6. ระบบ Unified Endpoint Management (UEM) - VMware Workspace ONE Standard จำนวน 300 ลิขสิทธิ์

6.1 สามารถในการบริหารจัดการอุปกรณ์พกพา และ บริหารความปลอดภัยของอุปกรณ์พกพา รวมทั้งการจัดการอุปกรณ์พกพาขององค์กร (Corporate Own Device) และการนำอุปกรณ์ส่วนตัวมาใช้ที่ทำงาน (Bring Your Own Device) โดยสามารถที่จะให้ผู้ใช้เลือกประเภทของอุปกรณ์พกพา ตอนติดตั้งระบบ ได้ตามความเหมาะสม

6.2 ต้องเป็น Licenses แบบ Device จำนวน 300 Device

6.3 รองรับอุปกรณ์เครื่องลูกข่ายที่เป็นประเภท PC/Notebook และ Mobile Devices ที่ใช้ระบบปฏิบัติการ ดังต่อไปนี้

6.3.1 macOS เวอร์ชัน 10 ขึ้นไป

6.3.2 Windows 10 หรือสูงกว่า

6.3.3 Mobile device ที่เป็น Android ไม่ต่ำกว่าเวอร์ชัน 8.0 และ iOS ไม่ต่ำกว่าเวอร์ชัน 12.0

6.4 สามารถทำงานร่วมกับ Active Directory เพื่อใช้ User ในการลงทะเบียนอุปกรณ์เข้าสู่ระบบ และสามารถที่จะเรียกขอ User Certificate ที่มาจาก Active Directory Certificate Service ไปยังอุปกรณ์ที่ลงทะเบียน

6.5 แสดงค่า Dashboard ภาพรวมของ Device ในองค์กร เช่น Ownership , Security , Enrollment Status , Platform และ Device Last Seen

6.6 สามารถทำงานแบบ Smart Group โดยเลือกตามเงื่อนไขต่างๆ ได้ ทั้ง เช่น ประเภทของเครื่อง, รุ่น ,Model ของเครื่อง, เวอร์ชันของระบบปฏิบัติการ และผู้ใช้ที่เป็นเจ้าของเครื่อง

6.7 สามารถแก้ไข Device Friendly Name , Asset Number , Device Ownership และ Device Category บนหน้าจอ Web Console

6.8 สามารถกำหนดนโยบายการทำ Security Compliance Policies เมื่อมีการตรวจพบเหตุการณ์ที่ไม่ปลอดภัย เช่น เมื่อเจอ Rooted Device หรือเครื่อง Non-Compliant ระบบสามารถกำหนด Action ได้ เช่น Bock/Remove All Managed Apps , Enterprise Wipe Command , Block Remove All Profiles และ Block Email ไปยังอุปกรณ์ และสามารถทำ Escalation เป็นช่วงเวลาแบบ ชั่วโมง และ วัน

6.9 รองรับการทำงานแบบ Remote Control หรือ Remote Support ที่สามารถดึงหน้าจอผู้ใช้งาน เพื่อให้ผู้ดูแลช่วยแก้ปัญหา โดยจะต้องเป็น Software ที่ พัฒนาโดยเจ้าของผลิตภัณฑ์เดียวกันกับระบบที่นำเสนอ และการใช้งาน Remote Control ต้องใช้งานหรือมี Interface อยู่บน Console เดียวกัน เพื่อความปลอดภัย โดยรองรับทั้ง Windows 10 ขึ้นไป , macOS และ Android

6.10 มีระบบ Workflow Automation หรือ Orchestration ที่อยู่ในรูปแบบ GUI เพื่อกำหนดเงื่อนไข และจัดลำดับในการติดตั้ง Software , Profile และ Script โดยใช้วิธีการ Drag and Drop รองรับการทำงานบนระบบปฏิบัติการ Windows และ macOS

6.11 ผู้ใช้งานสามารถบริหารจัดการ อุปกรณ์ที่ลงทะเบียนผ่านทาง Self Service Portal เพื่อที่จะตรวจสอบข้อมูลของ Serial number ของเครื่อง , Profile ที่ติดตั้ง และ Compliance ที่เช็ค และสามารถที่จะส่ง Action ไปยังเครื่องปลายทางได้เช่น Enterprise Wipe, Device Query และ Delete Device อีกทั้งยังสามารถเข้าไปตรวจสอบ Term of use ย้อนหลังได้

6.12 ระบบสามารถส่งการแจ้งเตือนในรูปแบบข้อความ (Notification) จากส่วนกลางไปยังเครื่องคอมพิวเตอร์ และ Mobile Device ได้ในรูปแบบ Actionable และ Informational โดยผู้ดูแลสามารถปรับเปลี่ยนรูปแบบในการของข้อความ เช่น Icon , Title และ Description

6.13 สามารถบริหารจัดการอุปกรณ์ Mobile Device (iOS and Android)

6.14 สามารถบริหารจัดการอุปกรณ์ที่ติดตั้งระบบปฏิบัติการ Windows 10, Windows 11

6.14.1 สามารถบริหารจัดการระบบปฏิบัติการ Windows ในรูปแบบของ Profile Management ทั้งแบบ User Profile และ Device Profile

6.14.2 สามารถจัดการและติดตั้ง Wi-Fi Profile และ VPN Profile ของเครื่องระบบปฏิบัติการ Windows โดยอัตโนมัติ

6.14.3 สามารถตั้งค่า Windows Licensing , Firewall , Windows Update และ Application Control ของ Windows ในรูปแบบการจัดการแบบ Profile

6.14.4 สามารถตั้ง Restriction ของระบบปฏิบัติการ Windows ในรูปแบบ Allow หรือ Don't Allow เช่น Date/Time , Region and Language , Cortana ,Bluetooth และ USB เป็นต้น และอยู่ในรูปแบบการจัดการแบบ Profile

6.14.5 แสดงรายละเอียดของ Hardware และ Software ที่ติดตั้งลงบนเครื่อง Computer

6.14.6 สามารถจัดการ Windows Update เพื่อทำการตรวจสอบและส่ง Patch ไป Update ยังเครื่องคอมพิวเตอร์ในเครือข่ายได้ โดยสามารถทำงานร่วมกับ WSUS (Windows Server Update Services) ในองค์กร และ Microsoft Update

6.15 สามารถบริหารการจัดการอุปกรณ์ที่ติดตั้งระบบปฏิบัติการ macOS

6.15.1 สามารถบริหารจัดการระบบปฏิบัติการ macOS ในรูปแบบของ Profile Management ทั้งแบบ User Profile และ Device Profile

6.15.2 สามารถที่จะจัดการและติดตั้ง Wi-Fi Profile และ VPN Profile ของเครื่องคอมพิวเตอร์ macOS

6.15.3 สามารถบริหารจัดการ Full Disk Encryption ด้วย FileVault

6.15.4 สามารถบันทึกและแสดงข้อมูลรายละเอียดของอุปกรณ์คอมพิวเตอร์ รายละเอียดดังนี้ ชื่ออุปกรณ์คอมพิวเตอร์, ชื่อและรุ่น (Version) ซอฟต์แวร์ (Application Software) ที่ติดตั้งบนเครื่อง และผู้ใช้งานอุปกรณ์คอมพิวเตอร์ (User Logon) หรือ ผู้ลงทะเบียนอุปกรณ์

6.15.5 สามารถติดตั้ง Software ที่อยู่บน App store และ In house software หรือ Internal software ลงบนเครื่องได้

6.15.6 สามารถทำงานร่วมกับ Apple Business Manager

6.15.7 รองรับการใช้งาน Per Application VPN บนเครื่องคอมพิวเตอร์ระบบปฏิบัติการ Windows หรือ macOS

6.16 สามารถจัดทำรายงานอุปกรณ์ที่มีการ Jailbroken สำหรับอุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS หรือ rooted สำหรับอุปกรณ์ที่ใช้ระบบปฏิบัติการ Android

6.17 สามารถจัดทำรายงานสรุปคุณสมบัติฮาร์ดแวร์ และสรุปแอปพลิเคชันที่ติดตั้งอยู่

6.18 มีรายงานของ Event log เช่น Device event และ Console event

6.19 สามารถตั้งค่าให้ส่งรายงาน (Report) เป็น Daily, Weekly, Monthly ในรูปแบบ email

6.20 การบริหารจัดการ Enterprise App Catalog ขององค์กร

6.20.1 รองรับ Application ที่เป็น SaaS App เช่น Salesforce , Google App , Content Locker และ Virtual Application ทั้ง Horizon และ Citrix

6.21 ระบบ UEM ต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant 2022 ของ Unified Endpoint Management

6.22 ลิขสิทธิ์ของ Software ที่นำเสนอต้องมีสิทธิ์ในการใช้งานไม่น้อยกว่า 3 ปี

6.23 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

7. ระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ จำนวน 300 ลิขสิทธิ์

7.1 มีความสามารถป้องกัน Malware บนระบบปฏิบัติการได้ดังต่อไปนี้ Windows 10, Windows 11, Windows Server 2012, 2012 R2 Windows Server 2016, Windows Server 2019, Windows server 2022, MacOS และ Linux Ubuntu, Red Hat, Centos ได้

7.2 สามารถใช้เทคโนโลยี as a service เพื่อป้องกันไวรัสบนเครื่องลูกข่ายที่และเข้าไปทำการบริหารจัดการ โปรแกรมป้องกันไวรัสจากส่วนกลาง ผ่านทาง web console ได้

7.3 สามารถตรวจสอบ Malware แบบอ้างอิงจากฐานข้อมูล (Signature) และวิเคราะห์พฤติกรรมอย่างน้อยดังนี้

7.3.1 Vulnerability Protection หรือ Live Protection หรือ Exploit Blocking

7.3.2 Smart Scan หรือ Real-time scanning หรือ On Demand

7.3.3 Behavior Monitoring หรือ Behavior analysis และ Ransomware Protection

7.3.4 ตรวจจับภัยคุกคามได้ทั้งแบบ Pre-Execute และ Runtime โดยใช้ Machine Learning หรือมีเทคโนโลยี Machine Learning

7.4 สามารถป้องกันช่องโหว่ของระบบปฏิบัติการ โดยไม่จำเป็นต้องทำการติดตั้ง patches บนระบบปฏิบัติการเหล่านั้นจริงได้ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ patches โดยที่ยังไม่ได้ทำการทดสอบกับการใช้งานจริงได้ และสามารถเลือกนโยบายแบบ Recommended และ Aggressive ได้

7.5 มีความสามารถในการป้องกันข้อมูลสำคัญขององค์กรไม่ให้รั่วไหลออกไปภายนอกองค์กร (Data loss prevention) ผ่านทาง FTP, HTTP, Web Mail, Printer, Windows Clipboard, และ Removable Storage ได้ โดยใช้เงื่อนไขอย่างน้อยดังนี้ File Attributes, Keywords และ Regular Expressions

7.6 สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาต (Lockdown, Block และ Allow) และไม่ต้องการให้ติดตั้ง บนเครื่องคอมพิวเตอร์ลูกข่ายได้ (Application Control) และสามารถกำหนด Rule โดยใช้เงื่อนไขต่าง ๆ ได้ หรือมีความสามารถที่ไม่อนุญาตให้โปรแกรมประยุกต์ใช้งานได้ หรือเสนอระบบ Application Control ที่มีคุณสมบัติเทียบเท่า

7.7 สามารถทำการป้องกันอันตรายที่มาจากทางเว็บไซต์ต่างๆ (Web Threats) ได้โดยใช้ Web Reputation ได้เป็นอย่างน้อย

7.8 มีความสามารถในการกำหนดสิทธิ์การใช้งาน เช่น Full Access, Read, Read and Execute, Modify, List Content ให้กับอุปกรณ์ USB Storage devices ได้และสามารถอนุญาตให้ใช้งาน USB Storage ได้เป็นรายยี่ห้อ (Vendor ID) และ Serial Number ที่มีการลงทะเบียนในระบบเท่านั้น

7.9 ระบบป้องกันไวรัสบนเครื่องลูกข่ายสามารถป้องกันการหยุดการทำงาน และถอดถอนการติดตั้งโดยใช้รหัสผ่าน หรือ Token ได้

7.10 สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาต และไม่ต้องการให้ติดตั้งไปยังเครื่องลูกข่ายได้ และสามารถกำหนด Rule โดยใช้เงื่อนไขได้ดังนี้

7.10.1 Application Reputation

7.10.2 File Path

7.10.3 Hash Values (SHA-1)

7.10.4 Certificate

7.10.5 Gray Software List

7.11 สามารถกำหนดนโยบายการอัปเดตให้เครื่องลูกข่ายที่กำหนด รวมถึงทำหน้าที่แจกจ่าย pattern ให้แก่เครื่องอื่น ๆ ในองค์กร แทนที่เครื่องแม่ข่ายหลักได้ (Update Agent)

7.12 สามารถทำการ Update ฐานข้อมูลไวรัส (pattern) แบบ Incremental ได้เพื่อลดจำนวนขนาดในการ Download ฐานข้อมูล

7.13 ระบบวิเคราะห์ และตอบสนองภัยคุกคามการตรวจจับแบบข้ามขั้น Extended detection and response (XDR) ต้องมีความสามารถในการทำ response ทั้งแบบ Manual และ Automation (Security Playbooks) ในกรณีที่พบปัญหา โดยมีความสามารถอย่างน้อยดังนี้ Add Block List, Collect File, Isolate Endpoint และ Remote shell session

7.14 รองรับการตรวจสอบภัยคุกคาม ด้วยเทคโนโลยี Sandboxing

7.15 สามารถทำการค้นหา ข้อมูลที่ไม่อนุญาตขององค์กรไม่ให้รั่วไหลออกนอกองค์กร ผ่านทาง FTP, HTTP, Web Mail โดยใช้เงื่อนไข ได้ดังนี้

7.15.1 File Attributes

7.15.2 Keywords

7.15.3 Regular Expressions

7.16 สามารถออกรายงานการทำงานในรูปแบบ PDF, DOCX, หรือ XLSX หรือ CSV ได้

7.17 มีความสามารถในการ Response หรือ Action หากเกิดภัยคุกคามเช่น Add to block list, Remove from Block list, Terminate, Collect file, Isolate endpoint, Restore connection และ Start remote shell session เป็นต้น

7.18 สามารถรองรับ Activity ได้จากหลาย Product security ไม่เพียง Endpoint แต่ยังรวมถึง Email, network, cloud เป็นต้น

7.19 ผลิตภัณฑ์ที่นำเสนอจะต้องเป็นแพลตฟอร์มเป็นลักษณะของ Software-as-a-Service ที่ hosted และ managed ผ่าน cloud

7.20 มีความสามารถในการบริหารจัดการ Endpoint and Workload บนหน้า Console เดียว

7.21 รองรับการส่ง Syslog SIEM และ SOAR

7.22 เก็บบันทึกรายละเอียดกิจกรรม Activity ของเครื่อง Endpoint, Server, Network ได้แก่ DomainName, EndpointID, EndpointName, IPv4, IPv6, URL, Port, FileSHA1, FileFullPath, ProcessFullPath, CLICommand, RegistryKey, RegistryValue และ UserAccount

7.23 มีความสามารถในการแบ่งปัน Suspicious Object ให้กับ Product อื่น ๆ เพื่อเพิ่มความสามารถในการป้องกันภัยคุกคาม

7.24 สามารถสร้าง workbench เมื่อมีการทริกเกอร์กับรูปแบบของการโจมตีโดยแสดงความเชื่อมโยงทั้งหมดของเหตุการณ์ที่เกิดขึ้นโดยอัตโนมัติ

7.25 มีความสามารถในการทำงานร่วมกับระบบตรวจจับและวิเคราะห์ภัยคุกคามชั้นสูง (Sandbox as a Service)

7.26 เจ้าของผลิตภัณฑ์ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platforms ปี 2023 หรือใหม่กว่า

7.27 ลิขสิทธิ์ของ Software ที่นำเสนอต้องมีสิทธิ์ในการใช้งานไม่น้อยกว่า 3 ปี

8. ซอฟต์แวร์ลิขสิทธิ์ระบบปฏิบัติการ Microsoft Windows Server Standard จำนวน 32 ลิขสิทธิ์

8.1 ชุดโปรแกรมระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับรองรับหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 16 แกนหลัก (16 core) ต่อ 1 ลิขสิทธิ์ ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยต้องมีหนังสือรับรองจากบริษัทเจ้าของผลิตภัณฑ์หรือบริษัทตัวแทนจำหน่ายในประเทศไทยที่ได้รับการแต่งตั้งอย่างถูกกฎหมายจากบริษัทเจ้าของผลิตภัณฑ์มาแสดงในวันยื่นข้อเสนอ

8.2 ซอฟต์แวร์ที่นำเสนอเป็นรุ่น Microsoft Windows Server 2022 หรือใหม่กว่า

9. ซอฟต์แวร์ลิขสิทธิ์ระบบจัดการฐานข้อมูล Microsoft SQL Server Standard จำนวน 1 ลิขสิทธิ์

9.1 ซอฟต์แวร์ที่นำเสนอต้องเป็นลิขสิทธิ์ถูกต้อง รองรับการติดตั้งได้ไม่น้อยกว่า 1 ชุด

9.2 ซอฟต์แวร์ที่นำเสนอเป็นรุ่น Microsoft SQL Server Standard 2022 หรือใหม่กว่า

10. ซอฟต์แวร์ลิขสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์ลูกข่ายเสมือน Windows Virtual Desktop Access จำนวน 300 ลิขสิทธิ์

10.1 มีจำนวนไม่น้อยกว่า 300 ลิขสิทธิ์

10.2 รองรับการใช้งานร่วมกับอุปกรณ์ที่ติดตั้งระบบปฏิบัติการ Windows 11 Pro ได้เป็นอย่างน้อย

10.3 เป็นลิขสิทธิ์แบบ Open Value Program (OV)

10.4 มีระบบสำหรับจัดเก็บ, ดาวน์โหลดตัวติดตั้ง และตรวจสอบลิขสิทธิ์ volume licensing (VLSC) ผ่านระบบ Volume Licensing in Microsoft 365 admin center

10.5 มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย

10.6 มีลิขสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์ลูกข่ายเสมือน Windows Virtual Desktop Access (VDA) Per Device

10.7 ลิขสิทธิ์ของ Software ที่นำเสนอต้องมีสิทธิ์ในการใช้งานไม่น้อยกว่า 3 ปี

11. ชุดโปรแกรมจัดการสำนักงานแบบที่ 1 ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย จำนวน 300 ลิขสิทธิ์

11.1 มีโปรแกรมสำหรับประมวลคำหรือระบบจัดเตรียมเอกสาร

11.2 มีโปรแกรมสำหรับประเภทตารางการคำนวณ

11.3 มีโปรแกรมสำหรับประเภทการนำเสนอข้อมูล

11.4 มีโปรแกรมสำหรับบริการจัดการจดหมายอิเล็กทรอนิกส์ (Email)

11.5 สามารถบริหารจัดการสิทธิ์แบบรวมศูนย์ได้จากส่วนกลางด้วย Key Management Service (KMS)

11.6 ประเภทลิขสิทธิ์ซอฟต์แวร์ที่เสนอ ต้องเป็นลิขสิทธิ์ไม่น้อยกว่า 3 ปี

12. การติดตั้งและฝึกอบรมการใช้ระบบ

12.1 ผู้ชนะการเสนอราคาต้องดำเนินการติดตั้งระบบ ตั้งค่าระบบ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ และเสริมความปลอดภัยของระบบ (hardening) ให้มีความมั่นคงปลอดภัยตามมาตรฐานที่สำนักข่าวกรองแห่งชาติกำหนด ดังนี้

12.1.1 เครื่องคอมพิวเตอร์แม่ข่าย (รายการที่ 1) ต้องติดตั้ง และตั้งค่า และเสริมความปลอดภัยของระบบ (hardening) ร่วมกับซอฟต์แวร์ 1) โปรแกรมบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่ายเสมือน (รายการที่ 5) 2) ระบบ Unified Endpoint Management (UEM) - VMware Workspace ONE Standard (รายการที่ 6) 3) ซอฟต์แวร์ลิขสิทธิ์ระบบปฏิบัติการ Microsoft Windows Server Standard (รายการที่ 7) 4) ซอฟต์แวร์ลิขสิทธิ์ระบบจัดการฐานข้อมูล Microsoft SQL Server Standard (รายการที่ 9) และซอฟต์แวร์ลิขสิทธิ์การเข้าใช้งานเครื่อง คอมพิวเตอร์ลูกข่ายเสมือน Windows Virtual Desktop Access

12.1.2 เครื่องคอมพิวเตอร์ Thin Client (รายการที่ 3) ต้องติดตั้ง และตั้งค่า และเสริมความปลอดภัยของระบบ (hardening) ร่วมกับซอฟต์แวร์ 1) ระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ (รายการที่ 7) 2) ชุดโปรแกรมจัดการสำนักงานแบบที่ 1 ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย (รายการที่ 11)

12.2 ผู้ชนะการเสนอราคาต้องทำการอบรมในรูปแบบ on-the-job-training และเสนอแนะการใช้งานให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จำนวนไม่เกิน 15 คน โดยมีระยะเวลาอบรมไม่น้อยกว่า 5 วัน และผู้จัดการอบรมต้องรับผิดชอบในส่วนของค่าใช้จ่าย การจัดเตรียมเอกสารประกอบการเรียนการสอน อาหารว่างและอาหารกลางวันสำหรับผู้เข้ารับการอบรม ณ สถานที่ซึ่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดเตรียมไว้ให้ สำหรับรายการดังนี้

12.2.1 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

12.2.2 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานอุปกรณ์กระจายสัญญาณเครือข่าย

12.2.3 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานเครื่องคอมพิวเตอร์ Thin Client

12.2.4 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานโปรแกรมบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่ายเสมือน

12.2.5 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานระบบ Unified Endpoint Management (UEM) - VMware Workspace ONE Standard

12.2.6 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

12.2.7 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานซอฟต์แวร์ลิขสิทธิ์ระบบปฏิบัติการ Microsoft Windows Server Standard

12.2.8 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานซอฟต์แวร์ลิขสิทธิ์ระบบจัดการฐานข้อมูล Microsoft SQL Server Standard

12.2.9 ติดตั้ง การตั้งค่าพื้นฐาน และสอนการใช้งานซอฟต์แวร์ลิขสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์

12.2.10 ลูกข่ายเสมือน Windows Virtual Desktop Access

12.2.11 การบริหารจัดการระบบ VDI ให้กับผู้ใช้งานของสำนักข่าวกรองแห่งชาติ

( )	( )	( )	( )	( )	( )	( )
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการและเลขานุการ