ขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะ
โครงการจัดหาระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์
(Threat Detection and Incident Response Platform)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ส่วนที่ ๑ บทนำ

๑.๑ หลักการและเหตุผล

ปัจจุบันสำนักงาน ป.ป.ช. มีระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรในเชิงลึก เพื่อทำหน้าที่เฝ้าระวังการถูกโจมตีจากผู้ไม่ประสงค์ดี (Hacker) ทั้งจากระบบเครือข่ายภายในและภายนอกของสำนักงาน ป.ป.ช. ซึ่งมีอายุการใช้งานเกิน ๗ ปีแล้ว และระบบดังกล่าวมีความล้าสมัย ซึ่งผู้ไม่ประสงค์ดี (Hacker) ได้พัฒนารูปแบบการโจมตีที่หลากหลาย และมุ่งโจมตีหน่วยงานราชการเป็นหลัก

ดังนั้น สำนักงาน ป.ป.ช. จึงมีความจำเป็นต้องปรับปรุงระบบจัดเก็บข้อมูล ระบบวิเคราะห์ข้อมูลจราจรในเชิงลึก และจัดหาระบบตรวจจับการโจมตีและตอบสนองภัยคุกคาม ระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ ที่มีประสิทธิภาพ ทันสมัย เพื่อให้สามารถจัดเก็บข้อมูลการใช้งานเป็นไปตามกฎหมายที่กำหนด และสามารถวิเคราะห์ข้อมูลการใช้งานเพื่อตรวจหาช่องโหว่หรือความเสี่ยงที่อาจเกิดขึ้น รวมทั้งตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ทันที

๑.๒ วัตถุประสงค์

๑.๒.๑ สำนักงาน ป.ป.ช. มีระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นไปตามที่กฎหมายกำหนด

๑.๒.๒ สำนักงาน ป.ป.ช. มีระบบวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ ทันสมัย เพื่อประเมินความเสี่ยง สำหรับใช้ป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ได้

๑.๒.๓ สำนักงาน ป.ป.ช. สามารถรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ทันที

๑.๒.๔ สำนักงาน ป.ป.ช. มี Playbook สำหรับการบริหารจัดการเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ ทันสมัย และเหมาะสม

๑.๒.๕ เจ้าหน้าที่ ป.ป.ช. สามารถใช้งานระบบเครือข่าย ระบบสารสนเทศ และการใช้อินเทอร์เน็ตได้อย่างสะดวก ต่อเนื่อง และมีความมั่นคงปลอดภัย

๑.๓ เป้าหมาย

สำนักงาน ป.ป.ช. มีระบบเครือข่ายและระบบสารสนเทศที่มีความมั่นคงปลอดภัย ไม่ถูกโจมตีหรือโจรกรรมข้อมูลจากผู้ไม่ประสงค์ดี รวมทั้งสามารถรับมือกับภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันที

๑.๔ ประโยชน์ที่คาดว่าจะได้รับ

๑.๔.๑ สำนักงาน ป.ป.ช. มีระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นไปตามที่กฎหมายกำหนด

๑.๔.๒ สำนักงาน ป.ป.ช. มีระบบวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ ทันสมัย เพื่อลดความเสี่ยงในการถูกโจมตีจากภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ได้

๑.๔.๓ สำนักงาน ป.ป.ช. สามารถรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ทันที

๑.๔.๔ เจ้าหน้าที่ ป.ป.ช. สามารถใช้งานระบบเครือข่าย ระบบสารสนเทศ และการใช้อินเทอร์เน็ตได้อย่างสะดวก ต่อเนื่อง และมีความปลอดภัย

/ส่วนที่ ๒...

ส่วนที่ ๒ ระบบที่ต้องการ

๒.๑ ลักษณะภาพรวมของระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่ใช้งานอยู่ในปัจจุบัน

ปัจจุบันสำนักงาน ป.ป.ช. มีระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ดังนี้

๒.๑.๑ ระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ยี่ห้อ SuperMicro รุ่น 6029P-E1CR12H ขนาด 40 TB Raid ๑ โดยสามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่สำนักงาน ป.ป.ช. ใช้งานได้เป็นระยะเวลา ๑๒๐ วัน เป็นอย่างน้อย

๒.๑.๒ ระบบวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ (Security Information and Event Management : SIEM) ยี่ห้อ LogRhythm Version 7.4.10 รองรับการจัดเก็บข้อมูลอุปกรณ์ ๖๖ สิทธิการใช้งาน

๒.๑.๓ ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ (Security Information and Event Management : SIEM) ยี่ห้อ Wazuh Version 4.9.0 จัดเก็บข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๑๐๕ เครื่อง อุปกรณ์โครงสร้างพื้นฐาน จำนวน ๗ เครื่อง และระบบสารสนเทศ จำนวน ๑๕๑ ระบบ

๒.๒ ความต้องการของระบบ

สำนักงาน ป.ป.ช. มีความประสงค์ที่จะปรับปรุงระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ และจัดหาระบบตรวจจับการโจมตีและตอบสนองภัยคุกคามทางไซเบอร์ และระบบบริหารจัดการภัยคุกคามทางไซเบอร์และตอบสนองต่อภัยคุกคามทางไซเบอร์แบบอัตโนมัติ เพื่อเพิ่มประสิทธิภาพการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ให้เป็นไปตามที่กฎหมายกำหนด และสามารถวิเคราะห์ ประเมินการบุกรุก การโจมตีภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ เพื่อป้องกันระบบเครือข่ายและระบบสารสนเทศของสำนักงาน ป.ป.ช. ให้มีความปลอดภัยมากยิ่งขึ้น รวมทั้งสามารถรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ทันที โดยผู้เสนอราคาจะต้องดำเนินการอย่างน้อยดังนี้

๒.๒.๑ จัดหาระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ พร้อมอุปกรณ์จัดเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ ข้อมูลการใช้งานคอมพิวเตอร์ จากอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และระบบสารสนเทศที่สำนักงาน ป.ป.ช. ใช้งาน (ตามภาคผนวก ๑) โดยสามารถจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่สำนักงาน ป.ป.ช. ใช้งานได้เป็นระยะเวลา ๑๘๐ วัน เป็นอย่างน้อย และเก็บข้อมูลไว้สำหรับตรวจสอบย้อนหลังอีก ๒ ปี

๒.๒.๒ จัดหาระบบวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ (Security Information and Event Management : SIEM) พร้อมอุปกรณ์สำหรับการนำข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บตามข้อ ๒.๒.๑ เพื่อนำข้อมูลมาวิเคราะห์ และแสดงผลในรูปแบบต่าง ๆ เพื่อให้ง่ายต่อการศึกษาและทำความเข้าใจ รวมถึงการประเมิน และการวางแผนรับมือการโจมตีประเภทต่างๆ ที่ตรวจพบ

๒.๒.๓ จัดหาอุปกรณ์จัดเก็บข้อมูล (ขนาดไม่น้อยกว่า 60 TB Raid 10) เพื่อจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ครอบคลุมระยะเวลาตามข้อ ๒.๒.๑

๒.๒.๔ จัดหาระบบตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response : XDR)

๒.๒.๕ จัดหาระบบบริหารจัดการภัยคุกคามทางไซเบอร์และตอบสนองต่อภัยคุกคามทางไซเบอร์แบบอัตโนมัติ (Security Orchestration, Automation and Response : SOAR)

๒.๒.๖ จัดฝึกอบรมหลักสูตร CompTIA Security+ ให้กับเจ้าหน้าที่ผู้ดูแลระบบรักษาความปลอดภัยของสำนักงาน ป.ป.ช. จำนวนไม่น้อยกว่า ๒ คน พร้อมสอบ Certificate CompTIA Security+

/๒.๒.๗ จัดฝึกอบรม...

๒.๒.๗ จัดฝึกอบรมหลักสูตร Security Awareness ให้ผู้ใช้งานระบบสารสนเทศ สำนักงาน ป.ป.ช. จำนวนไม่น้อยกว่า ๑ หลักสูตร อย่างน้อยปีละ ๑ ครั้ง ตลอดระยะเวลาการรับประกันกับผู้ขาย

๒.๒.๘ จัดทำ Playbook การรับมือภัยคุกคามทางไซเบอร์ จำนวนไม่น้อยกว่า ๒๐ Playbook บนระบบ Security Orchestration, Automation and Response : SOAR โดยจะต้องเสนอ Solution ให้สำนักงาน ป.ป.ช. พิจารณาให้ความเห็นชอบก่อน

๒.๒.๙ อุปกรณ์และระบบที่เสนอในโครงการทั้งหมดสามารถทำงานร่วมกันได้ ในการจัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ตรวจจับการโจมตีและตอบสนองภัยคุกคามทางไซเบอร์ และบริหารจัดการภัยคุกคามทางไซเบอร์และตอบสนองต่อภัยคุกคามทางไซเบอร์แบบอัตโนมัติ

** ทั้งนี้ การติดตั้งอุปกรณ์หรือระบบที่เสนอ และการปรับปรุงการทำงานให้สามารถทำงานร่วมกับระบบเครือข่าย ระบบสารสนเทศ และเครื่องคอมพิวเตอร์แม่ข่ายที่สำนักงาน ป.ป.ช. ใช้งานอยู่เดิมได้ตามข้อกำหนด ผู้เสนอราคาจะต้องเป็นผู้รับผิดชอบในการดำเนินการ และค่าใช้จ่ายที่เกิดขึ้น เพื่อให้สามารถทำงานได้ตามข้อกำหนดเป็นอย่างน้อย โดยผู้เสนอราคาต้องเป็นผู้ประเมินเอง

๒.๓ รายละเอียดและคุณสมบัติเฉพาะของระบบงานที่ต้องการ จะต้องมีคุณสมบัติไม่ต่ำกว่า หรือเทียบเท่า หรือดีกว่า อย่างน้อยดังนี้

๒.๓.๑ จัดหาและติดตั้งระบบและอุปกรณ์ ดังต่อไปนี้

ลำดับที่	รายการ	จำนวน
๑	ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	๑ ชุด
๒	ระบบวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Information and Event Management : SIEM)	๑ ชุด
๓	อุปกรณ์จัดเก็บข้อมูล ขนาดไม่น้อยกว่า 60 TB Raid 10	๑ ชุด
๔	ระบบตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response : XDR)	๑ ชุด
๕	ระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response : SOAR)	๑ ชุด

๒.๓.๒ คุณลักษณะเฉพาะขั้นต่ำ

๒.๓.๒.๑ ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ จำนวน ๑ ชุด แต่ละชุดจะต้องมีคุณสมบัติไม่ต่ำกว่า หรือเทียบเท่า หรือดีกว่า ดังนี้

๒.๓.๒.๑.๑ ระบบที่เสนอมีการทำงานเป็นแบบ Distributed Architecture โดยมีการติดตั้งอุปกรณ์ที่ทำหน้าที่เก็บบันทึกข้อมูลทางด้านการรักษาความปลอดภัยเครือข่าย (Log Management) แยกจากอุปกรณ์ที่ทำหน้าที่วิเคราะห์และบริหารจัดการข้อมูลความปลอดภัยเครือข่าย (Security information and Event Management: SIEM) เพื่อประสิทธิภาพในการทำงานที่ดี

๒.๓.๒.๑.๒ สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) จากอุปกรณ์ต้นทางได้ ทั้งนี้ ผู้ขายจะต้องประเมินและเสนอจำนวนอุปกรณ์ที่ใช้ในการรับข้อมูลจราจรทางคอมพิวเตอร์ให้เพียงพอตามรายการในภาคผนวก ๑ เป็นอย่างน้อย ในกรณีที่ระบบจัดเก็บข้อมูลจราจรทาง

/คอมพิวเตอร์...

คอมพิวเตอร์ ยังใช้งานการรับปริมาณข้อมูลได้ไม่เต็มตามจำนวนที่เสนอ สำนักงาน ป.ป.ช. สามารถเพิ่มจำนวนอุปกรณ์ต้นทางในการส่งข้อมูลการใช้งาน (Log) ได้ตามจำนวนปริมาณการรับข้อมูลที่เสนอ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

๒.๓.๒.๑.๓ สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) โดยรองรับปริมาณข้อมูลได้ไม่น้อยกว่า ๓๐๐ GB ต่อวัน หรือ ๘,๐๐๐ EPS หรือ ๔ Gbps ทั้งนี้ ต้องสามารถจัดเก็บได้ครบถ้วนตามอุปกรณ์ในภาคผนวก ๑ โดยผู้ขายเป็นผู้ประเมินและดำเนินการให้ครบถ้วน หากเสนอหน่วยในการคำนวณปริมาณการจัดเก็บข้อมูลแตกต่างจากที่กำหนดให้ผู้เสนอราคาคำนวณให้อยู่ในหน่วยที่กำหนด พร้อมแสดงวิธีการคำนวณเสนอมาพร้อมกับการยื่นซองเสนอราคา

๒.๓.๒.๑.๔ สามารถทำการส่งต่อ (Forwarding) ข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) ที่เก็บไปยังระบบวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ (SIEM) ที่เสนอได้

๒.๓.๒.๑.๕ สามารถบีบอัดข้อมูลเพื่อลดขนาดข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) ที่จัดเก็บได้ในอัตราส่วนไม่น้อยกว่า ๑๐ ต่อ ๑ เพื่อเพิ่มประสิทธิภาพของการพื้นที่ในการเก็บข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log)

๒.๓.๒.๑.๖ ระบบที่เสนอต้องมีความสามารถในการจัดการข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) ทั้งนี้ สามารถหาอุปกรณ์อื่นๆ เพิ่มเติมได้ เพื่อให้รองรับการจัดรูปแบบของข้อมูลให้อยู่ในรูปแบบมาตรฐานเดียวกัน (Normalizing) เพื่อให้ผู้ดูแลระบบสืบค้นได้อย่างมีประสิทธิภาพได้เป็นอย่างน้อย

๒.๓.๒.๑.๗ ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เสนอ ต้องรองรับการจัดเก็บข้อมูลการใช้งาน (Log) จากอุปกรณ์ได้หลากหลายรูปแบบ โดยต้องรองรับรูปแบบ Log ของอุปกรณ์หรือระบบที่สำนักงาน ป.ป.ช. ใช้งานอยู่ ตามภาคผนวก ๑ ได้เป็นอย่างน้อย และต้องสามารถพัฒนาให้ระบบที่เสนอสามารถรับข้อมูลจราจรคอมพิวเตอร์และข้อมูลการใช้งาน (Log) ที่มีรูปแบบต่างๆ ได้

๒.๓.๒.๑.๘ มีความสามารถในการรับข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) จาก Protocol หรือรูปแบบ อย่างน้อยดังนี้

- Syslog
- FTP (File Transfer Protocol)
- SFTP (Secure File Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- ODBC/JDBC
- OPSEC
- Flow เช่น sFlow, NetFlow ได้เป็นอย่างน้อย

๒.๓.๒.๑.๙ มีการตรวจสอบเพื่อยืนยันว่าข้อมูลที่เก็บบันทึกจะไม่มีการแก้ไขหรือเปลี่ยนแปลง (File Integrity) ด้วย Algorithm แบบ MD5 หรือ SHA-1 หรือ SHA-256 หรือดีกว่า และต้องไม่อนุญาตให้เปลี่ยนแปลงและแก้ไขข้อมูลที่จัดเก็บ

๒.๓.๒.๑.๑๐ สามารถแบ่งกลุ่มของอุปกรณ์ที่จัดเก็บได้ และสามารถกำหนดนโยบายระยะเวลาการเก็บรักษาข้อมูลของอุปกรณ์แต่ละกลุ่มได้แตกต่างกัน (Per Group) หรือเป็นรายอุปกรณ์ได้ (Per Device)

/๒.๓.๒.๑.๑๑ สามารถ...

๒.๓.๒.๑.๑๑ สามารถค้นหาข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) ได้ทั้งแบบ Simple Query (Free-text Search) และ Complex Query (Boolean, Regular Expression) เพื่อค้นหา Log ได้ โดยสามารถทำการสรุปข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) ในรูปแบบของแผนภูมิ (Chart) จากหน้าค้นหา (Search) ได้ทันทีเพื่อความสะดวกในการวิเคราะห์ข้อมูลดังกล่าว

๒.๓.๒.๑.๑๒ มีรูปแบบรายงาน (Predefine Report) และสามารถสร้าง (Custom) รูปแบบรายงานได้เอง และสามารถจัดส่งรายงานให้กับผู้ดูแลระบบตามช่วงเวลาได้

๒.๓.๒.๑.๑๓ สามารถส่งออกรูปแบบรายงานในรูปแบบไฟล์ดังต่อไปนี้ PDF หรือ HTML และ CSV ได้เป็นอย่างน้อย

๒.๓.๒.๑.๑๔ สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser และ CLI ได้

๒.๓.๒.๑.๑๕ สามารถกำหนดสิทธิ์การใช้งานระบบของผู้ดูแลระบบแต่ละคนได้แตกต่างกัน (Role Base Access Control)

๒.๓.๒.๑.๑๖ สามารถพิสูจน์ตัวตนของผู้ดูแลระบบบน Local system และ Active Directory หรือ LDAP Server ได้

๒.๓.๒.๑.๑๗ สามารถตรวจสอบสถานะการส่ง Log ของอุปกรณ์ต้นทางต่างๆ และแจ้งเตือนหากการรับส่งขัดข้อง

๒.๓.๒.๑.๑๘ สามารถจัดเก็บข้อมูล และเก็บรักษาข้อมูลให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และหน่วยงานที่เกี่ยวข้องกำหนด

๒.๓.๒.๑.๑๙ สามารถสำรองข้อมูลออกมาภายนอกได้

๒.๓.๒.๑.๒๐ ผู้ขายต้องมีกระบวนการหรือวิธีการในการตรวจสอบ หรือป้องกันการแก้ไขไฟล์ระบบ หรือไฟล์ที่สำคัญบนระบบปฏิบัติการ Linux และ Windows ได้ และสามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ขึ้น ทั้งนี้ สามารถเสนอระบบอื่นๆ (ถ้ามี) มาใช้งานร่วมกับระบบที่เสนอได้

๒.๓.๒.๑.๒๑ ระบบที่เสนอต้องมี Network Interface แบบ Gigabit Ethernet อย่างน้อย ๒ พอร์ต ต่อ ๑ อุปกรณ์ ที่เสนอภายในชุด

๒.๓.๒.๒ ระบบวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (SIEM) จำนวน ๑ ชุด แต่ละชุดจะต้องมีคุณสมบัติไม่ต่ำกว่า หรือเทียบเท่า หรือดีกว่า ดังนี้

๒.๓.๒.๒.๑ อุปกรณ์ที่เสนอเป็นอุปกรณ์ที่ทำหน้าที่ด้าน Security Information and Event Management (SIEM)

๒.๓.๒.๒.๒ สามารถเชื่อมโยงเหตุการณ์จาก Source ต่างๆ เข้าด้วยกัน (Correlation) ทั้งแบบ Real-time และ Historical เพื่อหาต้นตอของภัยคุกคาม โดยมี Rule ไม่น้อยกว่า ๑๐๐ Rules ที่สามารถใช้งาน และสามารถ Customize เพิ่มเติมได้

๒.๓.๒.๒.๓ สามารถสร้างความสัมพันธ์ของเหตุการณ์หลายๆ เหตุการณ์ในรูปแบบแผนภาพ (Event Graph หรือ Investigation timeline) แบบหลายลำดับชั้น เพื่อใช้ในการเฝ้าระวังเหตุการณ์แบบ Real-time และวิเคราะห์ย้อนหลัง (Historical) ได้

๒.๓.๒.๒.๔ มี Dashboard เพื่อใช้สำหรับวิเคราะห์ Log แบบ Real-time หรือ Near Real-Time ในรูปแบบของแผนภูมิ (Chart) และตาราง (Table) และสามารถ Customize เพิ่มเติมได้

/๒.๓.๒.๒.๕ สามารถ...

๒.๓.๒.๒.๕ สามารถปรับเวลา (Time Zone) ของปูมเหตุการณ์ต้นทาง (Event Log) กับเวลาของระบบให้ตรงกันเพื่อความแม่นยำในการวิเคราะห์เหตุการณ์

๒.๓.๒.๒.๖ รองรับการบริหารจัดการรายละเอียดของอุปกรณ์ หรือระบบต้นทางของ Log (Asset Management) เช่น ประเภทของอุปกรณ์ และสถานที่ตั้ง

๒.๓.๒.๒.๗ สามารถทำการวิเคราะห์เปรียบเทียบข้อมูลระหว่าง IP Address กับรายชื่อผู้ใช้งานหรือ Hostname ที่ใช้งานไอพีแอดเดรสนั้นๆ อยู่ และทำการแสดงผลออกมาเป็นชื่อผู้ใช้งานรายนั้นๆ หรือ Hostname เครื่องนั้นๆ ได้ทันที

๒.๓.๒.๒.๘ มีเครื่องมือที่ใช้สำหรับช่วยหาข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ต เช่น Whois หรือ Ping หรือ IP Lookup หรือ VIRUSTOTAL ได้ โดยผ่านหน้าจอ Interface ของระบบเอง โดยไม่ต้องอาศัยเครื่องมือจากภายนอกระบบ

๒.๓.๒.๒.๙ มีระบบบริหารจัดการเคส (Case Management) เพื่อใช้ในการบริหารจัดการ และติดตาม Incident ที่เกิดขึ้น โดยสามารถดำเนินการได้อย่างน้อยดังนี้

- การเปิดเคสสามารถทำได้โดยผู้ดูแลระบบ (Manual) และจากเงื่อนไขที่ใช้ในการเฝ้าระวัง (Auto)
- ระบบสามารถกำหนดประเภทของเคสได้ว่าเป็น Event หรือ Incident ได้เป็นอย่างน้อย
- ต้องแจ้งเคสไปยังผู้ดูแลอุปกรณ์หรือระบบที่เกี่ยวข้องทางจดหมายอิเล็กทรอนิกส์ เพื่อให้ทราบและดำเนินการต่อไป
- ต้องติดตามสถานะของเคสต่างๆได้
- ต้องออกรายงานสรุปเกี่ยวกับการจัดการเคสได้

๒.๓.๒.๒.๑๐ มีระบบการจัดการ Knowledge Base หรือ Cloud Knowledge Base เพื่อสร้างองค์ความรู้และคำแนะนำในการแก้ปัญหาต่างๆ หรือสามารถแนบ URL/Notes กับ Incident ได้ เพื่อใช้เป็นฐานความรู้ภายในทีม เพื่อให้ผู้ดูแลระบบสามารถศึกษาย้อนหลังได้

๒.๓.๒.๒.๑๑ มี Report ที่สามารถ Customize เพิ่มเติมได้ โดยสามารถ Export Report ในรูปแบบไฟล์ CSV และ PDF หรือ HTML ได้เป็นอย่างน้อย

๒.๓.๒.๒.๑๒ สามารถแจ้งเตือนแบบ Real-time เมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่สร้างไว้หรือเหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่านจดหมายอิเล็กทรอนิกส์ (Email) ได้เป็นอย่างน้อย และสามารถจัดการเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายตามภาคผนวก ๑ เพื่อตอบสนองเหตุการณ์ที่เกิดขึ้นได้แบบอัตโนมัติ (Automated Response) เช่น การ Disable User, การ Block IP Address ต้นทาง เป็นต้น

๒.๓.๒.๒.๑๓ สามารถบริหารจัดการผ่าน Web Interface ที่มีการเข้ารหัส หรือสามารถบริหารจัดการผ่าน Software Console ได้

๒.๓.๒.๒.๑๔ สามารถ Authentication โดยใช้ Local User และ Active Directory หรือ LDAP Server หรือ SAML ได้เป็นอย่างน้อย และสามารถกำหนดสิทธิ์การใช้งานระบบของผู้ดูแลระบบแต่ละคนได้แตกต่างกัน (Role Base Access Control)

๒.๓.๒.๒.๑๕ รองรับการรับข้อมูล Reputation เพื่อใช้ในการตรวจจับและแจ้งเตือนเมื่อมีการเชื่อมต่อไปยัง IP Address หรือ Domain ภายนอกองค์กรที่เป็นอันตราย

/๒.๓.๒.๒.๑๖ ระบบ...

๒.๓.๒.๒.๑๖ ระบบฐานข้อมูลสำหรับการจัดเก็บและการวิเคราะห์ของระบบที่เสนอจะต้องมีสิทธิการใช้งานที่ถูกต้องตามกฎหมาย

๒.๓.๒.๒.๑๗ สามารถแจ้งเตือน (Alert) ไปยังผู้ดูแลระบบเมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่สร้างไว้หรือเหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน SNMP หรือ Syslog หรือ E-mail ได้

๒.๓.๒.๒.๑๘ ระบบที่เสนอต้องสามารถตรวจสอบและระบุได้ว่าหมายเลข Public IP นั้นมาจากประเทศใด ตามข้อมูล IP Geography หรือ IP Geolocation ได้เป็นอย่างน้อย

๒.๓.๒.๒.๑๙ ระบบต้องวิเคราะห์ข้อมูลต่างๆ ในระบบเปรียบเทียบกับมาตรฐาน ISO 27001 หรือ ISO 27002 ได้เป็นอย่างน้อย เพื่อประเมินระบบของสำนักงาน ป.ป.ช. ในภาพรวม

๒.๓.๒.๒.๒๐ ระบบต้องสามารถนำข้อมูลผลการหาช่องโหว่จากทำ VA Scan จากอุปกรณ์ หรือซอฟต์แวร์ เช่น Nessus, Rapid7 เป็นต้น

๒.๓.๒.๒.๒๑ ผู้ขายจะต้องดำเนินการพัฒนา Rule ที่ใช้ในการตรวจสอบและเฝ้าระวัง โดยใช้ข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log) และข้อมูลอื่นใด มาใช้ในการพัฒนา rule โดยมีรายละเอียดอย่างน้อยดังนี้

- การพยายามเข้าใช้งานไม่สำเร็จเป็นจำนวนมากจากเครื่องต้นทางเดียวกันแต่ใช้งาน User ที่แตกต่างกัน
- การพยายามเข้าใช้งานไม่สำเร็จเป็นจำนวนมากจาก User เดียวกันแต่เกิดขึ้นในเวลาสั้นๆ
- การพยายามเข้าใช้งานไม่สำเร็จเป็นจำนวนมากจาก User เดียวกันแต่มาจากต้นทางต่างกัน
- ตรวจจับการเพิ่ม user account เข้าไปยัง admin group
- ตรวจจับการ Login สำเร็จของ Vendor/Outsource นอกเวลาทำการ
- ตรวจจับการใช้งาน Critical Command หรือ Suspicious Process Creation Command line บนระบบ Database ช่วงนอกเวลาทำการ
- ตรวจจับการใช้งานรีโมทจากภายนอก เพื่อเข้ามายัง Critical Server ผ่าน RDP, SSH, VNC และ Telnet เป็นต้น
- ตรวจจับ Deny Traffic เป็นจำนวนมากจากเครื่องต้นทางเดียวกันที่อยู่ภายใน
- ตรวจจับการเข้าถึงสำเร็จจากเครื่องภายนอก (Internet IP Source) ที่เคยมีประวัติการ Block จากอุปกรณ์ Security เช่น Firewall, IPS, Mail gateway, Web Gateway, Honey Pot และ WAF
- ตรวจจับการ Sweep Network หรือการเปิด connection ไปยังเครื่องต่างๆ เป็นจำนวนมาก
- ตรวจจับการ Scan Port หรือการเปิด connection ไปยังเครื่องปลายทางเพื่อตรวจสอบการใช้งาน Service Port ต่างๆ
- ตรวจจับการโจมตีประเภท Cross Site Scripting หรือ Command and Scripting Interpreter

/- ตรวจจับ...

- ตรวจจับการโจมตีประเภท SQL Injection Attacks หรือ SQL Anomaly

- ตรวจจับ Proxy Deny หรือ User Asset Access Anomaly เป็นจำนวนมากที่มาจากเครื่องต้นทางเดียวกัน

- ตรวจจับการพยายาม Login เข้าใช้งาน VPN จากประเทศที่ไม่อนุญาตให้เข้าถึง Network ภายใน

๒.๓.๒.๒.๒๒ สามารถรับข้อมูลจราจรทางคอมพิวเตอร์จากอุปกรณ์ของสำนักงาน ป.ป.ช. โดยรองรับปริมาณข้อมูลได้ไม่น้อยกว่า ๓๐๐ GB ต่อวัน หรือ ๘,๐๐๐ EPS หรือ ๔ Gbps ซึ่งสามารถคัดกรองข้อมูลที่จำเป็นต่อการวิเคราะห์ได้ หากเสนอหน่วยในการคำนวณปริมาณการจัดเก็บข้อมูลแตกต่างจากที่กำหนดให้ผู้เสนอราคาคำนวณให้อยู่ในหน่วยที่กำหนดพร้อมแสดงวิธีการคำนวณเสนอมาพร้อมกับการยื่นซองเสนอราคา

๒.๓.๒.๒.๒๓ สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser และ CLI ได้

๒.๓.๒.๒.๒๔ ระบบที่เสนอต้องมี Network Interface แบบ Gigabit Ethernet อย่างน้อย ๒ พอร์ต ต่อ ๑ อุปกรณ์ที่เสนอภายในชุด

๒.๓.๒.๓ อุปกรณ์จัดเก็บข้อมูล ขนาดไม่น้อยกว่า ๖๐ TB Raid ๑๐ จำนวน ๑ ชุด แต่ละชุดจะต้องมีคุณสมบัติไม่ต่ำกว่า หรือเทียบเท่า หรือดีกว่า ดังนี้

๒.๓.๒.๓.๑ เป็นอุปกรณ์ที่ทำหน้าที่เป็น Storage เพื่อใช้ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Log)

๒.๓.๒.๓.๒ มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด NVMe หรือ Solid State Drives หรือดีกว่าและมีความจุรวม หลังจากการทำ Raid ๑๐ แล้วไม่น้อยกว่า ๖๐ TB

๒.๓.๒.๓.๓ สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID ๐, ๑ และ ๑๐

๒.๓.๒.๓.๔ มี Gigabit Ethernet Port แบบ UTP จำนวนรวมไม่น้อยกว่า ๒ Ports

๒.๓.๒.๓.๕ มี Port ๑๐ Gbps แบบ SFP+ พร้อม Module Fiber Single Mode แบบ LC จำนวนรวมไม่น้อยกว่า ๒ Ports

๒.๓.๒.๓.๖ มีแหล่งจ่ายไฟ (Power supply) แบบ Redundant และสามารถถอดเปลี่ยนได้โดยไม่ต้องปิดระบบ (Hot-swappable Redundant Power Supply)

๒.๓.๒.๓.๗ ต้องทำงานร่วมกับระบบที่เสนอ และหรือระบบเครือข่ายของสำนักงาน ป.ป.ช. ได้ โดยผู้เสนอราคามีหน้าที่ในการคำนวณจำนวนพอร์ตให้เพียงพอต่อการใช้งาน

๒.๓.๒.๔ ระบบตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response – XDR) ในรูปแบบ Native XDR หรือ Open XDR จำนวน ๑ ชุด แต่ละชุดจะต้องมีคุณสมบัติไม่ต่ำกว่า หรือเทียบเท่า หรือดีกว่า ดังนี้

๒.๓.๒.๔.๑ ระบบที่เสนอจะต้องสามารถทำงานร่วมกับระบบตรวจจับและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Response (EDR)) ยี่ห้อ TrendMicro Vision One ที่สำนักงาน ป.ป.ช. ใช้งานอยู่ได้

/๒.๓.๒.๔.๒ มีสิทธิ...

๒.๓.๒.๔.๒ มีสิทธิการใช้งานไม่น้อยกว่า ๘,๐๐๐ อุปกรณ์ หรือรองรับปริมาณการรับส่งข้อมูลได้ไม่น้อยกว่า ๓๐๐ GB หรือ ๘,๐๐๐ EPS หรือ ๔ Gbps ต่อวัน

๒.๓.๒.๔.๓ เป็นซอฟต์แวร์ป้องกันการโจมตีผ่านช่องโหว่แบบ Advanced Malware ที่บริหารจัดการ ความปลอดภัยบนอุปกรณ์ ซึ่งสามารถทำงานร่วมกับระบบตรวจจับและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Response (EDR)) ที่สำนักงาน ป.ป.ช. ใช้งานอยู่ได้ หรือกรณีไม่สามารถทำงานร่วมกับระบบตรวจจับและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Response (EDR)) ที่สำนักงาน ป.ป.ช. ใช้งานอยู่ได้ ต้องมีความสามารถด้านการป้องกัน ภัยคุกคามในระดับ Endpoint อย่างน้อยดังนี้

(๑) Exploit Prevention
(๒) Malware Prevention
(๓) Fileless Attacks
(๔) AI-based / Machine Learning analysis
(๕) Behavioral Threat Protection
(๖) Ransomware Protection
(๗) Data Loss Prevention (DLP)

๒.๓.๒.๔.๔ เป็นอุปกรณ์ Network Sensor ที่สามารถทำงานร่วมกับอุปกรณ์ Next Generation Firewall ยี่ห้อ Palo Alto: PA-5250 ที่สำนักงาน ป.ป.ช. ใช้งานอยู่ได้ ในการตรวจจับ ค้นหา แจ้งเตือน และรายงานอันตรายจากภัยคุกคามขั้นสูงในระบบเครือข่ายให้กับผู้ดูแลระบบ และส่งข้อมูลเข้าสู่ระบบ เพื่อทำการวิเคราะห์ด้วยระบบ AI ในการตรวจจับการโจมตีแบบอัตโนมัติ (Automate Attack Detection with AI) เพื่อช่วยในการบริหารจัดการป้องกันภัยคุกคาม โดยใช้เทคโนโลยี Machine learning เรียนรู้พฤติกรรม ผู้ใช้งานในองค์กร โดยมีความสามารถอย่างน้อยดังนี้

(๑) Network traffic analysis (NTA)
(๒) Endpoint detection and response (EDR)
(๓) Root cause analysis of alerts
(๔) Timeline analysis of alerts
(๕) Threat hunting
(๖) Post-incident impact analysis หรือ Incident Analysis
(๗) Dashboards and reporting

๒.๓.๒.๔.๕ สามารถบริหารจัดการจากศูนย์กลาง (Centralize Management) ผ่าน Web Browser พร้อมสิทธิ์การใช้งานจำนวนไม่น้อยกว่า ๓๐๐ GB หรือ ๘,๐๐๐ EPS หรือ ๔ Gbps ต่อวัน และมีพื้นที่จัดเก็บข้อมูล Network Traffic Analysis ไม่น้อยกว่า ๑๐ TB หรือมีพื้นที่จัดเก็บข้อมูลรองรับการทำ Network Traffic Analysis ไม่น้อยกว่า ๓๐๐ GB ต่อวัน

๒.๓.๒.๔.๖ ระบบที่นำเสนอต้องสามารถวิเคราะห์ภัยคุกคามต่างๆ ได้อย่างน้อย ดังนี้

(๑) Behavioral Analytics เพื่อตรวจจับ Anomalies Indicative of Attack หรือ User Behavior Analytics (UBA) หรือ User and Entity Behavior Analytics (UEBA)

/(๒) Endpoint...

(๒) Endpoint Detection and Response (EDR) (ตรวจจับและตอบสนองต่อเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย)

(๓) Root Cause Analysis (วิเคราะห์หาต้นตอของปัญหาที่เกิดขึ้น)

(๔) Timeline Analysis of Alerts (สามารถแสดง Timeline ของเหตุการณ์ที่เกิดขึ้น)

(๕) Threat Hunting (การตรวจหาภัยคุกคาม อาจเกิดขึ้นในองค์กร)

๒.๓.๒.๔.๗ ระบบที่นำเสนอต้องสามารถเลือกแสดงข้อมูลการตรวจจับและป้องกันภัยคุกคามตาม Timeline นับตั้งแต่จุดเริ่มต้นจนถึงจุดสิ้นสุด หรือแสดงเป็นแผนภาพเหตุการณ์ในหน้าจอเดียวกัน โดยสามารถใช้อุปกรณ์ต่างๆ ที่มีอยู่เดิม หรือเสนอเพิ่มเติมได้

๒.๓.๒.๔.๘ รองรับแสดงรายการช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) หรือ Inventory ต่างๆ ของเครื่อง เช่น Application, User, Disk, Shares โดยครอบคลุมระบบปฏิบัติการ Windows และ Linux

๒.๓.๒.๔.๙ สามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) ระบุประเภทของภัยคุกคาม

(๒) วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

(๓) ระบุต้นทาง (Source) ปลายทาง (Destination)

(๔) ระบุระดับความรุนแรง (Severity)

(๕) รายละเอียดเหตุการณ์และพฤติกรรม

(๖) ค่าคะแนนหรือกำหนดระดับความสำคัญของภัยคุกคามเมื่อเกิดขึ้นกับ IP address, Host และ Username ที่สามารถบ่งบอกความสำคัญของแต่ละเหตุการณ์ที่เกิดขึ้นได้เป็นอย่างน้อย

(๗) สามารถแสดงเทคนิคของภัยคุกคามที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT&CK Stage ต่างๆ

(๘) จัดลำดับความสำคัญของเหตุการณ์ (Priority หรือ Top Cases)

๒.๓.๒.๔.๑๐ สามารถทำงานร่วมกับ Cloud Sandbox หรือ On-Premise Sandbox เพื่อวิเคราะห์ภัยคุกคาม และนำผลลัพธ์มาใช้ในการป้องกันได้ กรณีที่ต้องทำงานร่วมกับ On-Premise Sandbox ให้เสนอ On-Premise Sandbox เพิ่มเติมให้ครอบคลุม และเพียงพอต่อการทำงาน

๒.๓.๒.๔.๑๑ ระบบที่นำเสนอจะต้องสามารถรองรับเชื่อมต่อแบบ Single Sign-on เพื่อนำเข้าข้อมูลบัญชีผู้ใช้งานผ่านโปรโตคอล SAML 2.0 ได้

๒.๓.๒.๔.๑๒ กรณีใช้ Agent Software ที่ติดตั้งบน Endpoint ต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้ (Offline) หรือกรณีใช้ sensor ในการรับ - ส่ง ข้อมูล ให้แสดงรูปแบบการทำงานร่วมกันกับระบบที่เสนอ ในรูปแบบ Online และ Offline

๒.๓.๒.๔.๑๓ สามารถค้นหาข้อมูลโดยรองรับการสร้าง Rule เพื่อตรวจจับภัยคุกคาม เครื่องคอมพิวเตอร์ลูกข่ายจาก หลักฐานหรือร่องรอยที่ชี้ว่าระบบอาจถูกบุกรุก หลังจากเหตุการณ์เกิดขึ้นแล้ว หรือ Indicators of compromise (IOCs) และแบบแผนพฤติกรรมที่บ่งชี้ถึงความพยายามโจมตีหรือกิจกรรมอันตราย ซึ่งเป็นพฤติกรรมที่ไม่เคยเห็นมาก่อน หรือ Behavioral Rules หรือ Behavioral Indicators of Compromise (BIOCs)

/๒.๓.๒.๔.๑๔ มีวิธีการ...

๒.๓.๒.๔.๑๔ มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) โดยแยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่าย (Isolate Endpoint) ได้หลายๆ เครื่องพร้อมๆ กัน ผ่านหน้า Management Console

๒.๓.๒.๔.๑๕ สามารถสร้างแดชบอร์ด และสามารถแก้ไขเพิ่มเติมตามที่กำหนดได้ (Custom Dashboard)

๒.๓.๒.๔.๑๖ สามารถค้นหาข้อมูลหรือเก็บข้อมูลย้อนหลังได้ โดยมีพื้นที่สำหรับเก็บข้อมูลสำหรับระบบไม่น้อยกว่า ๑๘๐ วัน

๒.๓.๒.๕ ระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response - SOAR) จำนวน ๑ ชุด แต่ละชุดจะต้องมีคุณสมบัติไม่ต่ำกว่า หรือเทียบเท่า หรือดีกว่า ดังนี้

๒.๓.๒.๕.๑ เป็นระบบที่ออกแบบเพื่อจัดการเรื่อง Security Orchestration, Automation and Response (SOAR) โดยเฉพาะ และมีระบบ Threat Intelligence Management (TIM) แบบพร้อมใช้งานอยู่ในระบบเดียวกัน

๒.๓.๒.๕.๒ เป็น Software ที่ออกแบบมาเพื่อช่วยในการบริหารจัดการสำหรับ Security Operation Team โดยเฉพาะ โดยมีเครื่องมือที่ช่วยในการทำ Accelerate Response โดยรองรับการทำงานร่วมกับระบบต่างๆ ได้อย่างน้อย ดังนี้

(๑) Security Information and Event Management (SIEM)
(๒) Endpoint Detection and Response (EDR)
(๓) Threat Intelligence (TI)
(๔) Data Loss Prevention (DLP)
(๕) E-Mail
(๖) Ticketing Systems
(๗) Malware Analysis
(๘) Users and Entity Behavior Analytic

๒.๓.๒.๕.๓ มี Threat Intelligence Feeds ที่สามารถดึงข้อมูลผ่าน OpenAPI หรือ TAXII server หรือ TSV จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) อย่างน้อย ๑ Threat Source

๒.๓.๒.๕.๔ มีรูปแบบการบริหารจัดการ Standardize Process และติดตามเหตุการณ์ที่เกิดขึ้น (Incident) รวมไปถึงช่วยวิเคราะห์ (Analyst Metrics) เช่น Task-based Workflows, Playbook Editor, SLA and Metric Tracking เป็นอย่างน้อย

๒.๓.๒.๕.๕ มีระบบช่วยให้ทีมผู้ดูแลระบบต่างๆ สามารถทำงานร่วมกันได้ลักษณะ Collaborate and Learn เช่น Virtual War Room หรือห้องข้อความ เป็นอย่างน้อย และมีระบบ Machine Learning มาช่วยวิเคราะห์และเชื่อมโยงเหตุการณ์ต่างๆ ที่เกิดขึ้นได้

/๒.๓.๒.๕.๖ สามารถ...

๒.๓.๒.๕.๖ สามารถทำ Case Management เพื่อบริหารจัดการ Incident ต่างๆ ที่เกิดขึ้น เช่น กำหนดระยะเวลาในการตอบสนองต่อ Incident ประเภทต่างๆ ได้ รวมถึงแสดงผลการทำงานในภาพรวมลักษณะ SLA Dashboard ได้ หรือนำเสนอระบบอื่นๆ เพิ่มเติม เพื่อรองรับการทำงานในลักษณะดังกล่าว

๒.๓.๒.๕.๗ สามารถทำงานร่วมกับอุปกรณ์ Firewall ยี่ห้อ Palo Alto: PA-5250 ที่สำนักงาน ป.ป.ช.ใช้งานอยู่ได้ เพื่อทำการสั่ง Block IP Address หรือ URL แบบอัตโนมัติได้

๒.๓.๒.๕.๘ สามารถเชื่อมต่อระบบบริหารจัดการภัยคุกคามและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration, Automation and Response - SOAR) ให้สามารถทำงานร่วมกับระบบตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response : XDR) สำหรับเครื่องคอมพิวเตอร์ โดยมีความสามารถอย่างน้อย

(๑) สามารถเรียกข้อมูล incident จากระบบตรวจจับการโจมตีและตอบสนองภัยคุกคามสำหรับเครื่องคอมพิวเตอร์

(๒) สามารถ Update incident ในระบบตรวจจับการโจมตีและตอบสนองภัยคุกคามสำหรับเครื่องคอมพิวเตอร์

(๓) สามารถสั่งงานให้ isolate และยกเลิกการ isolate เครื่อง Endpoint

(๔) สามารถเรียกข้อมูลการตรวจสอบจาก Agent (Query Audit Report) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

(๕) สามารถทำ Incident Mirroring หรือ Incident Synchronization โดยเมื่อมีการเปลี่ยนแปลง incident หรือข้อมูลเหตุการณ์ในระบบบริหารจัดการและตอบสนองภัยคุกคามแบบอัตโนมัติ จะต้องสามารถส่งการเปลี่ยนแปลงดังกล่าวไปยังระบบตรวจจับและตอบสนองภัยคุกคามอื่นๆ ได้โดยอัตโนมัติ และในทางกลับกัน หากมีการเปลี่ยนแปลงข้อมูลเหตุการณ์ในระบบตรวจจับภัยคุกคาม ก็จะต้องสามารถส่งการเปลี่ยนแปลงกลับมา Update ที่ระบบบริหารจัดการและตอบสนองภัยคุกคามแบบอัตโนมัติได้เช่นกัน ซึ่งการทำงานนี้จะต้องทำผ่านกลไกการทำงานอัตโนมัติของแพลตฟอร์ม (Playbook) หรือเทียบเท่าได้

๒.๓.๒.๕.๙ ระบบหรืออุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับ ระบบวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (SIEM) ที่เสนอในการจัดซื้อครั้งนี้ได้

๒.๓.๒.๕.๑๐ สามารถใช้งานระบบ Playbook แบบ Drag and Drop หรือ Query Builder ได้ โดยมีรูปแบบ OOB (Out-of-Box) Predefined Connector มาให้และรูปแบบการสั่งการแบบอัตโนมัติ (Predefined Automated action) จำนวนไม่น้อยกว่า ๒๐๐ Playbook

๒.๓.๒.๕.๑๑ สามารถทำการสร้าง Playbook ได้อย่างน้อยดังนี้

(๑) Manual action and Task

(๒) การสร้างขั้นตอนในการตัดสินใจและอนุมัติ

(๓) การกำหนดเงื่อนไขได้

๒.๓.๒.๕.๑๒ สามารถทำการจำลองขั้นตอนของ Playbook หรือสั่ง Trigger Playbook เพื่อทดสอบการทำงานได้

/๒.๓.๒.๕.๑๓ มีระบบ...

๒.๓.๒.๕.๑๓ มีระบบ Machine Learning เพื่อช่วยงาน Security Operation Center โดยมีความสามารถแสดงให้เห็นภาพรวมเหตุการณ์ที่เกี่ยวข้องกัน

๒.๓.๒.๕.๑๔ สามารถบริหารแบบ GUI จัดการผ่าน Web Browser หรือมี Application เพื่อช่วยบริหารจัดการผ่าน Mobile โดยต้องสามารถแสดง Personal Dashboard และ Task list ของผู้ดูแลระบบความปลอดภัยได้เป็นอย่างน้อย

๒.๓.๒.๕.๑๕ มี Licenses สิทธิในการใช้งานที่สามารถรองรับผู้ใช้งานระดับ Security Analyst ได้ ไม่น้อยกว่า ๕ ผู้ใช้งาน

๒.๓.๒.๕.๑๖ สามารถนำเสนอเป็น Hardware หรือ Software โดยทำการติดตั้งระบบ Virtualization เดิมของสำนักงาน ป.ป.ช. ได้

๒.๓.๒.๕.๑๗ สามารถเชื่อมต่อเพื่อปรับปรุงฐานข้อมูลภัยคุกคามหรือบริการต่างๆ จากศูนย์กลางการให้บริการของผลิตภัณฑ์ ตลอดระยะเวลาของสัญญา

๒.๓.๒.๖ ฝึกอบรมหลักสูตร CompTIA Security+ ให้กับเจ้าหน้าที่ผู้ดูแลระบบรักษาความปลอดภัยของสำนักงาน ป.ป.ช. จำนวนไม่น้อยกว่า ๒ คน พร้อมสอบ Certificate CompTIA Security+

๒.๓.๒.๗ ฝึกอบรมหลักสูตร Security Awareness ให้ผู้ใช้งานระบบสารสนเทศ สำนักงาน ป.ป.ช. จำนวนไม่น้อยกว่า ๑ หลักสูตร อย่างน้อยปีละ ๑ ครั้ง ตลอดระยะเวลาการรับประกัน

๒.๓.๒.๘ เสนอแผนในการประชาสัมพันธ์ Infographic เพื่อเพิ่มความตระหนักด้าน Security Awareness และจัดทำ Infographic ที่อยู่ในรูปแบบนามสกุล (.ai) หรือ (.psd) ได้เป็นอย่างน้อย

๒.๓.๒.๙ จัดทำ VDO ที่เกี่ยวกับการเพิ่มความตระหนักด้าน Security Awareness เวลาไม่น้อยกว่า ๑๐ นาที

ส่วนที่ ๓ ขอบข่ายงาน

๓.๑ ขอบข่ายงาน

สำนักงาน ป.ป.ช. ต้องการจัดหาระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ พร้อมทั้งตั้งค่าการใช้งาน เชื่อมโยงกับระบบเครือข่าย และระบบสารสนเทศ ให้สามารถใช้งานร่วมกับอุปกรณ์และระบบที่สำนักงาน ป.ป.ช. ใช้งานอยู่ได้ โดยมีรายละเอียดดังต่อไปนี้

๓.๑.๑ จัดหาอุปกรณ์ ตามข้อกำหนดพร้อมติดตั้ง ให้สามารถทำงานร่วมกับระบบเครือข่าย และระบบสารสนเทศของสำนักงาน ป.ป.ช. ได้

๓.๑.๒ รายละเอียดการดำเนินการติดตั้ง เชื่อมโยงกับระบบเครือข่าย ระบบเครื่องคอมพิวเตอร์แม่ข่าย และระบบสารสนเทศต่างๆ ของสำนักงาน ป.ป.ช.

๓.๑.๒.๑ ปรับปรุงระบบเครือข่าย ระบบเครื่องคอมพิวเตอร์แม่ข่าย และระบบสารสนเทศต่างๆ ของสำนักงาน ป.ป.ช. ให้ส่งข้อมูลจราจรคอมพิวเตอร์ ข้อมูลการใช้งาน และข้อมูลอื่นที่จำเป็น ไปยังอุปกรณ์ที่เสนอ

๓.๑.๒.๒ ดำเนินการจัดเก็บข้อมูลที่ส่งมาให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และหน่วยงานที่เกี่ยวข้องกำหนด

๓.๑.๒.๓ ดำเนินการวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ข้อมูลการใช้งาน และข้อมูลอื่นเพื่อนำมาพัฒนา Rule ในการเฝ้าระวัง และติดตาม โดยมี rule ตามที่กำหนดเป็นอย่างน้อย

/๓.๑.๒.๔ ปรับแต่ง...

๓.๑.๒.๔ ปรับแต่งค่าการทำงานต่างๆ เช่น ปรับตั้งค่าหน้า Dashboard การตั้งค่า Mapping Policy การตั้งค่า Security Policy รวมถึงการตั้งค่าเกี่ยวกับการทำ Report ต่างๆ ให้สามารถทำงานร่วมกับอุปกรณ์ที่สำนักงาน ป.ป.ช. ใช้งานอยู่ได้

๓.๑.๒.๕ ติดตั้งอุปกรณ์จัดเก็บข้อมูล พร้อมทั้งปรับแต่งค่าการทำงานต่างๆ ให้สามารถใช้งานกับระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ที่เสนอ

๓.๑.๒.๖ งานฝึกอบรม ต้องทำการฝึกอบรมให้ใช้งาน ดูแล บำรุงรักษา และบริหารจัดการอุปกรณ์และซอฟท์แวร์ของอุปกรณ์ได้ รวมทั้งให้เจ้าหน้าที่ของสำนักงาน ป.ป.ช. สามารถดูแลจัดการและแก้ไขปัญหาเบื้องต้นได้

๓.๑.๒.๗ ในการติดตั้งหรือดำเนินการเกี่ยวกับอุปกรณ์หรือระบบที่สำนักงาน ป.ป.ช. ใช้งานอยู่เดิม ให้สามารถทำงานร่วมกับระบบที่เสนอได้ตามข้อกำหนด ผู้ยื่นเสนอราคาจะต้องเป็นผู้รับผิดชอบในการดำเนินการ และค่าใช้จ่ายที่เกิดขึ้น เพื่อให้สามารถทำงานได้ตามข้อกำหนดเป็นอย่างน้อย โดยผู้ยื่นเสนอราคาต้องเป็นผู้สำรวจและประเมินเอง

๓.๑.๓ จะต้องจัดส่งบุคลากรที่มีความรู้ความสามารถในการวิเคราะห์ข้อมูลจราจร และสร้างเงื่อนไขการตรวจสอบ (Rule) มาตรวจสอบและวิเคราะห์ข้อมูลจราจร เพื่อปรับปรุงการทำงานของอุปกรณ์ให้มีประสิทธิภาพมากยิ่งขึ้น โดยจะต้องเข้าดำเนินการ ณ สำนักงาน ป.ป.ช. เดือนละ ๒ วัน (วันละ ๖ ชั่วโมง) เป็นอย่างน้อย ตลอดระยะเวลาการรับประกันของสัญญา

ส่วนที่ ๔ ข้อกำหนดในการตรวจรับงาน

ผู้ขายจะต้องทำการทดสอบระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ และส่งมอบเอกสารรายงาน แผนการดำเนินงาน รายงานการศึกษาวิเคราะห์ออกแบบ และติดตั้งระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ ให้แก่สำนักงาน ป.ป.ช. ทั้งในรูปแบบเอกสาร และเอกสารอิเล็กทรอนิกส์ โดยมีรายละเอียดดังนี้

๔.๑ การทดสอบการทำงานของระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์

๔.๑.๑ ผู้ขายต้องจัดเตรียมขั้นตอนการทดสอบให้ทางสำนักงาน ป.ป.ช. รับทราบก่อนดำเนินการทดสอบเพื่อตรวจรับมอบ และต้องจัดเตรียมเครื่องมือและอุปกรณ์สำหรับทดสอบ โดยถือเป็นภาระของผู้ขาย

๔.๑.๒ หลังจากดำเนินการติดตั้งระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์และตั้งค่าการใช้งานร่วมกับอุปกรณ์ของสำนักงาน ป.ป.ช. เรียบร้อยแล้ว ทดสอบการทำงานของอุปกรณ์ต่างๆ ทุกชนิดให้ทำงานได้อย่างถูกต้อง

๔.๒ เอกสารแสดงระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์

หลังจากติดตั้งระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แล้วเสร็จผู้ขายต้องส่งมอบเอกสารและไฟล์เอกสารที่อยู่ในรูปแบบของ Microsoft Office โดยมีรายการดังต่อไปนี้ เป็นอย่างน้อย เอกสารแสดงรายละเอียดการติดตั้งและตั้งค่าอุปกรณ์ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์แต่ละตัวพร้อมคำอธิบายแต่ละคำสั่งที่ทำการติดตั้งให้ละเอียด เอกสารแสดงแผนผังการเชื่อมต่ออุปกรณ์ต่างๆ ของระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์

/ส่วนที่ ๕...

ส่วนที่ ๕ ระยะเวลาดำเนินงาน

กำหนดเวลางานแล้วเสร็จภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา โดยระยะเวลาดังกล่าวครอบคลุมเวลาในการฝึกอบรม การประชุม การทดสอบระบบ การติดตั้งระบบ การประเมินผลระบบ และการแก้ไขรายงานต่างๆ ในครั้งสุดท้าย

ส่วนที่ ๖ ข้อกำหนดสำหรับผู้ขาย

๖.๑ เงื่อนไขทั่วไป

๖.๑.๑ กรณีมอบหมายให้บุคคลซึ่งมิใช่กรรมการหรือหุ้นส่วนผู้มีอำนาจเต็มทำการยื่นซองแทนหรือผูกพันในนามนิติบุคคลนั้น ต้องมอบอำนาจเป็นหนังสือซึ่งปิดอากรแสตมป์ตามกฎหมายให้บุคคลนั้นเป็นผู้แทนที่มีอำนาจเต็มโดยชอบด้วยกฎหมาย

๖.๑.๒ ในการดำเนินการตามโครงการฯ ในกรณีที่มีความจำเป็นต้องใช้อุปกรณ์ และหรือซอฟต์แวร์ใดๆ เพื่อให้โครงการฯ ดำเนินต่อไปได้ โดยไม่ติดขัด ผู้ขายจะต้องจัดหาอุปกรณ์ และหรือ ซอฟต์แวร์ ดังกล่าวเพื่อให้โครงการดำเนินการต่อไปได้โดยไม่คิดค่าใช้จ่ายใดๆ

๖.๑.๓ ลิขสิทธิ์ซอฟต์แวร์ ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใดๆ ว่ามีการละเมิดลิขสิทธิ์ หรือสิทธิบัตรเกี่ยวกับคอมพิวเตอร์ และหรือ ซอฟต์แวร์ ที่เสนอ ผู้ขายต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้าง หรือเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว ผู้ขายต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่างๆ ที่เกิดขึ้นทั้งหมด

๖.๑.๔ ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์และอุปกรณ์ ที่เสนอต้องเป็นของใหม่ที่ยังมิได้ทำการติดตั้งใช้งาน ณ ที่ใดมาก่อน และไม่เป็นเครื่องที่นำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt) จะต้องเป็นรุ่นที่ยังอยู่ในสายการผลิตในวันยื่นซองประกวดราคา

๖.๑.๕ ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์และอุปกรณ์ที่เสนอ ต้องไม่เป็นผลิตภัณฑ์ของบริษัทผู้ผลิตที่อยู่ในระหว่างการคุ้มครองการเป็นบุคคล หรือนิติบุคคลผู้ล้มละลายตามคำสั่งของศาลที่ได้สั่งการตามกฎหมายของประเทศที่บริษัทของผู้ผลิตนั้นตั้งอยู่

๖.๑.๖ ระบบที่ผู้เสนอราคาเสนอนั้นต้องทำงานร่วมกับระบบเดิมได้ตามที่กำหนดไว้ข้างต้น ถ้ากรณีระบบที่เสนอนั้นไม่สามารถทำงานร่วมกับระบบเดิมได้ ให้ผู้เสนอราคาเสนอระบบใหม่ หรือปรับปรุงระบบให้ทำงานได้ไม่ ต่ำกว่าระบบเดิมที่สำนักงาน ป.ป.ช. ใช้งานอยู่ โดยผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๖.๑.๗ สำนักงาน ป.ป.ช. ขอสงวนสิทธิ์ กรณีมีปัญหาใดๆ เกิดขึ้น ทั้งในช่วงการพิจารณาข้อเสนอและดำเนินงานต่างๆ ภายหลังจากได้ทำสัญญากับผู้ขายแล้ว สำนักงาน ป.ป.ช. ขอสงวนสิทธิ์ในการตัดสินวินิจฉัยชี้ขาดปัญหาที่เกิดขึ้นดังกล่าว และให้ถือว่าคำวินิจฉัยของสำนักงานข้างต้นเป็นที่สิ้นสุดเด็ดขาดแล้ว ผู้เสนอราคาตลอดจน ผู้ขายต้องยอมรับคำวินิจฉัยดังกล่าวโดยจะไม่โต้แย้งหรือมีข้อแม้ใดๆ ทั้งสิ้น

๖.๑.๘ ผู้ขายต้องเก็บรักษาข้อมูลของสำนักงาน ป.ป.ช. ไว้เป็นความลับ และไม่เปิดเผยให้บุคคลภายนอกทราบ ทั้งนี้หากมีการฝ่าฝืน ผู้ขายจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นและตามที่กฎหมายกำหนด

๖.๑.๙ ด้วยสำนักงาน ป.ป.ช. มีกระบวนการทำงาน และมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ดังนั้น ผู้ขายต้องปฏิบัติตามขั้นตอนการทำงานของสำนักงาน ป.ป.ช. อย่างเคร่งครัด

/๖.๑.๑๐ ผู้ขาย...

๖.๑.๑๐ ผู้ขายต้องเก็บรักษาข้อมูลของสำนักงาน ป.ป.ช. ไว้เป็นความลับ และไม่เปิดเผยให้บุคคลภายนอกทราบ ทั้งนี้หากมีการฝ่าฝืนผู้ขายจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นและตามที่กฎหมายกำหนด และต้องลงนามในข้อตกลงใช้พื้นที่และรักษาความลับ (Non Disclosure Agreement & Data Center Access Request Form)

๖.๒ ข้อกำหนดในการติดตั้งอุปกรณ์และระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์

๖.๒.๑ ผู้ขายต้องจัดเตรียมบุคลากรที่มีความรู้ความสามารถทางด้านคอมพิวเตอร์ ด้านระบบเครือข่าย ด้านระบบสารสนเทศ และด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่จะปฏิบัติหน้าที่ในการสนับสนุนการดำเนินการติดตั้ง จำนวนไม่น้อยกว่า ๑ คน ที่สามารถติดต่อได้โดยตรง

๖.๒.๒ ผู้ขายต้องกำหนดตัวบุคคลที่ต้องรับผิดชอบ พร้อมทั้งรายชื่อผู้ปฏิบัติงานทั้งหมด และจัดส่งให้ผู้ควบคุมการติดตั้งระบบทราบเพื่อขออนุมัติสำหรับการเข้าปฏิบัติงานภายในบริเวณอาคารของสำนักงาน ป.ป.ช. เพื่อสะดวกในการสั่งการ หรือติดต่อประสานงานในการปฏิบัติงาน

๖.๒.๓ ผู้ขายต้องส่งรายละเอียดขั้นตอนและขอบเขตของการทำงานทั้งหมดให้กับ ผู้ควบคุมงานการติดตั้งระบบ เพื่อตรวจสอบขั้นตอนก่อนวันทำงาน ภายใน ๑๕ วัน หลังจากลงนามในสัญญา

๖.๒.๔ ในกรณีที่ผู้ขายมีรายละเอียดปลีกย่อยเกี่ยวกับขั้นตอนลำดับก่อนหลังในการติดตั้งระบบต้องขอคำปรึกษาและแจ้งให้ผู้ดูแลระบบของสำนักงาน ป.ป.ช. ทราบ

๖.๒.๕ ในแต่ละวันก่อนลงมือปฏิบัติงาน ผู้ขายต้องติดต่อกับผู้ควบคุมงานของสำนักงาน ป.ป.ช. พร้อมทั้งชี้แจงวัตถุประสงค์ในการปฏิบัติงานโดยสังเขป

๖.๒.๖ อุบัติเหตุหรือภยันตรายที่เกิดกับทรัพย์สิน บุคลากรของสำนักงาน ป.ป.ช. และระบบคอมพิวเตอร์ หรือข้อมูลของสำนักงาน ป.ป.ช. ผู้ขายต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการทำงานของผู้ขาย

๖.๒.๗ ผู้ขายต้องไม่ทำให้ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของสำนักงาน ป.ป.ช. ที่มีอยู่เดิมไม่สามารถทำงานได้หรือหยุดการทำงาน เว้นแต่ได้รับอนุญาตจากทางสำนักงาน ป.ป.ช.

๖.๒.๘ ผู้ขายต้องรับผิดชอบในการติดตั้งอุปกรณ์ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ตามข้อกำหนดของอาคารและเจ้าของสถานที่ ทั้งนี้หากต้องมีอุปกรณ์อื่นใด เพิ่มเติมเป็นหน้าที่ผู้ขายในการจัดหามาเพื่อให้การดำเนินการ แล้วเสร็จตามสัญญา

๖.๒.๙ ในระหว่างการติดตั้งส่งมอบอุปกรณ์ยังไม่เสร็จสมบูรณ์ในแต่ละงวด สำนักงาน ป.ป.ช. มีสิทธิ์ที่จะใช้อุปกรณ์ที่ติดตั้งแล้ว หากมีเหตุให้ต้องเลิกสัญญาอันเนื่องจากเป็นความบกพร่องของผู้ขาย ผู้ขายไม่มีสิทธิที่จะเรียกร้องจากสำนักงาน ป.ป.ช. ซึ่งค่าใช้งาน และ/หรือค่าเสียหายใดๆ อันเกิดจากการใช้อุปกรณ์ตามโครงการ และข้อมูลหรือค่าที่ใช้งานในอุปกรณ์ดังกล่าว ทั้งนี้สำนักงาน ป.ป.ช. ยังคงไว้ซึ่งความเป็นเจ้าของข้อมูล

๖.๒.๑๐ เมื่อทำการติดตั้งอุปกรณ์ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์เสร็จสิ้น ผู้ขายต้องส่งรายละเอียดการ Configuration ของอุปกรณ์และระบบต่างๆ ที่เสนอทั้งหมด ให้สำนักงาน ป.ป.ช. โดยจัดทำเป็นสำเนาส่งให้สำนักงาน ป.ป.ช. และจัดทำสำเนาทุกครั้งที่มีการเปลี่ยนแปลง ซึ่งในทุกครั้งที่มีการเปลี่ยนแปลงค่า Configuration ผู้ขายจะต้องบันทึกรายละเอียดการเปลี่ยนแปลงตามแบบคำขอปรับปรุงระบบ (Change Request From) ตามมาตรฐานระบบ ISO/IEC 27001 ส่งให้สำนักงาน ป.ป.ช. เห็นชอบก่อนการดำเนินการ

/ทุกครั้ง...

ทุกครั้ง เว้นแต่เกิดกรณีฉุกเฉิน ผู้ขายจะต้องแจ้งให้ผู้ดูแลระบบทราบและเห็นชอบก่อนดำเนินการ และจัดส่งแบบคำขอปรับปรุงระบบ (Change Request Form) ให้สำนักงาน ป.ป.ช. ภายใน ๑ วันทำการ

๖.๓ ข้อกำหนดในการติดตั้งระบบไฟฟ้าให้กับอุปกรณ์ระบบคอมพิวเตอร์ (ถ้ามี)

๖.๓.๑ ผู้ขายต้องรับผิดชอบในการติดตั้งอุปกรณ์ไฟฟ้าตามข้อกำหนดของอาคารและเจ้าของสถานที่

๖.๓.๒ ผู้ขายต้องรับผิดชอบในการติดตั้งอุปกรณ์ไฟฟ้าและวางสายไฟฟ้าพร้อมสายดินจาก แนววงจรหลัก (Main Circuit) ของอาคารในแต่ละชั้นไปยังจุดติดตั้งอุปกรณ์ระบบคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ ทั้งหมดสามารถทำงานได้ โดยสายไฟฟ้าดังกล่าวต้องติดตั้งอยู่ภายในท่อร้อยสายตามข้อกำหนดและมาตรฐานของอาคารที่ทำการติดตั้งสายไฟฟ้า

๖.๓.๓ ผู้ขายต้องรับผิดชอบในการติดตั้งสายดินให้กับอุปกรณ์คอมพิวเตอร์ เช่น ตู้จัดเก็บอุปกรณ์ระบบคอมพิวเตอร์ เพื่อให้อุปกรณ์ทั้งหมดทำงานได้อย่างถูกต้องและป้องกันปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ไม่ว่าด้วยสาเหตุใด

๖.๔ การบำรุงรักษาและซ่อมแซมแก้ไขระบบสารสนเทศและระบบคอมพิวเตอร์

ผู้ขายต้องรับประกันคุณภาพของระบบที่ทำการติดตั้ง ด้วยการบำรุงรักษา ซ่อมแซม แก้ไข หรือเปลี่ยนแทน เป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับตั้งแต่วันตรวจรับระบบเสร็จสมบูรณ์ทั้งหมด โดยที่สำนักงาน ป.ป.ช. ไม่ต้องรับผิดชอบค่าใช้จ่ายใดๆ ทั้งสิ้น โดยในระยะเวลารับประกันโดยต้องปฏิบัติตามเงื่อนไข ดังต่อไปนี้

๖.๔.๑ หากอุปกรณ์อื่นใด หรือระบบที่เสนอในโครงการ ชำรุด บกพร่อง หรือใช้งานไม่ได้ ไม่ว่าจะติดตั้ง ณ สถานที่ใด ตามที่กำหนดในสัญญา ความชำรุดนี้มิได้เกิดจากความผิดพลาดของสำนักงาน ป.ป.ช. ผู้ขายต้องเริ่มจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพดีใช้งานได้ดังเดิม โดยไม่คิดค่าใช้จ่ายใดๆ จากสำนักงาน ป.ป.ช. โดยสามารถแจ้งเหตุได้ทุกวัน อย่างน้อย ๓ ทาง คือ ทางโทรศัพท์พื้นฐาน โทรสาร และจดหมายอิเล็กทรอนิกส์ หลังจากรับแจ้งเหตุแล้ว ผู้ขายจะตอบกลับภายใน ๑ ชั่วโมง โดยโทรสาร หรือจดหมายอิเล็กทรอนิกส์ สำหรับสำนักงาน ป.ป.ช. ส่วนกลางจะดำเนินการแก้ไขให้แล้วเสร็จภายในระยะเวลา ๑ วัน นับจากได้รับแจ้งเหตุ ในกรณีที่เป็นอุปกรณ์หรือระบบคอมพิวเตอร์ที่สามารถเปลี่ยนทดแทนได้ ถ้าการซ่อมแซมแก้ไขไม่เสร็จภายในที่กำหนด ๑ วัน นับแต่เริ่มการซ่อมแซมแก้ไขผู้ขายต้องนำอุปกรณ์หรือเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันมาใช้แทนจนกว่าจะซ่อมแซมแล้วเสร็จสมบูรณ์ แต่ถ้าระบบคอมพิวเตอร์ยังคงขัดข้องอยู่ผู้ขายจะต้องถูกปรับตามอัตราที่ระบุไว้ในข้อ ๖.๔.๕.๑

๖.๔.๒ ผู้ขายมีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขรายการที่ชำรุด ไม่ว่าจะติดตั้งอยู่ ณ สถานที่ใดๆ ให้อยู่ในสภาพใช้งานได้ดี อยู่เสมอตลอดระยะเวลาการรับประกันด้วยค่าใช้จ่ายของผู้ขาย สำนักงาน ป.ป.ช. ยอมให้ระบบที่ติดตั้งขัดข้องภายหลังคำนวณตัวถ่วงแล้ว ไม่เกินเดือนละ ๑๒ ชั่วโมง ถ้าระบบสารสนเทศและระบบคอมพิวเตอร์ขัดข้องเกินระยะเวลาดังกล่าว ผู้ขายจะต้องถูกปรับตามอัตราที่ระบุไว้ในข้อ ๖.๔.๕.๑

๖.๔.๓ ผู้ขายต้องทำการบำรุงรักษา อุปกรณ์และซอฟต์แวร์ระบบ (System software) ที่เสนอตลอดระยะเวลารับประกัน โดยไม่คิดค่าใช้จ่ายใดๆ

๖.๔.๔ ผู้ขายต้องทำการบำรุงรักษา (Preventive maintenance) ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ อย่างน้อยทุก ๓ เดือนต่อ ๑ ครั้ง เพื่อให้ระบบอยู่ในสภาพที่ใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา โดยทำการบำรุงรักษาในเวลาที่ไม่กระทบกระเทือนต่อการปฏิบัติงานของสำนักงาน ป.ป.ช. หากผู้ขายไม่ปฏิบัติตามเงื่อนไขข้อนี้ สำนักงาน ป.ป.ช. จะปรับในอัตราที่ระบุไว้ในสัญญา

/๖.๔.๕ ค่าปรับ...

๖.๔.๕ ค่าปรับ

๖.๔.๕.๑ กรณีอุปกรณ์หรือระบบชำรุดไม่สามารถใช้งานได้ (คำนวณเดือนละ ๑ ครั้ง)

ค่าปรับ = ร้อยละ ๐.๐๒ ของ ((ผลรวมจำนวนชั่วโมงที่ขัดข้อง – ๑๒) * (มูลค่าของอุปกรณ์หรือระบบที่หยุดให้บริการ)

ผลรวมจำนวนชั่วโมงที่ขัดข้อง = ค่าสูงสุด (ชั่วโมงที่ขัดข้อง * ค่าตัวถ่วง)

ชั่วโมงที่ขัดข้อง = สำหรับจำนวนชั่วโมงที่ใช้ในการคำนวณค่าปรับ จะเริ่มนับตั้งแต่เวลาที่ผู้ขายเริ่มดำเนินการแก้ไข จนถึงเวลาที่ผู้ขายเริ่มดำเนินการแก้ไขแล้วเสร็จ

(หมายเหตุ เศษของจำนวนชั่วโมงนับเป็น ๑ ชั่วโมง)

๖.๔.๕.๒ กำหนดค่าตัวถ่วงของระบบเครือข่ายคอมพิวเตอร์

ลำดับที่	รายการ	ค่าถ่วง
๑	ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	๑.๐
๒	ระบบวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Information and Event Management: SIEM)	๑.๐
๓	อุปกรณ์จัดเก็บข้อมูล ขนาดไม่น้อยกว่า 60 TB Raid 1	๑.๐
๔	ระบบตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR)	๑.๐
๕	ระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR)	๑.๐

๖.๔.๖ ผู้ขายต้องจัดทำรายงานการบำรุงรักษาเป็นรายเดือน และส่งมอบให้สำนักงาน ป.ป.ช. ทุก ๓ เดือน อย่างน้อยดังนี้

- วันที่และเวลาที่มาถึง
- วันที่และเวลาที่แล้วเสร็จ
- ขั้นตอนดำเนินการ
- ผลการดำเนินการ
- รายการอุปกรณ์ และหมายเลขเครื่อง
- สถานะของอุปกรณ์
- คำแนะนำ

๖.๔.๗ ผู้ขายต้องจัดทำรายงานอุบัติการณ์ (Incident Report) ตามมาตรฐานระบบ ISO/IEC 27001 และส่งให้สำนักงาน ป.ป.ช. ภายใน ๓ วันทำการ ซึ่งประกอบด้วยเนื้อหาอย่างน้อยดังต่อไปนี้

- วันที่และเวลาที่เริ่มดำเนินการแก้ไข
- วันที่และเวลาที่แล้วเสร็จ
- ขั้นตอนดำเนินการ
- ผลการดำเนินการ

/- รายการ...

- รายการอุปกรณ์, หมายเลขเครื่อง, รายการซอฟต์แวร์
- สถานะของอุปกรณ์ และซอฟต์แวร์
- ปัญหาที่เกิดขึ้น
- วิธีการแก้ไขปัญหา
- ค่าการปรับเปลี่ยนในแต่ละรายการที่แก้ไข
- คำแนะนำ

๖.๕ การสนับสนุนโครงการ

ผู้ขายต้องจัดให้มีการสนับสนุนอย่างต่อเนื่องตลอดระยะเวลาการรับประกันระบบ โดยไม่มีค่าใช้จ่ายใดๆ ทั้งสิ้นจากสำนักงาน ป.ป.ช. ในเรื่องต่างๆ ดังนี้

๖.๕.๑ การติดตั้งซอฟต์แวร์ การแก้ไขข้อบกพร่องของซอฟต์แวร์ การแก้ไข ปรับปรุงเพิ่มเติมและติดตั้งซอฟต์แวร์ ในลักษณะของการ Upgrade ซอฟต์แวร์ หรือ Version ใหม่ของระบบคอมพิวเตอร์ ผู้ขายต้องดำเนินการให้ และอบรมเจ้าหน้าที่ของผู้ซื้อ โดยไม่คิดค่าใช้จ่ายใดๆ ตลอดระยะเวลาการรับประกัน

๖.๕.๒ ผู้ขายต้องจัดส่งบุคลากร จำนวน ๑ คน ที่มีความรู้ความสามารถทางด้านการเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ โดยต้องปฏิบัติหน้าที่ที่สำนักงาน ป.ป.ช. เป็นเวลาไม่น้อยกว่า ๑๕ วันทำการ นับจากวันติดตั้งและเริ่มใช้งานระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ เพื่อสนับสนุนและดำเนินการให้ผู้ใช้งานสามารถใช้งานระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ที่ติดตั้งได้ตามปกติ

๖.๕.๓ ผู้ขายต้องให้คำปรึกษาแก่เจ้าหน้าที่ของผู้ซื้อ เกี่ยวกับการแก้ไขหรือปรับปรุงระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ (Threat Detection and Incident Response Platform) ที่ส่งมอบ โดยไม่คิดค่าใช้จ่ายใดๆ ตลอดระยะเวลาการรับประกัน

๖.๖ การฝึกอบรม

ผู้ขายต้องจัดให้มีการฝึกอบรมบุคลากรของสำนักงาน ป.ป.ช. ตามความจำเป็นต่อการปฏิบัติงาน (On the job training) ตามข้อกำหนดต่อไปนี้

๖.๖.๑ ผู้ขายต้องรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด เช่น ค่าสถานที่ ค่าวิทยากร ค่าเอกสาร ค่าอุปกรณ์ในการฝึกอบรม ค่าอาหารว่าง ค่าอาหารกลางวัน และค่าเดินทาง (กรณีอบรมนอกสถานที่) เป็นต้น

๖.๖.๒ ผู้ขายต้องจัดให้มีการฝึกอบรมทั้งด้านวิชาการและด้านปฏิบัติการ โดยครอบคลุมเนื้อหาด้านฮาร์ดแวร์ และซอฟต์แวร์ ที่เกี่ยวข้องกับระบบที่เสนอทั้งหมด เพื่อให้สามารถปฏิบัติงานกับระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ (Threat Detection and Incident Response Platform) ได้อย่างมีประสิทธิภาพ โดยครอบคลุมเนื้อหาหลักสูตรต่อไปนี้เป็นอย่างน้อย

๖.๖.๒.๑ หลักสูตรสำหรับการใช้งาน การติดตั้งและกำหนดคุณสมบัติต่างๆ ให้กับอุปกรณ์และซอฟท์แวร์ทุกรายการที่เสนอ

๖.๖.๒.๒ หลักสูตรการใช้งานและดูแลระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ (Threat Detection and Incident Response Platform)

๖.๖.๒.๓ หลักสูตรการวิเคราะห์ปัญหาต่างๆ ที่เกิดระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์เบื้องต้น เพื่อให้บุคลากรของสำนักงาน ป.ป.ช. สามารถที่จะดูแลระบบได้ระดับหนึ่ง

๖.๖.๒.๔ หลักสูตร Security Awareness สำหรับผู้ดูแลระบบสารสนเทศ

/๖.๖.๒.๕ หลักสูตร...

๖.๖.๒.๕ หลักสูตร Security Awareness สำหรับผู้ใช้งานระบบสารสนเทศ

๖.๖.๒.๖ หลักสูตรอื่นๆ ตามความจำเป็น

๖.๖.๓ โดยผู้ขายจะต้องกำหนดวิชาที่อบรมในแต่ละช่วงเวลา ให้เหมาะสมกับการปฏิบัติงาน และภาษาที่ใช้ในการฝึกอบรมควรเป็นภาษาไทย

๖.๖.๔ ผู้ขายต้องเสนอหลักสูตรต่างๆ รายละเอียดการฝึกอบรมและหลักสูตรมาให้ครบถ้วน เช่น เนื้อหาหลักสูตร ช่วงเวลาในการอบรม ระดับผู้เข้ารับการอบรม และจำนวนผู้เข้าอบรม เป็นต้น

๖.๖.๕ ผู้ขายต้องเสนอแผนการอบรมและหลักสูตรการอบรมให้สำนักงาน ป.ป.ช. เห็นชอบทุกหลักสูตรก่อนเริ่มทำการฝึกอบรม โดยในแต่ละหลักสูตรจะมีผู้เข้ารับการอบรมอย่างน้อยจำนวน ๑๕ คน และจัดให้มีเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ให้เพียงพอต่อการอบรมในช่วงที่มีภาคปฏิบัติ

๖.๖.๖ ในระหว่างการฝึกอบรม สำนักงาน ป.ป.ช. สงวนสิทธิ ในการยกเลิกผู้บรรยายที่ไม่มีความรู้ความสามารถเพียงพอ และผู้ขายจะต้องจัดหาผู้บรรยายให้ใหม่ และทำการอบรมในหลักสูตรนั้นใหม่ รวมทั้งหากเนื้อหาในหลักสูตรใด ไม่ครบถ้วน ผู้ขายต้องจัดฝึกอบรมเพิ่มเติมให้ โดยไม่คิดค่าใช้จ่ายเพิ่ม

๖.๖.๗ เมื่อมีการ Upgrade ทั้ง ฮาร์ดแวร์ และ ซอฟต์แวร์ ให้ผู้ขายทำการฝึกอบรมในส่วนที่เพิ่มเติมหรือเปลี่ยนแปลงไปจากเดิมโดย สำนักงาน ป.ป.ช. ไม่เสียค่าใช้จ่ายใดๆ ทั้งสิ้น

๖.๖.๘ สำนักงาน ป.ป.ช. สงวนสิทธิที่จะให้ผู้ขายจัดอบรมในหลักสูตรมากกว่า ๑ ครั้ง ในกรณีที่สำนักงาน ป.ป.ช. เห็นสมควร

๖.๖.๙ ผู้ขายจะต้องรับผิดชอบต่อค่าใช้จ่ายที่เกิดขึ้นในระหว่างการอบรมทั้งหมด

๖.๗ เอกสารทางวิชาการ

๖.๗.๑ เพื่อให้การฝึกอบรม และการปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ และเป็นประโยชน์ในการค้นหาความรู้เพิ่มเติม ผู้ขายจะต้องจัดหาเอกสารวิชาการที่จำเป็นต่อการปฏิบัติงาน เช่น

๖.๗.๑.๑ เอกสารคู่มือปฏิบัติงานของระบบ และซอฟต์แวร์ต่างๆ จำนวนชุดของเอกสารคู่มือให้เท่ากับจำนวนชุดของอุปกรณ์ที่เสนอ ในวันส่งมอบระบบ

๖.๗.๑.๒ เอกสารวิชาการหรือคู่มือต่างๆ หากมีการ Revised หรือมีการออก Version ใหม่ ผู้ขายจะต้องจัดส่งเอกสารที่ปรับปรุงแล้ว มอบให้สำนักงาน ป.ป.ช. ทุกครั้งโดย ไม่มีค่าใช้จ่ายใดๆ ตามจำนวนชุดที่ สำนักงาน ป.ป.ช. มีอยู่เดิม

๖.๗.๑.๓ เอกสารคู่มือการปฏิบัติงานและแก้ไขปัญหาของระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ที่ทำการติดตั้ง สำหรับเจ้าหน้าที่ควบคุมระบบ (Operation manual) เป็นภาษาไทย จำนวน ๒ ชุด ให้สำนักงาน ป.ป.ช. ในวันส่งมอบระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์

๖.๗.๑.๔ เอกสารความก้าวหน้าของผลิตภัณฑ์ใหม่ๆ ที่เป็นยี่ห้อเดียวกันกับระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ที่เสนอ (ถ้ามี)

ส่วนที่ ๗ เงื่อนไขการส่งมอบงานและการจ่ายเงิน

๗.๑ ระยะเวลาดำเนินการ การส่งมอบ

๗.๑.๑ ระยะเวลาดำเนินการ

ระยะเวลาดำเนินโครงการฯ ของสำนักงาน ป.ป.ช. มีทั้งสิ้น ๑๘๐ วันนับจากวันถัดจากวันที่ลงนามในสัญญา

/๗.๑.๒ การส่งมอบ...

๗.๑.๒ การส่งมอบ

โครงการฯ มีรายละเอียดการส่งมอบ ดังนี้

งวดงานที่ ๑ ส่งมอบแผนการปฏิบัติงาน รายละเอียดขั้นตอนและขอบเขตของการทำงานทั้งหมดให้กับผู้ควบคุมงานการติดตั้งระบบเพื่อตรวจสอบขั้นตอน ตามข้อ ๖.๒.๓ จำนวน ๒ ชุด ภายใน ๑๕ วัน นับถัดจากวันลงนามในสัญญา และต้องมีรายละเอียดของแบบรูปแผนผังการติดตั้งระบบ อย่างน้อยดังนี้

- แบบรูปแผนผังของระบบและอุปกรณ์โดยภาพรวม ที่แสดงถึงการเชื่อมต่อกับระบบเครือข่ายและระบบคอมพิวเตอร์ของสำนักงาน ป.ป.ช. ที่จะต้องมีการใช้งานร่วมกับระบบตามโครงการ
- แบบรูปแผนผังของระบบและอุปกรณ์โดยละเอียดพร้อมรายการอ้างอิงถึงรายละเอียดของระบบที่เสนอ และอุปกรณ์ที่จะติดตั้ง

งวดงานที่ ๒ ส่งมอบรายงานการวิเคราะห์และออกแบบระบบที่เสนอ จำนวน ๒ ชุด ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยต้องมีรายละเอียด ดังนี้

- การออกแบบการทำงานและเชื่อมโยงระหว่างระบบงาน (System Overview) พร้อมคำอธิบาย
- รายงานการสำรวจ และการออกแบบการทำงานและเชื่อมโยงระหว่างระบบงาน (System Overview) เพื่อติดตั้งระบบ
- แผนการดำเนินการติดตั้งและเชื่อมโยงการทำงานของระบบ
- แผนการทดสอบระบบ (Test Plan)
- แผนการเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์
- แผนการฝึกอบรม

งวดงานที่ ๓ การติดตั้งอุปกรณ์และระบบที่เสนอ และส่งมอบรายงานการติดตั้ง ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยต้องมีรายละเอียด ดังนี้

- การส่งมอบและติดตั้งอุปกรณ์และระบบที่เสนอทั้งหมด
- รายงานการติดตั้งอุปกรณ์และระบบที่เสนอทั้งหมด

งวดงานที่ ๔ ส่งมอบเอกสารการตั้งค่าใช้งาน การทดสอบระบบ รายงานผลการใช้งาน และรายงานผลการอบรม จำนวน ๒ ชุด ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยต้องมีรายละเอียด ดังนี้

- รายละเอียดการตั้งค่าใช้งาน (Config) ระบบตามข้อ ๖.๒.๑๐
- เอกสารรายงานผลการทดสอบ ผลการใช้งาน และผลการฝึกอบรม
- คู่มือการติดตั้งและใช้งานระบบบริหารจัดการ อย่างละเอียด
- คู่มือการติดตั้งและใช้งานโปรแกรม อย่างละเอียด

๗.๑.๓ การจ่ายเงิน

สำนักงาน ป.ป.ช. จะจ่ายเงินค่าจ้าง เมื่อผู้ขายได้ดำเนินการส่งมอบงาน งวดที่ ๑ งวดที่ ๒ งวดที่ ๓ งวดที่ ๔ และดำเนินการตรวจรับพัสดุเรียบร้อยแล้ว

/ส่วนที่ ๘...

ส่วนที่ ๘ การรับประกันคุณภาพงาน

ผู้ขายต้องรับประกันคุณภาพระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ และอุปกรณ์ที่เสนอเป็นเวลาไม่น้อยกว่า ๑ ปี โดยที่สำนักงาน ป.ป.ช. ไม่ต้องรับผิดชอบค่าใช้จ่ายใดๆ ทั้งสิ้น อันเกิดจากการซ่อมแซมปรับปรุง เปลี่ยนแปลง แก้ไขระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ ของสำนักงาน ป.ป.ช. และสำหรับการเปลี่ยนแปลงหรือเพิ่มเติมอุปกรณ์ใดๆ ในระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ จะต้องแจ้งให้สำนักงาน ป.ป.ช. ทราบเป็นลายลักษณ์อักษรก่อนกระทำการใดๆ ทั้งสิ้น

ส่วนที่ ๙ คุณสมบัติผู้เสนอราคา และรายละเอียดการเสนอราคา

๙.๑ คุณสมบัติผู้เสนอราคา

๙.๑.๑ มีความสามารถตามกฎหมาย

๙.๑.๒ ไม่เป็นบุคคลล้มละลาย

๙.๑.๓ ไม่อยู่ระหว่างเลิกกิจการ

๙.๑.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๙.๑.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๙.๑.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๙.๑.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๙.๑.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ป.ป.ช. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๙.๑.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๙.๑.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

(๑) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(๒) กรณีข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

/(๓) การยื่น...

(๓) การยื่นข้อเสนอของกิจการร่วมค้า

(๓.๑) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(๓.๒) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ (๓.๑) ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

๙.๑.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

๙.๑.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

๑. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียน เกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงสถานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงสถานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปีโดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงสถานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม – เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

๒. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอ จะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๓ ล้านบาท

๓. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

๔. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทย

/แจ้งเวียน...

แจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวม ของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

๕. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ ๒ ข้อ ๓ และข้อ ๔ (๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิ ของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศ ว่าด้วยการรับรองเอกสาร พ.ศ. ๒๕๓๙ และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสารดังกล่าว ในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่า ผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

๖. กรณีตามข้อ ๑ - ข้อ ๕ ไม่ใช้บังคับกับกรณีดังต่อไปนี้

(๖.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(๖.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๔๘๓ และที่แก้ไขเพิ่มเติม

(๖.๓) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(๖.๔) การจัดซื้อจัดจ้างตามมาตรา ๕๖ วรรคหนึ่ง (๒) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

(๖.๕) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

(๖.๖) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

/๙.๑.๑๓ ผู้ยื่น...

๙.๑.๑๓ ผู้ยื่นข้อเสนอต้องมีบุคลากรผู้เชี่ยวชาญด้านระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ที่เกี่ยวข้องไม่น้อยกว่า ๒ คน และมีประสบการณ์ไม่น้อยกว่า ๕ ปี

๙.๑.๑๔ ผู้ยื่นข้อเสนอต้องมีผลงานการให้บริการ หรือพัฒนาระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ ให้หน่วยราชการหรือรัฐวิสาหกิจหรือเอกชนที่สำนักงาน ป.ป.ช. เชื่อถือ ซึ่งมีมูลค่าอย่างน้อย ๓ ล้านบาทต่อหนึ่งสัญญา จำนวนอย่างน้อย ๑ สัญญา โดยผู้เสนอราคาต้องเสนอชื่อสถานที่ติดตั้ง พร้อมทั้งสำเนาหนังสือรับรองผลงาน โดยต้องมีหัวหน้าหน่วยงานหรือผู้ทำการแทนของหน่วยงานนั้นเป็นผู้ลงนามรับรอง สำเนาสัญญา และตัวอย่างเอกสารประกอบหลังจากการติดตั้ง (ถ้ามี) ของหน่วยงานหรือองค์กรที่อ้างอิง ทั้งนี้ สำนักงาน ป.ป.ช. สงวนสิทธิที่จะตรวจสอบวินิจฉัยข้อเท็จจริงโดยตรงจากผู้รับรองที่เสนอมานั้น

๙.๒ รายละเอียดเอกสารประกอบการพิจารณาการเข้าประกวดราคา

๙.๒.๑ ผู้เสนอราคาต้องจัดเตรียมเอกสารแสดงคุณลักษณะเฉพาะของครุภัณฑ์ อุปกรณ์ และระบบที่นำเสนอทั้งหมด โดยไม่อนุญาตให้มีการขอส่งเอกสารเพิ่มเติมในภายหลังไม่ว่ากรณีใดๆ นับจากวันให้ยื่นซอง ทั้งนี้ สำนักงาน ป.ป.ช. สงวนสิทธิที่จะร้องขอเอกสารเพิ่มเติมในกรณีที่มีปัญหาหรือข้อสงสัย

๙.๒.๒ ผู้เสนอราคาต้องจัดทำตารางการเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะของครุภัณฑ์ อุปกรณ์ และระบบที่นำเสนอทั้งหมด ตามข้อกำหนดของสำนักงาน ป.ป.ช. กับที่เสนอเป็นข้อๆ ในแต่ละรายการอย่างละเอียด โดยพิมพ์เป็นเอกสารประกอบการนำเสนอ พร้อมทั้งบ่งชี้ในแต่ละรายการ และในแคตตาล็อกอย่างครบถ้วนและชัดเจน

๙.๒.๓ ผู้เสนอราคาต้องพร้อมที่จะจัดเตรียมอุปกรณ์ที่เสนอทั้งหมดอย่างละ ๑ ชิ้น พร้อมทั้งแสดงให้เห็นถึงการใช้งานเพื่อแสดงให้คณะกรรมการพิจารณาผลได้พิจารณาเพิ่มเติมเมื่อคณะกรรมการพิจารณามีการร้องขอ

๙.๒.๔ ผู้เสนอราคาต้องจัดส่งเอกสารหลักฐานแสดงผลงานการติดตั้งระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ ที่มีรายละเอียดอย่างน้อยดังนี้

๙.๒.๔.๑ สำเนาหนังสือรับรองผลงาน โดยต้องมีหัวหน้าหน่วยงานหรือผู้ทำการแทนของหน่วยงานนั้นเป็นผู้ลงนามรับรอง

๙.๒.๔.๒ สำเนาสัญญาว่าจ้างที่อ้างถึง

๙.๒.๔.๓ ตัวอย่างเอกสารประกอบหลังจากการติดตั้ง (ถ้ามี)

๙.๒.๕ ผู้เสนอราคาต้องส่งรายชื่อของทีมงาน พร้อมคุณวุฒิ ความเชี่ยวชาญ ประวัติการทำงาน และความรับผิดชอบที่ต้องรับผิดชอบในงานนี้ หากปรากฏว่ามีการส่งรายชื่อไม่เป็นตรงกับความจริง สำนักงาน ป.ป.ช. ขอสงวนสิทธิ์ไม่พิจารณาข้อเสนอของผู้เสนอราคารายนั้นทันที

๙.๒.๖ ผู้เสนอราคาต้องจัดส่งรายการเอกสารดังต่อไปนี้ เพื่อเป็นข้อมูลในการพิจารณา

๙.๒.๖.๑ ภาพรวมการทำงานของระบบ

๙.๒.๖.๒ แผนการทำงานในการติดตั้งระบบ

๙.๒.๖.๓ แผนการตรวจรับอุปกรณ์ทั้งหมด และระบบที่ติดตั้งใหม่ทั้งระบบ

๙.๒.๗ ผู้เสนอราคาจะต้องเสนอราคาแยกในแต่ละรายการของอุปกรณ์ และยืนราคาตามที่เสนอจนกว่าจะหมดระยะเวลารับประกัน ใช้ในกรณีที่สำนักงาน ป.ป.ช. มีความจำเป็นต้องมีการจัดซื้ออุปกรณ์ต่างๆ หรือจัดจ้างเพิ่มเติมในระหว่างการส่งมอบอุปกรณ์หรือระยะเวลารับประกัน

/๙.๒.๘ ผู้เสนอราคา...

๙.๒.๘ ผู้เสนอราคาต้องเสนอราคาค่าบำรุงรักษาหลังจากหมดระยะเวลารับประกันเป็นระยะเวลาไม่น้อยกว่า ๔ ปี และต้องยืนราคาที่เสนอเป็นระยะเวลาไม่น้อยกว่า ๕ ปี นับจากวันส่งมอบระบบ

ส่วนที่ ๑๐ ปัญหาข้อขัดแย้งหรือการตีความ

ในกรณีที่มีความจำเป็นต้องตีความข้อใด หรือมีข้อความใดที่ขัดแย้งในประกาศประกวดราคา หรือเอกสารเสนอราคา หรือในเอกสารอื่นใดก็ตาม ซึ่งมีความจำเป็นต้องวินิจฉัยตัดสินเพื่อให้การประกวดราคาครั้งนี้เป็นไปด้วยความเรียบร้อยบรรลุวัตถุประสงค์ของสำนักงานป.ป.ช. สำนักงานป.ป.ช. สงวนสิทธิ์ที่จะเป็นผู้ตีความและวินิจฉัย ข้อขัดแย้ง คำวินิจฉัยนี้ให้ถือเป็นอันเด็ดขาดและถึงที่สุด

ส่วนที่ ๑๑ ลิขสิทธิ์ซอฟต์แวร์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใดๆ ว่ามีการละเมิดลิขสิทธิ์ หรือสิทธิบัตรเกี่ยวกับคอมพิวเตอร์ และหรือซอฟต์แวร์ที่เสนอ ผู้ขายต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้าง หรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว ผู้ขายต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่างๆ ที่เกิดขึ้นทั้งหมด

ส่วนที่ ๑๒ การรักษาข้อมูล

ผู้เสนอราคาต้องเก็บรักษาข้อมูลของสำนักงาน ป.ป.ช. และข้อมูลส่วนบุคคลไว้เป็นความลับ และไม่เปิดเผยให้บุคคลภายนอกทราบ ทั้งนี้ หากฝ่าฝืนผู้เสนอราคาจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นและตามที่กฎหมายกำหนดและต้องลงนาม “สัญญาที่จะไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑๓ หลักเกณฑ์และสิทธิในการพิจารณา

๑๓.๑ หลักเกณฑ์และสิทธิในการพิจารณา

ในการพิจารณาเพื่อคัดเลือกผู้ขายเป็นไปตามข้อกำหนดต่อไปนี้

๑๓.๑.๑ หากผู้เสนอราคารายใดมีคุณสมบัติไม่ถูกต้องตามข้อกำหนด หรือยื่นหลักฐานการเสนอราคาไม่ถูกต้อง หรือไม่ครบถ้วนตามข้อกำหนดแล้ว คณะกรรมการประกวดราคาจะไม่รับพิจารณาข้อเสนอของผู้เสนอราคารายนั้น เว้นแต่เป็นข้อผิดพลาดหรือผิดหลงเพียงเล็กน้อยหรือผิดพลาดมาจากเงื่อนไขของเอกสารประกวดราคาซื้อในส่วนที่มิใช่สาระสำคัญ ทั้งนี้ เฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อสำนักงาน ป.ป.ช. เท่านั้น

๑๓.๑.๒ สำนักงาน ป.ป.ช. สงวนสิทธิ์ไม่พิจารณาราคาของผู้เสนอราคา โดยไม่มีการผ่อนผันในกรณีเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาซื้อที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้เสนอราคารายอื่น

๑๓.๑.๓ สำนักงาน ป.ป.ช. ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุดหรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกซื้อในจำนวน หรือขนาดหรือเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการประกวดราคาซื้อ โดยไม่พิจารณาจัดซื้อเลยก็ได้ สุดแต่จะพิจารณา และให้ถือว่าการตัดสินของสำนักงาน ป.ป.ช. เป็นเด็ดขาด ผู้เสนอราคาจะเรียกร้องค่าเสียหายใดๆ มิได้ รวมทั้งสำนักงาน ป.ป.ช.

/จะพิจารณา...

จะพิจารณายกเลิกการประกวดราคาซื้อ และลงโทษผู้เสนอราคาเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้เสนอราคาที่ได้รับคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่ เชื่อได้ว่าการเสนอราคากระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือ นิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

๑๓.๑.๔ ในกรณีที่ปรากฏข้อเท็จจริงภายหลังจากการประกวดราคาว่า ผู้เสนอราคาที่มีสิทธิได้รับการคัดเลือกเป็นผู้เสนอราคาที่มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่น หรือเป็นผู้เสนอราคาที่กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม สำนักงาน ป.ป.ช. มีอำนาจที่จะตัดรายชื่อผู้เสนอราคาที่มีสิทธิได้รับการคัดเลือกดังกล่าว และสำนักงาน ป.ป.ช. จะพิจารณาลงโทษผู้เสนอราคารายนั้นเป็นผู้ทิ้งงาน

๑๓.๑.๕ เงื่อนไขในการทำสัญญาจัดซื้อจัดจ้าง สำนักงาน ป.ป.ช. จะทำสัญญาจัดซื้อตามเงื่อนไขที่กำหนดพร้อมการรับประกันและบำรุงรักษาระบบและอุปกรณ์เป็นระยะเวลา ๑ ปีจากผู้เสนอราคาเท่านั้น นอกจากนี้สำนักงาน ป.ป.ช. ทรงไว้ซึ่งสิทธิที่จะทำหรือไม่ทำสัญญาในการรับประกันและบำรุงรักษาระบบและอุปกรณ์ในปีต่อไป ภายหลังจากที่หมดสัญญาการรับประกันและบำรุงรักษาระบบและอุปกรณ์กับผู้ขาย

๑๓.๑.๖ ในการพิจารณาผลการยื่นข้อเสนอการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ จะพิจารณาตัดสินโดยใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) เป็นไปตามหลักเกณฑ์การให้คะแนนทางเทคนิค (รายละเอียดตามเอกสารผนวก ๒ ที่แนบท้าย)

ส่วนที่ ๑๔ วงเงินในการจัดหา (เงินงบประมาณ)

วงเงินในการจัดหา (เงินงบประมาณ) เป็นเงิน ๑๙,๘๕๑,๘๐๐.๐๐ บาท (สิบเก้าล้านแปดแสนห้าหมื่นหนึ่งพันแปดร้อยบาทถ้วน)

ส่วนที่ ๑๕ หน่วยงานที่รับผิดชอบสถานที่ติดต่อ

สำนักเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช.

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผยตัวได้ที่

- ทางไปรษณีย์

  ส่งถึง เลขาธิการคณะกรรมการ ป.ป.ช.
  สำนักงาน ป.ป.ช. เลขที่ ๓๖๑ ถนนนนทบุรี ต.ท่าทราย อ.เมืองนนทบุรี
  จ.นนทบุรี ๑๑๐๐๐
- โทรศัพท์ ๐-๒๕๒๘-๔๘๐๐ ต่อ ๔๙๒๐, ๔๙๙๐ (กลุ่มจัดซื้อจัดจ้าง สำนักบริหารทรัพย์สิน สำนักงาน ป.ป.ช.)
- อีเมล์ egp23_nac@nacc.go.th (กลุ่มจัดซื้อจัดจ้าง สำนักบริหารทรัพย์สิน สำนักงาน ป.ป.ช.)

****

ภาคผนวก ๑
รายการอุปกรณ์

ลำดับที่	อุปกรณ์	ยี่ห้อ	จำนวน (ระบบ/ชุด)
๑	Firewall	PALO	๑
๒	Web Application Firewall	F5	๑
๓	SSL VPN	Juniper	๑
๔	SSL VPN	PALO	๑
๕	Email Server	Kolab	๑
๖	Mail Gateway	ProofPoint	๑
๗	Campus Firewall	Huawei	๑
๘	Branch Firewall	Huawei	๑
๙	Active Directory	Window Server	๑
๑๐	LDAP	LDAP	๑
๑๑	DNS Server	Window Server	๑
๑๒	DHCP Server	Window Server	๑
๑๓	Antivirus	Trendmicro	๑
๑๔	EDR	Trendmicro	๑
๑๕	Web Gateway	PACO	๑
๑๖	Web Gateway	Cisco	๑
๑๗	Server	Window Server	๓๒
๑๘	Server	Linux	๘๙
๑๙	Branch Network Device	Cisco	๓๑
๒๐	Branch Network Device	Huawei	๔๔
๒๑	Campus Network Device	Huawei	๑
๒๒	Video Conference Device	Huawei & Cisco	๑

<u>หมายเหตุ</u> รายการอาจมีการเปลี่ยนแปลง ตามที่สำนักงาน ป.ป.ช. ใช้งานในปัจจุบัน

หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ
โครงการจัดหาระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์
(Threat Detection and Incident Response Platform)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

<u>หลักเกณฑ์และสิทธิในการพิจารณา</u>

๑. ในการเสนอราคาครั้งนี้ สำนักงาน ป.ป.ช. จะพิจารณาตัดสินโดยใช้เกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (เกณฑ์ราคาประกอบเกณฑ์อื่น)

๒. สำนักงาน ป.ป.ช. จะพิจารณาให้คะแนนการประเมินค่าประสิทธิภาพต่อราคา (Price Perfermance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด คือ

- ราคาที่เสนอราคา (ตัวแปรหลัก) กำหนดน้ำหนักเท่ากับร้อยละ ๓๐
- ข้อเสนอด้านเทคนิคหรือข้อเสนออื่นๆ กำหนดน้ำหนักเท่ากับร้อยละ ๗๐

๓. เกณฑ์การพิจารณาข้อเสนอด้านเทคนิคหรือข้อเสนออื่นๆ (คะแนนเต็ม ๑๐๐ คะแนน)

สำนักงาน ป.ป.ช. จะพิจารณาข้อเสนอด้านเทคนิคหรือข้อเสนออื่นๆ ของผู้เสนอราคาเฉพาะที่มีคุณสมบัติและหลักฐานเอกสารถูกต้อง โดยมีเกณฑ์การพิจารณา ดังนี้

๓.๑ การพิจารณาด้านระยะเวลาการประกันอายุการใช้งาน คะแนนเต็ม ๔๐ คะแนน

๓.๒ การพิจารณาจากคุณสมบัติเพิ่มเติม คะแนนเต็ม ๖๐ คะแนน

๓.๑ <u>การพิจารณาด้านระยะเวลาการประกันอายุการใช้งาน (คะแนนเต็ม ๔๐ คะแนน)</u>

ประเด็นการให้คะแนน	คะแนนที่ได้			หมายเหตุ
	๑ ปี	๒ ปี	๓ ปี	
เสนอการรับประกันระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ (Threat Detection and Incident Response Platform)	๕	๒๐	๔๐	คะแนนเต็มไม่เกิน ๔๐ คะแนน

/๓.๒ <u>การพิจารณา</u>...

๓.๒ <u>การพิจารณาจากคุณสมบัติเพิ่มเติม (คะแนนเต็ม ๖๐ คะแนน)</u>

ประเด็นการให้คะแนน	คะแนนที่ได้		หมายเหตุ
	ไม่เสนอ	เสนอ	
๓.๒.๑ เสนอทีมผู้เชี่ยวชาญ จากเจ้าของผลิตภัณฑ์ (Vendor/Global MDR) หรือศูนย์บริการที่เป็นตัวแทนที่ได้รับแต่งตั้งในประเทศไทย (Local MDR) จากเจ้าของผลิตภัณฑ์ เพื่อช่วยในการบริหารจัดการระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ (Threat Detection and Incident Response Platform) รวมถึงทำหน้าที่เฝ้าระวัง ตรวจสอบความปลอดภัย และรับมือภัยคุกคามที่เกิดขึ้นกับเครื่องแม่ข่าย และลูกข่ายของสำนักงาน ป.ป.ช. แบบ ๒๔ x ๗	๐ คะแนน	๓๐ คะแนน	คะแนนเต็ม ไม่เกิน ๓๐ คะแนน
๓.๒.๒ เสนอความสามารถของระบบวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Information and Event Management : SIEM)) เพิ่มเติมจากขอบเขตของงานฯ ดังนี้ ๑) สามารถวิเคราะห์และเรียนรู้จากพฤติกรรมภายในระบบ เพื่อระบุเหตุการณ์ที่น่าสงสัยซึ่งเบี่ยงเบนไปจากพฤติกรรมปกติ (Baseline) ได้โดยอัตโนมัติ ๒) มีเทคโนโลยี AI/ML การให้ scoring ของแต่ละ Incident โดยอัตโนมัติ เพื่อจัดลำดับความเร่งด่วนในการจัดการกับ Incident	๐ คะแนน	๑๐ คะแนน	คะแนนเต็ม ไม่เกิน ๑๐ คะแนน

/<u>ประเด็น</u>...

ประเด็นการให้คะแนน	คะแนนที่ได้		หมายเหตุ
	ไม่เสนอ	เสนอ	
๓.๒.๓ เสนอความสามารถของระบบตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response – XDR) เพิ่มเติมจากขอบเขตของงานฯ ดังนี้ ๑) สามารถนำเข้าข้อมูล endpoint telemetry เพื่อใช้ในการวิเคราะห์ได้ไม่จำกัด ๒) สามารถทำงานร่วมกับอุปกรณ์ Next Generation Firewall ของสำนักงาน ป.ป.ช. ใช้งานอยู่ได้ (Palo Alto: PA-5250) ในการตรวจจับ ค้นหา แจ้งเตือน และรายงานอันตรายจากภัยคุกคามขั้นสูงในระบบเครือข่ายให้กับผู้ดูแลระบบ และส่งข้อมูลเข้าสู่ระบบ เพื่อทำการวิเคราะห์ด้วยระบบ AI ในการตรวจจับการโจมตีแบบอัตโนมัติ (Automate Attack Detection with AI) เพื่อช่วยในการบริหารจัดการป้องกันภัยคุกคาม โดยใช้เทคโนโลยี Machine learning เรียนรู้พฤติกรรม ผู้ใช้งานในองค์กร โดยมีความสามารถ User behavior analytics (UBA) or User and Entity behavior analytics (UEBA)	๐ คะแนน	๑๐ คะแนน	คะแนนเต็ม ไม่เกิน ๑๐ คะแนน

/ประเด็น...

ประเด็นการให้คะแนน	คะแนนที่ได้		หมายเหตุ
	ไม่เสนอ	เสนอ	
๓.๒.๒ เสนอความสามารถของระบบบริหารจัดการภัยและตอบสนองต่อภัยคุกคามแบบอัติโนมัติ (Security Orchestration, Automation and Response - SOAR) เพิ่มเติมจากขอบเขตของงานฯ ดังนี้ ๑) การหยุดหรือดำเนินการต่อเมื่อเกิดข้อผิดพลาดใน Playbook	๐ คะแนน	๑๐ คะแนน	คะแนนเต็ม ไม่เกิน ๑๐ คะแนน

***หมายเหตุ** ข้อเสนอที่เสนอมาเพื่อพิจารณาเป็นคะแนน จะนำไปเป็นส่วนหนึ่งของสัญญาที่จะบังคับใช้กับที่เสนอ

ปัญหาข้อขัดแย้งหรือการตีความ

ในกรณีที่มีความจำเป็นต้องตีความข้อใด หรือมีข้อความใดที่ขัดแย้งในประกาศเสนอราคา หรือเอกสารเสนอราคา หรือในเอกสารอื่นใดก็ตาม ซึ่งมีความจำเป็นต้องวินิจฉัยตัดสินเพื่อให้การเสนอราคาครั้งนี้เป็นไปด้วยความเรียบร้อยบรรลุวัตถุประสงค์ของสำนักงาน ป.ป.ช. สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะเป็นผู้ตีความและวินิจฉัยข้อขัดแย้ง คำวินิจฉัยนี้ให้ถือเป็นอันเด็ดขาดและถึงที่สุด

สัญญาที่จะไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สัญญาฉบับนี้ทำขึ้น ณ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เลขที่ ๓๖๑ ถนนนนทบุรี ตำบลท่าทราย อำเภอเมืองนนทบุรี จังหวัดนนทบุรี เมื่อวันที่..... ระหว่าง "สำนักงาน ป.ป.ช." โดย.....ซึ่งต่อไปนี้ เรียกว่า **"ผู้ให้ข้อมูล"** ฝ่ายหนึ่ง กับ ..... ซึ่งต่อไปนี้ เรียกว่า **"ผู้รับข้อมูล"** อีกฝ่ายหนึ่ง ทั้งสองฝ่ายได้ตกลงกัน โดยมีความตกลงดังต่อไปนี้

ข้อ ๑ คำนิยาม

"ข้อมูล" หมายความถึง บรรดาข้อความ เอกสาร ข้อมูล ตลอดจนรายละเอียดทั้งปวงที่เป็นของผู้ให้ข้อมูล ทั้งที่อยู่ในความควบคุมหรือครอบครองแม้จะไม่เป็นที่รับรู้ของสาธารณชนโดยทั่วไป และไม่ว่าจะอยู่ในรูปแบบหรือสื่อแบบใด ไม่ว่าจะถูกทำซ้ำ แก้ไข ดัดแปลง โดยผู้รับข้อมูลหรือไม่

"ข้อมูลส่วนบุคคล" หมายความถึง ข้อมูลเกี่ยวกับบุคคล ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อ ๒ วัตถุประสงค์

ผู้รับข้อมูลและผู้ให้ข้อมูลตกลงที่จะให้มีการรักษาข้อมูลเป็นความลับตามสัญญาฉบับนี้ ภายใต้โครงการหรือกิจกรรมหรือสัญญาจ้างหรือบันทึกข้อตกลง ที่..... เรื่อง..... ..... ลงวันที่..... ระหว่างสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ กับ..... เพื่อให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งต่อไปนี้ในสัญญาฉบับนี้ เรียกว่า "กิจกรรมตามสัญญา"

ข้อ ๓ การรักษาข้อมูลเป็นความลับ

๓.๑ ผู้รับข้อมูลตกลงว่าจะรักษาข้อมูลและเก็บข้อมูลไว้เป็นความลับโดยครบถ้วนและเคร่งครัด ผู้รับข้อมูลจะต้องไม่เปิดเผยข้อมูลหรือทำการอื่นใดในทำนองเดียวกันไม่ว่าทั้งหมดหรือบางส่วนตลอดระยะเวลาตามกิจกรรมตามสัญญาและตลอดไป

๓.๒ ผู้รับข้อมูลตกลงจะไม่เปิดเผยข้อมูลไม่ว่าทั้งหมดหรือแต่บางส่วนต่อบุคคลอื่นหรือองค์กรใดทราบโดยมิได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูล เว้นแต่กรณีจำต้องเปิดเผยตามกฎหมาย คำสั่งศาลหรือเจ้าพนักงานของรัฐ หรือหน่วยงานที่มีอำนาจกำกับดูแลที่อาศัยอำนาจตามกฎหมาย

/๓.๓ ผู้รับ...

๓.๓ ผู้รับข้อมูลตกลงที่จะควบคุมมิให้พนักงาน ลูกจ้าง ผู้รับจ้าง หรือตัวแทนของตนล่วงรู้หรือสามารถเข้าถึงข้อมูลนั้น เว้นแต่บุคคลเหล่านั้น ได้รับมอบหมายหรือมีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูล และตกลงที่จะควบคุมบุคคลเหล่านั้น มิให้เปิดเผยข้อมูลไม่ว่าด้วยวิธีการใด ๆ และไม่ว่าทั้งทางตรงและทางอ้อมแก่บุคคลอื่นใด

๓.๔ ผู้รับข้อมูลตกลงใช้มาตรการที่เหมาะสมในการเก็บรักษาข้อมูลเพื่อป้องกันมิให้ข้อมูลถูกนำไปใช้โดยมิได้รับอนุญาตหรือถูกเปิดเผยแก่บุคคลใด โดยผู้รับข้อมูลต้องใช้มาตรการการเก็บรักษาข้อมูลในระดับเดียวกันกับที่ผู้รับข้อมูลใช้กับข้อมูลของตน และต้องไม่น้อยกว่าระดับที่วิญญูชนที่ประกอบวิชาชีพเช่นนั้นพึงรักษาข้อมูลของตน โดยเฉพาะข้อมูลส่วนบุคคลที่ต้องดำเนินการเก็บรักษาข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๓.๕ ผู้รับข้อมูลตกลงที่จะปฏิบัติตามประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ ตลอดจนกฎหมาย ระเบียบ หลักเกณฑ์ วิธีการ หรือเงื่อนไขเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศซึ่งใช้บังคับทั้งที่ใช้บังคับอยู่ ณ วันทำสัญญา รวมถึงที่ได้มีการแก้ไขในอนาคต

๓.๖ ผู้รับข้อมูลตกลงที่จะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม ทั้งในเชิงองค์กรและเชิงเทคนิค ตามประกาศที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดและเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยคำนึงถึงลักษณะขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดในสัญญาฉบับนี้

๓.๗ ผู้รับข้อมูลตกลงที่จะดำเนินการตามข้อ ๓ แห่งสัญญาฉบับนี้ ตลอดระยะเวลาตามกิจกรรม ตามสัญญา และตลอดไป

ข้อ ๔ การเปิดเผยข้อมูล

ผู้ให้ข้อมูลและผู้รับข้อมูล ตกลงให้เปิดเผยข้อมูลที่ผู้รับข้อมูลได้รับจากผู้ให้ข้อมูลตามสัญญาฉบับนี้ในกรณีดังต่อไปนี้

๔.๑ ข้อมูลที่อยู่ในการรับรู้ การครอบครอง หรือการควบคุม ไม่ว่าด้วยวิธีใดของผู้รับข้อมูลที่ได้รับข้อมูลเหล่านั้นมาโดยชอบด้วยกฎหมาย ก่อนที่จะได้รับข้อมูลนั้นจากผู้ให้ข้อมูล

๔.๒ ข้อมูลที่เป็นที่รับรู้กันโดยทั่วไปหรือที่เป็นการรู้กันอย่างแพร่หลายในเวลาที่ได้รับข้อมูลนั้น ซึ่งไม่ได้เป็นผลมาจากการละเมิดหรือผิดเงื่อนไข ข้อกำหนดตามกิจกรรมตามสัญญาโดยผู้รับข้อมูล

๔.๓ ข้อมูลที่ผู้รับข้อมูลได้รับรู้มาจากบุคคลอื่นที่มีสิทธิให้ข้อมูลและไม่มีหน้าที่ต้องปกปิดข้อมูลตามสัญญาฉบับนี้

๔.๔ ข้อมูลที่เป็นข้อมูลสาธารณะอันประชาชนทั่วไปเข้าถึงข้อมูลได้

/๔.๕ ข้อมูล...

๔.๕ ข้อมูลที่ต้องเปิดเผยตามกฎหมาย ตามคำสั่งศาลหรือเจ้าพนักงานของรัฐ หรือหน่วยงานที่มีอำนาจกำกับดูแลที่อาศัยอำนาจตามกฎหมาย โดยผู้รับข้อมูลต้องมีหนังสือแจ้งให้ ผู้ให้ข้อมูลได้ทราบถึงข้อกฎหมายตามกฎหมาย หรือคำสั่งดังกล่าว พร้อมทั้งหมายศาลหรือคำสั่งของเจ้าพนักงานของรัฐอื่นใดก่อนดำเนินการเปิดเผยข้อมูลดังกล่าว

๔.๖ ข้อมูลที่เปิดเผยโดยได้รับความเห็นชอบเป็นหนังสือจากผู้ให้ข้อมูลเป็นลายลักษณ์อักษรก่อนที่ผู้รับข้อมูลจะเปิดเผยข้อมูลนั้น

ข้อ ๕ ข้อกำหนดและการใช้ข้อมูล

๕.๑ ผู้รับข้อมูลตกลงใช้ข้อมูลและข้อมูลส่วนบุคคล เฉพาะแต่การใดเพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้ในสัญญาเท่านั้น

๕.๒ ผู้รับข้อมูลตกลงจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่ประมวลผลในขอบเขตของกิจกรรมตามสัญญาและตกลงส่งมอบบันทึกรายการดังกล่าวให้แก่ผู้ให้ข้อมูลก่อนการประมวลผลข้อมูล หรือเมื่อมีการเปลี่ยนแปลงในกระบวนการประมวลผลข้อมูลทันทีที่ผู้ให้ข้อมูลร้องขอ

๕.๓ ผู้รับข้อมูลตกลงที่จะดำเนินการเพื่อช่วยเหลือผู้ให้ข้อมูลในการดำเนินการตามคำร้องขอที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อผู้ให้ข้อมูลที่เป็นการใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตของกิจกรรมตามสัญญา

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลต่อผู้รับข้อมูลโดยตรงนั้น ผู้รับข้อมูลตกลงจะดำเนินการแจ้งและส่งคำร้องขอดังกล่าวให้ผู้ให้ข้อมูลทันที โดยผู้รับข้อมูลจะตกลงที่จะไม่ดำเนินการตามคำร้องขอดังกล่าว เว้นแต่จะได้รับมอบหมายจากผู้ให้ข้อมูลเป็นลายลักษณ์อักษรให้ดำเนินการแทนผู้ให้ข้อมูล

ข้อ ๖ การทำซ้ำหรือดัดแปลง และทำให้เสียรูปซึ่งข้อมูล

๖.๑ ผู้รับข้อมูลตกลงที่จะไม่ทำซ้ำหรือดัดแปลงข้อมูลและข้อมูลส่วนบุคคลและตกลงที่จะควบคุมมิให้พนักงาน ลูกจ้าง ผู้รับจ้าง หรือตัวแทนของตนกระทำการดังกล่าวเช่นเดียวกัน

๖.๒ ผู้รับข้อมูลจะทำซ้ำหรือดัดแปลงข้อมูลและข้อมูลส่วนบุคคลมิได้ เว้นแต่ เป็นการทำซ้ำหรือดัดแปลงเพื่อใช้ตามวัตถุประสงค์ที่กำหนดไว้ในสัญญาฉบับนี้ และกิจกรรมตามสัญญา

๖.๓ ผู้รับข้อมูลตกลงจะไม่กระทำการวิศวกรรมย้อนกลับ ถอดรหัส หรือกระทำการอื่นใดที่ให้เกิดผลในลักษณะเดียวกันต่อข้อมูล รวมทั้งไม่เคลื่อนย้าย พิมพ์ทับ หรือทำให้เสียรูปซึ่งสัญลักษณ์ที่แสดงเครื่องหมายสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า ตราสัญลักษณ์และเครื่องหมายอื่นใดที่แสดงความเป็นกรรมสิทธิ์ของต้นฉบับหรือสำเนาของข้อมูลที่ได้รับจากผู้ให้ข้อมูล

/ข้อ ๗...

ข้อ ๗ ทรัพย์สินทางปัญญา

ผู้ให้ข้อมูลและผู้รับข้อมูลตกลงกันว่าสัญญาฉบับนี้ ไม่มีผลเป็นการโอนสิทธิหรือการอนุญาตให้ใช้สิทธิ ไม่ว่าโดยตรงหรือโดยอ้อม ให้แก่ผู้รับข้อมูลที่ได้รับข้อมูล ซึ่งสิทธิบัตร ลิขสิทธิ์ การออกแบบ เครื่องหมายการค้า ตราสัญลักษณ์ รูปประดิษฐ์อื่นใด ชื่อทางการค้า ความลับทางการค้า หรือสิทธิอื่นใดภายใต้กฎหมายว่าด้วยทรัพย์สินทางปัญญา ไม่ว่าจดทะเบียนไว้ตามกฎหมายหรือไม่ก็ตาม หรือสิทธิอื่นใดของผู้ให้ข้อมูลซึ่งปรากฏอยู่หรือนำมาทำซ้ำไว้ในข้อมูล

ทั้งนี้ ผู้รับข้อมูลรวมถึงบุคคลที่เกี่ยวข้องกับข้อมูลตกลงจะไม่ยื่นขอรับสิทธิหรือขอจดทะเบียนใด ๆ ตามกฎหมายว่าด้วยทรัพย์สินทางปัญญา ตลอดจนไม่นำไปใช้ โดยไม่ได้รับการอนุญาตเป็นหนังสือจากผู้ให้ข้อมูลเกี่ยวกับรายละเอียดข้อมูลหรือส่วนหนึ่งส่วนใด

ข้อ ๘ เหตุละเมิดต่อข้อมูลและข้อมูลส่วนบุคคล

๘.๑ กรณีที่มีเหตุอันถือว่าเป็นความเสี่ยงที่จะก่อให้เกิดเหตุละเมิด หรือรับทราบข้อเท็จจริงอันเป็นพฤติการณ์ใด ๆ แก่ข้อมูลและข้อมูลส่วนบุคคลของผู้ให้ข้อมูลที่กระทำต่อการรักษาความมั่นคงปลอดภัยของข้อมูลนั้น ทั้งในส่วนของการประมวลผลภายใต้กิจกรรมตามสัญญา ซึ่งจะก่อให้เกิดความเสียหาย ลบ ทำลาย สูญหาย แก้ไข เปลี่ยนแปลง เข้าถึง ใช้ เปิดเผย หรือด้วยวิธีการใด ๆ อันเป็นการมิชอบด้วยกฎหมายนั้น ผู้รับข้อมูลตกลงที่จะแจ้งผู้ให้ข้อมูลทราบทันที

๘.๒ กรณีที่พบว่ามีเหตุละเมิดต่อข้อมูลและข้อมูลส่วนบุคคล ภายใต้กิจกรรมตามสัญญานั้น ผู้รับข้อมูลตกลงที่จะใช้มาตรการตามที่เหมาะสมในการระบุสาเหตุของการละเมิดและป้องกันเหตุละเมิดดังกล่าวมิให้เกิดซ้ำ รวมทั้งต้องแจ้งรายละเอียดตามขอบเขตที่กฎหมายกำหนด ภายใน ๔๘ ชั่วโมงนับแต่เกิดเหตุละเมิดต่อผู้ให้ข้อมูลอันประกอบไปด้วยรายละเอียดของเหตุละเมิด รวมถึงประเภทของข้อมูลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิดและผลกระทบที่ได้รับ ตลอดจนมาตรการตอบสนองอื่น ๆ เพื่อบรรเทาผลกระทบความเสียหายทั้งในส่วนข้อมูลที่ถูกละเมิดและข้อมูลอื่น ๆ ที่เกี่ยวข้อง

๘.๓ ผู้รับข้อมูลตกลงให้ผู้ให้ข้อมูลใช้สิทธิทางศาลเพื่อขอให้ศาลมีคำสั่งใด ๆ ให้ผู้รับข้อมูลยับยั้งการกระทำการใด ๆ หรือกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามสัญญาฉบับนี้ไม่ว่าข้อใดข้อหนึ่ง

ข้อ ๙ การชดใช้ค่าเสียหาย

๙.๑ กรณีที่ผู้รับข้อมูล พนักงาน ลูกจ้าง ผู้รับจ้างหรือตัวแทนของตนฝ่าฝืนหรือไม่ปฏิบัติตามสัญญาฉบับนี้ไม่ว่าข้อใดข้อหนึ่งนั้น ผู้รับข้อมูลตกลงจะชดใช้ค่าเสียหาย โดยสิ้นเชิงให้แก่ผู้ให้ข้อมูลและ/หรือบุคคลที่มีสิทธิในการใช้ข้อมูลของผู้ให้ข้อมูลที่ได้รับความเสียหาย โดยต้องชดใช้ค่าเสียหายภายใน ๓๐ (สามสิบ) วัน นับแต่วันที่ได้รับแจ้งเป็นหนังสือจากผู้ให้ข้อมูล

๙.๒ กรณีที่ผู้ให้ข้อมูลใช้สิทธิทางศาลอันเนื่องมาจากการกระทำที่ผู้รับข้อมูลฝ่าฝืนหรือไม่ปฏิบัติตามสัญญาฉบับนี้ไม่ว่าข้อใดข้อหนึ่งหรือผู้ให้ข้อมูลได้รับความเสียหายจากการกระทำเช่นว่านั้น ผู้รับข้อมูลตกลงเป็นผู้รับผิดชอบค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้นในการดำเนินการดังกล่าว

/ข้อ ๑๐...

ข้อ ๑๐ การส่งคืน ลบ หรือการทำลายข้อมูล

๑๐.๑ เมื่อกิจกรรมตามสัญญาได้เสร็จสิ้นลงตามวัตถุประสงค์ผู้รับข้อมูลตกลงส่งมอบข้อมูลตลอดจนสำเนาของข้อมูลที่ได้ทำซ้ำขึ้นไม่ว่าในรูปแบบใดที่ผู้รับข้อมูลได้รับและจัดทำขึ้นคืนให้แก่ผู้ให้ข้อมูลภายในระยะเวลาที่ผู้ให้ข้อมูลแจ้งเป็นหนังสือแก่ผู้รับข้อมูล

๑๐.๒ ผู้รับข้อมูลตกลงจะลบหรือทำลายข้อมูลและข้อมูลส่วนบุคคล ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ หรืออุปกรณ์อื่นใดที่ใช้จัดเก็บข้อมูล ตลอดจนที่ทำซ้ำไว้และจัดเก็บด้วยวิธีการอื่นใด (ถ้ามี) ตลอดจนดำเนินการอื่นตามที่ได้รับแจ้งเป็นหนังสือจากผู้ให้ข้อมูล รวมถึงต้องไม่กระทำการอื่นใดอันเป็นการใช้ข้อมูลและข้อมูลส่วนบุคคลที่ได้รับจากผู้ให้ข้อมูลทันที

ข้อ ๑๑ การบังคับใช้

๑๑.๑ หากผู้รับข้อมูลกระทำการฝ่าฝืนหรือผิดสัญญาฉบับนี้ข้อหนึ่งข้อใดผู้รับข้อมูลตกลงให้ผู้ให้ข้อมูลดำเนินการเรียกร้องตามข้อสัญญาและดำเนินการตามกฎหมายได้ทันที

๑๑.๒ กรณีที่ปรากฏในภายหลังว่าส่วนหนึ่งส่วนใดของสัญญาฉบับนี้เป็นโมฆะให้ถือว่าข้อกำหนดส่วนที่เป็นโมฆะไม่มีผลบังคับในสัญญานี้ และข้อกำหนดอื่นที่เหลืออยู่ในสัญญาฉบับนี้ ยังคงใช้บังคับได้และมีผลอยู่อย่างสมบูรณ์

ทั้งนี้ สัญญาฉบับนี้ อยู่ภายใต้การบังคับใช้และตีความตามกฎหมายไทย

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว จึงได้ลงลายมือชื่อพร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญาต่างยึดถือไว้ฝ่ายละหนึ่งฉบับ

(ลงชื่อ)..... ผู้ให้ข้อมูล (ลงชื่อ)..... ผู้รับข้อมูล

(.....) (.....)

(ลงชื่อ)..... พยาน (ลงชื่อ)..... พยาน

(.....) (.....)