**บริษัท บริหารสินทรัพย์สุขุมวิท จำกัด**

**รายละเอียดคุณลักษณะเฉพาะ/ขอบเขตของงาน (Terms of Reference: TOR)**

# ซื้อระบบป้องกันการรั่วไหลของข้อมูล

---

## 1. ความเป็นมา

บริษัท บริหารสินทรัพย์สุขุมวิท จำกัด (บสส.) มีสถานะเป็นหน่วยงานของรัฐ มีวัตถุประสงค์ในการประกอบกิจการบริหารสินทรัพย์ โดยการรับซื้อ รับโอน และรับจ้างบริหารสินทรัพย์ด้อยคุณภาพ และทรัพย์สินรอการขาย ตามพระราชกำหนดบริษัทบริหารสินทรัพย์ พ.ศ.2541 มีความประสงค์จะดำเนินการจัดซื้อจัดจ้างพัสดุ เพื่อใช้ในการดำเนินกิจการของ บสส. จึงประกาศรายละเอียด คุณลักษณะเฉพาะและขอบเขตของงาน ดังมีรายละเอียดต่อไปนี้

## 2. วัตถุประสงค์

โดยที่ บสส. มีความประสงค์จะซื้อและติดตั้งระบบป้องกันการรั่วไหลของข้อมูลเพื่อ

2.1 ป้องกันข้อมูลที่สำคัญของ บสส. มิให้รั่วไหลออกไปภายนอก

2.2 ปรับปรุง Information / Data Classification เพื่อกำหนด และจัดแบ่งกลุ่มข้อมูลตามลำดับชั้นความสำคัญให้เป็นปัจจุบัน

2.3 จัดทำนโยบายการจัดการข้อมูล เพื่อลดความเสี่ยงการรั่วไหลของข้อมูลสำคัญผ่านช่องทางดังกล่าว

## 3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดา หรือ นิติบุคคล ผู้มีอาชีพรับจ้างตามขอบเขตของงานนี้

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ บสส. ณ วันยื่นเสนอราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการเสนอราคาจัดซื้อพัสดุครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องเป็นผู้มีประสบการณ์หรือมีผลงานในการติดตั้งระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System) หรือมีผลงานการเป็นที่ปรึกษาหรือผลงานในการทำโครงการที่เป็นประเภทเดียวกันกับงานตาม TOR นี้ ให้แก่หน่วยงานราชการ รัฐวิสาหกิจ หรือองค์กรเอกชนในประเทศไทย โดยมูลค่าของสัญญาต้องไม่น้อยกว่า 7,250,000 บาท (เจ็ดล้านสองแสนห้าหมื่นบาทถ้วน) ต่อสัญญา โดยเป็นผลงานที่แล้วเสร็จภายในระยะเวลาไม่เกิน 3 ปี( 2562-2565) นับถัดจากวันที่งานแล้วเสร็จจนถึงวันที่ยื่นข้อเสนอ โดยให้แนบหนังสือรับรองผลงานดังกล่าวมาแสดงในวันยื่นข้อเสนอ

3.12 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายผลิตภัณฑ์ที่เสนอ จากเจ้าของผลิตภัณฑ์หรือจากสาขาของเจ้าของผลิตภัณฑ์ที่ตั้งอยู่ในประเทศไทย โดยมีหนังสือยืนยันการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์หรือจากสาขาเจ้าของผลิตภัณฑ์ที่ตั้งอยู่ในประเทศไทยที่ถูกต้องตามกฎหมาย ในกรณีที่ผู้ยื่นข้อเสนอมิใช่ตัวแทนจำหน่ายตามข้อกำหนดข้างต้น ผู้ยื่นข้อเสนอต้องมีหนังสือยืนยันการแต่งตั้งให้เป็นตัวแทนจำหน่ายเฉพาะในการเสนอราคาครั้งนี้จากเจ้าของผลิตภัณฑ์ หรือจากสาขาของเจ้าของผลิตภัณฑ์ตามข้อกำหนดข้างต้น ซึ่งตัวแทนจำหน่ายนั้นต้องยังคงสถานะเป็นตัวแทนจำหน่ายในประเทศไทยที่ถูกต้องตามกฎหมายโดยมีหนังสือยืนยันการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์นั้นด้วย โดยหนังสือแต่งตั้งตัวแทนจำหน่ายทุกกรณีต้องมีสถานะยืนยันเป็นตัวแทนจนถึงวันที่ยื่นเสนอราคา

**4. รายละเอียดคุณลักษณะเฉพาะพัสดุ/ขอบเขตการให้บริการ**

พัสดุที่ บสส. ประสงค์จะซื้อ ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่จะใช้งานได้ทันที และมีคุณลักษณะเฉพาะตรงตามที่ บสส. กำหนดดังต่อไปนี้

4.1 ระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System: DLP) จำนวน 1 ระบบ มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

4.1.1 มีสิทธิการใช้งานและการบำรุงรักษาจำนวนอย่างน้อย 700 ผู้ใช้งาน เป็นระยะเวลาไม่น้อยกว่า 3 ปี

4.1.2 ป้องกันข้อมูลรั่วไหลจากช่องทางอย่างน้อยดังนี้

(1) Network (Data in Motion)

(2) Endpoint (Data in Use)

(3) Storage หรือ Server (Data at Rest)

4.1.3 ซอฟต์แวร์ระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System: DLP) ที่เสนอจะต้องอยู่ใน Gartner Magic Quadrant (Content-Aware Data Loss Prevention) กลุ่ม Leader ของปี 2017 หรือปีล่าสุด (ครั้งล่าสุด) และมีสาขาดำเนินธุรกิจเกี่ยวกับระบบป้องกันการรั่วไหลของข้อมูล Data Leak Prevention ประจำประเทศไทย โดยต้องส่งเอกสารหลักฐานแสดง Leader ของ Gartner Magic Quadrant ดังกล่าว และเอกสารแสดงสาขาหรือตัวแทนจำหน่ายที่ดำเนินธุรกิจเกี่ยวกับระบบป้องกันการรั่วไหลของข้อมูล Data Leak Prevention ประจำประเทศไทย

4.1.4 DLP Management Server ต้องสามารถใช้งานร่วมกับระบบบริหารจัดการฐานข้อมูล ฐานข้อมูล Oracle หรือ MS SQL ได้ ทั้งนี้ผู้เสนอราคาต้องเสนอซอฟต์แวร์ระบบบริหารจัดการฐานข้อมูลที่มีลิขสิทธิ์การใช้งานอย่างถูกต้อง เป็นระยะเวลาไม่น้อยกว่า 3 ปี มาพร้อมกันด้วย

4.1.5 ระบบที่เสนอต้องมีความสามารถในช่องทาง Network อย่างน้อยดังนี้

(1) ทำงานร่วมกับระบบ Email Gateway (MTA) ของ บสส.

(2) ทำงานร่วมกับระบบ Web Gateway (Proxy) ของ บสส.

(3) กำหนดนโยบายตามกลุ่มผู้ใช้ หรือ กำหนดตาม email address หรือ Domain ได้ และสามารถทำ Workflow Approve หรือ Reject Email ได้

(4) ตรวจจับข้อมูลรั่วไหลได้จากช่องทางการใช้ HTTP/HTTPS, SMTP และ FTP ได้

(5) รองรับในการตรวจจับข้อมูลจาก Port Mirror หรือ Network Tab ได้

(6) ทำงานร่วมกับ Office 365 และสามารถให้บริการเป็น Cloud Service ได้ และบริหารจัดการ DLP Policy/ Incident ได้จากระบบบริหารจัดการ DLP Centralize Management เดียวกัน

4.1.6 ระบบที่เสนอต้องมีความสามารถในช่องทาง Endpoint อย่างน้อยดังนี้

(1) ติดตั้งได้บนระบบปฏิบัติการ Microsoft Windows 7 ขึ้นไป

(2) ตรวจสอบข้อมูลบนเครื่อง Endpoint โดยใช้การ Discovery ข้อมูลได้

(3) ตรวจสอบข้อมูลตามช่องทางต่างๆ ได้แก่ Removable Storage, CD/DVD, Local Drive, Printer/ eFax, Clipboard ( Copy, Paste), Application File Access, Cloud Storage, File System หรือ File Server, Network Shares และ Instant Messaging ได้

(4) ตรวจสอบข้อมูลบน Browser และ Mail Client (Outlook) ได้

(5) สามารถเลือกกำหนด Action ได้อย่างน้อยดังต่อไปนี้ Block, Allow/Permit, Notify, Justify/Confirm

(6) ป้องกันการ Print Screen ได้โดยป้องกันการ Print Screen ผ่านปุ่ม Print Screen บน Keyboard

(7) แสดงข้อความแจ้งเตือนกรณี User ละเมิด Policy และแจ้งข้อความการละเมิด รวมถึงการ Block การใช้งานได้

(8) การแจ้งเตือนบน Endpoint สามารถแสดงผลได้ทั้งภาษาไทย และภาษาอังกฤษ

(9) สามารถกำหนด policy แยกตามกลุ่มผู้ใช้ได้ โดยกำหนดกลุ่มตาม Active Directory หรือ Customize Attribute ได้

(10) จัดกลุ่มของ Endpoint และกำหนดเปิดปิดช่องทางในการตรวจสอบ เช่น Email, Share Drive, Web/Browser

(11) บริหารจัดการทรัพยากร (Resource) ของซอฟต์แวร์ระบบ DLP บนเครื่อง Endpoint เช่น CPU หรือ Bandwidth หรือ Disk ได้

(12) ป้องกันไม่ให้ Agent บน Endpoint ถูกปิด Service หรือ Uninstall ได้

(13) ทำงานได้ตามปกติแม้ว่าจะไม่สามารถติดต่อกับ Management Server (Offline) หรือ Disconnected ออกจาก Network ของ บสส. (Off-Site)

(14) สามารถตรวจสอบและป้องกันข้อมูลผ่านทาง Application Cloud File Sync เป็นอย่างน้อยดังนี้ Dropbox, OneDrive, Google Drive และ iCloud

(15) บริหารจัดการ Endpoint ได้จากหน้า Management เช่น Restart/Stop Agent หรือ Get Agent logs หรือ Change Management Server ได้

(16) ทำ Classification Labeling ได้ โดยทำงานร่วมกับ Software Classification ที่เสนอในโครงการได้ และดึง หรือนำเข้า Policy/Tag ของการ Classified มาใช้งานได้

4.1.7 ระบบที่เสนอต้องมีความสามารถในช่องทาง Storage อย่างน้อยดังนี้

(1) ตรวจสอบข้อมูลบนระบบต่างๆ ได้แก่ Microsoft Exchange, SharePoint, SQL Databases, Web Servers, File Servers, Oracle โดยใช้การ Discovery ข้อมูลได้

(2) ทำการ Discovery ข้อมูล โดยกำหนดให้ค้นหา หรือ ยกเว้นการค้นหาเฉพาะไฟล์บางประเภท (File Type) หรือตำแหน่งที่วางไฟล์ (File Path) และสามารถค้นหาข้อมูลอ้างอิงตามลักษณะข้อมูลจาก Policy ที่กำหนดไว้ได้ เช่น ต้องการค้นหาเฉพาะข้อมูลที่เกี่ยวข้องกับ PCI-DSS เท่านั้น ค้นหาจากอายุและขนาดของไฟล์ เป็นต้น

(3) กำหนด Schedule ในการทำงาน Discovery ตามกำหนด Daily, Weekly ได้

(4) กำหนดให้ตรวจสอบโดยเจาะจงเฉพาะไฟล์ ตามวันและเวลาที่มีการแก้ไข (Date Modified), ตามวันและเวลามีการ Access (Date Accessed) ได้

(5) Copy/Quarantine ไฟล์ที่ละเมิด Policy และกำหนดให้ย้ายไปเก็บไว้ใน Path ที่ต้องการได้

(6) กำหนด Scanner/Detector หรือเพิ่มจำนวน Crawler ในการตรวจสอบข้อมูลบนเครือข่ายได้ เพื่อรองรับปริมาณของไฟล์จำนวนมากของ บสส.

4.1.8 ระบบที่เสนอต้องมีความสามารถด้านการทำ Content Detection Policy, Management, Incident อย่างน้อยดังนี้

(1) ทำ Fingerprint จากข้อมูลที่เป็น Structured Data ได้ เช่น ข้อมูลจาก Database, Directory server

(2) ทำ Fingerprint ไฟล์ข้อมูล CSV หรือรูปแบบอื่นได้ เพื่อทำ fingerprint ไฟล์ที่มีการ Export จาก Database ออกมาได้

(3) ทำ Fingerprint จากข้อมูลที่เป็น Unstructured Data ได้ เช่น เอกสาร Word, Excel, PowerPoint, PDF และ Binary File

(4) กำหนด Schedule ในการปรับปรุงข้อมูล Fingerprint ได้

(5) กำหนด Keyword (คำ) โดยรองรับภาษาไทยและภาษาอังกฤษได้เป็นอย่างน้อยหรือโดยการค้นหาที่ต้อง Match ทั้ง Keyword ไม่ใช่แค่ส่วนหนึ่งของ Keyword

(6) กำหนด Pattern/Regular Expression ของข้อมูล เช่น เลขบัตรเครดิต (สอดคล้องมาตรฐาน PCI-DSS), เลขบัตรประชาชนของไทย, SWIFT Code ได้ และสร้าง Customize Pattern (Data Identifiers) รวมถึงการกำหนด Algorithm/Script ในการตรวจสอบ Checksum ได้

(7) ระบุระดับความเสี่ยง (Severity) ของข้อมูลที่สูญหายโดยการกำหนดจากจำนวนของข้อมูลได้

(8) ตรวจสอบไฟล์และเนื้อหาในไฟล์ที่ถูกบีบอัด (Compressed Files) ที่ไม่ได้เข้ารหัสได้ เช่น Zip, 7Zip, RAR, TAR, UU Encoded, ISO, GZ Compress, Bzip2, LHA, Microsoft Cabinet

(9) ตรวจสอบได้ว่าเป็นไฟล์ที่ถูกเข้ารหัส (Encrypted Files) และกำหนด policy ให้ประเภทไฟล์ดังกล่าวได้ เช่น PGP, ZIP Encryption, PDF Encryption, Microsoft Office Encryption

(10) มี Policy Templates หรือ Solution Packs ที่สอดคล้องกับภาคเศรษฐกิจการเงิน (Financial Sector)

(11) ตรวจสอบเนื้อหาใน File format ต่าง ๆ ในแบบ True File Type ได้ เช่น Microsoft Office Documents (DOC, DOCX, PPT, PPTX, XLS, XLSX) PDF และ Binary File

(12) ป้องกันข้อมูลรั่วไหล หากมีการส่งไฟล์รูปภาพที่มีข้อความ Text ปรากฏในรูปภาพ โดยการแปลงข้อความที่ปรากฏเป็น Key Phase เพื่อตรวจสอบร่วมกับ DLP Policy ที่กำหนดไว้ ด้วยเทคโนโลยี Optical Characteristic Recognition (OCR) ผ่านทางโปรโตคอล SMTP และ HTTP ได้

(13) กำหนด Policy/Rule ที่ใช้ในการตรวจสอบข้อมูลร่วมกันได้บนทุกช่องทาง ได้แก่ Network, Endpoint และ Storage

(14) กำหนด Detection Rule ตามข้อกำหนดต่าง ๆ ได้ เช่น

a. Regular Expression/Pattern
b. Fingerprint Profiles
c. Keyword
d. File Type Match
e. File Size Match
f. File Name Match
g. Customize File type
h. Endpoint Protocol เช่น TCP/SMTP, TCP/HTTP หรือช่องทางใช้งาน เช่น Removable Storage, Local Drive, Printer/ eFax, Clipboard (Copy, Paste), Network Shares
i. Endpoint Device Class/ID เช่น Class ID ของ Removable Storage
j. Endpoint Location เช่น On-Site หรือ Off-Site

(15) สร้าง Detection Rule โดยผสมข้อกำหนดต่าง ๆ ข้างต้นได้ (And/Or) และสร้าง Exception Rule เพื่อทำการยกเว้นได้

(16) ตรวจสอบข้อมูล User โดย Integrate กับ Active Directory ได้ และสามารถกำหนด Policy ตามกลุ่มของ User อ้างอิงจาก Active Directory ดังกล่าว

(17) แจ้งเตือนผู้ละเมิดและผู้ที่เกี่ยวข้องในกรณีตรวจพบการละเมิดได้ ผ่านทางอีเมล์ ได้แก่ หัวหน้างาน หรือ เจ้าของข้อมูล

(18) กำหนด User Role ที่แตกต่างกันเพื่อใช้ในการบริหารจัดการระบบ เช่น การบริหารจัดการ Policy, การบริหารจัดการ System, การบริหารจัดการ Incident, หรือ กำหนดเป็น View only

(19) กำหนดการ Action เช่น Notify, Justify/Confirm, Allow, Block และ Quarantine และกำหนด Action แยกตามช่องทางการใช้ข้อมูลได้

(20) มี Dashboard สำหรับแสดงภาพรวมภายในองค์กร ที่สามารถแสดงนโยบายที่ถูกละเมิดและ Trend ของเหตุการณ์ที่เกิดได้

(21) มีระบบบริหารจัดการ Incident (Incident Management) ได้ซึ่งประกอบไปด้วย Incident Report ตามช่องทางต่าง ๆ และสามารถสร้าง Summary Report ตามความต้องการได้ เช่น แบ่งตามกลุ่มของ User/แผนก, ตาม Policy

(22) มีข้อมูล Incident Detail ซึ่งสอดคล้องกับ What, When, Who, Where, How ได้ และแสดงข้อมูลดังต่อไปนี้

a. ผู้ละเมิด (Sender, IP Address, Endpoint Name)

b. วัน เวลา

c. ผู้รับ หรือช่องทางในการส่งข้อมูล (Protocol)

d. ตัวอย่างข้อมูลที่ตรวจพบ หรือไฟล์ต้นฉบับ

(23) เปลี่ยนแปลง Status (สถานะ) ของ Incident ได้ เช่น New, Investigate/In progress, Escalate, Close

(24) บันทึกการแก้ไขเปลี่ยนแปลง Incident เพื่อใช้ในการตรวจสอบได้

(25) มีการจัดการ Incident ต่าง ๆ ที่เกิดขึ้นแบบ Workflow เช่น เมื่อมีการตรวจพบข้อมูลให้แจ้งเจ้าหน้าที่หรือผู้ที่เกี่ยวข้อง เพื่อเข้ามาตรวจสอบ และสามารถทำการ Escalate (ส่งต่อ) หรืออนุมัติการส่งข้อมูลกรณีใช้ร่วมกับระบบ Email Gateway หรือเพื่อการกักเก็บอีเมล์ได้

(26) สามารถ Export ข้อมูลรายงานในรูปแบบ CSV, XML หรือ PDF ได้

4.1.9 ระบบที่เสนอต้องมีความสามารถด้านระบบ Cloud Access Security Broker (CASB) โดยมีคุณสมบัติอย่างน้อยดังนี้

(1) ทำงานร่วมกับ DLP ที่เสนอข้างต้นในการบริหารจัดการ Incident ที่เกิดบนระบบ CASB ตาม Policy ของ DLP ได้บน DLP Management

(2) ตรวจสอบและจัดหมวดหมู่ Cloud Application ทั้งที่อนุญาต (Sanctioned) ให้ใช้งาน และไม่ได้อนุญาต (Unsanctioned) ให้ใช้งานภายในองค์กรได้

(3) เลือกแสดงผลและจัดทำรายงานการใช้งาน Cloud Application

(4) แสดงข้อมูลในลักษณะ Geo-location ของการเข้าถึง Cloud Application ต่างๆ ได้

(5) รวบรวมข้อมูลการทำ Cloud Application Discovery แบบศูนย์รวมได้

(6) ใช้ API ในการเชื่อมต่อไปยัง Cloud Services Provider เพื่อรับข้อมูล มาวิเคราะห์ได้

(7) มีรายงานแสดงผลการใช้งาน Cloud Application แบบ Usage Metrics เพื่อแสดงผลชื่อผู้ใช้ รายละเอียดกิจกรรม และปริมาณ Traffic ได้

(8) ปรับเปลี่ยน แก้ไขน้ำหนัก (weighting) ที่ใช้ในการประเมินความเสี่ยงของ Cloud Application ได้

(9) มีข้อมูลการจัดหมวดหมู่ของ Cloud Application เช่น Storage, CRM, Online Service ได้

(10) ให้ข้อมูลในเชิงลึกเกี่ยวกับการใช้งาน Cloud Application เพื่อระบุพื้นที่ที่มีความเสี่ยงสูง (high-risk areas) โดยสามารถระบุในลักษณะความเสี่ยงด้านการรักษาความปลอดภัย หรือความเสี่ยงด้านการปฏิบัติตามข้อกำหนด

(11) ตรวจสอบการตั้งค่า Configuration ต่างๆ บน Cloud Application เพื่อเปรียบเทียบกับเกณฑ์มาตรฐานและชุดแนวทางปฏิบัติที่ดีที่สุดในอุตสาหกรรม (Industrial Best Practice) เพื่อดูว่ามีช่องโหว่ด้านความปลอดภัยอยู่ที่ใดได้ บน Cloud Application โดยมี Predefined Policy เช่น ISO 27001 หรือ ISO 27002, NIST , PCI DSS

(12) ตรวจสอบและแสดงรายงาน เมื่อมีผู้ใช้งานดำเนินการสร้าง / ลบ / อัพโหลด / ดาวน์โหลดไฟล์และโฟลเดอร์ทั้งหมด รวมถึงการรายงานชื่อไฟล์และโฟลเดอร์ที่มีการเปลี่ยนแปลง บนพื้นที่เก็บข้อมูลระบบคลาวด์รายใหญ่ทั้งหมด ได้แก่ Office 365, Dropbox, G-Suite เป็นต้น

(13) สนับสนุนการทำงานร่วมกับ Microsoft 365 (Office 365) ได้

(14) ทำ Authentication ร่วมกับ Active Director Services (LDAPs, ADFS) ได้

(15) ทำงานร่วมกับ SAML-based federated authentication infrastructures ได้

(16) ทำ Data Discovery บน Cloud Storage เช่น Office 365, G-Drive

(17) ต้องมี Predefine policy ตามมาตรฐาน PCI, PII เป็นต้น

(18) Customized data type ในการทำ Data Discovery โดยใช้ keywords, dictionaries และ RegEx ได้

(19) ผลลัพธ์ที่ทำ Data Discovery นั้น ต้องแสดงรายชื่อไฟล์ที่ตรงตามมาตรฐานที่ทำการตรวจสอบ และแสดงรายละเอียด Sharing permissions ของไฟล์ และรายละเอียดเจ้าของไฟล์ (File Owner)

(20) กำหนดนโยบายเพื่อยกเว้นการตรวจสอบ (Exception Detection) ในบางกรณีได้

(21) ติดตั้งในรูปแบบ Reverse Proxy แบบ Cloud Services เพื่อรองรับการตรวจสอบ Cloud Application ทั้งแบบ Unsanctionable และ Sanctionable ได้

(22) ทำงานร่วมกับ Cloud Application แบบ API ได้

(23) ทำงานโดยวิเคราะห์ผ่าน Gateway log เช่น Proxy ได้

(24) มีระบบ Incident management, investigate

(25) มีระบบ Incident Management เพื่อตรวจสอบเหตุการณ์ที่เกิดขึ้น และมีการเก็บข้อมูล log เพื่อสนับสนุนการตรวจสอบรายละเอียดย้อนหลังได้ในภายหลัง

(26) Integrate Incident เข้ากับระบบ DLP ที่นำเสนอได้

(27) ส่ง log ไปยัง SIEM Solution ภายนอกได้

4.1.10 ระบบที่เสนอต้องมีระบบบริหารจัดการชั้นข้อมูล (Information / Data Classification) จำนวน 1 ระบบโดยมีคุณสมบัติอย่างน้อยดังนี้

(1) มีลิขสิทธิ์สำหรับใช้งานได้ไม่น้อยกว่า 700 Licenses

(2) ระบบบริหารจัดการชั้นข้อมูลที่เสนอ ต้องสามารถทำสัญลักษณ์อิเล็กทรอนิกส์ (Electronics Label) ให้กับเอกสารได้

(3) ซอฟต์แวร์ที่เสนอต้องสามารถทำงานในลักษณะส่วนเสริม (add-ins) เช่น แสดงตัวเลือกการจัดชั้นเอกสารบนแอพพลิเคชั่น Microsoft Office (Word, Excel, PowerPoint) ได้ เพื่อกำหนดระดับความสำคัญของไฟล์ดังกล่าว

(4) ซอฟต์แวร์ที่เสนอสามารถกำหนด Visual Masking บนไฟล์เอกสารได้ และต้องสามารถปรับตำแหน่งรูปแบบได้ เช่น การเพิ่มรูปภาพและข้อมูลที่มีความยืดหยุ่น เช่น ชื่อผู้ใช้ และวันที่ เป็นต้น

(5) ตรวจสอบข้อความ (content) บนไฟล์ Word, Excel และ PowerPoint ได้

(6) เพิ่มข้อมูลสำหรับการจัดชั้นเอกสาร (Classification) ในคุณสมบัติของไฟล์เอกสารได้และต้องสามารถทำงานร่วมกับ DLP ได้

(7) เลือกกำหนด label ไฟล์ได้โดยไม่เปลี่ยนแปลง Timestamp ของไฟล์ได้

(8) สามารถ labelling policy แบบกลุ่ม และรองรับทำงานร่วมกับ Active Directory ได้

(9) สามารทดสอบการทำงานของ Policy โดยไม่กระทบการใช้งานของผู้ใช้ได้ (Run Test Mode)

(10) สามารถตรวจสอบความสัมพันธ์ของข้อความกับไฟล์แนบ ว่าตรงกับ Classification ที่กำหนดไว้ ในกรณีส่งอีเมล์ผ่าน Microsoft Outlook

(11) ระบบที่เสนอต้องสามารถบริหารจัดการและกำหนดนโยบายการจัดสรรข้อมูลจากส่วนกลางได้

4.2 การติดตั้งระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System: DLP) มีขอบเขตการดำเนินงาน อย่างน้อยดังต่อไปนี้

4.2.1 ผู้เสนอราคาต้องส่งมอบแผนการดำเนินงานอย่างละเอียด และต้องผ่านความเห็นชอบจาก บสส. ภายใน 30 วัน นับถัดจากวันลงนามในสัญญา

4.2.2 ผู้เสนอราคาต้องติดตั้งระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System: DLP) พร้อมทั้งกำหนดเงื่อนไขในการตรวจจับการรั่วไหลของข้อมูลสำคัญ ผ่านช่องทางต่างๆ

4.2.3 ผู้เสนอราคาต้องทำการทดสอบ UAT ตาม Test Plan และ Test Case/script ที่จัดเตรียมไว้ และจัดทำรายงานผลการทดสอบ UAT

4.3 ทำการสำรวจ ตรวจสอบ นโยบายที่ใช้งานอยู่บนระบบเดิม และทบทวนเพื่อนำไปปรับใช้กับระบบ DLP ที่นำเสนอ พร้อมทั้งเปรียบเทียบตามกฎเกณฑ์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

4.3.1 ให้คำแนะนำในการปรับตั้งให้สอดคล้องตามนโยบายคุ้มครองข้อมูลส่วนบุคคล

4.3.2 จัดทำเอกสาร DLP Policy ออกแบบเงื่อนไข (Use Case) และให้คำแนะนำในการสร้างกฎเกณฑ์ (Rule Set) ที่สอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.3.3 ตรวจสอบ ประเมิน และวิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นจากการรั่วไหลของข้อมูลตามนโยบายที่ได้ถูกจัดทำไว้ ร่วมกับทีมงานของ บสส. เพื่อปรับปรุงให้สอดคล้องกับกฎระเบียบข้อบังคับของ บสส.

4.3.4 ตรวจสอบ ประเมิน และวิเคราะห์การจัดลำดับชั้นของข้อมูลตามเอกสารที่ได้ถูกจัดทำไว้ร่วมกับทีมงานของ บสส. เพื่อปรับปรุงให้สอดคล้องกับกฎระเบียบข้อบังคับของ บสส

4.3.5 จัดทำรายงานสรุปผลการดำเนินงาน และข้อเสนอแนะ หรือข้อคิดเห็น เป็นรายเดือนให้กับ บสส.

4.3.6 เข้าร่วมประชุมอย่างน้อยเดือนละ 1 ครั้ง หรือตามความจำเป็น เพื่อชี้แจ้งความคืบหน้าผลการดำเนินงานของโครงการให้กับผู้บริหาร คณะกรรมการ หรือผู้เกี่ยวข้อง (ถ้ามี) พร้อมจัดทำเอกสารและรายงานการประชุม

4.4 ผู้ยื่นข้อเสนอราคาต้องมีบุคลากรหลักที่เข้ามาปฏิบัติงานตลอดระยะเวลาโครงการและตามที่ระบุไว้ในแผนดำเนินงานระดับกิจกรรมอย่างน้อย ดังนี้

4.4.1 ผู้จัดการโครงการในส่วนผู้เชี่ยวชาญด้านการบริหารจัดการข้อมูลอย่างน้อย 1 คน มีคุณสมบัติอย่างน้อย ดังนี้

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี

(2) มีประสบการณ์ไม่น้อยกว่า 3 ปี ในการบริหารโครงการที่เกี่ยวข้องกับการบริหารจัดการข้อมูล (Information Classification) และการป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention) หรือโครงการที่เป็นประเภทเดียวกันกับงานตาม TOR นี้

4.4.2 ผู้จัดการโครงการในส่วนผู้เชี่ยวชาญด้านการติดตั้งผลิตภัณฑ์อย่างน้อย 1 คน มีคุณสมบัติอย่างน้อย ดังนี้

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี

(2) มีประสบการณ์ไม่น้อยกว่า 2 ปี ในการบริหารโครงการที่เกี่ยวข้องกับการบริหารจัดการข้อมูล (Information Classification) และการป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention) หรือโครงการที่เป็นประเภทเดียวกันกับงานตาม TOR นี้

(3) เป็นพนักงานประจำในบริษัทของผู้เสนอราคา

4.4.3 ผู้ปฏิบัติงานด้านการติดตั้งผลิตภัณฑ์อย่างน้อย 2 คน มีคุณสมบัติ อย่างน้อย ดังนี้

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี

(2) เป็นผู้มีความรู้ความเข้าใจในระบบรักษาความปลอดภัยของข้อมูลที่นำเสนอ และต้องได้รับ Certificate จากเจ้าของผลิตภัณฑ์

(3) มีประสบการณ์ในการทำโครงการการป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention) ให้กับสถาบันการเงินในประเทศไทย

(4) เป็นพนักงานประจำในบริษัทของผู้เสนอราคา

4.4.4 ผู้ปฏิบัติงานด้านการบริหารจัดการข้อมูลอย่างน้อย 2 คน มีคุณสมบัติ อย่างน้อย ดังนี้

(1) วุฒิการศึกษาไม่ต่ำกว่าปริญญาตรี

(2) มีประสบการณ์ไม่น้อยกว่า 2 ปี ในการปฏิบัติงานโครงการที่เกี่ยวข้องกับการป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention)

ทั้งนี้ ผู้เสนอราคาต้องเสนอเอกสารแสดงคุณสมบัติ และประสบการณ์ในการทำงานของบุคลากรตามข้อ 4.4.1 – 4.4.4 ซึ่งเอกสารดังกล่าวต้องลงนามรับรองโดยบุคลากรแต่ละคน มาให้ บสส. พิจารณาเห็นชอบก่อนเข้าดำเนินการภายใน 15 วัน นับถัดจากวันเริ่มต้นสัญญา โดยยื่นเอกสารดังนี้

(1) เอกสารประวัติการทำงาน (CV)

(2) สำเนาใบปริญญาบัตร หรือ สำเนา Transcript

(3) สำเนาบัตรพนักงาน หรือ สำเนาหนังสือรับรองการปฏิบัติงานจากบริษัท

(4) เอกสารอ้างอิงจากหน่วยงานที่ได้ไปทำงานตามรายละเอียดคุณสมบัติข้างต้น

**5. กำหนดเวลาส่งมอบพัสดุ**

ส่งมอบพัสดุภายในกำหนด 180 (หนึ่งร้อยแปดสิบ) วัน นับถัดจากวันที่ลงนามสัญญาซื้อขาย

**6. การส่งมอบพัสดุ**

ผู้เสนอราคาจะต้องดำเนินการตามขอบเขตของรายละเอียดคุณลักษณะเฉพาะพัสดุ/ขอบเขตการให้บริการของ บสส. และส่งมอบงานในรูปแบบของเล่มเอกสาร และ Soft file แบบแก้ไขได้ ใส่ Thumb Drive อย่างละ 1 ชุด โดยจัดทำด้วยภาษาไทย และมีรายละเอียดดังนี้

6.1 งวดที่ 1 ผู้เสนอราคาต้องดำเนินการและส่งมอบงานให้ บสส. ภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา ตามรายการ ดังนี้

(1) แผนการดำเนินงาน แสดงรายละเอียดของกิจกรรม ช่วงเวลาดำเนินงาน ผลลัพธ์ และผู้รับผิดชอบในขอบเขตของโครงการ โดยผ่านความเห็นชอบจาก บสส.

(2) เอกสารมาตรฐานการจัดระดับชั้นข้อมูล การทำป้ายชื่อ และการบริหารจัดการข้อมูล (Information Classification, Labeling and Handling Standard)

(3) เอกสารแสดงรายการทะเบียนข้อมูล พร้อมการจัดลำดับชั้นข้อมูล (Information Asset Register)

(4) เอกสารนโยบายค่าติดตั้งการจัดลำดับชั้นข้อมูล (Information Classification Policy Configuration) และการป้องกันข้อมูลรั่วไหล (DLP Policy Configuration)

(5) เอกสาร DLP Policy ออกแบบเงื่อนไข (Use Case) และให้คำแนะนำในการสร้างกฎเกณฑ์ (Rule Set) ที่สอดคล้องกับกฎเกณฑ์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(6) เอกสารแสดงคุณสมบัติของผู้ปฏิบัติงานตามข้อ 4.4

6.2 งวดที่ 2 ผู้เสนอราคาต้องดำเนินการและส่งมอบงานให้ บสส. ภายใน 180 วัน นับถัดจากวันที่ลงนามในสัญญา ตามรายการ ดังนี้

(1) เอกสารสิทธิการใช้งานโปรแกรมทั้งหมด

(2) รายงานสรุปผลการติดตั้งระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System : DLP) ตามสิทธิการใช้งานโปรแกรม พร้อมเอกสารและคู่มือของระบบโดยละเอียด

(3) Test case / script และรายงานผลการทดสอบ UAT พร้อมคำแนะนำเพิ่มเติม

(4) รายงานผลการติดตั้งและการกำหนดเงื่อนไขในการตรวจจับการรั่วไหลของข้อมูลสำคัญผ่านช่องทาง ต่างๆ ตาม TOR ข้อ 4.3

(5) เอกสารคำแนะนำในการปรับนโยบาย (Tuning) เพื่อลดผล False Positive

(6) รายงานการจัดอบรม ประกอบด้วยภาพถ่าย ใบเซ็นชื่อ และเอกสารประกอบการอบรมตามหัวข้อที่กำหนด

a. รายงานการจัดอบรม ความรู้ ความเข้าใจ ให้แก่บุคลากรของ บสส. เกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และเอกสารประกอบการอบรม

b. รายงานการจัดอบรม Data Classification and Data Leak Prevention Awareness ให้กับพนักงานที่ร่วมใน Workshop และเอกสารประกอบการอบรม

c. รายงานการจัดอบรมการใช้งานและการบำรุงรักษาระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System: DLP) ให้กับผู้ดูแลระบบและผู้เกี่ยวข้อง และเอกสารประกอบการอบรม

(7) รายงานสรุปผลการดำเนินงานและ ข้อเสนอแนะหรือข้อคิดเห็น เป็นรายเดือนให้กับ บสส.

(8) รายงานการประชุม

(9) รายการเอกสารที่เปลี่ยนแปลงตามงวดที่ 1 เพิ่มเติม (ถ้ามี)

**7. การทดสอบ ทดลอง และฝึกอบรม**

ผู้เสนอราคาต้องดำเนินการจัดอบรมภายใน 180 วัน นับถัดจากวันที่ลงนามในสัญญา ทั้งนี้ผู้ขายต้องเป็นผู้รับผิดชอบจัดเตรียม เอกสาร และอุปกรณ์ต่างๆ ที่ใช้ในการอบรมทั้งหมด โดยใช้สถานที่ของ บสส. แต่หากสถานการณ์การแพร่ระบาดโควิดยังอยู่ ให้ บสส. สามารถพิจารณาอบรมผ่านสื่ออิเล็กทรอนิกส์ได้

7.1 จัดอบรม ความรู้ ความเข้าใจให้แก่บุคลากรของ บสส. เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จำนวน 1 ครั้ง

7.2 จัดอบรม Data Classification and Data Leak Prevention Awareness แก่พนักงาน บสส. จำนวนอย่างน้อย 1 ครั้ง

7.3 จัดอบรมการใช้งานและการบำรุงรักษาระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Prevention System: DLP) และระบบ Information Classification System ให้กับผู้ดูแลระบบและผู้เกี่ยวข้อง จำนวนอย่างน้อย 1 ครั้ง

**8. การจ่ายเงิน**

บสส. จะจ่ายค่าพัสดุซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้วให้แก่ผู้ขาย โดยแบ่งออกเป็น 2 (สอง) งวด ดังนี้

งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 40 (สี่สิบ) ของราคาพัสดุตามสัญญา เมื่อผู้ขายได้ส่งมอบพัสดุ ข้อ 6.1 โดยถูกต้องและครบถ้วนตามสัญญาซื้อขายหรือข้อตกลงเป็นหนังสือ และ บสส. ได้ตรวจรับมอบพัสดุดังกล่าวเรียบร้อยแล้ว

งวดสุดท้าย เป็นจำนวนเงินในอัตราร้อยละ 60 (หกสิบ) ของราคาพัสดุตามสัญญา เมื่อผู้ขายได้ส่งมอบพัสดุ ข้อ 6.2 โดยถูกต้องและครบถ้วนตามสัญญาซื้อขายหรือข้อตกลงเป็นหนังสือ และ บสส. ได้ตรวจรับมอบพัสดุดังกล่าวเรียบร้อยแล้ว

**9. วงเงินงบประมาณ**

วงเงินงบประมาณในการซื้อ 14,500,000 บาท (สิบสี่ล้านห้าแสนบาท) (รวมภาษีมูลค่าเพิ่ม)

**10. หลักประกันการเสนอราคา**

ผู้ยื่นข้อเสนอต้องวางหลักประกันการเสนอราคาพร้อมกับการเสนอราคา จำนวน 725,000 บาท (เจ็ดแสนสองหมื่นห้าพันบาทถ้วน) ให้ไว้แก่ บสส. โดยใช้หลักประกันอย่างใดอย่างหนึ่งดังต่อไปนี้

(1) เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้น ชำระต่อเจ้าหน้าที่ หรือก่อนวันนั้นไม่เกิน 3 วันทำการ

(2) หนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศตามแบบที่คณะกรรมการนโยบายกำหนด

(3) พันธบัตรรัฐบาลไทย

(4) หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

**11. หลักเกณฑ์และสิทธิในการพิจารณา**

ในการพิจารณาผลการยื่นข้อเสนอ การจัดซื้อระบบป้องกันการรั่วไหลของข้อมูล บสส. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา (Price) โดยพิจารณาจากผู้เสนอราคาต่ำสุด

**12. กำหนดยืนราคา**

ผู้ยื่นข้อเสนอจะต้องยืนราคาตามที่เสนอ โดยมีกำหนดระยะเวลา 60 (หกสิบ) วัน นับแต่วันยืนยันเสนอราคาสุดท้ายเป็นต้นไป และภายในกำหนดยืนราคาผู้ยื่นข้อเสนอจะต้องรับผิดชอบราคาที่ตนเสนอไว้และจะถอนการเสนอราคามิได้

**13. การทำสัญญาซื้อขาย**

ผู้ยื่นข้อเสนอรายที่ได้รับเลือกให้เป็นผู้ขายจะต้องทำสัญญาซื้อขายตามแบบสัญญาที่ บสส. กำหนดหรือทำข้อตกลงเป็นหนังสือกับ บสส. ภายใน 7 (เจ็ด) วัน นับถัดจากวันที่ได้รับแจ้งจาก บสส. และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 (ห้า) ของราคาพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ให้ บสส. ยึดถือไว้ในขณะทำสัญญาหรือทำข้อตกลงเป็นหนังสือ โดยกำหนดให้ใช้หลักประกันสัญญาอย่างหนึ่งอย่างใดดังต่อไปนี้

(1) เงินสด

(2) เช็คหรือดราฟต์ที่ธนาคารสั่งจ่ายให้แก่ บสส. โดยเป็นเช็คหรือดราฟต์ลงวันที่ที่ทำสัญญาหรือก่อนหน้าวันทำสัญญานั้นไม่เกิน 3 (สาม) วันทำการ

(3) หนังสือค้ำประกันของธนาคารภายในประเทศ ตามตัวอย่างที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

(4) หนังสือค้ำประกันของบริษัทเงินทุน หรือ บริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

(5) พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ยภายใน 15 วัน นับถัดจากวันที่ผู้ขายพ้นจากข้อผูกพันตามสัญญาซื้อขายแล้ว

**14. ค่าปรับ**

14.1 กรณีที่ผู้ขายช่วงงานไปให้ผู้อื่นทำอีกทอดหนึ่ง โดยไม่ได้รับอนุญาตจาก บสส. ก่อน บสส. จะปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนเงินในอัตราร้อยละ 10 (สิบ) ของวงเงินของงานที่นำไปช่วงนั้น

14.2 กรณีผู้ขายไม่ปฏิบัติตามสัญญาซื้อขาย และ/หรือ เมื่อครบกำหนดส่งมอบพัสดุตามสัญญาซื้อขายแล้ว หากผู้ขายไม่ส่งมอบพัสดุ หรือ ส่งมอบไม่ถูกต้อง หรือ ส่งมอบไม่ครบจำนวน บสส. จะปรับผู้ขายเป็นรายวันในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของราคาพัสดุที่ยังไม่ส่งมอบพัสดุ หรือ ส่งมอบไม่ถูกต้อง แต่ทั้งนี้จะต้องไม่ต่ำกว่าวันละ 100 บาท (หนึ่งร้อยบาทถ้วน) จนกว่าผู้ขายจะส่งมอบถูกต้อง หรือ ส่งมอบครบจำนวน

14.3 กรณีเกิดความชำรุดบกพร่อง หรือขัดข้อง หรือไม่สามารถทำงานได้ครบถ้วนสมบูรณ์ ภายในระยะเวลาการรับประกัน 3 ปี ถ้าผู้ขายไม่จัดการซ่อมแซมแก้ไขหรือไม่ติดตั้งระบบป้องกันการรั่วไหลของข้อมูลใหม่ให้แล้วเสร็จภายในกำหนดเวลาการรับประกัน บสส. จะปรับผู้ขายเป็นรายวัน ในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของราคาพัสดุ แต่ทั้งนี้จะต้องไม่ต่ำกว่าวันละ 100 บาท (หนึ่งร้อยบาทถ้วน) นับตั้งแต่เวลาที่ครบกำหนดซ่อมแซมแก้ไขไปจนกว่าจะได้ดำเนินการซ่อมแซมแก้ไขแล้วเสร็จ

**15. การรับประกันความชำรุดบกพร่อง**

ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของพัสดุที่ซื้อขายที่เกิดขึ้นภายในระยะเวลา 3 (สาม) ปี นับถัดจากวันที่ บสส. รับมอบพัสดุสิ่งของ (งวดสุดท้าย) ) หากเกิดความชำรุดบกพร่อง หรือขัดข้อง หรือไม่สามารถทำงานได้ครบถ้วนสมบูรณ์ตามที่กำหนดไว้ ผู้ขายต้องทำการซ่อมแซมแก้ไขระบบป้องกันการรั่วไหลของข้อมูลดังกล่าวให้ทำงานได้อย่างสมบูรณ์ หรือติดตั้งระบบป้องกันการรั่วไหลของข้อมูลใหม่ที่ได้มาตรฐานและมีคุณสมบัติเท่ากับหรือดีกว่า ให้แล้วเสร็จ ภายใน 1 (หนึ่ง) วัน นับถัดจากวันที่ได้แจ้งจากผู้ซื้อหรือผู้ที่ได้รับมอบหมายจากผู้ซื้อไม่ว่าด้วยวาจา โทรศัพท์ โทรสาร SMS ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) หรือ ไลน์แอปพลิเคชั่น (LINE Application) ทั้งนี้ ด้วยค่าใช้จ่ายของผู้ขายเองทั้งสิ้น

**16. เงื่อนไขด้านความมั่นคงปลอดภัยสารสนเทศ**

ผู้เสนอราคาต้องยินยอมปฏิบัติตามนโยบายความปลอดภัยสารสนเทศของ บสส. รวมถึงคำสั่ง และวิธีปฏิบัติต่างๆ ที่เกี่ยวข้องโดยมีบทสรุปของนโยบายฯ ได้แก่

16.1 มีความตระหนักถึงการรักษาความปลอดภัยในข้อมูลและทรัพย์สินของ บสส.

16.2 รับผิดชอบในการจัดการด้านความปลอดภัยข้อมูล เช่น การจัดเก็บข้อมูล การโยกย้าย และการทำสำเนา ฯลฯ

16.3 หากมีความจำเป็นในการใช้ข้อมูลที่จัดอยู่ในชั้นลับขึ้นไป ต้องขออนุญาตจากเจ้าของข้อมูล และยินยอมลงนามในสัญญาไม่เปิดเผยข้อมูลของ บสส. ก่อนเข้าใช้ข้อมูลนั้นๆ

16.4 รักษาความถูกต้องและความลับข้อมูลของ บสส. ก่อนการนำไปใช้งานหรือทดสอบ

16.5 มีการจำกัดสิทธิในการเข้าใช้งานข้อมูลที่สำคัญของ บสส.

16.6 มีการจัดการเหตุการณ์ที่มีผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์

16.7 ยินยอมให้ บสส. มีสิทธิในการเข้าตรวจสอบการทำงาน

16.8 ดำเนินการให้ บสส. ได้สิทธิโดยชอบในการใช้ซอฟต์แวร์ที่มีผู้อื่นเป็นเจ้าของลิขสิทธิ์ หรือสิทธิบัตรหรือทรัพย์สินทางปัญญาอื่นๆ ทั้งนี้สำหรับข้อมูลที่เกิดขึ้นหรือซอฟต์แวร์ที่พัฒนาขึ้น (Source Code) ในโครงการนี้ถือเป็นกรรมสิทธิ์ หรือลิขสิทธิ์ หรือสิทธิของบสส.

16.9 ผู้เสนอราคาจะต้องแจ้ง บสส. ทันทีในกรณีที่เกิดเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ ของ บสส.

16.10 ห้ามมิให้นำอุปกรณ์ประมวลผลที่ไม่ใช่ของ บสส. มาต่อเข้ากับระบบเครือข่ายภายในของ บสส. เว้นแต่ได้รับอนุญาตจาก บสส. แล้ว

16.11 ห้ามมิให้นำข้อมูลและสื่อเก็บข้อมูลที่จัดอยู่ในลำดับชั้นลับขึ้นไปออกจาก บสส. โดยไม่มีการควบคุมที่เหมาะสม ทั้งนี้ต้องแจ้งให้ บสส. รับทราบและพิจารณาความเหมาะสมก่อน

16.12 ผู้เสนอราคาต้องใช้พอร์ตสื่อสาร (Service Port) ของระบบงาน ตามที่ บสส. กำหนดให้เท่านั้น ทั้งนี้หากผู้รับจ้างมีความจำเป็นต้องการใช้งานพอร์ตสื่อสารอื่นใด ให้แจ้งมายัง บสส. เพื่อพิจารณาให้ความเห็นชอบก่อน

**17. เงื่อนไขอื่น**

ผู้เสนอราคา/ผู้ยื่นข้อเสนอ ซึ่งเป็นผู้สนใจ หรือ เคยเป็นคู่ค้าของ บสส. ตกลงรับทราบนโยบายการคุ้มครองข้อมูลส่วนบุคคล ของ บสส. ที่ได้ประกาศใช้ในขณะนี้ เป็นอย่างดีแล้ว และเพื่อการเสนอราคา/ยื่นข้อเสนอตามเอกสารนี้ ผู้เสนอราคา/ผู้ยื่นข้อเสนอตกลงให้คำรับรองว่า เพื่อการคุ้มครองข้อมูลส่วนบุคคลของฝ่าย บสส. ผู้เสนอราคา/ผู้ยื่นข้อเสนอจะดำเนินการ เก็บ รวบรวม ใช้ หรือเปิดเผย รวมถึงกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอและเหมาะสม ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กฎ ระเบียบ ประกาศ คำสั่ง นโยบาย วิธีการปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งส่วนราชการ หน่วยงานของรัฐ รวมถึง บสส. ได้ประกาศใช้บังคับ ในขณะนี้ และ/หรือ ที่จะได้มีการแก้ไขหรือเพิ่มเติมในภายหน้าด้วย ตลอดจนจะกำกับดูแลให้บุคคลที่เกี่ยวข้องกับผู้เสนอราคา/ผู้ยื่นข้อเสนอปฏิบัติตามคำรับรองดังกล่าวด้วย

หาก ผู้เสนอราคา/ผู้ยื่นข้อเสนอฝ่าฝืนหรือไม่ปฏิบัติตามที่ได้ให้คำรับรองดังกล่าวข้างต้น ผู้เสนอราคา/ผู้ยื่นข้อเสนอ ตกลงยินยอมรับผิดโดยชดใช้ค่าสินไหมทดแทน และ/หรือ ค่าใช้จ่ายทั้งหมดที่เกิดขึ้นหรือเกี่ยวเนื่องจากการที่ฝ่าฝืนหรือไม่ปฏิบัติตามที่ได้ให้คำรับรองนั้น ไม่ว่าการนั้นจะเกิดขึ้นจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม ต่อ บสส. ทุกประการ

**18. ข้อสงวนสิทธิ์และอื่น ๆ**

18.1 บสส. สงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไขหรือข้อกำหนดของแบบสัญญาหรือข้อตกลงเป็นหนังสือเพื่อให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

18.2 บสส. สงวนสิทธิ์ในการปรับเพิ่มหรือลดเนื้องานที่อยู่ในรายละเอียดคุณลักษณะเฉพาะ/ขอบเขตของงาน (TOR) นี้ได้ โดยคิดราคางานเพิ่มหรือลดที่เกิดขึ้นจริงตามส่วนของราคาพัสดุตามสัญญา และให้ถือรายละเอียดคุณลักษณะเฉพาะ/ขอบเขตของงาน (TOR) นี้เป็นส่วนหนึ่งของสัญญา

18.3 เมื่อผู้ยื่นข้อเสนอรายใดได้รับเลือกให้เป็นผู้ขายและได้ตกลงซื้อพัสดุสิ่งของแล้ว ถ้าผู้ขายจะต้องสั่งหรือนำพัสดุสิ่งของเข้ามาจากต่างประเทศและพัสดุสิ่งของนั้นต้องนำเข้ามา โดยทางเรือในเส้นทางที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ยื่นข้อเสนอรายที่ได้รับเลือกให้เป็นผู้ขายนั้นจะต้องปฏิบัติตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์นาวี ดังนี้

(1) แจ้งการสั่งหรือนำพัสดุสิ่งของดังกล่าวเข้ามาจากต่างประเทศต่อกรมเจ้าท่า ภายใน 7 วัน นับตั้งแต่วันที่ผู้ขายสั่งหรือซื้อของจากต่างประเทศ เว้นแต่ เป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

(2) จัดการให้พัสดุสิ่งของดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทยจากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกพัสดุสิ่งของนั้น โดยเรืออื่นที่มิใช่เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุกของลงเรืออื่น หรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

(3) ในกรณีที่ไม่ปฏิบัติตาม (1) หรือ (2) ผู้ขายจะต้องรับผิดตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์นาวี

18.4 ผู้ยื่นข้อเสนอรายที่ได้รับเลือกให้เป็นผู้ขายพัสดุแล้ว ไม่ไปทำสัญญาหรือข้อตกลงเป็นหนังสือภายในเวลาที่กำหนดดังระบุไว้ใน ข้อ 13. บสส. มีสิทธิริบหลักประกันการเสนอราคา หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการเสนอราคาทันที และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็น ผู้ทิ้งงานตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

18.5 บสส. อาจประกาศยกเลิกการจัดซื้อตามรายละเอียดคุณลักษณะเฉพาะ/ขอบเขตงาน (TOR) ฉบับนี้ในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใดๆ จาก บสส. ไม่ได้

(1) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดซื้อหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

(2) การทำการจัดซื้อครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่ บสส. หรือ กระทบต่อประโยชน์สาธารณะ

(3) กรณีอื่นในทำนองเดียวกับ (1) หรือ (2) ตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

18.6 ในระหว่างระยะเวลาการซื้อ ผู้ยื่นข้อเสนอรายที่ได้รับเลือกให้เป็นผู้ขายต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายและระเบียบที่กำหนด รวมถึง ข้อตกลง เงื่อนไข ระเบียบ ประกาศ หลักเกณฑ์และวิธีปฏิบัติของ บสส. โดยเคร่งครัด

18.7 ผู้ยื่นข้อเสนอรายที่ได้รับเลือกให้เป็นผู้ขายจะต้องเก็บรักษาข้อมูลที่ได้รับจาก บสส. เพื่อการปฏิบัติงานตามสัญญา (ถ้ามี) ไว้เป็นความลับตลอดไป โดยจะไม่เปิดเผยข้อมูลดังกล่าวไม่ว่าด้วยวิธีการใดและแก่บุคคลใดทั้งสิ้น ทั้งนี้เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจาก บสส. แล้วเท่านั้น

18.8 บสส. ไม่อนุญาตให้ผู้ขายช่วงงาน หรือ โอนสิทธิเรียกร้องในการรับเงินค่าขายพัสดุจาก บสส. ไม่ว่าทั้งหมดหรือบางส่วนให้แก่บุคคลหนึ่งบุคคลใด เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจาก บสส.

18.9 บสส. จะประเมินผลการปฏิบัติงานที่แล้วเสร็จตามสัญญาของผู้ยื่นข้อเสนอรายที่ได้รับเลือกให้เป็นผู้ขายพัสดุ ตามหลักเกณฑ์การประเมินผลที่ บสส. และ/หรือ ตามที่ระเบียบกระทรวงการคลังกำหนด

18.10 ในกรณีที่รายละเอียดคุณลักษณะเฉพาะ/ขอบเขตของงาน (TOR) และ/หรือ เอกสารแนบท้าย (ถ้ามี) มีความขัดหรือแย้งกับแบบเอกสารต่าง ๆ เพื่อการจัดจ้างครั้งนี้ ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของ บสส. และให้ถือคำวินิจฉัยดังกล่าวเป็นที่สุด ผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร้องค่าเสียหายหรือค่าใช้จ่ายใดๆ จาก บสส. ทั้งสิ้น

18.11 บรรดาข้อมูล เอกสาร แบบสำรวจ รายงาน ผลการศึกษาวิเคราะห์ ผลสำเร็จของงาน รวมถึงทรัพย์สิน สิ่งต่างๆ ที่ผู้ขายได้จัดทำขึ้นจากการปฏิบัติงานและ/หรือส่งมอบให้แก่ บสส. (ถ้ามี) จะตกเป็นกรรมสิทธิ์และลิขสิทธิ์ของ บสส. โดยผู้ขายจะต้องไม่ส่งมอบ ไม่เผยแพร่ข้อมูลเอกสาร ทำซ้ำ ดัดแปลง หรือกระทำการใดๆ อันเป็นการละเมิดสิทธิของ บสส. ไม่ว่าด้วยวิธีการใดๆ ให้แก่ผู้หนึ่งผู้ใด หรือนำไปใช้ประโยชน์ไม่ว่าจะเพื่อประโยชน์ของตนเองหรือผู้อื่นทั้งทางตรงและทางอ้อม โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจาก บสส. ก่อนทั้งสิ้น

**19. การติดต่อและการรับส่งเอกสาร**

ชื่อ-สกุล สุลักษณ์ ฉันทวิทย์

ฝ่าย กลยุทธ์และวางแผนเทคโนโลยีสารสนเทศ ชั้น 29

โทรศัพท์ 02-6861800 ต่อ 2915

E-Mail: suluk@sam.or.th

เว็บไซต์ www.sam.or.th

บริษัท บริหารสินทรัพย์สุขุมวิท จำกัด เลขที่ 123 อาคารซันทาวเวอร์ส เอ ชั้น 27-30 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร 10900 ภายในวันที่ ..... ตั้งแต่เวลา .....น. ถึง .....น. ในวันและเวลาทำการของ บสส.

สาธารณชนที่ต้องการเสนอแนะ วิจารณ์ หรือมีความคิดเห็นต้องเปิดเผยชื่อ และที่อยู่ในข้อเสนอแนะวิจารณ์หรือมีความเห็นด้วย

**********