Azure Active Directory Premium P1

1.34.2 Intune

1.34.3 Azure Information Protection P1

1.35 ระบบต้องสามารถมีคุณสมบัติเบื้องต้น ในการจัดการเรื่องต่างๆ ดังต่อไปนี้

1.35.1 Identity management

1.35.2 Device management

1.35.3 Information protection

1.36 สามารถทำ Single sign-on (SSO) กับ หลายๆ Applications รวมถึง SaaS application ได้

1.37 สามารถทำ Multi-factor authentication ได้ โดยมีทางเลือกเงื่อนไขในการ Verification เพิ่มขึ้นไม่ว่าจะเป็น phone calls, text messages, หรือการแจ้งเตือนผ่าน mobile app และ ใช้ในการตรวจสอบความปลอดภัย เพื่อระบุตัวตนที่ไม่สอดคล้องกัน

1.38 สามารถทำ Conditional access โดยกำหนดนโยบายที่ให้การควบคุม ที่ระดับผู้ใช้, สถานที่,อุปกรณ์และระดับชั้นของแอพ เพื่อที่จะ allow , Block หรือ ร้องถามการเข้าถึงของผู้ใช้

1.39 สามารถให้ผู้ใช้แต่ละคนสามารถเข้าถึงฟังก์ชั่นเซิร์ฟเวอร์จากหลายๆ อุปกรณ์ได้

1.40 สามารถทำ Mobile device management ในการลงทะเบียนอุปกรณ์ขององค์กรและส่วนบุคคลเพื่อตั้งค่าบังคับใช้การปฏิบัติตามข้อกำหนดและปกป้องข้อมูลขององค์กร

1.41 สามารถทำ Mobile application management โดย publish, กำหนดค่าและอัปเดตแอพมือถือ บนอุปกรณ์ที่ลงทะเบียนและไม่ได้ลงทะเบียนและรักษาความปลอดภัยหรือลบข้อมูลองค์กรที่เกี่ยวข้องกับแอพนั้นได้

1.42 สามารถทำ Advanced Microsoft Office 365 data protection โดยการจัดการและการรักษาความปลอดภัยให้กับผู้ใช้ อุปกรณ์, แอพและข้อมูล

1.43 สามารถเชื่อมต่อการทำงานร่วมกันกับระบบ PC management โดยเป็นการบริหารจัดการแบบศูนย์กลางของพีซีแล็ปท็อปและอุปกรณ์มือถือจากคอนโซลเดียวในการดูแลระบบและจัดทำรายงานการกำหนดค่าฮาร์ดแวร์และซอฟต์แวร์โดยละเอียด

1.44 สามารถทำ Information protection โดยมีความสามารถดังต่อไปนี้

1.44.1 ทำ Persistent data protection โดยการเข้ารหัสข้อมูลที่ละเอียดอ่อนและกำหนดสิทธิ์การ ใช้งานเพื่อการป้องกันแบบถาวรโดยไม่คำนึงว่าจะจัดเก็บหรือแบ่งปันข้อมูลไว้ที่ใด

1.44.2 ทำ data classification และ labeling โดยกำหนดค่านโยบายเพื่อจัดประเภทและติดป้ายกำกับ (label)

1.44.3 ทำ Document tracking และ revocation โดยตรวจสอบกิจกรรมเกี่ยวกับข้อมูลที่ใช้ร่วมกันและยกเลิกการเข้าถึงในกรณีที่เกิดเหตุการณ์ที่ไม่คาดคิด

1.45 สามารถเชื่อมต่อและทำงานร่วมกับ Office 365 ที่มีอยู่ได้

1.46 สามารถใช้ระบบ Microsoft Intune ที่มาพร้อมกับ Microsoft 365 E3 ได้

1.47 สามารถรองรับ Platform ต่างๆ โดยที่ Intune ให้การจัดการอุปกรณ์มือถือและแอพพลิเคชั่นบนแพลตฟอร์มดังนี้เป็นอย่างน้อย Windows , Mac OS , iOS และ Android

1.48 สามารถทำการลงทะเบียนอุปกรณ์ (Device enrollment) ได้ทั้งแบบราย User และแบบจำนวนมาก (Bulk Registration) โดยสามารถส่ง E-mail เพื่อแจ้งให้ผู้ใช้งานติดตั้ง application และทำการลงทะเบียนด้วยตนเองได้

1.49 สามารถใช้ระบบ Mobile Device Management สามารถเปิดใช้งานการลงทะเบียนอุปกรณ์ด้วยตนเอง (Self-service enrollment) ผ่านการส่งข้อมูลทาง Email เพื่อให้ผู้ใช้งานสามารถกด Link URL หรือ Download application เพื่อให้สามารถลงทะเบียนด้วยตนเองได้

1.50 สามารถใช้ระบบ Mobile Device Management สามารถรองรับการ Enrollment/Register จากอุปกรณ์ลูกข่ายที่เป็นระบบปฏิบัติการ ได้เป็นอย่างน้อย

1.50.1 Apple ตั้งแต่ iOS, iPadOS version 14.0 ขึ้นไป และ MacOS Version 11.0 ขึ้นไป

1.50.2 Google Android ตั้งแต่ Android 8.0 ขึ้นไป

1.50.3 Windows 10, Windows 8.1RT และเวอร์ชั่นที่ใหม่กว่า

1.51 สามารถกำหนดระดับของสิทธิ์ในการเข้าใช้งานระบบของผู้ดูแลได้หลากหลาย (Role Base Access Control)

1.52 สามารถใช้ระบบ Mobile Device Management ได้ และมีต้องมีความสามารถต่าง ๆ ดังต่อไปนี้

1.52.1 สามารถสั่งบังคับให้เปลี่ยนค่าความปลอดภัยของเครื่อง Mobile device ให้สอดคล้องตามนโยบายที่กำหนดจากส่วนกลางได้ (Security configuration parameter enforcement) ผ่านการเชื่อมต่อทาง Internet

1.52.2 สามารถสร้างนโยบายความปลอดภัย (Security policy configuration) ได้

1.52.3 สามารถแสดงรายการ hardware inventory ของเครื่องทั้งหมดที่ Enroll เข้ามาในระบบ Mobile Device Management ได้

1.52.4 สามารถ refresh/update security configuration policy จากบนเครื่องอุปกรณ์ Mobile device ได้

1.52.5 สามารถแสดงรายการเครื่อง Mobile device ที่ Lost communication ได้

1.52.6 สามารถแสดงรายการอุปกรณ์ที่ไม่ได้ปฏิบัติตามนโยบายความปลอดภัย (non-compliance report) โดยให้ข้อมูลถึงนโยบายความปลอดภัยที่ไม่ปฏิบัติตามของแต่ละเครื่องได้

1.52.7 สามารถบังคับกำหนดนโยบาย Password/passcode และการเวลา Lock screen ของอุปกรณ์ลูกข่ายได้ ซึ่ง Password/passcode policy

1.52.8 สามารถใช้ระบบจัดกลุ่ม และแบ่งแยกนโยบายความปลอดภัย (Configuration Profile) ตามกลุ่มของพนักงาน หรือชนิดของอุปกรณ์ได้

1.52.9 ต้องมี web portal สามารถตรวจสอบตำแหน่งของเครื่อง (location tracking) สั่งลบข้อมูล (wipe) และ Lock เครื่องจากระยะไกลได้

1.52.10 สามารถมีวิธีการป้องกันการเข้าถึงข้อมูลในเครื่อง เมื่อมีการพยายามใส่ Password ผิดเข้า locked screen เกินกว่าที่กำหนดไว้ (incorrect password over threshold)

1.52.11 รองรับการทำรายงาน (Report) ในการแสดงข้อมูลเกี่ยวกับ software และ hardware ได้

1.53 สามารถจัดการเรื่องความปลอดภัยได้ดังต่อไปนี้

1.53.1 ระบบสามารถบังคับกำหนดนโยบาย Passcode และ Lock screen ของอุปกรณ์มือถือได้ ซึ่ง Passcode policy จะเป็นไปตามนโยบายของ ธปท. เช่น Passcode length, Passcode Content, Maximum number of failed Attempts เป็นต้น

1.53.2 ระบบสามารถแสดงรายการอุปกรณ์ที่ไม่ได้ปฏิบัติตามนโยบายความปลอดภัย (non-compliance report) เช่น Rooted เครื่องที่มี Application blacklist เป็นต้น

1.53.3 สามารถสั่งลบข้อมูลบนเครื่องจากระยะไกล (Remote wipe) ได้

1.53.4 สามารถสร้างเงื่อนไขเพื่อทำการตรวจสอบอุปกรณ์ว่าเป็นไปตามคุณลักษณะที่ตรงตามข้อกำหนดหรือไม่ (Compliance) และตั้งค่าให้ตอบสนองต่อผลของเงื่อนไขที่ได้กำหนดไว้ (Action) เช่น Device ที่ Rooted สามารถที่จะทำ Retire ได้ทันที

2. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องดำเนินการงานให้บริการสิทธิการใช้งานและบริการ e-Mail and Corporation Tool (M365) ต้องมีขอบเขตการดำเนินงานดังต่อไปนี้

2.1 ผู้ยื่นข้อเสนอต้องเสนอสิทธิ์การใช้งานซอฟต์แวร์ลิขสิทธิ์ Microsoft 365 E3 หรือดีกว่า ที่ถูกต้องตามกฎหมาย และนำเสนอแผนการดำเนินการ (Action Plan) ที่เกี่ยวข้องทั้งหมด เพื่อทำการย้าย Microsoft 365 E3 จาก CSP agreement มาเป็น New EA agreement เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง รวมถึงการดำเนินตามแผนงาน โดยมีระยะเวลาให้บริการ 3 ปี

2.2 ผู้ยื่นข้อเสนอต้องนำเสนอการให้บริการอย่างน้อยดังนี้

2.2.1 E-mail

2.2.2 Drive (Personal, Team)

2.2.3 Calendar

2.2.4 Group email

2.2.5 Office 365

2.2.6 SharePoint and Data Sharing Policy

2.2.7 Azure Active Directory สำหรับ M365

2.2.8 Microsoft 365 Enterprise Plan E3 License ไม่น้อยกว่า 1100 accounts

2.2.9 Power Apps Premium (Unlimited apps) ไม่น้อยกว่า 1 account

2.2.10 Power Automate Premium ไม่น้อยกว่า 1 account

2.2.11 Power BI Premium ไม่น้อยกว่า 50 accounts

3. ขอบเขตการให้บริการ Unified Support 1 ปีแรก

Unified Enterprise Support Thailand		
Quantity	Service	Service Type
Included	Enterprise Advisory Support Hours As-needed	Advisory Services
Included	Enterprise Azure Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise On-demand Assessment	On-Demand Assessment
Included	Enterprise On-Demand Assessment - Setup and Config Service As-needed	On-Demand Assessment Remote
Included	Enterprise On-Demand Education	On-Demand Education
Included	Enterprise Online Support Portal	Administrative
Included	Enterprise Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise Reactive Support Management	Service Delivery Management
Included	Enterprise Service Delivery Management	Service Delivery Management
Included	Enterprise Webcasts As-Needed	Webcast
Included	Reactive Enabled Contacts	Problem Resolution Support