รายละเอียดขอบเขตงานจ้างบริหารจัดการเฝ้าระวังภัยคุกคามของ สสวท. (SOC)

1. ความเป็นมา

ตามที่ สสวท. มีนโยบายในการปรับรูปแบบการทำงานเป็น IPST Go Digital เพื่อให้สอดคล้องกับสถานการณ์และเทคโนโลยีในปัจจุบัน โดยมีการปรับปรุงกระบวนการทำงานให้สามารถปฏิบัติงานผ่านบริการระบบงานดิจิทัลและนวัตกรรม โดยจะมีข้อมูลสำคัญต่างๆ ที่ต้องจัดเก็บในระบบบริหารจัดการข้อมูลและระบบสนับสนุนสารสนเทศ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ปี 2559 ในช่วงเวลาที่ผ่านมาได้มีกฎหมายและข้อบังคับที่ประกาศบังคับออกมาเพิ่มเติม ได้แก่ พรบ. คอมพิวเตอร์ 2560, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 และประกาศอื่นๆ ที่เกี่ยวข้องซึ่งได้ดำเนินการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐแล้ว จึงทำให้ต้องมีการปรับปรุงกระบวนการทำงาน การพัฒนาเพื่อยกระดับทักษะ/การสร้างทักษะขึ้นมาใหม่ (Upskill/Reskill) และจัดหาและพัฒนาเทคโนโลยีให้สามารถรองรับการบังคับใช้กฎหมายและข้อกำหนดต่างๆ ซึ่งต้องมีการดำเนินการการประเมินความเสี่ยงโดยเลือกดำเนินการที่ระบบดิจิทัลหลักที่สำคัญ

จึงมีความจำเป็นในการใช้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Operations Center) เพื่อทำหน้าที่เฝ้าระวังและการบริหารความเสี่ยงในการรับมือภัยคุมคามทางไซเบอร์ให้ครอบคลุมทั้งในด้านบุคลากร ด้านนโยบายการรักษาความปลอดภัยและด้านโครงสร้างพื้นฐานด้านสารสนเทศ ให้มีประสิทธิภาพมากยิ่งขึ้น

2. วัตถุประสงค์

2.1 เพื่อยกระดับการเตรียมความพร้อมในการเฝ้าระวัง และรับมือกับภัยคุกคามด้านไซเบอร์ให้มีประสิทธิภาะมากยิ่งขึ้น สอดคล้องกับ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.2 วิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคาม และ/หรือเหตุการณ์ผิดปกติอันอาจก่อให้เกิดความเสียหายอย่างรุนแรงกับข้อมูลและระบบสารสนเทศ ให้เป็นไปตามมาตรฐานสากลและสามารถรับมือกับภัยคุกคามทางดิจิทัลในทุกรูปแบบได้อย่างทันท่วงที

2.3 ให้การสนับสนุนด้านเทคนิค ในการรับมือและกู้คืนระบบ (Response and Recovery) เมื่อเกิดภัยคุกคามด้านสารสนเทศ และการแจ้งเตือนเหตุการณ์ผิดปกติสำคัญ ทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ตลอดจนให้คำแนะนำด้านเทคนิค ในการแก้ไขเหตุการณ์ภัยคุกคามต่อความมั่นคงปลอดภัยด้านสารสนเทศ หากมีการตรวจพบหรือตามที่ร้องขอด้วย

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงาน ของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดาเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและ การบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอ ณ วันประกาศจัดซื้อจัดจ้าง หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการยื่นข้อเสนอและเสนอราคาครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของ ผู้ยื่นข้อเสนอได้มีคาสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) ที่ ๐๔๐๕.๒ /ว๑๒๔ ลงวันที่ ๑ มีนาคม ๒๕๖๖

3.12 ผู้ยื่นข้อเสนอต้องมีประสบการณ์ในการให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Operations Center) หรือ ให้บริการจำลองการโจมตีจากภัยคุกคามไซเบอร์ (Cyber Drill) หรือ ประเภทเดียวกันกับงานที่จ้าง ให้แก่หน่วยงานราชการ หรือ เอกชนที่น่าเชื่อถือ มาก่อน โดยต้องมีหนังสือรับรองผลงานและสำเนาสัญญาย้อนหลังไม่เกิน 3 ปี นับถึงวันที่เสนอราคา จำนวน 1 ผลงาน ผลงานไม่น้อยกว่า 250,000 บาท (สองแสนห้าหมื่นบาทถ้วน)

4. ขอบเขตงาน

4.1 ให้บริการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของเครื่องและอุปกรณ์ตามรายงานที่กำหนด ไปยังระบบ SOC ของผู้ให้บริการ ไม่น้อยกว่า 250 Event Per Second (EPS) ระยะเวลา 8 เดือน

4.2 ให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวโยงของเหตุการณ์ และภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring Services) จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่าง ๆ ของ ที่เกี่ยวข้องทุกวันตลอด 24 ชั่วโมง และดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) ที่กำหนด รวมทั้ง ให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าว ตลอดระยะเวลาสัญญา

4.3 จัดให้มีทีมงานที่มีความรู้ความสามารถในด้านการวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) และทีมผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้อง เพื่อให้คำปรึกษาด้านเทคนิคแก่ หากมีการตรวจพบหรือตามที่ร้องขอตลอดระยะเวลาสัญญา

4.4 จัดให้มีทีมงานสนับสนุนด้านการค้นคว้าและติดตามข้อมูลข่าวสารเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศ (Security Research Team) เพื่ออัพเดทข้อมูลข่าวสาร หรือข่าวสารที่ทันสมัย และ/หรือภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ อย่างสม่ำเสมอตลอดระยะเวลาสัญญา

4.5 บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือ เหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต วิเคราะห์ความเกี่ยวโยงของเหตุการณ์ และภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring) และต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Use case) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคาม

4.6 จัดทำแผนการทำงาน การจัดการและแจ้งเตือนภัยคุกคาม (Incident Handling) ตลอดระยะเวลาตามสัญญา

4.7 มีระบบบันทึกรายงานและแสดงสถานะการแก้ไขและรายงานผลการแก้ไขปัญหาเพื่อรายงานการเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ (Security Monitoring) ผ่านทาง Web Portal และมีรายงานประจำเดือน ซึ่งมีรายละเอียดอย่างน้อย ดังต่อไปนี้

4.7.1 สรุปจำนวนเหตุการณ์ผิดปกติที่เกิดขึ้นทั้งหมด

4.7.2 สรุปจำนวนเหตุการณ์ที่เป็น Critical

4.7.3 สรุปจำนวนเหตุการณ์ทั้งหมดที่คุกคามระบบ โดยจำแนกตามสถานะความเร่งด่วน (Critical, High, Medium Low)

4.7.4 สรุปจำนวนเหตุการณ์ที่เกิดขึ้นในแต่ละวัน โดยจำแนกตามสถานะความเร่งด่วน (Critical, High, Medium Low)

4.7.5 สรุป Signature ที่เป็นสาเหตุในการเกิดเหตุการณ์ผิดปกติ ที่เกิดขึ้นมากที่สุด 10 อันดับ

4.7.6 สรุปรายการอุปกรณ์ ที่เฝ้าระวังภัยคุกคาม

4.7.7 สรุปจำนวน Ticket ที่เกิดขึ้นในรอบเดือน โดยจำแนกตามสถานะของ Ticket

4.7.8 สรุปรายละเอียดการทำงาน การวิเคราะห์เหตุการณ์ ของแต่ละ Ticket

4.7.9 สรุปการเรียกใช้ทีม CSIRT (ถ้ามี)

4.7.10 สรุปเหตุการณ์ที่เกิดขึ้นมากที่สุด 10 อันดับแรก จำแนกตามหัวข้อต่างๆ เช่น Rule Name, Source IP Address, Source Port, Target IP Address, Target Port เป็นต้น

4.8 ต้องมีระบบแสดงสถานะการให้บริการและผลจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบผ่านทาง Web Portal ได้ โดยมีข้อมูลอย่างน้อยดังต่อไปนี้

4.8.1 สถานะของการเปิดและปิด Tickets

4.8.2 สถานะของ Incidents ที่เกิดขึ้น

4.8.3 สรุปผลการให้บริการ (Service History) และสถิติย้อนหลังได้ไม่น้อยกว่า 30 วัน

4.8.4 สถานะของการเฝ้าระวัง เช่น จำนวนของ Log จำนวนของ Analyzed Incidents และ Top 5 attacks

4.8.5 สถิติของภัยคุกคามแบบ Real-time โดยแยกประเภทตามภัยคุกคามที่เกิดขึ้นเป็นประจำ (Top Attack) ไอพีแอดเดรสต้นทางและหมายเลขพอร์ต (Port Number) เป็นต้น

4.9 จัดทีม CSIRT หรือ Computer Security Incident Response Team เข้าช่วยแก้ไขปัญหาที่เกิดขึ้นกับ พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อเหตุการณ์ในระดับร้ายแรง และระดับวิกฤต ณ สสวท. จำนวนอย่างน้อย 1 ครั้ง หรือได้แจ้งผ่านทางโทรศัพท์ หรือ E-Mail รวมถึงช่องทางการสื่อสารอื่นๆ ตามที่ สสวท. กำหนดได้ทุกวัน ไม่เว้นวันหยุด ภายใน 4 ชั่วโมง เพื่อวิเคราะห์หาสาเหตุของการบุกรุก และจัดลำดับความสำคัญของการบุกรุก พร้อมทั้งสนับสนุนข้อมูลที่มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นร่วมกับหน่วยงานกลาง เช่น ThaiCERT, TB-CERT, หน่วยงานควบคุมและกำกับดูแลที่เกี่ยวข้องตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

4.10 ต้องเข้าร่วมประชุมเพื่อรายงานสรุปผลการจัดเก็บและการวิเคราะห์ข้อมูลประจำทุกเดือน

4.11 หาก สสวท. มีการทดสอบเจาะระบบสารสนเทศ ตามมาตรฐานสากล (Vulnerability Scanning and Penetration Testing) ผู้ให้บริการต้องสนับสนุนข้อมูลส่วนของ log และการตรวจจับการโจมตีให้กับ สสวท. ทั้งนี้ สสวท. จะแจ้งการดำเนินการล่วงหน้าไม่น้อยกว่า 14 วัน

4.12 ผู้ยื่นข้อเสนอต้องจัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้างซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

5. บุคลากรในโครงการ

5.1 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความรู้ความเชี่ยวชาญในการปฏิบัติงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามของผู้ให้บริการประจำในองค์กร ที่มีความเชี่ยวชาญในการเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ พร้อมทั้งมีใบรับรอง (Certificate) ในด้านที่เกี่ยวข้อง ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบสำเนาใบรับรอง ดังกล่าวมาพร้อมกับการยื่นข้อเสนอในครั้งนี้ โดยประกอบด้วยใบรับรอง ดังนี้

- การตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Information Security Management Systems (ISMS)

Auditor/Lead Auditor (In Accordance with ISO 27001:2013) อย่างน้อย 1 คน

- การเจาะระบบอย่างมีจรรยาบรรณ Certified Ethical Hacker (CEH) อย่างน้อย 1 คน
- ความรู้ด้าน Security ตามมาตรฐาน CompTIA (CompTIA Security+) อย่างน้อย 1 คน
- การวิเคราะห์การโจมตีทางไซเบอร์ GIAC Certified Intrusion Analyst (GCIA) อย่างน้อย 1 คน
- ความเชี่ยวชาญด้าน Security ตามมาตรฐาน GIAC (GIAC Security Expert) อย่างน้อย 1 คน

5.2 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ในศูนย์ปฏิบัติการไม่น้อยกว่า 4 คน ประกอบไปด้วยบุคลากรดังนี้

- ผู้จัดการศูนย์ปฏิบัติการ SOC (SOC Manager) ในด้านการควบคุมการทำงานเฝ้าระวังและวิเคราะห์ภัยคุกคาม
- เจ้าหน้าที่ผู้เชี่ยวชาญ (Security Analyst Tier 1) ในด้านการวิเคราะห์ภัยคุกคาม
- เจ้าหน้าที่ผู้เชี่ยวชาญพิเศษ (Security Analyst Tier 2) ในด้านการบริหารจัดการระบบเฝ้าระวังและการวิเคราะห์ภัยคุกคามไซเบอร์ขั้นสูง
- วิศวกรระบบ (System Engineer) ในด้านการดูแลระบบเฝ้าระวังฯ

6. กำหนดส่งมอบงานและการจ่ายเงิน

งวดที่ 1 สสวท. จะจ่ายเงินร้อยละ 60 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงาน ดังนี้

- ส่งมอบแผนการทำงานตลอดระยะเวลาตามสัญญา ภายใน 7 วัน นับถัดจากวันลงนามในสัญญา
- รายงานการติดตั้งอุปกรณ์หรือระบบที่ใช้ในการเฝ้าระวัง และ รายงานการฝึกอบรมในรูปแบบการสอนงาน (on the job training) ภายใน 30 วัน นับถัดจากวันลงนามในสัญญา
- รายงานตามขอบเขตงาน ข้อ 4.6 พร้อมไฟล์เอกสาร แบบ PDF ประจำเดือนที่ 1 ถึง เดือนที่ 5 ภายใน 7 วันทำการ นับถัดจากวันสุดท้ายของเดือนที่ 5 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว
- จัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้างซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี) ภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

งวดที่ 2 สสวท. จะจ่ายเงินร้อยละ 40 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงาน ดังนี้

รายงานตามขอบเขตงาน ข้อ 4.6 พร้อมไฟล์เอกสาร แบบ PDF ประจำเดือนที่ 6 ถึง เดือนที่ 8 ภายใน 7 วันทำการ นับถัดจากวันสุดท้ายของเดือนที่ 8 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

7. ระยะเวลาดำเนินงาน 8 เดือน นับถัดจากวันลงนามในสัญญา

8. วงเงินงบประมาณ 540,000 บาท (ห้าแสนสี่หมื่นบาทถ้วน)

9. หลักเกณฑ์และสิทธิในการพิจารณาราคา

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาตัดสิน โดยใช้หลักเกณฑ์ราคา เพียงอย่างเดียว และ การพิจารณาผู้ชนะการยื่นข้อเสนอ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาจาก ราคารวม (รวมภาษีมูลค่าเพิ่มแล้ว) ที่เสนอราคาต่ำสุด

10. ค่าปรับ

10.1 กรณีที่ผู้ยื่นข้อเสนอไม่สามารถดำเนินการ ตามข้อกำหนด ต้องชำระค่าปรับรายวันในอัตราร้อยละ 0.1 ของราคาค่าจ้าง ตามสัญญา

10.2 กรณีอุปกรณ์ของผู้ยื่นข้อเสนอ ไม่สามารถใช้งานได้และต้องส่งซ่อมแซม ผู้ยื่นข้อเสนอต้องนำอุปกรณ์ที่มีคุณสมบัติเทียบเท่าหรือดีกว่า มาสำรองใช้งานภายใน 24 ชั่วโมง และดำเนินการติดตั้งให้อุปกรณ์ที่นำมาทดแทนสามารถทำงานได้เป็นปกติ กรณีที่ไม่สามารถดำเนินการแก้ไขซ่อมแซม ภายในระยะเวลา 1 วัน หลังจากได้รับแจ้งเหตุผิดปกติ ต้องชำระค่าปรับรายชั่วโมงในอัตราร้อยละ 0.1 ของราคาค่าจ้าง ตามสัญญา นับถัดจากเวลาที่ครบตามกำหนดจนถึงเนินการแก้ไขซ่อมแซมแล้วเสร็จ

11. ความรับผิดของผู้รับจ้าง

ผู้รับจ้างจะต้องรับผิดต่ออุบัติเหตุ ความเสียหาย หรือภยันตรายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้าง และจะต้องรับผิดต่อความเสียหายจากการกระทาของลูกจ้างหรือตัวแทนของผู้รับจ้างและจากการปฏิบัติงานของผู้รับจ้างช่วงด้วย (ถ้ามี)

ความเสียหายใดๆ อันเกิดแก่งานที่ผู้รับจ้างได้ทำขึ้น แม้จะเกิดขึ้นเพราะเหตุสุดวิสัยก็ตาม ผู้รับจ้างจะต้องรับผิดชอบโดยซ่อมแซมให้คืนดีหรือเปลี่ยนให้ใหม่โดยค่าใช้จ่ายของผู้รับจ้างเอง เว้นแต่ความเสียหายนั้นเกิดจากความผิดของผู้ว่าจ้าง ทั้งนี้ ความรับผิดของผู้รับจ้างดังกล่าวในข้อนี้จะสิ้นสุดลงเมื่อผู้ว่าจ้างได้รับมอบงานครั้งสุดท้าย ซึ่งหลังจากนั้นผู้รับจ้างคงต้องรับผิดเพียงในกรณีชำรุดบกพร่องหรือความเสียหายดังกล่าวในข้อ 4 เท่านั้น

ผู้รับจ้างจะต้องรับผิดต่อบุคคลภายนอกในความเสียหายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้าง หรือลูกจ้าง หรือตัวแทนของผู้รับจ้าง รวมถึงผู้รับจ้างช่วง (ถ้ามี) ตามสัญญานี้ หากผู้ว่าจ้างถูกเรียกร้องหรือฟ้องร้องหรือต้องชดใช้ค่าเสียหายให้แก่บุคคลภายนอกไปแล้ว ผู้รับจ้างจะต้องดำเนินการใดๆ เพื่อให้มีการว่าต่างแก้ต่างให้แก่ผู้ว่าจ้างโดยค่าใช้จ่ายของผู้รับจ้างเอง รวมทั้งผู้รับจ้างจะต้องชดใช้ค่าเสียหายนั้นๆ ตลอดจนค่าใช้จ่ายใดๆ อันเกิดจากการถูกเรียกร้อง หรือถูกฟ้องร้องให้แก่ผู้ว่าจ้างทันที