

## ขอบเขตของงาน (Terms of Reference : TOR)

### โครงการจ้างบริการจัดเก็บ log file และบริหารจัดการด้านการรักษา ความมั่นคงปลอดภัยสารสนเทศ

#### 1. เหตุผลและความจำเป็น

สถาบันคุ้มครองเงินฝาก (สคฟ.) มีความประสงค์จะจัดหาผู้ให้บริการดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กำหนดไว้ และทำหน้าที่เป็นศูนย์การรักษาความปลอดภัยสารสนเทศ โดยผู้ยื่นข้อเสนอต้องดำเนินการครบวงจรด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ สคฟ. มีความสามารถในการเฝ้าระวัง การตรวจสอบ การป้องกัน การแจ้งเตือน และการรับมือต่อภัยคุกคามทางไซเบอร์ที่สอดคล้องกับสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็วในปัจจุบัน ทั้งรูปแบบภัยคุกคามจากภายใน และภัยคุกคามจากภายนอก รวมถึงมีความสามารถในการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability) ของระบบสารสนเทศเพื่อให้สามารถปฏิบัติงานตามพันธกิจของ สคฟ. ได้อย่างมีประสิทธิภาพ

#### 2. ขอบเขตงานที่ต้องการ

2.1 โครงการจ้างบริการจัดเก็บ log file และบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ มีวัตถุประสงค์ ดังนี้

2.1.1 เพื่อให้ สคฟ. มีการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log)

2.1.2 เพื่อให้ สคฟ. มีการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์

2.1.3 เพื่อให้ สคฟ. มีการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์

2.2 โดยผู้ยื่นข้อเสนอจะต้องดำเนินการอย่างน้อย ดังต่อไปนี้

2.2.1 ดำเนินการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log) เป็นระยะเวลา 3 ปี

2.2.1.1 ดำเนินการจัดเก็บ Log ของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายตามที่ สคฟ. กำหนด เพื่อปฏิบัติตาม “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ปี 2550” และ “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560” ต้องจัดเก็บได้ไม่น้อยกว่า 90 วันและไม่น้อยกว่าวันละ 30 GB.

2.2.1.2 ต้องมีระบบหรือเครื่องมือประเภท Log Transporter หรือ Log Collector หรือ Log Forwarder ที่อยู่ในรูปแบบ Virtual Machine มาติดตั้งที่ศูนย์คอมพิวเตอร์ของ สคฟ. เพื่อทำการส่งข้อมูล Log ไปจัดเก็บที่ศูนย์ข้อมูลของผู้ยื่นข้อเสนอได้อย่างปลอดภัย

2.2.1.3 ต้องสามารถรองรับการจัดเก็บข้อมูล Log ได้ ดังนี้

(1) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Windows 10, Windows 11, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022, CentOS, Red Hat Enterprise Linux, Amazon Linux, Ubuntu เป็นอย่างน้อย

(2) อุปกรณ์ Next-Generation Firewall

(3) ระบบบริหารจัดการเครือข่ายไร้สาย (Wi-Fi Controller)

(4) อุปกรณ์ Network Access Control

2.2.1.4 จัดทำรายงานสรุปสถานะการจัดเก็บ Log เป็นรายเดือน ประกอบด้วยข้อมูลสถานะการจัดเก็บ ปริมาณข้อมูลเป็นรายอุปกรณ์ ปริมาณข้อมูลเฉลี่ยต่อวัน เป็นอย่างน้อย

2.2.1.5 ให้ความร่วมมือในการสืบสวน การแสวงหาข้อมูล และการรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (ถ้ามี)

2.2.1.6 เมื่อสิ้นสุดสัญญาจ้าง ผู้ยื่นข้อเสนอต้องทำการจัดเก็บ Log ให้ครบตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กำหนดไว้ โดยมีระยะเวลาไม่น้อยกว่า 90 วัน เป็นอย่างน้อย หรือส่งมอบ Log ตามที่ สคฟ. ร้องขอ และต้องทำลายข้อมูล Log ที่จัดเก็บไว้ที่ผู้ยื่นข้อเสนออย่างถูกต้องตามหลักการมาตรฐาน พร้อมทั้งส่งหลักฐานการทำลายข้อมูลให้ สคฟ.

2.2.2 ดำเนินการเพื่อให้ สคฟ. มีการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์อย่างน้อย ดังนี้

2.2.2.1 ต้องให้บริการเป็นศูนย์การเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center: SOC) แก่ สคฟ. ตลอด 24 ชั่วโมง (24x7) เป็นระยะเวลา 3 ปี โดยต้องมีทีมงานผู้เชี่ยวชาญในการเฝ้าระวัง วิเคราะห์เหตุการณ์ แจ้งเตือนพร้อมคำแนะนำในการจัดการเหตุการณ์ ตามความรุนแรงของเหตุการณ์ ดังนี้

ระดับความรุนแรง ของเหตุการณ์	แจ้งเตือน สคฟ. พร้อมคำแนะนำในการแก้ไข
วิกฤต (Critical)	ภายใน 1 ชั่วโมง
สูง (High)	ภายใน 2 ชั่วโมง
กลาง (Medium)	ภายใน 24 ชั่วโมง
ต่ำ (Low)	ภายใน 48 ชั่วโมง

2.2.2.2 ระบบหรือเครื่องมือที่นำมาให้บริการต้องมีแพลตฟอร์มเป็นลักษณะของ Software-as-a-Service ที่ Hosted และ Managed บน Cloud และต้องได้รับการรับรองมาตรฐาน ISO/IEC:27001 หรือ SOC1 หรือ SOC2 ได้เป็นอย่างน้อย

2.2.2.3 ต้องสามารถรับข้อมูล Telemetry จากระบบตรวจจับและโต้ตอบภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response) บนเครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่ายของ สคฟ. จำนวนไม่น้อยกว่า 400 เครื่อง และต้องรับข้อมูล Log จากอุปกรณ์ Next-Generation Firewall และอุปกรณ์ Network Access Control ที่ สคฟ. ใช้งานอยู่ได้

2.2.2.4 สามารถเชื่อมต่อและทำการตรวจจับภัยคุกคามเชิงรุก (Threat Hunting) ร่วมกับระบบตรวจจับและโต้ตอบภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response: XDR) ที่ สคผ. ใช้งานอยู่ได้อย่างมีประสิทธิภาพ และต้องสามารถทำการโต้ตอบ (Response Action) ไปยังเครื่องคอมพิวเตอร์ของ สคผ. ได้ หากระบบหรือเครื่องมือที่เสนอไม่สามารถทำงานได้ตามข้อกำหนด ผู้ยื่นข้อเสนอสามารถเสนอระบบ XDR เพิ่มเติมได้ โดยต้องสามารถทำงานครอบคลุมเครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่าย ไม่น้อยกว่า 400 เครื่อง พร้อมทั้งทำการติดตั้งระบบหรือเครื่องมือที่เสนอให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

2.2.2.5 สามารถทำการตรวจสอบ (Monitoring) เชื่อมโยงข้อมูล (Correlation) และจัดลำดับความสำคัญ (Prioritization) การแจ้งเตือนที่เกิดขึ้นได้ และสามารถทำการค้นหาสิ่งผิดปกติจากหลักฐานเชื่อมโยงที่มีอยู่ (Indicators of Compromise) และหลักฐานจากรูปแบบการโจมตี (Indicators of Attack) โดยอัตโนมัติ และรองรับการเชื่อมโยงรวบรวมข้อมูลจากกิจกรรมต่างๆ ที่เกิดขึ้นจากแหล่งข้อมูลที่แตกต่างกัน เช่น Endpoint และ Server ได้

2.2.2.6 สามารถทำการวิเคราะห์เชิงลึกที่ครอบคลุม (Comprehensive Analysis) โดยจัดทำแผนการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นแบบละเอียด

2.2.2.7 สามารถเปิดเผยหรือแสดงการเชื่อมโยงกรณีถูกโจมตีจากกลุ่มผู้ไม่ประสงค์ดีที่มีการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack Detection) และเชื่อมโยงข้อมูลที่เกี่ยวข้อง Threat Intelligence ทั้งจากที่มาจากเจ้าของผลิตภัณฑ์, Government Agencies และ Third Party เช่น TAXII Feed, MISP Feed แล้วทำการ Block IOC ที่ได้รับจาก Feed

2.2.2.8 สามารถสร้างแผนภาพรวมของเหตุการณ์ที่เกิดขึ้น (Full Picture of The Attack) รวมถึงวิเคราะห์ต้นเหตุของเหตุการณ์ที่เกิดขึ้น (Root Cause Analysis) เพื่อแสดงที่มาของการโจมตี (Attack Vector), ช่วงเวลา (Dwell Time) และผลกระทบ (Impact Scope) ที่เกิดขึ้น รวมถึงสามารถเชื่อมโยงเหตุการณ์โจมตีหลายเหตุการณ์เข้าเป็น Incident เดียวกันได้หากมีความสัมพันธ์กัน

2.2.2.9 สามารถทำการค้นหาหลักฐานบ่งชี้ว่าถูกโจมตี (Indicator of Compromise) ตาม Threat Intelligence ที่สำคัญและแจ้งเตือนรายละเอียดหากตรวจพบ

2.2.2.10 สามารถทำการตอบสนองเพื่อตอบโต้ภัยคุกคามที่ระดับอันตรายได้อัตโนมัติผ่าน Automated Playbooks และสามารถสั่งงานเพิ่มเติมได้ เช่น Isolate Endpoint, Remote Shell, Remote Custom Script, Collect File, Dump Process Memory, Terminate Process, Add to Block List, Force Password Reset เป็นต้น

2.2.2.11 สามารถบริหารจัดการ Case ที่เกิดขึ้นได้ โดยจะต้องมีการวิเคราะห์, แจ้งเตือน แนะนำวิธีการแก้ไข และทำการปิด Case พร้อมระบุรายละเอียดเพิ่มเติมให้สำหรับ Case ที่เกิดขึ้น (Case Management)

2.2.2.12 สามารถออกแผนการตอบสนองต่อเหตุการณ์ภัยคุกคาม แบบ step-by-step เพื่อแก้ไขเหตุการณ์ที่เกิดขึ้น

2.2.2.13 ระบบหรือเครื่องมือที่เสนอต้องมีสาขาของเจ้าของผลิตภัณฑ์ตั้งอยู่ในประเทศไทยเพื่อรองรับบริการหลังการขาย และได้รับการรับรองและแต่งตั้งจากเจ้าของผลิตภัณฑ์อย่างเป็นทางการ

2.2.3 ดำเนินการเพื่อให้ สคผ. มีการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยต้องให้บริการระบบหรือเครื่องมือบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Attack Surface Risk Management หรือ Attack Surface Management) ที่ครอบคลุมเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศของ สคผ. จำนวนไม่น้อยกว่า 400 เครื่อง ตลอดอายุสัญญา 3 ปี ซึ่งต้องมีคุณสมบัติ ดังนี้

2.2.3.1 ระบบหรือเครื่องมือที่เสนอต้องสามารถแสดงค่าความเสี่ยงขององค์กร (Risk Index หรือ Risk Scoring) ในลักษณะของตัวเลขที่คำนวณจากองค์ประกอบ ดังต่อไปนี้ Exposure, Attack, และ Security Configurations ได้เป็นอย่างดี

2.2.3.2 สามารถค้นหาช่องทางที่มีความเสี่ยงจากภายในองค์กรและความเสี่ยงจากภายนอกองค์กร (Attack Surface Discovery) เช่น Devices, Internet-Facing Assets, Accounts, Application, Cloud Assets และ APIs ได้เป็นอย่างดี และจะต้องสามารถแสดงรายละเอียดของแต่ละรายการเพื่อให้ทราบถึงความเสี่ยงที่มีในองค์กรได้

2.2.3.3 สามารถทำ External Attack Surface Management สำหรับ Internet Facing Assets ได้ไม่น้อยกว่า 10 โดเมน

2.2.3.4 สามารถแสดงผลค่าความเสี่ยงได้ในหลายมิติ เช่น Account Compromise, Vulnerabilities, Activity and Behaviors, Cloud App Activity, System Configuration, XDR Detection, Threat Detection, Security Configuration และจะต้องสามารถตรวจสอบข้อมูลเจาะลึกลงไปในแต่ละหัวข้อเพื่อความชัดเจนของความเสี่ยงในแต่ละด้านได้

2.2.3.5 ระบบหรือเครื่องมือที่เสนอต้องรองรับการรับเข้าข้อมูลจากเจ้าของผลิตภัณฑ์ และจากผลิตภัณฑ์อื่นๆ เช่น Azure AD, Active Directory (on-premises), AWS Account, Rapid7, Tenable, Office365, Okta และ Qualys ได้เป็นอย่างดี เพื่อนำข้อมูลมาคำนวณหาค่าความเสี่ยงขององค์กรเพิ่มเติมได้

2.2.3.6 ระบบหรือเครื่องมือที่เสนอต้องสามารถค้นหาและตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) เช่น Windows 10, Windows 11, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022, CentOS, Red Hat Enterprise Linux, Amazon Linux, Ubuntu และช่องโหว่ของ Application เช่น Microsoft Office, Microsoft Exchange Server, Adobe, 7-zip, WinRAR, Apache, Oracle ได้เป็นอย่างดี

2.2.3.7 ระบบหรือเครื่องมือที่เสนอต้องมีความสามารถในการแนะนำแนวทางการแก้ไขปรับปรุง เพื่อลดความเสี่ยงต่อภัยคุกคามขององค์กรได้ (Risk Reduction Measures)

2.2.3.8 ระบบหรือเครื่องมือที่เสนอต้องมีแดชบอร์ดระดับผู้บริหาร (Executive Dashboard) เพื่อแสดงความเสี่ยงโดยรวมขององค์กร และแดชบอร์ดสำหรับผู้ดำเนินการ (Operation Dashboard) เพื่อแสดงรายละเอียดของความเสี่ยงแต่ละรายการได้

2.2.3.9 ระบบหรือเครื่องมือที่เสนอต้องสามารถบริหารจัดการร่วมกับ XDR และระบบ Endpoint Security ที่ทาง สคผ. ใช้งานอยู่ได้ เพื่อให้เกิดประโยชน์สูงสุดสำหรับการบริหารจัดการและการตรวจสอบภัยคุกคามที่เกิดขึ้นกับ สคผ.

2.2.3.10 ระบบหรือเครื่องมือที่เสนอต้องสามารถนำข้อมูลของภัยคุกคามที่ตรวจพบ (Attack Index) จาก XDR ที่ทาง สคผ. มีอยู่มาคำนวณหาค่าความเสี่ยงขององค์กร (Risk Index) ได้

2.2.3.11 ระบบหรือเครื่องมือที่เสนอต้องมีสาขาของเจ้าของผลิตภัณฑ์ตั้งอยู่ในประเทศไทย เพื่อรองรับบริการหลังการขาย และได้รับการรับรองและแต่งตั้งจากเจ้าของผลิตภัณฑ์อย่างเป็นทางการ

2.2.3.12 ระบบหรือเครื่องมือที่เสนอต้องสามารถทำงานร่วมกับ XDR และ Endpoint Security ที่ สคฟ. ใช้งานอยู่ได้ หากไม่สามารถทำงานได้ตามข้อกำหนดข้อใดข้อหนึ่ง ผู้ยื่นข้อเสนอสามารถเสนอระบบ XDR และ Endpoint Security อื่น ๆ เพิ่มเติมได้ โดยต้องครอบคลุมเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศ ของ สคฟ. จำนวนไม่น้อยกว่า 400 เครื่อง พร้อมทั้งทำการติดตั้งระบบหรือเครื่องมือที่เสนอให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

#### 2.2.4 ต้องจัดทำรายงานส่งให้ สคฟ. ดังนี้

2.2.4.1 รายงานสรุปสถานะการจัดเก็บ Log เป็นรายเดือน ที่ประกอบด้วยข้อมูลสถานะการจัดเก็บปริมาณข้อมูลเป็นรายอุปกรณ์ ปริมาณข้อมูลเฉลี่ยต่อวันเป็นอย่างน้อย

2.2.4.2 รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงภัยสารสนเทศ เป็นรายเดือน

2.2.4.3 จัดทำรายงานวิเคราะห์เหตุการณ์ที่เกิดขึ้น ตามข้อ 2.2.4.2 เพื่อหา Gap ของระบบสารสนเทศของ สคฟ. เป็นรายไตรมาส พร้อมทั้งจัดประชุมเพื่อให้คำปรึกษาแนะนำในการปิด Gap ดังกล่าวด้วย

2.2.5 ต้องร่วมมือกับ สคฟ. ดำเนินการซักซ้อมแผนการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ เพื่อเป็นการพัฒนาและปรับปรุงแผน อย่างน้อย 3 ครั้ง (ปีละ 1 ครั้ง)

2.2.6 จัดอบรมการใช้งานระบบหรือเครื่องมือที่นำมาให้บริการ สคฟ. อย่างน้อย 1 ครั้ง ภายในระยะเวลาของการให้บริการเดือนที่ 3 หากระบบหรือเครื่องมือที่นำมาให้บริการมีการปรับเปลี่ยนเวอร์ชันหรือฟังก์ชันอย่างมีนัยสำคัญ ต้องดำเนินการจัดอบรมเพิ่มเติมให้แก่ สคฟ.

2.2.7 หากระบบสารสนเทศของ สคฟ. ถูกภัยไซเบอร์คุกคามหรือโจมตีได้สำเร็จ ต้องมีทีมงานผู้เชี่ยวชาญดำเนินการแก้ไขและกู้คืนให้ระบบสารสนเทศกลับมาใช้งานได้โดยเร็ว พร้อมจัดทำสรุปปัญหา วิธีการแก้ไข วิธีการป้องกันและรับมือ โดยกระบวนการต่าง ๆ ต้องเป็นไปตามมาตรฐานสากล (ถ้ามี)

2.2.8 ผู้ให้บริการต้องรับประกันการให้บริการตามขอบเขตงานข้อ 2.2.1 – 2.2.3 ตลอดระยะเวลา 24 ชั่วโมงทุกวัน (24x7) ตลอดอายุสัญญา หากไม่สามารถให้บริการส่วนใดส่วนหนึ่งตามข้อกำหนด ต้องดำเนินการให้สามารถกลับมาให้บริการได้ ภายใน 4 ชั่วโมง นับถัดจากที่ได้รับแจ้งจาก สคฟ. เป็นลายลักษณ์อักษรผ่านช่องทางจดหมายอิเล็กทรอนิกส์

### 3. ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการ 3 ปี นับถัดจากวันที่ลงนาม

### 4. การส่งมอบงาน

ผู้ให้บริการจะต้องส่งมอบงานเป็นรายงวดตามสัญญา ทั้งหมด 36 งวด โดยมีสิ่งส่งมอบ ดังนี้

งวดที่	สิ่งส่งมอบ	ระยะเวลาส่งมอบ
1	1) แผนการทำงานโครงการ 2) รายงานการติดตั้ง การปรับตั้งค่า ระบบหรือเครื่องมือที่นำมาให้บริการ สคผ. 3) เอกสารการรับรองการให้บริการระบบหรือเครื่องมือตามข้อกำหนด 2.2.3 ที่ครอบคลุมเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศ ของ สคผ. จำนวนไม่น้อยกว่า 400 เครื่อง ของการให้บริการปีที่ 1 4) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 1 5) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 1	ข้อ 1 ภายใน 30 วัน นับถัดจากวันลงนามสัญญา ข้อ 2-5 ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 1
2	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 2 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 2	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 2
3	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 3 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 3 3) รายงานการวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนด 2.2.4.3 พร้อมทั้งรายงานการประชุมการให้คำปรึกษาปิด Gap รายไตรมาส 4) รายงานการจัดอบรมการใช้งานระบบหรือเครื่องมือที่นำมาให้บริการ สคผ. ตามข้อกำหนด 2.2.6	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 3
4	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 4 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 4	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 4
5	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 5 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 5	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 5
6	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 6 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 6 3) รายงานการวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนด 2.2.4.3 พร้อมทั้งรายงานการประชุมการให้คำปรึกษาปิด Gap รายไตรมาส	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 6

งวดที่	สิ่งส่งมอบ	ระยะเวลาส่งมอบ
7	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 7 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 7	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 7
8	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 8 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 8	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 8
9	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 9 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 9 3) รายงานการวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนด 2.2.4.3 พร้อมทั้งรายงานการประชุมการให้คำปรึกษาปิด Gap รายไตรมาส	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 9
10	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 10 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 10	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 10
11	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 11 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 11	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 11
12	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 12 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 12 3) รายงานการวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนด 2.2.4.3 พร้อมทั้งรายงานการประชุมการให้คำปรึกษาปิด Gap รายไตรมาส 4) รายงานการซักซ้อมแผนการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ร่วมกับ สคผ. ครั้งที่ 1 5) เอกสารการรับรองการให้บริการระบบหรือเครื่องมือตามข้อกำหนด 2.2.3 ที่ครอบคลุมเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศของ สคผ. จำนวนไม่น้อยกว่า 400 เครื่อง ของการให้บริการปีที่ 2	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 12
13	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 13	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 13





งวดที่	สิ่งส่งมอบ	ระยะเวลาส่งมอบ
	2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 21 3) รายงานการวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนด 2.2.4.3 พร้อมทั้งรายงานการประชุมการให้คำปรึกษาปิด Gap รายไตรมาส	
22	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 22 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 22	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 22
23	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 23 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 23	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 23
24	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 24 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 24 3) รายงานการวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนด 2.2.4.3 พร้อมทั้งรายงานการประชุมการให้คำปรึกษาปิด Gap รายไตรมาส 4) รายงานการซักซ้อมแผนการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ร่วมกับ สคผ. ครั้งที่ 2 5) เอกสารการรับรองการให้บริการระบบหรือเครื่องมือตามข้อกำหนด 2.2.3 ที่ครอบคลุมเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศของ สคผ. จำนวนไม่น้อยกว่า 400 เครื่อง ของการให้บริการปีที่ 3	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 24
25	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 25 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 25	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 25
26	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 26 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 26	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 26
27	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 27 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคผ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 27	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 27



งวดที่	สิ่งส่งมอบ	ระยะเวลาส่งมอบ
	2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคฟ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 35	
36	1) รายงานสรุปสถานะการจัดเก็บ Log ตามข้อกำหนด 2.2.4.1 ของการให้บริการเดือนที่ 36 2) รายงานสรุปภาพรวมเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สคฟ. ตามข้อกำหนด 2.2.4.2 ของการให้บริการเดือนที่ 36 3) รายงานการวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนด 2.2.4.3 พร้อมทั้งรายงานการประชุมการให้คำปรึกษาปิด Gap รายไตรมาส 4) รายงานการซักซ้อมแผนการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ร่วมกับ สคฟ. ครั้งที่ 3 5) หนังสือรับรองการจัดเก็บ Log ให้ครบตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กำหนดไว้หรือส่งมอบ Log ตามที่ สคฟ. ร้องขอ และเอกสารการทำลายข้อมูล Log ที่จัดเก็บไว้ที่ผู้ให้บริการอย่างถูกต้องตามหลักการมาตรฐานสากล	ภายใน 15 วัน นับถัดจากวันสิ้นสุดการให้บริการของเดือนที่ 36

## 5. เงื่อนไขการจ่ายเงิน

สคฟ. จะจ่ายเงินค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่ม ค่าดำเนินการอื่นใดและค่าใช้จ่ายที่พึงพอใจแก่ผู้ให้บริการ โดยแบ่งออกเป็น 36 งวด งวดละเท่ากัน

## 6. ความรับผิดชอบในความชำรุดบกพร่องของงานจ้าง

ผู้รับจ้างต้องรับประกันผลงานและการชำรุดเสียหายของระบบหรือเครื่องมือที่นำมาให้บริการ สคฟ. ตลอดระยะเวลา 24 ชั่วโมง ทุกวัน (24x7) ตลอดอายุสัญญา

เมื่อมีการชำรุดเสียหายเกิดขึ้นในงานที่จ้าง ไม่สามารถให้บริการระบบหรือเครื่องมือที่นำเสนอได้ ผู้รับจ้างต้องดำเนินการแก้ไขให้แล้วเสร็จและกลับมาใช้งานได้ตามปกติภายในกำหนด 4 ชั่วโมง นับถัดจากที่ได้รับแจ้งจาก สคฟ. เป็นหนังสือหรือด้วยวิธีการอื่นใด

## 7. ค่าปรับ

1) ในกรณีที่ผู้รับจ้างไม่สามารถปฏิบัติตามข้อกำหนดในขอบเขตของงานนี้ ไม่ว่าข้อหนึ่งข้อใด และ/หรือ ไม่สามารถส่งมอบงานได้ตามเวลาที่กำหนดในข้อ 4 สคฟ. มีสิทธิเรียกให้ผู้รับจ้างชำระค่าปรับเป็นรายวันในอัตรา 0.20 ของมูลค่างานรายงวด นับจากวันที่ครบกำหนด จนถึงวันที่ทำงานแล้วเสร็จ และได้แจ้งให้ สคฟ. ทราบแล้ว

2) ในกรณีที่ผู้รับจ้างไม่สามารถดำเนินการแจ้งเตือนเหตุการณ์ ภายในกำหนดเวลาตามข้อ 2.2.2.1 สคฟ. มีสิทธิเรียกให้ ผู้รับจ้างชำระค่าปรับเป็นรายชั่วโมง ในส่วนที่เกินเวลาที่กำหนดไว้ในขอบเขตของงานในอัตราชั่วโมงละ 0.035 ของมูลค่างานจ้างตามสัญญา โดยเศษของเวลาที่เกินกว่า 1 นาที ให้นับเป็นหนึ่งชั่วโมง อีกทั้งผู้รับจ้างจะต้องรับผิดชอบในค่าเสียหายที่อาจเกิดขึ้นจากการแจ้งเตือนเหตุการณ์วิกฤตที่ล่าช้าด้วย

3) ในกรณีที่ผู้รับจ้างไม่สามารถซ่อมแซม แก้ไข เปลี่ยนแปลง งานบริการ ระบบ เครื่องมือ หรือ อุปกรณ์ ที่เกิดขัดข้อง หรือเกิดจากการชำรุดบกพร่อง ภายในระยะเวลาที่กำหนด ในข้อ 2.2.8 สคผ. มีสิทธิเรียกให้ผู้รับจ้างชำระค่าปรับเป็นรายชั่วโมง ในส่วนที่เกินเวลาที่กำหนดไว้ในขอบเขตของงาน ในอัตราชั่วโมงละ 0.035 ของมูลค่างานตามสัญญา โดยเศษของเวลาที่เกินกว่า 15 นาที ให้นับเป็น หนึ่งชั่วโมง

## 8. คุณสมบัติของผู้ยื่นข้อเสนอ

8.1 มีความสามารถตามกฎหมาย

8.2 ไม่เป็นบุคคลล้มละลาย

8.3 ไม่อยู่ระหว่างเลิกกิจการ

8.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

8.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

8.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

8.7 เป็นนิติบุคคลผู้มีอาชีพขายหรือรับจ้าง

8.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการเสนอราคาครั้งนี้

8.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

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

8.11 ผู้ยื่นข้อเสนอต้องมีศูนย์การรักษาความปลอดภัยสารสนเทศ (Security Operation Center : SOC) ที่ให้บริการตลอด 24 ชั่วโมง หรือได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์ และต้องผ่านการตรวจรับรองมาตรฐานการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 หรือ SOC1 หรือ SOC2 โดยเอกสารรับรองมาตรฐาน (Certificate) ต้องมีอายุการรับรองจนถึงวันยื่นข้อเสนอ

8.12 ผู้ยื่นข้อเสนอต้องมีการมอบหมายทีมงานที่มีความรู้ความสามารถในการให้บริการ สคผ. สามารถติดต่อได้ตลอด 24 ชั่วโมง ตลอดอายุสัญญา

8.13 ผู้ยื่นข้อเสนอต้องจัดทำเอกสารการนำเสนอแผนงาน ขั้นตอน กระบวนการ วิธีการ รวมถึงเครื่องมือที่จะนำมาใช้ในการให้บริการ สคผ. ตามข้อกำหนด และต้องมีการนำเสนอให้คณะกรรมการจัดหาพัสดุ รายละเอียดไม่เกิน 1 ชั่วโมง (โดย 45 นาที สำหรับการนำเสนอ และ 15 นาที สำหรับการถาม - ตอบ)

8.14 ผู้ยื่นข้อเสนอต้องมีประสบการณ์ในการให้บริการศูนย์การรักษาความปลอดภัยสารสนเทศ (Security Operation Center : SOC) หรือโครงการติดตั้งอุปกรณ์และซอฟต์แวร์ป้องกันภัยคุกคามทาง Cyber Security แก่หน่วยงานต่าง ๆ ไม่น้อยกว่า 2 ผลงาน และมีมูลค่าโครงการไม่ต่ำกว่า 3,000,000 บาท (สามล้าน

บาทถ้วน) โดยต้องแสดงรายละเอียดผลงาน เช่น หนังสือรับรองผลงานจากผู้ว่าจ้างเดิม หรือ สำเนาสัญญาจ้าง หรือ เอกสารอื่นที่แสดงว่าผู้ยื่นข้อเสนอได้ให้บริการศูนย์ SOC เพื่อยืนยัน เป็นต้น หากไม่สามารถระบุชื่อ หน่วยงานหรือลูกค้าเนื่องจากติดสัญญาการรักษาความลับ ให้ระบุเป็นประเภทของหน่วยงาน เช่น หน่วยงาน ภาครัฐ เอกชน ราชการ สถาบันการเงิน เป็นต้น

8.15 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566 ดังนี้

(1) มูลค่าสุทธิของกิจการ

(1.1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(1.2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้าต้องมีทุนจดทะเบียนไม่ต่ำกว่า 2 ล้านบาท

(1.3) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอจนถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

ทั้งนี้ หนังสือรับรองวงเงินสินเชื่อให้เป็นไปตามแบบที่ กวจ. กำหนด

(2) ข้อยกเว้น

(2.1) กรณีตามข้อ (1.1) – ข้อ (1.3) ไม่ใช่บังคับกับกรณีดังต่อไปนี้

(2.1.1) ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(2.1.2) นิติบุคคลที่จัดตั้งตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

15.16 ผู้ยื่นข้อเสนอต้องลงนามในเอกสารข้อตกลงในการเก็บรักษาข้อมูลเป็นลับ (Non-disclosure Agreement)

15.17 ผู้ยื่นข้อเสนอต้องลงนามหนังสือข้อตกลงให้ประมวลผลข้อมูล (Data Processing Agreement)

## 9. วงเงินในการจัดหา

จำนวนเงิน 10,000,000.00 บาท (สิบล้านบาทถ้วน)

## 10. การยื่นข้อเสนอ

**ส่วนที่ 1** คุณสมบัติของผู้ยื่นข้อเสนอ อย่างน้อยต้องประกอบไปด้วยเอกสาร ดังต่อไปนี้

### 10.1 กรณีนิติบุคคล

(1) สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล ออกโดยกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ภายใน 6 เดือน นับจนถึงวันเสนอราคา (กรณีเป็นห้างหุ้นส่วนสามัญ ห้างหุ้นส่วนจำกัด บริษัทจำกัด หรือบริษัทมหาชนจำกัด)

(2) สำเนาหนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) บัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี) และบัญชีรายชื่อผู้ถือหุ้น (บอจ.5) (กรณีเป็นบริษัทจำกัด หรือบริษัทมหาชนจำกัด)

10.2 ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า ให้สำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (1) หรือ (2) ของผู้ร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน หรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่มีได้ถือสัญชาติไทย พร้อมทั้งรับรองสำเนาถูกต้อง

10.3 สำเนาใบทะเบียนพาณิชย์ (ถ้ามี)

10.4 สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ถ้ามี)

10.5 ในกรณีผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทน ให้แนบหนังสือมอบอำนาจ ซึ่งติดอากรแสตมป์ตามกฎหมาย โดยมีสำเนาบัตรประชาชนที่รับรองสำเนาถูกต้องแล้วเป็นหลักฐานแสดงตนของผู้มอบอำนาจและผู้รับมอบอำนาจ

10.6 หนังสือรับรองผลงาน และ/หรือ สำเนาสัญญาจ้าง ตามข้อ 8.14

10.7 แบบแสดงการลงทะเบียนในระบบ e – GP

ทั้งนี้เอกสารในข้อ 10.1 ถึงข้อ 10.7 ต้องมีลายมือชื่อของผู้มีอำนาจลงนาม หากเป็นเอกสารแสดงตนต้องมีลายมือชื่อรับรองสำเนาถูกต้อง พร้อมประทับตรานิติบุคคล (หากเป็นนิติบุคคลและมีตราประทับ) ในเอกสารทุกฉบับ

## ส่วนที่ 2 ข้อเสนอทางเทคนิค

ผู้ยื่นข้อเสนอต้องจัดทำ เอกสารนำเสนอ (Proposal) ต่อ สคฟ. โดยมีรายละเอียดอย่างน้อย ดังนี้

- แผนงาน/โครงการ (Project Schedule)
- แผนภาพขั้นตอน กระบวนการ วิธีการดำเนินการ และเครื่องมือที่นำมาใช้ในโครงการ

ทั้งนี้ ผู้ยื่นข้อเสนอต้องนำเสนอ Proposal ณ ที่ทำการของ สคฟ. ตามวันและเวลาที่ สคฟ. กำหนด

## ส่วนที่ 3 ข้อเสนอด้านราคา

ผู้ยื่นข้อเสนอต้องจัดทำข้อเสนอด้านราคาจำนวน 1 ชุด ลงลายมือชื่อผู้มีอำนาจพร้อมประทับตรา (ถ้ามี) ในเอกสารทุกหน้าโดยราคาที่เสนอเป็นราคา (แบบเหมารวม Lump Sum) ที่รวมภาษีมูลค่าเพิ่ม ค่าดำเนินการและค่าใช้จ่ายทั้งหมดแล้ว

## 11. หลักเกณฑ์การพิจารณาคัดเลือก

สคฟ. ได้กำหนดเกณฑ์ในการพิจารณาข้อเสนอโครงการจ้างบริการจัดเก็บ log file และบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณาคัดเลือกจากเกณฑ์ Price Performance โดยจะพิจารณาให้คะแนนตามที่กำหนด ดังนี้

(1) ข้อเสนอด้านราคา กำหนดน้ำหนักที่ร้อยละ 20

ตามการคำนวณของกรมบัญชีกลางจากสูตร ดังนี้

$$100 - ((\text{ราคาของผู้ยื่นข้อเสนอ} - \text{ราคาต่ำสุด}) / \text{ราคาต่ำสุด}) * 100$$

(2) ข้อเสนอด้านเทคนิค กำหนดน้ำหนักที่ร้อยละ 80 โดยมีเกณฑ์การให้คะแนน ดังนี้

(2.1) ด้านการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log) น้ำหนักร้อยละ 10

(2.2) ด้านการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ น้ำหนักร้อยละ 30

(2.2) ด้านการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ ร้อยละ 40

(3) การนำเสนอแผนงาน ขั้นตอน กระบวนการ วิธีการ และเครื่องมือที่ใช้ในโครงการที่เป็นประโยชน์กับ สคฟ. ดังนี้

(3.1) การนำเสนอด้านการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log) น้ำหนักร้อยละ 10 โดยมีรายละเอียด การนำเสนอระบบหรือเครื่องมือประเภท Log Transporter หรือ Log Collector หรือ Log Forwarder ที่เป็น Virtual Machine มาติดตั้งที่ศูนย์คอมพิวเตอร์ของ สคฟ. และทำการจัดส่ง Log ไปจัดเก็บที่ศูนย์ข้อมูลของ ผู้ยื่นข้อเสนอ พร้อมส่งเอกสารประกอบการนำเสนอ น้ำหนักคะแนนที่ร้อยละ 10

คะแนนย่อย	เกณฑ์การให้คะแนน/รายละเอียด
5	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคฟ. ด้านการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยส่วนมาก มากกว่าร้อยละ 90
3	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคฟ. ด้านการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยส่วนใหญ่ ระหว่าง ร้อยละ 70 และ 90
1	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคฟ. ด้านการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log) เป็นบางส่วนต่ำกว่า ร้อยละ 70

(3.2) การนำเสนอด้านการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ ร้อยละ 30 โดยมีรายละเอียดดังนี้

(3.2.1) การนำเสนอระบบหรือเครื่องมือที่นำมาให้บริการต้องมีแพลตฟอร์มเป็นลักษณะของ Software-as-a-Service ที่ Hosted และ Managed บน Cloud และต้องได้รับการรับรองมาตรฐาน ISO/IEC:27001 หรือ SOC1 หรือ SOC2 ได้เป็นอย่างน้อย พร้อมส่งเอกสารประกอบการนำเสนอ น้ำหนักคะแนนที่ร้อยละ 10

คะแนนย่อย	เกณฑ์การให้คะแนน/รายละเอียด
5	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ โดยส่วนมาก มากกว่าร้อยละ 90
3	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ โดยส่วนใหญ่ ระหว่างร้อยละ 70 และ 90
1	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ เป็นบางส่วนต่ำกว่าร้อยละ 70

(3.2.2) การนำเสนอ ขั้นตอน กระบวนการ หรือวิธีการออกแผนการตอบสนองต่อเหตุการณ์ภัยคุกคาม แบบ step-by-step และดำเนินการทำการตอบสนองเพื่อตอบโต้ภัยคุกคามที่ระดับอันตรายได้อัตโนมัติผ่าน Automated Playbooks และสามารถสั่งงานเพิ่มเติมได้ เช่น isolate endpoint, remote shell, remote custom script, collect file, dump process memory, terminate process, add to block list, force password reset เป็นต้น รวมทั้งการบริหารจัดการ Case ที่เกิดขึ้นได้ โดยจะต้องมีการวิเคราะห์, แจ้งเตือน แนะนำวิธีการแก้ไข และทำการปิด Case พร้อมระบุรายละเอียดเพิ่มเติมให้สำหรับ Case ที่เกิดขึ้น (Case Management) พร้อมส่งเอกสารประกอบการนำเสนอ น้าหนักคะแนนที่ร้อยละ 20

คะแนนย่อย	เกณฑ์การให้คะแนน/รายละเอียด
5	ขั้นตอน กระบวนการ หรือวิธีการ ที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ โดยส่วนมาก มากกว่าร้อยละ 90
3	ขั้นตอน กระบวนการ หรือวิธีการ ที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ โดยส่วนใหญ่ ระหว่าง ร้อยละ 70 และ 90
1	ขั้นตอน กระบวนการ หรือวิธีการ ที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการเฝ้าระวังและบริหารจัดการภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและไซเบอร์ เป็นบางส่วนต่ำกว่า ร้อยละ 70

(3.3) การนำเสนอด้านการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ ร้อยละ 40 โดยมีรายละเอียดดังนี้

(3.3.1) การนำเสนอระบบหรือเครื่องมือบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Attack Surface Risk Management หรือ Attack Surface Management) ที่ครอบคลุมเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศ ของ สคผ. จำนวนไม่น้อยกว่า 400 Licenses พร้อมส่งเอกสารประกอบการนำเสนอ น้าหนักคะแนนที่ร้อยละ 20

คะแนนย่อย	เกณฑ์การให้คะแนน/รายละเอียด
5	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยส่วนมาก มากกว่าร้อยละ 90



คะแนนย่อย	เกณฑ์การให้คะแนน/รายละเอียด
3	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ.ด้านการบริหารจัดการ ความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยส่วนใหญ่ ระหว่าง ร้อยละ 70 และ 90
1	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการบริหาร จัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ เป็นบางส่วนต่ำกว่า ร้อยละ 70

(3.3.2) การนำเสนอ ขั้นตอน กระบวนการ หรือวิธีการ ค้นหาช่องทางที่มีความเสี่ยงจาก ภายในองค์กรและความเสี่ยงจากภายนอกองค์กร (Attack Surface Discovery) เช่น Devices, Internet-Facing Assets, Accounts, Application, Cloud Assets และ APIs ได้เป็นอย่างดี และจะต้องสามารถ แสดงรายละเอียดของแต่ละรายการเพื่อให้ทราบถึงความเสี่ยงที่มีในองค์กรได้ และแสดงผลค่าความเสี่ยงได้ใน หลายมิติ เช่น Account Compromise, Vulnerabilities, Activity and Behaviors, Cloud App Activity, System Configuration, XDR Detection, Threat Detection, Security Configuration และจะต้องสามารถ ตรวจสอบข้อมูลเจาะลึกลงไปในแต่ละหัวข้อเพื่อความชัดเจนของความเสี่ยงในแต่ละด้านได้ พร้อมส่งเอกสาร ประกอบการนำเสนอ นักคะแนนที่ร้อยละ 20

คะแนนย่อย	เกณฑ์การให้คะแนน/รายละเอียด
5	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการบริหาร จัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยส่วนมาก มากกว่าร้อยละ 90
3	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ.ด้านการบริหารจัดการ ความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยส่วนใหญ่ ระหว่าง ร้อยละ 70 และ 90
1	ระบบหรือเครื่องมือที่ใช้ในโครงการ ตรงกับความต้องการของ สคผ. ด้านการบริหาร จัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ เป็นบางส่วนต่ำกว่า ร้อยละ 70

## 12. หน่วยงานรับผิดชอบ

ฝ่ายเทคโนโลยีสารสนเทศ สถาบันคุ้มครองเงินฝาก

อาคารเอสเจ อินฟินิท วัน บิสซิเนสคอมเพล็กซ์

ชั้น 25-27 เลขที่ 349 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900

โทรศัพท์ 0-2272-0300 ต่อ 275

E-mail/ไปรษณีย์อิเล็กทรอนิกส์ singhans@dpa.or.th