ขอบเขตงาน (Term of Reference)
โครงการจ้างบริการประเมินความปลอดภัยสารสนเทศ (IT Audit)

1. หลักการและเหตุผล

การยาสูบแห่งประเทศไทย มีวิสัยทัศน์ที่จะ “เป็นผู้นำในธุรกิจยาสูบในประเทศ” โดยมีพันธกิจ ที่จะรักษาส่วนแบ่งตลาดยาสูบไทย ขยายสู่ตลาดต่างประเทศ ด้วยผลิตภัณฑ์คุณภาพ พร้อมพัฒนาธุรกิจ เพื่อการเติบโตอย่างยั่งยืน โดยการที่จะทำให้บรรลุพันธกิจ การยาสูบแห่งประเทศไทยต้องมีการนำระบบสารสนเทศมาใช้ในองค์กรให้เกิดประสิทธิภาพและสนับสนุนพันธกิจให้ลุล่วงไปด้วยดี อย่างไรก็ตามจากสถานการณ์โรคระบาดปัจจุบันทำให้เกิดการทำงานแบบ work from home มากขึ้น ภัยคุกคามทางไซเบอร์ก็เพิ่มมากขึ้นเช่นกัน ประกอบกับกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่จะมีผลบังคับใช้ในปี 2565 ทำให้การยาสูบแห่งประเทศไทยต้องมีการประเมินความปลอดภัยของระบบสารสนเทศต่อภัยคุกคามทางไซเบอร์เพื่อเตรียมความพร้อมของระบบสารสนเทศสำหรับภัยไซเบอร์ที่เพิ่มมากขึ้นและพ.ร.บ.ฯ ที่กำลังจะประกาศใช้

โครงการจัดจ้างการประเมินความปลอดภัยสารสนเทศ เป็นหนึ่งในโครงการเสริมศักยภาพของระบบสารสนเทศที่จะช่วยให้ การยาสูบแห่งประเทศไทย สามารถให้บริการระบบสารสนเทศแก่บุคคลากรภายในและบุคคลภายนอกได้อย่างปลอดภัย

2. วัตถุประสงค์

โครงการจัดจ้างบริการประเมินความความปลอดภัยสารสนเทศ มีวัตถุประสงค์ในการจัดทำโครงการ ดังนี้

2.1 เพื่อตรวจสอบสถานะของความมั่นคงปลอดภัยของระบบสารสนเทศ

2.2 เพื่อกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างรูปธรรมและสอดคล้องกับสภาวะภัยคุกคามทางไซเบอร์ในปัจจุบัน

2.3 เพื่อตรวจสอบการตั้งค่าของระบบอุปกรณ์ด้านความปลอดภัยสารสนเทศว่ามีความเหมาะสมหรือไม่

2.4 เพื่อสร้างกระบวนการตรวจสอบสถานะความมั่นคงปลอดภัยทางไซเบอร์อย่างถูกต้องให้กับองค์กร

2.5 เพื่อสร้างความตระหนักให้กับบุคลากรถึงภัยคุกคามทางไซเบอร์

2.6 เพื่อสร้างความเชื่อมั่นให้กับการให้บริการของระบบสารสนเทศให้ทั้งบุคคลภายนอกและภายในองค์กร

3. รายละเอียดขอบเขตงาน

จ้างบริการพร้อมประเมินความปลอดภัยสารสนเทศโดยต้องดำเนินการให้คำแนะนำ พร้อมบริการประเมินความเสี่ยงระบบสารสนเทศ เพื่อให้โครงการจ้างบริการประเมินความมั่นคงปลอดภัยระบบสารสนเทศสามารถบรรลุตามวัตถุประสงค์ที่ตั้งไว้ของการยาสูบแห่งประเทศไทย ผู้รับจ้างจะต้องดำเนินโครงการฯ ตามรายละเอียดอย่างน้อย ดังต่อไปนี้

3.1. ศึกษาวิเคราะห์ระบบเครือข่ายสารสนเทศของการยาสูบแห่งประเทศไทย และจัดทำแผนดำเนินโครงการ (Project Plan) โดยต้องเสนอให้การยาสูบแห่งประเทศไทย เห็นชอบก่อนดำเนินงานในขั้นต่อไป

3.2. ก่อนเข้าดำเนินการในแต่ละครั้ง ต้องแจ้งแผนการเข้าดำเนินงาน รายละเอียดการดำเนินการ เครื่องมือที่ใช้ โปรแกรมที่เกี่ยวข้อง และวิธีการทดสอบ รวมถึงการประเมินผลกระทบที่อาจมีขึ้น เพื่อป้องกันไม่ให้เกิดความเสียหายต่อระบบที่ทดสอบ ให้การยาสูบแห่งประเทศไทยทราบล่วงหน้าอย่างน้อย 5 วันทำการ และจะดำเนินการได้หลังจากที่ได้รับความเห็นชอบจากการยาสูบแห่งประเทศไทย

3.3. ดำเนินการสืบหาข้อมูลที่เกี่ยวข้องกับองค์กรผ่าน Open Source Intelligence (OSINT) และ Threat Intelligence

3.4. การดำเนินการทดสอบเจาะระบบจะต้องใช้วิธีการที่เป็นไปตามมาตรฐาน ดังต่อไปนี้อย่างน้อย 1 มาตรฐาน ดังต่อไปนี้

3.4.1. Opensource Security Testing Methodology (OSSTM)

3.4.2. NIST SP800-115 Guideline on Network Security Testing

3.4.3. Open Web Application Security Project (OWASP) TOP 10

3.5. ดำเนินการทดสอบเจาะระบบเครือข่ายเทคโนโลยีสารสนเทศของการยาสูบแห่งประเทศไทย จากเครือข่ายภายนอก (External Infrastructure Penetration test) แบบ Black-box Test จำนวน 60 หมายเลขไอพี (IP Address) ดังนี้

3.5.1. ดำเนินการทดสอบเจาะระบบจากเครือข่ายภายนอกการยาสูบแห่งประเทศไทย และหลังทำการปิดช่องโหว่แล้ว ให้ดำเนินการทดสอบซ้ำ (Re-visit) จำนวน 1 ครั้ง

3.5.2. ดำเนินการทดสอบเจาะระบบด้วยวิธีการที่เป็นไปตามมาตรฐาน อย่างน้อย 1 มาตรฐาน ดังต่อไปนี้

3.5.2.1. Opensource Security Testing Methodology (OSSTM)

3.5.2.2. NIST SP800-115 Guideline on Network Security Testing

3.5.3. ดำเนินการทดสอบเจาะระบบจากเครือข่ายภายนอกการยาสูบแห่งประเทศไทย ในการทดสอบจะดำเนินการเหมือนกับการเจาะระบบโดยไวรัสหรือแฮกเกอร์ที่ปฏิบัติการจริง โดยทำการตรวจการเข้าถึงระบบจากเครือข่ายภายนอก (External Infrastructure Reconnaissance) การยาสูบแห่งประเทศไทย และทดสอบหาช่องทางในการเข้าถึงระบบ (Exploit) ผ่านช่องโหว่ต่างๆเพื่อมุ่งเจาะระบบ

3.5.4. ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว)

3.5.5. ระหว่างการเจาะระบบหากเกิดความผิดปกติของระบบที่ทำการทดสอบ จะต้องรีบแจ้งให้เจ้าหน้าที่ของการยาสูบแห่งประเทศไทย ทราบทันทีและต้องดำเนินการแก้ไขความผิดปกติให้เรียบร้อยโดยเร็ว

3.5.6. จัดทำรายงานสรุปช่องโหว่และผลการทดสอบอย่างละเอียด โดยรายงานจะต้องประกอบไปด้วยอย่างน้อย ดังนี้

1) บทสรุปผู้บริหาร
2) วิธีการและขั้นตอนการทดสอบ
3) รายละเอียดช่องโหว่ พร้อมประเมินความรุนแรงของช่องโหว่
4) คำแนะนำในการปิดช่องโหว่

3.5.7. จัดประชุมเพื่อนำเสนอผลการทดสอบ ต่อการยาสูบแห่งประเทศไทยดังต่อนี้

1) นำเสนอรายงานสรุปช่องโหว่ในหัวข้อ 3.5.6
2) ในกรณีระหว่างการทำการเจาะระบบแล้วเกิดเหตุการณ์ผิดปกติของระบบเกิดขึ้น ให้ผู้ทดสอบระบบนำเสนอข้อมูลเหตุการณ์ของความผิดปกติในที่ประชุม

3.5.8. ทำการทดสอบซ้ำหลังจากมีการปิดช่องโหว่แล้ว (Revisit) ภายใน 60 วันหลังจากการส่งรายงานตามข้อ 3.5.6

1) ผู้รับจ้างต้องรับผิดชอบในการแนะนำแนวทางการปิดช่องโหว่ให้กับผู้ดูแลและผู้พัฒนาระบบของการยาสูบแห่งประเทศไทย ภายหลังจากการทดสอบการเจาะระบบ
2) เจ้าหน้าที่ของการยาสูบแห่งประเทศไทย จะเป็นผู้ดำเนินการปิดช่องโหว่ที่ค้นพบตามคำแนะนำและวิธีการตามที่ผู้รับจ้างได้นำเสนอ โดยต้องให้คำปรึกษาจนดำเนินการแล้วเสร็จ ยกเว้นช่องโหว่ดังกล่าวเป็นข้อจำกัดของอุปกรณ์ฯ หรือระบบของการยาสูบแห่งประเทศไทย หรือตามที่คณะกรรมการฯ พิจารณาแล้วเห็นสมควร
3) หลังจากที่การยาสูบแห่งประเทศไทย ดำเนินการปิดช่องโหว่แล้ว ผู้รับจ้างต้องดำเนินการตรวจสอบผลการดำเนินการปิดช่องโหว่หรือจุดอ่อน (Retest) เพื่อยืนยันช่องโหว่ที่พบว่าได้รับการแก้ไขแล้ว

3.6. ดำเนินการทดสอบเจาะระบบเว็บแอพพลิเคชัน (Web Application Penetration Test) ของการยาสูบแห่งประเทศไทย แบบ Black-box Test และ Grey-box Test จำนวนไม่น้อยกว่า 3 เว็บแอพพลิเคชั่น ดังนี้

3.6.1. ดำเนินการทดสอบเจาะระบบเว็บแอพพลิเคชันและหลังจากทำการปิดช่องโหว่แล้ว ให้ดำเนินการทดสอบซ้ำ (Re-visit) จำนวน 1 ครั้ง

3.6.2. ทดสอบเจาะระบบเว็บแอพพลิเคชันทั้งแบบ Black-box Test และ Grey-box Test ให้ดำเนินการโดยอ้างอิงตาม Open Web Application Security Project (OWASP) Testing guide

3.6.3. ดำเนินการทดสอบเจาะระบบเว็บแอพพลิเคชันแบบ Black-box Test ในการทดสอบจะดำเนินการเหมือนกับการเจาะระบบโดยไวรัสหรือแฮกเกอร์ที่ปฏิบัติการจริง โดยทำการตรวจ

การเข้าถึงระบบจากเครือข่ายภายนอก (External Infrastructure Reconnaissance) การยาสูบแห่งประเทศไทย และทดสอบหาช่องทางในการเข้าถึงระบบ (Exploit) ผ่านช่องโหว่ต่างๆ

3.6.4. ดำเนินการทดสอบเจาะระบบเว็บแอพพลิเคชันแบบ Grey-box Test โดยการยาสูบแห่งประเทศไทย จะเตรียมข้อมูลให้บางส่วนในการเข้าถึง ผู้รับจ้างจะต้องดำเนินการค้นหาช่องโหว่ในทุกๆหน้า ทุกๆฟังก์ชันของระบบเป้าหมาย โดยจะต้องค้นหาช่องโหว่ทั้งด้านเทคนิคและช่องโหว่ด้าน Business Logic

3.6.5. ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว)

3.6.6. ระหว่างการเจาะระบบหากเกิดความผิดปกติของระบบที่ทำการทดสอบ จะต้องรีบแจ้งให้เจ้าหน้าที่ของการยาสูบแห่งประเทศไทย ทราบทันทีและต้องดำเนินการแก้ไขความผิดปกติให้เรียบร้อยโดยเร็ว

3.6.7. จัดทำรายงานสรุปช่องโหว่และผลการทดสอบอย่างละเอียด โดยรายงานจะต้องประกอบไปด้วยอย่างน้อย ดังนี้

1) บทสรุปผู้บริหาร
2) วิธีการและขั้นตอนการทดสอบ
3) รายละเอียดช่องโหว่ พร้อมประเมินความรุนแรงของช่องโหว่
4) คำแนะนำในการปิดช่องโหว่

3.6.8. จัดประชุมเพื่อนำเสนอผลการทดสอบต่อการยาสูบแห่งประเทศไทย

1) นำเสนอรายงานสรุปช่องโหว่ในหัวข้อ 3.6.7
2) ในกรณีระหว่างการทำการเจาะระบบแล้วเกิดเหตุการณ์ผิดปกติของระบบเกิดขึ้น ให้ผู้ทดสอบระบบนำเสนอข้อมูลเหตุการณ์ของความผิดปกติในที่ประชุม

3.6.9. ทำการทดสอบซ้ำหลังจากมีการปิดช่องโหว่แล้ว (Revisit) ภายใน 60 วันหลังจากการส่งรายงานตามข้อ 3.6.7

1) ผู้รับจ้างต้องรับผิดชอบในการแนะนำแนวทางการปิดช่องโหว่ให้กับผู้ดูแลและผู้พัฒนาระบบของการยาสูบแห่งประเทศไทย ภายหลังจากการทดสอบการเจาะระบบ
2) เจ้าหน้าที่ของการยาสูบแห่งประเทศไทย จะเป็นผู้ดำเนินการปิดช่องโหว่ที่ค้นพบตามคำแนะนำและวิธีการตามที่ผู้รับจ้างได้นำเสนอ โดยต้องให้คำปรึกษาจนดำเนินการแล้วเสร็จ ยกเว้นช่องโหว่ดังกล่าวเป็นข้อจำกัดของอุปกรณ์ฯ หรือระบบของการยาสูบแห่งประเทศไทย หรือตามที่คณะกรรมการฯ พิจารณาแล้วเห็นสมควร

3) หลังจากที่การยาสูบแห่งประเทศไทย ดำเนินการปิดช่องโหว่แล้ว ผู้รับจ้างต้องดำเนินการตรวจสอบผลการดำเนินการปิดช่องโหว่หรือจุดอ่อน (Retest) เพื่อยืนยันช่องโหว่ที่พบว่าได้รับการแก้ไขแล้ว

3.7. ดำเนินการทดสอบเจาะระบบเครือข่ายเทคโนโลยีสารสนเทศของการยาสูบแห่งประเทศไทย จากเครือข่ายภายใน (Internal Infrastructure Penetration test) แบบ Grey-box Test ผ่านระบบ VPN ของการยาสูบแห่งประเทศไทย จำนวน 3 หมายเลขไอพี (IP Address) ดังนี้

3.7.1. ดำเนินการทดสอบเจาะระบบจากเครือข่ายภายในการยาสูบแห่งประเทศไทย และหลังจากทำการปิดช่องโหว่แล้วให้ดำเนินการทดสอบซ้ำ (Re-visit) จำนวน 1 ครั้ง

3.7.2. ดำเนินการทดสอบเจาะระบบจากเครือข่ายภายในการยาสูบแห่งประเทศไทย แบบ Grey-box Test ให้ดำเนินการโดยอ้างอิงตามมาตรฐาน อย่างน้อย 1 มาตรฐาน ดังต่อไปนี้ ซึ่งการยาสูบแห่งประเทศไทย จะเตรียมข้อมูลให้บางส่วนในการเข้าถึง

3.7.2.1. Opensource Security Testing Methodology (OSSTM)

3.7.2.2. NIST SP800-115 Guideline on Network Security Testing

3.7.3. ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว)

3.7.4. ระหว่างการเจาะระบบหากเกิดความผิดปกติของระบบที่ทำการทดสอบ จะต้องรีบแจ้งให้เจ้าหน้าที่ของการยาสูบแห่งประเทศไทย ทราบทันทีและต้องดำเนินการแก้ไขความผิดปกติให้เรียบร้อยโดยเร็ว

3.7.5. จัดทำรายงานสรุปช่องโหว่และผลการทดสอบอย่างละเอียด โดยรายงานจะต้องประกอบไปด้วยอย่างน้อย ดังนี้

1) บทสรุปสำหรับผู้บริหาร
2) วิธีการและขั้นตอนการดำเนินการ
3) รายละเอียดช่องโหว่ พร้อมประเมินความรุนแรงของช่องโหว่
4) คำแนะนำในการปิดช่องโหว่

3.7.6. จัดประชุมเพื่อนำเสนอผลการทดสอบต่อการยาสูบแห่งประเทศไทย

1) นำเสนอรายงานสรุปช่องโหว่ในหัวข้อ 3.7.5
2) ในกรณีระหว่างการทำการเจาะระบบแล้วเกิดเหตุการณ์ผิดปกติของระบบเกิดขึ้น ให้ผู้ทดสอบระบบนำเสนอข้อมูลเหตุการณ์ของความผิดปกติในที่ประชุม

3.7.7. ทำการทดสอบซ้ำหลังจากมีการปิดช่องโหว่แล้ว (Revisit) ภายใน 60 วันหลังจากการส่งรายงานตามข้อ 3.7.5

1) ผู้รับจ้างต้องรับผิดชอบในการแนะนำแนวทางการปิดช่องโหว่ให้กับผู้ดูแลและผู้พัฒนาระบบของการยาสูบแห่งประเทศไทย ภายหลังจากการทดสอบการเจาะระบบ
2) เจ้าหน้าที่ของการยาสูบแห่งประเทศไทย จะเป็นผู้ดำเนินการปิดช่องโหว่ที่ค้นพบตามคำแนะนำและวิธีการตามที่ผู้รับจ้างได้นำเสนอ โดยต้องให้คำปรึกษาจนดำเนินการแล้วเสร็จ ยกเว้นช่องโหว่ดังกล่าวเป็นข้อจำกัดของอุปกรณ์ฯ หรือระบบของการยาสูบแห่งประเทศไทย หรือตามที่คณะกรรมการฯ พิจารณาแล้วเห็นสมควร
3) หลังจากที่การยาสูบแห่งประเทศไทย ดำเนินการปิดช่องโหว่แล้ว ผู้รับจ้างต้องดำเนินการตรวจสอบผลการดำเนินการปิดช่องโหว่หรือจุดอ่อน (Retest) เพื่อยืนยันช่องโหว่ที่พบว่าได้รับการแก้ไขแล้ว

3.8. ดำเนินการตรวจประเมินค้นหาภัยคุกคามของระบบสารสนเทศภายในของ การยาสูบแห่งประเทศไทย (Compromised Assessment หรือ Vulnerability assessment) จำนวน 1 ครั้ง จากเครือข่ายภายใน (Internal Infrastructure Penetration test) แบบ Black-box Test ไม่น้อยกว่า 10 หมายเลขไอพี (IP Address)

3.9. ดำเนินการทดสอบหลอกลวงผู้ปฏิบัติงาน (Phishing) 1 ครั้ง ดังนี้

3.9.1. ต้องนำเสนอรายละเอียดรูปแบบการทดสอบเพื่อให้การยาสูบแห่งประเทศไทย เห็นชอบก่อนการทดสอบทุกครั้ง

3.9.2. จัดทำและนำเสนอรายงานผลการทดสอบ สรุปความตระหนักของผู้ปฏิบัติงานและผู้บริหาร พร้อมข้อเสนอแนะแก่การยาสูบแห่งประเทศไทย

3.10. ต้องจัดให้มีการประชุมเพื่อรายงานผลและความคืบหน้าของโครงการต่อบริษัทฯ เป็นระยะเวลาที่ชัดเจนอย่างต่อเนื่องจนกระทั่งสิ้นสุดสัญญา

3.11. ต้องนำเสนอรายงานผลการดำเนินการ รายละเอียดช่องโหว่หรือจุดอ่อนที่พบ รวมถึงปริมาณช่องโหว่ของระบบ ความเสี่ยงที่พบ และผลกระทบที่อาจเกิดขึ้นอย่างละเอียดพร้อมแนวทางการแก้ไข รวมถึงเวลาโดยประมาณในการแก้ไขต่อการยาสูบแห่งประเทศไทย

3.12. ต้องรวบรวมและจัดทำรายงานการทดสอบเจาะระบบทั้งก่อนและหลังการแก้ไข รวมถึงบทวิเคราะห์คำแนะนำการแก้ไขและบทสรุปผู้บริหาร โดยจัดทำเป็นเอกสารพร้อมส่งทั้งแบบ Hardcopy และ Softcopy เพื่อนำเสนอผู้บริหารของการยาสูบแห่งประเทศไทย

3.13. การดำเนินงานของผู้รับจ้างต้องไม่ส่งผลกระทบหรือสร้างความเสียหายต่อระบบงานของการยาสูบแห่งประเทศไทย หากมีความเสียหายใดๆอันเกิดจากการดำเนินการของผู้รับจ้าง จะต้องรายงานให้การยาสูบแห่งประเทศไทย ทราบทันที และจะต้องเป็นผู้รับผิดชอบต่อความเสียหายนั้นรวมถึงจะต้องทำให้ระบบงานที่เสียหาย หรือได้รับผลกระทบนั้น กลับมาใช้งานได้เป็นปกติดังเดิมภายในระยะเวลาอันรวดเร็ว โดยไม่มีค่าใช้จ่ายใดๆทั้งสิ้น

3.14. ซอฟต์แวร์ทุกประเภทที่ผู้รับจ้างนำมาใช้ต้องไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมุ่งร้าย

3.15. ใช้เอกสารข้อมูล เครื่องมือ ฮาร์ดแวร์และซอฟท์แวร์ต่างๆ ในการดำเนินการอย่างถูกต้องตามกฎหมาย ไม่ละเมิดลิขสิทธิ์หรือสิทธิบัตรของผู้อื่น ในกรณีเอกสาร ข้อมูล เครื่องมือฮาร์ดแวร์ และซอฟท์แวร์ต่างๆ

ที่ทางผู้รับจ้างนำมาใช้ในการดำเนินการเป็นการละเมิดลิขสิทธิ์หรือสิทธิบัตรของผู้อื่น ผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายที่เกี่ยวกับหรือเกี่ยวเนื่องกับกรณีดังกล่าวทั้งสิ้นให้แก่การยาสูบแห่งประเทศไทย และ/หรือบุคคลภายนอกผู้ถูกละเมิดนั้น

3.16. ลงนามในสัญญาห้ามเปิดเผยข้อมูล และการยาสูบแห่งประเทศไทย ขอสงวนสิทธิในข้อมูลทั้งหมดของโครงการนี้และเอกสารทั้งหมดที่จัดทำขึ้นถือเป็นลิขสิทธิ์ของการยาสูบแห่งประเทศไทย โดยผู้รับจ้างจะไม่นำเอกสารและข้อมูลใดๆที่ได้รับ หรือจัดทำขึ้นเกี่ยวกับโครงการนี้ไปเปิดเผยหรือเผยแพร่ โดยไม่ได้รับความเห็นชอบอย่างเป็นทางการจากการยาสูบแห่งประเทศไทย อีกทั้งมีหน้าที่ในการเก็บรักษาข้อมูลที่ได้รับจาก การยาสูบแห่งประเทศไทย และที่เกี่ยวข้องกับการยาสูบแห่งประเทศไทย ตลอดจนรายงานผลการดำเนินงานไว้เป็นความลับ ทั้งในระหว่างระยะเวลาสัญญาและสิ้นสุดสัญญา

3.17. ผู้รับจ้างต้องนำเสนอผลที่ได้จากการทดสอบและหาแนวทางไปประเมินเรียนรู้ และหาแนวทางจัดการความรู้และนวัตกรรม เพื่อนำไป ปรับปรุงแก้ไขให้กับผู้ที่มีส่วนเกี่ยวข้อง

3.18. ผู้รับจ้างต้องเสนอแนวทางการทดสอบที่สำคัญให้สอดคล้องกับการกำกับดูแลจัดทำแผนปฏิบัติการดิจิทัลของการยาสูบแห่งประเทศไทย

3.19. ผู้รับจ้างต้องกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของ ผู้มีส่วนเกี่ยวข้องกับกระบวนการหลังเสร็จสิ้นการอบรมให้แก่พนักงานของการยาสูบแห่งประเทศไทย

4. ระยะเวลาดำเนินงาน

ระยะเวลาในการดำเนินการ 150 วันนับถัดจากวันลงนามในสัญญา (ไม่นับรวมระยะเวลาการพิจารณาและการตรวจรับของคณะกรรมการตรวจรับพัสดุ)

5. คุณสมบัติของผู้ยื่นข้อเสนอ

5.1 มีความสามารถตามกฎหมาย

5.2 ไม่เป็นบุคคลล้มละลาย

5.3 ไม่อยู่ระหว่างเลิกกิจการ

5.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

5.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

5.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

5.7 เป็นนิติบุคคลตามกฎหมาย ที่จดทะเบียนในประเทศไทย และเป็นผู้มีอาชีพรับจ้างงานตามการจัดหาดังกล่าว

5.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่การยาสูบแห่งประเทศไทย ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการเสนอราคาครั้งนี้

5.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

5.11 ผู้ยื่นข้อเสนอต้องเป็นผู้มีอำนาจหรือได้รับมอบอำนาจโดยชอบด้วยกฎหมายในการดำเนินการเกี่ยวกับกระบวนการจัดซื้อจัดจ้างทุกขั้นตอน

5.12 เป็นนิติบุคคลที่ประกอบธุรกิจเกี่ยวกับการเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ หรือดำเนินการทดสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศมาแล้วไม่น้อยกว่า 9 ปีนับจนถึงวันยื่นเอกสาร

5.13 มีความรู้ ความเชี่ยวชาญเป็นพิเศษ หรือมีทักษะสูงทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) ต้องมีประสบการณ์ตรงในการทดสอบเจาะระบบรักษาความมั่นคงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ หรือทำโครงการเกี่ยวกับการให้บริการที่ปรึกษาด้านความมั่นคงปลอดภัย หรือโครงการติดตั้งหรือจัดหาอุปกรณ์ความมั่นคงปลอดภัยให้กับหน่วยงานต่าง ๆ มาแล้วไม่น้อยกว่า 3 โครงการ มูลค่าต่อโครงการไม่น้อยกว่า 1,000,000 บาท ย้อนหลังไม่เกิน 5 ปี นับจากวันที่สิ้นสุดสัญญา

5.14 ต้องเสนอบุคลากรตามข้อ 11 ที่มีความรู้ความสามารถตามคุณสมบัติที่กำหนดเป็นผู้เข้าปฏิบัติงานจริงในโครงการ โดยมีคุณสมบัติได้รับใบประกาศนียบัตรการรับรองมาตรฐาน (Certification) ความรู้ความสามารถทางด้านความปลอดภัยคอมพิวเตอร์ โดยหน่วยงานระดับสากล จากการรับรองมาตรฐานอย่างน้อย 3 ประกาศนียบัตร ดังต่อไปนี้

5.14.1 CISSP (Certified Information Systems Security Professional)

5.14.2 CISM (Certified Information Security Manager)

5.14.3 CEH (Certified Ethical Hacker)

5.14.4 OPST (OSSTMM Professional Security Tester)

5.14.5 GPEN (GIAC Penetration Tester)

5.14.6 GXPEN (GIAC Exploit Researcher and Advanced Penetration Tester)

5.14.7 GIAC Web Application Penetration Tester (GWAPT)

5.14.8 OSCE Offensive Security Certified Expert (OSCE)

5.14.9 OSWE Offensive Security Web Expert (OSWE)

5.14.10 eWPTx Certification certificate

5.14.11 eWPTxv2 Certification certificate

5.14.12 OSCP (Offensive Security Certified Professional)

5.14.13 CREST (Council of Registered Ethical Security Testers)

5.14.14 eCXD (eLearnSecurity Certified eXploit Developer)

5.14.15 CISA (Certified Information System Auditor)

6. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐาน (พร้อมทั้งรับรองสำเนาถูกต้องทุกแผ่น) ยื่นมาพร้อมกับการเสนอราคาตามวันและเวลาที่การยาสูบแห่งประเทศไทยกำหนด โดยแยกเป็น 2 ส่วน คือ

6.1. ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณียื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี)

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) และบัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี) และบัญชีรายชื่อผู้ถือหุ้น (บอจ.5) พร้อมทั้งรับรองสำเนาถูกต้อง

หนังสือรับรองการจดทะเบียนนิติบุคคล ตาม (ก) และ (ข) จะต้องออกให้**ไม่เกิน 6 เดือน** นับถึงวันยื่นข้อเสนอ

(2) ในกรณีผู้เสนอราคาเป็นบุคคลธรรมดาหรือคณะบุคคลที่มิใช่นิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วนหรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่มิได้ถือสัญชาติไทย พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอราคาร่วมกันในฐานะเป็นกิจการร่วมค้า ให้ยื่นสำเนาเอกสารข้อตกลงของการร่วมค้าที่เป็นลายลักษณ์อักษรหรือสำเนาสัญญาของการร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้ร่วมค้า และในกรณีที่ผู้เข้าร่วมค้าฝ่ายใดเป็นบุคคลธรรมดาที่มิใช่สัญชาติไทยก็ให้ยื่นสำเนาหนังสือเดินทาง หรือผู้ร่วมค้าฝ่ายใดเป็นนิติบุคคลให้ยื่นเอกสารตามที่ระบุไว้ใน (1)

ผู้ยื่นข้อเสนอที่เสนอราคาในฐานะของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

(1) กรณีที่กิจการร่วมค้าได้จดทะเบียนเป็นนิติบุคคลใหม่ กิจการร่วมค้าจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคาหรือสอบราคา และการเสนอราคาให้เสนอราคาในนาม “กิจการร่วมค้า” ส่วนคุณสมบัติด้านผลงานก่อสร้าง กิจการร่วมค้าดังกล่าวสามารถนำผลงานก่อสร้างของผู้เข้าร่วมค้ามาใช้แสดงเป็นผลงานก่อสร้างของกิจการร่วมค้าที่เข้าประกวดราคาหรือสอบราคาได้

(2) กรณีที่กิจการร่วมค้าไม่ได้จดทะเบียนเป็นนิติบุคคลใหม่ นิติบุคคลแต่ละนิติบุคคลที่เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคาหรือสอบราคาเว้นแต่ในกรณีที่กิจการร่วมค้าได้มีข้อตกลงระหว่างผู้ร่วมค้าเป็นลายลักษณ์อักษรกำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้รับผิดชอบหลักในการเข้าเสนอราคากับหน่วยงานของรัฐ และแสดงหลักฐานดังกล่าวมาพร้อมการยื่นข้อเสนอ

ประกวดราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ กิจการร่วมค้านั้นสามารถใช้ผลงานก่อสร้างของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานก่อสร้างของกิจการร่วมค้าที่ยื่นข้อเสนอได้

กรณีที่กิจการร่วมค้า ที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

ทั้งนี้ “กิจการร่วมค้าที่จดทะเบียนเป็นนิติบุคคลใหม่” หมายความว่า กิจการร่วมค้าที่จดทะเบียนเป็นนิติบุคคลต่อกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

(3) สำเนาใบทะเบียนพาณิชย์ (ถ้ามี)

(4) สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ถ้ามี)

6.2. ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทนให้แนบหนังสือมอบอำนาจซึ่งติดอากรแสตมป์ตามกฎหมาย โดยมีหลักฐานแสดงตัวตนของผู้มอบอำนาจและผู้รับมอบอำนาจ ทั้งนี้ หากผู้รับมอบอำนาจเป็นบุคคลธรรมดาต้องเป็นผู้ที่บรรลุนิติภาวะตามกฎหมายแล้วเท่านั้น

(2) รายละเอียดทางเทคนิคตามขอบเขตงานที่การยาสูบแห่งประเทศไทยกำหนด

(3) แบบแสดงการลงทะเบียนในระบบ e-GP

(4) ต้องแสดงเอกสารหลักฐานหนังสือรับรอง ตามที่ระบุในข้อ 5.12, ข้อ 5.13, ข้อ 5.14 และข้อ 11

7. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

7.1 ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ การยาสูบแห่งประเทศไทยจะพิจารณาตัดสิน โดย**ใช้เกณฑ์ราคา** และจะ**พิจารณาจากราคารวมที่ต่ำสุด (รวมภาษีมูลค่าเพิ่ม)**

7.2 การยาสูบแห่งประเทศไทยสงวนสิทธิ์ไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอ โดยไม่มีการผ่อนผันในกรณีดังต่อไปนี้

(1) ไม่ปรากฏชื่อผู้ยื่นข้อเสนอรายนั้นในบัญชีรายชื่อผู้รับ/ผู้ซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์ หรือเป็นผู้ยื่นข้อเสนอที่ไม่มีหนังสือเชิญชวนจากการยาสูบแห่งประเทศไทย แล้วแต่กรณี

(2) ไม่กรอกชื่อผู้ยื่นข้อเสนอในการเสนอราคา

(3) เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้ยื่นข้อเสนอรายอื่น

7.3 การยาสูบแห่งประเทศไทยทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกจ้างในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการยื่นข้อเสนอ โดยไม่พิจารณาจ้างเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้ เพื่อประโยชน์ของการยาสูบแห่งประเทศไทยเป็นสำคัญ และให้ถือว่าการตัดสินของการยาสูบแห่งประเทศไทยเป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใดๆ มิได้ รวมทั้งการยาสูบแห่งประเทศไทยจะพิจารณายกเลิกการยื่นข้อเสนอ และลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อได้ว่าการยื่นข้อเสนอกระทำ

การโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

ในกรณีที่ผู้ยื่นข้อเสนอรายที่เสนอราคาต่ำสุด เสนอราคาต่ำจนคาดหมายได้ว่าไม่อาจดำเนินงานตามรายละเอียดขอบเขตของงานได้ การยาสูบแห่งประเทศไทยจะให้ผู้ยื่นข้อเสนอนั้นชี้แจง และแสดงหลักฐานที่ทำให้เชื่อได้ว่าผู้ยื่นข้อเสนอสามารถดำเนินงานตามรายละเอียดขอบเขตของงานให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้ การยาสูบแห่งประเทศไทยมีสิทธิที่จะไม่รับข้อเสนอ หรือไม่รับราคาของผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ ผู้ยื่นข้อเสนอดังกล่าวไม่มีสิทธิเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใดๆ จากการยาสูบแห่งประเทศไทย

8. การเสนอราคา

8.1. ผู้ยื่นข้อเสนอต้องยื่นเสนอราคาตามแบบที่การยาสูบแห่งประเทศไทยกำหนดไว้ โดยไม่มีเงื่อนไขใดๆ ทั้งสิ้นและจะต้องกรอกข้อความให้ถูกต้องครบถ้วน ลงลายมือชื่อของผู้ยื่นข้อเสนอให้ชัดเจน จำนวนเงินที่เสนอต้องระบุตรงกันทั้งตัวเลขและตัวหนังสือ โดยไม่มีการขูดลบหรือแก้ไข หากมีการขูดลบ ตกเติม แก้ไข เปลี่ยนแปลงจะต้องลงลายมือชื่อผู้ยื่นข้อเสนอพร้อมประทับ (ถ้ามี) กำกับไว้ด้วยทุกแห่ง

8.2. ผู้ยื่นข้อเสนอจะต้องเสนอราคาเป็นเงินบาท (รวมภาษีมูลค่าเพิ่ม) ซึ่งราคาที่เสนอจะต้องรวมค่าใช้จ่ายอื่นๆ ไว้แล้ว เช่น ค่าจัดส่งพัสดุ ค่าใช้จ่ายในการเดินทาง ค่าเครื่องมือ ค่าจ้างแรงงาน เป็นต้น โดยเสนอราคารวม ตามเงื่อนไขที่ระบุไว้ท้ายใบเสนอราคาให้ถูกต้อง ทั้งนี้ ราคารวมที่เสนอจะต้องตรงกันทั้งตัวเลขและตัวหนังสือ ถ้าไม่ตรงกันให้ถือตัวหนังสือเป็นสำคัญ

ราคาที่เสนอ จะต้องเสนอกำหนดยืนราคาตามเงื่อนไขที่ระบุไว้ท้ายใบเสนอราคา นับแต่วันเสนอราคา โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนเสนอไว้ และจะถอนการเสนอราคามิได้

9. ขอบเขตความรับผิดชอบ

9.1. ค่าใช้จ่ายในการประเมินความเสี่ยงระบบสารสนเทศ ผู้รับจ้าง เป็นผู้รับผิดชอบทั้งสิ้น

9.2. ผู้รับจ้างต้องรับผิดชอบต่อการยาสูบแห่งประเทศไทยในกรณีที่ ผู้รับจ้าง เจ้าหน้าที่หรือลูกจ้างของผู้รับจ้าง จงใจหรือประมาทเลินเล่อ หรือไม่มีความรู้ความชำนาญพอ และทำหรืองดเว้นการกระทำใดๆ เป็นเหตุให้อุปกรณ์หรือระบบต่าง ๆ ของการยาสูบแห่งประเทศไทยเสียหายหรือไม่อยู่ในสภาพที่ใช้การได้ดี โดยไม่อาจแก้ไขได้ ผู้รับจ้าง ต้องจัดหาอุปกรณ์หรือระบบต่าง ๆ ซึ่งมีคุณภาพและประสิทธิภาพในการใช้งานเทียบเท่าหรือดีกว่าชดใช้แทน และต้องสามารถใช้งานได้อย่างเดิมหลังมีการทดแทนแล้ว

9.3. การปฏิบัติงาน ให้ปฏิบัติงานในเวลาทำงานปกติของการยาสูบแห่งประเทศไทยโดยไม่กระทบกระเทือนต่อการปฏิบัติงานของการยาสูบแห่งประเทศไทย ในกรณีมีความประสงค์จะดำเนินงานในวันหยุดประจำสัปดาห์ วันหยุดตามประเพณีนิยมหรือนอกเวลาทำงานปกติของ การยาสูบแห่งประเทศไทย จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากการยาสูบแห่งประเทศไทยก่อน เพื่อการยาสูบแห่งประเทศไทยจะได้ให้คณะกรรมการตรวจรับพัสดุ หรือผู้ที่เกี่ยวข้องมาตรวจสอบเฝ้าดูแล และอำนวยความสะดวกหรือรู้เห็นในการดำเนินงานตลอดเวลา และผู้รับจ้างต้องยินยอมจ่ายค่าล่วงเวลาให้แก่คณะกรรมการ

ตรวจรับพัสดุ หรือผู้ที่เกี่ยวข้องตามระเบียบของ การยาสูบแห่งประเทศไทยทุกประการ เว้นแต่กรณีที่การยาสูบแห่งประเทศไทยเป็นผู้กำหนดให้เข้าปฏิบัติงานในวันหยุดดังกล่าว

9.4. ลิขสิทธิ์ซอฟต์แวร์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิ์เรียกร้องใดๆว่ามีการละเมิดลิขสิทธิ์หรือสิทธิบัตรเกี่ยวกับการประเมินความเสี่ยงระบบสารสนเทศ ที่ผู้รับจ้างดูแลรับผิดชอบ ผู้รับจ้างต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว และผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่างๆ ที่เกิดขึ้นทั้งหมดกับการยาสูบแห่งประเทศไทย

10. การฝึกอบรม

10.1. ทำการกำหนดเกณฑ์การประเมิน และขอบเขตการประเมินการรับรู้ ผู้ที่เกี่ยวข้องกับกระบวนการความมั่นคงปลอดภัยสารสนเทศ และมีการแสดงการวิเคราะห์ผลการประเมิน ก่อนการอบรม

10.2. จัดอบรมหลักสูตรการสร้างความตระหนักถึงภัยคุกคามด้านความปลอดภัยไซเบอร์ (Cyber Security Awareness) เป็นระยะเวลา 3 ชั่วโมง จำนวน 2 ครั้ง สำหรับผู้เข้าฝึกอบรมจำนวนอย่างน้อยครั้งละ 50 ท่าน พร้อมจัดทำสื่อการสอนในรูปแบบวิดีโอภาพและเสียง

10.3. จัดอบรมหลักสูตร CompTIA Security+ จำนวน 4 ท่านเป็นระยะเวลา 5 วัน พร้อมประสานงานให้ผู้เข้าอบรมเข้าสอบ โดยศูนย์ฝึกอบรมอย่างเป็นทางการ (Authorized Training) จำนวน 1 ครั้ง/ท่าน โดยผู้รับจ้างเป็นผู้ออกค่าใช้จ่ายในการอบรมทั้งหมด

10.4. ผู้สอนจะต้องมีคุณสมบัติที่แสดงว่ามีประสบการณ์ ความรู้ ความเชี่ยวชาญในหลักสูตรที่อบรมเป็นอย่างดี กรณีผู้เข้ารับการอบรมเห็นว่าผู้สอนไม่เป็นผู้มีความรู้ความเชี่ยวชาญพอในหลักสูตรที่เสนอการยาสูบแห่งประเทศไทย สงวนสิทธิ์ที่จะขอเปลี่ยนผู้สอนที่ขาดคุณสมบัติหรือไม่เหมาะสมในการอบรม โดยผู้ชนะการเสนอราคาจะต้องจัดหาผู้สอนใหม่และดำเนินการอบรมหลักสูตรนั้นซ้ำอีกครั้ง

10.5. จัดเตรียมอุปกรณ์ เอกสารการฝึกอบรม และสิ่งอำนวยความสะดวกอื่นๆที่เกี่ยวข้องในการฝึกอบรมให้เพียงพอกับจำนวนผู้เข้ารับการอบรมในแต่ละหลักสูตร

10.6. ทำการกำหนดเกณฑ์การประเมิน และขอบเขตการประเมินการรับรู้ ผู้ที่เกี่ยวข้องกับกระบวนการความมั่นคงปลอดภัยสารสนเทศ และมีการแสดงการวิเคราะห์ผลการประเมิน หลังการอบรมในข้อ 10.2

11. บุคลากรของผู้ยื่นข้อเสนอ

ผู้เสนอราคาต้องเสนอบุคลากรที่มีความรู้ความสามารถ ความเชี่ยวชาญและมีประสบการณ์ ที่เกี่ยวข้องกับการจัดจ้างในครั้งนี้ ประกอบด้วย

11.1. หัวหน้าโครงการฯ วุฒิการศึกษา ไม่ต่ำกว่าปริญญาโท สาขาวิศวกรรมศาสตร์ หรือ สาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์ในการบริหารโครงการที่เกี่ยวข้องการจัดจ้างในครั้งนี้ อย่างน้อย 9 ปี จำนวน 1 คน (โดยจะต้องใบประกาศนียบัตรการรับรองมาตรฐาน (Certification) อย่างน้อย 1 ใบประกาศนียบัตร ตามรายละเอียด ข้อ 5.14)

11.2. ผู้เชี่ยวชาญ วุฒิการศึกษา ไม่ต่ำกว่าปริญญาโท สาขาวิศวกรรมศาสตร์ หรือ สาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์อย่างน้อย 6 ปี จำนวน 1 คน (โดยจะต้องใบประกาศนียบัตรการรับรองมาตรฐาน (Certification) อย่างน้อย 1 ใบประกาศนียบัตร ตามรายละเอียด ข้อ 5.14)

11.3. นักวิเคราะห์ระบบ ไม่ต่ำกว่าวุฒิการศึกษา ปริญญาโท สาขาวิศวกรรมศาสตร์ หรือ สาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์อย่างน้อย 9 ปี จำนวน 2 คน

11.4. นักเจาะระบบ ไม่ต่ำกว่าวุฒิการศึกษา ปริญญาตรี สาขาวิศวกรรมศาสตร์ หรือ สาขาเทคโนโลยีสารสนเทศ หรือวิทยาศาสตร์ ที่มีประสบการณ์อย่างน้อย 5 ปี จำนวน 2 คน

ทั้งนี้ ต้องจัดรายผังโครงสร้างและความพร้อมด้านการบริหารบุคลากร รายชื่อ คุณวุฒิ และประสบการณ์ให้ทางการยาสูบแห่งประเทศไทย พิจารณาก่อนดำเนินงาน

12. เอกสารส่งมอบงาน

ต้องจัดทำเอกสารที่ครบถ้วนและถูกต้องโดยใช้ภาษาไทยเป็นหลัก ยกเว้นศัพท์วิชาการหรือศัพท์เทคนิคให้ใช้ภาษาอังกฤษ โดยจัดทำแบบ Hardcopy จำนวน 3 ชุด และแบบ Softcopy ในรูปแบบไฟล์อิเล็กทรอนิกส์ที่สามารถแก้ไขได้ โดยบรรจุในดิจิทัลมีเดีย จำนวน 1 ชุด จัดส่งตามขอบเขตงานของแต่ละงวด ดังนี้

งวดที่	วันที่ครบกำหนดส่งงาน	ผลงานที่ต้องส่งมอบ
1	ภายใน 15 วัน นับถัดจาก วันลงนามในสัญญา	• แผนการดำเนินโครงการ (Project Plan) ตามข้อ 3.1 • รายงานการหาข้อมูลขององค์กรผ่านการทำ OSINT และ Threat Intelligence ตามข้อ 3.3
2	ภายใน 90 วัน นับถัดจาก วันลงนามในสัญญา	• จัดทำแบบฟอร์ม Pretest ก่อนการอบรม • รายงานผลการเจาะระบบจากเครือข่ายภายนอก พร้อมคำแนะนำในการปิดช่องโหว่ ตามข้อ 3.5 • รายงานการผลเจาะระบบเว็บแอพพลิเคชัน พร้อมคำแนะนำในการปิดช่องโหว่ ตามข้อ 3.6 • รายงานการผลเจาะระบบจากเครือข่ายภายใน พร้อมคำแนะนำในการปิดช่องโหว่ ตามข้อ 3.7
3	ภายใน 150 วัน นับถัดจาก วันลงนามในสัญญา	• รายงานการตรวจหาภัยคุกคาม พร้อมคำแนะนำตามข้อ 3.8 • รายงานการทดสอบ Phishing Test พร้อมคำแนะนำในการปิดช่องโหว่ ตามข้อ 3.9 • จัดฝึกอบรมสร้างความตระหนักถึงภัยคุกคามด้านความปลอดภัยไซเบอร์ (Cyber Security Awareness) ตามข้อ 10.1 • จัดการอบรมหลักสูตร COMPTIA Security+ ตาม

งวดที่	วันที่ครบกำหนดส่งงาน	ผลงานที่ต้องส่งมอบ
		ข้อ 10.2 • เอกสารผลที่ได้จากการทดสอบและหาแนวทางไปประเมินเรียนรู้ ผลวิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นกับองค์กร และหาแนวทางจัดการความรู้และนวัตกรรม เพื่อนำไป ปรับปรุงแก้ไขให้กับผู้ที่มีส่วนเกี่ยวข้อง ตามข้อ 3.17 • เอกสารแนวทางการทดสอบที่สำคัญให้สอดคล้องกับการกำกับดูแลจัดทำแผนปฏิบัติการดิจิทัลของการยาสูบแห่งประเทศไทย ตามข้อ 3.18 • เอกสารกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการ บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของ ผู้มีส่วนเกี่ยวข้องกับกระบวนการหลังเสร็จสิ้นการอบรมให้แก่พนักงานของการยาสูบแห่งประเทศไทย ตามข้อ 3.19

13. การทำสัญญา

13.1 ในกรณีที่ผู้ชนะการเสนอราคา สามารถส่งมอบพัสดุได้ครบถ้วน ภายใน 5 วันทำการ นับแต่วันที่ทำข้อตกลง การยาสูบแห่งประเทศไทยจะพิจารณาจัดทำข้อตกลงเป็นหนังสือแทนการทำสัญญาก็ได้

13.2 ในกรณีที่ผู้ชนะการเสนอราคาไม่สามารถส่งมอบพัสดุได้ครบถ้วน ภายใน 5 วันทำการ หรือการยาสูบแห่งประเทศไทยเห็นว่าไม่สมควรจัดทำข้อตกลงเป็นหนังสือ ตามข้อ 13.1 ผู้ชนะการเสนอราคาจะต้องติดต่อทำสัญญากับการยาสูบแห่งประเทศไทย ที่กองสัญญา สำนักกฎหมาย ภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้งจากการยาสูบแห่งประเทศไทยเป็นลายลักษณ์อักษร และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของราคาพัสดุที่เสนอราคา ให้การยาสูบแห่งประเทศไทยยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) เงินสด

(2) เช็คหรือดราฟท์ที่ธนาคารสั่งจ่ายให้แก่ การยาสูบแห่งประเทศไทย โดยเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ในวันทำสัญญา หรือก่อนหน้านั้นไม่เกิน 3 วันทำการ ของการยาสูบแห่งประเทศไทย

(3) หนังสือค้ำประกันของธนาคารในประเทศ ตามตัวอย่างที่คณะกรรมการนโยบายกำหนด หรือจะเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนด

(4) หนังสือค้ำประกันของบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

(5) พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ยภายใน 15 วัน นับถัดจากวันที่ผู้ชนะการเสนอราคา พ้นจากข้อผูกพันตามสัญญาแล้ว

14. การจ่ายเงิน

การยาสูบแห่งประเทศไทยจะจ่ายค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอื่นๆ และค่าใช้จ่ายทั้งปวงแล้ว กำหนดการจ่ายเงินเป็น 3 งวด โดยการจ่ายเงินแต่ละงวดจะต้องผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว ดังนี้

งวดที่ 1 จ่ายเงินเป็นจำนวน ร้อยละ 20 ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากผู้รับจ้างส่งมอบงานตามข้อ 12 ในงวดงานที่ 1 และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 2 จ่ายเงินเป็นจำนวน ร้อยละ 30 ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากผู้รับจ้างส่งมอบงานตามข้อ 12 ในงวดงานที่ 2 และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 3 จ่ายเงินเป็นจำนวน ร้อยละ 50 ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากผู้รับจ้างส่งมอบงานตามข้อ 12 ในงวดงานที่ 3 และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

ผู้รับจ้างต้องส่งเอกสารการปฏิบัติงาน (Check list) ในแต่ละงวดงาน ตามแบบฟอร์มในเอกสารแนบ 1 แนบมาด้วยทุกงวดงาน

15. อัตราค่าปรับ

ในกรณีส่งมอบงานล่าช้า ผู้รับจ้างจะต้องชำระค่าปรับให้ ยสท. เป็นรายวัน ในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของราคาค่าจ้างทั้งหมด แต่ไม่ต่ำกว่าวันละ 100 บาท (หนึ่งร้อยบาทถ้วน) นับถัดจากวันครบกำหนดส่งมอบงานถูกต้องครบถ้วน

16. การบอกเลิกสัญญา

หากผู้ว่าจ้างเห็นว่าผู้รับจ้างไม่อาจปฏิบัติตามสัญญาได้ หรือผู้รับจ้างผิดสัญญาข้อใดข้อหนึ่ง หรือตกเป็นผู้ล้มละลาย ผู้ว่าจ้างมีสิทธิบอกเลิกสัญญาได้ และมีสิทธิจ้างผู้รับจ้างรายใหม่เข้าทำงานของผู้รับจ้างให้ลุล่วงไป การใช้สิทธิบอกเลิกสัญญานั้นไม่กระทบสิทธิของผู้ว่าจ้างที่จะเรียกร้องค่าเสียหายและค่าใช้จ่ายใดๆ (ถ้ามี) จากผู้รับจ้าง

ในกรณีที่ผู้ว่าจ้างใช้สิทธิบอกเลิกสัญญา ผู้ว่าจ้างมีสิทธิริบหรือบังคับจากหลักประกันการปฏิบัติตามสัญญาทั้งหมดหรือแต่บางส่วน ตามแต่จะเห็นสมควรได้ทันที นอกจากนั้น ผู้รับจ้างจะต้องรับผิดชอบในค่าเสียหายซึ่งเป็นจำนวนเกินกว่าหลักประกันการปฏิบัติตามสัญญา และค่าเสียหายต่างๆ ที่เกิดขึ้น รวมทั้งค่าใช้จ่ายที่เพิ่มขึ้นในการทำงานนั้นต่อให้แล้วเสร็จตามสัญญาซึ่งผู้ว่าจ้างจะหักจากจำนวนเงินใดๆ ที่จะจ่ายให้แก่ผู้รับจ้างก็ได้

การที่ผู้ว่าจ้างไม่ใช้สิทธิเลิกสัญญาดังกล่าวตามวรรคหนึ่งไม่เป็นเหตุให้ผู้รับจ้างพ้นจากความรับผิดตามสัญญา

17. การจ้างช่วง

ผู้รับจ้างจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนแห่งงานนี้ ไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากการยาสูบแห่งประเทศไทยแล้ว การที่การยาสูบแห่งประเทศไทยได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนั้น ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดหรือพันธะหน้าที่แห่งงานนี้ และผู้รับจ้างจะยังคงต้องรับผิดและความประมาทเลินเล่อของผู้รับจ้างช่วงหรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ

กรณีผู้รับจ้างไปจ้างช่วงงานแต่บางส่วนโดยฝ่าฝืนความในวรรคหนึ่ง ผู้รับจ้างต้องชำระค่าปรับให้แก่ การยาสูบแห่งประเทศไทย เป็นจำนวนเงินในอัตราร้อยละ 10 (สิบ) ของวงเงินของงานที่จ้างช่วงตามสัญญา ทั้งนี้ไม่ตัดสิทธิการยาสูบแห่งประเทศไทยในการบอกเลิกสัญญา

18. การงดหรือลดค่าปรับ หรือการขยายเวลาในการปฏิบัติตามสัญญา

ในกรณีที่มีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ว่าจ้าง หรือเหตุสุดวิสัยหรือเกิดจากพฤติการณ์อันหนึ่งอันใดที่ผู้รับจ้างไม่ต้องรับผิดตามกฎหมาย หรือเหตุอื่นตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ทำให้ผู้รับจ้างไม่สามารถปฏิบัติตามเงื่อนไขและกำหนดเวลาในข้อ 3 ข้อ 9 ข้อ 10 ข้อ 12 หรือข้อ 15 ได้ ผู้รับจ้างจะต้องแจ้งเหตุหรือพฤติการณ์ดังกล่าว พร้อมหลักฐานเป็นหนังสือให้ผู้ว่าจ้างทราบ เพื่อของดหรือลดค่าปรับ หรือขยายเวลาทำการตามสัญญาภายใน 15 (สิบห้า) วันนับถัดจากวันที่เหตุนั้นสิ้นสุดลง หรือตามที่กำหนดในกฎกระทรวงดังกล่าวแล้วแต่กรณี

ถ้าผู้รับจ้างไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้รับจ้างได้สละสิทธิเรียกร้องในการที่จะของดหรือลดค่าปรับ หรือขยายเวลาทำการตามสัญญาโดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น เว้นแต่กรณีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ว่าจ้างซึ่งมีหลักฐานชัดแจ้งหรือผู้ว่าจ้างทราบดีอยู่แล้วตั้งแต่ต้น

การงดหรือลดค่าปรับ หรือขยายกำหนดเวลาทำการตามสัญญาตามวรรคหนึ่ง อยู่ในดุลยพินิจของผู้ว่าจ้างที่จะพิจารณาตามที่เห็นสมควร

.....

หมายเหตุ ใช้สำหรับปีงบประมาณ 2565

..... ประธานคณะกรรมการร่างขอบเขตของงานฯ
(นางสาวพัชรินทร์ ลภะวงศ์)

..... คณะกรรมการร่างขอบเขตของงานฯ
(นายโสภณ ทองศรีงาม)

..... คณะกรรมการร่างขอบเขตของงานฯ
(นายพยนต์ อินจันทึก)

..... คณะกรรมการร่างขอบเขตของงานฯ
(นายไตรลักษณ์ พานิกุล)

..... คณะกรรมการร่างขอบเขตของงานฯ
(นายอาคม อิ่มเอม)

..... คณะกรรมการร่างขอบเขตของงานฯ
(นายธนวัฒน์ เสมสวัสดิ์)

..... คณะกรรมการร่างขอบเขตของงานฯ
(นายจิรายุทธ เนตรมะลิ)

เอกสารแนบ 1

ตัวอย่างเอกสารปฏิบัติงาน (Check List)

สิ่งที่ต้องดำเนินงานในงวดที่ ..... การตรวจรับงาน.....

สัญญาเลขที่.....วันที่ส่งมอบงาน.....วันที่ตรวจรับงาน.....

ข้อกำหนดตามขอบเขตของงาน(TOR)	สิ่งที่ต้องปฏิบัติ	ผ่าน	ไม่ผ่าน

บริษัทได้ส่งมอบงานตามข้อกำหนดของเขตของงาน (TOR) ครบทุกข้อ (เอกสารแนบ)

ลงชื่อ ..... ประธานกรรมการ

( )

ลงชื่อ ..... กรรมการตรวจรับพัสดุ

( )

ลงชื่อ ..... กรรมการตรวจรับพัสดุ

( )

ลงชื่อ ..... กรรมการตรวจรับพัสดุ

( )