ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการ Migration และสิทธิการใช้งานโปรแกรม Microsoft 365 Enterprise E3**

2. หน่วยงานเจ้าของโครงการ **ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ**

3. วงเงินงบประมาณที่ได้รับจัดสรร **1,000,000.00 บาท (หนึ่งล้านบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 6 กันยายน 2566

   เป็นเงิน 978,750.- บาท (เก้าแสนเจ็ดหมื่นแปดพันเจ็ดร้อยห้าสิบบาทถ้วน) ราคา / หน่วย

   4.1 Microsoft 365 E3 พร้อม Migration จำนวน 145 Licence @ 6,750.- = 978,750.- บาท

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   5.1 บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน)

   5.2 บริษัท เก้าพันวา จำกัด

   5.3 บริษัท เอ็ม 365 (ประเทศไทย) จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

   6.1 นายมานิต พรประสิทธิ์ ผู้ช่วยผู้บริหารฝ่ายบริหารและพัฒนาเทคโนโลยีสารสนเทศ

   6.2 นางวันเพ็ญ เพชรคอน **ผู้จัดการส่วน / ฝ่าย ปส.**

   6.3 นายกฤษณพันธ์ วันเสน เจ้าหน้าที่ดูแลระบบส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย / ฝ่าย ปส.

ผนวก 1

รายละเอียดข้อกำหนดสินค้าและบริการด้านเทคนิคและขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการ Migration และสิทธิการใช้งานโปรแกรม Microsoft 365 Enterprise E3

ผู้ยื่นข้อเสนอต้องเสนองานการจ้างผู้ให้บริการ Migration และสิทธิการใช้งานโปรแกรม Microsoft 365 Enterprise E3 โดยมีขอบเขตการดำเนินงาน ดังต่อไปนี้

บริการด้านเทคนิค(Technical Requirements)

ระบบ Microsoft 365 Enterprise Plan E3 ต้องมีคุณลักษณะเฉพาะและคุณสมบัติทางด้านเทคนิค อย่างน้อยดังต่อไปนี้

1. ต้องเสนอสิทธิ์การใช้งานซอฟต์แวร์ลิขสิทธิ์ Microsoft 365 E3 หรือดีกว่า ที่ถูกต้องตามกฎหมาย
2. สามารถติดตั้งและใช้งานโปรแกรม Office 365 บนเครื่องคอมพิวเตอร์ PC หรือ Mac หรือเครื่องแท็บเล็ต หรือสมาร์ทโฟน จำนวนรวมไม่น้อยกว่า 5 เครื่อง ต่อ 1 ลิขสิทธิ์
3. มีระบบปฏิบัติการ Windows 10 Enterprise ที่ต้องรองรับความสามารถในการปกป้องทางด้านความปลอดภัย (Security) เช่น Windows Defender ATP อย่างน้อยดังต่อไปนี้
    3.1 Microsoft Threat Protection ต้องสามารถเชื่อมต่อทำงานร่วมกันกับ Azure Advanced Threat Protection, Azure Information Protection, Microsoft Intune และแบบ end-to-end เพื่อช่วยในด้านความปลอดภัยจากการโจมตีแบบ attack surface, securing identities, endpoints.
    3.2 สามารถทำ Attack surface reduction โดยที่ผู้ดูแลระบบทางด้าน Security สามารถกำหนดค่าอุปกรณ์ ด้วย advanced web protection และ สามารถกำหนด ว่าจะ allow หรือ deny รายการ ของ URLs และ IP address ที่ระบุเฉพาะเจาะจงได้ รวมถึงสามารถควบคุม ปกป้อง ransomware, credential misuse การโจมตีที่ถูกส่งมาผ่านทาง removable storage.
    3.3 สามารถทำ antivirus โดยใช้รูปแบบ advanced machine learning และ AI models ในการป้องกันจากพวก Apex attackers โดยการใช้เทคนิคแบบ innovative vulnerability exploit และ malware.
4. มีระบบปฏิบัติการ Windows 10 Enterprise รองรับการทำ Password-less login เพื่อเพิ่มความปลอดภัยมากยิ่งขึ้น รองรับการทำ multi-factor authentication โดยไม่จำเป็นต้องใช้ passwords สำหรับ Windows 10 โดยใช้ Windows Hello ด้วยการ authentication แบบ FIDO2, Web Authentication (WebAuth) และ Microsoft Authenticator ได้
5. สามารถปกป้องข้อมูลของ BitLocker ได้
6. สามารถปกป้องข้อมูลของ Azure Information Protection ได้
7. สามารถป้องกันการสูญหายของข้อมูลของ Office 365 ได้ (Office 365 DLP)
8. สามารถสร้าง, ปรับปรุง, ลบชื่อบัญชีผู้ใช้งาน (Username) บน Cloud Service สำหรับ cloud identity ได้
9. สามารถใช้งานในระบบ Azure Active Directory อย่างไม่จำกัดจำนวน (Unlimited)

10. มีระบบบริหารจัดการเอกสารอิเล็กทรอนิกส์ โดยสามารถกำหนดสิทธิ์การเข้าถึงเอกสาร รวมทั้งสามารถเปิดไฟล์เอกสารอิเล็กทรอนิกส์ประเภท .docx, .xlsx, .pptx และ .pdf ได้เป็นอย่างน้อย
11. มีโปรแกรม Microsoft Office ซึ่งประกอบด้วย Word, PowerPoint, Excel, Outlook, OneNote, Publisher และ Access สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ได้
12. สามารถเข้าถึงแอปพลิเคชันและเอกสาร Office ได้จาก iPad และสมาร์ทโฟนทั่วไปได้ เช่น iOS, Android
13. มีพื้นที่เก็บเอกสารส่วนตัวแบบออนไลน์ ไม่น้อยกว่า 5 TB ต่อผู้ใช้หนึ่งราย (OneDrive for Business) และสามารถแชร์ไปยังบุคคลภายในและภายนอกองค์กรได้รวมถึงสามารถควบคุมการแชร์ข้อมูลได้ว่าจะสามารถ ดูได้หรือแก้ไขได้ในแต่ละไฟล์ และเข้าใช้งานจากที่ไหนก็ได้ ได้ทุกๆอุปกรณ์
14. สามารถใช้งาน Office Online ผ่าน web edition เช่น Outlook, Word, Excel และ PowerPoint เพื่อสร้าง แก้ไข แชร์ และทำงานเอกสารร่วมกันได้
15. สามารถใช้งานร่วมกับระบบปฏิบัติการ Microsoft Windows 10, Windows Server 2016 เป็นอย่างน้อย รวมถึง เบราว์เซอร์ ดังต่อไปนี้ Microsoft Edge, Safari, Chrome และ Firefox เวอร์ชันปัจจุบัน
16. สามารถทำ Cloud identity, Federated identity หรือ Multi-factor authentication ได้
17. สามารถทำ Directory Sync tool ได้
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
19. สามารถทำ archiving และ legal hold ด้วยพื้นที่ไม่น้อยกว่า 1.5 TB สำหรับเรื่องสนับสนุนนโยบายเรื่อง data loss prevention (DLP) สำหรับการทำ compliance บังคับใช้เพิ่มเติมใน email
20. สามารถกำหนด Custom Email Domain Address เป็นของตัวเองได้
21. สามารถทำการควบคุมการเข้าถึงเอกสาร และ email โดยสามารถระบุเป็นคนๆ ได้ และป้องกันการเข้าถึงข้อมูลจากบุคคลอื่นๆ จากการ viewing และ editing ถึงแม้ข้อมูลเหล่านี้จะถูกส่งออกไปจากองค์กร (Rights Management Services)
22. สามารถทำการเข้ารหัสข้อมูล (Message Encryption) ในการกำหนดนโยบาย เช่น Encrypt Only และ Do Not Forward และ การป้องกันการอ่าน messages ใน Outlook ได้
23. สามารถแสดงรายงาน Active และ inactive mailboxes หรือ New, deleted mailboxes/groups ได้
24. สามารถแสดงรายงาน Mailbox usage, Sent received mail และ Top senders and recipients ได้
25. สามารถแสดงรายงาน Spam, Malware detections ได้
26. สามารถแสดงรายงาน Top DLP policy matches for mail หรือ DLP policy matches by severity for mail ได้

27. รองรับ Protocol ทั้งแบบ IPv4 และ IPv6
28. รองรับมาตรฐานกลางด้าน Compliance ดังต่อไปนี้ EU Model, Clauses, SAS 70 / SSAE16 Assessments ISO 27001 certified, HIPAA-Business Associate Agreement, PCI-governed PAN data เป็นต้น
29. สามารถทำการ Online Meetings แบบ audio, HD video, และ web conferencing ผ่านทาง Internet ซึ่งสามารถเข้าร่วมการเข้าประชุมจากเครื่อง smartphone, tablet หรือ PC ได้ และสามารถกำหนดผู้เข้าร่วมประชุมได้
30. สามารถทำการ Broadcast meetings บน Internet ไปยัง 10,000 คนได้ โดยสามารถเข้าร่วมด้วย browser ได้
31. สามารถทำการ Instant messaging ติดต่อสื่อสารกันผ่านข้อมูลตัวอักษร, voice calls, และ video calls รวมทั้งสามารถแสดงสถานะว่า ว่าง Online อยู่หรือไม่
32. สามารถสนับสนุนการทำงานเป็นทีม ติดต่อเชื่อมต่อกันภายในทีมงาน ไม่ว่าจะเป็น Chat, Content, คน และเครื่องมือ ทำงานร่วมกัน ในการเข้าถึงแหล่งข้อมูลต่างๆ ได้ทันที ตามที่ต้องการ
33. สามารถทำ Intranet และ team sites ภายในองค์กรได้ เพื่อการ แชร์แหล่งข้อมูลต่าง ๆ
34. สามารถทำ Information protection ได้ เช่น Rights management, data loss prevention, และการเข้ารหัส encryption สำหรับ Exchange Online และ SharePoint Online เพื่อช่วยปกป้องข้อมูล Content ให้ปลอดภัยในรูปแบบ email
35. สามารถรองรับคุณสมบัติ Azure Active Directory Plan 1, Windows Hello, Credential Guard และ Direct access ได้
36. 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
37. ต้องเป็นการรวมชุดของระบบต่างๆ ดังต่อไปนี้

    37.1 Azure Active Directory Premium P1

37.2 Intune

37.3 Azure Information Protection P1

เข้าด้วยกันในชุด โดยความสามารถของ Feature ให้มีสิทธ์การใช้งานตามแต่ละระบบที่มีอยู่ในชุดได้

38. ระบบต้องสามารถมีคุณสมบัติเบื้องต้น ในการจัดการเรื่องต่างๆ ดังต่อไปนี้

38.1 identity management

38.2 device management

38.3 information protection

39. สามารถทำ single sign-on (SSO) กับ หลายๆ applications รวมถึง SaaS application ได้

40. สามารถทำ Multi-factor authentication ได้ โดยมีทางเลือกเงื่อนไขในการ verification เพิ่มขึ้นไม่ว่าจะเป็น phone calls, text messages, หรือการแจ้งเตือนผ่าน mobile app และ ใช้ในการตรวจสอบความปลอดภัยเพื่อระบุตัวตนที่ไม่สอดคล้องกัน

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

42. สามารถให้ผู้ใช้แต่ละคนสามารถเข้าถึงฟังก์ชั่นเซิร์ฟเวอร์จากหลายๆ อุปกรณ์ได้

43. สามารถทำ Mobile device management ในการลงทะเบียนอุปกรณ์ขององค์กรและส่วนบุคคลเพื่อตั้งค่าบังคับใช้การปฏิบัติตามข้อกำหนดและปกป้องข้อมูลขององค์กร

44. สามารถทำ Mobile application management โดย publish, กำหนดค่าและอัปเดตแอพมือถือบนอุปกรณ์ที่ลงทะเบียนและไม่ได้ลงทะเบียนและรักษาความปลอดภัยหรือลบข้อมูลองค์กรที่เกี่ยวข้องกับแอพนั้นได้

45. สามารถทำ Advanced Microsoft Office 365 data protection โดยการจัดการและการรักษาความปลอดภัยให้กับผู้ใช้ อุปกรณ์, แอพและข้อมูล

46. สามารถเชื่อมต่อการทำงานร่วมกันกับระบบ PC management โดยเป็นการบริหารจัดการแบบศูนย์กลางของพีซีแล็ปท็อปและอุปกรณ์มือถือจากคอนโซลเดียวในการดูแลระบบและจัดทำรายงานการกำหนดค่าฮาร์ดแวร์และซอฟต์แวร์โดยละเอียด

47. สามารถทำ Information protection โดยมีความสามารถดังต่อไปนี้

47.1 ทำ Persistent data protection โดยการเข้ารหัสข้อมูลที่ละเอียดอ่อนและกำหนดสิทธิ์การใช้งานเพื่อการป้องกันแบบถาวรโดยไม่คำนึงว่าจะจัดเก็บหรือแบ่งปันข้อมูลไว้ที่ใด

47.2 ทำ data classification และ labeling โดยกำหนดค่านโยบายเพื่อจัดประเภทและติดป้ายกำกับ (label)

47.3 ทำ Document tracking และ revocation โดยตรวจสอบกิจกรรมเกี่ยวกับข้อมูลที่ใช้ร่วมกันและยกเลิกการเข้าถึงในกรณีที่เกิดเหตุการณ์ที่ไม่คาดคิด

48. สามารถเชื่อมต่อและทำงานร่วมกับ Office 365 ที่มีอยู่ได้

49. สามารถใช้ระบบ Microsoft Intune ที่มาพร้อมกับ Microsoft 365 E3 ได้

50. สามารถรองรับ Platform ต่างๆ โดยที่ Intune ให้การจัดการอุปกรณ์มือถือและแอพพลิเคชั่นบนแพลตฟอร์ม Windows, Mac OS X, Windows Phone, iOS และ Android เมื่อ Intune เชื่อมต่อกับ System Center Configuration Manager ในการกำหนดค่าแบบไฮบริด รวมทั้งสามารถจัดการ Macs, Unix และ Linux server และเครื่อง Windows Server ได้

51. สามารถทำการลงทะเบียนอุปกรณ์ (Device enrollment) ได้ทั้งแบบราย User และแบบจำนวนมาก (Bulk Registration) โดยสามารถส่งเป็น SMS, QR Code และ ส่ง E-mail เพื่อแจ้งให้ผู้ใช้งานติดตั้ง application และทำการลงทะเบียนด้วยตนเองได้

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

53. สามารถใช้ระบบ Mobile Device Management สามารถรองรับการ Enrollment/Register จากอุปกรณ์ลูกข่ายที่เป็นระบบปฏิบัติการ ได้เป็นอย่างน้อย

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

    53.2 Google Android ตั้งแต่ Android 8.0 ขึ้นไป

    53.3 Windows 10, Windows 8.1RT และเวอร์ชั่นที่ใหม่กว่า

54. สามารถกำหนดระดับของสิทธิ์ในการเข้าใช้งานระบบของผู้ดูแลได้หลากหลาย (Role Base Access Control)

55. สามารถใช้ระบบ Mobile Device Management ได้ และมีต้องมีความสามารถต่าง ๆ ดังต่อไปนี้

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

    55.2 สามารถสร้างนโยบายความปลอดภัย (Security policy configuration) ได้

    55.3 สามารถแสดงรายการ hardware inventory ของเครื่องทั้งหมดที่ Enroll เข้ามาในระบบ Mobile Device Management ได้

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

    55.5 สามารถแสดงรายการเครื่อง Mobile device ที่ Lost communication ได้

    55.6 สามารถแสดงรายการอุปกรณ์ที่ไม่ได้ปฏิบัติตามนโยบายความปลอดภัย (non-compliance report) โดยให้ข้อมูลถึงนโยบายความปลอดภัยที่ไม่ปฏิบัติตามของแต่ละเครื่องได้

    55.7 สามารถบังคับกาหนดนโยบาย Password/passcode และการเวลา Lock screen ของอุปกรณ์ลูกข่ายได้ ซึ่ง Password/passcode policy

    55.8 สามารถใช้ระบบจัดกลุ่ม และแบ่งแยกนโยบายความปลอดภัย (Configuration Profile) ตามกลุ่มของพนักงาน หรือชนิดของอุปกรณ์ได้

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

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

55.11 รองรับการทำรายงาน (Report) ในการแสดงข้อมูลเกี่ยวกับ software และ hardware ได้

56. สามารถจัดการเรื่องความปลอดภัยได้ดังต่อไปนี้

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

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

56.3 สามารถสั่งลบข้อมูลบนเครื่องจากระยะไกล (Remote wipe) ได้

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

ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องดำเนินการงานการจ้างผู้ให้บริการ Migration และสิทธิการใช้งานโปรแกรม Microsoft 365 Enterprise E3 ต้องมีขอบเขตการดำเนินงานดังต่อไปนี้

1. ผู้ยื่นข้อเสนอต้องนำเสนอแผนการดำเนินการ (Action Plan) ที่เกี่ยวข้องทั้งหมด เพื่อทำการ Migration จากระบบ Google mail ไปเป็น Microsoft 365 Enterprise E3 และประกาศใช้งานจริง (Implementation) รวมถึงการดำเนิน Migration ตามแผนงาน โดยมีระยะเวลาดำเนินการภายใน 90 วัน นับถัดจากวันที่ลงนามสัญญา
2. ผู้ยื่นข้อเสนอต้องนำเสนอแผนการจัดเตรียมระบบพร้อมทั้งสร้างและตั้งค่าบัญชีผู้ใช้งานตามจำนวนในสัญญา และทำการ Migration พร้อมทั้งแผนการตรวจสอบและเปรียบเทียบความถูกต้องของข้อมูล
    - 2.1 E-mail
    - 2.2 Drive (Personal, Team)
    - 2.3 Calendar
    - 2.4 Group email
    - 2.5 Forwarding email setting
    - 2.6 Office 365
    - 2.7 Intune MDM/MAM
    - 2.8 E-mail DLP(DLP Rule และอนุญาตให้ใช้เฉพาะเครื่องขององค์กรหรือผ่าน Intune)
    - 2.9 SharePoint and Data Sharing Policy
    - 2.10 Azure Active Directory สำหรับ O365 และระบบงานอื่น ๆ ตามมาตรฐานความปลอดภัยของธนาคาร
3. ผู้ยื่นข้อเสนอต้องนำเสนอแผนการฝึกอบรม พร้อมเอกสารตัวอย่างเนื้อหาฉบับใช้งานจริง
    - 3.1 แผนอบรม User ทั่วไป ไม่น้อยกว่า 3 รอบ
    - 3.2 แผนอบรม User Admin ไม่น้อยกว่า 1 รอบ (เนื้อหาไม่น้อยกว่า M365 Management, Patch Management, Intune, DLP(Email), SharePoint, Azure Active Directory)
4. ผู้ยื่นข้อเสนอต้องมีศูนย์รับแจ้งปัญหา (Contact Center หรือ Help Desk) ที่ให้บริการภาษาไทยตลอด 24 ชั่วโมง 7 วัน ผ่านช่องทางโทรศัพท์และ/หรือช่องทางอื่นที่ติดต่อได้
5. ผู้ยื่นข้อเสนอต้องจัดทำรายงานการให้บริการของ ระบบ Microsoft 365 Enterprise Plan E3 โดยมีเกณฑ์ SLA ของผลิตภัณฑ์ไม่ต่ำกว่าร้อยละ 99.5
6. จำนวน License ทั้งหมด 145 accounts ที่จัดซื้อ และต้องจัดให้มี Trial License 955 account โดยระยะเวลาการใช้งานไม่น้อยกว่า 3 เดือนนับจากวันที่ลงนามในสัญญา และต้อง Migrate accounts มากกว่า 850 accounts

การให้บริการสนับสนุนตลอดระยะเวลาการใช้บริการ (Support)

1. ต้องจัดให้มีเจ้าหน้าที่ประสานงานที่มีความรู้ความชำนาญเกี่ยวกับการใช้งานบริการ Microsoft 365 Enterprise Plan E3 ในประเทศไทยพร้อมหมายเลขโทรศัพท์และช่องทางอื่นที่สามารถรับแจ้งเหตุขัดข้องและให้คำปรึกษาและแก้ไขปัญหาต่าง ๆ ในเบื้องต้น (On Phone Support) ทุกวันตลอด 24 ชั่วโมง
2. กรณีที่ไม่สามารถแก้ไขปัญหา หรือให้คำปรึกษากับทางธนาคารได้ตามข้อ 1. ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องติดต่อกลับธนาคารภายใน 2 ชั่วโมง นับจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร
3. ในกรณีที่การใช้บริการ Microsoft 365 Enterprise Plan E3 เกิดเหตุขัดข้องหรือความชำรุดบกพร่องผู้ให้บริการจะต้องดำเนินการแก้ไขเหตุขัดข้องหรือความชำรุดบกพร่องให้แล้วเสร็จและสามารถใช้งานได้เป็นปกติ ภายใน 4 ชั่วโมง นับจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร