

ข้อกำหนดรายละเอียดคุณลักษณะเฉพาะของพัสดุ (Terms of Reference : TOR)  
การจัดซื้ออุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอปพลิเคชัน  
(Application Firewall) จำนวน ๑ ระบบ

๑. ความเป็นมา

สำนักงาน กสทช. ได้มีการจัดหาอุปกรณ์รักษาความปลอดภัย (Firewall) เครือข่ายสารสนเทศ เพื่อทำหน้าที่ตรวจสอบและควบคุมระบบข้อมูลที่มาจากอินเทอร์เน็ต หรือมาจากเครือข่ายภายใน การมีอุปกรณ์รักษาความปลอดภัย (Firewall) นี้จะช่วยให้คอมพิวเตอร์ในเครือข่ายได้รับการป้องกันไม่ให้ Hacker หรือซอฟต์แวร์อันตรายโจมตีเข้าถึงเครื่องคอมพิวเตอร์ผ่านทางเครือข่ายหรืออินเทอร์เน็ต โดยอุปกรณ์รักษาความปลอดภัย (Firewall) เครือข่ายสารสนเทศ สำนักงาน กสทช. ปัจจุบัน ได้แก่ ระบบและอุปกรณ์รักษาความปลอดภัย (Firewall) เครือข่ายสารสนเทศ สำนักงาน กสทช. สัญญาเลขที่ ๘๖๒๐๒๒๗ ลงวันที่ ๒๗ กันยายน ๒๕๖๒, และได้จ้างเหมาบริการบำรุงรักษาจนถึงปัจจุบัน

เนื่องจากระบบและอุปกรณ์รักษาความปลอดภัย (Firewall) เครือข่ายสารสนเทศ เป็นอุปกรณ์เก่า และมีการใช้งานมาเป็นเวลานาน ในปัจจุบันมีการบุกรุกและโจมตีในรูปแบบใหม่ ๆ ที่มีความก้าวหน้าและรุนแรงมากขึ้น ทำให้ขาดประสิทธิภาพต่อการป้องกันการโจมตีจากภายนอกและเครือข่ายภายในสำนักงาน กสทช.

ดังนั้นจึงมีความจำเป็นต้องจัดซื้ออุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอปพลิเคชัน (Application Firewall) เพื่อป้องกันการถูกโจมตีจากภายนอกและภายในเครือข่าย สำนักงาน กสทช. ให้มีประสิทธิภาพมากยิ่งขึ้น

๒. วัตถุประสงค์

จัดซื้ออุปกรณ์รักษาความปลอดภัย (Firewall) เครือข่ายสารสนเทศ สำนักงาน กสทช. ประกอบด้วย Firewall สำหรับอินเทอร์เน็ตโซน เพื่อมาทดแทนอุปกรณ์เดิมที่เสื่อมสภาพ และขาดประสิทธิภาพ

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพื้นฐานที่กำหนด ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๒ ตลอดจนแนวปฏิบัติตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ตามที่แนบในภาคผนวก ๑

๓.๒ ผู้ยื่นข้อเสนอต้องเป็นผู้ผลิตหรือเป็นสาขาของผู้ผลิตในประเทศไทย หรือได้รับการแต่งตั้งจากผู้ผลิตหรือสาขาของผู้ผลิตให้เป็นตัวแทนจำหน่ายในประเทศไทย

๔. รายละเอียดคุณลักษณะเฉพาะ

๔.๑ ข้อกำหนดทั่วไป

๔.๑.๑ อุปกรณ์รักษาความปลอดภัย (Firewall) เครือข่ายสารสนเทศ สำนักงาน กสทช. ต้องเป็นเครื่องใหม่ไม่เคยผ่านการใช้งานมาก่อน

๔.๑.๒ ผู้ขายต้องติดตั้งโปรแกรมสำเร็จรูปและแอปพลิเคชันที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และสำนักงาน กสทช. มีสิทธิ์ใช้ได้ถูกต้องตามกฎหมาย โดยก่อนการติดตั้งต้องขอความเห็นชอบจากสำนักงานเทคโนโลยีสารสนเทศก่อนการดำเนินการ

๔.๑.๓ ผู้ขายต้องแนบแค็ตตาล็อก/รายละเอียดผลิตภัณฑ์ที่เสนอ (เฉพาะในส่วนของความต้องการด้านฮาร์ดแวร์และซอฟต์แวร์) พร้อมทั้งเปรียบเทียบรายละเอียดของผลิตภัณฑ์ที่นำเสนอกับรายละเอียดตามข้อกำหนดของ สำนักงาน กสทช. แต่ละข้อมาพร้อมใบเสนอราคา

๔.๑.๔ ผู้ขายต้องดำเนินการจัดฝึกอบรมระบบฯ ที่นำเสนอทั้งหมดที่เกี่ยวข้องกับการใช้งาน โดยละเอียดและฝึกปฏิบัติการใช้งานให้กับเจ้าหน้าที่ผู้ดูแลระบบจำนวนไม่น้อยกว่า ๕ คน โดยไม่คิดค่าใช้จ่าย ใดๆ ทั้งสิ้น พร้อมทั้งส่งมอบคู่มือการใช้งานระบบฯ ที่เสนอ ในรูปแบบเอกสาร และ CD/DVD ตามจำนวนผู้เข้ารับการฝึกอบรม

#### ๔.๒ ความต้องการทางด้านเทคนิค

อุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอปพลิเคชัน(Application Firewall) ซอฟต์แวร์บริหารจัดการข้อมูลอุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

๔.๒.๑ อุปกรณ์รักษาความปลอดภัย สำหรับอินเทอร์เน็ตโซน ๑ ชุด จำนวน ๒ เครื่อง มีคุณสมบัติอย่างน้อยดังต่อไปนี้

๔.๒.๑.๑ เป็น Firewall Appliance ที่ใช้เทคโนโลยีแบบ Stateful Inspection และมี Firewall Throughput ไม่น้อยกว่า ๗๒.๖ Gbps

๔.๒.๑.๒ มี Next Generation Firewall Throughput ไม่น้อยกว่า ๓๓.๓ Gbps และ Threat Prevention Throughput ไม่น้อยกว่า ๑๑ Gbps

๔.๒.๑.๓ รองรับ VPN Throughput ไม่น้อยกว่า ๔๐ Gbps

๔.๒.๑.๔ สามารถรองรับ Concurrent Connections อย่างน้อย ๑๖,๒๐๐,๐๐๐ Connections และรองรับจำนวน Connection ไม่น้อยกว่า ๓๕๕,๐๐๐ Connections ต่อวินาที

๔.๒.๑.๕ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T จำนวนไม่น้อยกว่า ๘ พอร์ต และมีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑/๑๐GbE SFP+ จำนวนไม่น้อยกว่า ๔ พอร์ต พร้อมเสนอ Transceiver ชนิด ๑๐G SR จำนวน ๓ โมดูล โดย Transceiver ที่นำเสนอต้องเป็นผลิตภัณฑ์ยี่ห้อเดียวกับอุปกรณ์ที่นำเสนอ

๔.๒.๑.๖ อุปกรณ์มี Storage บนตัวอุปกรณ์แบบ SSD ขนาดไม่น้อยกว่า ๙๖๐ GB

๔.๒.๑.๗ มี IPS throughput ไม่น้อยกว่า ๔๖.๔ Gbps

๔.๒.๑.๘ สามารถตรวจสอบและควบคุม Applications ได้อย่างน้อย ๑๐,๐๐๐ Applications และ Social Network Widgets ได้อย่างน้อย ๒๕๐,๐๐๐ Widgets

๔.๒.๑.๙ สามารถมีกลไกการทำงานในลักษณะของการแจ้งเตือนและสอบถามผู้ใช้งานได้ในแบบ Real-Time เพื่อเป็นการให้ข้อมูลและสอบถามผู้ใช้งาน Applications และ URLs ในแต่ละ Filtering rule ได้

๔.๒.๑.๑๐ รองรับการกำหนด Security Policy ตาม User, User Group และ Machine ด้วยการ Integrate เข้ากับ Active Directory ได้โดยไม่ต้องติดตั้งซอฟต์แวร์ (Agent) เพิ่มเติมบน Domain Controller และเครื่องของผู้ใช้งาน รวมทั้งสามารถทำการ Authentication ผ่าน Browser ได้สำหรับ ผู้ใช้งานที่ไม่ได้อยู่ใน Domain ขององค์กร

- ๔.๒.๑.๑๑ สามารถแสดงสถิติการใช้งาน (Hit Count Statistic) ของแต่ละ Policy ทั้ง access control rule และ NAT rule ได้
- ๔.๒.๑.๑๒ สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPFv๒ และ v๓ , BGP, RIP, IGMP และ PIM ได้เป็นอย่างดีน้อย
- ๔.๒.๑.๑๓ สามารถทำงานในลักษณะ ISP Redundancy ได้ทั้งแบบ Primary/Backup และ Load Sharing
- ๔.๒.๑.๑๔ สามารถทำงานเป็น Intrusion Prevention System (IPS) ได้ โดยจะต้องมีพื้นฐานการทำงานในการป้องกันภัยคุกคามได้แก่ known exploit, protocol misuse, tunneling attempt, vulnerability และ outbound malware communication เป็นอย่างน้อย
- ๔.๒.๑.๑๕ การทำงานของ IPS สามารถทำงานในลักษณะของ Fail-open เมื่อระดับการทำงานของ CPU และ Memory เกินค่า Threshold ที่กำหนด และสามารถกำหนดค่า Threshold ตามที่ต้องการได้
- ๔.๒.๑.๑๖ สามารถตรวจจับ Virus โดยป้องกันการดาวน์โหลดไฟล์ที่มีมัลแวร์ และตรวจสอบไฟล์ที่มีการมีการย่อขนาดไฟล์ได้เช่น zip, gzip, gz, ๗z, rar, tar เป็นอย่างน้อย รวมทั้งสามารถ scan virus ตาม link ที่แนบในอีเมลได้
- ๔.๒.๑.๑๗ สามารถตรวจจับ Bot ได้โดยวิธีการตรวจสอบจาก C&C address หรือ website, communication pattern ของ Bot และ Bot behavior ได้เป็นอย่างดีน้อย
- ๔.๒.๑.๑๘ สามารถป้องกันการโจมตีผ่านโปรโตคอล DNS ในรูปแบบ DGA (Domain Generation Algorithm) และ DNS Tunneling โดยการใช้ Machine Learning ในการตรวจสอบได้แบบ real time โดยไม่ต้องรอเวลาในการอัปเดต ได้เป็นอย่างดีน้อย
- ๔.๒.๑.๑๙ สามารถรับข้อมูล Syslog message เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้ หรือนำเสนออุปกรณ์อื่นเพิ่มเติมเพื่อทำงานเป็นไปตามข้อกำหนดได้
- ๔.๒.๑.๒๐ สามารถป้องกัน Spam ที่มาในรูปแบบของ Email ผ่านโปรโตคอล POP๓ และ SMTP และสามารถป้องกันโดยใช้รูปแบบ IP reputation anti-spam, Content-based anti-spam, Block/allow list anti-spam ได้
- ๔.๒.๑.๒๑ สามารถทำงานแบบ URL Filtering เพื่อเพิ่มความปลอดภัยในการใช้งาน Web site ได้ โดยมีการจัดประเภทของ Content ได้ทั้งแบบ Pre-defined category และ custom category ได้ พร้อมทั้งสามารถ Update ฐานข้อมูลได้อย่างสม่ำเสมอ
- ๔.๒.๑.๒๒ สามารถทำงานแบบ High Availability ทั้งแบบ Active/Active และ Active/Passive โดยสามารถทำ Session failover ในกรณีเกิด Device และ link failure ได้ พร้อมทั้งสามารถทำ High Availability อุปกรณ์ที่ติดตั้ง Software version ต่างกันภายใน Cluster เดียวกันได้
- ๔.๒.๑.๒๓ รองรับการทำงานร่วมกับอุปกรณ์กระจาย Traffic (Traffic Distribution) ภายใต้ผลิตภัณฑ์ยี่ห้อเดียวกันสำหรับใช้กระจายปริมาณ Traffic ในการ

ตรวจสอบเพื่อขยายประสิทธิภาพการทำงานและการทำ Redundancy แบบ N+๑ ได้ในอนาคต

๔.๒.๑.๒๔ สามารถจัดการระบบผ่านทาง SSH, Web-based GUI, Application GUI และ Console ได้

๔.๒.๑.๒๕ มีแหล่งจ่ายไฟจำนวนไม่น้อยกว่า ๒ หน่วยทำงานแบบ hot-swappable หรือแบบ replaceable และมีพัดลมระบายอากาศไม่น้อยกว่า ๒ หน่วย

๔.๒.๑.๒๖ ผลิตภัณฑ์ที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย CB, UL, FCC, CE และ VCCI เป็นอย่างน้อย

๔.๒.๑.๒๗ ผลิตภัณฑ์ที่นำเสนอต้องได้รับการรับรองจาก Gartner ให้อยู่ในกลุ่ม Leader ของผลิตภัณฑ์ประเภท Network Firewall ปี ๒๐๒๒ เป็นอย่างน้อย

๔.๒.๒ อุปกรณ์รักษาความปลอดภัย สำหรับ Server Farm ๑ ชุด จำนวน ๒ เครื่อง มีคุณสมบัติอย่างน้อยดังต่อไปนี้

๔.๒.๒.๑ เป็น Firewall Appliance ที่ใช้เทคโนโลยีแบบ Stateful Inspection และมี Firewall Throughput ไม่น้อยกว่า ๕๕ Gbps

๔.๒.๒.๒ มี Next Generation Firewall Throughput ไม่น้อยกว่า ๑๘.๖ Gbps และ Threat Prevention Throughput ไม่น้อยกว่า ๔.๙๕ Gbps

๔.๒.๒.๓ รองรับ VPN Throughput ไม่น้อยกว่า ๒๒.๑ Gbps

๔.๒.๒.๔ สามารถรองรับ Concurrent Connections อย่างน้อย ๑๖,๒๐๐,๐๐๐ Connections และรองรับจำนวน-Connection ไม่น้อยกว่า ๑๙๐,๐๐๐ Connections ต่อวินาที

๔.๒.๒.๕ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T จำนวนไม่น้อยกว่า ๘ พอร์ต และมีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑/๑๐GbE SFP+ จำนวนไม่น้อยกว่า ๘ พอร์ต พร้อมเสนอ Transceiver ชนิด ๑๐G SR จำนวน ๓ โมดูล และชนิด ๑๐๐๐BASE SX จำนวน ๔ โมดูล โดย Transceiver ที่นำเสนอต้องเป็นผลิตภัณฑ์ที่ห่อเดียวกับอุปกรณ์ที่นำเสนอ

๔.๒.๒.๖ อุปกรณ์มี Storage บนตัวอุปกรณ์แบบ SSD ขนาดไม่น้อยกว่า ๔๘๐ GB

๔.๒.๒.๗ มี IPS throughput ไม่น้อยกว่า ๒๕.๗ Gbps

๔.๒.๒.๘ สามารถตรวจสอบและควบคุม Applications ได้อย่างน้อย ๑๐,๐๐๐ Applications และ Social Network Widgets ได้อย่างน้อย ๒๕๐,๐๐๐ Widgets

๔.๒.๒.๙ สามารถมีกลไกการทำงานในลักษณะของการแจ้งเตือนและสอบถามผู้ใช้งานได้ในแบบ Real-Time เพื่อเป็นการให้ข้อมูลและสอบถามผู้ใช้งาน Applications และ URLs ในแต่ละ Filtering rule ได้

๔.๒.๒.๑๐ รองรับการกำหนด Security Policy ตาม User, User Group และ Machine ด้วยการ Integrate เข้ากับ Active Directory ได้โดยไม่ต้องติดตั้งซอฟต์แวร์ (Agent) เพิ่มเติมบน Domain Controller และเครื่องของผู้ใช้งาน รวมทั้งสามารถทำการ Authentication ผ่าน Browser ได้สำหรับผู้ใช้งานที่ไม่ได้อยู่ใน Domain ขององค์กร

- ๔.๒.๒.๑๑ สามารถแสดงสถิติการใช้งาน (Hit Count Statistic) ของแต่ละ Policy ทั้ง access control rule และ NAT rule ได้
- ๔.๒.๒.๑๒ สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPFv๒ และ v๓ , BGP, RIP, IGMP และ PIM ได้เป็นอย่างดีน้อย
- ๔.๒.๒.๑๓ สามารถทำงานในลักษณะ ISP Redundancy ได้ทั้งแบบ Primary/Backup และ Load Sharing
- ๔.๒.๒.๑๔ สามารถทำงานเป็น Intrusion Prevention System (IPS) ได้ โดยจะต้องมีพื้นฐานการทำงานในการป้องกันภัยคุกคามได้แก่ known exploit, protocol misuse, tunneling attempt, vulnerability และ outbound malware communication เป็นอย่างน้อย
- ๔.๒.๒.๑๕ การทำงานของ IPS สามารถทำงานในลักษณะของ Fail-open เมื่อระดับการทำงานของ CPU และ Memory เกินค่า Threshold ที่กำหนด และสามารถกำหนดค่า Threshold ตามที่ต้องการได้
- ๔.๒.๒.๑๖ สามารถตรวจจับ Virus โดยป้องกันการดาวน์โหลดไฟล์ที่มีมัลแวร์ และ ตรวจสอบไฟล์ที่มีการมีการย่อขนาดไฟล์ได้เช่น zip,gzip,gz,tz,rar,tar เป็นอย่างน้อย รวมทั้งสามารถ scan virus ตาม link ที่แนบในเนื้อเมลล์ได้
- ๔.๒.๒.๑๗ สามารถตรวจจับ Bot ได้โดยวิธีการตรวจสอบจาก C&C address หรือ website, communication pattern ของ Bot และ Bot behavior ได้เป็นอย่างดีน้อย
- ๔.๒.๒.๑๘ สามารถป้องกันการโจมตีผ่านโปรโตคอล DNS ในรูปแบบ DGA (Domain Generation Algorithm) และ DNS Tunneling โดยการใช้ Machine Learning ในการตรวจสอบได้แบบ real time โดยไม่ต้องรอเวลาในการอัปเดต ได้เป็นอย่างดีน้อย
- ๔.๒.๒.๑๙ สามารถรับข้อมูล Syslog message เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้ หรือนำเสนออุปกรณ์อื่นเพิ่มเติมเพื่อทำงานเป็นไปตามข้อกำหนดได้
- ๔.๒.๒.๒๐ สามารถป้องกัน Spam ที่มาในรูปแบบของ Email ผ่านโปรโตคอล POP๓ และ SMTP และสามารถป้องกันโดยใช้รูปแบบ IP reputation anti-spam, Content-based anti-spam, Block/allow list anti-spam ได้
- ๔.๒.๒.๒๑ สามารถทำงานแบบ URL Filtering เพื่อเพิ่มความปลอดภัยในการใช้งาน Web site ได้ โดยมีการจัดประเภทของ Content ได้ทั้งแบบ Pre-defined category และ custom category ได้ พร้อมทั้งสามารถ Update ฐานข้อมูลได้อย่างสม่ำเสมอ
- ๔.๒.๒.๒๒ สามารถทำงานแบบ High Availability ทั้งแบบ Active/Active และ Active/Passive โดยสามารถทำ Session failover ในกรณีเกิด Device และ link failure ได้ พร้อมทั้งสามารถทำ High Availability อุปกรณ์ที่ติดตั้ง Software version ต่างกันภายใน Cluster เดียวกันได้
- ๔.๒.๒.๒๓ รองรับการทำงานร่วมกับอุปกรณ์กระจาย Traffic (Traffic Distribution) ภายใต้อัตลักษณ์ที่หือเดียวกันสำหรับใช้กระจายปริมาณ Traffic ในการ

ตรวจสอบเพื่อขยายประสิทธิภาพการทำงานและการทำ Redundancy แบบ N+๑ ได้ในอนาคต

- ๔.๒.๒.๒๔ สามารถจัดการระบบผ่านทาง SSH, Web-based GUI, Application GUI และ Console ได้
- ๔.๒.๒.๒๕ มีแหล่งจ่ายไฟจำนวนไม่น้อยกว่า ๒ หน่วย และมีพัดลมระบายอากาศไม่น้อยกว่า ๒ หน่วย
- ๔.๒.๒.๒๖ ผลิตภัณฑ์ที่หือที่นำเสนอต้องได้รับการรับรองมาตรฐานความปลอดภัย CB, UL, FCC, CE และ VCCI เป็นอย่างน้อย
- ๔.๒.๒.๒๗ ผลิตภัณฑ์ที่หือที่นำเสนอต้องได้รับการรับรองจาก Gartner ให้อยู่ในกลุ่ม Leader ของผลิตภัณฑ์ประเภท Network Firewall ปี ๒๐๒๒ เป็นอย่างน้อย
- ๔.๒.๓ ซอฟต์แวร์บริหารจัดการข้อมูลอุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์
  - ๔.๒.๓.๑ เป็นซอฟต์แวร์ระบบบริหารจัดการที่มีระบบปฏิบัติการแบบเฉพาะที่ทำการ Hardening เรียบร้อยแล้ว สามารถจัดการ policy, จัดเก็บ log, วิเคราะห์ และทำรายงานได้บนอุปกรณ์เดียวกัน และบริหารจัดการผ่าน Application GUI
  - ๔.๒.๓.๒ สามารถบริหารจัดการอุปกรณ์ Security Gateway ได้อย่างน้อย ๕ Gateways
  - ๔.๒.๓.๓ สามารถสื่อสารแบบเข้ารหัสกับอุปกรณ์ Security Gateways ในแบบ Certificate ได้เป็นอย่างน้อย
  - ๔.๒.๓.๔ สามารถแบ่งกลุ่มของ Security Policy เป็น Section Title เพื่อความสะดวกในการบริหารจัดการ Security Policy จำนวนมากได้และสามารถสร้าง policy โดยแบ่งชั้นแบบ inline layer หรือ sub-rule ได้
  - ๔.๒.๓.๕ มีกลไกในการตรวจสอบ Security Policy แบบ Heuristic Verification เพื่อให้แน่ใจได้ว่า Security Policy ทั้งหมดใช้ร่วมงานกันได้และไม่มีการซ้ำซ้อนเกิดขึ้น
  - ๔.๒.๓.๖ สามารถจัดการ security policy ต่างๆ และจัดเก็บ Log ได้ทั้งแบบ real time และตรวจสอบย้อนหลัง
  - ๔.๒.๓.๗ ระบบสามารถให้ผู้บริหารจัดการระบบเข้าใช้งานได้พร้อมกันหลายคน โดยแยกการทำงานกันไม่ให้เกิดการขัดแย้งของ policy ได้
  - ๔.๒.๓.๘ สามารถกำหนด Threat Prevention Profiles สำหรับป้องกันการโจมตีแบบอัตโนมัติ (Autonomous) ได้ โดยมี Profile ให้เลือกได้แก่ recommended และ strict profile สำหรับ perimeter, Data Center East/West, Internal network และ Guest network ได้เป็นอย่างน้อย
  - ๔.๒.๓.๙ สามารถหาความสัมพันธ์ (Correlation) ของ Log ต่างๆ ที่จัดเก็บ พร้อมทั้งแสดงข้อมูลเป็นเหตุการณ์ (Event) ต่างๆ และ แนวโน้มของเหตุการณ์ ในลักษณะของ Timelines, Charts และ Maps ได้
  - ๔.๒.๓.๑๐ สามารถทำการกำหนด Exception ในหมวดของ IPS Protection ได้โดยตรงจาก Log หรือ Event ทันที
  - ๔.๒.๓.๑๑ สามารถใช้งานแบบ Indexed Search Logging ได้ โดยค้นหา Log ได้แบบ Google-Like Search และสามารถแสดง Log ที่เกิดจาก feature Firewall,

- IPS, URL Filtering, Anti-Virus และ Anti-Bot บนหน้า view เดียวกันแบบ Single Unified Log View ได้
- ๔.๒.๓.๑๒ สามารถจัดทำรายงานแบบ Predefined Report ได้แก่รายงานประเภท Threat Prevention Report, Application and URL Filtering Report และ User Activity Report ได้เป็นอย่างดี รวมทั้งสามารถปรับแต่ง (customize) รายงานเพิ่มเติมได้
- ๔.๒.๓.๑๓ สามารถกำหนดช่วงเวลาที่ต้องการให้สร้างและแสดงผลรายงานได้ (scheduled report) และกำหนดให้ส่งรายงานผ่านทาง Email ได้เป็นอย่างดี
- ๔.๒.๓.๑๔ มีกระบวนการในการขออนุมัติการแก้ไขเปลี่ยนแปลง Policy Firewall และ กำหนดสิทธิ์แยกผู้ดูแลระบบให้เป็นผู้ขอและผู้อนุมัติ โดยระบบสามารถส่ง อีเมลเพื่อแจ้งขออนุมัติพร้อมรายละเอียดการแก้ไขเปลี่ยนแปลง Policy ในรูปแบบรายงาน (Review Change Report) โดยอัตโนมัติได้เป็นอย่างดี
- ๔.๒.๓.๑๕ รองรับการตรวจสอบแบบ Real Time Compliance Monitoring สำหรับ อุปกรณ์ Security ที่เสนอมาได้ และสามารถรองรับการตรวจสอบตามกฎ มาตรฐานสากลต่างๆ เช่น PCI-DSS, HIPPA, SOX และ ISO ๒๗๐๐๒ ได้ในอนาคต
- ๔.๒.๓.๑๖ ต้องติดตั้งซอฟต์แวร์บริหารจัดการข้อมูลอุปกรณ์รักษาความปลอดภัย บนเครือข่ายคอมพิวเตอร์ บนระบบคอมพิวเตอร์แม่ข่ายเสมือน ที่สำนักงาน กสทช. จัดเตรียมไว้ให้

๕. กำหนดเวลาส่งมอบพัสดุ

ภายในระยะเวลา ๑๕๐ วัน นับตั้งแต่วันที่ลงนามในสัญญา

๖. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

สำนักงาน กสทช. จะพิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา

๗. วงเงินงบประมาณ

วงเงินรวมทั้งสิ้น ๑๓,๓๗๕,๐๐๐ บาท (สิบสามล้านสามแสนเจ็ดหมื่นห้าพันบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายที่ปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากงบประมาณรายจ่ายปี ๒๕๖๘ รายจ่ายเกี่ยวกับ ครุภัณฑ์ ที่ดิน และสิ่งก่อสร้าง รายการครุภัณฑ์คอมพิวเตอร์

๘. งานงวดงานและการจ่ายเงิน

สำนักงาน กสทช. จะชำระเงินค่าพัสดุเป็นจำนวนงวดเดียว เมื่อผู้ขายส่งมอบพัสดุล้วนถูกต้อง และ คณะกรรมการตรวจรับ พัสดุได้ตรวจรับเรียบร้อยแล้ว

#### ๙. อัตราค่าปรับ

ผู้ขายจะต้องติดตั้งและส่งมอบงานแล้วเสร็จตามสัญญา มิฉะนั้นต้องชำระค่าปรับให้ สำนักงาน กสทช. เป็นรายวันในอัตราร้อยละ ๐.๒ (๐.๒%) ของค่าพัสดุที่ยังไม่ได้รับมอบ จนถึงวันที่ผู้ขายได้ส่งมอบงาน ให้สำนักงาน กสทช. เป็นที่เรียบร้อยแล้ว ในระหว่างที่สำนักงาน กสทช. ยังไม่ได้ใช้สิทธิ์บอกเลิกสัญญานั้น หากสำนักงาน กสทช. เห็นว่าผู้ขายไม่อาจปฏิบัติตามสัญญาต่อไปได้ สำนักงาน กสทช. จะใช้สิทธิ์บอกเลิกสัญญากับเรียกร้องให้ชดใช้ราคาที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญาถ้าสำนักงาน กสทช. ดำเนินการ โดยการจัดซื้อจากบุคคลอื่นเต็มจำนวน หรือเฉพาะจำนวนที่ขาดส่ง และถ้าสำนักงาน กสทช. ได้แจ้งข้อเรียกร้อง ให้ชำระค่าปรับไปยังผู้ขายเมื่อครบกำหนดส่งมอบแล้ว สำนักงาน กสทช. มีสิทธิ์ที่จะปรับผู้ขายจนถึงวันบอกเลิกสัญญาได้อีกด้วย

#### ๑๐. การปฏิบัติตามกฎหมายที่เกี่ยวข้อง

๑๐.๑ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะ หรือผู้ได้รับการคัดเลือก จะต้องดำเนินการ ปฏิบัติให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ที่เกี่ยวข้อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. ฉบับล่าสุด ซึ่งรวมถึงหลักการวิศวกรรมความมั่นคงปลอดภัย (แบบฟอร์มความต้องการด้านความมั่นคง ปลอดภัยของระบบทางด้านเทคนิค (System Security Requirement) เอกสารเผยแพร่สามารถศึกษา รายละเอียดหรือ download ในเว็บไซต์สำนักงาน กสทช. ([www.nbt.go.th](http://www.nbt.go.th))

๑๐.๑.๑ กรณีมีการใช้บริการคลาวด์ (Cloud) ต้องปฏิบัติตามข้อกำหนดด้านการใช้บริการ คลาวด์ (Cloud Security Requirement) ตามที่ผู้ว่าจ้างกำหนด

๑๐.๑.๒ ตรวจสอบความมั่นคงปลอดภัยของซอร์สโค้ด (Source Code Scanning) และ ดำเนินการแก้ไขก่อนนำระบบขึ้นให้บริการ

๑๐.๒ กรณีที่ขอบเขตของงานเกี่ยวข้องกับการประมวลผล (เก็บรวบรวม ใช้ เปิดเผย) ข้อมูลส่วนบุคคล ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะ หรือผู้ได้รับการคัดเลือก ต้องดำเนินการตามเงื่อนไขและ รายละเอียดตามที่กำหนดไว้ในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับสำนักงาน กสทช. (ภาคผนวก ๒)

#### ๑๑. เงื่อนไขอื่น ๆ

๑๑.๑ ผู้ขายจะต้องบำรุงรักษา และรับประกันการใช้งานระบบทั้งฮาร์ดแวร์ และซอฟต์แวร์ระบบ ที่นำเสนอ ตลอดจนจะต้องรับผิดชอบดูแลแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นในระบบ รวมทั้งปรับแต่งระบบ ให้สามารถ ใช้งานได้อย่างมีประสิทธิภาพ

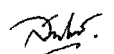
๑๑.๒ การรับประกัน มีระยะเวลาทั้งสิ้น ๓ ปี โดยนับตั้งแต่วันที่สำนักงาน กสทช. ได้รับมอบระบบฯ ไว้ใช้งาน โดยสมบูรณ์ทั้งระบบ หากมีการชำรุดบกพร่องหรือข้อขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายจะต้อง จัดเจ้าหน้าที่เข้ามาซ่อมแซม แก้ไข ภายในระยะเวลา ๒๔ ชั่วโมง และให้แล้วเสร็จโดยเร็วที่สุด ภายใน ๔๘ ชั่วโมง นับตั้งแต่วันที่ได้รับแจ้งจากสำนักงาน กสทช. โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น หากผู้ขายดำเนินการล่าช้า กว่าเงื่อนไขที่กำหนดไว้ ผู้ขายจะต้องชำระค่าปรับให้แก่ สำนักงาน กสทช. เป็นรายวัน ที่ล่าช้าในอัตราร้อยละ ๑,๐๐๐ บาท ไปจนถึงวันที่ผู้ขาย แก้ไขระบบฯ ให้สามารถใช้งานได้เป็นปกติ

๑๑.๓ ผู้ขายจะต้องมี Help Desk ซึ่งสามารถติดต่อประสานงานและร้องขอความช่วยเหลือให้คำปรึกษา ทางโทรศัพท์ ได้ในเวลาราชการ ตั้งแต่วันจันทร์-ศุกร์ เวลา ๐๘.๓๐ น. - ๑๗.๐๐ น.

### คุณสมบัติของผู้ยื่นข้อเสนอ

๑. มีความสามารถตามกฎหมาย
๒. ไม่เป็นบุคคลล้มละลาย
๓. ไม่อยู่ระหว่างเลิกกิจการ
๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
๕. ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา
๗. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว
๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน กสทช. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้
๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอ ได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น
๑๐. ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง
๑๑. ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้
  - (๑) กรณีเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ
  - (๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งยังไม่มีงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่น้อยกว่า ๓,๐๐๐,๐๐๐ บาท
  - (๓) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ผู้ยื่นข้อเสนอสามารถขอหนังสือรับรองวงเงินสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหรือบริษัททุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารกลางของประเทศนั้น ตามรายชื่อบริษัทเงินทุนที่ธนาคารกลางของประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน โดยต้องมียอดเงินรวมของวงเงินสินเชื่อไม่น้อยกว่า ๓,๓๔๓,๗๕๐.- บาท คิดเป็น ๑

proof





ใน ๔ ของมูลค่าโครงการหรือรายการที่ยื่นเสนอในแต่ละครั้ง ทั้งนี้ สำหรับธนาคารภายในประเทศหนังสือรับรองวงเงินสินเชื่อให้เป็นไปตามแบบที่กำหนด

(๔) กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาถือสัญชาติไทย/บุคคลธรรมดาที่มีได้ถือสัญชาติไทย จะต้องแสดงหนังสือรับรองบัญชีเงินฝาก โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่าไม่น้อยกว่า ๓,๓๔๓,๗๕๐.- บาท คิดเป็น ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือก จะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา ทั้งนี้ หนังสือรับรองบัญชีเงินฝากซึ่งธนาคารออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอหรือวันลงนามในสัญญา ไม่เกิน ๙๐ วัน

คุณสมบัติในข้อ (๑) - (๔) นี้ ยกเว้นกรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๕๘๓ และที่แก้ไขเพิ่มเติม

๑๒. ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค่านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียว เป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญา มากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

ทั้งนี้ กิจการร่วมค้า หมายถึง "กิจการที่มีข้อตกลงระหว่างผู้เข้าร่วมค้าเป็นลายลักษณ์อักษรว่าจะดำเนินการร่วมกันเป็นทางการค้าหรือหากำไรระหว่างบริษัทกับบริษัท บริษัทกับห้างหุ้นส่วนนิติบุคคล ห้างหุ้นส่วนนิติบุคคลกับห้างหุ้นส่วนนิติบุคคล หรือระหว่างบริษัทและ/หรือห้างหุ้นส่วนนิติบุคคลกับบุคคลธรรมดา คณะบุคคลที่มีใช้นิติบุคคล ห้างหุ้นส่วนสามัญ นิติบุคคลอื่น หรือนิติบุคคลที่ตั้งขึ้นตามกฎหมายของต่างประเทศ โดยข้อตกลงนั้นอาจกำหนดให้มีผู้เข้าร่วมค้าหลักก็ได้"

แบบหนังสือรับรองวงเงินสินเชื่อ

เลขที่.....

วันที่.....

เรื่อง รับรองวงเงินสินเชื่อ

ตามที่.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....เลขประจำตัว  
ผู้เสียภาษีอากร /เลขประจำตัวประชาชนเลขที่.....จะยื่นข้อเสนอในการจัดซื้ออุปกรณ์รักษา  
ความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอปพลิเคชัน (Application Firewall) จำนวน  
๑ ระบบ ซึ่งตามประกาศและเอกสารประกวดราคาข้อๆ กำหนดเงื่อนไขการยื่นข้อเสนอกรณีที่ยื่นข้อเสนอไม่มี  
มูลค่าสิทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงิน  
สินเชื่อจากธนาคาร โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่า งบประมาณของโครงการหรือรายการที่ยื่น  
ข้อเสนอใน แต่ละครั้ง จึงมีความประสงค์ให้ธนาคาร..... (ชื่อธนาคาร).....รับรองวงเงินสินเชื่อ  
เพื่อประกอบการพิจารณาด้วย นั้น

.....(ชื่อธนาคาร).....ขอรับรองว่า.....(ชื่อผู้ประกอบการ นิติบุคคล/  
บุคคลธรรมดา).....มีวงเงินทุนหมุนเวียนในวงเงินไม่ต่ำกว่า.....บาท  
(.....จำนวนเงินเป็นอักษร.....) และยินดีให้วงเงินสินเชื่อภายในวงเงิน ..... บาท  
(.....จำนวนเงินเป็นอักษร.....)



ขอแสดงความนับถือ

.....

.....(ชื่อผู้ลงนาม).....

.....(ชื่อธนาคาร).....

Proof

  
Dmlr.  


แบบหนังสือรับรองวงเงินสินเชื่ออิเล็กทรอนิกส์

เลขที่.....

วันที่.....

เรื่อง รับรองวงเงินสินเชื่อ

ตามที่.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....เลขประจำตัวผู้เสียภาษีอากร/เลขประจำตัวประชาชน เลขที่.....จะยื่นข้อเสนอในการจัดซื้ออุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอปพลิเคชัน (Application Firewall) จำนวน ๑ ระบบ ซึ่งตามประกาศและเอกสารประกวดราคาซื้อฯ กำหนดเงื่อนไขการยื่นข้อเสนอกรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสิทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงินสินเชื่อจากธนาคาร โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่า งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอใน แต่ละครั้ง จึงมีความประสงค์ให้ธนาคาร..... (ชื่อธนาคาร).....รับรองวงเงินสินเชื่อเพื่อประกอบการพิจารณาด้วย นั้น

.....(ชื่อธนาคาร).....ขอรับรองว่า.....(ชื่อผู้ประกอบการนิติบุคคล/บุคคลธรรมดา).....มีวงเงินทุนหมุนเวียนในวงเงินไม่ต่ำกว่า..... บาท (.....จำนวนเงินเป็นอักษร.....) และยินดีให้วงเงินสินเชื่อภายในวงเงิน..... บาท (.....จำนวนเงินเป็นอักษร.....)

ขอแสดงความนับถือ

..... (ชื่อธนาคาร).....

**\*\* เอกสารฉบับนี้จัดทำโดยระบบอิเล็กทรอนิกส์ \*\***

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล  
(Data Processing Agreement : DPA) กับสำนักงาน กสทช.

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (“ข้อตกลง”) นี้ จัดทำขึ้นเพื่อให้สอดคล้องกับหน้าที่ของสำนักงาน กสทช. และ ผู้ประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๔๐ วรรคสามและมาตรา ๓๗ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และข้อ ๖ ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และถือเป็นส่วนหนึ่งของการจัดซื้ออุปกรณ์รักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในระดับแอปพลิเคชัน (Application Firewall) จำนวน ๑ ระบบซึ่งสำนักงาน กสทช. มีฐานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” และผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” ซึ่งเป็นผู้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของสำนักงาน กสทช. โดยผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. เพื่อป้องกันการถูกโจมตีจากภายนอกและภายในเครือข่าย สำนักงาน กสทช.
๒. เพื่อให้ทราบต้นทางและปลายทางของข้อมูล เพื่อป้องกันไม่ให้ Hacker หรือซอฟต์แวร์อันตรายโจมตีเข้าถึงเครื่องคอมพิวเตอร์ผ่านทางเครือข่ายหรืออินเทอร์เน็ตภายในเครือข่าย สำนักงาน กสทช.

โดยข้อมูลส่วนบุคคลที่มีการประมวลผลตามวัตถุประสงค์ข้างต้น ประกอบด้วย

๑. IP Address / Log
๒. ประเภทของข้อมูลถูกจัดเก็บในรูปแบบไฟล์อิเล็กทรอนิกส์
๓. ข้อมูลอื่นใดที่อาจมีความจำเป็นเพื่อให้บรรลุวัตถุประสงค์ตามขอบเขตงานในสัญญาหลัก

การควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่สำนักงาน กสทช. มอบหมายหรือแต่งตั้งให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการ ซึ่งจะต้องดำเนินการตามหน้าที่และความรับผิดชอบตามขอบเขตงานในสัญญาหลัก และดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชกฤษฎีกา ระเบียบ และประกาศที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงนี้ รวมเรียกว่า “กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” ทั้งนี้มีผลใช้บังคับอยู่นับแต่วันที่มีการทำในสัญญาหลัก และที่จะมีการแก้ไขเพิ่มเติมในภายหลัง โดยผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งต่อไปนี้เรียกว่า “ผู้ประมวลผลข้อมูลส่วนบุคคล” ต้องดำเนินงานตามสัญญาหลัก ในส่วนของข้อมูลตามที่กำหนดในวัตถุประสงค์ข้างต้น ให้เป็นไปตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

๑. ผู้ประมวลผลข้อมูลส่วนบุคคลรับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยจะดำเนินการตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย
๒. ผู้ประมวลผลข้อมูลส่วนบุคคลจะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้จำกัดเฉพาะบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้เท่านั้น และจะดำเนินการเพื่อให้บุคคลดังกล่าวทำการประมวลผลและรักษาความลับของข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

๓. ผู้ประมวลผลข้อมูลส่วนบุคคลจะควบคุมดูแลให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของการดำเนินการตามขอบเขตงานในขอบเขตงานในสัญญาหลัก หรือที่แก้ไขเพิ่มเติมในภายหลัง โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของขอบเขตงานในสัญญาหลักหรือที่แก้ไขเพิ่มเติมในภายหลัง หรือกฎหมายที่เกี่ยวข้องที่กำหนดไว้เป็นประการอื่น

๔. ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการเพื่อช่วยเหลือหรือสนับสนุนสำนักงาน กสทช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อสำนักงาน กสทช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อสำนักงาน กสทช. อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตงานในสัญญาหลัก

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรง ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่สำนักงาน กสทช. ทันที โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่เป็นผู้ตอบสนองต่อคำร้องดังกล่าว เว้นแต่สำนักงาน กสทช. จะได้มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเฉพาะเรื่องที่เกี่ยวข้องกับคำร้องดังกล่าว

๕. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลในขอบเขตงานในสัญญาหลัก และจะดำเนินการส่งมอบบันทึกการดังกล่าวให้แก่สำนักงาน กสทช. ภายใน ๓๐ วันนับถัดจากวันลงนามในสัญญา หรือเมื่อสำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร

๖. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเหมาะสมทั้งมาตรการเชิงองค์กรและเชิงเทคนิค รวมถึงมาตรการทางกายภาพที่จำเป็นตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และตามประกาศสำนักงาน กสทช. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. รวมถึงที่ได้มีแก้ไขเพิ่มเติมในอนาคต โดยคำนึงถึงระดับความเสี่ยงตามลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดในขอบเขตงานในสัญญาหลัก เป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสียหายอันเนื่องมาจากการประมวลผลข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง รั่ว เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือไม่ชอบด้วยกฎหมาย เป็นต้น โดยต้องจัดให้มีมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสมซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องส่งคืนข้อมูลส่วนบุคคลให้กับสำนักงาน กสทช. หรือดำเนินการลบ ทำลาย ยกเลิกการเข้าถึง หรือทำให้เป็นข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ ทั้งนี้ ตามที่สำนักงาน กสทช. กำหนดโดยทันทีเมื่อการ

ดำเนินการประมวลผลตามวัตถุประสงค์ของขอบเขตงานในสัญญาหลัก เสร็จสิ้นลง โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องควบคุมดูแล ตรวจสอบ และรับรองว่าข้อมูลส่วนบุคคลดังกล่าวจะไม่อยู่ในความครอบครองของตนเองและของบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลอีกต่อไป

๘. เหตุแห่งการละเมิดข้อมูลส่วนบุคคล

๘.๑ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้ทราบหรือมีเหตุอันควรทราบว่ามีเหตุแห่งการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ภายใน ๒๔ ชั่วโมงนับแต่ทราบหรือมีเหตุอันควรทราบถึงเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการดังต่อไปนี้

(ก) ให้ข้อมูลที่จำเป็นแก่สำนักงาน กสทช. เพื่อให้สำนักงาน กสทช. สามารถปฏิบัติหน้าที่ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและทันภายในระยะเวลาที่กฎหมายกำหนด เช่น ลักษณะของเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ประเภทและจำนวนโดยประมาณของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุแห่งการละเมิด และรายละเอียดของเจ้าของข้อมูลส่วนบุคคลดังกล่าว ผลกระทบที่อาจเกิดขึ้นได้จากเหตุแห่งการละเมิด มาตรการที่ได้ดำเนินการแล้วหรือที่จะเสนอให้ดำเนินการ และมาตรการที่จะเยียวยาผลกระทบที่อาจเกิดขึ้นจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

(ข) ให้ความร่วมมืออย่างเต็มที่กับสำนักงาน กสทช. และดำเนินการใด ๆ ตามที่สำนักงาน กสทช. กำหนดเพื่อช่วยในการดำเนินการตรวจสอบ บรรเทา และเยียวยาความเสียหายอันเกิดจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

๘.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เปิดเผยเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่บุคคลอื่นใดทราบโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน เว้นแต่กรณีที่เป็นการปฏิบัติตามกฎหมาย

๘.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องชดใช้บรรดาค่าใช้จ่ายที่เกิดขึ้นจริงในการดำเนินการใด ๆ เพื่อจัดการเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงาน กสทช. หากปรากฏว่า ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลของ ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลช่วงที่อยู่ในความรับผิดชอบของตน เป็นผู้ก่อให้เกิดเหตุแห่งการละเมิดข้อมูลส่วนบุคคลดังกล่าวขึ้น

๙. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

๙.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลรับรองและยืนยันว่าจะไม่ส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานในสัญญาหลัก ไปยังต่างประเทศโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช.

๙.๒ ในกรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. แล้ว ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานในสัญญาหลักไปยังต่างประเทศได้ ทั้งนี้ การส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลดังกล่าวจะต้องกระทำภายใต้บทบัญญัติของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งเป็นลายลักษณ์อักษรของสำนักงาน กสทช. เท่านั้น โดย ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องเข้าทำข้อตกลงเพิ่มเติมหรือจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลบังคับใช้

## ๑๐. การให้บริการช่วง

๑๐.๑ ภายใต้หน้าที่และขอบเขตงานที่กำหนดในสัญญาหลัก ผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถว่าจ้างหรือแต่งตั้งบุคคลภายนอกเป็นผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเพื่อทำการประมวลผลข้อมูลส่วนบุคคลตามขอบเขตงานในสัญญาหลัก ในนามของสำนักงาน กสทช. ได้ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน

๑๐.๒ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับอนุญาตให้สามารถว่าจ้างผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ตามข้อ ๑๐.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเป็นลายลักษณ์อักษร โดยกำหนดขอบเขตเนื้อหาและหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงให้สอดคล้องกับหน้าที่และความรับผิดชอบของ ผู้ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้

ในกรณีที่สำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตรวจสอบการปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ได้รับจากสำนักงาน กสทช. และจัดทำผลการตรวจสอบ รวมทั้งส่งมอบผลการตรวจสอบให้แก่สำนักงาน กสทช. ในกรณีที่ปรากฏว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงไม่ปฏิบัติตามหรือมีเหตุอันควรเชื่อว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงอาจไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรืออาจก่อให้เกิดความเสียหายต่อสำนักงาน กสทช. ไม่ว่าในกรณีใด ๆ สำนักงาน กสทช. อาจขอให้ ผู้ประมวลผลข้อมูลส่วนบุคคลเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ทันที โดยสำนักงาน กสทช. ไม่ต้องรับผิดชอบในความเสียหายหรือค่าใช้จ่ายใด ๆ อันเกิดจากการเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

## ๑๑. การตรวจสอบ

๑๑.๑ ในกรณีที่สำนักงาน กสทช. มีการร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการส่งมอบข้อมูลที่จำเป็นทั้งหมดให้แก่สำนักงาน กสทช. เพื่อเป็นการปฏิบัติหน้าที่ตามข้อตกลงนี้

๑๑.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงอนุญาตให้สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. เข้าตรวจสอบการปฏิบัติหน้าที่ของ ผู้ประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ โดยสำนักงาน กสทช. จะแจ้งให้ ผู้ประมวลผลข้อมูลส่วนบุคคลทราบล่วงหน้าเป็นลายลักษณ์อักษรไม่น้อยกว่า ๗ วัน และ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงให้ความร่วมมือแก่สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. ในการเข้าตรวจสอบดังกล่าวข้างต้น

## ๑๒. การชดใช้และการเยียวยา

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องชดใช้ค่าเสียหายหรือค่าใช้จ่ายใด ๆ ให้แก่สำนักงาน กสทช. ในกรณีที่เกิดความเสียหาย การสูญหาย การเรียกร้อง ค่าเสียหาย ความรับผิดทางแพ่ง โทษปรับทางปกครอง หรือค่าใช้จ่ายใด ๆ ที่เกิดขึ้นต่อบุคคลภายนอก หรือในกรณีที่สำนักงาน กสทช. จะต้องรับผิดชอบอันเนื่องมาจากการไม่ปฏิบัติตามข้อใดข้อหนึ่งภายใต้ข้อตกลงนี้หรือตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือการละเมิดคำรับรองและรับประกันของ ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่ได้รับมอบหมายจากผู้ประมวลผลข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคล ผู้รับจ้างช่วง ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง หรือตัวแทนของ ผู้ประมวลผลข้อมูลส่วนบุคคล

๑๓. การบอกกล่าว

บรรดาคำบอกกล่าวหรือการติดต่อสื่อสารใด ๆ ตามข้อตกลงนี้ ให้ทำเป็นลายลักษณ์อักษร โดยให้ส่งโดยบุคคล หรือไปรษณีย์ หรือโทรสาร ไปยังสถานที่ของผู้รับตามที่ระบุไว้ในข้อตกลงนี้ หรือตามที่ได้รับแจ้งเปลี่ยนแปลงจากผู้รับ (ถ้ามี) คำบอกกล่าวหรือการติดต่อสื่อสารทั้งหลายจะถือว่าผู้รับได้รับแล้วเมื่อคำบอกกล่าวหรือการติดต่อสื่อสารนั้นไปถึงสถานที่นั้นแล้ว

๑๔. หน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามข้อตกลงนี้จะสิ้นสุดลงนับแต่วันที่การปฏิบัติงานตามขอบเขตงานในสัญญาหลักเสร็จสิ้น หรือวันที่ ผู้ประมวลผลข้อมูลส่วนบุคคลและสำนักงาน กสทช. ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกการดำเนินการตามขอบเขตงานนี้แล้วแต่กรณีใดจะเกิดขึ้นก่อน โดยคู่สัญญาตกลงจะไม่โอนสิทธิเรียกร้องตามข้อตกลงนี้ให้แก่บุคคลอื่น