ร่างขอบเขตของงาน

โครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์

(Cyber Security Managed Services)

1. ความเป็นมา

ด้วยปัจจุบันมีภัยคุกคามทางไซเบอร์ต่าง ๆ ที่เกิดขึ้นมากมาย และเกิดขึ้นใหม่อย่างหลากหลายรูปแบบ ซึ่ง สำนักงานการบินพลเรือนแห่งประเทศไทย (กพท.) มีระบบต่าง ๆ ที่ให้บริการประชาชนและเจ้าหน้าที่ของ กพท. ในการปฏิบัติงาน ดังนั้น กพท. จึงดำเนินโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เพื่อช่วยให้รับรู้ถึงสถานการณ์ภัยคุกคามทางไซเบอร์ต่าง ๆ และระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็ว แม่นยำ และเพื่อให้ กพท. มีความพร้อมในการรับมือและสามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้ทันท่วงที

2. วัตถุประสงค์

เพื่อให้ กพท. มีระบบสำหรับเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามหรือเหตุการณ์ผิดปกติอันอาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและข้อมูลของ กพท.

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1. มีความสามารถตามกฎหมาย

3.2. ไม่เป็นบุคคลล้มละลาย

3.3. ไม่อยู่ระหว่างเลิกกิจการ

3.4. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษาเป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.7. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)

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

3.11. ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริการพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) 0405.2/ว 124 ลงวันที่ 1 มีนาคม 2566 ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ โดยต้องมีทุนจดทะเบียนไม่ต่ำกว่า 2,000,000 บาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มูลค่าดังกล่าวอีกครั้งในวันลงนามในสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการ หรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการ หรือรายการที่ยื่นเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตในประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

(5) กรณีตามข้อ (1) – (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(5.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.12. ผู้ยื่นข้อเสนอต้องมีผลงานด้านการให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center) หรือผลงานที่มีลักษณะเกี่ยวข้องทางด้านความมั่นคงปลอดภัยทางเครือข่าย (Network Security) หรือความมั่นคงปลอดภัยทาง

(นายวีระ ระบายศรี) (นางสาวอรวรรณ ใจเอื้อ) (นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี) (นางสาวนวรา ประไพศิลป์)

ไซเบอร์ (Cyber Security) ในวงเงินไม่น้อยกว่า 3,000,000 บาท (สามล้านบาทถ้วน) และเป็นผลงานที่แล้วเสร็จไม่เกินกว่า 5 ปี นับถึงวันที่ยื่นเสนอราคา โดยสัญญาต้องมีอายุสัญญาไม่น้อยกว่า 1 ปี และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ กพท. เชื่อถือ

หากเป็นผลงานกับหน่วยงานของรัฐ จะต้องแนบหนังสือรับรองผลงาน และสำเนาสัญญาจ้าง พร้อมรับรองสำเนาถูกต้องมาพร้อมกันในวันยื่นข้อเสนอ

หากเป็นผลงานกับหน่วยงานของเอกชน จะต้องแนบหนังสือรับรองผลงาน และสำเนาสัญญาจ้าง และใบกำกับภาษี พร้อมรับรองสำเนาถูกต้องมาพร้อมกันในวันยื่นข้อเสนอ

3.13. ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(นายวีระ ระบายศรี) (นางสาวอรวรรณ ใจเอื้อ) (นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี) (นางสาวนวรา ประไพศิลป์)

4. ขอบเขตของงาน

ผู้รับจ้างต้องมีบริการศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ เพื่อให้ กพท. ได้รับแจ้งเตือนภัยคุกคามทางไซเบอร์ วิธีการตรวจสอบและแก้ไขอย่างถูกต้อง มีประสิทธิภาพ โดยมีขอบเขตการดำเนินงานและคุณลักษณะอย่างน้อยดังนี้

4.1 ดำเนินงานด้านบริการตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์ โดยใช้ช่องทาง SSL VPN ของ กพท. หรือ IPsec Site-to-Site VPN หรือช่องทางที่ กพท. กำหนด ครอบคลุมรายการอุปกรณ์ อย่างน้อยดังต่อไปนี้

- Firewall จำนวน 2 ชุด
- Antivirus จำนวน 1 ระบบ
- Active Directory จำนวน 2 ชุด
- Application Server จำนวนไม่น้อยกว่า 8 ระบบ

กรณีอุปกรณ์ดังกล่าวไม่ส่ง Log มายังอุปกรณ์/ระบบของผู้รับจ้าง ผู้รับจ้างต้องดำเนินการประสานงานร่วมกับเจ้าหน้าที่ กพท. และบริษัทผู้รับจ้างบำรุงรักษาอุปกรณ์ดังกล่าว เพื่อดำเนินการนำเข้า Log ของอุปกรณ์ที่ใช้ในการ Monitor มายังอุปกรณ์/ระบบของผู้รับจ้างให้ครบถ้วน ทั้งนี้ระหว่างสัญญา กพท. สงวนสิทธิ์ในการปรับเปลี่ยน เพิ่ม/ลด ระบบหรืออุปกรณ์ในการเฝ้าระวังภัยคุกคามได้ตามความต้องการ

4.2 ระบบของศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ต้องมีซอฟต์แวร์สำหรับการส่งต่อข้อมูล (Log Forwarder) จากเครื่องคอมพิวเตอร์แม่ข่าย ของ กพท.

4.3 ผู้รับจ้างต้องดำเนินการสำรองข้อมูล Log ไว้อย่างน้อย 90 วัน และต้องส่งมอบข้อมูล Log ดังกล่าวทั้งหมดให้ กพท. ในแต่ละงวดงาน

4.4 ผู้รับจ้างต้องสามารถวิเคราะห์เหตุการณ์ผิดปกติที่เกิดจากภัยคุกคามด้านเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ในเรื่องที่เกี่ยวข้องกับความผิดปกติของภัยคุกคามด้านความปลอดภัยสารสนเทศ (Security Monitoring) ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ พร้อมให้คำปรึกษาและร่วมกับ กพท. ในการแก้ไขอุปกรณ์ที่เกี่ยวข้องเพื่อหาแนวทางการป้องกันไม่ให้เกิดเหตุการณ์ขึ้นอีก

4.5 ผู้รับจ้างต้องทำการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ ผ่านทางโทรศัพท์, ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือระบบการสื่อสารอื่น ๆ ที่ กพท. กำหนด ตาม Service Level Agreement (SLA) และระดับความรุนแรงที่ กพท. กำหนดดังต่อไปนี้

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)

ระดับความรุนแรง	ผลกระทบและการดำเนินการ	เวลาในการแจ้งเตือนแก่ กพท.	ให้คำแนะนำในการแก้ไข
สูงมาก (Very High)	**ผลกระทบ:** การดำเนินกิจกรรมหลักของ กพท. หยุดชะงัก และจำเป็นต้องแก้ไขอย่างเร่งด่วนที่สุด **การดำเนินการ:** ต้องตรวจสอบและแก้ไขปัญหาโดยเร่งด่วน	ภายใน 30 นาที	ภายใน 1 ชั่วโมง
สูง (High)	**ผลกระทบ:** กิจกรรมหลักของ กพท. ไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ และจำเป็นต้องแก้ไขอย่างเร่งด่วน **การดำเนินการ:** ต้องตรวจสอบเฝ้าระวังและแก้ไขปัญหา	ภายใน 1 ชั่วโมง	ภายใน 2 ชั่วโมง
ปานกลาง (Medium)	**ผลกระทบ:** มีผลกระทบต่อประสิทธิภาพการทำงานทั่วไป และมีผลกระทบต่อการดำเนินธุรกิจโดยบางส่วนเล็กน้อย **การดำเนินการ:** ควรตรวจสอบหรือเฝ้าระวัง	ภายใน 2 ชั่วโมง	ภายใน 3 ชั่วโมง
ต่ำ (Low)	**ผลกระทบ:** มีผลกระทบต่อประสิทธิภาพการทำงานทั่วไปบางส่วน และไม่มีผลกระทบต่อการดำเนินธุรกิจโดยภาพรวม **การดำเนินการ:** ควรเฝ้าระวังและควรเก็บไว้เป็นข้อมูลประกอบการเฝ้าระวัง (Information)	ภายใน 24 ชั่วโมง	ภายใน 24 ชั่วโมง

4.6 การแจ้งเตือนภัยคุกคามทางไซเบอร์ ต้องครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

- ระบุประเภทของภัยคุกคาม
- วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม
- ระบุต้นทาง (Attacker) และปลายทาง (Target)
- ระดับความรุนแรง (Severity)
- คำแนะนำพร้อมขั้นตอนการดำเนินการแก้ไขเชิงเทคนิคและแนวทางในการป้องกันไม่ให้เกิดเหตุการณ์เดิมซ้ำอีก
- รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด

4.7 ดำเนินการตั้งค่าระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ ให้สามารถกำหนดเงื่อนไขรูปแบบการเฝ้าระวังและตรวจจับภัยคุกคาม (Use Case) ตามที่ได้ทำการประเมินและตกลงร่วมกับทาง กพท. ได้ไม่น้อยกว่า 5 Use Cases โดยเครื่องมือต้องรองรับการตรวจจับเหตุการณ์การคุกคามซึ่งครอบคลุมในเรื่องอย่างน้อยดังต่อไปนี้

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)

- Unauthorized Access
- Malicious Code
- Inappropriate Usage
- Malware Attack
- Denial of Service (DOS)
- Identity-Based Attack โดยสามารถตรวจจับ Brute Force Attacks และ Password Spraying ได้เป็นอย่างน้อย
- Supply Chain Attack

4.8 ผู้รับจ้างต้องดำเนินการจัดทำรายงานสรุปผลการเฝ้าระวังภัยคุกคามแบบรายเดือน (Monthly Report) และรายงานข่าวสารที่เกี่ยวกับภัยคุกคามใหม่ที่เกิดขึ้นด้านความปลอดภัยไซเบอร์ที่เกิดขึ้นทั่วโลก ให้แก่ กพท. แบบรายเดือน ภายในวันที่ 10 ของเดือนถัดไป และจัดประชุมประจำเดือน กับ กพท. เพื่อสรุปภาพรวมผลการเฝ้าระวังภัยคุกคามและภัยคุกคามใหม่ที่เกิดขึ้น และให้คำปรึกษาในการรับมือภัยคุกคามที่เกิดขึ้นให้เจ้าหน้าที่ กพท.

4.9 ผู้รับจ้างต้องดำเนินการจัดทำรายงานสรุปผลการดำเนินการเฝ้าระวังภัยคุกคามเหตุการณ์ผิดปกติที่เป็นภัยคุกคามเป็นรายเดือน (Monthly Report) ภายในวันที่ 10 ของเดือนถัดไป โดยมีรายละเอียดดังต่อไปนี้

- รายงานสรุปสำหรับผู้บริหาร (Executive Summary) เพื่ออธิบายผู้บริหารให้เข้าใจสถานะความเสี่ยงและสภาพปัจจุบัน
- รายงานสรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้น โดยมีการวิเคราะห์ภัยคุกคามในเชิงลึก โดยมีเนื้อหาตามรายการอย่างน้อยดังต่อไปนี้
  - Top Attackers Report
  - Top Threat Report
  - รายงานสรุปการแจ้งเตือนเหตุการณ์ที่ตรวจพบ (Incident Report) ประจำเดือน

4.10 ผู้รับจ้างต้องดำเนินการแจ้งข่าวสารที่เกี่ยวข้องกับระบบรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายที่เกิดขึ้นผ่านทางระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)
- ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)
- ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)
- ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)

(นายวีระ ระบายศรี) (นางสาวอรวรรณ ใจเอื้อ) (นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี) (นางสาวนวรา ประไพศิลป์)

- ช่องโหว่ใหม่ (Vulnerability) ของโปรแกรมต่าง ๆ รวมถึง API และ Web Services ที่ผู้รับจ้างเห็นว่าจะก่อให้เกิดผลเสียหายต่อการดำเนินงานของ กพท.

โดยข่าวสารดังกล่าวประกอบด้วยเนื้อหาที่สำคัญอย่างน้อยดังต่อไปนี้

1. คำอธิบายทั่วไป (Overview)
2. คำอธิบายอย่างละเอียด (Description)
3. ผลกระทบ (Impact)
4. ระบบที่ได้รับผลกระทบ (System Affected)
5. ทางแก้ไข (Solution) (ถ้ามี) และ
6. อ้างอิง (Reference)

4.11 ผู้รับจ้างต้องดำเนินการศึกษาและปรับปรุงแนวทางการปฏิบัติการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ กพท. และดำเนินการจัดทำคู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) จำนวนอย่างน้อย 6 รูปแบบ เพื่ออ้างอิงในการปฏิบัติการในการจัดการหรือตอบรับภัยคุกคามต่าง ๆ ได้อย่างถูกต้องให้กับ กพท. นำส่งตามงวดงานอย่างน้อยงวดงานละ 1 รูปแบบ โดยต้องมีเนื้อหาครอบคลุมรายละเอียดอย่างน้อย ดังต่อไปนี้

- โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ
- โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงาน จะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจน ภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้อง
- เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT
- ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)
- ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์
- ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(นายวีระ ระบายศรี)
(นางสาวอรวรรณ ใจเอื้อ)
(นางสาวปราญชลี มกรสุต)
(นายคณิตสรณ์ พินทุสรศรี)
(นางสาวนวรา ประไพศิลป์)

- ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติ การบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการ ด้านนิติวิทยาศาสตร์/การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี
- กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุ และแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

4.12 เมื่อพบเหตุการณ์ต้องสงสัยระดับสูงมาก (Very High) ผู้รับจ้างต้องจัดให้มีทีมงานผู้เชี่ยวชาญเพื่อดำเนินการสืบสวน วิเคราะห์หาสาเหตุ และพิสูจน์หลักฐาน (Forensic) ภัยคุกคามที่เกิดขึ้น เช่น Malware, Ransomware พร้อมนำเสนอแผนภูมิรูปภาพสรุปเหตุการณ์ ที่แสดงถึงการวิเคราะห์ช่องทางที่เข้ามาโจมตีและผลกระทบที่เกิดขึ้น ในรายงานสรุปผลวิเคราะห์เฝ้าระวังและรายงานผลภัยคุกคามต่าง ๆ รวมทั้งให้คำแนะนำแนวทางการแก้ไขและป้องกันปัญหาตามที่ กพท. ร้องขอ จำนวนไม่เกิน 3 เคสต่อสัญญา

4.13 ผู้รับจ้างต้องให้บริการค้นหาภัยคุกคามเชิงรุก (Threat Hunting) หรือดำเนินการค้นหารูปแบบการโจมตีจาก Threat Intelligence โดยใช้เครื่องมือของผู้รับจ้าง และแจ้งเตือนให้ทราบถึงภัยคุกคามที่จะเกิดขึ้นกับ กพท.

4.14 ผู้รับจ้างต้องติดตั้งอุปกรณ์/ระบบ สำหรับจัดเก็บข้อมูล Log จากอุปกรณ์เครือข่าย อุปกรณ์รักษาความปลอดภัย เครื่องคอมพิวเตอร์แม่ข่าย และอื่น ๆ ที่เกี่ยวข้อง ของ กพท. เข้าสู่ระบบวิเคราะห์ข้อมูลผ่านระบบของผู้รับจ้าง เพื่อเป็นประโยชน์ต่อการวิเคราะห์ภัยคุกคามทางไซเบอร์

4.15 ดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

4.15.1 ทดสอบเจาะระบบครั้งที่ 1 ในรูปแบบ Grey-Box จำนวนอย่างน้อย 4 โดเมน

4.15.2 วิเคราะห์ และจัดลำดับความเสี่ยง โดยอ้างอิงตาม OWASP Top 10 เวอร์ชั่นล่าสุด หรือมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง และเสนอจุดอ่อน ผลกระทบ ตลอดจนให้คำแนะนำในการปรับปรุงแก้ไขช่องโหว่ที่ตรวจพบ จากการทดสอบเจาะระบบ (Penetration Testing) ตามข้อ 4.15.1

4.15.3 ทดสอบเจาะระบบครั้งที่ 2 (Revisit) ในรูปแบบ Grey-Box จำนวนอย่างน้อย 4 โดเมน

4.15.4 วิเคราะห์ และจัดลำดับความเสี่ยง โดยอ้างอิงตาม OWASP Top 10 เวอร์ชั่นล่าสุด หรือมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง และเสนอจุดอ่อน ผลกระทบ ตลอดจนให้คำแนะนำในการปรับปรุงแก้ไขช่องโหว่ที่ตรวจพบ จากการทดสอบเจาะระบบ (Penetration Testing) 4.15.3

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นางสาวปราญชลี มกรสุต)
(นายคณิตสรณ์ พินทุสรศรี)	(นางสาวนวรา ประไพศิลป์)	

4.16 ผู้รับจ้างต้องทำการทดสอบ Phishing E-mail ด้วยรูปแบบเหตุการณ์เสมือน ให้กับบุคลากรของ กพท. โดยมีรายละเอียดการดำเนินการ ดังนี้

4.16.1 ดำเนินการทดสอบ Phishing E-mail จำนวน 2 รอบ โดยรอบที่ 1 จัดขึ้นก่อนการฝึกอบรมหลักสูตรการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness Training) ตามข้อ 5.1. และรอบที่ 2 จัดขึ้นหลังจากการฝึกอบรมตามข้อ 5.1. โดยกำหนดกลุ่มเป้าหมายเป็นบุคลากรของ กพท. จำนวนไม่น้อยกว่า 450 คนต่อรอบ และต้องได้รับความเห็นชอบจากผู้บริหารของ กพท. ก่อน

4.16.2 การทำ Phishing E-mail จะต้องไม่ให้มีผลกระทบต่อบุคคลหรือหน่วยงานภายนอก และต้องกำหนดเทคนิคหรือวิธีการที่ทำให้กลุ่มเป้าหมายรู้ตัวล่วงหน้าน้อยที่สุด เพื่อให้เกิดประสิทธิภาพสูงสุด

4.16.3 จัดทำรายงานผลการทดสอบเพื่อวัดผล เปรียบเทียบ และสรุปผลการทดสอบทั้ง 2 รอบ เพื่อใช้นำเสนอต่อผู้บริหารของ กพท.

4.17 ผู้รับจ้างมีหน้าที่สนับสนุน และดำเนินการปิดและ/หรือลดช่องโหว่ ของอุปกรณ์/ระบบของผู้รับจ้างตามข้อ 4.14 โดยรายงานผลตามรูปแบบที่ กพท. กำหนด

4.18 ระบบตรวจจับภัยคุกคามที่เสนอต้องเป็นผลิตภัณฑ์ที่มีความน่าเชื่อถือ สามารถตรวจจับและติดตามภัยคุกคามอย่างมีประสิทธิภาพ และสามารถวิเคราะห์และรายงานที่เหมาะสม โดยผลิตภัณฑ์ที่เสนอจะต้องอยู่หรือเคยอยู่ในเกณฑ์ Leader ตามรายงานการวิจัยของ Gartner Report ประเภท Security Information and Event Management นับตั้งแต่ปี ค.ศ.2019

4.19 ศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ต้องอยู่ในประเทศไทย และได้รับรองมาตรฐาน ISO 27001 เป็นอย่างน้อย

5. การฝึกอบรม

ผู้รับจ้างต้องดำเนินการฝึกอบรมให้กับ กพท. อย่างน้อย 3 หลักสูตรดังนี้

5.1 หลักสูตรการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness Training) สำหรับเจ้าหน้าที่ กพท. อย่างน้อยจำนวน 25 คน ประกอบด้วยเนื้อหาตามหัวข้อเรื่องอย่างน้อย ดังนี้

- ความหมายของ Cybersecurity
- ความรู้พื้นฐานของ Cybersecurity
- รูปแบบภัยคุกคามของ Cybersecurity
- ความตระหนักรู้ด้าน Cybersecurity

โดยใช้ระยะเวลาการฝึกอบรมไม่น้อยกว่า 0.5 วัน พร้อมจัดทำแบบทดสอบเพื่อวัดผลการฝึกอบรม และจัดทำสื่อวิดีโอการสอน ความยาวสื่อไม่น้อยกว่า 3 ชั่วโมง เพื่อให้ กพท. นำไปใช้เผยแพร่ต่อไป

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)

5.2 หลักสูตร Information System Security สำหรับเจ้าหน้าที่ผู้รับผิดชอบดูแลด้านความมั่นคงปลอดภัยสารสนเทศของ กพท. อย่างน้อย 10 คน ประกอบด้วยเนื้อหาตามหัวข้อเรื่องอย่างน้อย ดังนี้

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

โดยใช้ระยะเวลาการฝึกอบรมไม่น้อยกว่า 3 วัน พร้อมจัดทำแบบทดสอบเพื่อวัดผลการฝึกอบรม และบันทึกวิดีโอการสอนเพื่อให้ กพท. นำไปใช้เผยแพร่ต่อไป

5.3 หลักสูตร Cybersecurity Awareness for Management สำหรับผู้บริหารของ กพท. อย่างน้อย 10 คน ประกอบด้วยเนื้อหาตามหัวข้อเรื่องอย่างน้อย ดังนี้

- ความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางดิจิทัล
- ความเสี่ยงและภัยคุกคาม
- ประโยชน์จากการป้องกันภัยคุกคาม
- กฎหมายที่เกี่ยวข้อง
- บทบาทหน้าที่ของผู้บริหารและการจัดการองค์กร
- การพัฒนานโยบายและยุทธศาสตร์ด้านความมั่นคงปลอดภัยทางดิจิทัล

โดยใช้ระยะเวลาการฝึกอบรมไม่น้อยกว่า 0.5 วัน พร้อมจัดทำสื่อวิดีโอการสอน ความยาวสื่อไม่น้อยกว่า 3 ชั่วโมง เพื่อให้ กพท. นำไปใช้เผยแพร่ต่อไป

6. กำหนดเวลาส่งมอบพัสดุ

ระยะเวลา 15 เดือน (1 ตุลาคม 2566 – 31 ธันวาคม 2567)

7. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

8. วงเงินงบประมาณ

งบประมาณ จำนวน 8,408,750.00 บาท (แปดล้านสี่แสนแปดพันเจ็ดร้อยห้าสิบบาทถ้วน) (ผูกพันปี 2566-2567) ซึ่งได้รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นทั้งปวงไว้ด้วยแล้ว

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)

9. งวดงานและการจ่ายเงิน

สำนักงานการบินพลเรือนแห่งประเทศไทยจะจ่ายเงินค่าจ้างให้แก่ผู้รับจ้าง โดยกำหนดการจ่ายเงินเป็นงวด ๆ ดังนี้

งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 20 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 1-3 ดังนี้

- ส่งมอบรายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์ ตามข้อ 4.8
- ส่งมอบรายงานประจำเดือน รายงานสรุปสำหรับผู้บริหาร (Executive Summary) และรายงานสรุปเหตุการณ์ภัยคุกคามที่มีการวิเคราะห์ภัยคุกคามในเชิงลึก ตามข้อ 4.9
- ส่งมอบรายงานประจำเดือน สรุปข่าวสารที่เกี่ยวข้องกับระบบรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายที่เกิดขึ้น ตามข้อ 4.10
- ส่งมอบคู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) ตามข้อ 4.11 อย่างน้อย 2 รูปแบบ
- ส่งมอบรายงานผลการติดตั้งอุปกรณ์/ระบบ ตามข้อ 4.14
- รายงานผลการทดสอบเจาะระบบ (Penetration Testing) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 1 ตามข้อ 4.15.1 และ 4.15.2
- ดำเนินการทดสอบ Phishing E-mail รอบที่ 1 ตามข้อ 4.16
- จัดการฝึกอบรม ตามข้อ 5

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 2 เป็นจำนวนเงินในอัตราร้อยละ 20 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 4-6 ดังนี้

- ส่งมอบรายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์ ตามข้อ 4.8
- ส่งมอบรายงานประจำเดือน รายงานสรุปสำหรับผู้บริหาร (Executive Summary) และรายงานสรุปเหตุการณ์ภัยคุกคามที่มีการวิเคราะห์ภัยคุกคามในเชิงลึก ตามข้อ 4.9
- ส่งมอบรายงานประจำเดือน สรุปข่าวสารที่เกี่ยวข้องกับระบบรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายที่เกิดขึ้น ตามข้อ 4.10
- ส่งมอบคู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) ตามข้อ 4.11 อย่างน้อย 1 รูปแบบ
- ดำเนินการทดสอบ Phishing E-mail รอบที่ 2 ตามข้อ 4.16

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

(นายวีระ ระบายศรี) (นางสาวอรวรรณ ใจเอื้อ) (นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี) (นางสาวนวรา ประไพศิลป์)

งวดที่ 3 เป็นจำนวนเงินในอัตราร้อยละ 20 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 7-9 ดังนี้

- ส่งมอบรายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์ ตามข้อ 4.8
- ส่งมอบรายงานประจำเดือน รายงานสรุปสำหรับผู้บริหาร (Executive Summary) และรายงานสรุปเหตุการณ์ภัยคุกคามที่มีการวิเคราะห์ภัยคุกคามในเชิงลึก ตามข้อ 4.9
- ส่งมอบรายงานประจำเดือน สรุปข่าวสารที่เกี่ยวข้องกับระบบรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายที่เกิดขึ้น ตามข้อ 4.10
- ส่งมอบคู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) ตามข้อ 4.11 อย่างน้อย 1 รูปแบบ
- รายงานผลการทดสอบเจาะระบบ (Penetration Testing) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 2 ตามข้อ 4.15.3 และ 4.15.4

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 4 เป็นจำนวนเงินในอัตราร้อยละ 20 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 10-12 ดังนี้

- ส่งมอบรายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์ ตามข้อ 4.8
- ส่งมอบรายงานประจำเดือน รายงานสรุปสำหรับผู้บริหาร (Executive Summary) และรายงานสรุปเหตุการณ์ภัยคุกคามที่มีการวิเคราะห์ภัยคุกคามในเชิงลึก ตามข้อ 4.9
- ส่งมอบรายงานประจำเดือน สรุปข่าวสารที่เกี่ยวข้องกับระบบรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายที่เกิดขึ้น ตามข้อ 4.10
- ส่งมอบคู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) ตามข้อ 4.11 อย่างน้อย 1 รูปแบบ

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 5 (งวดสุดท้าย) เป็นจำนวนเงินในอัตราร้อยละ 20 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 13-15 ดังนี้

- ส่งมอบรายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์ ตามข้อ 4.8
- ส่งมอบรายงานประจำเดือน รายงานสรุปสำหรับผู้บริหาร (Executive Summary) และรายงานสรุปเหตุการณ์ภัยคุกคามที่มีการวิเคราะห์ภัยคุกคามในเชิงลึก ตามข้อ 4.9
- ส่งมอบรายงานประจำเดือน สรุปข่าวสารที่เกี่ยวข้องกับระบบรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายที่เกิดขึ้น ตามข้อ 4.10

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)

- ส่งมอบคู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) ตามข้อ 4.11 อย่างน้อย 1 รูปแบบ

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

10. อัตราค่าปรับ

ค่าปรับตามสัญญาจ้างหรือข้อตกลงจ้างเป็นหนังสือจะกำหนด ดังนี้

10.1. กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากสำนักงาน จะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

10.2. กรณีผู้รับจ้างปฏิบัติผิดสัญญาจ้าง นอกเหนือจากข้อ 10.1. จะกำหนดค่าปรับเป็นรายวันเป็นจำนวนเงินตายตัวในอัตราร้อยละ 0.10 ของราคางานจ้าง

10.3. หากอุปกรณ์/ระบบ ในโครงการชำรุด บกพร่อง หรือใช้งานไม่ได้ทั้งหมดหรือเพียงบางส่วน ผู้รับจ้างต้องจัดการซ่อมแก้ไขให้แล้วเสร็จภายใน 6 ชั่วโมง นับจากได้รับแจ้งจาก กพท. หากไม่สามารถดำเนินการได้ตามเวลาดังกล่าว ผู้รับจ้างจะต้องจ่ายค่าปรับให้แก่ กพท. เป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้าง

11. ข้อตกลงห้ามเปิดเผยข้อมูล

ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการนี้ทั้งหมดที่ กพท. จัดหาให้ หรือผู้รับจ้างดำเนินการและจัดหาให้ กพท. ถือเป็นความลับ และเป็นสมบัติของ กพท. โดยผู้รับจ้างต้องไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใด ยกเว้นแต่จะได้รับอนุญาตจาก กพท. เป็นลายลักษณ์อักษร หากผู้รับจ้างละเมิดโดยมีการนำไปเผยแพร่ และเปิดเผยโดยไม่ได้รับอนุญาต กพท. มีสิทธิ์ฟ้องร้องเรียกค่าเสียหายและดำเนินการตามกฎหมายได้

12. ความคุ้มครองเกี่ยวกับลิขสิทธิ์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับงานจ้างตามสัญญานี้ โดย กพท. มิได้แก้ไขดัดแปลงไปจากเดิม ผู้รับจ้างจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว เพื่อให้ กพท. สามารถใช้งานจ้างนั้นต่อไปได้ หากผู้รับจ้างมิอาจกระทำได้และ กพท. ต้องรับผิดชอบชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์ดังกล่าว ผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหาย ค่าปรับและค่าใช้จ่ายอื่น ๆ รวมทั้งค่าธรรมเนียม และค่าทนายความ ทั้งนี้ กพท. จะแจ้งผู้รับจ้างทราบเป็นลายลักษณ์อักษรในเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าว โดยไม่ชักช้า

13. เงื่อนไขอื่น ๆ

13.1. ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กพท. รวมถึงนโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)

13.2. ผู้รับจ้างต้องมีเจ้าหน้าที่ อย่างน้อย 1 คน ที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยระบบไอทีและต้องได้รับใบ Certificate ที่ได้รับการยอมรับในระดับสากล ที่เทียบเท่าหรือมากกว่า อย่างน้อย 1 ใบ ดังนี้ Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) โดยใบ Certificate ต้องยังไม่หมดอายุ ณ วันที่ยื่นเสนอราคา ทั้งนี้เจ้าหน้าที่ดังกล่าวต้องเป็นพนักงานของบริษัทผู้เสนอราคา โดยจะต้องแนบสำเนาบัตรประชาชนของเจ้าหน้าที่ พร้อมประวัติการทำงาน เอกสารรับรองการเป็นพนักงาน และสำเนาใบ Certificate ซึ่งพนักงานผู้เชี่ยวชาญดังกล่าวต้องให้คำแนะนำเรื่องภัยคุกคามทางไซเบอร์ที่พบ ให้ข้อเสนอแนะแนวทางในการป้องกันและตอบสนองภัยคุกคามทางไซเบอร์ต่าง ๆ และให้คำปรึกษาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ กพท. ร้องขอ

13.3. ผู้รับจ้างต้องจัดสรรหาบุคลากรผู้เชี่ยวชาญ ที่มีความชำนาญด้านความมั่นคงปลอดภัยระบบไอทีและต้องได้รับใบ Certificate ที่ได้รับการยอมรับในระดับสากล ที่เทียบเท่าหรือมากกว่า อย่างน้อย 1 ใบ ดังนี้ CompTIA Cybersecurity Analyst (CySA+), Certified Information Security Manager (CISM) โดยใบ Certificate ต้องยังไม่หมดอายุ ณ วันที่ยื่นเสนอราคา โดยจะต้องแนบสำเนาบัตรประชาชนของเจ้าหน้าที่ พร้อมประวัติการทำงาน และสำเนาใบ Certificate เพื่อเข้าปฏิบัติงานที่ กพท. อย่างน้อย 1 วัน/สัปดาห์ ในวันเวลาทำการของ กพท. หรือตามที่ กพท. กำหนด เพื่อให้บริการและรับแจ้งปัญหาเกี่ยวกับระบบความมั่นคงปลอดภัยสารสนเทศของ กพท. รวมถึงให้ความรู้และแนะนำกรอบแนวปฏิบัติที่ดี (Best Practice) และเทคนิควิธีการและเครื่องมือที่เหมาะสม (Techniques and Tools) ในการปฏิบัติหน้าที่ของบุคลากรของ กพท. ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) ในทุกมิติ

13.4. ในกรณีที่ กพท. มีการย้ายสถานที่ทำการในระหว่างระยะเวลาสัญญา ผู้รับจ้างต้องดำเนินการให้ระบบสามารถใช้งานได้ตามปกติ และสนับสนุนการแก้ไขปัญหาการใช้งานเป็นระยะเวลาอย่างน้อย 1 เดือนหลังจากทำการย้ายสถานที่ติดตั้ง โดยไม่มีค่าใช้จ่ายเพิ่มเติม

13.5. ผู้รับจ้างต้องใช้พัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างทั้งหมดตามสัญญา (ถ้ามี)

13.6. ผู้รับจ้างต้องจัดทำแผนการใช้พัสดุที่ผลิตภายในประเทศ โดยยื่นให้แก่ผู้ว่าจ้างภายใน 60 วัน นับถัดจากวันลงนามในสัญญา (ถ้ามี)

14. หน่วยงานผู้รับผิดชอบโครงการ

ฝ่ายบริหารเทคโนโลยีดิจิทัล กองพัฒนามาตรฐานการจัดการและความปลอดภัยไซเบอร์
สำนักงานการบินพลเรือนแห่งประเทศไทย เลขที่ 333/105 อาคารหลักสี่พลาซ่า อาคาร 2
แขวงตลาดบางเขน เขตหลักสี่ กรุงเทพฯ 10210 โทรศัพท์ 02 568 8809 อีเมล์ itd_is@caat.or.th

(นายวีระ ระบายศรี)

(นางสาวอรวรรณ ใจเอื้อ)

(นางสาวปราญชลี มกรสุต)

(นายคณิตสรณ์ พินทุสรศรี)

(นางสาวนวรา ประไพศิลป์)