รายละเอียดคุณลักษณะเฉพาะโครงการจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูล ของสำนักงานประกันสังคม

1. หลักการและเหตุผล

สำนักงานประกันสังคมมีการจัดเก็บข้อมูลเป็นจำนวนมากซึ่งมีความสำคัญไม่ว่าจะเป็น ข้อมูลนายจ้าง ข้อมูลสถานประกอบ ข้อมูลสถานพยาบาล ข้อมูลผู้ประกันตนที่รวมไปถึงข้อมูลสิทธิประโยชน์ ฯลฯ ซึ่งข้อมูลเหล่านี้จำเป็นต้องมีการป้องกันการเข้าถึง และรวมไปถึงการเข้ารหัสไฟล์ฐานข้อมูล เพื่อให้สามารถนำข้อมูลไปใช้ได้อย่างปลอดภัย ซึ่งจากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทย รวบรวมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) พบว่าความพยายามบุกรุกเข้าระบบสารสนเทศ (Intrusion Attempts) เป็นภัยคุกคามไซเบอร์ อันดับ 1 ของประเทศไทย ไม่ว่าจะเป็นการเผยแพร่ข้อมูลที่ไม่เป็นจริง การพยายามบุกรุกเข้าระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาคธุรกิจ รายบุคคล และสถิติจากศูนย์กลางเฝ้าระวังและรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ (SSO Security Operation Center) ของสำนักงานประกันสังคม ในปี พ.ศ. 2565 พบว่าจำนวนภัยคุกคามและการโจมตีทางไซเบอร์ จากการตรวจพบทั้งหมด 7,724 เหตุการณ์ เช่น การโจมตีจาก Malware ผ่านเครือข่ายอินเทอร์เน็ต การโจมตีผ่านระบบเครือข่าย การโจมตี DoS ฯลฯ เป็นต้น ดังนั้น ในการดำเนินการใดก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคล จึงจำเป็นต้องปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ที่บังคับใช้ โดยจะมีบทบาทในการคุ้มครองและให้สิทธิที่ผู้ใช้งานควรมีต่อข้อมูลส่วนบุคคลของผู้ใช้งานได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคล ในการเก็บรวบรวม ใช้ หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม ซึ่งล้วนแล้วเกี่ยวข้องกับ พ.ร.บ. ฉบับนี้ที่จะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมาย ซึ่งบทลงโทษสำหรับผู้ที่ไม่ปฏิบัติตามนั้น มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง จึงมีความจำเป็นต้องกำหนดนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงแผนแม่บทว่าด้วยเรื่อง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ในการเสริมสร้างศักยภาพในการป้องกัน รับมือ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และคุ้มครองข้อมูลส่วนบุคคล หากต้องการป้องกันข้อมูล จำเป็นต้องมีองค์ประกอบ 2 ส่วน ได้แก่ ส่วนที่ 1 ความปลอดภัยของข้อมูล ได้แก่ การตรวจสอบสิทธิ์การใช้งาน การเข้ารหัสข้อมูล การป้องกันข้อมูลสูญหาย การตอบโต้ละเมิดการเฝ้าระวังการจู่โจมหรือการโจมตี และ การควบคุมการเข้าถึง ส่วนที่ 2 ข้อมูลส่วนบุคคล ได้แก่ ข้อกฎหมายหรือ พ.ร.บ. การกำหนดสิทธิ หน้าที่และความรับผิดชอบในการบริหารจัดการข้อมูลหรือธรรมาภิบาลข้อมูล การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล เป็นต้น หากหน่วยงานใดมีองค์ประกอบ 2 ส่วนนี้แล้วจะทำให้ข้อมูลที่นำไปใช้จะมีความปลอดภัยและน่าเชื่อถือ

สำนักงานประกันสังคม จึงให้ความสำคัญต่อความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลอย่างยิ่ง เพื่อให้ผู้ใช้บริการเชื่อมั่นได้ว่าสำนักงานประกันสังคมได้ดูแลรักษาข้อมูลส่วนบุคคลของผู้ประกันตนเป็นอย่างดีและจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม อีกทั้งยังสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ตั้งแต่กระบวนการเก็บรวบรวม การจัดเก็บรักษา การใช้ การเปิดเผย ตลอดจนการเปิดโอกาสให้เจ้าของข้อมูลส่วนบุคคลมีส่วนร่วมในการตรวจสอบและขอใช้สิทธิของตนเองตามที่กฎหมายกำหนด ดังนั้นทางสำนักงานประกันสังคมจึงมีความจำเป็นที่ต้องจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม ด้วยการเข้ารหัสไฟล์ฐานข้อมูล (Database File Encryption) และระบบปกปิดข้อมูล

(Data Masking) เพื่อให้ข้อมูลของผู้ประกันตนมีความปลอดภัย อีกทั้งสร้างความน่าเชื่อถือต่อผู้ประกันตน และเป็นภาพลักษณ์ที่ดีต่อสำนักงานประกันสังคม

ปัจจุบันฐานข้อมูลของสำนักงานประกันสังคมยังไม่มีการเข้ารหัสป้องกันไฟล์ข้อมูล จึงทำให้เกิดความเสี่ยงในการเข้าถึงข้อมูลโดยผู้ไม่ได้รับอนุญาต หรือผู้ไม่ประสงค์ดี เช่น การสำรองไฟล์ฐานข้อมูล (Backup Database File) หรือการสำเนาไฟล์ฐานข้อมูล (Copy Database File) จากที่หนึ่งไปอีกที่หนึ่ง, การสำเนาชุดเครื่องเสมือนของระบบฐานข้อมูล (Cloning VM ของ Database Server) ไปยังอีกที่หนึ่งเพื่อใช้งาน, วิธีการทำลายข้อมูลที่ (Destroy Information) ไม่ถูกต้องหรือไม่ครบถ้วน ซึ่งรวมไปถึงการโจรกรรมข้อมูลซึ่งบางระบบไม่มีการปกปิดข้อมูลส่วนบุคคล เช่น จากการทำรายงาน การนำข้อมูลไปวิเคราะห์ หรือการนำข้อมูลไปทำการทดสอบกับแอปพลิเคชันต่างๆ เป็นต้น ทำให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูล (Data Leak) หรือการละเมิดสิทธิ์ส่วนบุคคลของการเปิดเผยข้อมูลส่วนบุคคล ก่อให้เกิดผลกระทบกับหน่วยงานและเจ้าของข้อมูล ซึ่งเทคโนโลยีที่นำมาใช้เพื่อรักษาความปลอดภัยข้อมูล อย่างเช่น การเข้ารหัสไฟล์ฐานข้อมูล (Database File Encryption) ที่ไม่สามารถนำข้อมูลไปใช้งานได้หากไม่ได้รับอนุญาตการเข้าถึง และการป้องกันการรั่วไหลของข้อมูล อย่างเช่น ระบบปกปิดข้อมูล (Data Masking) ที่ช่วยปกปิดข้อมูลบางส่วน เพื่อนำไปใช้ประโยชน์ด้านต่างๆ เช่น การแสดงผลในแอปพลิเคชัน การทำรายงาน การส่งข้อมูลให้กับหน่วยงานที่เกี่ยวข้อง

ดังนั้น ทางสำนักงานประกันสังคมจึงมีความจำเป็นที่จะต้องจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม ด้วยการเข้ารหัสไฟล์ฐานข้อมูล (Database File Encryption) และระบบปกปิดข้อมูล (Data Masking) เพื่อให้ข้อมูลของผู้ประกันตนมีความปลอดภัย อีกทั้งสร้างความน่าเชื่อถือต่อผู้ประกันตน และเป็นภาพลักษณ์ที่ดีต่อสำนักงานประกันสังคม

2. วัตถุประสงค์

2.1 เพื่อจัดหาระบบเข้ารหัสไฟล์ฐานข้อมูลของผู้ประกันตน (Database File Encryption) ให้มีความปลอดภัย

2.2 เพื่อจัดหาระบบปกปิดข้อมูล (Data Masking) ให้สามารถปกปิดข้อมูลส่วนบุคคลที่ไม่ต้องการให้แสดงข้อมูล

2.3 เพื่อปกป้องข้อมูลในกรณีที่ต้องนำข้อมูลไปใช้ประโยชน์อื่นๆ เช่น การทำรายงาน การวิเคราะห์ข้อมูล ช่วงการใช้ข้อมูลระหว่างการพัฒนาแอปพลิเคชัน (Development) หรือการทดสอบข้อมูลบนแอปพลิเคชันในระบบทดสอบ (UAT) เป็นต้น

2.4 เพื่อทำให้ข้อมูลผู้ประกันตนได้รับความคุ้มครองตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล

2.5 เพื่อเพิ่มประสิทธิภาพและความปลอดภัยของไฟล์ฐานข้อมูล

2.6 เพื่อเป็นการสร้างความเชื่อมั่นให้กับผู้ดูแลระบบ ผู้ให้บริการ ตลอดจนผู้ใช้บริการข้อมูลประกันสังคมทั่วประเทศ ซึ่งเป็นการสร้างภาพลักษณ์ที่ดีให้แก่องค์กร

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานประกันสังคม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอจะต้องแสดงหลักฐานการมีสิทธิเสนอราคาดังนี้

3.11.1 ระบบปกป้องข้อมูล (Data Masking)

3.11.2 ระบบเข้ารหัสไฟล์ฐานข้อมูล (Database file encryption)

โดยผู้ยื่นข้อเสนอจะต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่าย พร้อมทั้งให้การสนับสนุนทางด้านเทคนิค จากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย ทั้งนี้เอกสารหลักฐานดังกล่าวต้องมีอายุครอบคลุมถึงวันที่เสนอราคา

3.12 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความรู้ ความสามารถ โดยมีประกาศนียบัตรด้านความมั่นคงปลอดภัยทางสารสนเทศ Certified ISO/IEC 27001 หรือ Certified Information Systems Auditor (CISA) หรือ Certified Information Systems Security Professional (CISSP) จำนวน 1 คน เป็นอย่างน้อย

3.13 ผู้ยื่นข้อเสนอต้องมีผลงานการขายพร้อมติดตั้งระบบรักษาความมั่นคงปลอดภัยสารสนเทศ โดยผลงานมีมูลค่าไม่ต่ำกว่า 29,000,000 บาท (ยี่สิบเก้าล้านบาทถ้วน) และต้องเป็นผลงานที่เป็นคู่สัญญาเดียวกันโดยตรงกับหน่วยงานรัฐบาล หรือหน่วยงานรัฐวิสาหกิจ หรือหน่วยงานเอกชน ที่เป็นผลงานที่สิ้นสุดแล้วโดยมีวงเงินในสัญญาเดียว ย้อนหลังไม่เกิน 5 ปี นับถึงวันยื่นเอกสารประกวดราคา โดยแนบหนังสือรับรองผลงานและ/หรือสำเนาสัญญาและ/หรือสำเนาใบสั่งซื้อสั่งจ้าง มาพร้อมกับเอกสารการประกวดราคา

3.14 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สุทธิที่ปรากฏงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปี สุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่ได้ชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า 20 ล้านบาท

(3) สำหรับการจัดซื้อจัดจ้าง ครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในการบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันที่ยื่นข้อเสนอไม่เกิน 90 วัน)

(5) กรณีตาม (1) - (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

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

4. เงื่อนไขการเสนอราคา

4.1 ผู้ยื่นข้อเสนอจะต้องจัดทำตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะโครงการจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม เป็นรายข้อทุกข้อ และทุกรายการ โดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบตามตารางที่ 1 ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความหรือเอกสารในส่วนอื่นที่จัดทำเสนอมา ผู้ยื่นข้อเสนอจะต้องระบุให้เห็นอย่างชัดเจนสามารถตรวจสอบได้ง่ายไว้ในเอกสารเปรียบเทียบด้วยว่าสิ่งที่ต้องการอ้างอิงถึงนั้นอยู่ในส่วนใดตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึงให้หมายเหตุหรือขีดเส้นใต้หรือระบายสีพร้อมเขียนหัวข้อกำกับไว้เพื่อให้สามารถไปตรวจสอบกับเอกสารเปรียบเทียบได้ง่ายและตรงกัน หากผู้ยื่นข้อเสนอไม่ดำเนินการตามข้อนี้ สำนักงานประกันสังคม สงวนสิทธิที่จะไม่พิจารณาผู้ยื่นข้อเสนอที่ไม่ดำเนินการตามเงื่อนไขดังกล่าว

ตารางที่ 1 ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะโครงการจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม

หัวข้อ	ข้อกำหนดสำนักงานประกันสังคม	คุณสมบัติที่ผู้ยื่นข้อเสนอ	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารรายละเอียดเฉพาะโครงการฯ	ให้คัดลอกรายละเอียดคุณลักษณะเฉพาะที่สำนักงานประกันสังคมกำหนดมากรอกในช่องนี้	ให้ระบุคุณลักษณะเฉพาะที่ผู้ยื่นข้อเสนอเสนอในช่องนี้	ระบุหมายเลขหน้าของเอกสารอ้างอิงของผู้ยื่นข้อเสนอ

4.2 สำนักงานประกันสังคมสงวนสิทธิที่จะขอเอกสารชี้แจงเพิ่มเติมจากผู้ยื่นข้อเสนอ และผู้ยื่นข้อเสนอจะต้องจัดส่งเอกสารชี้แจง (Clarification) เพิ่มเติมให้ถูกต้องครบถ้วนภายในระยะเวลาที่สำนักงานประกันสังคมกำหนด หากมิได้แจ้งกำหนดไว้ให้ถือว่าต้องจัดส่งภายใน 3 วัน มิฉะนั้นสำนักงานฯ จะตัดสิทธิการเข้าประกวดราคา

4.3 ผลิตภัณฑ์ต่างๆ ทุกผลิตภัณฑ์ที่นำเสนอในโครงการฯ จะต้องเป็นของแท้ ของใหม่ยังไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ พร้อมทั้งอยู่ในสภาพที่จะใช้งานได้ทันที และปัจจุบันผลิตภัณฑ์ดังกล่าวจะต้องเป็นผลิตภัณฑ์ที่ยังอยู่ในสายการผลิต (Production Line) ต้องได้รับลิขสิทธิ์การใช้งาน (License) ถูกต้องจากเจ้าของลิขสิทธิ์ โดยต้องแสดงเอกสารยืนยันจากเจ้าของผลิตภัณฑ์หรือตัวแทนเจ้าของผลิตภัณฑ์

5. ขอบเขตการดำเนินงาน

5.1 ผู้ขายต้องเสนอแผนงานและขั้นตอนการดำเนินงานตั้งแต่เริ่มต้นโครงการจนถึงสิ้นสุดโครงการโดยละเอียด ที่เกี่ยวกับการติดตั้งระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม ตามโครงการนี้ การติดตั้งระบบบนเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานประกันสังคม รวมถึงแผนการทดสอบระบบหลังการติดตั้ง ต่อสำนักงานประกันสังคมเป็นลายลักษณ์อักษรภายใน 30 วัน นับถัดจากวันลงนามในสัญญา

5.2 ผู้ขายจะต้องออกแบบ อุปกรณ์หรือซอฟต์แวร์ที่ใช้ในโครงการที่ศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรองของสำนักงานประกันสังคมให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

5.3 ผู้ขายจะต้องจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม ตามคุณลักษณะเฉพาะที่กำหนดในโครงการให้สำนักงานประกันสังคม พร้อมลิขสิทธิ์การใช้งานซอฟต์แวร์จำนวนไม่น้อยกว่า 20 ลิขสิทธิ์การใช้งาน

5.4 ผู้ขายต้องดำเนินการติดตั้งอุปกรณ์หรือซอฟต์แวร์ทั้งหมดที่ใช้ในโครงการ ทั้งการตั้งค่า (Configuration) การปรับแต่งระบบ (Customization) รวมไปถึงการทดสอบการทำงานที่เป็นการทดสอบสภาวะการทำงานของอุปกรณ์ (Equipment Testing) และการทดสอบการทำงานร่วมกับระบบสารสนเทศของสำนักงานประกันสังคม (System Integration Test) ซึ่งการดำเนินการติดตั้งทุกขั้นตอน จะต้องดำเนินการร่วมกับเจ้าหน้าที่ผู้รับผิดชอบของสำนักงานประกันสังคม

5.5 ผู้ขายจะต้องจัดทำการตั้งค่าระบบปกป้องข้อมูล (Data Masking) บนเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล (Database Server) ได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย ตามที่สำนักงานประกันสังคมกำหนด ได้แก่

1) ระบบแจ้งประสบอันตรายอันเนื่องจากการทำงานระบบบริการอิเล็กทรอนิกส์ กองทุนเงินทดแทน
2) ระบบงานกองทุนเงินทดแทน
3) ระบบใบเสร็จรับเงินอิเล็กทรอนิกส์
4) ระบบฐานข้อมูลสถานประกอบการ
5) ระบบสอบทรัพย์
6) ระบบอื่นๆ ตามความต้องการของสำนักงานประกันสังคม (ถ้ามี)

5.6 ผู้ขายจะต้องจัดทำการเข้ารหัสไฟล์ฐานข้อมูล (Database file encryption) บนเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล (Database Server) ได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย ตามที่สำนักงานประกันสังคมกำหนด ได้แก่

1) ระบบแจ้งประสบอันตรายอันเนื่องจาการทำงานระบบบริการอิเล็กทรอนิกส์ กองทุนเงินทดแทน

2) ระบบงานกองทุนเงินทดแทน

3) ระบบใบเสร็จรับเงินอิเล็กทรอนิกส์

4) ระบบฐานข้อมูลสถานประกอบการ

5) ระบบสอบทรัพย์

6) ระบบอื่นๆ ตามความต้องการของสำนักงานประกันสังคม (ถ้ามี)

5.7 ผู้ขายจะต้องดำเนินการฝึกอบรมการใช้งานระบบงานตามที่สำนักงานประกันสังคมกำหนด ตามข้อ 5.5 และข้อ 5.6 ให้กับเจ้าหน้าที่ผู้เกี่ยวข้องที่ดูแลระบบของสำนักงานประกันสังคม จำนวนไม่น้อยกว่า 5 คน พร้อมจะต้องดำเนินการจัดทำเอกสารคู่มือการฝึกอบรมการใช้งานเป็นภาษาไทยที่อยู่ในรูปแบบเอกสารและไฟล์อิเล็กทรอนิกส์ ประกอบด้วย

5.7.1 การกำหนดค่า (configuration) ของระบบ

5.7.2 การดูแลบำรุงรักษาของระบบ

5.8 ผู้ขายจะต้องทำการบริหารโครงการ จัดเตรียมประชุมและรายงาน ผลการดำเนินงาน ปัญหาที่เกิด การแก้ไขปัญหา รายงานผลบริหารความเสี่ยง รวมถึงทำการสรุปปัญหาและวิธีการแก้ไขปัญหา และรายงานความก้าวหน้าของการดำเนินงานให้กับคณะกรรมการตรวจรับ

5.9 ผู้ขายจะต้องยินยอมปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของ สำนักงานประกันสังคม รวมถึง นโยบาย คำสั่งและวิธีปฏิบัติที่เกี่ยวข้องอย่างเคร่งครัด โดยมีรายละเอียด ดังนี้

5.9.1 ผู้ขายห้ามนำอุปกรณ์ประมวลผลที่ไม่ใช่ของสำนักงานประกันสังคม มาเชื่อมต่อเข้ากับระบบเครือข่ายภายในของ สำนักงานประกันสังคม เว้นแต่ได้รับอนุญาตจากสำนักงานประกันสังคมแล้ว

5.9.2 ผู้ขายห้ามนำข้อมูลและสื่อเก็บข้อมูลออกจากสำนักงานประกันสังคม โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรและการนำข้อมูลออกไปต้องมีการควบคุมที่เหมาะสมที่สำนักงานประกันสังคมเห็นชอบ

5.10 ผู้ขายจะต้องตั้งค่าระบบตามข้อ 5.5 และข้อ 5.6 เพื่อส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไปยังอุปกรณ์จัดเก็บมูลจราจรทางคอมพิวเตอร์ที่ทางสำนักงานประกันสังคมใช้งานอยู่ได้

5.11 ผู้ขายจะต้องติดตั้ง ปรับแต่ง (Configuration) อุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ที่เสนอมาทั้งหมดในโครงการฯ ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ หากระบบปกป้องข้อมูล และระบบรักษาความปลอดภัยข้อมูลด้วยการเข้ารหัสไฟล์ฐานข้อมูลที่เสนอมา ไม่สามารถใช้งานได้อย่างมีประสิทธิภาพ ผู้ขายจะต้องจัดหาทั้งอุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์เพิ่มเติม เพื่อให้ระบบฯ สามารถทำงานได้อย่างมีประสิทธิภาพ ทั้งนี้ค่าใช้จ่ายที่เกิดทั้งหมดในการดำเนินการดังกล่าว ผู้ขายจะต้องรับผิดชอบทั้งหมด

5.12 ผู้ขายจะต้องจัดทำขั้นตอนการกอบกู้ระบบตามข้อ 5.5 และข้อ 5.6

5.13 ผู้ขายจะต้องร่วมทำการทดสอบแผนการกอบกู้ระบบคอมพิวเตอร์ (Disaster Recovery Plan - DRP) ของสำนักงานประกันสังคม (ถ้ามี)

6. รายละเอียดและคุณลักษณะเฉพาะ

ระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูล จำนวน 1 ระบบ โดยมีคุณลักษณะพื้นฐานอย่างน้อยเทียบเท่าหรือดีกว่า ดังนี้

6.1 ระบบปกป้องข้อมูล Data Masking จำนวน 1 ชุด ประกอบด้วย

6.1.1 ระบบสำหรับการปกป้องข้อมูล Data Masking จำนวนไม่น้อยกว่า 20 ลิขสิทธิ์การใช้งาน ดังนี้

6.1.1.1 ระบบที่เสนอต้องสามารถทำงานร่วมกับฐานข้อมูล ได้อย่างน้อยดังนี้

1) Microsoft MS-SQL Server
2) Oracle database
3) IBM DB2
4) MySQL

6.1.1.2 ระบบที่เสนอสามารถทำ Dynamic Data Masking เพื่อปกปิดและควบคุมการเข้าถึงข้อมูลบนฐานข้อมูล ได้อย่างน้อยดังนี้

1) Redact
2) Query Rewrite หรือเทียบเท่า

6.1.1.3 ระบบที่เสนอสามารถกำหนดรูปแบบของข้อมูล (Data Pattern) โดยใช้ Regular Expression (Regex) และตั้งค่าอักขระที่จะไปแทนที่ข้อมูล (Replacement character) เพื่อทำ Redact ได้

6.1.1.4 ระบบที่เสนอมี Built-in Regular Expression (Regex) เพื่อทำ Redact ได้

6.1.1.5 ระบบที่เสนอสามารถทำ Redact เพื่อปกปิดและควบคุมการเข้าถึงข้อมูลบนฐานข้อมูลในระดับ session ได้

6.1.1.6 ระบบที่เสนอมีฟังก์ชันการเขียนข้อความค้นหาข้อมูลใหม่ Query Rewrite หรือเทียบเท่า เพื่อควบคุมการเข้าถึงฐานข้อมูลของผู้ใช้งานได้

6.1.1.7 ระบบที่เสนอสามารถค้นหาข้อมูล (Discovery) และจัดประเภทข้อมูล (classification) ที่มีความสำคัญได้

6.1.1.8 ระบบที่เสนอสามารถตรวจสอบและควบคุมกิจกรรมของผู้ใช้งานที่ได้รับสิทธิพิเศษ (Privileges user) เช่น ผู้ดูแลฐานข้อมูลหรือผู้ดูแลระบบ

6.1.1.9 ระบบที่เสนอสามารถตรวจหาความเสี่ยงจากภายใน (Insider Threats) หรือการรั่วไหลของข้อมูล (Data leak หรือ Data breach) ได้

6.1.1.10 ระบบที่เสนอสามารถตั้งค่านโยบายสำหรับควบคุมการเข้าถึงข้อมูลการใช้งานและการจัดเก็บเพื่อตรวจสอบตามมาตรฐาน (Compliance) ได้

6.1.1.11 ระบบที่เสนอสามารถตั้งค่านโยบาย (Policy) เพื่อควบคุมการเข้าใช้งานของผู้ใช้งาน เช่น Log หรือ Ignore หรือ Alert หรือ Block ได้

6.1.1.12 ระบบที่เสนอสามารถแสดงรายงานที่เกี่ยวกับการเข้าถึงข้อมูล เพื่อสนับสนุนในการตรวจสอบการปฏิบัติตามข้อกำหนดได้

6.1.1.13 ระบบที่เสนอสามารถรองรับการทำงานร่วมกับระบบวิเคราะห์และจัดการข้อมูลความปลอดภัยสารสนเทศ (SIEM) ได้

6.1.1.14 ระบบที่เสนอสามารถสร้างรายงาน Query Rewrite หรือเทียบเท่า เพื่อตรวจสอบการใช้งาน ได้อย่างน้อยดังนี้

1) Query Rewrite Log หรือ Display Name
2) Client/Server หรือ HostName หรือ IP Address
3) Session หรือ Connection
4) Access Period (Start – End Date Time)

6.1.1.15 ระบบที่เสนอสามารถใช้เทคโนโลยี Machine Learning ในการวิเคราะห์พฤติกรรมของผู้ใช้ข้อมูลในระบบฐานข้อมูลและตรวจสอบความผิดปกติ เพื่อช่วยระบุความเสี่ยงจากภัยคุกคาม

6.1.1.16 ระบบที่เสนอสามารถทำงานร่วมกับระบบศูนย์กลางการบริหารจัดการนโยบายภายใต้เครื่องหมายการค้าเดียวกัน

6.1.2 ระบบควบคุมการทำงานของระบบปกป้องข้อมูล Data Masking ใช้งาน จำนวนไม่น้อยกว่า 6 ลิขสิทธิ์การใช้งาน ดังนี้

6.1.2.1 ระบบที่เสนอเป็น Hardware Appliance หรือ Software สำหรับติดตั้งบนเครื่องแม่ข่ายคอมพิวเตอร์ หรือ Virtual Appliance ที่ถูกออกแบบมาเพื่อควบคุมการทำงานของระบบปกป้องข้อมูล Data Masking ได้

6.1.2.2 ระบบที่เสนอสามารถตรวจสอบกิจกรรมในฐานข้อมูลแบบเรียลไทม์ (Real-time Data Monitoring) และแสดงข้อมูลของพฤติกรรมที่ผิดปกติหรือไม่ได้รับอนุญาตได้

6.1.2.3 ระบบที่เสนอต้องมีรายงานตัวอย่างแม่แบบ (Template หรือ predefine report) สำหรับการปฏิบัติตามกฎระเบียบ ได้เป็นอย่างน้อย ดังนี้

1) GDPR
2) HIPAA
3) PCI DSS

6.1.2.4 ระบบที่เสนอสามารถแสดงข้อมูลการใช้งานหรือข้อมูลของระบบในลักษณะ Dashboard ได้

6.1.2.5 ระบบที่เสนอสามารถแสดงข้อมูลตรวจสอบการใช้งานของผู้ใช้งาน เช่น IP Address หรือ Protocol หรือ Sessions (timestamps, database names) หรือ SQL (statements, commands, objects, fields, and values) ได้

6.1.2.6 ระบบที่เสนอสามารถเข้าใช้งานระบบ ผ่าน web browser ได้

6.1.2.7 ระบบที่เสนอสามารถจัดการกระบวนการปฏิบัติตามกฎระเบียบ (Compliance workflow) เช่น การประเมินความเสี่ยง, การจัดการเหตุการณ์ หรือการรายงานได้แบบอัตโนมัติ

6.1.2.8 ระบบที่เสนอสามารถออกรายงานการเข้าใช้งานฐานข้อมูลของผู้ใช้งานในรูปแบบ PDF หรือ CSV ได้

6.1.2.9 ระบบที่เสนอต้องสามารถแจ้งเตือนและส่งต่อข้อมูล Log ช่องทางได้อย่างน้อยดังนี้

1) SMTP
2) SNMP
3) Syslog

6.1.3 ระบบศูนย์กลางการบริหารจัดการนโยบายการใช้งาน จำนวนไม่น้อยกว่า 2 ลิขสิทธิ์การใช้งาน ดังนี้

6.1.3.1 ระบบที่เสนอเป็น Hardware Appliance หรือ Software สำหรับติดตั้งบนเครื่องแม่ข่าย หรือ Virtual Appliance ที่ถูกออกแบบมาเพื่อทำหน้าที่รวบรวมข้อมูลจากระบบควบคุมการทำงานของระบบปกป้องข้อมูล Data Masking

6.1.3.2 ระบบที่เสนอสามารถรวบรวมข้อมูลจากระบบควบคุมการทำงานของระบบปกป้องข้อมูล Data Masking เพื่อสร้างรายงานได้

6.1.3.3 ระบบที่เสนอสามารถจัดการข้อมูลจากระบบปกป้องข้อมูล Data Masking เพื่อบริหารจัดการจากส่วนกลางได้

6.1.3.4 ระบบที่เสนอสามารถกำหนดสิทธิ์การใช้งานระบบของผู้ใช้แบบ Role Base ได้

6.1.3.5 ระบบที่เสนอต้องสามารถทำงานร่วมกับระบบ LDAP หรือ Active Directory เพื่อรองรับการพิสูจน์ตัวตนได้

6.1.3.6 ระบบที่เสนอสามารถเข้าใช้งานระบบ ผ่าน web browser ได้

6.2 ระบบรักษาความปลอดภัยข้อมูลด้วยการเข้ารหัสไฟล์ฐานข้อมูล (Database file encryption) จำนวน 1 ชุด ประกอบด้วย

6.2.1 ซอฟต์แวร์เข้ารหัสไฟล์ (File Encryption) จำนวนไม่น้อยกว่า 20 ลิขสิทธิ์การใช้งาน ดังนี้

6.2.1.1 ซอฟต์แวร์ที่เสนอทำหน้าที่ในการเข้ารหัสไฟล์ (File Encryption) ต้องทำงานบนระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย ได้อย่างน้อยดังนี้

1) Microsoft Windows Server
2) Red Hat Enterprise Linux (RHEL)
3) Ubuntu

6.2.1.2 ซอฟต์แวร์ที่เสนอสามารถทำการเข้ารหัส และถอดรหัส (Encrypt/Decrypt) ที่จัดเก็บใน Storage ตามรูปแบบจัดเก็บข้อมูล ได้อย่างน้อยดังนี้

1) Databases
2) Cloud

6.2.1.3 ซอฟต์แวร์ที่เสนอสามารถรองรับการเข้ารหัสไฟล์ฐานข้อมูล ได้อย่างน้อยดังนี้

1) Oracle
2) Microsoft SQL Server
3) IBM DB2
4) MySQL

6.2.1.4 ซอฟต์แวร์ที่เสนอ สามารถทำงานตามที่กำหนดได้ อย่างน้อยดังนี้

1) File – Level Encryption
2) User Access Control
3) Live data Transformation หรือ Re-keying
4) Integration to SIEM หรือ Log Server

6.2.1.5 ซอฟต์แวร์ที่เสนอ สามารถปฏิบัติตามนโยบายการเข้ารหัส (Policy) การควบคุมการเข้าถึง (Access Control) จากระบบบริหารจัดการคีย์แบบส่วนกลาง (Centralized Key)

6.2.1.6 ซอฟต์แวร์ที่เสนอมีความสามารถในการเปลี่ยนคีย์เข้ารหัส (Re-Keying) ได้โดยผ่านระบบบริหารจัดการคีย์แบบส่วนกลาง (Centralized key) โดยไม่หยุดการทำงานของแอปพลิเคชั่น

6.2.1.7 ซอฟต์แวร์ที่เสนอผ่านการรับรองมาตรฐาน FIPS 140-2 Level 1 เป็นอย่างน้อย

6.2.1.8 ซอฟต์แวร์ที่เสนอต้องสามารถทำงานร่วมกับระบบบริหารจัดการคีย์แบบส่วนกลาง (Centralized key) ภายใต้เครื่องหมายการค้าเดียวกัน

6.2.2 ระบบบริหารจัดการคีย์แบบส่วนกลาง (Centralized key) จำนวนไม่น้อยกว่า 4 ชุด ดังนี้

6.2.2.1 ระบบที่เสนอเป็น Hardware Appliance หรือ Software สำหรับติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย หรือ Virtual Appliance ที่ถูกออกแบบมาเพื่อทำหน้าที่บริหารจัดการกุญแจเข้ารหัสและกำหนดนโยบายจากระบบควบคุมการทำงานของระบบเข้ารหัสไฟล์ฐานข้อมูล (Database file encryption)

6.2.2.2 ระบบที่เสนอต้องสามารถบริหารจัดการกุญแจเข้ารหัส ได้อย่างน้อยดังนี้

1) การสร้าง (Generate)
2) การลบ (Deletion)
3) การสำรอง (Backup)
4) การกู้คืน (Restore)
5) การปิดการใช้งาน (Deactivation)

6.2.2.3 ระบบที่เสนอผ่านการรับรองมาตรฐาน FIPS 140-2 level 1 เป็นอย่างน้อย

6.2.2.4 ระบบที่เสนอสามารถบริหารจัดการแบบ Multi-tenancy หรือ Multi-domain ได้

6.2.2.5 ระบบที่เสนอสามารถรองรับการสร้างโดเมน (Domain) เพื่อเข้าใช้ได้ไม่น้อยกว่า 1,000 โดเมน

6.2.2.6 ระบบที่เสนอสามารถติดตั้งให้ทำงานแบบ Clustering ได้

6.2.2.7 ระบบที่เสนอสามารถเข้าใช้งานระบบ ผ่าน web browser ได้

6.2.2.8 ระบบที่เสนอสามารถยืนยันตัวตน (Authentication) ได้อย่างน้อยดังนี้

1) Local User
2) Active Directory (AD)
3) Lightweight Directory Access Protocol (LDAP)
4) Certificate based authentication

6.2.2.9 ระบบที่เสนอสามารถควบคุมนโยบาย (Policy) เพื่อควบคุมการเข้าถึง (Access Policy) การเข้ารหัสไฟล์ โฟล์เดอร์ บนเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล (Database Server) โดยสามารถทำงานร่วมกับซอฟต์แวร์เข้ารหัสไฟล์ (File Encryption) ที่นำเสนอได้

6.2.2.10 ระบบที่เสนอสามารถรองรับการบริหารจัดการ (Manage) ด้วยโปรโตคอลได้อย่างน้อยดังนี้

1) SNMP เวอร์ชั่น v1, v2c และ v3
2) KMIP

6.2.2.11 ระบบที่เสนอสามารถรองรับการบริหารจัดการการเข้ารหัสข้อมูลเพื่อป้องกันข้อมูล ได้อย่างน้อยดังนี้

1) การเข้ารหัสไฟล์ (File encryption)
2) การเข้ารหัสแอปพลิเคชัน (Application encryption)

6.3 เครื่องคอมพิวเตอร์แม่ข่ายสำหรับรองรับการติดตั้งสำหรับข้อ 6.1 และ 6.2 (กรณีที่ไม่ได้นำเสนอ Hardware Appliance) สำหรับศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง จำนวนอย่างน้อย 2 ชุด โดยมีคุณลักษณะพื้นฐานอย่างน้อยเทียบเท่า หรือดีกว่า ดังนี้

6.3.1 เครื่องคอมพิวเตอร์แม่ข่ายจำนวน 2 เครื่อง โดยมีคุณสมบัติดังต่อไปนี้

6.3.1.1 มีหน่วยประมวลผลกลาง (CPU) แบบ 20 แกนหลัก (20 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Sever) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.3 GHz จำนวนไม่น้อยกว่า 2 หน่วย

6.3.1.2 หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 24 MB

6.3.1.3 มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR4 หรือดีกว่า ขนาดไม่น้อยกว่า 256 GB

6.3.1.4 สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5

6.3.1.5 มีหน่วยจัดเก็บข้อมูล ความจุไม่น้อยกว่า 10 TB

6.3.1.6 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10 Gb Base-T หรือดีกว่า จำนวน ไม่น้อยกว่า 2 ช่อง

6.3.1.7 มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

6.4 ซอฟต์แวร์สำหรับเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อ 6.3 โดยมีคุณลักษณะพื้นฐานอย่างน้อยเทียบเท่า หรือดีกว่า ดังนี้

6.4.1 มีซอฟต์แวร์ระบบบริหารจัดการศูนย์กลางจำนวน 1 ระบบ ไม่น้อยกว่า 4 CPU สำหรับศูนย์คอมพิวเตอร์หลัก (DC)

6.4.2 มีซอฟต์แวร์ระบบบริหารจัดการศูนย์กลางจำนวน 1 ระบบ ไม่น้อยกว่า 4 CPU สำหรับศูนย์คอมพิวเตอร์สำรอง (DR)

7. ระยะเวลาดำเนินการ

ผู้ขายต้องดำเนินงานตามรายละเอียดคุณลักษณะเฉพาะโครงการจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม และส่งมอบงานภายในระยะเวลา 150 วัน (หนึ่งร้อยห้าสิบวัน) นับถัดจากวันลงนามในสัญญา

8. การส่งมอบงาน

ผู้ขายต้องส่งมอบงานการติดตั้งอุปกรณ์ให้พร้อมใช้งานภายในระยะเวลา 150 วันนับถัดจากวันลงนามในสัญญา โดยผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายในการติดตั้งและการฝึกอบรม ซึ่งมีรายละเอียดในการส่งมอบ ดังนี้

8.1 **งวดที่ 1** ส่งมอบงานภายใน 30 วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

8.1.1 แผนภาพรวมการบริหารงาน (Project Management Plan)

8.1.2 แผนการดำเนินงานและระยะเวลาในการดำเนินการ พร้อมขั้นตอนการดำเนินงาน

8.1.3 แผนการฝึกอบรม

8.1.4 แผนการออกแบบการเชื่อมต่ออุปกรณ์ทั้งหมดในโครงการฯ

8.2 **งวดที่ 2** ส่งมอบงานภายใน 60 วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

8.2.1 รายงานผลการตรวจนับและตรวจคุณสมบัติของอุปกรณ์หรือซอฟต์แวร์ทั้งหมดของโครงการ

8.2.2 รายงานออกแบบการเชื่อมต่ออุปกรณ์ทั้งหมดในโครงการฯ

8.2.3 ส่งเอกสารแสดงลิขสิทธิ์การใช้งาน (License) ที่ถูกต้องจากเจ้าของลิขสิทธิ์ของรายการที่ติดตั้งทั้งหมด

8.3 **งวดที่ 3** ส่งมอบงานภายใน 120 วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

8.3.1 รายงานการผลการติดตั้งอุปกรณ์หรือซอฟต์แวร์ที่ใช้ในโครงการตามข้อกำหนดเทคนิค

8.3.2 รายงานผลการทดสอบสภาวะการทำงานของอุปกรณ์ (Equipment Test)

8.3.3 รายงานผลการทดสอบการทำงานร่วมกับระบบสารสนเทศของสำนักงานประกันสังคม (System Integration Testing) ตามข้อ 5.5 และข้อ 5.6

8.4 **งวดที่ 4** ส่งมอบงานภายใน 150 วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

8.4.1 เอกสารคู่มือการใช้งานอุปกรณ์ (User Manual) คู่มือการดูแลอุปกรณ์ (Admin user manual) โดยจัดส่งในรูปแบบเอกสาร และไฟล์อิเล็กทรอนิกส์ จำนวนอย่างน้อย 1 ชุด

8.4.2 สิทธิการเข้าถึงทุกอุปกรณ์พร้อมรหัสผ่าน (Root Access) ของทุกอุปกรณ์ในโครงการฯ

8.4.3 รายงานการฝึกอบรมเจ้าหน้าที่ผู้เกี่ยวข้องที่ดูแลระบบของสำนักงานประกันสังคม

9. การรับประกัน การบำรุงรักษา และการซ่อมแซมแก้ไขอุปกรณ์ต่างๆ ในระบบดังนี้

9.1 ผู้ขายจะต้องรับประกันการชำรุดบกพร่องของอุปกรณ์ทุกชิ้นส่วน ซึ่งรวมถึงอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ทั้งหมดในโครงการเป็นเวลาอย่างน้อย 1 ปี นับถัดจากวันที่ผู้ซื้อรับมอบงานถูกต้องครบถ้วนตามสัญญาเรียบร้อยแล้ว หากครบระยะเวลา 1 ปีแล้ว แต่ยังไม่สิ้นปีปฏิทิน ผู้ขายจะต้องรับประกันต่อไปจนถึงวันที่ 31 ธันวาคมในปีปฏิทินนั้น ๆ

9.2 ในช่วงระยะเวลาของการรับประกัน หากอุปกรณ์ในโครงการดังกล่าวชำรุดหรือเกิดขัดข้อง ทั้งอุปกรณ์ฮาร์ดแวร์ หรือซอฟต์แวร์ หรืออุปกรณ์ที่ติดตั้งทั้งหมดเสียหายไม่สามารถใช้งานได้ตามปกติ ไม่ว่าจะเป็นกรณีปัญหาบางส่วนหรือทั้งระบบ ในเวลาสัปดาห์ละ 7 วัน วันละ 24 ชั่วโมง 7 x 24 (ของทุกวันไม่เว้นวันหยุดราชการ) ผู้ขายจะต้องจัดให้มีช่างที่มีความรู้ความชำนาญมาจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพที่ใช้งานได้ดีตามปกติ โดยต้องเข้ามาดำเนินการตรวจสอบ วิเคราะห์ และแก้ไขปัญหาของระบบและอุปกรณ์ให้แล้วเสร็จ และอยู่ในสภาพที่สามารถใช้งานได้ตามปกติ ดังนี้

9.2.1 อุปกรณ์ที่ติดตั้งใช้งาน ณ ศูนย์คอมพิวเตอร์หลัก จังหวัดนนทบุรี ภายใน 4 ชั่วโมง

9.2.2 อุปกรณ์ที่ติดตั้งใช้งาน ณ ศูนย์คอมพิวเตอร์สำรอง จังหวัดระยอง ภายใน 8 ชั่วโมง

นับตั้งแต่เวลาที่ได้รับแจ้งผ่านทางโทรสาร(FAX) หรือทางจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือแจ้งให้ทราบทางวาจาหรือทางโทรศัพท์ ไม่ว่าวิธีใดวิธีหนึ่ง เป็นเวลาเริ่มต้น เพื่อใช้ในการคำนวณ

ระยะเวลาในการเข้ามาดำเนินการแก้ไข หากผู้ขายไม่สามารถดำเนินการแก้ไขระบบและอุปกรณ์ให้สามารถใช้งานได้ตามปกติ ผู้ขายจะต้องจัดหาอุปกรณ์ที่มีประสิทธิภาพเทียบเท่าหรือดีกว่ามาทดแทนให้กับสำนักงานประกันสังคมใช้งานจนกว่าจะสามารถซ่อมแซมแก้ไขได้แล้วเสร็จ พร้อมทั้งแจ้งให้เจ้าหน้าที่ของสำนักงานประกันสังคมผู้มีหน้าที่รับผิดชอบทราบในทันที

9.3 กรณีที่ผู้ขายไม่สามารถเข้ามาดำเนินการได้ภายในเวลาที่กำหนดตามข้อ 9.2 ผู้ขายจะต้องยินยอมให้สำนักงานประกันสังคมคิดค่าปรับเป็นรายชั่วโมง โดยจำนวนชั่วโมงที่ใช้ในการคำนวณค่าปรับจะเริ่มต้นตั้งแต่เวลาที่เกินระยะเวลาที่กำหนดตามข้อ 9.2 จนกว่าผู้ขายจะดำเนินการแก้ไขให้แล้วเสร็จ หรือนำอุปกรณ์ที่มีประสิทธิภาพเทียบเท่าหรือดีกว่ามาให้ใช้ทดแทน

9.4 หากอุปกรณ์ที่ผู้ขายนำมาทดแทนไม่สามารถทำงานได้ ทางสำนักงานประกันสังคมจะคำนวณค่าปรับ โดยคำนวณนับต่อเนื่องจากเวลาที่สำนักงานประกันสังคมส่งใบรายการแจ้งอุปกรณ์/ระบบเสียหรือขัดข้องผ่านทางโทรสาร (FAX) หรือทางจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือแจ้งให้ทราบทางวาจาหรือทางโทรศัพท์ ไม่ว่าวิธีใดวิธีหนึ่ง

9.5 กรณีผู้ขายมีความจำเป็นต้องนำอุปกรณ์และอุปกรณ์สนับสนุนต่างๆ กลับไปซ่อม ผู้ขายจะต้องซ่อมแซมโดยใช้อะไหล่แท้ ที่เป็นของใหม่ และให้แล้วเสร็จภายในเวลาไม่เกิน 30 วัน นับถัดจากวันที่นำอุปกรณ์และอุปกรณ์สนับสนุนไปซ่อม และหากผู้ขายไม่สามารถซ่อมแซมอุปกรณ์ที่เสียหายให้แล้วเสร็จตามระยะเวลาที่กำหนดได้ ผู้ขายต้องทำการส่งมอบอุปกรณ์และทำหนังสือส่งมอบอุปกรณ์ที่นำมาทดแทน ให้เป็นทรัพย์สินของสำนักงานประกันสังคม ทั้งนี้หากผู้ขายไม่สามารถส่งมอบอุปกรณ์ทดแทนได้ หรือส่งมอบอุปกรณ์ที่มีคุณสมบัติไม่เทียบเท่าหรือไม่ดีกว่า สำนักงานประกันสังคมจะดำเนินการตามข้อ 10.2

9.6 กรณีที่ผู้ขายไม่ปฏิบัติตามสัญญาหรือข้อตกลงการรับประกันและก่อให้เกิดความเสียหายต่อการทำงานของสำนักงานประกันสังคม ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมดอันจะเกิดจากการที่สำนักงานประกันสังคมต้องดำเนินการแก้ไขปัญหาดังกล่าว

9.7 ผู้ขายจะต้องจัดเจ้าหน้าที่ผู้มีความชำนาญเข้าทำการตรวจสอบและบำรุงรักษา (Preventive Maintenance) ณ ที่ทำการติดตั้งอุปกรณ์ แบบ On-site โดยการตรวจสอบสภาพการทำงานของอุปกรณ์ต่างๆ ของอุปกรณ์ในโครงการฯ ทั้งในส่วนของฮาร์ดแวร์และ ซอฟต์แวร์ทุกๆ 3 เดือน ภายในระยะเวลาการรับประกัน และจัดทำรายงานการตรวจสอบและบำรุงรักษา (Preventive Maintenance) ทุกครั้ง การบำรุงรักษาแต่ละครั้งจะต้องมีเอกสารรายงานการบำรุงรักษา (Service Report) เป็นหลักฐาน และจัดทำ Logbook/Check list ของงานที่ทำการบำรุงรักษาเก็บเป็นเอกสารของแต่ละแห่งที่มีการติดตั้งใช้งานพร้อมกับรายงานประวัติการซ่อมบำรุงตลอดระยะเวลาเพื่อใช้อ้างถึงในกรณีที่มีข้อสงสัยเกี่ยวกับปัญหาที่เกิดขึ้น

9.8 การบำรุงรักษาแบบ Software Maintenance ครอบคลุมถึง License of Software Release upgrades หรือ License of Software version, Patches/Fixes, Software media, Document ตลอดระยะเวลาของสัญญานี้ สำนักงานประกันสังคมสามารถขอ Upgrade System Software และ Application Software ของระบบต่างๆ ที่สามารถทำงานบน Hardware เดิมได้ โดยไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม ตามสิทธิประโยชน์ที่สำนักงานประกันสังคมพึงมีได้ และไม่ขัดต่อมาตรฐานของผลิตภัณฑ์นั้นๆ ทั้งนี้ รวมถึง Software Subscription

9.9 กรณีที่สำนักงานประกันสังคมจำเป็นต้องปรับเปลี่ยนสถานที่และตำแหน่งที่ติดตั้งระบบอุปกรณ์หรือทำการเคลื่อนย้ายระบบหรืออุปกรณ์ ให้เป็นภาระรับผิดชอบของผู้ขายด้วย

10. การคิดค่าปรับ

10.1 กรณีส่งมอบไม่ถูกต้องครบถ้วน และกรณีติดตั้งไม่แล้วเสร็จตามกำหนดสัญญา

10.1.1 หากผู้ขายไม่ส่งมอบและติดตั้งบางรายการหรือทั้งหมดภายในกำหนดเวลา หรือส่งมอบไม่ตรงตามข้อกำหนด หรือมีคุณสมบัติไม่ถูกต้องตามข้อกำหนด หรือส่งมอบและติดตั้งแล้วเสร็จภายในกำหนดแต่ไม่สามารถใช้งานได้อย่างมีประสิทธิภาพ หรือใช้งานไม่ได้ครบถ้วนตามข้อกำหนด หรือผู้ขายไม่ปฏิบัติตามข้อกำหนดข้อใดข้อหนึ่ง ผู้ซื้อมีสิทธิที่จะไม่รับอุปกรณ์ต่างๆ ในระบบนั้น และถือว่าอุปกรณ์ต่างๆ ในระบบดังกล่าวยังไม่ส่งมอบ ซึ่งผู้ซื้อมีสิทธิที่จะใช้งานอุปกรณ์ต่างๆ ในระบบที่ส่งมอบแต่ไม่ถูกต้องครบถ้วนได้ โดยไม่เสียค่าใช้จ่าย โดยผู้ขายจะต้องชำระค่าปรับให้ผู้ซื้อ เป็นรายวันในอัตราร้อยละ 0.20 (ศูนย์จุดสองศูนย์) ของราคาตามสัญญา นับถัดจากวันครบกำหนดตามข้อกำหนด จนถึงวันที่ผู้ขายได้นำอุปกรณ์มาส่งมอบและติดตั้งให้แก่ผู้ซื้อจนถูกต้องครบถ้วนตามข้อกำหนด ในกรณีนี้ผู้ขายต้องรีบนำอุปกรณ์นั้นกลับคืนโดยเร็วที่สุดเท่าที่จะทำได้และนำอุปกรณ์มาส่งมอบให้ใหม่ หรือต้องทำการแก้ไขให้ถูกต้องตามสัญญาด้วยค่าใช้จ่ายของผู้ขายเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าวผู้ขายจะนำมาอ้างเป็นเหตุขอขยายเวลาทำการตามสัญญาหรือของดหรือลดค่าปรับไม่ได้

10.1.2 หากการส่งมอบดังกล่าวไม่ครบถ้วน ไม่สามารถใช้งานได้ ไม่แล้วเสร็จทันตามกำหนด ผู้ซื้อมีสิทธิเรียกค่าเสียหายใดๆ อันเนื่องมาจากผู้ขายไม่ปฏิบัติตามสัญญานี้ และถ้าผู้ซื้อจัดซื้ออุปกรณ์รวมถึงการติดตั้งจากบุคคลอื่นเต็มจำนวนหรือเฉพาะจำนวนที่ขาดส่ง แล้วแต่กรณี ผู้ขายจะต้องชดใช้ราคาที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญานี้ด้วย รวมทั้งค่าใช้จ่ายใดๆ ที่ผู้ซื้อต้องใช้จ่ายในการจัดหาผู้ขายรายใหม่ดังกล่าวด้วย

10.1.3 หากผู้ซื้อเห็นว่าผู้ขายไม่อาจปฏิบัติตามสัญญาต่อไปได้ ผู้ซื้อจะใช้สิทธิบอกเลิกสัญญา และริบหรือบังคับจากหลักประกัน กับเรียกร้องให้ชดใช้ราคาที่เพิ่มขึ้นตามที่กำหนดไว้ในข้อ 10.1.2 ก็ได้ และถ้าผู้ซื้อได้แจ้งข้อเรียกร้องให้ชำระค่าปรับไปยังผู้ขายเมื่อครบกำหนดส่งมอบแล้ว ผู้ซื้อมีสิทธิที่จะปรับผู้ขายจนถึงวันบอกเลิกสัญญาได้อีกด้วย

10.2 กรณีอุปกรณ์ต่างๆ ในระบบขัดข้องในช่วงระยะเวลารับประกัน ดังนี้

10.2.1 กรณีที่สามารถซ่อมแซมได้ภายในเวลาที่กำหนดในข้อ 9.2 ให้มีเวลาอุปกรณ์ต่างๆ ในระบบขัดข้องรวมตามเกณฑ์การคำนวณนับไม่เกินเดือนละ 36 ชั่วโมง หรือร้อยละ 5 ของเวลาใช้งานทั้งหมดของอุปกรณ์ต่างๆ ในระบบแล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้ขายจะต้องยอมให้สำนักงานประกันสังคมคิดค่าปรับเวลาที่ไม่สามารถใช้งานอุปกรณ์ต่างๆ ในระบบในส่วนที่เกินกำหนดข้างต้น เป็นรายชั่วโมงในอัตราร้อยละ 0.035 (ศูนย์จุดศูนย์สามห้า) ของราคาตามสัญญาต่อชั่วโมง เศษของชั่วโมงให้ปรับเป็นหนึ่งชั่วโมง

10.2.2 ในกรณีที่ไม่สามารถซ่อมแซมได้ภายในเวลาที่กำหนดในข้อ 9.2 ผู้ขายจะต้องยอมให้สำนักงานประกันสังคมคิดค่าปรับเวลาที่ไม่สามารถใช้อุปกรณ์ต่างๆ ในระบบ ในส่วนที่เกินกำหนดเวลาข้างต้น เป็นรายชั่วโมงในอัตราร้อยละ 0.035 (ศูนย์จุดศูนย์สามห้า) ของราคาตามสัญญาต่อชั่วโมง เศษของชั่วโมงให้ปรับเป็นหนึ่งชั่วโมง เวลาที่ถูกปรับแล้วจะไม่นำไปรวมคิดค่าปรับตามกรณี ข้อ 10.2.1 อีก

10.2.3 สำนักงานประกันสังคมสงวนสิทธิที่จะยึดหลักค้ำประกันสัญญา ในกรณีที่ผู้ขายไม่ปฏิบัติตามสัญญาหรือข้อตกลง หรือกระทำให้เกิดความเสียหายต่ออุปกรณ์ต่างๆ ในระบบของสำนักงานประกันสังคม หากสำนักงานประกันสังคมพิจารณาแล้วว่าเกิดความเสียหายจริง ทั้งนี้ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมด อันจะเกิดจากการที่สำนักงานประกันสังคมต้องดำเนินการแก้ไขปัญหา หรือจัดหาอะไหล่ หรือจัดหาอุปกรณ์ต่างๆ ในระบบใหม่ทดแทน

11. ในระหว่างการดำเนินการ หากผู้ขายทำให้อุปกรณ์ต่างๆ ของสำนักงานประกันสังคม ชำรุดเสียหายหรือทำให้สถานที่ส่วนใดส่วนหนึ่งของอาคารชำรุดเสียหาย ผู้ขายจะต้องแก้ไขปรับปรุงหรือทำขึ้นใหม่ให้คงเดิมและใช้งานได้ตามปกติ และผู้ขายเป็นผู้รับภาระค่าใช้จ่ายเองทั้งหมด

12. การดำเนินการใดๆ ไม่ว่าจะเป็นส่วนของฮาร์ดแวร์และซอฟต์แวร์ที่ผู้ขายเสนอ หากมีปัญหาเกี่ยวกับลิขสิทธิ์ ผู้ขายจะต้องดำเนินการขออนุญาต ทำการตกลงอย่างอื่นอย่างใดกับบุคคลผู้เป็นเจ้าของลิขสิทธิ์เพื่อให้สามารถใช้ลิขสิทธิ์นั้นๆ ได้อย่างถูกต้องตามกฎหมาย โดยให้ถือเป็นภาระหน้าที่ของผู้ขายเพียงฝ่ายเดียวและเป็นผู้รับภาระค่าใช้จ่ายเองทั้งหมด

13. ลิขสิทธิ์และข้อตกลงในการรักษาความลับของข้อมูลหรือเอกสาร

13.1 การรักษาความลับ ให้มีผลนับแต่วันที่ทำสัญญานี้ และมีผลอยู่ตลอดไป แม้ว่าสัญญานี้ครบกำหนดระยะเวลา หรือสิ้นสุดลงไม่ว่าด้วยเหตุใดๆ

13.2 ผู้ขายจะต้องรักษาความลับข้อมูลตลอดระยะเวลาสัญญา และหลังจากเสร็จสิ้นสัญญา โดยข้อมูลทั้งหมดซึ่งผู้ขายได้รับรู้เนื่องจากปฏิบัติงานตามสัญญาให้ถือเป็นความลับที่ผู้ขายจะต้องไม่นำไปเปิดเผยแก่ผู้อื่นเป็นอันขาด รวมถึงการควบคุมดูแลเจ้าหน้าที่ของผู้รับจ้างไม่ให้เผยแพร่หรือเปิดเผยข้อมูลแก่ผู้อื่น หากผู้ขายละเมิดข้อตกลงนี้ สำนักงานประกันสังคมมีสิทธิดำเนินการทางกฎหมายแก่ผู้ขายได้

13.3 หากผู้ขายนำข้อมูลของสำนักงานประกันสังคม ไปเผยแพร่หรือเปิดเผยโดยไม่ได้รับอนุญาตจากสำนักงานประกันสังคมหรือเปิดเผยข้อมูลของสำนักงานประกันสังคม ด้วยความประมาท เลินเล่อ สำนักงานประกันสังคมมีสิทธิดำเนินการทางกฎหมายแก่ผู้ขายได้

13.4 ระบบงานและเอกสารทั้งหมดที่จัดทำขึ้น ถือเป็นลิขสิทธิ์ของสำนักงานประกันสังคม โดยผู้ขายจะต้องไม่เผยแพร่ข้อมูล เอกสาร หรืออื่นๆ ที่จัดทำขึ้นเกี่ยวกับระบบงาน โดยไม่ได้รับความเห็นชอบอย่างเป็นลายลักษณ์อักษรจากสำนักงานประกันสังคม รวมทั้งจะต้องไม่แสวงหาหรือยินยอมให้บุคคลอื่นแสวงหาประโยชน์ใดๆ จากข้อมูลเอกสารดังกล่าว ทั้งในทางพาณิชย์หรือในกรณีอื่นอันอาจก่อให้เกิดความเสียหายแก่สำนักงานประกันสังคมด้วยประการใดทั้งสิ้น

13.5 การเข้าปฏิบัติงานของผู้ขาย จะต้องเป็นไปตามนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยต้องมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยในข้อมูลและทรัพย์สินของสำนักงานประกันสังคมและรับผิดชอบต่อการบริหารจัดการด้านความมั่นคงปลอดภัยข้อมูล หากผู้ขายพบเจอเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นกับข้อมูล และทรัพย์สินของสำนักงานประกันสังคม ต้องแจ้งหน่วยงานของสำนักงานประกันสังคมที่ควบคุมดูแลการดำเนินงานโครงการให้ทราบทันที

13.6 การรักษาความลับของข้อมูลใดๆ ผู้ขายต้องยินยอมลงนามในข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) รายละเอียดตามภาคผนวก ก

14. หลักเกณฑ์ในการพิจารณา

สำนักงานประกันสังคมจะพิจารณาโดยใช้เกณฑ์ราคา จากผู้ยื่นข้อเสนอที่เสนอราคารวมต่ำสุด

15. วงเงินงบประมาณในการจัดหา

งบประมาณ 135,000,000 บาท (หนึ่งร้อยสามสิบห้าล้านบาทถ้วน) ซึ่งเป็นราคารวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

16. เงื่อนไขการจ่ายเงิน

สำนักงานประกันสังคมจะทำการชำระเงินตามระเบียบพัสดุ ระเบียบการจ่ายเงินของสำนักงานประกันสังคม และผ่านการตรวจรับและเห็นชอบจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว โดยจะทำการจ่ายเงินเป็นจำนวน 4 งวด ดังนี้

งวดที่ 1 จ่ายเงินร้อยละ 5 ของวงเงินตามสัญญา เมื่อได้ส่งมอบงานตามข้อ 8.1

งวดที่ 2 จ่ายเงินร้อยละ 35 ของวงเงินตามสัญญา เมื่อได้ส่งมอบงานตามข้อ 8.2

งวดที่ 3 จ่ายเงินร้อยละ 35 ของวงเงินตามสัญญา เมื่อได้ส่งมอบงานตามข้อ 8.3

งวดที่ 4 จ่ายเงินร้อยละ 25 ของวงเงินตามสัญญา เมื่อได้ส่งมอบงานตามข้อ 8.4

17. สถานที่/พื้นที่ดำเนินการ

ศูนย์คอมพิวเตอร์หลัก (จังหวัดนนทบุรี) และศูนย์คอมพิวเตอร์สำรอง (จังหวัดระยอง) สำนักงานประกันสังคม

18. ติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่

หน่วยงาน : สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม

โทรศัพท์ : 0-2956-2371

โทรสาร : 0-2527-7843

E-mail Address : thanakorn.c@sso.go.th และ potjanee.k@sso.go.th

ภาคผนวก ก

หนังสือแสดงเจตนาไม่เปิดเผยข้อมูลของสำนักงานประกันสังคม

เขียนที่ .....

วันที่ .....

ข้าพเจ้า (นาย,นาง,นางสาว) .....เลขที่บัตรประจำตัวประชาชน .....ทำงานในตำแหน่ง..... ของบริษัท.....อันเป็นบริษัทเอกชนซึ่งเข้ามาดำเนินโครงการจัดหาระบบบริหารจัดการด้านความปลอดภัยฐานข้อมูลของสำนักงานประกันสังคม ขอแสดงเจตนาไม่เปิดเผยข้อมูลต่อสำนักงานประกันสังคมไว้ดังต่อไปนี้

ข้อ 1. ข้าพเจ้าฯ จะไม่เปิดเผยหรือเผยแพร่ข้อมูลต่าง ๆ รายละเอียดทางเทคนิค โปรแกรมคอมพิวเตอร์ เอกสารหรือวัสดุใด ๆ ไม่ว่าอยู่ในรูปแบบใดของสำนักงานประกันสังคม อันข้าพเจ้าได้รับมาเนื่องจากการที่ได้เข้ามาปฏิบัติงานในสำนักงานประกันสังคม โดยจะรักษาไว้เป็นความลับ

ข้อ 2. ข้าพเจ้าฯ จะไม่กระทำหรือร่วมกับบุคคลอื่นใดกระทำการคัดลอก เลียนแบบ สำเนาบันทึกดัดแปลง ไม่ว่าโดยวิธีใดๆ เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจากสำนักงานประกันสังคม

ข้อ 3. หากข้าพเจ้าฯ ได้ฝ่าฝืนตามข้อ 1. และข้อ 2. รวมทั้งบุคคลอื่นใด ซึ่งได้ทราบข้อมูลของสำนักงานประกันสังคมจากข้าพเจ้าฯ โดยมิชอบ ได้ฝ่าฝืนตามข้อ 1. และข้อ 2. ข้าพเจ้าฯ ยินยอมรับผิดตามกฎหมายทั้งคดีแพ่งและคดีอาญา

ข้อ 4. หนังสือฉบับนี้ ให้มีผลตั้งแต่วันนี้เป็นต้นไป และมีผลตลอดไปไม่ว่าด้วยเหตุใด

ข้าพเจ้าฯ ได้อ่านและเข้าใจข้อความข้างต้นแล้ว จึงลงลายมือชื่อไว้เป็นหลักฐานพร้อมมอบให้แก่สำนักงานประกันสังคม

..... ผู้ยินยอมตกลง

(.....)

..... พยาน

(.....)

..... พยาน

(.....)