ข้อกำหนด และขอบเขตของงาน
จ้างตรวจสอบช่องโหว่และประเมินความมั่นคงปลอดภัยเครือข่ายของ สป.อว.

---

1. หลักการและเหตุผล

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564 มีการกำหนดให้มีการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology : IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) รวมถึงให้มีการทดสอบเจาะระบบของโฮสต์ เครือข่ายและแอปพลิเคชันของบริการสำคัญโดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง และควรมีการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการเตรียมความพร้อมและยกระดับการตรวจสอบการบุกรุกตามลักษณะภัยไซเบอร์ที่มากขึ้นผ่านการจำลองการโจมตีเสมือนจริงที่เป็นที่นิยมใช้ในอุตสาหกรรม โดยมีความใกล้เคียงกับสถานการณ์การโจมตีที่เกิดขึ้นจากผู้ไม่หวังดี (Hacker) และสามารถตรวจสอบความพร้อมของบุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ให้มีความสอดคล้องกับสถานการณ์ภัยคุกคามปัจจุบัน เพื่อนำไปปรับปรุงระบบและกระบวนการรักษาความปลอดภัยอย่างเป็นระบบ เป็นรูปธรรม และนำไปปฏิบัติได้จริง

กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม (กรข.) สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) จึงมีความจำเป็นต้องเช่าใช้บริการระบบตรวจสอบช่องโหว่และประเมินความมั่นคงปลอดภัยระบบเครือข่ายและระบบสารสนเทศเพื่อตรวจสอบช่องโหว่และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของ สป.อว. ให้สามารถให้บริการได้อย่างต่อเนื่อง ลดความเสี่ยงที่อาจเกิดจากภัยคุกคามทางไซเบอร์ และช่องโหว่ในรูปแบบต่างๆ ได้อย่างมีประสิทธิภาพต่อไป และสอดคล้องตามประมวลและแนวทางปฏิบัติฯ ดังกล่าวข้างต้น

2. วัตถุประสงค์

2.1 เพื่อตรวจสอบช่องโหว่ของระบบสารสนเทศ และระบบเครือข่ายของ สป.อว.

2.2 เพื่อจำลองสถานการณ์โจมตีจริงด้วยการทดสอบฟิชชิง (Phishing Simulation) เพื่อวัดผลการตอบสนองของบุคลากร และปรับปรุงแผนรับมือให้มีประสิทธิภาพมากยิ่งขึ้น

2.3 เพื่อยกระดับความมั่นคงปลอดภัยสารสนเทศในการป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ต่อทรัพยากรข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่ายที่สำคัญของ สป.อว.

3. **คุณสมบัติผู้ยื่นข้อเสนอ**

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

3.11 ผู้ยื่นข้อเสนอต้องเป็นตัวแทนที่ได้รับการแต่งตั้งอย่างเป็นทางการ ให้มีสิทธิ์ในการจำหน่ายและบริการหลังการขายจากบริษัทผู้ผลิต หรือตัวแทนจำหน่ายผู้ผลิตในประเทศไทยสำหรับโครงการนี้ โดยแนบเอกสารดังกล่าวในวันยื่นข้อเสนอด้วย

3.12 ผู้ให้บริการจะต้องจัดให้มีบุคลากรที่มีความรู้ความชำนาญเพื่อดำเนินงานตามขอบเขตงาน โดยมีคุณวุฒิ ประสบการณ์ และจำนวนอย่างน้อย ดังนี้

3.12.1 หัวหน้าโครงการ วุฒิการศึกษาไม่ต่ำกว่า ปริญญาตรี สาขาวิศวกรรมศาสตร์ หรือ สาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ หรือสาขาที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ ที่มีประสบการณ์อย่างน้อย 10 ปี และมีประสบการณ์ในการบริหารโครงการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ จำนวน 1 คน

3.12.2 ผู้ทดสอบเจาะระบบ วุฒิการศึกษาไม่ต่ำกว่า ปริญญาตรี สาขาวิศวกรรมศาสตร์ หรือสาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์การทำงานอย่างน้อย 2 ปี จำนวน 1 คน และได้รับประกาศนียบัตรอย่างน้อย 1 ใบ ได้แก่ Offensive Security Certified Professional (OSCP) หรือ CompTIA Pentest+ หรือ CompTIA CySA+ หรือ CompTIA SEC+

4. รายละเอียดคุณลักษณะเฉพาะด้านเทคนิค

4.1. สิทธิ์การใช้งานซอฟต์แวร์ประเมินและตรวจสอบช่องโหว่ภายในเครือข่าย จำนวน 1 ชุด

4.1.1 มีสิทธิ์การใช้งานที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย เป็นระยะเวลาไม่น้อยกว่า 1 ปี

4.1.2 โปรแกรมที่นำเสนอต้องถูกออกแบบมาเพื่อทำหน้าที่ตรวจสอบและประเมินความเสี่ยงจากช่องโหว่ (Vulnerability) โดยเฉพาะ

4.1.3 รองรับการตรวจหาช่องโหว่ในระบบได้แบบไม่จำกัดจำนวนอุปกรณ์ IP Address

4.1.4 สามารถบริหารจัดการได้ผ่าน Web Based GUI แบบ HTTPS

4.1.5 รองรับการตรวจสอบ (Scan) ได้หลากหลาย เช่น แบบ non-credentialed หรือ credentialed ได้

4.1.6 สามารถตรวจสอบช่องโหว่ภายในระบบเครือข่ายผ่าน IPv4 หรือ IPv6 ได้

4.1.7 สามารถทำการตรวจสอบช่องโหว่ของอุปกรณ์เครือข่าย เช่น Cisco, Juniper, HP, F5 และ SonicWall ได้

4.1.8 สามารถทำการตรวจสอบช่องโหว่ของระบบฐานข้อมูลได้ เช่น Oracle หรือ SQL Server หรือ MySQL ได้

4.1.9 สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการคอมพิวเตอร์ เช่น Windows, MacOS, และ Linux (Ubuntu) ได้

4.1.10 สามารถตรวจสอบช่องโหว่ของ Web application (Web application scans) ได้

4.1.11 สามารถทำการตั้งเวลาการ Scan ล่วงหน้าได้

4.1.12 มี Templates สำหรับทำการตรวจสอบ compliance และ configuration

4.1.13 สามารถแจ้งเตือนการสแกนผ่านช่องทาง Email ได้

4.1.14 มีฐานข้อมูลของช่องโหว่ (Plugin) ไม่น้อยกว่า 250,000 Plugins

4.1.15 มีฐานข้อมูลของช่องโหว่ที่ครอบคลุมมาตรฐาน CVE ไม่น้อยกว่า 100,000 CVE IDs

4.1.16 สามารถอัปเดตฐานข้อมูลของช่องโหว่ได้โดยอัตโนมัติ

4.1.17 สามารถรองรับการสแกนในรูปแบบของ External Attack Surface Scans ได้

4.1.18 รองรับการ Scan ในการหาช่องโหว่โดยอ้างอิงมาตรฐานด้านความปลอดภัย เช่น DISA หรือ CIS หรือ PCI ได้

4.1.19 มีการจัดลำดับคะแนนความเสี่ยงของช่องโหว่ตามมาตรฐาน CVSS และจัดลำดับความรุนแรง ได้แก่ Critical, High, Medium, Low และ Info

4.1.20 สามารถออกรายงานในรูปแบบ HTML หรือ CSV formats ได้

4.1.21 มีกระบวนการในการจัดลำดับความสำคัญของช่องโหว่ โดยอาศัยการวิเคราะห์เชิงลึกและการคาดการณ์ (Vulnerability Priority Rating) ได้

5. ขอบเขตการดำเนินงาน

5.1. ศึกษา วิเคราะห์ และจัดทำรายงานผลการศึกษาเบื้องต้น (Inception Report) โดยมีเนื้อหาประกอบด้วย วิธีการ รูปแบบ และเครื่องมือที่เหมาะสมสำหรับจะนำมาใช้ในการประเมินช่องโหว่ การทดสอบการเจาะระบบ (Vulnerability Assessment and Penetration Testing) และการจำลองการโจมตีเสมือนจริง รวมถึงการจำลองสถานการณ์การโจมตี Phishing Simulation เพื่อกำหนดแนวทางการดำเนินงานโครงการ พร้อมทั้งจัดทำแผนการดำเนินงานที่เหมาะสม

5.2. ดำเนินการติดตั้งโปรแกรมหรือซอฟต์แวร์ต่างๆ ที่ได้นำเสนอในโครงการนี้ ให้สามารถใช้งานได้และตรงตามคุณสมบัติที่ระบุไว้ข้างต้น โดยในระหว่างการติดตั้งซอฟต์แวร์ที่นำเสนอภายในโครงการนี้ จะต้องไม่มีผลกระทบต่อการทำงานของระบบงานต่างๆ หรือก่อให้เกิดความเสียหายแก่ สป.อว. ทั้งนี้ หากเกิดผลกระทบหรือความเสียหาย ผู้รับจ้างต้องเป็นผู้ดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติ และรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

5.3. ดำเนินการจัดทำคู่มือการติดตั้ง (Configuration) และคู่มือการใช้งานซอฟต์แวร์ พร้อมรูปประกอบอย่างละเอียด ให้กับ สป.อว.

5.4. ก่อนเข้าดำเนินการในแต่ละครั้ง ต้องแจ้งแผนการเข้าดำเนินงาน รายละเอียดการดำเนินการ เครื่องมือที่ใช้ โปรแกรมที่เกี่ยวข้อง และวิธีการทดสอบ รวมถึงการประเมินผลกระทบที่อาจมีขึ้น เพื่อป้องกันไม่ให้เกิดความเสียหายต่อระบบที่ทดสอบ ให้ทราบล่วงหน้าอย่างน้อย 5 วันทำการ และจะดำเนินการได้หลังจากที่ได้รับความเห็นชอบจาก สป.อว.

5.5. ดำเนินการประเมินช่องโหว่และทดสอบเจาะระบบ เครือข่ายภายในของ สป.อว. (Internal Penetration Testing and Vulnerabilities Assessment) มีขั้นตอนหรือกระบวนการอย่างน้อยดังต่อไปนี้

1) ตรวจการเข้าถึงเครือข่ายภายใน (Internal Network Reconnaissance) อย่างน้อยดังนี้
   - Administrator Desktops
   - Active Directory Services
   - Routing Infrastructure
   - Key Internal Websites
   - การเดาสุ่ม Username และ Password

2) ตรวจสอบช่องโหว่ของเครือข่ายภายในจะต้องครอบคลุมในระดับระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ในระบบเครือข่าย (Network Equipment) และอุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) ของ สป.อว. จำนวนไม่น้อยกว่า 500 หมายเลขไอพี (Internal Vulnerability Assessment) โดยครอบคลุมอย่างน้อยดังนี้
   - Execute vulnerability and port scanning assessments
   - Scanning vulnerability and port from internal network
   - Exploitation frameworks (where appropriate)
   - Open ports
   - Misconfiguration
   - The presence of known vulnerabilities and/or system weaknesses

3) ดำเนินการทดสอบเจาะระบบจากเครือข่ายภายในของ สป.อว. แบบ Grey-box Test ให้ดำเนินการโดยอ้างอิงตามมาตรฐาน NIST SP800-115 และใช้ Version ล่าสุดที่มีการประกาศในการใช้งาน

4) ดำเนินการทดสอบหาช่องทางในการเจาะเข้าถึงเครือข่ายเทคโนโลยีสารสนเทศของ สป.อว. (Internal Penetration Testing) อย่างน้อยดังนี้

- Port scanning
- Vulnerability scanning
- Exploitation frameworks (where appropriate)
- Identification and Authentication Failures
- Vulnerable and Outdated Components

5) ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test)

6) ดำเนินการทดสอบเจาะระบบไม่ให้กระทบกับการใช้งานระบบเทคโนโลยีสารสนเทศ โดยระหว่างการทดสอบเจาะระบบหากเกิดความผิดปกติของระบบที่ทำการทดสอบ จะต้องรีบแก้ไขและแจ้งให้บุคลากรของ สป.อว. ทราบทันที

5.6. ดำเนินการตรวจสอบช่องโหว่และทดสอบเจาะระบบเว็บแอปพลิเคชัน (Vulnerabilities Assessment & Web Application Penetration test) จำนวน 10 Web Application โดยตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Web Application Security Assessment) โดยครอบคลุมอย่างน้อยดังนี้

1) ทดสอบเจาะระบบเว็บแอปพลิเคชันทั้งแบบ Grey Box ให้ดำเนินการโดยอ้างอิงตาม Open Web Application Security Project (OWASP) Testing guide และใช้ Version ล่าสุดที่มีการประกาศในการใช้งาน

2) ดำเนินการทดสอบเจาะระบบเว็บแอปพลิเคชันแบบ Grey Box ในการทดสอบจะดำเนินการเหมือนกับการเจาะระบบโดยไวรัสหรือแฮกเกอร์ที่ปฏิบัติการจริง และทดสอบหาช่องทางในการเข้าถึงระบบ (Exploit) ผ่านช่องโหว่ต่าง ๆ โดยคลอบคลุมรายละเอียดดังนี้

- External assessment (identification of application security issues via Internet presented applications or through simulated-external applications as applicable)
- Testing from the perspective of an unregistered user – 'Black Box' testing
- Review of the ability to withstand attacks from injected or manipulated code
- Assess scenarios through which a non-load-based denial of service condition can be introduced
- Assess user access controls, user segregation and authentication

- Attempt to gain unauthorized access to data, to modify data without authority, or to otherwise compromise the security model implemented by the system

3) ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test)

4) ดำเนินการทดสอบเจาะระบบไม่ให้กระทบกับการใช้งานระบบเทคโนโลยีสารสนเทศ โดยระหว่างการทดสอบเจาะระบบ หากเกิดความผิดปกติของระบบที่ทำการทดสอบจะต้องรีบแก้ไขและแจ้งให้เจ้าหน้าที่ ให้ทราบทันที

5.7. วิเคราะห์และประเมินผลพฤติการณ์แวดล้อม ผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ ผลจากการทดสอบเจาะระบบ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใดเทียบเคียงกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 พร้อมทั้งประชุมชี้แจงผลการทดสอบและวิเคราะห์การเจาะระบบ ที่มีผลกระทบในระดับวิกฤต (Critical) และระดับสูง (High) พร้อมข้อเสนอแนะและแนวทางการแก้ไขโดยละเอียด

5.8. ให้คำปรึกษาและดำเนินการจัดทำรายงานผลการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่และการเจาะเข้าถึงเครือข่ายและระบบเทคโนโลยีสารสนเทศ โดยรายงานจะต้องมีเนื้อหาสาระประกอบไปด้วยอย่างน้อย ดังนี้

- บทสรุปผู้บริหาร
- วิธีการและขั้นตอนการทดสอบ
- รายละเอียดช่องโหว่ พร้อมประเมินความรุนแรงของช่องโหว่
- คำแนะนำในการปิดช่องโหว่

5.9. ให้คำปรึกษาและดำเนินการจัดทำแนวทางในการปรับปรุงแก้ไขระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศ ให้มีความมั่นคงปลอดภัยสอดคล้องตามมาตรฐานสากล โดยอ้างอิงจากรายงานผลการประเมินความเสี่ยงที่เกิดจากช่องโหว่และการเจาะเข้าถึงเครือข่ายและระบบเทคโนโลยีสารสนเทศ

5.10. ดำเนินการตรวจสอบซ้ำช่องโหว่ที่ได้มีการตรวจพบ และได้รับการแก้ไขแล้วจากเจ้าหน้าที่ พร้อมรายงานฉบับสมบูรณ์

5.11. ดำเนินการสร้างและจำลองฟิชชิงได้หลายรูปแบบ จำนวนไม่น้อยกว่า 4 ครั้ง (ทุก 3 เดือน) โดยสามารถรองรับผู้ใช้งานได้ไม่น้อยกว่า 800 คน พร้อมรายงานในรูปแบบของสถิติ หรือแสดงผลรวมข้อมูลผลการทดสอบ (Phishing Simulation Results)

6. การส่งมอบงาน

6.1. ผู้เสนอราคาจะต้องดำเนินการส่งมอบงานหลังครบกำหนดการปฏิบัติงานสิ้นสุดของแต่ละงวดงาน ภายในระยะเวลา 7 วันทำการ ต้องจัดทำเอกสารรายงานการบำรุงรักษาฯ ในรูปแบบเอกสาร จำนวน 2 ชุด และรูปแบบ Electronic File (USB) จำนวน 1 ชุด พร้อมส่งให้ทาง สป.อว. เป็นรายงวด (งวดละ 3 เดือน) รวม 4 งวด โดยมีรายงานผลการดำเนินการ ดังต่อไปนี้

- **เอกสารรายงาน (ในงวดที่ 1)** ประกอบด้วยรายละเอียดดังนี้
  - แผนการดำเนินงานโครงการ
  - รายงานผลการทดสอบ Phishing Simulation ครั้งที่ 1
  - รายละเอียดการกำหนดค่าการใช้งาน (System Configuration)
  - คู่มือการติดตั้ง (Configuration) และคู่มือการใช้งานซอฟต์แวร์ พร้อมรูปประกอบ
  - รายงานผลการเข้าดำเนินการ ประจำงวด
  - สรุปรายการเอกสารการเปลี่ยนแปลงการตั้งค่าของระบบ (Change Report) ประจำเดือน (หากมี)
- **เอกสารรายงาน (ในงวดที่ 2)** ประกอบด้วยรายละเอียดดังนี้
  - รายงานผลการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่และการเจาะเข้าถึงเครือข่ายและระบบเทคโนโลยีสารสนเทศ ครั้งที่ 1
  - รายงานผลการทดสอบ Phishing Simulation ครั้งที่ 2
  - รายงานผลการเข้าดำเนินการ ประจำงวด
  - สรุปรายการเอกสารการเปลี่ยนแปลงการตั้งค่าของระบบ (Change Report) ประจำเดือน (หากมี)
- **เอกสารรายงาน (ในงวดที่ 3)** ประกอบด้วยรายละเอียดดังนี้
  - รายงานผลการทดสอบ Phishing Simulation ครั้งที่ 3
  - รายงานผลการเข้าดำเนินการ ประจำงวด
  - สรุปรายการเอกสารการเปลี่ยนแปลงการตั้งค่าของระบบ (Change Report) ประจำเดือน (หากมี)
- **เอกสารรายงาน (ในงวดที่ 4)** ประกอบด้วยรายละเอียดดังนี้
  - รายงานผลการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่และการเจาะเข้าถึงเครือข่ายและระบบเทคโนโลยีสารสนเทศ ครั้งที่ 2
  - รายงานผลการทดสอบ Phishing Simulation ครั้งที่ 4
  - รายงานผลการเข้าดำเนินการ ประจำงวด
  - สรุปรายการเอกสารการเปลี่ยนแปลงการตั้งค่าของระบบ (Change Report) ประจำเดือน (หากมี)

6.2. หากเอกสารส่งมอบประกอบไปด้วยข้อมูลที่สำคัญของหน่วยงาน อาทิเช่น หมายเลขและ IP Address เอกสารการกำหนดค่าต่างๆ ของโปรแกรมหรือระบบ เอกสารลิขสิทธิ์ (License) ของอุปกรณ์หรือระบบ ข้อมูลส่วนบุคคล รวมถึงบัญชีและรหัสผ่านของผู้ใช้งานระบบสารสนเทศระดับผู้ใช้งานทั่วไป เป็นต้น ผู้ให้บริการต้องจัดทำป้ายแสดงระดับชั้นความลับ ให้มีตราหรือเครื่องหมายหรือชื่อขององค์กร และมีข้อความระบุว่า "Confidential" หรือคำว่า "ลับ" จำนวน 1 ชุดบนเอกสาร และจัดทำเอกสารรูปแบบเฉพาะที่ปิดบังข้อมูลที่สำคัญของหน่วยงาน โดยมีข้อความว่า "Internal Use" หรือคำว่า "ใช้ภายใน" จำนวน 1 ชุดบนเอกสาร ที่จะจัดส่งให้กับทาง สป.อว. (รวมทั้งหมด 2 ชุด) และข้อมูลแบบ Electronic File (USB) ซึ่งต้องทำการเข้ารหัสข้อมูล (Encrypted) เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญ โดยต้องมีข้อความระบุว่า "Confidential" หรือ "ลับ" บนซองเอกสารทึบแสงที่ปิดผนึกเรียบร้อยนำส่งมอบให้กับทาง สป.อว. จำนวน 2 ชุด พร้อมดำเนินการส่งรหัสผ่าน ให้กับผู้ดูแลระบบผ่านทางช่องทางตามที่ สป.อว. เป็นผู้กำหนด ด้วยโปรแกรม WinZip หรือ 7Zip เป็นต้น

6.3. หากเอกสารส่งมอบประกอบไปด้วยข้อมูลสำคัญที่ส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายของ สป.อว. อาทิเช่น ผลการตรวจสอบช่องโหว่ (VA), ผลการทดสอบเจาะระบบ (PenTest), และบัญชีและรหัสผ่านของผู้ใช้งานระบบสารสนเทศ ระดับผู้ดูแลระบบ เป็นต้น ผู้ให้บริการต้องจัดทำป้ายแสดงระดับชั้นความลับ ให้มีตราหรือเครื่องหมาย หรือชื่อขององค์กร และมีข้อความระบุว่า "Secret" หรือคำว่า "ลับมาก" จำนวน 1 ชุดบนเอกสาร และข้อมูลแบบ Electronic File (USB) ซึ่งต้องทำการเข้ารหัสข้อมูล (Encrypted) เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญ โดยต้องมีข้อความระบุว่า "Secret" หรือ "ลับมาก" บนซองเอกสารทึบแสงที่ปิดผนึกเรียบร้อยนำส่งมอบให้กับทาง สป.อว. จำนวน 1 ชุด พร้อมดำเนินการส่งรหัสผ่าน ให้กับผู้ดูแลระบบผ่านทางช่องทางตามที่ สป.อว. เป็นผู้กำหนด ด้วยโปรแกรม WinZip หรือ 7Zip เป็นต้น

7. การปฏิบัติตามนโยบายด้าน ICT ของ สป.อว.

ผู้ให้บริการหรือเจ้าหน้าที่ที่ของผู้ให้บริการจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของ สป.อว. และขั้นตอนปฏิบัติต่างๆ ตามนโยบาย ISO 27001:2022 รวมถึงคำสั่งและวิธีปฏิบัติที่เกี่ยวข้องอย่างเคร่งครัด

8. การปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement)

ผู้ให้บริการหรือเจ้าหน้าที่ของผู้ให้บริการจะต้องดำเนินการลงนามการปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement) ให้กับ สป.อว. สำหรับโครงการนี้ เพื่อเป็นการรักษาความลับทางด้านข้อมูลไม่ให้รั่วไหลสู่สาธารณะโดยไม่ได้รับอนุญาต

9. ระยะเวลาการรับประกัน

9.1. มีสิทธิ์การใช้งานและการรับประกันผลิตภัณฑ์ซอฟต์แวร์ที่นำเสนอในโครงการนี้ทั้งหมด เป็นระยะเวลาไม่น้อยกว่า 1 ปี ในกรณีที่เกิดปัญหาเมื่อได้รับแจ้งปัญหาทาง E-mail หรือทางโทรศัพท์ ผู้เสนอราคาต้องให้คำปรึกษา แก้ไขปัญหาเบื้องต้นทางโทรศัพท์ ซึ่งต้องถือปฏิบัติในระยะเวลาประกัน

9.2. ผู้เสนอราคาต้องเป็นผู้ประสานงานหลักในการแก้ไขปัญหา กรณีที่มีการแจ้งปัญหาการใช้งานไปยังบริษัทเจ้าของผลิตภัณฑ์ที่นำเสนอในโครงการนี้ กรณีหากมีค่าใช้จ่ายเกิดขึ้น ทางผู้เสนอราคาต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ซึ่งต้องถือปฏิบัติในระยะเวลาการรับประกัน

10. เงื่อนไขการชำระเงิน

ทาง สป.อว. จะชำระเงินค่าดำเนินการเป็นรายงวด (งวดละ 3 เดือน/ครั้ง) รวม 4 งวด ดังนี้

- **งวดที่ 1** ชำระเงิน 40% ของมูลค่าตามสัญญา เมื่อผู้รับจ้างได้ดำเนินการส่งมอบเอกสารรายงาน (ในงวดที่ 1) เรียบร้อย ให้แก่คณะกรรมการตรวจรับพัสดุของสำนักงานฯ และเมื่อคณะกรรมการตรวจรับฯ เห็นว่าผู้รับจ้างดำเนินการได้ถูกต้องครบถ้วนตามรายละเอียดและเงื่อนไขในข้อตกลงจ้างหรือสัญญาจ้างแล้ว สำนักงานฯ จึงจะดำเนินการเบิกจ่ายเงินให้ผู้รับจ้างต่อไป
- **งวดที่ 2** ชำระเงิน 20% ของมูลค่าตามสัญญา เมื่อผู้รับจ้างได้ดำเนินการส่งมอบเอกสารรายงาน (ในงวดที่ 2) เรียบร้อย ให้แก่คณะกรรมการตรวจรับพัสดุของสำนักงานฯ และเมื่อคณะกรรมการตรวจรับฯ เห็นว่าผู้รับจ้างดำเนินการได้ถูกต้องครบถ้วนตามรายละเอียดและเงื่อนไขในข้อตกลงจ้างหรือสัญญาจ้างแล้ว สำนักงานฯ จึงจะดำเนินการเบิกจ่ายเงินให้ผู้รับจ้างต่อไป
- **งวดที่ 3** ชำระเงิน 20% ของมูลค่าตามสัญญา เมื่อผู้รับจ้างได้ดำเนินการส่งมอบเอกสารรายงาน (ในงวดที่ 3) เรียบร้อย ให้แก่คณะกรรมการตรวจรับพัสดุของสำนักงานฯ และเมื่อคณะกรรมการตรวจรับฯ เห็นว่าผู้รับจ้างดำเนินการได้ถูกต้องครบถ้วนตามรายละเอียดและเงื่อนไขในข้อตกลงจ้างหรือสัญญาจ้างแล้ว สำนักงานฯ จึงจะดำเนินการเบิกจ่ายเงินให้ผู้รับจ้างต่อไป
- **งวดที่ 4** ชำระเงิน 20% ของมูลค่าตามสัญญา เมื่อผู้รับจ้างได้ดำเนินการส่งมอบเอกสารรายงาน (ในงวดที่ 4) เรียบร้อย ให้แก่คณะกรรมการตรวจรับพัสดุของสำนักงานฯ และเมื่อคณะกรรมการตรวจรับฯ เห็นว่าผู้รับจ้างดำเนินการได้ถูกต้องครบถ้วนตามรายละเอียดและเงื่อนไขในข้อตกลงจ้างหรือสัญญาจ้างแล้ว สำนักงานฯ จึงจะดำเนินการเบิกจ่ายเงินให้ผู้รับจ้างต่อไป

11. งบประมาณ

วงเงินงบประมาณ 1,500,000 บาท (หนึ่งล้านห้าแสนบาทถ้วน)

12. ระยะเวลาดำเนินการ

ตั้งแต่เดือนตุลาคม 2569 ถึงเดือนกันยายน 2570

13. หลักเกณฑ์การพิจารณา

เกณฑ์การพิจารณาผู้ชนะการเสนอราคา ใช้เกณฑ์ราคาและพิจารณาจากราคารวม

14. ค่าปรับ

หากผู้รับจ้างไม่สามารถส่งมอบให้แล้วเสร็จตามเวลาที่กำหนดไว้ ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ทาง สป.อว. เป็นรายวันอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของมูลค่างวดงานที่ยังไม่ได้รับมอบ นับถัดจากวันครบกำหนดส่งมอบจนถึงวันที่ผู้ให้บริการได้ส่งมอบงานจนถูกต้องครบถ้วน

15. กำหนดยืนราคา 90 วัน

16. สถานที่ส่งมอบพัสดุ

สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม เลขที่ 75/47 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร โทร. 0 2333 3811

(นายทวีศักดิ์ นาเมืองรักษ์)	(นางสาวศุภกร สาระวงศ์)	(นายกิติศักดิ์ วงศ์ธานุวัฒน์)
นักวิชาการคอมพิวเตอร์ชำนาญการ	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	เจ้าหน้าที่ระบบงานคอมพิวเตอร์
ผู้กำหนดคุณลักษณะเฉพาะ	ผู้กำหนดคุณลักษณะเฉพาะ	ผู้กำหนดคุณลักษณะเฉพาะ