ข้อกำหนดและขอบเขตของงาน (Terms of Reference : TOR)
โครงการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน
(Unified Digital Evidence Exchange: U-DEX)

---

๑. ความเป็นมา

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือสำนักงาน กสทช. มีหน้าที่สนับสนุนการกำกับดูแลการประกอบกิจการโทรคมนาคม การคุ้มครองผู้ใช้บริการและประชาชน ตลอดจนการกำหนดและติดตามมาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้เป็นไปตามกฎหมายและอำนาจหน้าที่ของสำนักงาน กสทช. ในสภาวการณ์ปัจจุบันที่โลกกำลังก้าวเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบ เทคโนโลยีสารสนเทศและการสื่อสารได้กลายเป็นปัจจัยพื้นฐานสำคัญในการขับเคลื่อนยุทธศาสตร์ชาติและการพัฒนาเศรษฐกิจสังคมของประเทศไทยซึ่งโอกาสในการสร้างมูลค่าทางเศรษฐกิจและการยกระดับคุณภาพชีวิตของประชาชน แต่ในขณะเดียวกันก็นำมาซึ่งภัยคุกคามรูปแบบใหม่ที่มีความซับซ้อนและรุนแรงยิ่งขึ้น ปัจจุบันมีการนำบริการโทรคมนาคม โครงข่ายอินเทอร์เน็ต อุปกรณ์สื่อสาร และบริการดิจิทัลมาใช้เป็นช่องทางหรือองค์ประกอบในการกระทำความผิดทางเทคโนโลยี การตรวจสอบข้อเท็จจริง การติดตามเส้นทางการเชื่อมต่อ การพิสูจน์ทราบผู้ใช้บริการ อุปกรณ์ ช่วงเวลา และความสัมพันธ์ของเหตุการณ์ จึงจำเป็นต้องอาศัยข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลผู้ใช้บริการ และข้อมูลประกอบการให้บริการโทรคมนาคมที่มีความถูกต้อง ครบถ้วน มีเวลาอ้างอิงที่สอดคล้องกัน สามารถสืบค้นย้อนหลังได้ และมีหลักฐานแสดงการเข้าถึงหรือดำเนินการกับข้อมูลที่ตรวจสอบย้อนหลังได้ ทั้งนี้ การเก็บรักษาเพื่อการใช้ สืบค้น เปิดเผย ส่งมอบ และทำลายข้อมูลดังกล่าวต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมว่าด้วยหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ มาตรา ๒๖ กำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบ และอาจสั่งให้เก็บเพิ่มขึ้นได้ไม่เกิน ๒ ปีในกรณีพิเศษ

โดยที่ปัญหาอาชญากรรมทางเทคโนโลยี หรือ ภัยไซเบอร์ ได้ทวีความรุนแรง และสร้างความเสียหายต่อระบบเศรษฐกิจและสังคมของประเทศในวงกว้าง ผ่านการกระทำโดยโครงข่ายโทรคมนาคม โดยเลขหมายโทรคมนาคมของผู้ให้บริการที่ได้รับใบอนุญาตประกอบกิจการโทรคมนาคมตามพระราชบัญญัติประกอบกิจการโทรคมนาคม พ.ศ. ๒๕๔๔ โดยคณะกรรมการกิจการโทรคมนาคมแห่งชาติตามกฎหมายว่าด้วยองค์กรจัดสรรคลื่นความถี่และกำกับกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการโทรคมนาคม ดังนั้น เพื่อประโยชน์ในการกำกับข้อมูลและการพิสูจน์หลักฐานเพื่อการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี หรือภัยไซเบอร์ ที่มีความซับซ้อนมากขึ้นซึ่งต้องใช้เวลาในการสืบสวนสอบสวน เพื่อสร้างความมั่นคงปลอดภัยในโลกดิจิทัลเพื่อสร้างความเชื่อมั่นของประชาชน

Proof

คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) โดยอาศัยอำนาจตามพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. ๒๕๔๔ มาตรา ๑๗ "ให้คณะกรรมการมีหน้าที่จัดให้มีการบริการโทรคมนาคมพื้นฐานโดยทั่วถึง และให้มีอำนาจกำหนดให้ผู้รับใบอนุญาตต้องจัดให้มีบริการโทรคมนาคมดังต่อไปนี้ด้วย" (๕) **"จัดให้มีการดำเนินการที่เกี่ยวข้องกับกิจการโทรคมนาคมเพื่อประโยชน์ด้านความมั่นคงหรือประโยชน์สาธารณะ"** (เพิ่มเติม (๕) โดยคำสั่งหัวหน้าคณะรักษาความสงบแห่งชาติ คำสั่งที่ ๘/๒๕๖๒) วรรคสาม "ให้คณะกรรมการจัดให้มีการประกาศตามวรรคสองไว้เป็นการล่วงหน้าเพื่อให้ผู้ประสงค์จะขอรับใบอนุญาตได้ทราบขอบเขตการจัดให้มีบริการโทรคมนาคมตามวรรคหนึ่งก่อนการยื่นคำขออนุญาตด้วย" และวรรคสี่ "การกำหนดให้ผู้รับใบอนุญาตจัดให้มีบริการโทรคมนาคมตามมาตรานี้**ต้องไม่ทำให้เกิดภาระเกินสมควร**แก่การลงทุนของผู้รับใบอนุญาต และต้องให้มีการปฏิบัติโดยเท่าเทียมกันในระหว่างผู้รับใบอนุญาตที่ประกอบกิจการโทรคมนาคมในลักษณะและประเภทเดียวกัน" จึงได้มีมติเห็นชอบการกำหนดมาตรการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเพิ่มเติม และมอบหมายให้สำนักงาน กสทช. ปรับปรุงประกาศสำนักงาน กสทช. เรื่อง มาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคม ลงวันที่ ๒๘ สิงหาคม ๒๕๖๘ ให้เหมาะสมยิ่งขึ้น โดยให้มีการเก็บข้อมูลบริการโทรคมนาคมของผู้รับใบอนุญาตเพิ่มขึ้นจาก ๙๐ วัน และสอดคล้องกับกรอบระยะเวลาตามมาตรา ๒๖ แห่ง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และเพื่อมิให้เป็นภาระแก่ผู้รับใบอนุญาตประกอบกิจการโทรคมนาคม ต่อมาที่ประชุม กสทช. ครั้งที่ ๑๑/๒๕๖๙ (ต่อเนื่อง) เมื่อวันที่ ๑ วันที่ ๒ วันที่ ๗ และวันที่ ๘ เมษายน ๒๕๖๙ จึงมีมติเห็นชอบให้ดำเนินโครงการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน (Unified Digital Evidence Exchange : U-DEX) โดยใช้เงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมเพื่อประโยชน์สาธารณะ (USO) บัญชี ๓ USO โทรคมนาคม ซึ่งเป็นโครงการจัดให้มีการบริหารจัดการเพื่อสนับสนุนผู้ให้บริการที่ได้รับใบอนุญาตประกอบกิจการโทรคมนาคม (บริการโทรศัพท์เคลื่อนที่) ปฏิบัติตามประกาศสำนักงาน กสทช. โดยเท่าเทียมกัน ต่อไป

ต่อมาสำนักงาน กสทช. ออกประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคม (ฉบับที่ ๒) ข้อ ๑๒ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการกรณีที่มีการใช้บริการอยู่ย้อนหลังไม่น้อยกว่า ๑๘๐ วัน ตลอดเวลาที่ใช้บริการในกรณีมีความจำเป็นต้องใช้ข้อมูล เพื่อดำเนินคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี โดยผู้รับใบอนุญาตต้องเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการเฉพาะเท่าที่จำเป็นต่อการดำเนินคดีเท่านั้น กรณีการให้บริการโทรคมนาคมสิ้นสุดลงผู้รับใบอนุญาตมีหน้าที่ต้องเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการตามวรรคหนึ่งไว้ไม่น้อยกว่าหนึ่งร้อยแปดสิบวัน นับแต่วันสิ้นสุดสัญญา ทั้งนี้ การเก็บรักษาข้อมูลส่วนบุคคลตามวรรคหนึ่งและวรรคสอง เฉพาะข้อมูลของผู้ใช้บริการที่จำเป็นต่อการดำเนินคดีความผิดตามกฎหมาย โดยให้สำนักงาน กสทช. สำนักงานตำรวจแห่งชาติ และผู้รับใบอนุญาตร่วมกันกำหนดข้อมูลสำหรับที่ต้องเก็บรักษา

Proof

เพื่อให้การดำเนินการตามมติ กสทช. และประกาศสำนักงาน กสทช. ดังกล่าวข้างต้น จึงมีความจำเป็นต้องดำเนินโครงการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน (Unified Digital Evidence Exchange : U-DEX) โดยใช้เงินกองทุน USO ในการสนับสนุนให้ผู้รับใบอนุญาตประกอบกิจการโทรคมนาคม (บริการโทรศัพท์เคลื่อนที่) เก็บข้อมูล Log file ที่จำเป็นตามระยะเวลาที่เพิ่มขึ้นเพื่อใช้เป็นพยานหลักฐานดิจิทัลที่ไม่สามารถแก้ไขได้และเน้นการแลกเปลี่ยนข้อมูลระหว่างรัฐและเอกชน โดยขอบเขตของงานนี้เป็นการดำเนินการเพื่อบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนในการสร้างกลไกแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างผู้ให้บริการโทรคมนาคมและหน่วยงานบังคับใช้กฎหมายที่สำคัญได้อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์

๒.๑ โครงการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน (Unified Digital Evidence Exchange : U-DEX) เพื่อจัดหาระบบจัดเก็บข้อมูลการใช้บริการโทรศัพท์เคลื่อนที่จากเดิมที่กฎหมายกำหนดเป็นเวลา ๒ ปี นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบ

๒.๒ เพื่อสนับสนุนการใช้ข้อมูลบริการโทรศัพท์เคลื่อนระหว่างผู้ให้บริการโทรคมนาคมและหน่วยงานบังคับใช้กฎหมาย

๒.๓ เพื่อให้ประชาชนมีข้อมูลในการตรวจสอบการใช้บริการผ่านโทรศัพท์เคลื่อนที่ย้อนหลังด้วยความมั่นคงปลอดภัย

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพื้นฐานที่กำหนด ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ตลอดจนแนวปฏิบัติตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ตามที่กำหนดในเอกสารประกวดราคาจ้างด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

๓.๒ ผู้ยื่นข้อเสนอต้องเป็นผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมที่ต้องเปิดดำเนินกิจการอยู่และต้องไม่เป็นผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมที่ให้บริการโครงข่ายโทรศัพท์เคลื่อนที่หรือมีความเกี่ยวโยงทางตรงหรือทางอ้อมอันอาจก่อให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูลของผู้ให้บริการโทรศัพท์เคลื่อนที่รายอื่น

๓.๓ ผู้ยื่นข้อเสนอต้องมีผลงานด้านติดตั้งระบบคอมพิวเตอร์แม่ข่ายที่ศูนย์คอมพิวเตอร์เสมือนมูลค่ารวมไม่น้อยกว่า ๓๕๐,๐๐๐,๐๐๐ บาท (สามร้อยห้าสิบล้านบาทถ้วน) ภายใต้สัญญาเดียวที่ส่งมอบงานและตรวจรับแล้วเสร็จไม่เกิน ๕ ปี นับถึงวันที่ยื่นข้อเสนอ โดยเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่สำนักงาน กสทช. เชื่อถือ และไม่ใช่ผลงานอันเกิดจากการจ้างช่วง โดยต้องยื่นสำเนาหนังสือรับรองผลงานพร้อมสำเนาสัญญาพร้อมหลักฐานการชำระภาษีประกอบการยื่นข้อเสนอ

Proof

๔. ขอบเขตการดำเนินงาน (Scope of Work)

๔.๑ นิยาม/ความหมาย

ในข้อกำหนดและขอบเขตของงานนี้

“โครงการฯ” หมายถึง โครงการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน (U-DEX) ซึ่งมีรายละเอียดตามข้อกำหนดและขอบเขตการดำเนินงานนี้

“U-DEX” หรือ Unified Digital Evidence Exchange หมายถึง ระบบหรือแพลตฟอร์มกลางที่ออกแบบมาเพื่อการแลกเปลี่ยน ตรวจสอบ และจัดการพยานหลักฐานดิจิทัลแบบบูรณาการระหว่างหน่วยงานบังคับใช้กฎหมาย กระบวนการยุติธรรม หรือหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อมูลมีความถูกต้อง ปลอดภัย และตรวจสอบย้อนกลับได้ ซึ่งในโครงการนี้หมายถึงข้อมูลเกี่ยวกับการใช้โทรศัพท์เคลื่อนที่

“ระบบบริหารจัดการ” หมายถึง การจัดหาและติดตั้งระบบบริหารจัดการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและข้อมูลอาชญากรรมอย่างเป็นระบบและปลอดภัยให้แก่หน่วยงานภาครัฐที่เกี่ยวข้อง เพื่อวิเคราะห์ ป้องกัน และปราบปรามอาชญากรรม ภายใต้โครงการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน (D-SAFE) โดยคำนึงถึงการเคารพสิทธิความเป็นส่วนตัวของประชาชนตามกฎหมายคุ้มครองข้อมูล

“การบริหารจัดการ” หมายถึง การดำเนินการเพื่อให้ระบบบริหารจัดการมีความพร้อมบริการโครงการ จัดหาระบบการให้บริการอินเทอร์เน็ตความเร็วสูงที่กำหนดการควบคุมดูแลการจัดให้มีบุคลากรบริการ การบำรุงรักษา และการดำเนินงานอื่น ๆ ที่เกี่ยวข้องเพื่อรักษาไว้ซึ่งคุณภาพบริการตลอดระยะเวลาบริการ

“อุปกรณ์บริการ” หมายถึง เครื่องอุปกรณ์ที่ให้บริการและระบบต่าง ๆ ทั้งหมด

“การบำรุงรักษา” หมายถึง การบำรุงรักษาเพื่อป้องกัน (Preventive Maintenance) หรือ PM การซ่อมแซมแก้ไขข้อชำรุดขัดข้อง (Corrective Maintenance) หรือ CM อุปกรณ์บริการเพื่อให้อุปกรณ์สามารถใช้งานและให้บริการอินเทอร์เน็ตความเร็วสูงได้อย่างดี มีคุณภาพและประสิทธิภาพตลอดระยะเวลาบริการ

“การบำรุงรักษาเพื่อป้องกัน” (Preventive Maintenance) หรือ PM หมายถึง การบำรุงรักษาเพื่อให้สามารถใช้งานได้ดีตามรอบระยะเวลาที่กำหนด รวมถึงการเปลี่ยนวัสดุสิ้นเปลืองอะไหล่ ซึ่งหมดอายุการใช้งานตามระยะเวลาการใช้งานตามปกติ

“การซ่อมแซมแก้ไขข้อชำรุดขัดข้อง” (Corrective Maintenance) หรือ CM หมายถึง การบำรุงรักษาเพื่อซ่อมแซมแก้ไขข้อชำรุดขัดข้องจากการใช้งานตามปกติ หรืออุบัติเหตุใด ๆ อันเกิดจากความผิดหรือความประมาทเลินเล่อของพนักงานของผู้รับจ้าง ให้คืนสภาพและหรือให้สามารถใช้งานได้ดีเช่นเดิม ภายในระยะเวลาที่กำหนด ทั้งนี้ ไม่รวมถึงกรณีเกิดการชำรุดหรือเสื่อมสภาพจากการหมดอายุการใช้งานซึ่งต้องจัดซื้อใหม่หรือภัยธรรมชาติหรือเหตุสุดวิสัย

“สำนักงาน กสทช.” หมายถึง สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ

“ผู้ว่าจ้าง” หมายถึง สำนักงาน กสทช. และให้หมายรวมถึงคณะกรรมการตรวจรับพัสดุ บุคคล หรือหน่วยงานที่ได้รับมอบหมายจากสำนักงาน กสทช.

Proof

"ผู้รับจ้าง" หมายถึง ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะการประกวดราคาและเข้าทำสัญญาบริการตามแบบที่กำหนดกับสำนักงาน กสทช. เรียบร้อยแล้ว

"ผู้รับบริการ" หมายถึง หน่วยงานที่เกี่ยวข้อง

"ช่วงเวลาการจัดเก็บ" หมายถึง ชุดข้อมูลที่จัดเก็บในช่วงระยะเวลาตั้งแต่วันที่ ๙๑ จนถึง ๒ ปี (๗๓๐ วัน)

"ศูนย์ข้อมูล" (Data Center) หรือ DC หมายถึง ศูนย์ข้อมูลหลักที่ถูกออกแบบและติดตั้งระบบคอมพิวเตอร์ เซิร์ฟเวอร์ (Server) ระบบจัดเก็บข้อมูล (Storage) และอุปกรณ์เครือข่าย เพื่อใช้จัดเก็บและบริหารจัดการข้อมูลดิจิทัลอย่างต่อเนื่องตลอด ๒๔ ชั่วโมง

"ศูนย์ข้อมูลสำรอง" (Disaster Recovery) หรือ DR หมายถึง ศูนย์สำรองที่ถูกจัดเตรียมไว้เพื่อกู้คืนระบบสารสนเทศ ข้อมูล และเครือข่าย ให้กลับมาทำงานได้ตามปกติอย่างรวดเร็ว หลังจากเผชิญเหตุขัดข้องร้ายแรง ภัยพิบัติทางธรรมชาติ หรือการโจมตีทางไซเบอร์

"ข้อมูลที่จัดเก็บ" หรือ ข้อมูลส่วนบุคคลของผู้ใช้บริการประเภทเสียง (Voice) ภายใต้บริการโทรศัพท์เคลื่อนที่ที่จำเป็นต่อ การดำเนินคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี ตามแนวปฏิบัติการดำเนินการตามประกาศสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยีสำหรับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคม (ฉบับวันที่ ๑๕ มิถุนายน ๒๕๖๙) หมายถึง วันเวลาเริ่มต้นใช้งาน, วันเวลาสิ้นสุดใช้งาน, เลขหมายต้นทาง (A NUMBER), เลขหมายที่ติดต่อ (B NUMBER) , ประเภทการใช้งาน (RECORD TYPE), จำนวนเวลาที่ใช้งาน (วินาที) DURATION, รหัสซิมการ์ด (IMSI), หมายเลขเครื่องโทรศัพท์ (IMEI), รหัสพื้นที่ (Location Area Code (LAC), รหัสเสาสัญญาณ (Cell ID (CI), รหัสพื้นที่ (Tracking Area Code (TAC), รหัสเสาสัญญาณ (E-UTRAN Cell ID (EC)), รหัสผู้ให้บริการ (Public Land Mobile Network (PLMIN), ชื่อเสาสัญญาณ (Site name), จังหวัด (PROVINCE), อำเภอ (AMPHOR), ตำบล (TUMBOL)

๔.๒ จัดทำแผนการดำเนินงานเพื่อการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน มีรายละเอียดการดำเนินงาน ดังนี้

๔.๒.๑ ผู้รับจ้างต้องดำเนินการออกแบบชุดอุปกรณ์เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการโทรศัพท์เคลื่อนที่ทั้ง ๓ หน่วยงาน เช่น True, AIS และ NT เป็นอย่างน้อย

๔.๒.๒ ผู้รับจ้างต้องออกแบบระบบและจัดทำแบบ Network Diagram การติดตั้งอุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ สิทธิการใช้งาน ระบบเครือข่าย ระบบจัดเก็บข้อมูล ระบบสำรองและกู้คืนข้อมูล ระบบรักษาความมั่นคงปลอดภัย รวมถึงวัสดุอุปกรณ์ประกอบอื่น ๆ ทั้งหมดที่จำเป็นต่อการทำงานของระบบ

๔.๒.๓ ผู้รับจ้างมีหน้าที่หลักในการประสานงานผู้ให้บริการโทรศัพท์เคลื่อนที่ทั้ง ๓ หน่วยงาน โดยต้องได้รับความยินยอมให้เชื่อมต่อข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการโทรศัพท์เคลื่อนที่เพื่อการจัดเก็บข้อมูลให้เป็นไปตามวัตถุประสงค์โครงการ

Proof

ทั้งนี้ เพื่อให้เป็นไปตามมาตรฐานการจัดเก็บข้อมูลผู้รับจ้างต้องให้บุคคลากรที่มีความเชี่ยวชาญเฉพาะด้านรับรองเป็นเอกสารประกอบการพิจารณา โดยก่อนผู้รับจ้างดำเนินการจัดหาและติดตั้งต้องได้รับความเห็นชอบจาก สำนักงาน กสทช. ก่อนดำเนินการ

๔.๓ ผู้รับจ้างต้องจัดหาและติดตั้ง ระบบบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน มีรายละเอียดการดำเนินงาน ดังนี้

๔.๓.๑ ติดตั้งอุปกรณ์ ณ ศูนย์ DC จำนวน ๓ ชุด มีรายการอุปกรณ์และคุณลักษณะเป็นไปตามที่กำหนดไว้ใน **(ภาคผนวก ๑)** อย่างน้อยดังนี้

(๑) เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทำหน้าที่เป็นทรัพยากรประมวลผลหลักสำหรับติดตั้งและให้บริการระบบ Software, Virtualization, Log Processing, Monitoring และ Application ที่เกี่ยวข้องกับโครงการ รวมทั้งรองรับการประมวลผล การจัดทำดัชนีข้อมูล การสืบค้น การบริหารจัดการ และระบบงานอื่นตามสถาปัตยกรรมที่กำหนด

(๑.๑) ระบบจัดเก็บข้อมูลหลัก (Primary Storage) ทำหน้าที่จัดเก็บข้อมูลหลักของระบบงาน ฐานข้อมูล ระบบจำลองเสมือน ระบบวิเคราะห์ข้อมูล และระบบอื่นที่เกี่ยวข้องภายในศูนย์ข้อมูลหลัก รวมถึงรองรับการใช้งานร่วมกับระบบประมวลผลและระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ระบบจัดเก็บข้อมูลต้องมีพื้นที่ใช้งานจริงหลังการป้องกันข้อมูลสูญหายและมีความสามารถเพียงพอต่อ Capacity Sizing ของระบบ

(๑.๒) ระบบจัดเก็บข้อมูลสำรอง (Backup Storage) ทำหน้าที่จัดเก็บข้อมูลสำรองของระบบงานภายในศูนย์ข้อมูลหลัก เพื่อรองรับการกู้คืนข้อมูลในกรณีข้อมูลหลักเกิดความเสียหาย ถูกลบ หรือไม่สามารถใช้งานได้ รวมถึงรองรับการสำรองหรือทำสำเนาข้อมูลตามสถาปัตยกรรมของโครงการ

(๑.๓) ระบบเครือข่ายศูนย์ข้อมูล (Data Center Network) ทำหน้าที่เชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูล อุปกรณ์รักษาความมั่นคงปลอดภัย ระบบกระจายภาระการใช้งาน และระบบอื่นที่เกี่ยวข้อง โดยต้องรองรับการเชื่อมต่อแบบ Redundant การกำหนดเส้นทางข้อมูล และการเชื่อมต่อระบบตามสถาปัตยกรรมของโครงการ นอกจากนี้ ต้องมีเครือข่ายสำหรับการบริหารจัดการ (Management Network) แยกจากเครือข่ายที่ใช้รับส่งข้อมูลหลัก สำหรับเชื่อมต่อช่องทางบริหารจัดการของ Server, Storage, Network, Security, Backup และอุปกรณ์อื่นที่เกี่ยวข้อง

(๑.๔) ระบบรักษาความมั่นคงปลอดภัยเครือข่าย ทำหน้าที่รักษาความมั่นคงปลอดภัยเครือข่ายสำหรับควบคุม ตรวจสอบ และป้องกันการรับส่งข้อมูลระหว่างเครือข่ายระบบงาน เครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูล และระบบอื่นที่เกี่ยวข้อง ณ ศูนย์ข้อมูลหลัก ทั้งนี้ ระบบดังกล่าวต้องสามารถทำงานร่วมกับระบบบริหารจัดการความมั่นคงปลอดภัย ระบบยืนยันตัวตน ระบบบริหารจัดการสิทธิ์ผู้ดูแลระบบ และระบบวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยของโครงการตามสถาปัตยกรรมที่กำหนด

(๑.๕) ระบบกระจายภาระการใช้งาน (Application Delivery Controller / Load Balancer) ทำหน้าที่กระจายภาระการใช้งานสำหรับกระจายการใช้งานของระบบงาน Web Application หรือบริการต่าง ๆ ไปยังเครื่องคอมพิวเตอร์แม่ข่ายหลายเครื่อง เพื่อเพิ่มประสิทธิภาพและความพร้อมใช้งานของระบบ

Proof

(๒) ระบบซอฟต์แวร์ (Software Platform) ระบบซอฟต์แวร์และสิทธิการใช้งานที่จำเป็นต่อการทำงานของโครงการ โดยรายละเอียด **(ภาคผนวก ๒)** มีระบบอย่างน้อยดังต่อไปนี้

(๒.๑) ระบบซอฟต์แวร์การจำลองเสมือน (Virtualization Platform) ทำหน้าที่สร้างและบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Machine) เพื่อรองรับการติดตั้งและใช้งานระบบงานต่าง ๆ ของโครงการบนทรัพยากรเครื่องคอมพิวเตอร์แม่ข่ายร่วมกัน รวมถึงรองรับ High Availability, Resource Management, Live Migration, Snapshot และการบริหารจัดการจากส่วนกลาง

(๒.๒) ระบบรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Detection and Response) หรือ EDR ทำหน้าที่ป้องกัน ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายเสมือนของโครงการ เพื่อช่วยลดความเสี่ยงจาก Malware, Ransomware และพฤติกรรมที่อาจเป็นภัยคุกคามต่อระบบ โดยสามารถบริหารจัดการจากส่วนกลางได้

(๒.๓) ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log Management Platform) ทำหน้าที่รวบรวม จัดเก็บ บริหารจัดการ จัดทำดัชนี สืบค้น และวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลบันทึกเหตุการณ์จากระบบและอุปกรณ์ต่าง ๆ ของโครงการ รวมทั้งรองรับการบริหารวงจรชีวิตของข้อมูลและการควบคุมสิทธิการเข้าถึงข้อมูล ทั้งนี้ ระบบต้องรองรับสถาปัตยกรรมการทำงานแบบกระจายหรือแบบแยกส่วนสำหรับศูนย์ข้อมูลหลักทั้ง ๓ ชุดและศูนย์ข้อมูลสำรอง และสามารถบริหารจัดการจากส่วนกลางได้

(๒.๔) ระบบตรวจสอบและบริหารจัดการโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ (Infrastructure Monitoring System) ทำหน้าที่ตรวจสอบสถานะ ความพร้อมใช้งาน และประสิทธิภาพของระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย ระบบจำลองเสมือน และระบบฐานข้อมูลของโครงการ โดยสามารถรวบรวมและแสดงสถานะของอุปกรณ์และระบบจากศูนย์ข้อมูลหลักทั้ง ๓ แห่ง และศูนย์ข้อมูลสำรองผ่านระบบบริหารจัดการส่วนกลางได้ Software, License, Subscription และ Technical Support ที่จำเป็นต้องจัดหาให้ครบถ้วน

๔.๓.๒ ศูนย์ข้อมูลสำรอง DR มีรายการอุปกรณ์และคุณลักษณะเป็นไปตามที่กำหนดไว้ใน **(ภาคผนวก ๑)** อย่างน้อยดังนี้

ผู้รับจ้างต้องจัดหา ติดตั้ง และบริหารจัดการระบบ ณ ศูนย์ข้อมูลสำรองสำหรับรองรับข้อมูลและระบบงานจากศูนย์ข้อมูลหลักทั้ง ๓ ชุด ในการสำรองข้อมูล การทำสำเนาข้อมูล การสืบค้น การกู้คืนระบบ และการให้บริการในกรณีที่ศูนย์ข้อมูลหลักเกิดเหตุขัดข้องหรือไม่สามารถให้บริการได้ ทั้งนี้ ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ ณ ศูนย์ข้อมูลสำรองต้องรองรับข้อมูลจากผู้ให้บริการโทรศัพท์เคลื่อนที่ทั้ง ๓ หน่วยงาน หรือปริมาณข้อมูลรวมเฉลี่ยไม่น้อยกว่า 1,050 GB. ต่อวัน ตามสถาปัตยกรรมที่เสนอ โดยศูนย์ข้อมูลสำรองต้องมีองค์ประกอบอย่างน้อย อย่างน้อยดังนี้

Proof

(๑) เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทำหน้าที่เป็นทรัพยากรประมวลผลสำหรับรองรับระบบ Standby ระบบกู้คืนข้อมูลและระบบงาน ระบบสืบค้นและบริหารจัดการระบบ Dashboard, Gateway, Virtualization และ Software อื่นที่เกี่ยวข้องกับการทำงานของศูนย์ข้อมูลสำรอง รวมถึงรองรับการเปิดใช้งานระบบงานที่ทำสำเนา สำรอง หรือกู้คืนมาจากศูนย์ข้อมูลหลักเมื่อเกิดเหตุขัดข้องหรือ Disaster

(๒) ระบบจัดเก็บข้อมูลหลัก (Primary Storage) ทำหน้าที่จัดเก็บข้อมูลที่ทำสำเนา จำลอง หรือส่งต่อจากศูนย์ข้อมูลหลัก เพื่อรองรับการกู้คืนข้อมูล การสืบค้น และการให้บริการต่อเนื่องจากศูนย์ข้อมูลสำรองระบบต้องมีพื้นที่และทรัพยากรเพียงพอต่อข้อมูลจากศูนย์ข้อมูลหลักทั้ง ๓ ชุด

(๓) ระบบจัดเก็บข้อมูลสำรอง (Backup Storage) ทำหน้าที่จัดเก็บข้อมูลสำรองหรือสำเนาข้อมูล ณ ศูนย์ข้อมูลสำรอง เพื่อป้องกันความเสียหายจากเหตุขัดข้องที่กระทบต่อศูนย์ข้อมูลหลัก และรองรับการกู้คืนข้อมูลหรือระบบงานเมื่อมีความจำเป็น

(๔) ระบบเครือข่ายศูนย์ข้อมูลสำรอง ทำหน้าที่เชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูลหลัก ระบบสำรองข้อมูล อุปกรณ์รักษาความมั่นคงปลอดภัย อุปกรณ์กระจายภาระการใช้งาน ระบบบริหารจัดการ และระบบอื่นที่เกี่ยวข้อง ทั้งนี้ ระบบเครือข่ายต้องรองรับการสื่อสารและการรับส่งข้อมูลระหว่างศูนย์ข้อมูลหลักกับศูนย์ข้อมูลสำรอง เพื่อรองรับการทำ Replication, Recovery, Failover และการให้บริการกรณีศูนย์ข้อมูลหลักไม่สามารถให้บริการได้ โดยต้องมี Management Network แยกจากเครือข่ายรับส่งข้อมูลหลักสำหรับบริหารจัดการอุปกรณ์และระบบภายในศูนย์ข้อมูลสำรอง

(๕) ระบบรักษาความมั่นคงปลอดภัยเครือข่าย ทำหน้าที่ควบคุมและป้องกันการรับส่งข้อมูล ณ ศูนย์ข้อมูลสำรอง รวมถึงรองรับการรักษาความมั่นคงปลอดภัยเมื่อมีการย้ายหรือกู้คืนบริการจากศูนย์ข้อมูลหลักมายังศูนย์ข้อมูลสำรอง

(๖) ระบบกระจายภาระการใช้งาน ทำหน้าที่กระจายภาระงานของระบบงาน ณ ศูนย์ข้อมูลสำรอง และรองรับการให้บริการเมื่อมีการกู้คืนหรือย้ายระบบจากศูนย์ข้อมูลหลัก

(๗) ระบบซอฟต์แวร์ Software Platform, License หรือ Subscription ทำหน้าที่รองรับการทำงานของศูนย์ข้อมูลสำรองตามสถาปัตยกรรมของโครงการ โดยระบบซอฟต์แวร์ต้องสามารถทำงานร่วมกับระบบของศูนย์ข้อมูลหลักทั้ง ๓ ชุด และรองรับการบริหารจัดการ การสืบค้น การสำรอง การกู้คืน และการตรวจสอบสถานะระบบตามรายละเอียดใน **(ภาคผนวก ๒)**

๔.๓.๓ เนื่องจากเป็นการดำเนินการเกี่ยวข้องกับการเก็บข้อมูลที่มีความซับซ้อนสูง ผู้รับจ้างที่ต้องมีบุคคลากรที่มีความเชี่ยวชาญเฉพาะด้าน โดยต้องยื่นเอกสารหลักฐานในขั้นตอนการยื่นข้อเสนอ โดยมีรายละเอียด ดังนี้

(1) ผู้จัดการโครงการ (Project Manager) โดยมีประกาศนียบัตร PMP หรือ PRINCE2 Certificate ที่ยังไม่หมดอายุ ณ วันที่ยื่นข้อเสนอ (จำนวน ๑ คน)

(2) ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย (Senior Security Specialist) ได้รับประกาศนียบัตร ได้รับประกาศนียบัตร CISSP หรือ CISM หรือ NSE 7 ที่ยังไม่หมดอายุ ณ วันที่ยื่นข้อเสนอ (จำนวน ๑ คน)

Proof

(๓) ผู้เชี่ยวชาญด้านระบบจัดเก็บข้อมูล (Senior Storage Engineer) ได้รับประกาศนียบัตร ระดับ Professional จากเจ้าของผลิตภัณฑ์ (ที่ยังไม่หมดอายุ ณ วันที่ยื่นข้อเสนอ (จำนวน ๑ คน)

(๔) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Project DPO) (จำนวน ๑ คน) ได้รับประกาศนียบัตร DPO หรือ CIPP/E ที่ยังไม่หมดอายุ ณ วันที่ยื่นข้อเสนอ

๔.๔ การตรวจสอบและทดสอบความพร้อมก่อนให้บริการ

ผู้รับจ้างต้องดำเนินการตรวจสอบก่อนให้บริการระบบสำหรับการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชนผู้รับจ้างต้องดำเนินการตรวจสอบ ปรับแต่ง และทดสอบระบบทั้งหมดที่จัดหาและติดตั้งตามข้อ ๔.๓ ก่อนเปิดให้บริการจริง เพื่อยืนยันว่าอุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ สิทธิการใช้งาน ระบบเครือข่าย ระบบประมวลผล ระบบจัดเก็บข้อมูล ระบบสำรองและกู้คืนข้อมูล ระบบรักษาความมั่นคงปลอดภัย และองค์ประกอบอื่นที่เกี่ยวข้อง สามารถทำงานร่วมกันได้อย่างถูกต้องตามสถาปัตยกรรมและขอบเขตของโครงการ โดยมีรายละเอียดการดำเนินงานอย่างน้อย ดังนี้

๔.๔.๑ ตรวจสอบความครบถ้วนของอุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ License หรือ Subscription และองค์ประกอบต่าง ๆ ที่ติดตั้ง ณ ศูนย์ข้อมูลหลัก DC จำนวน ๓ ชุด และศูนย์ข้อมูลสำรอง DR จำนวน ๑ ชุด ทั้งหมดภายใต้โครงการฯ

๔.๔.๒ ปรับแต่งประสิทธิภาพของระบบ (System Fine Tuning) ผู้รับจ้างต้องดำเนินการปรับแต่งค่าการทำงานของระบบ Hardware และ Software ที่เกี่ยวข้องให้เหมาะสมกับสถาปัตยกรรม ปริมาณข้อมูล และลักษณะการใช้งานของโครงการ เพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพและมีเสถียรภาพ

๔.๔.๓ ทดสอบการเชื่อมต่อระหว่างอุปกรณ์และระบบที่เกี่ยวข้องทั้งภายในศูนย์ข้อมูลหลัก DC ศูนย์ข้อมูลสำรอง DR และระหว่างระบบที่ต้องทำงานร่วมกัน เพื่อยืนยันว่า Server, Storage, Network, Security, Backup, ADC และ Software Platform สามารถรับส่งข้อมูลและทำงานร่วมกันได้ตามสถาปัตยกรรมที่เสนอ การทดสอบต้องครอบคลุม Network Interface, Protocol และเส้นทางการเชื่อมต่อที่ใช้งานจริง รวมถึงการเชื่อมต่อระหว่างศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองตามรูปแบบที่กำหนดไว้ในโครงการ กำหนดให้อุปกรณ์และ Software/Firmware ที่เสนอสามารถทำงานร่วมกัน และให้ยืนยัน Interface, Protocol, Network Port Mapping หรือ Connection Diagram สำหรับการเชื่อมต่อที่เกี่ยวข้อง

๔.๔.๔ ทดสอบการรับและจัดเก็บข้อมูล ผู้รับจ้างต้องทดสอบการรับข้อมูลจากแหล่งข้อมูลที่เกี่ยวข้องกับโครงการ และตรวจสอบว่าระบบสามารถรับ จัดเก็บ ประมวลผล และบริหารจัดการข้อมูลได้ตามรูปแบบการทำงานที่กำหนด ทั้งนี้ สำหรับระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ ต้องตรวจสอบว่าระบบสามารถรวบรวมข้อมูลจากระบบและอุปกรณ์ที่เกี่ยวข้องผ่านวิธีการที่กำหนด เช่น Syslog, SNMP, API, Agent, Forwarder หรือวิธีการอื่นที่ระบบรองรับ และสามารถนำข้อมูลเข้าสู่กระบวนการจัดทำดัชนีและการสืบค้นได้

Proof

๔.๔.๕ ทดสอบระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์

ผู้รับจ้างต้องทดสอบการทำงานของ Log Management Platform ให้สามารถรวบรวม จัดเก็บ บริหารจัดการ สืบค้น และวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลบันทึกเหตุการณ์ตามขอบเขตของโครงการ ดังนี้

(๑) ทดสอบการสืบค้นข้อมูลตามช่วงเวลา แหล่งข้อมูล Host, IP Address, User, Field, Keyword หรือเงื่อนไขที่ระบบรองรับ รวมถึงการแสดงผลข้อมูลผ่าน Dashboard, Report หรือรูปแบบที่ระบบรองรับ

(๒) ตรวจสอบว่าระบบสามารถบริหารจัดการจากส่วนกลางและรองรับสถาปัตยกรรมศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรอง

๔.๔.๖ การทดสอบการแบ่งแยกข้อมูล (Data Segregation)

ทดสอบการแบ่งแยกข้อมูลของผู้ให้บริการโทรศัพท์เคลื่อนที่แต่ละราย ณ ศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรอง เพื่อยืนยันว่าข้อมูลของผู้ให้บริการโทรศัพท์เคลื่อนที่แต่ละรายถูกจัดเก็บและบริหารจัดการแยกออกจากกันตามสิทธิที่กำหนด โดยต้องทดสอบว่าผู้ใช้งานของผู้ให้บริการโทรศัพท์เคลื่อนที่รายหนึ่งไม่สามารถเข้าถึง มองเห็น หรือสืบค้นข้อมูลของผู้ให้บริการโทรศัพท์เคลื่อนที่รายอื่นได้ และเมื่อมีการสำรอง ทำสำเนา หรือโอนย้ายข้อมูลไปยังศูนย์ข้อมูลสำรอง ระบบยังคงรักษาการแบ่งแยกข้อมูลดังกล่าวไว้ได้ รวมถึงระบบรักษา Data Segregation และสิทธิการเข้าถึงข้อมูลทั้งที่ DC และ DR รวมถึงตลอดกระบวนการจัดเก็บ สำรอง และเรียกคืนข้อมูล

๔.๔.๗ การตรวจสอบความสามารถด้านปริมาณข้อมูลและระยะเวลาการจัดเก็บ

ตรวจสอบ Configuration, Capacity Sizing และทรัพยากรของระบบที่ติดตั้งจริง เพื่อยืนยันว่าระบบสามารถรองรับปริมาณข้อมูลตามที่กำหนดในโครงการ ได้แก่ ปริมาณข้อมูลดิบเฉลี่ยไม่น้อยกว่า 350 GB ต่อวันต่อผู้ให้บริการโทรศัพท์เคลื่อนที่ และศูนย์ข้อมูลสำรองสามารถรองรับข้อมูลจากผู้ให้บริการโทรศัพท์เคลื่อนที่ทั้ง ๓ ราย รวมไม่น้อยกว่า 1,050 GB ต่อวัน รวมถึงตรวจสอบระบบและพื้นที่จัดเก็บข้อมูลที่จัดหาไว้สามารถรองรับระยะเวลาการจัดเก็บข้อมูลตามที่กำหนดสามารถจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และ Log ได้ไม่น้อยกว่า ๗๓๐ วัน และสามารถนำข้อมูลกลับมาสืบค้นและตรวจสอบย้อนหลังได้ ทั้งนี้ การตรวจสอบ Configuration และ Capacity Sizing ก่อนเปิดบริการไม่ใช่การรอทดสอบด้วยการเก็บข้อมูลจริงครบ ๗๓๐ วัน

๔.๔.๘ การทดสอบความพร้อมใช้งานของระบบ (High Availability)

ผู้รับจ้างต้องทดสอบความสามารถด้าน High Availability ขององค์ประกอบสำคัญที่มีการออกแบบให้ทำงานแบบสำรองหรือทดแทนกัน เพื่อยืนยันว่าเมื่อองค์ประกอบหนึ่งเกิดเหตุขัดข้อง ระบบสามารถทำงานต่อได้ตามรูปแบบ High Availability ที่เสนอให้ครอบคลุมระบบที่มีข้อกำหนดด้าน High Availability เช่น ระบบ Virtualization, Log Management Platform, ระบบเครือข่าย ระบบจัดเก็บข้อมูล อุปกรณ์รักษาความมั่นคงปลอดภัย และระบบกระจายภาระการใช้งาน Virtualization Platform High Availability, Resource Scheduling, Live Migration, Snapshot และ Centralized Management

Proof

๔.๔.๙ การทดสอบการสำรองและกู้คืนข้อมูล

ทดสอบการสำรองและกู้คืนข้อมูลของระบบที่เกี่ยวข้องตามสถาปัตยกรรมที่เสนอ เพื่อยืนยันว่าระบบสามารถสำรองข้อมูลและนำข้อมูลที่สำรองไว้กลับมาใช้งานได้ โดยให้ตรวจสอบการทำงานร่วมกันระหว่างระบบประมวลผล ระบบจัดเก็บข้อมูล ระบบ Virtualization และระบบสำรองข้อมูล รวมถึงการสำรอง ทำ Replication, Snapshot, Backup หรือกลไกอื่นที่กำหนดไว้สำหรับศูนย์ข้อมูลสำรอง Log Management Platform รองรับ High Availability รวมถึง Replication, Snapshot และ Backup ไปยังศูนย์ข้อมูลสำรอง และกำหนดให้ Virtualization สามารถทำงานร่วมกับระบบสำรองและกู้คืน Virtual Machine ได้

๔.๔.๑๐ การทดสอบระบบรักษาความมั่นคงปลอดภัย

ผู้รับจ้างต้องทดสอบการทำงานของระบบรักษาความมั่นคงปลอดภัยที่จัดหาในโครงการ อย่างน้อยดังนี้

(๑) อุปกรณ์รักษาความปลอดภัยเครือข่าย
(๒) ระบบบริหารจัดการสิทธิ์ผู้ดูแลระบบ (PAM)
(๓) ระบบยืนยันตัวตนส่วนกลางและ MFA/AAA
(๔) ระบบบริหารจัดการและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย
(๕) ระบบรักษาความปลอดภัยอุปกรณ์ปลายทาง (EDR)

ทั้งนี้ ในส่วนของ EDR ต้องตรวจสอบว่าระบบสามารถตรวจจับและตอบสนองต่อเหตุการณ์ที่เกี่ยวข้อง และสามารถบริหารจัดการเครื่องที่อยู่ภายใต้การควบคุมจากส่วนกลาง เช่น Endpoint Isolation หรือ Network Quarantine และ Centralized Management เป็นอย่างน้อย

๔.๔.๑๑ การทดสอบระบบตรวจสอบและบริหารจัดการโครงสร้างพื้นฐาน

ทดสอบระบบ Infrastructure Monitoring ให้สามารถตรวจสอบสถานะความพร้อมใช้งาน และประสิทธิภาพของระบบที่อยู่ในขอบเขตโครงการได้ และตรวจสอบการแสดงสถานะของระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย ระบบจำลองเสมือน และระบบฐานข้อมูลจากระบบบริหารจัดการส่วนกลาง รวมถึง Dashboard, Network Topology, Historical Information, Threshold และการแจ้งเตือนเมื่อระบบเกิดข้อขัดข้องหรือมีค่าการทำงานเกินเกณฑ์ที่กำหนด เช่น Monitoring System รองรับ Dashboard, Network Topology, Historical Correlation, Threshold/Alert และการจัดทำรายงานสถานะ ความพร้อมใช้งาน และประสิทธิภาพ เป็นอย่างน้อย

๔.๔.๑๒ การทดสอบการบริหารจัดการระบบจากส่วนกลาง

ตรวจสอบระบบที่กำหนดให้มีการบริหารจัดการจากส่วนกลางสามารถตรวจสอบสถานะและบริหารจัดการระบบที่เกี่ยวข้อง ณ ศูนย์ข้อมูลหลักทั้ง ๓ ชุด และศูนย์ข้อมูลสำรองได้ตามสิทธิและหน้าที่ของแต่ละระบบ ให้ครอบคลุมอย่างน้อยระบบ Virtualization, EDR, Log Management Platform, Infrastructure Monitoring และระบบบริหารจัดการความมั่นคงปลอดภัยที่เกี่ยวข้อง ตามความสามารถของผลิตภัณฑ์และสถาปัตยกรรมที่ติดตั้ง

Proof

๔.๔.๑๓ การแก้ไขผลการทดสอบก่อนเปิดให้บริการ

การตรวจสอบหรือทดสอบพบว่าอุปกรณ์ ระบบ Software, Configuration, License, การเชื่อมต่อ หรือองค์ประกอบใดไม่สามารถทำงานได้ตามข้อกำหนด หรือสถาปัตยกรรมที่เสนอ ผู้รับจ้างต้องดำเนินการแก้ไข ปรับแต่ง หรือดำเนินการอื่นที่จำเป็นให้ระบบสามารถทำงานได้ครบถ้วนก่อนเปิดให้บริการ

๔.๔.๑๔ การจัดทำรายงานผลการตรวจสอบและทดสอบระบบ

จัดทำรายงานผลการตรวจสอบ การปรับแต่ง และการทดสอบระบบก่อนเปิดให้บริการ โดยแสดงรายการที่ตรวจสอบ วิธีการทดสอบ ผลการทดสอบ ปัญหาที่พบ และผลการแก้ไข เพื่อส่งมอบให้สำนักงาน กสทช. ใช้ประกอบการตรวจรับงานก่อนเข้าสู่ระยะการให้บริการ การปรับแต่งต้องครอบคลุมองค์ประกอบที่เกี่ยวข้องกับการประมวลผล การจัดเก็บข้อมูล การรับส่งข้อมูล การสืบค้น การสำรองและกู้คืนข้อมูล และระบบบริหารจัดการตามที่ติดตั้งใช้งานจริง

๔.๕ การให้บริการระบบสำหรับการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชนระยะที่ ๒ (๖๐ เดือน) ผู้รับจ้างต้องดำเนินการ อย่างน้อยดังนี้

๔.๕.๑ การบริหารจัดการ ดูแลระบบ และควบคุมการทำงานของระบบสารสนเทศให้สามารถให้บริการได้อย่างต่อเนื่อง มีเสถียรภาพ และมีความมั่นคงปลอดภัยตลอดระยะเวลาการให้บริการ ๕ ปี (๖๐ เดือน) โดยอย่างน้อยต้องดำเนินการ ดังนี้

(๑) จัดให้มีบุคลากรผู้รับผิดชอบในการบริหารจัดการระบบ และประสานงานกับผู้ว่าจ้างตลอดระยะเวลาการให้บริการ

(๒) ตรวจสอบ ติดตาม และเฝ้าระวังสถานะและประสิทธิภาพของระบบ อุปกรณ์ เครือข่าย และองค์ประกอบที่เกี่ยวข้อง พร้อมดำเนินการแก้ไขเมื่อพบความผิดปกติ

(๓) บริหารจัดการบัญชีผู้ใช้งาน สิทธิ์การเข้าถึง การตั้งค่าระบบ และองค์ประกอบของระบบให้มีความถูกต้องและเหมาะสม

(๔) ดำเนินการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบและข้อมูล รวมถึงการตรวจสอบและจัดเก็บข้อมูล Log ตามข้อกำหนดที่เกี่ยวข้อง

(๕) จัดทำรายงานผลการบริหารจัดการระบบ ปัญหา เหตุขัดข้อง การดำเนินการแก้ไข และข้อเสนอแนะในการปรับปรุงระบบ เสนอต่อผู้ว่าจ้างตามระยะเวลาที่กำหนด

(๖) การบริหารจัดการระบบต้องเป็นไปตามนโยบาย มาตรฐาน กฎหมาย และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

๔.๕.๒ การบริการบำรุงรักษา และการรักษาระดับคุณภาพการให้บริการภายหลังจากการดำเนินงาน ได้รับการตรวจรับครบถ้วนแล้ว ผู้รับจ้างต้องดำเนินการบริหารจัดการระบบบำรุงรักษาเชิงแก้ไข (Corrective Maintenance) ให้บริการสนับสนุนทางเทคนิค ตรวจสอบสถานะระบบและรักษาระดับคุณภาพการให้บริการ (Service Level Agreement) หรือ SLA ให้เป็นไปตามเกณฑ์ที่กำหนด ตลอดระยะเวลาการให้บริการ ๕ ปี (๖๐ เดือน) นับถัดจากวันที่ผู้ว่าจ้างมีหนังสือแจ้งให้เริ่มดำเนินงาน โดยผู้รับจ้างมีหน้าที่บำรุงรักษาอุปกรณ์บริการตลอดจนสิ่งอำนวยความสะดวกต่าง ๆ ให้อยู่ในสภาพพร้อมใช้งานอย่างดี มีประสิทธิภาพตลอดเวลาการให้บริการ โดยต้องจัดให้มีบริการบำรุงรักษา ดังนี้

Proof

(๑) จัดให้มีศูนย์บริการสนับสนุนและให้คำปรึกษาแนะนำเกี่ยวกับการใช้งานและการแก้ไขปัญหาเบื้องต้น ด้วยเจ้าหน้าที่เทคนิคให้บริการตลอดเวลาในวันทำการปกติ โดยต้องแจ้งรายชื่อพร้อมหมายเลขโทรศัพท์ และ ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-Mail) เพื่อการติดต่อสื่อสารได้โดยตรง

(๒) จัดให้มีศูนย์บริการรับแจ้งข้อขัดข้องลักษณะ Call Center Service หรือ Help Desk หรือมีระบบรับแจ้งข้อขัดข้องทางอิเล็กทรอนิกส์แบบอื่น เพื่อให้เจ้าหน้าที่ของผู้ว่าจ้างหรือผู้รับบริการประเภทต่าง ๆ สามารถแจ้งข้อขัดข้องได้ทางโทรศัพท์ โทรสาร e-Mail หรือ Application ทางอิเล็กทรอนิกส์อื่น โดยผู้รับจ้างต้องแจ้งรายละเอียดช่องทางการรับแจ้งข้อขัดข้องให้ทราบพร้อมกับการรายงานผลการทดสอบความพร้อมในการเปิดให้บริการ

(๓) การแจ้งข้อขัดข้องของการใช้บริการ ให้ถือวันเวลาที่ได้รับแจ้งเป็นเวลาเริ่มให้บริการบำรุงรักษาและซ่อมแซมแก้ไข ซึ่งผู้รับจ้างต้องบริการตามข้อกำหนดระดับคุณภาพการให้บริการ (Service Level Agreement: SLA) ที่กำหนด

(๔) เพื่อประสิทธิภาพการบริการแก้ไขข้อขัดข้องเป็นไปตามข้อกำหนดระดับคุณภาพการให้บริการ (Service Level Agreement: SLA) กำหนดให้ผู้รับจ้างต้องรวบรวมข้อมูลตามสถานที่หรือจุดบริการแต่ละชุด ดังนี้

(๔.๑) ชื่อผู้แจ้งเหตุขัดข้องหรือผู้รับผิดชอบ

(๔.๒) หมายเลขโทรศัพท์ที่สามารถติดต่อได้ตลอดเวลา เพื่อความสะดวกในการติดต่อประสานงานของช่างหรือเจ้าหน้าที่ของผู้รับจ้างในระหว่าง การเดินทางหรือเมื่อเดินทางไปถึง ณ สถานที่ปฏิบัติงานนั้นแล้ว

(๔.๓) อาการหรือเหตุขัดข้องเบื้องต้น

(๕) การบำรุงรักษาเพื่อป้องกัน (Preventive Maintenance)

(๕.๑) ตรวจสภาพการทำงานของอุปกรณ์ของบริการแต่ละประเภท และทำความสะอาดให้เรียบร้อยและอยู่ในสภาพพร้อมใช้งาน รวมทั้งเปลี่ยนวัสดุ อะไหล่ หรืออุปกรณ์อื่นใดที่พบว่ามีการเสื่อมสภาพ หมดอายุการใช้งาน ซึ่งหากปล่อยทิ้งไว้จะกระทบต่อคุณภาพการให้บริการ

(๕.๒) ตรวจสอบการทำงานของอุปกรณ์ของบริการแต่ละประเภท รวมทั้งการปรับแต่งประสิทธิภาพการบริการ (Performance Service Tuning) ให้อยู่ในสภาพพร้อมใช้งานได้อย่างดี

(๕.๓) เมื่อทำการบำรุงรักษาเรียบร้อยแล้ว ต้องทำการทดสอบความเชื่อมโยงและคุณภาพบริการโดยรวมว่าสามารถใช้งานได้ตามปกติด้วยคุณภาพบริการที่กำหนด

(๕.๔) รอบระยะเวลาของการทำ Preventive Maintenance ทุก ๓ เดือนครั้ง โดยแต่ละครั้งต้องอยู่ระหว่าง ๗๐ - ๑๐๐ วัน เพื่อให้อุปกรณ์ได้รับการบำรุงรักษาภายในระยะเวลาไม่กระชั้นชิดหรือห่างกันเกินไปในรอบการบริการแต่ละครั้ง ทั้งนี้ ผู้รับจ้างต้องจัดทำแผนการบำรุงรักษาที่แสดงรายละเอียดกำหนดเวลาเข้าทำการบำรุงรักษาบริการแต่ละประเภทในแต่ละปีโดยละเอียด และส่งให้ผู้ว่าจ้างทราบล่วงหน้าอย่างน้อย ๓๐ วัน

Proof

(๖) การซ่อมแซมแก้ไขข้อชำรุดขัดข้อง (Corrective Maintenance)

ตรวจสอบข้อขัดข้องระบบ ทำการแก้ไข และจัดการให้สามารถปฏิบัติงานได้ดีดังเดิม รวมถึงการเปลี่ยนอะไหล่ ชิ้นส่วน หรืออุปกรณ์ที่ชำรุด เสื่อมสภาพ หรือหมดอายุการใช้งาน เมื่อได้รับแจ้งจากผู้แจ้งเหตุขัดข้องหรือผู้รับบริการประเภทต่าง ๆ หรือระบบควบคุมคุณภาพการให้บริการที่ผู้ว่าจ้างจัดทำขึ้น ไปยังศูนย์บริการรับแจ้งข้อขัดข้อง (Call Center Service หรือ Help Desk) ของผู้รับจ้าง โดยเมื่อได้รับแจ้งเหตุหรือมีเหตุขัดข้องแล้ว จะต้องส่งช่างหรือเจ้าหน้าที่ผู้มีความรู้ความชำนาญ ไปทำการตรวจวิเคราะห์และแก้ไขข้อขัดข้อง ณ จุดบริการต่าง ๆ เพื่อไปตรวจวิเคราะห์ข้อขัดข้องภายในเวลา ๑ ชั่วโมง นับแต่เวลาที่เดินทางไปถึงจุดบริการนั้น ๆ การวิเคราะห์ข้อขัดข้องและระบุระดับการบริการ (Service Level) จะต้องได้รับความเห็นพ้องของเจ้าหน้าที่ของ ผู้ว่าจ้างด้วยและผู้รับจ้างต้องดำเนินการแก้ไขข้อขัดข้องนั้นภายในระยะเวลาที่กำหนด

ทั้งนี้ ช่างหรือเจ้าหน้าที่ของผู้รับจ้างสามารถติดต่อสอบถามให้คำแนะนำหรือขอทราบข้อเท็จจริงเกี่ยวกับเหตุหรือข้อขัดข้องนั้นเพิ่มเติมจากเจ้าหน้าที่ผู้แจ้งเหตุขัดข้องนั้นในเบื้องต้นเพื่อประเมินสถานการณ์ก่อนเดินทางหรือระหว่างเดินทาง เพื่อเตรียมการด้านอะไหล่ วัสดุ อุปกรณ์ให้พร้อมและสามารถเปลี่ยนทดแทนเพื่อบริการซ่อมแซมแก้ไขได้อย่างรวดเร็วภายในเวลาที่กำหนด และหากจำเป็นต้องเปลี่ยนเครื่องและอุปกรณ์ทดแทน ต้องเป็นยี่ห้อ รุ่น เช่นเดียวกับของเดิมหรือรุ่นใหม่ที่ผลิตทดแทนซึ่งมีคุณสมบัติเช่นเดิมหรือดีกว่า โดยต้องจัดทำรายงานการเปลี่ยนแปลงอุปกรณ์ทดแทนพร้อมรายละเอียดของอุปกรณ์ที่เปลี่ยนทดแทน และข้อมูลประกอบต่าง ๆ ที่เกี่ยวข้อง

๔.๕.๓ ข้อกำหนดระดับการบริการ (Service Level Agreement)

ระดับความรุนแรง	ผลกระทบ	ระยะเวลาตอบกลับ	ระยะเวลาแก้ไข
Severity ๑ (Critical)	ระบบหลักล่มโดยสิ้นเชิง (Total Outage)	ภายใน ๑๕ นาที	ภายใน ๔ ชม.
Severity ๒ (High)	ระบบบางส่วนของศูนย์หลักเสียหาย หรือศูนย์สำรองล่ม	ภายใน ๓๐ นาที	ภายใน ๘ ชม.
Severity ๓ (Medium)	อุปกรณ์บริหารจัดการหรือระบบวิเคราะห์มีปัญหา (ระบบหลักยังทำงานได้)	ภายใน ๑ ชม.	ภายใน ๔๘ ชม.
Severity ๔ (Low)	อุปกรณ์ทำงานได้ปกติ แต่ต้องการคำปรึกษา หรือเป็นปัญหาภายนอก	ภายใน ๔ ชม.	ภายใน ๗๒ ชม.

(๑) ระดับที่ ๑ (Critical) ความสำคัญสูงสุด โดยอุปกรณ์แกนหลัก (Core Infrastructure) ของศูนย์ข้อมูลหลัก หากระบบเหล่านี้ดาวน์ ส่งผลกระทบทำให้บริการทั้งหมดหยุดทำงานทันที ดังนี้

(๑.๑) อุปกรณ์กระจายสัญญาณสำหรับศูนย์ข้อมูล (Core/Spine-Leaf Switch ของศูนย์หลัก)

(๑.๒) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับศูนย์ข้อมูลหลัก (Main Enterprise Server)

(๑.๓) ระบบจัดเก็บข้อมูลหลัก ประจำศูนย์ข้อมูลหลัก (Main Storage Production)

(๑.๔) อุปกรณ์รักษาความปลอดภัยเครือข่ายสำหรับศูนย์ข้อมูลหลัก (Core Firewall/IPS ของศูนย์หลัก)

Proof

(๑.๕) อุปกรณ์กระจายภาระงานสำหรับศูนย์ข้อมูลหลัก (Load Balancer ของศูนย์หลัก)

(๑.๖) ระบบบริหารจัดการการจำลองเสมือน (Hypervisor/ Virtualization Platform)

(๑.๗) ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย (Server OS ที่รัน Production Apps)

(๒) ระดับที่ ๒ (High) ความสำคัญสูง โดยระบบของศูนย์ข้อมูลสำรอง (DR Site) หรืออุปกรณ์ที่ช่วยกระจายความเสี่ยง/ระบุตัวตน หากล่มจะทำให้ไม่มีระบบ Backup รองรับ หรือความปลอดภัยลดลง ดังนี้

(๒.๑) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับศูนย์ข้อมูลสำรอง

(๒.๒) ระบบจัดเก็บข้อมูลหลัก ประจำศูนย์ข้อมูลสำรอง

(๒.๓) อุปกรณ์ข้อมูลสำรองระดับองค์กร (Enterprise Backup Hardware/Tape/Target Storage)

(๒.๔) อุปกรณ์รักษาความปลอดภัยเครือข่ายสำหรับศูนย์ข้อมูลสำรอง

(๒.๕) ระบบตรวจสอบและยืนยันตัวตนกลาง (Centralized Authentication/AD/Identity Server)

(๒.๖) อุปกรณ์กระจายภาระงานสำหรับศูนย์ข้อมูลสำรอง

(๓) ระดับที่ ๓ (Medium) ความสำคัญปานกลาง โดยระบบบริหารจัดการ (Management), ระบบมอนิเตอร์ และระบบวิเคราะห์ข้อมูล หากระบบเหล่านี้มีปัญหา ตัวระบบเครือข่ายและ Server หลักยังคงให้บริการได้ตามปกติ แต่ผู้ดูแลระบบจะขาดเครื่องมือในการควบคุมหรือตรวจสอบ

(๓.๑) อุปกรณ์กระจายสัญญาณสำหรับบริหารจัดการ (Management Switch)

(๓.๒) อุปกรณ์บริหารจัดการตรวจสอบสิทธิ์การเข้าถึง (Access Control/TACACS+/RADIUS)

(๓.๓) ระบบบริหารจัดการและวิเคราะห์ข้อมูลความมั่นคงปลอดภัย (SIEM / SOAR / Security Analytics)

(๓.๔) ระบบรักษาความปลอดภัยปลายทาง (Endpoint Security/EDR)

(๓.๕) ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจร (Log Management /Traffic Analytics)

(๓.๖) ระบบตรวจสอบและสังเกตการณ์ (Monitoring/ Observability Software)

(๔) ระดับที่ ๔ (Low) การสนับสนุนทั่วไป โดยไม่มีผลกระทบต่อการทำงานของระบบ (Non-disruptive) เช่น การสอบถามข้อมูลทางเทคนิค, การขอคู่มือการใช้งาน, การอัปเดต Patch ประจำงวดที่ไม่มีความเสี่ยงเร่งด่วน หรือปัญหาด้านเอกสาร/รายงาน MA โดยรายการ

Proof

ที่เกี่ยวข้อง ใช้ครอบคลุมทุกอุปกรณ์ในโครงการ เมื่อเป็นการร้องขอปรึกษาการใช้งาน (Request for usage consultation) หรือการปรึกษาคอนฟิกูเรชันทั่วไปที่ไม่ใช่เหตุการณ์ผิดปกติ (Incident)

(๕) กรณีเกิดอุบัติเหตุ เหตุสุดวิสัยจากภัยพิบัติ หรือเหตุอื่นใดซึ่งมิใช่เกิดจากความผิดหรือความบกพร่องของผู้รับจ้าง เป็นเหตุให้เกิดข้อขัดข้องหรือการบริการต้องหยุดชะงักลง เมื่อได้รับแจ้งเหตุจากเจ้าหน้าที่ผู้รับผิดชอบแล้ว ต้องให้ความร่วมมือในการเข้าตรวจสอบและซ่อมแซมแก้ไข กรณีเช่นนี้ถือเป็นกรณียกเว้นข้อกำหนดระดับการให้บริการ (SLA) ตามข้อ ๔.๕.๓ แต่ผู้รับจ้างจะต้องทำการซ่อมแซมแก้ไข หรือเปลี่ยนทดแทน หรือการจัดให้มีโครงข่ายสื่อสารสำรองเพื่อให้สามารถบริการได้โดยเร็ว ทั้งนี้ อย่างช้าต้องไม่เกิน ๒๔ ชั่วโมง หรือภายในวันเวลาที่จะกำหนดตามความยากง่ายของเหตุดังกล่าว เพื่อให้บริการระบบฯ สามารถกลับมาใช้งานได้ตามปกติ ทั้งนี้ การหยุดชะงักการให้บริการดังกล่าวไม่ถือว่าเป็นความผิดหรือความบกพร่องของผู้รับจ้างในการหยุดให้บริการ

๔.๕.๔ ประสิทธิภาพรวมของการให้บริการ

เพื่อประสิทธิภาพของการให้บริการโครงการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน (U-DEX) ด้านการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนการสืบค้นข้อมูลให้เป็นไปตามวัตถุประสงค์โครงการได้อย่างต่อเนื่องด้วยคุณภาพและประสิทธิภาพการบริการตลอดระยะเวลาบริการ ผู้ว่าจ้างจะประเมินผลภาพรวมประสิทธิภาพการใช้งานเดือนละครั้ง โดยยอมรับให้มีเวลาขัดข้องสะสมรวมของบริการอินเทอร์เน็ตความเร็วสูง (High Service Level) ตามข้อ ๔.๕.๓ ไม่เกิน ๖ ชั่วโมงต่อเดือนต่อจุดบริการ นับแต่เวลาได้ทราบผลการวิเคราะห์ข้อขัดข้อง คิดเป็นความสามารถใช้งานเชื่อมต่อสัญญาณอินเทอร์เน็ตได้ไม่ต่ำกว่าร้อยละ ๙๙.๐ ต่อเดือน (% Available Service = ๙๙.๐) โดยมีสูตรการคำนวณ ดังนี้

$$\text{Availability Service} = \left\{\frac{\text{Total operation minutes} - \text{Total minutes of service downtime}}{\text{Total operation minutes}}\right\} \times ๑๐๐$$

ทั้งนี้ การนับเวลาจะไม่รวมเหตุเสียเนื่องจากอุปกรณ์ปลายทางหรือเหตุอื่นที่ไม่เกี่ยวเนื่องกับโครงข่ายหรือเหตุตามข้อ ๔.๕.๓

๔.๕.๕ ผู้รับจ้างต้องจัดทำรายงานคุณภาพการให้บริการต่อวันของแต่ละจุดบริการในรอบ ๓ เดือน

จัดทำและส่งมอบรายงานผลการตรวจสอบสถานะและประสิทธิภาพการทำงานของระบบโดยอัตโนมัติ (Automated System Health Check Report) เป็นประจำทุก ๓ เดือน และจัดทำรายงานผลการดำเนินงาน รายงานเหตุขัดข้อง รายงานการบำรุงรักษาเชิงแก้ไข รายงานสถานะการจัดเก็บข้อมูล และรายงานอื่นที่เกี่ยวข้อง เพื่อประกอบการตรวจรับงานบริการตามรอบระยะเวลาที่กำหนด ทั้งนี้ หากในงวดบริการใด ผู้รับจ้างไม่สามารถรักษาระดับคุณภาพการให้บริการตาม SLA หรือไม่สามารถส่งมอบรายงานและเอกสารประกอบการตรวจรับได้ครบถ้วน ผู้ว่าจ้างมีสิทธิระงับการตรวจรับ ระงับการจ่ายเงิน หักค่าบริการ หรือดำเนินการตามเงื่อนไขค่าปรับที่กำหนดไว้ในสัญญาแล้วแต่กรณี และผู้รับจ้างต้องส่งรายงานในรูปแบบสะสมผลการให้บริการต่อเนื่องจนสิ้นสุดการให้บริการ

Proof

๕. กำหนดระยะเวลาส่งมอบการดำเนินงาน

ระยะเวลาดำเนินงานรวม ๗๒ เดือน โดยแบ่งเป็นความสำเร็จของการดำเนินงาน ดังนี้

๕.๑ งานสำรวจและตรวจสอบให้เสร็จ ภายใน ๑๒ เดือน (การดำเนินงานระยะที่ ๑ งวดงานที่ ๑ ถึงงวดที่ ๓)

๕.๒ งานให้บริการต่อเนื่อง ภายใน ๖๐ เดือนนับถัดจากส่งมอบงานระยะที่ ๑ เรียบร้อยแล้ว

๖. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

สำนักงาน กสทช. จะพิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคาและพิจารณาราคารวม

๗. วงเงินงบประมาณ

กรอบวงเงินที่ได้รับการจัดสรรเพื่อการจ้างครั้งนี้ จำนวน **๙๘๐,๐๐๐,๐๐๐ บาท (เก้าร้อยแปดสิบล้านบาทถ้วน)** ซึ่งรวมภาษีมูลค่าเพิ่มภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กองทุน USO) บัญชี ๓ USO โทรคมนาคม

๘. งวดงานและการจ่ายเงิน

๘.๑ งวดงานการดำเนินงานมีจำนวน ๒ ระยะ (ระยะที่ ๑ ในงวดที่ ๑ ถึงงวดที่ ๓) และ (ระยะที่ ๒ ในงวดที่ ๔ ถึง งวดที่ ๑๓) รายละเอียด ดังนี้

งวด	รายละเอียดงานที่ส่งมอบ	ระยะเวลาดำเนินงาน นับถัดจากวันลงนามในสัญญา	อัตราร้อยละของค่าจ้างตามสัญญา
๑	ดำเนินการตามข้อ ๔.๒	ภายใน ๓๐ วัน	ร้อยละ ๕
๒	ดำเนินการตามข้อ ๔.๓	ภายใน ๒๗๐ วัน	ร้อยละ ๒๕
๓	ดำเนินการตามข้อ ๔.๔	ภายใน ๓๖๕ วัน	ร้อยละ ๒๕
๔ ถึง ๑๓	ดำเนินการตามข้อ ๔.๕	ภายใน ๖ เดือน นับถัดจากงวดที่ ๑ (๖๐ เดือน) ชำระเป็นรายงวดเท่า ๆ กัน (๖ เดือนครั้ง) จำนวน ๑๐ งวด (ร้อยละ ๔.๕ ต่องวด)	ร้อยละ ๔๕

ทั้งนี้ การส่งมอบงานแต่ละงวดต้องจัดทำรายงานประกอบการส่งมอบบริการในรูปแบบเอกสาร (Hard Copy) จำนวน ๒ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ (Soft Copy) อีกจำนวน ๒ ชุด

Proof

๘.๒ การจ่ายเงินล่วงหน้า

ผู้ว่าจ้างตกลงจ่ายเงินค่าจ้างล่วงหน้าให้แก่ผู้รับจ้าง ไม่เกินอัตราร้อยละ ๑๕ ของค่าจ้างงานระยะที่ ๑ ตามสัญญา ซึ่งไม่เกินร้อยละ ๑๐ ของค่าจ้างบริการทั้งหมดตามสัญญา โดยจะจ่ายให้ภายหลังจากที่ผู้รับจ้างได้วางหลักประกันการรับเงินค่าจ้างล่วงหน้าเป็นหนังสือค้ำประกันหรือหนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศหรือพันธบัตรรัฐบาลไทย เต็มตามจำนวนเงินค่าจ้างล่วงหน้านั้น โดยผู้รับจ้างต้องออกใบเสร็จรับเงินค่าจ้างล่วงหน้าตามแบบที่ผู้ว่าจ้างกำหนด และผู้รับจ้างตกลงที่จะกระทำตามเงื่อนไขอันเกี่ยวกับการใช้จ่ายและการใช้คืนเงินค่าจ้างล่วงหน้า ดังนี้

๘.๒.๑ ผู้รับจ้างจะใช้เงินค่าจ้างล่วงหน้าเพื่อเป็นค่าใช้จ่ายในการปฏิบัติงานตามสัญญาเท่านั้น หากผู้รับจ้างใช้จ่ายเงินค่าจ้างล่วงหน้าหรือส่วนใดส่วนหนึ่งของเงินค่าจ้างล่วงหน้านั้นในทางอื่น ผู้ว่าจ้างอาจจะเรียกเงินค่าจ้างล่วงหน้านั้นคืนจากผู้รับจ้างหรือบังคับเอาจากหลักประกันการรับเงินค่าจ้างล่วงหน้าได้ทันที

๘.๒.๒ เมื่อผู้ว่าจ้างเรียกร้อง ผู้รับจ้างต้องแสดงหลักฐานการใช้จ่ายเงินค่าจ้างล่วงหน้าเพื่อพิสูจน์ว่าได้เป็นไปตามข้อ ๘.๒.๑ ภายใน ๑๕ วัน นับถัดจากวันได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง หากผู้รับจ้างไม่อาจแสดงหลักฐานภายในกำหนด ผู้ว่าจ้างอาจเรียกเงินค่าจ้างล่วงหน้าคืนจากผู้รับจ้างหรือบังคับเอาจากหลักประกันการรับเงินค่าจ้างล่วงหน้าได้ทันที

๘.๒.๓ ในการจ่ายเงินค่าจ้างสำหรับงานระยะที่ ๑ (งวดที่ ๑ ถึงงวดที่ ๓) ผู้ว่าจ้างจะหักคืนเงินค่าจ้างล่วงหน้าในแต่ละงวด (งวดที่ ๑ ถึงงวดที่ ๒) เพื่อชดใช้คืนเงินค่าจ้างล่วงหน้าไว้จำนวนร้อยละ ๑๕ ของจำนวนเงินค่าจ้างแต่ละงวดจนกว่าจำนวนเงินที่หักไว้จะครบตามจำนวนเงินค่าจ้างล่วงหน้าที่ได้รับไปแล้ว ยกเว้นงวดสุดท้ายของงานบริการส่วนที่ ๑ (งวดที่ ๓) จะหักไว้เป็นจำนวนกับเงินค่าจ้างล่วงหน้าที่เหลือทั้งหมด

๘.๒.๔ เงินจำนวนใด ๆ ก็ตามที่ผู้รับจ้างจะต้องจ่ายให้แก่ผู้ว่าจ้างเพื่อชำระหนี้หรือเพื่อชดใช้ความรับผิดต่าง ๆ ตามสัญญา ผู้ว่าจ้างจะหักเอาจากเงินค่าจ้างงวดที่จะจ่ายให้แก่ผู้รับจ้างก่อนที่จะหักใช้เงินค่าจ้างล่วงหน้า

๘.๒.๕ ในกรณีที่มีการบอกเลิกสัญญา หากเงินค่าจ้างล่วงหน้าที่เหลือเกินกว่าจำนวนเงินที่ผู้รับจ้างจะได้รับหลังจากหักชดใช้กรณีอื่นแล้ว ผู้รับจ้างจะต้องจ่ายคืนเงินจำนวนที่เหลือนั้นให้แก่ผู้ว่าจ้างภายใน ๗ วัน นับถัดจากวันได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง

๘.๒.๖ ผู้ว่าจ้างจะคืนหลักประกันเงินค่าจ้างล่วงหน้าให้แก่ผู้รับจ้างต่อเมื่อผู้ว่าจ้างได้หักเงินค่าจ้างไว้ครบจำนวนเงินค่าจ้างล่วงหน้าตามข้อ ๘.๒.๓ แล้ว

Proof

๙. อัตราค่าปรับ

๙.๑ ค่าปรับสำหรับการดำเนินงาน (ระยะที่ ๑)

โดยที่ผู้ว่าจ้างต้องการความสำเร็จพร้อมกันทั้งหมด โดยผู้รับจ้างต้องส่งมอบการดำเนินงานให้ครบถ้วนถูกต้องภายใน ๓๖๕ วันนับถัดจากวันลงนามในสัญญา กรณีผู้รับจ้างไม่สามารถส่งมอบให้ครบถ้วนถูกต้องภายในกำหนดไม่ว่าทั้งหมด หรือบางส่วน และผู้ว่าจ้างยังมิได้บอกเลิกสัญญา ผู้รับจ้างต้องชำระค่าปรับในอัตราร้อยละ ๐.๐๕ ของค่าจ้างทั้งสัญญา นับถัดจากวันครบกำหนดจนถึงวันที่ส่งมอบครบถ้วนถูกต้อง หรือจนถึงวันที่ผู้ว่าจ้างบอกเลิกสัญญา แล้วแต่กรณี

๙.๒ ค่าปรับสำหรับการดำเนินงาน (ระยะที่ ๒)

๙.๒.๑ กรณีเกิดปัญหาข้อขัดข้องและผู้รับจ้างได้รับแจ้งข้อขัดข้องนั้นแล้วไม่เดินทางไปทำการตรวจวิเคราะห์และแก้ไขข้อขัดข้อง ณ จุดบริการชุดหนึ่งชุดใด ภายใน ๔ ชั่วโมง นับแต่เวลาได้รับแจ้งข้อขัดข้อง หรือไม่ทำการตรวจวิเคราะห์ให้ทราบข้อขัดข้อง วิธีการแก้ไขและกำหนดระดับการบริการ (Service Level Agreement) ภายใน ๑ ชั่วโมง นับแต่เวลาที่เดินทางไปถึงจุดบริการนั้น ๆ ตามข้อ ๔.๕.๓ ต้องชำระค่าปรับในอัตราชั่วโมงละ ๕,๐๐๐ บาท ต่อกรณี เศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง

๙.๒.๒ กรณีได้ดำเนินการตามข้อ ๔.๕.๓ แล้ว แต่ไม่ดำเนินการแก้ไขปัญหาหรือไม่บริการด้วยคุณภาพและประสิทธิภาพตามที่กำหนดให้แล้วเสร็จภายในระยะเวลาที่กำหนดตามข้อตกลงระดับบริการ (Service Level Agreement) แต่ละระดับตามข้อ ๔.๕.๓ (๑) - (๓) ต้องชำระค่าปรับในอัตราชั่วโมงละ ๕,๐๐๐ บาท เศษของชั่วโมงให้นับเป็น ๑ ชั่วโมง

๙.๒.๓ กรณีการชำรุดขัดข้องเกิดอุบัติเหตุ เหตุสุดวิสัยจากภัยพิบัติ หรือเหตุอื่นใดซึ่งมิใช่เกิดจากความผิดหรือความบกพร่องของผู้รับจ้าง เป็นเหตุให้เกิดข้อขัดข้องหรือการบริการต้องหยุดชะงักลง และไม่ทำการซ่อมแซมแก้ไข หรือเปลี่ยนทดแทน หรือการจัดให้มีโครงข่ายสื่อสารสำรองเพื่อให้สามารถบริการได้โดยเร็วภายในระยะเวลาที่กำหนดตามข้อ ๔.๕.๓(๕) ต้องชำระค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๐๕ ของค่าจ้างบริการแต่ละงวดที่เกิดต่อกรณี นับถัดจากวันครบกำหนดจนถึงวันที่ได้ดำเนินการแก้ไขครบถ้วนถูกต้อง

๙.๒.๔ กรณีมีเวลาขัดข้องสะสมรวมของบริการอินเทอร์เน็ตความเร็วสูง (High Service Level) ตามข้อ ๔.๕.๓ ในรอบเดือนเกิน ๔ ชั่วโมงต่อเดือนต่อจุดบริการ นับแต่เวลาได้ทราบผลการวิเคราะห์ข้อขัดข้อง ต้องชำระค่าปรับประสิทธิภาพรวมการบริการในอัตราชั่วโมงละ ๕,๐๐๐ บาท เศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง ทั้งนี้ ไม่รวมเหตุเสียเนื่องจากอุปกรณ์ปลายทางหรือเหตุอื่นที่ไม่เกี่ยวเนื่องกับโครงข่าย

๙.๒.๕ นอกจากกรณีตามข้อ ๙.๒.๒ ถึงข้อ ๙.๒.๔ แล้ว หากผู้ว่าจ้างพบว่าผู้รับจ้างไม่ดำเนินงานบริการระยะที่ ๒ ให้เป็นไปตามสัญญาหรือรายละเอียดแนบท้ายสัญญา ผู้ว่าจ้างจะแจ้งให้ผู้รับจ้างทราบเพื่อปรับปรุงแก้ไขภายในเวลาที่กำหนด หากล่วงเลยกำหนดเวลาดังกล่าวต้องชำระค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ของค่าจ้างบริการแต่ละงวดที่เกิดกรณีนั้น ๆ นับถัดจากวันครบกำหนดจนถึงวันที่ผู้รับจ้างปรับปรุงแก้ไขให้ครบถ้วนถูกต้อง

Proof

๙.๒.๖ ค่าปรับดังกล่าวในข้อ ๙.๑ และข้อ ๙.๒ ผู้ว่าจ้างจะหักจากค่าจ้างบริการที่ต้องจ่ายในงวดนั้นจนครบจำนวนค่าปรับ หากค่าจ้างบริการงวดนั้นไม่เพียงพอหักค่าปรับ ผู้ว่าจ้างจะหักจากค่าจ้างบริการงวดถัดไปจนครบจำนวนค่าปรับ

๑๐. การปฏิบัติตามกฎหมายที่เกี่ยวข้อง

๑๐.๑ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะการประกวดราคา จะต้องดำเนินการปฏิบัติให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กฎหมาย ระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. ฉบับล่าสุด ซึ่งรวมถึงหลักการวิศวกรรมความมั่นคงปลอดภัย (แบบฟอร์มความต้องการด้านความมั่นคงปลอดภัยของระบบทางด้านเทคนิค (System Security Requirement) เอกสารเผยแพร่สามารถศึกษารายละเอียดหรือ Download ในเว็บไซต์สำนักงาน กสทช. (www.nbtc.go.th)

๑๐.๒ กรณีมีการใช้บริการคลาวด์ (Cloud) ต้องปฏิบัติตามข้อกำหนดด้านการใช้บริการคลาวด์ (Cloud Security Requirement) ตามที่ผู้ว่าจ้างกำหนด

๑๐.๓ ตรวจสอบความมั่นคงปลอดภัยของซอร์สโค้ด (Source Code Scanning) และดำเนินการแก้ไขก่อนนำระบบขึ้นให้บริการ

๑๐.๔ กรณีที่ขอบเขตของงานเกี่ยวข้องกับการประมวลผล (เก็บรวบรวม ใช้ เปิดเผย) ข้อมูลส่วนบุคคลผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะ หรือผู้ได้รับการคัดเลือก ต้องดำเนินการตามเงื่อนไขและรายละเอียดตามที่กำหนดไว้ในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA) กับสำนักงาน กสทช. ตามที่กำหนดใน **(ภาคผนวก ๔)** ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

๑๐.๕ ในการจัดเก็บข้อมูลการจราจรคอมพิวเตอร์เป็นไปอย่างถูกต้องตามกฎหมาย เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้รับจ้าง พ.ศ. ๒๕๖๔ รวมถึงกฎระเบียบ และข้อบังคับอื่นที่เกี่ยวข้อง ให้พิจารณาเลือกใช้ผลิตภัณฑ์ที่ผ่านมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

๑๑. เงื่อนไขอื่น ๆ

๑๑.๑ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะการประกวดราคา จะต้องเข้าทำสัญญาตามแบบที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ภายใน ๑๕ วันนับถัดจากวันที่ได้รับหนังสือแจ้งจากสำนักงาน กสทช. ทั้งนี้ สำนักงาน กสทช. สงวนสิทธิ์ในการเปลี่ยนแปลงแก้ไขสัญญาให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

๑๑.๒ ผู้รับจ้างต้องทำแผนการดำเนินงานทั้งงานระยะที่ ๑ และงานระยะที่ ๒ ซึ่งครอบคลุมการดำเนินงานและระยะเวลาดำเนินงานตามขอบเขตของงานแนบท้ายสัญญา ภายใน ๑๕ วันนับถัดจากวันลงนามในสัญญาเพื่อสำนักงาน กสทช. โดยคณะกรรมการตรวจรับพัสดุในฐานะผู้บริหารสัญญาจะกำกับติดตามผลการดำเนินงาน ทั้งนี้ แผนการดำเนินงานดังกล่าวถือเป็นส่วนหนึ่งของสัญญา ผู้รับจ้างต้องปฏิบัติงานให้เป็นไปตามแผนงานโดยเคร่งครัด

Proof

๑๑.๓ สำนักงาน กสทช. สงวนสิทธิ์ในการเปลี่ยนแปลง เพิ่ม ลด เนื้องานให้สอดคล้องกับข้อเท็จจริงในการดำเนินโครงการฯ โดยการเปลี่ยนแปลงดังกล่าวจะใช้ราคาต่อหน่วยในสัญญาที่ได้ลงนามไว้ เป็นฐานในการคำนวณเพื่อปรับเพิ่มหรือลดวงเงินในการดำเนินโครงการฯ ดังกล่าว

๑๑.๔ ในกรณีที่สำนักงาน กสทช. มีความจำเป็นไม่อาจทำสัญญางานจ้างได้ หรือมีเหตุจำเป็นอื่น ๆ ที่เป็นอุปสรรคต่อสำนักงาน กสทช. ขอสงวนสิทธิ์ที่จะยกเลิกการดำเนินการจัดจ้างครั้งนี้ได้ทุกขั้นตอน โดยผู้ยื่นข้อเสนอไม่อาจเรียกร้องให้สำนักงาน กสทช. ต้องรับผิดชอบชดใช้ หรือชำระค่าใช้จ่ายใด ๆ ให้แก่ผู้ยื่นข้อเสนอ

๑๑.๕ สำนักงาน กสทช. ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกข้อเสนอเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการคัดเลือกฯ โดยไม่พิจารณาข้อเสนอเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้ เพื่อประโยชน์ของทางราชการและสำนักงาน กสทช. เป็นสำคัญ และให้ถือว่าการตัดสินของสำนักงาน กสทช. เป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใด ๆ มิได้รวมทั้งสำนักงาน กสทช. จะพิจารณายกเลิกการคัดเลือกและลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อได้ว่าการเสนอราคากระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จหรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

๑๑.๖ รายได้ที่เกิดขึ้นจากการประกอบกิจการโทรคมนาคมตามขอบเขตการดำเนินงานนี้ ผู้รับจ้างมีหน้าที่ต้องนำส่งค่าธรรมเนียมใบอนุญาตประกอบกิจการโทรคมนาคม และจัดสรรรายได้ให้แก่กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมเพื่อประโยชน์สาธารณะ ตามกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม และตามกฎหมายว่าด้วยองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม และตามประกาศที่ กสทช. กำหนด

Proof

ภาคผนวก

ภาคผนวก ๑	รายละเอียดคุณลักษณะเฉพาะอุปกรณ์ฮาร์ดแวร์ (Hardware Specifications)	จำนวน ๑๗ หน้า
ภาคผนวก ๒	รายละเอียดคุณลักษณะเฉพาะซอฟต์แวร์ (Software Specifications)	จำนวน ๘ หน้า
ภาคผนวก ๓	รายละเอียดข้อกำหนดบริการพื้นที่ศูนย์ข้อมูลและระบบโครงข่ายเชื่อมต่อ	จำนวน ๒ หน้า
ภาคผนวก ๔	ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล	จำนวน ๕ หน้า

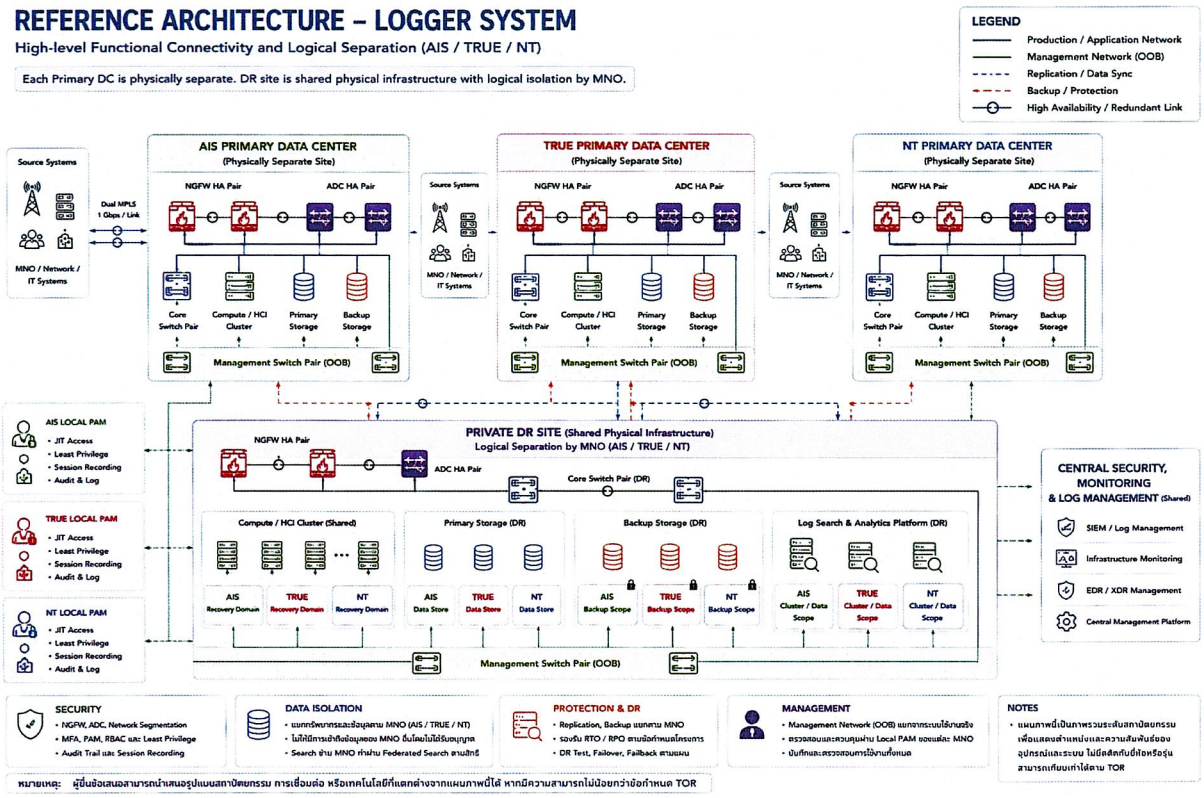
นายพีระเชฎฐ์ พงษ์ศิริ

นายชยวีร์ อังศุสิงห์ | นายปริญญา เทศบรรทัด

นายนพดล เทียมนรา | นายฉัตรบดี ฉัตรภูติ

นายศุภาวุฒิ ปาติมานนท์ | นางสาวสุวิชชา อ่อนศรี

Proof



ภาพประกอบ ตัวอย่างการเชื่อมต่อภาพรวมของระบบ (อุปกรณ์ฮาร์ดแวร์, ซอฟต์แวร์ และระบบโครงข่ายเชื่อมต่อ)

คุณสมบัติทั่วไป มีรายละเอียดอย่างน้อยดังนี้

๑. ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองอุปกรณ์หลักในโครงการ ได้แก่ ระบบจัดเก็บข้อมูลหลักประจำศูนย์ข้อมูลหลัก, ระบบจัดเก็บข้อมูลหลักประจำศูนย์ข้อมูลสำรอง อุปกรณ์รักษาความปลอดภัยเครือข่ายประจำศูนย์ข้อมูลหลัก อุปกรณ์รักษาความปลอดภัยเครือข่ายประจำศูนย์ข้อมูลสำรอง ระบบจัดเก็บ และวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ จากเจ้าของผลิตภัณฑ์ที่มีสาขาจดทะเบียนในประเทศไทยเพื่อยืนยันความพร้อมในการสนับสนุนด้านเทคนิคเพื่อประสิทธิภาพการให้บริการตลอดระยะเวลาโครงการ

๒. ผู้ยื่นข้อเสนอต้องจัดทำข้อเสนอทางเทคนิค (Technical Proposal) เพื่อแสดงรายละเอียดการออกแบบ สถาปัตยกรรม และการทำงานร่วมกันของระบบที่เสนอ โดยอย่างน้อยต้องประกอบด้วย System Architecture, Bill of Materials (BOM), Capacity Calculation หรือ Capacity Sizing, License List, License Summary, Backup Copy Architecture และ Replication Architecture เฉพาะส่วนที่เกี่ยวข้องตามขอบเขตของระบบที่เสนอ เพื่อแสดงให้เห็นถึงรุ่น จำนวน ขนาดระบบ

Proof

สิทธิการใช้งาน และความครบถ้วนของ Hardware, Software, License, Subscription และองค์ประกอบที่เกี่ยวข้อง ว่ามีความเพียงพอตามข้อกำหนดและผลการคำนวณของโครงการ และสามารถทำงานร่วมกันได้ตามสถาปัตยกรรมที่เสนอ ทั้งนี้ ข้อเสนอทางเทคนิคดังกล่าวต้องลงนามรับรองโดยผู้มีอำนาจลงนามผูกพันผู้ยื่นข้อเสนอ หรือผู้รับมอบอำนาจโดยชอบด้วยกฎหมาย โดยผู้ยื่นข้อเสนอต้องรับรองความถูกต้องและความครบถ้วนของข้อมูลและการออกแบบที่ตนจัดทำ

๓. ในกรณีที่รายละเอียดคุณลักษณะเฉพาะของระบบหรืออุปกรณ์ข้อใดกำหนดให้ต้องมีเอกสารทางเทคนิคอย่างเป็นทางการของเจ้าของผลิตภัณฑ์ หรือหนังสือรับรองจากเจ้าของผลิตภัณฑ์เป็นการเฉพาะ ให้ผู้ยื่นข้อเสนอยื่นเอกสารดังกล่าวเฉพาะระบบหรือหัวข้อที่กำหนด เพื่อยืนยันคุณลักษณะรุ่น สิทธิการใช้งาน การรองรับ หรือการสนับสนุนตามข้อกำหนดของระบบหรืออุปกรณ์นั้น

๔. คุณลักษณะของระบบและอุปกรณ์ที่กำหนดเป็นลักษณะการรองรับ ให้ถือเป็นว่ามีความสามารถในการทำงานตามข้อกำหนดทางเทคนิคทุกประการ โดยต้องครอบคลุมถึงความครบถ้วนของฟังก์ชันการทำงาน ความเพียงพอของสิทธิการใช้งาน (License/Data Source) ทุกประเภท ไม่น้อยกว่าจำนวนจริงรวมสำรอง ตลอดจนกลไกความต่อเนื่องของบริการและการสนับสนุนทางเทคนิคอย่างต่อเนื่องตลอดระยะเวลาไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

๕. ผู้รับจ้างต้องรับผิดชอบการบริการทั้งหมดให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยเป็นค่าใช้จ่ายในส่วนของผู้รับจ้างที่ต้องรับผิดชอบ

Proof

ภาคผนวก ๑
รายละเอียดคุณลักษณะเฉพาะอุปกรณ์ฮาร์ดแวร์
(Hardware Specifications)

ภาคผนวก ๑ รายละเอียดคุณลักษณะเฉพาะอุปกรณ์ฮาร์ดแวร์ (Hardware Specifications) มีรายการอย่างน้อยดังต่อไปนี้

๑. อุปกรณ์กระจายสัญญาณสำหรับใช้ในศูนย์ข้อมูล (Data Center Switch)
๒. อุปกรณ์กระจายสัญญาณสำหรับใช้ในศูนย์ข้อมูลสำรอง (Data Center Switch)
๓. อุปกรณ์กระจายสัญญาณสำหรับบริหารจัดการประจำศูนย์ข้อมูลหลัก (Management Switch - DC)
๔. อุปกรณ์กระจายสัญญาณสำหรับบริหารจัดการประจำศูนย์ข้อมูลสำรอง (Management Switch - DR)
๕. เครื่องคอมพิวเตอร์แม่ข่ายสำหรับศูนย์ข้อมูลหลัก (Server - DC)
๖. อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับศูนย์ข้อมูลสำรอง (DR)
๗. ระบบจัดเก็บข้อมูลหลักประจำศูนย์ข้อมูลหลัก (Primary Storage) จำนวน ๓ ระบบ
๘. ระบบจัดเก็บข้อมูลหลักประจำศูนย์ข้อมูลสำรอง (Primary Storage)
๙. ระบบจัดเก็บข้อมูลสำรองประจำศูนย์ข้อมูลหลัก (Backup Storage) จำนวน ๓ ระบบ
๑๐. ระบบจัดเก็บข้อมูลสำรองประจำศูนย์ข้อมูลสำรอง (Backup Storage) จำนวน ๑ ระบบ
๑๑. อุปกรณ์รักษาความปลอดภัยเครือข่าย ประจำศูนย์ข้อมูลหลัก (Next-Generation Firewall)
๑๒. อุปกรณ์รักษาความปลอดภัยเครือข่าย ประจำศูนย์ข้อมูลสำรอง (Next-Generation Firewall)
๑๓. ระบบบริหารจัดการและวิเคราะห์ข้อมูลความมั่นคงปลอดภัย (Log Management and SIEM)
๑๔. อุปกรณ์กระจายภาระการใช้งานสำหรับศูนย์ข้อมูลหลัก (Application Delivery Controller / Load Balancer - ADC DC) จำนวน ๖ เครื่อง
๑๕. อุปกรณ์กระจายภาระการใช้งานสำหรับศูนย์ข้อมูลสำรอง (Application Delivery Controller / Load Balancer - ADC DR) จำนวน ๒ เครื่อง

Proof

ส่วนที่ ๑ ระบบเครือข่ายศูนย์ข้อมูล (Data Center Network Layer)

๑. อุปกรณ์กระจายสัญญาณสำหรับใช้ในศูนย์ข้อมูล (Data Center Switch) มีคุณลักษณะอย่างน้อย ดังนี้

๑.๑ จัดหาอุปกรณ์จำนวน ๒ เครื่องต่อศูนย์ข้อมูล สำหรับศูนย์ข้อมูล AIS, TRUE และ NT รวมจำนวน 6 เครื่อง

๑.๒ มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model เป็นอุปกรณ์ที่ออกแบบสำหรับใช้งานในศูนย์ข้อมูล สามารถติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว และมีความสูงไม่เกิน 1U หรือ 1RU

๑.๓ มีช่องเชื่อมต่อระบบเครือข่ายแบบ 25 Gigabit Ethernet หรือเครือข่ายแบบ 25 Gigabit Ethernet ชนิด SFP28 ดีกว่า จำนวนไม่น้อยกว่า ๒๔ ช่อง และมีช่องเชื่อมต่อระบบเครือข่ายแบบ 40/100 Gbps. ชนิด QSFP28 หรือดีกว่า จำนวนไม่น้อยกว่า ๔ ช่อง โดยช่องเชื่อมต่อดังกล่าวต้องสามารถใช้งานพร้อมกันได้ตาม Port Mapping

๑.๔ มี Switching Capacity ไม่น้อยกว่า 2 Tbsp. และรองรับ MAC Address ได้ไม่น้อยกว่า 32,000 MAC Address

๑.๕ มี Power Supply จำนวนไม่น้อยกว่า ๒ ชุด และมีระบบระบายความร้อนที่รองรับการทำงานแบบ Redundant หรือ Hot Back Up หรือ Hot-Swap หรือให้ผลด้านความต่อเนื่องเทียบเท่า รวมทั้งมีสัญญาณหรือระบบแสดงสถานะการทำงานของช่องเชื่อมต่อและอุปกรณ์

๑.๖ รองรับ VLAN, Link Aggregation, RSTP หรือ MSTP และรองรับการเชื่อมโยงอุปกรณ์ตั้งแต่ ๒ เครื่องขึ้นไป โดยใช้ M-LAG หรือ MC-LAG หรือ MCLAG หรือ DRNI หรือเทคโนโลยีที่ให้ผลด้านความต่อเนื่องและการกระจายการเชื่อมต่อเทียบเท่า

๑.๗ สามารถค้นหาเส้นทางเครือข่ายสำหรับ IPv4 และ IPv6 โดยรองรับ Static Routing, OSPF หรือ OSPFv3 และ BGP ได้เป็นอย่างน้อย โดยต้องรวม Software License หรือ Subscription ที่จำเป็นสำหรับคุณสมบัติที่กำหนดไว้ในข้อเสนอ

๑.๘ สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser หรือ HTTPS หรือ CLI และ SSH รองรับ SNMPv3 และสามารถส่งข้อมูล Log File ในรูปแบบ Syslog ไปยังระบบบริหารจัดการ Log หรือระบบ SIEM ของโครงการได้

๑.๙ ผู้ยื่นข้อเสนอต้องจัดหา Transceiver Module, DAC Cable, AOC Cable, Patch Cord, License และอุปกรณ์ประกอบให้ครบถ้วนตาม Port Mapping และ Connection Diagram โดยอุปกรณ์ประกอบต้องได้รับการรับรองหรือระบุว่ารองรับโดยผู้ผลิตอุปกรณ์

๑.๑๐ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ

Proof

๒. อุปกรณ์กระจายสัญญาณสำหรับใช้ในศูนย์ข้อมูลสำรอง (Data Center Switch) มีคุณลักษณะอย่างน้อย ดังนี้

๒.๑ จัดหาอุปกรณ์จำนวนไม่น้อยกว่า ๒ เครื่อง สำหรับติดตั้ง ณ ศูนย์ข้อมูลสำรอง เพื่อรองรับการเชื่อมต่อเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูล ระบบสำรองข้อมูล อุปกรณ์รักษาความมั่นคงปลอดภัย และระบบอื่นที่เกี่ยวข้องกับการกู้คืนและให้บริการระบบเมื่อศูนย์ข้อมูลหลักไม่สามารถให้บริการได้

๒.๒ มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model เป็นอุปกรณ์ที่ออกแบบสำหรับใช้งานในศูนย์ข้อมูล สามารถติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว และมีความสูงไม่เกิน 1U หรือ 1RU

๒.๓ มีช่องเชื่อมต่อระบบเครือข่ายแบบ 10/25 Gbps. ชนิด SFP28 หรือดีกว่า จำนวนไม่น้อยกว่า ๒๔ ช่อง และมีช่องเชื่อมต่อระบบเครือข่ายแบบ 40/100 Gbps. ชนิด QSFP28 หรือดีกว่า จำนวนไม่น้อยกว่า ๔ ช่อง โดยช่องเชื่อมต่อดังกล่าวต้องสามารถใช้งานพร้อมกันได้ตาม Port Mapping

๒.๔ มี Switching Capacity ไม่น้อยกว่า 2 Tbsp. และรองรับ MAC Address ได้ไม่น้อยกว่า 32,000 MAC Address

๒.๕ มี Power Supply จำนวนไม่น้อยกว่า ๒ ชุด และมีระบบระบายความร้อนที่รองรับการทำงานแบบ Redundant หรือ Hot Back Up และ Hot-Swap หรือให้ผลด้านความต่อเนื่องเทียบเท่า รวมทั้งมีสัญญาณหรือระบบแสดงสถานะการทำงานของช่องเชื่อมต่อและอุปกรณ์

๒.๖ รองรับ VLAN, Link Aggregation, RSTP หรือ MSTP และรองรับการเชื่อมโยงอุปกรณ์ตั้งแต่ ๒ เครื่องขึ้นไป โดยใช้ M-LAG หรือ MC-LAG หรือ MCLAG หรือ DRNI หรือเทคโนโลยีที่ให้ผลด้านความต่อเนื่องและการกระจายการเชื่อมต่อเทียบเท่า

๒.๗ สามารถค้นหาเส้นทางเครือข่ายสำหรับ IPv4 และ IPv6 โดยรองรับ Static Routing, OSPF หรือ OSPFv3 และ BGP ได้เป็นอย่างน้อย โดยต้องรวม Software License หรือ Subscription ที่จำเป็นสำหรับคุณสมบัติที่กำหนดไว้ในข้อเสนอ

๒.๘ สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser หรือ HTTPS หรือ CLI และ SSH รองรับ SNMPv3 และสามารถส่งข้อมูล Log File ในรูปแบบ Syslog ไปยังระบบบริหารจัดการ Log หรือระบบ SIEM ของโครงการได้

๒.๙ ผู้ยื่นข้อเสนอต้องจัดหา Transceiver Module, DAC Cable, AOC Cable, Patch Cord, License และอุปกรณ์ประกอบให้ครบถ้วน โดยอุปกรณ์ประกอบต้องได้รับการรับรองหรือระบุว่ารองรับโดยผู้ผลิตอุปกรณ์

๒.๑๐ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ต้องไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ

Proof

๓. อุปกรณ์กระจายสัญญาณสำหรับบริหารจัดการประจำศูนย์ข้อมูลหลัก (Management Switch - DC) มีคุณลักษณะอย่างน้อย ดังนี้

๓.๑ จัดหาอุปกรณ์จำนวน ๒ เครื่องต่อศูนย์ข้อมูล สำหรับศูนย์ข้อมูล AIS, TRUE และ NT รวมจำนวน ๖ เครื่อง เพื่อเชื่อมต่อช่องทางบริหารจัดการของเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูล อุปกรณ์เครือข่าย อุปกรณ์รักษาความมั่นคงปลอดภัย และระบบอื่นที่เกี่ยวข้องกับโครงการ

๓.๒ มีลักษณะการทำงานไม่น้อยกว่า Layer 2 ของ OSI Model เป็นอุปกรณ์ Ethernet Switch ระดับองค์กร สามารถติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว และมีความสูงไม่เกิน 1U หรือ 1RU

๓.๓ มีช่องเชื่อมต่อระบบเครือข่ายแบบ 10/100/1000BASE-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒๔ ช่อง และมีช่องเชื่อมต่อแบบ SFP+ หรือดีกว่า ซึ่งรองรับความเร็ว 10 Gbps. จำนวนไม่น้อยกว่า ๔ ช่อง โดยช่องเชื่อมต่อดังกล่าวต้องสามารถใช้งานพร้อมกันได้ตาม Port Mapping

๓.๔ มี Switching Capacity ไม่น้อยกว่า 128 Gbps. รองรับ MAC Address ได้ไม่น้อยกว่า 16,000 MAC Address และมีสัญญาณหรือระบบแสดงสถานะการทำงานของช่องเชื่อมต่อและอุปกรณ์

๓.๕ รองรับ VLAN, Link Aggregation หรือ LACP และ RSTP หรือ MSTP รวมทั้งรองรับการใช้อุปกรณ์ตั้งแต่ ๒ เครื่องขึ้นไปเพื่อเพิ่มความพร้อมใช้งานและมีเส้นทางสำรอง โดยใช้ Stacking หรือ iStack หรือ IRF หรือ Virtual Chassis หรือ Multi-Chassis Link Aggregation หรือ Link Aggregation ร่วมกับ RSTP หรือ MSTP หรือเทคโนโลยีที่ให้ผลด้านความต่อเนื่องเทียบเท่า

๓.๖ สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser หรือ HTTPS และ SSH รองรับ SNMPv3 สามารถส่งข้อมูล Log File ในรูปแบบ Syslog และรองรับการปรับเทียบเวลาผ่าน NTP หรือ SNTP โดยมี Console Port หรือ Dedicated Management Port หรือช่องทางบริหารจัดการอุปกรณ์สำหรับการติดตั้ง กำหนดค่า และแก้ไขปัญหา

๓.๗ ผู้ยื่นข้อเสนอต้องจัดหา Transceiver Module, DAC Cable, AOC Cable, Patch Cord, Stack Cable, License และอุปกรณ์ประกอบให้ครบถ้วน

๓.๘ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ต้องไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ

๔. อุปกรณ์กระจายสัญญาณสำหรับบริหารจัดการประจำศูนย์ข้อมูลสำรอง (Management Switch - DR) มีคุณลักษณะอย่างน้อย ดังนี้

๔.๑ จัดหาอุปกรณ์จำนวน ๒ เครื่อง สำหรับติดตั้ง ณ ศูนย์ข้อมูลสำรอง เพื่อเชื่อมต่อช่องทางบริหารจัดการของเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูล ระบบสำรองข้อมูล อุปกรณ์เครือข่าย อุปกรณ์รักษาความมั่นคงปลอดภัย อุปกรณ์กระจายภาระการใช้งาน และระบบอื่นที่เกี่ยวข้องกับศูนย์ข้อมูลสำรอง

๔.๒ มีลักษณะการทำงานไม่น้อยกว่า Layer 2 ของ OSI Model เป็นอุปกรณ์ Ethernet Switch ระดับองค์กร สามารถติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว และมีความสูงไม่เกิน 1U หรือ 1RU

๔.๓ มีช่องเชื่อมต่อระบบเครือข่ายแบบ 10/100/1000BASE-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒๔ ช่อง และมีช่องเชื่อมต่อแบบ SFP+ หรือดีกว่า ซึ่งรองรับความเร็ว 10 Gbps. จำนวนไม่น้อยกว่า ๔ ช่อง โดยช่องเชื่อมต่อดังกล่าวต้องสามารถใช้งานพร้อมกันได้ตาม Port Mapping

๔.๔ มี Switching Capacity ไม่น้อยกว่า 128 Gbps. รองรับ MAC Address ได้ไม่น้อยกว่า 16,000 MAC Address และมีสัญญาณหรือระบบแสดงสถานะการทำงานของช่องเชื่อมต่อและอุปกรณ์

Proof

๔.๕ รองรับ VLAN, Link Aggregation หรือ LACP และ RSTP หรือ MSTP รวมทั้งรองรับการใช้อุปกรณ์ตั้งแต่ ๒ เครื่องขึ้นไปเพื่อเพิ่มความพร้อมใช้งานและมีเส้นทางสำรอง โดยใช้ Stacking หรือ iStack หรือ IRF หรือ Virtual Chassis หรือ Multi-Chassis Link Aggregation หรือ Link Aggregation ร่วมกับ RSTP หรือ MSTP หรือเทคโนโลยีที่ให้ผลด้านความต่อเนื่องเทียบเท่า

๔.๖ สามารถบริหารจัดการอุปกรณ์ผ่าน Web Browser หรือ HTTPS และ SSH รองรับ SNMPv3 สามารถส่งข้อมูล Log File ในรูปแบบ Syslog และรองรับการปรับเทียบเวลาผ่าน NTP หรือ SNTP โดยมี Console Port หรือ Dedicated Management Port หรือช่องทางบริหารจัดการอุปกรณ์สำหรับการติดตั้ง กำหนดค่า และแก้ไขปัญหา

๔.๗ ผู้ยื่นข้อเสนอต้องจัดหา Transceiver Module, DAC Cable, AOC Cable, Patch Cord, Stack Cable, License และอุปกรณ์ประกอบให้ครบถ้วน

๔.๘ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ต้องไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ

ส่วนที่ ๒ ระบบประมวลผลและการจัดเก็บข้อมูล (Compute & Storage Layer)

๕. เครื่องคอมพิวเตอร์แม่ข่ายสำหรับศูนย์ข้อมูลหลัก (Server - DC) โดยมีคุณลักษณะของแต่ละชุดอย่างน้อยดังนี้

๕.๑ จัดหาเครื่องคอมพิวเตอร์แม่ข่ายจำนวน ๒ เครื่องต่อศูนย์ข้อมูล สำหรับศูนย์ข้อมูล AIS, TRUE และ NT รวมจำนวน ๖ เครื่อง โดยระบบของแต่ละศูนย์ข้อมูลต้องสามารถทำงานเป็นอิสระจากศูนย์ข้อมูลชุดอื่นตามสถาปัตยกรรมที่เสนอ

๕.๒ เป็นเครื่องคอมพิวเตอร์แม่ข่ายแบบติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว มีความสูงไม่เกิน 2U พร้อมสายไฟ และอุปกรณ์ที่จำเป็นสำหรับติดตั้งใช้งานครบถ้วน

๕.๓ มีหน่วยประมวลผลกลางที่ออกแบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายโดยเฉพาะ รองรับการประมวลผลแบบ 64 Bit จำนวนไม่น้อยกว่า ๒ หน่วยต่อเครื่อง และมีจำนวนแกนประมวลผลจริงรวมไม่น้อยกว่า 48 Cores ต่อเครื่อง พร้อมหน่วยความจำหลักชนิด ECC DDR4 หรือดีกว่า ขนาดติดตั้งไม่น้อยกว่า 256 GB. ต่อเครื่อง

๕.๔ สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1 และ 5 และมีหน่วยจัดเก็บข้อมูลชนิด Enterprise SSD, NVMe SSD หรือเทคโนโลยีที่ดีกว่า ขนาดความจุไม่น้อยกว่า 900 GB. จำนวนไม่น้อยกว่า 4 หน่วยต่อเครื่อง ทั้งนี้ หากผลการคำนวณขนาดระบบตามข้อ ๕.๗ ต้องใช้จำนวนหรือความจุสูงกว่าที่กำหนด ผู้ยื่นข้อเสนอต้องจัดหาให้เพียงพอโดยรวมอยู่ในราคาเสนอ

๕.๕ มีช่องเชื่อมต่อระบบเครือข่ายแบบ 10/25 Gigabit Ethernet ชนิด SFP28 หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่องต่อเครื่อง พร้อม Transceiver Module, DAC Cable, AOC Cable หรือสายสัญญาณที่จำเป็นครบถ้วนตาม Network Port Mapping และ Connection Diagram ที่เสนอ

๕.๖ มีช่องเชื่อมต่อสำหรับบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายจากระยะไกลโดยเฉพาะ จำนวนไม่น้อยกว่า ๑ ช่อง และมี Power Supply แบบ Redundant หรือ Hot-Swap จำนวนไม่น้อยกว่า ๒ หน่วยต่อเครื่อง

Proof

๕.๗ เครื่องคอมพิวเตอร์แม่ข่ายต้องรองรับระบบปฏิบัติการและระบบ Virtualization ที่เสนอในผนวก ๒ โดยผู้ยื่นข้อเสนอต้องจัดทำ Consolidated Capacity Sizing แยกสำหรับศูนย์ข้อมูล AIS, TRUE และ NT ซึ่งรวมความต้องการของระบบปฏิบัติการ ระบบ Virtualization และ Software กับเอกสาร Sizing ของเจ้าของผลิตภัณฑ์ หลังรวม System Overhead และทรัพยากรที่ใช้สำหรับการป้องกันข้อมูลหรือการทำงานทดแทนแล้ว ต้องมีทรัพยากร CPU, Memory และ Storage สำรองสำหรับการใช้งานไม่น้อยกว่าร้อยละ ๓๐ หากผลการคำนวณสูงกว่าคุณลักษณะขั้นต่ำในข้อ ๕.๓ ถึงข้อ ๕.๕ ผู้ยื่นข้อเสนอต้องจัดหา Configuration ตามผลการคำนวณที่สูงกว่าโดยรวมอยู่ในราคาเสนอ

๕.๘ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ต้องไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ โดยการรับประกันและ Technical Support ต้องครอบคลุมระยะเวลาไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

๖. อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับศูนย์ข้อมูลสำรอง (DR) โดยมีคุณลักษณะของแต่ละชุดอย่างน้อยดังนี้

๖.๑ จัดหาเครื่องคอมพิวเตอร์แม่ข่ายสำหรับศูนย์ข้อมูลสำรอง จำนวนรวม ๔ เครื่อง โดยต้องสามารถรองรับระบบงานและข้อมูลจากศูนย์ข้อมูล AIS, TRUE และ NT ตามขอบเขตและสถาปัตยกรรมที่เสนอ

๖.๒ เป็นเครื่องคอมพิวเตอร์แม่ข่ายแบบติดตั้งในตู้ Rack มาตรฐาน ๑๙ นิ้ว มีความสูงไม่เกิน 2U พร้อมสายไฟ และอุปกรณ์ที่จำเป็นสำหรับติดตั้งใช้งานครบถ้วน

๖.๓ มีหน่วยประมวลผลกลางที่ออกแบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายโดยเฉพาะ รองรับการประมวลผลแบบ 64 Bit จำนวนไม่น้อยกว่า ๒ หน่วยต่อเครื่อง และมีจำนวนแกนประมวลผลจริงรวมไม่น้อยกว่า 48 Cores ต่อเครื่อง พร้อมหน่วยความจำหลักชนิด ECC DDR4 หรือดีกว่า ขนาดติดตั้งไม่น้อยกว่า 256 GB. ต่อเครื่อง

๖.๔ สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1 และ 5 และมีหน่วยจัดเก็บข้อมูลชนิด Enterprise SSD, NVMe SSD หรือเทคโนโลยีที่ดีกว่า ขนาดความจุไม่น้อยกว่า 900 GB. จำนวนไม่น้อยกว่า ๔ หน่วยต่อเครื่อง ทั้งนี้ หากผลการคำนวณขนาดระบบตามข้อ ๖.๗ ต้องใช้จำนวนหรือความจุสูงกว่าที่กำหนด ผู้ยื่นข้อเสนอต้องจัดหาให้เพียงพอต่อการใช้งานอย่างมีประสิทธิภาพ

๖.๕ มีช่องเชื่อมต่อระบบเครือข่ายแบบ 10/25 Gigabit Ethernet ชนิด SFP28 หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่องต่อเครื่อง พร้อม Transceiver Module, DAC Cable, AOC Cable หรือสายสัญญาณที่จำเป็นครบถ้วน

๖.๖ มีช่องเชื่อมต่อสำหรับบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายจากระยะไกลโดยเฉพาะ จำนวนไม่น้อยกว่า ๑ ช่อง และมี Power Supply แบบ Redundant หรือ Hot-Swap จำนวนไม่น้อยกว่า ๒ หน่วยต่อเครื่อง

Proof

๖.๗ เครื่องคอมพิวเตอร์แม่ข่ายต้องรองรับระบบปฏิบัติการและระบบ Virtualization ผู้ยื่นข้อเสนอต้องจัดทำ Consolidated Capacity Sizing สำหรับศูนย์ข้อมูลสำรอง ซึ่งรวมความต้องการของระบบปฏิบัติการ ระบบ Virtualization และ Software รวมทั้งระบบงานและข้อมูลที่ต้องรองรับจากศูนย์ข้อมูล AIS, TRUE และ NT โดยใช้ค่าความต้องการที่สูงกว่าระหว่างข้อกำหนดในผนวก ข กับเอกสาร Sizing ของเจ้าของผลิตภัณฑ์ หลังรวม System Overhead และทรัพยากรที่ใช้สำหรับการป้องกันข้อมูลหรือการทำงานทดแทนแล้ว ต้องมีทรัพยากร CPU, Memory และ Storage สำรองสำหรับการใช้งานไม่น้อยกว่าร้อยละ ๓๐ หากผลการคำนวณสูงกว่าคุณลักษณะขั้นต่ำในข้อ ๖.๓ ถึงข้อ ๖.๕ ผู้ยื่นข้อเสนอต้องจัดหา Configuration ตามผลการคำนวณที่สูงกว่าโดยรวมอยู่ในราคาเสนอ

๖.๘ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์อุปกรณ์ต้องไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ โดยการรับประกันและ Technical Support ต้องครอบคลุมระยะเวลาไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

๗. ระบบจัดเก็บข้อมูลหลักประจำศูนย์ข้อมูลหลัก (Primary Storage) จำนวน ๓ ระบบ โดยระบบจัดเก็บข้อมูลแต่ละระบบต้องมีคุณลักษณะอย่างน้อยดังนี้

๗.๑ จัดหาระบบจัดเก็บข้อมูลจำนวน ๑ ระบบต่อศูนย์ข้อมูล สำหรับศูนย์ข้อมูล AIS, TRUE และ NT รวมจำนวน ๓ ระบบ โดยระบบของแต่ละศูนย์ข้อมูลต้องสามารถทำงานเป็นอิสระจากศูนย์ข้อมูลชุดอื่นตามสถาปัตยกรรมที่เสนอ

๗.๒ เป็นอุปกรณ์จัดเก็บข้อมูลแบบภายนอก (External Storage) ที่สามารถทำงานในระบบ SAN (Storage Area Network) หรือ NAS (Network-Attached Storage) ได้ และมี Controller, Storage Node หรือ Node Canister จำนวนไม่น้อยกว่า ๒ หน่วยต่อระบบ โดยเมื่อหน่วยหนึ่งขัดข้องระบบต้องสามารถให้บริการข้อมูลผ่านหน่วยที่เหลือได้ตามสถาปัตยกรรมที่เสนอ

๗.๓ มีสื่อจัดเก็บข้อมูลชนิด Enterprise SSD, NVMe SSD, SAS, NL-SAS หรือเทคโนโลยีที่ดีกว่าอย่างใดอย่างหนึ่งหรือหลายชนิดร่วมกัน และมีพื้นที่ใช้งานสุทธิไม่น้อยกว่า 340 TB. โดยมีสัดส่วนของ SSD ไม่น้อยกว่า 40 TB. ต่อระบบ ภายหลังหักพื้นที่สำหรับ RAID หรือ Data Protection, Spare หรือ Rebuild Area, Metadata และ System Reserve ตาม Configuration ที่เสนอแล้ว โดยไม่รวมผลจาก Compression, Deduplication, Thin Provisioning, Data Reduction Ratio, Logical Capacity หรือ Effective Capacity (1 TB. เท่ากับ 10^{12} Bytes)

๗.๔ รองรับการป้องกันข้อมูลด้วย RAID 6 หรือ RAID-TP หรือ Distributed RAID แบบ Dual-Parity หรือเทคโนโลยีที่สามารถทนต่อการชำรุดพร้อมกันของสื่อจัดเก็บข้อมูลไม่น้อยกว่า ๒ หน่วยภายในกลุ่มการป้องกันข้อมูลเดียวกัน โดยข้อมูลยังสามารถเข้าถึงได้

๗.๕ มีช่องเชื่อมต่อระบบเครือข่ายแบบ Ethernet ที่รองรับความเร็วไม่น้อยกว่า 25 Gigabit Ethernet จำนวนรวมไม่น้อยกว่า ๔ ช่องต่อระบบ โดยกระจายการเชื่อมต่อผ่าน Controller หรือ Node มากกว่าหนึ่งหน่วย และรองรับการให้บริการ Block Storage ผ่าน iSCSI หรือ NVMe over TCP (NVMe/TCP) อย่างน้อยหนึ่งรูปแบบ พร้อม Transceiver Module, DAC Cable, AOC Cable หรือสายสัญญาณที่จำเป็นครบถ้วนตาม Network Port Mapping และ Connection Diagram ที่เสนอ

Proof

๗.๖ รองรับการจัดเก็บข้อมูลสำหรับระบบงานที่ใช้ S3 หรือ Object หรือ Block Storage โดยอุปกรณ์ที่เสนอโดยตรง หรือผ่าน Software หรือองค์ประกอบที่ทำงานร่วมกับอุปกรณ์ตามสถาปัตยกรรมที่เสนอ โดยผู้ยื่นข้อเสนอต้องจัดหา Software, License และองค์ประกอบที่จำเป็นให้ครบถ้วนและแสดงไว้ใน Bill of Materials (BOM)

๗.๗ รองรับ Thin Provisioning หรือ Dynamic Provisioning, Snapshot หรือ Point-in-Time Copy และ Remote Replication หรือ Asynchronous Replication พร้อมสามารถบริหารจัดการและตรวจสอบสถานะของระบบผ่าน Graphical User Interface (GUI) หรือ Web-Based Management ได้ โดยต้องจัดหา License หรือ Subscription ที่จำเป็นสำหรับ Configuration ที่เสนอให้ครบถ้วน

๗.๘ ผู้ยื่นข้อเสนอต้องจัดทำ Capacity Sizing แยกสำหรับศูนย์ข้อมูล AIS, TRUE และ NT โดยใช้ปริมาณข้อมูลเข้าไม่น้อยกว่า 350 GB. ต่อวันต่อศูนย์ข้อมูล และระยะเวลาจัดเก็บไม่น้อยกว่า ๒ ปี นับแต่วันที่ข้อมูลเข้าสู่ระบบ

๗.๙ มี Power Supply แบบ Redundant หรือ Hot-Swap จำนวนไม่น้อยกว่า ๒ หน่วยต่อระบบ

๗.๑๐ มีส่วนควบคุม (Controller) จำนวนอย่างน้อย 2 Controller ทำงานแบบ Active-Active และไม่หยุดทำงานเมื่อมี Controller ใดเสียหาย โดยในแต่ละส่วนควบคุมมีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๔๘ แกนหลัก (48 core)

๗.๑๑ มีหน่วยความจำ Cache ที่อยู่ใน Controller ขนาดรวมกันไม่น้อยกว่า 512 GB. ต่อชุด

๗.๑๒ ระบบที่เสนอจะต้องรองรับ Real-time Ransomware Detection สำหรับข้อมูลที่ให้บริการทั้งในรูปแบบ SAN หรือ NAS โดยสามารถตรวจจับพฤติกรรมหรือกิจกรรมที่ผิดปกติซึ่งอาจเกิดจากการโจมตีของ Ransomware ได้แบบ Real-time ทั้งนี้ ความสามารถดังกล่าวสามารถเป็นความสามารถที่ติดตั้งมาพร้อมกับระบบ (Built-in) หรือสามารถใช้ ระบบหรือซอฟต์แวร์ภายนอก (External Solution) เพื่อให้เป็นไปตามข้อกำหนดดังกล่าวได้

๗.๑๓ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ต้องไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ โดยการรับประกัน Software/Firmware Update อะไหล่ และ Technical Support ต้องครอบคลุมระยะเวลาไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

๘. ระบบจัดเก็บข้อมูลหลักประจำศูนย์ข้อมูลสำรอง (Primary Storage) มีคุณลักษณะอย่างน้อยดังนี้

๘.๑ จัดหาระบบจัดเก็บข้อมูลหลักประจำศูนย์ข้อมูลสำรอง จำนวน ๑ ระบบ สำหรับรับและจัดเก็บข้อมูลจากระบบของศูนย์ข้อมูล AIS, TRUE และ NT ตามสถาปัตยกรรมการทำ Replication ที่เสนอ และรองรับการกู้คืนหรือให้บริการเมื่อระบบของศูนย์ข้อมูลหลักชุดใดชุดหนึ่งไม่สามารถให้บริการได้

๘.๒ เป็นอุปกรณ์จัดเก็บข้อมูลแบบภายนอก (External Storage) ที่สามารถทำงานในระบบ SAN หรือ NAS ได้ มีส่วนควบคุมอุปกรณ์แบบ Controller หรือ Node จำนวนไม่น้อยกว่า ๒ ชุด และระบบต้องสามารถให้บริการต่อเนื่องได้เมื่อ Controller หรือ Node ชุดใดชุดหนึ่งขัดข้อง

Proof

๘.๓ มีหน่วยจัดเก็บข้อมูลชนิด SSD, NVMe SSD, SAS, NL-SAS หรือเทคโนโลยีที่ดีกว่า โดยมีพื้นที่ใช้งานสุทธิ (Usable Capacity) ไม่น้อยกว่า 1,020 TB. โดยมีสัดส่วนของ SSD ไม่น้อยกว่า 120 TB. ภายหลังหักพื้นที่สำหรับการป้องกันข้อมูล พื้นที่สำรองสำหรับการกู้คืนข้อมูล พื้นที่ Metadata และพื้นที่สงวนตามสถาปัตยกรรมที่เสนอแล้ว โดยต้องไม่อาศัยความจุที่เกิดจากการบีบอัดข้อมูล การลดข้อมูลซ้ำ หรือเทคโนโลยี Data Reduction ของระบบจัดเก็บข้อมูล

๘.๔ รองรับการป้องกันข้อมูลแบบ RAID 6 หรือ RAID-TPหรือ Distributed RAID 6 หรือ Dynamic Drive Protection (DDP) แบบ Dual Parity หรือเทคโนโลยีที่ให้ผลเทียบเท่า โดยต้องสามารถรองรับความเสียหายของหน่วยจัดเก็บข้อมูลพร้อมกันได้ไม่น้อยกว่า ๒ หน่วยโดยข้อมูลไม่สูญหาย

๘.๕ มีช่องเชื่อมต่อระบบเครือข่ายที่รองรับและสามารถใช้งานที่ความเร็ว 25 Gigabit Ethernet จำนวนรวมไม่น้อยกว่า ๔ ช่อง กระจายอยู่บน Controller หรือ Node ไม่น้อยกว่า ๒ ชุด รองรับการให้บริการแบบ Block Storage ผ่าน iSCSI หรือ NVMe over TCP พร้อม Transceiver Module, DAC Cable, AOC Cable หรือสายสัญญาณที่จำเป็นครบถ้วนตามที่เสนอ

๘.๖ รองรับการจัดเก็บข้อมูลสำหรับระบบงานที่ใช้ S3 หรือ Object หรือ Block Storage โดยอุปกรณ์ที่เสนอโดยตรง หรือผ่าน Software หรือองค์ประกอบที่ทำงานร่วมกับอุปกรณ์ตามสถาปัตยกรรมที่เสนอ โดยผู้ยื่นข้อเสนอต้องจัดหา Software, License และองค์ประกอบที่จำเป็นให้ครบถ้วนและแสดงไว้ใน Bill of Materials (BOM)

๘.๗ ผู้ยื่นข้อเสนอต้องจัดทำ Consolidated Capacity Sizing สำหรับศูนย์ข้อมูลสำรอง โดยคำนวณจากปริมาณข้อมูลเข้าสู่ระบบรวมไม่น้อยกว่า 1,050 GB. ต่อวัน และระยะเวลาจัดเก็บข้อมูลไม่น้อยกว่า ๒ ปี หรือไม่น้อยกว่า ๗๓๐ วันนับแต่วันที่ข้อมูลเข้าสู่ระบบ

๘.๘ มี Power Supply แบบ Redundant หรือ Hot-Swap จำนวนไม่น้อยกว่า ๒ ชุด

๘.๙ มีส่วนควบคุม (Controller) จำนวนอย่างน้อย 2 Controller ทำงานแบบ Active-Active และไม่หยุดทำงานเมื่อมี Controller ใดเสียหาย โดยในแต่ละส่วนควบคุมมีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๔๘ แกนหลัก (48 core)

๘.๑๐ มีหน่วยความจำ Cache ที่อยู่ใน Controller ขนาดรวมกันไม่น้อยกว่า 512 GB. ต่อชุด

๘.๑๑ ระบบที่เสนอจะต้องรองรับ Real-time Ransomware Detection สำหรับข้อมูลที่ให้บริการทั้งในรูปแบบ SAN หรือ NAS โดยสามารถตรวจจับพฤติกรรมหรือกิจกรรมที่ผิดปกติซึ่งอาจเกิดจากการโจมตีของ Ransomware ได้แบบ Real-time ทั้งนี้ ความสามารถดังกล่าวสามารถเป็นความสามารถที่ติดตั้งมาพร้อมกับระบบ (Built-in) หรือสามารถใช้ ระบบหรือซอฟต์แวร์ภายนอก (External Solution) เพื่อให้เป็นไปตามข้อกำหนดดังกล่าวได้

๘.๑๒ อุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อน และอุปกรณ์ต้องไม่อยู่ในสถานะ End of Sale, End of Life หรือ End of Support ณ วันยื่นข้อเสนอ โดยการรับประกันและ Technical Support ต้องครอบคลุมระยะเวลาไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

Proof

๙. ระบบจัดเก็บข้อมูลสำรองประจำศูนย์ข้อมูลหลัก (Backup Storage) จำนวน ๓ ระบบ โดยมีคุณลักษณะของแต่ละระบบอย่างน้อยดังนี้

๙.๑ ผู้ยื่นข้อเสนอต้องจัดหาระบบจัดเก็บข้อมูลสำรองประจำศูนย์ข้อมูลหลัก จำนวน ๓ ระบบ สำหรับติดตั้ง ณ ศูนย์ข้อมูล AIS, TRUE และ NT ชุดละ ๑ ระบบ โดยเป็น Backup Storage Appliance หรือ Enterprise Storage หรือ Backup Software ร่วมกับ Storage Repository และสามารถทำงานร่วมกับ Backup Software หรือ Media Agent หรือ Backup Server ที่เสนอในโครงการได้

๙.๒ ระบบต้องมี Controller หรือ Storage Node ไม่น้อยกว่า ๒ หน่วยต่อระบบ หรือมีสถาปัตยกรรมแบบกระจายที่ให้ผลด้านความพร้อมใช้งานเทียบเท่า และรองรับการทำงานแบบ High Availability หรือ Active-Active หรือเทคโนโลยีที่ให้ผลเทียบเท่า โดยเมื่อส่วนประกอบหนึ่งหน่วยขัดข้องระบบต้องยังสามารถให้บริการข้อมูลได้

๙.๓ ระบบต้องมีพื้นที่สำหรับ Backup Data ที่ใช้งานได้จริงหลังการกำหนดค่าป้องกันข้อมูล และหักพื้นที่สงวนของระบบไม่น้อยกว่า 70 TB. ต่อระบบ โดยไม่รวมผลจาก Deduplication หรือ Compression หรือ Thin Provisioning หรือ Data Reduction และหาก Solution ต้องใช้พื้นที่สำหรับ DDB หรือ Index หรือ Metadata แยกต่างหาก ต้องจัดหาเพิ่มเติมโดยไม่นับรวมในความจุดังกล่าว (1 TB. เท่ากับ 10^{12} Bytes)

๙.๔ พื้นที่ Backup Data ต้องใช้ RAID 6 หรือ Distributed RAID 6 หรือ RAID-TP หรือ Dual-Parity Protection หรือเทคโนโลยีที่สามารถทนต่อการชำรุดพร้อมกันของสื่อจัดเก็บข้อมูลไม่น้อยกว่า ๒ หน่วย และสามารถขยายความจุเพิ่มเติมได้ตามสถาปัตยกรรมของผู้ผลิตโดยไม่จำเป็นต้องเปลี่ยนระบบทั้งหมด

๙.๕ ระบบต้องมี Network Interface หรือ Front-End Ethernet Port ที่รองรับความเร็วไม่น้อยกว่า 25 Gigabit Ethernet จำนวนรวมไม่น้อยกว่า ๔ พอร์ตต่อระบบ และรองรับการเชื่อมต่อผ่าน iSCSI หรือ NFS หรือ SMB/CIFS หรือ S3 หรือ Protocol หรือ Interface มาตรฐานอื่นที่ผู้ผลิตรับรองสำหรับใช้เป็น Backup Storage หรือ Backup Repository พร้อมรองรับเส้นทางเชื่อมต่อมากกว่าหนึ่งเส้นทางตามสถาปัตยกรรมที่เสนอ และจัดหา Transceiver Module หรือ DAC Cable หรือ AOC Cable หรือสายสัญญาณอื่นที่จำเป็นให้ครบถ้วน

๙.๖ Backup Solution ต้องรองรับ Deduplication หรือ Compression หรือ Data Reduction โดยสามารถดำเนินการที่ Backup Software หรือ Media Agent หรือ Backup Storage หรือองค์ประกอบอื่นของ Solution และรองรับการส่งสำเนาข้อมูลไปยังศูนย์ข้อมูลสำรองด้วย Backup Copy หรือ Secondary Copy หรือ Auxiliary Copy หรือ Replication Backup หรือเทคโนโลยีที่ให้ผลเทียบเท่า

๙.๗ ระบบต้องสามารถบริหารจัดการผ่าน Web-Based GUI หรือ Management Console และตรวจสอบสถานะ Capacity, Controller หรือ Node, Storage Media, Network Interface, System Health และ Alarm หรือ Alert ได้ โดยอุปกรณ์ต้องมี Power Supply แบบ Redundant หรือระบบจ่ายไฟที่ให้ผลเทียบเท่า และมี Cooling Fan แบบ Redundant หรือระบบระบายความร้อนที่ให้ผลเทียบเท่า

๙.๘ Backup Solution ต้องรองรับการเข้ารหัสข้อมูลสำรองขณะจัดเก็บที่ Backup Software หรือ Backup Storage หรือองค์ประกอบอื่นของ Solution และรองรับการป้องกันข้อมูลระหว่างการรับส่งด้วย TLS หรือ IPsec หรือ Secure Protocol อื่นตามสถาปัตยกรรมที่เสนอ

Proof

๙.๙ ผู้ยื่นข้อเสนอต้องจัดหา License หรือ Subscription และ Technical Support ที่จำเป็นสำหรับความสามารถทั้งหมดที่เสนอให้ครบถ้วนตลอดระยะเวลาไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรุ่นผลิตภัณฑ์และ Software/Firmware Version ต้องอยู่ในระยะที่ผู้ผลิตให้การสนับสนุนตลอดระยะเวลาดังกล่าว

๑๐. ระบบจัดเก็บข้อมูลสำรองประจำศูนย์ข้อมูลสำรอง (Backup Storage) จำนวน ๑ ระบบ โดยมีคุณลักษณะของแต่ละระบบอย่างน้อยดังนี้

๑๐.๑ ผู้ยื่นข้อเสนอต้องจัดหาระบบจัดเก็บข้อมูลสำรองประจำศูนย์ข้อมูลสำรอง จำนวน ๑ ระบบ โดยเป็น Backup Storage Appliance หรือ Enterprise Storage หรือ Backup Software ร่วมกับ Storage Repository และสามารถทำงานร่วมกับ Backup Software หรือ Media Agent หรือ Backup Server ที่เสนอในโครงการได้

๑๐.๒ ระบบต้องมี Controller หรือ Storage Node ไม่น้อยกว่า ๒ หน่วยต่อระบบ หรือมีสถาปัตยกรรมแบบกระจายที่ให้ผลด้านความพร้อมใช้งานเทียบเท่า และรองรับการทำงานแบบ High Availability หรือ Active-Active หรือเทคโนโลยีที่ให้ผลเทียบเท่า โดยเมื่อส่วนประกอบหนึ่งหน่วยขัดข้อง ระบบต้องยังสามารถให้บริการข้อมูลได้

๑๐.๓ ระบบต้องมีพื้นที่สำหรับ Backup Data ที่ใช้งานได้จริงหลังการกำหนดค่าป้องกันข้อมูล และหักพื้นที่สงวนของระบบไม่น้อยกว่า 170 TB. โดยไม่รวมผลจาก Deduplication หรือ Compression หรือ Thin Provisioning หรือ Data Reduction และหาก Solution ต้องใช้พื้นที่สำหรับ DDB หรือ Index หรือ Metadata แยกต่างหาก ต้องจัดหาเพิ่มเติมโดยไม่นับรวมในความจุดังกล่าว (1 TB. เท่ากับ 10^{12} Bytes)

๑๐.๔ พื้นที่ Backup Data ต้องใช้ RAID 6 หรือ Distributed RAID 6 หรือ RAID-TP หรือ Dual-Parity Protection หรือ Erasure Coding หรือเทคโนโลยีที่สามารถทนต่อการชำรุดพร้อมกันของสื่อจัดเก็บข้อมูลไม่น้อยกว่า ๒ หน่วย และสามารถขยายความจุเพิ่มเติมได้ตามสถาปัตยกรรมของผู้ผลิต โดยไม่จำเป็นต้องเปลี่ยนระบบทั้งหมด

๑๐.๕ ระบบต้องมี Network Interface หรือ Front-End Ethernet Port ที่รองรับความเร็วไม่น้อยกว่า 25 Gigabit Ethernet จำนวนรวมไม่น้อยกว่า ๘ พอร์ตต่อระบบ และรองรับการเชื่อมต่อผ่าน iSCSI หรือ NFS หรือ SMB/CIFS หรือ S3 หรือ S3-Compatible Protocol หรือ Interface มาตรฐานอื่นที่ผู้ผลิตรับรองสำหรับใช้เป็น Backup Storage หรือ Backup Repository พร้อมรองรับเส้นทางเชื่อมต่อมากกว่าหนึ่งเส้นทางตามสถาปัตยกรรมที่เสนอ และจัดหา Transceiver Module หรือ DAC Cable หรือ AOC Cable หรือสายสัญญาณอื่นที่จำเป็นให้ครบถ้วน

๑๐.๖ ระบบต้องสามารถรับ Backup Copy หรือ Secondary Copy หรือ Auxiliary Copy หรือ Replicated Backup จากศูนย์ข้อมูลหลักของ AIS, TRUE และ NT รวมไม่น้อยกว่า ๓ แหล่งต้นทาง และสามารถกำหนด Backup Destination หรือ Disk Library หรือ Repository หรือ Storage Pool หรือ Volume หรือ Policy เพื่อแยกบริหารจัดการข้อมูลสำรองของแต่ละแหล่งต้นทางได้

Proof

๑๐.๗ Backup Solution ต้องรองรับ Deduplication หรือ Compression หรือ Data Reduction และรองรับการป้องกันข้อมูลสำรองจากการแก้ไข เขียนทับ หรือลบก่อนครบระยะเวลาที่กำหนดด้วย Immutable Backup หรือ WORM หรือ Storage Lock หรือ Compliance Lock หรือ Object Lock หรือ Safeguarded Copy หรือเทคโนโลยีที่ให้ผลเทียบเท่า โดยความสามารถดังกล่าวสามารถดำเนินการที่ Backup Software หรือ Backup Storage หรือองค์ประกอบอื่นของ Solution ได้

๑๐.๘ ข้อมูลสำรองที่จัดเก็บในระบบต้องสามารถนำมาใช้สำหรับการ Restore หรือ Recovery ผ่าน Backup Software หรือ Recovery Workflow ที่เสนอได้

๑๐.๙ ระบบต้องสามารถบริหารจัดการผ่าน Web-Based GUI หรือ Management Console และตรวจสอบสถานะ Capacity, Controller หรือ Node, Storage Media, Network Interface, System Health, Alarm หรือ Alert และสถานะ Backup Copy หรือ Replication Backup ได้ โดยอุปกรณ์ต้องมี Power Supply แบบ Redundant หรือระบบจ่ายไฟที่ให้ผลเทียบเท่า และมี Cooling Fan แบบ Redundant หรือระบบระบายความร้อนที่ให้ผลเทียบเท่า

๑๐.๑๐ Backup Solution ต้องรองรับการเข้ารหัสข้อมูลสำรองขณะจัดเก็บที่ Backup Software หรือ Backup Storage หรือองค์ประกอบอื่นของ Solution และรองรับการป้องกันข้อมูลระหว่างการรับส่งด้วย TLS หรือ IPsec หรือ Secure Protocol อื่นตามสถาปัตยกรรมที่เสนอ

๑๐.๑๑ ผู้ยื่นข้อเสนอต้องจัดหา License หรือ Subscription และ Technical Support ที่จำเป็นสำหรับ Backup, Backup Copy, Recovery, Deduplication, Compression, Immutable Backup, Encryption และการบริหารจัดการให้ครบถ้วนตลอดระยะเวลาไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรุ่นผลิตภัณฑ์และ Software/Firmware Version ต้องอยู่ในระยะที่ผู้ผลิตให้การสนับสนุนตลอดระยะเวลาดังกล่าว

ส่วนที่ ๓ ระบบบริหารจัดการความมั่นคงปลอดภัย (Security & Compliance Layer)

๑๑. อุปกรณ์รักษาความปลอดภัยเครือข่าย ประจำศูนย์ข้อมูลหลัก (Next-Generation Firewall) มีคุณลักษณะอย่างน้อย ดังนี้

๑๑.๑ ผู้ยื่นข้อเสนอต้องจัดหาอุปกรณ์ Next-Generation Firewall (NGFW) แบบ Hardware Appliance ระดับองค์กร จำนวน ๖ เครื่อง สำหรับติดตั้ง ณ ศูนย์ข้อมูลของผู้ให้บริการ AIS, TRUE และ NT ชุดละ ๒ เครื่อง และสามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้ว หรือมี Rack Mount Kit ที่ผู้ผลิตรองรับสำหรับรุ่นที่เสนอ

๑๑.๒ มี Network Interface แบบ 1 Gbps. หรือดีกว่ารวมไม่น้อยกว่า ๘ พอร์ตต่อเครื่อง และในจำนวนดังกล่าวต้องมี Network Interface แบบ 10 Gbps. หรือดีกว่าไม่น้อยกว่า ๔ พอร์ตต่อเครื่อง พร้อมจัดหา Transceiver Module หรือ DAC Cable หรือ AOC Cable หรือสายสัญญาณที่จำเป็นให้ครบถ้วนตาม Network Port Mapping และมี Power Supply หรือ Power Adapter จำนวนรวมไม่น้อยกว่า ๒ ชุดต่อเครื่องสำหรับรองรับการทำงานแบบ Redundant ตามการออกแบบที่เสนอ

Proof

๑๑.๓ รองรับ Stateful Firewall และ Intrusion Prevention System (IPS) และ (Application Identification หรือ Application Control) และ (Anti-Malware หรือ Anti-Virus) และ (URL Filtering หรือ Web Filtering) และ (DNS Security หรือ DNS Filtering) และการวิเคราะห์ไฟล์ต้องสงสัยด้วยระบบ Sandbox แบบ Cloud หรือ On-premises หรือเทคโนโลยีอื่นที่ให้ผลเทียบเท่า โดยความสามารถทั้งหมดต้องสามารถเปิดใช้งานร่วมกันได้ตาม Software Version และ License หรือ Security Subscription ที่เสนอ

๑๑.๔ มี Firewall Throughput หรือ Firewall/App-ID Throughput ไม่น้อยกว่า 9 Gbps. และมี Threat Prevention Throughput หรือ NGFW Throughput ไม่น้อยกว่า 5 Gbps. ต่อเครื่อง รวมทั้งรองรับ Concurrent Sessions หรือ Concurrent Connections ไม่น้อยกว่า 1,000,000 Sessions และ New Sessions per Second หรือ Connections per Second ไม่น้อยกว่า 100,000 Sessions per Second ต่อเครื่อง

๑๑.๕ อุปกรณ์จำนวน ๒ เครื่องที่ติดตั้งภายในศูนย์ข้อมูลเดียวกันต้องรองรับการทำงานแบบ Active/Passive หรือ Active/Standby หรือ Active/Active หรือ Clustering หรือเทคโนโลยีที่ให้ผลด้านความพร้อมใช้งานเทียบเท่าหรือดีกว่า

๑๑.๖ รองรับการกำหนด Security Policy โดยใช้ Source, Destination, Service หรือ Port, Application, User หรือ User Group และ Security Zone หรือ Interface เป็นเงื่อนไขได้ และรองรับการทำงานร่วมกับระบบยืนยันตัวตนหรือ Directory Service ผ่าน LDAP หรือ Active Directory หรือ RADIUS หรือมาตรฐานอื่นที่ให้ผลเทียบเท่า

๑๑.๗ รองรับ Site-to-Site VPN ผ่าน IPsec VPN หรือเทคโนโลยีที่ให้ผลเทียบเท่าหรือดีกว่า รองรับ Static Routing และรองรับ OSPF หรือ BGP อย่างน้อยหนึ่ง Protocol รวมทั้งรองรับ Network Address Translation (NAT) สามารถส่ง Traffic Log หรือ Security Log หรือ Threat Log หรือ Event ไปยังระบบ Log Management หรือ SIEM ผ่าน Syslog หรือ API หรือวิธีการมาตรฐานอื่นที่ผู้ผลิตรองรับ และสามารถบริหารจัดการผ่าน Graphical User Interface (GUI) และ CLI หรือ SSH หรือระบบบริหารจัดการส่วนกลางที่เสนอ

๑๑.๘ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Security Subscription รวมทั้ง Signature Update หรือ Threat Intelligence Update และ Technical Support ที่จำเป็นสำหรับความสามารถตามข้อกำหนดให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรุ่นผลิตภัณฑ์ที่เสนอต้องได้รับการสนับสนุนจากผู้ผลิตครอบคลุมตลอดระยะเวลาดังกล่าว และต้องได้รับสิทธิ์ในการติดตั้ง Patch, Update หรือ Upgrade Software/Firmware ให้เป็นเวอร์ชั่นที่ผู้ผลิตรองรับตลอดระยะเวลาโดยไม่มีค่าใช้จ่ายเพิ่มเติม

Proof

๑๒. อุปกรณ์รักษาความปลอดภัยเครือข่าย ประจำศูนย์ข้อมูลสำรอง (Next-Generation Firewall) มีคุณลักษณะอย่างน้อย ดังนี้

๑๒.๑ ผู้ยื่นข้อเสนอต้องจัดหาอุปกรณ์ Next-Generation Firewall (NGFW) แบบ Hardware Appliance ระดับองค์กร จำนวน ๒ เครื่อง สำหรับติดตั้ง ณ ศูนย์ข้อมูลสำรอง เพื่อควบคุม ตรวจสอบ และป้องกันการรับส่งข้อมูล รวมทั้งรองรับการให้บริการเมื่อมีการย้ายหรือกู้คืนระบบจากศูนย์ข้อมูลหลัก โดยอุปกรณ์ต้องสามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้ว หรือมี Rack Mount Kit

๑๒.๒ มี Network Interface แบบ 25 Gbps. หรือดีกว่าไม่น้อยกว่า ๔ พอร์ตต่อเครื่อง พร้อมจัดหา Transceiver Module, DAC Cable, AOC Cable หรือสายสัญญาณที่จำเป็นให้ครบถ้วนตาม Network Port Mapping และมี Power Supply จำนวนไม่น้อยกว่า ๒ ชุดต่อเครื่อง เพื่อรองรับการทำงานแบบ Redundant ตามการออกแบบที่เสนอ

๑๒.๓ รองรับ Stateful Firewall, Intrusion Prevention System (IPS), Application Identification หรือ Application Control, Anti-Malware หรือ Anti-Virus, URL Filtering หรือ Web Filtering, DNS Security หรือ DNS Filtering และการวิเคราะห์ไฟล์ต้องสงสัยด้วยระบบ Sandbox แบบ Cloud หรือ On-premises หรือเทคโนโลยีอื่นที่ให้ผลเทียบเท่า โดยความสามารถทั้งหมดต้องสามารถเปิดใช้งานร่วมกันได้ตาม Software Version และ License หรือ Security Subscription ที่เสนอ

๑๒.๔ มี Firewall Throughput หรือ Firewall/App-ID Throughput ไม่น้อยกว่า 150 Gbps. และมี Threat Prevention Throughput หรือ NGFW Throughput ไม่น้อยกว่า 30 Gbps. ต่อเครื่อง รวมทั้งรองรับ Concurrent Sessions หรือ Concurrent Connections ไม่น้อยกว่า 5,000,000 Sessions และ New Sessions per Second หรือ Connections per Second ไม่น้อยกว่า 250,000 Sessions per Second ต่อเครื่อง

๑๒.๕ อุปกรณ์ทั้ง ๒ เครื่องต้องรองรับการทำงานร่วมกันแบบ Active/Passive หรือ Active/Standby หรือ Active/Active หรือ Clustering หรือเทคโนโลยีอื่นที่ให้ผลด้านความพร้อมใช้งานเทียบเท่าหรือดีกว่า และสามารถสลับการทำงานโดยอัตโนมัติเมื่ออุปกรณ์หรือเส้นทางเชื่อมต่อหลักเกิดขัดข้อง

๑๒.๖ รองรับการกำหนด Security Policy โดยใช้ Source, Destination, Service หรือ Port, Application, User หรือ User Group และ Security Zone หรือ Interface เป็นเงื่อนไขได้ และรองรับการทำงานร่วมกับระบบยืนยันตัวตนหรือ Directory Service ผ่าน LDAP, Active Directory, RADIUS หรือมาตรฐานอื่นที่ให้ผลเทียบเท่า

๑๒.๗ รองรับ Site-to-Site VPN ผ่าน IPsec VPN หรือเทคโนโลยีอื่นที่ให้ผลเทียบเท่าหรือดีกว่า รองรับ Static Routing และ OSPF หรือ BGP อย่างน้อยหนึ่ง Protocol รวมทั้งรองรับ Network Address Translation (NAT) สามารถส่ง Traffic Log, Security Log, Threat Log หรือ Event ไปยังระบบ Log Management หรือ SIEM ผ่าน Syslog, API หรือวิธีการมาตรฐานอื่นที่ผู้ผลิตรองรับ และสามารถบริหารจัดการผ่าน Graphical User Interface (GUI) และ CLI, SSH หรือระบบบริหารจัดการส่วนกลางที่เสนอ

Proof

๑๒.๘ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Security Subscription รวมทั้ง Signature Update หรือ Threat Intelligence Update และ Technical Support ที่จำเป็นสำหรับความสามารถตามข้อกำหนดให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรุ่นผลิตภัณฑ์ที่เสนอต้องได้รับการสนับสนุนจากผู้ผลิตครอบคลุมตลอดระยะเวลาดังกล่าว และต้องได้รับสิทธิ์ในการติดตั้ง Patch, Update หรือ Upgrade Software/Firmware ให้เป็นเวอร์ชั่นที่ผู้ผลิตรองรับตลอดระยะเวลาโดยไม่มีค่าใช้จ่ายเพิ่มเติม

๑๓. ระบบบริหารจัดการและวิเคราะห์ข้อมูลความมั่นคงปลอดภัย (Log Management and SIEM) มีคุณลักษณะอย่างน้อย ดังนี้

๑๓.๑ สามารถรวบรวม วิเคราะห์ เชื่อมโยง ตรวจจับ และแจ้งเตือนเหตุการณ์ด้านความมั่นคงปลอดภัย โดยเป็น Software Platform หรือ Virtual Appliance หรือ Hardware Appliance หรือ Cloud Service หรือรูปแบบที่ให้ความสามารถเทียบเท่า

๑๓.๒ รองรับการรับ Log หรือ Event หรือ Alert หรือ Security Telemetry จากอุปกรณ์หรือระบบที่เกี่ยวข้อง ผ่าน Syslog หรือ API หรือ Agent หรือ Collector หรือ Connector และสามารถทำ Normalization หรือ Enrichment หรือ Correlation รวมทั้งเชื่อมต่อกับระบบ Log Management Platform หลักของโครงการได้โดยไม่ต้องจัดเก็บ Raw Log ทั้งหมดซ้ำ

๑๓.๓ ระบบต้องมีสิทธิรองรับแหล่งข้อมูลทั้งหมดตาม รายการอุปกรณ์ที่เสนอ, Data Source Inventory และ Integration Matrix โดยกรณีคิดสิทธิแบบ Node หรือ Asset หรือ Device หรือ Data Source ต้องมีจำนวนไม่น้อยกว่าจำนวนแหล่งข้อมูลจริงรวมสำรอง

๑๓.๔ รองรับการค้นหาข้อมูลแบบ Real-Time และ Historical Search และรองรับการตรวจจับด้วย Correlation Rule หรือ Detection Rule หรือ User and Entity Behavior Analytics หรือ Anomaly Detection หรือ Risk-Based Detection อย่างน้อยหนึ่งรูปแบบ

๑๓.๕ รองรับการนำ Threat Intelligence หรือ Indicator of Compromise มาใช้เพิ่มบริบทของเหตุการณ์ รองรับการเชื่อมโยงเหตุการณ์กับ MITRE ATT&CK หรือกรอบการวิเคราะห์ภัยคุกคามที่เทียบเท่า และสามารถกำหนด Severity หรือ Risk Score ได้

๑๓.๖ รองรับการสร้าง Alert หรือ Incident หรือ Case และสามารถดำเนินการตอบสนองผ่าน Automation หรือ Playbook หรือ Script หรือ API หรือระบบภายนอกได้อย่างน้อยหนึ่งรูปแบบ

๑๓.๗ รองรับการจัดทำ Dashboard หรือ Report โดยกำหนดสิทธิ์ตาม Role มี Administrative Audit Log และเชื่อมต่อกับระบบยืนยันตัวตนผ่าน Active Directory หรือ LDAP/LDAPS หรือ SAML หรือ OpenID Connect หรือ RADIUS อย่างน้อยหนึ่งรูปแบบ

๑๓.๘ ระบบต้องรองรับ High Availability หรือ Failover หรือ Backup and Restore หรือ Cloud Service Availability หรือกลไกที่ให้ผลด้านความต่อเนื่องของบริการเทียบเท่าตามสถาปัตยกรรมที่เสนอ

๑๓.๙ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Security Subscription รวมทั้ง Threat Intelligence Update หรือ Software Update และ Technical Support ที่จำเป็นให้ครบถ้วนไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

Proof

๑๔. อุปกรณ์กระจายภาระการใช้งานสำหรับศูนย์ข้อมูลหลัก (Application Delivery Controller / Load Balancer - ADC DC) จำนวน ๖ เครื่อง โดยมีคุณลักษณะของแต่ละเครื่องอย่างน้อยดังนี้

๑๔.๑ ผู้ยื่นข้อเสนอต้องจัดหาอุปกรณ์ Application Delivery Controller หรือ Load Balancer แบบ Hardware Appliance จำนวน ๖ เครื่อง สำหรับติดตั้ง ณ ศูนย์ข้อมูลของ AIS หรือ TRUE หรือ NT ชุดละ ๒ เครื่อง

๑๔.๒ รองรับการทำ Load Balancing ระดับ Layer 4 และ Layer 7 และรองรับ Content Routing หรือ Content Rewrite หรือ Scripting อย่างน้อยหนึ่งรูปแบบ

๑๔.๓ รองรับ HTTP หรือ HTTPS หรือ TCP หรือ UDP รองรับ Health Check หรือ Service Monitoring รองรับ Session Persistence หรือ Session Affinity และรองรับวิธีการกระจายภาระ เช่น Round Robin หรือ Least Connection หรือ Weighted Algorithm หรือ Source IP-based อย่างน้อยหนึ่งรูปแบบ

๑๔.๔ มี Layer 4 Throughput และ Layer 7 Throughput หรือมีค่าที่ผู้ผลิตระบุเป็น L4/L7 Performance ไม่น้อยกว่า 30 Gbps. รองรับ Concurrent Connections ไม่น้อยกว่า 25,000,000 Connections รองรับ Layer 4 Connections per Second ไม่น้อยกว่า 500,000 Connections per Second และรองรับ Layer 7 Requests per Second ไม่น้อยกว่า 650,000 Requests per Second ต่อเครื่อง

๑๔.๕ รองรับ SSL Offloading หรือ SSL/TLS Termination หรือ SSL Acceleration และมี Hardware SSL Accelerator หรือ Cryptographic Accelerator หรือหน่วยประมวลผลเฉพาะสำหรับ SSL/TLS

๑๔.๖ รองรับ Global Server Load Balancing หรือกลไกที่ให้ผลด้านการกระจายบริการระหว่างศูนย์ข้อมูลเทียบเท่า

๑๔.๗ มี Network Interface แบบ 10 Gigabit Ethernet SFP+ หรือดีกว่าไม่น้อยกว่า ๔ พอร์ตต่อเครื่อง มี Power Supply ไม่น้อยกว่า ๒ ชุดแบบ Redundant หรือ Hot-Swap และต้องจัดหา Interface Module หรือ Transceiver Module หรือ DAC Cable หรือ AOC Cable หรือสายสัญญาณที่จำเป็นให้ครบถ้วนตาม Network Port Mapping

๑๔.๘ อุปกรณ์จำนวน ๒ เครื่องภายในแต่ละศูนย์ข้อมูลต้องรองรับ High Availability แบบ Active/Standby หรือ Active/Passive หรือ Active/Active หรือรูปแบบที่ให้ผลเทียบเท่า รองรับการบริหารจัดการผ่าน Web-Based GUI หรือ CLI หรือ SSH หรือ API และสามารถส่ง Log ไปยังระบบ Log Management หรือ SIEM หรือ Monitoring ผ่าน Syslog หรือ API

๑๔.๙ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Feature License หรือ Subscription รวมทั้ง Software/Firmware Update และ Technical Support ที่จำเป็นให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรุ่นผลิตภัณฑ์ที่เสนอต้องได้รับการสนับสนุนจากผู้ผลิตครอบคลุมตลอดระยะเวลาดังกล่าว และต้องได้รับสิทธิ์ในการติดตั้ง Patch หรือ Update หรือ Upgrade Software/Firmware ให้เป็นเวอร์ชั่นที่ผู้ผลิตรองรับโดยไม่มีค่าใช้จ่ายเพิ่มเติม

Proof

๑๕. อุปกรณ์กระจายภาระการใช้งานสำหรับศูนย์ข้อมูลสำรอง (Application Delivery Controller / Load Balancer - ADC DR) จำนวน ๒ เครื่อง โดยมีคุณลักษณะของแต่ละเครื่องอย่างน้อยดังนี้

๑๕.๑ ผู้ยื่นข้อเสนอต้องจัดหาอุปกรณ์ Application Delivery Controller หรือ Load Balancer แบบ Hardware Appliance จำนวน ๒ เครื่อง สำหรับติดตั้ง ณ ศูนย์ข้อมูลสำรอง เพื่อกระจายภาระการใช้งานและรองรับการให้บริการเมื่อมีการกู้คืนหรือย้ายระบบจากศูนย์ข้อมูลหลัก

๑๕.๒ รองรับการทำ Load Balancing ระดับ Layer 4 และ Layer 7 และรองรับ Content Routing หรือ Content Rewrite หรือ Scripting อย่างน้อยหนึ่งรูปแบบ

๑๕.๓ รองรับ HTTP หรือ HTTPS หรือ TCP หรือ UDP รองรับ Health Check หรือ Service Monitoring รองรับ Session Persistence หรือ Session Affinity และรองรับวิธีการกระจายภาระ เช่น Round Robin หรือ Least Connection หรือ Weighted Algorithm หรือ Source IP-based อย่างน้อยหนึ่งรูปแบบ

๑๕.๔ มี Layer 4 Throughput และ Layer 7 Throughput หรือมีค่าที่ผู้ผลิตระบุเป็น L4/L7 Performance ไม่น้อยกว่า 30 Gbps. รองรับ Concurrent Connections ไม่น้อยกว่า 25,000,000 Connections รองรับ Layer 4 Connections per Second ไม่น้อยกว่า 500,000 Connections per Second และรองรับ Layer 7 Requests per Second ไม่น้อยกว่า 650,000 Requests per Second ต่อเครื่อง

๑๕.๕ รองรับ SSL Offloading หรือ SSL/TLS Termination หรือ SSL Acceleration และมี Hardware SSL Accelerator หรือ Cryptographic Accelerator หรือหน่วยประมวลผลเฉพาะสำหรับ SSL/TLS

๑๕.๖ รองรับ Global Server Load Balancing หรือกลไกที่ให้ผลด้านการกระจายบริการระหว่างศูนย์ข้อมูลหรือการรองรับบริการจากศูนย์ข้อมูลสำรองเทียบเท่า

๑๕.๗ มี Network Interface แบบ 10 Gigabit Ethernet SFP+ หรือดีกว่าไม่น้อยกว่า ๔ พอร์ตต่อเครื่อง มี Power Supply ไม่น้อยกว่า ๒ ชุดแบบ Redundant หรือ Hot-Swap และต้องจัดหา Interface Module หรือ Transceiver Module หรือ DAC Cable หรือ AOC Cable หรือสายสัญญาณที่จำเป็นให้ครบถ้วนตาม Network Port Mapping

๑๕.๘ อุปกรณ์ทั้ง ๒ เครื่องต้องรองรับ High Availability แบบ Active/Standby หรือ Active/Passive หรือ Active/Active หรือรูปแบบที่ให้ผลเทียบเท่า รองรับการบริหารจัดการผ่าน Web-Based GUI หรือ CLI หรือ SSH หรือ API และสามารถส่ง Log ไปยังระบบ Log Management หรือ SIEM หรือ Monitoring ผ่าน Syslog หรือ API

๑๕.๙ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Feature License หรือ Subscription รวมทั้ง Software/Firmware Update และ Technical Support ที่จำเป็นให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรุ่นผลิตภัณฑ์ที่เสนอต้องได้รับการสนับสนุนจากผู้ผลิตครอบคลุมตลอดระยะเวลาดังกล่าว และต้องได้รับสิทธิ์ในการติดตั้ง Patch หรือ Update หรือ Upgrade Software/Firmware ให้เป็นเวอร์ชันที่ผู้ผลิตรองรับโดยไม่มีค่าใช้จ่ายเพิ่มเติม

Proof

ภาคผนวก ๒

รายละเอียดคุณลักษณะเฉพาะซอฟต์แวร์

(Software Specifications)

ภาคผนวก ๒ รายละเอียดคุณลักษณะเฉพาะซอฟต์แวร์ (Software Specifications) มีรายการดังต่อไปนี้

๑. ระบบซอฟต์แวร์การจำลองเสมือน (Virtualization Platform) จำนวน ๑ ระบบ
๒. ระบบรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Detection and Response) จำนวน ๑ ระบบ
๓. ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log Management Platform) จำนวน ๑ ระบบ
๔. ระบบตรวจสอบและบริหารจัดการโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ (Infrastructure Monitoring System) จำนวน ๑ ระบบ
๕. ระบบบริหารจัดการตรวจสอบสิทธิการเข้าถึง (Privileged Access Management)
๖. ระบบยืนยันตัวตนส่วนกลาง (Centralized Authentication / MFA / AAA)

๑. ระบบซอฟต์แวร์การจำลองเสมือน (Virtualization Platform) จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังนี้

๑.๑ ต้องเป็นระบบแพลตฟอร์มโครงสร้างพื้นฐานเสมือนแบบรวมศูนย์ จำนวน ๑ ระบบ สำหรับศูนย์ข้อมูลหลัก ๓ ชุด และศูนย์ข้อมูลสำรอง โดยเป็น Software Platform หรือ Hyper-Converged Infrastructure Appliance หรือ Software-Defined Infrastructure Platform หรือรูปแบบที่ให้ความสามารถเทียบเท่า

๑.๒ ระบบต้องรวมความสามารถด้าน Server Virtualization, Software-Defined Storage, Network Virtualization และ Centralized Management โดยความสามารถดังกล่าวต้องเป็นผลิตภัณฑ์หรือ Module ของผู้ผลิตรายเดียวกัน หรือเป็นชุดผลิตภัณฑ์ที่ผู้ผลิตรับรองการทำงานร่วมกันแบบ End-to-End

๑.๓ ระบบต้องมี Compute Node รวมไม่น้อยกว่า 10 Nodes โดยศูนย์ข้อมูลหลักแต่ละชุดมี Compute Node ไม่น้อยกว่า 2 Nodes พร้อมกลไก Quorum โดยใช้ Witness แยกจาก Cluster หรือเพิ่ม Node ตามสถาปัตยกรรมที่ผู้ผลิตรับรอง และศูนย์ข้อมูลสำรองต้องมี Compute Node ไม่น้อยกว่า 4 Nodes

๑.๔ รองรับการสร้าง แก้ไข เปิด ปิด ลบ Clone และกำหนด CPU, Memory, Storage และ Network ให้แก่ Virtual Machine รวมทั้งรองรับ High Availability, Dynamic Resource Scheduling, Live Migration และ Snapshot โดยสามารถกู้คืน Virtual Machine บน Node อื่นเมื่อ Node ขัดข้องได้

Proof

๑.๕ รองรับ Distributed Storage โดยใช้ Data Replication ไม่น้อยกว่า 2 Copies หรือ Erasure Coding ที่ให้ระดับการป้องกันข้อมูลเทียบเท่า และรองรับ SSD Read/Write Acceleration, Storage Policy, Data Locality หรือกลไกจัดวางข้อมูลที่เทียบเท่า รวมทั้งปรับสมดุลข้อมูลเมื่อเพิ่มหรือลด Node ได้

๑.๖ พื้นที่จัดเก็บข้อมูลของระบบตามข้อ ๑.๕ ใช้สำหรับรองรับ Virtual Machine และองค์ประกอบของแพลตฟอร์ม โดยไม่นำไปรวมคำนวณเป็นความจุของระบบจัดเก็บข้อมูลหลักหรือระบบจัดเก็บข้อมูลสำรอง

๑.๗ รองรับ Network Virtualization ซึ่งมี Virtual Switch, VLAN Tagging และการแสดง Network Topology รวมทั้งรองรับ Distributed Firewall หรือ Micro-Segmentation หรือกลไกควบคุมการรับส่งข้อมูลระหว่าง Virtual Machine ที่ให้ผลเทียบเท่า

๑.๘ รองรับการบริหารจัดการ Cluster, Host, Virtual Machine, Storage และ Network จากส่วนกลางผ่าน Web-Based Management พร้อมแสดง Dashboard, Resource Utilization, Alarm หรือ Event และรองรับ Role-Based Access Control, Administrative Audit Log และ API หรือ Syslog สำหรับเชื่อมต่อระบบอื่น

๑.๙ รองรับการเชื่อมต่อระบบจัดเก็บข้อมูลภายนอกกับ Host หรือ Virtual Machine ผ่าน iSCSI ที่ความเร็วไม่น้อยกว่า 25 Gbps. และ Multipath หรือวิธีการที่ผู้ผลิตรับรองซึ่งให้ความพร้อมใช้งานและสมรรถนะเทียบเท่า รวมทั้งสามารถทำงานร่วมกับระบบ Backup and Recovery ที่เสนอในโครงการได้

๑.๑๐ รองรับ Cross-Site Disaster Recovery ระหว่างศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรอง โดยสามารถกำหนด Replication Policy, Protection Group, Recovery Plan, DR Test, Failover และ Failback พร้อมจัดหาสิทธิให้ครอบคลุม Virtual Machine

๑.๑๑ ผู้ยื่นข้อเสนอต้องจัดหา License หรือ Subscription ให้ครอบคลุม Compute Node และองค์ประกอบทั้งหมดตามสถาปัตยกรรมที่เสนอ รวมทั้ง Witness, Management และ Disaster Recovery พร้อมแสดง License Calculation ตามจำนวน Physical CPU Socket หรือ Core หรือ Node หรือ Virtual Machine ตามเกณฑ์ของผู้ผลิต และแนบ Architecture Diagram, Compatibility Matrix และ BOM ที่สามารถตรวจสอบจำนวนสิทธิได้

๑.๑๒ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Subscription รวมทั้ง Software Update และ Technical Support ที่จำเป็นให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยต้องได้รับสิทธิในการติดตั้ง Patch, Update หรือ Upgrade ให้เป็น Version ที่ผู้ผลิตรองรับตลอดระยะเวลาโดยไม่มีค่าใช้จ่ายเพิ่มเติม

๒. ระบบรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Detection and Response) จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังนี้

๒.๑ ผู้ยื่นข้อเสนอต้องจัดให้มีระบบ EDR หรือ XDR จำนวน ๑ ระบบ สำหรับป้องกัน ตรวจจับ วิเคราะห์ สืบค้น และตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่ายหรือเครื่องแม่ข่ายเสมือนหรือ Workload ของโครงการ

Proof

๒.๒ รองรับ Agent แบบ Full Protection บน Windows Server และ Linux ที่ติดตั้งใช้งานจริง โดย Operating System, Version, Kernel และ CPU Architecture ต้องอยู่ในรายการที่เจ้าของผลิตภัณฑ์รองรับอย่างเป็นทางการ

๒.๓ รองรับ Deep Learning หรือ Artificial Intelligence หรือ Machine Learning หรือ Behavioral Analysis และสามารถตรวจจับมัลแวร์ที่ไม่รู้จักโดยไม่พึ่งพา Signature เพียงอย่างเดียว รวมถึง Zero-day หรือ Fileless Attack

๒.๔ รองรับการตรวจจับและหยุด Process ที่มีพฤติกรรมเข้ารหัสข้อมูลจาก Ransomware และสามารถกู้คืนไฟล์กลับสู่สถานะก่อนถูกแก้ไขโดยอัตโนมัติ หรือมีกลไกที่เจ้าของผลิตภัณฑ์รับรองว่าให้ผลด้านการกู้คืนหรือจำกัดความเสียหายเทียบเท่า

๒.๕ สำหรับ Windows Server ต้องรองรับ Application Allowlisting หรือ Server Lockdown หรือ Unauthorized File Protection และรองรับ File Integrity Monitoring หรือกลไกตรวจสอบการเปลี่ยนแปลงไฟล์สำคัญ

๒.๖ สำหรับ Linux ต้องรองรับ Runtime Detection โดยสามารถตรวจจับพฤติกรรมที่ผิดปกติของ Process หรือ File หรือ Network Connection และสามารถหยุด Process หรือกักกันภัยคุกคามหรือแยกเครื่องออกจากเครือข่ายได้

๒.๗ รองรับ Threat Hunting ผ่าน Live Query หรือ Query Engine และสามารถแสดงความสัมพันธ์ของเหตุการณ์เป็น Threat Graph หรือ Attack Story หรือ Attack Chain หรือรูปแบบที่ให้ความสามารถเทียบเท่า

๒.๘ มีระบบบริหารจัดการแบบรวมศูนย์ รองรับ Dashboard การแจ้งเตือน การกำหนด Policy การแบ่งสิทธิผู้ดูแลระบบตาม Role การสั่ง Response and Remediation และการส่ง Alert หรือ Event หรือ Incident ไปยังระบบ Log Management หรือ SIEM ผ่าน Syslog หรือ API หรือ Connector

๒.๙ ผู้ยื่นข้อเสนอต้องจัดหา License หรือ Subscription ไม่น้อยกว่าจำนวน Windows Server และ Linux Workload ที่ติดตั้งจริงแล้วแต่จำนวนใดจะมากกว่า โดยต้องครอบคลุม Full Malware Protection, EDR หรือ XDR, Threat Hunting, Ransomware Protection, Endpoint Isolation หรือเทียบเท่า หรือดีกว่า

๒.๑๐ ผู้ยื่นข้อเสนอต้องรับผิดชอบจัดหาและต่ออายุ Software License หรือ Security Subscription รวมทั้ง Agent Update หรือ Detection/Security Update หรือ Threat Intelligence Update และ Technical Support ให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรับผิดชอบค่าใช้จ่ายทั้งหมด

๓. ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log Management Platform) จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังนี้

๓.๑ ผู้ยื่นข้อเสนอต้องจัดให้มีแพลตฟอร์ม Log Management ระดับองค์กรแบบ Self-Managed จำนวน ๑ ชุด ติดตั้งบนโครงสร้างพื้นฐานแบบ Virtual Machine ของโครงการ โดยผลิตภัณฑ์ที่เสนอต้องเป็นรุ่นเชิงพาณิชย์ที่ผู้ผลิตประกาศให้ใช้งานทั่วไปแล้ว ไม่ใช่รุ่น Trial, Community, Beta หรือรุ่นที่สิ้นสุดการสนับสนุน

Proof

๓.๒ ระบบต้องประกอบด้วย Cluster ประจำศูนย์ข้อมูลหลักของ AIS, True และ NT ชุดละ 1 Cluster และ Cluster สำหรับศูนย์ข้อมูลสำรองส่วนกลางจำนวน 1 Cluster โดยข้อมูลของแต่ละผู้ให้บริการต้องแยกจากกัน

๓.๓ ระบบประจำศูนย์ข้อมูลหลักแต่ละชุดต้องรองรับปริมาณข้อมูลนำเข้าไม่น้อยกว่า 350 GB. ต่อวัน และศูนย์ข้อมูลสำรองต้องรองรับข้อมูลรวมจากศูนย์ข้อมูลหลักไม่น้อยกว่า 1,050 GB. ต่อวัน

๓.๔ รองรับการนำเข้าข้อมูล AAA Logs และ CGNAT Logs ที่ผ่านการจัดเตรียมจากผู้ให้บริการตามรูปแบบข้อมูลและช่องทางที่กำหนดในการออกแบบระบบ

๓.๕ รองรับการจัดทำดัชนีและการสืบค้นแบบ Full-Text Search หรือ Structured Search และผู้ใช้งานที่ได้รับสิทธิ์สามารถเลือกสืบค้นข้อมูลของแต่ละ Cluster จากส่วนกลางผ่าน Cross-Cluster Search หรือ Federated Search หรือเทคโนโลยีที่มีความสามารถเทียบเท่า โดยไม่ต้องนำ Raw Log ทั้งหมดมารวมไว้ใน Cluster เดียว

๓.๖ รองรับการบริหารวงจรข้อมูลและการเคลื่อนย้ายข้อมูลระหว่างพื้นที่จัดเก็บไม่น้อยกว่า ๒ ระดับชั้นโดยอัตโนมัติ โดยข้อมูลของศูนย์ข้อมูลหลักต้องสามารถสืบค้นย้อนหลังได้ไม่น้อยกว่า ๗๓๐ วัน

๓.๗ รองรับ Role-Based Access Control เพื่อแยกข้อมูลของ AIS, True และ NT และสามารถกำหนดสิทธิ์การค้นหา แสดงผล ส่งออกข้อมูล หรือบริหารระบบตามบทบาท รวมทั้งเชื่อมต่อระบบยืนยันตัวตนผ่าน Active Directory หรือ LDAP/LDAPS หรือ SAML อย่างน้อยหนึ่งรูปแบบ

๓.๘ รองรับการเข้ารหัสการสื่อสารระหว่างผู้ใช้งาน ระบบรับข้อมูล Node และ Cluster ด้วย TLS Version 1.2 หรือสูงกว่า และต้องไม่ส่งข้อมูลจราจร ข้อมูลดัชนีหรือผลการสืบค้นออกนอกโครงสร้างพื้นฐานของโครงการเว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษร

๓.๙ รองรับ Audit Log สำหรับการเข้าสู่ระบบ การยืนยันตัวตนล้มเหลว การเปลี่ยนแปลงสิทธิ์ การปรับเปลี่ยนค่าระบบ และกิจกรรมของผู้ดูแลระบบ โดยผู้ใช้งานทั่วไปต้องไม่สามารถแก้ไขหรือลบ Audit Log ดังกล่าวได้

๓.๑๐ รองรับ High Availability สำหรับองค์ประกอบสำคัญและสามารถทำ Cross-Cluster Replication หรือ Multisite Replication หรือ Data Synchronization หรือวิธีการที่มีความสามารถเทียบเท่าไปยังศูนย์ข้อมูลสำรอง รวมทั้งรองรับ Snapshot หรือ Backup and Restore

๓.๑๑ ความสามารถที่ใช้ปฏิบัติตามข้อกำหนดต้องเป็นความสามารถของผลิตภัณฑ์หรือโมดูลที่ผู้ผลิตรับรองและรวมสิทธิการใช้งานไว้ใน BOM โดยต้องไม่อาศัย Trial License หรือ Community Plugin หรือซอฟต์แวร์จากบุคคลภายนอกที่ไม่มีการสนับสนุนจากผู้ผลิต

๓.๑๒ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Subscription, Security Patch, Software Update หรือ Upgrade และ Technical Support ให้ครอบคลุมจำนวน Cluster ปริมาณข้อมูล ระยะเวลาจัดเก็บและทรัพยากรตามสถาปัตยกรรมที่เสนออย่างครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยไม่มีค่าใช้จ่ายเพิ่มเติม และผู้ผลิตต้องมีช่องทางประกาศ Security Advisory หรือข้อมูลช่องโหว่ของผลิตภัณฑ์อย่างเป็นทางการ

Proof

๔. ระบบตรวจสอบและบริหารจัดการโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ (Infrastructure Monitoring System) จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังนี้

๔.๑ ผู้ยื่นข้อเสนอต้องจัดให้มีระบบ Infrastructure Monitoring จำนวน ๑ ระบบ แบบ Self-Hosted หรือ On-Premises สำหรับตรวจสอบและบริหารจัดการอุปกรณ์และระบบจากส่วนกลาง

๔.๒ รองรับการรวบรวมและแสดงสถานะจากศูนย์ข้อมูลหลัก ๓ ชุด และศูนย์ข้อมูลสำรอง ผ่าน Central Server หรือ Site Server หรือ Polling Engine หรือ Probe หรือ Collector ตามสถาปัตยกรรมที่เสนอ

๔.๓ รองรับการตรวจสอบผ่าน ICMP หรือ SNMP หรือ WMI หรือ API หรือ Agent และรองรับข้อมูล Traffic Flow ผ่าน NetFlow หรือ IPFIX หรือ sFlow หรือ J-Flow หรือ NetStream อย่างน้อยหนึ่งรูปแบบ

๔.๔ รองรับการตรวจสอบอุปกรณ์เครือข่ายหลายผู้ผลิต โดยแสดง Availability, CPU, Memory, Interface Utilization, Latency, Packet Loss, Error หรือ Discard และแสดงความสัมพันธ์หรือ Topology ของอุปกรณ์ได้

๔.๕ รองรับการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายระบบปฏิบัติการ Windows Server และ Linux โดยแสดง CPU, Memory, Disk, Network, Process หรือ Service ตามวิธีการที่ผลิตภัณฑ์รองรับ

๔.๖ รองรับการตรวจสอบระบบจำลองเสมือนหรือ HCI ที่เสนอในโครงการผ่าน SNMP หรือ API หรือ Agent หรือ Connector ที่เจ้าของผลิตภัณฑ์รองรับ โดยแสดงสถานะ Host, Virtual Machine, CPU, Memory, Storage หรือ Network รวมทั้งข้อมูลย้อนหลังหรือแนวโน้มการใช้ทรัพยากรได้

๔.๗ รองรับการตรวจสอบประสิทธิภาพฐานข้อมูลอย่างน้อย 1 Instance และไม่น้อยกว่าจำนวนที่ระบุใน Database Monitoring Inventory โดยรองรับอย่างน้อย ๓ ความสามารถจาก Query Response Time, Wait Analysis, Blocking หรือ Deadlock, Long-running Query, Execution Plan, Resource-intensive Query หรือ Query/Table Advisory

๔.๘ รองรับ Custom Dashboard และสามารถนำข้อมูลย้อนหลังจาก Network, Server, Virtual Machine หรือ Database อย่างน้อย 2 ประเภทมาเปรียบเทียบหรือเชื่อมโยงบนช่วงเวลาเดียวกัน เพื่อช่วยวิเคราะห์สาเหตุของปัญหาได้

๔.๙ รองรับการกำหนด Threshold หรือ Baseline หรือ Anomaly Condition และแจ้งเตือนผ่าน e-mail หรือ SNMP Trap หรือ Webhook หรือวิธีการอื่นที่ผลิตภัณฑ์รองรับ

๔.๑๐ รองรับ Historical Report หรือ Capacity Report หรือ Availability Report และสามารถกำหนดเวลาจัดทำหรือส่งรายงานโดยอัตโนมัติได้

๔.๑๑ รองรับการกำหนดสิทธิ์ตาม Role มี Administrative Audit Log และเชื่อมต่อกับ Active Directory หรือ LDAP/LDAPS หรือ SAML หรือ OpenID Connect อย่างน้อยหนึ่งรูปแบบ

๔.๑๒ ระบบต้องรองรับ High Availability หรือ Failover หรือ Backup and Restore ตามสถาปัตยกรรมที่เสนอ โดยความสามารถหลักต้องเป็นความสามารถมาตรฐานหรือโมดูลที่เจ้าของผลิตภัณฑ์รองรับอย่างเป็นทางการ ไม่ใช้ Trial License, Community Edition หรือ Custom Code ที่จัดทำขึ้นเฉพาะเพื่อให้ผ่านข้อกำหนด และต้องมี Official Documentation, Release Note, Security Hardening Guide หรือ Security Advisory ที่ตรวจสอบได้

Proof

๔.๑๓ ผู้ยื่นข้อเสนอต้องจัดหา License หรือ Subscription รองรับไม่น้อยกว่า 100 Nodes หรือ Licensing Metric ที่ให้ผลเทียบเท่า และต้องไม่น้อยกว่าจำนวนรายการทั้งหมดที่จัดหาในโครงการ

๔.๑๔ ผู้ยื่นข้อเสนอต้องแสดง Proposed Architecture, Monitoring Inventory, Module หรือ Component, Integration Method และ Capacity Sizing พร้อมจัดหา Software Update, Version Upgrade และ Technical Support ให้ครบถ้วนต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

๕. ระบบบริหารจัดการตรวจสอบสิทธิการเข้าถึง (Privileged Access Management) มีคุณลักษณะอย่างน้อย ดังนี้

๕.๑ จัดให้มีระบบ Privileged Access Management (PAM) จำนวน ๑ ระบบ สำหรับควบคุม ตรวจสอบ บันทึก และบริหารจัดการการเข้าถึงระบบสำคัญของผู้ดูแลระบบหรือผู้ใช้งานที่มีสิทธิ์สูง โดยสามารถเสนอเป็น Hardware Appliance หรือ Virtual Appliance หรือ Software Platform ตามรูปแบบที่เจ้าของผลิตภัณฑ์รองรับ พร้อมระบุชื่อผู้ผลิต ผลิตภัณฑ์ รุ่นหรือ Software Version และรูปแบบการติดตั้งที่เสนอ

๕.๒ รองรับผู้ใช้งานที่มีสิทธิ์สูงไม่น้อยกว่า ๑๐ ราย พร้อม License และสิทธิ์การใช้งานที่เพียงพอสำหรับความสามารถทั้งหมดตามข้อกำหนด

๕.๓ รองรับการจัดเก็บ Password, Credential, Secret หรือ SSH Key ภายในระบบ Vault ที่มีการเข้ารหัส รองรับการเปลี่ยนหรือหมุนเวียนรหัสผ่านแบบอัตโนมัติตาม Policy และสามารถเชื่อมต่อระบบปลายทางโดยไม่เปิดเผย Credential แก่ผู้ใช้งาน

๕.๔ รองรับการควบคุมการเข้าถึงระบบปลายทางผ่าน RDP และ SSH เป็นอย่างน้อย

๕.๕ รองรับการกำหนดสิทธิ์ตาม User, User Group, Role หรือ Policy ตามหลัก Least Privilege รวมทั้งการให้สิทธิ์แบบจำกัดช่วงเวลาหรือ Just-in-Time (JIT) และกระบวนการ Request and Approval

๕.๖ รองรับ Session Recording สำหรับ RDP และ SSH โดยสามารถบันทึกภาพหรือวิดีโอพร้อมข้อมูลประกอบของ Session ค้นหาและเล่นย้อนหลัง ติดตาม Session ที่กำลังใช้งานแบบ Real-Time และสั่งยุติ Session ได้

๕.๗ รองรับการเชื่อมต่อกับ Active Directory หรือ LDAP และเชื่อมต่อกับระบบยืนยันตัวตนแบบหลายปัจจัยผ่าน RADIUS หรือ SAML ได้

๕.๘ สามารถจัดเก็บ Audit Log และส่ง Log หรือ Security Event ไปยังระบบ Log Management หรือ SIEM ของโครงการผ่าน Syslog หรือ API ได้

๕.๙ รองรับ High Availability หรือ Clustering พร้อมความสามารถในการสำรองและกู้คืนระบบหรือ Disaster Recovery ตามรูปแบบที่ผู้ผลิตรองรับ โดยผู้ยื่นข้อเสนอต้องจัดหาอุปกรณ์ Software และ License ที่จำเป็นให้ครบถ้วน

๕.๑๐ กรณีเสนอเป็น Virtual Appliance หรือ Software Platform ผู้ยื่นข้อเสนอต้องรวมทรัพยากร CPU, Memory, Storage และ Network ที่จำเป็นไว้ในการคำนวณ Capacity Sizing ของระบบที่เสนอ และกรณีเสนอเป็น Hardware Appliance ต้องรวมอุปกรณ์ License และองค์ประกอบที่จำเป็นไว้ใน Bill of Materials ให้ครบถ้วน

Proof

๕.๑๑ ผู้ยื่นข้อเสนอต้องจัดหา Software License หรือ Subscription และ Technical Support ที่จำเป็นสำหรับความสามารถตามข้อกำหนดให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒ โดยรุ่นผลิตภัณฑ์ที่เสนอต้องได้รับการสนับสนุนจากผู้ผลิตตลอดระยะเวลาดังกล่าว และต้องได้รับสิทธิ์ในการติดตั้ง Patch, Update หรือ Upgrade Software/Firmware ให้เป็นเวอร์ชั่นที่ผู้ผลิตรองรับโดยไม่มีค่าใช้จ่ายเพิ่มเติม

๖. ระบบยืนยันตัวตนส่วนกลาง (Centralized Authentication / MFA / AAA) มีคุณลักษณะอย่างน้อย ดังนี้

๖.๑ ผู้ยื่นข้อเสนอต้องจัดให้มีระบบยืนยันตัวตนส่วนกลางและการยืนยันตัวตนหลายปัจจัยสำหรับใช้ร่วมกับระบบ PAM อุปกรณ์รักษาความปลอดภัยเครือข่าย ระบบบริหารจัดการ หรือระบบอื่นที่เกี่ยวข้องกับโครงการ โดยสามารถเสนอเป็น Hardware Appliance หรือ Virtual Appliance, Software Platform หรือรูปแบบอื่นที่เจ้าของผลิตภัณฑ์รองรับ พร้อมระบุชื่อผู้ผลิต ผลิตภัณฑ์ รุ่นหรือ Software Version และรูปแบบการติดตั้งที่เสนอ

๖.๒ ผู้ยื่นข้อเสนอต้องจัดหาสิทธิการใช้งาน MFA สำหรับผู้ใช้งานที่เป็นบุคคลและมีบัญชีระบุตัวตนได้เป็นรายบุคคลไม่น้อยกว่า ๑๐ ราย และต้องมีจำนวนไม่น้อยกว่าจำนวนผู้ใช้งานที่เป็นบุคคลของระบบ PAM ตามข้อ ๕. รวมถึงผู้ดูแลระบบอื่นที่อยู่ในขอบเขตการใช้งาน MFA ตาม User Sizing ที่เสนอ โดยคำนวณจากจำนวนบุคคลที่ไม่ซ้ำกัน

๖.๓ สามารถบริหารจัดการผู้ใช้งานหรือกลุ่มผู้ใช้งาน และสามารถกำหนดนโยบายการยืนยันตัวตนตามสิทธิ์ที่ได้รับ รวมทั้งต้องเชื่อมต่อกับแหล่งข้อมูลบัญชีผู้ใช้งานอย่างน้อยหนึ่งรูปแบบ ได้แก่ Active Directory หรือ Microsoft Entra ID หรือ LDAP/LDAPS หรือ Identity Provider หรือระบบอื่นที่ให้ผลเทียบเท่า

๖.๔ รองรับการยืนยันตัวตนหลายปัจจัยโดยระบบที่เสนอโดยตรง หรือโดยทำงานร่วมกับ External Identity Provider หรือ MFA Provider โดยรองรับวิธีการไม่น้อยกว่า ๒ รูปแบบจาก Mobile Push หรือ OTP หรือ Software Token หรือ Hardware Token หรือ FIDO/FIDO2 หรือ Certificate หรือ Smart Card หรือ Biometrics

๖.๕ สามารถทำงานร่วมกับระบบ PAM ตามข้อ ๕ เพื่อบังคับใช้ MFA ก่อนอนุญาตให้ผู้ใช้งานเข้าถึงระบบ PAM โดยใช้ SAML ๒.๐ หรือ RADIUS หรือมาตรฐานอื่นที่ผลิตภัณฑ์ทั้งสองฝั่งรองรับอย่างน้อยหนึ่งรูปแบบ พร้อมแสดง Authentication Flow และหลักฐานทางเทคนิคของผลิตภัณฑ์ทั้งสองฝั่ง

๖.๕.๑ กรณีใช้ Identity Broker หรือ Cloud Identity Service หรือระบบที่ไม่ได้ให้บริการ MFA โดยตรง ผู้ยื่นข้อเสนอต้องจัดหา External Identity Provider หรือ MFA Provider พร้อม License และ Technical Support ให้ครบถ้วน และต้องแสดงว่าโซลูชันโดยรวมสามารถรับคำขอยืนยันตัวตนจากระบบ PAM บังคับใช้ MFA และส่งผลการยืนยันตัวตนกลับไปยังระบบ PAM ได้

๖.๕.๒ มีเอกสารทางเทคนิคอย่างเป็นทางการยืนยันว่าผลิตภัณฑ์ทั้งสองฝั่งรองรับ Protocol และ Version ที่ใช้ร่วมกัน และผู้ยื่นข้อเสนอรับผิดชอบการติดตั้ง การตั้งค่า การทดสอบ และการแก้ไขปัญหาการทำงานร่วมกันให้ครบถ้วน

Proof

๖.๖ สามารถทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยเครือข่าย หรือระบบ VPN หรือระบบ Log Management/SIEM หรือระบบบริหารจัดการอื่นที่เกี่ยวข้องกับโครงการ โดยใช้ SAML 2.0 หรือ OpenID Connect/OAuth 2.0 หรือ RADIUS หรือ LDAP/LDAPS หรือ API หรือ Agent หรือ Connector ตามที่ผลิตภัณฑ์ต้นทางและผลิตภัณฑ์ปลายทางรองรับ

๖.๗ สามารถกำหนด Authentication Policy ตามเงื่อนไขอย่างน้อย ๒ ประเภทจากผู้ใช้งานหรือกลุ่มผู้ใช้งาน หรือระบบที่เข้าถึง หรืออุปกรณ์ หรือแหล่งที่มา หรือเครือข่าย หรือสถานที่ หรือช่วงเวลา หรือบริบท หรือระดับความเสี่ยง และสามารถกำหนดให้อนุญาตหรือปฏิเสธหรือเรียกใช้ MFA เพิ่มเติมตามนโยบายได้

๖.๘ สามารถบันทึกและตรวจสอบเหตุการณ์ที่เกี่ยวข้องกับการยืนยันตัวตนหรือการบริหารจัดการระบบ เช่น Authentication Event หรือ Audit Event หรือ Administrative Activity หรือ Configuration Change ตามความสามารถของผลิตภัณฑ์ที่เสนอ และสามารถส่งหรือเชื่อมโยงเหตุการณ์ดังกล่าวไปยังระบบ Log Management หรือ SIEM ของโครงการผ่าน Syslog หรือ API หรือ Connector หรือ Logging Service หรือวิธีการอื่นที่ผลิตภัณฑ์รองรับ

๖.๙ ระบบต้องรองรับการบริหารจัดการผ่าน Graphical User Interface หรือ Web-Based Management หรือ Management Console และสามารถกำหนดสิทธิ์ผู้ดูแลระบบตาม Role หรือ Policy ได้

๖.๑๐ กรณีติดตั้งระบบบนโครงสร้างพื้นฐานของโครงการ ผู้ยื่นข้อเสนอต้องรวมทรัพยากร CPU, Memory, Storage และ Network ที่จำเป็นไว้ในการคำนวณ Capacity Sizing และต้องจัดหา License, Subscription, Token, Agent, Connector หรือองค์ประกอบที่จำเป็นให้ครบถ้วนตามสถาปัตยกรรมที่เสนอ

๖.๑๑ จัดหา Software License หรือ Security Subscription รวมทั้ง User License หรือ MFA License หรือ Token License หรือ Agent หรือ Connector ตามที่จำเป็นสำหรับ Configuration ที่เสนอ พร้อม Technical Support ให้ครบถ้วนและต่อเนื่องไม่น้อยกว่า ๗๒ เดือน ทั้งนี้ ระยะเวลาการบริการให้รวมบริการในระยะที่ ๒

Proof

ภาคผนวก ๓
รายละเอียดข้อกำหนดบริการพื้นที่ศูนย์ข้อมูลและระบบโครงข่ายเชื่อมต่อ
(Colocation and Network Connectivity Requirements)

---

๑. บริการพื้นที่ศูนย์ข้อมูล (Data Center Colocation Service)

๑.๑ ผู้ยื่นข้อเสนอต้องเสนอการจัดหาบริการพื้นที่ศูนย์ข้อมูล (Colocation) สำหรับติดตั้งอุปกรณ์ของโครงการ ณ ศูนย์ข้อมูลหลักของ AIS, TRUE และ NT รวมทั้งศูนย์ข้อมูลสำรอง (Disaster Recovery Site: DR) โดยรวมค่าใช้จ่ายที่เกี่ยวข้องตลอดระยะเวลาการให้บริการไว้ในราคาเสนอ

๑.๒ ศูนย์ข้อมูลหลักของ AIS, TRUE และ NT ต้องจัดให้มีพื้นที่ติดตั้งอุปกรณ์แห่งละไม่น้อยกว่า 2 Full Rack โดยแต่ละ Rack มีขนาดไม่น้อยกว่า 42U และรองรับอุปกรณ์มาตรฐาน Rack Mount ขนาด ๑๙ นิ้ว

๑.๓ ศูนย์ข้อมูลสำรอง (DR) ต้องจัดให้มีพื้นที่ติดตั้งอุปกรณ์ไม่น้อยกว่า 4 Full Rack โดยแต่ละ Rack มีขนาดไม่น้อยกว่า 42U และรองรับอุปกรณ์มาตรฐาน Rack Mount ขนาด ๑๙ นิ้ว โดยแต่ละ Rack ต้องมีระบบจ่ายไฟแบบ Redundant จำนวนไม่น้อยกว่า ๒ เส้นทาง ได้แก่ Power Feed A และ Power Feed B ขนาดไม่น้อยกว่า 32 Ampere ต่อ Feed ต่อ Rack พร้อม Rack PDU และระบบระบายความร้อนที่เพียงพอต่ออุปกรณ์ที่ติดตั้ง

๑.๔ ศูนย์ข้อมูลต้องมีระบบไฟฟ้าสำรอง ระบบระบายความร้อน ระบบรักษาความปลอดภัยทางกายภาพ ระบบควบคุมการเข้าออก ระบบตรวจจับและป้องกันอัคคีภัย และองค์ประกอบพื้นฐานที่เหมาะสมสำหรับการให้บริการศูนย์ข้อมูลระดับองค์กร

๑.๕ ศูนย์ข้อมูลต้องได้รับการรับรองมาตรฐาน ISO/IEC 27001 หรือ ISO 22301 หรือฉบับที่เป็นปัจจุบัน และมีโครงสร้างพื้นฐานในระดับไม่น้อยกว่า Uptime Institute Tier III, TIA-942 Rated-3 หรือมาตรฐานสากลที่ให้ผลด้านความพร้อมใช้งานเทียบเท่า

๑.๖ ผู้ยื่นข้อเสนอต้องรวม Cross-connect, Internal Cabling, Patch Cord และองค์ประกอบที่จำเป็นสำหรับการเชื่อมต่ออุปกรณ์ภายในศูนย์ข้อมูลตามสถาปัตยกรรมที่เสนอไว้ในราคาเสนอให้ครบถ้วน

๒. บริการระบบโครงข่ายเชื่อมต่อ (Network Connectivity Service)

๒.๑ การเชื่อมต่อจากระบบต้นทางเข้าสู่ศูนย์ข้อมูลหลัก

๒.๑.๑ ผู้ยื่นข้อเสนอต้องเสนอวงจร MPLS จำนวนไม่น้อยกว่า 2 Links ต่อศูนย์ข้อมูลหลักของ AIS, TRUE และ NT สำหรับเชื่อมต่อระบบต้นทางเข้าสู่ศูนย์ข้อมูลหลัก โดยแต่ละ Link มี Bandwidth ไม่น้อยกว่า 1 Gbps.

Proof

๒.๑.๒ วงจรดังกล่าวต้องรองรับการทำงานแบบ High Availability โดยเมื่อ Link ใด Link หนึ่งขัดข้อง ระบบต้องสามารถรับส่งข้อมูลผ่าน Link ที่เหลือได้

๒.๒ การเชื่อมต่อระหว่างศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรอง

๒.๒.๑ ผู้ยื่นข้อเสนอต้องเสนอวงจรเชื่อมต่อระหว่างศูนย์ข้อมูลหลักของ AIS, TRUE และ NT ไปยังศูนย์ข้อมูลสำรอง โดยใช้ WDM หรือ MPLS จำนวนไม่น้อยกว่า 2 Links ต่อศูนย์ข้อมูลหลัก และแต่ละ Link มี Bandwidth ไม่น้อยกว่า 5 Gbps.

๒.๒.๒ วงจรดังกล่าวต้องรองรับการทำงานแบบ High Availability และรองรับการรับส่งข้อมูล การทำ Replication, Backup Copy และ Recovery ระหว่างศูนย์ข้อมูลหลักกับศูนย์ข้อมูลสำรองตามสถาปัตยกรรมที่เสนอ

๒.๓ ผู้ให้บริการระบบโครงข่ายต้องมีระบบตรวจสอบสถานะวงจรและช่องทางรับแจ้งเหตุ พร้อมให้บริการสนับสนุนด้านเทคนิคตลอด ๒๔ ชั่วโมง ๗ วัน

ทั้งนี้ ผู้ยื่นข้อเสนอต้องรวมค่าใช้จ่ายสำหรับพื้นที่ Rack, Power, Rack PDU, Cross-connect, Cabling, CPE/NTU/Router, Interface, Installation, MPLS, WDM/MPLS, Technical Support และค่าใช้จ่ายอื่นที่จำเป็นต่อการเปิดให้บริการระบบไว้ในราคาเสนอทั้งหมด หาก Configuration หรือสถาปัตยกรรมที่ผู้ยื่นข้อเสนอเลือกใช้จำเป็นต้องใช้พื้นที่ Rack ระบบไฟฟ้า หรือวงจรสื่อสารมากกว่าคุณลักษณะขั้นต่ำที่กำหนด ผู้ยื่นข้อเสนอต้องจัดหาเพิ่มเติมให้เพียงพอโดยรวมค่าใช้จ่ายไว้ในราคาเสนอ

Proof

ภาคผนวก ๔

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

(Data Processing Agreement : DPA) กับสำนักงาน กสทช.

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ("ข้อตกลง") นี้ จัดทำขึ้นเพื่อให้สอดคล้องกับหน้าที่ของสำนักงาน กสทช. และ ผู้ประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๔๐ วรรคสามและมาตรา ๓๗ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และข้อ ๖ ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และถือเป็นส่วนหนึ่งของการจัดจ้างโครงการบริหารจัดการการใช้งานข้อมูลเพื่อป้องกันอาชญากรรมกับประชาชน (U-DEX) ซึ่งสำนักงาน กสทช. มีฐานะเป็น "ผู้ควบคุมข้อมูลส่วนบุคคล" และผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล" ซึ่งเป็นผู้ดำเนินการเก็บ รวบรวม ใช้ หรือเปิดเผย ("ประมวลผล") ข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของสำนักงาน กสทช. โดยผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเพื่อวัตถุประสงค์ในการลงทะเบียนเข้าใช้งานศูนย์บริการ

๒. เพื่อดำเนินการตามวัตถุประสงค์ที่กำหนดไว้ในสัญญาหลักตามขอบเขตของงานในสัญญาหลัก

โดยข้อมูลส่วนบุคคลที่มีการประมวลผลตามวัตถุประสงค์ข้างต้น ประกอบด้วย

๑. ชื่อ นามสกุล ตำแหน่ง หมายเลขโทรศัพท์ e-Mail ลายมือชื่อ ของผู้เข้าร่วมการลงทะเบียนเข้าใช้งานศูนย์บริการ

๒. บันทึกไฟล์เสียงและคลิปวิดีโอการฝึกอบรมการใช้งานการลงทะเบียนเข้าใช้งานศูนย์บริการ

๓. ข้อมูลอื่นใดที่อาจมีความจำเป็นเพื่อให้บรรลุวัตถุประสงค์ตามขอบเขตงานในสัญญาหลัก

๔. ข้อมูลตามข้อ ๑. ถึงข้อ ๓. จะถูกจัดเก็บเอกสารในรูปแบบเอกสาร (Hard copy) และรูปแบบDigital File (Soft copy)

การควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่สำนักงาน กสทช. มอบหมายหรือแต่งตั้งให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการ ซึ่งจะต้องดำเนินการตามหน้าที่และความรับผิดชอบตามขอบเขตงานในบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก/ใบสั่งจ้าง (แล้วแต่กรณี) และดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชกฤษฎีกา ระเบียบ และประกาศ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงนี้ รวมเรียกว่า "กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล" ทั้งที่มีผลใช้บังคับอยู่นับแต่วันที่มีการทำสัญญาหลัก และ

ที่จะมีการแก้ไขเพิ่มเติมในภายหลัง โดยผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งต่อไปนี้เรียกว่า "ผู้ประมวลผลข้อมูลส่วนบุคคล" ต้องดำเนินงานตามสัญญาหลัก ในส่วนของข้อมูลตามที่กำหนดในวัตถุประสงค์ข้างต้น ให้เป็นไปตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

๑. ผู้ประมวลผลข้อมูลส่วนบุคคลรับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยจะดำเนินการตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

๒. ผู้ประมวลผลข้อมูลส่วนบุคคลจะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้จำกัดเฉพาะบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้เท่านั้น และจะดำเนินการเพื่อให้บุคคลดังกล่าวทำการประมวลผลและรักษาความลับของข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

๓. ผู้ประมวลผลข้อมูลส่วนบุคคลจะควบคุมดูแลให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของการดำเนินการตามขอบเขตงานในสัญญาหลัก หรือที่แก้ไขเพิ่มเติมในภายหลัง โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของขอบเขตงานในสัญญาหลัก หรือที่แก้ไขเพิ่มเติมในภายหลัง หรือ กฎหมายที่เกี่ยวข้องที่กำหนดไว้เป็นประการอื่น

๔. ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการเพื่อช่วยเหลือหรือสนับสนุนสำนักงาน กสทช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อสำนักงาน กสทช. อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตงานในสัญญาหลักในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรง ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่สำนักงาน กสทช. ทันที โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่เป็นผู้ตอบสนองต่อคำร้องดังกล่าว เว้นแต่สำนักงาน กสทช. จะได้มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเฉพาะเรื่องที่เกี่ยวข้องกับคำร้องดังกล่าว

๕. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลในขอบเขตงานในสัญญาหลักและจะดำเนินการส่งมอบบันทึกรายการดังกล่าวให้แก่สำนักงาน กสทช. ภายใน ๓๐ วันนับถัดจากวันลงนามในสัญญา หรือเมื่อสำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร

๖. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเหมาะสมทั้งมาตรการเชิงองค์กรและเชิงเทคนิค รวมถึงมาตรการทางกายภาพที่จำเป็นตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และตามประกาศสำนักงาน กสทช. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. รวมถึงที่ได้มีการแก้ไขเพิ่มเติมในอนาคต โดยคำนึงถึงระดับความเสี่ยงตามลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดในขอบเขตงานในสัญญาหลักเป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบ

Proof

จากเหตุการละเมิดข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือไม่ชอบด้วยกฎหมาย เป็นต้น โดยต้องจัดให้มีมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (Physical Measures) ที่จำเป็นด้วย โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบทสภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องส่งคืนข้อมูลส่วนบุคคลให้กับสำนักงาน กสทช. หรือดำเนินการลบ ทำลาย ยกเลิกการเข้าถึง หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้ ทั้งนี้ ตามที่สำนักงาน กสทช. กำหนดโดยทันทีเมื่อการดำเนินการประมวลผลตามวัตถุประสงค์ของขอบเขตงานใน สัญญาหลักเสร็จสิ้นลง โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องควบคุมดูแล ตรวจสอบ และรับรองว่าข้อมูลส่วนบุคคลดังกล่าวจะไม่อยู่ในความครอบครองของตนเองและของบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลอีกต่อไป

๘. เหตุแห่งการละเมิดข้อมูลส่วนบุคคล

๘.๑ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้ทราบหรือมีเหตุอันควรทราบว่ามีเหตุแห่งการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ภายใน ๒๔ ชั่วโมงนับแต่ทราบหรือมีเหตุอันควรทราบถึงเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการดังต่อไปนี้

(ก) ให้ข้อมูลที่จำเป็นแก่สำนักงาน กสทช. เพื่อให้สำนักงาน กสทช. สามารถปฏิบัติหน้าที่ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและทันตามระยะเวลาที่กฎหมายกำหนด เช่น ลักษณะของเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ประเภทและจำนวนโดยประมาณของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุแห่งการละเมิด และรายละเอียดของเจ้าของข้อมูลส่วนบุคคลดังกล่าวผลกระทบที่อาจเกิดขึ้นได้จากเหตุแห่งการละเมิด มาตรการที่ได้ดำเนินการแล้วหรือที่จะเสนอให้ดำเนินการ และมาตรการที่จะเยียวยาผลกระทบที่อาจเกิดขึ้นจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

(ข) ให้ความร่วมมืออย่างเต็มที่กับสำนักงาน กสทช. และดำเนินการใด ๆ ตามที่สำนักงาน กสทช. กำหนดเพื่อช่วยในการดำเนินการตรวจสอบ บรรเทา และเยียวยาความเสียหายอันเกิดจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

๘.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เปิดเผยเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่บุคคลอื่นใดทราบโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน เว้นแต่กรณีที่เป็นการปฏิบัติตามกฎหมาย

๘.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องชดใช้บรรดาค่าใช้จ่ายที่เกิดขึ้นจริงในการดำเนินการใด ๆเพื่อจัดการเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงาน กสทช. หากปรากฏว่าผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลช่วงที่อยู่ในความรับผิดชอบของตน เป็นผู้ก่อให้เกิดเหตุแห่งการละเมิดข้อมูลส่วนบุคคลดังกล่าวนั้น

Proof

๙. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

๙.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลรับรองและยืนยันว่าจะไม่ส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานในสัญญาหลัก ไปยังต่างประเทศโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช.

๙.๒ ในกรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. แล้ว ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานในบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก/ใบสั่งจ้าง (แล้วแต่กรณี) ไปยังต่างประเทศได้ ทั้งนี้ การส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลดังกล่าวจะต้องกระทำภายใต้บทบัญญัติของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งเป็นลายลักษณ์อักษรของสำนักงาน กสทช. เท่านั้น โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องเข้าทำข้อตกลงเพิ่มเติมหรือจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลบังคับใช้

๑๐. การให้บริการช่วง

๑๐.๑ ภายใต้หน้าที่และขอบเขตงานที่กำหนดในสัญญาหลักผู้ประมวลผลข้อมูลส่วนบุคคล ไม่สามารถว่าจ้างหรือแต่งตั้งบุคคลภายนอกเป็นผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเพื่อทำการประมวลผลข้อมูลส่วนบุคคลตามขอบเขตงานในสัญญาหลักในนามของสำนักงาน กสทช. ได้ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน

๑๐.๒ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับอนุญาตให้สามารถว่าจ้างผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ตามข้อ ๑๐.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเป็นลายลักษณ์อักษร โดยกำหนดขอบเขตเนื้อหาและหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงให้สอดคล้องกับหน้าที่และความรับผิดชอบของ ผู้ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้

ในกรณีที่สำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตรวจสอบการปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับจากสำนักงาน กสทช. และจัดทำผลการตรวจสอบ รวมทั้งส่งมอบผลการตรวจสอบให้แก่สำนักงาน กสทช. ในกรณีที่ปรากฏว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงไม่ปฏิบัติตามหรือมีเหตุอันควรเชื่อว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงอาจไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรืออาจก่อให้เกิดความเสียหายต่อสำนักงาน กสทช. ไม่ว่าในกรณีใด ๆ สำนักงาน กสทช. อาจขอให้ผู้ประมวลผลข้อมูลส่วนบุคคลเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ทันที โดยสำนักงาน กสทช. ไม่ต้องรับผิดในความเสียหายหรือค่าใช้จ่ายใด ๆ อันเกิดจากการเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

๑๑. การตรวจสอบ

๑๑.๑ ในกรณีที่สำนักงาน กสทช. มีการร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการส่งมอบข้อมูลที่จำเป็นทั้งหมดให้แก่สำนักงาน กสทช. เพื่อเป็นการปฏิบัติหน้าที่ตามข้อตกลงนี้

๑๑.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงอนุญาตให้สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. เข้าตรวจสอบการปฏิบัติหน้าที่ของ ผู้ประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ โดยสำนักงาน กสทช. จะแจ้งให้ ผู้ประมวลผลข้อมูลส่วนบุคคลทราบล่วงหน้าเป็นลายลักษณ์อักษรไม่น้อยกว่า ๗ วัน และ ผู้ประมวลผลข้อมูลส่วนบุคคล

Proof

ตกลงให้ความร่วมมือแก่สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. ในการเข้าตรวจสอบดังกล่าวข้างต้น

๑๒. การชดใช้และการเยียวยา

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องชดใช้ค่าเสียหายหรือค่าใช้จ่ายใด ๆ ให้แก่สำนักงาน กสทช. ในกรณีที่เกิดความเสียหาย การสูญหาย การเรียกร้องค่าเสียหาย ความรับผิดทางแพ่ง โทษปรับทางปกครอง หรือค่าใช้จ่ายใด ๆ ที่เกิดขึ้นต่อบุคคลภายนอก หรือในกรณีที่สำนักงาน กสทช. จะต้องรับผิดอันเนื่องมาจากการไม่ปฏิบัติตามข้อใดข้อหนึ่งภายใต้ข้อตกลงนี้หรือตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือการละเมิดคำรับรองและรับประกันของผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่ได้รับมอบหมายจากผู้ประมวลผลข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคล ผู้รับจ้างช่วง ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง หรือตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคล

๑๓. การบอกกล่าว

บรรดาคำบอกกล่าวหรือการติดต่อสื่อสารใด ๆ ตามข้อตกลงนี้ ให้ทำเป็นลายลักษณ์อักษร โดยให้ส่งโดยบุคคล หรือไปรษณีย์ หรือโทรสาร ไปยังสถานที่ของผู้รับตามที่ระบุไว้ในข้อตกลงนี้ หรือตามที่ได้รับแจ้งเปลี่ยนแปลงจากผู้รับ (ถ้ามี) คำบอกกล่าวหรือการติดต่อสื่อสารทั้งหลายจะถือว่าผู้รับได้รับแล้ว เมื่อคำบอกกล่าวหรือการติดต่อสื่อสารนั้นไปถึงสถานที่นั้นแล้ว

๑๔. หน้าที่และความรับผิดของ ผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามข้อตกลงนี้จะสิ้นสุดลงนับแต่วันที่การปฏิบัติงานตามขอบเขตงานในสัญญาหลักเสร็จสิ้น หรือวันที่ผู้ประมวลผลข้อมูลส่วนบุคคลและสำนักงาน กสทช. ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกการดำเนินการตามขอบเขตงานนี้ แล้วแต่กรณีใดจะเกิดขึ้นก่อน โดยคู่สัญญาตกลงจะไม่โอนสิทธิเรียกร้องตามข้อตกลงนี้ให้แก่บุคคลอื่น

Proof