ขอบเขตงาน (Terms of Reference: TOR)
โครงการจัดทำระบบความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานการบินพลเรือนแห่งประเทศไทย

---

1. หลักการและเหตุผล

ด้วยสำนักงานการบินพลเรือนแห่งประเทศไทย เป็นหน่วยงานที่จัดตั้งขึ้นตามพระราชกำหนดการบินพลเรือน พ.ศ. 2558 เพื่อปฏิบัติภารกิจ ในการกำกับดูแล ควบคุม ส่งเสริมและพัฒนากิจการการบินพลเรือนให้เป็นไปตามกฎหมายและมาตรฐานสากล จากที่ กพท. ได้ดำเนินโครงการจัดทำศูนย์ข้อมูลหลักและเครือข่าย (Data Center and Network) เพื่อให้บริการจัดการระบบเครือข่ายและแอพพลิเคชั่นสำคัญๆ ของสำนักงานแล้วนั้น การจัดทำโครงการระบบความมั่นคงปลอดภัยด้านสารสนเทศเป็นโครงการที่จำเป็นในการประเมินและตรวจสอบความปลอดภัยของระบบสารสนเทศ ทั้งจากปัจจัยภายในและปัจจัยภายนอก ซึ่งเกิดจากการบุกรุกระบบโดยไวรัส มัลแวร์ แฮกเกอร์ ตลอดจนความผิดพลาดต่างๆ จากผู้ใช้งาน อาจจะส่งผลโดยตรงกับเครือข่ายของ กพท. หรือโดยตรงต่อฐานข้อมูลที่มีค่าประเมินมูลค่ามิได้ ก่อให้เกิดความเสียหายต่อข้อมูลและสำนักงานในการให้บริการประชาชน

ดังนั้น การป้องกันและการวางแผนรับมือกับภัยคุกคามต่างๆ เป็นสิ่งที่จำเป็นสำหรับ กพท. โดยสามารถแบ่งแยกประเภทของการป้องกันระบบและฐานข้อมูลเพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศแบ่งได้ ดังนี้

1.1 ความมั่นคงปลอดภัยของฐานข้อมูล จากไวรัส มัลแวร์ ที่มีจำนวนมากในเครือข่ายอินเตอร์เน็ต ซึ่งมีความเสี่ยงสูงที่ระบบของสำนักงานจะถูกโปรแกรมไวรัสหรือมัลแวร์เข้าโจมตี

1.2 การกำหนดสิทธิการเข้าถึงระบบของผู้ใช้งาน เป็นมาตรการความปลอดภัยขั้นพื้นฐานที่จำเป็น ช่วยให้ระบบมีผู้ใช้งานที่ถูกต้อง และจำกัดสิทธิ์ในส่วนที่ต้องการความปลอดภัยสูงให้ผู้ใช้งานเฉพาะด้านเท่านั้น

1.3 การตรวจประเมินช่องโหว่ของระบบและการป้องกันการบุกรุกระบบจากภายนอก เป็นมาตรการขั้นสูงสำหรับการสร้างความมั่นคงปลอดภัยด้านสารสนเทศ โดยการตรวจสอบประเมินความเสี่ยงของระบบค้นหาจุดบกพร่องหรือช่องทางที่จะมีความเสี่ยงในการบุกรุกระบบจากแฮกเกอร์ซึ่งมีความเชี่ยวชาญในการบุกรุกและโจมตีระบบ เพื่อให้ระบบสารสนเทศของสำนักงานปลอดภัยขั้นสูง

การดำเนินโครงการจัดทำระบบความมั่นคงปลอดภัยด้านสารสนเทศสำนักงานนี้เพื่อสร้าง ความมั่นคงปลอดภัยและความน่าเชื่อถือของระบบและฐานข้อมูลที่สำคัญ ช่วยเพิ่มเสถียรภาพของการให้บริการด้านระบบเทคโนโลยีสารสนเทศ และเพิ่มความปลอดภัยจากการบุกรุกระบบหรือคุกคามจากช่องทางต่างๆทั้งภายในและภายนอกสำนักงาน

2. วัตถุประสงค์และเป้าหมายโครงการ

2.1. วัตถุประสงค์

2.1.1. เพื่อให้การปฏิบัติงานของสำนักงานการบินพลเรือนแห่งประเทศไทยมีประสิทธิภาพตอบสนองการให้บริการต่างๆของสำนักงาน สร้างความเชื่อมั่นและเชื่อถือของข้อมูลและบริการต่างๆด้านสารสนเทศในระดับสูง

2.1.2. เพื่อให้ระบบสารสนเทศและเครือข่ายของสำนักมีความมั่นคงปลอดภัยในระดับสากล เป็นที่ยอมรับและเชื่อถือของหน่วยงานที่เกี่ยวข้อง

2.2. เป้าหมาย

2.2.1. มีระบบป้องกันไวรัส และมัลแวร์ ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์สำหรับพนักงาน

2.2.2. มีระบบบริหารจัดการสิทธิ์การเข้าถึงเครือข่ายของสำนักงาน

2.2.3. มีเครื่องมือและวิธีการตรวจประเมินช่องโหว่ระบบเครือข่ายของสำนักงาน

2.3. ประโยชน์ที่คาดว่าจะได้รับ

2.3.1. มีเครื่องมือป้องกันการบุกรุกด้วย ไวรัสและมัลแวร์ ซึ่งเป็นอันตรายต่อคอมพิวเตอร์และระบบสารสนเทศของสำนักงาน

2.3.2. มีระบบการบริหารผู้ใช้งานระบบสารสนเทสของสำนักงานที่มีประสิทธิภาพ

2.3.3. มีแผนการป้องกันช่องโหว่ระบบและแผนการบริหารความเสี่ยงของระบบสารสนเทศของสำนักงาน

3. คุณสมบัติผู้เสนอราคา

3.1. ผู้เสนอราคาต้องเป็นผู้มีอาชีพขายพัสดุที่จัดซื้อดังกล่าว

3.2. ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้วหรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

3.3. ผู้เสนอราคาไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานการบินพลเรือนแห่งประเทศไทย หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

3.4. ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

3.5. บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

3.6. บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญากับหน่วยงานภาครัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement: e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลาง ที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

3.7. คู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทถ้วน คู่สัญญาอาจจ่ายเป็นเงินสดก็ได้

4. ขอบเขตการดำเนินโครงการ

4.1. เครื่องแม่ข่ายและระบบป้องกันไวรัส จำนวน 1 ระบบ คุณลักษณะพื้นฐาน ดังนี้

4.1.1.เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 2 สำหรับระบบป้องกันไวรัส จำนวน 1 เครื่อง คุณลักษณะพื้นฐานดังนี้

4.1.1.1. มีหน่วยประมวลผลกลาง แบบ 8 แกนหลัก (8 Core) หรือ ดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (SERVER) โดยเฉพาะ และมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.4 GHz จำนวนไม่น้อยกว่า 2 หน่วย

4.1.1.2. หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วย ความจำแบบ Cache Memory ไม่น้อยกว่า 20 MB

4.1.1.3. มีหน่วยความจำหลัก(RAM) ชนิด ECC DDR3 หรือดีกว่า ขนาดไม่น้อยกว่า 32 GB

4.1.1.4. สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5

4.1.1.5. มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SCSI หรือ SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที ชนิด Solid State Drives หรือดีกว่า และมีขนาดความจุไม่น้อยกว่า 450 GB จำนวนไม่น้อยกว่า 4 หน่วย

4.1.1.6. มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน 1 หน่วย

4.1.1.7. มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

4.1.1.8. มีจอภาพแบบ LCD หรือดีกว่า ขนาดไม่น้อยกว่า 17 นิ้ว จำนวน 1 หน่วย

4.1.1.9. มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

4.1.1.10. มีลิขสิทธิ์ Window Server Standard License ในเวอร์ชั่นล่าสุด หรือดีกว่า จำนวน 1 ลิขสิทธิ์

4.1.2. ลิขสิทธิ์สำหรับป้องกันไวรัส จำนวน 330 ลิขสิทธิ์ คุณลักษณะพื้นฐานดังนี้

4.1.2.1. สามารถติดตั้งโปรแกรมบริหารจัดการได้บนเครื่อง Windows Server 2008 หรือ 2012, VMWare ESX และรองรับการใช้งานกับ Enterprise Database Server Microsoft SQL Server 2008, 2012 ได้

4.1.2.2. มีระบบการจัดการเป็นแบบ Web-Base Management

4.1.2.3. มี Logs สำหรับเก็บข้อมูลต่างๆ เช่น Server Logs, Audit logs เพื่อย้อนหลังเวลามีบุคคลเข้ามาแก้ไข หรือเปลี่ยนแปลงค่า Configuration ได้

4.1.2.4. สามารถใช้ Agent เพียงตัวเดียวสำหรับบริหารจัดการ Security Policy ต่างๆ และติดตั้งโปรแกรมต่างๆ ได้เพิ่มได้ อย่างน้อย 4 ชนิด เช่น Antivirus, Host IPS, Web Security, Host NAC, Policy Auditor, DLP, Endpoint Encryption, AV บน VMWare

4.1.2.5. สามารถควบคุมการ deploy DATs, engines, service packs, hotfixes และโปรแกรมต่างๆ ของเครื่องลูกข่ายได้

4.1.2.6. สามารถสแกนหาจำนวนเครื่องภายใน Subnet เพื่อให้เรารู้จำนวนเครื่องทั้งหมดหรือแจ้งเตือนได้เมื่อมีเครื่องแปลกปลอมเข้ามาเชื่อมต่อในระบบได้

4.1.2.7. สามารถตรวจดูรายละเอียดของเครื่องต่างๆได้ เช่น ชื่อเครื่อง, OS version, Domain, IP Address, MAC, ขนาดของ RAM, ความจุของฮาร์ดดิสก์ เป็นต้น

4.1.2.8. สามารถกำหนด, สร้างโปรแกรมการบริหาร และควบคุม กระจายการอัพเดทเป็นแบบอัตโนมัติตามส่วนบังคับการรอง (Regional Node) ได้ไม่จำกัดจำนวน โดยยังอยู่ภายใต้การบริหาร และควบคุมจากส่วนกลาง (HQ)

4.1.2.9. สามารถที่จะก็อปปี้นโยบายการป้องกันไวรัสจากเครื่องเซริฟเวอร์ไปยังเครื่องเซริฟเวอร์อื่นๆได้ หรือก็อปปี้ภายในเครื่องเซริฟเวอร์เองได้ระหว่างกลุ่มได้

4.1.2.10. สามารถที่จะเอ็กพอร์ทนโยบายต่างๆ ออกมาจากเครื่อง แล้วสามารถที่จะนำกลับหรือนำไปใช้กลับเครื่องอื่นได้

4.1.2.11. มีรายงานแสดงผลเป็นแบบ Dash Board แบบ Real Time และ สามารถกำหนดช่วงเวลา Refresh ข้อมูล และปรับแต่งแก้ไขรายงานได้

4.1.2.12. สามารถทำรายงาน Compliance Report เพื่อวัดผลการดำเนินงานการติดตั้งโปรแกรมหรือนำเอานโยบายไปใช้ (policy enforcement)

4.1.2.13. สามารถตั้งเวลาในการทำ Schedule Report และส่งผลไปยัง Email, FTP ได้

4.1.2.14. สามารถทำ Synchronize จำนวนเครื่องที่อยู่ใน Active Directory พร้อมติดตั้งโปรแกรมได้

4.1.2.15. ตัวโปรแกรมต้องสามารถทำการตรวจจับ Viruses, Worms, Trojan Horses, Adware, Spyware, Dialers, Rootkits และ Malware อื่นๆได้ภายในตัวโปรแกรมเดียว โดยที่ไม่ต้องลงโปรแกรมเสริมอื่นใด

4.1.2.16. เครื่องลูกข่ายต้องสามารถทำการปรับปรุงฐานข้อมูลไวรัส (Virus Signature/ Pattern) และส่วนประกอบของโปรแกรมป้องกันไวรัส (Scan Engine) ได้ทั้งภายใน LAN และทางอินเทอร์เน็ทตามลำดับนโยบายที่กำหนดไว้พร้อมทั้งสามารถทำการอัพเดทไปยังช่องทางเลือกลำดับหลังของนโยบายที่กำหนดไว้ได้โดยอัตโนมัติ

4.1.2.17. สามารถกำหนดนโยบายรักษาความปลอดภัย ควบคุม บริหาร จัดการ การทำงานของโปรแกรมจากเครื่องจัดการและบริหารโปรแกรมป้องกันไวรัสจากศูนย์กลางได้ และรองรับการกำหนดนโยบายแยกตามประเภทของเครื่องลูกข่าย

4.1.2.18. สามารถทำงานร่วมกับ MS Outlook ในการตรวจสอบ Virus ได้

4.1.2.19. สามารถทำการสั่งสแกนตามนโยบายที่กำหนดไว้ได้หลายรูปแบบตามเวลาที่ต้องการ

4.1.2.20. สามารถป้องกันการปิด Service ของโปรแกรม Antivirus ได้ถึงแม้ว่าจะมีสิทธิเป็น Administrator ของระบบก็ตาม

4.1.2.21. สามารถจัดการควมคุมอุปกรณ์ที่จะนำมาต่อพ่วงกับคอมพิวเตอร์ อาทิเช่น USB Drive, Aircard, Wifi, Lan adapter, กล้อง Web cam, คีย์บอร์ดเม้าท์ เป็นต้น

4.1.2.22. สามารถตรวจสอบ แจ้งเตือนและเก็บ logs ข้อมูลการกระทำและไฟล์หลักฐานแต่ละเหตุการณ์ที่ละเมิดนโยบายได้

4.1.2.23. รองรับการใช้งานและกำหนดนโยบายเพื่อบังคับใช้หรือปลดออกเฉพาะคนหรือกลุ่มร่วมกับ Domain user หรือ Group Domain ใน Active Directory ได้

4.1.2.24. สามารถเตือนผู้ใช้ถึงความเสี่ยงในแต่ละเว็บหรือไฟล์ดาวน์โหลดได้ โดยแบ่งบอกออกเป็นสีแดง สีเหลือง สีเขียว

4.1.2.25. สามารถเตือนผู้ใช้ถึงความภัยในแต่ละเว็บจากผลค้นหาของ Google, MSN, Yahoo

4.1.2.26. สามารถกำหนด Traffic ที่วิ่งทั้งขาเข้าและขาออก ผ่านแต่ละ application, service และ network port ได้

4.1.2.27. ผลิตภัณฑ์ที่นำเสนอจะต้องอยู่ในอันดับ 1-4 ใน Endpoint Protection ของ Magic Quadrant Gartner

4.1.2.28. เจ้าหน้าที่ที่ติดตั้งจะต้องมีใบประกาศนียบัตรที่ได้รับการรับรองจากเจ้าของผลิตภัณฑ์

4.2. ระบบยืนยันตัวบุคคลและควบคุมการเข้าถึงระบบงาน (Active Directory) คุณลักษณะพื้นฐานดังนี้

4.2.1.เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 1 สำหรับยืนยันตัวบุคคลและควบคุมการเข้าถึงระบบงาน จำนวน 1 เครื่อง คุณลักษณะพื้นฐานดังนี้

4.2.1.1. มีหน่วยประมวลผลกลาง แบบ 6 แกนหลัก (6 Core) หรือ ดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (SERVER) โดยเฉพาะ และมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.0 GHz จำนวนไม่น้อยกว่า 1 หน่วย

4.2.1.2. หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory ไม่น้อยกว่า 15 MB

4.2.1.3. มีหน่วยความจำหลัก(RAM) ชนิด ECC DDR3 หรือดีกว่า ขนาดไม่น้อยกว่า 8 GB

4.2.1.4. สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5

4.2.1.5. มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SCSI หรือ SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า 7,200 รอบต่อนาที ชนิด Solid State Drives หรือดีกว่า และมีขนาดความจุไม่น้อยกว่า 140 GB จำนวนไม่น้อยกว่า 2 หน่วย

4.2.1.6. มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน 1 หน่วย

4.2.1.7. มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface แบบ 10/100/1000 Base-T) หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

4.2.1.8. มีจอภาพแบบ LCD หรือดีกว่า ขนาดไม่น้อยกว่า 17 นิ้ว จำนวน 1 หน่วย

4.2.1.9. มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

4.2.1.10. มีลิขสิทธิ์ Window Server Standard License ในเวอร์ชั่นล่าสุด หรือดีกว่า จำนวน 1 ลิขสิทธิ์

4.2.2.ระบบยืนยันตัวบุคคลและควบคุมการเข้าถึงระบบงาน คุณลักษณะพื้นฐานดังนี้

4.2.2.1. สามารถทำงานร่วมกับเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการต่างๆ ทั้งแบบ 32 และ 64 bit ได้แก่ Windows XP, Windows Vista, Windows7, Windows8, Windows8.1, Windows10, Windows server 2003, Windows server 2008, Windows Server 2012 ได้เป็นอย่างน้อย

4.2.2.2. มีระบบจัดการผู้ใช้ สามารถกำหนดและบังคับนโยบายสำหรับรหัสผ่านของผู้ใช้ โดยต้องทำงานได้อย่างน้อย ดังนี้

4.2.2.2.1. เก็บบันทึกค่า รหัสผ่าน ที่เคยใช้งานแล้วเพื่อตรวจสอบไม่ให้มีการตั้งค่าซ้ำกับรหัสผ่านเดิม

4.2.2.2.2. กำหนดอายุการใช้งานสูงสุดของรหัสผ่านที่อนุญาตให้ใช้ได้

4.2.2.2.3. กำหนดความซับซ้อนของรหัสผ่านที่สามารถตั้งได้ เช่น ให้มีตัวเลขผสมตัวอักษร หรือมีอักขระพิเศษร่วมด้วย เป็นต้น

4.2.2.2.4. กำหนดจำนวนครั้งที่อนุญาตให้ใส่รหัสผ่านผิดก่อนทำการ Lock account ตามช่วงเวลาที่กำหนด

4.2.2.3. สามารถบริหารจัดการผู้ใช้งาน (User) และเครื่องคอมพิวเตอร์จากส่วนกลางผ่านเครื่องมือในการจัดการแบบ GUI

4.2.2.4. สามารถพิสูจน์ตัวตน (User Authentication) และ ตรวจสอบสิทธิ (User Authorization) การเข้าใช้งานข้อมูล ซอฟต์แวร์เครื่องแม่ข่าย ลูกข่าย เครื่องพิมพ์ หรือทรัพยากรอื่นๆ บนเครือข่ายได้

4.2.2.5. มีระบบ Single Sign-on โดยผู้ใช้ระบบสามารถ Login เข้าเว็บไซต์เพื่อใช้ระบบงานต่างๆ แบบครั้งเดียว โดยไม่ต้อง Login ใหม่เมื่อมีการใช้งานระบบใหม่

4.2.2.6. สามารถใช้งาน Username และ Password จากระบบปฏิบัติการของเครื่องคอมพิวเตอร์ในการ Login ครั้งแรกได้ โดยต้องสนับสนุน Windows logon ได้เป็นอย่างน้อย

4.2.2.7. มีระบบบริหารตรวจสอบสิทธิและบัญชีรายชื่อผู้ใช้ได้

4.2.2.8. สามารถจัดการเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ที่ใช้ในระบบของโครงการทั้งในส่วนของการทำ Authentication การอ้างอิง User และ Group เพื่อใช้งานระบบต่างๆ

4.2.2.9. สามารถค้นหาข้อมูลรายนามผู้ใช้, เครื่องคอมพิวเตอร์, เครื่องพิมพ์ ที่มีในเครือข่ายได้จากเครื่องคอมพิวเตอร์ลูกข่าย

4.2.2.10. มีระบบ IT Policy Enforcement หรือ Group Policy Enforcement สำหรับเครื่องคอมพิวเตอร์ลูกข่ายได้จากส่วนกลาง

4.2.2.11. สามารถกำหนดค่า Configuration ในการ Update Patch ของระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ลูกข่ายได้จากส่วนกลาง

4.2.2.12. สามารถกำหนดค่า Settings ของเว็บบราวเซอร์ Internet Explorer ของเครื่องคอมพิวเตอร์ลูกข่ายได้จากส่วนกลาง

4.2.2.13. เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็นระบบยืนยันตัวบุคคลและควบคุมการเข้าถึงระบบงาน ต้องทำงานเป็นแบบ High Availability

4.3. ระบบตรวจสอบและบริหารจัดการช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ จำนวน 1 ระบบ คุณลักษณะพื้นฐาน ดังนี้

4.3.1. ระบบที่นำเสนอต้องเป็น Hardware Appliance หรือ Software ที่ออกแบบมาเพื่อตรวจสอบและบริหารจัดการช่องโหว่โดยเฉพาะ และมีลิขสิทธิ์รองรับการตรวจสอบจำนวน IP Address ได้ไม่น้อยกว่า 128 IP Addresses

4.3.2. ผลิตภัณฑ์ที่นำเสนอจะต้องได้รับการรับรองจากอยู่ในกลุ่ม Strong Positive จากหน่วยงานที่ทำการวิจัยตลาดชั้นนำ (Gartner) ในเรื่องของ Vulnerability Assessment ในปีล่าสุด

4.3.3. สามารถตรวจสอบ (Scan) ช่องโหว่ของระบบดังต่อไปนี้ภายใต้อุปกรณ์ที่นำเสนอ หรือสามารถที่จะเสนออุปกรณ์และซอฟต์แวร์เพิ่มเติม (Third party) เพื่อให้ระบบสามารถทำงานได้อย่างสมบูรณ์ได้

4.3.4. ระบบปฏิบัติการ (Operating System) ได้แก่ Microsoft Windows, UNIX, Linux Red Hat, CentOS, Solaris และ VMware

4.3.5. ระบบฐานข้อมูล (Database) ได้แก่ Microsoft SQL Server, Oracle, Sybase SQL, MySQL, AS/400, PostgreSQL และ DB2

4.3.6. Web Application ตามรายละเอียด ดังนี้

4.3.6.1. สามารถตรวจสอบช่องโหว่ของ Web Application โดยครอบคลุม OWASP Top 10 ได้

4.3.6.2. รองรับการทำ Credential Scan ผ่านหน้า HTTP Web Login

4.3.6.3. รองรับการตรวจสอบแบบ Web Spidering หรือ Crawling

4.3.6.4. รองรับการตรวจสอบ (Scan) ทั้งแบบ Non-credential Scan และ Credential Scan

4.3.7. สามารถตรวจสอบช่องโหว่ของอุปกรณ์เครือข่ายโดยไม่ต้องติดตั้งโปรแกรมเพิ่มเติมในอุปกรณ์ที่ต้องการตรวจสอบ (Agentless)

4.3.8. มีการจัดลำดับความรุนแรงของช่องโหว่และแสดงรายละเอียดของปัญหา เช่น Malware, Exploit Exposure หรือ CVSS base score ได้เป็นอย่างน้อย

4.3.9. ต้องสามารถตั้งค่าระดับความสำคัญหรือจัดกลุ่มของอุปกรณ์ที่ต้องการทำการตรวจสอบได้

4.3.10. สามารถกำหนดให้ตรวจสอบเฉพาะ Ports ที่ต้องการได้ และได้ทั้ง TCP และ UDP ports (Common Ports)

4.3.11. สามารถสร้าง และแก้ไขรูปแบบในการตรวจสอบ (Modify Scan Template) ได้

4.3.12. สามารถให้คำแนะนำ, วิธีในการแก้ไขปัญหาของช่องโหว่ (Remediation) รวมถึงการแสดงแหล่งที่สามารถดาวน์โหลดซอฟท์แวร์ปรับปรุงแก้ไข (Patch/Hotfix) ต่างๆได้

4.3.13. สามารถอัพเดตฐานข้อมูลการตรวจสอบช่องโหว่จากผู้ผลิตได้โดยอัตโนมัติ (Automatic) หรือโดยผู้ดูแลระบบ (Manual)

4.3.14. สามารถทำ Vulnerability Exception ได้

4.3.15. สามารถแจ้งเตือนผลการตรวจสอบช่องโหว่และรายงานให้ผู้ดูแลระบบผ่านทาง Email, SNMP และ Syslog ได้

4.3.16. สามารถสร้างรายงานได้หลากหลายรูปแบบ เช่น Audit Report, Executive Overview หรือ Baseline comparison เป็นอย่างน้อย

4.3.17. สามารถสร้างรายงานตามรูปแบบไฟล์ PDF, HTML, XML และ CSV ได้เป็นอย่างน้อย

4.3.18. มีระบบ Ticket สำหรับติดตามการแก้ไขช่องโหว่ที่ตรวจพบ และสามารถทำงานร่วมกับ Third Party Ticketing System ได้ เช่น BMC Remedy เป็นต้น

4.3.19. สามารถบริหารการจัดการผ่านทาง Secure Web Browser (HTTPS) ได้

4.3.20. สามารถกำหนดสิทธิของผู้ใช้งาน เพื่อเข้าถึงระบบด้วยสิทธิ์ที่ต่างกันได้ (Role-Based Management)

4.3.21. มี API เพื่อทำงานร่วมกับระบบอื่นๆได้ เช่น SIEM, IPS เป็นต้น

4.3.22. รองรับมาตรฐาน Compliance เช่น PCI DSS, ISO, NERC, FISMA, HIPAA, USGCB และ CIS ได้เป็นอย่างน้อย

4.3.23. ระบบที่นำเสนอต้องสามารถตรวจสอบช่องโหว่ที่ค้นพบ (Vulnerability Validation) โดยทำการทดสอบการเจาะระบบเครือข่ายคอมพิวเตอร์ (Penetration Testing) ได้

4.3.24. สามารถสร้างรายงานผลการตรวจสอบช่องโหว่จากการทดสอบการเจาะระบบเครือข่ายคอมพิวเตอร์ (Penetration Testing) ได้

4.3.25. มีระบบที่สามารถตั้ง Automatic Scan ได้เมื่อพบช่องโหว่ใหม่เกิดขึ้นโดยไม่ต้อง Scan ใหม่ทั้งหมด โดยกำหนด Criteria ในการตรวจสอบจาก CVSS Score และ CVE ID ได้เป็นอย่างน้อย

4.4. งานติดตั้งกำหนดค่าอุปกรณ์ และการอบรม จำนวน 1 งาน ดังนี้

4.4.1. ผู้เสนอราคาต้องจัดเตรียมผู้จัดการโครงการเพื่อบริหารจัดการโครงการและประสานงานกับเจ้าหน้าที่สำนักงานการบินพลเรือนแห่งประเทศไทย อย่างน้อย 1 คน โดยผู้จัดการโครงการจะต้องมีคุณสมบัติดังนี้

4.4.1.1. จบปริญญาตรีขึ้นไปในสาขาคอมพิวเตอร์หรือสาขาที่เกี่ยวข้อง

4.4.1.2. มีประสบการณ์ทำงานในสายงานที่เกี่ยวข้องไม่น้อยกว่า 5 ปี

4.4.2. ผู้เสนอราคาจะต้องจัดทำการตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศให้กับทางสำนักงาน โดยครอบคลุมไปถึงการตรวจสอบช่องโหว่ของระบบ Network และช่องโหว่ในระบบ Web Application โดยการใช้ระบบตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศในโครงการ เป็นระยะเวลา 2 ครั้งต่อระยะเวลาโครงการ ซึ่งผู้ปฏิบัติงานจะต้องเป็นผู้เชี่ยวชาญเฉพาะทางโดยจะต้องได้รับรองมาตรฐานอย่างน้อยดังต่อไปนี้

4.4.2.1. Certified Information Systems Security Professional (CISSP)

4.4.2.2. Certified Information Systems Auditor (CISA)

4.4.2.3. Certified Ethical Hacker (CEH)

4.4.3. ผู้เสนอราคาจะต้องออกแบบระบบความปลอดภัยสำหรับเครือข่ายให้คณะกรรมการตรวจรับโครงการหรือผู้ได้รับมอบหน้าที่ในการดูแลโครงการเพื่อพิจารณาก่อนการติดตั้งหรือการกำหนดค่าใดๆ

4.4.4. ผู้เสนอราคาจะต้องจัดการฝึกอบรมการใช้งานระบบ การกำหนดค่าติดตั้งระบบเบื้องต้น พร้อมจัดเตรียมเอกสารการฝึกอบรม เป็นเอกสารจำนวนอย่างน้อย 5 ชุด และเป็นเอกสารแบบไฟล์ลงแผ่น จำนวนอย่างน้อย 5 ชุด ให้แก่เจ้าหน้าที่สำนักงานการบินพลเรือนแห่งประเทศไทย อย่างน้อย 5 ท่าน เป็นจำนวนอย่างน้อย 1 คอร์ส

5. **เงื่อนไข ผู้ประสงค์จะเสนอราคาจะต้องแนบรายการดังต่อไปนี้ ในวันยื่นข้อเสนอ**

5.1. ผู้เสนอราคาจะต้องทำเอกสารข้อเสนอทางเทคนิค และตารางเปรียบเทียบรายละเอียดและเงื่อนไขเฉพาะต่อข้อกำหนดและรายละเอียด (Specification) เป็นรายข้อทุกข้อ (Statement of Compliance) ของขอบเขตการดำเนินโครงการตามรายละเอียด โดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบตามตารางที่ 1.1 ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความหรือเอกสารในส่วนอื่นที่ จัดทำเสนอมา ผู้เสนอราคาต้องระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้โดยง่ายไว้ใน เอกสารเปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงนั้น อยู่ในส่วนใดตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึง ให้หมายเหตุหรือขีดเส้นใต้หรือระบายสีพร้อม เขียนหัวข้อกำกับไว้ เพื่อให้สามารถตรวจสอบกับเอกสารเปรียบเทียบได้ง่ายและตรงกันด้วย หากผู้เสนอราคาไม่ดำเนินการตามข้อนี้คณะกรรมการพิจารณาผลการเสนอราคาขอสงวนสิทธิ์ ในการไม่พิจารณาข้อเสนอของผู้เสนอราคา

ตารางที่ 1.1 ตารางเปรียบเทียบคุณสมบัติข้อกำหนดและรายละเอียดข้อเสนอโครงการ

อ้างถึงข้อ	**ข้อกำหนดอุปกรณ์ที่ต้องการ**	**ข้อกำหนด/อุปกรณ์ที่นำเสนอ**	**เอกสารอ้างอิง**
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารประกวดราคา	ให้คัดลอกคุณลักษณะเฉพาะและ/หรือ คุณสมบัติทางเทคนิคเบื้องต้นที่สำนักงานกำหนดมากรอกในนี้	ให้ระบุคุณลักษณะเฉพาะที่บริษัทฯ เสนอให้ชัดเจน ทั้งรุ่น และขนาด ต้องตรงกับเอกสารอ้างอิง	ระบุหมายเลขหน้าของเอกสารอ้างอิงของบริษัทฯ

6. ระยะเวลาในการดำเนินงาน/งวดงาน/เงื่อนไขการจ่ายเงิน/รายละเอียดของงานที่ส่งมอบ

สำนักงานจะพิจารณาเพื่อตรวจรับมอบงานเมื่อผู้เสนอราคาส่งมอบงานถูกต้องครบถ้วน ส่งมอบแผน อุปกรณ์ โปรแกรม ระบบงานและเอกสารต่าง ๆ ตามที่กำหนด โดยการจ่ายเงินจะกระทำได้ต่อเมื่อผ่านการตรวจรับมอบโดยคณะกรรมการตรวจรับฯ ของ กพท. ตามเงื่อนไขดังนี้ (ระยะเวลา 270 วัน)

งวดงานที่	ระยะเวลาดำเนินการ	การเบิกจ่ายเงิน	รายละเอียดของงานที่ส่งมอบต่อคณะกรรมการตรวจรับงาน
1	ภายใน 30 วัน นับจากวันลงนามในสัญญา	ร้อยละ 15 ของราคาตามสัญญา	- เมื่อส่งมอบแผนการดำเนินงานโดยละเอียด ประกอบด้วย แผนการดำเนินงาน ตารางกิจกรรม Network Diagram รายละเอียดคณะทำงานพร้อมระบุความรับผิดชอบ โดยจัดทำเป็นเอกสารรายงานจำนวน 5 ชุดพร้อมบันทึกรายงานลงซีดีให้กรรมการ
2	ภายใน 60 วัน นับจากวันลงนามในสัญญา	ร้อยละ 45 ของราคาตามสัญญา	เมื่อผู้เสนอราคาส่งมอบงาน ดังนี้ - **<u>ส่งมอบรายการอุปกรณ์ระบบตามข้อ 4.1 – 4.3</u>** เรียบร้อยแล้ว โดยจัดทำเป็นเอกสาร รายงาน จำนวน 5 ชุดพร้อมบันทึกรายงานลงซีดีส่งให้กรรมการ เอกสารการส่งมอบงานในแต่ละงวดงาน จัดทำรายการอุปกรณ์พร้อมระบุ Serial Number (ถ้ามี) ภาพถ่ายแสดงพื้นที่ก่อนเข้าและดำเนินการในแต่ละงวดงาน โดยจัดส่งเป็นเอกสารในรูปแบบกระดาษและไฟล์อิเล็กทรอนิกส์ที่สามารถแก้ไขและปรับปรุงได้
3	ภายใน 90 วัน นับจากวันลงนามในสัญญา	ร้อยละ 30 ของราคาตามสัญญา	เมื่อผู้เสนอราคาส่งมอบงาน ดังนี้ - **<u>ส่งมอบรายงานการติดตั้งระบบตามข้อ 4.1 – 4.4</u>** เรียบร้อยและส่งมอบคู่มือการอบรมการใช้งาน โดยจัดทำเป็นเอกสารรายงานจำนวน 5 ชุดพร้อมบันทึกรายงานลงซีดีส่งให้กรรมการ
4	ภายใน 270 วันนับจากวันลงนามในสัญญา	ร้อยละ 10 ของราคาตามสัญญา	- เมื่อส่งมอบเอกสารการดำเนินงาน คู่มือการบริหารจัดการระบบงานในโครงการ และจัดฝึกอบรมการบริหารจัดการอุปกรณ์คอมพิวเตอร์ และซอร์ฟแวร์ลิขสิทธิ์ พร้อมระบบงานที่เกี่ยวข้องโดยจัดทำเป็นเอกสารรายงานจำนวน 5 ชุดพร้อมบันทึกรายงานลงซีดีส่งให้กรรมการ

7. การรับประกันผลงาน

7.1. การรับประกันผลงาน ผู้ชนะการประกวดราคาจะต้องรับประกันความชำรุดบกพร่อง หรือความขัดข้องของอุปกรณ์ทั้งโครงการที่เกิดขึ้น เป็นระยะเวลารับประกัน 1 ปี นับจากวันที่ส่งมอบงวดสุดท้าย

7.2. การบำรุงรักษาและซ่อมแซมแก้ไขภายในกำหนดเวลารับประกันผลงาน ผู้ชนะการประกวดราคาจะต้องบำรุงรักษาอุปกรณ์ที่จัดซื้อ ทั้งโครงการ โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น เมื่อเกิดข้อผิดพลาด หรือขัดข้องอันเนื่องจากการใช้งานตามปกติ ผู้ชนะการประกวดราคาจะต้องรับจัดการซ่อมแซมหรือแก้ไขให้อยู่ในสภาพใช้งานได้ดังเดิม ให้แล้วเสร็จเบื้องต้นภายใน 3 วันทำการ นับแต่เวลารับแจ้ง

8. อัตราค่าปรับ

ผู้ขายไม่ปฏิบัติตามสัญญาหรือผิดสัญญาข้อหนึ่งข้อใด และ กพท. ยังไม่ได้บอกเลิกสัญญา ผู้ขายจะต้องถูกปรับเป็นรายวันในอัตราร้อยละ 0.1 ของราคาจัดซื้อ นับแต่วันที่ล่วงเลยกำหนดวันแล้วเสร็จตามสัญญาจนถึงวันที่ส่งมอบงานครบถ้วนเรียบร้อย

9. ลิขสิทธิ์ซอฟต์แวร์

ลิขสิทธิ์ในซอฟต์แวร์ทั้งหมด ตลอดจนกรรมสิทธิ์คู่มือ หรือเอกสารต่างๆ ทั้งหมด ให้ตกเป็นของ กพท. ทันทีที่มีการส่งมอบ จนถึงสิ้นสุดระยะเวลารับประกัน

10. ปัญหาข้อขัดแย้งและการตีความ

ในกรณีที่มีความจำเป็นต้องตีความข้อใด หรือมีข้อความใดที่ขัดแย้งในประกาศประกวดราคาหรือเอกสารเสนอราคา หรือเอกสารอื่นใดก็ตาม ซึ่งมีความจำเป็นต้องวินิจฉัยตัดสินในการประกวดราคาเป็นไปด้วยความเรียบร้อย และบรรลุวัตถุประสงค์ สำนักงานการบินพลเรือนแห่งประเทศไทยสงวนสิทธิ์ที่จะเป็นผู้ตีความและวินิจฉัยข้อขัดแย้ง ซึ่งให้ถือเป็นอันเด็ดขาดและถึงที่สุด

11. วงเงินในการจัดหา

วงเงินงบประมาณ เป็นเงิน 2,800,000.00 บาท (สองล้านแปดแสนบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม 7% ไว้ด้วยแล้ว วงเงินราคากลาง 2,795,737.91 บาท ผู้เสนอราคาจะต้องเสนอราคาขั้นต่ำ (Minimum Bid) ไม่น้อยกว่าครั้งละ 5,000.00 บาท จากราคาสูงสุดในการประกวดราคาฯ และการเสนอลดราคาครั้งถัดๆไป ต้องเสนอ ลดราคาครั้งละไม่น้อยกว่า 5,000.00 บาท จากราคาครั้งสุดท้ายที่เสนอ

12. หน่วยงานผู้รับผิดชอบ

ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานการบินพลเรือนแห่งประเทศไทย

หมายเหตุ ทั้งนี้หากผู้ประสงค์เสนอราคามีข้อเสนอแนะ ข้อคิดเห็น สามารถส่งมาได้ที่ www.caat.or.th

ลงชื่อ ..... (ประธานกรรมการ)
(นายศุภกร จันทร์ญาโณทัย)

ลงชื่อ ..... (กรรมการ)
(นายวีระ ระบายศรี)

ลงชื่อ ..... (กรรมการ)
(นายประมุข นิภารักษ์)

ลงชื่อ ..... (กรรมการ)
(นางสาวภมรรัตน์ สุนทร)