รายละเอียดคุณลักษณะเฉพาะร่างขอบเขตงาน (TOR)
การจัดหาสิขสิทธิ์โปรแกรมสำหรับสถานศึกษาแบบรายปี

* * * * * * * * * * * * * * *

1. โปรแกรมสำเร็จรูป Microsoft Volume License จำนวน 300 ลิขสิทธิ์ มีคุณสมบัติเฉพาะดังต่อไปนี้

1.1. มหาวิทยาลัยจะต้องมีสิทธิ์ใช้งานซอฟต์แวร์ไมโครซอฟท์ สำหรับบุคลากรและอาจารย์จำนวนไม่น้อยกว่า 300 สิทธิ์ โดยสามารถใช้งานบริการและซอฟต์แวร์ ดังนี้เป็นอย่างน้อย

1.1.1. รองรับการติดตั้ง Microsoft 365 Apps เพื่อใช้งานในรูปแบบ Offline บนอุปกรณ์คอมพิวเตอร์บนระบบปฏิบัติการ Windows หรือ Mac จำนวน 5 อุปกรณ์ต่อผู้ใช้งาน

1.1.2. รองรับการติดตั้ง Microsoft 365 Apps เพื่อใช้งานความสามารถพิเศษบนอุปกรณ์พกพาในรูปแบบ Smartphone จำนวน 5 อุปกรณ์ต่อผู้ใช้งาน และ Tablet จำนวน 5 อุปกรณ์ต่อผู้ใช้งาน

1.1.3. รองรับการใช้งาน Office for the web หรือ Office WebApp ในรูปแบบออนไลน์

1.1.4. รองรับระบบ Email ในรูปแบบ Exchange Plan 2 โดยมีพื้นที่เก็บจดหมายอิเล็กทรอนิกส์จำนวนไม่น้อยกว่า 100 GB ต่อผู้ใช้งาน

1.1.5. รองรับระบบจัดเก็บข้อมูล และเอกสารของมหาวิทยาลัยฯ บน SharePoint

1.1.6. รองรับการใช้งานโปรแกรมการสื่อสาร การทำงาน การเรียนและประชุมออนไลน์ผ่าน Microsoft Teams

1.1.7. รองรับระบบพื้นที่จัดเก็บข้อมูลส่วนบุคคล OneDrive for Business ขนาดเริ่มต้นที่ 1 TB และปรับเพิ่มได้ไม่น้อยกว่า 5 TB

1.1.8. รองรับโปรแกรมทางการศึกษาในการจัดการเนื้อหา (Content) อาทิเช่น Microsoft Forms, Microsoft Stream และ Microsoft Sway เป็นอย่างน้อย

1.1.9. รองรับการสร้างนวัตกรรม Power Platform อาทิเช่น Power Apps และ Power Automate เป็นอย่างน้อย

1.1.10. รองรับการใช้งานโปรแกรมทางธุรกิจ (Business Apps) อาทิเช่น Planner และ Booking เป็นอย่างน้อย

1.1.11. รองรับระบบวิเคราะห์ข้อมูลทางการเรียนการสอน Education Analytics

1.1.12. รองรับการติดตั้งและใช้งานซอฟต์แวร์สำหรับคอมพิวเตอร์ลูกข่ายภายใน ดังรายการต่อไปนี้เป็นอย่างน้อย

1) Windows 10 Education Upgrade หรือเวอร์ชั่นล่าสุด
2) Microsoft Office Professional Plus and Office for Mac หรือเวอร์ชั่นล่าสุด
3) Microsoft Core CAL Suite (CAL)

1.2. มหาวิทยาลัยฯ จะต้องมีสิทธิ์ใช้งาน Office 365 A3 for Student Use Benefit สำหรับนักศึกษาจำนวนไม่น้อยกว่า 12,000 สิทธิ์

1.3. มหาวิทยาลัยฯ จะต้องมีสิทธิ์ใช้งาน Visio Plan 2 for faculty สำหรับบุคลากรจำนวนไม่น้อยกว่า 10 สิทธิ์

1.4. มหาวิทยาลัยฯ จะต้องมีสิทธิ์ในการติดตั้งและใช้งานซอฟต์แวร์ที่ไมโครซอฟท์ยังให้บริการอยู่ได้ ดังรายการต่อไปนี้

1.4.1. Microsoft Windows Server Standard Edition Core License หรือรุ่นล่าสุด จำนวนไม่ต่ำกว่า 16 ชุด

1.5. มหาวิทยาลัยฯ มีสิทธิ์ทำการอัพเกรด (Upgrade Right) ซอฟต์แวร์รุ่นใหม่ได้ ในกรณีที่ไมโครซอฟท์ได้วางจำหน่ายซอฟต์แวร์รุ่นใหม่ และยังสามารถใช้ซอฟต์แวร์รุ่นก่อนหน้า (Down Grade Right) ที่ไมโครซอฟท์ยังให้บริการอยู่ได้

1.6. มหาวิทยาลัยฯ จะต้องได้รับสิทธิ์สมัครเป็นสมาชิกโปรแกรม Azure Dev Tools for Teaching สำหรับอาจารย์ และนักศึกษาในสาขาที่เกี่ยวกับการเรียนการสอนสาขาวิชาด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ และด้านคณิตศาสตร์ ในการใช้ซอฟต์แวร์ต่าง ๆ เพื่อการเรียนการสอนได้

1.7. มหาวิทยาลัยจะต้องมีสิทธิ์ใช้บริการ Office 365 A1 สำหรับสถานศึกษา ไม่จำกัดการใช้งานสำหรับบุคลากรและนักศึกษา

1.8. ผู้ชนะเสนอราคาจะต้องติดตั้งระบบบริหารจัดการรหัสผลิตภัณฑ์หรือ Key Management Service (KMS) ให้กับมหาวิทยาลัย โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

1.9. ผู้เสนอราคาต้องได้รับการแต่งตั้งและรับรองจากเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทย หรือผู้นำเข้าหลักที่ได้รับอนุญาตโดยตรง สำหรับโครงการนี้

1.10. ผู้เสนอราคาที่ได้รับการคัดเลือกต้องสนับสนุนการใช้งานและแก้ไขปัญหาทางเทคนิคของ Microsoft 365 ให้แก่มหาวิทยาลัย ซึ่งเป็นพนักงานประจำของผู้เสนอราคาเพื่อติดต่อประสานงานการให้บริการด้านเทคนิคแก่มหาวิทยาลัย

2. โปรแกรมป้องกันไวรัส จำนวน 50 ลิขสิทธิ์ มีคุณสมบัติเฉพาะดังต่อไปนี้

2.1 โปรแกรมบริหารจัดการกลาง สำหรับเครื่องลูกข่ายและเครื่องแม่ข่าย มีคุณสมบัติเฉพาะดังต่อไปนี้

2.1.1 โปรแกรมบริหารจัดการต้องรองรับการใช้งานกับ Database Microsoft SQL Server 2014 Express SP2 (64bit) หรือดีกว่า และรองรับการใช้งาน MySQL Standard Edition 5.7 32-bit/64-bit หรือดีกว่า

2.1.2 โปรแกรมบริหารจัดการกลางต้องรองรับการใช้งานกับ Windows server 2022, Windows server 2019, Windows server 2016, Windows server 2012, 2012 r2, Windows server 2016 (64bit) All edition , Windows server 2019(64bit) All edition

2.1.3 การบริหารจัดการต้องสามารถทำได้ทั้งรูปแบบของ On-Cloud และ On premise

2.1.4 สามารถกำหนดสิทธิ์ให้กับผู้ดูแลระบบในการใช้งานตัวบริหารจัดการที่แตกต่างกัน

2.1.5 มีโปรแกรมที่ใช้เข้าถึงตัวบริหารจัดการแบบ On premise โดยไม่จำเป็นต้องผ่านการใช้ Remote-Desktop เช่น Administration console , Web console

2.1.6 สามารถแสดงรายงานของไฟล์ที่ถูกสำรองข้อมูลไว้หากถูกลบไป (Backup) หรือ โดนกักกัน (Quarantine) ไว้ได้จากส่วนกลาง หรือ สามารถสั่งคืนค่าไฟล์ดังกล่าว และดาวน์โหลดไฟล์ดังกล่าวได้จากส่วนกลาง

2.1.7 สามารถทำการกู้คืนและสำรองฐานข้อมูลของเครื่องแม่ข่ายเพื่อป้องกันในกรณีระบบเกิดการเสียหาย (Backup copying and restoration)

2.1.8 โปรแกรมการบริหารจัดการกลางต้องสามารถกำหนดการเข้าได้ในรูปแบบการทำ (Two-step verification) ได้

2.1.9 โปรแกรมบริหารจัดการต้องสามารถควบคุมบริหารจัดการแอนตี้ไวรัสได้ดังต่อไปนี้ในโปรแกรมบริหารจัดการเดียว เช่น Virtual, Windows, Linux Mac OS, Mobile devices, Embedded Systems

2.1.10 สามารถทำการ Update โดยกำหนดให้เครื่องลูกอื่นๆ เป็นแหล่งของการเข้ามา Update ได้ (Distribution points)

2.1.11 สามารถทำการเก็บรายละเอียด (Inventory) ของ Software และ Hardware ทั้งเครื่องแม่ข่ายและเครื่องลูกข่ายได้

2.1.12 โปรแกรมบริหารจัดการสามารถออก Report ในรูปแบบ PDF, XML, HTML

2.1.13 สามารถกำหนด User name, Password เพื่อสามารถแก้ไขหรือ Uninstall โปรแกรมได้จากโปรแกรมบริหารจัดการกลางได้

2.1.14 มีฟีเจอร์การสั่งลบไฟล์ที่เครื่องลูกข่ายโดยสั่งผ่านตัวบริหารจัดการกลาง (Wipe data) โดยต้องสามารถระบุเป็น Folders, Predefined folders, File by extension

2.1.15 มีเทคโนโลยีตรวจสอบช่องโหว่ (Vulnerabilities) ของ Software ภายในเครื่องแม่ข่ายและเครื่องลูกข่าย

2.1.16 รองรับการทำงานร่วมกันกับ SIEM Systems ได้

2.1.17 สามารถกำหนดค่าเมื่อการเกิดการแพร่ระบายของไวรัสให้เครื่องลูกข่ายรับ Polices ตามที่ผู้ดูแลระบบกำหนดเพื่อลดปัญหาที่จะเกิดขึ้น (Virus Outbreak)

2.1.18 สามารถส่งข้อความไปที่เครื่องปลายตามที่กำหนดได้ (Send message to user)

2.1.19 สามารถสั่ง Turn On, Shut down, Restart เครื่องปลายทางได้จากตัวบริหาร

2.1.20 ต้องเป็น License ที่เป็นลิขสิทธิ์จากเจ้าของผลิตภัณฑ์ โดยมีเอกสารรับรองจากเจ้าของผลิตภัณฑ์สำหรับโครงการนี้

2.1.21 ผู้เสนอราคาต้องได้รับการแต่งตั้งและรับรองจากเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง สำหรับโครงการนี้

2.2 โปรแกรมป้องกันไวรัสเครื่องลูกข่าย (Endpoint Security) มีคุณสมบัติเฉพาะดังต่อไปนี้

2.2.1 สามารถติดตั้งและทำงานได้บนเครื่องที่มีระบบปฏิบัติการ Windows 11, Windows 10, 8.1, 8, 7sp1, Windows Server 2008 R2 SP1(64 Bit), 2012 R2 (64Bit), 2016(64Bit), 2019(64Bit) เป็นอย่างน้อย

2.2.2 สามารถกำหนด อนุญาต/ไม่อนุญาต/แจ้งเตือน การเข้าใช้งานเว็บไซต์ (Web control) ของผู้ใช้งานแต่ละคนได้

2.2.3 สามารถเลือกการใช้งานของโปรแกรม (Application Control) โดยเลือกเป็น Deny List, Allow list ของ Application ได้

2.2.4 สามารถป้องกันเครื่องโดนเข้ารหัสบน Share Folders, Map drive ได้และกำหนดเวลาในการเข้าใช้งาน Share Folders หลังจากทำการป้องกันแล้ว (Protection of share folders against external encryption)

2.2.5 มีฟังชั่น AMSI Protection Provider ที่ทำการตรวจจับ Script malware ที่มากับ MS office file, Archives, Distribution packages

2.2.6 สามารถอนุญาต/ไม่อนุญาต การใช้งานอุปกรณ์พกพาจำพวก Removable Drive, CD/DVD drives, Smart card readers, External network adapters, Portable devices, Cameras and

2.2.7 สามารถทำการเก็บข้อมูลการใช้งานไฟล์ เช่น ลบไฟล์ สร้างไฟล์ใหม่ บนอุปกรณ์ Removable Drive และออกรายงาน (Report) ได้

2.2.8 มีคุณสมบัติป้องกันดังนี้ Ransomware, Advance threats, Fileless threats, Software exploits

2.2.9 มีฟีเจอร์กันป้องกันการโจมตีทางระบบเน็ตเวิกค์ (Network-Attack) โดยจะต้องสามารถออกรายงานเกี่ยวกับการโจมตีทางระบบเน็ตเวิกค์และสามารถทำการ (Block) การถูกโจมตีได้โดยอัตโนมัติ

2.2.10 สแกนไฟล์ในรูปแบบ Archives files, Distribution packages และ Microsoft Office formats ได้

2.2.11 สามารถป้องกันแอนตี้ไวรัสในตัวเองได้ (Self – Defense) จากโปรแกรมที่เป็นอันตรายรวมถึงมัลแวร์ที่ พยายามบล็อกการทำงานหรือแม้กระทั่งลบออกจากคอมพิวเตอร์

2.2.12 สามารถทำการ Scan โดยไม่ไป Scan หรือตรวจสอบไฟล์เดิมซ้ำที่ใช้เทคโนโลยี iSwift และ iChecker เพื่อเก็บค่าการสแกนของไฟล์ต่างๆ เป็นการลดเวลาในการตรวจสอบไฟล์

2.2.13 สามารถทำงานแบบ Personal firewall

2.2.14 รวบรวมข้อมูลเกี่ยวกับกิจกรรมที่น่าสงสัยโดยมัลแวร์เพื่อคืนค่าในระบบปฏิบัติการ (Remediation Engine) หรือสามารถย้อนคืนค่าการทำงานใน Operation System กรณี Malware สร้างความเสียหายใน Operation System (Roll back action)

2.2.15 สามารถทำงานในรูปแบบของ (Host Intrusion Prevention) เพื่อกำหนดสิทธิ์ให้กับโปรแกรมต่างๆ ที่ติดตั้งอยู่เครื่องลูกข่ายตามฐานข้อมูลของภัยคุกคามได้ เพื่อป้องกันการเกิดความเสียหายจากโปรแกรมที่ไม่พึงประสงค์

2.2.16 สามารถสร้างภาพการทำงานของภัยคุกคามที่ตรวจสอบได้ โดยต้องสามารถแสดงการทำงานเริ่มต้นและสิ้นสุดของภัยคุกคามเพื่อบอกสาเหตุการโดนโจมตีได้

2.2.17 ในหน้าการแสดงผลข้อมูลของภัยคุกคามได้ดังนี้

1) Data on the file, including name and path, MD5/SHA256 hash, Appearance history
2) Registry changes, Autorun detects
3) History of the file presence on the device.
4) Response status (i.e. quarantined, disinfected)

2.2.18 มีความสามารถในการสร้างข้อกำหนดไม่ให้ไฟล์ที่ต้องสงสัยติดตั้งลงเครื่องลูกข่ายตามที่ผู้ดูแลระบบกำหนดได้ (Execution Prevention Rules)

2.2.19 สามารถแสดงรายละเอียดการใช้งานบริการคลาวด์ (Cloud Discovery) ต้องเป็น License ที่เป็นลิขสิทธิ์จากเจ้าของผลิตภัณฑ์ โดยมีเอกสารรับรองจากเจ้าของผลิตภัณฑ์สำหรับโครงการนี้

2.2.20 ผู้เสนอราคาต้องได้รับการแต่งตั้งและรับรองจากเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง สำหรับโครงการนี้