

ขอบเขตของงาน จ้างเหมาบริการวางจรสื่อสารพร้อมอุปกรณ์ และโครงข่ายอินเทอร์เน็ตแบบองค์กร
พร้อมระบบรักษาความปลอดภัยแบบเบ็ดเสร็จในจุดเดียว

1. คุณสมบัติผู้รับจ้าง

- 1.1 ผู้รับจ้างต้องเป็นผู้มีอาชีพรับจ้างงานที่เสนอราคาจ้าง
- 1.2 ผู้รับจ้างต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานของทางราชการ และได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ
- 1.3 ผู้รับจ้างต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้รับจ้างรายอื่น ณ วันประกาศสอบราคา หรือไม่เป็น ผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม
- 1.4 ผู้รับจ้างต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของ ผู้รับจ้างได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นนั้น
- 1.5 ผู้รับจ้างต้องไม่เป็นผู้ที่ถูกประเมินสิทธิผู้รับจ้างในสถานะที่ห้ามเข้าเสนอราคา และห้ามทำสัญญาตามที่ กวพ. กำหนด
- 1.6 ✓ ผู้รับจ้างที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะซึ่งได้มีการระบุชื่อไว้ในบัญชีรายชื่อว่าเป็นคู่สัญญาที่ไม่ได้ แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ
- 1.7 ✓ ผู้รับจ้างที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement: e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่ เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ
- 1.8 ✓ คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การรับจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาท คู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้
- 1.9 ผู้รับจ้างจะต้องมีวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตภายในประเทศ (National Internet Exchange: NIX) อย่างน้อย 2 แห่ง ความเร็วรวมไม่น้อยกว่า 15 Gbps โดยผู้รับจ้างจะต้อง แสดงแผนผังการเชื่อมต่อตาม Map of Internet Connectivity in Thailand ซึ่งจัดทำโดยศูนย์ เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ฉบับล่าสุด โดยให้ระบุเส้นทางเชื่อมต่อ ภายในประเทศที่จะให้บริการ
- 1.10 ผู้รับจ้างจะต้องมีวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตเพื่อออกต่างประเทศ (International Internet Gateway: IIG) อย่างน้อย 2 แห่ง รวมกันความเร็วไม่น้อยกว่า 600 Mbps โดยผู้รับจ้างต้องแสดงแผนผังการเชื่อมต่อตาม Map of Internet connectivity in Thailand ซึ่งจัดทำ โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ฉบับล่าสุด โดยให้ระบุเส้นทาง เชื่อมต่อต่างประเทศที่จะให้บริการ
- 1.11 ผู้รับจ้างจะต้องมีผู้ชำนาญการพร้อมปฏิบัติงาน (On-Call Service) ตลอด 24 ชั่วโมงตลอด 7 วัน (24 x 7) และมีผู้ชำนาญการพร้อมให้คำปรึกษาและพร้อมปฏิบัติงาน ในกรณีที่มีปัญหาเร่งด่วน (Urgent Case) ตลอดอายุสัญญา
- 1.12 ผู้รับจ้างจะต้องให้บริการ ตั้งแต่วันที่ 1 ตุลาคม 2559 ถึง 30 กันยายน 2560

2. รายละเอียด/ข้อกำหนดคุณลักษณะเฉพาะด้านโครงข่าย

2.1. ผู้รับจ้างจะต้องเชื่อมต่อเครือข่ายอินเทอร์เน็ตของ สำนักงานคณะกรรมการส่งเสริมการลงทุน ไปยังผู้รับจ้างด้วยวงจรสื่อสารความเร็วสูง ผ่านโครงข่ายใยแก้วนำแสง (Fiber Optic) วงจรเช่าแบบ MPLS ในลักษณะ Point to Multipoint หรือแบบ Ethernet Service โดยผู้ให้เช่า ต้องจัดหา ติดตั้ง วงจรสื่อสาร วงจรเครือข่ายหลัก วงจรเครือข่ายสำรอง โดยที่วงจรเครือข่ายหลัก และวงจรเครือข่ายสำรองจะต้องเป็นผู้ให้บริการโครงข่ายคนละรายกัน และจัดหาอุปกรณ์ ตลอดอายุสัญญาอย่างต่อเนื่อง ตลอด 24 ชั่วโมง 7 วัน โดยไม่จำกัดจำนวนผู้ใช้ จำนวนชั่วโมงการใช้งาน และปริมาณข้อมูลเข้าออก โดยมีจุดติดตั้ง และความเร็วของวงจร ดังต่อไปนี้

ลำดับ	สถานที่	วงจรหลัก	วงจรสำรอง
1	สำนักงานคณะกรรมการส่งเสริมการลงทุน (สำนักงานใหญ่) 555 ถ.วิภาวดีรังสิต เขตจตุจักร กทม.	100 Mbps.	50 Mbps.
2	ศูนย์ประสานการบริการด้านการลงทุน และ ศูนย์บริการวีซ่าและใบอนุญาตทำงาน ชั้น 18 อาคารจัตุรัสจามจุรี ถ.พญาไท เขตปทุมวัน กทม.	30 Mbps.	10 Mbps.
3	ศูนย์เศรษฐกิจการลงทุนภาคที่ 1 จังหวัดเชียงใหม่ 108-110 อาคารแอรพอร์ต บิสิเนส ปาร์ค 90 ถนนมहितล ต.หายยา อ.เมือง จ.เชียงใหม่	10 Mbps.	5 Mbps.
4	ศูนย์เศรษฐกิจการลงทุนภาคที่ 1 จังหวัดพิษณุโลก 59/15 ชั้นที่ 3 อาคารไทยศิวารัตน์ ถ.บรมไตรโลกนาถ 2 อ.เมือง จ.พิษณุโลก	5 Mbps.	5 Mbps.
5	ศูนย์เศรษฐกิจการลงทุนภาคที่ 2 จังหวัดนครราชสีมา 2112/22 ถ.มิตรภาพ อ.เมือง จ.นครราชสีมา	10 Mbps.	5 Mbps.
6	ศูนย์เศรษฐกิจการลงทุนภาคที่ 3 จังหวัดขอนแก่น 177/54 ถ.มิตรภาพ อ.เมือง จ.ขอนแก่น	10 Mbps.	5 Mbps.
7	ศูนย์เศรษฐกิจการลงทุนภาคที่ 4 จังหวัดชลบุรี 46 หมู่ 5 นิคมอุตสาหกรรมแหลมฉบัง ถ.สุขุมวิท อ.ศรีราชา จ.ชลบุรี	15 Mbps.	10 Mbps.
8	ศูนย์เศรษฐกิจการลงทุนภาคที่ 5 จังหวัดสงขลา 7-15 ชั้น 5 อาคารไชนยงค์ ถ.จุดอุทิศ 1 อ.หาดใหญ่ จ.สงขลา	10 Mbps.	5 Mbps.
9	ศูนย์เศรษฐกิจการลงทุนภาคที่ 6 จังหวัดสุราษฎร์ธานี 49/21-22 ถ.ศรีวิชัย ต.มะขามเตี้ย อ.เมือง จ.สุราษฎร์ธานี	10 Mbps.	5 Mbps.
10	CAT Data Center (บางรัก) 13 อาคาร กสท โทรคมนาคม จำกัด (มหาชน) ถ.เจริญกรุง เขตบางรัก กทม.	50 Mbps.	-

- 2.2. ผู้รับจ้างต้องจัดหาวงจรการใช้งานอินเทอร์เน็ต ความเร็วภายในประเทศไม่น้อยกว่า 200 Mbps และอินเทอร์เน็ตระหว่างประเทศ ความเร็วไม่น้อยกว่า 50Mbps สำหรับรองรับการใช้งานอินเทอร์เน็ตรวมสำนักงาน ตามข้อ 2.1
- 2.3. ผู้รับจ้างจะต้องเสนอ วงจรสื่อสารข้อมูลอินเทอร์เน็ตภายในประเทศ ความเร็วรวมไม่น้อยกว่า 50 Mbps และวงจรสื่อสารข้อมูลอินเทอร์เน็ตระหว่างประเทศได้ไม่น้อยกว่า 10 Mbps รวมอุปกรณ์ Router ติดตั้งที่สำนักงานคณะกรรมการส่งเสริมการลงทุน สำนักงานใหญ่ 1 วงจร โดยจะต้องเป็นผู้ให้บริการอินเทอร์เน็ต (ISP) และผู้ให้บริการโครงข่าย (Carrier Provider) ที่ไม่ซ้ำกับข้อ 2.2
- 2.4. ผู้รับจ้างจะต้องเสนอ Core Router ตามข้อ 2.1 สำหรับรองรับการให้บริการเชื่อมต่อวงจรแต่ละสาขาของสำนักงานฯ จำนวน 10 แห่ง เพื่อให้การควบคุมเส้นทาง (Routing) ของแต่ละสาขาได้ โดยติดตั้งที่ผู้รับจ้าง
- 2.5. ผู้รับจ้างจะต้องเสนอจำนวน Public IP Address จำนวนไม่น้อยกว่า 32 IP Address
- 2.6. ผู้รับจ้างจะต้องเป็นผู้ดูแล Domain และ Name server ของสำนักงาน จำนวน 1 Domain
- 2.7. ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบดูแลการใช้งาน การบำรุงรักษา การแก้ไขปัญหา และการให้บริการระบบเครือข่ายอินเทอร์เน็ตและอินเทอร์เน็ต กับสำนักงานฯ ตลอดระยะเวลาของสัญญา
- 2.8. ผู้รับจ้างจะต้องเสนอเครื่องมือ สำหรับการ Monitor Network traffic ให้กับทางสำนักงานฯ โดยสามารถเข้า Monitor Network traffic ได้ตลอด 24 ชั่วโมง
- 2.9. ผู้รับจ้างจะต้องสามารถให้บริการระบบเครือข่ายอินเทอร์เน็ตแบบองค์กร/อินเทอร์เน็ตแบบส่วนตัว ให้แก่สำนักงานฯ โดยสำนักงานฯ จะต้องสามารถใช้งานอินเทอร์เน็ตแบบองค์กร/อินเทอร์เน็ต ได้อย่างต่อเนื่องตามจำนวนขนาดที่ให้บริการกับสำนักงานฯ
- 2.10. ผู้รับจ้างจะต้องแสดงภาพกราฟสถิติของปริมาณการใช้งานสายสัญญาณระหว่างประเทศในเส้นทางที่เป็นเส้นทางหลักของผู้รับจ้าง โดยผู้รับจ้างจะต้องมีปริมาณการใช้งานที่เข้าหรือออกในเส้นทางนั้นโดยเฉลี่ยตลอด 3 เดือนที่ผ่านมา ณ วันที่เสนอราคา ไม่เกินร้อยละ 80 ของขนาดช่องสัญญาณนั้น
- 2.11. ผู้รับจ้างจะต้องแสดงภาพกราฟสถิติของปริมาณการใช้งานสายสัญญาณภายในประเทศในเส้นทางที่เป็นเส้นทางหลักของผู้รับจ้าง โดยผู้รับจ้างจะต้องมีปริมาณการใช้งานที่เข้าหรือออกในเส้นทางนั้นโดยเฉลี่ยตลอด 3 เดือนที่ผ่านมา ณ วันที่เสนอราคา ไม่เกินร้อยละ 80 ของขนาดช่องสัญญาณนั้น
- 2.12. ผู้รับจ้างต้องจัดทำกราฟแสดงสถิติปริมาณข้อมูลซึ่งเก็บทุกๆ 5 นาที ในรอบวันที่ผ่านมาของการใช้งานอินเทอร์เน็ต/อินเทอร์เน็ต ที่เสนอให้สำนักงานฯ ทราบ โดยสำนักงานฯ จะต้องสามารถตรวจสอบรายงานการใช้งานได้ตลอดเวลา 24 ชั่วโมง ผ่านทางระบบเครือข่ายอินเทอร์เน็ต โดยแยกแสดงการใช้งานเป็นแบบต่อเนื่องรายวัน, รายสัปดาห์ และรายเดือน
- 2.13. กรณีผู้รับจ้างจะดำเนินการปรับปรุงหรือซ่อมแซมบำรุงเครือข่ายภายในของผู้รับจ้าง ซึ่งอาจส่งผลกระทบทำให้อินเทอร์เน็ตที่ให้บริการกับสำนักงานฯ ไม่สามารถใช้งานได้โดยมีประสิทธิภาพ ผู้รับจ้างจะต้องแจ้งให้กับสำนักงานฯ รับทราบล่วงหน้าไม่น้อยกว่า 3 วันทำการ โดยแจ้งเป็นหนังสือ (ลายลักษณ์อักษร) หรือ Email หรือ SMS ทางใดทางหนึ่ง มิฉะนั้นจะถือว่าในช่วงเวลาทั้งหมดที่มีการปรับปรุงหรือ

ซ่อมบำรุงนั้นทำให้การใช้งานระบบอินเทอร์เน็ตไม่สามารถใช้ได้อย่างเต็มประสิทธิภาพ และสำนักงานฯ สามารถออกหนังสือแจ้งเตือน ขอคืนเงิน และปรับเป็นเงินตามจำนวนที่ได้ระบุไว้ในสัญญา

3. รายละเอียด/ข้อกำหนดคุณลักษณะเฉพาะด้านความปลอดภัย

3.1. Firewall จำนวน 2 ระบบทำงานในลักษณะ Active-Standby

3.1.1. ผู้รับจ้างต้องจัดให้มีบริการ Firewall ที่รองรับการใช้งาน Throughput ไม่น้อยกว่า 600 Mbps และ การใช้งานของผู้ใช้งานพร้อมกันไม่น้อยกว่า 500 คน รวมถึงการใช้งาน VPN, NAT, IPS และระบบ เก็บ Log ที่สามารถเก็บข้อมูลไม่น้อยกว่า 90 วัน ตาม พ.ร.บ.ว่าด้วยการกระทำความผิดทาง คอมพิวเตอร์

3.2. Web Application Firewall จำนวน 2 ระบบ โดยมีคุณลักษณะดังนี้

3.2.1. ระบบจะต้องสามารถรองรับการทำงานแบบ Active-Active หรือ Active-Passive หรือ Clustering ได้

3.2.2. ระบบจะต้องสามารถรองรับการทำงานแบบ ใช้งาน sub-domain ได้ไม่น้อยกว่า 10 sub-domain

3.2.3. ระบบที่นำเสนอจะต้องมีความสามารถในการตรวจจับพฤติกรรมการใช้งาน Web Application ของ ผู้ที่เข้ามาใช้บริการของ Web Application บน Server ต่าง ๆ ได้ โดยตัวระบบเองจะต้องสามารถ ดูแลและปกป้อง Server ได้มากกว่า 1 เครื่อง

3.2.4. มีระบบการตรวจจับโดยใช้ Signature หรือติ๊กว่า โดยจะต้องสามารถป้องกันการโจมตีได้

3.2.5. ระบบที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge) หรือ Transparent หรือ Proxy Mode ได้

3.2.6. มีความสามารถในการทำงานและปกป้อง Web Application ต่าง ๆ ได้ โดยจะต้องรองรับ HTTP และ HTTPS ได้เป็นอย่างดี

3.2.7. ระบบที่นำเสนอจะต้องมีความสามารถในการป้องกันการรั่วไหลของข้อมูลได้ (Data Leakages หรือ Information Leakages)

3.2.8. ระบบที่นำเสนอจะต้องรองรับการทำ SSL Termination หรือ Passive Decryption

3.2.9. มีระบบจัดการ Log โดยสามารถแสดง Alert หรือแจ้งเตือนในกรณีที่เกิดเหตุการณ์ต่าง ๆ ได้ โดย สามารถ Alert ผ่านทาง SMTP และ/หรือ SNMP ได้เป็นอย่างดี

3.2.10. ระบบที่นำเสนอจะต้องสามารถส่ง Syslog Server หรือสามารถส่งข้อมูลไปยังระบบ SIM/SIEM ได้

3.2.11. รองรับระบบ Centralized Management ซึ่งเป็นระบบเสริม เพื่อใช้ช่วยในส่วนของการบริหาร จัดการระบบให้ง่ายขึ้นในกรณีที่มีจำนวน Application เป็นจำนวนมาก

3.2.12. สามารถทำงานร่วมกับ NTP หรือ SNTP ได้เพื่อให้สามารถ Sync เวลาจาก Time Server ได้

3.2.13. สามารถทำงานในลักษณะ Session Control ได้หลายรูปแบบ

3.2.14. มีความสามารถในการเรียนรู้ Traffic ได้โดยอัตโนมัติ เพื่อวิเคราะห์พฤติกรรมการใช้งาน Web Application ขององค์กร

- 3.2.15. สามารถทำรายงานในรูปแบบ PDF หรือ CSV หรือ HTML เป็นอย่างน้อย
- 3.2.16. รองรับการป้องกันการ Attack ด้วยวิธีต่าง ๆ ด้วยรูปแบบอย่างน้อย ดังต่อไปนี้ Data Destruction หรือ Data Encoding, Parameter Tempering, Denial of Service หรือ Cookie Poisoning ,Cross-site Scripting, Credit Card Exposure หรือ Brute Force Attacks, OS Command Injection หรือ Stealth Commanding, SQL Injection, Buffer Overflow หรือ Application Buffer Overflow Attacks, Patient Data disclosure หรือ Web Server Reconnaissance, Malicious Encoding หรือ Unauthorized Navigation, Web Server and Platform Attack หรือ Hidden Field Manipulation Data Destruction หรือ Data Encoding
- 3.2.17. ระบบที่เสนอต้องได้รับการรับรองมาตรฐาน FCC และ UL หรือเทียบเท่า กรณีได้รับมาตรฐานอื่นที่เทียบเท่า ต้องมีเอกสารเปรียบเทียบความเทียบเท่าของมาตรฐานที่ได้รับกับมาตรฐานที่กำหนดด้วย
- 3.2.18. มีการรับประกันผลิตภัณฑ์จากบริษัทผู้ผลิต หรือตัวแทนที่ได้รับการแต่งตั้งเป็นทางการ ไม่น้อยกว่า 1 ปี ซึ่งครอบคลุมถึงการ Update Software และ/หรือ Hardware ของผลิตภัณฑ์ที่เสนอด้วย
- 3.3. Web Security Gateway จำนวน 1 ระบบ โดยมีคุณลักษณะดังนี้**
- 3.3.1. มี License รองรับผู้ใช้งานทั้งด้าน Web Security Gateway ไม่น้อยกว่า 500 ผู้ใช้งาน (User)
- 3.3.2. สามารถทำการบริหารจัดการ การกำหนดนโยบาย รวมทั้งการดูรายงานต่างๆ ผ่าน Web browser ในลักษณะ single web-based user management interface ได้
- 3.3.3. มีฐานข้อมูล Web Category มากกว่า 40 ล้านเว็บไซต์ และแบ่งเป็นหมวดหมู่ไม่น้อยกว่า 100 Categories โดยรองรับได้ไม่น้อยกว่า 50 ภาษา
- 3.3.4. มีฐานข้อมูลเว็บไซต์ในลักษณะ Web Categories ที่มี Update เมื่อมีการเปลี่ยนแปลงเนื้อหา หรือหมวดหมู่ในเว็บไซต์ต่างๆ รวมทั้งสามารถทำการเปลี่ยนแปลง Category ของ URL ที่มีใน Database เพื่อความเหมาะสมขององค์กรได้
- 3.3.5. สามารถกำหนด Policy แบบเฉพาะเจาะจงผู้ใช้งานที่ Log-in ผ่านระบบ โดยยึดจาก Username และ Password ในกรณีที่เครื่องคอมพิวเตอร์เครื่องหนึ่งๆ ถูกใช้งานจากผู้ใช้หลาย ๆ คน
- 3.3.6. สามารถกำหนดสิทธิการใช้งานเว็บไซต์ โดยกำหนดจาก ผู้ใช้, กลุ่มของผู้ใช้, IP address Workstation และ Network ได้
- 3.3.7. สามารถกำหนดนโยบายการใช้งานเว็บไซต์ในรูปแบบต่างๆ เช่น Allow, Block, Quota และการ block file type ตามเวลาที่กำหนดได้
- 3.3.8. สามารถกำหนดสิทธิการใช้งาน protocols อื่นๆ นอกเหนือจาก HTTP, HTTPS เช่น IM, P2P file sharing, Skype, Streaming media protocols โดยสามารถรองรับการจัดการ Protocol ได้มากกว่า 120 Protocols ตามวัน/เวลาที่กำหนดได้ หรือเสนออุปกรณ์ต่อพ่วงที่ทำหน้าที่ Application control โดยสามารถรองรับ protocols ได้ไม่น้อยกว่า 120 Protocols
- 3.3.9. สามารถควบคุมการใช้งาน Application โดยใช้ระบบ Application Recognition แบบใช้ Signature ได้

- 3.3.10. มี Database Category ของ URLs ที่มี/เป็น spyware, malicious mobile code, bot networks, phishing และ pharming และสามารถ update database ของข้อมูลเกี่ยวกับ Security Threat ใหม่ ๆ ที่ค้นพบโดยเจ้าของผลิตภัณฑ์ได้แบบ real-time
 - 3.3.11. สามารถวิเคราะห์และตรวจสอบข้อมูลจราจรที่ถูกเข้ารหัส (Encrypted SSL traffic) โดยทำการถอดการเข้ารหัส(Decrypt) และวิเคราะห์เนื้อหา (content) ภายในเพื่อตรวจสอบด้านความปลอดภัย และสามารถทำการเข้ารหัส(re-encrypt) ข้อมูลกลับคืนอย่างเดิมได้
 - 3.3.12. สามารถกำหนดให้ยกเว้นการถอดรหัส (SSL Decryption By Pass) โดยกำหนดเป็นบางหมวดหมู่ (Category) ได้ เช่น ธนาคารหรือสถาบันการเงิน เพื่อป้องกันการละเมิดสิทธิส่วนบุคคลของผู้ใช้ได้
 - 3.3.13. สามารถอัปเดตฐานข้อมูล (Signature) ของไวรัสได้โดยอัตโนมัติตลอดระยะเวลาที่รับประกัน
 - 3.3.14. สามารถจัดหมวดหมู่เว็บไซต์ของเว็บไซต์ที่มีเนื้อหาแบบ Dynamics ซึ่งพัฒนาโดยเทคโนโลยี Web 2.0 เช่น Facebook, LinkedIn และเว็บไซต์ที่ยังไม่ได้รับการจัดหมวดหมู่ โดยตรวจสอบข้อมูลบนเว็บไซต์จากส่วนประกอบต่างๆ และเนื้อหาภายในแบบ Real-Time ได้
 - 3.3.15. สามารถควบคุมและบริหารจัดการ ซึ่งรวมถึงการแก้ไข Configuration , การทำรายงานและการตรวจดู Log ของระบบ ได้จากศูนย์กลาง (Centralized Management) ผ่านทาง Secure Web Management (HTTPS)
 - 3.3.16. มีข้อความแจ้งเตือน (Block/Warning Page) ในรูปแบบ HTML โดยสามารถเปลี่ยนแปลงข้อความหรือรูปภาพ (Customized Block Page) ได้โดยไม่ต้องอาศัยเว็บเซิร์ฟเวอร์ภายนอก
 - 3.3.17. สามารถแสดงผลการใช้งาน Internet ของผู้ใช้งานผ่านทาง Web browser ในลักษณะ real-time ได้
 - 3.3.18. มีเครื่องมือ Management Dashboard เพื่อให้ผู้บริหารสามารถดูข้อมูล ณ ปัจจุบัน และข้อมูลย้อนหลังของการใช้งานของผู้ใช้งานระบบที่สำคัญต่างๆ รวมทั้งตรวจสอบการทำงานของระบบ (Health Check) และข้อมูลสถิติด้านความปลอดภัย ผ่าน Web Browser ได้
 - 3.3.19. สามารถสร้างรายงานผ่านทาง Web browser ได้
 - 3.3.20. สามารถสร้างรายงานในรูปแบบของ PDF และ CSV ได้
 - 3.3.21. สามารถสร้างและส่งรายงานโดยอัตโนมัติตามระยะเวลาที่กำหนดผ่านทาง e-mail ได้ เช่น ทุกๆ 1 เดือน เป็นต้น
 - 3.3.22. สามารถส่ง alert ผ่านทาง e-mail หรือ SNMP ได้
- 3.4 เครื่องหมายรับรองความปลอดภัยทางอิเล็กทรอนิกส์ (SSL) โดยมี คุณลักษณะดังนี้**
- 3.4.1 SSL Certificate ที่ออกหรืออนุมัติโดย Certificate Authority ที่ก่อตั้งในปี 2539 หรือก่อนหน้า
 - 3.4.2 รองรับ Encryption strength สูงสุด 256 Bit
 - 3.4.3 รองรับ Root strength 2048 Bit
 - 3.4.4 รองรับ SHA-2 algorithms

- 3.4.5 รองรับการตรวจสอบองค์กรก่อนออก SSL Certificate ระดับ Organization Validation
- 3.4.6 รองรับการแสดงข้อมูลองค์กรใน SSL Certificate
- 3.4.7 รองรับการใช้งานกับทุก Browser
- 3.4.8 รองรับการติดตั้งได้ไม่จำกัด Server (Unlimited SSL server licensing) โดยไม่มีค่าใช้จ่าย
- 3.4.9 รองรับการ Reissues ได้ไม่จำกัด (Unlimited reissues) โดยไม่มีค่าใช้จ่าย
- 3.4.10 รองรับทุก sub-domain ภายใน domain เดียวกันได้ (Unlimited sub domain)
- 3.4.11 รองรับ 3 sub-domain เพิ่มเติมได้แก่ owa.domain.com, mail.domain.com, autodiscover.domain.com โดยไม่มีค่าใช้จ่าย
- 3.4.12 รองรับการให้บริการ Malware Scanning โดยไม่มีค่าใช้จ่าย
- 3.4.13 รองรับการให้ประกันมูลค่า \$1,250,000 ตามเงื่อนไขของ Certificate Authority

4. การส่งมอบงานและการจ่ายเงิน

ผู้รับจ้างจะต้องจัดทำเอกสารรายงานให้กับทางสำนักงานฯ เพื่อให้คณะกรรมการตรวจรับใช้ในการตรวจรับงาน ประกอบไปด้วย

- รายงานปริมาณการใช้งานอินเทอร์เน็ตและอินทราเน็ตของสำนักงานฯ ในแต่ละวัน
 - รายงานปริมาณการใช้งานทางด้านความมั่นคงปลอดภัยสารสนเทศเบื้องต้น โดยสรุปผลการป้องกันและโจมตีทางเครือข่าย พร้อมทั้งให้คำแนะนำในการแก้ไขปัญหา หรือข้อควรระวังให้กับเจ้าหน้าที่สำนักงานฯ
- สำนักงานฯ จะชำระเงินเป็นรายเดือน หลังจากผู้รับจ้างได้ให้บริการเรียบร้อย และส่งมอบงานภายในวันที่ 15 ของเดือนถัดไป และคณะกรรมการตรวจรับได้ตรวจรับงานที่ส่งมอบในแต่ละงวดเรียบร้อยแล้ว

5. ค่าปรับ

- 5.1. ในกรณีเกิดเหตุขัดข้องจนไม่สามารถใช้งานได้ ผู้รับจ้างจะต้องแก้ไขให้สามารถกลับมาใช้งานได้ระดับความรุนแรง ตามรายละเอียดดังนี้
- 5.1.1. รุนแรงมาก เกิดข้อผิดพลาด/บกพร่องของระบบขั้นรุนแรงมากกับระบบ และส่งผลกระทบต่อการทำงานของบริการอื่น ๆ ต้องหยุดชะงักหรือไม่สามารถให้บริการได้ ซึ่งจำเป็นต้องได้รับการแก้ไขโดยด่วนที่สุด อาทิ ระบบ Firewall หลัก หยุดทำงาน ระบบ VPN Server หยุดทำงาน จะต้องมีการ Response time ภายในระยะเวลา 30 นาที และ Recovery time ภายในระยะเวลา 4 ชั่วโมง
 - 5.1.2. รุนแรง เกิดข้อผิดพลาด/บกพร่องของระบบขั้นรุนแรงกับระบบ และส่งผลกระทบต่อการทำงานของธุรกิจ และมีความจำเป็นต้องแก้ไขอย่างทันด่วนที่ อาทิ ระบบที่มีการทำงานแบบ Active-Standby หรือ Load Balance หยุดทำงานไปหนึ่งตัวจะต้องมีการ Response time ภายในระยะเวลา 60 นาที และ Recovery time ภายในระยะเวลา 4 ชั่วโมง
 - 5.1.3. ปานกลาง เกิดข้อผิดพลาด/บกพร่องของระบบขั้นรุนแรงปานกลางกับระบบ และส่งผลกระทบต่อกิจกรรมที่สำคัญและจำเป็นต่อการดำเนินธุรกิจ ส่งผลให้ธุรกิจไม่สามารถดำเนินการได้อย่างมี

ประสิทธิภาพ และจำเป็นจะต้องแก้ไขอย่างเร่งด่วน อาทิ ระบบ Firewall หลักทำงานไม่เสถียร จะต้องมีการ Response time ภายในระยะเวลา 2 ชั่วโมง และ Recovery time ภายในระยะเวลา 8 ชั่วโมง

5.1.4.ต่ำ เกิดปัญหา หรือ คำร้องที่มีผลกระทบต่อประสิทธิภาพการทำงานทั่วไป แต่ไม่มีผลกระทบต่อ การดำเนินธุรกิจโดยภาพรวม อาทิ ระบบ Firewall มีความผิดปกติ (ไม่มีผลต่อการให้บริการ) จะต้องมีการ Response time ภายในระยะเวลา 4 ชั่วโมง และ Recovery time ภายในระยะเวลา 12 ชั่วโมง

5.2. เมื่อพ้นกำหนดแล้ว สำนักงานฯ ขอสงวนสิทธิ์ในการปรับต่อวัน ในอัตราร้อยละ 0.1 ของราคาจ้าง บำรุงรักษา ตามแยกตาม ราคาที่เสนอ ด้านเครือข่าย และ ด้านความปลอดภัย (โดยเศษของชั่วโมงให้นับเป็นหนึ่งวัน)