ข้อกำหนด และขอบเขตของงาน
เช่าระบบตรวจสอบและป้องกัน Web Application
และควบคุมการเข้าถึงการใช้งานระบบสารสนเทศ ของ สป.อว. (อาคารพระจอมเกล้า)
ประจำปีงบประมาณ พ.ศ. 2566

---

1. หลักการและเหตุผล

ด้วย กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (กรข.) สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) ได้ดำเนินการบริหารจัดการระบบรักษาความมั่นคงปลอดภัยสารสนเทศ ให้สอดคล้อง เป็นไปตามมาตรฐานความมั่นคงปลอดภัย ISO/IEC27001:2013 โดยมุ่งเน้นการปกป้องข้อมูลสารสนเทศ ให้ธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วนสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) เพื่อให้การดำเนินการตรวจสอบติดตาม และป้องกัน มีประสิทธิภาพสูงสุด รวมถึงการบริหารจัดการทรัพยากรและต้นทุนเป็นไปอย่างคุ้มค่า ลดความซ้ำซ้อน และลดความเสี่ยงอันอาจจะเกิดจากการโจมตีจาก Attack vector ต่างๆ

ปัจจุบัน กรข. ได้ดำเนินการขยายขอบเขตมาตรฐานการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ สป.อว. ไปยังศูนย์ข้อมูลสารสนเทศ (อาคารอุดมศึกษา 1) ซึ่งจะต้องมีการทบทวนมาตรการการกำกับดูแล การบริหารจัดการความเสี่ยง ตลอดจนข้อปฏิบัติตามหลักการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (State of Applicability : SoA) ทั้งในส่วนของการจัดการ, การบริหาร, และวิธีการทางเทคนิค เพื่อให้ Data Center ทั้ง 2 แห่งเป็นไปตามมาตรฐานและวัตถุประสงค์ดังกล่าวข้างต้น โดยหากนำอุปกรณ์ตรวจสอบและป้องกันภัยคุมคามที่มีอยู่เดิมมาใช้งาน จำเป็นต้องมีการขยายทั้งในส่วนของอุปกรณ์ Hardware เพิ่มเติม และค่าใช้จ่าย Subscription license เพื่อให้ครอบคลุมกับปริมาณ Throughput และจำนวนผู้ใช้งานของทั้ง 2 ฝั่ง ซึ่งจะมีค่าใช้จ่ายเริ่มต้น และภาระผูกพันธ์ในการ Maintenance ระบบตามมาในภายหลัง.

ในการนี้ กรข. จึงจำเป็นต้องเช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามสารสนเทศของ สป.อว. เพื่อให้สามารถตรวจสอบ ป้องกัน และควบคุมการเข้าถึงการใช้งานระบบสารสนเทศ โดยมีเทคโนโลยีที่ทันสมัยมาป้องกัน และควบคุมการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ของ สป.อว. ได้อย่างมีประสิทธิภาพ สามารถบริหารต้นทุนด้านเทคโนโลยีได้อย่างมีนัยสำคัญ และยังคงมีมาตรการทางด้านความมั่นคงปลอดภัยเพื่อให้สอดคล้องและเป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเริ่มตั้งแต่เดือนตุลาคม 2565 ถึงเดือนกันยายน 2566 รวมระยะเวลา 12 เดือน

2. วัตถุประสงค์

2.1. เพื่อการบริหารจัดการทรัพยากรและงบประมาณเกิดความคุ้มค่า และลดความซ้ำซ้อน
2.2. เพื่อให้คงไว้ซึ่งมาตรการกำกับดูแลการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013
2.3. เพื่อรองรับการขยายขอบเขตมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 ไปยังอาคารอุดมศึกษา 1 และ 2
2.4. เพื่อลดความเสี่ยงจากการโจมตีจาก Attack Vector ต่างๆ

3. คุณสมบัติของผู้เสนอราคา

3.1. มีความสามารถตามกฎหมาย

3.2. ไม่เป็นบุคคลล้มละลาย

3.3. ไม่อยู่ระหว่างเลิกกิจการ

3.4. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

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 หรือสาขาผู้ผลิตในประเทศไทยสำหรับโครงการนี้ โดยแนบเอกสารดังกล่าวในวันยื่นข้อเสนอด้วย ทั้งนี้ ดูรายละเอียดอุปกรณ์ข้างต้นได้ ที่เอกสารข้อกำหนดและขอบเขตของงานฯ

3.12. ผู้เสนอราคาต้องมีทีมงาน หรือพนักงานประจำ ที่มีความรู้ความเชี่ยวชาญด้าน Cyber Security เป็นอย่างดี โดยได้รับประกาศนียบัตร Certified Ethical Hacker (CEH) หรือ CompTIA CySA+ อย่างน้อย 1 ท่าน โดยแนบสำเนาเอกสารดังกล่าวในวันยื่นข้อเสนอด้วย

4. ขอบเขตการดำเนินงาน

ผู้ให้บริการจะต้องดำเนินการจัดหาระบบตรวจสอบและป้องกัน Web Application และควบคุมการเข้าถึงการใช้งานระบบสารสนเทศ ดังต่อไปนี้

4.1. ระบบป้องกันการโจมตีและการเข้าถึงเว็บไซต์และเครือข่าย

4.1.1. สามารถป้องกันเว็บแอพพลิเคชัน (Web Application Firewall) โดยมีคุณลักษณะเฉพาะด้านเทคนิค ดังต่อไปนี้

- สามารถแสดงรายงานบน Security Dashboard แบบ Real-time หรือ Near Real-time โดยสามารถแสดงถึงข้อมูลแหล่งที่มาของการโจมตี เช่น IP Addresses, User Agents, Countries และ ASNs ได้
- สามารถป้องกันการโจมตีผ่านทาง Website ตาม OWASP TOP 10 เช่น SQL injection, Broken Authentication, Cross-site Scripting ได้
- สามารถตั้งค่า Web Application Firewall (WAF) ได้แบบไม่จำกัดจำนวน (Unlimited Custom WAF rules) และการตั้งค่าการเปิดปิด WAF Rule ต้องมีผลบังคับใช้ (Effective) ภายในเวลาไม่เกิน 30 วินาที
- สามารถตั้งค่า IP Firewall โดยสามารถกำหนดเงื่อนไขด้วย IP address, IP address range, Autonomous System Number (ASN) or country ได้
- สามารถตั้งค่า Rate Limit Rules ซึ่งสามารถกำหนดการป้องกันการเข้าถึง Website ได้ไม่น้อยกว่า 100 rules
- สามารถตั้งค่า Page Rules ได้ไม่น้อยกว่า 100 rules

4.1.2. สามารถป้องกันการโจมตีประเภท DNS (DNS Security) โดยมีคุณลักษณะเฉพาะด้านเทคนิค ดังต่อไปนี้

- รองรับการกำหนดนโยบาย DNS Security โดยสามารถกำหนด Security Categories, Content Categories, และ Security Risk Subcategories ได้เป็นอย่างน้อย
- รองรับการใช้งาน DNS over HTTPS และ DNS over TLS ได้

4.1.3. สามารถทำ Load Balance โดยมีคุณลักษณะเฉพาะด้านเทคนิค ดังต่อไปนี้

- สนับสนุนการทำ Load Balancing โดยสามารถทำ Automatic Failover, Geographic routing and active health checks ได้ไม่น้อยกว่า 6 Origins

4.1.4. สามารถป้องกันการโจมตีประเภท DDoS (DDoS Mitigation) โดยมีคุณลักษณะเฉพาะด้านเทคนิค ดังต่อไปนี้

- สามารถป้องกันการโจมตีจากในระดับเครือข่าย (DDoS attack) ที่ระดับ Network layer 3, 4 และ 7
- ผู้ให้เช่าหรือผู้ให้บริการต้องให้บริการป้องกันการโจมตีในระดับเครือข่าย (DDoS attack) แบบไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี โดยไม่มีค่าใช้จ่ายเพิ่มเติม (Unlimited DDOS protection)
- ผู้ให้เช่าหรือผู้ให้บริการต้องมีเครือข่ายที่มีความสามารถในการป้องกันการโจมตีจากในระดับเครือข่าย (DDoS) ขนาด 142 Tbps เป็นอย่างน้อย
- เป็นผลิตภัณฑ์ที่ถูกจัดอยู่ในกลุ่ม Leader ของ The Forrester Wave ในหัวข้อของ DDoS Mitigation Solution ปี 2021 หรือปีล่าสุด

4.1.5. สามารถทำ Web Proxy โดยมีคุณลักษณะเฉพาะด้านเทคนิค ดังต่อไปนี้

- ผู้ให้บริการต้องมี Point of Presence (PoP) อย่างน้อย 250 จุดทั่วโลก และ POP อย่างน้อย 5 จุดในไทยที่มีการเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตระว่างประเทศ (International Internet Gateway: IIG) ในประเทศไทย ซึ่งแต่ละ POP ต้องมีความสามารถ DDoS mitigation, WAF และ CDN ได้
- สามารถทำการตรวจสอบการออกใบรับรอง SSL (certificate transparency monitoring) โดยสามารถแจ้งเตือนเมื่อมีผู้ทำการออกใบรับรองภายใต้ชื่อโดเมนเดียวกันกับของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย และนวัตกรรม
- สามารถตรวจจับและระบุการใช้งาน JavaScript ทั้งหมดได้ โดยต้องสามารถระบุได้ว่ามีการตรวจจับ Javascription นั้นๆครั้งแรกและครั้งล่าสุด ณ วันเวลาใด
- สามารถทำการแจ้งเตือนสถานะได้เป็นอย่างน้อยดังนี้
  - มีการเรียกใช้งาน JavaScript ใหม่
  - มีการเปลี่ยนแปลง JavaScript ที่ใช้งานอยู่
  - มีการเรียกใช้งาน JavaScript จากโดเมนใหม่
- ผู้ให้เช่าหรือผู้ให้บริการต้องให้บริการ authoritative DNS services สำหรับโดเมนสาธารณะ และผู้ให้บริการต้องมี Host Domains ทุกภูมิภาคทั่วโลก โดยต้องมี Node หลายจุดในแต่ละพื้นที่โดยเฉพาะในประเทศไทย
- มีระบบ Content Caching โดยสามารถทำ Static Content Caching และสามารถกำหนด Cache ในระดับ File Type ได้
- สามารถทำการ Purge Cache ทั้งหมดได้ในทันที หรือทำการ Custom Purge เฉพาะ URL, Host name และ Tag ได้ โดยต้องสามารถใช้ API ในการอัพเดท Cache เมื่อมีการอัพเดท Content ได้
- บริการต้องสามารถรองรับการใช้ Bandwidth Consumption ได้ไม่น้อยกว่า 5 TB ต่อเดือน
- สามารถลดขนาด บีบอัด และทำการลบ Metadata ของไฟล์ โดย สามารถเลือกได้ทั้งแบบ Lossless และ Lossy รวมถึงรองรับ Web
- สามารถทำการลบตัวอักษรที่ไม่จำเป็นใน Source code เช่น Whitespace และ Comments เพื่อช่วยเพิ่มประสิทธิภาพให้กับ Page load time
- มีระบบ Always Online ที่สามารถทำการแสดง static content ในกรณีที่ Server ต้นทางไม่สามารถใช้งานได้ เพื่อให้ผู้ใช้งานยังสามารถเรียกเข้าใช้งานเว็บไซต์ได้ในขณะที่ Server down
- มีระบบที่ช่วยเพิ่มประสิทธิภาพและลด Latency ให้กับ Dynamic Content โดยสามารถดูเปอร์เซ็นต์ประสิทธิภาพที่เพิ่มขึ้น และ Response time ได้ผ่านทาง Dashboard

4.1.6. สามารถเชื่อมต่อเครือข่ายแบบเสมือน (Virtual Private Network) โดยมีคุณลักษณะเฉพาะด้านเทคนิค ดังต่อไปนี้

- รองรับการทำ Single-sign on authentication และสามารถเชื่อมต่อกับระบบภายนอก (Integrate with 3rd party) Identity Provider ได้แก่ Azure AD, Okta, SAML หรือ OIDC ได้เป็นอย่างน้อย
- รองรับการตรวจสอบคุณลักษณะของอุปกรณ์ที่จะทำการเข้าถึงแอพพลิเคชั่น (Device Posture Check) เช่น Device Serial Number, OS Version และ Application Check ได้เป็นอย่างน้อย

4.1.7. สามารถแสดงรายงาน (Dashboard Functions) โดยมีคุณลักษณะเฉพาะด้านเทคนิค ดังต่อไปนี้

- สามารถแสดงรายงาน (Analytic) บน Dashboard แบบ Real-time หรือ Near Real-time โดย Dashboard ที่แสดงต้องประกอบด้วยข้อมูล Total Requests, Cached Request, Bandwidth Saved, Threat Sources, Top Threat Origin และ Top Traffic Origin ได้เป็นอย่างน้อย
- บริการที่เสนอรองรับการส่ง Raw Log ผ่านทาง Logpull REST API และสามารถเรียกดู Firewall Event Log และ Audit Log ได้ผ่านทาง Portal ที่ใช้งาน
- บริการที่เสนอต้องรองรับการกำหนดสิทธิเข้าใช้งาน และรองรับการทำ Two-Factor Authentication ได้

4.2. ซอฟต์แวร์วิเคราะห์และตรวจสอบความปลอดภัยเว็บไซต์

4.2.1. รองรับ Web Technology ที่ถูกพัฒนาขึ้นจาก HTML5, JSON, AJAX, และ JavaScript เป็นอย่างน้อย

4.2.2. สามารถแสดงคำนะนำสำหรับการแก้ไขช่องโหว่ด้านความปลอดภัยที่ตรวจพบได้

4.2.3. สามารถจัดลำดับความเสี่ยงที่เกิดขึ้นกับ Web Application และ Web Service เป็น Critical, High, Medium, Low ได้เป็นอย่างน้อย

4.2.4. สามารถสร้างรูปแบบ Profile สำหรับใช้ในการตรวจสอบความปลอดภัย Web Application โดยสามารถกำหนดค่าชื่อโดเมน (Domain Name), ขั้นตอนการเข้าสู้ระบบ (Login Macro), กำหนดค่าพร็อกซี่ (Proxy), กำหนดประเภทของการสแกน (Scan Type) ได้เป็นอย่างน้อย

4.2.5. สามารถกำหนดเวลาในการตรวจสอบได้ล่วงหน้า (Schedule) ได้แบบรายวัน (Daily), รายสัปดาห์ (Weekly), รายเดือน (Monthly) เป็นอย่างน้อย

4.2.6. สามารถเปรียบเทียบความแตกต่างของการตรวจสอบแต่ละครั้ง (Scan Compare) ได้

4.2.7. สามารถตรวจสอบหมวดหมู่ด้านความปลอดภัย (Vulnerability Category) ดังต่อไปนี้ Cross Site Script (XSS), Injection Flaw (SQL Injection, XML Injection), Buffer Overflow, Denial of Service (DoS), URL Redirection, Session Fixation, Path Disclosure และ Directory Traversal ได้เป็นอย่างน้อย

4.2.8. สามารถนำผลลัพธ์จากการวิเคราะห์ Web Application หรือ Web Service มาจัดหมวดหมู่เพื่อเปรียบเทียบกับมาตรฐานด้านความปลอดภัย PCI DSS, ISO27001, HIPAA, และ SAN CWE Top25 เป็นอย่างน้อย และสามารถออกรายงานได้

5. ข้อกำหนดอื่น ๆ

5.1. สามารถป้องกันการถูกโจมตีบนเว็บไซต์ ได้ไม่น้อยกว่า 2 โดเมนเนม และ Sub-domain แบบไม่จำกัดตามที่ สป.อว. เป็นผู้กำหนด

5.2. สามารถพิสูจน์ตัวตนและรักษาความปลอดภัยในการเข้าสู่ระบบเครือข่ายของ สป.อว. จำนวนไม่น้อยกว่า 50 ผู้ใช้งาน ตามที่ สป.อว. เป็นผู้กำหนด

5.3. ผู้ให้บริการต้องสามารถให้ทาง สป.อว. เริ่มใช้งานระบบตรวจสอบและป้องกัน Web Application และควบคุมการเข้าถึงการใช้งานระบบสารสนเทศ ได้ตั้งแต่เดือนตุลาคม 2565 ถึงเดือนกันยายน 2566

5.4. ผู้ให้บริการต้องรับประกันคุณภาพการให้บริการ (SLA) ของระบบบริการ Cloud Services โดยมีค่าเฉลี่ยในการทำงาน (Uptime) ไม่น้อยกว่า 99.90 %

5.5. ผู้ให้บริการต้องมีศูนย์รับแจ้งเหตุ ผ่านทางโทรศัพท์ และ E-Mail ได้ทุกวันไม่เว้นวันหยุดราชการตลอด 24 ชั่วโมง

5.6. ผู้ให้บริการต้องมีระบบแจ้งเตือนไปยังผู้ดูแลระบบของ สป.อว. ในกรณีที่ระบบไม่สามารถใช้งานได้ตลอดระยะเวลาของสัญญา

5.7. ผู้ให้บริการจะต้องจัดทำแผนการดำเนินโครงการในภาพรวมทั้งหมด เพื่อให้คณะกรรมการและผู้เกี่ยวข้องสามารถติดตามการดำเนินโครงการได้

5.8. ระบบที่นำเสนอทั้งหมดในโครงการนี้ ผู้ให้บริการต้องดำเนินการจัดการให้ผู้ดูแลระบบของ สป.อว. สามารถใช้งานได้ 1 ปีเป็นอย่างน้อย โดยมีสิทธิ์การใช้งานถูกต้องตามกฎหมาย

5.9. ผู้ให้บริการต้องติดตั้งและเชื่อมต่อกับ Application กับระบบที่นำเสนอฯ โดยครอบคลุมการทำ Secure Web Gateway DNS Policies, Secure Web Gateway Network Policies, Secure Web Gateway HTTP Policies เป็นอย่างน้อย

5.10. ผู้ให้บริการดำเนินการตั้งค่านโนบายการเข้าใช้งาน (Access Policies) เพื่อทำการควบคุมการเข้าถึงไปยัง Web Application

5.11. ผู้ให้บริการดำเนินการสร้างและตั้งค่า Tunnel สำหรับการเชื่อมต่อไปยัง Web Application และ Network รวมถึงการทำ Split Tunnel

5.12. ผู้ให้บริการต้องทำการวิเคราะห์และบริหารจัดการปรับแต่งค่าการทำงานหรือค่าพารามิเตอร์ของระบบฯ ให้สอดคล้องกับนโยบายแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ (ISO27001:2013) ของ สป.อว.

5.13. ผู้ให้บริการต้องให้คำปรึกษาแนะนำ และดำเนินการด้านเทคนิคเกี่ยวกับระบบตรวจสอบและป้องกัน Web Application และควบคุมการเข้าถึงการใช้งานระบบสารสนเทศ เพื่อควบคุมการปฏิบัติงานของระบบคอมพิวเตอร์ให้ใช้งานได้เป็นปกติ

5.14. เมื่อผู้ให้บริการได้รับแจ้งเหตุขัดข้องจาก สป.อว. ผ่านทางโทรศัพท์, โทรสาร, จดหมายอิเล็กทรอนิกส์, โปรแกรม LINE หรือหนังสือราชการ ผู้ให้บริการจะต้องดำเนินการตรวจสอบลักษณะปัญหา และแก้ไขปัญหาเบื้องต้นผ่านทางโทรศัพท์ หรือด้วยวิธีการ Remote Desktop ผ่านช่องทางของหน่วยงาน หรือจัดส่งเจ้าหน้าที่เข้ามาดำเนินการแก้ไขปัญหา ณ สป.อว. (อาคารพระจอมเกล้า) ด้วยวิธีการที่เหมาะสมกับลักษณะของปัญหาที่เกิดขึ้น

5.15. หากระบบที่นำเสนอภายในโครงการนี้เกิดการขัดข้องหรือการทำงานบกพร่องจนไม่สามารถให้บริการได้ ผู้ให้บริการจะต้องดำเนินการแก้ไขข้อขัดข้องให้อยู่ในสภาพใช้งานได้ตามปกติ โดยมีกำหนดระยะเวลาดังนี้

- ในเวลาราชการภายใน 4 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้ง
- นอกเวลาราชการภายใน 8 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้ง

6. การส่งมอบงาน

ผู้เสนอราคาจะต้องดำเนินการส่งมอบงานหลังครบกำหนดการปฏิบัติงานสิ้นสุดของแต่ละงวดงาน ภายในระยะเวลา 5 วันทำการ ต้องจัดทำเอกสารรายงานการใช้งานในรูปแบบเอกสารจำนวน 3 ชุด และรูปแบบ Electronic File จำนวน 1 ชุด โดยมีป้ายแสดงชั้นความลับ พร้อมส่งให้ทาง สป.อว. เป็นรายเดือน รวมทั้งหมด 12 งวด โดยมีรายงานผลการดำเนินการ ดังต่อไปนี้

6.1. <u>เอกสารรายงาน (งวดที่ 1) ประกอบด้วยรายละเอียดดังนี้</u>

6.1.1. ผังภาพรวมของโครงสร้างการเชื่อมต่อระบบฯ ที่นำเสนอทั้งหมด พร้อมระบุรายละเอียดกำกับแต่ละรายการในผังภาพให้ชัดเจน

6.1.2. เอกสารสิทธิ์การใช้งาน (License) และบัญชีผู้ใช้งาน (Account) ในโครงการนี้ทั้งหมด

6.1.3. รายละเอียดการกำหนดค่าการใช้งานระบบฯ (System Configuration)

6.1.4. รายงานผลการเข้าดำเนินการ Preventive Maintenance หรือการตรวจสอบ (Service Report) ประจำเดือน โดยเอกสารดังกล่าวจะต้องมีรายละเอียดดังต่อไปนี้

- ระบุวันที่ เดือน ปี และเวลา ที่เข้ามาดำเนินการหรือตรวจสอบ
- รายละเอียดผลการดำเนินงานหรือตรวจสอบสถานะการทำงานของระบบต่างๆ ในโครงการนี้ทั้งหมด
- รายงานผลการตรวจพบภัยคุกคามของระบบที่นำเสนอในโครงการนี้ทั้งหมด
- ความคิดเห็นหรือข้อเสนอแนะ (หากมี)
- รายงานผลการดำเนินการ Corrective Maintenance โดยต้องสรุปรายการเอกสารการเปลี่ยนแปลงการตั้งค่าของระบบ (Change Report) ประจำเดือน (หากมี)

6.2. <u>เอกสารรายงาน (งวดที่ 2 ถึงงวดที่ 12) ประกอบด้วยรายละเอียดดังนี้</u>

6.2.1. รายละเอียดการกำหนดค่าการใช้งานระบบฯ (System Configuration)

6.2.2. รายงานผลการเข้าดำเนินการ Preventive Maintenance หรือการตรวจสอบ (Service Report) ประจำเดือน โดยเอกสารดังกล่าวจะต้องมีรายละเอียดดังต่อไปนี้

- ระบุวันที่ เดือน ปี และเวลา ที่เข้ามาดำเนินการหรือตรวจสอบ

- รายละเอียดผลการดำเนินงานหรือตรวจสอบสถานการณ์ทำงานของระบบต่างๆ ในโครงการนี้ทั้งหมด
- รายงานผลการตรวจพบภัยคุกคามของระบบที่นำเสนอในโครงการนี้ทั้งหมด
- ความคิดเห็นหรือข้อเสนอแนะ (หากมี)
- รายงานผลการดำเนินการ Corrective Maintenance โดยต้องสรุปรายการเอกสารการเปลี่ยนแปลงการตั้งค่าของระบบ (Change Report) ประจำเดือน (หากมี)

ในกรณีที่เอกสารส่งมอบประกอบไปด้วยข้อมูลที่สำคัญของหน่วยงาน เช่น หมายเลข IP address, เอกสารการกำหนดการตั้งค่าอุปกรณ์หรือระบบฯ, เอกสารลิขสิทธิ์ (License) ของระบบ, ข้อมูลส่วนบุคคล รวมถึงบัญชีและรหัสผ่านของผู้ใช้งานระบบสารสนเทศระดับผู้ใช้งานทั่วไป เป็นต้น ทางผู้ให้บริการต้องจัดทำป้ายแสดงระดับชั้นความลับให้มีตราหรือเครื่องหมาย หรือชื่อขององค์กร และมีข้อความระบุว่า “Confidential” หรือคำว่า “ลับ” จำนวน 1 ชุดบนเอกสาร และจัดทำเอกสารรูปแบบเฉพาะที่ปิดบังข้อมูลที่สำคัญของหน่วยงาน โดยมีข้อความว่า “Internal Use” หรือคำว่า “ใช้ภายใน” จำนวน 2 ชุดบนเอกสาร ที่จะจัดส่งให้กับทาง สป.อว. (รวมทั้งหมด 3 ชุด) และข้อมูลแบบ Electronic File ซึ่งต้องทำการเข้ารหัสข้อมูล (Encrypted) เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญ โดยต้องมีข้อความระบุว่า “Confidential” หรือคำว่า “ลับ” บนเอกสารซองเอกสารทึบแสงที่ปิดผนึกเรียบร้อยนำส่งมอบให้กับทาง สป.อว. จำนวน 1 ชุด พร้อมดำเนินการส่งรหัสผ่านให้กับผู้ดูแลระบบผ่านทางช่องตามที่ สป.อว. เป็นผู้กำหนด ด้วยโปรแกรม WinZip หรือ WinRAR หรือ 7Zip เป็นต้น

7. การปฏิบัติตามนโยบายด้าน ICT ของ สป.อว.

ผู้ให้บริการจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สป.อว. และขั้นตอนปฏิบัติต่าง ๆ ตามนโยบาย ISO27001:2013 รวมถึงคำสั่งและวิธีปฏิบัติที่เกี่ยวข้องอย่างเคร่งครัด

8. การปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement)

ผู้ให้บริการหรือทีมงานผู้ให้บริการจะต้องดำเนินการลงนามการปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement) ให้กับสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำหรับโครงการนี้ เพื่อเป็นการรักษาความลับทางด้านข้อมูลไม่ให้รั่วไหลสู่สาธารณะโดยไม่ได้รับอนุญาต

9. การอบรม

ผู้ให้บริการต้องจัดอบรมการใช้งาน และการแก้ปัญหาเบื้องต้นของระบบฯและโปรแกรมที่นำเสนอ ให้กับผู้ดูแลระบบของ สป.อว. จำนวนไม่น้อยกว่า 5 คน ณ สป.อว. (อาคารพระจอมเกล้า) โดยผู้ให้บริการต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ในการจัดหาเอกสารประกอบการอบรมแต่ละหลักสูตรให้กับ สป.อว.

10. ระยะเวลาดำเนินการ

กำหนดส่งมอบงานเป็นรายเดือน จำนวนระยะเวลา 12 เดือน ตั้งแต่เดือน ตุลาคม 2565 ถึงเดือน กันยายน 2566

11. งบประมาณ

วงเงินงบประมาณ 2,100,000.- บาท (สองล้านหนึ่งแสนบาทถ้วน)

12. การจ่ายเงิน

ผู้ว่าจ้างจะแบ่งจ่ายค่าบริการเป็นรายเดือน ทั้งหมด 12 เดือน เดือนละเท่าๆกัน ซึ่งเป็นราคารวมภาษีมูลค่าเพิ่ม และภาษีอากรอื่นๆแล้ว ทั้งนี้จะเริ่มจ่ายในเดือนแรกหลังจากดำเนินการและส่งมอบตามข้อ 4, ข้อ 5 และข้อ 6 แล้วเสร็จ

13. หลักเกณฑ์การพิจารณา

เกณฑ์การพิจารณาผู้ชนะการเสนอราคา ใช้เกณฑ์ราคาและพิจารณาจากราคารวม

14. กำหนดยืนราคา 90 วัน

(นายทวีศักดิ์ นาเมืองรักษ์)	(นายจิรายุ ชัยมีบุญ)	(นางสาวศุภกร สาระวงศ์)
นักวิชาการคอมพิวเตอร์ชำนาญการ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	เจ้าหน้าที่ระบบงานคอมพิวเตอร์
ผู้กำหนดคุณลักษณะเฉพาะ	ผู้กำหนดคุณลักษณะเฉพาะ	ผู้กำหนดคุณลักษณะเฉพาะ